



Nessus Meta Scan Basic With Credentials

Report generated by Nessus™

Wed, 02 Oct 2019 00:19:07 CDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.1.154.....4

Nessus Essentials

Vulnerabilities by Host

192.168.1.154

6

CRITICAL

1

HIGH

11

MEDIUM

4

LOW

150

INFO

Scan Information

Start time: Wed Oct 2 00:06:24 2019

End time: Wed Oct 2 00:19:06 2019

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.1.154

MAC Address: 00:50:56:9A:E4:4C

OS: Linux Kernel 2.6.24-16-server on Ubuntu 8.04

Vulnerabilities

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2019/05/10

Plugin Output

tcp/1524

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
```

```
----- snip -----
```

```
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
```

```
root@metasploitable:/#
```

```
----- snip -----
```

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

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

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

See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

Solution

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

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

tcp/22

Synopsis

The remote SSL certificate uses a weak key.

Description

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

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

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

See Also

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

Solution

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

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2018/11/15

Plugin Output

tcp/5432

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

Plugin Output

udp/2049

```
The following NFS shares could be mounted :
```

```
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- cdrom
```

- dev
- etc
- home
- initrd
- initrd.img
- lib
- lost+found
- media
- mnt
- nohup.out
- opt
- proc
- root
- sbin
- srv
- sys
- tmp
- usr
- var
- vmlinuz

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

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

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2008/08/08, Modified: 2019/09/13

Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).  
Upgrade to Ubuntu 18.10.
```

```
For more information, see : https://wiki.ubuntu.com/Releases
```

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS Base Score

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

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900

```
Nessus logged in using a password of "password".
```

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?b06c7e95>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

High

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)

CVSS Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2019/03/27

Plugin Output

tcp/5432

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

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

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
AES128-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
AES256-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
RC4-SHA	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

<http://www.apacheweek.com/issues/03-01-24>

<https://download.oracle.com/sunalerts/1000718.1.html>

Solution

Disable these methods. Refer to the plugin output for more information.

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 v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	9506
BID	9561
BID	11604
BID	33374

BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2019/03/27

Plugin Output

tcp/80

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive.

Nessus sent the following TRACE request :

```
----- snip -----
TRACE /Nessus1188076537.html HTTP/1.1
Connection: Close
Host: 192.168.1.154
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

```
----- snip -----
```

and received the following response from the remote server :

```
----- snip -----
HTTP/1.1 200 OK
Date: Wed, 02 Oct 2019 04:37:36 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE /Nessus1188076537.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.1.154
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
Accept-Language: en  
Accept-Charset: iso-8859-1,*,utf-8
```

```
----- snip -----
```

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Solution

Place the appropriate restrictions on all NFS shares.

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)

CVSS Base Score

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

Plugin Information

Published: 2009/10/26, Modified: 2019/07/16

Plugin Output

tcp/2049

```
The following shares have no access restrictions :  
  
/ *
```

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

<https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing>

<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 Base Score

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

CVSS Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/445

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

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

See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22

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

```
  arcfour
  arcfour128
  arcfour256
```

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

```
  arcfour
  arcfour128
  arcfour256
```

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 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 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2018/11/15

Plugin Output

tcp/5432

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain  
| -Not After  : Apr 16 14:07:45 2010 GMT
```

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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain  
| -Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain
```


Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

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 Base Score

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

Plugin Information

Published: 2004/12/03, Modified: 2019/03/13

Plugin Output

tcp/5432

The SSL certificate has already expired :

```
Subject      : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
Issuer       : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
Not valid before : Mar 17 14:07:45 2010 GMT
Not valid after  : Apr 16 14:07:45 2010 GMT
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

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 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/5432

```
The identities known by Nessus are :
```

```
192.168.1.154
192.168.1.154
```

```
The Common Name in the certificate is :
```

```
ubuntu804-base.localdomain
```

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)

CVSS 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: 2019/02/28

Plugin Output

tcp/5432

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

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

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 certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/5432

```
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=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	70574
CVE	CVE-2014-3566
XREF	CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2019/07/22

Plugin Output

tcp/5432

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2018/07/27

Plugin Output

tcp/445

Nessus detected that the Samba Badlock patch has not been applied.

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
```

