JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Vulnerability Reporting

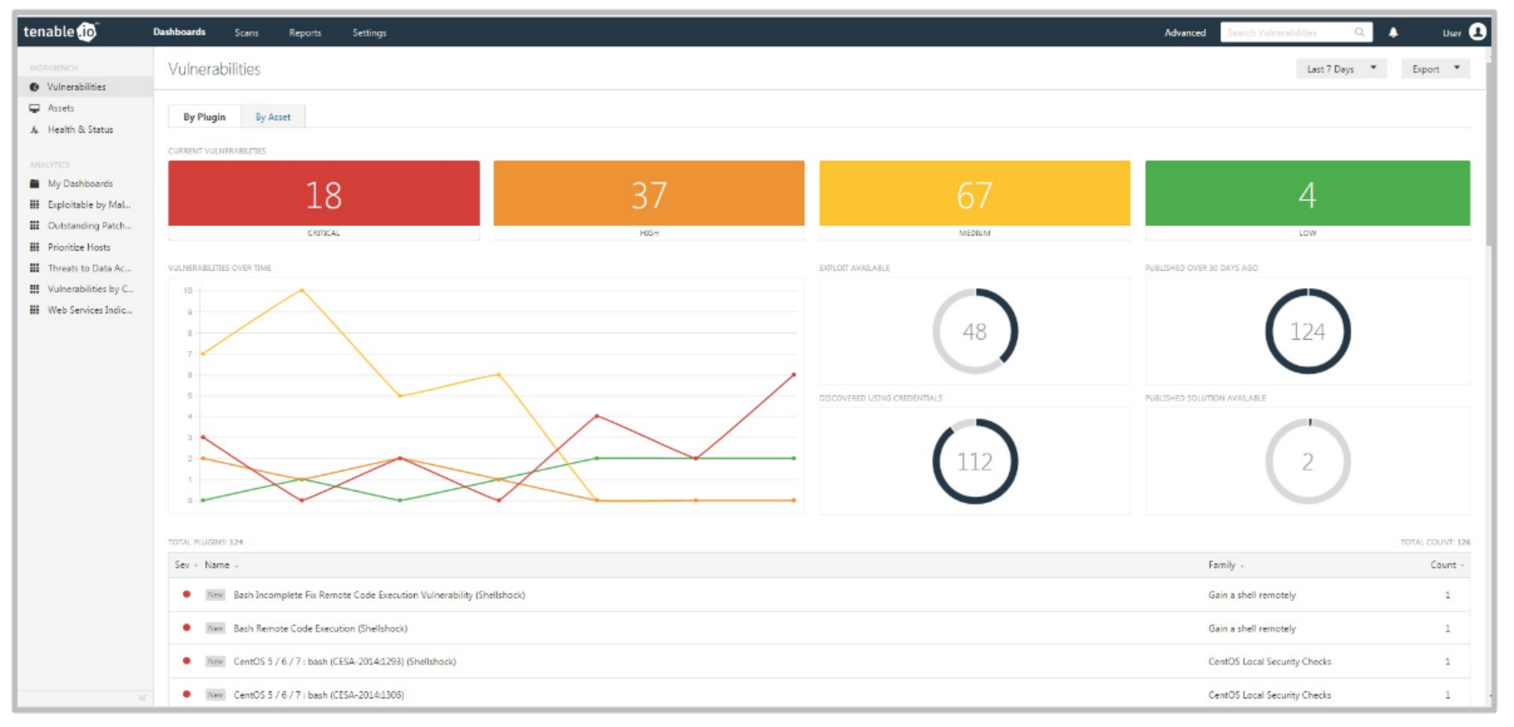
VULNERABILITY MANAGEMENT

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



CURRENT VULNERABILITIES

18	37	67	4
CRITICAL	HIGH	MEDIUM	LOW

EXPLOIT AVAILABLE: 48

PUBLISHED OVER 30 DAYS AGO: 124

DISCOVERED USING CREDENTIALS: 112

PUBLISHED SOLUTION AVAILABLE: 2

