SYSTEM HARDENING:

Vulnerabilities and Remediations

-By Anish Niure

Abstract:

In this report we are going to list the various vulnerabilities, found in the targets we have penetrate through in the back. I have used Nessus to provide me the detail information about the existing vulnerabilities and quoted the solutions to those vulnerabilities. Confidentiality, integrity, and Availability in cyber space is measured in terms of strong policy, secure system, and invincible defending. To be invincible, we have to always consider for every minute possibility that can overcome with time and must win every time. In this project I have listed the major vulnerabilities and basic remediations, that can harden the system. However, in real world not only the machines but the whole infrastructure physically and technically be protected. All fundamentals in the workspace are responsible for the security and to preserve CIA trade.

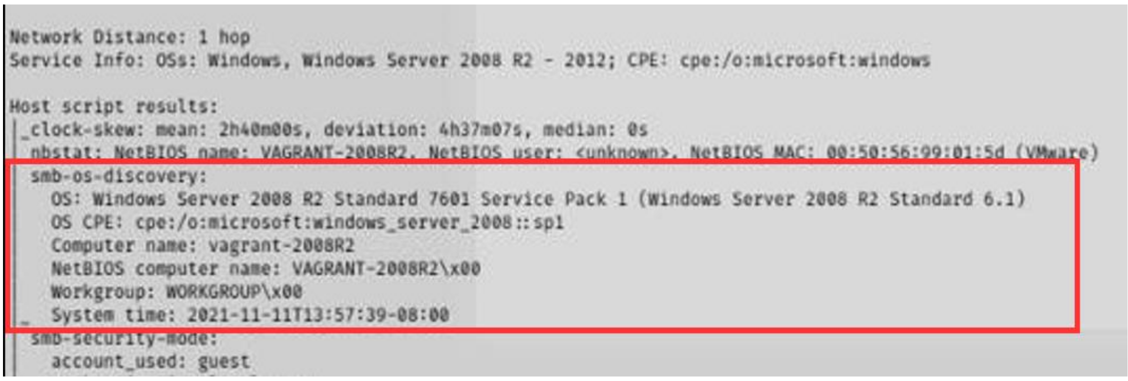
Hardening the system Vulnerabilities: Minimum Improvement in the system will take the external threats to think twice, because not a single system is 100 percent secure, the defence in depth policy is adopted, and we need to think how long we will be isolate our system from the threats. The report will provide the general idea to search the vulnerabilities and to mitigate them.

Contents

1.0 Windows Operating Systems

1.1 Target 192.168.1.103

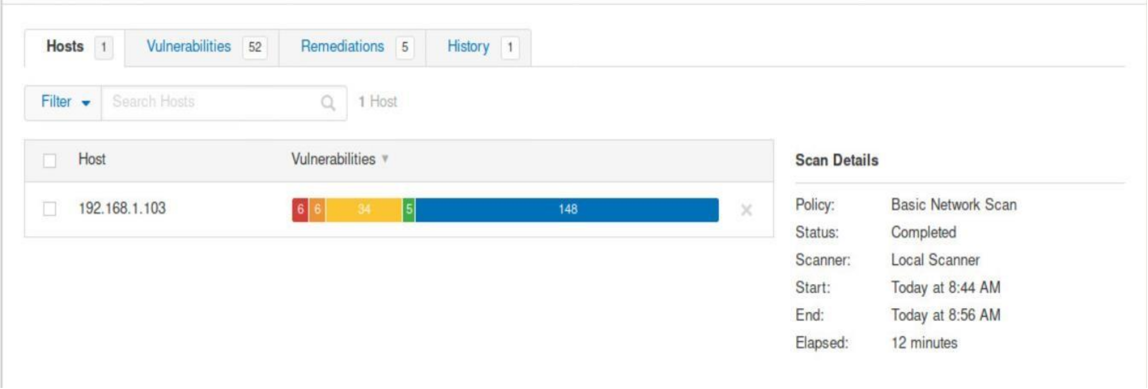
Operating system: Windows Server 2008 R2 Standard 6.1.



```
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h40m00s, deviation: 4h37m07s, median: 0s
| nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:99:01:5d (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: vagrant-2008R2
|   NetBIOS computer name: VAGRANT-2008R2\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-11-11T13:57:39-08:00
| smb-security-mode:
|   account_used: guest
```

fig: nmap scan nmap -sV -A -p- 192.168.1.103



Host	Vulnerabilities
192.168.1.103	6 6 34 5 148

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 8:44 AM
End:	Today at 8:56 AM
Elapsed:	12 minutes

fig: nessus scan [6 critical, 6 high and other vulnerabilities]

Findings:

Vulnerabilities:

1. **Manage Engine Desktop Central 8/9 <Build 91100 Multiple RCE**

Our target is running Manage Engine Desktop Central 9 in port 8022, which is vulnerable to multiple remote code execution. It cannot properly sanitize the user inputs, which can be exploited by any threats to upload malicious files. [1]

2. **Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (Uncredentialed Check)**
   This vulnerability is found in remote Desktop Protocol operating in port 3389 and can allow any malicious actor to send specially crafted requests, and on successful exploit they can execute the malicious scripts. [2]

3. **MS11-030 Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)**
   Any threats can sed specially crafted LLMNR queries and in successful exploitation can upload or install malicious programs or software that can allow them to execute backdoor session. [3]

4. **MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution**
   The target machine windows server 2008 R2 is critically vulnerable to MS14-066, in which attacker can inject arbitrary code on a target server. [4]

5. **Unsupported Windows OS (remote)**
   The Microsoft version 2008 R2 is no longer supported which is likely to contain many security vulnerabilities.

6. **Elasticsearch ESA-1015-06**
   In port 8009, in our target is running Apache Jserv (protocol v1.3), which makes it vulnerable to ElasticSearch which can allow remote code execution. [5]

7. **SSL Certificate Cannot Be Trusted**

Solutions:

1. **Mitigation to ManageEngine Desktop Central existing old version.**
   - The manageEngine Desktop Central should be updated to version 9 or later. [1]

2. **Mitigation to BlueKeep exploit. [2]**
   - Do not use RDP port if not necessarily required.
   - Enable network level Authentication (NLA) on the target machine.
   - Configure firewalls behind the RDP port in our case, port 3389.

3. **Mitigation to MS11-030.**
   - Update the Microsoft versions, enable services like auto updating in Microsoft can update the patched versions of this vulnerabilities if possible, running Microsoft defender firewall can prevent from executing malwares. [3]

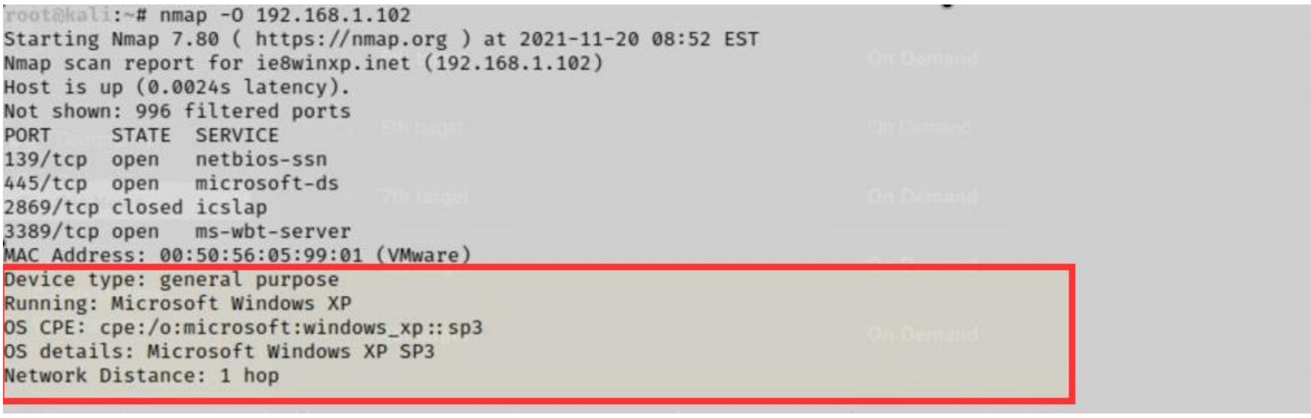
4. **Mitigation to MS14-066.**
   - Easy mitigating technique is to update the most recent security features from Microsoft.

