

Location A

Fri, 17 May 2024 19:20:56 Central European Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.1
- 192.168.0.8
- 192.168.0.14
- 192.168.0.108
- 192.168.0.112
- 192.168.0.175
- 192.168.0.239
- 192.168.100.1
- 192.168.100.100
- 192.168.100.101
- 192.168.100.102
- 192.168.100.103
- 192.168.100.104
- 192.168.100.105
- 192.168.100.106

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

192.168.0.1



Host Information

IP:	192.168.0.1
OS:	Linux Kernel 2.6

Vulnerabilities

73124 - NAT-PMP Detection (remote network)

Synopsis

Nessus was able to obtain information about the remote network.

Description

The remote device has the NAT-PMP protocol enabled. This protocol may allow any application on an internal subnet to request port mappings from the outside to the inside.

If this service is reachable from the outside your network, it may allow a remote attacker to gain more information about your network and possibly to break into it by creating dynamic port mappings.

Solution

Filter incoming traffic to UDP port 5351.

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 v2.0 Base Score

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

References

XREF CERT:184540

Plugin Information

Published: 2014/03/20, Modified: 2019/03/06

Plugin Output

udp/5351/nat-pmp

According to the remote NAT-PMP service, the public IP address of this host is :

176.121.85.74

It was possible to create (and destroy) a mapping from 176.121.85.74:55082 to 192.168.100.104:55082

12217 - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

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

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

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

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

See Also

http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

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)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/04/27, Modified: 2020/04/07

Plugin Output

udp/53/dns

Nessus sent a non-recursive query for example.edu
and received 1 answer :

93.184.215.14

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Plugin Output

tcp/443/www

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : C=CN/CN=tplinkwifi.net  
| -Issuer : C=CN/CN=tplinkwifi.net
```

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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is 59473 seconds.

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

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

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :  
- tplinkwifi.net
```

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: 2024/04/23

Plugin Output

tcp/0

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

```
cpe:/o:linux:linux_kernel -> Linux Kernel
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:isc:bind:9.16.37-debian -> ISC BIND  
cpe:/a:isc:bind:9.16.37:Debian -> ISC BIND  
cpe:/a:tp-link:tp-link -> tp-link
```

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

Version : 9.16.37-Debian

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

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

The remote host name is :

dnsb

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 : 65

19689 - Embedded Web Server Detection**Synopsis**

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/1900/www

84502 - HSTS Missing From HTTPS Server**Synopsis**

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/1900/www

The remote web server type is :

TP-LINK/TP-LINK UPnP/1.1 MiniUPnPd/1.8

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 200 OK

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
ETag: "2f9-110-65b967cb"
Last-Modified: Tue, 30 Jan 2024 21:19:07 GMT
Date: Fri, 17 May 2024 16:34:57 GMT
X-Frame-Options: deny
Content-Security-Policy: frame-ancestors 'none'
Cache-Control: no-cache
Expires: 0
Content-Type: text/html
Content-Length: 272
```

Response Body :

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="refresh" content="0; URL=/webpages/index.html" />
</head>
</html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/443/www

Response Code : HTTP/1.1 200 OK

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
ETag: "2f9-110-65b967cb"
Last-Modified: Tue, 30 Jan 2024 21:19:07 GMT
Date: Fri, 17 May 2024 16:34:57 GMT
X-Frame-Options: deny
Content-Security-Policy: frame-ancestors 'none'
Cache-Control: no-cache
Expires: 0
Content-Type: text/html
Content-Length: 272
```

Response Body :

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="refresh" content="0; URL=/webpages/index.html" />
</head>
</html>
```

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/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: 2024/03/19

Plugin Output

tcp/80/www

Port 80/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/443/www

Port 443/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/1900/www

Port 1900/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/20001/ssh

Port 20001/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 credentialled 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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS

```
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 13.285 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialated 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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:30 Central European Standard Time
Scan duration : 1160 sec
Scan for malware : no
```

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 : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
```

The remote host is running Linux Kernel 2.6

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 SSH service.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/20001/ssh

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

```
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
kexguess2@matt.ucc.asn.au
```

The server supports the following options for server_host_key_algorithms :

ssh-rsa

```
The server supports the following options for encryption_algorithms_client_to_server :  
aes256-ctr  
  
The server supports the following options for encryption_algorithms_server_to_client :  
aes256-ctr  
  
The server supports the following options for mac_algorithms_client_to_server :  
hmac-sha1  
hmac-sha2-256  
  
The server supports the following options for mac_algorithms_server_to_client :  
hmac-sha1  
hmac-sha2-256  
  
The server supports the following options for compression_algorithms_client_to_server :  
none  
  
The server supports the following options for compression_algorithms_server_to_client :  
none
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

<https://tools.ietf.org/html/rfc4252#section-8>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/20001/ssh

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/20001/ssh

The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1

10267 - SSH Server Type and Version Information**Synopsis**

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/20001/ssh

SSH version : SSH-2.0-dropbear_2019.78

SSH supported authentication : publickey,password,lockedMinute:120,failedAttempts:0,remainAttempts:10

56984 - SSL / TLS Versions Supported**Synopsis**

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/443/www

This port supports TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

Subject Name:

Country: CN
Common Name: tplinkwifi.net

Issuer Name:

Country: CN
Common Name: tplinkwifi.net

Serial Number: 00 8C 7B C8 F4 5B AD 96 13

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 01 00:00:00 2010 GMT
Not Valid After: Dec 31 00:00:00 2030 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 DB AC 21 6D B7 8C 44 CE 84 B6 10 C7 DF A7 B5 54 51 A5 02
F3 57 35 95 3F E7 7B 36 55 4C 6E 28 0D 03 63 47 9E B0 A6 A9
D9 22 BA 8E 31 69 77 EE 98 A2 18 36 75 38 42 B0 E7 4E D4 56
A7 4F 2C 23 53 63 86 A3 3A 2D 97 BB 47 EC 75 CE CD 20 DC 6E
5F 31 79 D4 DA FA 67 06 F7 1D 26 DE 96 D5 05 88 49 9A 31 62
4D 6C DD 4E 14 92 2B 37 EC F3 3E 50 3C 0B 0D 0F 13 DA 69 5B
57 74 2D 7F 2E 0C 62 6C A7 35 8B EC 2C 1C 14 EB 3E BC 29 7A
9F 8B F7 DA A9 4B 0E 0E 24 E7 25 FC EC 8B C5 BA D5 35 7B A9
A8 BB 59 8A AD C0 5F 58 08 7F C1 4F 16 17 10 D2 E2 9E B8 E1
27 BA 2E 87 F0 3C 51 03 B9 20 DD 0C 53 9E 45 05 FE 72 FF BA
B4 57 17 FE C5 9C 60 38 94 43 06 BC 40 97 B1 C1 60 A7 32 D5
28 36 51 F8 09 39 F5 26 0F AA 44 C8 28 B7 38 93 BC 7A 07 DC
FB E4 E8 17 04 79 9B 40 23 20 78 00 29 28 B1 91 47
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 73 F2 2F 9D E0 1E 7A 06 C4 95 6B 5C 5F 56 F6 B9 23 05 5E

```
A2 8D EB 80 F8 A8 A9 EA F3 B0 20 ED 47 52 01 BE 37 C8 E4 7D  
07 18 56 D0 C1 61 EE 6F D0 22 01 6E 96 5D EB 61 92 87 45 7D  
DE 7D DE FA 84 95 91 5E 02 F1 54 A4 68 69 7A 5E F4 DB A6 64  
BD BE B8 3B 6A 3A 29 21 8F 15 C1 E7 4D 52 29 30 B5 2E 3E 0D  
97 29 6C BE F6 BC 93 54 F7 91 60 C2 9F 41 56 E6 8C 77 D3 0B  
9C EC 8D 9D 7A DD 92 5E 30 A8 DF A1 E1 F3 D4 CA 54 96 11 D8  
E6 2E 13 36 19 E2 BB E7 E0 00 79 A3 76 8E 55 24 FA 72 45 58  
1F 99 05 3B CC B1 C6 D9 33 9C A0 23 1E D9 7C BC D1 C0 8F E8  
7E A5 83 6B 6E CF 03 C8 20 DA F9 00 20 0F 51 FA 2B 85 B3 AF  
95 16 91 E3 7D C2 89 C3 58 B1 FE F0 20 0A 03 6B 3C 36 92 23  
5E 1F 0B 79 5B 63 FE A9 57 B6 4F 45 FE BF 0C 52 94 26 AB C3  
A1 05 75 6E 01 1D 63 41 CA C3 7A 16 64 84 07 B5 40
```

Extension: Basic Constraints (2.5.29.19)

Critical: 0

Extension: Comment (2.16.840.1.113730.1.13)

Critical: 0

Comment: OpenSSL Generated Certificate

Extension: Subject Key Identifier (2.5.29.14)

Critical: 0

Subject Key Identifier: 6A 13 94 44 E1 33 4E CB BE 95 32 E1 06 72 3D BA 23 83 06 7A

Extension: Authority Key Identifier (2.5.29.35)

Critical: 0

Key Identifier: 40 9F 11 30 DB 84 DF 8E 21 2C 1C 8A BD 52 B4 70 D8 6F A1 77

Fingerprints :

SHA-256 Fingerprint: A8 1C 94 0D BE 13 07 DB 74 A7 D8 32 AC D2 69 A4 34 25 3D 9C
A6 01 9F 42 31 5A 80 C1 EA D5 8D 2B

SHA-1 Fingerprint: E2 BE 1E 16 1D 4E 3D 2A 7C 1F 85 3B 1D 8B F5 41 00 91 0E 63

MD5 Fingerprint: A1 C5 7C 4B A5 83 DB 35 46 D4 8F EA 88 A6 CA 0C

PEM certificate :

-----BEGIN CERTIFICATE-----

```
MIIDSjCCAjKgAwIBAgIJAIx7yPRbrZYTMA0GCSqGSIb3DQEBCwUAMCYxCAzAJBgNVBAYTAKNOMRcwF0YDVQQDDA50cGxpbtm3aWZpLm5ldDAeFw0xMDAxMDew  
MDAwMDBaFw0zMDEyMzEwMDAwMDBaMCYxCzAJBgNVBAYTAKNOMRcwFQYDVQQDDA50cGxpbtm3aWZpLm5ldDCCASiwdQYJKoZIhvvcNAQEBBQADggEPADCCAQoC  
ggEBANusIW23jETOhLYQx9+ntVRRpQLzVzWP+d7NLVMBigNA2NHnCrCmqdkiu04xaXfumKIYNNu40rDnTrRp08sI1NjhqM6LZe7R+x1zs0g3G5fMXnU2vpn  
BvcdJt6W1QWISZoxYk1s3u4Ukis37PM+UDwLDQ8T2mlbV3Qtfy4MYmynNYvsLBwU6z68KXqfi/faqus0DiTnJfzsi8W61TV7qai7WYqtwF9YCH/BTxYXENLi  
nrjh7ouh/A8UQ05IN0MU5FBf5y/7q0Vxf+xZxg0JRDBrxAl7HBYKcy1Sg2UfgJ0fUmD6pEyCi30J08egfc++ToFwR5m0AjIHgAKSiXkUccAwEEAAaN7MHKw  
CQYDVROTBAlwADAsBglghkgBvhvCAQ0EHxYdT3Blb1NTTCBHZw5lcmF0ZwQgQ2VydGlnawNhGUVhHOYDVRO0BBYEFGoTLEThM07LvpUy4QZyPbojgwZ6MB8G  
A1UdIwQYMBaaFECfETDbHN+0ISwcir1stHDYb6F3MA0GCSqGSIb3DQEBCwUAA4IBAQbz8i+d4B56bsSva1xfVva5IwVeoo3rgPioqerzsCDtR1IBvjfI5H0H  
GFbQwWHub9AiAw6WXethkodFfd593vqElZFeAvFUgHpeI7026Zkvb6402o6KSGPFchNtViIpMLUuPg2XKWy+9ryTVPeRYMKfQVbjmjhFTC5zsjZ163ZjeMkjf  
oeHz1MpUlhHY5i4Tnhniu+fgAhmjdo5VJPpyRvgfmQu7zLHG2T0coCMcE2Xy80cCP6H6lg2tuzwPIINr5ACAPUforhb0vlRaR433CicNYsf7wIAoDazw2kiNe  
Hwt5W2P+qVe2T0X+vwxSLcarw6EFdw4BHWNBysn6FmSEB7VA
```

-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Plugin Output

tcp/443/www

Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256  
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384  
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256  
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/443/www

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256  
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384  
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256  
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384  
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256  
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384  
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256  
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

62563 - SSL Compression Methods Supported

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

<http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml>
<https://tools.ietf.org/html/rfc3749>
<https://tools.ietf.org/html/rfc3943>
<https://tools.ietf.org/html/rfc5246>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/443/www

Nessus was able to confirm that the following compression method is supported by the target :

DEFLATE (0x01)

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/443/www

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/443/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

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/80/www

A web 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/443/www

A TLSv1.2 server answered on this port.

tcp/443/www

A web server is running on this port through TLSv1.2.

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/1900/www

A web 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/20001/ssh

An SSH 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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

TLSv1.2 is enabled and the server supports at least one cipher.

117860 - TP-Link HTTP Server Detection

Synopsis

It is possible to fingerprint the remote TP-Link HTTP server.

Description

The remote host has an accessible TP-Link HTTP administrative page.

It is possible to determine the model information from the host.

Note: In some instances, it may be possible to identify the device firmware version.

See Also

<https://www.tp-link.com/us/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/01, Modified: 2024/04/23

Plugin Output

tcp/80/www

```
URL : http://192.168.0.1/
Version : unknown
Hardware Version : Archer AX1500 v1.20
Model : Archer AX1500
```

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

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

SSH was detected on port 20001 but no credentials were provided.
SSH 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 192.168.100.104 to 192.168.0.1 :
192.168.100.104
192.168.0.1

Hop Count: 1

35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play
https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol
<http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt>

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information

Plugin Output

udp/1900/ssdp

The device responded to an SSDP M-SEARCH request with the following locations :

<http://192.168.0.1:1900/bgfaf/rootDesc.xml>

And advertises these unique service names :

```
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::upnp:rootdevice
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:device:InternetGatewayDevice:1
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:device:WANConnectionDevice:1
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:device:WANDevice:1
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:service:WANIPConnection:1
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:service:WANPPPCoNnection:1
uuid:a5124735-7c8a-4bc9-8352-77cf8a5717a9::urn:schemas-upnp-org:service:Layer3Forwarding:1
```

35712 - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

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

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/06/12

Plugin Output

tcp/1900/www

Here is a summary of <http://192.168.0.1:1900/bgfaf/rootDesc.xml> :

```
deviceType: urn:schemas-upnp-org:device:InternetGatewayDevice:1
friendlyName: Archer AX1500
manufacturer: TP-Link
manufacturerURL: http://www.tp-link.com/
modelName: Archer AX1500
modelDescription: Archer AX1500
modelName: Archer AX1500
modelNumber: 1.20
modelURL: http://www.tp-link.com/
serialNumber: 00000000
ServiceID: urn:upnp-org:serviceId:Layer3Forwarding1
serviceType: urn:schemas-upnp-org:service:Layer3Forwarding:1
controlURL: /bgfaf/ctl/L3F
eventSubURL: /bgfaf/evt/L3F
SCPDURL: /bgfaf/L3F.xml
ServiceID: urn:upnp-org:serviceId:WANCommonIFC1
serviceType: urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
controlURL: /bgfaf/ctl/CmnIfCfg
eventSubURL: /bgfaf/evt/CmnIfCfg
SCPDURL: /bgfaf/WANCfg.xml
ServiceID: urn:upnp-org:serviceId:WANIPConn1
serviceType: urn:schemas-upnp-org:service:WANIPConnection:1
controlURL: /bgfaf/ctl/IPConn
eventSubURL: /bgfaf/evt/IPConn
SCPDURL: /bgfaf/WANIPConn.xml
```

192.168.0.8



Host Information

IP: 192.168.0.8
OS: Microsoft Windows

Vulnerabilities

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows -> Microsoft Windows

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 : 70

10107 - HTTP Server Type and Version**Synopsis**

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

The remote web server type is :

Microsoft-HTTPAPI/2.0

24260 - HyperText Transfer Protocol (HTTP) Information**Synopsis**

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 17 May 2024 16:33:42 GMT
Connection: close
Content-Length: 315

Response Body :

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/80/www

Port 80/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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 29.800 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:30 Central European Standard Time
Scan duration : 561 sec
Scan for malware : no
```

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
Confidence level : 70
Method : HTTP
```

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:W64240:00204ffff:M1460:
P2:B11113:F0x12:W65535:00204ffff010303080402080afffffff44454144:M1460:
P3:B00000:F0x00:W0:00:M0
P4:190803_7_p=80R
```

The remote host is running Microsoft Windows

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/80/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

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 192.168.100.104 to 192.168.0.8 :
192.168.100.104
192.168.0.8

Hop Count: 1

192.168.0.14



Host Information

IP: 192.168.0.14

OS: Linux Kernel 2.4

Vulnerabilities

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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

The difference between the local and remote clocks is 7 seconds.

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

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 : 70

44318 - HNAP Detection**Synopsis**

The remote device has HNAP enabled.

Description

The remote service supports the Home Network Administration Protocol (HNAP), a SOAP-based protocol that provides a common interface for administrative control of networked devices.

See Also

<http://www.nessus.org/u?78450add>

<http://www.nessus.org/u?11760f94>

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2010/01/26, Modified: 2019/11/22

Plugin Output

tcp/80/www

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

The remote web server type is :

Boa/0.94.14rc21

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/80/www

Port 80/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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 14.510 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:30 Central European Standard Time
```

Scan duration : 470 sec
Scan for malware : no

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 : Linux Kernel 2.4
Confidence level : 70
Method : SinFP

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.

SinFP:
P1:B10113:F0x12:W5840:00204fffff:M1460:
P2:B10113:F0x12:W5792:00204fffff0402080afffffff4445414401030300:M1460:
P3:B00000:F0x00:W0:00:M0
P4:190803_7_p=80R
HNAP:! vendor=; model=DIR-605L
HTTP:! Server: Boa/0.94.14rc21

The remote host is running Linux Kernel 2.4

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/80/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

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 192.168.100.104 to 192.168.0.14 :
192.168.100.104
192.168.0.14

Hop Count: 1

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 302 rather than 404. The requested URL was :

<http://192.168.0.14/VBSqCIAfiQry.html>

192.168.0.108**Host Information**

IP: 192.168.0.108
OS: Linux Kernel 2.6

Vulnerabilities**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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE-1999-0524
XREF-CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

The difference between the local and remote clocks is 1 second.

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE matched on the remote system :

cpe:/a:jquery:jquery -> jQuery

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 : 65
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Headers :
```

```
CACHE-CONTROL: no-cache
Content-Length: 37831
Content-Type: text/html
```

```
Response Body :
```

```

<!DOCTYPE html> <html> <head> <title></title> <meta charset="UTF-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="format-detection" content="telephone=no"> <script src="jsBase/lib/jquery.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/jquery.ui.core.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/jquery.ui.widget.js?version=@WebVersion@"></script> <script src="jsBase/lib/jquery.base64.js?version=@WebVersion@"></script>
<script>jQuery.noConflict();</script> <link rel="stylesheet" type="text/css" href="jsBase/widget/css/jquery.powertip.min.css?version=@WebVersion@"> <script type="text/javascript" src="jsBase/widget/js/jquery.powertip.min.js?version=@WebVersion@"></script> <script src="jsBase/lib/jquery.pubsub.js?version=@WebVersion@"></script> <script src="jsBase/common/extend.js?version=@WebVersion@"></script> <script type="text/javascript"> // forced to add parameters to ensure the FF image loading do not fail
var cssList = ['css/reset.css', 'css/ui.css', 'css/custom.css', 'css/skin.css', 'css/pictures.css', 'css/main.css', 'css/alarm.css', 'css/set.css', 'css/resize.css', 'css/playback.css', 'jsBase/widget/css/ui.css', 'jsBase/widget/css/skin.css', 'css/fn.css', 'css/thermal.css', 'jsBase/widget/css/colorpicker.css'];
for (var i = 0; i < cssList.length; i++) {
var lt = "?WebVersion=@WebVersion@";
//To solve the problem of css loading in ie7 8
if (!(jQuery.browser.ie7 || jQuery.browser.ie8)) {
if (location.href.split('?')[1]) {
lt += "&" + location.href.split('?')[1];
}
}
var cssNode = document.createElement("link");
cssNode.rel = 'stylesheet';
cssNode.type = "text/css";
cssNode.media = 'screen';
cssNode.href = cssList[i] + lt;
var head = document.getElementsByTagName("head")[0] || document.documentElement;
head.appendChild(cssNode);
}
cssList = null;
lt = null;</script> </head> <body> <div id="login" class="login"> <div class="login-container"> <div class="login-content"> <div id="login_logo"></div> <div class="login-inputbox fn-clear"> <form autocomplete="off"> <div class="login-input-item"> <label t="sys.UserName+" class="login-input-title"> </label> <input type="text" id="login_user" class="fn-width163 fn-mart3"> </div> <div class="login-input-item"> <label class="login-input-title" t="sys.Password+:"> </label> <input id="login_psw" onpaste="return false" type="text" maxlength="64" class="fn-width163 fn-mart3"> <a btn-for="onFindPwd" class="login-input-item-FindPwd fn-ib fn-verticalbottom fn-lineh20 ellipsisNode fn-width110" t="sys.ForgetPassword" style="cursor: pointer; display:none" href="javascript:;"/> </a> </div> <div class="login-input-item fn-hide" id="GM_deviceName"> <label t="DeviceName+" class="login-input-title"> </label> <select class="ui-select fn-width169" id="login_pin_deviceName"> <option value="C95E11D0B39363FCAF717BB8C2F" t="GB35114.PleaseCheckUShieldFirst"> </option> </select> </div> <div class="login-input-item fn-hide" id="GM_PIN"> <label t="com.Ping+" class="login-input-title"> </label> <input type="password" id="login_pin" class="fn-width163 fn-mart3 u-input"> <span class="login-input-item-FindPwd fn-ib fn-verticalbottom fn-lineh20 ellipsisNode fn-width110" id="login_pin_tip" t="com.LoginPinTip"></span> <div class="login-input-item fn-hide" id="login_securityCheck"> <label class="ui-label fn-padl70"></label> <div class="fn-left fn-width165"> <ul class="ui-pwd-strength"> <li class="weak" t="com.Weak"></li> <li class="middle" t="com.Middle"></li> <li class="strong" t="com.Strong"></li> </ul> </div> <div class="login-input-item" id="login_type"> <label class="login-input-title" t="sys.UserType+:"> </label> <select class="fn-width169" id="login_selType"> <option value="Direct" t="sys.LocalUser"></option> <option value="ActiveDirectory" t="sys.ADUser"></option> <option value="LDAP" t="sys.LDAPUser"></option> </select> </div> <div class="ui-button-box login-btnbox"> <a btn-for="onLogin" t="com.Login" class="u-button fn-width80" href="javascript:;"/> </a> <a btn-for="onCancel" t="com.Cancel" class="u-button fn-width80" href="javascript:;"/> </a> </div> </div> <div class="u-dialog fn-width370" id="login_PasswordUpdateDlg"> <div class="u-dialog-head"> <h1 t=""></h1> <i class="i-close" data-action="close"></i> </div> <div class="u-dialog-content fn-clear"> <div class="ui-form-item"> <i class="i-dialog-warn"></i> <span class="u-dialog-context" t="sys.PasswordExpiredTip"></span> </div> <div class="ui-form-item fn-textcenter"> <input type="checkbox" chk-for="onCheckIgnoreTip" id="login_CheckIgnoreTip"> <span t="com.noTip"></span> </div> <div class="u-dialog-foot"> <a class="u-button" data-action="confirm" t="com.OK"></a> </div> </div> <div id="device_init" class="u-dialog fn-width700" style="text-align:left"> <div class="u-dialog-head"> <h1 t="sys.DevInit"></h1> </div> <div class="u-dialog-content fn-clear fn-pad30"> <div class="ui-form-item" > <label class="ui-label fn-width170" t="sys.UserName"> </label> <div class="fn-left fn-width450"> <span class="ui-text">admin</span> </div> </div> <div class="ui-form-item" > <label class="ui-label fn-width170" t="sys.Password"> </label> <div> <input type="password" class="fn-mart2 fn-width320" data-pwd="pwdInit" name="newpwd" maxlength="32" onpaste="return false" oncontextmenu="return false"> <span class="u-input-error fn-ib fn-color-red"></span> </div> </div> <div class="ui-form-item"> <label class="ui-label fn-width170"></label> <div class="fn-left fn-width165" > <ul class="ui-pwd-strength"> <li class="weak" t="com.Weak"></li> <li class="middle" t="com.Middle"></li> <li class="strong" t="com.Strong"></li> </ul> </div> <div class="ui-form-item" > <label class="ui-label fn-width170" t="sys.Pwdconfirm"> </label> <div> <input type="password" class="fn-mart2 fn-width320" data-pwd="pwdInit" name="newpwdcfm" maxlength="32" onpaste="return false" oncontextmenu="return false"> <span class="u-input-error fn-ib fn-color-red" id="device_init_cfmChk" t="com.PwdDiffTip" style="display: none"></span> </div> </div> <div class="ui-form-item"> <label class="ui-label fn-width170"></label> <div class="fn-left fn-width450"> <span class="ui-text" t="com.PwdTip1"></span> </div> </div> <div class="fn-split-line fn-hide" id="devInit_split"></div> <div class="ui-form-item fn-hide" id="devInit_phone_container"> <label class="ui-label fn-width170"> <input type="checkbox" id="devInit_phone_enable"> <span t="itc.BoundPhone"></span> </label> <div class="fn-left fn-width450"> <input type="text" id="devInit_bindPhone" maxlength="11" class="fn-mart2 fn-width320"> <span class="fn-ib" t="com.BindPhoneOrMailTip"></span> <span class="fn-ib fn-color-red" id="devInit_bindPhone_tip"></span> </div> <div class="ui-form-item fn-hide" id="devInit_mail_container"> <label class="ui-label fn-width170" t="sys.BindMail"></span> </label> <div class="fn-left fn-width450"> <input type="text" id="devInit_bindMail" maxlength="63" class="fn-mart2 fn-width320 u-input"> <span class="u-input-error fn-ib fn-color-red" id="devInit_bindMail_tip"></span> <span class="fn-ib" t="com.BindPhoneOrMailTip"></span> </div> <div class="ui-form-item" > <label class="ui-label fn-width170"></label> <div class="fn-left fn-width450"> <div class="u-tip fn-mart4"></div> </div> </div> <div class="u-dialog-foot"> <div class="ui-form-item" > <a class="u-button" data-action="confirm" href="javascript:;"/> <span t="com.Save"></span> </div> </div> <div id="login_find1" class="u-dialog fn-width800"> <div class="u-dialog-head"> <h1 t="sys.ResetPwd1"></h1> </div> <div class="u-dialog-content fn-clear"> <div id="QR_edition_wrap" class="fn-hide"> <div class="ui-form-item fn-hide"> <label id="FP_SNNo" class="ui-label fn-width24" t="net.SNNo"></label> <span class="ui-text" id="FP_SN"></span> </div> <div class="ui-form-item"> <label id="FP_NoteTip" class="ui-label fn-width86" t="com.QRNoteTip"></label> <div class="fn-left fn-width292" style="background-color: white; margin-left: 20px; margin: 10px; height: 292px" id="FP_QR"></div> <div id="FP_Right" class="fn-left fn-width281 fn-height252 fn-padl10 fn-mart8" style="padding: 20px 10px; border: 1px solid #000"> <div class="ui-form-item"> <label t="sys.ResetNote" class="ui-label fn-bold fn-width281"></label> </div> <div class="ui-form-item" > <p id="QR_ScanNote"></p> </div> </div> <div id="FP_QRTip1" class="ui-form-item" > <span class="ui-text fn-padl94" t="sys.WeChatScan"></span> </div> <div class="ui-form-item"> <span class="ui-text fn-padl94" t="sys.WeChatScan"></span> </div>

