tenable Nessus

CustomScanWindows

Report generated by Nessus™ Thu, 18 Apr 2024 02:13:06 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.198.200

7	5	8	0	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Apr 18 02:04:43 2024
End time:	Thu Apr 18 02:10:44 2024

Host Information

Netbios Name:	PCXP
IP:	192.168.198.200
MAC Address:	08:00:27:21:87:1D
OS:	Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Windows XP for Embedded Systems

Vulnerabilities

34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System'

privileges.

ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

See Also

https://www.nessus.org/u?adf86aac

Solution

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

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

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	31874
CVE	CVE-2008-4250
MSKB	958644
XREF	MSFT:MS08-067
XREF	CERT:827267
XREF	IAVA:2008-A-0081-S
XREF	EDB-ID:6824
XREF	EDB-ID:7104
XREF	EDB-ID:7132
XREF	CWE:94

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2008/10/23, Modified: 2020/08/05

Plugin Output

tcp/445/cifs

35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Synopsis

It is possible to crash the remote host due to a flaw in SMB.

Description

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

See Also

http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Solution

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

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	31179
BID	33121
BID	33122
CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114
MSKB	958687
XREF	MSFT:MS09-001
XREF	CWE:399

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information

Published: 2009/01/13, Modified: 2024/03/26

Plugin Output

tcp/445/cifs

47556 - MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)

Synopsis

It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.

Description

The remote host is affected by several vulnerabilities in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

These vulnerabilities depend on access to a shared drive, but do not necessarily require credentials.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-012

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	38049
BID	38051
BID	38054
BID	38085
CVE	CVE-2010-0020
CVE	CVE-2010-0021
CVE	CVE-2010-0022

CVE	CVE-2010-0231
MSKB	971468
XREF	MSFT:MS10-012
XREF	CWE:20
XREF	CWE:94
XREF	CWE:264
XREF	CWE:310
XREF	CWE:362

Exploitable With

Core Impact (true)

Plugin Information

Published: 2010/09/13, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

48405 - MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)

Synopsis

It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.

Description

The remote host is affected by several vulnerabilities in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host. These vulnerabilities depend on access to a shared drive, but do not necessarily require credentials.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-054

Solution

Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	42224
BID	42263
BID	42267
CVE	CVE-2010-2550
CVE	CVE-2010-2551
CVE	CVE-2010-2552
MSKB	982214
XREF	EDB-ID:14607

XREF	MSFT:MS10-054

Exploitable With

Core Impact (true)

Plugin Information

Published: 2010/08/23, Modified: 2018/11/15

Plugin Output

tcp/445/cifs

53503 - MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)

Synopsis

It is possible to execute arbitrary code on the remote Windows host due to flaws in its SMB implementation.

Description

The remote host is affected by a vulnerability in the SMB server that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host. This vulnerability depends on access to a Windows file share, but does not necessarily require credentials.

See Also

https://www.nessus.org/u?c0a773fa

Solution

Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008 R2.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	47198
CVE	CVE-2011-0661
MSKB	2508429
XREF	IAVA:2011-A-0050-S

XREF	MSFT:MS11-020

Plugin Information

Published: 2011/04/20, Modified: 2020/08/05

Plugin Output

tcp/445/cifs

73182 - Microsoft Windows XP Unsupported Installation Detection

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

http://www.nessus.org/u?2f80aef2

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

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

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

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

XREF	EDB-ID:41929
XREF	IAVA:0001-A-0023

Plugin Information

Published: 2014/03/25, Modified: 2020/09/22

Plugin Output

tcp/0

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2023/07/27

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows XP Service Pack 2


Microsoft Windows XP Service Pack 3
```

```
Windows XP for Embedded Systems
```

97833 - 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

http://www.nessus.org/u?68fc8eff

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

http://www.nessus.org/u?065561d0

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

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

http://www.nessus.org/u?b9d9ebf9

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

http://www.nessus.org/u?234f8ef8

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

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.7

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212

MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CISA-KNOWN-EXPLOITED:2022/08/10
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/04/27
XREF	CISA-KNOWN-EXPLOITED:2022/06/14

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c80000000000000000000000000728d9e40150000110000000
00ffffffff0000000000000000000000005400000054000200230000001100005c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c80000000000000000000000000728d9e401500001000000
```