5. **ElasticSearch mitigation.**
    - Update the Apache Jserv to the latest version.

6. **SSL certificate.**
    - Generating or purchasing, proper SSL certificate for SSH connection can eradicate the SSH certificate issue.

1.2 Target 192.168.1.102

Operating System: Windows XP SP3.



```
root@kali:~# nmap -O 192.168.1.102
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-20 08:52 EST
Nmap scan report for ie8winxp.inet (192.168.1.102)
Host is up (0.0024s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2869/tcp closed icslap
3389/tcp open   ms-wbt-server
MAC Address: 00:50:56:05:99:01 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
```

fig: nmap scan os detection

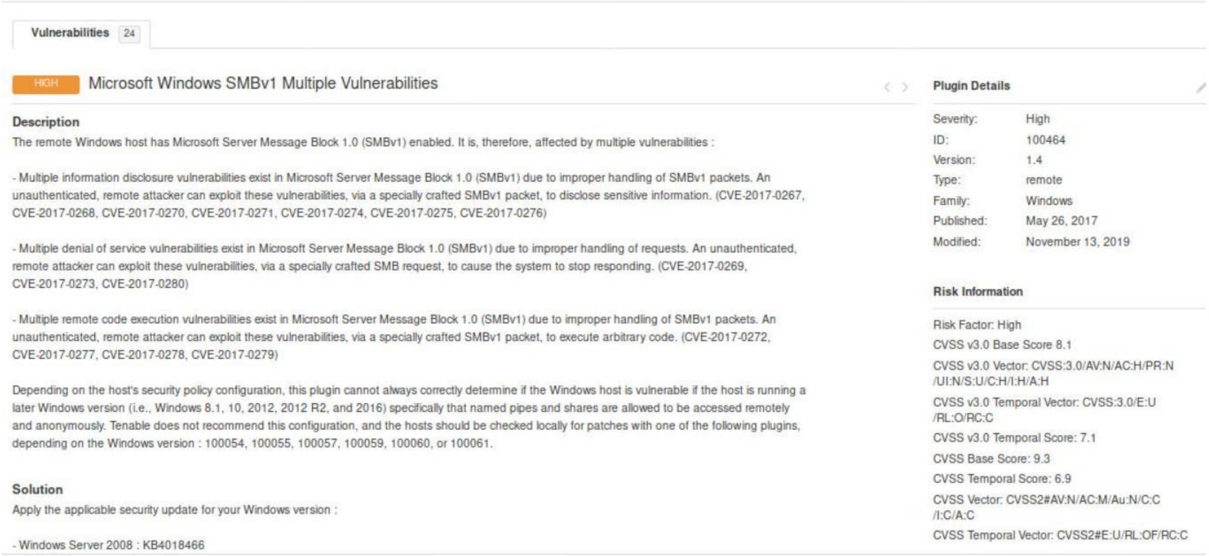
Findings:

Vulnerabilities:

1. **Microsoft Windows XP Unsupported Installation Detection**
   Because the target Microsoft XP is not longer supported by the vendor, the patches are not released, due to which containing many security exploits is high.

2. **Microsoft RPD RCE (CVE-2019-0708) (Uncredentialed Check)**
   This vulnerability is found in remote Desktop Protocol operating in port 3389 and can allow any malicious actor to send specially crafted requests, and on successful exploit they can execute the malicious scripts. [2]

3. **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (EternalBlue)**
   It is a software vulnerability of windows operating system, running (SMB) version 1, (SMBv1) protocol, which is file sharing protocol that allows access to files in remote server from port 445. Our target is running smbv1 which makes it vulnerable to the eternal blue, as well as multiple denial of service exploits. [6]



Microsoft Windows SMBv1 Multiple Vulnerabilities

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)

- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.

Solution

Apply the applicable security update for your Windows version :

- Windows Server 2008 : KB4018466

Plugin Details

Severity:	High
ID:	100464
Version:	1.4
Type:	remote
Family:	Windows
Published:	May 26, 2017
Modified:	November 13, 2019

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 8.1

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 7.1

CVSS Base Score: 9.3

CVSS Temporal Score: 6.9

CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Fig: Nessus report on SMB1 Vulnerabilities

4. **Microsoft Windows Remote Desktop Protocol Server Man-in-the Middle Weakness**
   The RDP version our target is using is vulnerable to man-in-the-middle attack because the does not validate the identity for the server when setting up encryption. So, any attacker with this ability can easily intercept the traffic. [7]

Solutions:

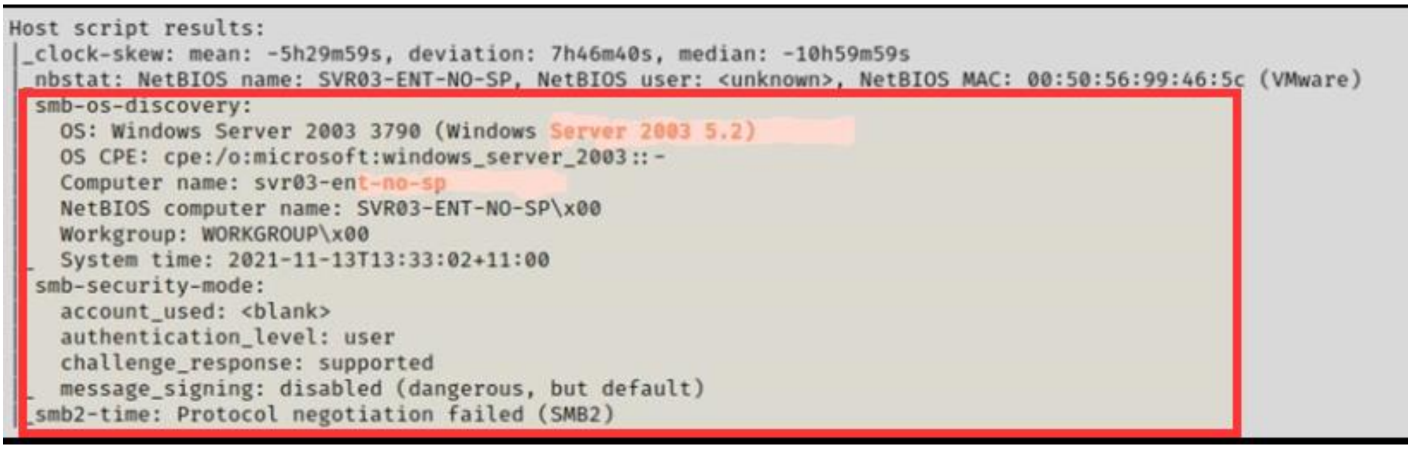
1. **Install vender supported Operating system.**
   - Upgrading to latest windows 10 -11, is the easy solution for this risk because many patches are available to the current operating systems.

2. **Mitigation to BlueKeep exploit RDP RCE and RDP Man in the Middle weakness. [2]**
   - Do not use RDP port if not necessarily required.
   - Enable network level Authentication (NLA) on the target machine.
   - Configure firewalls behind the RDP port in our case, port 3389.
   - Use system monitoring tools, install sysinternals in the machine, and keep monitoring the system.