```

id="FP_QRTip"> </div> <div class="ui-form-item fn-textcenter fn-hide fn-marb10" id="FP_QRTip2"> <a data-action="showWechatQRCode" href="javascript:;" t="sys.PhoneNumChangedTip" style="text-decoration: underline; color: grey"> </div> <div class="ui-form-item"> <label class="ui-label fn-width86" t="com.InputSaveCodeTip"> </label> <div class="fn-left fn-width270"> <input type="text" id="security_code" class="fn-mart2 fn-marl5 fn-width610"> </div> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="login_find2" class="u-dialog fn-width800"> <div class="u-dialog-head"> <h1 t="sys.ResetPwd2"></h1> <div class="u-dialog-content fn-clear"> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="sys.UserName"> </label> admin </div> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="sys.Password"> </label> <div class="fn-left fn-width270"> <input type="password" class="ui-input" data-pwd="resetUser" style="width:260px" maxlength="32" onpaste="return false" oncontextmenu="return false"> </div> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="sys.Pwdconfirm"> </label> <div class="fn-left fn-width270"> <input type="password" class="ui-input" data-pwd="resetUserCfm" maxlength="32" style="width:260px" onpaste="return false" oncontextmenu="return false"> </div> <div class="ui-form-item"> <label class="ui-label fn-padl20"></label> <div class="fn-left fn-width270"> <div class="u-tip fn-mart4"></div> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="login_find3" class="u-dialog fn-width510"> <div class="u-dialog-head"> <h1 t="com.Prompt"></h1> </div> <div class="u-dialog-content fn-clear"> <div id="QR_edition_wrap3" class="ui-form-item fn-marb20"> <label id="QR_ResetPswWithWeChatTip"></label> </div> <div class="ui-form-item"> <div class="fn-left password-reset-qr fn-marl134"></div> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="login_permission1" class="u-dialog fn-width800"> <div class="u-dialog-head fn-padt0 fn-padb0"> <h1 t="sys.SoftwareLicence" id="login_permission1_h1" class="login-init-title-h1"></h1> <h1 t="sys.LicenceAndPolicy" id="login_permission1_h2" class="login-init-title-h1 fn-hide"></h1> </div> <div class="u-dialog-content fn-clear fn-height275 fn-padl30 fn-padb30 fn-padr30"> <ul class="u-tab fn-bg-dialog fn-hide" id="login_permission1_h2_title"> <li t="sys.SoftwareLicence" class="fn-border-li" id="login_permission1_title1"> <li t="sys.PrivacyPolicy" class="fn-border-li" id="login_permission1_title2"> <div class="ui-form-item"> <div id="login_permission_container" class="ui-textarea fn-width740 fn-height252 fn-ws-pre-wrap" style="background:#E2E2E2"></div> <div id="login_permission_container2" class="ui-textarea fn-width740 fn-height252 fn-ws-pre-wrap fn-hide" style="background:#E2E2E2"></div> </div> <div class="ui-form-item"> <label class="ui-checkbox"> <input type="checkbox" name="licence_check" autocomplete="off"> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="login_permission3" class="u-dialog fn-width800"> <div class="u-dialog-head"> <h1 t="sys.RemoteUpgrade"></h1> </div> <div class="u-dialog-content fn-clear fn-height275 fn-pad30"> <div class="u-dialog-head"> <h1 class="cloud-access-note" t="sys.CloudAccess"></h1> </div> <div class="u-dialog-content fn-clear fn-pad30"> <div class="ui-form-item"> <label class="ui-checkbox"> <input type="checkbox" name="access_check" checked="true"> </label> </div> <div class="ui-form-item fn-padl20"> </div> <div class="ui-form-item fn-padl20 cloudApp"> <div class="fn-left fn-width171" style="display:block;background-color: white; margin-left: 263px; margin-top: 20px; height:171px" id="Le_QR"></div> </div> <div class="ui-form-item fn-wid100p cloudApp"> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="login_permission4" class="u-dialog fn-width800"> <div class="u-dialog-head"> <h1 t="sys.AutocheckNote"></h1> </div> <div class="u-dialog-content fn-clear fn-height275 fn-pad30" id="login_online_AutocheckNote"> <label class="ui-checkbox"> <input type="checkbox" name="autocheck_check" checked="true"> </label> </div> <div class="ui-form-item fn-padl20"> <div class="u-tip fn-mart4 fn-marl20"></div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="login_permission4" class="u-dialog fn-width800"> <div class="u-dialog-head"> <h1 t="com.RegionSet"></h1> </div> <div class="u-dialog-content fn-clear fn-height275" style="padding:60px 0 0 60px"> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="com.Region"></label> <div class="ui-custom-select fn-ib fn-width200" id="nation_select_wrap" t="com.Language"> <select class="ui-select fn-width200" id="init_language" disabled="disabled"> <option value="English" selected="selected">English</option> <option value="Spanish">Spanish</option> <option value="French">French</option> </select> </div> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="med.VideoStandard"></label> <select class="ui-select fn-width200" id="video_standard" disabled="disabled"> <option value="PAL" t="med.PAL" selected="selected"></option> <option value="NTSC" t="med.NTSC"></option> </select> </div> <div class="u-tip fn-mart4 fn-marl20"></div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> </div> <div id="devinit_time_zone" class="u-dialog fn-width800"> <div class="u-dialog-head"> <h1 t="com.TimeZoneSet"></h1> </div> <div class="u-dialog-content fn-textleft fn-height275" style="padding:60px 0 0 60px"> <div class="ui-form-item"> <label class="ui-label fn-width160" t="sys.DateFormat"></label> <select class="ui-select" style="width:316px" id="time_zone_date_format"> <option value="yyyy-MM-dd" t="com.YearToDay">XXXX-XX-XX(月日)</option> <option value="MM-dd-yyyy" t="com.MonthDayYear">XX-XX-XXXX(日月)</option> <option value="dd-MM-yyyy" t="com.DayMonthYear">XX-XX-XXXX(日月)</option> </select> </div> <div class="ui-form-item"> <label class="ui-label fn-width160" t="com.TimeZones"></label> <select class="ui-select" style="width:316px" id="time_zone_select"></select> </div> <div class="ui-form-item"> <label class="ui-label fn-width160" t="sys.SysTime" id="syncPCBt"></label> <input type="text" class="fn-left" id="sys_time_ymd" style="width:92px"> <div id="sys_time_his" class="fn-left"></div> SyncPC </div> <div class="ui-form-item"> <label class="ui-label fn-width160 fn-color-red" t="com.WillBeChangeTo">□□□□□</label> <div id="sys_time_will_be" class="fn-color-red fn-lineh26" style="font-size:14px"></div> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> </div> <div id="login_modify" class="u-dialog fn-width436"> <div class="u-dialog-head"> <h1 t="com.FirstLoginChgPwdTip"></h1> <i class="i-close" data-action="close" id="i_close"></i> </div> <div class="u-dialog-content"> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="sys.NewPwd"></label> <div class="fn-left fn-width169"> <input type="password" class="fn-mart2" name="newpwd" maxlength="32" onpaste="return false" oncontextmenu="return false"> </div> </div> <div class="ui-form-item"> <label class="ui-label fn-padl20" t="sys.Pwdconfirm"></label> <div class="fn-left fn-width169" t="sys.Pwdconfirm"></div> <input type="password" class="fn-mart2" name="newpwd2" maxlength="32" onpaste="return false" oncontextmenu="return false"> <span id="login_pwd_cfm_tip" class="u-input-error"

fn-color-red"> </div> </div> <div class="ui-form-item" id="no_tip"> <label class="ui-label fn-padl20"></label> <label class="ui-checkbox"> <input type="checkbox"> </label> </div> <div class="u-dialog-foot"> </div> </div> <div id="main" class="main-container" style="display:none"> <div class="main-head"> <div id="main_logo"></div> </div> <ul class="u-tab main"> <li data-for="preview"> <li data-for="AIPreview" style="display:none" class="disabled"> <li data-for="SDEVPreview" class="disabled"> <li data-for="playback" class="disabled"> <li data-for="report" class="disabled"> <li data-for="search" class="disabled"> <li data-for="set" class="disabled"> <li data-for="alarm" class="fn-relative disabled"> <div class="main-nav-alarm" id="d_alarmtip" style="display:none"></div> <li data-for="logout" class="disabled"> <div class="u-tab-content fn-pad0"> <div class="tab-panel" data-page="preview"> <div class="main-top"> <div id="pre_stream" class="fn-left fn-mart3 fn-marl5"> <select class="fn-width100" id="pre_type"> <option value="0">TCP</option> <option value="4">UDP</option> <option t="net.Multicast" value="3">Multicast</option> </select> </div> <div id="pre_alarm_wrap"></div> <div class="duckbackground play_type_icon" id="duck_wrap" style="display:none"> </div> <select sel-for="onChangeResolute" style="float:right; height:18px; margin-top:4px; display:none"> <option value="1920x1080">1920x1080</option> <option value="1280x960">1280x960</option> <option value="1280x720">1280x720</option> <option value="704x576">704x576</option> <option value="704x480">704x480</option> <option value="640x480">640x480</option> <option value="352x240">352x240</option> <option value="320x240">320x240</option> </select> <div class="ui-rainBrush" style="display:none"> <div class="ui-rainBrush-wrap fn-hide"> </div> </div> <div class="ui-ClearFrostHeater" style="display:none"> <div class="ui-ClearFrostHeater-wrap fn-hide"> </div> </div> <div class="u-bottom"> <div class="fn-relative"> <div class="main-left-container"> <div class="main-face-analysis" style="display:none"></div> <div class="main-class-analysis" style="display:none"></div> </div> <div class="main-video-container"> <div id="preview_video" style="z-index:10001" class="main-video" dhvideowhmode="OriginalSize"></div> <div class="main-middle-container"> <div class="main-object-NonMotor" style="display:none"> </div> </div>

```

<div class="ui-video-bar" id="pre_video_bar"></div> <div class="main-bottom-container"> <div class="main-report-container" style="display:none"> </div> </div> <div class="main-right-container"> <div class="main-ptz-control fn-border-radius fn-marbl0" style="display:none"></div> <div class="main-ptz-distance fn-border-radius fn-marbl0" style="display:none"></div> <div class="main-ptz-setting fn-border-radius fn-marbl0" style="display:none"></div> <div class="main-image-adjust fn-border-radius fn-marbl0" style="display:none"></div> <div class="main-fusion-adjust fn-border-radius fn-marbl0" style="display:none"></div> <div class="main-depth-focus fn-border-radius fn-marbl0" style="display:none"></div> <div class="main-trigger-track fn-border-radius" style="display:none"></div> <div class="main-fisheye fn-border-radius" style="display:none"></div> <div class="main-face-feature" style="display:none"></div> <div class="main-trigger-VRtrack fn-border-radius" style="display:none"></div> <div class="main-traffic" style="display:none"></div> <div class="main-trafficVehicle" style="display:none"></div> <div class="main-kitchen-feature" style="display:none"></div> <div class="main-class-feature" style="display:none"></div> <div class="main-ptz-status fn-hide fn-wordwrap-breakword"> <i class="main-ptz-status-icon"></i> <span id="PTZ_status" class="fn-marl3"></span> </div> </div> <div id="ptzHeater_dialog" class="u-dialog fn-width470"> <div class="u-dialog-head"> <h1 t="adv.Heater"></h1> <a class="i-close" data-action="close"></a> </div> <div class="u-dialog-content fn-clear fn-pad30"> <div class="ui-form-item"> <label class="ui-label" for="ptzHeater_Time" t="com.maxRunningTime"></label> <input type="text" id="ptzHeater_Time" class="u-input"> <span id="ptzHeater_Time_tip" t="com.Minute+(0-1440)"></span> </div> </div> <div class="u-dialog-foot"> <div class="ui-form-item"> <a class="ui-button" data-action="confirm" href="javascript:;" t="com.Save"> </a> <a class="ui-button" data-action="close" href="javascript:;" t="com.Cancel"> </a> </div> </div> <div class="tab-panel" data-page="AIpreview"> <div class="sdev-open-close-wrap"> <i class="sdev-open-close-icon"></i> </div> <div class="sdev-menu-title" t="sys.AppList"> </div> <ul class="sdev-menu-list"> <li class="set-item set-item-current" appname="cameraNewConfig"> <i class="set-item-icon"></i> <span class="set-menu-label fn-ib fn-width130" t="med.VideoInputConfig" title="Conditions">Conditions</span> </li> <li class="set-item" appname="cameraNewConfig"> <i class="set-item-icon"></i> <span class="set-menu-label fn-ib fn-width130" t="med.VideoInputConfig" title="Conditions">Conditions</span> </li> </ul> </div> <div class="sdev-content-wrap"> <div class="sdev-body"> <iframe src="" appname="cameraNewConfig"></iframe> </div> </div> </div> <div class="tab-panel" data-page="ptz"> <div class="main-top"> <a class="main-top-icon-help" href="ptz.htm" title::com.Help"></a> </div> <div class="main-bottom"> <div class="fn-relative"> <div class="main-video-container"> <div class="main-video" dhvideowhmode="Original Size"></div> <div class="ui-video-bar"></div> </div> <div class="main-right-container"> <div class="main-ptz-control fn-border-radius fn-marbl0"></div> <div class="main-zoom-focus fn-border-radius" style="display:none"></div> <div class="main-trigger-track fn-border-radius" style="display:none"></div> </div> </div> <div class="tab-panel" data-page="playback"> </div> <div class="tab-panel" data-page="report"> </div> <div class="tab-panel" data-page="search"> <div class="set-container"> <div class="set-sidebar"> <ul id="srch-menu"></ul> </div> <div class="set-content"> <div id="srch-content" class="set-content-box fn-minwid912"></div> </div> <div id="search-advance"> </div> <script type="text/template" id="srch_menu"> <% $each(data, function(i, item) { %> <li class="set-item" filename="<%= item.filename %>" <% if(item.condition !== undefined) { %> style="display:none;" <% } %> <i class="set-item-icon"></i> <span class="set-menu-label fn-ib fn-width140" t="<%= value.t %>"></span> </a> <ul style="display:none"> <% $.each(value.member, function(i, item) { %> <li class="set-item" filename="<%= item.filename %>" index="<%= item.index %>" <% if(item.condition !== undefined) { %> style="display:none;" <% } %> <% if(item.vsp !== undefined) { %> vsp="vsp" <% } %> <i class="set-item-icon"></i> <span class="set-menu-label fn-ib fn-width130" t="<%= item.t %>"></span> </li> <% } ); %> </ul> </li> <% } ); %> </script> </div> <div class="tab-panel" data-page="alarm"> </div> <div class="tab-panel" data-page="logout"> </div> </div> <div id="timeout_logout" class="u-dialog fn-width436"> <div class="u-dialog-head"> <h1 t="com.Prompt"> </h1> </div> <div class="u-dialog-content fn-clear fn-textcenter"> <i class="i-dialog-warn"></i> <span t="com.ErrorAuthorizeReloginTip"></span> <div class="u-dialog-foot"> <a class="ui-button" data-action="confirm" href="javascript:;" t="com.Ok" > </a> </div> <div id="download" src="" style="display:none"></div> <script src="jsBase/lib/md5.js?version=@WebVersion@"></script> <script src="jsBase/lib/base64.js?version=@WebVersion@"></script> <script src="jsCore/common.js?version=@WebVersion@"></script> <script src="js/publicFunc.js?version=@WebVersion@"></script> <script src="jsBase/lib/sea.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.tab.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.table.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.pagination.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.textfield.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.numberfield.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.datepicker.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.timefield.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.tip.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.dialog.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.ipfield.js?version=@WebVersion@"></script> <script src="jsBase/widget/js/dui.validator.js?version=@WebVersion@"></script> <script src="js/timeZoneExcel.js?version=@WebVersion@"></script> <script type="text/javascript"> seajs.config({ base: './jsBase', paths: { 'js': '../js', 'html': '../html', 'platformHtm': '../platformHtm', 'jsCore': '../jsCore' } }); seajs.use('/jsCore/app', function(App) { window.webApp = new App(); });</script> </body> </html>

```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/80

```
URL : http://192.168.0.108/jsBase/lib/jquery.js?version=@WebVersion@
Version : unknown
```

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/80

```
Port 80/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/554

Port 554/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 : 10.7.3
Nessus build : 20038

```
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 73.698 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:35 Central European Standard Time
Scan duration : 501 sec
Scan for malware : no
```

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 : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
```

The remote host is running Linux Kernel 2.6

103869 - Open Network Video Interface Forum (ONVIF) Protocol Detection

Synopsis

The remote device supports ONVIF

Description

The remote device answered a NetworkVideoTransmitter WS-Discovery request. Therefore, it supports ONVIF.

See Also

<https://www.onvif.org/>

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information

Published: 2017/10/17, Modified: 2024/03/19

Plugin Output

udp/3702/onvif

The ONVIF service listening on UDP port 3702 advertises the following information:

Endpoint: http://192.168.0.108/onvif/device_service
Name: General
Hardware: BCS-L-TIP14FSR3-W

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

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 192.168.100.104 to 192.168.0.108 :
192.168.100.104
192.168.0.108

Hop Count: 1

192.168.0.112



Host Information

IP: 192.168.0.112

Vulnerabilities

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

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 14.349 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:36 Central European Standard Time
Scan duration : 758 sec
Scan for malware : no

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 192.168.100.104 to 192.168.0.112 :
192.168.100.104

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.

192.168.0.175



Host Information

IP: 192.168.0.175
OS: Linux Kernel 2.6

Vulnerabilities

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/8002/www

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority  
| -Issuer : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/8002/www

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

```
| -Subject : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

tcp/8002/www

TLSv1 is enabled and the server supports at least one cipher.

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1.

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

<https://datatracker.ietf.org/doc/html/rfc8996>
<http://www.nessus.org/u?c8ae820d>

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF

CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/8002/www

TLSv1.1 is enabled and the server supports at least one cipher.

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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE

CVE-1999-0524

XREF

CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

The difference between the local and remote clocks is 3 seconds.

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

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 : 65

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/7676/www

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8187/www

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/8002/www

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

<http://www.nessus.org/u?d9c03a9a>

<http://www.nessus.org/u?b019cbdb>

[https://www.owasp.org/index.php/Test_HTTP_Methods_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/8080/www

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD POST OPTIONS are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/7676/www

The remote web server type is :
UPnP/1.1 Samsung AllShare Server/1.0

10107 - HTTP Server Type and Version**Synopsis**

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8080/www

The remote web server type is :
WebServer

10107 - HTTP Server Type and Version**Synopsis**

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8187/www

```
The remote web server type is :  
UPnP/1.1 Samsung AllShare Server/1.0
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8000/www

```
Response Code : HTTP/1.1 200 OK  
  
Protocol version : HTTP/1.1  
HTTP/2 TLS Support: No  
HTTP/2 Cleartext Support: No  
SSL : no  
Keep-Alive : no  
Options allowed : (Not implemented)  
Headers :  
  
X-Powered-By: Express  
Access-Control-Allow-Origin: *  
Access-Control-Allow-Methods: GET,PUT,POST,DELETE,OPTIONS  
Access-Control-Allow-Headers: Content-Type, Authorization  
Date: Fri, 17 May 2024 16:49:36 GMT  
Connection: keep-alive  
Content-Length: 22
```

Response Body :

Server is running...

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8001/www

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET,PUT,POST,DELETE
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, SilentLaunch
Content-Type: application/json; charset=utf-8
Content-Length: 60
Date: Fri, 17 May 2024 16:49:36 GMT
Connection: keep-alive

Response Body :

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8002/www

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

X-Powered-By: Express
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET,PUT,POST,DELETE
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, SilentLaunch
Content-Type: application/json; charset=utf-8
Content-Length: 60
Date: Fri, 17 May 2024 16:49:45 GMT
Connection: keep-alive

Response Body :

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8080/www

Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, GET, HEAD, POST
Headers :

Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
Content-Type: text/html
Content-Length: 345
Connection: close
Date: Fri, 17 May 2024 16:49:36 GMT
Server: WebServer

Response Body :

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/9080/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Access-Control-Allow-Origin: *
Cache: no-cache
Content-Type: application/json
Connection: close
Content-Length: 9
Date: Fri May 17 18:49:48 2024

Response Body :

status=ok

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/7676/www

Port 7676/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/8000/www

Port 8000/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/8001/www

Port 8001/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/8002/www

Port 8002/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/8080/www

Port 8080/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/8187/www

Port 8187/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/9080/www

Port 9080/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/9999

Port 9999/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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 45.300 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:42 Central European Standard Time
Scan duration : 1228 sec
Scan for malware : no
```

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 : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
```

The remote host is running Linux Kernel 2.6

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

<https://www.openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

Plugin Output

tcp/8002/www

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/8002/www

This port supports TLSv1.0/TLSv1.1/TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8002/www

Subject Name:

Country: KR
Organization: SmartViewSDK
Common Name: SmartViewSDK

Issuer Name:

Country: KR
Organization: SmartViewSDK
Common Name: SmartViewSDK Root Ceritificate Authority

Serial Number: 00 F3 BF 81 80 FD E8 D8 E8

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 29 05:34:23 2016 GMT

Not Valid After: Jul 29 05:34:23 2036 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 B7 5D B4 BD 14 1B 46 3B 2F AB FD 95 DC E2 22 7F CB B6 58
44 9D 89 BF CA 48 CB C1 AA 4D A7 A0 5C 5E 57 E5 87 33 95 9D
81 BC 7E EF 3E 07 EA 08 7C DF CA 23 28 5D A1 C3 03 97 19 6E
9D 22 FB 02 D9 1F 13 87 F2 68 28 4E 7E 39 7C 05 D6 C8 32 13
F5 A3 92 70 FC 66 A4 82 31 87 30 E1 2A 37 41 90 F2 20 80 D6
49 07 49 A6 71 F5 66 58 8A D1 0C 6F B1 E3 99 E3 33 F6 0B 30
2B 9B 87 AE 55 C8 1D 59 D0 B1 83 EA F0 E9 FA 98 E9 54 0F B1
A7 AC F8 70 CE 9A F6 F8 F6 4C C3 43 5A 27 AF 40 26 5E 3D 44
DC C2 32 41 74 70 03 FC 46 DA 35 C3 FC 08 6E 44 34 6D F2 8B
EF AB BC 63 36 7C 89 1A 4F 02 BE E1 9D 04 7E 8A D6 F5 09
6E 3C 81 A9 B0 C6 50 A9 BB 80 19 1B 3E 10 A6 30 6C 5B 79 B4
3A A4 5A C3 20 38 C8 1D 47 F1 AA CC BD 29 84 FB 9D AD 3C 35
4C F0 45 0F CE 9F 8D 18 86 2B 98 27 50 53 50 58 FF

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 29 35 10 DC EA 5A 02 F3 40 E3 CA 94 AD 00 C3 FC B1 D5 03
2A 6C 7D 10 74 75 9F 7E 1A 1E 08 F4 66 C3 44 E6 20 2B E2 90
FE F9 05 F6 F7 16 7E CC AE 7B 7F 02 20 CA 36 94 2C EC 45
54 6E 82 B4 8C 2F 6F C7 05 04 48 E6 ED AB 68 8C 27 7A AC 4F
0B AF 2D DA F5 71 C2 38 DF D4 0E D6 CE 88 6A 09 2E 09 0E FA
D0 4B 37 38 00 50 0D DA A5 DD B7 30 DF E9 8D F3 08 93 48 47
B7 70 FE E9 C5 79 80 B3 5D 44 58 91 79 3D 03 37 44 B8 98 0B
1A 0E F4 C1 10 90 23 DF 6D D3 48 D5 22 68 BF 83 53 0D 45 00
EE 09 86 D3 1D E3 2F D4 C1 69 B3 0E 7F F6 94 B5 D4 2F 66 51
6A 02 60 23 06 C2 B0 77 30 AE F4 D3 45 9A 1F EE FF B4 B4 44
8E 84 AC 46 62 9D C7 DE F0 79 18 8F F6 C0 F0 DC 4E 8B 2A 0A
85 C1 A2 0D 93 C9 77 0C 4C 7C D7 7B 37 3A 30 9F 5A 08 00 DD
ED AF 4C DD AC 5B E5 A5 D8 54 12 C4 A1 0F 86 D4 03

Extension: Basic Constraints (2.5.29.19)

Critical: 0

Extension: Authority Key Identifier (2.5.29.35)

Critical: 0

Key Identifier: 50 CA 10 A9 EF 83 3E B7 61 B0 0A 21 F7 83 70 1A BB 40 17 EC

Extension: Subject Key Identifier (2.5.29.14)

Critical: 0

Subject Key Identifier: 7C 81 BB 3A 13 73 83 D5 48 07 51 1E 5C 6C E7 7A 0E 38 7A 97

Extension: Key Usage (2.5.29.15)

Critical: 0

Key Usage: Digital Signature, Non Repudiation, Key Encipherment

Extension: Extended Key Usage (2.5.29.37)

Critical: 0

Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)

Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)

Extension: Subject Alternative Name (2.5.29.17)

Critical: 0

DNS: 127.0.0.1

DNS: localhost

Fingerprints :

SHA-256 Fingerprint: C7 70 42 FE 73 8B 31 A4 C4 CF 9E F9 1C CF DC 9A 9F A6 91 72
D7 A6 71 31 F8 4A 0F C0 72 DD 71 12

SHA-1 Fingerprint: B1 5E 72 C0 04 B4 38 25 65 1E E7 A7 2B 66 18 56 30 5D E5 6B

MD5 Fingerprint: 18 9B 26 34 FC CA F1 EF 31 E1 7B 7B 02 AC C5 BD

PEM certificate :