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
blowfish-cbc  
cast128-cbc  
rijndael-cbc@lysator.liu.se
```

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
blowfish-cbc  
cast128-cbc  
rijndael-cbc@lysator.liu.se
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :
```

```
  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

```
The following server-to-client Message Authentication Code (MAC) algorithms
are supported :
```

```
  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

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

<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

Low

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)

CVSS Base Score

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

CVSS Temporal Score

2.2 (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: 2019/07/23

Plugin Output

tcp/5432

```
List of RC4 cipher suites supported by the remote server :
```

```
High Strength Ciphers (>= 112-bit key)
```

```
RC4-SHA          Kx=RSA      Au=RSA      Enc=RC4(128)      Mac=SHA1
```

```
The fields above are :
```

```
{OpenSSL ciphername}  
Kx={key exchange}  
Au={authentication}  
Enc={symmetric encryption method}  
Mac={message authentication code}  
{export flag}
```

10407 - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor

Low

CVSS Base Score

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

Plugin Information

Published: 2000/05/12, Modified: 2019/03/05

Plugin Output

tcp/6000

```
X11 Version : 11.0
```

Synopsis

There is an AJP connector listening on the remote host.

Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See Also

<http://tomcat.apache.org/connectors-doc/>

<http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/04/05, Modified: 2011/03/11

Plugin Output

tcp/8009

The connector listing on this port supports the ajp13 protocol.

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```
The Linux distribution detected was :  
- Ubuntu 8.04 (gutsy)
```

Synopsis

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

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2019/06/04

Plugin Output

tcp/80

```
URL      : http://192.168.1.154/
Version  : 2.2.99
backported : 1
modules  : DAV/2
os       : ConvertedUbuntu
```

Synopsis

The local security checks are disabled.

Description

Local security checks have been disabled for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Address the problem(s) so that local security checks are enabled.

Risk Factor

None

Plugin Information

Published: 2006/06/23, Modified: 2018/11/02

Plugin Output

tcp/0

The local checks failed because :

```
- Plugin      : ssh_get_info2.nasl
  Plugin ID   : 97993
  Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH
Library)
  Protocol    : SSH
  Message     : 'dpkg' did not return any result

- Plugin      : ssh_get_info.nasl
  Plugin ID   : 12634
  Plugin Name : Authenticated Check : OS Name and Installed Package Enumeration
  Message     :
Local security checks have not been enabled due to an error identified by ssh_get_info2.nasl
(97993).
```

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Nessus was able to execute credentialed checks because it was possible to log in to the remote host using provided credentials, no access or privilege issues were reported, and no subsequent failures were reported for the successful credentials.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/05/24, Modified: 2018/10/02

Plugin Output

tcp/22

```
Nessus was able to log in to the following host as msfadmin
with no privilege or access problems reported:
```

```
Protocol      : SSH
Port          : 22
```

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

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

Plugin Output

tcp/0

The remote operating system matched the following CPE :

```
cpe:/o:canonical:ubuntu_linux:8.04
```

Following application CPE's matched on the remote system :

```
cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8
cpe:/a:apache:http_server:2.2.99
cpe:/a:isc:bind:9.4.
cpe:/a:isc:bind:9.4.2 -> ISC BIND 9.4.2
cpe:/a:mysql:mysql:
cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH 4.7
cpe:/a:php:php:5.2.4 -> PHP 5.2.4
cpe:/a:php:php:5.2.4-2ubuntu5.10
cpe:/a:postgresql:postgresql:
cpe:/a:samba:samba:3.0.20 -> Samba 3.0.20
```


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

Plugin Information

Published: 1999/10/12, Modified: 2019/06/05

Plugin Output

udp/53

```
Version : 9.4.2
```

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

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

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2014/03/03, Modified: 2019/06/05

Plugin Output

udp/53

```
DNS server answer for "version.bind" (over UDP) :
```

```
9.4.2
```

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

```
The remote host name is :  
metasploitable
```

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 100
```

Synopsis

This plugin parses information from the nessusd.dump log file and reports on errors.

