Nessus Report

Nessus Scan Report

Sat, 09 Dec 2017 14:28:52 EET

Table Of Contents

Vulnerabilities By Host

192.168.10.1

Scan Information

Start time:	Sat Dec 9 13:09:35 2017
End time:	Sat Dec 9 13:17:16 2017

Host Information

IP:	192.168.10.1
MAC Address:	00:50:56:01:2a:23
OS:	FreeBSD 10.3-RELEASE-p16 (amd64)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	32	35

Results Details

0/icmp

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	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 370 seconds.
```

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : FreeBSD 10.3-RELEASE-p16 (amd64)
Confidence level : 98
Method : NTP


The remote host is running FreeBSD 10.3-RELEASE-p16 (amd64)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
```

```
Scan Start Date : 2017/12/9 13:10 EET
Scan duration : 433 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```

The following card manufacturers were identified :

00:50:56:01:2a:23 : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:freebsd:freebsd:10.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 98
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.10.234 to 192.168.10.1 :
192.168.10.234
192.168.10.1

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

53/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/53

```
Port 53/tcp was found to be open
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2003/02/13, Modification date: 2017/05/16

Ports

tcp/53

80/tcp

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:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

nginx
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

```
Port 80/tcp was found to be open
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/04/28, Modification date: 2015/10/13

Ports

tcp/80

```


CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://192.168.10.1/zLXTyjvsoEtT.html
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/80

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

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

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/80

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: nginx
  Date: Sat, 09 Dec 2017 11:09:44 GMT
  Content-Type: text/html
  Content-Length: 178
  Connection: keep-alive
  Location: https://192.168.10.1/
  X-Frame-Options: SAMEORIGIN

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

123/udp

97861 - Network Time Protocol (NTP) Mode 6 Scanner

Synopsis

The remote NTP server responds to mode 6 queries.

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

See Also

https://ntpscan.shadowserver.org

Solution

Restrict NTP mode 6 queries.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Publication date: 2017/03/21, Modification date: 2017/03/21

Ports

udp/123

```
  Nessus elicited the following response from the remote
  host by sending an NTP mode 6 query :

'version="ntpd 4.2.8p9@1.3265-o Sat Feb 11 03:58:47 UTC 2017 (1)",
processor="amd64", system="FreeBSD/10.3-RELEASE-p16", leap=0,
stratum=12, precision=-24, rootdelay=0.000, rootdisp=0.000,
refid=127.0.0.1, reftime=0x00000000.00000000, clock=0xddd6429f.fa1b7d9d,
peer=0, tc=3, mintc=3, offset=0.000000, frequency=0.000,
sys_jitter=0.000000, clk_jitter=0.000, clk_wander=0.000'
```

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

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

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2017/05/31

Ports

udp/123

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

Version : 4.2.8p9
```

443/tcp

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

http://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:

Publication date: 2010/12/15, Modification date: 2017/05/18

Ports

tcp/443

```
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=US/ST=State/L=Locality/O=pfSense webConfigurator Self-Signed Certificate/
E=admin@pfSense.localdomain/CN=pfSense-58aedd90745fe
|-Issuer  : C=US/ST=State/L=Locality/O=pfSense webConfigurator Self-Signed Certificate/
E=admin@pfSense.localdomain/CN=pfSense-58aedd90745fe
```

57582 - SSL Self-Signed Certificate

Synopsis

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

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper 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:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

tcp/443

```
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=US/ST=State/L=Locality/O=pfSense webConfigurator Self-Signed Certificate/
E=admin@pfSense.localdomain/CN=pfSense-58aedd90745fe
```

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:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/443

```
The remote web server type is :

nginx
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/443

```
Port 443/tcp was found to be open
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/443

```
Subject Name:

Country: US
State/Province: State
Locality: Locality
Organization: pfSense webConfigurator Self-Signed Certificate
Email Address: admin@pfSense.localdomain
Common Name: pfSense-58aedd90745fe

Issuer Name:

Country: US
State/Province: State
Locality: Locality
Organization: pfSense webConfigurator Self-Signed Certificate
Email Address: admin@pfSense.localdomain
Common Name: pfSense-58aedd90745fe