-----BEGIN CERTIFICATE-----

MIIIDsTCCApmpgAwIBAgIJAP0/gYD96NjoMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNVBAYTAKtSMRUwEwYDVQQKEwxTbWFydFZpZXdTREsxMTAvBgNVBAMTKFNT

YXJ0Vmlld1NESyBSb290IElcmloaWZpY2F0ZSBBdXRob3JpdHkwHhcNMTYwNzI5MDUzNDIzWhcNMzYwNzI5MDUzNDIzWjA7M0swCQYDVQQGEwJLUjEVMBMG
A1UEChMMU21hcnaWV3U0RLMRUwEwYDVQQDEwxTbwFydFZpZXdTREswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3XbS9FBtG0y+r/ZXc41J/
y7ZYRJ2Jv8pIy8GqTaegXF5X5YczL2BvH7vPgfqCHzfyiMoXaHDA5cZbp0i+wLZh0H8mg0Tn45fAXWyDT9a0ScPxmpIIxhzDhKjdBkPIggNZJB0mmcfcVm
WIrRDG+x45nJM/YLMCubh65Vb1Z0LG6vDp+pjpVA+xp6z4cM6a9vj2TMNDWievQCZePUTcwyJBdhAD/EbaNcp8CG5ENG3y1+rq7xjNnyJGk8CvuGdBH6K
1vUJbjyBqbDGUKm7gBkbPhCmMGxbobQ6pFrIDjIHUfxqsyQYT7na08NUzwRQ/On40YhiuYJ1BTUFj/AgMBAAGjgZswgZgwCQYDVR0TBAIwADAfBgNVHSM
GDAwBgBRQyhCp74M+t2GwCiH3g3aa0AX7DAdBgNVHQ4EFgQUFig70hNzg9VIB1EeXGzne44epcwCwYDVR0PBAQDAGxGMB0GA1UdJQOWMBQGCCsGAQUFBwMB
BggRBgEFBQcDAjAfBgNVHREEGDAWggkxMjcuMC4wLjGCCXvY2FsaG9zdDANBgkqhkiG9w0BAQsFAAOCAQEAKTUQ30paAvNA48qUrQD/LHVApSfRB0dZ9+
Gh4I9GbDR0YgK+K0/vkF9vcWfsyue39/AiDKNpQs7EVUboK0jC9vxwUES0btq2iMJ3qsTwuvLdr1ccI439Q01s6IagkuCQ760Es30ABQDdq13bcw3+mN8wiT
SEe3cP7pxMAs11EWJF5PQM3RLiYCxo09MEQkCPfbdNI1Sjov4NTDUU7gmG0x3jL9TbabM0f/aUtdQvZLFqAmAjBsKwdzCu9NNFmh/u/7S0RI6ErEZincfe
8HkYj/bA8Nx0iyoKhcGiDZPJdwxFNd7Nzown1oIAN3tr0zdrFvlpdhUEsShD4bUAw==
-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/8002/www

Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/8002/www

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256  
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384  
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256  
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384  
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1  
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1  
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256  
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384  
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256  
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

SSL Version : TLSv11

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1  
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
```

SSL Version : TLSv1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1  
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8002/www

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	SHA256
ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	SHA384
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	SHA1
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	SHA1
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	SHA256
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	SHA384

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/8002/www

The following root Certification Authority certificate was found :

```
| -Subject : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
| -Issuer : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
| -Valid From : Jul 29 05:34:10 2016 GMT
| -Valid To : Jul 29 05:34:10 2036 GMT
| -Signature Algorithm : SHA-256 With RSA Encryption
```

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2022/04/11

Plugin Output

tcp/8002/www

A TLSv1/TLSv11/TLSv12 server is listening on this port that requests a client certificate.

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384

- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS
<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8002/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RSA-AES128-SHA256	0x00, 0x9C	RSA RSA	AES-GCM(128)	SHA256	
RSA-AES256-SHA384	0x00, 0x9D	RSA RSA	AES-GCM(256)	SHA384	
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH RSA	AES-CBC(128)	SHA1	
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH RSA	AES-CBC(256)	SHA1	
AES128-SHA	0x00, 0x2F	RSA RSA	AES-CBC(128)	SHA1	
AES256-SHA	0x00, 0x35	RSA RSA	AES-CBC(256)	SHA1	
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH RSA	AES-CBC(128)	SHA256	
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH RSA	AES-CBC(256)	SHA384	
RSA-AES128-SHA256	0x00, 0x3C	RSA RSA	AES-CBC(128)	SHA256	
RSA-AES256-SHA256	0x00, 0x3D	RSA RSA	AES-CBC(256)	SHA256	

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

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

Plugin Output

tcp/7676/www

A web 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/8000/www

A web 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/8001/www

A web 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/8002/www

A TLSv1 server answered on this port.

tcp/8002/www

A web server is running on this port through TLSv1.

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/8080/www

A web 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/8187/www

A web 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/9080/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

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2023/07/10

Plugin Output

tcp/8002/www

NPN Supported Protocols:

http/1.1
http/1.0

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>
<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/8002/www

The target advertises that the following protocols are supported over SSL / TLS:

http/1.0
http/1.1

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1.

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>
<http://www.nessus.org/u?c8ae820d>

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

References

XREF CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/8002/www

TLSv1.1 is enabled and the server supports at least one cipher.

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8002/www

TLSv1.2 is enabled and the server supports at least one cipher.

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 192.168.100.104 to 192.168.0.175 :
192.168.100.104
192.168.0.175

Hop Count: 1

10386 - Web Server No 404 Error Code Check**Synopsis**

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Plugin Output

tcp/9080/www

Unfortunately, Nessus has been unable to find a way to recognize this page so some CGI-related checks have been disabled.

192.168.0.239



Host Information

IP: 192.168.0.239
OS: Linux Kernel 3.10, Linux Kernel 3.13, Linux Kernel 4.2, Linux Kernel 4.8

Vulnerabilities

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/8002/www

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority  
| -Issuer : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/8002/www

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

```
| -Subject : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
```

12218 - mDNS Detection (Remote Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/04/28, Modified: 2021/06/28

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

- mDNS hostname : Samsung.local.
- Advertised services :
 - o Service name : ab92d698af9a1b5ac3cd5b7119e6f5547e7865b4._spotify-connect._tcp.local.
Port number : 54885
 - o Service name : Samsung Q77AA 55 TV._airplay._tcp.local.
Port number : 42771

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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

The difference between the local and remote clocks is -2 seconds.

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel -> Linux Kernel

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 : 59

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8187/www

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/8002/www

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8187/www

The remote web server type is :

UPnP/1.1 Samsung AllShare Server/1.0

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/9080/www

The remote web server type is :

NRDP/2020.1.7.1

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8001/www

Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

content-length: 29

Response Body :

<html><body>401</body></html>

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8002/www

Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes

```
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
content-length: 29

Response Body :

<html><body>401</body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/9080/www

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Headers :
```

```
Date: Fri, 17 May 2024 18:54:28 CEST
Server: NRDP/2020.1.7.1
Connection: keep-alive
Cache-Control: no-cache
Content-Length: 9
```

```
Response Body :
```

```
status=ok
```

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/8001/www

Port 8001/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/8002/www

Port 8002/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/8080

Port 8080/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/8187/www

Port 8187/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/9080/www

Port 9080/tcp was found to be open

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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 10.346 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialled 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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:46 Central European Standard Time
Scan duration : 1248 sec
Scan for malware : no
```

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 : Linux
Confidence level : 59
Method : SinFP
```

The remote host is running Linux

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/8002/www

This port supports TLSv1.3/TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8002/www

Subject Name:

Country: KR
Organization: SmartViewSDK
Common Name: SmartViewSDK

Issuer Name:

Country: KR
Organization: SmartViewSDK
Common Name: SmartViewSDK Root Ceritificate Authority

Serial Number: 00 C3 AB EA F9 EF A9 AC 39

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Sep 21 08:36:31 2016 GMT
Not Valid After: Sep 21 08:36:31 2036 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C9 01 57 A5 C8 7E 64 19 22 10 26 95 38 6E 78 1E B5 C1 87
0D C6 00 DC 20 D1 4F A5 07 70 F8 9F D8 0D 32 97 09 71 11 24
D0 DF 95 F2 22 D9 62 B7 97 F2 FC B8 0D 1A 63 71 0C 5F 4A E8
07 64 BC EA 65 15 90 FC 62 7A 43 64 1C 2F 0A FB E8 B5 A6 E4
7A 40 E8 82 AA F6 28 3F F6 9D E2 22 96 E3 D0 7A C9 05 17 57
34 93 05 4D 1C 09 8C 43 CE 0A 04 54 00 FC 0D 73 CC 2A E2 11
D5 14 B2 0C 29 51 FE 54 34 C0 11 9D DB E4 FA 92 52 15 D5 E9
9E 58 03 25 31 47 B6 03 C0 15 46 70 E3 CA 89 9D 01 7D 80 4F
47 1C 8A 05 E7 E8 61 4A 0A 7E 54 C4 92 E7 42 14 D6 A8 C0 1E
05 42 B1 48 E2 72 77 15 20 1D 8E 90 CC 1A 78 86 89 4A 30 71
02 41 1A 4B 0A BD 63 A9 13 9A 01 0E 9F 43 DF A2 38 1E 97 B3
CB 85 BE 21 75 8C 4C 67 FF BD 05 65 9F DB E1 6D 3A 59 42 3A
8E A4 65 16 C5 BE 2F 27 69 42 79 62 E6 36 DF 3D 2D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 59 2D 51 EB 1A 1F 76 E1 D0 3C 1E 4F B3 8A 49 C7 29 75 AF
73 7A 93 AB 62 2A 76 2E 90 1D F7 EF 0C 17 EB 53 66 15 4B DD
D7 14 1D 11 03 C3 C7 BD 4B 9B 84 99 82 86 F2 73 B8 32 A2 BA
A7 DF AA 99 3E B5 CC CB 95 3A 60 1F 26 E2 1D 88 6F DD EB 30
53 5A E7 72 A0 E3 8D 7D 9B 97 94 24 F2 AC C2 90 46 42 5E 99
68 08 4E 31 F5 1B 23 29 55 F9 20 D4 EF 1F FC 68 E0 02 D7
27 BD 84 21 04 8B C3 E7 6B 76 D0 2D 4E 5A CA 8B FB 3E 4B E0
9A 68 8A 48 66 FE 12 BE F7 5B 0B 52 8C 5D 4F 72 54 27 9E D2
D8 09 46 2E 59 29 2D 9C 23 9A 28 A8 D3 00 00 28 9D 1E 75 AA
7C 71 3B 46 74 5D 73 70 D1 3E 52 6B 89 44 7E D7 58 DC 48 55
50 C5 FC AA 2F 8D 6B 0E 41 2B B9 3A D4 9E 17 44 6C 2F 30 6B
7A 33 B8 1E 43 7D 36 44 F9 30 81 85 14 71 04 81 AD 62 72 BD
13 5C 0F 9E 95 8F 88 53 2F A9 16 BB 9B 9B D6 C3 8D

Extension: Basic Constraints (2.5.29.19)
Critical: 0

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 50 CA 10 A9 EF 83 3E B7 61 B0 0A 21 F7 83 70 1A BB 40 17 EC

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 44 78 94 95 36 04 1A 86 10 32 C3 09 D4 E2 3D A1 85 C1 D5 87

Extension: Key Usage (2.5.29.15)
Critical: 0
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0

Fingerprints :

SHA-256 Fingerprint: 04 26 AC 7F 01 AF E6 49 4C 5C 6C 00 80 70 CB 1D AA A3 C7 AB
F8 FC F0 73 8F D5 2C 33 33 62 EA 8A
SHA-1 Fingerprint: 2D 48 B8 37 DA BE A9 E6 75 88 EC D8 B8 09 35 29 56 56 D1 0C
MD5 Fingerprint: 63 A6 64 9E C4 84 50 BC 61 E5 DE 02 17 02 10 64

PEM certificate :

-----BEGIN CERTIFICATE-----
MIID0TCCAOmgAwIBAgIJAM0r6vnvqaw5MA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNVBAYTAKtSMRUwEwYDVQQKEwxTbWFydFZpZXdTREsxMTAvBgNVBAMTKFNT
YXJ0Vmld1NEsYBsb290IENlcmloaWZpY2F0ZSBbdXRob3JpdHkwHhcNMtYwOTIxMDgznjMxWhcNMzYwOTIxMDgznjMXWjA7MQswCQYDVQQGEwJLUjEVMBMG
A1UEChMMU21hcnRwaWV3U0RLMRUwEwYDVQQDEwxTbwFydFZpZXdTREswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJAVelyH5KGSIQJpU4bnge
tcGHdCYA3CDRT6UhCpif2A0ylwlxEStQ35XyItlIt5fy/LgNmNxDF9k6Adkv0plFZD8YnpDZBwvCvvotabkekDogqr2KD/2neIiluPQeskFF1c0kwVNHAmm
Q84KBFAQ/A1zzCriEdUUsgwpUf5UNMARndvk+pJSFdXpnlgDJTFHtgPAFUZw48qJnQF9gE9HHIoF5+-hhSgp+VMSS50IU1qjAHgVCsUjicncVIB20kMiaeIaJ
SjBxAkEaSwg9Y6kTmgE0nPfojgel7PLhb4hdYxMZ/+9BWwf2+Ft0llCo6kZRbfvi8naUJ5YuY23z0tAgMBAAGjgYsgwYgwCQYDVROTBAlwADAfBgNVHSME
GDAWgBRQyhCp74M+t2GwCiH3g3Aau0AX7AdBgnVH4EFgQURhiUlTYEGoYQMsMJ10I9oYXb1YcwCwYDVROPBaqDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMB
BggRgBFQcDAjAPBgnVHREECDAgHwR/AAABMA0GCSqGSIb3DQEBCwUA4IBAQBZ0lHrGh924dA8Hk+ziknHKXWvc3qTq2Iqdi6QHffvDBfrU2YV593XF8OR
A8PHVJubhJmChvJzuDKiuqffqpk+tczLltPgHybiHYhv3ewu1rncqDjjdebl5Qk8qzCKEZCXploCE4x9RsjsKSVZ9SDU7/x/8a0AC1ye9hCEEi8Pna3bQLU5a
yov7PkvgmmiKSGb+Er73WwtSjF1PclQnntLYCUyuWSktnCoAKkjTAAAonR51qnxx00Z0XXNw0T5Sa4LEftdY3EhVUMX8qi+Naw5BK7k61J4XRGwvMGT6M7ge
Q302RPkwgYUucQSBrWJyvRNcD56Vj4hTL6kWu5ub1sON
-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/8002/www

Here is the list of SSL CBC ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/8002/www

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
TLS_AES_128_GCM_SHA256	0x13, 0x01	- -	AES-GCM(128)	AEAD	
TLS_AES_256_GCM_SHA384	0x13, 0x02	- -	AES-GCM(256)	AEAD	
TLS_CHACHA20_POLY1305_SHA256	0x13, 0x03	- -	ChaCha20-Poly1305(256)	AEAD	

SSL Version : TLSv12
High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH RSA	AES-GCM(128)	SHA256	
ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH RSA	AES-GCM(256)	SHA384	
ECDHE-RSA-CHACHA20-POLY1305	0xCC, 0xA8	ECDH RSA	ChaCha20-Poly1305(256)	SHA256	
RSA-AES-128-CCM-AEAD	0xC0, 0x9C	RSA RSA	AES-CCM(128)	AEAD	
RSA-AES-128-CCM8-AEAD	0xC0, 0xA0	RSA RSA	AES-CCM8(128)	AEAD	
RSA-AES128-SHA256	0x00, 0x9C	RSA RSA	AES-GCM(128)	SHA256	
RSA-AES-256-CCM-AEAD	0xC0, 0x9D	RSA RSA	AES-CCM(256)	AEAD	
RSA-AES-256-CCM8-AEAD	0xC0, 0xA1	RSA RSA	AES-CCM8(256)	AEAD	
RSA-AES256-SHA384	0x00, 0x9D	RSA RSA	AES-GCM(256)	SHA384	
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH RSA	AES-CBC(128)	SHA1	

```
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8002/www

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
ECDHE-RSA-AES128-SHA256	0xC0	0x2F	ECDH RSA	AES-GCM(128)	SHA256
ECDHE-RSA-AES256-SHA384	0xC0	0x30	ECDH RSA	AES-GCM(256)	SHA384
ECDHE-RSA-CHACHA20-POLY1305	0xCC	0x8	ECDH RSA	ChaCha20-Poly1305(256)	SHA256
ECDHE-RSA-AES128-SHA	0xC0	0x13	ECDH RSA	AES-CBC(128)	SHA1
ECDHE-RSA-AES256-SHA	0xC0	0x14	ECDH RSA	AES-CBC(256)	SHA1
ECDHE-RSA-AES128-SHA256	0xC0	0x27	ECDH RSA	AES-CBC(128)	SHA256
ECDHE-RSA-AES256-SHA384	0xC0	0x28	ECDH RSA	AES-CBC(256)	SHA384

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/8002/www

The following root Certification Authority certificate was found :

```
| -Subject : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
| -Issuer : C=KR/0=SmartViewSDK/CN=SmartViewSDK Root Ceritificate Authority
| -Valid From : Jul 29 05:34:10 2016 GMT
| -Valid To : Jul 29 05:34:10 2036 GMT
| -Signature Algorithm : SHA-256 With RSA Encryption
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS
<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8002/www

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
RSA-AES-128-CCM-AEAD 0xC0, 0x9C RSA RSA AES-CCM(128) AEAD  
RSA-AES-128-CCM8-AEAD 0xC0, 0xA0 RSA RSA AES-CCM8(128) AEAD  
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256  
RSA-AES-256-CCM-AEAD 0xC0, 0x9D RSA RSA AES-CCM(256) AEAD  
RSA-AES-256-CCM8-AEAD 0xC0, 0xA1 RSA RSA AES-CCM8(256) AEAD  
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384  
ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1  
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1  
ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256  
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384  
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256  
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

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/8001/www

A web 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/8002/www

A TLSv1.2 server answered on this port.

tcp/8002/www

A web server is running on this port through TLSv1.2.

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/8187/www

A web 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/9080/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

84821 - TLS ALPN Supported Protocol Enumeration**Synopsis**

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/html/rfc7301>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2023/11/16

Plugin Output

tcp/8002/www

http/1.1

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8002/www

TLSv1.2 is enabled and the server supports at least one cipher.

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

<https://tools.ietf.org/html/rfc8446>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8002/www

TLSv1.3 is enabled and the server supports at least one cipher.

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 192.168.100.104 to 192.168.0.239 :
192.168.100.104
192.168.0.239

Hop Count: 1

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/9080/www

Unfortunately, Nessus has been unable to find a way to recognize this

page so some CGI-related checks have been disabled.

192.168.100.1



Host Information

IP: 192.168.100.1
MAC Address: E4:6F:13:67:97:CA
OS: Linux Kernel 2.4

Vulnerabilities

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.0

CVSS v2.0 Base Score

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

References

Plugin Information

Published: 2010/11/23, Modified: 2023/10/17

Plugin Output

tcp/0

IP forwarding appears to be enabled on the remote host.

Detected local MAC Address : d8c0a6ed35
Response from local MAC Address : d8c0a6ed35

Detected Gateway MAC Address : e46f136797ca
Response from Gateway MAC Address : e46f136797ca

10663 - DHCP Server Detection

Synopsis

The remote DHCP server may expose information about the associated network.

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2001/05/05, Modified: 2019/03/06

Plugin Output

udp/67

Nessus gathered the following information from the remote DHCP server :

Master DHCP server of this network : 0.0.0.0
IP address the DHCP server would attribute us : 192.168.100.104
DHCP server(s) identifier : 192.168.100.1
Netmask : 255.255.255.0
Router : 192.168.100.1
Domain name server(s) : 192.168.100.1

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

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

Plugin Output

icmp/0

The difference between the local and remote clocks is 8 seconds.

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :
cpe:/o:linux:linux_kernel -> Linux Kernel

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 : 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 :

E4:6F:13:67:97:CA : D-Link International

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:
- E4:6F:13:67:97:CA

44318 - HNAP Detection

Synopsis

The remote device has HNAP enabled.

Description

The remote service supports the Home Network Administration Protocol (HNAP), a SOAP-based protocol that provides a common interface for administrative control of networked devices.

See Also

<http://www.nessus.org/u?78450add>
<http://www.nessus.org/u?11760f94>

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2010/01/26, Modified: 2019/11/22

Plugin Output

tcp/80/www

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

The remote web server type is :

Boa/0.94.14rc21

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/80/www

Port 80/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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 15.397 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:48 Central European Standard Time
Scan duration : 467 sec
Scan for malware : no
```

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 : Linux Kernel 2.4
Confidence level : 70
Method : SinFP
```

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.

```
SinFP:
P1:B10113:F0x12:W5840:00204ffff:M1460:
P2:B10113:F0x12:W5792:00204ffff0402080afffffff4445414401030300:M1460:
P3:B00000:F0x00:W0:00:M0
P4:190803_7_p=80
HNAP:!vendor=; model=DIR-605L
HTTP:!Server: Boa/0.94.14rc21
```

The remote host is running Linux Kernel 2.4

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/80/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

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 192.168.100.104 to 192.168.100.1 :  
192.168.100.104  
192.168.100.1
```

Hop Count: 1

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 302 rather than 404. The requested URL was :

<http://192.168.100.1/Scdoc7h6Tsj6.html>

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

```
- mDNS hostname : dlinkrouter.local.  
- Advertised services :  
o Service name : D-Link DIR-605L Configuration Utility._http._tcp.local.  
Port number : 80  
o Service name : D-Link HNAP Service._dhnap._tcp.local.  
Port number : 80
```

192.168.100.100

0

2

5

0

40

CRITICAL

HIGH

MEDIUM

LOW

INFO

Host Information

IP: 192.168.100.100
MAC Address: FC:58:DF:2E:85:A3
OS: Nutanix

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/4011

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/5011

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/4011

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL  
| -Issuer : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/5011

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

| -Subject : CN=CP-STB-D64-00000000071412E/0=Cyfrowy Polsat S.A./C=PL
| -Issuer : CN=CP-STB-D64/0=Cyfrowy Polsat S.A./C=PL

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>
<http://www.nessus.org/u?ac7327a0>
<http://cr.yo.to/talks/2013.03.12/slides.pdf>
<http://www.isg.rhul.ac.uk/tls/>
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/4011

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>
<http://www.nessus.org/u?ac7327a0>
<http://cr.yo.to/talks/2013.03.12/slides.pdf>
<http://www.isg.rhul.ac.uk/tls/>
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/5011

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/4011

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

| -Subject : CN=CP-STB-CA-R00T-2/0=Cyfrowy Polsat S.A./C=PL

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 : 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 :

FC:58:DF:2E:85:A3 : Interphone Service

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:

- FC:58:DF:2E:85:A3

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8080/www

The remote web server type is :

BH

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/9090/www

The remote web server type is :

BH

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8080/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
Content-Length: 195
Content-Type: text/html; charset=ISO-8859-1
Date: Fri, 17 May 2024 16:56:38 GMT
SERVER: BH

Response Body :

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body><h1><b>Client error:</b>&ampnbsp403&ampnbspForbidden</h1><hr><address>BH</address></body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/9090/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No

```
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
Content-Length: 195
Content-Type: text/html; charset=ISO-8859-1
Date: Fri, 17 May 2024 16:56:38 GMT
SERVER: BH

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body><h1><b>Client error:</b>&nbsp;403&nbsp;Forbidden</h1><hr><address>BH</address></body></html>
```

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/4011

Port 4011/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/5011

Port 5011/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/8000

Port 8000/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/8080/www

Port 8080/tcp was found to be open

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/9090/www

Port 9090/tcp was found to be open

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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 193.958 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:52 Central European Standard Time
Scan duration : 1132 sec
Scan for malware : no
```

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 : Nutanix
Confidence level : 70
Method : SinfP
```

The remote host is running Nutanix

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 have 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

Steps to resolve this issue include :

- 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: 2023/06/20

Plugin Output

tcp/0

Port 5011 was detected as being open but is now closed
Port 4011 was detected as being open but is now closed

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/4011

This port supports TLSv1.2.