Description

This plugin parses information from the nessusd.dump log file and reports on errors.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/09/17, Modified: 2019/03/12

Plugin Output

tcp/0

The nessusd.dump log file contained errors from the following plugins:

- mysql_version.nasl reported 1 error
- netstat_portscan.nasl reported 1 error

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: 2018/11/15

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:9A:E4:4C : VMware, Inc.
```


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: 2018/08/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:50:56:9A:E4:4C
```

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/10/02

Plugin Output

tcp/21

```
The remote FTP banner is :  
  
220 (vsFTPd 2.3.4)
```

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

Plugin Information

Published: 2000/01/04, Modified: 2019/06/07

Plugin Output

tcp/80

```
The remote web server type is :  
Apache/2.2.8 (Ubuntu) DAV/2
```

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 and HTTP pipelining are enabled, etc...

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

Solution

[illegible]

None

Plugin Information

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

Response Code : HTTP/1.1 200 OK

```
Protocol version : HTTP/1.1
```

SSL : no

```
Keep-Alive : yes
```

Options allowed : (Not implemented)

Headers :

Date: Wed, 02 Oct 2019 04:38:04 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

```
Keep-Alive: timeout=15, max=100
```

Connection: Keep-Alive

Content-Type: text/html

Response Body :

```
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

[illegible]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

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

Solution

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

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/03/06

Plugin Output

icmp/0

```
The difference between the local and remote clocks is 2267 seconds.
```

Synopsis

It is possible to obtain network information.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2018/09/13

Plugin Output

tcp/445

```
Here is the browse list of the remote host :
```

```
METASPLOITABLE ( os : 0.0 )  
OWASPBWA ( os : 0.0 )
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

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

- NULL session
- Guest account
- Supplied credentials

See Also

<https://support.microsoft.com/en-us/help/143474/restricting-information-available-to-anonymous-logon-users>

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2018/11/15

Plugin Output

tcp/445

```
- NULL sessions are enabled on the remote host.
```


Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Unix  
The remote native LAN manager is : Samba 3.0.20-Debian  
The remote SMB Domain Name is : METASPLOITABLE
```

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: 2015/06/02

Plugin Output

tcp/139

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

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: 2015/06/02

Plugin Output

tcp/445

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

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: 2017/06/19

Plugin Output

tcp/445

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

Synopsis

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

Description

Nessus was able to obtain the set of SMB2 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: 2018/09/12

Plugin Output

tcp/445

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

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Solution

Ensure each share is intended to be exported.

Risk Factor

None

References

CVE CVE-1999-0554

Plugin Information

Published: 2000/06/07, Modified: 2018/11/01

Plugin Output

tcp/2049

```
Here is the export list of 192.168.1.154 :  
  
/ *
```

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: 2019/08/20

Plugin Output

tcp/21

```
Port 21/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: 2019/08/20

Plugin Output

tcp/22

```
Port 22/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: 2019/08/20

Plugin Output

tcp/23

```
Port 23/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: 2019/08/20

Plugin Output

tcp/25

```
Port 25/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: 2019/08/20

Plugin Output

tcp/53

```
Port 53/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: 2019/08/20

Plugin Output

tcp/80

```
Port 80/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: 2019/08/20

Plugin Output

tcp/111

```
Port 111/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: 2019/08/20

Plugin Output

tcp/139

```
Port 139/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: 2019/08/20

Plugin Output

tcp/445

```
Port 445/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: 2019/08/20

Plugin Output

tcp/512

```
Port 512/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: 2019/08/20

Plugin Output

tcp/513

```
Port 513/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: 2019/08/20

Plugin Output

tcp/514

```
Port 514/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: 2019/08/20

Plugin Output

tcp/1099

```
Port 1099/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: 2019/08/20

Plugin Output

tcp/1524

```
Port 1524/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: 2019/08/20

Plugin Output

tcp/2049

```
Port 2049/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: 2019/08/20

Plugin Output

tcp/2121

```
Port 2121/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: 2019/08/20

Plugin Output

tcp/3306

```
Port 3306/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: 2019/08/20

Plugin Output

tcp/3632

```
Port 3632/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: 2019/08/20

Plugin Output

tcp/5432

