CSS-Pluto

Report generated by Nessus™ Sat, 31 Jul 2021 09:55:09 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.35.50

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	0	0	0	13

Scan Information

Start time:	Sat Jul 31 06:35:42 2021
End time:	Sat Jul 31 06:39:07 2021

Host Information

IP:	192.168.35.50
OS:	Windows Server 2016 Standard Evaluation 14393

Vulnerabilities

140657 - Microsoft Netlogon Elevation of Privilege (Zerologon) (Remote)

Synopsis

The Netlogon service on the remote host is vulnerable to the zerologon vulnerability.

Description

The Netlogon service on the remote host is vulnerable to the zerologon vulnerability. An unauthenticated, remote attacker can exploit this, by spoofing a client credential to establish a secure channel to a domain controller using the Netlogon remote protocol (MS-NRPC). The attacker can then use this to change the computer's Active Directory (AD) password, and escalate privileges to domain admin.

In order for this plugin to run, you must disable 'Only use credentials provided by the user' in the scanner settings.

See Also

http://www.nessus.org/u?dfa970a7

http://www.nessus.org/u?f2e259c1

https://www.secura.com/blog/zero-logon

https://www.secura.com/pathtoimg.php?id=2055

https://github.com/SecuraBV/CVE-2020-1472

http://www.nessus.org/u?26edeb9b

https://www.kb.cert.org/vuls/id/490028

Solution

Refer to Microsoft's advisory for security guidance.

Risk Factor

High

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

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

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

CVE	CVE-2020-1472
XREF	IAVA:2020-A-0438-S
XREF	IAVA:0001-A-0647

Plugin Information

Published: 2020/09/18, Modified: 2021/07/19

Plugin Output

tcp/135/epmap

```

Nessus was able to bypass Netlogon authentication on dynamic port 49665 by spoofing a client
 credential after 4 attempts using the Zerologon exploit.

Authentication request:
0x00:  93 1C 00 00 0C 00 00 00 00 00 00 00 0C 00 00 00    ................
0x10:  5C 00 5C 00 43 00 53 00 53 00 2D 00 50 00 4C 00    \.\.C.S.S.-.P.L.
0x20:  55 00 54 00 4F 00 00 00 0B 00 00 00 00 00 00 00    U.T.O...........
0x30:  0B 00 00 00 43 00 53 00 53 00 2D 00 50 00 4C 00    ....C.S.S.-.P.L.
```

```
0x40:  55 00 54 00 4F 00 24 00 00 00 06 00 0A 00 00 00    U.T.O.$.........
0x50:  00 00 00 00 0A 00 00 00 43 00 53 00 53 00 2D 00    ........C.S.S.-.
0x60:  50 00 4C 00 55 00 54 00 4F 00 00 00 00 00 00 00    P.L.U.T.O.......
0x70:  00 00 00 00 FF FF 2F 21                            ....../!

Authentication response:
0x00:  0B 0D DF 10 80 D1 69 48 FF FF 2F 21 E8 03 00 00    ......iH../!....
0x10:  00 00 00 00                                        ....
```

tcp/135/epmap

```
Nessus was able to bypass Netlogon authentication on dynamic port 49667 by spoofing a client
 credential after 10 attempts using the Zerologon exploit.

Authentication request:
0x00:  41 B1 00 00 0C 00 00 00 00 00 00 00 0C 00 00 00    A...............
0x10:  5C 00 5C 00 43 00 53 00 53 00 2D 00 50 00 4C 00    \.\.C.S.S.-.P.L.
0x20:  55 00 54 00 4F 00 00 00 0B 00 00 00 00 00 00 00    U.T.O...........
0x30:  0B 00 00 00 43 00 53 00 53 00 2D 00 50 00 4C 00    ....C.S.S.-.P.L.
0x40:  55 00 54 00 4F 00 24 00 00 00 06 00 0A 00 00 00    U.T.O.$.........
0x50:  00 00 00 00 0A 00 00 00 43 00 53 00 53 00 2D 00    ........C.S.S.-.
0x60:  50 00 4C 00 55 00 54 00 4F 00 00 00 00 00 00 00    P.L.U.T.O.......
0x70:  00 00 00 00 FF FF 2F 21                            ....../!

Authentication response:
0x00:  8B CE 41 B2 36 F4 78 0C FF FF 2F 21 E8 03 00 00    ..A.6.x.../!....
0x10:  00 00 00 00                                        ....
```