3. **Mitigation for MS17_010(Eternal Blue).**
   - Stop using smbv1, upgrade to the latest version of SMB protocol.[6]

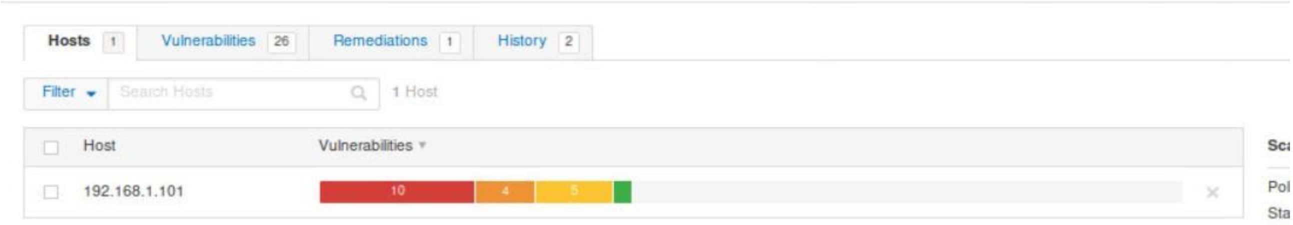
1.3 Target 192.168.1.101

Operating System- Windows server 2003 5.2



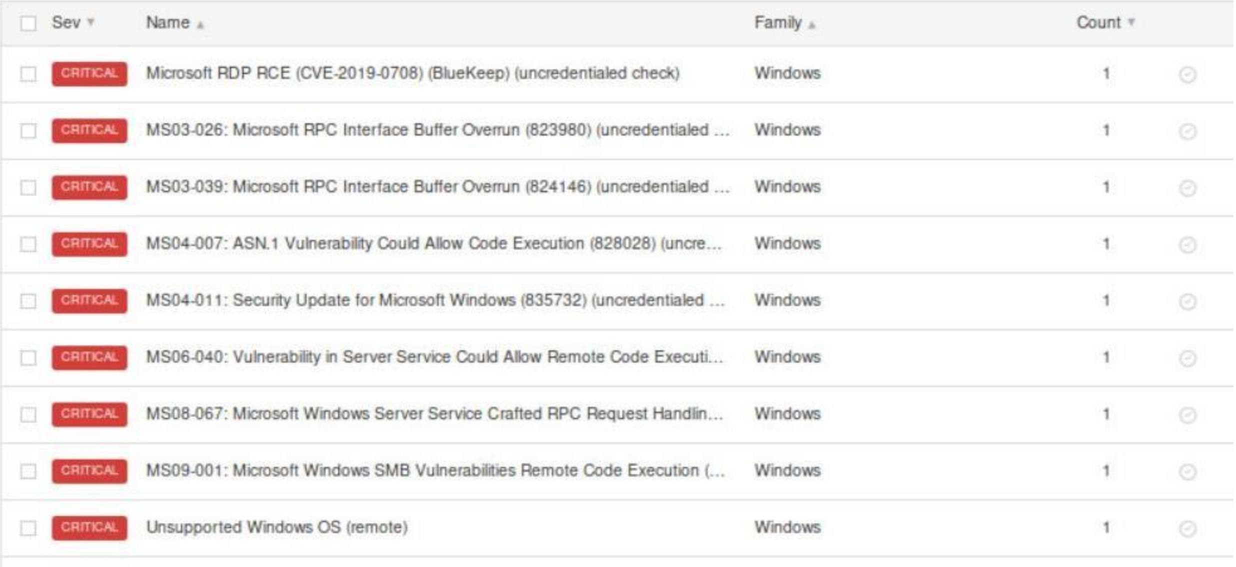
```
Host script results:
|_clock-skew: mean: -5h29m59s, deviation: 7h46m40s, median: -10h59m59s
| nbstat: NetBIOS name: SVR03-ENT-NO-SP, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:99:46:5c (VMware)
| smb-os-discovery:
|   OS: Windows Server 2003 3790 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::-
|   Computer name: svr03-ent-no-sp
|   NetBIOS computer name: SVR03-ENT-NO-SP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-11-13T13:33:02+11:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

fig: nmap scan os detection



□	Host	Vulnerabilities
□	192.168.1.101	10 4 5

fig: nessus scan [10 critical, 6 high and other vulnerabilities]



□	Sev	Name	Family	Count
□	CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Windows	1
□	CRITICAL	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed ...	Windows	1
□	CRITICAL	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed ...	Windows	1
□	CRITICAL	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncre...	Windows	1
□	CRITICAL	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed ...	Windows	1
□	CRITICAL	MS06-040: Vulnerability in Server Service Could Allow Remote Code Executi...	Windows	1
□	CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handlin...	Windows	1
□	CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (...	Windows	1
□	CRITICAL	Unsupported Windows OS (remote)	Windows	1

Findings:

Vulnerabilities:

1. **Microsoft windows server 2003 unsupported Installation**

Microsoft windows server 2003 is not supported by the vendor anymore so, new patches and updates are not implemented which makes the operating system more vulnerable.

2. **Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)**
   This vulnerability is found in remote Desktop Protocol operating in port 3389 and can allow any malicious actor to send specially crafted requests, and on successful exploit they can execute the malicious scripts. [2]

3. **MS03-026: Microsoft RPC Interface Buffer Overrun (823980) uncredentialed check.**
   The RPC interface, in this vulnerability, due to flaw on function RemoteActivation() can allow attacker to execute arbitrary code on the remote host with the system Privilege. [8]

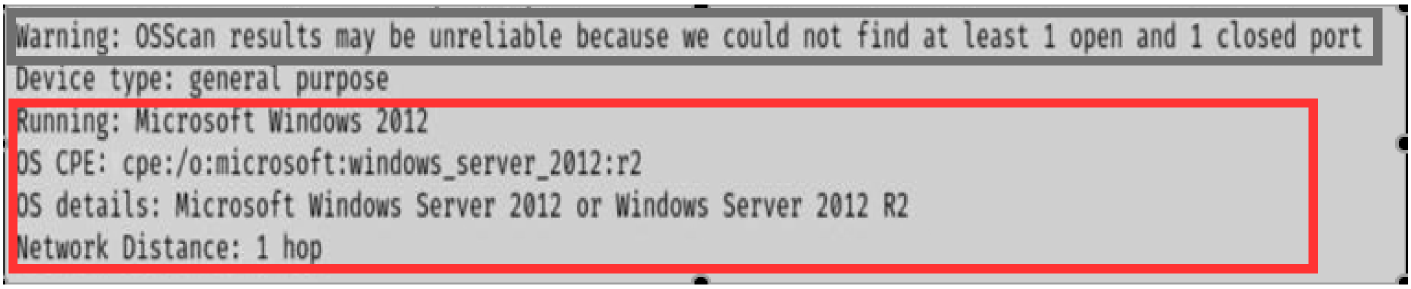
4. **MS04-007: ASN.1 Vulnerability could allow code Execution.**
   This vulnerability is due to flaw in the ASN.1 library that exists in the Microsoft, this vulnerability causes the buffer overflow and on successful exploitation attacker can execute code to get system privilege in the system. [9]

Solutions:

- Because the system is no longer supported by the vendor, this machine is highly vulnerable and the best option to keep oneself safe is by just upgrading to newer and secure OS like windows 10 or windows server 2016 and 2019.
- The host has enabled the RDP port 3389 which is one focus for the actors so defining some firewalls behind this port can secure the vulnerabilities of this port such as BlueKeep, RPC buffer overrun which exists in this target.
- Updating the security version to the newest one, can save the target from multiple vulnerabilities that cause buffer overflow, because the vulnerabilities are older, and the vendor has already released patches for these vulnerabilities.
- Using the recommended smv2 or smv3 with regular system monitor can prevent the system with multiple smb vulnerabilities.

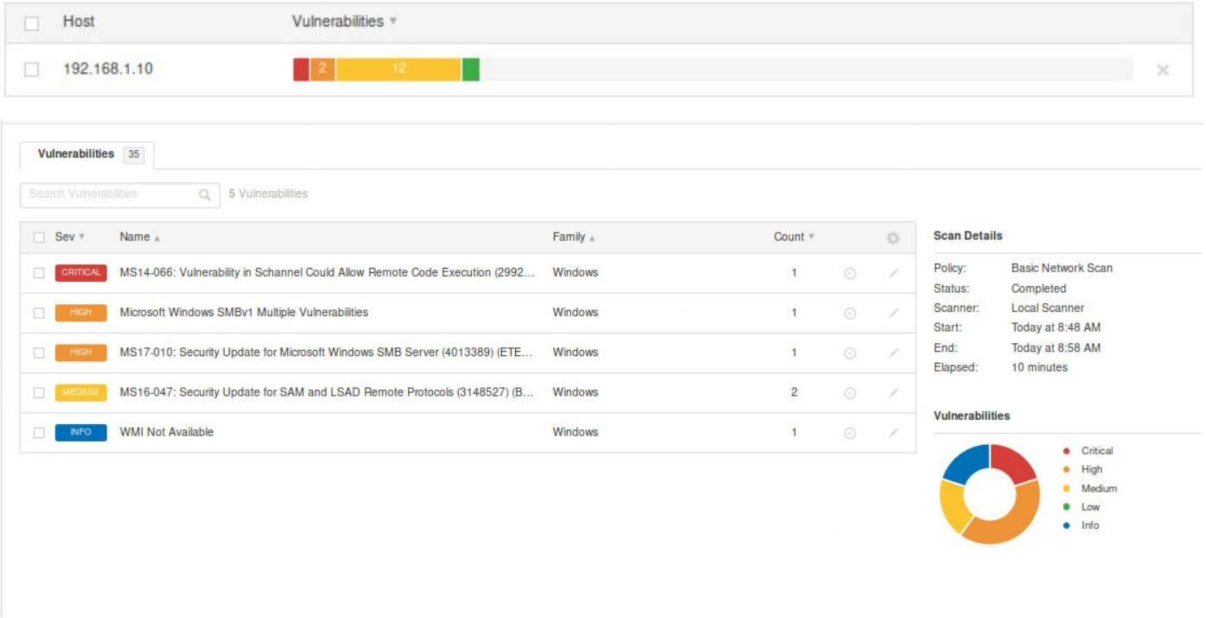
1.5 Target: 192.168.1.10

Operating System: Windows Server 2012 R2