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/5011

This port supports TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/4011

Subject Name:

Common Name: CP-STB-D64-000000000071412E
Organization: Cyfrowy Polsat S.A.
Country: PL

Issuer Name:

Common Name: CP-STB-D64

Organization: Cyfrowy Polsat S.A.
Country: PL

Serial Number: 50 8A BE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 03 14:20:07 2022 GMT
Not Valid After: Jul 25 14:20:07 2048 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 CF 53 FB 78 A6 42 8D BC C7 8E 5D 4E A3 E9 3E 50 B8 AA 85
F0 0A A1 29 4B 0E DE 9D E8 13 DB D9 D9 71 DD 54 17 C5 9A FB
FA 4F 47 88 23 DD 70 6D 50 04 9F 3D D8 97 EE 00 07 E8 B7 12
7B 90 80 62 AA 90 4C AB D4 7A 1F 05 84 F8 3A 28 F9 44 24 4B
20 ED B5 00 BC EE 0D 61 36 68 6A 5C DC 3D 32 0B B0 66 8A D1
83 83 CA ED B4 CF BF CB 3E E1 A0 51 EF DC 79 B9 4A CD BC EB
CF 68 6A 69 C7 C0 37 52 C5 CF EF 1E 8C 8E 3D 01 29 D1 CD 68
BF 37 89 C3 1A 57 84 CA 19 A8 AD 29 CA 00 0B 34 C2 3D 17 80
2D F3 8E 05 DD 87 21 D4 74 63 A5 E3 4B 68 60 C5 C7 B0 3F 64
7A 8F 28 D3 C1 7E CB AE C8 09 EA BD 8D 82 46 2C A2 04 F9 D2
D5 25 E9 08 40 26 4D BC EC FE D7 F3 67 22 EB C8 4B 4C DB 57
7B B6 13 55 7E 4B 7F BB 3F 40 F8 44 C1 C0 4D 8E 59 44 78
F8 DA D2 58 31 E6 FF D9 A8 F9 0E 9C 24 E3 ED BE A9

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 9A CA 47 10 FE F4 57 64 16 BE 5E 35 6E A4 E5 FC B6 BF D1
78 63 B1 C6 A5 45 9A 1F 65 C7 BD 46 4E C1 38 21 9F FA 90 67
4D 7A B5 05 E8 0B 27 3C B1 BF 81 6B 33 A2 3B 9C 42 98 FD 5D
C4 92 D7 C2 E6 18 C0 BF 35 F5 F8 C8 46 B6 DE 04 62 9A B6 A1
C2 EF 27 1C 5C CC 70 AB 2A 85 C0 F0 41 8E 3F D5 A8 75 59 47
51 9D FC D5 4E 1F 57 B9 B1 31 86 85 5A B3 E6 08 E9 6D F3 5C
F1 AA DD 4C 63 AF 5A 0C 4A F8 B8 82 8C 66 FF 54 17 F0 BE 2F
C1 22 32 FE 19 83 D3 2B 2F FE A2 35 81 02 E8 FA 1C D7 37 5B
3D 6D C7 0F E4 56 11 D2 AC 6C CB C4 F6 BA 8B 34 FF 3F 04 E7
B9 D4 AF 80 10 48 2C 98 90 33 AF 3A 23 4F A0 49 41 89 16 61
EF 6F 0C 69 55 8C D9 E2 B9 A0 F6 48 A7 45 5A 8C 33 97 AD ED
FE C5 8C 29 26 89 1B 6C 17 E0 75 D5 F3 1C 93 9A E9 8D AB F8
5F 33 22 9D 8C 3B 58 16 9A D3 54 E2 2B 8D E9 C0 F4

Fingerprints :

SHA-256 Fingerprint: B8 D0 CC 10 C0 79 BC 92 3D 94 75 1E 19 30 5E AB 21 1B CE E6

77 F9 99 AA 94 F5 EB 6C 4A 47 6C F9

SHA-1 Fingerprint: 3F E2 05 75 F1 25 77 18 5E DA A5 60 C0 B5 65 1C FA 27 E2 9B

MD5 Fingerprint: 73 3A AE 41 C0 BE C9 71 90 51 6B 9E 13 97 41 EA

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIDUIq+MA0GCSqGSIb3DQEBCwUAMEAxEzARBgNVBAMCkNQLVNUQi1ENjQxHDAaBgNVBAoME0N5ZnJvd3kgUG9sc2F0IFMuQS4xCzAJ
BgNVBAYTALBMMB4XDTIyMDYwMzE0MjAwN1oXDT04MDcyNTE0MjAwN1owUTEkMCIGA1UEAwbb01AtU1RCLU02NC0wMDAwMDAwNzE0MTJFMRwwGyDV00K
DBNDewZyb3d5IFBvbHNhdCBTLkEuMqswCQYDVQQGEwJQTDCASiWdQYJKoZIhvCNQEBBQADggEPADCCAQoCggEBAM9T+3imQo28x45dTqPpPlC4qoXwCqEp
Sw7enegT29nZcd1UF8Wa+/pPR4gj3XBtUASfpdiX7gAH6LcSe5CAYqqQTkvUeh8FhpG6KPLEJEs97bUAv04NYTZoalzCPTILsGaK0YDyu20z7/LPuGgUe/c
eb1Kzbzrz2hzacfAN1Lfz+8ejI4gASnRzWi/N4nDgleEyhmorSnKAAsoWj0Xcg3zjgXdhvHudG014toYMXHsD9keo8o08F+y67ICeq9jYJGLKIE+dLVJekI
QCZNV0z+1/NnIuvIS0zbV3u2E1V+S3+3uz9A+ETBwE20WUR4+NtSwDHm/9mo+Q6cJOPtvqkCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAmspHEP70V2QWv141
bqTl/La/0XhjscalRZofZce9Rk7B0CGf+pBnTxq1BegLJzyxv4FrM6I7nEKY/V3EkfC5hjAvzX1+MhGtt4EYpq2ocLvJxxczHcrKoXA8EGOP9WodvlHUZ38
1U4fv7mxMYaFWrPmCOLt81zxqt1MY69aDER4uIKMzv9UF/C+l8EiMv4Zg9MrL/6iNYEC6Poc1zdbPw3HD+RWEkdKsbMvE9rqLNP8/B0e51K+AEEgsmJAzrzoj
T6BJQYkWYe9vDG1VjNniuaD2SKdFWowzl63t/swMKSaJG2wX4HXV8xyTnumNq/hfMyKdjDtYFprTV0IrjenA9A==
-----END CERTIFICATE-----

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/5011

Subject Name:

Common Name: CP-STB-D64-000000000071412E
Organization: Cyfrowy Polsat S.A.
Country: PL

Issuer Name:

Common Name: CP-STB-D64
Organization: Cyfrowy Polsat S.A.
Country: PL

Serial Number: 50 8A BE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 03 14:20:07 2022 GMT
Not Valid After: Jul 25 14:20:07 2048 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 CF 53 FB 78 A6 42 8D BC C7 8E 5D 4E A3 E9 3E 50 B8 AA 85
F0 0A A1 29 4B 0E DE 9D E8 13 DB D9 D9 71 DD 54 17 C5 9A FB
FA 4F 47 88 23 DD 70 6D 50 04 9F 3D D8 97 EE 00 07 E8 B7 12
7B 90 80 62 AA 90 4C AB D4 7A 1F 05 84 F8 3A 28 F9 44 24 4B
20 ED B5 00 BC EE 0D 61 36 68 6A 5C DC 3D 32 0B B0 66 8A D1
83 83 CA ED B4 CF BF CB 3E E1 A0 51 EF DC 79 B9 4A CD BC EB
CF 68 6A 69 C7 C0 37 52 C5 CF EF 1E 8C 8E 3D 01 29 D1 CD 68
BF 37 89 C3 1A 57 84 CA 19 A8 AD 29 CA 00 0B 34 C2 3D 17 80
2D F3 E8 05 DD 87 21 D4 74 63 A5 E3 4B 68 60 C5 C7 B0 3F 64
7A 8F 28 D3 C1 7E CB AE C8 09 EA BD 8D 82 46 2C A2 04 F9 D2
D5 25 E9 08 40 26 4D BC EC FE D7 F3 67 22 EB C8 4B 4C DB 57
7B B6 13 55 7E 4B 7F B7 BB 3F 40 F8 44 C1 C0 4D 8E 59 44 78
F8 DA D2 58 31 E6 FF D9 A8 F9 0E 9C 24 E3 ED BE A9
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 9A CA 47 10 FE F4 57 64 16 BE 5E 35 6E A4 E5 FC B6 BF D1
78 63 B1 C6 A5 45 9A 1F 65 C7 BD 46 4E C1 38 21 9F FA 90 67
4D 7A B5 05 E8 0B 27 3C B1 BF 81 6B 33 A2 3B 9C 42 98 FD 5D
C4 92 D7 C2 E6 18 C0 BF 35 F5 F8 C8 46 B6 DE 04 62 9A B6 A1
C2 EF 27 1C 5C CC 70 AB 2A 85 C0 F0 41 8E 3F D5 A8 75 59 47
51 9D FC D5 4E 1F 57 B9 B1 31 86 85 5A B3 E6 08 E9 6D F3 5C
F1 AA DD 4C 63 AF 5A 0C 4A F8 B8 82 8C 66 FF 54 17 F0 BE 2F
C1 22 32 FE 19 83 D3 2B 2F FE A2 35 81 02 E8 FA 1C D7 37 5B
3D 6D C7 0F E4 56 11 D2 AC 6C CB C4 F6 BA 8B 34 FF 3F 04 E7
B9 D4 AF 80 10 48 2C 98 90 33 AF 3A 23 4F A0 49 41 89 16 61
EF 6F 0C 69 55 8C D9 E2 B9 A0 F6 48 A7 45 5A 8C 33 97 AD ED
FE C5 8C 29 26 89 1B 6C 17 E0 75 D5 F3 1C 93 9A E9 8D AB F8
5F 33 22 9D 8C 3B 58 16 9A D3 54 E2 2B 8D E9 C0 F4

Fingerprints :

SHA-256 Fingerprint: B8 D0 CC 10 C0 79 BC 92 3D 94 75 1E 19 30 5E AB 21 1B CE E6
77 F9 99 AA 94 F5 EB 6C 4A 47 6C F9

SHA-1 Fingerprint: 3F E2 05 75 F1 25 77 18 5E DA A5 60 C0 B5 65 1C FA 27 E2 9B

MD5 Fingerprint: 73 3A AE 41 C0 BE C9 71 90 51 6B 9E 13 97 41 EA

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIDUiq+MA0GCSqGSIb3DQEBCwUAMEAxEzARBgNVBAMMCKNQLVNUQi1ENjQxHDAaBgNVBAoME0N5ZnJvd3kgUG9sc2F0IFMuQS4xCzAJ
BgNVBYTA1BMMB4XDTIyMDYwMzE0MjAwN1oXTDQ4MDcyNTE0MjAwN1owUTEkMCIGA1UEAwvbQ1AtU1RCLUQ2NC0wMDAwMDAwNzE0MTJFMRwwGgYDVQ0K
DBNDewZyb3d5IFBvBhNhdcBTLLkEuMqswCQYDVQQGEwJQTDCASiWdQYJKoZIhvCNAQEBBQADggEPADCCA0oCggEBAM9t+3imQo28x45dTqPpLc4qoxwCqEp
Sw7enegT29nZcd1UF8Wa+/pPR4gj3XBtUASFpDix7gAH6LcSe5CAYqqQTkvUeh8FhpG6KPlEJEs97bUAwO4NYTzoalzcPTILsGaK0Y0Dyu20z7/LPuGgUe/c
ebLKzbzr2hqcacfAN1LFz+8ejI49ASnRzWi/N4nDGleEyhmorSnKAAs0wj0XgC3zjgXdhvHdG0l40toYMXhsD9keo8o08F+y67ICeq9jYJGLKIE+dLVJekI
QCZNV0z+1/NiUvIS0zbV3u2E1V+S3+3uz9A+ETBwE20WUR4+NrsWDHm/9mo+06cJ0PtvkCAwEAATBnBqkhkiG9w0BAQsFAAOCAQEAmspHEP70V2QWvL41
bqTl/La/0XhjscaLRZofZce9Rk7B0Cgf+pBnTxq1BegLjzyxv4FrM6I7neKY/V3Ektfc5hjAvzX1+MhGtt4EYpq2ocLvjxxczHrKoXA8EGOP9WodvlHUZ38
1U4fV7mxMYaFWrPmC0lt81zxqt1MY69aDER4uIKMZv9UF/C+l8EiMv4zg9MrL/6iNYEC6Poc1zdbPw3HD+RWEdkSbMvE9rqLNP8/B0e51K+AEEgsmJAzrz0j
T6BJQYKwYe9vDGlvJnniaD2SKdFWowzl63t/swMKSAJG2wX4HXV8xyTmumNq/hfMyKdjDtYFprTV0IrjenA9A==
-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/4011

Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/5011

Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/4011

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Null Ciphers (no encryption)

Name Code KEX Auth Encryption MAC

NULL-MD5 0x00, 0x01 RSA RSA RSA None MD5
NULL-SHA 0x00, 0x02 RSA RSA RSA None SHA1
RSA-NULL-SHA256 0x00, 0x3B RSA RSA RSA None SHA256

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/5011

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12

Null Ciphers (no encryption)

Name Code KEX Auth Encryption MAC

NULL-MD5 0x00, 0x01 RSA RSA None MD5
NULL-SHA 0x00, 0x02 RSA RSA None SHA1
RSA-NUL-SHA256 0x00, 0x3B RSA RSA None SHA256

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Plugin Output

tcp/4011

The following root Certification Authority certificate was found :

```
| -Subject : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL  
| -Issuer : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL  
| -Valid From : Oct 27 07:44:18 2017 GMT  
| -Valid To : Oct 26 07:44:18 2047 GMT  
| -Signature Algorithm : SHA-256 With RSA Encryption
```

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2022/04/11

Plugin Output

tcp/4011

A TLSv12 server is listening on this port that requests a client certificate.

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2022/04/11

Plugin Output

tcp/5011

A TLSv12 server is listening on this port that requests a client certificate.

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS
<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/4011

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

Null Ciphers (no encryption)

Name	Code	KEX	Auth	Encryption	MAC
NULL-MD5	0x00,	0x01	RSA	RSA	None
NULL-SHA	0x00,	0x02	RSA	RSA	None
RSA-NUL	0x00,	0x3B	RSA	RSA	None
SHA256					SHA256

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00,	0x0A	RSA	RSA	3DES-CBC(168)
					SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RSA-AES128-SHA256	0x00,	0x9C	RSA	RSA	AES-GCM(128)
RSA-AES256-SHA384	0x00,	0x9D	RSA	RSA	AES-GCM(256)
					SHA384

```
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS
<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/5011

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

Null Ciphers (no encryption)

Name Code KEX Auth Encryption MAC

```
NULL-MD5 0x00, 0x01 RSA RSA None MD5
NULL-SHA 0x00, 0x02 RSA RSA None SHA1
RSA-NULL-SHA256 0x00, 0x3B RSA RSA None SHA256
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
-----  
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256  
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1  
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1  
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1  
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1  
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5  
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1  
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1  
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256  
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

91263 - SSL/TLS Service Requires Client Certificate

Synopsis

The remote service requires an SSL client certificate to establish an SSL/TLS connection.

Description

The remote service encrypts communications using SSL/TLS and requires a client certificate in order to establish an SSL/TLS connection.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/05/19, Modified: 2016/05/19

Plugin Output

tcp/5011

A TLSv12 server is listening on this port and requires client certificate verification.

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/4011

A TLSv1.2 server answered 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/5011

A TLSv1.2 server answered 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/8000

The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.

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/8080/www

A web 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/9090/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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/4011

TLSv1.2 is enabled and the server supports at least one cipher.

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/5011

TLSv1.2 is enabled and the server supports at least one cipher.

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 192.168.100.104 to 192.168.100.100 :
192.168.100.104
192.168.100.100

Hop Count: 1

35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

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

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

<http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt>

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2018/09/12

Plugin Output

udp/1900/ssdp

The device responded to an SSDP M-SEARCH request with the following locations :

http://192.168.100.100:8080/upnpdev/devc/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/00

And advertises these unique service names :

```
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::upnp:rootdevice
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::urn:schemas-upnp-org:device:MediaServer:2
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::urn:schemas-upnp-org:service:ConnectionManager:2
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::urn:schemas-upnp-org:service:ContentDirectory:2
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::urn:dial-multiscreen-org:service:dial:1
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::urn:adbglobal-com:service:X_ADB_RemoteControl:1
uuid:1864edb0-1dd2-11b2-8ff1-fc58df2e85a3::urn:adbglobal-com:service:X_ADB_CerberLite:1
```

35712 - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

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

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/06/12

Plugin Output

tcp/8080/www

Here is a summary of http://192.168.100.100:8080/upnpdev/devc/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/00 :

```
deviceType: urn:schemas-upnp-org:device:MediaServer:2
friendlyName: POLSATBOX4KLITE-
manufacturer: ADB
manufacturerURL: http://www.adbglobal.com/
modelName: POLSAT BOX 4K LITE
modelDescription: BH/DLNA Media Server
modelName: POLSAT BOX 4K LITE
modelNumber: 23.5.15 RELEASE
serialNumber: 1111-111111-1111
ServiceID: urn:upnp-org:serviceId:ConnectionManager
serviceType: urn:schemas-upnp-org:service:ConnectionManager:2
controlURL: /upnpfun/ctrl/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/00
eventSubURL: /upnpfun/evnt/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/00
SCPDURL: /upnpdev/serv/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/00
ServiceID: urn:upnp-org:serviceId:ContentDirectory
serviceType: urn:schemas-upnp-org:service:ContentDirectory:2
controlURL: /upnpfun/ctrl/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/01
eventSubURL: /upnpfun/evnt/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/01
SCPDURL: /upnpdev/serv/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/01
ServiceID: urn:adbglobal-com:serviceId:X_ADB_RemoteControl
```

```
serviceType: urn:adbglobal-com:service:X_ADB_RemoteControl:1
controlURL: /upnpfun/ctrl/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/03
eventSubURL: /upnpfun/evnt/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/03
SCPDURL: /upnpdev/serv/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/03
ServiceID: urn:adbglobal-com:serviceId:X_ADB_CerberLite
serviceType: urn:adbglobal-com:service:X_ADB_CerberLite:1
controlURL: /upnpfun/ctrl/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/04
eventSubURL: /upnpfun/evnt/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/04
SCPDURL: /upnpdev/serv/uuid_1864edb0-1dd2-11b2-8ff1-fc58df2e85a3/04
```

192.168.100.101

0

0

1

0

29

CRITICAL

HIGH

MEDIUM

LOW

INFO

Host Information

Netbios Name: LAPTOP-5LEH76CL
IP: 192.168.100.101
MAC Address: 70:1C:E7:A0:17:16
OS: Microsoft Windows 10

Vulnerabilities

[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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_10 -> Microsoft Windows 10 64-bit

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

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 : WMsgKRpc0116990

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 : WMsgKRpc0116990

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

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-64817070e4c0158b14

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c9dbf19-d39e-4bb9-90ee-8f7179b20283, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2ffad55a566f0e8b10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2ffad55a566f0e8b10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95095ec8-32ea-4eb0-a3e2-041f97b36168, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2ffad55a566f0e8b10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e38f5360-8572-473e-b696-1b46873beeab, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2ffad55a566f0e8b10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d22895ef-aff4-42c5-a5b2-b14466d34ab4, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2ffad55a566f0e8b10

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 : Local RPC service
Named pipe : LRPC-3103c25a692d738cb8
```

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c503f532-443a-4c69-8300-ccdf1fbdb3839, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6CCDE722BD1F783BF169A9EFECE5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c503f532-443a-4c69-8300-ccdf1fbdb3839, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4645d2f33e5cf397c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-b8cad9c9e2b2d18900

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9fa6aff6-e0ad-48df-a6b4-e64be66a17a1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-047e129313b3eab912

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : db2ce634-191d-42af-a28c-16be97924ca7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307a1e33

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a36f6c1d-ed97-46b4-9762-3f13a0f6dea9, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307a1e33

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a36f6c1d-ed97-46b4-9762-3f13a0f6dea9, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-844accc431d1828be5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3cc5a774-9689-4395-83d9-2d51d69adc0f, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307a1e33

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3cc5a774-9689-4395-83d9-2d51d69adc0f, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-844accc431d1828be5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 97be9507-17da-4999-87d7-66c0b2d83cc7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307a1e33

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 97be9507-17da-4999-87d7-66c0b2d83cc7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-844accc431d1828be5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d424f01c-1055-43b1-b519-0482344ce002, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307a1e33

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d424f01c-1055-43b1-b519-0482344ce002, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-844accc431d1828be5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d424f01c-1055-43b1-b519-0482344ce002, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-040915ec9a3a10422c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307a1e33

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-844accc431d1828be5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-040915ec9a3a10422c

Object UUID : 8489be1c-80a4-48bc-901a-aa91bd827a7c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-55e7a91ff7307ale33

Object UUID : 8489be1c-80a4-48bc-901a-aa91bd827a7c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-844accc431d1828be5

Object UUID : 8489be1c-80a4-48bc-901a-aa91bd827a7c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-040915ec9a3a10422c

Object UUID : 8489be1c-80a4-48bc-901a-aa91bd827a7c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-547bf0e36d51115320

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beac-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.transport
Type : Local RPC service
Named pipe : wcncsvc.transport

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : wcncsvc.transport

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c100beab-d33a-4a4b-bf23-bbef4663d017, version 1.0
Description : Unknown RPC service
Annotation : wcncsvc.wcnprpc
Type : Local RPC service
Named pipe : wcncsvc.wcnprpc

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 : OLE11AFE35B37A78DC2061A7E18FDBC

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 : LRPC-3e1fe1b6493578f082

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE11AFE35B37A78DC2061A7E18FDBC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e1fe1b6493578f082

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 923c9623-db7f-4b34-9e6d-e86580f8ca2a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE11AFE35B37A78DC2061A7E18FDBC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 923c9623-db7f-4b34-9e6d-e86580f8ca2a, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e1fe1b6493578f082

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e8748f69-a2a4-40df-9366-62dbeb696e26, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE11AFE35B37A78DC2061A7E18FDBC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e8748f69-a2a4-40df-9366-62dbeb696e26, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e1fe1b6493578f082

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c8ba73d2-3d55-429c-8e9a-c44f006f69fc, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE11AFE35B37A78DC2061A7E18FDBC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c8ba73d2-3d55-429c-8e9a-c44f006f69fc, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e1fe1b6493578f082

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 43890c94-bfd7-4655-ad6a-b4a68397cdcb, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE11AFE35B37A78DC2061A7E18FDBC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 43890c94-bfd7-4655-ad6a-b4a68397cdcb, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e1fe1b6493578f082

Object UUID : 00000002-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE319B5D1B958F554F5F564337B54D

Object UUID : 00000002-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-68c2221b378f319f8a

Object UUID : 00000002-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE319B5D1B958F554F5F564337B54D

Object UUID : 00000002-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-68c2221b378f319f8a

Object UUID : 00000002-0000-0000-0000-000000000000
UUID : b1ef227e-dfa5-421e-82bb-67a6a129c496, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE319B5D1B958F554F5F564337B54D

Object UUID : 00000002-0000-0000-0000-000000000000
UUID : b1ef227e-dfa5-421e-82bb-67a6a129c496, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-68c2221b378f319f8a

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000002
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc04EEF3272

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000002
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc04EEF3272

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

UUID : bf4dc912-e52f-4904-8ebe-9317c1bdd497, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7D8C3BAD30A3B971AEC8CEA3AB54

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bf4dc912-e52f-4904-8ebe-9317c1bdd497, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-dd080ad1eb3c110d17

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : be7f785e-0e3a-4ab7-91de-7e46e443be29, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0ffbb02b815a16693

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 54b4c689-969a-476f-8dc2-990885e9f562, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0ffbb02b815a16693

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLEDIF1C1AC299FDA1C706C737DBCD07

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : LRPC-31bdd42bffa86295bb

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-5c5eecd72fb16fad71

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a4b8d482-80ce-40d6-934d-b22a01a44fe7, version 1.0
Description : Unknown RPC service
Annotation : LicenseManager
Type : Local RPC service
Named pipe : LicenseServiceEndpoint

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : RasmanLrpC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : VpnikeRpC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : LRPC-bcc2e56cc8a256eedb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Local RPC service
Named pipe : tapsrvlpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Local RPC service
Named pipe : unimdmSvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 714dc5c4-c5f6-466a-b037-a573c958031e, version 1.0

Description : Unknown RPC service
Annotation : ProcessTag Server Endpoint
Type : Local RPC service
Named pipe : OLE1C53E7160F456CFB3117DD1BC97F

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 714dc5c4-c5f6-466a-b037-a573c958031e, version 1.0
Description : Unknown RPC service
Annotation : ProcessTag Server Endpoint
Type : Local RPC service
Named pipe : LRPC-b9c9c4df88d65d8015

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : LRPC-f9f1f5b0913ab8f761

Object UUID : 49541cea-a719-4e75-8d58-a3a7bfff960e
UUID : 850cee52-3038-4277-b9b4-e05db8b2c35c, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Association RPC Interface
Type : Local RPC service
Named pipe : LRPC-d317ae39ea4e05bf74

Object UUID : 80b4038a-1d09-4c05-b1b6-249a4c2e0736
UUID : a1d4eae7-39f8-4bca-8e72-832767f5082a, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Inbound RPC Interface
Type : Local RPC service
Named pipe : LRPC-d317ae39ea4e05bf74

Object UUID : 145857ef-d848-4a7e-b544-c1984d26cf05
UUID : 2e7d4935-59d2-4312-a2c8-41900aa5495f, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Challenge RPC Interface
Type : Local RPC service
Named pipe : LRPC-d317ae39ea4e05bf74

Object UUID : 289e5e0f-414a-4de9-8d17-244507fffc07
UUID : bd84cd86-9825-4376-813d-334c543f89b1, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Query RPC Interface
Type : Local RPC service
Named pipe : LRPC-d317ae39ea4e05bf74

Object UUID : 1475c123-1193-4379-81ac-302c4383421d
UUID : 5b665b9a-a086-4e26-ae24-96ab050b0ec3, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework AEP Store Access RPC Interface
Type : Local RPC service
Named pipe : LRPC-d317ae39ea4e05bf74

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0497b57d-2e66-424f-a0c6-157cd5d41700, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-909a998689cadbb8a2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12ala, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-909a998689cadbb8a2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-909a998689cadbb8a2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-909a998689cadbb8a2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-909a998689cadbb8a2

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

UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : LRPC-bf65d76c3b020d714f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : LRPC-bf65d76c3b020d714f

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 : Local RPC service
Named pipe : LRPC-da8b208795b78ed130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : LRPC-da8b208795b78ed130

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : TeredoDiagnostics

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : TeredoControl

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 : Local RPC service
Named pipe : LRPC-da8b208795b78ed130

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 : Local RPC service
Named pipe : TeredoDiagnostics

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 : Local RPC service
Named pipe : TeredoControl

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 : Local RPC service
Named pipe : OLED117349B9368DA7FF7338D28BB53

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 : Local RPC service
Named pipe : LRPC-da8b208795b78ed130

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 : Local RPC service
Named pipe : TeredoDiagnostics

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 : Local RPC service
Named pipe : TeredoControl

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 : Local RPC service
Named pipe : OLED117349B9368DA7FF7338D28BB53

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c27f3c08-92ba-478c-b446-b419c4cef0e2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-5943f49cf4cd581cbc

Object UUID : ce4375e7-9dfc-42f8-999e-08ca7d1c6681
UUID : 98e96949-bc59-47f1-92d1-8c25b46f85c7, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-0e8e17730df07ea159

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f2c9b409-c1c9-4100-8639-d8ab1486694a, version 1.0
Description : Unknown RPC service
Annotation : Witness Client Upcall Server
Type : Local RPC service
Named pipe : LRPC-d45dcb8881c6caca8c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : eb081a0d-10ee-478a-a1dd-50995283e7a8, version 3.0
Description : Unknown RPC service
Annotation : Witness Client Test Interface
Type : Local RPC service
Named pipe : LRPC-d45dcb8881c6caca8c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Local RPC service
Named pipe : LRPC-d45dcb8881c6caca8c

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 : Local RPC service
Named pipe : LRPC-8b395fb5a19ab6da8d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8b395fb5a19ab6da8d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8b395fb5a19ab6da8d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8b395fb5a19ab6da8d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8b395fb5a19ab6da8d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 25952c5d-7976-4aa1-a3cb-c35f7ae79d1b, version 1.0
Description : Unknown RPC service
Annotation : Wireless Diagnostics
Type : Local RPC service
Named pipe : LRPC-7bee5dc42cfa901a80

Object UUID : 6e616c77-7673-0063-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-7bee5dc42cfa901a80

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214ea9, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service

Type : Local RPC service
Named pipe : LRPC-7bee5dc42cfa901a80

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214ea9, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service
Type : Local RPC service
Named pipe : LRPC-52048ce852421029fe

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214eb0, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service LowPriv
Type : Local RPC service
Named pipe : LRPC-7bee5dc42cfa901a80

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214eb0, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service LowPriv
Type : Local RPC service
Named pipe : LRPC-52048ce852421029fe

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c3f42c6e-d4cc-4e5a-938b-9c5e8a5d8c2e, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-7bee5dc42cfa901a80

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c3f42c6e-d4cc-4e5a-938b-9c5e8a5d8c2e, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-52048ce852421029fe

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3C32E56E6165437B6733B051436A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8046da8a8a8147f1f9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b37f900a-eae4-4304-a2ab-12bb668c0188, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3C32E56E6165437B6733B051436A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b37f900a-eae4-4304-a2ab-12bb668c0188, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8046da8a8a8147f1f9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e7f76134-9ef5-4949-a2d6-3368cc0988f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3C32E56E6165437B6733B051436A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e7f76134-9ef5-4949-a2d6-3368cc0988f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8046da8a8a8147f1f9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7aeb6705-3ae6-471a-882d-f39c109edc12, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3C32E56E6165437B6733B051436A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7aeb6705-3ae6-471a-882d-f39c109edc12, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8046da8a8a8147f1f9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f44e62af-dab1-44c2-8013-049a9de417d6, version 1.0
Description : Unknown RPC service
Type : Local RPC service

Named pipe : OLE3C32E56E6165437B6733B051436A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f44e62af-dab1-44c2-8013-049a9de417d6, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8046da8a8a8147f1f9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3C32E56E6165437B6733B051436A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8046da8a8a8147f1f9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-315a80a3ab383a6ce7

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 : audit

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 : securityevent

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 : LSARPC_ENDPOINT

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 : lsacap

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 : LSA_IDPEXT_ENDPOINT

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 : LSA_EAS_ENDPOINT

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 : lsapolICYlookup

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 : lsasspirpc

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 : protected_storage

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 : SidKey Local End Point

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 : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsapolICYlookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : audit

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 : Local RPC service
Named pipe : securityevent

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 : Local RPC service
Named pipe : LSARPC_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : lsapolICYlookup

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 : Local RPC service
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : audit

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 : Local RPC service
Named pipe : securityevent

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 : Local RPC service
Named pipe : LSARPC_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : lsapolicylookup

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 : Local RPC service
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-bd9df5372ca4b1fb43

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : nlapl

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : nlaapi

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bdal-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpsvc6

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

UUID : 3c4728c5-f0ab-448b-bdal-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bdal-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-a97c4be3bffa8522c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : OLE0EB65665B50BA0A578F129EA97B0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : LRPC-6f15aled0a8a960e05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : OLE0EB65665B50BA0A578F129EA97B0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : LRPC-6f15aled0a8a960e05

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCP/IP
Type : Local RPC service
Named pipe : eventlog

Object UUID : f2add560-eb85-4170-82a2-a48e789690cd
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e01f492cbc9a34da0

Object UUID : 045ad40c-5920-4757-90a5-ae0e7e6f6838
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e01f492cbc9a34da0

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-77a0d756a2e9a148c5

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-fe38f9cbfc460bc2c7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-fe38f9cbfc460bc2c7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-fe38f9cbfc460bc2c7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-fe38f9cbfc460bc2c7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4baa3ca4bef1f2da5c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-fe38f9cbfc460bc2c7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4baa3ca4bef1f2da5c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-fe38f9cbfc460bc2c7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4baa3ca4bef1f2da5c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : df4df73a-c52d-4e3a-8003-8437fdf8302a, version 0.0
Description : Unknown RPC service
Annotation : WM.WindowManagerRPC\Server
Type : Local RPC service
Named pipe : LRPC-decd7e1630ae1992fb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-decd7e1630ae1992fb

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

UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-aa7566d97c1f592b16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-decd7e1630ae1992fb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-aa7566d97c1f592b16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-ee960b64ffa4c50472

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-decd7e1630ae1992fb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-aa7566d97c1f592b16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-ee960b64ffa4c50472

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-a043c4bde7d7edf275

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-decd7e1630ae1992fb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-aa7566d97c1f592b16

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-ee960b64ffa4c50472

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-a043c4bde7d7edf275

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-9c346aaa72fa505c13

Object UUID : b5cccd5ef-4238-440b-bba0-999f828f1cfe
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9917d6b3d88a23b36b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9917d6b3d88a23b36b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9da764bfd2a8c0ff5d

Object UUID : fdd099c6-df06-4904-83b4-a87a27903c70
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e45d9c63ed2f33885b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Reset module
Type : Local RPC service
Named pipe : LRPC-e45d9c63ed2f33885b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint for NCB Reset module
Type : Local RPC service
Named pipe : LRPC-9cd209dd40d70fee7a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-e45d9c63ed2f33885b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-9cd209dd40d70fee7a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : OLE1B81AFD206193AA43CAF8CC3BC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-981f1ec6c94b853b55

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : LRPC-e45d9c63ed2f33885b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : LRPC-9cd209dd40d70fee7a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : OLE1B81AFD206193AA43CAF8CC3BC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service

Annotation : Network Connection Broker server endpoint
Type : Local RPC service
Named pipe : LRPC-981f1ec6c94b853b55

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-757c28790fd7072e66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 085b0334-e454-4d91-9b8c-4134f9e793f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8782d3b9-ebbd-4644-a3d8-e8725381919b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3b338d89-6cfa-44b8-847e-531531bc9992, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0361ae94-0316-4c6c-8ad8-c594375800e2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

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

UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

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

UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2c7fd9ce-e706-4b40-b412-953107ef9bb0, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c521facf-09a9-42c5-b155-72388595cbf0, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1832bcf6-cab8-41d4-85d2-c9410764f75a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4dace966-a243-4450-ae3f-9b7bcb5315b8, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e53d94ca-7464-4839-b044-09a2fb8b3ae5, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 082a3471-31b6-422a-b931-a54401960c62, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4ed8abcc-f1e2-438b-981f-bb0e8abc010c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95406f0b-b239-4318-91bb-cea3a46ff0dc, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fae436b0-b864-4a87-9eda-298547cd82f2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

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

UUID : 178d84be-9291-4994-82c6-3f909aca5a03, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d47017b-b33b-46ad-9e18-fe96456c5078, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd59071b-3215-4c59-8481-972edadc0f6a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b8cadbaf-e84b-46b9-84f2-6f71c03f9e55, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b8cadbaf-e84b-46b9-84f2-6f71c03f9e55, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

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

Object UUID : b8cadbaf-e84b-46b9-84f2-6f71c03f9e55, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b8cadbaf-e84b-46b9-84f2-6f71c03f9e55, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b8cadbaf-e84b-46b9-84f2-6f71c03f9e55, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE2FADAEF4093E2A564E8AFCB98990

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0fc1692f65648d0e5b

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

UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE2FADAEF4093E2A564E8AFCB98990

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0fc1692f65648d0e5b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eb75be962ffd471d26

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE2FADAEF4093E2A564E8AFCB98990

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0fc1692f65648d0e5b

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32

UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eb75be962fdd471d26

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE2FADAEF4093E2A564E8AFCB98990

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0fc1692f65648d0e5b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eb75be962fdd471d26

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-64817070e4c0158b14

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-60c183be931037d1e4

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e670a78131dc1cccf7

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b36e57c5b2ce2d4495

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86

UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE2FADAEF4093E2A564E8AFBCB98990

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0fc1692f65648d0e5b

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eb75be962fdd471d26

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-64817070e4c0158b14

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : csepub

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 : umpo

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 : actkernel

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-60c183be931037d1e4

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-e670a78131dc1cccf7

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-b36e57c5b2ce2d4495

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 : OLE2FADAEF4093E2A564E8AFBCB98990

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-0fc1692f65648d0e5b

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-eb75be962fdd471d26

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 : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddbd0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\LAPTOP-5LEH76CL

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 : \\LAPTOP-5LEH76CL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\LAPTOP-5LEH76CL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bc31db, version 1.0
Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\LAPTOP-5LEH76CL

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\wksvc
Netbios name : \\LAPTOP-5LEH76CL

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 : \\LAPTOP-5LEH76CL

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
Named pipe : \pipe\lsass
Netbios name : \\LAPTOP-5LEH76CL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191felb, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\LAPTOP-5LEH76CL

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
Named pipe : \pipe\lsass
Netbios name : \\LAPTOP-5LEH76CL

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
Named pipe : \pipe\eventlog
Netbios name : \\LAPTOP-5LEH76CL

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 : \\LAPTOP-5LEH76CL

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 : \\LAPTOP-5LEH76CL

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 : \\LAPTOP-5LEH76CL

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 : \\LAPTOP-5LEH76CL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LAPTOP-5LEH76CL
```

