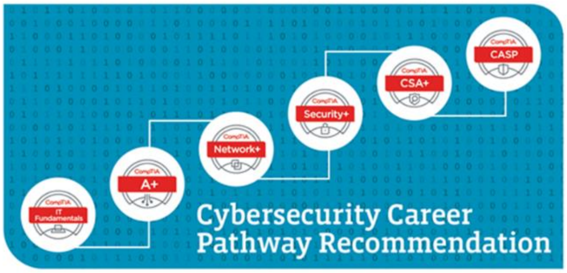
Introduction

- **Exam Foundations**
  - **CompTIA Cybersecurity Analyst**
    - CompTIA Cybersecurity Analyst (CSA+) is an international, vendor-neutral cybersecurity certification that applies behavioral analytics to improve the overall state of IT security. CSA+ validates critical knowledge and skills that are required to prevent, detect and combat cybersecurity threats.

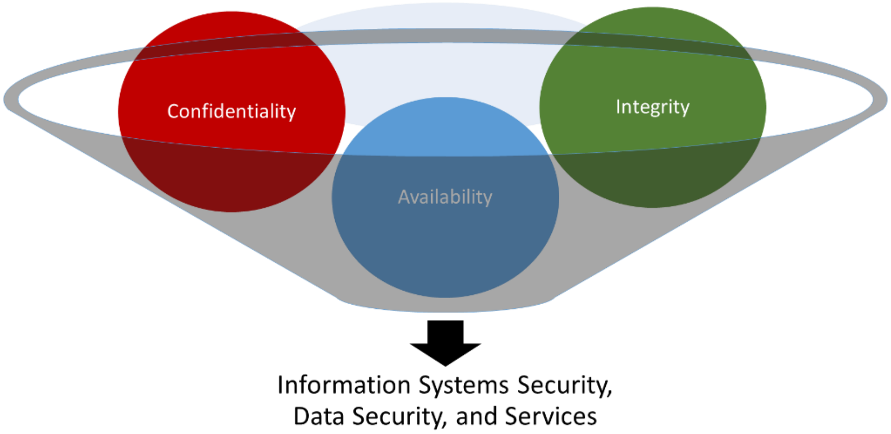
      -CompTIA.org
  - **Exam Description**
    - **CompTIA Cybersecurity Analyst (CSA+) covers:**
      - Configuration and use threat detection tools
      - Performing data analysis and interpretation of the results to identify vulnerabilities, threats and risks to an organization
      - Securing and protecting applications and systems
  - **The Four Domains**
    - Threat Management (27%)
    - Vulnerability Management (26%)
    - Cyber Incident Response (23%)
    - Security Architecture and Tool Sets (24%)
  - **Exam Details**
    - Up to 85 questions in 165 minutes
    - Requires a 750 out of 900 (83.33%)
    - Recommended Experience:
      - CompTIA Network+ and/or Security+
      - 3-4 years of hands-on InfoSec
    - Cost: $320 (US Dollars)
    - Released: February 15, 2017
  - **Cybersecurity Career Path**



Enter where it makes sense for you.
Consider your experience and existing certifications or course of study.

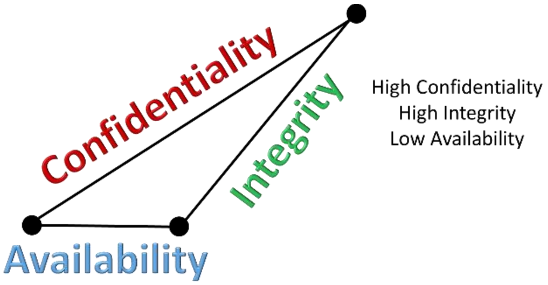
Domain 1: Threat Management

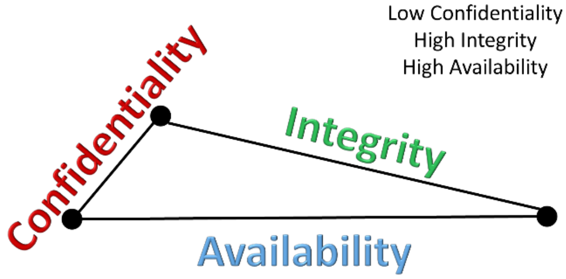
- **Intro to Threat Management**
  - **What does this section cover?**
    - Identification of threats to your cybersecurity posture
    - Methods to secure your networks
    - Understanding of response and countermeasures
    - Threats, Vulnerabilities, and Risk
    - Footprinting and Reconnaissance
  - **Overview of Threat Management**
    - Threats to Confidentiality, Integrity, and Availability of your organization
    - Coverage of the controls used to secure our networks and endpoints
    - Evaluation of the security of controls
    - Information gathering (passive and active reconnaissance and footprinting)
- **Security Triad (CIA)**
  - **COMPONENTS OF SECURITY (CIA)**

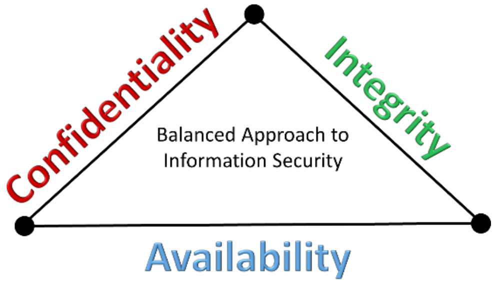


  - **CONFIDENTIALITY**
    - How secure is the information?
    - How secure does the data need to be?
    - Best methods
      - Physical Protections
        - Locked doors, fences, security guards, security cameras, safes, …
    - Electronic Protections
      - Encryption (storage and in transit), passwords, firewalls, two-factor authentication, …
    - Failure of confidentiality occurs if someone can obtain and view the data

- **INTEGRITY**
  - How correct is the information?
  - Has the data been modified during retrieval, in transit, or in storage?
  - Best methods
    - Hashing of files and information
    - Checksums during data transmission
  - Failure of integrity occurs if someone modifies the data being stored or when it is in transit
- **AVAILABILITY**
  - How much uptime is the system providing?
  - Is the data accessible by users at all times?
  - Best methods
    - Redundancy in the system design, including components and data paths
    - Backup strategies and disaster recovery plan
  - Failure of availability occurs if the data cannot be accessed by the end user
- **APPROACHES TO THE SECURITY**

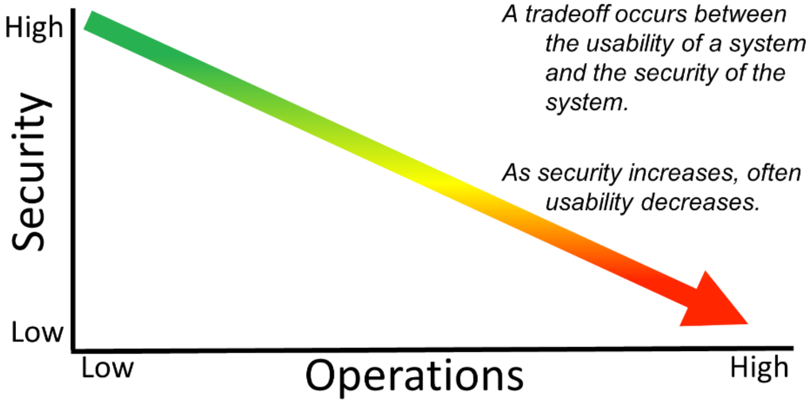






- **IMPORTANCE OF CIA TRIAD**
  - Cybersecurity analysts characterize risks, attacks, and security controls by assigning them to one or more of the CIA goals

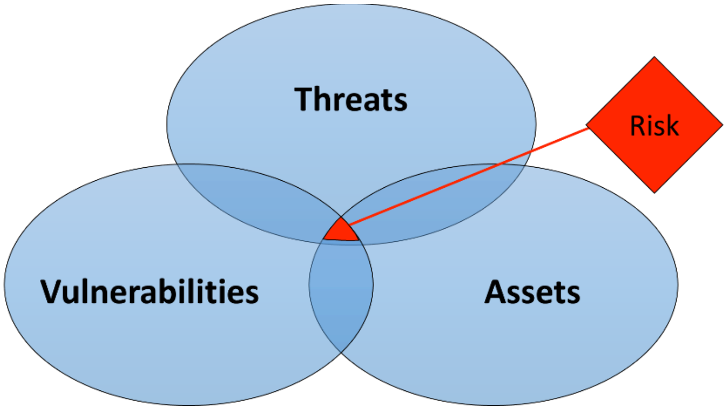
- **SECURITY VS OPERATIONS**



A tradeoff occurs between the usability of a system and the security of the system.

As security increases, often usability decreases.

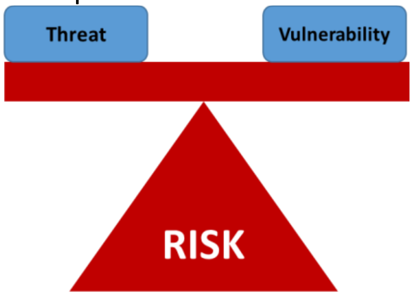
- **Risk Considerations**
  - **WHERE RISK EXISTS…**



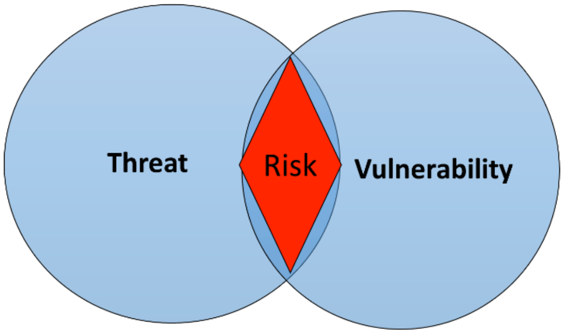
  - **ASSETS**
    - Any item that has a value to the organization
    - Examples:
      - Information or Data
      - Network Equipment
      - Servers/Computers
      - Software
      - Personnel
      - Processes
  - **VULNERABILITY**
    - Any weakness in the system design, implementation, software code, or lack of preventative mechanisms
    - Examples:
      - Software bugs
      - Misconfigured software
      - Misconfigured network devices

            - Improper physical security
    - **VULNERABILITIES**
        - Cybersecurity professionals control vulnerabilities
        - Vulnerabilities are internal factors
    - **THREAT**
        - Any condition that can cause harm, loss, damage, or compromise of an asset
        - Examples:
            - Natural Disasters
            - Cyber Attacks
            - Breach of integrity of data
            - Disclosure of confidential data
            - Malware
    - **THREATS**
        - Cybersecurity professionals cannot control threats, but they can be mitigated
        - Threats are external factors
    - **RISK**
        - Probability (or likelihood) of the realization of a threat
        - Vulnerability without a threat equates to no risk…

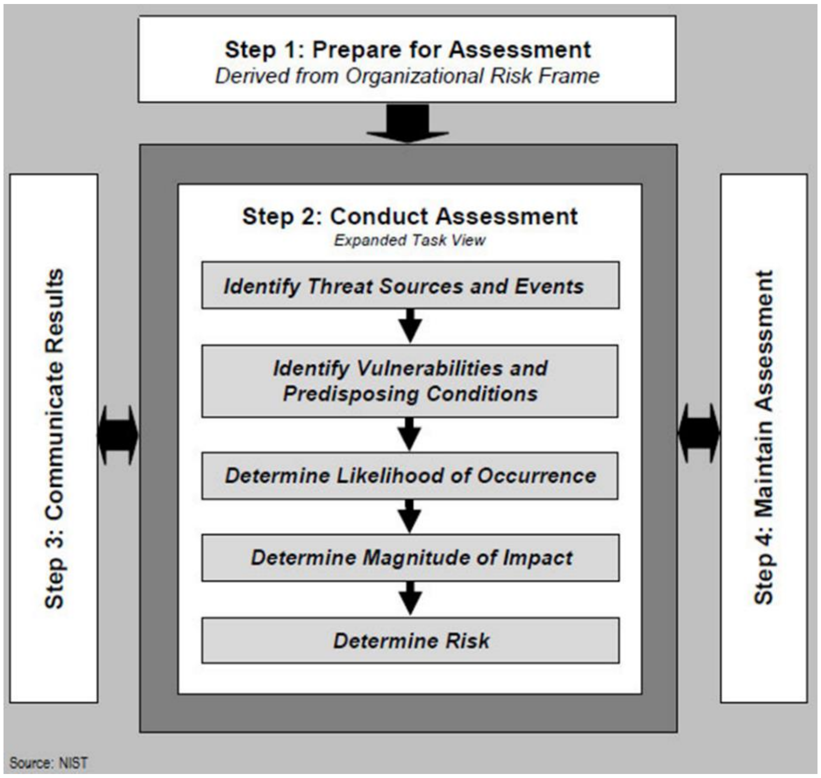
RISK = Vulnerability X Threat



- **Risk Assessment**
    - **WHERE RISK EXISTS…**



- **RISK ASSESSMENTS**
    - Organizations should conduct routine risk assessments
    - Risk assessments measure your current level of risk based on threats, vulnerabilities, and mitigations in place
    - National Institute of Standards and Technology (NIST) publishes NIST Special Publication 800-30 as a foundation for risk assessments
- **NIST SP 800-30**


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Source: NIST

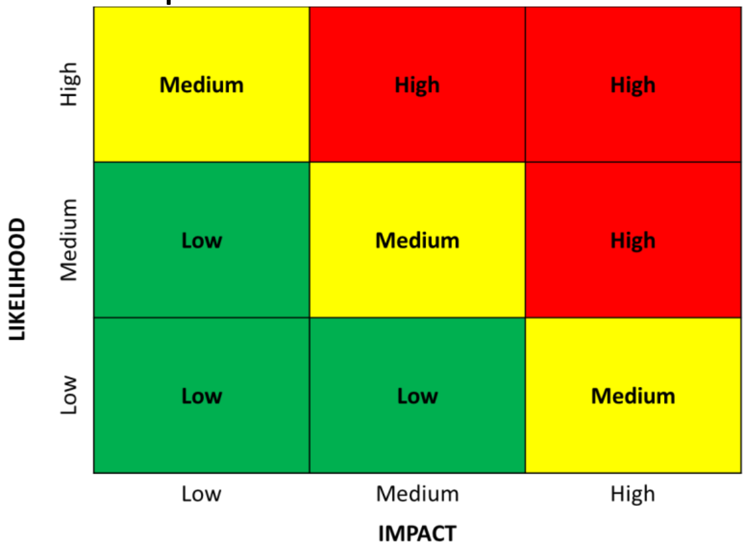
- **Identify Threats**
    - **Identify Threats**
        - Adversarial Threats
        - Accidental Threats
        - Structural Threats
        - Environmental Threats
    - **Adversarial Threats**
        - Consider their capability, intent, and likelihood
        - Examples:
            - Trusted insiders
            - Competitors
            - Suppliers
            - Customers
            - Business partners

            - Nation states
    - **Accidental Threats**
        - Occurs when someone makes a mistake that hurts the security of the system
        - Example:
            - System administrator accidently takes servers offline causing loss of availability
            - Amazon Web Services (Feb 2017)
                - Technician utilized a SOP to take a small number of servers offline, but input the command incorrectly
                - Caused a large number of servers to go offline
                - It took down the entire US-EAST-1 region!
                - https://aws.amazon.com/message/41926/
    - **Structural Threats**
        - Occurs when equipment, software, or environmental controls fail
        - Example:
            - IT server fails due to hard drive failure
            - Servers fail due to overheating (HVAC fail)
            - Software failure (OS bug or crash)
    - **Environmental Threats**
        - Occurs when natural or man-made disasters occur
        - Example:
            - Fires
            - Flooding
            - Severe storms
            - Loss of power from the city power grid
            - Fiber or telecommunication lines cut
    - **Always Remember…**
        - Threats come from both external and internal sources, but most risk assessors think of internal sources first…
        - We aren't just worried about hackers, but also the trusted insider…
        - As you design security controls, don't forget to think about disgruntled employees, inept administrators, or the insider threat!
    - **Best Practices**
        - It can be helpful to get copies of a similar organization's risk assessment to use as a baseline for your own organization
        - Conduct quality assessment checks throughout the process to ensure you stay on track

- **Identify Vulnerabilities**
  - **Identify Vulnerabilities**
    - During the identification of threats, we generally look external to the organization, but...
    - Identifying vulnerabilities focuses on internal factors
    - Our focus it to match up vulnerabilities to the threats identified
  - **Always Remember…**
    - If you have a threat without a vulnerability, it isn't a risk.
      - Threat
        - Hackers are using a zero-day exploit against Windows XP systems
      - Vulnerability
        - We don't use Windows XP systems
      - Risk
        - NONE
    - If you have a vulnerability without a threat, it isn't a risk.
      - Threat
        - Hackers haven't found any exploitable coding errors
      - Vulnerability
        - Unpatched operating system software
      - Risk
        - NONE
- **Likelihood, Impact, and Risk**
  - **Likelihood and Impact**
    - Measurement of the risk that the combined threat and vulnerability pose is based on the likelihood and impact
    - Likelihood is the chance that the risk will be realized
    - Impact is the severity of damage that occurs if the risk is realized
  - **Likelihood Factors**
    - What is the likelihood that the threat will initiate the risk?
      - Example: How likely is it that the hacker attacks us?
    - What is the likelihood that if the risk occurs it will have a bad impact for us?
      - Example: If the organization has proper security controls, the threat may be mitigated with no adverse effects to the organization.
    - Likelihood is qualitative
      - Low, Medium, High
  - **Impact**
    - Always assume the threat takes place and the risk is realized when measuring

    - Identify the severity of the impact
    - Consider each of the pieces of CIA triad: confidentiality, integrity, and availability
    - Impact is qualitative
      - Low, Medium, High

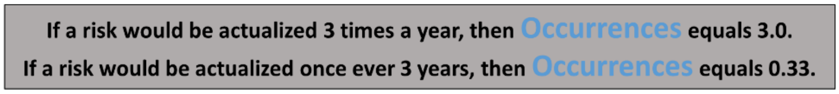
- **Qualitative and Quantitative Assessments**
  - **Qualitative vs Quantitative**
    - Qualitative measurement is subjective
    - Quantitative is based on numbers
    - For the CompTIA CSA+ exam, you do not need to understand quantitative assessments, but they are covered on exams like CASP and CISSP.
  - **Qualitative Example**



LIKELIHOOD \ IMPACT	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

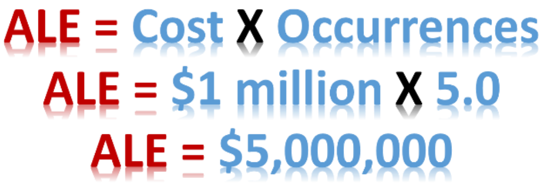
  - **ANNUAL LOSS EXPECTANCY (ALE)**
    - Common calculation to determine the cost associated with risk
    - Aids in determining when to accept, avoid, transfer, or mitigate the risk

ALE = Cost X Occurrences



If a risk would be actualized 3 times a year, then Occurrences equals 3.0.

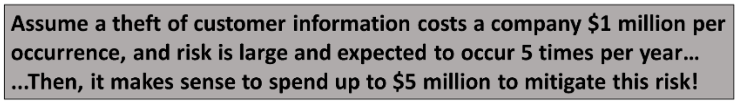
If a risk would be actualized once ever 3 years, then Occurrences equals 0.33.



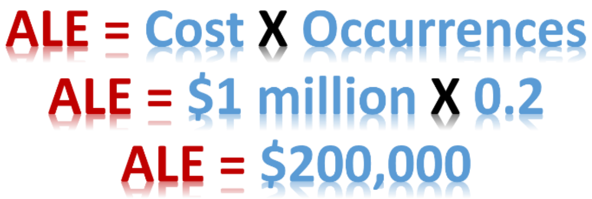
ALE = Cost X Occurrences

ALE = $1 million X 5.0

ALE = $5,000,000



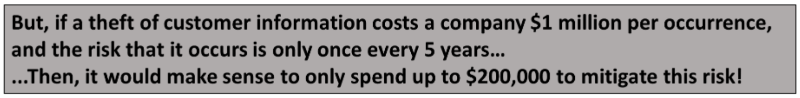
Assume a theft of customer information costs a company $1 million per occurrence, and risk is large and expected to occur 5 times per year…
…Then, it makes sense to spend up to $5 million to mitigate this risk!



ALE = Cost X Occurrences

ALE = $1 million X 0.2

ALE = $200,000



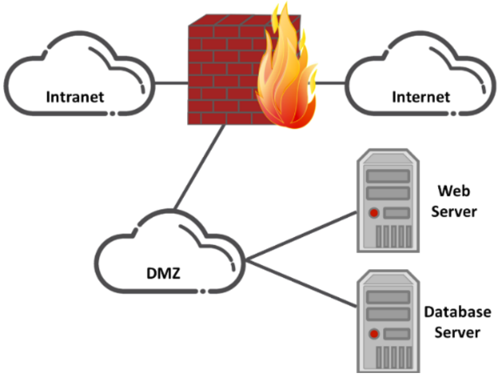
But, if a theft of customer information costs a company $1 million per occurrence, and the risk that it occurs is only once every 5 years…
…Then, it would make sense to only spend up to $200,000 to mitigate this risk!

**** If it costs >$200,000 to mitigate, just accept the risk and pay $200k each time ****

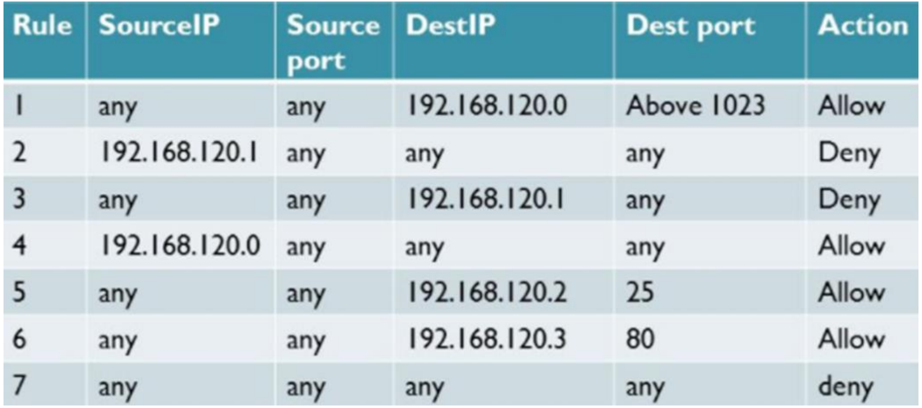
- **Risk Controls and Mitigations**
  - **Risk Controls**
    - Cybersecurity professionals work to minimize risk to the organization through risk management and controls
    - Four ways to handle risk:
      - Risk Acceptance
      - Risk Avoidance
      - Risk Mitigation
      - Risk Transference
  - **RISK ACCEPTANCE**
    - Organization accepts the risk associated with a system's vulnerabilities and their associated risks
    - Risk acceptance is common when the risk is low enough to not apply countermeasures, or adequate countermeasures have already been applied
  - **RISK AVOIDANCE**
    - Risk is too high to accept, so the system configuration or design is changed to avoid the risk associated with a specific vulnerability
    - Example:
      - Utilizing Windows XP is too dangerous, so we install Windows 10 instead to avoid the risk of an unsupported operating system

- **RISK MITIGATION**
  - Main goal of security is to minimize risk to a level acceptable to the organization
  - Our goal is not necessarily to eliminate all risks…
  - By adding risk controls, we can mitigate the risk down to an acceptable level
- **RISK TRANSFERENCE**
  - If the organization cannot afford to accept, avoid, or mitigate the risk, they can transfer the risk to another business
  - Example:
    - If the organization is concerned that it would be too costly to recover from a flood, they can purchase flood insurance
- **RISK CONTROLS**
  - Technical controls
    - Systems, devices, software, and settings used to enforce CIA requirements
    - Examples
      - Using firewalls, IDS, and IPS
      - Installing antivirus and endpoint security
  - Operational controls
    - Practices and procedures to increase security
    - Examples
      - Conducting penetration tests
      - Utilizing standard operating procedures

- **Network Perimeter Security**
  - **Firewalls**
    - Most common network perimeter security
    - Firewalls are at network boundaries
    - Generally, setup as triple-homed devices
      - Internet, DMZ, and intranet
  - **Triple-Homed Firewalls**



- **Demilitarized Zone (DMZ)**
  - Special network zone hosting servers that gets traffic from the internet
  - Acts as a semi-trusted zone
- **Access Control List (ACL)**
  - All traffic passing through the firewall is checked against the ACL
  - ACL contains rules to define what traffic can pass through the firewall
- **Access Control List (ACL)**
  - Firewall should be denied by default
    - If no rule says allowed, traffic is denied



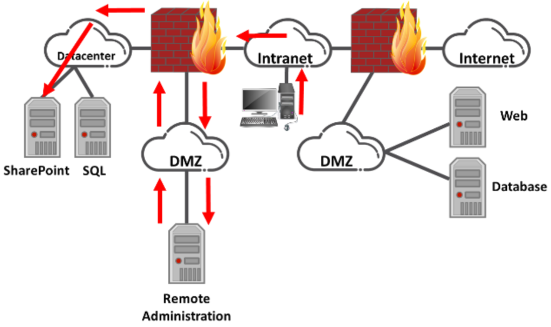
Rule	SourceIP	Source port	DestIP	Dest port	Action
1	any	any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	any	any	any	Deny
3	any	any	192.168.120.1	any	Deny
4	192.168.120.0	any	any	any	Allow
5	any	any	192.168.120.2	25	Allow
6	any	any	192.168.120.3	80	Allow
7	any	any	any	any	deny

- **Firewall Types**
  - Packet Filtering
    - Check each packet against rules for IP and port
  - Stateful Inspection
    - Maintains information about the state of each connection (basic firewalls sold today)
  - Next-Generation (NGFWs)
    - Uses contextual information about users, apps, and processes to make decisions
  - Web Application (WAFs)
    - Protects against web application attacks like SQL injection and Cross-site Scripting (SQL/XSS)

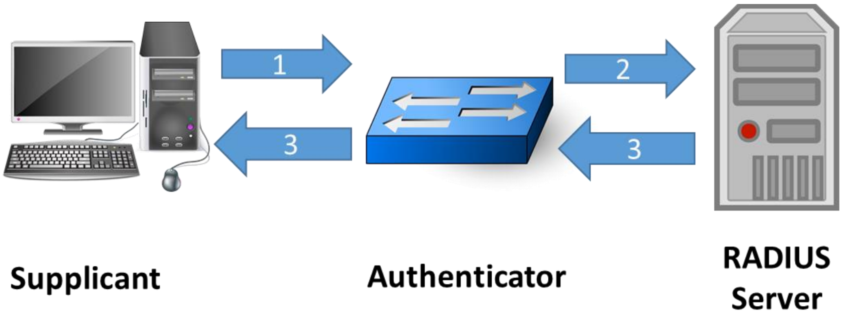
- **Common TCP Ports**

Port	Service
20, 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
69	TFTP
80	HTTP
110	POP3
123	NTP
143	IMAP
161	SNMP
389	LDAP
443	HTTPS
1433	SQL Server
1521	Oracle
1720	H.323
1723	PPTP
3389	RDP

- **Network Segmentation**
  - **Network Segmentation**
    - Separates networks of different security levels from each other
    - Much like we did intranet, internet, and DMZ
    - We apply the same principles to break apart our large networks into more secure enclaves



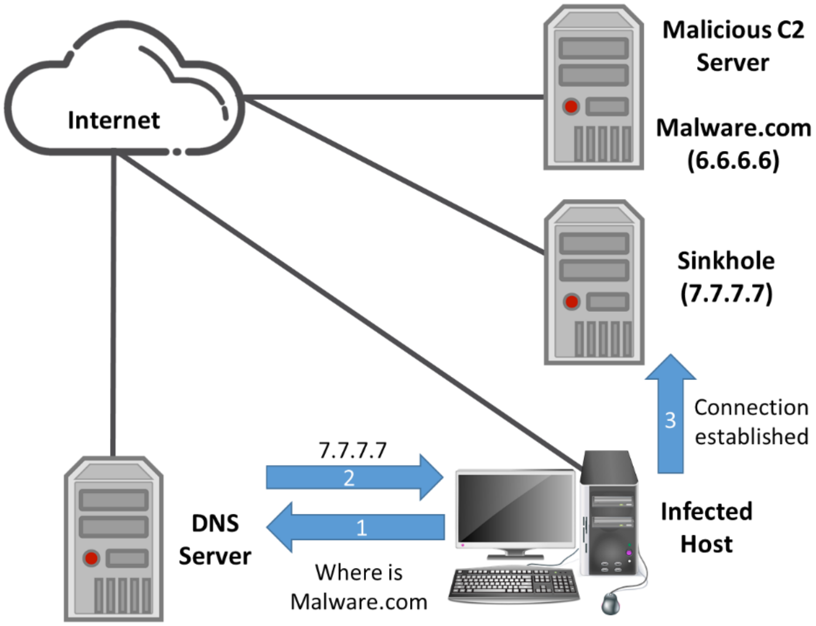
- **Network Access Control**
  - **Network Access Control (NAC)**
    - Limits network access to only authorized individuals and systems
    - Ensures the systems connecting to the network meet basic security requirements
  - **802.1x**
    - 802.1x protocol is most common standard utilized for NAC
    - Works for wired and wireless networks



  - **Agent-based and Agentless**
    - Agent-based
      - Requires the device requesting access to have special software to communicate with NAC service (such as 802.1x)
    - Agentless
      - NAC authentication is conducted in a web browser and doesn't need special software (such as Wireless at a hotel)
  - **In-Band and Out-of-Band**
    - In-Band
      - Uses dedicated appliances placed between the devices and the services they are requesting
      - Example: Hotel networks that require you to enter your name and room number before gaining access
    - Out-of-Band
      - Relies on existing network and has device communicate to authentication servers (like 802.1x)
  - **NAC Approval Criteria**
    - Time of Day
    - Role of the user
      - Admins can access datacenter only when inside datacenter
    - Location of the user
      - User must be in datacenter to access
    - System health status

        - Anti-virus up to date, security patches installed, host firewall enabled, etc.