```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
```

fig: nmap scan os detection



□	Host	Vulnerabilities
□	192.168.1.10	2 12

Vulnerabilities 35

Search Vulnerabilities 5 Vulnerabilities

□	Sev	Name	Family	Count
□	CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992...	Windows	1
□	HIGH	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	1
□	HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETE...	Windows	1
□	MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (B...	Windows	2
□	INFO	WMI Not Available	Windows	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 8:48 AM
End:	Today at 8:58 AM
Elapsed:	10 minutes

Vulnerabilities

fig: Nessus Scan [2 high and 12 medium vulnerabilities.]

Findings:

Vulnerabilities:

1. **MS14-066: Vulnerability ins Channel Could Allow Remote Code Execution (2992611)**
   This vulnerability is in the SSL port misconfiguration, Attacker can exploit this vulnerability by sending crafted packets to the target machine, from the secure channel port. [12]

2. **Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness**
   The RDP version our target is using is vulnerable to man-in-the-middle attack because the does not validate the identity for the server when setting up encryption. So any attacker with this ability can easily intercept the traffic. [7]

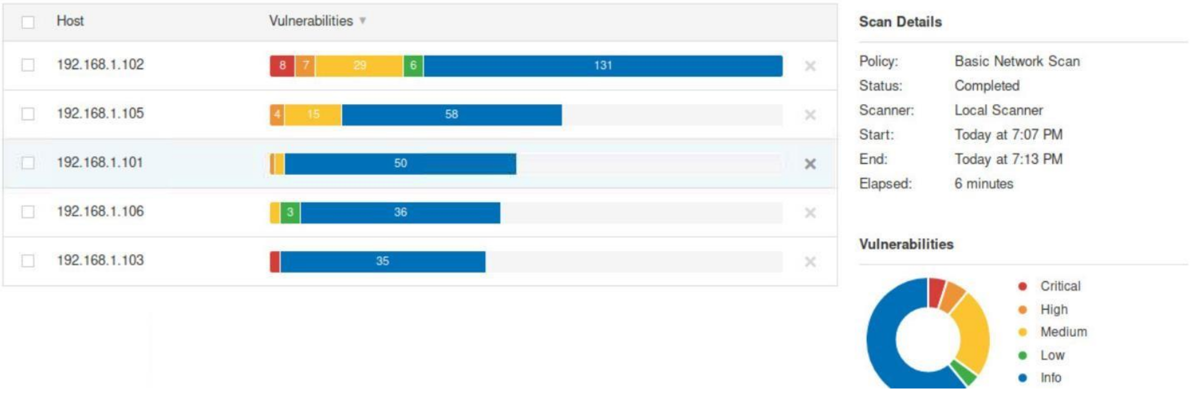
3. **EternalBlue(MS10-010) exploitation**
   This exploitation is because of the smbv1 enabled in the port 445, the weakness allows to execute remote code.

Solutions:

- Install the patches for windows 2012 R2 for this vulnerability.
- Enable firewall behind the port 3389, or stopping the remote desktop service if not required, also regularly monitoring the rdesktop users and the traffic, windows defender firewall should be enabled to mitigate rdesktop Protocol.
- Stop using the smbv1 instead smbv3 or smbv3 should be installed to reduce the eternal blue exploitation.

- We had seen the pawned password used in the administrator account of the domain, which can be fruitful for any attacker and easily brute force the password and decrypt the hash, so strong password policy should be implemented, in the domain environment,

2.0 Linux Operating Systems



□ Host	Vulnerabilities ▾	
□ 192.168.1.102	8 7 29 6 131	×
□ 192.168.1.105	4 15 58	×
□ 192.168.1.101	50	×
□ 192.168.1.106	3 36	×
□ 192.168.1.103	35	×

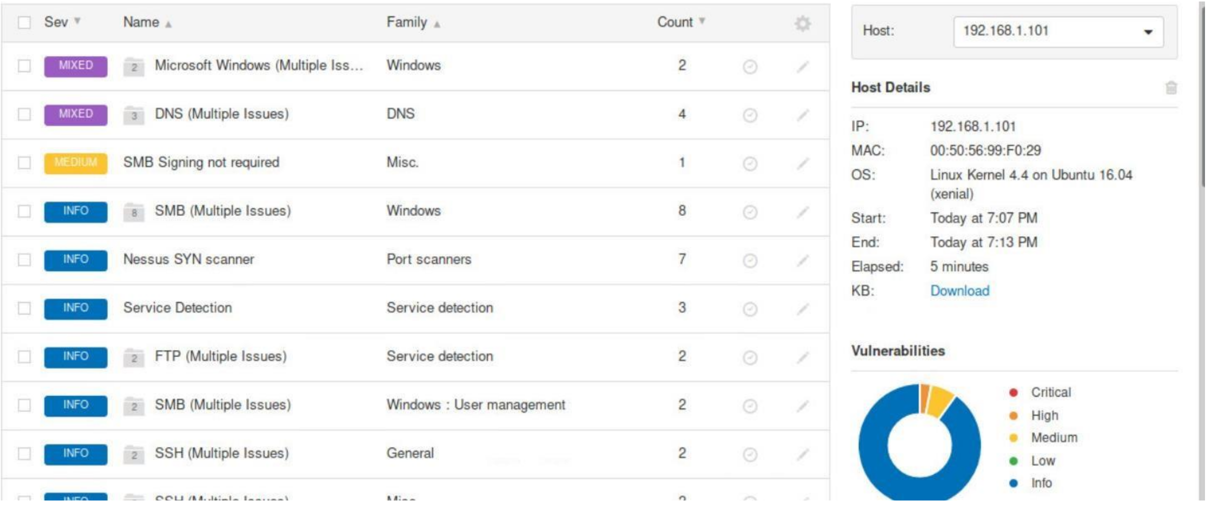
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 7:07 PM
End:	Today at 7:13 PM
Elapsed:	6 minutes

Vulnerabilities

2.1 Target: 192.168.1.101

Operating System: Linux Kernel 4.4 on Ubuntu 16.04(xenial)



□	Sev	Name	Family	Count
□	MIXED	2 Microsoft Windows (Multiple Iss...	Windows	2
□	MIXED	3 DNS (Multiple Issues)	DNS	4
□	MEDIUM	SMB Signing not required	Misc.	1
□	INFO	8 SMB (Multiple Issues)	Windows	8
□	INFO	Nessus SYN scanner	Port scanners	7
□	INFO	Service Detection	Service detection	3
□	INFO	2 FTP (Multiple Issues)	Service detection	2
□	INFO	2 SMB (Multiple Issues)	Windows : User management	2
□	INFO	2 SSH (Multiple Issues)	General	2
□	INFO	SSH (Multiple Issues)	Misc.	2

Host: 192.168.1.101

Host Details

IP:	192.168.1.101
MAC:	00:50:56:99:F0:29
OS:	Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Start:	Today at 7:07 PM
End:	Today at 7:13 PM
Elapsed:	5 minutes
KB:	Download

Vulnerabilities

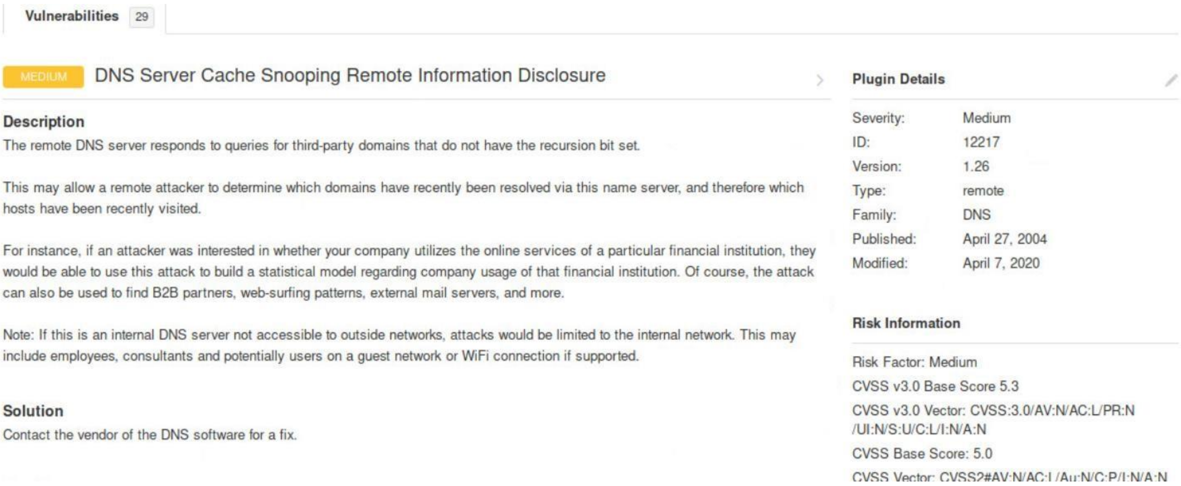
Findings:

Vulnerabilities:

1. **DNS Server Snooping Remote Information Disclosure.**