10547 - Microsoft Windows LAN Manager SNMP LanMan Services Disclosure

Synopsis

The list of LanMan services running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan services on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.3.1.1

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

3.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2024/03/22

Plugin Output

udp/161/snmp

```
Temi
Server
WebClient
Client DNS
Client DHCP
Workstation
Listener RIP
Audio Windows
Plug and Play
Servizi IPSEC
Servizio SNMP
Ora di Windows
Registro eventi
Servizi terminal
Spooler di stampa
Accesso secondario
Browser di computer
Centro sicurezza PC
Connessioni di rete
Servizio helper IPv6
Archiviazione protetta
Gestione dischi logici
Sistema di eventi COM+
Servizi di crittografia
Servizi semplici TCP/IP
Aggiornamenti automatici
Helper NetBIOS di TCP/IP
Notifica eventi di sistema
Registro di sistema remoto
Rilevamento hardware shell
Utilità di pianificazione
RPC (Remote Procedure Call)
Servizio di rilevamento SSDP
Servizio di segnalazione errori
Strumentazione gestione Windows
NLA (Network Location Awareness)
Guida in linea e supporto tecnico
VirtualBox Guest Additions Service
Zero Configuration reti senza fili
Gestione account di protezione (SAM)
Compatibilità di Cambio rapido utente
Utilità di avvio processo server DCOM
Servizio Gateway di livello applicazione
Acquisizione di immagini di Windows (WIA)
Manutenzione collegamenti distribuiti client
Servizio Ripristino configurazione di sistema
Windows Firewall / Condivisione connessione Internet (ICS)
```

26919 - Microsoft Windows SMB Guest Account Local User Access

Synopsis

It is possible to log into the remote host.

Description

The remote host is running one of the Microsoft Windows operating systems or the SAMBA daemon. It was possible to log into it as a guest user using a random account.

Solution

In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'. Disable the Guest account if applicable.

If the SAMBA daemon is running, double-check the SAMBA configuration around guest user access and disable guest access if appropriate

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0505

Exploitable With

Metasploit (true)

Plugin Information

Published: 2007/10/04, Modified: 2020/09/21

Plugin Output

tcp/445/cifs

26920 - SMB NULL Session Authentication

Synopsis

It is possible to log into the remote host with a NULL session.

Description

The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

http://www.nessus.org/u?e32d594f

http://www.nessus.org/u?9182e66b

http://www.nessus.org/u?a33fe205

Solution

Please contact the product vendor for recommended solutions.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.0 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

6.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

References

BID	494
CVE	CVE-1999-0519
CVE	CVE-1999-0520
CVE	CVE-2002-1117

Plugin Information

Published: 2007/10/04, Modified: 2022/10/07

Plugin Output

tcp/445/cifs

```
It was possible to bind to the following pipes:
  - browser
```

41028 - SNMP Agent Default Community Name (public)

Synopsis

The community name of the remote SNMP server can be guessed.

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

VPR Score

5.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	2112
CVE	CVE-1999-0517

Plugin Information

Published: 2002/11/25, Modified: 2022/06/01

Plugin Output

udp/161/snmp

```

The remote SNMP server replies to the following default community
```

```
string :

public
```

10043 - Chargen UDP Service Remote DoS

Synopsis

The remote host is running a 'chargen' service.

Description

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.

The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay.

An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

See Also

http://www.nessus.org/u?f0dbdf05

Solution

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103

Exploitable With

Metasploit (true)

Plugin Information

Published: 1999/11/29, Modified: 2020/06/12

Plugin Output

udp/19

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.

- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

tcp/7/echo

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it.

This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

Below are some examples of how to disable the echo service on some common platforms, however many services can exhibit this behavior and the list below is not exhaustive.

Consult vendor documentation for the service exhibiting the echo behavior for more information.

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process.

- Under Ubuntu systems, comment out the 'echo' line in /etc/systemd/system.conf and retart the systemd service.