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/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 : 192.168.100.101
```

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/49665/dce-rpc

```
The following DCERPC services are available on TCP port 49665 :
```

```
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 : 49665
IP : 192.168.100.101
```

```
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 : 49665
IP : 192.168.100.101
```

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/49666/dce-rpc

The following DCERPC services are available on TCP port 49666 :

```
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 : 49666
IP : 192.168.100.101
```

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/49667/dce-rpc

The following DCERPC services are available on TCP port 49667 :

```
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 : 49667
IP : 192.168.100.101
```

```
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 : 192.168.100.101
```

```
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 : 192.168.100.101
```

```
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 : 192.168.100.101
```

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/49668/dce-rpc

The following DCERPC services are available on TCP port 49668 :

```
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 : 49668
IP : 192.168.100.101

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 : 49668
IP : 192.168.100.101

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 : 49668
IP : 192.168.100.101

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 : 49668
IP : 192.168.100.101

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 : 49668
IP : 192.168.100.101
```

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/49669/dce-rpc

The following DCERPC services are available on TCP port 49669 :

```
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 : 49669
IP : 192.168.100.101
```

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 : unknown
Confidence level : 56
```

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 :

70:1C:E7:A0:17:16 : Intel Corporate

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:

- 70:1C:E7:A0:17:16

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

192.168.100.101 resolves as LAPTOP-5LEH76CL.

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

Nessus was able to obtain the following information about the host, by parsing the SMB2 Protocol's NTLM SSP message:

Target Name: LAPTOP-5LEH76CL
NetBIOS Domain Name: LAPTOP-5LEH76CL
NetBIOS Computer Name: LAPTOP-5LEH76CL
DNS Domain Name: LAPTOP-5LEH76CL
DNS Computer Name: LAPTOP-5LEH76CL
DNS Tree Name: unknown
Product Version: 10.0.17134

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 :
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: 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

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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 116.181 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:52 Central European Standard Time
Scan duration : 564 sec
Scan for malware : no
```

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 10
Confidence level : 56
Method : MLSinFP
```

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.

```
SinFP:!:
P1:B11113:F0x12:W8192:00204ffff:M1460:
P2:B11113:F0x12:W8192:00204ffff0103030801010402:M1460:
P3:B00000:F0x00:W0:00:M0
P4:190803_7_p=139
```

The remote host is running Microsoft Windows 10

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.
```

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: 2024/04/19

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 192.168.100.104 to 192.168.100.101 :  
192.168.100.104  
192.168.100.101
```

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 vulnerabilities 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: 2024/05/06

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 3 NetBIOS names have been gathered :

LAPTOP-5LEH76CL = File Server Service
LAPTOP-5LEH76CL = Computer name
WORKGROUP = Workgroup / Domain name

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

70:1c:e7:a0:17:16

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

- mDNS hostname : LAPTOP-5LEH76CL.local.
- Advertised services :
 - o Service name : 413547789._teamviewer._tcp.local.

Port number : 2020

192.168.100.102

0

0

0

0

4

CRITICAL

HIGH

MEDIUM

LOW

INFO

Host Information

IP: 192.168.100.102
MAC Address: BC:45:5B:4F:DE:33

Vulnerabilities

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 Organizational Unique Identifier (OUI). These OUs 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 :

BC:45:5B:4F:DE:33 : Samsung Electronics Co.,Ltd

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:
- BC:45:5B:4F:DE:33

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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 204.530 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialled 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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 18:56 Central European Standard Time
Scan duration : 779 sec
Scan for malware : no
```

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 192.168.100.104 to 192.168.100.102 :  
192.168.100.104
```

```
ttl was greater than 50 - Completing Traceroute.
```

```
?
```

```
Hop Count: 1
```

```
An error was detected along the way.
```

192.168.100.103



Host Information

IP: 192.168.100.103

MAC Address: FC:58:DF:2E:84:B4

OS: Nutanix

Vulnerabilities

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/4011

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

<https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

CVSS v2.0 Base Score

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

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/5011

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/4011

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL  
| -Issuer : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/5011

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : CN=CP-STB-D64-000000000714240/0=Cyfrowy Polsat S.A./C=PL  
| -Issuer : CN=CP-STB-D64/0=Cyfrowy Polsat S.A./C=PL
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>
<http://www.nessus.org/u?ac7327a0>
<http://cr.yp.to/talks/2013.03.12/slides.pdf>
<http://www.isg.rhul.ac.uk/tls/>
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/4011

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	SHA1

The fields above are :

```
{Tenable ciphersuite}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>
<http://www.nessus.org/u?ac7327a0>
<http://cr.yp.to/talks/2013.03.12/slides.pdf>
<http://www.isg.rhul.ac.uk/tls/>
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.4 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/5011

List of RC4 cipher suites supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/4011

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

| -Subject : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL

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 : 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

Plugin Output

tcp/0

The following card manufacturers were identified :

FC:58:DF:2E:84:B4 : Interphone Service

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:

- FC:58:DF:2E:84:B4

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8080/www

The remote web server type is :

BH

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/9090/www

The remote web server type is :

BH

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8080/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

```
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
Content-Length: 195
Content-Type: text/html; charset=ISO-8859-1
Date: Fri, 17 May 2024 17:06:01 GMT
SERVER: BH

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body><h1><b>Client error:</b>&nbsp;403&nbsp;Forbidden</h1><hr><address>BH</address></body></html>
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/9090/www

Response Code : HTTP/1.1 403 Forbidden

```
Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Connection: close
Content-Length: 195
Content-Type: text/html; charset=ISO-8859-1
Date: Fri, 17 May 2024 17:06:01 GMT
SERVER: BH
```

Response Body :

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body><h1><b>Client error:</b>&nbsp;403&nbsp;Forbidden</h1><hr><address>BH</address></body></html>
```

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/4011

Port 4011/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/5011

Port 5011/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/8000

Port 8000/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/8080/www

Port 8080/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

Plugin Output

tcp/9090/www

Port 9090/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

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 113.952 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
```

```
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 19:02 Central European Standard Time
Scan duration : 1130 sec
Scan for malware : no
```

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 : Nutanix
Confidence level : 70
Method : SinFP
```

The remote host is running Nutanix

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 have 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

Steps to resolve this issue include :

- 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: 2023/06/20

Plugin Output

tcp/0

```
Port 5011 was detected as being open but is now closed
Port 4011 was detected as being open but is now closed
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/4011

```
This port supports TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/5011

This port supports TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/4011

Subject Name:

Common Name: CP-STB-D64-0000000000714240
Organization: Cyfrowy Polsat S.A.
Country: PL

Issuer Name:

Common Name: CP-STB-D64
Organization: Cyfrowy Polsat S.A.
Country: PL

Serial Number: 50 8B D0

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 03 14:20:07 2022 GMT
Not Valid After: Jul 25 14:20:07 2048 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 DE 92 92 FB DA 7F 4E BA 95 B7 B9 AA 53 F6 CC 7A FE 45 F2
BD A4 D6 06 51 B6 20 FA F9 8B D3 03 4E A6 4F 13 81 49 34 0C
0B 1F 34 E4 5F 85 E4 2F C3 B2 90 FC B5 5E F2 53 50 51 86 C5
8B FC 5B E6 9E C8 1C 87 78 72 B6 10 FC 66 2E A8 A6 E2 14 BC
03 1A E0 C2 B8 EB 3A 94 89 8A FD E8 85 B3 DD 62 8E 39 8C 4F
80 52 00 C0 99 9A 3D D9 E5 B1 6B 60 F7 91 6B 90 6E BD 9E 50
59 3E 81 9A D4 E4 04 83 DF 6F E4 CA AD 60 AF 4E 73 3A 27 6A
A6 33 11 32 89 37 2F 28 A7 AB 83 CE D8 9C DD B4 8D 76 6E 65
CA CD 73 03 AB 90 E0 66 44 3C 88 E0 3A 9E 03 C7 50 9F B4 2C
05 15 85 2B E6 C3 81 8B C2 48 40 C5 5A 5A CF D0 3D 9B BB 0F
19 57 24 2B 9C A4 9C BD B6 9E C9 2E F2 57 07 F2 4F DC 4A C2
E4 76 84 04 B5 02 A3 9D E2 C3 38 FF 80 9B 02 42 39 E8 2F D5
B9 AA B3 74 15 C0 CD 5C 1A 2A FA 2C 7A 92 51 A8 21

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 69 66 75 7C 3C F1 EF DC 75 19 62 63 B2 30 74 CD 72 CF 74
65 AC 9F 3D 5A 58 08 BA B4 EC 81 93 39 AE 98 5E 79 5D C0 90
1F CA A0 77 58 1F 38 F5 69 0B 43 DD C3 04 6A 42 63 2A 7A FE
AD CC 60 25 67 E3 32 65 6E 02 45 97 B5 C0 53 E2 2E 50 E6 2F
C3 DE 99 61 A4 E7 39 07 F0 69 15 7A 09 46 04 5B C9 5C DA 35
32 7D E8 73 03 CD 18 44 A3 CA 01 1B 14 AD C5 2D 80 DB 2F 34
26 19 48 27 AB 77 DC C4 F7 17 22 FC 77 57 15 C1 AC 7E 7C 98
15 CB 0A 81 D7 85 58 B0 2B 08 54 1D D4 0A 09 33 88 AF 5E FF
88 C9 22 BB CA 3D B0 FD 06 22 D1 CA F1 28 B7 2A 70 2F 45 D9
21 67 B0 13 A8 7D 9F 80 99 D2 B5 22 16 17 5D 0F 58 41 45 F1
F0 ED E9 4B A1 7E 88 91 41 AA FA FE A8 A6 42 38 77 6E E3 D1
03 44 18 94 CB 1A F0 8B C3 04 19 91 EE F6 44 C5 5C 0C 94 F5
6E 31 29 A5 53 06 50 F3 A2 9B 6C B9 5A 85 DB 8F 2C

Fingerprints :

SHA-256 Fingerprint: F4 CE 41 9B D9 6F 5F 3E 2A 5E C4 7A 64 20 EC 6D 42 B0 A5 74
B9 74 61 10 88 66 EA 7E 6B E4 27 50
SHA-1 Fingerprint: 20 A2 97 F7 20 52 B1 75 CD C7 A9 AD CD 8A 82 F6 B5 D6 08 6B
MD5 Fingerprint: 02 56 BE F1 00 EC 0F C6 E7 F2 B1 9B C3 B7 4E FB

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDDDCAfSgAwIBAgIDUIvQMA0GCSqGSIb3DQEBCwJAMEAxEzARBgNVBAMMCKNQLVNUQi1ENjQxHDAaBgNVBAoME0N5ZnJvd3kgUG9sc2F0IFMuQS4xCzAJ
BgNVBAYTA1BMMB4XDTIyMDYwMzE0MjAwN1oXDTQ4MDcyNTE0MjAwN1owUTEkMCIGA1UEAwBQ1AtU1RCLUQ2NC0wMDAwMDAwNzE0MjQwMRwwGgYDVQQK
DBnBZy+vml0wN0pk8TgUk0DAAsfNORfheQw7KQ/LVe8LNQUybFi/xb5p7IHId4crYQ/GYuqKbiFLwDGuDCuOs6lImK/eiFs91ijjmMT4BSAMCZmj3Z5bFrYPe
a5BuVz5QWT6BmtTkbIPfb+TKrWCvTnM6J2qmMxEyiTcvKKerg87YnN20jXZuZcrNcwOrk0BmRDyI4DqeA8d0n70sBRWFK+bDqYvCSEDFwlP0D2buw8ZVyr
nKScvbaeyS7yVwfyT9xKwuR2hAS1Aq0d4sM4/4CbAKI56C/vuaqzdBXAzvWaKvosepJRqCECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAaWZ1fDzx79x1GWJj
sjB0zXLPdGwsnz1aWAi6t0yBkzumF55XcCOH8qqgd1gfOPVpC0PdwRq0mMqev6tzGALZ+MyZW4CRze1wFPiLlDmL8PemWGk5zkh8GkVeglGBFvJXNo1Mn3o
cwPNGESjygEbFK3FLYDbLzQmUGnq3fcxPcXIvx3VxXBrH58mBXLCcoHXhViwKwhUhdQKCT0Ir17/iMKiu8o9sP0GIthK8Si3KnAvRdkhZ7AtqH2fgJnStSIW
F10PWEFF8fdt6UuhfoiRQar6/qimQjh3buPRA0QYLMsa8IvDBBmR7vZEvxWmlPVuMSmlUwZQ86KbbLlahduPLA==
-----END CERTIFICATE-----

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/5011

Subject Name:

Common Name: CP-STB-D64-0000000000714240
Organization: Cyfrowy Polsat S.A.
Country: PL

Issuer Name:

Common Name: CP-STB-D64
Organization: Cyfrowy Polsat S.A.
Country: PL

Serial Number: 50 8B D0

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jun 03 14:20:07 2022 GMT
Not Valid After: Jul 25 14:20:07 2048 GMT

Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 DE 92 92 FB DA 7F 4E BA 95 B7 B9 AA 53 F6 CC 7A FE 45 F2
BD A4 D6 06 51 B6 20 FA F9 8B D3 03 4E A6 4F 13 81 49 34 0C
0B 1F 34 E4 5F 85 E4 2F C3 B2 90 FC B5 5E F2 53 50 51 86 C5
8B FC 5B E6 9E C8 1C 87 78 72 B6 10 FC 66 2E A8 A6 E2 14 BC
03 1A E0 C2 B8 EB 3A 94 89 8A FD E8 85 B3 DD 62 8E 39 8C 4F
80 52 00 C0 99 9A 3D D9 E5 B1 6B 60 F7 91 6B 90 6E BD 9E 50
59 3E 81 9A D4 E4 04 83 DF 6F E4 CA AD 60 AF 4E 73 3A 27 6A
A6 33 11 32 89 37 2F 28 A7 AB 83 CE D8 9C DD B4 8D 76 6E 65
CA CD 73 03 AB 90 E0 66 44 3C 88 E0 3A 9E 03 C7 50 9F B4 2C
05 15 85 2B E6 C3 81 8B C2 48 40 C5 5A 5A CF D0 3D 9B BB 0F
19 57 24 2B 9C A4 9C BD B6 9E C9 2E F2 57 07 F2 4F DC 4A C2
E4 76 84 04 B5 02 A3 9D E2 C3 38 FF 80 9B 02 42 39 E8 2F D5
B9 AA B3 74 15 C0 CD 5C 1A 2A FA 2C 7A 92 51 A8 21

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 69 66 75 7C 3C F1 EF DC 75 19 62 63 B2 30 74 CD 72 CF 74
65 AC 9F 3D 5A 58 08 BA B4 EC 81 93 39 AE 98 5E 79 5D C0 90
1F CA A0 77 58 1F 38 F5 69 0B 43 DD C3 04 6A 42 63 2A 7A FE
AD CC 60 25 67 E3 32 65 6E 02 45 97 B5 C0 53 E2 2E 50 E6 2F
C3 DE 99 61 A4 E7 39 07 F0 69 15 7A 09 46 04 5B C9 5C DA 35
32 7D E8 73 03 CD 18 44 A3 CA 01 1B 14 AD C5 2D 80 DB 2F 34
26 19 48 27 AB 77 DC F7 17 22 FC 77 57 15 C1 AC 7E 7C 98
15 CB 0A 81 D7 85 58 B0 2B 08 54 1D D4 0A 09 33 88 AF 5E FF
88 C9 22 BB CA 3D B0 FD 06 22 D1 CA F1 28 B7 2A 70 2F 45 D9
21 67 B0 13 A8 7D 9F 80 99 D2 B5 22 16 17 5D 0F 58 41 45 F1
F0 ED E9 4B A1 7E 88 91 41 AA FA FE A8 A6 42 38 77 6E E3 D1
03 44 18 94 CB 1A F0 8B C3 04 19 91 EE F6 44 C5 5C 0C 94 F5
6E 31 29 A5 53 06 50 F3 A2 9B 6C B9 5A 85 DB 8F 2C

Fingerprints :

SHA-256 Fingerprint: F4 CE 41 9B D9 6F 5F 3E 2A 5E C4 7A 64 20 EC 6D 42 B0 A5 74
B9 74 61 10 88 66 EA 7E 6B E4 27 50

SHA-1 Fingerprint: 20 A2 97 F7 20 52 B1 75 CD C7 A9 AD CD 8A 82 F6 B5 D6 08 6B

MD5 Fingerprint: 02 56 BE F1 00 EC 0F C6 E7 F2 B1 9B C3 B7 4E FB

PEM certificate :

-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIDUIvQMA0GCSqGSIb3DQEBCwUAMEAxEzARBgNVBAMCkNQLVNUQi1ENjQxHDAaBgNVBAoME0N5ZnJvd3kgUG9sc2F0IFMuQS4xCzAJ
BgNVBAYTA1BMMB4XDTIyMDYwMzE0MjAwN1oXTDQ4MDcyNTE0MjAwN1owUTEkMCIGA1UEAwBQ1AtU1RCLUQ2NC0wMDAwMDAwMDAwNzE0MjQwMRwwGgYDVQQK
DBNDeWzb3d5IFBvBhNhdcBTlKeUmQswCQYDVEJQTDCCASiWdQYJKoZIhvCNAQEBCBQADggEPADCCA0oCggEBAN6Skvaf066lbe5qlP2zHr+RfK9pNYG
UbYg+vml0wN0pk8Tgk0DAsfNORfheQvw7KQ/LVe8LNQUbF1/xb5p7IHId4crYQ/GYukKbiFLwDGUDCuOs6lImk/eifFs91ijjmMT4BSAMCZmj3Z5bFrYPeR
a5BuVZ5QWT6BmtTkBIPfb+TKRwCvTnM6J2qmMxEy1TcvKKer87YnN20jXzuZcrNcw0rk0BmRdyI4Dqea8dQn70sBRWFK+bDgYvcSEDFWlrP0D2buw8ZVyr
nKScvbaey57yVwfT9xKwuR2hA51Aq0d4sM4/4CbAKi56C/VuaqzdBXAzVwaVosepJRqCECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAAwZ1fDzx79x1GWj
sjB0zXLPdGwsnzlaWAi6t0yBkzumF55XcCOH8qgd1gf0PVpc0PdwRqQmMqev6tzGALZ+MyZw4CRZelwFPiLLdMl8PemWGk5zkh8GkVeglBFvJXN01Mn3o
cwPNGESjygEbFK3FLYDbLzQmGUgnq3fcxPcIXv3xVxBrH58mBXLCoHxhViwKwhUhDQKCTOIr17/iMkiu8o9sP0GIthK8Si3KnAvRdkhZ7ATqH2fgJnStSIW
F10PWEFF8fDt6UuhfoiRQar6/qimQjh3buPRA0QYlMsaa8IvDBBmR7vZEvxWmLPvUmslUwZQ86KbbLlahduPLA==
-----END CERTIFICATE-----

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/4011

Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
<http://www.nessus.org/u?cc4a822a>
<https://www.openssl.org/~bodo/tls-cbc.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/5011

Here is the list of SSL CBC ciphers supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/4011

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12

Null Ciphers (no encryption)

Name Code KEX Auth Encryption MAC

NULL-MD5 0x00, 0x01 RSA RSA None MD5
NULL-SHA 0x00, 0x02 RSA RSA None SHA1
RSA-NUL-SHA256 0x00, 0x3B RSA RSA None SHA256

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1  
  
High Strength Ciphers (>= 112-bit key)  
  
Name Code KEX Auth Encryption MAC  
-----  
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256  
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384  
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1  
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1  
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1  
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1  
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1  
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5  
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1  
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1  
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256  
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/5011

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
Null Ciphers (no encryption)

Name Code KEX Auth Encryption MAC