- **Defense Deception Methods**
    - **Defense Deception Methods**
        - Cybersecurity professionals may want to go beyond just standard defense and attempt to lure an attacker to specific targets
            - Examples:
                - Honeypots
                - DNS Sinkholes
    - **Honeypot**
        - System designed to look like a lucrative target due to the types of services being run or vulnerabilities contained
        - In reality, honeypots are designed to falsely appear vulnerable and to fool malicious attackers to waste time going after them
        - They simulate successful attacks and allow us to monitor attacker techniques
    - **DNS Sinkhole**
        - Provide false DNS information to malicious software
        - Compromised system requests DNS information from the server, but the server detects the suspicious request and gives the IP address of the sinkhole instead of the real Command and Control server

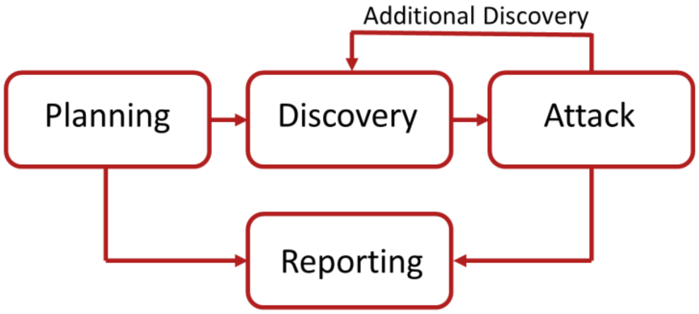


- **Secure Endpoint Management**
    - **Secure Endpoint Management**
        - Hardening System Configurations

        - Patch Management
        - Compensating Controls
        - Group Policies
        - Endpoint Security Software
    - **Hardening System Configurations**
        - Hardening a system makes it as resistant to attack as possible
        - Examples:
            - Disabling unnecessary services
            - Disabling unnecessary ports
            - Verifying secure configurations
            - Centrally controlling device security settings
    - **Patch Management**
        - Once a patch is released by the vendor, attackers begin to reverse engineer it
        - Organizations must ensure proper patch management to prevent attacks
        - Examples:
            - Microsoft System Center Configuration Manager (SCCM)
    - **Compensating Controls**
        - If you can't implement a security control, you can compensate for it
        - Provides a similar level of security by using an alternate means
        - Examples:
            - WannaCry outbreak required disabling SMBv1, but this could break an file share
            - Point-of-Sale or embedded systems can't be updated without possibility of breaking
    - **Group Policy Objects (GPO)**
        - Provides admins an efficient way to manage system and security configuration settings across many devices in a network
        - Examples:
            - Require the use a firewall on all hosts
            - Mapping to a share drive on login
            - Run scripts at login to verify compliance
    - **Endpoint Security Software**
        - Specialized software to enforce the company's security objectives/policies
        - This software should report to a centralized management system for cyber security analysts to view and analyze
        - Examples:
            - Antivirus or anti-malware
            - Host-based IDS or IPS

- **Going the Extra Mile…**
  - Mandatory Access Control (MAC) sets all security permissions centrally and the users cannot change permissions locally
  - Discretionary Access Control (DAC) allows the owners of a file or resource to control the permissions on that resource
  - MAC has great security, but is an administration nightmare…only used in very sensitive environments (SE Linux)

- **Penetration Testing**
  - **Penetration Testing (PenTest)**
    - Penetration testers simulate a cyber-attack against your organization's resources using the same information, tools, and techniques available to an attacker
    - Goal:
      - To gain access to your systems and report the findings to management
  - **Who can do the PenTest?**
    - Can be performed by internal staff or external consultants
    - Requires highly skilled individuals
    - Tests are very time consuming and costly
  - **Phases of a PenTest**



NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) divides PenTests into four phases

  - **Planning**
    - An important phase of a PenTest
    - No technical work is performed
    - Timing, Scope, and Authorization is gained during the Planning Phase
    - You should NEVER conduct a PenTest without authorization…it's illegal!
  - **Discovery**
    - Testers conduct reconnaissance and gather as much information on the network, system, users, and applications

            - Examples:
                - Open source research
                - Port scanning
                - Enumeration
                - Vulnerability scanning
                - Web application scanning
        - **Execute the Attack**
            - Seeks to bypass the security controls and gain access to the system
            - Attack Phase (aka Exploitation)
                - Gaining Access
                - Escalating Privileges
                - System Browsing
                    - May refer back to discovery phase again
                - Installing Additional Tools

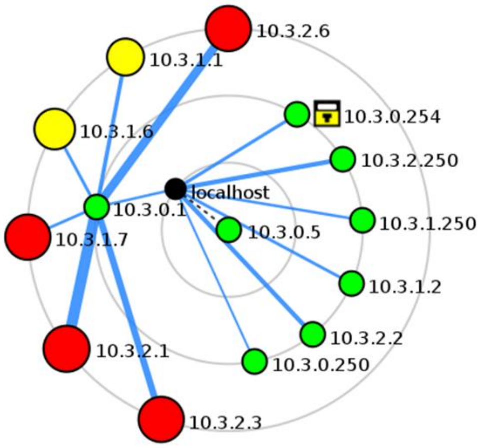
Source: NIST SP 800-115

    - **Reporting**
        - Testers should prepare a detailed report after the test
        - Contains results of the PenTest, describing their successful attacks and suggestions on how to fix them
        - Should be prioritized based on the risk posed by each vulnerability exploited
- **Security Exercises and Training**
    - **Beyond a PenTest**
        - Security exercises can put penetration testers and defenders against each other to provide additional training
        - Performed in a simulated environment…not production network
        - Conducted by three types of teams: Red, Blue, and White
    - **Red Team**
        - Participates as the attacker
        - Uses reconnaissance and exploitation tools to gain access to the network
        - Similar to penetration testers
    - **Blue Team**
        - Participates as the defender
        - Secures the network and attempts to keep red team out through the use of security controls
        - Usually made up of system and network administrators
    - **White Team**
        - Participates as the referee
        - Coordinates the exercise and arbitrates disputes
        - Maintains the simulated environment and monitors the exercise

- **Reverse Engineering**
  - **Reverse Engineering**
    - Malware authors do not explain how their software works
    - Reverse engineering is a technique to take a finished product and understand its inner workings through decomposition
    - Conducted through dynamic or static analysis
  - **Dynamic Analysis**
    - Malware is placed in a sandbox and its behavior observed on the system and the virtual network
    - Automated solutions can do this in near real-time, where email attachments are launched and automatically analyzed for malicious activity
  - **Static Analysis: Software**
    - Analysis of the code of the malware
      - For Ruby and Python, the code is readable because they are interpreted languages
      - For C/C++ and Java, code is compiled into binary
    - Static analysis of compiled code requires a decompiler or analysis in binary format
  - **Reverse Engineering Hardware**
    - Very difficult to perform due to embedded software in firmware
    - Most often, dynamic analysis is conducted on hardware
    - *Hardware should be purchased from a trusted supplier to minimize the risk of malware being inserted into the firmware of hardware devices during procurement and shipment to your company*
- **Reconnaissance and Intelligence**
  - Reconnaissance and Intelligence
    - Gathering of information to better understand the security landscape
    - Some security standards and laws, such as the PCI-DSS standard, require information gathering from inside and outside your network to ensure compliance through vulnerability scans performed quarterly
    - Numerous tools and techniques for conducting this discovery
- **Footprinting the Network**
  - **Footprinting the Network**
    - Creates a map of the network, systems, and other infrastructure of the company
    - Created using a mixture of information gathering tools and manual research
    - Guidance can be found in the NIST SP 800-115 and the Open Source Security Testing Methodology Manual (OSSTMM)

- **Active Reconnaissance**
    - Utilizes host scanning tools to gather information about systems, services, and vulnerabilities in the network
    - Does not include exploitation of the vulnerabilities, only identification of them
    - Permission should be sought out before conducting active reconnaissance because it could be construed as an attack by mistake

- **Network Mapping**
    - **Network Mapping**
        - Network mapping tools used during active reconnaissance can approximate the network by using
            - Time to live (TTL)
            - Traceroute information
            - Other responses from the network devices
        - Zenmap and nmap are useful for conducting network mapping
    - **Network Mapping (Zenmap)**

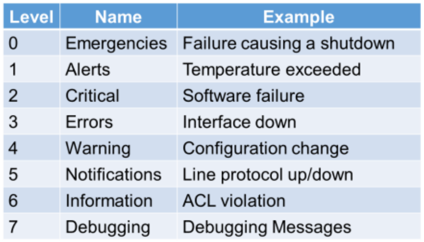


- **Network Mapping Challenges**
    - Firewalls and Layer 3 Switch ACLs can make it difficult to map a network fully
    - Wireless networks are also a challenge
    - Virtualized networks and infrastructure
    - Cloud services

- **Port Scanning**
    - **Port Scanning**
        - Most common method to gather information on a network and devices
        - Port scanners perform:
        - Host discovery
        - Port scanning and service identification

        - Service Version identification
        - Operating System Identification
        - Port scanners also used for network inventory tasks and security audits
    - **Service Scanning (Zenmap)**
        - Service identification attempts to identify the service and its version through banner grabbing or comparing TCP/UDP packet responses to known signatures
    - **OS Scanning (Zenmap)**
        - OS fingerprinting uses TCP/IP stack responses from the TCP and UDP packets sent to identify Windows, Linux, or OSX, and if possible, the version
    - **Importance of Port Numbers**
        - Well-known ports (0-1023)
        - Registered ports (1024-49151)
    - **Where you scan from matters…**
        - Internal scans will see more information than an external scan
        - If you are trying to simulate a cyber-attack during a PenTest, you should be scanning from the outside the network to match the attacker's perspective
- **Other Port Scanners**
    - **Angry IP Scanner**
        - Multiplatform (Windows, Linux, MacOS)
        - Graphical port scanner
        - Doesn't provide service or OS information by default
            - Must use "fetchers" to get more details
        - Well-known, but not as full featured as nmap or Zenmap
    - **Other Port Scanners**
        - Many other port scanners exist
        - Metasploit built-in scanners
        - Qualys Vulnerability Management
        - Tenable's Nessus Vulnerability Scanner
        - You can even write your own in a language like Python!
- **Passive Reconnaissance**
    - **Passive Reconnaissance**
        - More difficult than active reconnaissance
        - Relies on logs and other data
        - Data you receive may be out of date
        - Often used during a cyber incident response
    - **Log and Configuration Analysis**
        - Local system configuration data and log files can be used to build a network map

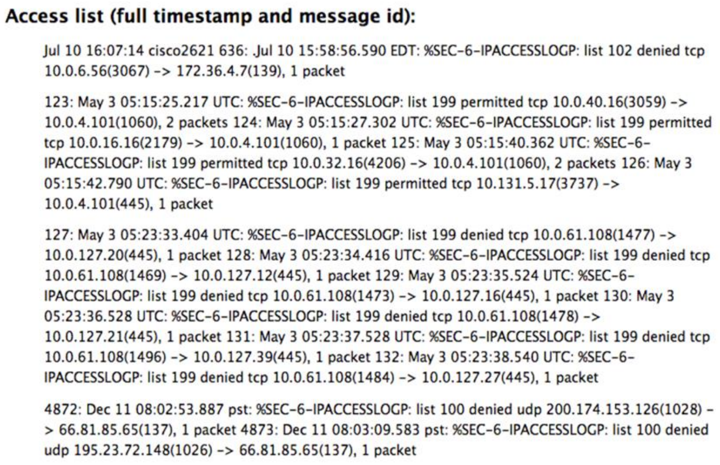
        - Some tools exist to parse configuration files into a usable topology
        - Much of this is done manually, though
- **Passive Recon: Network Devices**
    - **Network Devices**
        - Network devices log many activities, their status, and events
        - Includes traffic patterns and utilization
        - Logs files, configuration files, and network flows are great for passive recon
    - **Logs Files**
        - Network devices send their logs to the display console (only logged in user sees them) by default
        - You should configure them to send logs to centralized logging server (SYSLOG) or use SNMP to send the information
    - **Levels of Events in Your Logs**



Level	Name	Example
0	Emergencies	Failure causing a shutdown
1	Alerts	Temperature exceeded
2	Critical	Software failure
3	Errors	Interface down
4	Warning	Configuration change
5	Notifications	Line protocol up/down
6	Information	ACL violation
7	Debugging	Debugging Messages

An Example from Cisco Devices

    - **Logs File Example**

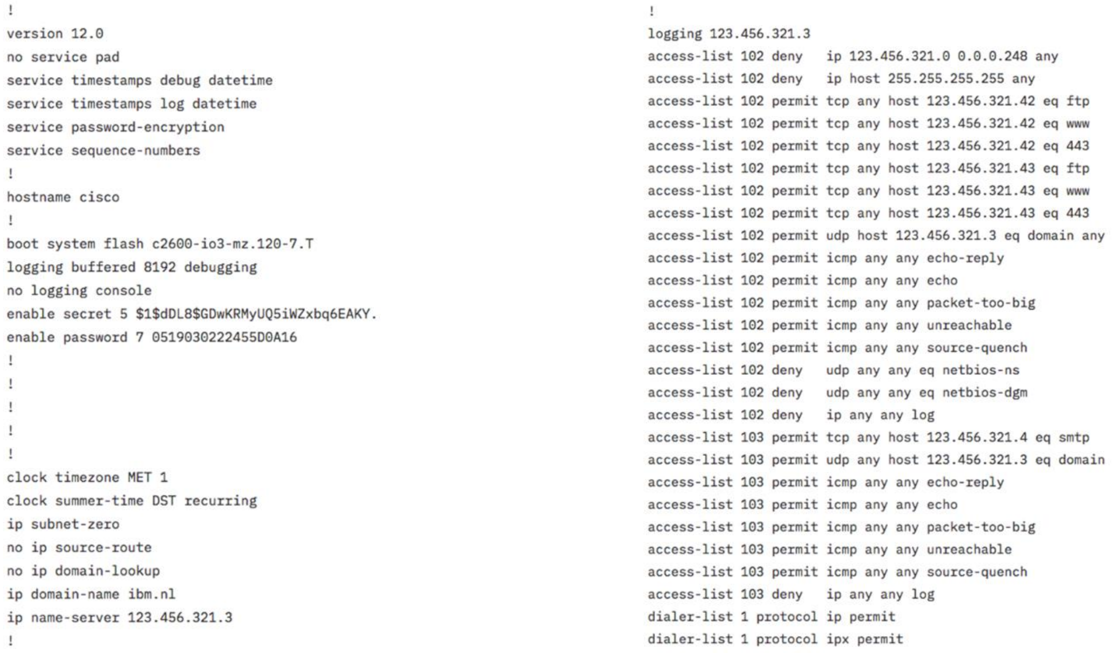


Access list (full timestamp and message id):

```
Jul 10 16:07:14 cisco2621 636: .Jul 10 15:58:56.590 EDT: %SEC-6-IPACCESSLOGP: list 102 denied tcp
10.0.6.56(3067) -> 172.36.4.7(139), 1 packet

123: May 3 05:15:25.217 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.0.40.16(3059) ->
10.0.4.101(1060), 2 packets 124: May 3 05:15:27.302 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted
tcp 10.0.16.16(2179) -> 10.0.4.101(1060), 1 packet 125: May 3 05:15:40.362 UTC: %SEC-6-
IPACCESSLOGP: list 199 permitted tcp 10.0.32.16(4206) -> 10.0.4.101(1060), 2 packets 126: May 3
05:15:42.790 UTC: %SEC-6-IPACCESSLOGP: list 199 permitted tcp 10.131.5.17(3737) ->
10.0.4.101(445), 1 packet

127: May 3 05:23:33.404 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1477) ->
10.0.127.20(445), 1 packet 128: May 3 05:23:34.416 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp
10.0.61.108(1469) -> 10.0.127.12(445), 1 packet 129: May 3 05:23:35.524 UTC: %SEC-6-
IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1473) -> 10.0.127.16(445), 1 packet 130: May 3
05:23:36.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1478) ->
10.0.127.21(445), 1 packet 131: May 3 05:23:37.528 UTC: %SEC-6-IPACCESSLOGP: list 199 denied tcp
10.0.61.108(1496) -> 10.0.127.39(445), 1 packet 132: May 3 05:23:38.540 UTC: %SEC-6-
IPACCESSLOGP: list 199 denied tcp 10.0.61.108(1484) -> 10.0.127.27(445), 1 packet

4872: Dec 11 08:02:53.887 pst: %SEC-6-IPACCESSLOGP: list 100 denied udp 200.174.153.126(1028) -
> 66.81.85.65(137), 1 packet 4873: Dec 11 08:03:09.583 pst: %SEC-6-IPACCESSLOGP: list 100 denied
udp 195.23.72.148(1026) -> 66.81.85.65(137), 1 packet
```

    - **Configuration Files**
        - Invaluable when mapping a network
        - Identifies all routes and devices in detail
        - Provides details of SNMP and SYSLOG servers on the network, user & admin accounts, and more

- **Configuration File Example**



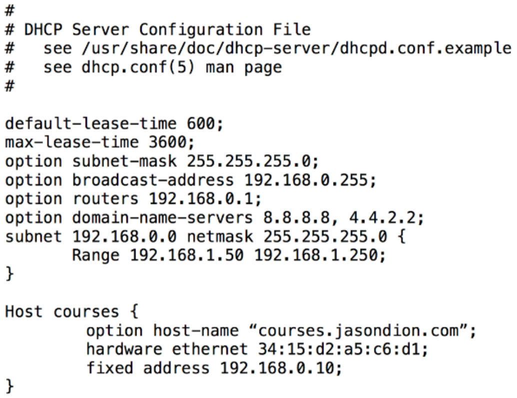
```
!
version 12.0
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
service sequence-numbers
!
hostname cisco
!
boot system flash c2600-io3-mz.120-7.T
logging buffered 8192 debugging
no logging console
enable secret 5 $1$dDL8$GDwKRMyUQ5iWZxbq6EAKY.
enable password 7 0519030222455D0A16
!
!
!
!
!
clock timezone MET 1
clock summer-time DST recurring
ip subnet-zero
no ip source-route
no ip domain-lookup
ip domain-name ibm.nl
ip name-server 123.456.321.3
!
```

```
!
logging 123.456.321.3
access-list 102 deny   ip 123.456.321.0 0.0.0.248 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 permit tcp any host 123.456.321.42 eq ftp
access-list 102 permit tcp any host 123.456.321.42 eq www
access-list 102 permit tcp any host 123.456.321.42 eq 443
access-list 102 permit tcp any host 123.456.321.43 eq ftp
access-list 102 permit tcp any host 123.456.321.43 eq www
access-list 102 permit tcp any host 123.456.321.43 eq 443
access-list 102 permit udp host 123.456.321.3 eq domain any
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any packet-too-big
access-list 102 permit icmp any any unreachable
access-list 102 permit icmp any any source-quench
access-list 102 deny   udp any any eq netbios-ns
access-list 102 deny   udp any any eq netbios-dgm
access-list 102 deny   ip any any log
access-list 103 permit tcp any host 123.456.321.4 eq smtp
access-list 103 permit udp any host 123.456.321.3 eq domain
access-list 103 permit icmp any any echo-reply
access-list 103 permit icmp any any echo
access-list 103 permit icmp any any packet-too-big
access-list 103 permit icmp any any unreachable
access-list 103 permit icmp any any source-quench
access-list 103 deny   ip any any log
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
```

- **Netflow Data**
  - Cisco network protocol
  - Captures IP traffic information for traffic monitoring to provide flow and volume
  - Contains IP, source port, destination port, and class of service
  - Other vendors have "flows", like Juniper's Jflow and cflowd, Citrix's AppFlow, and HP's NetStream

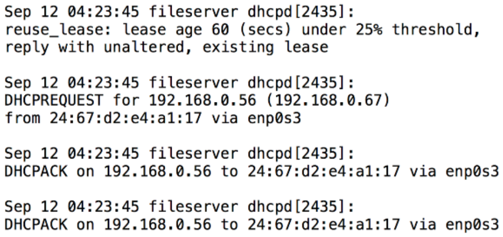
- **Passive Recon: Netstat**
  - **Netstat**
    - Built-in utility in Windows, Linux, MacOS, and Unix operating systems
    - Provides active TCP and UDP connections
    - Identify process using a connection
    - Provides statistics on sent/received data
    - Route table information
  - **netstat -a**
    - Provides active TCP and UDP connections filtered by TCP, UDP, ICMP, IP, IPv6, and more
  - **netstat -0**
    - Identify process using a connection
  - **netstat -e**
    - Ethernet statistics on sent/received data

  - netstat -r
    - Displays route table information
- **DHCP Logs and Configs**
  - **What is DHCP?**
    - Dynamic Host Configuration Protocol
    - Provides an IP address, default gateway, subnet mask, and DNS server to a host
    - DHCP server logs and configurations are useful during passive reconnaissance
    - Combined with firewall logs, you can determine which hosts use dynamic or static IPs
  - **Example DHCP Configuration**



```
#
# DHCP Server Configuration File
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcp.conf(5) man page
#

default-lease-time 600;
max-lease-time 3600;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers 192.168.0.1;
option domain-name-servers 8.8.8.8, 4.4.2.2;
subnet 192.168.0.0 netmask 255.255.255.0 {
       Range 192.168.1.50 192.168.1.250;
}

Host courses {
        option host-name “courses.jasondion.com”;
        hardware ethernet 34:15:d2:a5:c6:d1;
        fixed address 192.168.0.10;
}
```

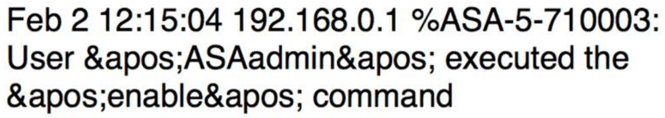
  - **Example DHCP Logs**



```
Sep 12 04:23:45 fileserver dhcpd[2435]:
reuse_lease: lease age 60 (secs) under 25% threshold,
reply with unaltered, existing lease

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPREQUEST for 192.168.0.56 (192.168.0.67)
from 24:67:d2:e4:a1:17 via enp0s3

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPACK on 192.168.0.56 to 24:67:d2:e4:a1:17 via enp0s3

Sep 12 04:23:45 fileserver dhcpd[2435]:
DHCPACK on 192.168.0.56 to 24:67:d2:e4:a1:17 via enp0s3
```

- **Firewall Logs and Configs**
  - **Firewall Logs and Configs**
    - Both firewall and router logs and configurations indicate accepted and blocked connections
    - It is a good way to passively understand your network design
    - Reading configurations is quicker than “reverse engineering” the log files
  - **Firewall Logs**
    - Often use log levels to categorize information and debug messages
    - Cisco, Palo Alto, and Check Point all log things a little different, but have common items
      - Date/Time Stamp

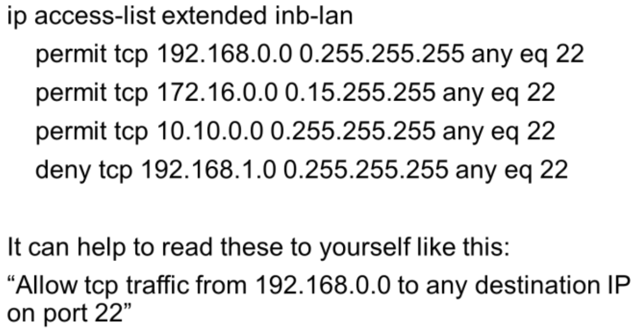
            - Details of the event
        - Logs are designed to be human readable
        - Access logs on Cisco using “show logging” command
    - **Example Firewall Logs**



```
Feb 2 12:15:04 192.168.0.1 %ASA-5-710003:
User &apos;ASAadmin&apos; executed the
&apos;enable&apos; command
```

https://www.cisco.com/c/en/us/about/security-center/identify-incidents-via-syslog.html

    - **Example Firewall Config**



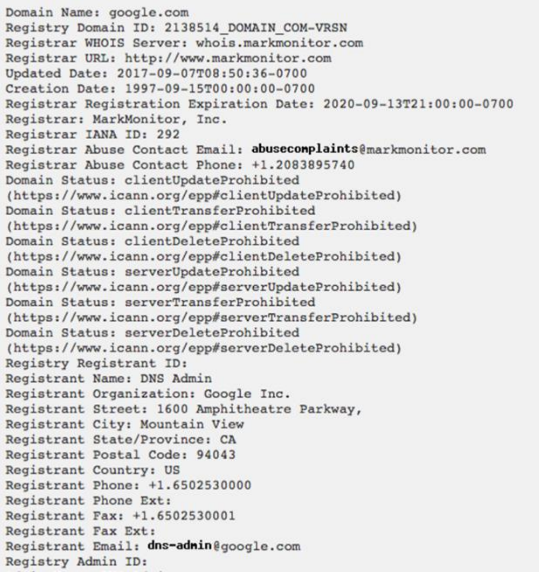
```
ip access-list extended inb-lan
   permit tcp 192.168.0.0 0.255.255.255 any eq 22
   permit tcp 172.16.0.0 0.15.255.255 any eq 22
   permit tcp 10.10.0.0 0.255.255.255 any eq 22
   deny tcp 192.168.1.0 0.255.255.255 any eq 22
```

It can help to read these to yourself like this:
“Allow tcp traffic from 192.168.0.0 to any destination IP on port 22”

- **System and Host Log Files**
    - **Host/Server Log Files**
        - System logs are collected by the system
        - Useful for troubleshooting and reconstructed a cyber attack
        - Log files provide information on system configuration, applications, and user accounts
        - You have to have system access to get these logs, though
    - **Windows System Log Types**
        - Application logs
            - Logged by programs/applications
        - Security logs
            - Records login events, resource usage, files created/open/deleted, etc.
        - Setup logs
            - Records application setup actions
        - System logs
            - Events from Windows components
        - Forwarded Events logs
            - Event subscriptions from remote computers

- **Linux System Logs**
    - /var/log directory
    - Other applications may store their own log files elsewhere
- **DNS Harvesting**
    - **Why Use DNS?**
        - Often our first step in information gathering
        - DNS information is publicly available
        - A quick Whois search can give you many details to use
        - Hostnames can tell you about the server (DC1.jasondion.com might be a domain controller…)
    - **nslookup**
    - **DNS Records**
        - MX (mail server records)
        - A (address records)
        - C (canonical records)
        - PTR (pointer records)
    - **tracert**
- **Domain Names and IP Ranges**
    - **Domain Names**
        - The human readable names we use to locate servers, like jasondion.com
        - Managed by registrars
        - Generic top-level domains
            - .com, .net, .org, .edu, .mil, .gov
        - Country code top-level domain (ccTLD)
            - .com.uk, .edu.it
    - **IP Ranges**
        - Five regional authorities
            - AFRINIC (Africa)
            - ARIN (USA, Canada, Antarctica, and Caribbean)
            - APNIC (Asia, Australia, New Zealand, etc)
            - LACNIC (Latin America, Caribbean)
            - RIPE (Europe, Russia, Middle East)
        - Each authority provides Whois services for their IP space
- **DNS Zone Transfers**
    - **DNS Zone Transfers**
        - Design to replicate DNS databases between two DNS servers
        - This is a vulnerability if zone transfers are allowed, so most prevent zone transfers to servers that aren't trusted
        - You can use dig to perform the transfer: # dig axfr @dns-server domain.name

  - **Try Performing a Zone Transfer**
    - DigiNinja provides a couple DNS servers that ALLOW zone transfers for you to practice this technique
    - Open up your Linux terminal and try it against nsztm1.digi.ninja and nsztm2.digi.ninja
  - **DNS Brute Forcing**
    - Used when you can't perform a DNS zone transfer
    - Simply sends manual or scripted DNS queries for each IP of the organization
    - Organizations can protect against this by sending responses slowly or with IDS/IPS rules to prevent this
- **Whois and Host Commands**
  - **Whois**
    - Allows search of databases for domain and IP blocks
    - Provides detailed registration information used when claiming the domain name
    - Names, Addresses, IPs, Phone numbers, and more can be gained
  - **Whois Example**



```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-09-07T08:50:36-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited
(https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited
(https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited
(https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: DNS Admin
Registrant Organization: Google Inc.
Registrant Street: 1600 Amphitheatre Parkway,
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6502530001
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
Registry Admin ID:
```