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho

Then launch cmd.exe and type :

net stop simptcp net start simptcp

To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635

Plugin Information

Published: 1999/06/22, Modified: 2020/06/12

Plugin Output

udp/7

10548 - Microsoft Windows LAN Manager SNMP LanMan Shares Disclosure

Synopsis

The list of LanMan shares of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan shares on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.27.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

3.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Shared
ShareXP
SharedDocs
```

10546 - Microsoft Windows LAN Manager SNMP LanMan Users Disclosure

Synopsis

The list of LanMan users of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of LanMan users on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.25.1.1

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

3.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0499

Plugin Information

Published: 2000/11/10, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Guest
xpadmin
Administrator
HelpAssistant
```

```
SUPPORT_388945a0
```

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

tcp/17/qotd

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.

When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).

An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0103

Plugin Information

Published: 1999/11/30, Modified: 2019/10/04

Plugin Output

udp/17/qotd

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```
The remote operating system matched the following CPE's :

  cpe:/o:microsoft:windows -> Microsoft Windows
  cpe:/o:microsoft:windows_xp::sp2 -> Microsoft Windows XP
  cpe:/o:microsoft:windows_xp::sp3 -> Microsoft Windows XP
```

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.

- On Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

tcp/13/daytime

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.

In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.

- On Windows systems, set the following registry keys to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :

net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information

Published: 1999/06/22, Modified: 2014/05/09

Plugin Output

udp/13/daytime

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

11367 - Discard Service Detection

Synopsis

A discard service is running on the remote host.

Description

The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.

This service is unused these days, so it is advised that you disable it.

Solution

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process

- Under Windows systems, set the following registry key to 0 :

HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

None

Plugin Information

Published: 2003/03/12, Modified: 2011/03/11

Plugin Output

tcp/9/discard

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:21:87:1D : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:21:87:1D
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The difference between the local and remote clocks is -1 seconds.
```

13855 - Microsoft Windows Installed Hotfixes

Synopsis

It was not possible to enumerate installed hotfixes on the remote Windows host.

Description

Using the supplied credentials, Nessus was unable to log into the remote Windows host, enumerate installed hotfixes, or store them in its knowledge base for other plugins to use.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/07/30, Modified: 2023/07/10

Plugin Output

tcp/0

```

The required registry information for the location of SystemRoot was not
successfully written in Nessus scan data.

Solution : Ensure the account you are using can connect to the IPC$
administrative SMB share
```

10397 - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```

Here is the browse list of the remote host :

PCXP ( os : 5.1 )
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- Guest account
- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2023/07/25

Plugin Output

tcp/445/cifs

```
- Remote users are authenticated as 'Guest'.
- NULL sessions may be enabled on the remote host.
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

tcp/445/cifs

```
The remote host SID value is : S-1-5-21-583907252-1682526488-1343024091

The value of 'RestrictAnonymous' setting is : unknown
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 5.1
The remote native LAN manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : PCXP
```

10428 - Microsoft Windows SMB Registry Not Fully Accessible Detection

Synopsis

Nessus had insufficient access to the remote registry.

Description

Nessus did not access the remote registry completely, because full administrative rights are required.

If you want the permissions / values of all the sensitive registry keys to be checked, we recommend that you complete the 'SMB Login'

options in the 'Windows credentials' section of the policy with the administrator login name and password.

Solution

Use an administrator level account for scanning.

Risk Factor

None

Plugin Information

Published: 2000/05/29, Modified: 2018/10/02

Plugin Output

tcp/445/cifs

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```

An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```

The following shares can be accessed as ujuvqjeu :

- Shared  - (readable,writable)
  + Content of this share :
..

- ShareXP  - (readable,writable)
  + Content of this share :
..
Desktop.ini

- SharedDocs  - (readable,writable)
  + Content of this share :
..
desktop.ini
Immagini
Musica
Video

```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host when logged in as ujuvqjeu:

  - IPC$
  - SharedDocs
  - ShareXP
  - ADMIN$
  - C$
  - Shared
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```

The remote host supports the following versions of SMB :
  SMBv1
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/0

```

Nessus SNMP scanner was able to retrieve the open port list
with the community name: p*****
It found 8 open TCP ports and 15 open UDP ports.
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/7/echo

```
Port 7/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/7

```
Port 7/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/9/discard

```
Port 9/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/9

```
Port 9/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/13/daytime

```
Port 13/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/13/daytime

```
Port 13/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/17/qotd

```
Port 17/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/17/qotd

```
Port 17/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/19/chargen