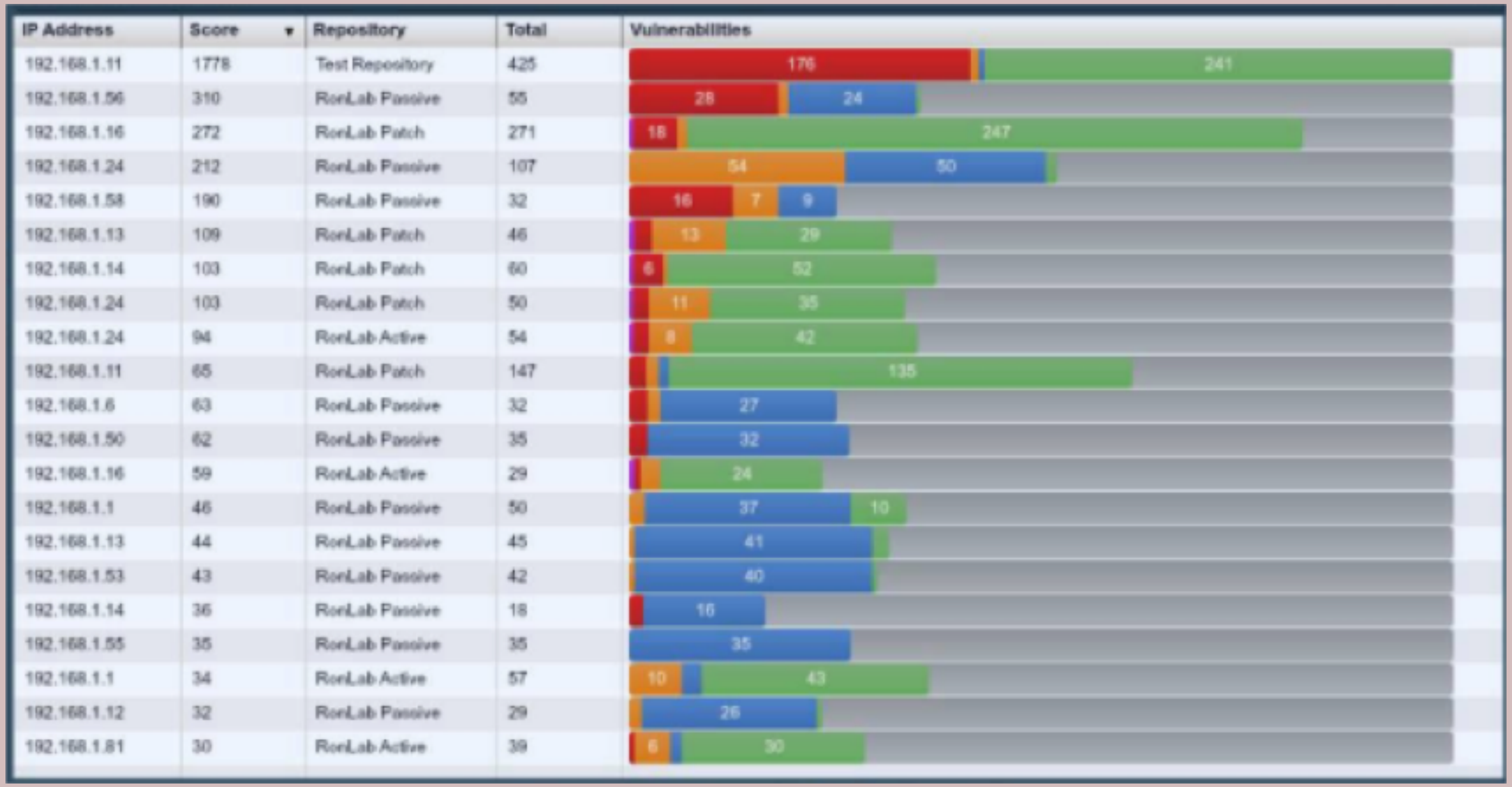
TOTAL PLUGINS: 124

TOTAL COUNT: 126

Sev	Name	Family	Count
●	New Bash Incomplete Fix Remote Code Execution Vulnerability (Shellshock)	Gain a shell remotely	1
●	New Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1
●	New CentOS 5 / 6 / 7 : bash (CESA-2014:1293) (Shellshock)	CentOS Local Security Checks	1
●	New CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1