  - **Host**
    - Provides information about a systems IPv4 and IPv6 addresses and servers
- **Info Gathering and Aggregation**
  - **Information Gathering**
    - Can be done using packet captures
    - Requires an intruder to breach a company's network to gather this info
    - Treasure trove of information

            - What hosts are on the network
            - What operating systems are the running
            - What shares are available
        - This is done using tools like Wireshark
            - Beyond the scope of this lesson…
    - **Information Aggregation**
        - Gathering information from various platforms for analysis with a single tool
        - theHarvester
            - Gathers emails, domains, hostnames, employee names, open ports, banners, etc.
            - Text-based tool installed in Kali
    - **Maltego**
        - Builds relationship maps between people and resources
    - **Shodan**
        - Search engine for internet-connected devices and their vulnerabilities
- **Organizational Intelligence**
    - **Organizational Intelligence**
        - Your organization has an online profile, whether you know it or not…
        - This can be used by an attacker against you…
        - In a penetration test, we act as the attacker, so we must use this information too!
    - **Organizational Data**
        - Locations (of facilities and buildings)
            - Your physical security posture
            - Business hours
        - Work routine of the organization
        - Organizational charts
            - Relationships between departments and people
        - Documents (contains metadata)
        - Financial data
        - Personal information of your employees
        - Useful during social engineering
    - **Document Harvesting**
        - Metadata
            - Contains author's name and software version used
        - EXIF data
            - Photos could contain geolocation coordinates
        - It is important to scrub metadata and EXIF data from documents posted on the web
        - Emails

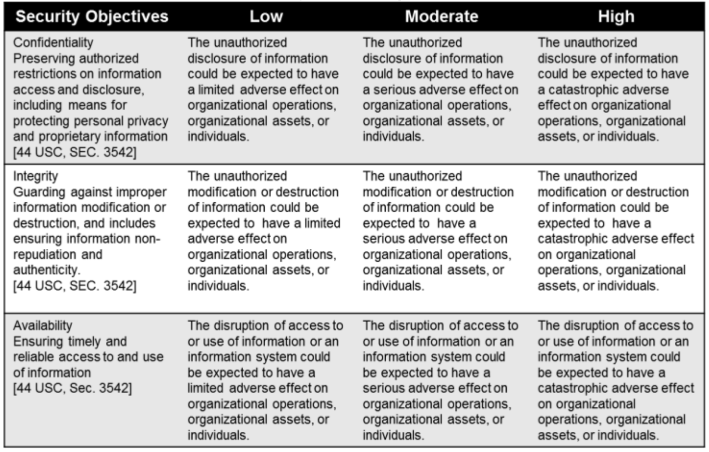
        - Can you be used to perform contact chaining and conduct social engineering campaigns
  - **Immersion**
    - https://immersion.media.mit.edu/demo
  - **Where Can I Get Documents?**
    - Organizations are getting smarter and posted less sensitive information online
      …on the Internet nothing is ever gone!
    - The Internet Archive
      - archive.org
    - Time Travel Service
      - timetravel.mementoweb.org
    - Google Cache View
    - Cachedview.com
  - **Where Can I Get More?**
    - Social media is great to find details about the organization's employees
    - Many people post what companies they work for and don't set their privacy settings up properly
    - Paid public record searches, like Zaba Search, NETR Online, etc.
  - **The Threat: Social Engineering**
    - Exploits the human element of security
    - Occurs via phone, email, social media, or even in person
    - Social Engineering Toolkit (SET)
    - Creepy (geolocation tool)
    - Metasploit (phishing and other tools)
- **Detecting, Preventing, and Responding to Reconnaissance**
  - **Detecting, Preventing, and Responding to Reconnaissance**
    - Successful reconnaissance doesn't always mean a successful attack, but we want to limit the damage that could occur as much as possible
    - We utilize the same technique to limit both casual and directed reconnaissance
  - **Detecting Recon: Overview**
    - Monitoring must occur at connection points between two network zones
    - Perform data collection so you can analyze the data at a later time
  - **Detecting Recon: Data Sources**
    - Network traffic analysis using IDS, IPS, HIDS, NIDS, firewalls, and other security devices
    - Packet analysis
    - Protocol analysis
    - Traffic and flow analysis
    - Device and system logs

        - Port and vulnerability scans
        - Security Information and Event Management Logs
        - If you outsource your services, you might have to rely on your SaaS or PaaS provider to detect it for you…
    - **Detecting Recon: Data Analysis**
        - Anomaly Analysis
            - What is different about this? What's not normal?
        - Trend Analysis
            - Helps to identify future problems based on past
            - Example: Traffic congestion
        - Signature Analysis
            - Fingerprint or hash used to detect threats
        - Heuristic or Behavioral Analysis
            - Detects threats based on behavior
            - Useful to detect unknown threats
        - Manual Analysis
            - Human expertise is used to analyze the data
    - **Preventing Passive Recon**
        - Control the information your release
        - Blacklist system that are abusing your services
        - Use CAPTCHAs to prevent scripts and bots
        - Utilize third-party registration for domains/Ips
        - Set rate limits for lookups and searches
        - Avoid publishing zone files, if possible
        - Educate your users about social media risks
    - **Preventing Active Recon**
        - Employ network defenses
        - Limit external exposure of services and know your forward-facing footprint
        - Utilize an IPS to limit or stop probes/scans
        - Utilize monitoring and alert systems based on signature, behavior, or anomaly

Domain 2: Vulnerability Management

- **Intro to Vulnerability Management**
    - **What does this section cover?**
        - Requirements to conduct vulnerability scans
        - How scan targets are selected
        - How to determine the scan frequency
        - How to customize scan settings to meet policy
        - Maintenance of the scanning tools
        - How to remediate scan findings
        - How to prioritize remediation efforts and how to maximize your limited resources
        - How to overcome objections from the rest of the Information Technology team
    - **What is Vulnerability Management?**
        - Identification, prioritization, and remediation of vulnerabilities before a threat can exploit them
        - An organized approach to scanning and continuous assessment of your organizational security posture
    - **Bottom Line…**
        - In this course, we will discuss the high-level concerns of how to develop a vulnerability management program for your organization, AND
        - How to analyze vulnerability scans to better secure your organization's networks
- **Regulatory Requirements**
    - **Vulnerability Management Requirements**
        - As you begin to develop your vulnerability management program, you must understand the requirements you might have…
        - Regulatory Requirements
            - (HIPAA, GLBA, PCI DSS, FISMA, etc.)
        - Corporate Policy-based Requirements
            - (Targets, frequency, etc.)
    - **Regulatory Requirements**
        - Laws and regulations that govern information storage and processing
            - HIPAA
            - GLBA
            - FERPA
        - Laws and regulations that require vulnerability management programs
            - PCI DSS
            - FISMA

- **Payment Card Industry Data Security Standard (PCI DSS)**
  - Specifies security controls for credit card processors and merchants
  - Most specific of any requirement for vulnerability management
  - Examples:
    - Internal and external scans must be conducted
    - Scanned at least quarterly and all major changes
    - Internal scans by qualified personnel
    - External scans by Approved Scanning Vendor
    - Remediate any high-risk vulnerabilities and rescan until a "clean" report is achieved
- **Federal Information Security Management Act (FISMA)**
  - Specifies security controls for government
    - Both agencies and organizations that run systems
  - Systems are classified as low, moderate, or high impact which dictate the requirements
- **Federal Information Security Management Act (FISMA)**



Security Objectives	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 USC, SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information [44 USC, Sec. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

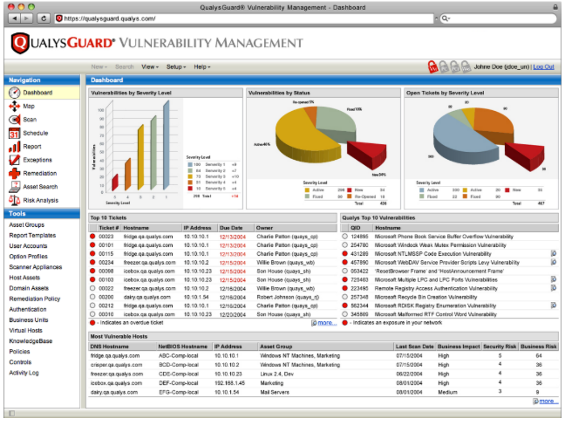
- **FISMA Requirements**
  - Scan systems when new threats emerge
  - Use tools/techniques that are interoperable
  - Analyze scan reports from assessments
  - Remediate vulnerabilities based on risk
  - Share findings with other agencies to eliminate similar vulnerabilities in other systems

- **Corporate Policy Requirements**
  - **Corporate Policy Requirements**
    - Laws and regulations that require vulnerability management programs (like PCI DSS, and FISMA) don't apply to all companies
    - But…vulnerability management is still very important to them as a key component to security

        - Therefore…organizations can (and do) require scanning under their own corporate policies
    - **Scan Targets**
        - What systems do you want to be covered by your scans?
        - Do you scan all systems or just *critical* assets?
        - Scanning tools like *QualysGuard* can be used to build your asset inventory automatically
        - Admins then take that information and classify the systems as critical or non-critical
    - **QualysGuard Vulnerability Scanner**
    - **Scan Frequency**
        - How often do we scan the systems?
        - Schedule determined by your goals to meet security, compliance, or other business requirements
        - Automated email reports or alerts can be configured, as well
        - For example, the Nessus scanner allows you to setup daily, weekly, monthly, or other scheduled scans by date/time
    - **Tenable's Nessus Vulnerability Scanner**
    - **Scan Frequency Considerations**
        - Organizational risk appetite
            - How much time between a new threat and a scan?
        - Regulatory requirements
            - Do you fall under FISMA or PCI DSS?
        - Technical constraints
            - Network may not support scanning everything
        - Business constraints
            - Do you have to avoid high business activity times?
        - Licensing limitations
            - Scanners can control how many concurrent scans can be performed through licensing
    - **Best Practices for a New Program**
        - Start small
            - Start with a small section of the network's assets
        - Expand slowly
            - Gradually add more scope to your scans
        - Prevent overwhelming the enterprise systems and your system administration team
- **Scanning Tools**
    - **Vulnerability Scanning Tools**
        - QualysGuard
        - Tenable's Nessus

- Rapid7’s Nexpose
- OpenVAS
- Nikto Web Application scanner
- Microsoft Baseline Security Analyzer

○ **QualysGuard Vulnerability Scanner**



Top 10 Tickets

	Ticket #	Hostname	IP Address	Due Date	Owner
●	00023	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
●	00101	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
●	00115	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
●	00234	freezer.qa.qualys.com	10.10.10.2	12/15/2004	Willie Brown (quays_wb)
●	00098	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (quays_sh)
●	00103	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (quays_sh)
○	00022	freezer.qa.qualys.com	10.10.10.2	12/16/2004	Willie Brown (quays_wb)
○	00200	dairy.qa.qualys.com	10.10.1.54	12/16/2004	Robert Johnson (quays_rj)
○	00212	fridge.qa.qualys.com	10.10.10.1	12/16/2004	Charlie Patton (quays_cp)
○	00010	icebox.qa.qualys.com	10.10.10.23	12/20/2004	Son House (quays_sh)

● - Indicates an overdue ticket more...

Qualys Top 10 Vulnerabilities

	QID	Hostname
○	124895	Microsoft Phone Book Service Buffer Overflow Vulnerability
○	254780	Microsoft Windock Weak Mutex Permission Vulnerability
●	431289	Microsoft NTLMSSP Code Execution Vulnerability
●	457890	Microsoft WebDAV Service Provider Scripts Levy Vulnerability
○	053422	‘ResetBrowser Frame’ and ‘HostAnnouncement Frame’
●	725403	Microsoft Multiple LPC and LPC Ports Vulnerabilities
●	223495	Remote Registry Access Authentication Vulnerability
○	257348	Microsoft Recycle Bin Creation Vulnerability
●	562344	Microsoft RDISK Registry Enumeration Vulnerability
○	345809	Microsoft Malformed RTF Control Word Vulnerability

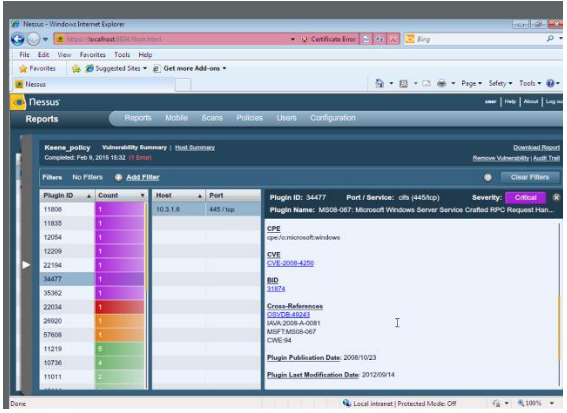
● - Indicates an exposure in your network

Most Vulnerable Hosts

DNS Hostname	NetBIOS Hostname	IP Address	Asset Group	Last Scan Date	Business Impact	Security Risk	Business Risk
fridge.qa.qualys.com	ABC-Comp-local	10.10.10.1	Windows NT Machines, Marketing	07/15/2004	High	5	64
crisper.qa.qualys.com	BCD-Comp-local	10.10.10.2	Windows NT Machines, Marketing	07/15/2004	High	4	36
freezer.qa.qualys.com	CDE-Comp-local	10.10.10.23	Linux 2.4, Dev	06/22/2004	High	4	36
icebox.qa.qualys.com	DEF-Comp-local	192.168.1.45	Marketing	08/01/2004	High	4	36
dairy.qa.qualys.com	EFG-Comp-local	10.10.1.54	Mail Servers	08/01/2004	Medium	3	9

more...

○ **Tenable’s Nessus Vulnerability Scanner**


Nessus - Windows Internet Explorer
https://localhost:8834/flash.html
Certificate Error
Bing
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Get more Add-ons
Nessus
Page Safety Tools
Nessus
user | Help | About | Log out
Reports
Reports Mobile Scans Policies Users Configuration
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter
Clear Filters
Done
Local intranet | Protected Mode: Off
100%

Keene_policy Vulnerability Summary | Host Summary
Completed: Feb 9, 2015 15:32 (1 Error)

Plugin ID	Count
11808	1
11835	1
12054	1
12209	1
22194	1
34477	1
35362	1
22034	1
26920	1
57608	1
11219	5
10736	4
11011	2

Host	Port
10.3.1.6	445 / tcp

Plugin ID: 34477 Port / Service: cifs (445/tcp) Severity: Critical
Plugin Name: MS08-067: Microsoft Windows Server Service Crafted RPC Request Han...

CPE
cpe:/o:microsoft:windows

CVE
CVE-2008-4250

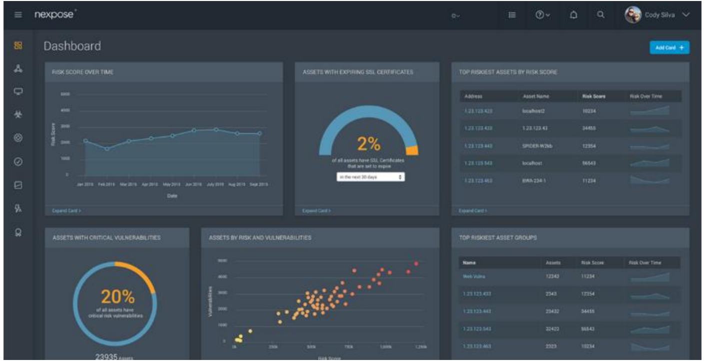
BID
31874

Cross-References
OSVDB:49243
IAVA:2008-A-0081
MSFT:MS08-067
CWE:94

Plugin Publication Date: 2008/10/23

Plugin Last Modification Date: 2012/09/14

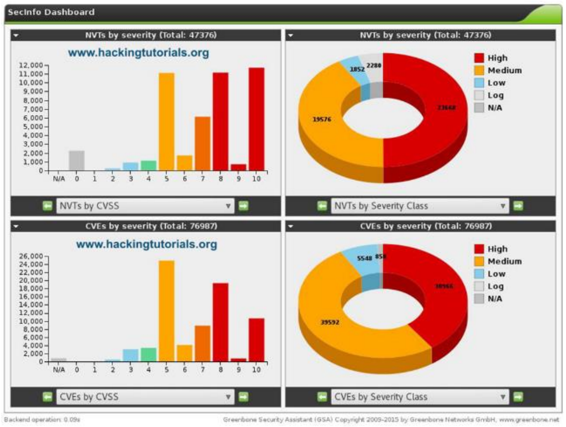
○ **Rapid7’s Nexpose**


nexpose
Cody Silva
Dashboard
Add Card +
RISK SCORE OVER TIME
Risk Score
Date
Expand Card
ASSETS WITH EXPIRING SSL CERTIFICATES
2%
of all assets have SSL Certificates that are set to expire
in the next 30 days
TOP RISKIEST ASSETS BY RISK SCORE
ASSETS WITH CRITICAL VULNERABILITIES
20%
of all assets have critical risk vulnerabilities
23935 Assets
ASSETS BY RISK AND VULNERABILITIES
Vulnerabilities
Risk Score
TOP RISKIEST ASSET GROUPS

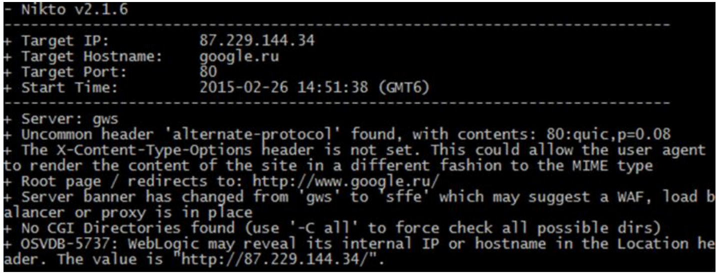
Address	Asset Name	Risk Score	Risk Over Time
1.23.123.423	localhost2	10234	
1.23.123.433	1.23.123.43	34455	
1.23.123.443	SPIDER-W2kb	12354	
1.23.123.543	localhost	56543	
1.23.123.463	BWA-234-1	11234	

Name	Assets	Risk Score	Risk Over Time
Web Vulns	12343	11234	
1.23.123.433	2343	12354	
1.23.123.443	23432	34455	
1.23.123.543	32423	56543	
1.23.123.463	2323	10234	