```
Port 19/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/19

```
Port 19/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/123/ntp

```
Port 123/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/137/netbios-ns

```
Port 137/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Port 161/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/445

```
Port 445/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/500

```
Port 500/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/520

```
Port 520/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/1034

```
Port 1034/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/1900/upnp-client

```
Port 1900/udp was found to be open
```

14274 - Nessus SNMP Scanner

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2023/11/08

Plugin Output

udp/4500

```
Port 4500/udp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.1
Nessus build : 20016
Plugin feed version : 202404140447
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : CustomScanWinXP
Scan policy used : Basic Network Scan
Scanner IP : 192.168.198.100
Port scanner(s) : snmp_scanner
Port range : 1-65535
Ping RTT : 852.382 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : no
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/18 2:05 CEST
Scan duration : 323 sec
Scan for malware : no
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF	IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\PCXP\ADMIN$' with the supplied credentials.
```

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0934

Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.

No sensitive information has been disclosed.

Version : unknown
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SNMP:Hardware: x86 Family 25 Model 68 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version
 5.1 (Build 2600 Uniprocessor Free)
NTP:!:unknown
SinFP:
   P1:B11113:F0x12:W64240:O0204ffff:M1460:
   P2:B11113:F0x12:W64240:O0204ffff010303000101080a000000000000000001010402:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190801_7_p=9


The remote host is running one of these operating systems :
Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems
```

21745 - OS Security Patch Assessment Failed

Synopsis

Errors prevented OS Security Patch Assessment.

Description

OS Security Patch Assessment is not available for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Fix the problem(s) so that OS Security Patch Assessment is possible.

Risk Factor

None

References

XREF	IAVB:0001-B-0501

Plugin Information

Published: 2006/06/23, Modified: 2021/07/12

Plugin Output

tcp/0

```
OS Security Patch Assessment failed because :

  - Plugin      : smb_registry_full_access.nasl
    Plugin ID   : 10428
    Plugin Name : Microsoft Windows SMB Registry Not Fully Accessible Detection
    Protocol    : SMB
    Message     : The remote registry was not fully accessible.

  - Plugin      : smb_hotfixes.nasl
    Plugin ID   : 13855
    Plugin Name : Microsoft Windows Installed Hotfixes
    Protocol    : SMB
    Message     : unable to determine systemroot

  - Plugin      : ms_bulletin_checks_possible.nasl
    Plugin ID   : 57033
    Plugin Name : Microsoft Patch Bulletin Feasibility Check
    Protocol    : SMB
    Message     :
Nessus is not able to test for missing Microsoft patches for the
following reasons :

- The KB item "SMB/Registry/Enumerated" is missing.
```

```
  - The systemroot share was not identified.
  - Third party patch management checks, if configured, did not run.
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/04/09

Plugin Output

tcp/0

```
. You need to take the following action :

[ MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)
 (53503) ]

+ Action to take : Microsoft has released a set of patches for Windows XP, Vista, 2008, 7, and 2008
 R2.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2024/03/25

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 08:00:27:21:87:1d
```

35296 - SNMP Protocol Version Detection

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2019/11/22

Plugin Output

udp/161/snmp

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

19763 - SNMP Query Installed Software Disclosure

Synopsis

The list of software installed on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of installed software on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.6.3.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2005/09/20, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Oracle VM VirtualBox Guest Additions 7.0.14
WebFldrs XP
```

34022 - SNMP Query Routing Information Disclosure

Synopsis

The list of IP routes on the remote host can be obtained via SNMP.

Description

It is possible to obtain the routing information on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.4.21