```
-----  
NULL-MD5 0x00, 0x01 RSA RSA None MD5  
NULL-SHA 0x00, 0x02 RSA RSA None SHA1  
RSA-NUL-SHA256 0x00, 0x3B RSA RSA None SHA256
```

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

```
-----  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1
```

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

```
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384
AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1
AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1
CAMELLIA128-SHA 0x00, 0x41 RSA RSA Camellia-CBC(128) SHA1
CAMELLIA256-SHA 0x00, 0x84 RSA RSA Camellia-CBC(256) SHA1
IDEA-CBC-SHA 0x00, 0x07 RSA RSA IDEA-CBC(128) SHA1
RC4-MD5 0x00, 0x04 RSA RSA RC4(128) MD5
RC4-SHA 0x00, 0x05 RSA RSA RC4(128) SHA1
SEED-SHA 0x00, 0x96 RSA RSA SEED-CBC(128) SHA1
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
```

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10))

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/4011

The following root Certification Authority certificate was found :

```
| -Subject : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL
| -Issuer : CN=CP-STB-CA-ROOT-2/0=Cyfrowy Polsat S.A./C=PL
| -Valid From : Oct 27 07:44:18 2017 GMT
| -Valid To : Oct 26 07:44:18 2047 GMT
| -Signature Algorithm : SHA-256 With RSA Encryption
```

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2022/04/11

Plugin Output

tcp/4011

A TLSv12 server is listening on this port that requests a client certificate.

35297 - SSL Service Requests Client Certificate

Synopsis

The remote service requests an SSL client certificate.

Description

The remote service encrypts communications using SSL/TLS, requests a client certificate, and may require a valid certificate in order to establish a connection to the underlying service.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/01/06, Modified: 2022/04/11

Plugin Output

tcp/5011

A TLSv12 server is listening on this port that requests a client certificate.

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256

- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS
<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/4011

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

Null Ciphers (no encryption)

Name	Code	KEX	Auth	Encryption	MAC
NULL-MD5	0x00, 0x01	RSA	RSA	None	MD5
NULL-SHA	0x00, 0x02	RSA	RSA	None	SHA1
RSA-NULL-SHA256	0x00, 0x3B	RSA	RSA	None	SHA256

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RSA-AES128-SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	SHA256
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	SHA384
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	SHA1
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	SHA1
CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	SHA1
IDEA-CBC-SHA	0x00, 0x07	RSA	RSA	IDEA-CBC(128)	SHA1
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	SHA1
SEED-SHA	0x00, 0x96	RSA	RSA	SEED-CBC(128)	SHA1
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	SHA256
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	SHA256

The fields above are :

```
{Tenable ciphername}  
{Cipher ID code}  
Kex={key exchange}  
Auth={authentication}  
Encrypt={symmetric encryption method}  
MAC={message authentication code}  
{export flag}
```

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

<https://ssl-config.mozilla.org/>

Solution

Only enable support for recommended cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/5011

The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined below:

Null Ciphers (no encryption)

Name	Code	KEX	Auth	Encryption	MAC
NULL-MD5	0x00, 0x01	RSA	RSA	None	MD5
NULL-SHA	0x00, 0x02	RSA	RSA	None	SHA1
RSA-NULL-SHA256	0x00, 0x3B	RSA	RSA	None	SHA256

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC(168)	SHA1

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
RSA-AES128-SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	SHA256
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	SHA384
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	SHA1
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	SHA1
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	SHA1
CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	SHA1
IDEA-CBC-SHA	0x00, 0x07	RSA	RSA	IDEA-CBC(128)	SHA1
RC4-MD5	0x00, 0x04	RSA	RSA	RC4(128)	MD5
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	SHA1
SEED-SHA	0x00, 0x96	RSA	RSA	SEED-CBC(128)	SHA1
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	SHA256
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	SHA256

The fields above :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

91263 - SSL/TLS Service Requires Client Certificate

Synopsis

The remote service requires an SSL client certificate to establish an SSL/TLS connection.

Description

The remote service encrypts communications using SSL/TLS and requires a client certificate in order to establish an SSL/TLS connection.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/05/19, Modified: 2016/05/19

Plugin Output

tcp/4011

A TLSv12 server is listening on this port and requires client certificate verification.

91263 - SSL/TLS Service Requires Client Certificate

Synopsis

The remote service requires an SSL client certificate to establish an SSL/TLS connection.

Description

The remote service encrypts communications using SSL/TLS and requires a client certificate in order to establish an SSL/TLS connection.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/05/19, Modified: 2016/05/19

Plugin Output

tcp/5011

A TLSv12 server is listening on this port and requires client certificate verification.

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/4011

A TLSv1.2 server answered 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/5011

A TLSv1.2 server answered 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

Plugin Output

tcp/8000

The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.

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/8080/www

A web 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/9090/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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/4011

TLSv1.2 is enabled and the server supports at least one cipher.

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/5011

TLSv1.2 is enabled and the server supports at least one cipher.

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 192.168.100.104 to 192.168.100.103 :
192.168.100.104
192.168.100.103

Hop Count: 1

10829 - UPnP Client Detection

Synopsis

This machine is a UPnP client.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/12/29, Modified: 2019/03/06

Plugin Output

udp/1900/ssdp

35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

https://en.wikipedia.org/wiki/Universal_Plug_and_Play
https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol
<http://quimby.gnu.org/internet-drafts/draft-cai-ssdp-v1-03.txt>

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2018/09/12

Plugin Output

udp/1900/ssdp

The device responded to an SSDP M-SEARCH request with the following locations :

http://192.168.100.103:8080/upnpdev/devc/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/00

And advertises these unique service names :

```
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::upnp:rootdevice
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::urn:schemas-upnp-org:device:MediaServer:2
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::urn:schemas-upnp-org:service:ConnectionManager:2
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::urn:schemas-upnp-org:service:ContentDirectory:2
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::urn:dial-multiscreen-org:service:dial:1
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::urn:adbglobal-com:service:X_ADB_RemoteControl:1
uuid:18645170-1dd2-11b2-8921-fc58df2e84b4::urn:adbglobal-com:service:X_ADB_CerberLite:1
```

35712 - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

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

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/06/12

Plugin Output

tcp/8080/www

Here is a summary of http://192.168.100.103:8080/upnpdev/devc/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/00 :

```
deviceType: urn:schemas-upnp-org:device:MediaServer:2
friendlyName: POLSATBOX4KLITE
manufacturer: ADB
manufacturerURL: http://www.adbglobal.com/
modelName: POLSAT BOX 4K LITE
modelDescription: BH/DLNA Media Server
modelName: POLSAT BOX 4K LITE
modelNumber: 23.5.15 RELEASE
serialNumber: 1111-111111-1111
ServiceID: urn:upnp-org:serviceId:ConnectionManager
serviceType: urn:schemas-upnp-org:service:ConnectionManager:2
controlURL: /upnpfun/ctrl/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/00
eventSubURL: /upnpfun/evnt/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/00
SCPDURL: /upnpdev/serv/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/00
ServiceID: urn:upnp-org:serviceId:ContentDirectory
serviceType: urn:schemas-upnp-org:service:ContentDirectory:2
controlURL: /upnpfun/ctrl/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/01
eventSubURL: /upnpfun/evnt/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/01
SCPDURL: /upnpdev/serv/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/01
ServiceID: urn:adbglobal-com:serviceId:X_ADB_RemoteControl
serviceType: urn:adbglobal-com:service:X_ADB_RemoteControl:1
controlURL: /upnpfun/ctrl/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/03
eventSubURL: /upnpfun/evnt/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/03
SCPDURL: /upnpdev/serv/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/03
ServiceID: urn:adbglobal-com:serviceId:X_ADB_CerberLite
serviceType: urn:adbglobal-com:service:X_ADB_CerberLite:1
controlURL: /upnpfun/ctrl/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/04
eventSubURL: /upnpfun/evnt/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/04
SCPDURL: /upnpdev/serv/uuid_18645170-1dd2-11b2-8921-fc58df2e84b4/04
```

192.168.100.104



Host Information

Netbios Name:	DESKTOP-FLHPJPQ
IP:	192.168.100.104
OS:	Windows 11

Vulnerabilities

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

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/8834/www

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

```
| -Subject : O=Nessus Users United/OU=Nessus Server/L>New York/C=US/ST=NY/CN=DESKTOP-FLHPJPQ  
| -Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L>New York/C=US/ST=NY/CN=Nessus Certification Authority
```

12634 - Authenticated Check : OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet, or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/07/06, Modified: 2022/09/26

Plugin Output

tcp/0

Nessus can run commands on localhost to check if patches are applied.

However, the execution of the command "uname -a" failed, so OS Security Patch Assessment is not available.

SSH Version Banner :

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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows -> Microsoft Windows

Following application CPE matched on the remote system :

cpe:/a:tenable:nessus -> Tenable Nessus

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 : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service

Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : lsapolICYlookup

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

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 : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 6c637067-6569-746e-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-5294823af673fd7fe6

Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Annotation : Group Policy RPC Interface
Type : Local RPC service
Named pipe : LRPC-b730b0653f75dadca9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c503f532-443a-4c69-8300-ccdf1fdbdb3839, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE259DA74C41F657A834239CE5F68A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c503f532-443a-4c69-8300-ccdf1fdbdb3839, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-132fdcc5c583321836

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ffe01159-cfe1-4002-91de-0e0ef32731f5, version 1.0
Description : Unknown RPC service
Annotation : NaturalAuthentication

Type : Local RPC service
Named pipe : LRPC-0a716efa5152c3e199

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : cc4b408c-4c4e-422f-9849-47bb47bd4d2e, version 1.0
Description : Unknown RPC service
Annotation : NaturalAuthentication

Type : Local RPC service
Named pipe : LRPC-0a716efa5152c3e199

Object UUID : 314c8427-4ad7-4233-995a-bbd062ed11e9
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a26731dbda81aeb0e6

Object UUID : 9575918f-89b5-49cd-9307-f9fc0d9a5b05
UUID : ba4aa15a-be94-47fb-9fbf-fef110e7efad, version 1.0
Description : Unknown RPC service
Annotation : DevQueryBroker client query RPC interface
Type : Local RPC service
Named pipe : LRPC-9cc2f67a73c3057bb3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b04d3c44-f014-4530-88f3-ee7daa3e69b9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0fdcb52859fc425412

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bf4dc912-e52f-4904-8ebe-9317c1bdd497, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE92DA95BA47C78D7427BEDEAB52D9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bf4dc912-e52f-4904-8ebe-9317c1bdd497, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-0a4e46fe205c9c3d34

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a533b58-0ed9-4085-b6e8-95795e147972, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE61346968765FA8DBF1F14BB2B062

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a533b58-0ed9-4085-b6e8-95795e147972, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-49a484a17eb5285000

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5dea026d-f999-40b1-a234-2164fd086783, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE61346968765FA8DBF1F14BB2B062

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5dea026d-f999-40b1-a234-2164fd086783, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-49a484a17eb5285000

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5dea026d-f999-40b1-a234-2164fd086783, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e26a3ade6848c96177

Object UUID : fccae962-4722-40c7-a46d-fe5153280723
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE61346968765FA8DBF1F14BB2B062

Object UUID : fccae962-4722-40c7-a46d-fe5153280723
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-49a484a17eb5285000

Object UUID : fccae962-4722-40c7-a46d-fe5153280723
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e26a3ade6848c96177

Object UUID : fccae962-4722-40c7-a46d-fe5153280723

UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-cbffc405b8d8ba205c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2acb9d68-b434-4b3e-b966-e06b4b3a84cb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE61346968765FA8DBF1F14BB2B062

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2acb9d68-b434-4b3e-b966-e06b4b3a84cb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-49a484a17eb5285000

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2acb9d68-b434-4b3e-b966-e06b4b3a84cb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e26a3ade6848c96177

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2acb9d68-b434-4b3e-b966-e06b4b3a84cb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-cbffc405b8d8ba205c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2acb9d68-b434-4b3e-b966-e06b4b3a84cb, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a9ded909848c42ba80

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 : OLEA348B732BA055AB6C742DD98A252

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 : LRPC-2e6c325cf47c3ada22

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEA348B732BA055AB6C742DD98A252

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2e6c325cf47c3ada22

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 923c9623-db7f-4b34-9e6d-e86580f8ca2a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEA348B732BA055AB6C742DD98A252

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 923c9623-db7f-4b34-9e6d-e86580f8ca2a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2e6c325cf47c3ada22

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLE0261738FA68023314DAEC0362E27

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : LRPC-f6be685b8a96b446a0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 44d1520b-6133-41f0-8a66-d37305ecc357, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b9e97dbf228cbf6573

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f5663d1c-7cd6-4109-9d01-2c187b75c38f, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b9e97dbf228cbf6573

Object UUID : ccb8aa07-7225-4ea0-8501-4b3c1b1acd43
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3DDA15B95654E0E9783B0512EB7D

Object UUID : ccb8aa07-7225-4ea0-8501-4b3c1b1acd43
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-094393dd0b4ef1c9f0

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3DDA15B95654E0E9783B0512EB7D

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-094393dd0b4ef1c9f0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : LRPC-818b3f8ed806d6760a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a4b8d482-80ce-40d6-934d-b22a01a44fe7, version 1.0
Description : Unknown RPC service
Annotation : LicenseManager
Type : Local RPC service
Named pipe : LicenseServiceEndpoint

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : caaa9188-2b56-486f-b07f-71a679722189, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : RealtekAudioRpcEndpoint

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0497b57d-2e66-424f-a0c6-157cd5d41700, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-e7b20543017ffeedee

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12ala, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-e7b20543017ffeedee

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-e7b20543017ffeedee

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-e7b20543017ffeedee

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-e7b20543017ffeedee

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0f738e20-73c0-4ca8-aa6a-8dfef545fea8, version 1.0
Description : Unknown RPC service
Annotation : AppInfo

Type : Local RPC service
Named pipe : LRPC-e7b20543017ffeedee

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEBCCBEC1762D4FF7625EE14BFF63D

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-5cc73c02b4cedfd97e

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEBCCBEC1762D4FF7625EE14BFF63D

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-5cc73c02b4cedfd97e

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : b1ef227e-dfa5-421e-82bb-67a6a129c496, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEBCCBEC1762D4FF7625EE14BFF63D

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : b1ef227e-dfa5-421e-82bb-67a6a129c496, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-5cc73c02b4cedfd97e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b9ef87fa-3709-4ac7-b21e-dee603f05983, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE520F559B391305FAF87324AAD733

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b9ef87fa-3709-4ac7-b21e-dee603f05983, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : PenFreControl

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c27f3c08-92ba-478c-b446-b419c4cef0e2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-7ea5fe69e8d4b22978

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-c39825cfa4be7a9bee

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7df1ceae-de4e-4e6f-ab14-49636e7c2052, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-5a757f781bf43bb3d8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d4051bde-9cdd-4910-b393-4aa85ec3c482, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d4051bde-9cdd-4910-b393-4aa85ec3c482, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c9dbf19-d39e-4bb9-90ee-8f7179b20283, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c9dbf19-d39e-4bb9-90ee-8f7179b20283, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95095ec8-32ea-4eb0-a3e2-041f97b36168, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95095ec8-32ea-4eb0-a3e2-041f97b36168, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e38f5360-8572-473e-b696-1b46873beeab, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e38f5360-8572-473e-b696-1b46873beeab, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d22895ef-aff4-42c5-a5b2-b14466d34ab4, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d22895ef-aff4-42c5-a5b2-b14466d34ab4, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98cd761e-e77d-41c8-a3c0-0fb756d90ec2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98cd761e-e77d-41c8-a3c0-0fb756d90ec2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1d45e083-478f-437c-9618-3594ced8c235, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLECF0D20D688CF3F844C54A5BC9767

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1d45e083-478f-437c-9618-3594ced8c235, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a19edd8e6565a33193

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 714dc5c4-c5f6-466a-b037-a573c958031e, version 1.0
Description : Unknown RPC service
Annotation : ProcessTag Server Endpoint
Type : Local RPC service
Named pipe : OLE4BB151F6AE777ABFAFD8277BDCA2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 714dc5c4-c5f6-466a-b037-a573c958031e, version 1.0
Description : Unknown RPC service
Annotation : ProcessTag Server Endpoint
Type : Local RPC service
Named pipe : LRPC-bcb646913e8acf5569

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a00e7603-27b5-4a1a-8452-d001f41188a9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : SECOMNRpcEndpoint.{2F0652D5-A8C1-4125-9DE2-115DFCD3504B}

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : RasmanLrpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : VpniKERpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : LRPC-4faaeadf783564b9b43

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 78dcce84-7f13-4139-b8cd-ef22aa0408b, version 1.0
Description : Unknown RPC service
Annotation : StateRepository
Type : Local RPC service
Named pipe : OLE4454F012E4ECD64EC91A9A012358

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 78dcce84-7f13-4139-b8cd-ef22aa0408b, version 1.0
Description : Unknown RPC service
Annotation : StateRepository
Type : Local RPC service
Named pipe : LRPC-ab09e02f79f9754519

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30034843-029d-46ec-8fff-5d12987f85c4, version 1.0
Description : Unknown RPC service
Annotation : INgcProvisioningHandler
Type : Local RPC service
Named pipe : LRPC-f3250377bb9cf07f52

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bef2320-f308-4720-b913-0129cecfa6b9, version 1.0
Description : Unknown RPC service
Annotation : IVscProvisioningHandler
Type : Local RPC service
Named pipe : LRPC-f3250377bb9cf07f52

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d24ff0b-1bab-404c-a0fd-42c85577bf68, version 1.0
Description : Unknown RPC service
Annotation : INgcHandler
Type : Local RPC service
Named pipe : LRPC-f3250377bb9cf07f52

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7642249b-84c2-4404-b6eb-1e0a2458839a, version 1.0
Description : Unknown RPC service
Annotation : INgcSecureBioHandler
Type : Local RPC service
Named pipe : LRPC-f3250377bb9cf07f52

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e6f89680-fc98-11e3-80d4-10604b681cfa, version 1.0
Description : Unknown RPC service
Annotation : INgcGidsHandler
Type : Local RPC service
Named pipe : LRPC-f3250377bb9cf07f52

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 : Local RPC service
Named pipe : LRPC-d639a851bb39892020

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : LRPC-814a1557f522e7b475

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : LRPC-814a1557f522e7b475

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 : Local RPC service
Named pipe : LRPC-afcec28fc77d16a2c1

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 : Local RPC service
Named pipe : LRPC-afcec28fc77d16a2c1

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 : Local RPC service
Named pipe : TeredoDiagnostics

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 : Local RPC service
Named pipe : TeredoControl

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 : Local RPC service
Named pipe : LRPC-afcec28fc77d16a2c1

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 : Local RPC service
Named pipe : TeredoDiagnostics

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 : Local RPC service
Named pipe : TeredoControl

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : LRPC-afcec28fc77d16a2c1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : TeredoDiagnostics

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : TeredoControl

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : OLE13B985F6ED655902AC2D74AEB39F

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0e3ae095-8a23-48f4-9782-03c1594a890e, version 1.0
Description : Unknown RPC service
Annotation : NGC Service KSP RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c225e799-29de-42af-bc05-1e2127cc056e, version 1.0
Description : Unknown RPC service
Annotation : NGC Service Management RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d9844ed9-f72a-4745-a4a1-ee71f950781d, version 1.0
Description : Unknown RPC service
Annotation : NGC Service Silent Management RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2b70bed6-1757-4d22-9f39-448589fbebf5, version 1.0
Description : Unknown RPC service
Annotation : NGC Service Ticket RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9cbc9d3a-7586-4814-8d70-18737dcbe523, version 1.0
Description : Unknown RPC service
Annotation : NGC Service LocalAccount Vault Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4e25f4a2-21e8-40ce-b401-32050413143a, version 1.0
Description : Unknown RPC service
Annotation : Device Credential RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd6b7e61-2bed-4d48-a267-d746fe449fed, version 1.0
Description : Unknown RPC service
Annotation : Device Credential Presence RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8337aebc-5564-46fd-bc41-7798f18d2e4b, version 1.0
Description : Unknown RPC service
Annotation : Device Credential Manager RPC Interface
Type : Local RPC service
Named pipe : LRPC-cb17f795d568a98be2

Object UUID : 49541cea-a719-4e75-8d58-a3a7bfff960e
UUID : 850cee52-3038-4277-b9b4-e05db8b2c35c, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Association RPC Interface
Type : Local RPC service
Named pipe : LRPC-0c5d9cf3dce8b83d4b

Object UUID : 80b4038a-1d09-4c05-b1b6-249a4c2e0736
UUID : a1d4eae7-39f8-4bca-8e72-832767f5082a, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Inbound RPC Interface
Type : Local RPC service
Named pipe : LRPC-0c5d9cf3dce8b83d4b

Object UUID : 145857ef-d848-4a7e-b544-c1984d26cf05
UUID : 2e7d4935-59d2-4312-a2c8-41900aa5495f, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Challenge RPC Interface
Type : Local RPC service
Named pipe : LRPC-0c5d9cf3dce8b83d4b

Object UUID : 289e5e0f-414a-4de9-8d17-244507fffc07
UUID : bd84cd86-9825-4376-813d-334c543f89b1, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Query RPC Interface
Type : Local RPC service
Named pipe : LRPC-0c5d9cf3dce8b83d4b

Object UUID : 1475c123-1193-4379-81ac-302c4383421d
UUID : 5b665b9a-a086-4e26-ae24-96ab050b0ec3, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework AEP Store Access RPC Interface
Type : Local RPC service
Named pipe : LRPC-0c5d9cf3dce8b83d4b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service

Named pipe : LRPC-70e62647ee6719c864

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-70e62647ee6719c864

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-ac66dfeb758ad183b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-70e62647ee6719c864

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-ac66dfeb758ad183b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-87169b2479550a3354

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-70e62647ee6719c864

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-ac66dfeb758ad183b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-87169b2479550a3354

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-29ef44354b39dbabf6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f2c9b409-c1c9-4100-8639-d8ab1486694a, version 1.0
Description : Unknown RPC service
Annotation : Witness Client Upcall Server
Type : Local RPC service
Named pipe : LRPC-47cc9f9d19d1598d8f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : eb081a0d-10ee-478a-a1dd-50995283e7a8, version 3.0
Description : Unknown RPC service
Annotation : Witness Client Test Interface
Type : Local RPC service
Named pipe : LRPC-47cc9f9d19d1598d8f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Local RPC service
Named pipe : LRPC-47cc9f9d19d1598d8f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 25952c5d-7976-4a11-a3cb-c35f7ae79d1b, version 1.0
Description : Unknown RPC service
Annotation : Wireless Diagnostics

Type : Local RPC service
Named pipe : LRPC-6df5a0d8ea9b4470e4

Object UUID : 6e616c77-7673-0063-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-6df5a0d8ea9b4470e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214ea9, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service
Type : Local RPC service
Named pipe : LRPC-6df5a0d8ea9b4470e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214ea9, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service
Type : Local RPC service
Named pipe : LRPC-f41fdcd6884a971bf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214eb0, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service LowPriv
Type : Local RPC service
Named pipe : LRPC-6df5a0d8ea9b4470e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214eb0, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service LowPriv
Type : Local RPC service
Named pipe : LRPC-f41fdcd6884a971bf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6df5a0d8ea9b4470e4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f41fdcd6884a971bf7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEEB47CDE7F2A6245053EFDE07888A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-7704dd47eb29c0ab97

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 : Local RPC service
Named pipe : LRPC-9fc9e5ale0790e06b8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942bleca65d1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9fc9e5ale0790e06b8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9fc9e5ale0790e06b8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9fc9e5ale0790e06b8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service

Type : Local RPC service
Named pipe : LRPC-9fc9e5ale0790e06b8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-8f4e9f981bdbde0dcb

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : sensvc

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-4c74bcbba42bceb1a3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEECA9D6B07322066672523373BCF9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4e5b7f303b590bd018

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b37f900a-eae4-4304-a2ab-12bb668c0188, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEECA9D6B07322066672523373BCF9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b37f900a-eae4-4304-a2ab-12bb668c0188, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4e5b7f303b590bd018

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f44e62af-dab1-44c2-8013-049a9de417d6, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEECA9D6B07322066672523373BCF9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f44e62af-dab1-44c2-8013-049a9de417d6, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4e5b7f303b590bd018

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c2d1b5dd-fa81-4460-9dd6-e7658b85454b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEECA9D6B07322066672523373BCF9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c2d1b5dd-fa81-4460-9dd6-e7658b85454b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4e5b7f303b590bd018

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 13560fa9-8c09-4b56-a1fd-04d083b9b2a1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEECA9D6B07322066672523373BCF9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 13560fa9-8c09-4b56-a1fd-04d083b9b2a1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4e5b7f303b590bd018

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 : Local RPC service
Named pipe : DNSResolver

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 : Local RPC service
Named pipe : LRPC-c8432f9229cbf40c10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-37720abf99e5545b94

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : 96864963-599b-40af-85c6-ddb358d99505

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : db2ce634-191d-42af-a28c-16be97924ca7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEB289DD0AEA277DE7EB176D45A4A0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : db2ce634-191d-42af-a28c-16be97924ca7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-036a5d2bca7e703488

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 97be9507-17da-4999-87d7-66c0b2d83cc7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEB289DD0AEA277DE7EB176D45A4A0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 97be9507-17da-4999-87d7-66c0b2d83cc7, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-036a5d2bca7e703488

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6328dcc4-1658-4133-8062-a9943dac2093, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEB289DD0AEA277DE7EB176D45A4A0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6328dcc4-1658-4133-8062-a9943dac2093, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-036a5d2bca7e703488

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6328dcc4-1658-4133-8062-a9943dac2093, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-1ff3118a02f9a4e930

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bdal-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bdal-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bdal-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service

Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 10d20e7a-2530-494a-ac01-b8dd04480ad2, version 1.0
Description : Unknown RPC service
Annotation : camsvc
Type : Local RPC service
Named pipe : OLE0D72B3A8F582F7A84C53D91657E7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 10d20e7a-2530-494a-ac01-b8dd04480ad2, version 1.0
Description : Unknown RPC service
Annotation : camsvc
Type : Local RPC service
Named pipe : LRPC-001991dcb9d5960f4b

Object UUID : bae10e73-0001-0000-9dab-7d0f635c171a
UUID : 509bc7ae-77be-4ee8-b07c-0d096bb44345, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEC29E919E8DCD68BE613BD62A7418

Object UUID : bae10e73-0001-0000-9dab-7d0f635c171a
UUID : 509bc7ae-77be-4ee8-b07c-0d096bb44345, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-d8fa25805836e8da13

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a69816f5-83b6-4d48-8633-067f99f5f2d3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-df972d1d951d39de54

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-df972d1d951d39de54

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e5d1b8e26684b18dc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : OLE34C6572C864928B95A4622D30880

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : LRPC-0f2816017826443440

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : OLE34C6572C864928B95A4622D30880

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : LRPC-0f2816017826443440

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3f787932-3452-4363-8651-6ea97bb373bb, version 1.0
Description : Unknown RPC service
Annotation : NSP Rpc Interface
Type : Local RPC service
Named pipe : OLE3364490F892E0772E092BC0CBA9E

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3f787932-3452-4363-8651-6ea97bb373bb, version 1.0
Description : Unknown RPC service
Annotation : NSP Rpc Interface
Type : Local RPC service
Named pipe : LRPC-66491dfef34a442a6a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3f787932-3452-4363-8651-6ea97bb373bb, version 1.0

Description : Unknown RPC service
Annotation : NSP Rpc Interface
Type : Local RPC service
Named pipe : INlmDiagnosticsApi

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bd6ca954-842e-468f-8b07-89cbfa9522dc, version 1.0
Description : Unknown RPC service
Annotation : NetworkProfiles Telemetry RPC Interface
Type : Local RPC service
Named pipe : OLE3364490F892E0772E092BC0CBA9E

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bd6ca954-842e-468f-8b07-89cbfa9522dc, version 1.0
Description : Unknown RPC service
Annotation : NetworkProfiles Telemetry RPC Interface
Type : Local RPC service
Named pipe : LRPC-66491def34a442a6a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bd6ca954-842e-468f-8b07-89cbfa9522dc, version 1.0
Description : Unknown RPC service
Annotation : NetworkProfiles Telemetry RPC Interface
Type : Local RPC service
Named pipe : INlmDiagnosticsApi

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3364490F892E0772E092BC0CBA9E

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-66491def34a442a6a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : INlmDiagnosticsApi

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-25a8c9709f37b654c6

Object UUID : b5cccd5ef-4238-440b-bba0-999f828f1cfe
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-01839a37042e5debd6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-01839a37042e5debd6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-e50d56fef14d5032a9

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-3e02f13d6829ca5326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-3e02f13d6829ca5326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-3e02f13d6829ca5326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e02f13d6829ca5326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b581c13b77caf705e2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e02f13d6829ca5326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b581c13b77caf705e2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e02f13d6829ca5326

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b581c13b77caf705e2

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : fdd099c6-df06-4904-83b4-a87a27903c70
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-1485a48b9b9037845b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-98190bd5d9a5564cae

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-1485a48b9b9037845b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : OLE50FAE857AF59C029796F54787319

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service

Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-c1d01d48164d68e6de

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6b0bb9878475dfced5

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 : WMsgKRpc014BDC1

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 : WMsgKRpc014BDC1

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-d2a9970cfa06a364f3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 085b0334-e454-4d91-9b8c-4134f9e793f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8782d3b9-ebbd-4644-a3d8-e8725381919b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3b338d89-6cfa-44b8-847e-531531bc9992, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bdAA0970-413b-4a3e-9e5d-f6dc9d7e0760, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0361ae94-0316-4c6c-8ad8-c594375800e2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd59071b-3215-4c59-8481-972edad0f6a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd59071b-3215-4c59-8481-972edad0f6a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaa18f8cb50d72b62

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaa18f8cb50d72b62

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaa18f8cb50d72b62

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2c7fd9ce-e706-4b40-b412-953107ef9bb0, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4dace966-a243-4450-ae3f-9b7bcb5315b8, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 178d84be-9291-4994-82c6-3f909aca5a03, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e53d94ca-7464-4839-b044-09a2fb8b3ae5, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fae436b0-b864-4a87-9eda-298547cd82f2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 082a3471-31b6-422a-b931-a54401960c62, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6982a06e-5fe2-46b1-b39c-a2c545bfa069, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0ff1f646-13bb-400a-ab50-9a78f2b7a85a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4ed8abcc-f1e2-438b-981f-bb0e8abc010c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95406f0b-b239-4318-91bb-cea3a46ff0dc, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d47017b-b33b-46ad-9e18-fe96456c5078, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaa18f8cb50d72b62

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-54fc8f4936ddd9e3e6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaa18f8cb50d72b62

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-54fc8f4936ddd9e3e6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f2c469663ec08480cd

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaa18f8cb50d72b62

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-54fc8f4936ddd9e3e6

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f2c469663ec08480cd

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaal18f8cb50d72b62

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-54fc8f4936ddd9e3e6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f2c469663ec08480cd

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-57c6f7934d11a1331f

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ea0d7f9a9f8b2b3779

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE7C64E9A98E23F75E1167F36180C2

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-ceaal18f8cb50d72b62

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-54fc8f4936ddd9e3e6

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f2c469663ec08480cd

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-57c6f7934d11a1331f

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : csepub

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 : umpo

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 : actkernel

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-ea0d7f9a9f8b2b3779

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 : OLE7C64E9A98E23F75E1167F36180C2

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-ceaa18f8cb50d72b62

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-54fc8f4936ddd9e3e6

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-f2c469663ec08480cd

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-57c6f7934d11a1331f

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 : csepub

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 : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRp0142820

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 : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRp0142820

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

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 : imsfk

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 : audit

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 : securityevent

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 : LSARPC_ENDPOINT

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 : lsacap

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 : LSA_IDPEXT_ENDPOINT

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 : LSA_EAS_ENDPOINT

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 : lsapolICYlookup

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 : lsasspirpc

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 : protected_storage

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 : SidKey Local End Point

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 : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : imsfk

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso

Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsapolICYlookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : imsfk

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 : Local RPC service
Named pipe : audit

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 : Local RPC service
Named pipe : securityevent

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 : Local RPC service
Named pipe : LSARPC_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : lsapolICYlookup

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 : Local RPC service
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : sams lpc

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 : Local RPC service
Named pipe : imsfk

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 : Local RPC service
Named pipe : audit

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 : Local RPC service
Named pipe : securityevent
```