- **OpenVAS (Open-source Scanner)**

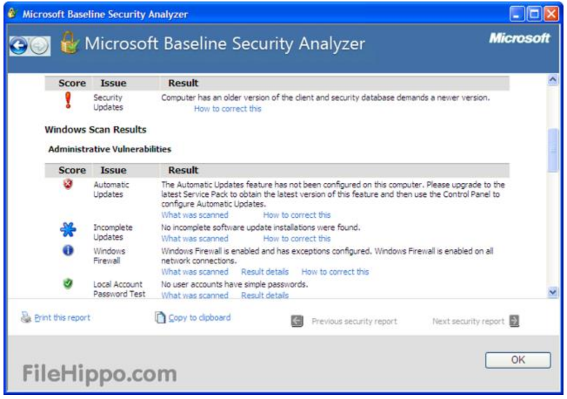


- **Nikto (Web Application Scanner)**



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          87.229.144.34
+ Target Hostname:    google.ru
+ Target Port:        80
+ Start Time:         2015-02-26 14:51:38 (GMT6)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'alternate-protocol' found, with contents: 80:quic,p=0.08
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://www.google.ru/
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load b
alancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-5737: WebLogic may reveal its internal IP or hostname in the Location he
ader. The value is "http://87.229.144.34/".
```

- **Microsoft's Baseline Security Analyzer**


Microsoft Baseline Security Analyzer
Microsoft Baseline Security Analyzer
Microsoft

Score	Issue	Result
!	Security Updates	Computer has an older version of the client and security database demands a newer version. How to correct this

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
✱	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
i	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details

- **Scoping Scans**
  - **Scope**
    - Describes the extent of the scan
    - What networks and systems are included?
    - How will you test if a system is on the network?
    - What tests will be performed against the systems during a scan?
  - **The Importance of Scope**
    - Develop scope properly and gain agreement from staff and management
    - Ensures you are unlikely to cause issues during your scanning efforts

- **Minimizing the Scope**
    - Network segmentation often allows you to minimize your scope for compliance scans
    - PCI DSS networks should be segmented from the rest of the organizational network

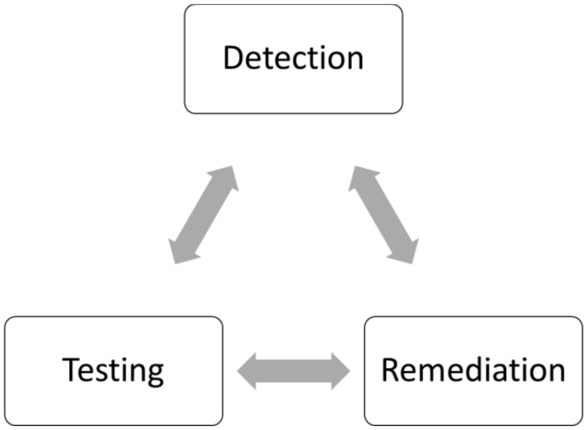
- **Configuring Scans**
    - **Configuring Scans**
        - Scheduling automated scans
        - Producing reports
        - Providing authenticated access for scans
        - Choosing plugins and scan agents
        - Conduct scans from different perspectives
            - Internal, external, etc.
- **Scanning Sensitivity**
    - **Scan Sensitivity Levels**
        - Choose level appropriate with objectives
    - **Plug-ins**
        - Provide the scan functionality for different functions
        - Enable/disable them based on your needs
        - If Linux system, disable Windows plug-ins
        - Some scans can disrupt your systems or cause loss of data…
        - Ensure you are scanning safely and with permission
    - **Templates for Scans**
        - Vendors provide templates for scans with common settings
        - Admins can also create their own templates for commonly used scans
        - This prevents errors and saves time
- **Scanning Perspective**
    - **Scanning Perspective**
        - Comprehensive scanners provide you with different scan perspectives
        - External scans provide viewpoint of attacker
        - Internal scans provide insider threat viewpoint
        - Datacenter scans provide a close internal scan, one that might be blocked by other security devices
    - **Internal and External Scans**
        - Remember, PCI-DSS requires both internal and external scans to be conducted
        - Internal can be performed by your own techs
        - External must use approved outsiders to scan
            - You can run an external scan prior to your real assessment to know where you stand, though!

- **Policies Define Scan Perspective**
- **Authenticated Scanning**
  - **Authenticated Scanning**
    - Firewalls, intrusion protection systems, and other security devices can prevent some details of a scan from being successful
    - Using an authenticated scan can overcome this issue
    - Provide the scanner read-only access to the servers
    - Scanner can access the operating system, databases, and applications on the server
  - **Nessus Authenticated Scanning**
  - **QualysGuard Authenticated Scanning**
  - **Agent-based Scanning**
    - Small software agents installed on your server or clients
    - Provides an “inside-out” perspective of vulnerabilities on the server or client
    - Agent-based approaches require more resources on the server and often system administrators fight against their installation
- **Maintaining Scanners**
  - **Maintaining Scanners**
    - Vulnerability management tools are vulnerable to vulnerabilities themselves!
    - You should always update the tools and its plug-ins/signatures before use
    - This can be automated, as well, but check to verify the update has occurred before use
  - **Updating Scanners**
    - Regular patching is critical to a secure scanner
    - Implements bug fixes
    - Feature enhancements
    - Improves scan quality
  - **Nessus Scanner Vulnerabilities**
  - **Updating Plug-ins**
    - Plug-ins can be automatically set to update daily
    - Provides signatures for latest vulnerabilities
- **Standardizing Vulnerabilities**
  - **Standardizing Vulnerabilities**
    - Vulnerability management used to be performed by numerous different types of software with no common protocol
    - Security Content Automation Protocol (SCAP) led by NIST standardized vulnerability management between different software

https://scap.nist.gov
NIST SP 800-117
Guide to Adopting and Using the SCAP

- **SCAP**
  - Common Configuration Enumeration (CCE)
    - Standard names for system configuration issues
  - Common Platform Enumeration (CPE)
    - Standard names for product names and versions
  - Common Vulnerabilities and Exposures (CVE)
    - Standard names for security-related software flaws
  - Common Vulnerability Scoring System (CVSS)
    - Standard approach for severity of software flaws
  - Extensible Configuration Checklist Description Format (XCCDF)
    - Language for checklists and reporting results
  - Open Vulnerability and Assessment Language (OVAL)
    - Language for low-level testing procedures used by the checklists

- **Workflow for Remediation**
  - **Workflow for Remediation**



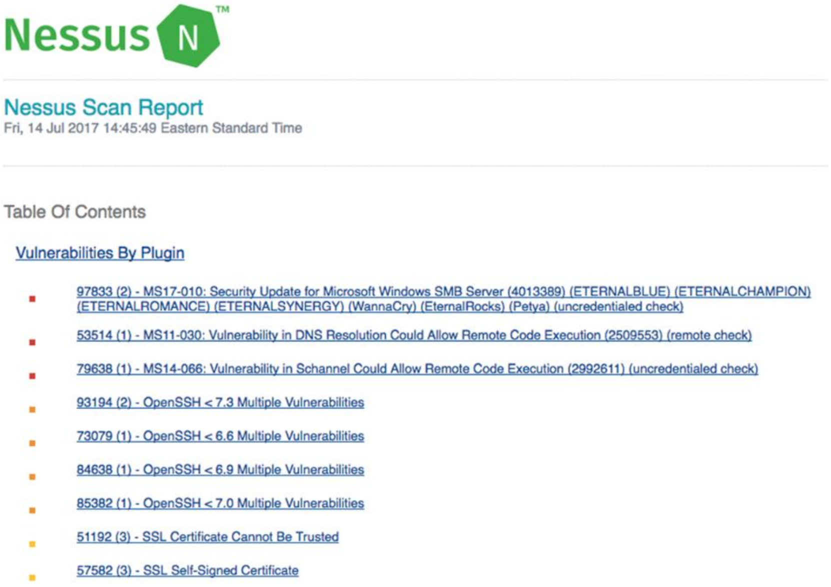
  - **Continuous Monitoring**
    - Provides for on-going scanning of the network
    - Checks for vulnerabilities as often as possible based on resources available
    - Provides earlier detection of vulnerabilities
  - **Automation**
    - Many products include built-in workflows and automation to track vulnerabilities through the cycle
    - Can automatically close out vulnerabilities when testing shows they are solved
    - Some tools can be integrated into your IT Service Management system, too!

- **Vulnerability Reporting**
    - **Vulnerability Reporting**
        - Vulnerability analysts need to communicate the issues found to the system administrators
        - Scanners provide detailed reporting that can be automated to alert system administrators at periodic intervals
        - Critical vulnerabilities found can be sent out of cycle
    - **Dashboards**
        - Managers love dashboards
        - Provide a high-level summary of issues
    - **Overview of Hosts**
        - Shows which hosts are most vulnerable
    - **Overview of Criticality**
        - Shows which vulnerabilities are most critical
    - **Details of a Vulnerability**
- **Remediation Priority**
    - **Remediation Priority**
        - Man-hours, money, equipment and other items are a limited resource
        - Vulnerability Management is all about prioritization of organizational efforts
        - *You can't fix everything right away…*
    - **How critical is the System and Information It Contains?**
        - Take into account confidentiality, integrity, and availability if the vulnerability was exploited
        - Example:
            - If an attacker was able to breach your customer database and get all their information…
            - How bad is this?
    - **How Difficult is it to Fix the Vulnerability?**
        - How much time and money will it cost to fix it?
        - Example:
            - I can spend all my time and money fixing the #1 vulnerability, or I can fix vulnerabilities 2, 3, 4, & 5
            - Which should I do?
    - **How Severe is the Vulnerability?**
        - Each vulnerability is given a criticality value in the Common Vulnerability Scoring System (CVSS)
        - Different vulnerabilities are more severe than others
        - Example:
            - Known-exploit against a software bug that allows for remote-code execution is very severe

            - Cross-site scripting vulnerability might be less severe if it’s on an intranet server only
    - **How Exposed is the Server to the Vulnerability?**
        - External facing servers are more exposed than intranet servers
        - Often, you should fix a lower external vulnerability before a higher internal one…
- **Implementing and Testing**
    - **Implementing and Testing a Solution**
        - Vulnerability analysts don’t implement the fixes
        - Their role is to find the issues and pass them to the system administrators to fix
        - Fixes may not be quick, often they require approval from the Change Control Board
        - Fixes should be tested in a lab environment prior to rolling it out to the enterprise
    - **Coordinating Your Efforts**
        - Vulnerability Analysts view fixes as the highest priority…
        - Not everyone in the organization does…
        - You need to coordinate with others to get these vulnerabilities remediated
        - Service degradation, promises to customers, and IT governance can slow down your efforts
    - **Service Degradation**
        - Vulnerability scanning places a resource tax upon the network and its servers when scans are conducted
        - Scans can risk disrupting business functions
        - Overcoming objections:
            - Consider different scanning times (non-peak hours)
            - Change scanning settings to lower intensity modes
    - **Promises to Customers**
        - MOUs and SLAs have specific uptime, performance, and other requirements that the organization must meet
        - Scans can risk disrupting business functions
        - Overcoming objections:
            - Ensure the cybersecurity team is involved in the drafting of the MOUs and SLAs
            - Discuss appropriate times and scope for scans
    - **IT Governance**
        - Can create hurdles in getting approval to implement changes
        - Fixes can risk disrupting business functions
        - Overcoming objections:

- Work within the organization policies when possible to get resources and support
- Utilize the Emergency Change Control Board when critical fixed must be implemented quickly

- **Interpreting Scan Results**
  - **Importance of Scan Results**
    - Scanners do a great job of automating the identification of vulnerabilities
    - …but, a trained analyst is required to understand the implications of those vulnerabilities
      - Eliminating false positives
      - Finding root causes
      - Prioritizing remediation actions
  - **Scan Results**



Nessus

Nessus Scan Report

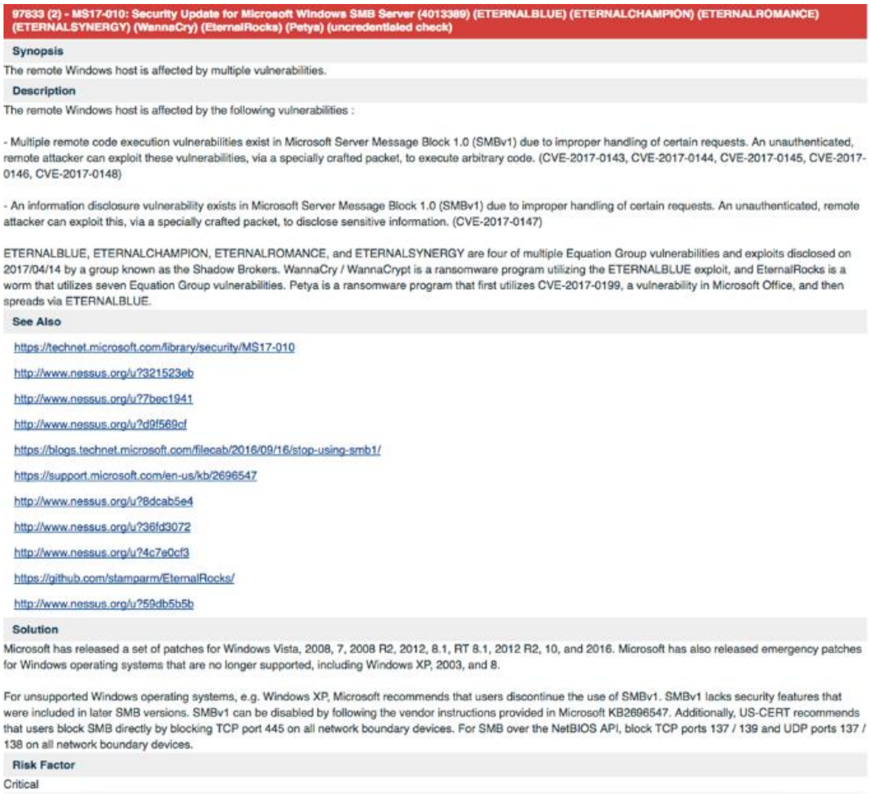
Fri, 14 Jul 2017 14:45:49 Eastern Standard Time

Table Of Contents

Vulnerabilities By Plugin

- 97833 (2) - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
- 53514 (1) - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
- 79638 (1) - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
- 93194 (2) - OpenSSH < 7.3 Multiple Vulnerabilities
- 73079 (1) - OpenSSH < 6.6 Multiple Vulnerabilities
- 84638 (1) - OpenSSH < 6.9 Multiple Vulnerabilities
- 85382 (1) - OpenSSH < 7.0 Multiple Vulnerabilities
- 51192 (3) - SSL Certificate Cannot Be Trusted
- 57582 (3) - SSL Self-Signed Certificate

- **Detailed Scan Results**



97833 (2) - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

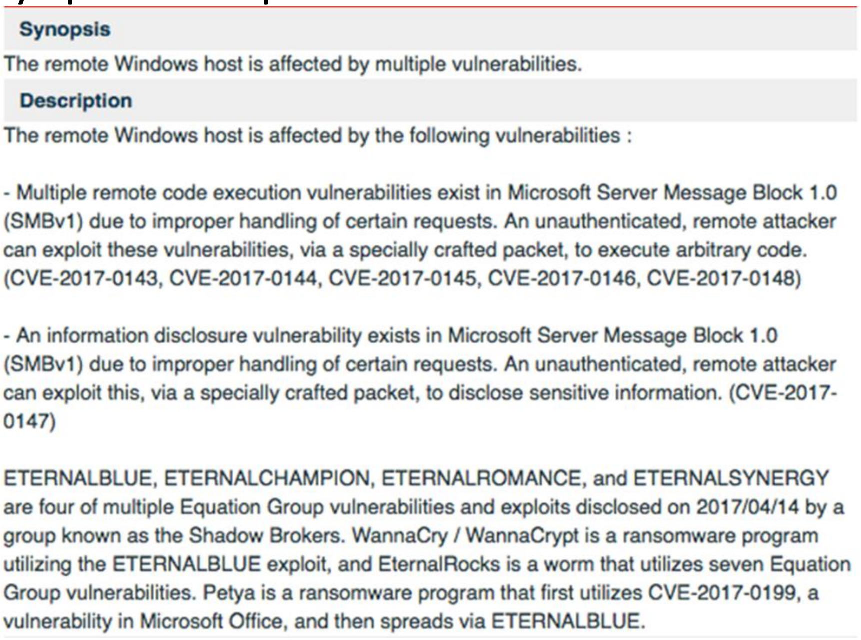
Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

Critical

- **Synopsis and Description**



Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

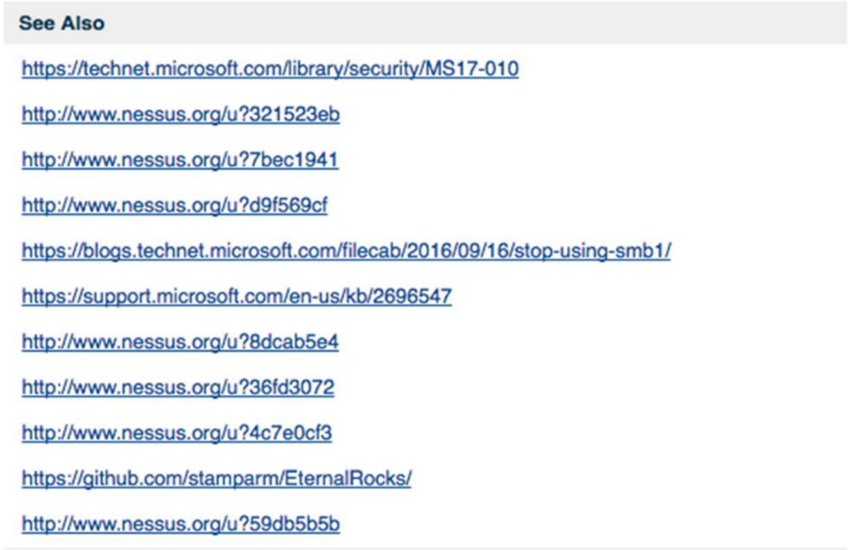
The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

- **See Also**



See Also

https://technet.microsoft.com/library/security/MS17-010

http://www.nessus.org/u?321523eb

http://www.nessus.org/u?7bec1941

http://www.nessus.org/u?d9f569cf

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

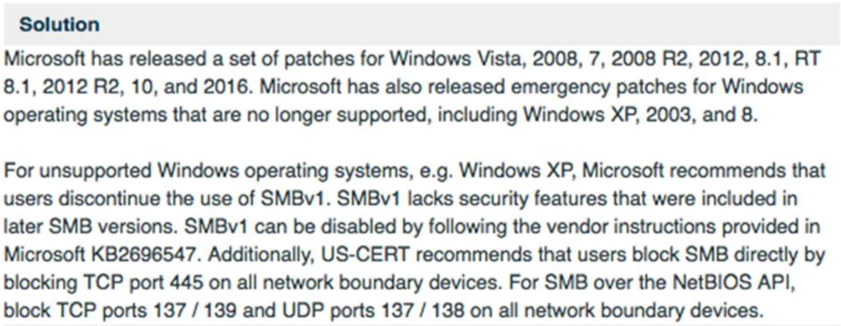
http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

- **Solution**

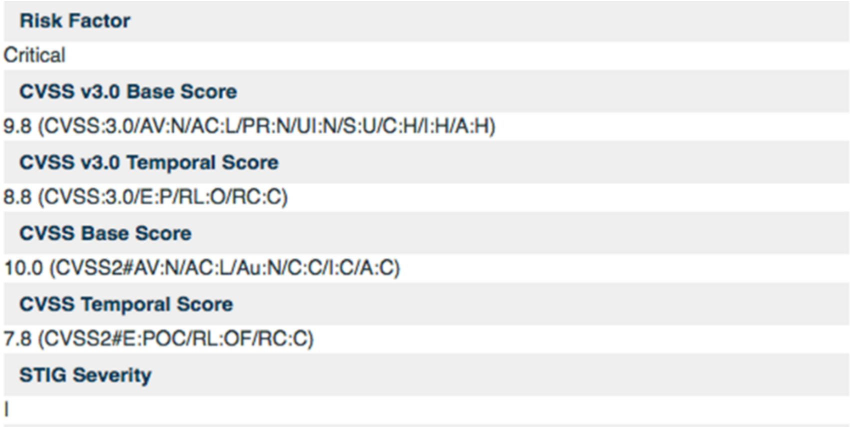


Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

- **Risk Factor and CVSS Score**



Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

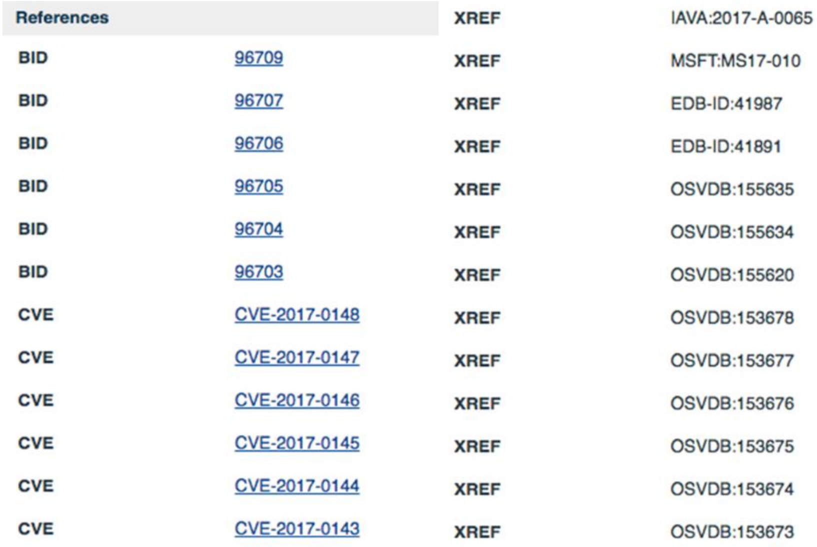
CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

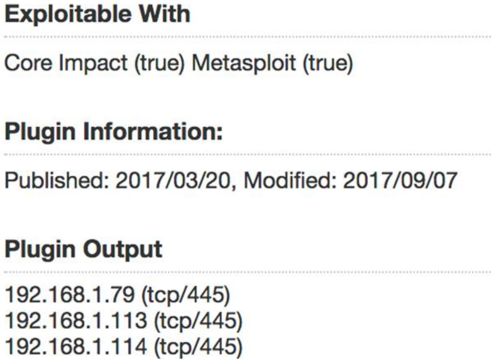
I

- **References**



References		XREF	IAVA:2017-A-0065
BID	96709	XREF	MSFT:MS17-010
BID	96707	XREF	EDB-ID:41987
BID	96706	XREF	EDB-ID:41891
BID	96705	XREF	OSVDB:155635
BID	96704	XREF	OSVDB:155634
BID	96703	XREF	OSVDB:155620
CVE	CVE-2017-0148	XREF	OSVDB:153678
CVE	CVE-2017-0147	XREF	OSVDB:153677
CVE	CVE-2017-0146	XREF	OSVDB:153676
CVE	CVE-2017-0145	XREF	OSVDB:153675
CVE	CVE-2017-0144	XREF	OSVDB:153674
CVE	CVE-2017-0143	XREF	OSVDB:153673

- **Exploitable, Plugin, and Hosts**



Exploitable With

Core Impact (true) Metasploit (true)

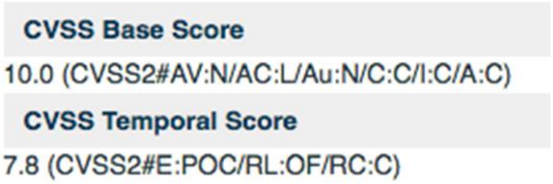
Plugin Information:

Published: 2017/03/20, Modified: 2017/09/07

Plugin Output

```
192.168.1.79 (tcp/445)
192.168.1.113 (tcp/445)
192.168.1.114 (tcp/445)
```

- **Interpreting CVSS**
  - **Common Vulnerability Scoring System (CVSS)**
    - Industry standard for identifying the severity of a vulnerability
    - Analysts use this score to help prioritize remediation efforts
    - Measured in six categories
      - Three for the exploitability
      - Three for the impact



CVSS Base Score

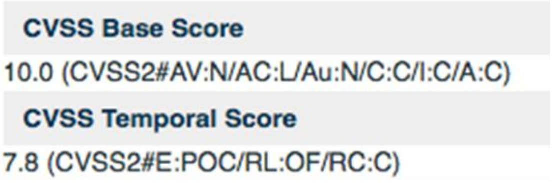
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

  - **CVSS 3.0 and CVSS**
    - CySA+ focuses on CVSS not CVSS 3.0
    - CVSS 3.0 adds two additional measures

        - User Interaction (exploitability metric)
        - Scope (both exploitability and impact metric)

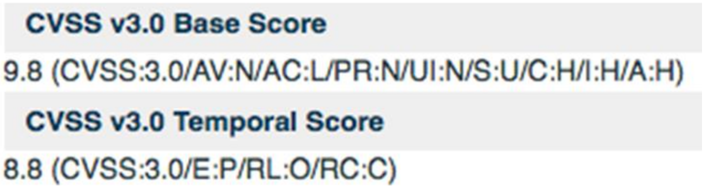


CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)



CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

- ○ **Access Vector (AV) Metric**
    - Describes the method an attacker would use to exploit the vulnerability

Value	Method	Description	Score
L	Local	Physical or logical access to the system required	0.395
A	Adjacent Network	Access to LAN for affected system required	0.646
N	Network	Remote access from WAN	1.000

- ○ **Access Complexity (AC) Metric**
    - Describes the difficulty an attacker would have to exploit the vulnerability

Value	Method	Description	Score
H	High	Requires difficult/ specialized conditions	0.350
M	Medium	Requires "somewhat specialized" conditions	0.610
L	Low	No specialized conditions required	0.710

- ○ **Authentication (Au) Metric**
    - Describes the number of times an attacker would have to authenticate

Value	Method	Description	Score
M	Multiple	Requires two or more authentications	0.450
S	Single	Requires one authentication	0.560
N	None	No authentication required	0.704

- **Confidentiality (C) Metric**
  - Describes the impact to confidentiality of data processed by the system

Value	Method	Description	Score
N	None	No impact to confidentiality	0.0
P	Partial	Considerable disclosure of information	0.275
C	Complete	Total disclosure of information	0.660

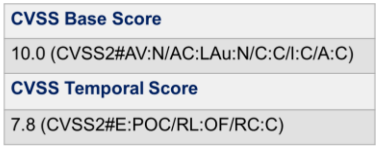
- **Integrity (I) Metric**
  - Describes the impact to integrity of data processed by the system

Value	Method	Description	Score
N	None	No impact to integrity of the system	0.0
P	Partial	Modification of some information possible	0.275
C	Complete	Total loss of integrity	0.660

- **Availability (A) Metric**
  - Describes the impact to availability of the system

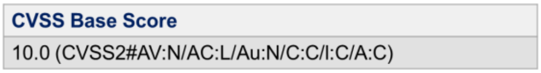
Value	Method	Description	Score
N	None	No impact to availability of the system	0.0
P	Partial	Reduced performance or loss of functionality	0.275
C	Complete	Total loss of availability	0.660

- **CVSS Vector**
  - Single-line format to show the vulnerability ratings for all six metrics

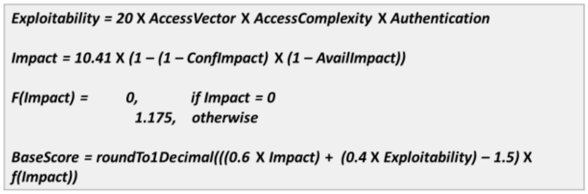


CVSS Base Score
10.0 (CVSS2#AV:N/AC:LAu:N/C:C/I:C/A:C)
CVSS Temporal Score
7.8 (CVSS2#E:POC/RL:OF/RC:C)

- **Calculating the CVSS Score**
  - **CVSS Score**



CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)



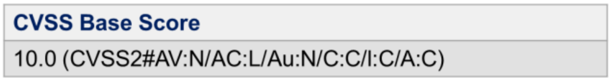
Exploitability = 20 X AccessVector X AccessComplexity X Authentication

Impact = 10.41 X (1 – (1 – ConfImpact) X (1 – AvailImpact))

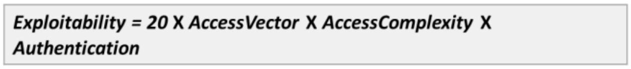
F(Impact) = 0, if Impact = 0
1.175, otherwise

BaseScore = roundTo1Decimal(((0.6 X Impact) + (0.4 X Exploitability) – 1.5) X f(Impact))

- **Exploitability Score**



CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)



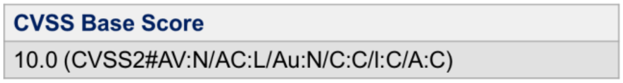
Exploitability = 20 X AccessVector X AccessComplexity X Authentication

Exploitability = 20 x Network x Low x None

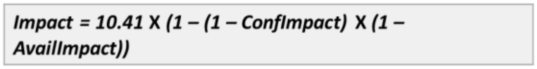
Exploitability = 20 x 1.000 x 0.710 x 0.704

Exploitability = 9.9968 => 10.0

- **Impact Score**



CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)



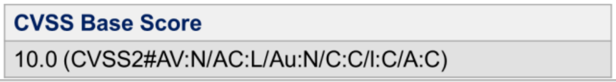
Impact = 10.41 X (1 – (1 – ConfImpact) X (1 – AvailImpact))

Impact = 10.41 x (1- (1 – Complete) x
(1 – Complete) x (1 – Complete))

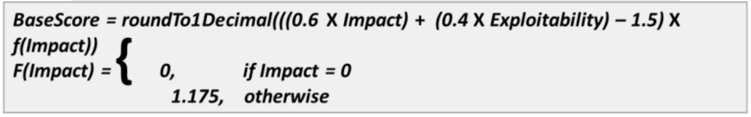
Impact = 10.41 x (1- (1 – 0.660) x
(1 – 0.660) x (1 – 0.660))

Impact = 10.0

- **Base Score**



CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)



BaseScore = roundTo1Decimal(((0.6 X Impact) + (0.4 X Exploitability) – 1.5) X f(Impact))

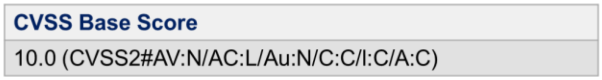
$$F(Impact) = \begin{cases} 0, & \text{if } Impact = 0 \\ 1.175, & \text{otherwise} \end{cases}$$

BaseScore = (((0.6 x Impact) +
(0.4 x Exploitability)
– 1.5 x f(Impact)

BaseScore = (((0.6 x 10.0) +
(0.4 x 10.0)
– 1.5) x 1.176)

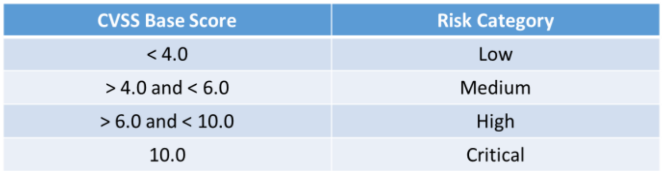
BaseScore = 9.996 => 10.0

- **Why is a Base Score important?**



CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

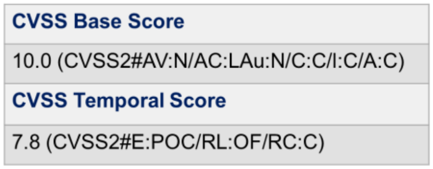
  - Numerical ratings are used by the vulnerability software to categorize vulnerabilities



CVSS Base Score	Risk Category
< 4.0	Low
> 4.0 and < 6.0	Medium
> 6.0 and < 10.0	High
10.0	Critical

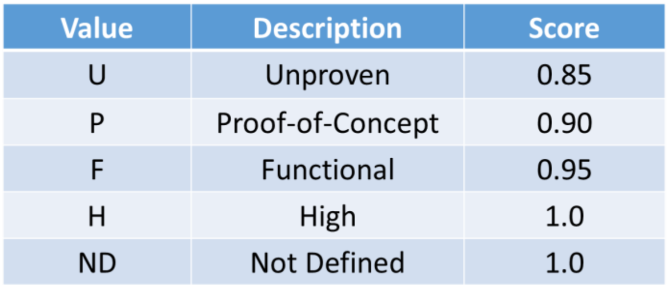
  - Risk factor: Critical

- **CVSS Temporal Score**
  - **CVSS Temporal Score**
    - Temporal scores change over the lifetime of the vulnerability
    - As exploits are developed, disclosed, and mitigations made available, the score changes
  - **Temporal Metrics**
    - Exploitability
    - Remediation Level
    - Report Confidence
  - **Temporal Metrics: Exploitability**
    - Current state of exploitation techniques or automated exploitation available



CVSS Base Score
10.0 (CVSS2#AV:N/AC:LAu:N/C:C/I:C/A:C)
CVSS Temporal Score
7.8 (CVSS2#E:POC/RL:OF/RC:C)

  - **Exploitability (E) Metric**
    - Current state of exploitation techniques or automated exploitation available



Value	Description	Score
U	Unproven	0.85
P	Proof-of-Concept	0.90
F	Functional	0.95
H	High	1.0
ND	Not Defined	1.0

- **Remediation Level (RL) Metric**
  - Used to decrease temporal score as mitigations and fixes are made available

Value	Description	Score
O	Official Fix	0.87
T	Temporary Fix	0.90
W	Workaround	0.95
U	Unavailable	1.0
ND	Not Defined	1.0

- **Report Confidence (RC) Metric**
  - Used to show the level of confidence in the existence of the vulnerability and the technical details of the report

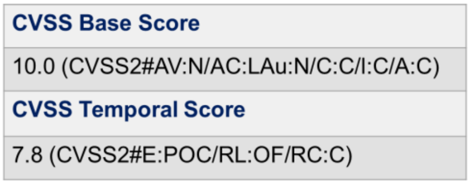
Value	Description	Score
UC	Unconfirmed	0.90
UR	Uncorroborated	0.95
C	Confirmed	1.0
ND	Not Defined	1.0

- **Calculating Temporal Metrics**

TemporalScore =

BaseScore x Exploitability x

RemediationLevel x ReportConfidence



CVSS Base Score
10.0 (CVSS2#AV:N/AC:LAu:N/C:C/I:C/A:C)
CVSS Temporal Score
7.8 (CVSS2#E:POC/RL:OF/RC:C)

- **Validation of Results**
  - **Validating of Results**
    - CVSS Scores are helpful, but they alone don't tell you how a vulnerability affects *your* systems
    - Some vulnerabilities are:
      - False Positives
      - Documented Exceptions
      - Informational Results

- **False Positives**
    - Scanners can often report that a vulnerability exists even if it doesn't
    - How often this occurs is known as the *false positive error rate*
    - Vulnerabilities are validated and verified
        - Check if a patch is missing
        - Attempt to exploit erroneous code
        - Verify the system configuration
- **Documented Exceptions**
    - Accepted vulnerabilities that are known, but will not be fixed by the organization
    - Once this risk is accepted by management, they should be documented in the scanner to prevent future reporting of them
- **Informational Results**
    - Not everything reported by the scanner is considered a vulnerability
    - Some are reported as "informational"
    - Typical "informational" items are configurations that would allow an attacker to perform reconnaissance
- **Compare Results with Other Information Sources**
    - Logs from servers, network devices, applications, and other sources
    - Configuration management systems
    - Security Information and Event Monitoring (SIEM)
- **Conduct Trend Analysis**
    - Trend analysis also allows the analyst to ensure the vulnerability management program is working effectively

- **Common Vulnerabilities**
    - **Common Vulnerabilities**
        - Vulnerability scanners can detect 1000s of different types of vulnerabilities
        - We are NOT going to cover each and every one of them individually…
        - But, we will cover the different types
        - Server and Host Vulnerabilities
        - Network Vulnerabilities
        - Virtualization Vulnerabilities
        - Web Application Vulnerabilities
        - Internet of Things (IoT) Vulnerabilities
- **Server and Host Vulnerabilities**
    - **Server and Host**
        - Missing Patches
        - Unsupported Software (OS/Apps)
        - Buffer Overflows
        - Privilege Escalation

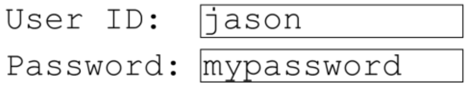
        - Arbitrary Code Execution
        - Insecure Protocol Use
        - Debugging Modes
    - **Missing Patches**
        - One of the most common issues found
        - Comes from improper patch management
    - **Unsupported Software**
        - Software vendors don't support software forever, they have an "end of life" date
        - After this date, no more patches are released for the software
    - **Buffer Overflows**
        - Occurs when the attacker manipulates a program to place more data into memory than it is allocated for causing overflow
        - Another specific type is integer overflow
        - These vulnerabilities tend to exist for a long time, but are corrected by a patch
        - In 2015, over 85% of the data breaches were cause by buffer overflows
    - **Privilege Escalation**
        - Occurs when an attacker upgrades their level of access to an admin or root user
        - For example, CVE-2016-7255 is an example in Windows Vista, 2008, 7, 8.1, 10, and 2016 machines
        - Kernel-mode drivers are exploited to allow local users to become an admin
    - **Arbitrary Code Execution**
        - Allows attacker to run software on a targeted victim machine
        - Remote code execution is worse, because it allows it to occur over network
    - **Insecure Protocol Use**
        - Older protocols not design for security
        - FTP, Telnet, SMBv1, …
    - **Debugging Modes**
        - Debugging modes give lots of information to developers, but should be disabled prior to server and code deployment
        - Debugging information could give attackers a lot of information during a reconnaissance
- **Network Vulnerabilities**
    - **Network Vulnerabilities**
        - Missing Firmware Updates
        - SSL and TLS Issues
        - Domain Name Service (DNS) Issues

        - Internal IP Disclosure
        - Virtual Private Network (VPN) Issues
    - **Missing Firmware Updates**
        - Network devices rely on firmware for their operating systems
        - Firmware needs patching and upgrades
    - **SSL and TLS Issues**
        - Secure Socket Layer (SSL) and Transport Layer Security (TLS) are designed to secure information sent over the internet (such as HTTPS)
    - **Outdated SSL/TLS Versions**
        - SSL is insecure and shouldn't be used
        - Admins should disable support for older versions (SSL and TLS before v1.2)
    - **Insecure Cipher Use**
        - SSL/TLS are only the protocol used, not the cipher
        - Cipher is the encryption algorithm
    - **SSL/TLS Certificate Problems**
        - Certificates identify servers and exchange the encryption keys
    - **DNS Issues**
        - DNS servers are victims of reconnaissance and other attacks
    - **Internal IP Disclosure**
        - Networks that use NAT attempt to hide their internal IP structure
        - Information could be leaked in headers if a server isn't configured properly
    - **VPN Issues**
        - VPNs consist of application protocols and SSL/TLS encrypted tunnels
        - Configuration issues and missing firmware patches can also affect VPNs
- **Virtualization Vulnerabilities**
    - **Virtualization Vulnerabilities**
        - VM Escape
        - Management Interface Access
        - Virtual Host Patching
        - Virtual Guest Issues
        - Virtual Network Issues
    - **VM Escape**
        - Most serious of all virtualization issues
        - Occurs when an attack can break out of the virtual machine (guest) and reach the host (hypervisor)
        - In May 2017, a hacking contestant stitched together 3 different exploits and managed to perform a VM escape
          Source: https://arstechnica.com/information-technology/2017/03/hack-

that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/

- **Management Interface Access**
    - This interface controls access to all the virtual machines and can configure them
    - Should be highly secured, including use of two-factor authentication
- **Virtual Host Patching**
    - Just like other servers, Virtual hosts need patching of their OS and software
    - This can help prevent VM Escape
- **Virtual Guest Issues**
    - Each guest represents another server on the network, and they all need patching
    - Ensure your remediation and patch management considers all your VMs
    - Ensure your vulnerability management program also scans Guest VMs
- **Virtual Network Issues**
    - Virtual firewalls, routers, and switches all need to be considered as part of your scanning program
    - If embedded as part of your VM solution, ensure appropriate patching is being done to prevent attacks

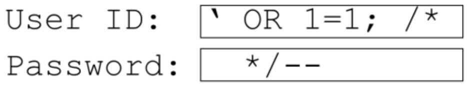
- **Web Application Vulnerabilities**
    - **Web Application Vulnerabilities**
        - Injection Attacks
        - Cross-Site Scripting (XSS)
        - Cross-Site Request Forgery (CSRF)
    - **Injection Attacks**
        - Send commands through a web server to a backend system, bypassing the normal security controls
        - Most commonly done as an SQL inject
        - Prevent this through input validation and using least privilege for the databases
    - **SQL Injection Attacks**



User ID: jason

Password: mypassword