```
Port 5432/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: 2019/08/20

Plugin Output

tcp/5900

```
Port 5900/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: 2019/08/20

Plugin Output

tcp/6000

```
Port 6000/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: 2019/08/20

Plugin Output

tcp/6667

```
Port 6667/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: 2019/08/20

Plugin Output

tcp/8009

```
Port 8009/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: 2019/08/20

Plugin Output

tcp/8180

```
Port 8180/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: 2019/08/20

Plugin Output

tcp/8787

```
Port 8787/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.
- Whether credentialed or third-party patch management checks are possible.
- 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: 2019/03/06

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 8.7.1  
Plugin feed version : 201910010400  
Scanner edition used : Nessus Home  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.202  
Port scanner(s) : nessus_syn_scanner  
Port range : default  
Thorough tests : no  
Experimental tests : no  
Paranoia level : 1
```



```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2019/10/2 0:06 CDT
Scan duration : 739 sec
```

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: 2019/09/04

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6.24-16-server on Ubuntu 8.04
Confidence level : 100
Method : LinuxDistribution
```

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.

```
SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
uname:Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

SinFP:

```
P1:B10113:F0x12:W5840:00204ffff:M1460:
P2:B10113:F0x12:W5792:00204ffff0402080affffff4445414401030307:M1460:
P3:B10120:F0x04:W0:00:M0
P4:80701_7_p=8009
```

```
SMTP:!!220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!!i/CN:ubuntu804-base.localdomaini/O:OCOSAi/OU:Office for Complication of Otherwise Simple
Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
```

The remote host is running Linux Kernel 2.6.24-16-server on Ubuntu 8.04

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: 2019/08/21

Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'password' authentication.

The output of "uname -a" is :
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

The remote Debian system is :
lenny/sid

This is a Ubuntu system
Local security checks have been disabled because of the following
error :

sh_shell_handler [channel 0]: ERROR - unable to reach command end marker.
Command did not complete due to timeout or other error.
We are able to identify the remote host, but encountered an error.
Local security checks have NOT been enabled.

Runtime : 31.148853 seconds
```

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: 2018/11/15

Plugin Output

tcp/5432

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/08/04, Modified: 2019/06/19

Plugin Output

tcp/80

Nessus was able to identify the following PHP version information :

Version : 5.2.4-2ubuntu5.10
Source : X-Powered-By: PHP/5.2.4-2ubuntu5.10

Synopsis

The remote host is missing several patches.

Description

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2019/09/10

Plugin Output

tcp/0

```
. You need to take the following action :  
[ Samba Badlock Vulnerability (90509) ]  
+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
```

Synopsis

The remote service supports encrypting traffic.

Description

The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

<https://www.postgresql.org/docs/9.2/protocol-flow.html#AEN96066>

<https://www.postgresql.org/docs/9.2/protocol-message-formats.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/19, Modified: 2018/11/15

Plugin Output

tcp/5432

```
Here is the PostgreSQL's SSL certificate that Nessus
was able to collect after sending a pre-login packet :
```

```
----- snip -----
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```



```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
             7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
             73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
             D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
             8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
             98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
             00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

----- snip ----- [...]
```

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

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

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2007/09/14, Modified: 2019/06/27

Plugin Output

tcp/5432

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111

```
The following RPC services are available on TCP port 111 :  
- program: 100000 (portmapper), version: 2
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111

```
The following RPC services are available on UDP port 111 :  
- program: 100000 (portmapper), version: 2
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/2049

```
The following RPC services are available on TCP port 2049 :
```

- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/2049

```
The following RPC services are available on UDP port 2049 :
```

- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/35343

```
The following RPC services are available on TCP port 35343 :
```

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/35785

```
The following RPC services are available on UDP port 35785 :
```

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/50346

```
The following RPC services are available on TCP port 50346 :
```

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/51443

```
The following RPC services are available on TCP port 51443 :  
- program: 100024 (status), version: 1
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/58114

```
The following RPC services are available on UDP port 58114 :  
- program: 100024 (status), version: 1
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/59011

```
The following RPC services are available on UDP port 59011 :
```

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

References

CVE CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2014/02/19

Plugin Output

udp/111

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/21