This allows the remote attacker to determine the domain name and the hosts visiting the domain, which leaks the DNS and hosts information, because the DNS server answers the third-party domains that do not have the recursion bit set. [15]

Remediations:

1. Fix the DNS software, contacting the vendor.



Vulnerabilities 29

MEDIUM DNS Server Cache Snooping Remote Information Disclosure

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

Solution

Contact the vendor of the DNS software for a fix.

Plugin Details

Severity:	Medium
ID:	12217
Version:	1.26
Type:	remote
Family:	DNS
Published:	April 27, 2004
Modified:	April 7, 2020

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.3

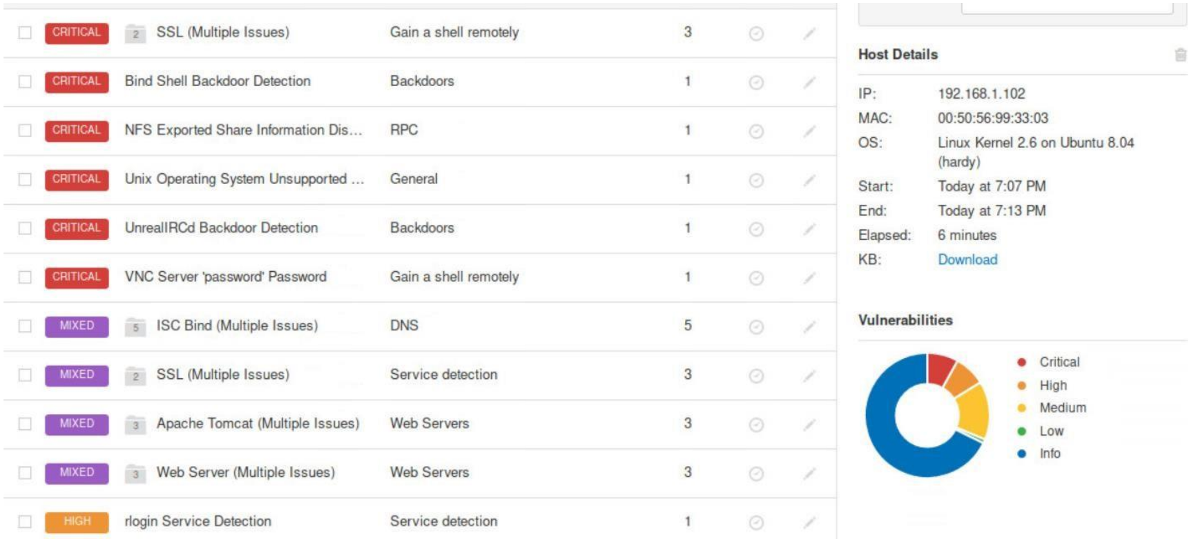
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

2.2 Target: 192.168.1.102

Operating System: Linux Kernel 2.6 on ubuntu 8.04 (hardy)



□	CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3	⊘	✎
□	CRITICAL	Bind Shell Backdoor Detection	Backdoors	1	⊘	✎
□	CRITICAL	NFS Exported Share Information Dis...	RPC	1	⊘	✎
□	CRITICAL	Unix Operating System Unsupported ...	General	1	⊘	✎
□	CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1	⊘	✎
□	CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1	⊘	✎
□	MIXED	5 ISC Bind (Multiple Issues)	DNS	5	⊘	✎
□	MIXED	2 SSL (Multiple Issues)	Service detection	3	⊘	✎
□	MIXED	3 Apache Tomcat (Multiple Issues)	Web Servers	3	⊘	✎
□	MIXED	3 Web Server (Multiple Issues)	Web Servers	3	⊘	✎
□	HIGH	rlogin Service Detection	Service detection	1	⊘	✎

Host Details

IP:	192.168.1.102
MAC:	00:50:56:99:33:03
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 7:07 PM
End:	Today at 7:13 PM
Elapsed:	6 minutes
KB:	Download

Vulnerabilities

Findings:

Vulnerabilities:

1. **Debian OpenSSH/OpenSSL Package Random Number Generator Weakness.**
   Anyone can conduct the man in the middle attack due to the bug in the ssl in our target machine which makes easy for attacker to obtain the private parts of the SSH. [16]

2. **Bind Shell backdoor Detection**
   Without any authentication, any attacker can use the this weakness to create the remote session, [17]

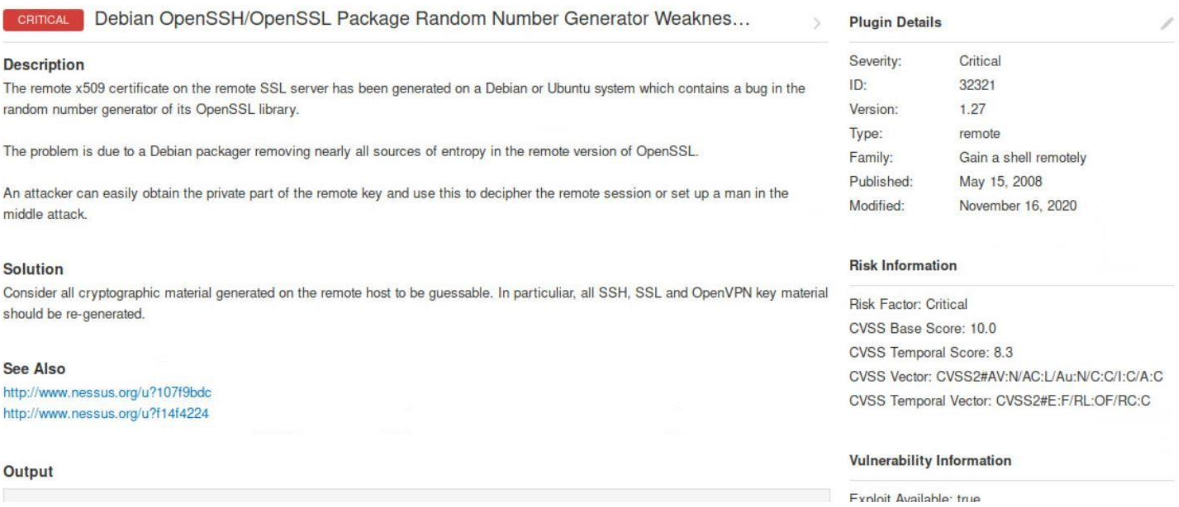
3. **NFS Exported Share Information Disclosure**
   This vulnerability can allow the share to mount on their system which will disclose the information of the target machine.

4. **Unix Operating System Unsupported Version Detection**
   Ubuntu 8.4 is outdated version, which is not supported by the vendor anymore and the security patches are not released anymore.

5. **UnrecallRCd Backdoor Detection.**

Solutions:

- Securing the encryption key by regenerating all the SSH and SSL keys.[16]
- Monitor the traffics and verify if the host has been already compromised and secure the listening with the firewall and proper authentication method to prevent bind shell backdoor detection.[17]
- Configuring the shares, implementing proper authentication method, filtering the smb ports eradicates the NFS share weakness.
- Update the operating system to the newest and secure version.
- Use the strong password, timely monitor the logs, any report any breaches.



CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator Weaknes...

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

Plugin Details

Severity:	Critical
ID:	32321
Version:	1.27
Type:	remote
Family:	Gain a shell remotely
Published:	May 15, 2008
Modified:	November 16, 2020

Risk Information

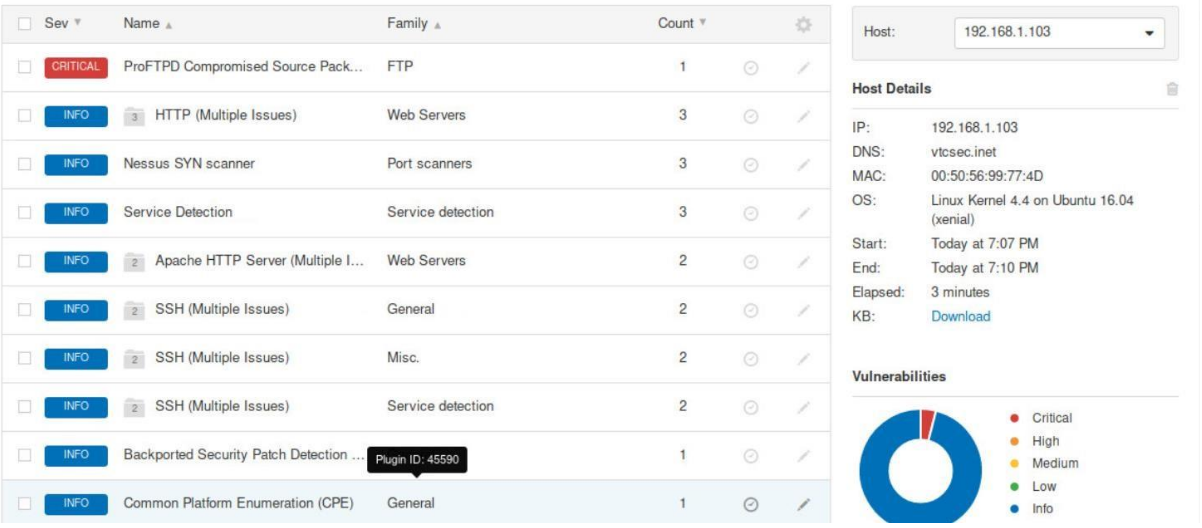
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 8.3
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

Exploit Available: true

2.3 Target: 192.168.1.103