An attacker may use this information to gain more knowledge about the network topology.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2008/08/21, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
127.0.0.0/255.0.0.0
192.168.198.0/255.255.255.0
192.168.198.200/255.255.255.255
192.168.198.255/255.255.255.255
224.0.0.0/240.0.0.0
255.255.255.255/255.255.255.255
```

10550 - SNMP Query Running Process List Disclosure

Synopsis

The list of processes running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of running processes on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.4.2.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
 PID   CPU   MEM COMMAND            ARGS
   1   733    16 System Idle Process
   4     2   220 System
 324     0   372 smss.exe
 680     0  2884 csrss.exe       ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On
SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserS
 704     0  4408 winlogon.exe
 748     0  3156 services.exe
 760     0  5932 lsass.exe
 916     0  3304 VBoxService.exe
 964     0  4444 svchost.exe     -k DcomLaunch
1052     0  4268 svchost.exe     -k rpcss
1148     0 17496 svchost.exe     -k netsvcs
1200     0  3312 svchost.exe     -k NetworkService
1232     0  4216 svchost.exe     -k LocalService
1300     0  1552 logon.scr       /s
1328     0  3380 alg.exe
1464     0  1836 wscntfy.exe
1584     0 14376 explorer.exe
1628     0  4552 spoolsv.exe
1760     0  3440 VBoxTray.exe
1956     0  3324 tcpsvcs.exe
1988     0  3644 snmp.exe
2040     0  3924 svchost.exe     -k imgsvc
```

10800 - SNMP Query System Information Disclosure

Synopsis

The System Information of the remote host can be obtained via SNMP.

Description

It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2001/11/06, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
System information :
 sysDescr     : Hardware: x86 Family 25 Model 68 Stepping 1 AT/AT COMPATIBLE - Software: Windows
 2000 Version 5.1 (Build 2600 Uniprocessor Free)
 sysObjectID  : 1.3.6.1.4.1.311.1.1.3.1.1
 sysUptime    : 0d 0h 1m 13s
 sysContact   :
 sysName      : PCXP
 sysLocation  :
 sysServices  : 76
```

10551 - SNMP Request Network Interfaces Enumeration

Synopsis

The list of network interfaces cards of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0

An attacker may use this information to gain more knowledge about the target host.

Solution

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

Risk Factor

None

Plugin Information

Published: 2000/11/13, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
Interface 1 information :
ifIndex       : 1
ifDescr       : MS TCP Loopback interface
```

185519 - SNMP Server Detection

Synopsis

An SNMP server is listening on the remote host.

Description

The remote service is an SNMP agent which provides management data about the device.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2023/11/14, Modified: 2023/11/14

Plugin Output

udp/161/snmp

```
Nessus detected the following SNMP versions:
  - SNMPv1 (public community)
  - SNMPv1 (configured community)
  - SNMPv2c (public community)
  - SNMPv2c (configured community)
```

40448 - SNMP Supported Protocols Detection

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/31, Modified: 2023/11/08

Plugin Output

udp/161/snmp

```
This host supports SNMP version SNMPv1.
This host supports SNMP version SNMPv2c.
```

35713 - Scan for UPnP hosts (multicast)

Synopsis

This machine is a UPnP client.

Description

This machine answered to a multicast UPnP NOTIFY packet by trying to fetch the XML description that Nessus advertised.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2023/10/17

Plugin Output

udp/1900/upnp-client

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

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

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

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

http://www.nessus.org/u?234f8ef8

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

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, 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

None

References

XREF	IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/7/echo

```
An echo server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/19/chargen

```
A chargen server is running on this port.
```

17975 - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/13/daytime

```
A DAYTIME server is running on this port
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.198.100 to 192.168.198.200 :
192.168.198.100
192.168.198.200

Hop Count: 1
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2024/03/26

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 6 NetBIOS names have been gathered :

 PCXP             = Computer name
 PCXP             = File Server Service
 MSHOME           = Workgroup / Domain name
 MSHOME           = Browser Service Elections
 MSHOME           = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :

   08:00:27:21:87:1d
```

192.168.198.201

1	1	2	0	43
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Apr 18 02:04:43 2024
End time:	Thu Apr 18 02:13:06 2024

Host Information

Netbios Name:	CHRIS-PC
IP:	192.168.198.201
MAC Address:	08:00:27:1C:89:0E
OS:	Microsoft Windows 7 Professional

Vulnerabilities

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2023/07/27

Plugin Output

tcp/0

```

The following Windows version is installed and not supported:

Microsoft Windows 7 Professional
```

97833 - 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

http://www.nessus.org/u?68fc8eff

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

http://www.nessus.org/u?065561d0

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

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

http://www.nessus.org/u?b9d9ebf9

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

http://www.nessus.org/u?234f8ef8

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

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.7

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212

MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CISA-KNOWN-EXPLOITED:2022/08/10
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/04/27
XREF	CISA-KNOWN-EXPLOITED:2022/06/14

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c8000000000000000000000000000087bdd0008000110000000
00ffffffff0000000000000000000000005400000054000200230000001100005c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c8000000000000000000000000000087bdd00080001000000
```