```
Process ID   : 5095
Executable   : /usr/sbin/xinetd
Command line  : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/22

```
Process ID   : 4666
Executable  : /usr/sbin/sshd
Command line : /usr/sbin/sshd
```


Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/23

```
Process ID   : 5095
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/25

```
Process ID   : 5032
Executable  : /usr/lib/postfix/master
Command line : /usr/lib/postfix/master
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/53

```
Process ID   : 4644
Executable  : /usr/sbin/named
Command line : /usr/sbin/named -u bind
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/53

```
Process ID   : 4644
Executable   : /usr/sbin/named
Command line  : /usr/sbin/named -u bind
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/69

```
Process ID   : 5095
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/80

```
Process ID   : 5176
Executable  : /usr/sbin/apache2
Command line : /usr/sbin/apache2 -k start
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/111

```
Process ID   : 4261
Executable   : /sbin/portmap
Command line  : /sbin/portmap
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/111

```
Process ID   : 4261
Executable  : /sbin/portmap
Command line : /sbin/portmap
```


Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/137

```
Process ID   : 5039
Executable  : /usr/sbin/nmbd
Command line : /usr/sbin/nmbd -D
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/138

```
Process ID   : 5039
Executable  : /usr/sbin/nmbd
Command line : /usr/sbin/nmbd -D
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/139

```
Process ID   : 5041
Executable   : /usr/sbin/smbd
Command line  : /usr/sbin/smbd -D
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/445

```
Process ID   : 5041
Executable   : /usr/sbin/smbd
Command line  : /usr/sbin/smbd -D
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/512

```
Process ID   : 5095
Executable  : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/513

```
Process ID   : 5095
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/514

```
Process ID   : 5095
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/637

```
Process ID   : 4277
Executable   : /sbin/rpc.statd
Command line : /sbin/rpc.statd
```


Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/1099

```
Process ID   : 5195
Executable   : /usr/bin/grmiregistry-4.2
Command line : /usr/bin/rmiregistry
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/1524

```
Process ID   : 5095
Executable   : /usr/sbin/xinetd
Command line : /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/2121

```
Process ID   : 9551
Executable  : /usr/sbin/proftpd
Command line : proftpd: (accepting connections)
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/3306

```
Process ID      : 4784
Executable     : /usr/sbin/mysqld
Command line    : /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/
var/run/mysqld/mysqld.pid --skip-external-locking --port=3306 --socket=/var/run/mysqld/mysqld.sock
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/3632

```
Process ID   : 4901
Executable   : /usr/bin/distccd
Command line : distccd --daemon --user daemon --allow 0.0.0.0/0
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/5432

```
Process ID   : 4884
Executable   : /usr/lib/postgresql/8.3/bin/postgres
Command line : /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c
config_file=/etc/postgresql/8.3/main/postgresql.conf
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/5900

```
Process ID      : 5215
Executable     : /usr/bin/Xtightvnc
Command line    : Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -
rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/
X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/
X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/6000

```
Process ID      : 5215
Executable     : /usr/bin/Xtightvnc
Command line    : Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -
rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/
X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/
X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/
X11/75dpi/,/usr/share/fonts/X11/100dpi/ -co /etc/X11/rgb
```


Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/6667

```
Process ID   : 5216
Executable   : /usr/bin/unrealircd
Command line : /usr/bin/unrealircd
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/6697

```
Process ID   : 5216
Executable  : /usr/bin/unrealircd
Command line : /usr/bin/unrealircd
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/8009

```
Process ID      : 5157
Executable     : /usr/bin/jsvc
Command line    : /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/
tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
-Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed
-Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/
var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/
catalina.policy org.apache.catalina.startup.Bootstrap
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/8180

```
Process ID      : 5157
Executable     : /usr/bin/jsvc
Command line   : /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/
tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid
-Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed
-Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/
var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/
catalina.policy org.apache.catalina.startup.Bootstrap
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/8787

```
Process ID   : 5199
Executable  : /usr/bin/ruby1.8
Command line : ruby /usr/sbin/druby_timeserver.rb
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/33707

```
Process ID   : 4277
Executable   : /sbin/rpc.statd
Command line : /sbin/rpc.statd
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/33839