```
select * from Users where user_id= ‘jason’ and password = ‘mypassword’
```



User ID: ` OR 1=1; /*

Password: */--

```
select * from Users where user_id= ‘` OR 1 = 1; /* ‘ and password =‘ */--’
```

- **Cross-Site Scripting (XSS)**
    - Attacker embeds scripting commands on a website that is executed by a regular user without knowing it
    - Victim in this case is the regular user, not the server
    - If one of these are discovered during a scan, you need to work with the developer to fix the code and setup proper controls to prevent it in the future
- **Cross-Site Request Forgery**
    - Attacker forces a user to execute actions on web server which they authenticated
    - Attacker cannot see web server's response, but this attack can be used to have victim transfer funds, change their password, etc.
- **Web Application Scans**
    - Nessus and Qualysguard can scan for web vulnerabilities, but they aren't specialized (like Nikto) to do it

- **Internet of Things (IoT)**
    - **Internet of Things (IoT)**
        - Smart TVs and Consumer Devices
        - SCADA
            - Supervisory Control and Data Acquisition Systems
        - ICS
            - Industrial Control Systems

Domain 3: Cyber Incident Response

- **Intro to Cyber Incident Response**
    - **What does this section cover?**
        - Phases of an incident response
        - Creating an incident response team
        - How to classify an incident
        - Analyzing network events
        - Detecting network probes and attacks
        - Investigating issues on a host/server
        - Investigating service and applications
        - Building a basic forensic toolkit
        - Capabilities of different forensic tools
        - How to conduct a forensic investigation
    - **What is Cyber Incident Response?**
        - Actions taken in response to a security incident or event
        - An organized approach to understanding the incident, mitigating its negative effects, planning the recovery, and investigating the root cause
    - **Bottom Line…**
        - We will discuss the high-level concepts of how to develop a cyber incident response program and how the incident response team should operate during a cyber incident, including the basics of digital forensics and its associated toolsets
- **Security Incidents**
    - **Cyber Incidents Will Happen**
        - No matter what your organization does to prevent a cyber incident…eventually one will happen to you
        - How will you respond?
        - How will you react?
        - How will you recover?
    - **You Must Plan Your Response**
        - Plan in advance your response
        - Allows you to have a coordinated and methodical response
        - Prior planning minimizes the damage and decreases your response time
    - **Security Events and Incidents**
        - Event
            - Any observable occurrence in a system or network
        - Adverse Event
            - Any event that has negative consequences
        - Incidents

        - An imminent threat of violation, or a violation itself, of a security policy, acceptable use policy, or standard security practice

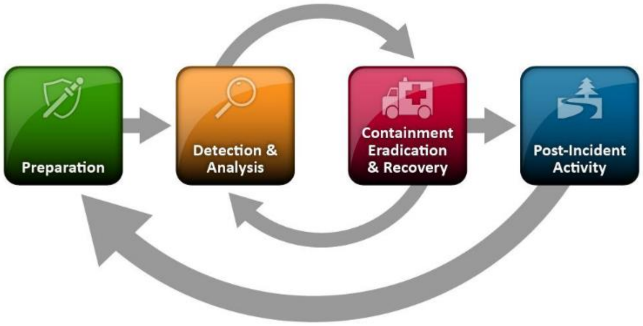
Not every event is an incident, but every incident contains at least one event.

  - **Computer Security Incident Response Team (CSIRT)**
    - Team of professionals responsible for handling a security incident within an organization by using standardized procedures
- **Incident Response Teams**
  - **Creating the Team**
    - Members are permanent or temporary
    - Core team is cybersecurity professionals with incident response experience
    - Temporary members brought in for specific cases (like a DB Admin for SQL)
    - Smaller organizations have CSIRT as a collateral role in addition to their day job
  - **What does management do?**
    - Active role in an incident response
    - Ensure team has funding, resources, and expertise needed to conduct incident response
    - Make critical business decisions
    - Communicate with legal or news media
    - Communicate with key stakeholders
  - **So, who is on the CSIRT?**
    - Leader is a skilled Incident Responder
    - Subject matter experts
    - IT support staff
    - Legal counsel
    - Human resource staff
    - Public relations and marketing staff
  - **Can you outsource the CSIRT?**
    - Retaining a third-party gives you instant capability without daily resourcing
    - Can be very expensive
    - Ensure your organization is comfortable with the third-party's guaranteed response time
    - Agree upon the scope of work to be performed
  - **Scope of Control for a CSIRT**
    - What would trigger activation of CSIRT?
    - Who authorizes the activation?

- Do they respond for all parts of the organization, or just specific ones?
- Can CSIRT talk to law enforcement?
- Can CSIRT talk to the media?
- How would CSIRT escalate an issue?

- **Testing the Teams**
  - Plans without testing are ineffective
  - You must ensure the teams are trained and ready for an incident response
  - Testing allows a walkthrough of the policy, procedures, and playbooks
  - Can be combined with a penetration test to simulate a real attacker

- **Incident Response Phases**



This process is not linear…it is cyclical
NIST SP 800-61
(Computer Security Incident Handling Guide)

- **Preparation**
  - Takes preparation to build a well-prepared CSIRT
  - Requires proper policy foundation within the organization
  - Preparation includes building proper cyber defenses in the organization
  - Also, includes identifying/training personnel and building response kits
- **Preparation: Toolkits**
  - Digital forensic workstations
  - Forensic software
  - Packet capture devices
  - Spare servers/network gear
  - Backup devices
  - Blank removable media
  - Collection, analysis, & reporting laptops
  - Portable printers
  - Office supplies
  - Evidence collection materials
- **Detection and Analysis**
  - Hardest to standardize

        - Tools help in detection, but it takes a trained analyst to understand all the details during analysis
        - When detection occurs, analysts shift to validation mode, then into analysis
        - Primarily passive activities designed to uncover and analyze incident
    - **Detection and Analysis: Event Indicators**
        - Alerts
            - IDS/IPS, SIEM, Anti-virus, or other software alerts
        - Logs
            - From operating systems, services, applications, network devices, and network flows
        - Publicly Available Information
            - News, media, and other open-source information
        - People
            - Suspicious activity reported by users or admins
    - **Detection and Analysis: Best Practices for Analysis**
        - Profile networks/systems
        - Understand the baseline
        - Create good logging policies
        - Conduct event correlation
        - Synchronize network & system clocks
        - Maintain organization knowledge base
        - Capture network traffic ASAP in incident
        - Filter information to reduce confusion
        - Know when to bring in outside help
    - **Containment, Eradication, and Recovery**
        - Focuses on stopping the spread of the incident, remove it from the network, and recovering from it
        - Phase focuses on active detection and removal of the incident
    - **Containment, Eradication, and Recovery (5 Steps)**
        - Pick containment strategy
        - Use strategy to limit the damage incident causes
        - Gather evidence needed for potential future legal actions
        - Identify attacking system or attacker
        - Remove effects of incident and recover normal business operations
    - **Post-Incident Activities**
        - CSIRT isn't done once the incident is contained and eradicated, they still need to conduct:
            - Event reconstruction

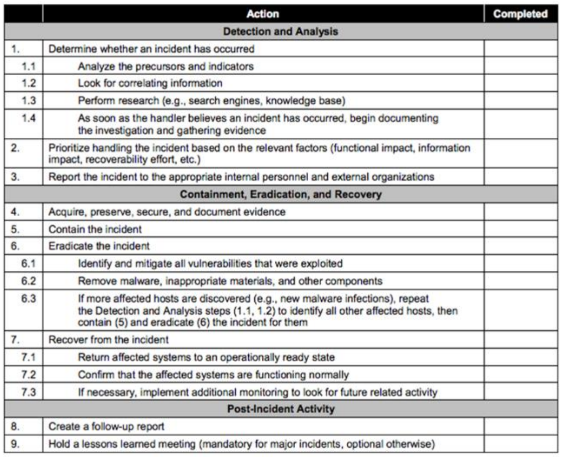
        - Lessons learned
        - Evidence retention
    - **Post-Incident Activities: Event Reconstruction**
        - Recreate a timeline of the incident
        - Identify the root cause of the intrusion and/or incident
        - Conduct consultations with system administrators and management
    - **Post-Incident Activities: Lessons Learned**
        - Utilizes the timeline to aid improvement of procedures and tools used by CSIRT
        - Group discussion to determine how the incident was handled, and how it could have been handled better.
        - Lessons learned must be fed into the ITSM processes in order to follow-on actions to be taken
        - What happened and when?
        - How did staff perform?
        - Were procedures followed?
        - Were procedures adequate?
        - What should have been done differently?
        - Was information shared effectively?
        - How could we detect incident sooner?
        - What new tools or resources does the organization need?
    - **Post-Incident Activities: Evidence Retention**
        - Large quantities of evidence have been collected
        - What do we do with it all?
        - CSIRT must identify internal/external retention requirements

If legal actions will be conducted, consult an attorney before deleting anything!

    - **Post-Incident Activities: Evidence Retention Timelines**
        - US Government Agencies must retain all incident handling items for **3 years** due to legal requirements
        - Most organizations maintain records for **2 years**, unless otherwise required by regulatory requirements
- **Policy & Procedures**
    - **Incident Response Policy**
        - Foundation of the organization’s Incident Response program
        - Guides efforts at a high-level
        - Provides authority for response efforts
        - Approved by CEO or CIO

- Should be fairly timeless

- **Contents of the Policy**
  - Statement of management commitment
  - Purpose
  - Objectives
  - Scope of policy
  - Definitional terms
  - Roles, responsibilities, and authority
  - Incident prioritization scheme
  - Measures of performance for CSIRT
  - Reporting requirements
  - Contact information
- **Incident Response Procedures**
  - Detailed information
  - Step-by-step guidelines
  - Not a replacement for CSIRT's professional judgement and expertise
  - Often developed as a specific *playbook*
- **What is a Playbook?**
  - Describes a response to a high severity type of incident, such as:
    - Data breach of financial information
    - Data breach of personally identifiable information
    - Phishing attack against customers
    - Web server defacements
    - Loss of corporate laptop
    - Intrusion into the corporate network
    - Windows Golden Ticket reset
- **Incident Response Checklist**

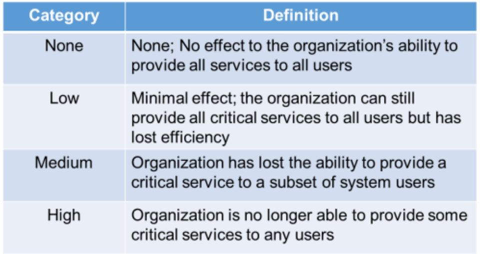


	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

NIST SP 800-61
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- **Communication and Info Sharing**
  - **Communication and Info Sharing**
    - During an incident, how will you communicate and share information?
  - **Internal Communication**
    - How will the CSIRT communicate amongst themselves and to leadership?
    - How will management communicate to the other employees?
  - **Internal Communication**
    - Incident response plan dictates how you will communicate during an incident
    - Use an out-of-band communication
  - **External Communication**
    - When will you communicate with outside people like law enforcement, media, shareholders, and others?
    - Your incident response plan should state when…
  - **External Communication**
    - Law Enforcement
      - If incident involves criminal acts (ask attorney first)
    - Information Sharing Partners
      - Do you want to share indications of your incident?
    - Vendors
      - Can provide patches and support during incident
    - Other organizations affected
      - Do you have evidence others were targeted?
    - Media or General Public
      - May be mandatory depending on type of incident
      - Do you volunteer the information to the media?
- **Incident Classification**
  - **Incident Classification**
    - All incidents should be classified by their threat and severity
    - Allows comparison of current incident with past and future ones
    - Aids in personnel's understanding of the incident being worked on
  - **Classifying Threats**
    - External or Removable Media
      - Attack executed by removable media or peripheral
    - Attrition
      - Attack employing brute-force to compromise, deny, or degrade services, systems, or networks
    - Web
      - Attack executed from web-based application or site
    - Email
      - Attack executed from email or attachment

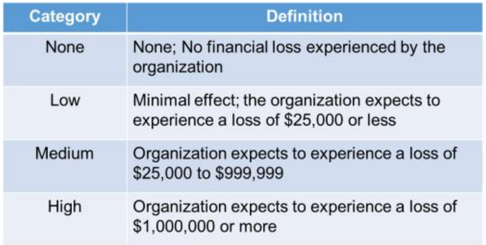
    - Impersonation
        - Attack that replaces something benign with something malicious (spoofing, SQL inject, etc)
    - Improper Usage
        - Violation of organization's AUP (P2P program)
    - Loss or Theft of Equipment
        - Computing device or media is lost or stolen
    - Unknown
        - Attack that comes from an unknown origin
    - Other
        - Attack that comes from a known origin, but doesn't fit into the other categories
    - Advanced Persistent Threat (APT)
        - Not a category under NIST, but prevalent today
        - Often funded by nation stations, organized crime, or other sources
        - Highly skilled and sophisticated attackers
        - Often takes advantage of zero-day vulnerabilities
- **Classifying Severity: Scope of Impact**
    - Degree of impairment that an incident causes an organization and the effort to recover from the incident
    - Functional impact
        - Degree of impairment to an organization



Category	Definition
None	None; No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

NIST 800-61(Table 3-2)

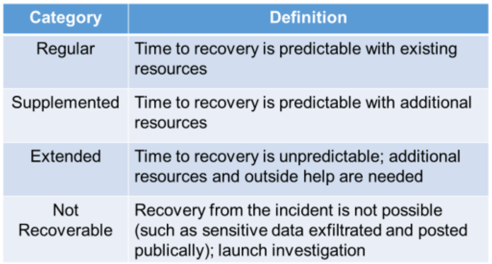
    - Economic impact
        - Amount of financial loss to an organization



Category	Definition
None	None; No financial loss experienced by the organization
Low	Minimal effect; the organization expects to experience a loss of $25,000 or less
Medium	Organization expects to experience a loss of $25,000 to $999,999
High	Organization expects to experience a loss of $1,000,000 or more

Not covered by NIST 800-61

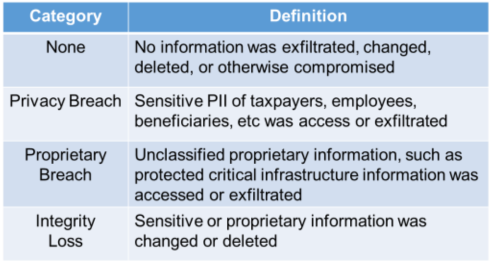
- Recoverability impact
  - Amount of time lost by an organization



Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (such as sensitive data exfiltrated and posted publically); launch investigation

NIST 800-61 (Table 3-4)

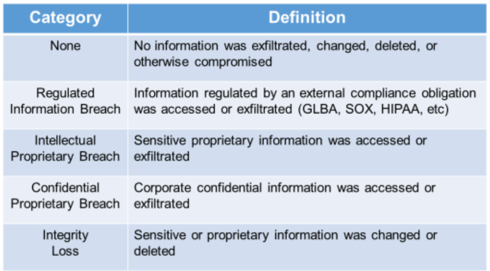
- **Classifying Severity: Types of Data**
  - The type of data involved in the incident also affects the classification of severity
  - Information impact
    - Degree of information compromise during incident
  - Information impact (Government)



Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive PII of taxpayers, employees, beneficiaries, etc was access or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

NIST 800-61 (Table 3-3)

  - Information impact (Private Company)

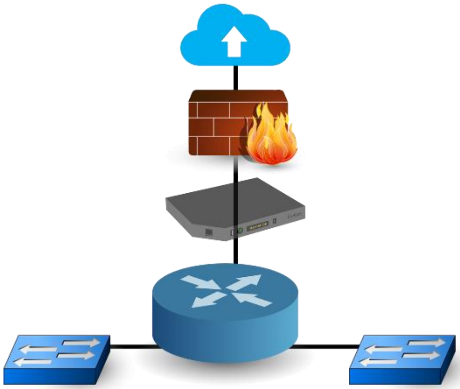


Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Regulated Information Breach	Information regulated by an external compliance obligation was accessed or exfiltrated (GLBA, SOX, HIPAA, etc)
Intellectual Proprietary Breach	Sensitive proprietary information was accessed or exfiltrated
Confidential Proprietary Breach	Corporate confidential information was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

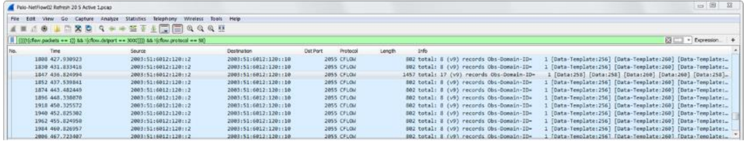
Not covered by NIST 800-61

- **Network Event Monitoring**
  - **Network Event Monitoring**
    - Network event analysis is a common task for cybersecurity analysts
    - Gather, correlate, and analyze data from different systems/sensors on network
    - Used to detect or prevent incidents

- **Router-based Monitoring**
  - Provides data flow on the network and information on the status of the device
  - Relies on capturing the data about the traffic passing through a router
  - Called *network flows*
- **Network Flows**
  - Netflow, sFlow, J-Flow, …
    - All are standards for monitoring traffic flows
    - Count information about the traffic at the interface
    - Samples traffic (1:100, 1:1000, etc)
  - RMON
    - Operates at layers 1, 2, 3, 4 of the OSI model
    - Operates as client/server model with probes
    - Provides statistics, history, alarms, and events to a Management Information Base (MIB)
  - SNMP (Simple Network Management)
    - Collects information about routers/switches
    - Information is about the devices themselves, not the traffic crossing those devices

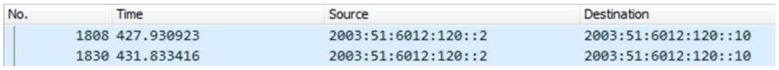


- **Example Network Flows**

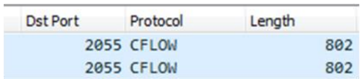


Palo-NetFlow02 Refresh 20 S Active 1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression… +

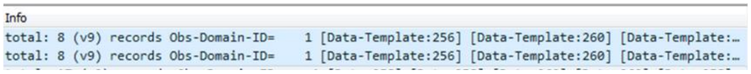
```
(((!(cflow.packets == 1)) && !(cflow.dstport == 3000))) && !(cflow.protocol == 58)
No.   Time        Source               Destination           Dst Port Protocol  Length Info
 1808 427.930923  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1830 431.833416  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1847 436.824994  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW       1457 total: 17 (v9) records Obs-Domain-ID=  1 [Data:258] [Data:258] [Data:260] [Data:260] [Data:258]…
 1852 437.539841  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1874 443.482449  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1896 448.338078  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1918 450.325572  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1940 452.825302  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1962 455.824958  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 1984 460.826957  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
 2006 467.723407  2003:51:6012:120::2  2003:51:6012:120::10      2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=  1 [Data-Template:256] [Data-Template:260] [Data-Template:…
```



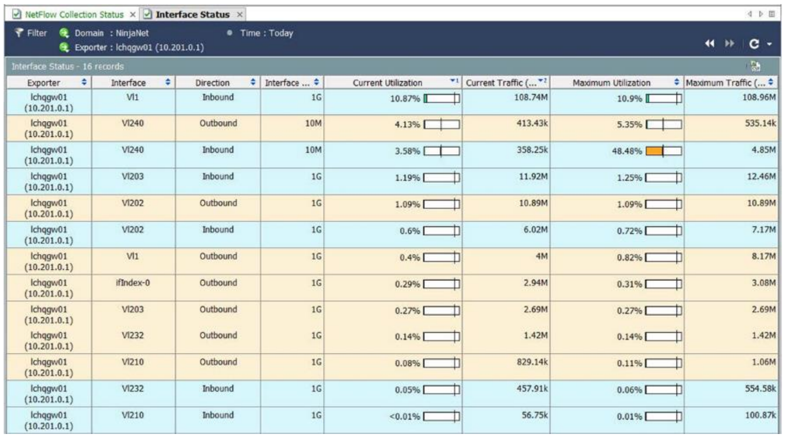
```
No.   Time        Source               Destination
 1808 427.930923  2003:51:6012:120::2  2003:51:6012:120::10
 1830 431.833416  2003:51:6012:120::2  2003:51:6012:120::10
```



```
Dst Port Protocol  Length
    2055 CFLOW        802
    2055 CFLOW        802
```