Operating System: Linux Kerel 4.4 on Ubuntu 16.02 (xenial)



□	Sev	Name	Family	Count
□	CRITICAL	ProFTPD Compromised Source Pack...	FTP	1
□	INFO	3 HTTP (Multiple Issues)	Web Servers	3
□	INFO	Nessus SYN scanner	Port scanners	3
□	INFO	Service Detection	Service detection	3
□	INFO	2 Apache HTTP Server (Multiple I...	Web Servers	2
□	INFO	2 SSH (Multiple Issues)	General	2
□	INFO	2 SSH (Multiple Issues)	Misc.	2
□	INFO	2 SSH (Multiple Issues)	Service detection	2
□	INFO	Backported Security Patch Detection ...	Plugin ID: 45590	1
□	INFO	Common Platform Enumeration (CPE)	General	1

Host: 192.168.1.103

Host Details

IP:	192.168.1.103
DNS:	vtcsec.inet
MAC:	00:50:56:99:77:4D
OS:	Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Start:	Today at 7:07 PM
End:	Today at 7:10 PM
Elapsed:	3 minutes
KB:	Download

Vulnerabilities

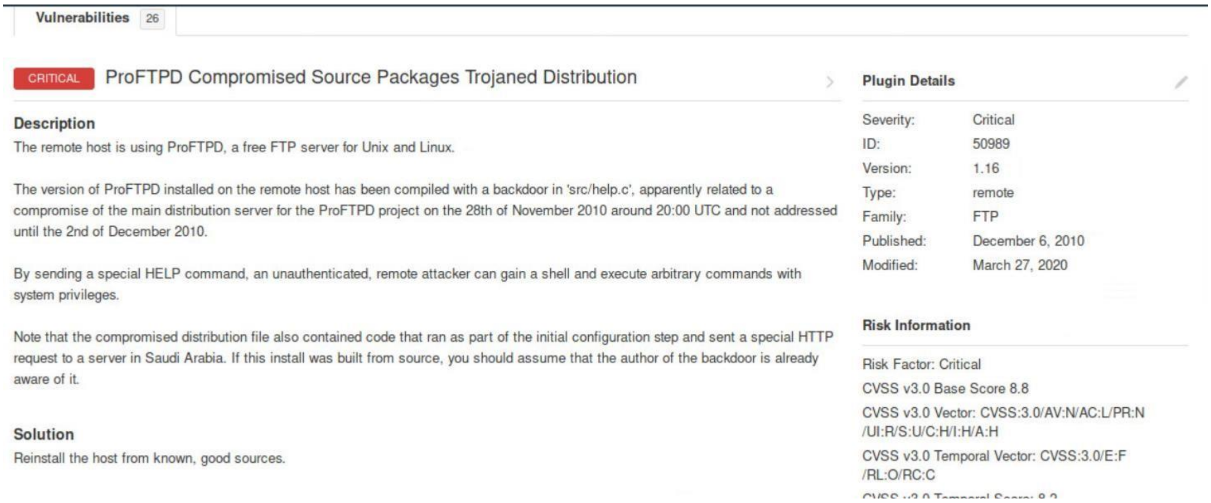
Findings:

Vulnerabilities:

1. **ProFTPD Compromised Source Packages Trojaned Distribution**
   The ftp server enabled in the target machines has a lot of security bugs and many modules are available in the Metasploit for backdooring purpose, from which any one can connect or exploit the target machine.

Solutions:

- Reinstalling the host from known and good sources, update the version of the machine.
- Overall, use the proper password policy make root user password strong, give the least privilege to the users, and regular monitor the logs and traffics coming and going from the device.



Vulnerabilities 26

CRITICAL ProFTPD Compromised Source Packages Trojaned Distribution

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

The version of ProFTPD installed on the remote host has been compiled with a backdoor in 'src/help.c', apparently related to a compromise of the main distribution server for the ProFTPD project on the 28th of November 2010 around 20:00 UTC and not addressed until the 2nd of December 2010.

By sending a special HELP command, an unauthenticated, remote attacker can gain a shell and execute arbitrary commands with system privileges.

Note that the compromised distribution file also contained code that ran as part of the initial configuration step and sent a special HTTP request to a server in Saudi Arabia. If this install was built from source, you should assume that the author of the backdoor is already aware of it.

Solution

Reinstall the host from known, good sources.

Plugin Details

Severity:	Critical
ID:	50989
Version:	1.16
Type:	remote
Family:	FTP
Published:	December 6, 2010
Modified:	March 27, 2020

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 8.8

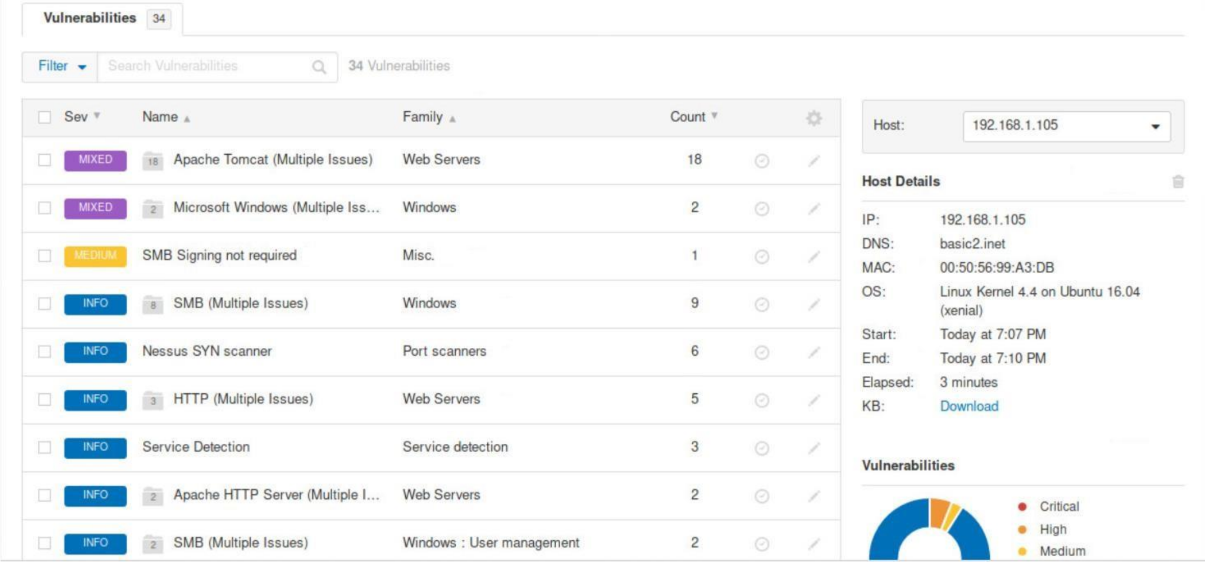
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N /UI:R/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:F /RL:O/RC:C

CVSS v3.0 Temporal Score: 8.2

2.4 Target: 192.168.1.105

Operating System: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)



Vulnerabilities 34

Filter ▾ Search Vulnerabilities 34 Vulnerabilities

□ Sev	Name	Family	Count
□ MIXED	18 Apache Tomcat (Multiple Issues)	Web Servers	18
□ MIXED	2 Microsoft Windows (Multiple Iss…	Windows	2
□ MEDIUM	SMB Signing not required	Misc.	1
□ INFO	8 SMB (Multiple Issues)	Windows	9
□ INFO	Nessus SYN scanner	Port scanners	6
□ INFO	3 HTTP (Multiple Issues)	Web Servers	5
□ INFO	Service Detection	Service detection	3
□ INFO	2 Apache HTTP Server (Multiple I…	Web Servers	2
□ INFO	2 SMB (Multiple Issues)	Windows : User management	2

Host: 192.168.1.105

Host Details

IP:	192.168.1.105
DNS:	basic2.inet
MAC:	00:50:56:99:A3:DB