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 : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\DESKTOP-FLHPJPQ

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 : \\DESKTOP-FLHPJPQ

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\DESKTOP-FLHPJPQ

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 : \\DESKTOP-FLHPJPQ

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 : \\DESKTOP-FLHPJPQ

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113bel, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\DESKTOP-FLHPJPQ

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 : \\DESKTOP-FLHPJPQ

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\DESKTOP-FLHPJPQ

```
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 : \\DESKTOP-FLHPJPQ

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddbd0, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\DESKTOP-FLHPJPQ

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 : \\DESKTOP-FLHPJPQ

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
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-FLHPJPQ

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
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-FLHPJPQ

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
Named pipe : \pipe\lsass
Netbios name : \\DESKTOP-FLHPJPQ
```

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/49664/dce-rpc

The following DCERPC services are available on TCP port 49664 :

```
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 : 49664
IP : 192.168.100.104

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-e000-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 192.168.100.104

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 : 49664
IP : 192.168.100.104

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 : 49664
IP : 192.168.100.104
```

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/49665/dce-rpc

The following DCERPC services are available on TCP port 49665 :

```
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.100.104
```

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/49666/dce-rpc

The following DCERPC services are available on TCP port 49666 :

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 : 49666
IP : 192.168.100.104

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 : 49666
IP : 192.168.100.104

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/49667/dce-rpc

The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49667
IP : 192.168.100.104

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/49668/dce-rpc

The following DCERPC services are available on TCP port 49668 :

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 : 49668
IP : 192.168.100.104

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942bleca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 192.168.100.104

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 : 49668
IP : 192.168.100.104

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 : 49668
IP : 192.168.100.104

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 : 49668
IP : 192.168.100.104

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/49669/dce-rpc

The following DCERPC services are available on TCP port 49669 :

```
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 : 49669
IP : 192.168.100.104
```

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 : 70
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8834/www

The remote web server type is :

NessusWWW

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

192.168.100.104 resolves as DESKTOP-FLHPJPQ.

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8834/www

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Cache-Control: must-revalidate
X-Frame-Options: DENY
Content-Type: text/html
ETag: 7f9a074d885fc3d7a56fdd9c35e66392
Connection: close
X-XSS-Protection: 1; mode=block
Server: NessusWW
Date: Fri, 17 May 2024 17:05:02 GMT
X-Content-Type-Options: nosniff
Content-Length: 1217
Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self'; frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; connect-src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self' www.tenable.com; object-src 'none'; base-uri 'self'; Strict-Transport-Security: max-age=31536000
Expect-CT: max-age=0

Response Body :

```
<!doctype html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; connect-src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self' www.tenable.com; object-src 'none'; base-uri 'self';" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta charset="utf-8" />
<title>Nessus</title>
<link rel="stylesheet" href="nessus6.css?v=1715293282346" id="theme-link" />
<link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
<link rel="stylesheet" href="wizard_templates.css?v=11939be86ca24a4dbbe8f9b85f95e140" />
<!--[if lt IE 11]>
<script>
window.location = '/unsupported6.html';
</script>
<![endif]-->
<script src="nessus6.js?v=1715293282346"></script>
<script src="pendo-client.js"></script>
<!--Resource-Script-->
</head>
<body>
</body>
</html>
```

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

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

Description

The remote host listens on tcp port 445 and replies to SMB requests.

By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/445/cifs

The following 2 NetBIOS names have been gathered :

DESKTOP-FLHPJPQ = Computer name
DESKTOP-FLHPJPQ = Workgroup / Domain name

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

Nessus was able to obtain the following information about the host, by parsing the SMB2 Protocol's NTLM SSP message:

Target Name: DESKTOP-FLHPJPQ
NetBIOS Domain Name: DESKTOP-FLHPJPQ
NetBIOS Computer Name: DESKTOP-FLHPJPQ
DNS Domain Name: DESKTOP-FLHPJPQ
DNS Computer Name: DESKTOP-FLHPJPQ
DNS Tree Name: unknown
Product Version: 10.0.22621

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 :
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

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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 19:02 Central European Standard Time
Scan duration : 473 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

<https://www.tenable.com/products/nessus/nessus-professional>

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF

IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2023/02/08

Plugin Output

tcp/8834/www

URL : <https://DESKTOP-FLHPJPQ:8834/>
Version : unknown

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/135/epmap

Port 135/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/137

Port 137/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/138

Port 138/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/139/smb

Port 139/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/445/cifs

Port 445/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/500

Port 500/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/1900

Port 1900/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/3702

Port 3702/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Plugin Output

udp/4500

Port 4500/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/5040

Port 5040/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/5050

Port 5050/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/5353

Port 5353/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/5355

Port 5355/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/8834/www

Port 8834/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49664/dce-rpc

Port 49664/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49665/dce-rpc

Port 49665/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49666/dce-rpc

Port 49666/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49667/dce-rpc

Port 49667/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49668/dce-rpc

Port 49668/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49669/dce-rpc

Port 49669/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

tcp/49672

Port 49672/tcp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/53599

Port 53599/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/53600

Port 53600/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/58209

Port 58209/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/58211

Port 58211/udp was found to be open

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: If the scan policy has WMI Netstat enabled, this plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2024/04/24

Plugin Output

udp/61503

Port 61503/udp was found to be open

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 : Windows 11
Confidence level : 70
Method : Misc
```

The remote host is running Windows 11

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2024/03/19

Plugin Output

tcp/0

Nessus can run commands on localhost to check if patches are applied.

Credentialed checks of Windows are not supported using SSH.

The remote host is not currently supported by this plugin.

Runtime : 1.87761 seconds

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 : ssh_get_info2.nasl
Plugin ID : 97993
Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
Protocol : LOCALHOST
Message :
Credentialed checks of Windows are not supported using SSH.
```

```
- Plugin : ssh_get_info.nasl
Plugin ID : 12634
Plugin Name : Authenticated Check : OS Name and Installed Package Enumeration
Protocol : LOCALHOST
Message :
Remote host was not identified as a known device or operating
system and the execution of "uname -a" failed.
```