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: 2021/07/12

Plugin Output

tcp/53

```
Port 53/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: 2021/07/12

Plugin Output

tcp/88

```
Port 88/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: 2021/07/12

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: 2021/07/12

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: 2021/07/12

Plugin Output

tcp/389/ldap

```
Port 389/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: 2021/07/12

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: 2021/07/12

Plugin Output

tcp/464

```
Port 464/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: 2021/07/12

Plugin Output

tcp/593/http-rpc-epmap

```
Port 593/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: 2021/07/12

Plugin Output

tcp/636

```
Port 636/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: 2021/07/12

Plugin Output

tcp/3268/ldap

```
Port 3268/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: 2021/07/12

Plugin Output

tcp/3269

```
Port 3269/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: 2021/06/28

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.15.0
Nessus build : 20271
Plugin feed version : 202107310212
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : CSS-Pluto
Scan policy used : Zerologon Remote Scan
Scanner IP : 192.168.35.129
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 259.363 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
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 : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/31 6:35 EDT
Scan duration : 193 sec
```

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: 2020/06/12

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 00:0c:29:13:8b:34
```

192.168.35.50

0	2	0	0	55
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Jul 31 09:46:22 2021
End time:	Sat Jul 31 09:55:08 2021

Host Information

Netbios Name:	CSS-PLUTO
IP:	192.168.35.50
MAC Address:	00:0C:29:13:8B:34
OS:	Windows Server 2016 Standard Evaluation 14393

Vulnerabilities

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)

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

l

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

Exploitable With

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

Plugin Information

Published: 2017/03/20, Modified: 2020/10/15

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001807c8000000000000000000000000000088ac7010800011000000
00ffffffff0000000000000000000000005400000054000200230000001100005c00500049005000
```

```
45005c0000000000

Received:
ff534d4225050200c09807c8000000000000000000000000000088ac701080001000000
```

100464 - Microsoft Windows SMBv1 Multiple Vulnerabilities

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

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

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

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

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

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

See Also

http://www.nessus.org/u?c21268d4

http://www.nessus.org/u?b9253982

http://www.nessus.org/u?23802c83

http://www.nessus.org/u?8313bb60

http://www.nessus.org/u?7677c678

http://www.nessus.org/u?36da236c

http://www.nessus.org/u?0981b934

http://www.nessus.org/u?c88efefa

http://www.nessus.org/u?695bf5cc

http://www.nessus.org/u?459a1e8c

http://www.nessus.org/u?ea45bbc5

http://www.nessus.org/u?4195776a

http://www.nessus.org/u?fbf092cf

http://www.nessus.org/u?8c0cc566

Solution

Apply the applicable security update for your Windows version :

- Windows Server 2008 : KB4018466
- Windows 7 : KB4019264
- Windows Server 2008 R2 : KB4019264
- Windows Server 2012 : KB4019216
- Windows 8.1 / RT 8.1. : KB4019215
- Windows Server 2012 R2 : KB4019215
- Windows 10 : KB4019474
- Windows 10 Version 1511 : KB4019473
- Windows 10 Version 1607 : KB4019472
- Windows 10 Version 1703 : KB4016871
- Windows Server 2016 : KB4019472

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

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

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

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

References

BID	98259
BID	98260
BID	98261
BID	98263
BID	98264
BID	98265

BID	98266
BID	98267
BID	98268
BID	98270
BID	98271
BID	98272
BID	98273
BID	98274
CVE	CVE-2017-0267
CVE	CVE-2017-0268
CVE	CVE-2017-0269
CVE	CVE-2017-0270
CVE	CVE-2017-0271
CVE	CVE-2017-0272
CVE	CVE-2017-0273
CVE	CVE-2017-0274
CVE	CVE-2017-0275
CVE	CVE-2017-0276
CVE	CVE-2017-0277
CVE	CVE-2017-0278
CVE	CVE-2017-0279
CVE	CVE-2017-0280
MSKB	4016871
MSKB	4018466
MSKB	4019213
MSKB	4019214
MSKB	4019215
MSKB	4019216
MSKB	4019263
MSKB	4019264
MSKB	4019472
MSKB	4019473
MSKB	4019474

Plugin Information

Published: 2017/05/26, Modified: 2019/11/13

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: 2021/07/22

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_server_2016
```