OS:	Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Start:	Today at 7:07 PM
End:	Today at 7:10 PM
Elapsed:	3 minutes
KB:	Download

Vulnerabilities

Findings:

Vulnerabilities:

1. **Apache Tomcat Prior to 9.0.0 < 9.0.10 multiple vulnerabilities exist such as insecure default settings for the CORS filter (CVE-2019-8014), validation in hostname.**
   The target machine is running the Apache Tomcat server which has listed many vulnerabilities.

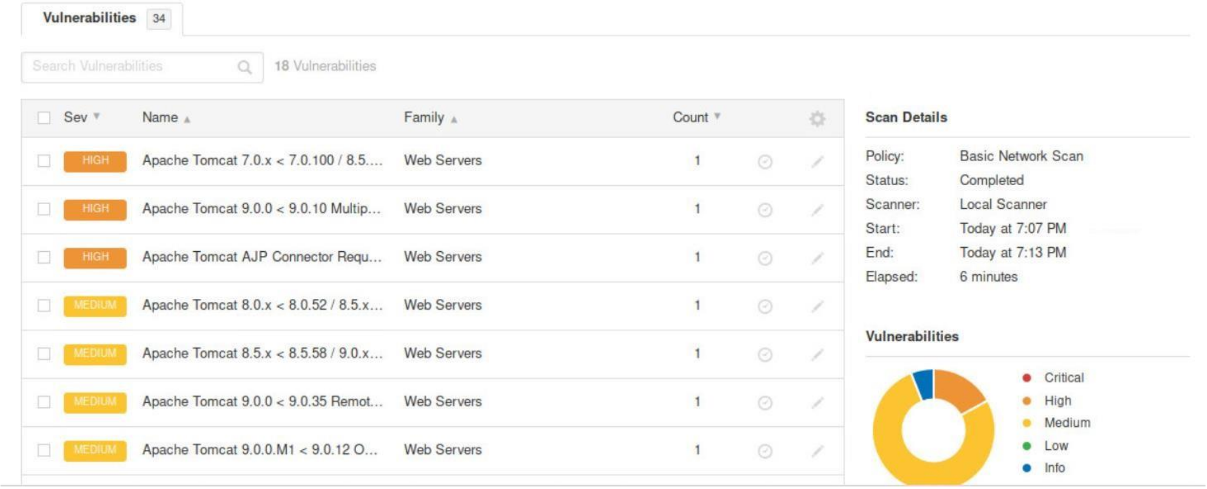
2. **Apache Tomcat AJP Connector Request Injection (Ghostcat)**

3. **Microsoft Windows SMB Shares Unpriviledge Access.**
   Anyone can access the share in the target machine using the given credentials, which allow the attacker read, write to the file. [18]

4. **SMB Signing Not required.**

Solutions:

- Update the Tomcat server to the most recent one.
- Anyone can access the share in the target machine using the given credentials, so securing the share files and give minimum permission to the file to be share, encryption of the files with the strong algorithm.
- The target does not require SMB signing which can be mitigated, by enabling the authentication level in the SMB.
- Overall, do not include any users' credentials in the webpages, use good encryption method in order to protect the share files, update the security feature of the system to the most recent one.



Vulnerabilities 34

Search Vulnerabilities 18 Vulnerabilities

□	Sev ▾	Name ▴	Family ▴	Count ▾
□	HIGH	Apache Tomcat 7.0.x < 7.0.100 / 8.5....	Web Servers	1
□	HIGH	Apache Tomcat 9.0.0 < 9.0.10 Multip...	Web Servers	1
□	HIGH	Apache Tomcat AJP Connector Requ...	Web Servers	1
□	MEDIUM	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x...	Web Servers	1
□	MEDIUM	Apache Tomcat 8.5.x < 8.5.58 / 9.0.x...	Web Servers	1
□	MEDIUM	Apache Tomcat 9.0.0 < 9.0.35 Remot...	Web Servers	1
□	MEDIUM	Apache Tomcat 9.0.0.M1 < 9.0.12 O...	Web Servers	1

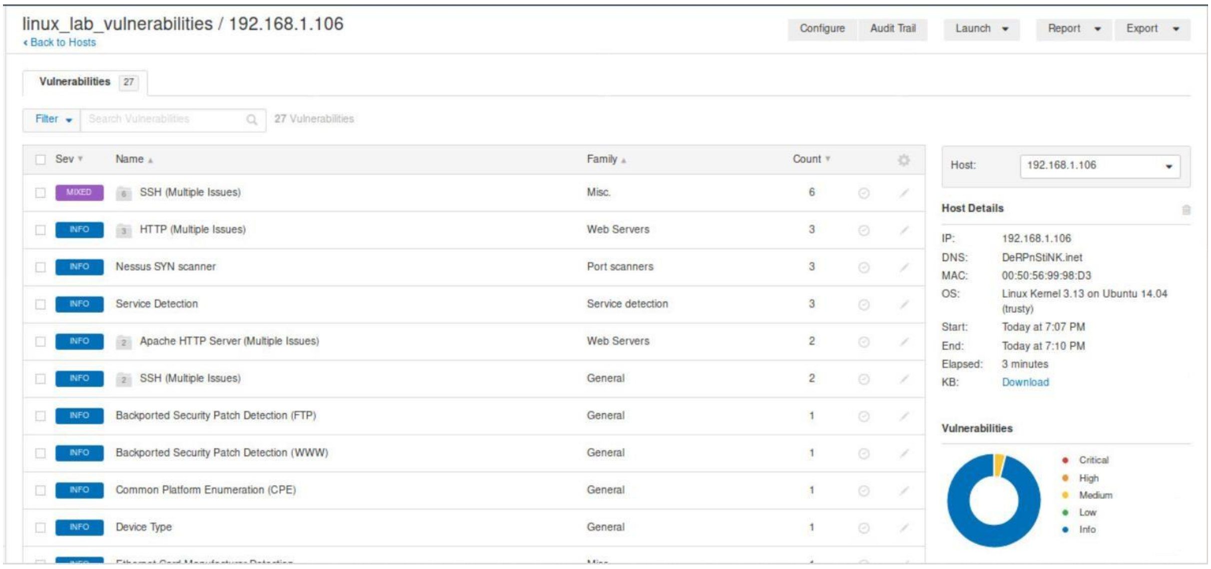
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 7:07 PM
End:	Today at 7:13 PM
Elapsed:	6 minutes

Vulnerabilities

2.5 Target: 192.168.1.106

Operating System: Linux Kernel 3.14 on Ubuntu 14.04 (trusty)



linux_lab_vulnerabilities / 192.168.1.106
‹ Back to Hosts

□	Sev	Name	Family	Count
□	MIXED	6 SSH (Multiple Issues)	Misc.	6
□	INFO	3 HTTP (Multiple Issues)	Web Servers	3
□	INFO	Nessus SYN scanner	Port scanners	3
□	INFO	Service Detection	Service detection	3
□	INFO	2 Apache HTTP Server (Multiple Issues)	Web Servers	2
□	INFO	2 SSH (Multiple Issues)	General	2
□	INFO	Backported Security Patch Detection (FTP)	General	1
□	INFO	Backported Security Patch Detection (WWW)	General	1
□	INFO	Common Platform Enumeration (CPE)	General	1
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1

Host: 192.168.1.106

Host Details

IP:	192.168.1.106
DNS:	DeRPnStiNK.inet
MAC:	00:50:56:99:98:D3
OS:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Start:	Today at 7:07 PM
End:	Today at 7:10 PM
Elapsed:	3 minutes
KB:	Download

Vulnerabilities

Findings:

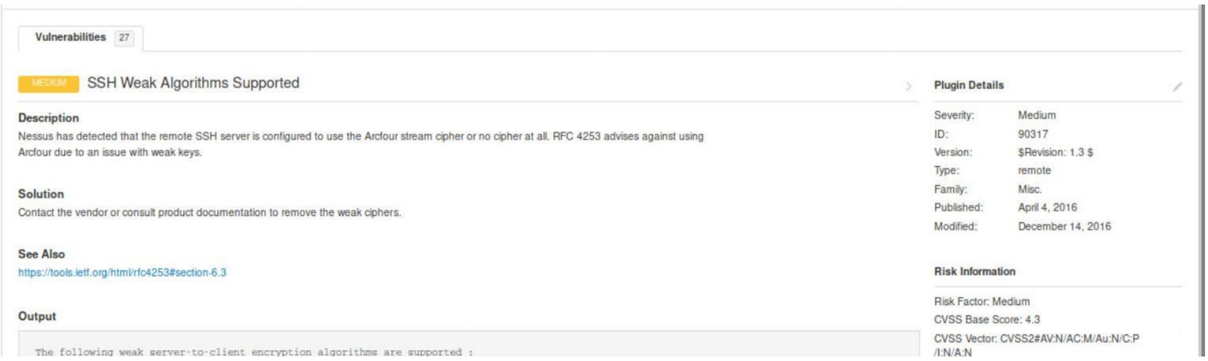
Vulnerabilities:

1. **SSH Weak Algorithms Supported.**

   The ssh in the target machine have weak algorithm, due to which anyone can easily ucipher the credentials or passphrases in the target.

Solutions:

- Remove the weak cipher algorithm, enable proper authentication.



MEDIUM SSH Weak Algorithms Supported

Description
Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution
Contact the vendor or consult product documentation to remove the weak ciphers.

See Also
https://tools.ietf.org/html/rfc4253#section-6.3

Output