SSH Version Banner :

```
- 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.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

Plugin Output

tcp/8834/www

This port supports TLSv1.3/TLSv1.2.

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8834/www

Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: DESKTOP-FLHPJPQ

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 81 10

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 17 15:33:32 2024 GMT
Not Valid After: May 16 15:33:32 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B1 46 58 18 5E 76 BE 53 B5 92 4F FE 56 77 1C F1 79 ED B4
31 D7 6A B8 63 66 3A BC 43 52 65 3D 8B 09 1C 45 A8 09 6B F8
9A 2D 20 19 70 64 8F 6A 87 FF 70 0A 53 77 D7 83 7C DC DA 6F
F8 41 01 AF 8B 6B 76 3E CD D8 E6 98 53 B0 2A 47 3F D2 BB AE
E9 69 47 F8 76 9F 0B 5D E7 D2 95 04 CA 79 C0 B5 83 33 CC 63

98 0B DA 38 52 8B B2 CE 35 5B 9B 7F 21 C6 8D 92 A1 80 1B 4C
25 34 66 E6 1F 7D 35 10 4A BB B0 B8 EC D7 13 51 9C A3 46 02
65 19 23 BC 7E 80 B5 8C 15 F6 2E 01 8B 65 31 34 71 48 81 21
04 90 6B EF 0A CB 74 AB FB 63 1C 50 F1 B0 E3 C1 D3 4D A2 7A
0D C1 23 51 12 F4 0E 29 0D A2 D3 3D 50 22 49 76 48 FE 15
06 3F 32 9C 55 12 F5 EF D0 95 7E AB E9 82 DB 22 9B DD FB D2
E3 67 A5 32 E1 B4 29 37 D3 E1 41 8F BE CF A8 B2 79 0F C4 1A
1B 8A 21 5B AA 2B EF 9D 3A E2 15 B8 38 21 9D 8D 81
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 2E 2A 77 67 A9 C6 F7 DC 43 28 B2 D2 E7 06 37 E3 31 82 6A
64 68 90 FF 7E 1A F2 D7 3B EE D5 83 DF 65 6C 68 71 B5 3E 5F
59 3B F2 2B 5B 7D 59 6A CF 68 7C BE 9B ED 8B CA C2 AD 67 F0
61 8E 94 29 A4 94 A1 FB 40 8B FD 83 6A 59 94 07 6D E9 1E F4
0B 18 C0 6D 54 5C 4C 8D 05 6B D5 6F 0A A7 C8 9D 53 A2 B9 BA
12 4B 3E 0C 1A B5 87 48 91 E6 BD 25 C1 14 BF 5E 92 CE 0F F4
80 5D 1F 23 FA 4F 97 FA B4 3F A2 E7 B8 93 AA 12 3B 8F E5 82
97 3C 03 99 1E 35 4A FA 52 ED 16 02 BD AA 66 62 D7 EF A6 A6
18 56 B5 20 06 D5 11 32 39 C9 58 39 8B 5F 2A 66 2D 3F 77 A1
F1 94 3C 9E 5D 4D F7 97 F0 6E 68 16 8E A8 07 92 95 1B C5 7B
76 14 42 FB 5E 92 6F 4C EB EA 90 95 E6 4C 60 26 0A 06 2D 1D
D2 C1 09 F4 17 E8 ED CF 99 C2 77 A7 92 71 59 C1 D0 BF 8F 92
52 D4 1A C0 66 BF 78 E7 BF 52 AD 81 D2 94 06 6D FC

Extension: 2.16.840.1.113730.1.1

Critical: 0

Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)

Critical: 1

Key Usage: Digital Signature, Non Repudiation, Key Encipherment

Extension: Subject Key Identifier (2.5.29.14)

Critical: 0

Subject Key Identifier: 2D 41 57 82 F4 52 C0 8C 55 93 1B 08 A4 4A 4A AF CD 8E C9 4C

Extension: Authority Key Identifier (2.5.29.35)

Critical: 0

Key Identifier: D1 BD EE D7 E1 92 1C E6 52 9B 69 91 A7 65 F2 14 AC 1C 4F 92

Extension: Extended Key Usage (2.5.29.37)

Critical: 0

Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)

Fingerprints :

SHA-256 Fingerprint: DE 03 B6 9F 31 4E 09 3D FC 51 5A 34 38 03 DB 67 F8 F3 9E C7
85 EE 9E B5 14 AA A4 D4 94 6E 44 BF

SHA-1 Fingerprint: 61 3C B5 33 32 4C 03 FA 40 9C 20 A2 91 5F CF 3E 55 2F E7 C7

MD5 Fingerprint: 4D 89 67 08 47 7C 92 89 9B 36 07 78 54 40 7E F1

PEM certificate :

-----BEGIN CERTIFICATE-----

MIIIEjCCAvqgAwIBAgIDAIEQMA0GCSqGSIb3DQEBCwUAMIGdMRwwGgYDVQQKDBNOZXNzdXMgVXNlcnMgVW5pdGVkMScwJQYDVQQLDB50ZXNzdXMgQ2VydGlmawNhgdGlvbIBBdXRob3JpdhKxETAPBgNVBAcMCE5ldyBzb3JrMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTlkxJzAlBgNVBAMMk5lc3N1cyBDZXJ0awZpY2F0aw9uIEF1dGhvcml0eTAeFw0yNDA1MTcxNTMzMzJaFw0y0DA1MTYxNTMzMzJaMH0xHDAaBgNVBAoME05lc3N1cyBvC2VycyBvbml0ZWQxFjAUBgNVBAsMDU5lc3N1cyBTZXJ2ZXIxETAPBgNVBAcMCE5ldyBzb3JrMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTlkxGDAwBgNVBAMMD0RFU0tUT1AtRkxIUEpQUTCCASIwDQYJKoIhvcNAQEBBQADggEPADCCAQoCggEBALFGWBhedr5TtZJP/lz3HPF57bQx12q4Y2Y6vENSZT2LCRxFqA1r+JotIBlwZI9qh/9wClN314N83Npv+EEBr4trdj7N20aYu7AqRz/Su67paUf4dp8LXefSlQTKeC1gzPMY5gL2jhSi7L0NVubfyHGjZKhgBtMJTRm5h99NRBKu7C47NcTUzyjRgJlGS08foC1jBX2LgGLZTE0cUiBIQSqa+8Ky35r+2McUPGw48HTTaJ6DcEjURL0DA4pDaLTPVAiSXZt/hUGPzKcVRl179CVfqvpqgtisim9370uNnpTLhtCk30+FBj77PqlJ5D8QaG4ohW6or75064hW40CGdjYECAwEAAaN6MHgwEQYJYIZIAyb40gEBBAQDAgZAMA4GA1UdDwEB/wQEAwIF4DAdBgNVHQ4EFgQULUFXgvRSwIXVkxsIpEpKr820yUuwHwYDVR0BwgFoA0b3u1+GSH0ZSm2mRp2XyFKwct5IwEYDVROLBawCgYIKwYBBQUH AwEwDQYJKoZIhvvcNAQELBQAQDggEBAC4qdZepxvfCQyiy0ucGN+MxmfpkaJD/fhry1zvu1YpFzWxocbU+X1k78itbfVlqz2h8vpvti8rCrWfwYY6UKaSuoftAi/2DalmUB23pHvQLGMBtVFxFmjQVr1W8Kp8idU6K5uhJLPgwatYdIkea9JcEUv16Szg/_0gF0f1/pPL/q0P6LnuJ0qEjuP5YKXPA0ZHjVK+lltFgK9qmZi1++mphhwtsAG1REy0clY0YtfKmYtP3eh8ZQ8n1lN95fbwmgWjqgHkpUbxxT2FEL7XpJvT0vqkJxmTGAmCgYtHdLBcfQX603PmcJ3p5JxWchQv4+SutQawGa/e0e/Uq2B0pQGbfw=

-----END CERTIFICATE-----

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html>
<http://www.nessus.org/u?e17ffced>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2023/07/10

Plugin Output

tcp/8834/www

Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

TLS_AES_128_GCM_SHA256 0x13, 0x01 - - AES-GCM(128) AEAD
TLS_AES_256_GCM_SHA384 0x13, 0x02 - - AES-GCM(256) AEAD
TLS_CHACHA20_POLY1305_SHA256 0x13, 0x03 - - ChaCha20-Poly1305(256) AEAD

SSL Version : TLSv12
High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8834/www

Here is the list of SSL PFS ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)

Name Code KEX Auth Encryption MAC

ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384

The fields above are :

{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}

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/8834/www

A TLSv1.2 server answered on this port.

tcp/8834/www

A web server is running on this port through TLSv1.2.

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

<http://www.nessus.org/u?2fb3aca6>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

The STS header line is :

Strict-Transport-Security: max-age=31536000

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

<https://tools.ietf.org/html/rfc5246>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8834/www

TLSv1.2 is enabled and the server supports at least one cipher.

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

<https://tools.ietf.org/html/rfc8446>

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

TLSv1.3 is enabled and the server supports at least one cipher.

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: 2024/04/19

Plugin Output

tcp/0

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

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 vulnerabilities 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: 2024/05/06

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

tcp/445/cifs

The following 2 NetBIOS names have been gathered :

DESKTOP-FLHPJPQ = Computer name
DESKTOP-FLHPJPQ = Workgroup / Domain name

192.168.100.105



Host Information

Netbios Name: LAPTOP-EHBLJCJ73
IP: 192.168.100.105
MAC Address: 7C:B2:7D:22:D2:A6
OS: Microsoft Windows 10

Vulnerabilities

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:O/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: 2024/04/23

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_10 -> Microsoft Windows 10 64-bit

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 : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service

Named pipe : samss lpc

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : lsapolICYlookup

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

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 : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 6c637067-6569-746e-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-0f335ba41bcb9a7c51

Object UUID : 24d1f7c7-76af-4f28-9cccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Annotation : Group Policy RPC Interface
Type : Local RPC service
Named pipe : LRPC-ala934b66ea1680d58

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : cc105610-da03-467e-bc73-5b9e2937458d, version 1.0
Description : Unknown RPC service
Annotation : LiveIdSvc RPC Interface
Type : Local RPC service
Named pipe : LRPC-66b5b42658d5385b79

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : faf2447b-b348-4feb-8dbe-beeee5b7f7778, version 1.0
Description : Unknown RPC service
Annotation : OnlineProviderCert RPC Interface
Type : Local RPC service
Named pipe : LRPC-66b5b42658d5385b79

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 572e35b4-1344-4565-96a1-f5df3bfa89bb, version 1.0
Description : Unknown RPC service
Annotation : LiveIdSvcNotify RPC Interface

Type : Local RPC service
Named pipe : liveidsvcnotify

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8eefaa2e8-d033-4a08-a484-139c0b09371d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : GenericMessagingAddin.a25f7075798e4468b721ac8e31f6c7d8

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8eefaa2e8-d033-4a08-a484-139c0b09371d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : DeviceSettingsSystemAddin.e54395024c7f4af993775c2768e00e5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8eefaa2e8-d033-4a08-a484-139c0b09371d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : VantageCoreAddin.addb563ac1be4c0a949e87a5a11b8f92

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8eefaa2e8-d033-4a08-a484-139c0b09371d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE71F492C782CE0A0E98DD56982FC0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8eefaa2e8-d033-4a08-a484-139c0b09371d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : 8EEFA2E8-D033-4A08-A484-139C0B09371D

Object UUID : 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57
UUID : 8c7daf44-b6dc-11d1-9a4c-0020af6e7c57, version 1.0
Description : Application Management service
Windows process : svchost.exe
Annotation : Group Policy RPC Interface
Type : Local RPC service
Named pipe : LRPC-6b5dcb224d20f85da1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c503f532-443a-4c69-8300-ccdf1fbdb3839, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3B1800B317CF263798C9808C8E3A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c503f532-443a-4c69-8300-ccdf1fbdb3839, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-48f50e8ae3dd2ed8d2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bf4dc912-e52f-4904-8ebe-9317c1bdd497, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE76AAEAE3EEABFC76B5D5B4C5C0F18

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bf4dc912-e52f-4904-8ebe-9317c1bdd497, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-bd977607c2c9c40c1f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a4b8d482-80ce-40d6-934d-b22a01a44fe7, version 1.0
Description : Unknown RPC service
Annotation : LicenseManager
Type : Local RPC service
Named pipe : LicenseServiceEndpoint

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0497b57d-2e66-424f-a0c6-157cd5d41700, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-9bf126991256b0b9c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12ala, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-9bf126991256b0b9c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo

Type : Local RPC service
Named pipe : LRPC-9bfc126991256b0b9c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-9bfc126991256b0b9c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : LRPC-9bfc126991256b0b9c

Object UUID : ccb8aa07-7225-4ea0-8501-4b3c1b1acd43
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5E5F0BC5B5D6F2C7E0B6C6067351

Object UUID : ccb8aa07-7225-4ea0-8501-4b3c1b1acd43
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-abf70b41d096312699

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE5E5F0BC5B5D6F2C7E0B6C6067351

Object UUID : 582a47b2-bcd8-4d3c-8acb-fe09d5bd6eec
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-abf70b41d096312699

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 : OLEFB3E7611E59FD8858B55FD7FDB61

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 : LRPC-40b6e93cba0c649c93

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEFB3E7611E59FD8858B55FD7FDB61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0c53aa2e-fb1c-49c5-bfb6-c54f8e5857cd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-40b6e93cba0c649c93

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 923c9623-db7f-4b34-9e6d-e86580f8ca2a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEFB3E7611E59FD8858B55FD7FDB61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 923c9623-db7f-4b34-9e6d-e86580f8ca2a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-40b6e93cba0c649c93

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e8748f69-a2a4-40df-9366-62dbeb696e26, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEFB3E7611E59FD8858B55FD7FDB61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e8748f69-a2a4-40df-9366-62dbeb696e26, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-40b6e93cba0c649c93

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

UUID : c8ba73d2-3d55-429c-8e9a-c44f006f69fc, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEFB3E7611E59FD8858B55FD7FDB61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c8ba73d2-3d55-429c-8e9a-c44f006f69fc, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-40b6e93cba0c649c93

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 43890c94-bfd7-4655-ad6a-b4a68397cdcb, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEFB3E7611E59FD8858B55FD7FDB61

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 43890c94-bfd7-4655-ad6a-b4a68397cdcb, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-40b6e93cba0c649c93

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLE5561941809416F15015D13F42367

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : LRPC-61439430ea88247823

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7a20fce4-dec4-4c59-be57-212e8f65d3de, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-fed161b3bf14bf43a3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : be6293d3-2827-4dda-8057-8588240124c9, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-547381b1da17e9330b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 54b4c689-969a-476f-8dc2-990885e9f562, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-547381b1da17e9330b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d04ad7e1-b4a8-48e8-837f-a375e9ca8787, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : AesmRpcEndpoint

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30034843-029d-46ec-8fff-5d12987f85c4, version 1.0
Description : Unknown RPC service
Annotation : INgcProvisioningHandler
Type : Local RPC service
Named pipe : LRPC-792cbae282f3c0183a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bef2320-f308-4720-b913-0129cecfa6b9, version 1.0
Description : Unknown RPC service
Annotation : IVscProvisioningHandler
Type : Local RPC service
Named pipe : LRPC-792cbae282f3c0183a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d24ff0b-1bab-404c-a0fd-42c85577bf68, version 1.0
Description : Unknown RPC service
Annotation : INgcHandler
Type : Local RPC service
Named pipe : LRPC-792cbae282f3c0183a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7642249b-84c2-4404-b6eb-1e0a2458839a, version 1.0
Description : Unknown RPC service
Annotation : INgcSecureBioHandler
Type : Local RPC service
Named pipe : LRPC-792cbae282f3c0183a

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

UUID : e6f89680-fc98-11e3-80d4-10604b681cfa, version 1.0
Description : Unknown RPC service
Annotation : INgcGidsHandler
Type : Local RPC service
Named pipe : LRPC-792cbae282f3c0183a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0e3ae095-8a23-48f4-9782-03c1594a890e, version 1.0
Description : Unknown RPC service
Annotation : NGC Service KSP RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c225e799-29de-42af-bc05-1e2127cc056e, version 1.0
Description : Unknown RPC service
Annotation : NGC Service Management RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d9844ed9-f72a-4745-a4a1-ee71f950781d, version 1.0
Description : Unknown RPC service
Annotation : NGC Service Silent Management RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2b70bed6-1757-4d22-9f39-448589fbef5, version 1.0
Description : Unknown RPC service
Annotation : NGC Service Ticket RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9cbc9d3a-7586-4814-8d70-18737dcbe523, version 1.0
Description : Unknown RPC service
Annotation : NGC Service LocalAccount Vault Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4e25f4a2-21e8-40ce-b401-32050413143a, version 1.0
Description : Unknown RPC service
Annotation : Device Credential RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd6b7e61-2bed-4d48-a267-d746fe449fed, version 1.0
Description : Unknown RPC service
Annotation : Device Credential Presence RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8337aebc-5564-46fd-bc41-7798f18d2e4b, version 1.0
Description : Unknown RPC service
Annotation : Device Credential Manager RPC Interface
Type : Local RPC service
Named pipe : LRPC-5acd489b7be7e4adef

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF6E09459E1FED5C2A8D7D60C8775

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 8ec21e98-b5ce-4916-a3d6-449fa428a007, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9e2da0aeb0ab3ea113

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF6E09459E1FED5C2A8D7D60C8775

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : 0fc77b1a-95d8-4a2e-a0c0-cff54237462b, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9e2da0aeb0ab3ea113

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : b1ef227e-dfa5-421e-82bb-67a6a129c496, version 0.0
Description : Unknown RPC service
Type : Local RPC service

Named pipe : OLEF6E09459E1FED5C2A8D7D60C8775

Object UUID : 00000001-0000-0000-0000-000000000000
UUID : b1ef227e-dfa5-421e-82bb-67a6a129c496, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-9e2da0aeb0ab3ea113

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : LRPC-3e4b784781a36d8adb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 11c6212d-d5f3-4500-ab16-634dc63037be, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE47E712E9010104C4C918F050D417

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 11c6212d-d5f3-4500-ab16-634dc63037be, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : DaxRpcEndpoint

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7df1ceae-de4e-4e6f-ab14-49636e7c2052, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-cd589cb4fe64a5fdc2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d4051bde-9cdd-4910-b393-4aa85ec3c482, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d4051bde-9cdd-4910-b393-4aa85ec3c482, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2e1ecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c9dbf19-d39e-4bb9-90ee-8f7179b20283, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c9dbf19-d39e-4bb9-90ee-8f7179b20283, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2e1ecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2e1ecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95095ec8-32ea-4eb0-a3e2-041f97b36168, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95095ec8-32ea-4eb0-a3e2-041f97b36168, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2e1ecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e38f5360-8572-473e-b696-1b46873beeab, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e38f5360-8572-473e-b696-1b46873beeab, version 1.0
Description : Unknown RPC service

Type : Local RPC service
Named pipe : LRPC-b2elecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d22895ef-aff4-42c5-a5b2-b14466d34ab4, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : d22895ef-aff4-42c5-a5b2-b14466d34ab4, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2elecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98cd761e-e77d-41c8-a3c0-0fb756d90ec2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98cd761e-e77d-41c8-a3c0-0fb756d90ec2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2elecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1d45e083-478f-437c-9618-3594ced8c235, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEE4BB4B9D5CC5591FDD3610CD0137

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1d45e083-478f-437c-9618-3594ced8c235, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b2elecef3ed791e9e1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c27f3c08-92ba-478c-b446-b419c4cef0e2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-3e961a7fcfcee3562a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae2dc901-312d-41df-8b79-e835e63db874, version 1.0
Description : Unknown RPC service
Annotation : appxsvc
Type : Local RPC service
Named pipe : LRPC-ec7e85663bd03f0f2c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ff9fd3c4-742e-45e0-91dd-2f5bc632a1df, version 1.0
Description : Unknown RPC service
Annotation : appxsvc
Type : Local RPC service
Named pipe : LRPC-ec7e85663bd03f0f2c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : RasmanLrpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : VpnikeRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Local RPC service
Named pipe : LRPC-acbc71ee4d0d7339dd

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 714dc5c4-c5f6-466a-b037-a573c958031e, version 1.0
Description : Unknown RPC service
Annotation : ProcessTag Server Endpoint
Type : Local RPC service
Named pipe : OLE4EC8B279320BAD25E63E663A16C4

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 714dc5c4-c5f6-466a-b037-a573c958031e, version 1.0
Description : Unknown RPC service

Annotation : ProcessTag Server Endpoint
Type : Local RPC service
Named pipe : LRPC-79c2ddfe5130f20703

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : LRPC-90a07c422a01b54173

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1.0
Description : Unknown RPC service
Annotation : IdSegSrv service
Type : Local RPC service
Named pipe : LRPC-90a07c422a01b54173

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 : Local RPC service
Named pipe : LRPC-56a30a99afed56ff2f

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 : Local RPC service
Named pipe : LRPC-56a30a99afed56ff2f

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 : Local RPC service
Named pipe : TeredoDiagnostics

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 : Local RPC service
Named pipe : TeredoControl

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 : Local RPC service
Named pipe : LRPC-56a30a99afed56ff2f

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 : Local RPC service
Named pipe : TeredoDiagnostics

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 : Local RPC service
Named pipe : TeredoControl

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : LRPC-56a30a99afed56ff2f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : TeredoDiagnostics

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : TeredoControl

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0

Description : Unknown RPC service
Annotation : Adh APIs
Type : Local RPC service
Named pipe : OLE36AD5CAD1FF766E9F90B3BF0DC11

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 : Local RPC service
Named pipe : LRPC-43226a5b10e0d773b3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 944be8cf-bd2b-46e4-90a9-2b947b152a6d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : HsaSampleRpcEndpoint

Object UUID : bae10e73-0001-0000-9dab-7d0f635c171a
UUID : 509bc7ae-77be-4ee8-b07c-0d096bb44345, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEA5F77C5DDFE206AF7F386F9C2C52

Object UUID : bae10e73-0001-0000-9dab-7d0f635c171a
UUID : 509bc7ae-77be-4ee8-b07c-0d096bb44345, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-117e8eb1467288192a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-8d7574969c92c1d1f0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-8d7574969c92c1d1f0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-16472efee621532e29

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-8d7574969c92c1d1f0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-16472efee621532e29

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f47433c3-3e9d-4157-aad4-83aa1f5c2d4c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-597f4f64ce2cf2203b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-8d7574969c92c1d1f0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-16472efee621532e29

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs

Type : Local RPC service
Named pipe : LRPC-597f4f64ce2cf2203b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-2fdf12ba2115514481

Object UUID : d1382b90-d093-4d55-a33f-0d2344c81f77
UUID : 98e96949-bc59-47f1-92d1-8c25b46f85c7, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-d1cb231fd011a62830

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f2c9b409-c1c9-4100-8639-d8ab1486694a, version 1.0
Description : Unknown RPC service
Annotation : Witness Client Upcall Server
Type : Local RPC service
Named pipe : LRPC-fd4af39ce7413ab980

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : eb081a0d-10ee-478a-a1dd-50995283e7a8, version 3.0
Description : Unknown RPC service
Annotation : Witness Client Test Interface
Type : Local RPC service
Named pipe : LRPC-fd4af39ce7413ab980

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Local RPC service
Named pipe : LRPC-fd4af39ce7413ab980

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 25952c5d-7976-4aa1-a3cb-c35f7ae79d1b, version 1.0
Description : Unknown RPC service
Annotation : Wireless Diagnostics
Type : Local RPC service
Named pipe : LRPC-5d0d6b92b02e70f981

Object UUID : 6e616c77-7673-0063-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-5d0d6b92b02e70f981

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214ea9, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service
Type : Local RPC service
Named pipe : LRPC-5d0d6b92b02e70f981

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214ea9, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service
Type : Local RPC service
Named pipe : LRPC-0d01d353b677a10d9a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214eb0, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service LowPriv
Type : Local RPC service
Named pipe : LRPC-5d0d6b92b02e70f981

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 266f33b4-c7c1-4bd1-8f52-ddb8f2214eb0, version 1.0
Description : Unknown RPC service
Annotation : Wlan Service LowPriv
Type : Local RPC service
Named pipe : LRPC-0d01d353b677a10d9a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-5d0d6b92b02e70f981

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service

Named pipe : LRPC-0d01d353b677a10d9a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE9423F3C9C131456D9E6060ABF8CF

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : af7fead8-c34a-461f-8894-6d6f0e5eddcd, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f53e4ecaba6f3833c0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c3f42c6e-d4cc-4e5a-938b-9c5e8a5d8c2e, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-5d0d6b92b02e70f981

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c3f42c6e-d4cc-4e5a-938b-9c5e8a5d8c2e, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-0d01d353b677a10d9a

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c3f42c6e-d4cc-4e5a-938b-9c5e8a5d8c2e, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : OLE9423F3C9C131456D9E6060ABF8CF

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c3f42c6e-d4cc-4e5a-938b-9c5e8a5d8c2e, version 1.0
Description : Unknown RPC service
Annotation : IhvExtRpcServer
Type : Local RPC service
Named pipe : LRPC-f53e4ecaba6f3833c0

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 : Local RPC service
Named pipe : LRPC-c37e3be0176d91642c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c37e3be0176d91642c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c37e3be0176d91642c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c37e3be0176d91642c

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c37e3be0176d91642c

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-f6720cccebb5c23d77

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF8781E6516A0246F15720D408CC3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1.0
Description : Unknown RPC service
Type : Local RPC service

Named pipe : LRPC-eec85de43911e6c568

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b37f900a-eae4-4304-a2ab-12bb668c0188, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF8781E6516A0246F15720D408CC3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b37f900a-eae4-4304-a2ab-12bb668c0188, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eec85de43911e6c568

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e7f76134-9ef5-4949-a2d6-3368cc0988f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF8781E6516A0246F15720D408CC3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e7f76134-9ef5-4949-a2d6-3368cc0988f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eec85de43911e6c568

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7aeb6705-3ae6-471a-882d-f39c109edc12, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF8781E6516A0246F15720D408CC3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7aeb6705-3ae6-471a-882d-f39c109edc12, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eec85de43911e6c568

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f44e62af-dab1-44c2-8013-049a9de417d6, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF8781E6516A0246F15720D408CC3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f44e62af-dab1-44c2-8013-049a9de417d6, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eec85de43911e6c568

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c2d1b5dd-fa81-4460-9dd6-e7658b85454b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF8781E6516A0246F15720D408CC3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c2d1b5dd-fa81-4460-9dd6-e7658b85454b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-eec85de43911e6c568

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-cb7ad9c18b984dd570

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : a167c71c-cea5-4772-8b2f-ad89e15b6009

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-bb6e13e6e04c2c1a8f

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : OLE9AD609B75FC72A2400A3EA25F260

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

UUID : b18fbab6-56f8-4702-84e0-41053293a869, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : LRPC-725f8438f2218902e5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : OLE9AD609B75FC72A2400A3EA25F260

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1.0
Description : Unknown RPC service
Annotation : UserMgrCli
Type : Local RPC service
Named pipe : LRPC-725f8438f2218902e5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : nlaplg

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4c8d0bef-d7f1-49f0-9102-caa05f58d114, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : nlaapi

Object UUID : 314c8427-4ad7-4233-995a-bbd062ed11e9
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-afa4623c380fa020b5

Object UUID : 9575918f-89b5-49cd-9307-f9fc0d9a5b05
UUID : ba4aa15a-be94-47fb-9fb-fef110e7efad, version 1.0
Description : Unknown RPC service
Annotation : DevQueryBroker client query RPC interface
Type : Local RPC service
Named pipe : LRPC-7b524286986f8506d7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-f9305d65dbc406ae2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-f9305d65dbc406ae2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : LRPC-f9305d65dbc406ae2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f9305d65dbc406ae2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-21a18e66d3e051e059

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f9305d65dbc406ae2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-21a18e66d3e051e059

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f9305d65dbc406ae2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : ubpmtaskhostchannel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-21a18e66d3e051e059

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

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 : Local RPC service
Named pipe : DNSResolver

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 : Local RPC service
Named pipe : LRPC-adalb94621381f678c

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 : Local RPC service
Named pipe : dhcpcsvc6

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 : Local RPC service
Named pipe : dhcpcsvc6

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 : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 49541cea-a719-4e75-8d58-a3a7bfff960e
UUID : 850cee52-3038-4277-b9b4-e05db8b2c35c, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Association RPC Interface
Type : Local RPC service
Named pipe : LRPC-eb8f35e04cda735e39

Object UUID : 80b4038a-1d09-4c05-b1b6-249a4c2e0736
UUID : a1d4eae7-39f8-4bca-8e72-832767f5082a, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Inbound RPC Interface
Type : Local RPC service
Named pipe : LRPC-eb8f35e04cda735e39

Object UUID : 145857ef-d848-4a7e-b544-c1984d26cf05
UUID : 2e7d4935-59d2-4312-a2c8-41900aa5495f, version 1.0

Description : Unknown RPC service
Annotation : Device Association Framework Challenge RPC Interface
Type : Local RPC service
Named pipe : LRPC-eb8f35e04cda735e39

Object UUID : 289e5e0f-414a-4de9-8d17-244507fffc07
UUID : bd84cd86-9825-4376-813d-334c543f89b1, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework Query RPC Interface
Type : Local RPC service
Named pipe : LRPC-eb8f35e04cda735e39

Object UUID : 1475c123-1193-4379-81ac-302c4383421d
UUID : 5b665b9a-a086-4e26-ae24-96ab050b0ec3, version 1.0
Description : Unknown RPC service
Annotation : Device Association Framework AEP Store Access RPC Interface
Type : Local RPC service
Named pipe : LRPC-eb8f35e04cda735e39

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-3e09fbfb689b87b20b

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 : Local RPC service
Named pipe : eventlog

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-4f9386e5bd846ebea1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a69816f5-83b6-4d48-8633-067f99f5f2d3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4a105f1ec4cdc0c4f1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4a105f1ec4cdc0c4f1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b54e9aa3-cf29-4f21-a8ea-98c5850ce296, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a2d59684b00add0743

Object UUID : b5cccd5ef-4238-440b-bba0-999f828f1cfe
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6ebf0623bf3a49ae80

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6ebf0623bf3a49ae80

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-6f14ae792e2471716c

Object UUID : fdd099c6-df06-4904-83b4-a87a27903c70
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-be66fdf4d6c6b28365

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

UUID : 5222821f-d5e2-4885-84f1-5f6185a0ec41, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-4775ae9c99e562cbba

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-be66fdf4d6c6b28365

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : OLEFF26CFF8D807887183BE63D81AE3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 880fd55e-43b9-11e0-b1a8-cf4edfd72085, version 1.0
Description : Unknown RPC service
Annotation : KAPI Service endpoint
Type : Local RPC service
Named pipe : LRPC-0419706d412c197337

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e40f7b57-7a25-4cd3-a135-7f7d3df9d16b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-cfab5a721e7a7605cd

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 : WMsgKRpc019DB91

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 : WMsgKRpc019DB91

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-a9f5fb4560ee82107d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 085b0334-e454-4d91-9b8c-4134f9e793f3, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8782d3b9-ebbd-4644-a3d8-e8725381919b, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3b338d89-6cfa-44b8-847e-531531bc9992, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0361ae94-0316-4c6c-8ad8-c594375800e2, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd59071b-3215-4c59-8481-972edadc0f6a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd59071b-3215-4c59-8481-972edadc0f6a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2d98a740-581d-41b9-aa0d-a88b9d5ce938, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c605f9fb-f0a3-4e2a-a073-73560f8d9e3e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2513bcbe-6cd4-4348-855e-7efb3c336dd3, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 20c40295-8dba-48e6-aebf-3e78ef3bb144, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 55e6b932-1979-45d6-90c5-7f6270724112, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76c217bc-c8b4-4201-a745-373ad9032bla, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 88abcbc3-34ea-76ae-8215-767520655a23, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2c7fd9ce-e706-4b40-b412-953107ef9bb0, version 0.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c521facf-09a9-42c5-b155-72388595cbf0, version 0.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1832bcf6-cab8-41d4-85d2-c9410764f75a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4dace966-a243-4450-ae3f-9b7bcb5315b8, version 2.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 178d84be-9291-4994-82c6-3f909aca5a03, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e53d94ca-7464-4839-b044-09a2fb8b3ae5, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fae436b0-b864-4a87-9eda-298547cd82f2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 082a3471-31b6-422a-b931-a54401960c62, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6982a06e-5fe2-46b1-b39c-a2c545bfa069, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0ff1f646-13bb-400a-ab50-9a78f2b7a85a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4ed8abcc-f1e2-438b-981f-bb0e8abc010c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 95406f0b-b239-4318-91bb-cea3a46ff0dc, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0d47017b-b33b-46ad-9e18-fe96456c5078, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 7cd4a68a-505e-456b-b11e-ca76a5dd491c
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0c37e875591e48f49

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0c37e875591e48f49

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 9b008953-f195-4bf9-bde0-4471971e58ed, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a0ae21fd58d73643a3

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0c37e875591e48f49

Object UUID : db57eb61-1aa2-4906-9396-23e8b8024c32
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a0ae21fd58d73643a3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0c37e875591e48f49

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a0ae21fd58d73643a3

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 697dcda9-3ba9-4eb2-9247-e11f1901b0d2, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-515a63e43d07e823eb

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : umpo

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : actkernel

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-b6db363cfef45fefb5

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE6F4258A1D8A381B6881C131F61FD

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-c6f8c25c8ea8bf237d

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-f0c37e875591e48f49

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a0ae21fd58d73643a3

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-515a63e43d07e823eb

Object UUID : 9e56cbc5-e634-4267-818e-ffa7dce1fa86
UUID : d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : csepub

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 : umpo

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 : actkernel

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-b6db363cfef45fefb5

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 : OLE6F4258A1D8A381B6881C131F61FD

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-c6f8c25c8ea8bf237d

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-f0c37e875591e48f49

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-a0ae21fd58d73643a3

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-515a63e43d07e823eb

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 : csepub

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 : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0

Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc011F580

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 : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddbd0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc011F580

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddbd0, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

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 : audit

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 : securityevent

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 : LSARPC_ENDPOINT

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 : lsacap

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 : LSA_IDPEXT_ENDPOINT

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 : LSA_EAS_ENDPOINT

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 : lsapolICYlookup

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 : lsasspirpc

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 : protected_storage

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 : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-e000-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsapolICYlookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : audit

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 : Local RPC service
Named pipe : securityevent

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 : Local RPC service
Named pipe : LSARPC_ENDPOINT

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 : Local RPC service
Named pipe : lsacap

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 : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

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 : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

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 : Local RPC service
Named pipe : lsapolicylookup

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 : Local RPC service
Named pipe : lsasspirpc

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 : Local RPC service
Named pipe : protected_storage

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 : Local RPC service
Named pipe : SidKey Local End Point

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 : Local RPC service
Named pipe : samss lpc

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 : Local RPC service
Named pipe : audit

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 : Local RPC service
Named pipe : securityevent

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 : 00000000-0000-0000-0000-000000000000
UUID : 650a7e26-eab8-5533-ce43-9c1dfce11511, version 1.0
Description : Unknown RPC service
Annotation : Vpn APIs
Type : Remote RPC service
Named pipe : \PIPE\ROUTER
Netbios name : \\LAPTOP-EHBLJCJ73
```

```
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 : \\LAPTOP-EHBLJCJ73
```

```
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 : \\LAPTOP-EHBLJCJ73
```

```
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 : \\LAPTOP-EHBLJCJ73
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113bel, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LAPTOP-EHBLJCJ73
```

```
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 : \\LAPTOP-EHBLJCJ73
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LAPTOP-EHBLJCJ73
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fb8-9f8f-b89e2018337c, version 1.0
```

```
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\LAPTOP-EHBLJCJ73

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 : \\LAPTOP-EHBLJCJ73

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\LAPTOP-EHBLJCJ73

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 : \\LAPTOP-EHBLJCJ73

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
Named pipe : \pipe\lsass
Netbios name : \\LAPTOP-EHBLJCJ73

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191felb, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\LAPTOP-EHBLJCJ73

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
Named pipe : \pipe\lsass
Netbios name : \\LAPTOP-EHBLJCJ73
```

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/49664/dce-rpc

The following DCERPC services are available on TCP port 49664 :

```
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 : 49664
IP : 192.168.100.105

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 : 49664
IP : 192.168.100.105

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 : 49664
IP : 192.168.100.105

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 : 49664
IP : 192.168.100.105
```

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/49665/dce-rpc

The following DCERPC services are available on TCP port 49665 :

```
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84dalddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 192.168.100.105
```

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/49666/dce-rpc

The following DCERPC services are available on TCP port 49666 :

```
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 : 49666
IP : 192.168.100.105
```

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/49667/dce-rpc

The following DCERPC services are available on TCP port 49667 :

```
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 : 49667
IP : 192.168.100.105
```

```
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 : 49667
IP : 192.168.100.105
```

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/49668/dce-rpc

The following DCERPC services are available on TCP port 49668 :

```
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 : 49668
IP : 192.168.100.105

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 : 49668
IP : 192.168.100.105

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 : 49668
IP : 192.168.100.105

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 : 49668
IP : 192.168.100.105

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 : 49668
IP : 192.168.100.105
```

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/49672/dce-rpc

The following DCERPC services are available on TCP port 49672 :

```
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 : 49672
IP : 192.168.100.105
```

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 : unknown
Confidence level : 56
```

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 Organizational 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 :

7C:B2:7D:22:D2:A6 : Intel Corporate

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:

- 7C:B2:7D:22:D2:A6

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

192.168.100.105 resolves as LAPTOP-EHBLJCJ73.

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

Nessus was able to obtain the following information about the host, by parsing the SMB2 Protocol's NTLM SSP message:

Target Name: LAPTOP-EHBLJCJ73
NetBIOS Domain Name: LAPTOP-EHBLJCJ73
NetBIOS Computer Name: LAPTOP-EHBLJCJ73
DNS Domain Name: LAPTOP-EHBLJCJ73
DNS Computer Name: LAPTOP-EHBLJCJ73
DNS Tree Name: unknown
Product Version: 10.0.19041

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 :
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: 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

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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 213.851 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 19:07 Central European Standard Time
Scan duration : 572 sec
Scan for malware : no
```

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 10
Confidence level : 56
Method : MLSinFP
```

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.

```
SinFP:!:
P1:B11113:F0x12:W8192:00204ffff:M1460:
P2:B11113:F0x12:W8192:00204ffff0103030801010402:M1460:
P3:B00000:F0x00:W0:00:M0
P4:190803_7_p=139
```

The remote host is running Microsoft Windows 10

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.
```

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: 2024/04/19

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 192.168.100.104 to 192.168.100.105 :  
192.168.100.104  
192.168.100.105
```

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 vulnerabilities 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: 2024/05/06

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 3 NetBIOS names have been gathered :

LAPTOP-EHBLJCJ73 = File Server Service
LAPTOP-EHBLJCJ73 = Computer name
WORKGROUP = Workgroup / Domain name

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

7c:b2:7d:22:d2:a6

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

- mDNS hostname : LAPTOP-EHBLJCJ73.local.
- Advertised services :
 - o Service name : 1613728797._teamviewer._tcp.local.
- Port number : 2020

192.168.100.106

0

0

0

0

16

CRITICAL

HIGH

MEDIUM

LOW

INFO

Host Information

IP: 192.168.100.106
MAC Address: 28:56:5A:75:2A:D7

Vulnerabilities

11933 - Do not scan printers

Synopsis

The remote host appears to be a fragile device and will not be scanned.

Description

The remote host appears to be a network printer, multi-function device, or other fragile device. Such devices often react very poorly when scanned. To avoid problems, Nessus has marked the remote host as 'Dead' and will not scan it.

Solution

If you are not concerned about such behavior, enable the 'Scan Network Printers' setting under the 'Do not scan fragile devices' advanced settings block and re-run the scan. Or if using Nessus 6, enable 'Scan Network Printers' under 'Fragile Devices' in the Host Discovery section and then re-run the scan.

Risk Factor

None

References

XREF IAVB:0001-B-0525

Plugin Information

Published: 2003/12/01, Modified: 2024/04/08

Plugin Output

tcp/0

SNMP reports it as Brother NC.

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 4 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/21

Port 21/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

tcp/23

Port 23/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/69

Port 69/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/80

Port 80/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

tcp/443

Port 443/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

tcp/515

Port 515/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

tcp/631

Port 631/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/3702

Port 3702/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/5353

Port 5353/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/9100

Port 9100/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

tcp/54921

Port 54921/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 : 10.7.3
Nessus build : 20038
Plugin feed version : 202405171054
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Location A
Scan policy used : Basic Network Scan
Scanner IP : 192.168.100.104
Port scanner(s) : snmp_scanner
Port range : default
Ping RTT : 58.032 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
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 : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/17 19:09 Central European Standard Time
Scan duration : 26 sec
Scan for malware : no
```

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 2 NetBIOS names have been gathered :

BRW28565A752AD7 = Computer name
BRW28565A752AD7 = File Server Service

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

28:56:5a:75:2a:d7