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: 2020/08/20

Plugin Output

tcp/135/epmap

```

The following DCERPC services are available locally :

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 : WMsgKRpc089F20

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 : WMsgKRpc089F20

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
```

```
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEB2261B4F613EB9131DA057FD4107

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6936cc2ed5dcc6f55c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fc48cd89-98d6-4628-9839-86f7a3e4161a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : dabrpc

Object UUID : 3bdb59a0-d736-4d44-9074-c1ee00000001
UUID : f3f09ffd-fbcf-4291-944d-70ad6e0e73bb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-7e8cf55c302ad23039

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d2716e94-25cb-4820-bc15-537866578562, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE10B1A6ADEF34A689A434298E0198

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d2716e94-25cb-4820-bc15-537866578562, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRP [...]
```

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: 2020/08/20

Plugin Output

tcp/445/cifs

```

The following DCERPC services are available remotely :

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 : \\CSS-PLUTO

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 : \\CSS-PLUTO

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\CSS-PLUTO

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 : \\CSS-PLUTO

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 : \\CSS-PLUTO

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
Named pipe : \PIPE\atsvc
Netbios name : \\CSS-PLUTO

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\CSS-PLUTO

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 : \\CSS-PLUTO

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449 [...]
```

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: 2020/08/20

Plugin Output

tcp/49664/dce-rpc

```
The following DCERPC services are available on TCP port 49664 :

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 : 49664
IP : 192.168.35.50
```

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: 2020/08/20

Plugin Output

tcp/49665/dce-rpc

```

The following DCERPC services are available on TCP port 49665 :

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 : 49665
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
```

```
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000 [...]
```

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: 2020/08/20

Plugin Output

tcp/49667/dce-rpc

```

The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 5fc860e0-6f6e-4fc2-83cd-46324f25e90b
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 9a81c2bd-a525-471d-a4ed-49907c0b23da
```

```
UUID : 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0.0
Description : Unknown RPC service
Annotation : RemoteAccessCheck
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000 [...]
```

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: 2020/08/20

Plugin Output

tcp/49669/dce-rpc

```
The following DCERPC services are available on TCP port 49669 :

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 : 49669
IP : 192.168.35.50

Object UUID : b5ccd5ef-4238-440b-bba0-999f828f1cfe
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49669
IP : 192.168.35.50
```

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: 2020/08/20

Plugin Output

tcp/49670/dce-rpc

```
The following DCERPC services are available on TCP port 49670 :

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 : 49670
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
```

```
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49670
IP : 192.168.35.50
```

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: 2020/08/20

Plugin Output

tcp/49671/dce-rpc

```

The following DCERPC services are available on TCP port 49671 :

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
Type : Remote RPC service
TCP Port : 49671
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49671
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49671
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
```

```
TCP Port : 49671
IP : 192.168.35.50

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49671
IP : 192.168.35.50
```