Overview of Hosts

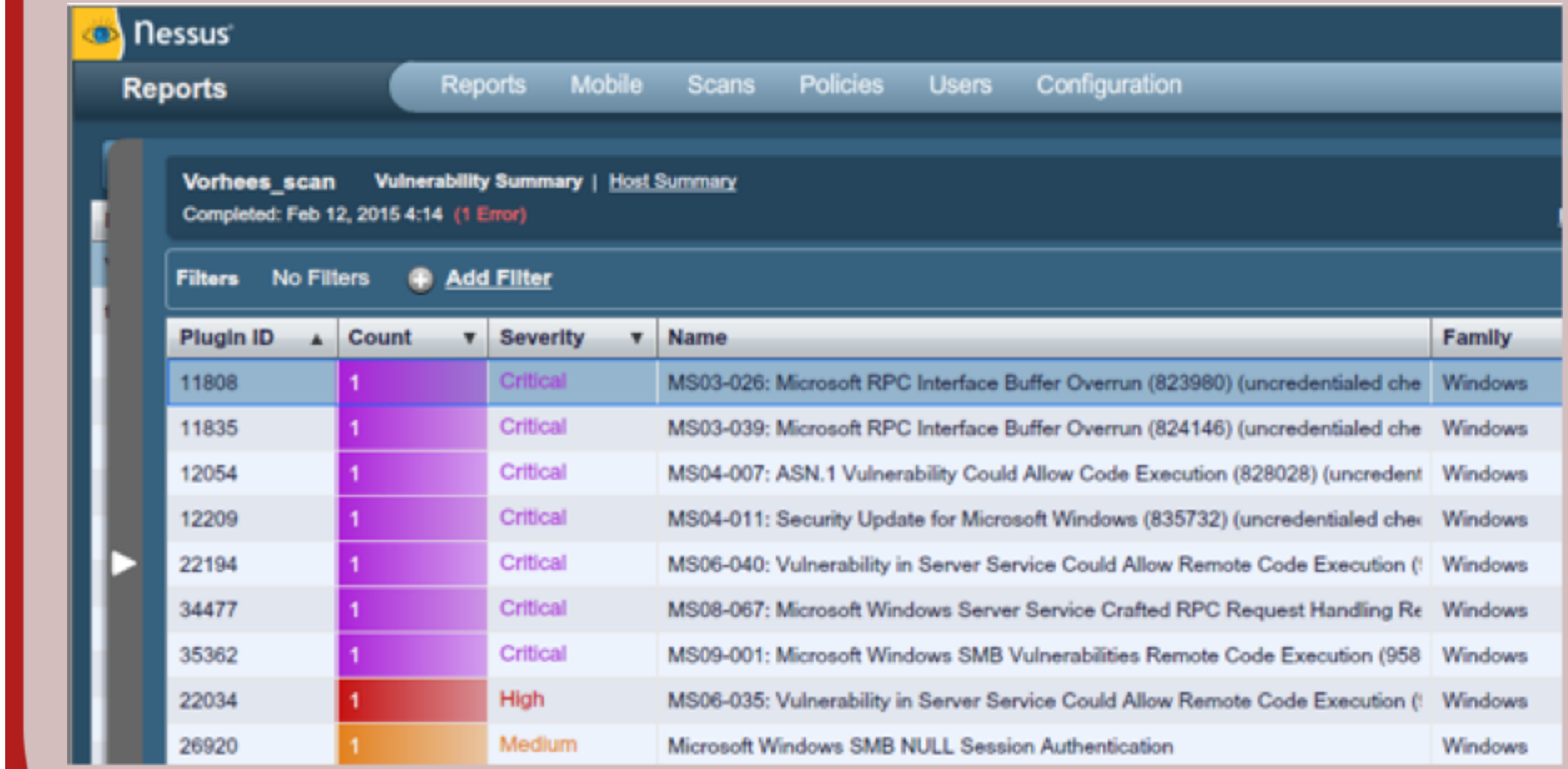
- Shows which hosts are most vulnerable



IP Address	Score	Repository	Total	Vulnerabilities
192.168.1.11	1778	Test Repository	425	176 241
192.168.1.56	310	RonLab Passive	55	28 24
192.168.1.16	272	RonLab Patch	271	18 247
192.168.1.24	212	RonLab Passive	107	54 50
192.168.1.58	190	RonLab Passive	32	16 7 9
192.168.1.13	109	RonLab Patch	46	13 29
192.168.1.14	103	RonLab Patch	60	6 52
192.168.1.24	103	RonLab Patch	50	11 35
192.168.1.24	94	RonLab Active	54	8 42
192.168.1.11	65	RonLab Patch	147	135
192.168.1.6	63	RonLab Passive	32	27
192.168.1.50	62	RonLab Passive	35	32
192.168.1.16	59	RonLab Active	29	24
192.168.1.1	46	RonLab Passive	50	37 10
192.168.1.13	44	RonLab Passive	45	41
192.168.1.53	43	RonLab Passive	42	40
192.168.1.14	36	RonLab Passive	18	16
192.168.1.55	35	RonLab Passive	35	35
192.168.1.1	34	RonLab Active	57	10 43
192.168.1.12	32	RonLab Passive	29	26
192.168.1.81	30	RonLab Active	39	6 30