```
The following weak server-to-client encryption algorithms are supported :
```

Plugin Details

Severity:	Medium
ID:	90317
Version:	$Revision: 1.3 $
Type:	remote
Family:	Misc.
Published:	April 4, 2016
Modified:	December 14, 2016

Risk Information

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

3.0 Conclusion:

Though, I have discussed various vulnerabilities in each Operating system and has discussed mitigation measures for each one, there are a lot of other vulnerabilities in those system. Different types of methodologies in the attacking surface results different types of vulnerabilities as well. I have discussed minimum and easy accessed vulnerabilities, however implementing those security features cannot be taken for hundred percent satisfaction. Through the developing cyber day to day, lots of threats, lots of vulnerabilities and lots of security questions are being answered day to day. The most important remediation for the system is to know the services running in one self's workspace and being updated about those services. In this report, many machines were of older versions and had a lot of security questions, however simple updates and changing passwords policies could have made pen testing a nightmare. Simple steps taken can prevent thousands exploits.

Thank you!!!

References

[1] tenable, "ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE," 11 19 2019. [Online]. Available: https://www.tenable.com/plugins/nessus/90192.

[2] MSRC, "Remote Desktop Services Remote Code Execution Vulnerability," [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708. [Accessed 14 05 2019].

[3] Microsoft, "Microsoft Security Bulletin MS11-030 - Critical," 12 04 2011. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030.

[4] Microsoft, "Microsoft Schannel Remote Code Execution Vulnerability - CVE-2014-6321," 31 03 2015. [Online]. Available: https://docs.microsoft.com/en-us/securityupdates/securitybulletins/2014/ms14-066.

[5] tenable, "Elasticsearch ESA-2015-06," 11 1 2019. [Online]. Available: https://www.tenable.com/plugins/nessus/119499.

[6] MS-ISAC, "EternalBlue," 01 2019. [Online]. Available: https://www.cisecurity.org/wpcontent/uploads/2019/01/Security-Primer-EternalBlue.pdf.

[7] tenable, "Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness," 30 3 2021. [Online]. Available: https://www.tenable.com/plugins/nessus/18405.

[8] tenable, "MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)," 15 11 2018. [Online]. Available: https://www.tenable.com/plugins/nessus/11808.

[9] Microsoft, "Microsoft Security Bulletin MS04-007 - Critical," 09 06 2004. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2004/ms04-007.

[10] Microsoft, "MS16-047: Security update for SAM and LSAD remote protocols: April 12, 2016," [Online]. Available: https://support.microsoft.com/en-gb/topic/ms16-047-security-update-forsam-and-lsad-remote-protocols-april-12-2016-1e5d4c49-0cf9-fd9f-e911-45b7f18ffce2.

[11] tenable, "SMB Signing not required," 2021 15 3. [Online]. Available: https://www.tenable.com/plugins/nessus/57608.

[12] tenable, "MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)," [Online]. Available: https://www.tenable.com/plugins/nessus/79638. [Accessed 15 10 2021].

[13] tenable, "SSL Medium Strength Cipher Suites Supported (SWEET32)," [Online]. Available: https://www.tenable.com/plugins/nessus/42873. [Accessed 2 3 2021].

[14] nessus, "SSL RC4 Cipher Suites Supported (Bar Mitzvah)," [Online]. Available: https://www.tenable.com/plugins/nnm/7282. [Accessed 8 16 2018].

[15] Tenab;e, "DNS Server Cache Snooping Remote Information Disclosure," 4 07 2020. [Online]. Available: https://www.tenable.com/plugins/nessus/12217.

[16] Tenable, "Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)," 16 11 2020. [Online]. Available: https://www.tenable.com/plugins/nessus/32321.

[17] tenable, "Bind Shell Backdoor Detection," 2019 10 5. [Online]. Available: https://www.tenable.com/plugins/nessus/51988.

[18] tenable, "Microsoft Windows SMB Shares Unprivileged Access," 02 09 2020. [Online]. Available: https://www.tenable.com/plugins/nessus/42411.