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: 2020/08/20

Plugin Output

tcp/49685/dce-rpc

```

The following DCERPC services are available on TCP port 49685 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0
Description : DNS Server
Windows process : dns.exe
Type : Remote RPC service
TCP Port : 49685
IP : 192.168.35.50
```

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: 2020/08/20

Plugin Output

tcp/54072/dce-rpc

```
The following DCERPC services are available on TCP port 54072 :

Object UUID : 5bc1ed07-f5f5-485f-9dfd-6fd0acf9a23c
UUID : 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1.0
Description : Unknown RPC service
Annotation : Frs2 Service
Type : Remote RPC service
TCP Port : 54072
IP : 192.168.35.50
```

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: 2020/08/20

Plugin Output

tcp/63333/dce-rpc

```
The following DCERPC services are available on TCP port 63333 :

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 : 63333
IP : 192.168.35.50
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

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: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53/dns

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

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

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: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

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: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 70
```

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 :

00:0C:29:13:8B:34 : VMware, Inc.
```

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:
  - 00:0C:29:13:8B:34
```

43829 - Kerberos Information Disclosure

Synopsis

The remote Kerberos server is leaking information.

Description

Nessus was able to retrieve the realm name and/or server time of the remote Kerberos server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/01/08, Modified: 2015/09/24

Plugin Output

tcp/88

```

Nessus gathered the following information :

  Server time  : 2021-07-31 13:48:43 UTC
  Realm        : MEGACORP.COM
```

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/07/12, Modified: 2012/02/20

Plugin Output

tcp/389/ldap

```
[+]-namingContexts:
   |  DC=MEGACORP,DC=COM
   |  CN=Configuration,DC=MEGACORP,DC=COM
   |  CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
   |  DC=DomainDnsZones,DC=MEGACORP,DC=COM
   |  DC=ForestDnsZones,DC=MEGACORP,DC=COM
[+]-currentTime:
   |  20210731135153.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=CSS-PLUTO,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=MEGACORP,DC=COM
[+]-namingContexts:
   |  DC=MEGACORP,DC=COM
   |  CN=Configuration,DC=MEGACORP,DC=COM
   |  CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
   |  DC=DomainDnsZones,DC=MEGACORP,DC=COM
   |  DC=ForestDnsZones,DC=MEGACORP,DC=COM
[+]-defaultNamingContext:
   |  DC=MEGACORP,DC=COM
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
[+]-configurationNamingContext:
   |  CN=Configuration,DC=MEGACORP,DC=COM
[+]-rootDomainNamingContext:
   |  DC=MEGACORP,DC=COM
[+]-supportedControl:
   |  1.2.840.113556.1.4.319
   |  1.2.840.113556.1.4.801
```

```
     |  1.2.840.113556.1.4.473
     |  1.2.840.113556.1.4.528
     |  1.2.840.113556.1.4.417
     |  1.2.840.113556.1.4.619
     |  1.2.840.113556.1.4.841
     |  1.2.840.113556.1.4.529
     |  1.2.840.113556.1.4.805
     |  1.2.840.113556.1.4.521
     |  1.2.840.113556.1.4.970
     |  1.2.840.113556.1.4.1338
     |  1.2.840.113556.1.4.474
     |  1.2.840.113556.1.4.1339
     |  1.2.840.113556.1.4.1340
     |  1.2.840.113556.1.4.1413
     |  2.16.840.1.113730.3.4.9
     |  2.16.840.1.113730.3.4.10
     |  1.2.840.113556.1.4.1504
     |  1.2.840.113556.1.4.1852
     |  1.2.840.113556.1.4.802
     |  1.2.840.113556.1.4.1907
     |  1.2.840.113556.1.4.1948
     |  1.2.840.113556.1.4.1974
     |  1.2.840.113556.1.4.1341
     |  1.2.840.113556.1.4.2026
     |  1.2.840.113556.1.4.2064
     |  1.2.840.113556.1.4.2065
     |  1.2.840.113556.1.4.2066
     |  1.2.840.113556.1.4.2090
     |  1.2.840.113556.1.4.2205
     |  1.2.840.113556.1.4.2204
     |  1.2.840.113556.1.4.2206
     |  1.2.840.113556.1.4.2211
     |  1.2.840.113556.1.4.2239
     |  1.2.840.11 [...]
```