```
Info
total: 8 (v9) records Obs-Domain-ID=   1 [Data-Template:256] [Data-Template:260] [Data-Template:…
total: 8 (v9) records Obs-Domain-ID=   1 [Data-Template:256] [Data-Template:260] [Data-Template:…
```

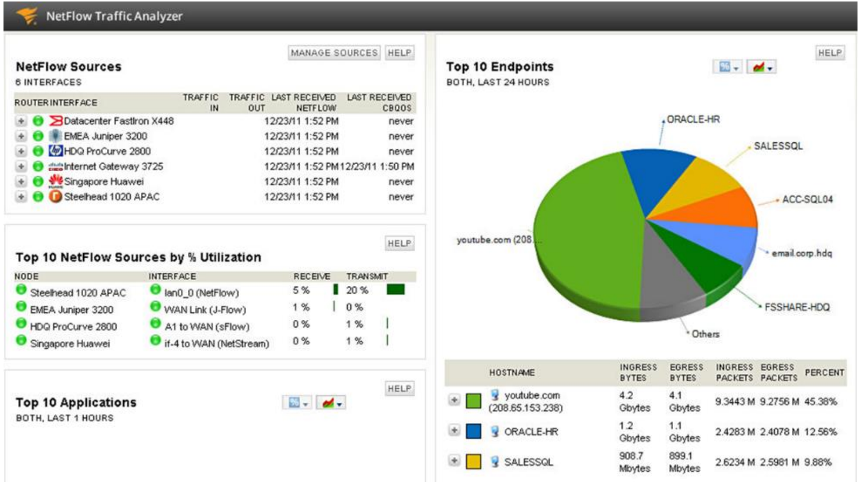


Interface Status - 16 records

Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic (...	Maximum Utilization	Maximum Traffic (...
lchqgw01 (10.201.0.1)	Vl1	Inbound	1G	10.87%	108.74M	10.9%	108.96M
lchqgw01 (10.201.0.1)	Vl240	Outbound	10M	4.13%	413.43k	5.35%	535.14k
lchqgw01 (10.201.0.1)	Vl240	Inbound	10M	3.58%	358.25k	48.48%	4.85M
lchqgw01 (10.201.0.1)	Vl203	Inbound	1G	1.19%	11.92M	1.25%	12.46M
lchqgw01 (10.201.0.1)	Vl202	Outbound	1G	1.09%	10.89M	1.09%	10.89M
lchqgw01 (10.201.0.1)	Vl202	Inbound	1G	0.6%	6.02M	0.72%	7.17M
lchqgw01 (10.201.0.1)	Vl1	Outbound	1G	0.4%	4M	0.82%	8.17M
lchqgw01 (10.201.0.1)	ifIndex-0	Outbound	1G	0.29%	2.94M	0.31%	3.08M
lchqgw01 (10.201.0.1)	Vl203	Outbound	1G	0.27%	2.69M	0.27%	2.69M
lchqgw01 (10.201.0.1)	Vl232	Outbound	1G	0.14%	1.42M	0.14%	1.42M
lchqgw01 (10.201.0.1)	Vl210	Outbound	1G	0.08%	829.14k	0.11%	1.06M
lchqgw01 (10.201.0.1)	Vl232	Inbound	1G	0.05%	457.91k	0.06%	554.58k
lchqgw01 (10.201.0.1)	Vl210	Inbound	1G	<0.01%	56.75k	0.01%	100.87k

- **SNMP v3**
  - Simple Network Management Protocol
  - Adds encryptions, authentication, and user capabilities to SNMP traffic
  - SNMP v1 and SNMP v2 are considered obsolete and a security risk
- **Active Monitoring**
  - Request is sent to a remote system and data is collected from the end point
  - Data contains information about:
    - Availability
    - Routes
    - Packet delays
    - Packet loss
    - Bandwidth
- **Active Monitoring (Examples)**
  - Ping
    - Data acquired by using ICMP on remote system
    - Basic up and down information and latency only
  - iPerf
    - Measures maximum bandwidth of a given network
    - Remote testing of a link
    - Useful to determine a baseline of the network
- **Passive Monitoring**
  - Uses a network tap to copy all traffic between two devices
  - Useful for after-the-fact analysis
  - Detailed information about:
    - Rate of traffic
    - Protocols used
    - Content

- **Network Monitoring Tools**
  - **Network Monitoring Tools**
    - Many network monitoring tools are available for different use cases
    - Combination of network data is more powerful than a single piece of data
    - Different tools can analyze data in different ways, as well
  - **Wireshark**
    - Passive monitoring and packet capture
    - Used for packet analysis
  - **SolarWinds: Netflow Traffic Analyzer**



NetFlow Sources
6 INTERFACES

ROUTER INTERFACE	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
Datacenter FastIron X448			12/23/11 1:52 PM	never
EMEA Juniper 3200			12/23/11 1:52 PM	never
HDQ ProCurve 2800			12/23/11 1:52 PM	never
Internet Gateway 3725			12/23/11 1:52 PM	12/23/11 1:50 PM
Singapore Huawei			12/23/11 1:52 PM	never
Steelhead 1020 APAC			12/23/11 1:52 PM	never

Top 10 NetFlow Sources by % Utilization

NODE	INTERFACE	RECEIVE	TRANSMIT
Steelhead 1020 APAC	lan0_0 (NetFlow)	5 %	20 %
EMEA Juniper 3200	WAN Link (J-Flow)	1 %	0 %
HDQ ProCurve 2800	A1 to WAN (sFlow)	0 %	1 %
Singapore Huawei	if-4 to WAN (NetStream)	0 %	1 %

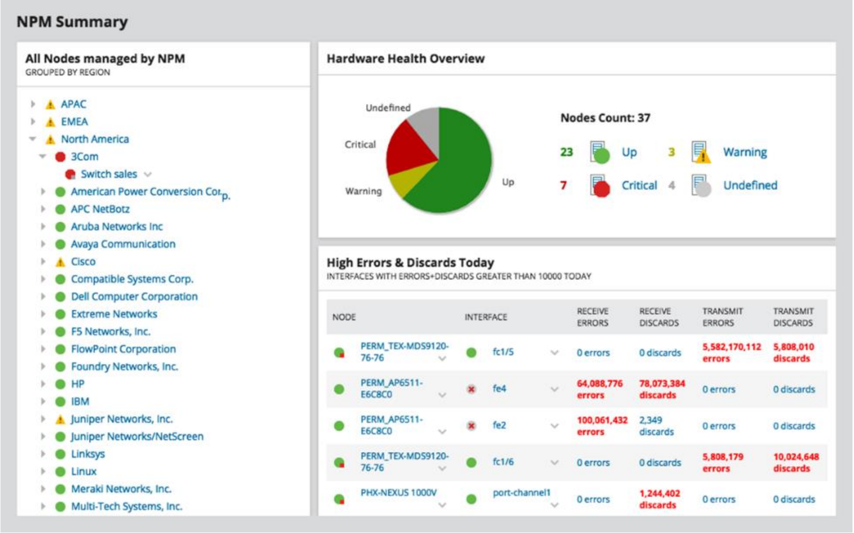
Top 10 Applications
BOTH, LAST 1 HOURS

Top 10 Endpoints
BOTH, LAST 24 HOURS

	HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
🟩	youtube.com (208.65.153.238)	4.2 Gbytes	4.1 Gbytes	9.3443 M	9.2756 M	45.38%
🟦	ORACLE-HR	1.2 Gbytes	1.1 Gbytes	2.4283 M	2.4078 M	12.56%
🟨	SALESSQL	908.7 Mbytes	899.1 Mbytes	2.6234 M	2.5981 M	9.88%

http://demo.solarwinds.com

  - **SolarWinds: Network Performance Monitor**



NPM Summary

All Nodes managed by NPM
GROUPED BY REGION

- APAC
- EMEA
- North America
  - 3Com
    - Switch sales
  - American Power Conversion Corp.
  - APC NetBotz
  - Aruba Networks Inc
  - Avaya Communication
  - Cisco
  - Compatible Systems Corp.
  - Dell Computer Corporation
  - Extreme Networks
  - F5 Networks, Inc.
  - FlowPoint Corporation
  - Foundry Networks, Inc.
  - HP
  - IBM
  - Juniper Networks, Inc.
  - Juniper Networks/NetScreen
  - Linksys
  - Linux
  - Meraki Networks, Inc.
  - Multi-Tech Systems, Inc.

Hardware Health Overview

Nodes Count: 37

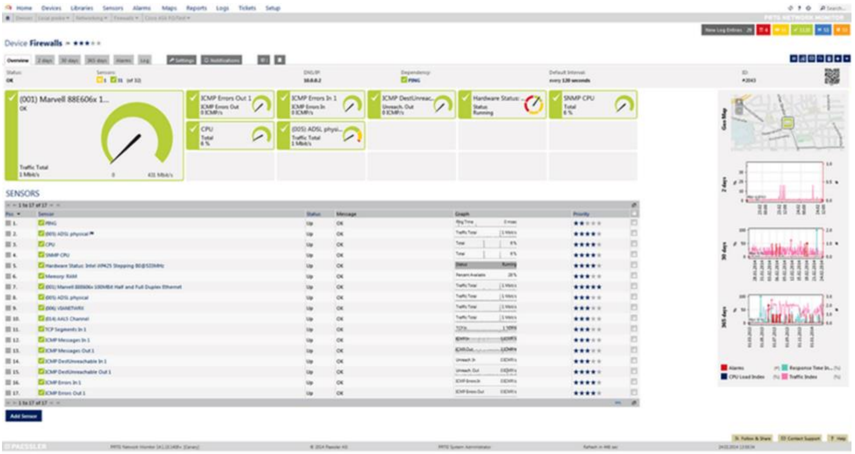
23	Up	3	Warning
7	Critical	4	Undefined

High Errors & Discards Today
INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
PERM_TEX-MDS9120-76-76	fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
PERM_AP6511-E6C8C0	fe4	64,088,776 errors	78,073,384 discards	0 errors	0 discards
PERM_AP6511-E6C8C0	fe2	100,061,432 errors	2,349 discards	0 errors	0 discards
PERM_TEX-MDS9120-76-76	fc1/6	0 errors	0 discards	5,808,179 errors	10,024,648 discards
PHX-NEXUS 1000V	port-channel1	0 errors	1,244,402 discards	0 errors	0 discards

http://demo.solarwinds.com

  - **PRTG**
    - Paessler Router Traffic Grapher
    - Server monitoring, network monitoring, and bandwidth monitoring



- Packet sniffing
  - Monitors packet headers to determine traffic type
- Flows
  - Collects information about connections
- SNMP
  - Network devices report about events through traps
- WMI (Windows Management Instrumentation)
  - Management data of the operating system using scripts or application access

- **Nagios**
  - Network and system log monitoring tool
  - Provides GUI for system, services, and monitoring capabilities
  - “Critical” in Nagios isn’t based on CVE’s, but by thresholds you set during config
- **Catci**
  - Uses SNMP polling of network devices for status information and shows a GUI

- **Detecting Network Events**
  - **Detecting Network Events**
    - Cybersecurity analysts should be able to determine an incident based on events
    - Analysis of logs and other data are key to understanding if an event will become an incident
    - Types of Network Events:
      - Beaconing
      - Unusual bandwidth consumption
      - Link and connection failures
      - Unexpected traffic

- **Beaconing**
  - Beaconing or a heartbeat sends a signal to a Command and Control system due to a botnet or malware infection
  - Usually sent over HTTP or HTTPS
  - Can be difficult to detect
  - Generally occurs at a certain frequency or pattern
- **Unusual Bandwidth Consumption**
  - Unusual bandwidth consumption could cause service issues or can be a sign of larger trouble
- **Link and Connection Failures**
  - Generally occur due to a hardware, firmware, or software issues
  - Could be as simple as a bad module, broken cable, or unplugged connector
- **Unexpected Traffic**
  - Detected by IDS/IPS, traffic monitoring systems, or by manual observation
  - Understanding your baseline is important
  - Not all unexpected traffic is malicious, but it should be investigated/understood
  - Could be unusual based on type of traffic, end point location, or amount
- **Detecting Unexpected Traffic**
  - Baselines or Anomaly-based
    - Monitoring system alarm based on traffic that is outside the normal baseline
  - Heuristics or Behavior-based
    - Uses signatures and defined rules to detect
  - Protocol Analysis
    - Seeks to detect protocols where they aren't expected, like VPNs or IPv6 tunnels

- **Network Probes and Attacks**
  - **Network Probes and Attacks**
    - Much of your incident handling will involve network probes and attacks
    - Network probes are usually part of reconnaissance efforts and are easy to detect (like a port scan)
  - **Denial of Service (DoS)**
    - Detection:
      - Attacks on a given network, system, or service from a single source
      - Attempts to overwhelm system or network
    - Prevention:
      - Block the attacker using your firewall or IPS

- **Distributed Denial of Service (DDoS)**
    - Attacks on a given network, system, or service from simultaneous multiple sources
    - Attempts to overwhelm system or network
    - Detection:
        - Traffic coming from known botnet IPs
        - Monitoring your traffic and usage patterns
    - Prevention:
        - Network designed with distributed network of endpoints (like Akamai)
        - Ensure your networks can scale upwards
- **Detecting Rogue Devices**
    - MAC Address Validation
        - Ensure all devices are "Known Devices"
        - Check device MAC against vendor codes
    - Scan the Network to identify devices
    - Conduct physical site inspections
    - Analyze traffic for irregular behavior
- **Rogue Wired Devices**
    - Usually occurs when an employee or attacker connects a wired device
        - Adds a switch or hub to the network
    - Network Access Control and Port Security can prevent this occurring
- **Rogue Wireless Devices**
    - Can be detected by conducting wireless surveys and mapping the area
    - Often used as an Evil Twin to trick users to connect to them and steal information

- **Server and Host Events**
    - **System Monitoring**
        - Processor (CPU), Memory, and Drives
        - CPU attacks usually occur as DoS
        - Memory is monitored by the OS based on given thresholds
            - Memory leaks occur when programs don't release memory after being terminated
            - Eventually, all memory can be used up
            - System restarted to release the memory
    - **System Monitoring Tools: Windows**
        - Resource Monitor (or resmon)
            - Built-in Windows tool for monitoring
            - CPU, Memory, Disk, and Network Utilization
        - Performance Monitor (or perfmon)
            - Built-in Windows tool for monitoring

            - Supports collection from remote systems
    - **System Monitoring Tools: Linux**
        - ps
            - CPU and memory utilization, process info
        - top
            - Like ps, but also provides sorting by top usage
        - df
            - Report of disk usage
        - w
            - Accounts logged on, who ran process
    - **Malware and Unsupported Software**
        - Use centralized management tools to conduct installs and inventory
        - Antivirus and antimalware tools
        - Conduct blacklisting of software/files
        - Application whitelisting
    - **Unauthorized Access, Changes, and Privileges**
        - Users and permissions are complex with the number of systems in use
        - Central Management tools (SIM/SIEM) can correlate logs for analysis
            - Authentication logs
            - User creation logs
            - System logs
            - Application logs
            - Security event logs
- **Service and Application Events**
    - **Service/Application Events**
        - Services and Applications should be monitored per good ITSM processes
            - Are they up/down?
            - Are they responding properly?
            - Are they functioning properly?
            - Are they conducting transactions properly?
            - Are they logging properly?
    - **Service Anomalies**
        - Non-security issues:
            - Authentication errors
            - Permission issues
            - Services don’t start on boot up
            - Service failures
        - Investigate the issue to ensure it is not security related
        - Use antivirus, antimalware, file integrity checking, and whitelisting to verify

- **Checking Service Status**
  - Windows:
    - services.msc (GUI) or sc (command line)
  - Linux:
    - service –status-all (command line)
- **Service/Application Logs**
  - Windows:
    - Use Windows Event Viewer to view Application Logs
  - Linux:
    - Log to the /var/log directory
    - Use tail to view the end of the log files
- **Service/Application Behavior**
  - Create and understand a baseline
  - Log/alert on anything outside of baseline
- **Service/Application Attacks**
  - Anomalous Activity
    - Doesn't match the typical behavior
    - Investigate the activity and solve
  - New Accounts
    - Were they authorized?
    - Do they have excessive permissions?
  - Unexpected Output
    - Improper output or garbage output
    - User and admin training imperative to determining the root cause
  - Unexpected outbound communication
    - Why is the application sending out data?
    - Detect with network monitoring
  - Service Interruption
    - Simple issue or a DDoS?
    - Monitoring tools can help determine reason
  - Memory Overflows
    - Causes OS errors and crashes
    - Monitoring for them is hard
    - Detecting after a crash is easier

- **Digital Forensics**
  - **Digital Forensics**
    - Forensics are used to determine any changes, activities, or actions that have occurred on a host or server
    - Allows incident responders to determine what occurred by putting together various pieces of information

        - Similar techniques are used by incident response teams and law enforcement
    - **Documentation in Digital Forensics**
        - Documentation is one of the most important steps in digital forensics
        - Everything you do needs to be repeatable by a third-party investigator
        - Chain of Custody is imperative for use in law enforcement
    - **Forensics Toolkits**
        - Consist of specialized software and hardware to conduct imaging of hard disks and follow-on analysis
        - Mobile devices require additional specialized tool kits

- **Forensic Toolkit Components**
    - **Forensic Toolkit**
        - Contain a wide variety of software and hardware needed to conduct collection and analysis of data in the field
        - Toolkits vary widely in cost and capability
    - **Digital Forensic Workstation**
        - Conducts data capture and analysis
            - Multicore CPU
            - Maximum RAM
            - Large, fast storage
    - **Forensic Investigation Software**
        - Capture and analyze forensic images
        - Document and track investigations
            - Forensic Toolkit (FTK)
            - EnCase
            - SANS Investigative Forensic Kit (SIFT)
            - The Sleuth Kit (TSK)
    - **Write Blocker**
        - Ensures hard drives being imaged cannot be written to or its data changed
            - Hardware variants
            - Software variants
        - Ensures integrity of the captured disk
    - **Forensic Drive Duplicator**
        - Designed to copy hard drives without changing the original
        - Dedicated device that copies drive and hashes the disk image
    - **Wiped Drives and Removable Media**
        - Clean hard drives that are ready to receive disk images on
        - Drives are prepared using a drive wipe before use in the field

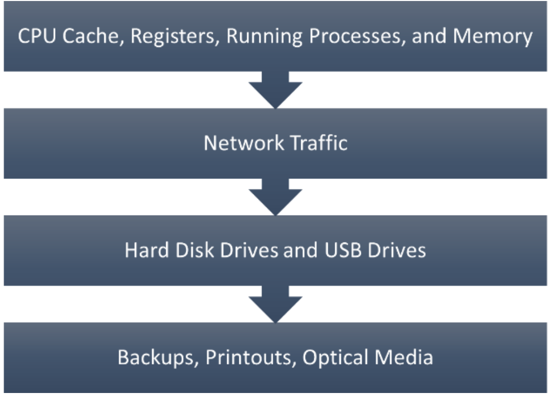
  - **Cables and Drive Adapters**
    - Be ready to copy/collect any type of media you come across while in the field
  - **Digital Camera**
    - Used to photograph system layout, system configurations, drive labels, how a machine is cabled, etc.
  - **Label Maker and Labels**
    - Label cables, components, and other items collected while in the field
  - **Documentation and Checklists**
    - Chain of Custody forms, incident response forms and plan, and more
- **Mobile Forensic Toolkits**
  - **Mobile Forensic Toolkits**
    - Mobile devices have different operating systems and security issues
    - Capturing data from mobile devices can be more difficult and needs special tools
  - **Tools to Access the SIM Card**
    - Different phones require small screwdrivers or a push pin-style tool
  - **Connection Cables**
    - Lightning cables or 30-pin for Apple
    - USB Micro, Mini, or USB-C for Android
  - **Mobile Forensic Software**
    - Specialized software for accessing mobile devices
- **Forensic Software**
  - **Forensic Software**
    - Commercial and Open-Source for:
      - Imaging
      - Analysis
      - Hashing and validation
      - Process and memory dumps
      - Password cracking
      - Log viewer
  - **Imaging Media and Drives**
    - Bit by bit copy of a drive, including the slack space and unallocated space
    - FTK Imager
    - EnCase Imager
    - dd
  - **Analysis Software**
    - Creates timeline of system changes
    - Validates file against known good copy
    - File system analysis for hidden files, changes, access, and metadata
    - Windows Registry analysis

  - Log file parsing and analysis
  - Examples:
    - Commercial:
      - FTK and EnCase
    - Open-source:
      - SIFT, CAINE, and Autopsy
- **Hashing and Validation**
  - Creates a unique file integrity check of a disk image after creation
  - Used as part of chain of custody
  - EnCase uses built-in hashing with its .EO1 format
  - Should use both MD5 & SHA1/SHA256
- **Process and Memory Dumps**
  - State of the Operating System and data in-resident memory at time of collection
  - Difficult to collect without changing the contents contained
  - Useful to capture decryption keys for full disk encryption
  - Hibernation files and crash dumps can also contain some of this data
- **Process and Memory Dumps**
  - Tools
    - fmem and LiME (Linux)
    - DumpIt (Windows)
    - Volatility Framework (Windows, Linux, OS X)
    - EnCase
    - FTK
  - Memory dumps on system can be found at %SystemRoot%\MEMORY.DMP
  - Dumps analyzed with Microsoft's WinDbg
- **Password Cracking/Recovery**
  - Encrypted and password protected files required cracking or guessing password
  - Hacking tools like John The Ripper and Cain and Able can be used
  - DOC, XLS, PPT, and ZIP files have other specialized password cracking tools:
    - Advanced Office Password Breaker
    - ElcomSoft's Distributed Password Recovery
    - Zip2John
    - …numerous otherS
- **Log Viewers**
  - Used to analyze log files from collected system images
  - Can create timelines and visual the data

- **Training and Certification**
    - **Importance of Training and Certification**
        - Full-time forensic personnel should be properly trained and certified
        - If not, evidence might not be able to be used in court
        - Forensic experts and their credentials are called into question by the defense
    - **Industry Certifications**

CCE	Certified Computer Examiner
CFCE	Certified Forensic Computer Examiner
CHFI	Computer Hacking Forensic Investigator
GCFA	GIAC Certified Forensic Analyst
GCFE	GIAC Certified Forensic Examiner
CSFA	Cybersecurity Forensic Analyst
ACE	AccessData Certified Examiner (FTK)
EnCE	EnCase Certified Examiner
DMC	Digital Media Collector
DFE	Digital Forensic Examiner

- **Forensic Investigation Process**
    - **Forensic Investigation Process**
        - Determine what you want to find out
        - Determine location to find that info
        - Document your plan
        - Acquire/preserve the evidence needed
        - Perform initial analysis (log actions)
        - Conduct deeper analysis (log actions)
        - Report on your findings
    - **Order of Volatility (Data Collection Priorities)**



CPU Cache, Registers, Running Processes, and Memory

Network Traffic

Hard Disk Drives and USB Drives

Backups, Printouts, Optical Media

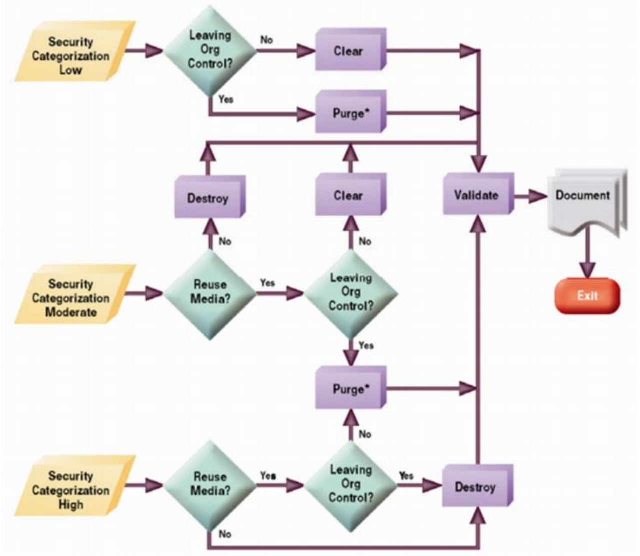
-
    - **What do you do when you find something you don't expect?**
        - There's always a risk you will find what you didn't want to find…
        - …Employee breaking the AUP

        - …Evidence of illegal activities
- **Disk Imaging**
    - **Imaging Media and Drives**
        - Bit by bit copy of a drive, including the slack space and unallocated space
        - FTK Imager
        - EnCase Imager
        - dd
    - **dd**
        - Standard Linux and UNIX tool
        - Can clone drives using bit-by-bit copy

```
# dd bs-64k if=/dev/disk1/sda1 of=/mnt/usb1/sda1.img
```

    - **FTK Imager**
        - Commercial product that is free to use
        - Documents chain of custody, adds hash, and creates metadata tags for later analysis
    - **Forensic Drive Duplicators**
        - Very expensive, dedicated devices
        - Creates images, hashes, and chain of custody metadata
    - **Write Blockers**
        - Maintain data integrity on the source disk
        - Hardware write blockers should be used for best forensic integrity
    - **Encrypted Drives**
        - Try to find the password because brute forcing is VERY slow (if possible)
        - Capture the computer while logged in to bypass drive encryption when possible
- **Incident Containment**
    - **Incident Containment**
        - Perform this as quickly as possible
        - Isolate the issue
        - Stop the spread of the incident
    - **Containment Considerations**
        - Containment isn't perfect…it is quick and dirty
        - Can cause some loss of business functionality
        - Coordinate with stakeholders before you take actions
    - **Segmentation**
        - Proactive strategy to prevent spread from one part of network to another
    - **Isolation or Removal**
        - Remove a system from your network and directly connect to internet
        - Remove the attacker (disconnect PC)
    - **Objective of Containment**
        - Limit the damage to the organization

        - Provide incident handlers an opportunity to collect evidence and repair issue
        - Maintain and operate services for your customers to use
    - **Identifying Attackers**
        - Do you need to identify the attacker?
        - Is there a good business reason why?
        - Attackers cover their tracks well, and identifying them can take a lot of time and resources, where your goal is simply to minimize business impact…
        - Law enforcement has a different viewpoint on this, though…
- **Eradication and Recovery**
    - **Eradication and Recovery**
        - Remove any artifacts of the incident
        - Restore the network to full functionality
        - Correct any security deficiencies
        - Remove malicious code, sanitize compromised media, and fix any of the affected user accounts
    - **What Recovery is Not**…
        - Not a rebuilding of the entire network…
        - Not a full redesign of the system…
        - Not a reason to buy all new equipment…
    - **Reconstruction and Reimaging**
        - Once an attacker touches your system, consider it compromised
        - Reconstruct or reimage the system from a known good backup
        - Consider the root cause of the incident so that the system isn't susceptible to the same attack vector again
    - **Patching**
        - Patch any systems that may be vulnerable to the same attack vector
        - This is a good time to rescan and patch ALL of your systems…
    - **Sanitization and Disposal**
        - **Clear**
            - Logical techniques used to sanitize data (reset to factory state or overwriting a disk with all 0s)
        - **Purge**
            - Physical or logical techniques to make data recovery from a disk infeasible using newest techniques (degaussing or overwrite 0s 35x)
        - **Destroy**
            - Data recovery infeasible and disk drive unusable for storage (melting, incinerating, destroying)



  - **Validation Effort**
    - Only authorized user accounts exist on each system in the network
    - Verify permission assigned to each user
    - Verify all systems are logging correctly
    - Verify vulnerability scans on all systems are routinely conducted
- **Finishing the Response**
  - **Finishing the Response**
    - Change Management Process
    - Lessons-Learned
    - Final Report
  - **Change Management Process**
    - Emergency Change Management Board may have authorized numerous actions during the incident response
    - Follow-up to ensure all changes have been documented properly
    - Need to ensure that network diagrams and vulnerability scan profiles updated
  - **Lessons-Learned**
    - Documents the details, the root cause, and the solution to a security incident
    - Fact-finding meetings should be conducted as close to the end of an incident response as possible
    - Needed changes identified during the lessons-learned process should be fed into the resourcing and Change Management process
  - **Final Report**
    - Every incident should finish with a compiled written report
    - Established organizational “memory”

    - Can serve as documentation in case further legal action occurs in the future
    - Can identify other deficiencies in the incident response that need to be addressed by management
  - **Final Report Includes…**
    - Timeline of incident and response events
    - Root cause of incident
    - Location and description of evidence
    - Actions taken to contain, eradicate, and recovery (and the reasoning for them)
    - Estimated impact to organization ($, time)
    - Post-recovery validation effort results
    - Documentation of lessons-learned

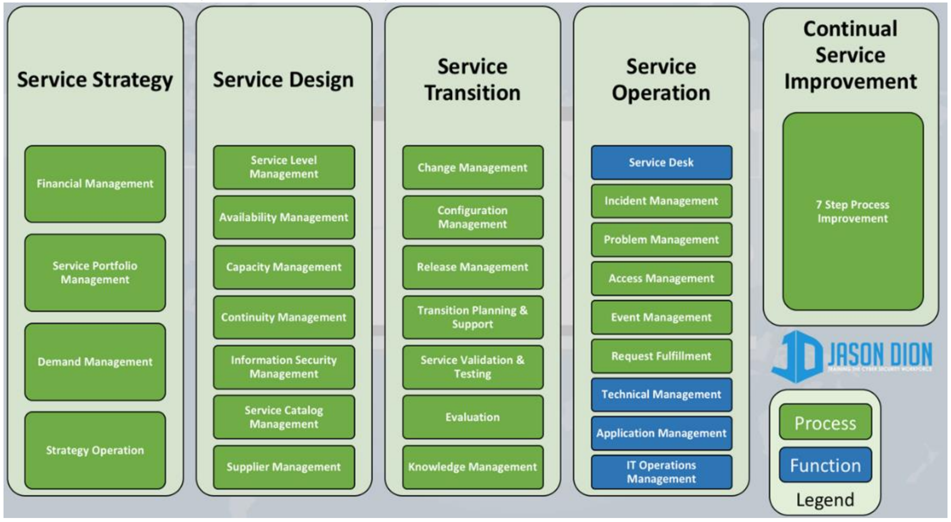
Domain 4: Security Architecture & Tool Sets

- **Security Architecture & Tool Sets**
  - **What does this section cover?**
    - Security Policies and Compliance
    - Adopting a Security Framework
    - Defense in Depth Architectures
    - Identity and Access Management
    - Security in Software Development
- **Policy Documents**
  - **Policy Documents**
    - Information Security Policy Framework
      - Policies
      - Standards
      - Procedures
      - Guidelines
  - **Policies**
    - High-level statements of intent
    - Contains broad statements about cybersecurity objectives in the company
    - Framework to meet the business goals and to define roles, responsibilities, and terms used in other security documents
  - **Policy Examples**
    - Information Security
    - Acceptable Use
    - Data Ownership
    - Data Classification
    - Data Retention
    - Account Management
    - Password
  - **Who Approves the Policies?**
    - The CEO, CISO, CIO, or CSO will approve the policy for the organization
    - Without management buy-in, the policy is a waste of your time and effort
    - Top-down approach is most effective
  - **Standards**
    - Used to implement a policy
    - Includes mandatory actions, steps, or rules needed to achieve cybersecurity
    - Approved by a lower level than C-Suite, such as Director of Information Systems

        - Standards can also exist in industry frameworks (COBIT, ITIL, etc.)
    - **Procedures**
        - Detailed step-by-step instructions created for people to perform an action
        - Actionable steps to create a consistent method for achieving a security objective
        - Example:
            - The service desk has a procedure for how to create a new user's account
            - Encompass all the security related policies, standards, and guidelines for action by your front-line employees
    - **Guidelines**
        - Not required actions, just recommended
        - Flexible in nature to allow for exceptions and allowances during a unique situation
        - Example:
            - The organization may create guidelines showing users how to store data files in a cloud service and how to encrypt the files
            - These aren't required, but may be useful to the end user and can be changed quickly
    - **Are the Rules Meant to Be Broken?**
        - Most of the time, the policies, standards, and procedures should be followed
        - How do you get permission to break these established "rules"?
        - Your information security framework should include the method for granting any necessary "exceptions"
    - **Exceptions**
        - Specific approval to deviate from a policy, standard, procedure
        - Approval authority is specified in policy
        - Exception request includes:
            - Policy, standard, or procedure requiring exception
            - Reason for exception request
            - Scope and duration of exception
            - Risks associated
            - Description of compensating controls to lower risk
- **Standard Frameworks**
    - **Standard Frameworks**
        - Creating your own cybersecurity program is daunting task
        - Standard frameworks exist to help
        - Provide a standardized approach

- **NIST Cybersecurity Framework**
    - Designed to meet one or more objective
        - Describe current posture
        - Describe desired state
        - Identify and prioritize areas for improvement
        - Assess progress toward desired state
        - Communicate risk among internal and external stakeholders
    - Framework Core is a set of five security functions that apply to all industries
    - Framework Implementation Tiers measure how the organization is positioned to meet cybersecurity objectives
    - Framework Profiles describe how the organization might approach the functions covered by Framework Core
- **ISO 27001**
    - Used to be the most commonly used information security standard
    - Declining in usage outside of regulated companies that require ISO compliance
    - To become ISO 27001 certified, an external accessor validates organizational compliance
- **ISO 27001: 14 Categories**
    - Information Security Policies
    - Organization of Information Security
    - Human Resource Strategy
    - Asset Management
    - Access Control
    - Cryptography
    - Physical and Environment Security
    - Communications Security
    - System Acquisition
    - Information Security Incident Management
    - Information Security Aspects of Business Continuity
    - Compliance with internal requirements

- **Information Technology Infrastructure Library (ITIL)**
  - Comprehensive approach to ITSM



- **COBIT**
  - Control Objectives for Information & Related Technologies
  - Set of best practices for IT governance developed by ISACA
  - Divides IT activities into four domains:
    - Plan and Organize
    - Acquire and Implement
    - Deliver and Support
    - Monitor and Evaluate
- **COBIT Framework Components**
  - COBIT framework
  - Process descriptions
  - Control objectives
  - Management guidelines
  - Maturity models
- **The Open Group Architecture Framework (TOGAF)**
  - Widely adopted approach to EA
  - Four domains:
    - Business Architecture
      - Integrates EA with business strategy
    - Application Architecture
      - Contains apps/systems used, interaction between systems, and the relation to the business processes
    - Data Architecture
      - Details approach to storing and managing info assets

        - Technical Architecture
            - Details infrastructure needed to support other domains
    - **Sherwood Applied Business Security Architecture (SABSA)**
        - Alternative model for security architecture that maps to architectural layers from different perspectives
        - Used in Enterprise Architecture (EA)

View	Architecture Layer
Business	Contextual Security
Architect	Conceptual Security
Designer	Logical Security
Builder	Physical Security
Tradesman	Component Security
Service Manager	Security Service Management

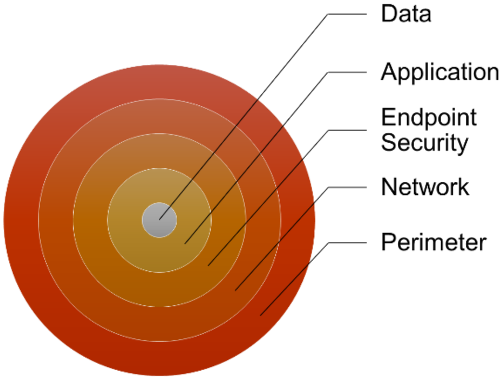
- **Policy-Based Controls**
    - **Policy-Based Controls**
        - Policies provide the control objectives the organization wants to achieve
        - This is the desired end state, not the method or activities to accomplish them
        - Security controls are used to achieve the control objectives
            - Physical Controls
            - Logical Controls
            - Administrative Controls
    - **Physical Controls**
        - Controls that impact the physical world
        - Examples:
            - Fences, gates, locks, lighting, alarm systems, fire suppressions systems, etc.
    - **Logical Controls**
        - Technical controls to enforce confidentiality, integrity, and availability
        - Examples:
            - ACLs in firewalls and routers, encryption schemes
    - **Administrative Controls**
        - Procedural controls to implement good cybersecurity practices
        - Examples:
            - Separation of duties, background checks, reviewing of log files, etc.
    - **Combining Control Objectives**
        - Physical, Logical, and Administrative controls are most effective when they are combined together
        - Example:
            - To prevent theft of the data from a server

        - Physical controls for building access
        - Logical controls like encryption
        - Administrative controls like requiring two people

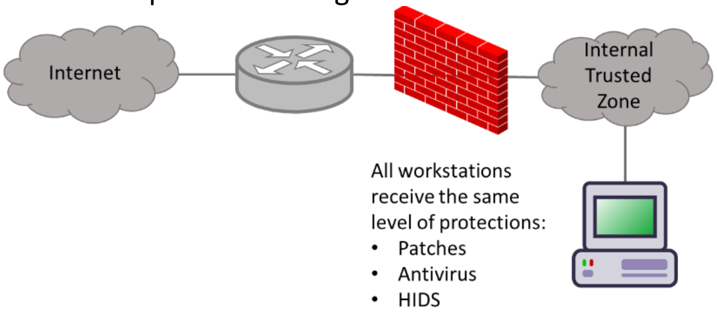
- **Audits and Assessments**
    - **Quality Control**
        - Louis V. Gerstner, former IBM Chairman
          You get what you inspect, not what you expect…
        - Evaluation of your cybersecurity program is essential to it being effectively run
        - Evaluation occurs as audits or assessments
    - **Audits**
        - Formal review of organizational cybersecurity program (internally)
        - Or, it can be for a specific compliance requirement (externally), like PCI DSS
        - Rigorous, formal testing of controls resulting in formal declaration by the auditor of compliance
    - **Assessments**
        - Less formal review of security controls
        - Usually request by the organization itself for process improvement purposes
        - Information gathered through interviews with employees (which is considered the truth) instead of independent verification
- **Laws and Regulations**
    - **Compliance with Laws and Regulations**
        - United States has various laws and regulations that must be adhered to, based on your industry (CSA+ focus)
        - European Union also has broad-ranging data protection regulations
    - **Health Insurance Portability and Accountability Act (HIPAA)**
        - Security and privacy rules for healthcare
        - Affects healthcare providers, insurers, and others storing health information
    - **Gramm-Leach-Bliley Act (GLBA)**
        - Requires financial institutions to have formal security programs in place
        - Must designate a “responsible” individual
    - **Sarbanes-Oxley (SOX) Act**
        - Requires publicly traded companies to maintain good security around their IT systems storing and processing their financial records
    - **Family Educational Rights and Privacy Act (FERPA)**
        - Requires educational institutions to implement security and privacy controls for educational records

- **Payment Card Industry Data Security Standard (PCI DSS)**
  - Rules about storage, processing, and transmission of credit/debit card info
  - Not a law, but a contractual obligation
- **Data Breach Notifications (Various State Laws)**
  - Requires companies to notify victims of data breaches in a timely manner

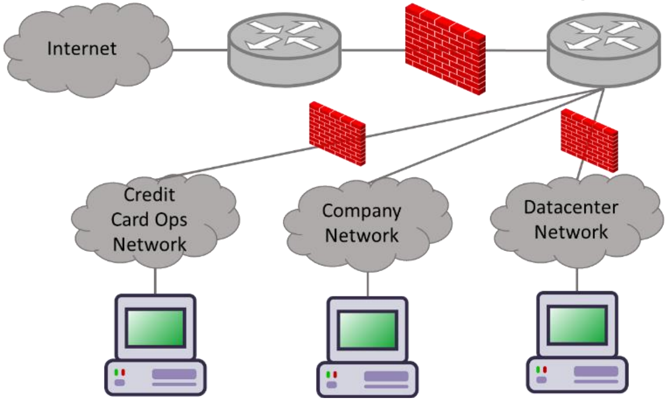
- **Defense in Depth**
  - **Defense in Depth**
    - Foundation of good security architecture
    - Does not rely on a single defensive measure or control for protection
  - **Layered Security Defense**



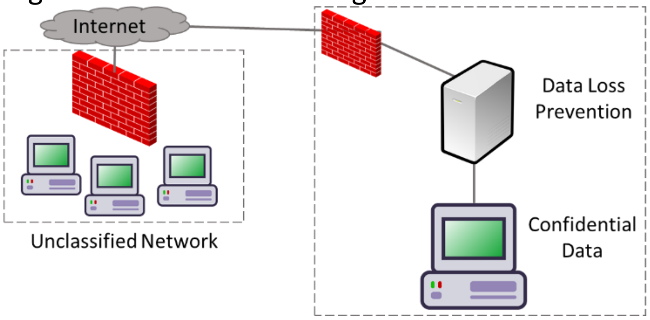
    - Difficult to design and implement
    - Must consider business needs and usability in the design of layered controls
    - Four design models
      - Uniform Protection
      - Protected Enclaves
      - Risk or Threat Analysis-based
      - Information Classification-based
  - **Uniform Protection**
    - Gives same level of protection to all data, systems, or networks
    - Can be expensive for larger networks



- **Protected Enclave**
  - Enclaves that house more sensitive data are given additional protections



- **Risk or Threat Analysis-based**
  - Addresses specific risks or threats in the design of the networks and systems
  - Example
    - If you are concerned with phishing as a threat vector, you could employ additional controls to securely scan and filter your incoming emails
- **Information or Classification-based**
  - Map data protection to different classes of information
  - Higher classification levels get additional attention and security controls



- **Combining Design Models**
  - Often, these four models are combined as opposed to picking a single model

- **Types of Controls**
  - **Types of Controls**
    - Controls prevent, detect, counteract, or limit certain security risks
      - Technical Controls
      - Administrative Controls
        - Legal Controls
      - Physical Controls

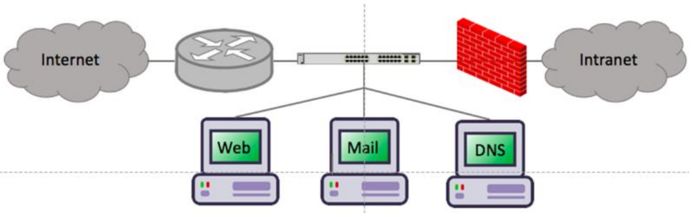
}Based on their Implementation

    - Preventive Controls
    - Detective Controls
    - Corrective Controls
    - Compensating Controls

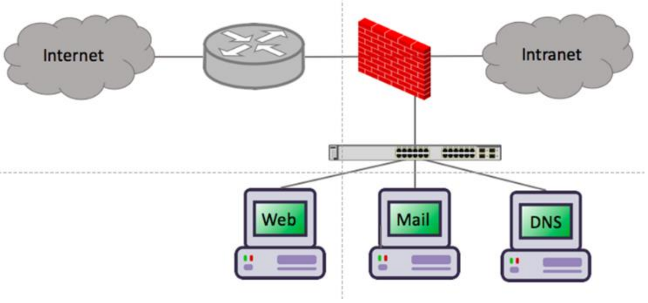
Based on when the control acts

- **Technical Controls**
  - Designed to provide security through technical measures
  - Examples
    - Firewalls
    - IDS/IPS
    - Authentication Systems
    - Network Segmentation
- **Administrative Controls (or Procedural Controls)**
  - Designed to provide security through processes and procedures
  - Legal controls are a type of these controls that are put in place by the law
  - Examples
    - Incident Response Plans
    - User Awareness Training
    - Account Creation Policy
    - Acceptable Use Policy
- **Physical Controls**
  - Designed to provide security by preventing physical access or harm to the organization's systems or facilities
  - Examples
    - Fences
    - Mantraps
    - Security Guards
    - Fire Suppression Systems
- **Preventative Controls**
  - Designed to stop an incident before it has occurred
  - Proactive measures
  - Examples
    - Firewalls
    - Antivirus
    - Training
    - Security Guards
- **Detective Controls**
  - Designed to detect when an incident occurs, capture details about it, and send an alarm/notification so someone can act
  - Examples
    - Intrusion Detection System
    - Security Cameras

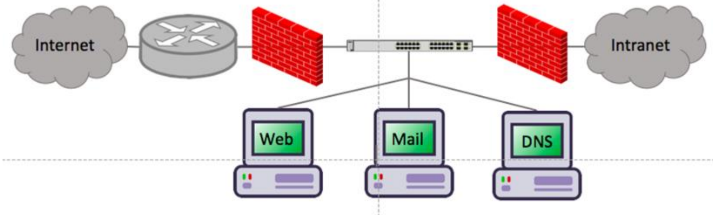
            - Logs
    - **Corrective Controls**
        - Designed to fix an issue after an incident has occurred
        - Part of incident response process
        - Reactive measures
        - Examples
            - Security Patching
            - System Rebuilding
            - Restore from Backups
    - **Compensating Controls**
        - Designed to satisfy a security requirement not being met by other controls
        - Minimizes threat down to an acceptable level of risk (based on risk appetite)
        - Examples
            - Blocking certain ports instead of upgrading all of the operating systems
            - Segmenting vulnerable software to a separate part of the network
- **Layered Network Design**
    - **Layered Network Design**
        - Combining the network architecture, configuration management, practices, and policies
        - Can be accomplished through
            - Network segmentation
            - Firewalls
            - Outsourcing network segments
    - **Network Segmentation**
        - Compartmentalization of the network
        - Benefits
            - Reduces the network's attack surface
            - Limits scope of regulatory compliance
            - Increases availability of critical services
            - Increases network efficiency
        - Segmentation is implemented through firewalls, routers, switches, and VLANs
    - **Single Firewall or Router**
        - Simplest network design utilized used to create a DMZ for a lower trusted segment of the network
        - Ensure you put protections in place between DMZ and intranet



- **Multiple Interface Firewalls**
  - Different ACL and rulesets applied to each interface, creating multiple network segments
  - Often called service-leg DMZ



- **Multi-Firewall**
  - Dual-firewalls (or more) puts a firewall at each control point
  - Allows for more stringent controls as you move deeper into the network



- **Outsourcing Segments**
  - Remote Services
    - SaaS and PaaS rely on providers for security and network designs
  - Directly Connected Remote Network
    - Acts as an extension of your intranet
    - Utilizes IaaS with direct point-to-point VPNs
    - To users, it appears the IaaS is just part of your network
    - Low-level host protections at IaaS are still handled by the third-party service provider

- **Layered Host Security**
  - **Layered Host Security**
    - Servers, desktops, laptops, smartphones are all considered hosts on your network
    - Often the most at-risk part of the network since your users directly use them

- **Common Security Controls**
    - Passwords and strong authentication
    - Encryption (file or full disk)
    - Host firewalls and Host-based IPS
    - Data Loss Prevention (DLP) software
    - Whitelisting/Blacklisting of software
    - Antimalware/Antivirus software
    - Patch management
    - System hardening
    - Configuration management
    - File Integrity Monitoring
    - Logging of events and issues
- **Cryptography: Encryption and Hashing**
    - Encrypting files or the full disk can protect "data at rest"
    - Proper storage of the encryption keys/passphrases is critical to security
    - Hashing of files can be used to ensure file integrity, as well
- **Logging, Monitoring, and Validation**
    - Logs must be securely stored and centrally monitored
    - Specialized log server or SIEM (Security Information and Event Management)
    - Tripwire, AlienVault, Splunk, …
    - Configuration Management (Microsoft SCCM and others) allow validation of system settings and software across the connected hosts

- **Data Analytics**
    - **Data Analytics**
        - Integrating logs across the devices provides the most value and information
        - Manual review of logs is time consuming
        - Automated systems can help prioritize items for review based on heuristics and previous signatures created
        - You need to conduct data aggregation and correlation, trend analysis, and historical analysis
    - **Data Aggregation and Correlation**
        - Combine data from multiple sources to identify events impacting different systems
            - System logs, authentication logs, application logs, event logs, and others into central analysis node
        - Effective as a detective control
    - **Trend Analysis**
        - Analyzes system, events, and devices to detect trends and patterns
        - Identifies issues that are outside of expected growth or usage patterns

- **Historical Analysis**
    - Analyzes system, events, and devices over time to detect trends and patterns
    - Helpful during incident responses as it looks back over a longer period of time
- **Personnel Security**
    - **Policies, Processes, and Standards**
        - Foundation of administrative controls
        - Includes:
            - Change control
            - Configuration management
            - Monitoring and response
            - **Personnel security controls**
            - Business continuity
            - Disaster Recovery
    - **Separation of Duties**
        - Requires more than one person to perform a task by breaking the task into additional parts
        - Provides a system of checks and balances to prevent fraud and abuse
    - **Dual Control**
        - Process requiring two individuals to perform the action together
        - Example:
            - Unlocking a safe or a server room
    - **Succession Planning**
        - Focuses on ensuring important duties will always have someone who can perform them
        - Prevents issues from task not being performed during personnel turnover
        - Example:
            - A primary and backup administrator
    - **Cross Training of Employees**
        - Focuses on teaching employees skills to cover tasks other coworkers perform
        - On-the-job training is used to ensure you have additional resources for a big project in the future or if someone quits
    - **Background Checks**
        - Conducted prior to hiring an employee
        - Example:
            - Bank runs credit check on new hires
    - **Mandatory Vacation Time**
        - Staff members must take vacation

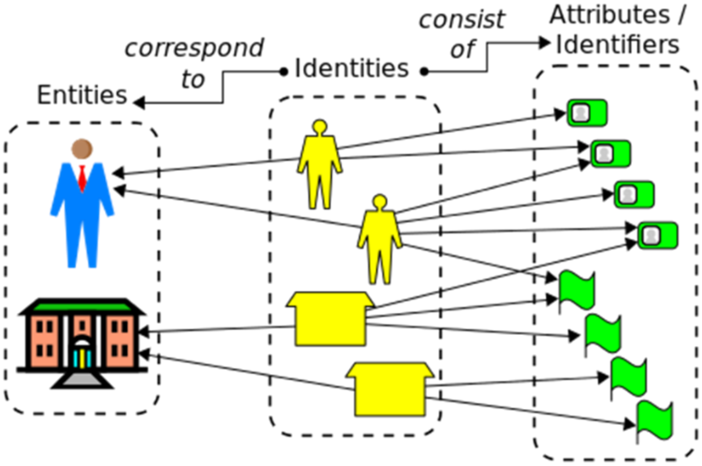
        - Allows us to identify any issues being hidden since the person will not maintain continuous access to the systems
    - **Termination**
        - Policies and procedures focus on what to do when an employee is terminated
        - Retrieving company property, disabling accounts, changing security codes, etc.
- **Outsourcing Concerns**
    - **Outsourcing Concerns**
        - If you outsource, there are additional things you need to be concerned with…
        - Proper vetting of the provider
        - Employment practice
        - Access control
        - Data ownership and control
        - Incident response and notification process
    - **Proper Vetting and Employment Practices**
        - What kind of background checks are you doing on the service provider?
        - What kind of background checks are done on their employees?
        - What internal personnel controls are used?
        - How do they handle employee issues?
    - **Access Control**
        - How is access control handled to the system?
        - How is your data physically or logically segmented from other organizations that the service provider handles?
    - **Data Ownership and Control**
        - Who owns the data?
        - Is it encrypted when stored?
        - Does the service provider have access to just the data, or do they also have the encryption keys?
    - **Incident Response and Notification Processes**
        - How will you be notified if there is a breach?
        - Or, will you even be notified if there is a breach?
- **User Awareness Training**
    - **User Awareness Training**
        - Users are the biggest threat to networks
        - Proper security training is the most cost-effective control that can be applied in an organization
        - All the technical controls in the world won't stop a threat if a user lets the bad guys into your network…

    - **Areas to Discuss**
        - Acceptable Use Policy
        - Threats face by the organization
        - How to report a security issue
        - Physical security concepts
        - BYOD Policy
        - Data handling requirements
        - Best practices for passwords, emails, remote work, secure web browsing, etc.
    - **Spearphishing and Phishing**
- **Analyzing Secure Architectures**
    - **Analyzing Architectures**
        - Attackers always look for the flaw in the architecture's security controls
        - Penetration testers act like an attacker to find these flaws, gaps, and single points of failure
        - When analyzing security controls, determine if they meet the given requirement or stated goal
    - **Reviewing Architectures**
        - Operational View
            - Focuses on how a function is performed or is supposed to accomplish
        - Technical View
            - Focuses on technologies, configurations, and settings used in an architecture (system or service)
        - Logical View
            - Focuses on the interconnections of systems with less technical details than the technical view
    - **Common Issue: Single Points of Failure**
        - Singular part of the system that could cause the entire system to fail or the desired security level to fail is exploited
    - **Common Issue: Data Validation and Trust**
        - Data is commonly assumed to be valid and trustworthy in a system
        - Can cause issues, such as trusting input provided to web application will be valid
        - Can lead to SQL injections or other issues
        - To prevent this, systems should be designed with validation and integrity checking
    - **Common Issue: Users**
        - The largest cause of a security failure
        - Mistakes and abuse can be at fault
        - To prevent this:

        - Use automated monitoring to detect error
        - Constrain interfaces to only allow activities
        - Implement procedural checks and balances
        - Provide user awareness training
  - **Common Issue: Authentication & Authorization**
    - User credentials, passwords, and permissions can cause security failure
    - To prevent this:
      - Multifactor authentication
      - Centralized account management
      - Centralized privilege management
      - Monitor privileged account access
      - User awareness training
  - **Architecture Reviews**
    - Step-by-step analysis of organization security needs
    - Begin with the design requirements and then look at technical and logical diagrams
    - Identify issues and report them per your organizational processes
  - **Maintaining Secure Architectures**
    - Threats change over time and systems become outdated
    - Conduct scheduled reviews
      - Systems, networks, and processes
    - Continual Improvement
      - Incremental improvements over time
    - Retirement of processes
      - Policies can become no longer relevant
- **What is Identity?**
  - **What is Identity?**
    - Collection of user information, rights, credentials, group memberships, & roles
    - Set of claims about an individual or account holder made about one party to another party
    - Key part of authentication, authorization, and trust
  - **Attributes of Identity**
    - Name, address, title, contact information, identification number, etc…
    - Attributes populate the directory and can be used as an authentication process
  - **AAA: Authentication, Authorization, and Accounting**
    - Used to control access to computers, networks, and services
    - AAA systems use usernames, passwords, or other attributes of an identity to authorize access

- Authentication
  - Individual proves who they are
- Authorization
  - Individual is provided access to a given resource
- Accounting
  - Logs and monitors a user when an authentication or authorization attempt is made or completed

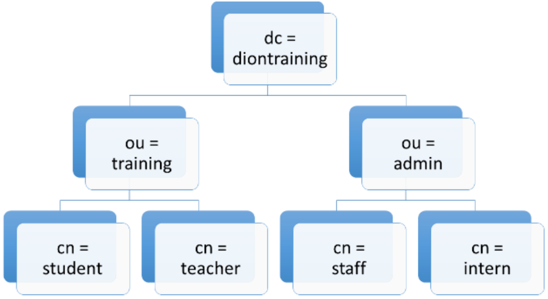
- **Centralized Identity and Access Management (IAM)**
  - Systems built to create, store, and manage identity information, including group memberships, roles, permissions, and more



- **What does IAM do for us?**
  - Provisioning accounts
  - Authentication
  - Single-Sign-On (SSO)
  - LDAP Directory
  - Account Maintenance
  - Reporting
  - Monitoring
  - Logging
  - Auditing

- **Identity Systems**
  - **Identity Systems**
    - Provide common functions
      - Identity creation and management
      - Authentication and authorization
      - Federation of identity information
    - To provide these functions, we use:
      - Directories
      - Authentication services

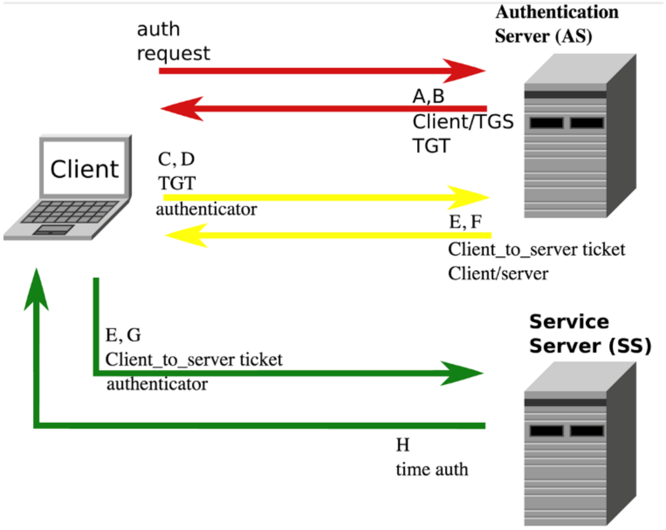
        - Identity Management Platforms and federated identity tools
- **Directory Services**
    - Used in networks to provide information about systems and users
    - LDAP (Lightweight Directory Access Protocol) is commonly used
        - Microsoft's Active Directory, Oracle's Internet Directory, IBM's Security Directory, OpenLDAP, 389 Directory Server, ApacheDS, and OpenDJ
    - Can be used to make organizational information available to email and other programs
- **LDAP Directory Structure**



dc = domain name
ou = organizational unit
cn = common name

- **Securing LDAP**
    - Enable and require TLS for LDAP query
    - Set password storage to use salted hash
    - Disable unauthenticated and anonymous LDAP modes (require user/password)
    - Replicate LDAP to a redundant server to prevent outages or Denial of Service
    - Strong ACLs on LDAP to limit access to objects using least privilege model
- **LDAP Injection**
    - Type of attack where improperly filtered input via web applications send arbitrary LDAP queries to the server
    - Prevent this by:
        - Escaping all variable using the right LDAP encoding function
        - Use frameworks that automatically protect from injection (*LINQ to Active Directory)*