```
Process ID   : 4644
Executable  : /usr/sbin/named
Command line : /usr/sbin/named -u bind
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/40135

```
Process ID   : 4277
Executable  : /sbin/rpc.statd
Command line : /sbin/rpc.statd
```


Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/44718

```
Process ID      : 5195
Executable     : /usr/bin/grmiregistry-4.2
Command line   : /usr/bin/rmiregistry
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/45233

```
Process ID   : 4644
Executable   : /usr/sbin/named
Command line  : /usr/sbin/named -u bind
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

udp/48656

```
Process ID   : 4964
Executable   : /usr/sbin/rpc.mountd
Command line : /usr/sbin/rpc.mountd
```

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/01/07

Plugin Output

tcp/52201

```
Process ID   : 4964
Executable  : /usr/sbin/rpc.mountd
Command line : /usr/sbin/rpc.mountd
```

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2011/03/11

Plugin Output

tcp/25

```
Remote SMTP server banner :  
  
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

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/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ssh-dss
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for encryption_algorithms_server_to_client :

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
```

The server supports the following options for compression_algorithms_client_to_server :

```
none
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none
zlib@openssh.com
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2019/05/28

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.99
- 2.0

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

Plugin Information

Published: 1999/10/12, Modified: 2019/01/08

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

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: 2019/03/01

Plugin Output

tcp/5432

```
This port supports SSLv3/TLSv1.0.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2019/06/25

Plugin Output

tcp/5432

```
The host name known by Nessus is :
```

```
metasploitable
```

```
The Common Name in the certificate is :
```

```
ubuntu804-base.localdomain
```

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: 2019/07/18

Plugin Output

tcp/5432

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
            0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
            1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
            68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
            83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
            A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
            15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                    83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

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: 2018/11/15

Plugin Output

tcp/5432

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

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

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
AES128-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
AES256-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1

The fields above are :

{OpenSSL ciphername}

```
Kx={key exchange}  
Au={authentication}  
Enc={symmetric encryption method}  
Mac={message authentication code}  
{export flag}
```

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2019/05/10

Plugin Output

tcp/5432

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

SSL Version : TLSv1

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

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(128)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
AES128-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
AES256-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
RC4-SHA	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1

SSL Version : SSLv3

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

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(128)	Mac=SHA1
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1

High Strength Ciphers (\geq 112-bit key)

DHE-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
AES128-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
AES256-SHA	Kx=RSA	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
RC4-SHA	Kx=RSA	Au=RSA	Enc=RC4(128)	Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Note that this service does not encrypt traffic by default but does support upgrading to an encrypted connection using STARTTLS.

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: 2018/02/15

Plugin Output

tcp/5432

```
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: 2018/11/15

Plugin Output

tcp/5432

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

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

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
----------------------	-------	--------	-------------------	----------

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES128-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA1
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1

The fields above are :

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
```

```
Mac={message authentication code}  
{export flag}
```

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/06/05

Plugin Output

tcp/445

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/11/30, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Samba Version is : Samba 3.0.20-Debian
```

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

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

See Also

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

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

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

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

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

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

Plugin Information

Published: 2017/02/03, Modified: 2018/11/15

Plugin Output

tcp/445

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

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: 2019/08/27

Plugin Output

tcp/21

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


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: 2019/08/27

Plugin Output

tcp/22

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

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: 2019/08/27

Plugin Output

tcp/23

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

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: 2019/08/27

Plugin Output

tcp/25

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

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: 2019/08/27

Plugin Output

tcp/80

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

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: 2019/08/27

Plugin Output

tcp/1524

```
A shell server (Metasploitable) is running on this port.
```

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: 2019/08/27

Plugin Output

tcp/5900

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

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/04/06, Modified: 2019/07/15

Plugin Output

tcp/6667

```
An IRC daemon is listening on this port.
```

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

tcp/3306

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


Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

Synopsis

A TFTP server is listening on the remote port.

Description

The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 2003/08/13, Modified: 2019/02/27

Plugin Output

udp/69

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 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

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.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information

Published: 2017/11/22, Modified: 2018/07/11

Plugin Output

tcp/5432