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/07/12, Modified: 2012/02/20

Plugin Output

tcp/3268/ldap

```
[+]-namingContexts:
   |  DC=MEGACORP,DC=COM
   |  CN=Configuration,DC=MEGACORP,DC=COM
   |  CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
   |  DC=DomainDnsZones,DC=MEGACORP,DC=COM
   |  DC=ForestDnsZones,DC=MEGACORP,DC=COM
[+]-currentTime:
   |  20210731135153.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=CSS-PLUTO,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=MEGACORP,DC=COM
[+]-namingContexts:
   |  DC=MEGACORP,DC=COM
   |  CN=Configuration,DC=MEGACORP,DC=COM
   |  CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
   |  DC=DomainDnsZones,DC=MEGACORP,DC=COM
   |  DC=ForestDnsZones,DC=MEGACORP,DC=COM
[+]-defaultNamingContext:
   |  DC=MEGACORP,DC=COM
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=MEGACORP,DC=COM
[+]-configurationNamingContext:
   |  CN=Configuration,DC=MEGACORP,DC=COM
[+]-rootDomainNamingContext:
   |  DC=MEGACORP,DC=COM
[+]-supportedControl:
   |  1.2.840.113556.1.4.319
   |  1.2.840.113556.1.4.801
```

```
     |  1.2.840.113556.1.4.473
     |  1.2.840.113556.1.4.528
     |  1.2.840.113556.1.4.417
     |  1.2.840.113556.1.4.619
     |  1.2.840.113556.1.4.841
     |  1.2.840.113556.1.4.529
     |  1.2.840.113556.1.4.805
     |  1.2.840.113556.1.4.521
     |  1.2.840.113556.1.4.970
     |  1.2.840.113556.1.4.1338
     |  1.2.840.113556.1.4.474
     |  1.2.840.113556.1.4.1339
     |  1.2.840.113556.1.4.1340
     |  1.2.840.113556.1.4.1413
     |  2.16.840.1.113730.3.4.9
     |  2.16.840.1.113730.3.4.10
     |  1.2.840.113556.1.4.1504
     |  1.2.840.113556.1.4.1852
     |  1.2.840.113556.1.4.802
     |  1.2.840.113556.1.4.1907
     |  1.2.840.113556.1.4.1948
     |  1.2.840.113556.1.4.1974
     |  1.2.840.113556.1.4.1341
     |  1.2.840.113556.1.4.2026
     |  1.2.840.113556.1.4.2064
     |  1.2.840.113556.1.4.2065
     |  1.2.840.113556.1.4.2066
     |  1.2.840.113556.1.4.2090
     |  1.2.840.113556.1.4.2205
     |  1.2.840.113556.1.4.2204
     |  1.2.840.113556.1.4.2206
     |  1.2.840.113556.1.4.2211
     |  1.2.840.113556.1.4.2239
     |  1.2.840.11 [...]
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/02/10, Modified: 2019/11/22

Plugin Output

tcp/389/ldap

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/02/10, Modified: 2019/11/22

Plugin Output

tcp/3268/ldap

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: 2019/03/06

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'css-pluto'.
```

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 SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2020/01/22

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows Server 2016 Standard Evaluation 14393
The remote native LAN manager is : Windows Server 2016 Standard Evaluation 6.3
The remote SMB Domain Name is : MEGACORP
```

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
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

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
3.1        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: 2021/07/12

Plugin Output

tcp/53/dns

```
Port 53/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: 2021/07/12

Plugin Output

tcp/88

```
Port 88/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: 2021/07/12

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: 2021/07/12

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: 2021/07/12

Plugin Output

tcp/389/ldap

```
Port 389/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: 2021/07/12

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: 2021/07/12

Plugin Output

tcp/464

```
Port 464/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: 2021/07/12

Plugin Output

tcp/593/http-rpc-epmap

```
Port 593/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: 2021/07/12

Plugin Output

tcp/636

```
Port 636/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: 2021/07/12

Plugin Output

tcp/3268/ldap

```
Port 3268/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: 2021/07/12

Plugin Output

tcp/3269

```
Port 3269/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: 2021/06/28

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.15.0
Nessus build : 20271
Plugin feed version : 202107310212
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : CSS-Pluto
Scan policy used : Basic Network Scan
Scanner IP : 192.168.35.129
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 53.450 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/7/31 9:46 EDT
Scan duration : 522 sec
```

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 '\\CSS-PLUTO\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: 2021/05/12

Plugin Output

tcp/0

```

Remote operating system : Windows Server 2016 Standard Evaluation 14393
Confidence level : 70
Method : smb

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.

NTP:!:unknown
SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1460:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:181500_7_p=53


The remote host is running Windows Server 2016 Standard Evaluation 14393
```

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

```
The following service errors were logged :

  - Plugin      : smb_login.nasl
    Plugin ID   : 10394
    Plugin Name : Microsoft Windows SMB Log In Possible
    Protocol    : SMB
    Message     :
It was not possible to log into the remote host via smb (invalid credentials).
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF	IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2021/07/23

Plugin Output

tcp/0

```
Port 636 was detected as being open but is now closed
```

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: 2021/04/14

Plugin Output

tcp/593/http-rpc-epmap

```
An http-rpc-epmap 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: 2019/03/06

Plugin Output

tcp/0

104410 - Target Credential Status by Authentication Protocol - Failure for Provided Credentials

Synopsis

Nessus was unable to log into the detected authentication protocol, using the provided credentials, in order to perform credentialed checks.

Description

Nessus failed 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 failure in protocol negotiation or communication that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may have been invalid. A protocol failure may indicate a compatibility issue with the protocol configuration. A protocol failure due to an environmental issue such as resource or congestion issues may also prevent valid credentials from being identified. 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

Address the reported problem(s) so that credentialed checks can be executed.

Risk Factor

None

References

XREF	IAVB:0001-B-0503

Plugin Information

Published: 2017/11/06, Modified: 2020/10/19

Plugin Output

tcp/445/cifs

```
Nessus was unable to log into the following host for which
credentials have been provided :

  Protocol        : SMB
  Port            : 445
  Failure details :

  - User : MEGACORP\administrator

    - Plugin      : smb_login.nasl
      Plugin ID   : 10394
      Plugin Name : Microsoft Windows SMB Log In Possible
      Message     :
Failed to authenticate using the supplied credentials.
```

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: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.35.129 to 192.168.35.50 :
192.168.35.129
192.168.35.50

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```

The remote host is a VMware virtual machine.
```

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: 2021/07/19

Plugin Output

tcp/445/cifs

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

33139 - WS-Management Server Detection

Synopsis

The remote web server is used for remote management.

Description

The remote web server supports the Web Services for Management (WS-Management) specification, a general web services protocol based on SOAP for managing systems, applications, and other such entities.

See Also

https://www.dmtf.org/standards/ws-man

https://en.wikipedia.org/wiki/WS-Management

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2008/06/11, Modified: 2021/05/19

Plugin Output

tcp/5985

```

Here is some information about the WS-Management Server :

  Product Vendor  : Microsoft Corporation
  Product Version : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

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 5 NetBIOS names have been gathered :

 CSS-PLUTO         = Computer name
 MEGACORP          = Workgroup / Domain name
 MEGACORP          = Domain Controllers
 CSS-PLUTO         = File Server Service
 MEGACORP          = Domain Master Browser

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

   00:0c:29:13:8b:34
```