Overview of Criticality

- Shows which vulnerabilities are most critical

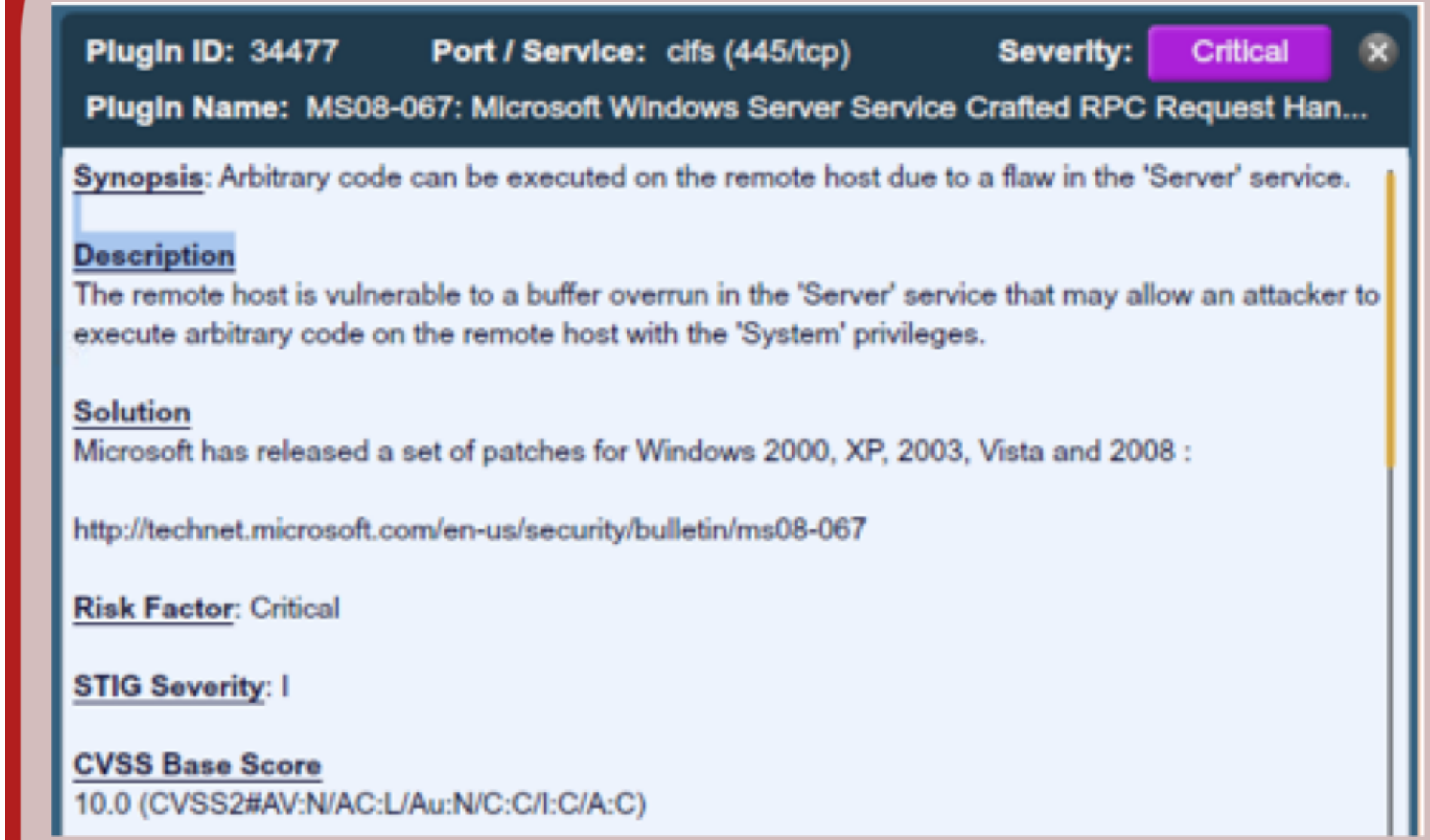


Vorhees_scan Vulnerability Summary | Host Summary
Completed: Feb 12, 2015 4:14 (1 Error)

Filters No Filters Add Filter

Plugin ID ▲	Count ▼	Severity ▼	Name	Family
11808	1	Critical	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed che	Windows
11835	1	Critical	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed che	Windows
12054	1	Critical	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredent	Windows
12209	1	Critical	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed che	Windows
22194	1	Critical	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (!	Windows
34477	1	Critical	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Re	Windows
35362	1	Critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958	Windows
22034	1	High	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (!	Windows
26920	1	Medium	Microsoft Windows SMB NULL Session Authentication	Windows

Details of a Vulnerability



Plugin ID: 34477 **Port / Service:** cifs (445/tcp) **Severity:** Critical

Plugin Name: MS08-067: Microsoft Windows Server Service Crafted RPC Request Han...

Synopsis: Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description

The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :

http://technet.microsoft.com/en-us/security/bulletin/ms08-067

Risk Factor: Critical

STIG Severity: I

CVSS Base Score

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

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE