JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Passive Recon: Network Devices

THREAT MANAGEMENT

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

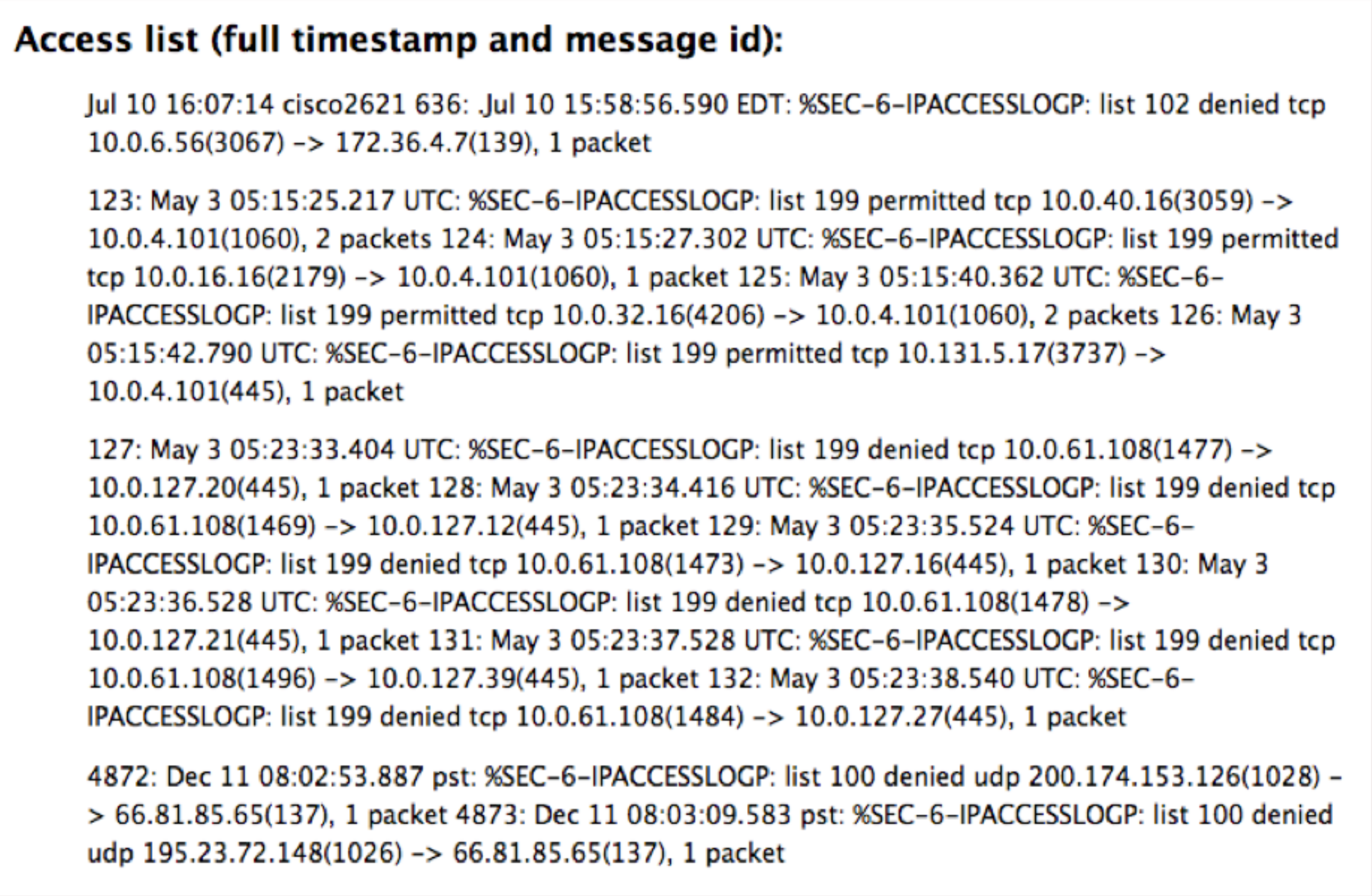
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