        - Minimize privileges assigned to LDAP web apps
        - Use input validation to whitelist what is allowed
- **Authentication Protocols**
    - Protocols used to supply verification of user's identity to a relying system
    - Examples:

        - TACACS+
        - RADIUS
        - Kerberos
- **TACACS+**
    - Cisco extension to the Terminal Access Control Access Control System
    - Uses TCP to provide AAA services
    - Lacks integrity checking of data it sends
        - Subject to replay attacks
    - Encryption flaws
        - Encryption key can be discovered by attacker
    - Don’t use TACACS+ unless on an isolated network, it is just too flawed…
- **RADIUS**
    - Remote Authentication Dial-in User Service
    - Most common AAA for networks, wireless networks, and other services
    - Operates over TCP or UDP in a client-server model
    - Password obscured using shared secret and MD5 hash (not considered strong)
    - RADIUS traffic should be encrypted using IPSec between endpoints
- **Kerberos**
    - Designed with security in mind
    - Operates on untrusted networks using encryption of its data
    - Principles (users) comprised of three elements:
        - Primary (usually a username)
        - Instance (unique ID incase usernames are similar)
        - Realm (group of primaries)
    - Replaced NTLM for AAA in Windows domains
- **Kerberos Authentication**



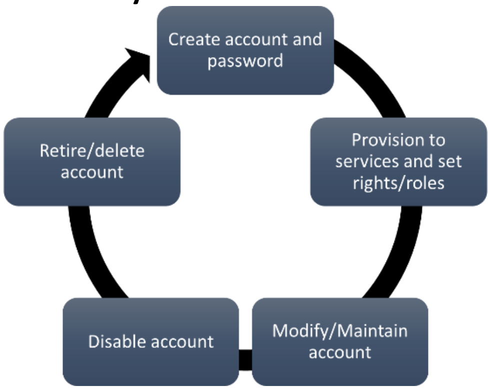
- **Single-Sign-On (SSO)**
  - Allows users to authenticate once and then be able to use multiple systems
  - Examples:
    - LDAP
    - CAS (Central Authentication Service)
  - Benefits:
    - Reduce password reuse
    - Fewer password resets and support calls
- **Shared Authentication**
  - OpenID
    - Open-source standard for decentralized authentication
    - Uses Google ID to logon to all sites
  - OAuth
    - Open authentication standard used to share elements of identify with third-party (ie., Google provides your info)
  - OpenID Connect
    - Authentication layer built using OAuth protocol
  - Facebook Connect
    - Facebook login to authenticate to other websites and services

- **Threats to Identity Systems**
  - **Threats to Identity Systems**
    - Threats to the underlying authentication and authorization system
      - Exploit how users log in
      - How credentials are handled
      - How users are authorized
    - Target account lifecycle
      - Creating credentials
      - Preventing credential removal
      - Elevating privileges of credentials
    - Attack the account itself
      - Phishing
      - Compromise systems holding credentials
  - **Personnel-based Threats**
    - Targets users through phishing or social engineering techniques
    - User awareness training helps prevent this
    - Insider threat would also fall into this category
  - **Endpoint Threats**
    - Targets your endpoints through…
      - Local exploits
      - Keyloggers

            - Local administrative credentials
            - Password stores and tokens
        - Protect by using anti-malware and anti-virus
        - Protect by using strong authentication stores
    - **Other Identity Threats**
        - Sever-based Threats
            - Attacks your servers to send identity and authentication information to AAA servers
        - Application/Service Threats
            - Attacks your applications and/or services that rely on identity and authentication
        - Roles, Rights, and Permission Threats
            - Threats focused on users or groups roles, rights, and permissions
- **Attacking AAA Protocols and Systems**
    - **Attacking AAA Protocols and Systems**
        - Directory, authentication, and SSO systems are great targets for attacks to go after
        - Attackers use specific vulnerabilities and misconfigurations to target the AAA protocol itself or how a server implements the protocol
        - Attempting system compromises of domain controllers and AAA systems is common
    - **Attacking LDAP**
        - Target unencrypted LDAP traffic to capture traffic for replay attacks
            - Use secure binding to prevent this
        - Target improper access controls to harvest directory information or to modify directory
            - Setup good access controls
        - Perform LDAP injection against vulnerable web applications that interface with directory
            - Validate web-based input and use least privilege
        - Conduct Denial-of-Service against LDAP to cause services to fail which rely on it
            - Design scalable LDAP for redundancy
    - **RADIUS**
        - Authentication commonly used for network devices and VPNs can be attacked by…
            - Session replay of server or client responses
            - Compromising shared secret key from client machines
            - Brute-force share secret key from a stolen password
            - Denial-of-Service to prevent user authentication

- **Kerberos**
  - Relies on central key distribution center (KDC)
  - Compromise of KDC allows impersonation as any user
  - Common attacks:
    - Stealing administrator account credentials
    - Kerberos ticket reuse
      - Pass-the-ticket allows impersonation for ticket lifespan
      - Pass-the-key allows reusing secret key to get new tickets
    - Ticket Granting Ticket (TGT) attacks
      - "Golden Ticket" allows creation of new tickets, account changes, and creation of new accounts/services
- **Active Directory**
  - Core identity store and AAA service for Microsoft Windows domains
    - Many exploits built for clients, servers, and AD
  - Many Windows domains contain older systems still…
    - or are at least backward configurations still activated which makes them vulnerable to attack
  - Very common target for attackers
- **Attacks on Active Directory**
  - Malware focused on stealing credentials…or Phishing or social engineering
  - Malware focused on Windows server exploit
  - Focus on attacking older services like NTLM, LANMAN, NetBIOS, unsigned LDAP, or SMB
  - Privilege creep of service accounts
  - Overuse of domain admin credentials
  - Privilege escalation attacks
- **OAuth, OpenID, OpenID Connect**
  - OAuth and OpenID are implemented by each service provider leading to configuration flaws
  - Open redirects are a common attack
    - Redirects and forwards aren't validated
    - Untrusted user input can be sent to web apps
    - Users can be redirected to untrusted websites
    - Potential for phishing, pharming, or bypassing of website security
  - Original account information will not be compromised, but your web application may allow in untrusted users
  - OpenID attacks have been directed at vulnerabilities in the protocol itself
    - Example:
      - Attackers forged request to gain arbitrary logins

        - OAuth2 is vulnerable to cross-site request forgery (CSRF) attacks
        - Attack attempts to get user to click a link so that their browser performs an action as the user
        - OpenID Connect provides extra encryption and signing to prevent many of these exploits
- **Targeting Account Lifecycle**
    - **Targeting Account Lifecycle**


Create account and password
Provision to services and set rights/roles
Modify/Maintain account
Disable account
Retire/delete account

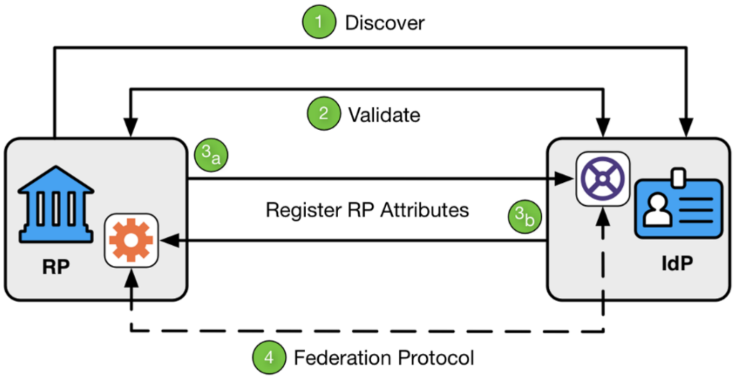
    - **Utilize Least Privilege**
        - Users should only be provided with the lowest set of privileges and access necessary to perform their job functions
    - **Prevent Privilege Creep**
        - Accounts tend to gain privileges overtime based on rotating job functions a user undertakes
        - Always ensure to remove old rights when they are no longer needed
            - Employee get promoted or moved to another job
    - **Identity Lifecycle Management**
        - Numerous tools exist to help with this
        - Centrify, Okta, and Ping Identity provide account lifecycle maintenance and monitoring features
- **Identity Exploits**
    - **Impersonation Attacks**
        - Attacks takes on the identity of a legitimate user
        - Usually involves credential theft or open redirects (OAuth)
    - **Session Hijacking**
        - Attacker takes over an existing session by acquiring or guessing the session key
        - Prevented through encrypting sessions
    - **Man-in-the-Middle (MITM)**
        - Attacker accesses the information flow between systems or services
        - Prevented through using session or link encryption tunnels

- **Privilege Escalation**
    - Attacker elevates their permissions from one level to a higher level
    - Usually follows an attack on a normal user account credentials
- **Rootkits**
    - Attacker uses malware to provide continued access to a server/client while hiding their own presence

- **Credential Theft**
    - **Credential Theft**
        - Attackers can target users, services, or simply brute force credentials to compromise them
    - **Phishing**
        - Aimed at stealing credentials by tricking users into clicking on a link in an email and entering their username/password
    - **Compromise Other Websites (Password Reuse)**
        - Aimed at stealing credentials from a less secure server, then reusing them in your organization
        - If the other server stored them as MD5 or other weak key stores, it becomes easy to crack the passwords
    - **Brute-Force Attack**
        - Login using every different combination until you gain access
        - Prevent:
            - Limit number of login attempts
            - Use CAPTCHA-style to prevent automation
- **Securing Authentication and Authorization**
    - **Securing Authentication**
        - Technical and administrative controls can help secure the authentication process
        - Uses strong passwords/passphrases
        - Password management is a concern
            - Consider Single-Sign-On
            - Token-based for multifactor
            - Password safes (LastPass, Dashlane, etc)
        - Encrypt communications between clients and authenticators using TLS
    - **Securing Authorization (Users)**
        - Access control ensures users are matched with rights/privileges
        - Polices to control what rights are given
        - Implement management systems for approving rights
        - Monitor/report on which accounts have which rights assigned
    - **Securing Authorization (Admin)**
        - Privileged User Management concerns giving admin rights to users
        - Use additional monitoring and logging

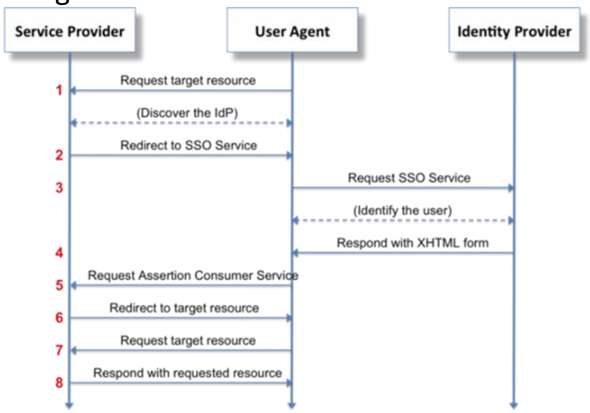
        - Implement separation of duties
        - Use appropriate training
        - Prevent admin accounts from being used as daily accounts
    - **Multifactor Authentication**
        - Use two or more factors for authentications
        - Knowledge factors
        - Possession factors
        - Biometric factors
        - Location factors
    - **Context-Based Authentication**
        - Authentication decision is based on information about the user, system, etc.
        - User's role or group membership
        - Time of day in relation to user's hours
        - IP address and reputation
        - Frequency of access
        - Location (IP or GPS)
        - Type of device
- **Identity as a Service (IDaaS)**
    - **Identity as a Service (IDaaS)**
        - Provides authentication services, usually through cloud-based resources
            - Identity lifecycle management
            - Directory services (LDAP, AD, or others)
            - Access management
            - SSO via SAML, OAuth, or other technology
            - Privilege account management/monitoring
            - Reporting, auditing, and other oversight/visibility into the identity lifecycle
    - **Challenges with IDaaS**
        - Will you centralize your directory services or will internal and external directories be used?
        - How about authentication? Centralized or federated?
        - Will you use local or cloud-based authoritative credential stores?
    - **IDaaS Benefits**
        - If your current organization doesn't already have strong identity management, IDaaS can be a big improvement in security…
            - …can be better managed
            - …can be more capable
            - …can be more secure
        - Centralized monitoring and reporting can help detect issues sooner than traditional systems

- **Detecting Identity Attacks**
  - **Detecting Identity Attacks**
    - Identity and Access Management systems should be fed into the SIEM
    - Configure your SIEM to detect:
      - Privileged account usage
      - Privilege changes and grants
      - Account creation or modifications
      - Terminated user account usage
      - Lifecycle management events
      - Separation of duty violations
  - **Active Monitoring**
    - Knowledgeable technicians should actively monitor identity systems
    - Humans should analyze reports to identify issues
    - Remember, you must know what normal looks like in order to detect the abnormal
- **Federated Identity Systems**
  - **Federated Identity Systems**
    - Moves the trust boundary outside your organization to Google, Facebook, LinkedIn, or other identity providers
    - Identity Provider (IDP)
      - Provides identities & release data to relying parties
    - Relying Party (RP) or Service Provider (SP)
      - Members of the federation that provides services to the user when identified by identity provider
    - Consumer or User
      - Asked to make decision on who to share their identity with by IDP in order to get services from RP/SP



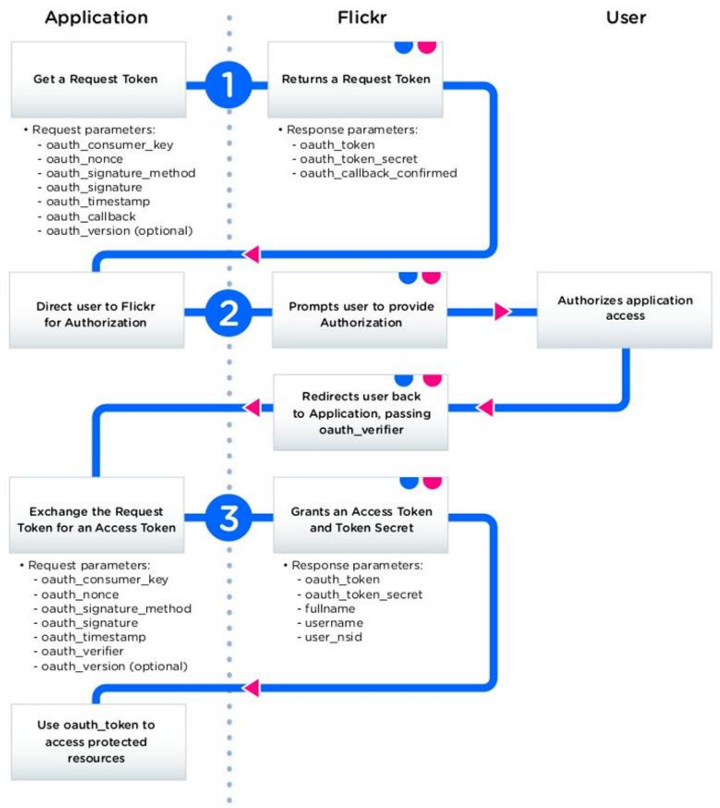
  - **Choosing a Federated Identity System**
    - Do you care that the user says who they are?
      - If not, use Google, Facebook, etc.

            - Otherwise, find identity provider that vets its users
        - When users sign up for your site using federated ID, you immediately provision a user account on your system mapped to the attributes released by IDP
    - **Federated Identity Systems Technologies**
        - Security Assertion Markup Language (SAML)
        - OAuth and OAuth 2.0
        - Active Directory Federation Services (ADFS)
        - OpenID Connect
    - **Security Assertion Markup Language (SAML)**
        - XML-based language to send authentication and authorization data between IDP and RP
        - Used to enable SSO for web apps & services
        - Allows attribute, authentication, and authorization decisions to be exchanged



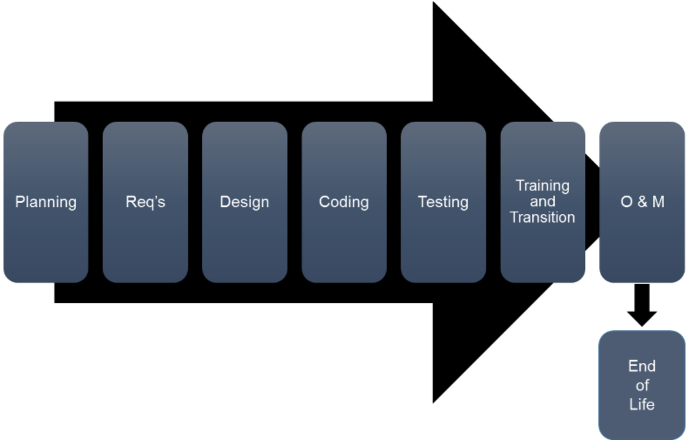
    - **OAuth and OAuth 2.0**
        - Developed by the Internet Engineering Task Force (IETF) to provide an authorization framework to allow service provider applications to access HTTP-based services
        - Provides access delegation to allow service providers to provide actions on behalf of user
        - Supports web clients, desktops, mobile devices, and other embedded device types
        - OAuth has types of four parties served:
            - Clients
                - Applications that the user wants to access/use
            - Resource Owners
                - End user being serviced
            - Resource Servers
                - Servers provided by a service the user wants to access

      - Authorization Servers
        - Servers owned by the identity provider (IDP)
  - **Flickr Federated Example (OAuth Authentication Process)**



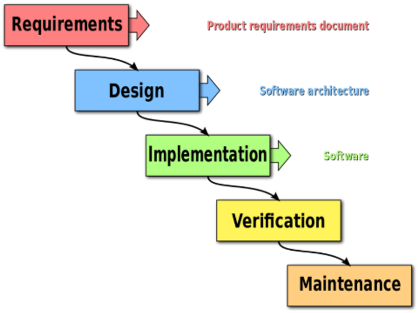
  - **Active Directory Federation Services (ADFS)**
    - Microsoft's answer to federated identities
    - Provides authentication and identify data as claims to service providers
    - Partner sites use trust policies to match claims to claims supported by their services to make their own authorization decisions
    - Works similar to the OAuth authentication process
  - **Incident Response for Federated Identity Systems**
    - Check your contract (if you have one)
    - IDP usually responsible for notifying account owners (users) and RP/SP of a breach and required response (like password resets)
    - RP/SP must determine their response if IDP was compromised (what response, if any)
    - If your users' accounts are compromised,
      how will you provide them access?
      - Think about if a Facebook login got stolen…

- **Software Development Life Cycle**
  - **Software Development Life Cycle (SDLC)**
    - Software development doesn't always follow formal models
    - Many different forms of SDLC…but all share 8 basic functions/phases
    - SDLC can also be used for applications, services, systems, or other desired outputs
    - Planning for security early in the process will provide better security at a cheaper price…

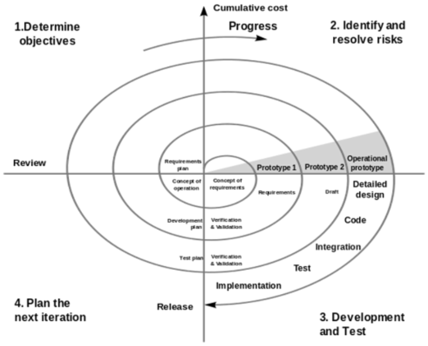


  - **Planning**
    - Initial investigations into the effort conducted
    - Determines feasibility of designing the desired software, costs, and any alternate solutions
    - End result: decision to move forward or not
  - **Requirements**
    - Gain customer or stakeholder input to determine required functionality
    - What should the program do?
    - What does your current program not do?
  - **Design**
    - Creates designs for functionality, architecture, integration points, techniques, data flows, processes, and other elements
  - **Coding**
    - Programmers start writing the code for the software and conduct testing of individual units of code and through code analysis
  - **Testing**
    - Formal testing with outside development team (stakeholders, customers, beta group, etc.)
    - User Acceptance Testing ensure users are satisfied with the functionality
  - **Training and Transition**
    - Ensures the end users are trained on software

        - Consists of acceptance, installation, and deployment of software into live environment
    - **Operations and Maintenance**
        - Longest phase of the SDLC
        - Patching, updating, modification, and daily support for the new software occurs
    - **End of Life**
        - Disposition and retirement of the software
        - How will you stop supporting the software?
        - Will you migrate users to a new version?
- **Software Development Models**
    - **Software Development Models**
        - Many models of software development exist
        - Models provide a common framework to use
        - Can use detailed practices, procedures, and documentation
        - Can also be less formal and haphazard
    - **Waterfall Model**
        - Linear model with each phase following the previous phase

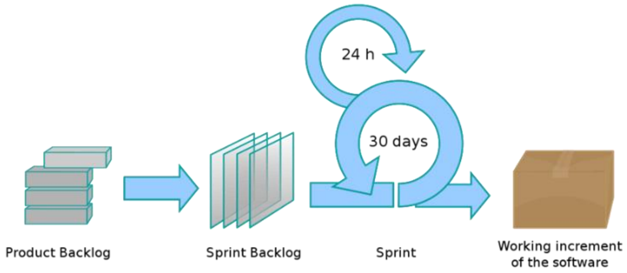


    - **Spiral Model**
        - Modification of Waterfall, it adds iterative process to revisit phases over and over

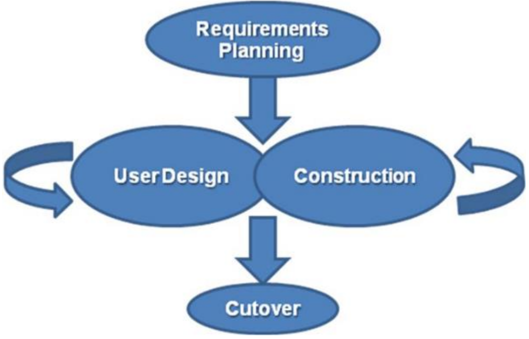


    - **Agile**
        - Iterative and incremental process
        - Foundations of Agile:

- Individuals and interactions are most important
- Working software is better than the documentation
- Customer collaboration over contract negotiation
- Responding to changes fast is better than a plan

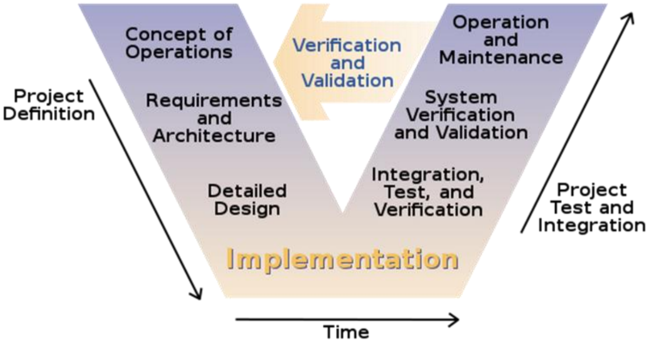


- **Terms Used in Agile**
  - Backlogs
    - List of features or tasks to complete
  - Planning Poker
    - Estimation tool for planning in Agile
  - Timeboxing
    - Agreed upon time to work on specific goal
  - User stories
    - Describe high-level user requirements
  - Velocity tracking
    - Adds up estimates for current sprint efforts and compares to what was actually complete
- **RAD (Rapid Application Development)**
  - Iterative process relying on building prototypes
  - Provides a highly responsive development environment for modularized work
  - No planning phase… they just start coding



- **Terms Used in RAD**
  - Business Modeling
    - Focuses on understanding business processes

        - Data Modeling
            - Gather and analyze datasets and the relationships
        - Process Modeling
            - Define the processes and data flows
        - Application Generation
            - Code & convert data and processes into prototype
        - Testing and Turnover
            - Focus on interfaces between components and verifying functionality
    - **Big Bang SDLC Model**
        - All coding is based on requirements and making resources available
        - Doesn't scale well, works best for single coder
        - No planning or process
    - **V Model**
        - Extension of the waterfall which pairs testing and development phases together


Concept of Operations
Verification and Validation
Operation and Maintenance
Project Definition
Requirements and Architecture
System Verification and Validation
Detailed Design
Integration, Test, and Verification
Project Test and Integration
Implementation
Time

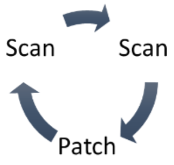
- **Coding for Security**
    - **Coding for Security**
        - Security should be added in requirements
        - Security is built during design and coding
        - Security is *then* tested in prototypes and final products
    - **Secure Coding Practices**
        - Have an organizational secure coding policy
        - Conduct risk assessments (and ongoing assessments) to prioritize issues to remediate
        - User input validation (prevent XSS/SQL inject)
        - Consider your error messages
            - What information is being given? Too much?
        - Database security in application and database
            - Prevents data leaks
        - Encrypt sensitive information being stored

        - Hash passwords your applications store
        - Design for availability and scalability
            - Conduct load and stress testing
        - Conduct monitoring and logging
        - If possible, utilize multifactor authentication
        - Code for secure session management
            - Prevents session hijacking
        - Proper cookie management
            - Secure cookies if used in web applications
        - Encrypt network traffic
            - Use TLS to prevent network-based data capturing
        - Secure the underlying infrastructure
            - As a cybersecurity analyst, your biggest impact will usually be on the infrastructure and not the code
    - **Open Web Application Security Project (OWASP)**
        - Community hosting standards, guides, best practices, and open source tools
        - Provides updated lists of proactive controls to test your web application's security
        - Check out OWASP.org
    - **Source Code Management**
        - Use check-in/check-out and revision history to ensure you know what code is current version
        - Source Control Management or Version Control tools, like Git, Subversion, or CVS
- **Testing Application Code**
    - **Testing Application Code**
        - Scanning using a tool
        - Automated vulnerability scanning tools
        - Manual penetration testing
        - Code review
        - OWASP considers code reviews the best and most thorough of these options
        - "360 Reviews" combined code review with penetration testing, then review's code again
    - **Code Reviews**
        - Shares knowledge of the code with others
        - More experience is learned across the team
        - Detects problems and enforces good coding
        - Agile and formal models:
            - Pair Programming

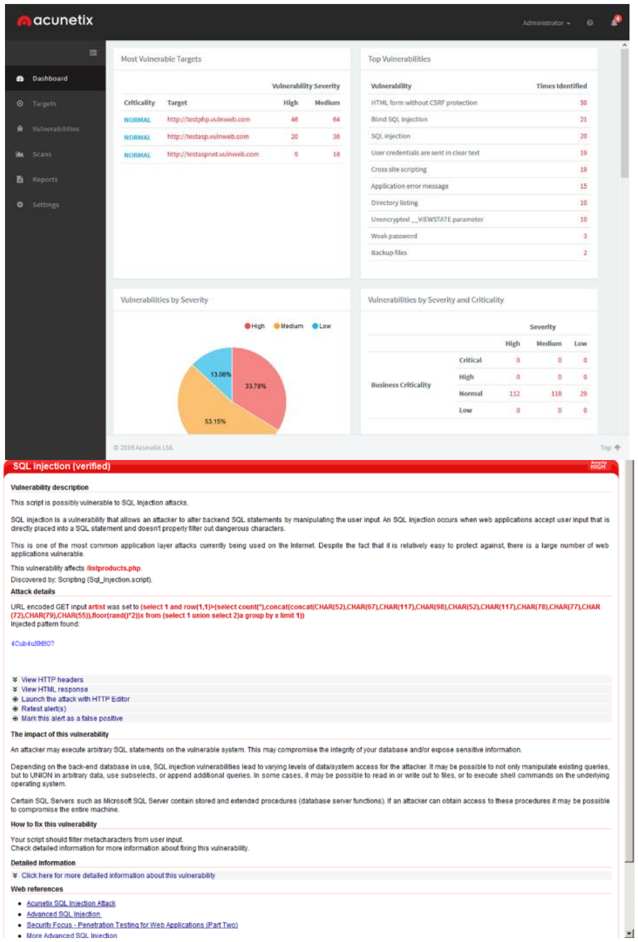
            - Over-the-Shoulder
            - Pass-Around
            - Tool-Assisted
            - Fagan
    - **Pair Programming**
        - Agile development technique
        - Two developers use one workstation
        - Provides real-time code review but is costly
    - **Over-the-Shoulder**
        - Agile development technique
        - Developer who coded software explains it to another developer
        - Lower cost than pair programming since it occurs at intervals instead of having a constant review
    - **Pass-Around**
        - Form of review with one or more reviewers
        - Code is emailed or shared for review
        - Code documentation is much more important
    - **Tool-Assisted**
        - Formal or informal software-based tools conduct code reviews
        - Specialized software allows the reviewers to mark up the code, provide feedback, and more
    - **Fagan**
        - Structured formal code review by a team of reviewers
        - Specifies entry/exit criteria for each process
        - More costly and harder to implement than other types of code reviews
- **Finding Security Flaws**
    - **Finding Security Flaws**
        - Coding flaws are always going to occur
            - Programming and syntax errors
            - Business logic and process errors
            - Error handling
            - Incorrect integration with other services
    - **Static Analysis**
        - Conducted by reviewing the code manually or with an automated tool
        - Code is not run during static analysis
        - Form of white-box testing
    - **Dynamic Analysis**
        - Code is executed while providing specific input
        - Uses automated tools or manual input
        - Types
            - Fuzzing

- Fault Injection
- Mutation Testing
- Stress Testing (Load Testing)
- Security Regression Testing

- **Fuzzing**
  - Sends invalid or random data to an application to test ability to handle unexpected data
  - Typically automated to use large datasets
  - Used to detect input validation, logic issues, memory leaks, and error handling
- **Fault Injections**
  - Directly inserts faults into error handling parts of the code to test them
  - Examples:
    - Compile-time injection
      - Injects faults by modifying source code before compiling
    - Protocol software injection
      - Uses fuzzing to send noncompliant data to a protocol
    - Runtime injection
      - Inserts data into running memory of the program or by sending in a fault to the program to deal with it
- **Mutation Testing**
  - Makes small changes to the program itself to determine they would cause a failure
  - If they cause a failure then they are rejected
  - Used to test if code is testing for possible issues with unexpected input types
- **Stress Testing (Load Testing)**
  - Ensures applications and systems can support the expected production load
  - Uses automated tools to "stress" an expected load and determine if it's handled properly
  - Test for the worst-case scenario
  - Can be conducted against entire system or just a single component
- **Security Regression Testing**
  - Ensures that any changes made do not create new problems or issues in the application
  - Used most commonly when a new patch or update is added
  - Verifies no new vulnerabilities or misconfigurations have been added



- **Web App Vulnerability Scanning**
  - **Web Application Vulnerability Scanning**
    - Dedicated web app vulnerability scanners do better than Nessus, Nexpose, and OpenVAS
    - Identify problems with applications and the underlying web servers, databases, and infrastructure
    - Examples
      - Acunetix WVS
      - Archni
      - Burp Suite
      - IBM’s AppScan
      - HP’s WebInspect
      - Netsparker
      - QualysGuard’s Web Application Scanner
      - W3AF
  - **Acunetix**



Most Vulnerable Targets

		Vulnerability Severity	
Criticality	Target	High	Medium
NORMAL	http://testphp.vulnweb.com	46	64
NORMAL	http://testasp.vulnweb.com	20	36
NORMAL	http://testaspnet.vulnweb.com	9	18

Top Vulnerabilities

Vulnerability	Times Identified
HTML form without CSRF protection	50
Blind SQL Injection	21
SQL injection	20
User credentials are sent in clear text	19
Cross site scripting	19
Application error message	15
Directory listing	10
Unencrypted __VIEWSTATE parameter	10
Weak password	3
Backup files	2

Vulnerabilities by Severity and Criticality

		Severity		
		High	Medium	Low
Business Criticality	Critical	0	0	0
	High	0	0	0
	Normal	112	118	29
	Low	0	0	0

SQL injection (verified)

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects /listproducts.php.

Discovered by: Scripting (Sql_Injection.script).

Attack details

URL encoded GET input artist was set to (select 1 and row(1,1)>(select count(*),concat(concat(CHAR(52),CHAR(67),CHAR(117),CHAR(98),CHAR(52),CHAR(117),CHAR(78),CHAR(77),CHAR(72),CHAR(79),CHAR(55)),floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))
Injected pattern found:

4Cub4uNMH07

- View HTTP headers
- View HTML response
- Launch the attack with HTTP Editor
- Retest alert(s)
- Mark this alert as a false positive

The impact of this vulnerability

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

How to fix this vulnerability

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

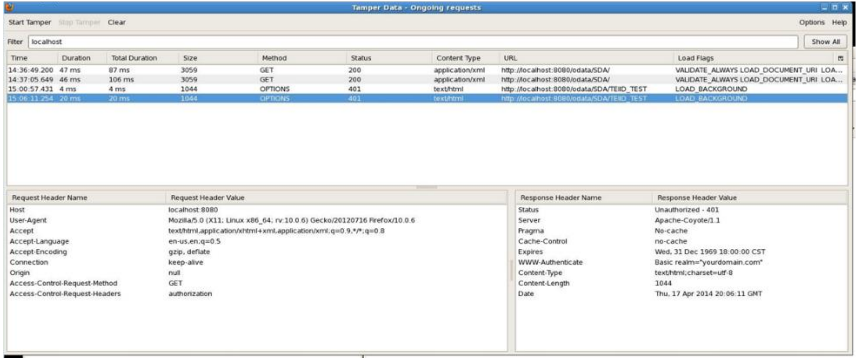
Detailed information

- Click here for more detailed information about this vulnerability

Web references

- Acunetix SQL Injection Attack
- Advanced SQL Injection
- Security Focus - Penetration Testing for Web Applications (Part Two)
- More Advanced SQL Injection

- **Manual Scanning**
  - Uses and interception proxy to capture communications between browser and server
  - Testers can modify data sent and received
  - Examples
    - Tamper Data for Firefox and Chrome
    - HttpFox
    - Fiddler
    - Burp Suite
- **Tamper Data**



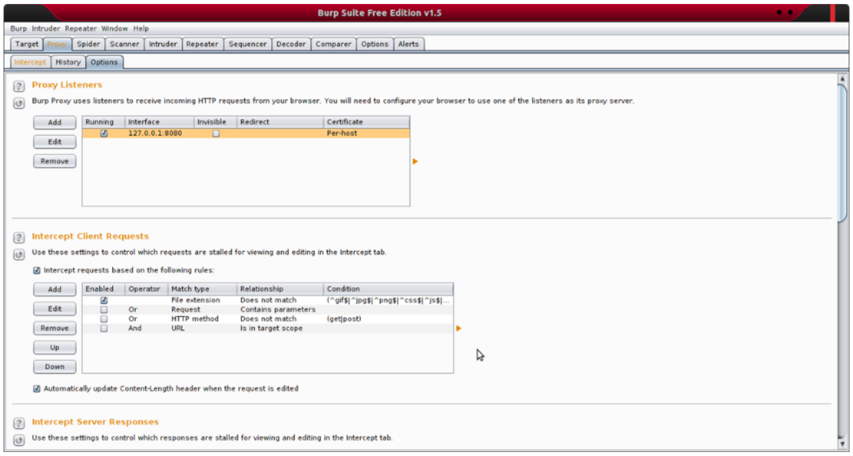
Filter: localhost

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
14:36:49.200	47 ms	87 ms	3059	GET	200	application/xml	http://localhost:8080/odata/SDA/	VALIDATE_ALWAYS LOAD_DOCUMENT_URI LOA...
14:37:05.649	46 ms	106 ms	3059	GET	200	application/xml	http://localhost:8080/odata/SDA/	VALIDATE_ALWAYS LOAD_DOCUMENT_URI LOA...
15:00:57.431	4 ms	4 ms	1044	OPTIONS	401	text/html	http://localhost:8080/odata/SDA/TEIID_TEST	LOAD_BACKGROUND
15:06:11.254	20 ms	20 ms	1044	OPTIONS	401	text/html	http://localhost:8080/odata/SDA/TEIID_TEST	LOAD_BACKGROUND

Request Header Name	Request Header Value
Host	localhost:8080
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:10.0.6) Gecko/20120716 Firefox/10.0.6
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	keep-alive
Origin	null
Access-Control-Request-Method	GET
Access-Control-Request-Headers	authorization

Response Header Name	Response Header Value
Status	Unauthorized - 401
Server	Apache-Coyote/1.1
Pragma	No-cache
Cache-Control	no-cache
Expires	Wed, 31 Dec 1969 18:00:00 CST
WWW-Authenticate	Basic realm="yourdomain.com"
Content-Type	text/html;charset=utf-8
Content-Length	1044
Date	Thu, 17 Apr 2014 20:06:11 GMT

- **Burp Suite**
  - Automated and Manual modes



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	□		Per-host

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

☑ Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

- **Outsource Your Scanning**
  - Even the best vulnerability scanners will miss business logic issues and other flaws
  - Outsourcing to a security firm can identify issues that a web application scanner can't
  - These firms can provide both static and dynamic analysis of your applications

Conclusion

- **CompTIA CSA+ Complete Course**
  - **Domain 1 Threat Management**
    - Threats
    - Tools and Techniques
    - Reconnaissance and Footprinting
    - …and so much more!
  - **Domain 2 Vulnerability Management**
    - Vulnerability Management programs
    - How to create one in your organization
    - Tools used in Vulnerability Management
    - …and so much more!
  - **Domain 3 Cyber Incident Response**
    - Phases of an incident response
    - Creating an incident response team
    - How to classify an incident
    - Analyzing network events
    - Basics of Digital Forensics
  - **Domain 4 Security Architecture and Tools**
    - Different frameworks
      - COBIT, ITIL, NIST, ISO, …
    - Policies, procedures, guidelines, and controls
    - Defense in Depth
    - Software Development Lifecycle
  - **Are You Ready?**
    - Take the practice exam in this course
    - Did you score at least 85% or higher?
    - If you need more practice, take additional practice exams to hone your skills
  - **Tell Me When You Pass!**