```
TLsv1 is enabled and the server supports at least one cipher.
```

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: 2019/03/06

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.202 to 192.168.1.154 :  
192.168.1.202  
192.168.1.154  
  
Hop Count: 1
```

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/07/24

Plugin Output

tcp/512

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :
```

```
Port      : 512
Type      : spontaneous
Banner    :
0x00:  01 57 68 65 72 65 20 61 72 65 20 79 6F 75 3F 0A    .Where are you?.
      0x10:
```

```
Nessus detected the following process listening on this port :
```

```
/usr/sbin/xinetd
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/07/24

Plugin Output

tcp/514

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org :

```
Port      : 514
Type      : spontaneous
Banner    :
0x00:  01 67 65 74 6E 61 6D 65 69 6E 66 6F 3A 20 54 65      .getnameinfo: Te
      0x10:  6D 70 6F 72 61 72 79 20 66 61 69 6C 75 72 65 20      mporary failure
      0x20:  69 6E 20 6E 61 6D 65 20 72 65 73 6F 6C 75 74 69      in name resoluti
      0x30:  6F 6E 0A                                           on.
```

Nessus detected the following process listening on this port :

```
/usr/sbin/xinetd
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/07/24

Plugin Output

tcp/8787

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org :

```
Port      : 8787
Type      : get_http
Banner    :
0x0000:  00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16      .....F.....O:
0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F      DRb::DRbConnErro
0x0020:  72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C      r.:.bt[."//usr/l
0x0030:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F      ib/ruby/1.8/drb/
0x0040:  64 72 62 2E 72 62 3A 35 37 33 3A 69 6E 20 60 6C      drb.rb:573:in `l
0x0050:  6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72      oad'"7/usr/lib/r
0x0060:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E      uby/1.8/drb/drb.
0x0070:  72 62 3A 36 31 32 3A 69 6E 20 60 72 65 63 76 5F      rb:612:in `recv_
0x0080:  72 65 71 75 65 73 74 27 22 37 2F 75 73 72 2F 6C      request'"7/usr/l
0x0090:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F      ib/ruby/1.8/drb/
0x00A0:  64 72 62 2E 72 62 3A 39 31 31 3A 69 6E 20 60 72      drb.rb:911:in `r
0x00B0:  65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75      ecv_request'"</u
0x00C0:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F      sr/lib/ruby/1.8/
0x00D0:  64 72 62 2F 64 72 62 2E 72 62 3A 31 35 33 30 3A      drb/drb.rb:1530:
0x00E0:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C      in `init_with_cl
0x00F0:  69 65 6E 74 27 22 39 2F 75 73 72 2F 6C 69 62 2F      ient'"9/usr/lib/
0x0100:  72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62      ruby/1.8/drb/drb
0x0110:  2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74      .rb:1542:in `set
0x0120:  75 70 5F 6D 65 73 73 61 67 65 27 22 33 2F 75 73      up_message'"3/us
0x0130:  72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64      r/lib/ruby/1.8/d
0x0140:  72 62 2F 64 72 62 2E 72 62 3A 31 34 39 34  [...]  [...]
```

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/09/25

Plugin Output

tcp/0

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


19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/07/22, Modified: 2014/03/12

Plugin Output

tcp/5900

```
The remote VNC server chose security type #2 (VNC authentication)
```

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900

```
The remote VNC server supports the following security type  
which does not perform full data communication encryption :
```

```
2 (VNC authentication)
```

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

<https://en.wikipedia.org/wiki/Vnc>

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900

```
The highest RFB protocol version supported by the server is :  
3.3
```

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.

It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

<http://support.microsoft.com/default.aspx?kbid=241520>

Risk Factor

None

Plugin Information

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/80

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: 2019/05/31

Plugin Output

udp/137

The following 7 NetBIOS names have been gathered :

METASPLOITABLE	= Computer name
METASPLOITABLE	= Messenger Service
METASPLOITABLE	= File Server Service
__MSBROWSE__	= Master Browser
WORKGROUP	= Workgroup / Domain name
WORKGROUP	= Master Browser
WORKGROUP	= Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

<http://vsftpd.beasts.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/09/25

Plugin Output

tcp/21

```
Source  : 220 (vsFTPd 2.3.4)
Version : 2.3.4
```