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



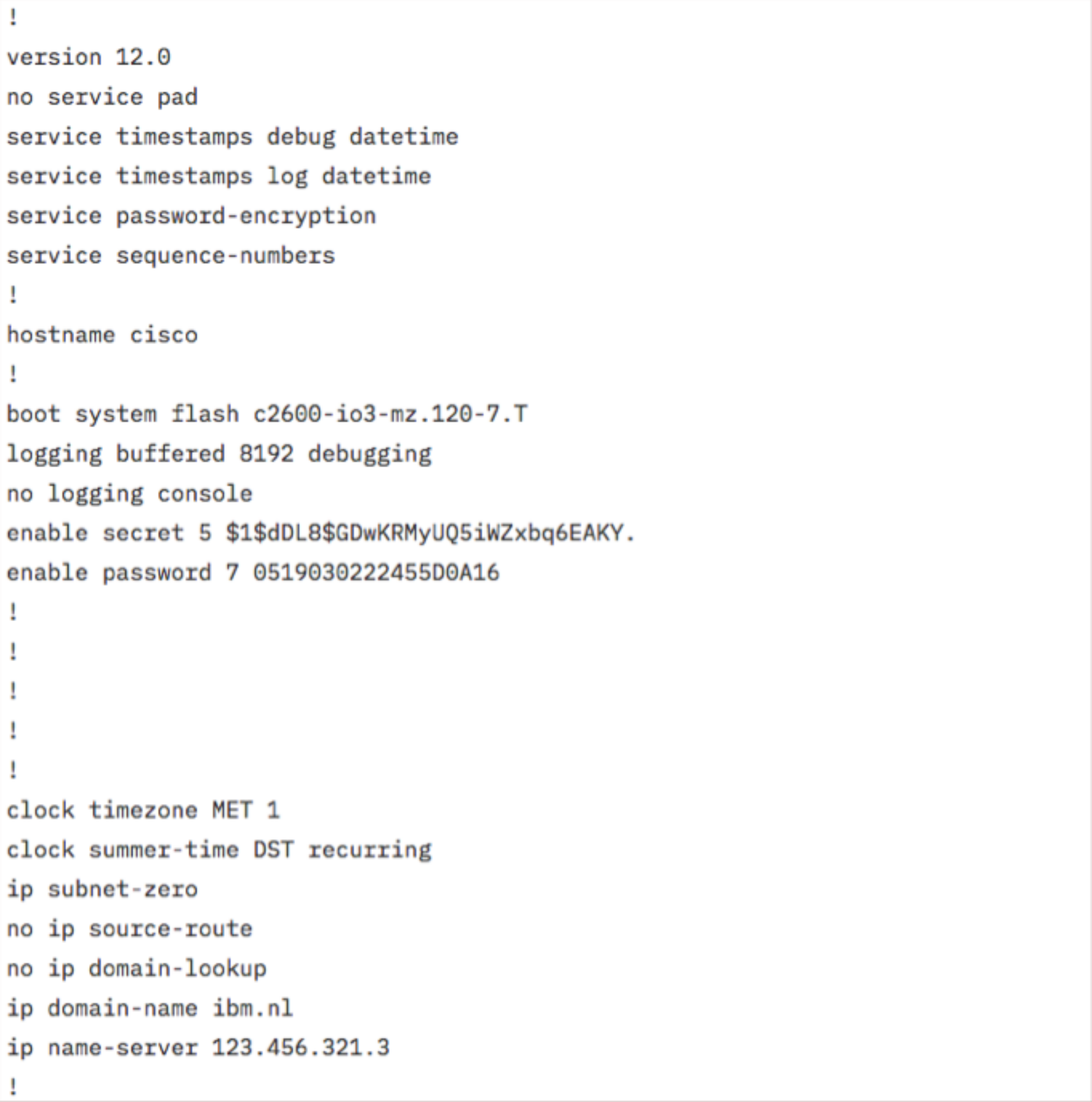
Access list (full timestamp and message id):

```
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

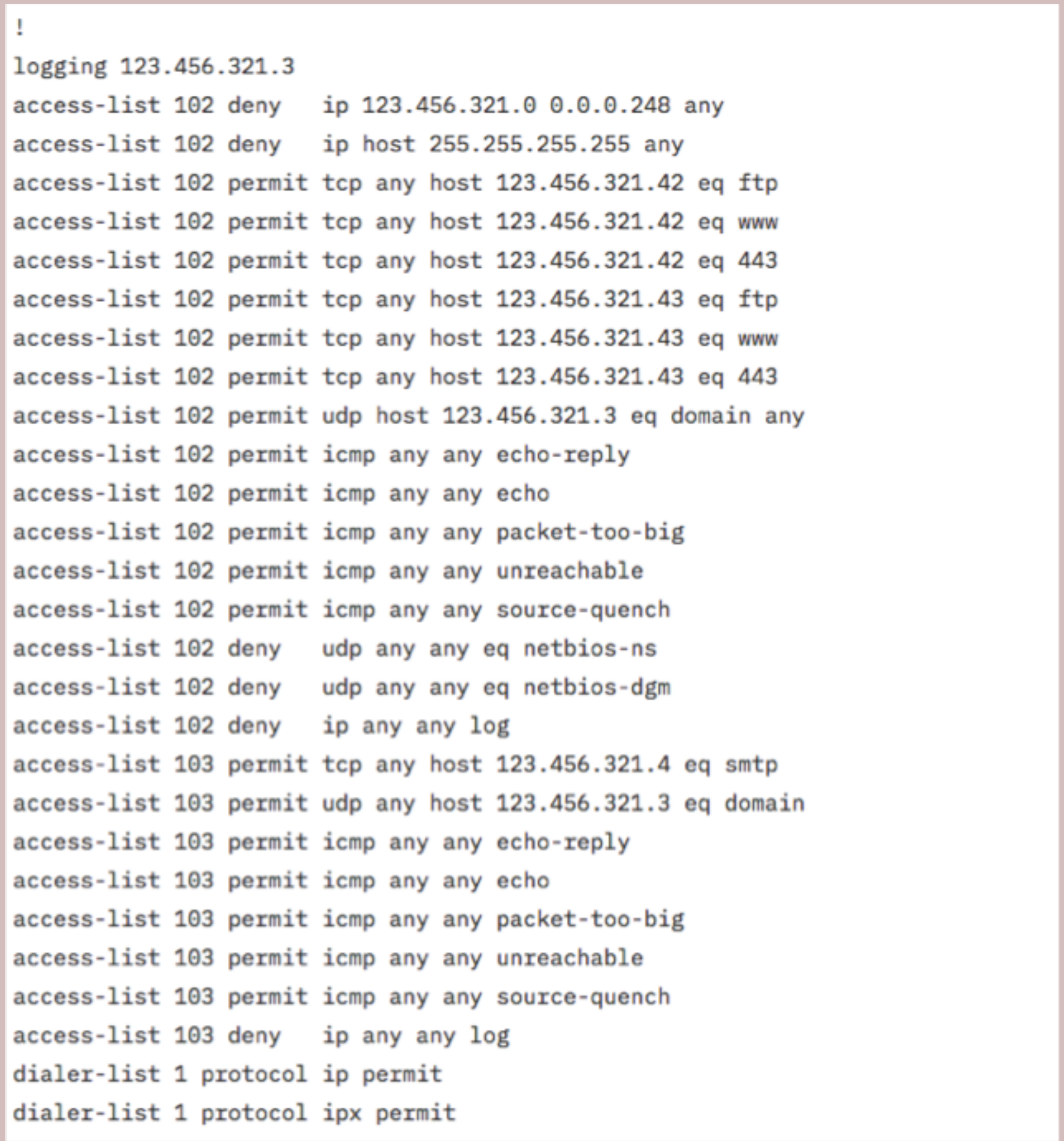
- Invaluable when mapping a network
- Identifies all routes and devices in detail
- Provides details of SNMP and SYSLOG servers on the network, user & admin accounts, and more

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
!
```

Configuration File Example



```
!
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