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information

Published: 2016/04/13, Modified: 2019/07/23

Plugin Output

tcp/49157/dce-rpc

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/04/03

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_7:::professional -> Microsoft Windows 7
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

```

The following DCERPC services are available locally :

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc048D50

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc048D50

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-116c01b969e7d8fa99

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc049731

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc049731

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4b112204-0e19-11d3-b42b-0000f81feb9f, version 1.0
Description : SSDP service
Windows process : unknow
Type : Local RPC service
Named pipe : LRPC-cc13678e7b05ee3cba

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LRPC-d52e01efd64b238d2c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-ab [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```

The following DCERPC services are available remotely :

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\CHRIS-PC

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
```

```
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CHRIS-PC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49152/dce-rpc

```

The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.198.201
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49153/dce-rpc

```

The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.198.201
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49154/dce-rpc

```

The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
```

```
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.198.201
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49155/dce-rpc

```

The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.198.201

```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49156/dce-rpc

```

The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.198.201

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.198.201
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49157/dce-rpc

```
The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.198.201
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```

The following card manufacturers were identified :

08:00:27:1C:89:0E : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:1C:89:0E
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
This host returns non-standard timestamps (high bit is set)
The difference between the local and remote clocks is 370 seconds.
```

24904 - Link Layer Topology Discovery (LLTD) Detection

Synopsis

The remote host speaks the LLTD protocol

Description

The remote host responds to the LLTD (Link Layer Topology Discovery) protocol.

This protocol can be used to enumerate the IPv4 and IPv6 addresses of a remote host, its name, the characteristics of the physical layer it is connected to, as well as the topology of the network, etc...

This plugin attempts to extract the IP addresses of the remote host as well as the physical layer it is connected to the network with.

See Also

http://www.microsoft.com/whdc/Rally/LLTD-spec.mspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/03/30, Modified: 2011/03/21

Plugin Output

tcp/0

```
  - Host ID : 0800271c890e
  - Physical medium : ethernetCsmacd
  - IPv4 address : 192.168.198.201
  - IPv6 address : fe80::f8ad:fe3c:e7f0:3f7c
  - Link speed : 1 Gb/s
  - Machine name : chris-PC
```

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?51eae65d

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'chris-PC'.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 7 Professional 7601 Service Pack 1
The remote native LAN manager is : Windows 7 Professional 6.1
The remote SMB Domain Name is : CHRIS-PC
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```

The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/5357/www

```
Port 5357/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/49152/dce-rpc

```
Port 49152/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/49153/dce-rpc

```
Port 49153/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/49154/dce-rpc

```
Port 49154/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/49155/dce-rpc

```
Port 49155/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/49156/dce-rpc

```
Port 49156/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/49157/dce-rpc

```
Port 49157/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/03/13

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.1
Nessus build : 20016
Plugin feed version : 202404140447
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : CustomScanWinXP
Scan policy used : Basic Network Scan
Scanner IP : 192.168.198.100
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 174.205 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : no
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/4/18 2:04 CEST
Scan duration : 497 sec
Scan for malware : no
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF	IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\CHRIS-PC\ADMIN$' with the supplied credentials.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 7 Professional
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:Server: Microsoft-HTTPAPI/2.0

SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1460:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190801_7_p=49155


The remote host is running Microsoft Windows 7 Professional
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2024/03/25

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 08:00:27:1c:89:0e
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

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

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

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

http://www.nessus.org/u?234f8ef8

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

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, 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

None

References

XREF	IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/5357/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.198.100 to 192.168.198.201 :
192.168.198.100
192.168.198.201

Hop Count: 1
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2024/03/26

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 6 NetBIOS names have been gathered :

 CHRIS-PC          = Computer name
 WORKGROUP         = Workgroup / Domain name
 CHRIS-PC          = File Server Service
 WORKGROUP         = Browser Service Elections
 WORKGROUP         = Master Browser
 __MSBROWSE__      = Master Browser

The remote host has the following MAC address on its adapter :

   08:00:27:1c:89:0e
```