Serial Number: 00
```

```
Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 23 13:03:12 2017 GMT
Not Valid After: Aug 16 13:03:12 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E3 9F B1 C9 4D 14 35 C0 60 A9 9A 55 09 F5 E8 D4 64 89 5C
            C2 BC 02 B4 BB D6 6C BA FA 05 76 F3 8F 12 A9 1C 07 95 78 57
            30 C7 70 0E 12 05 21 39 4E 1A D3 00 A2 91 7A D8 1E 3A 29 44
            06 09 20 04 C9 7A 49 3D 84 A3 EE 68 BF FF 88 75 6B 8C 62 9C
            32 0D B8 BF 2D 7F 3E 18 21 2F AB 6F 24 84 D0 DC 4D 8B 02 EF
            16 8E 45 D6 A0 9E 86 96 15 B4 1C 2C C3 6B C2 22 52 18 EF FC
            A4 A2 B1 C4 D3 1D 31 19 87 18 6D E2 53 C9 AD 0E 70 61 21 D8
            75 78 A1 48 06 5D D6 98 32 93 33 82 7D B6 54 61 31 33 37 34
            48 2E BD A2 91 E9 7C 62 3D 37 30 B4 4A A1 5E 1C E6 18 09 66
            9C 00 5D 1C DF F3 40 3B B4 7D 97 8A C0 B6 0D FD E1 C7 67 DA
            9B 42 4C 15 BB F4 65 DA 3F A6 B6 60 85 38 5D A5 0F BB F7 C8
            25 39 DD 15 3D 60 DA 62 F8 3F 70 F6 98 C6 89 06 EB D9 97 0B
            36 C9 A4 EB B7 61 41 96 D2 81 7A AC AA 23 0D C2 B1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 B8 8E C2 50 A3 62 61 E2 0C 79 F7 E8 F9 B6 09 61 7C 17 81
           B6 30 1E 7F 22 80 E3 72 8B E1 C5 A9 3E DE C4 5F 8E CD BB 62
           52 32 0E 40 83 D4 37 03 25 2D 40 30 9D 3F 55 EF 90 23 FF 56
           C7 8D D7 A7 C1 C2 62 C4 D4 8C 21 BB 13 59 67 1F 20 50 02 87
           DC C9 9C CC AC 0B 9E DB 6E BA 94 BF 0E A1 BF 2F D7 FC 6E 7F
           DD 5F 91 51 13 C2 A5 C4 6D  [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2017/11/13

Ports

tcp/443

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

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

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
```

```
SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES256-SHA            Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES256-SHA          Kx=ECDH        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}
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/443

```
A TLSv1.1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.1.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/443

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
  Server: nginx
  Date: Sat, 09 Dec 2017 11:09:44 GMT
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Connection: keep-alive
  Last-Modified: Sat, 09 Dec 2017 11:09:44 GMT
  X-Frame-Options: SAMEORIGIN
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  Strict-Transport-Security: max-age=31536000
  X-Content-Type-Options: nosniff

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <link rel="stylesheet" href="/css/pfSense.css" />
 <title>Login</title>
 <script type="text/javascript">
 //<![CDATA{
 var events = events || [];
 //]]>
 </script>
<script type="text/javascript">if (top != self) {top.location.href =
 self.location.href;}</script><script type="text/javascript">var csrfMagicToken =
 "sid:3ab7327de0fbae27180d8592844ec4b051d19510,1512817784";var csrfMagicName = "__csrf_magic";</
script><script src="/csrf/csrf-magic.js" type="text/javascript"></script></head>
<body id="login" class="no-menu">
 <div id="jumbotron">
  <div class="container">
   <div class="col-sm-offset-3 col-sm-6 col-xs-12">

    <div class="panel panel-default">
     <div class="panel-heading">
      <h2 class="panel-title">Login to pfSense </h2>
     </div>

     <div class="panel-body">
      <div class="alert alert-warning hidden" id="no_cookies">The browser must support cookies to
 login.</div>

      <form method="post"  action="/index.php" class="form-horizontal"><input type='hidden'
 name='__csrf_magic' value="sid:3ab7327de0fbae27180d8592844ec4b051d19510,1512817784" />
       <div class="form-group">
        <label for="usernamefld" class="col-sm-3 control-label">Username</label>
        <div class="col-sm-9 col-md-7">
         <input type="text" class="form-control" name="usernamefld" id="usernamefld"
 placeholder="En [...]
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).
The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.
All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/11/16, Modification date: 2013/11/19

Ports

tcp/443

```
The STS header line is :

Strict-Transport-Security: max-age=31536000
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2017/11/06

Ports

tcp/443

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

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

http://www.openssl.org/docs/apps/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:

Publication date: 2011/12/07, Modification date: 2017/06/12

Ports

tcp/443

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH        Au=RSA     Enc=AES-GCM(128)        Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH        Au=RSA     Enc=AES-GCM(256)        Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH      Au=RSA     Enc=AES-GCM(128)        Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH      Au=RSA     Enc=AES-GCM(256)        Mac=SHA384
    DHE-RSA-AES256-SHA           Kx=DH        Au=RSA     Enc=AES-CBC(256)        Mac=SHA1
    ECDHE-RSA-AES256-SHA          Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES256-SHA256         Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384       Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

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

62564 - TLS Next Protocols Supported

Synopsis

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

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections. Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04

https://technotes.googlecode.com/git/nextprotoneg.html

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/10/16, Modification date: 2017/11/13

Ports

tcp/443

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

  http/1.1
```

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

http://www.openssl.org/docs/apps/ciphers.html

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/443

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES256-SHA            Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES256-SHA          Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES256-SHA256         Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384       Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384

The fields above are :

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

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/12/08, Modification date: 2015/12/08

Ports

tcp/443

```
NPN Supported Protocols:

  http/1.1
```

500/udp

11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection

Synopsis

A VPN server is listening on the remote port.

Description

The remote host seems to be enabled to do Internet Key Exchange (IKE) version 1. This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.
Make sure that the use of this VPN endpoint is done in accordance with your corporate security policy.
Note that if the remote host is not configured to allow the Nessus host to perform IKE/IPSEC negotiations, Nessus won't be able to detect the IKE service.
Also note that this plugin does not run over IPv6.

Solution

If this service is not needed, disable it or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 2003/12/02, Modification date: 2016/06/13

Ports

udp/500

```
Nessus was able to get the following IKE vendor ID(s):
XAUTH
Dead Peer Detection v1.0
```

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection

Synopsis

A VPN server is listening on the remote port.

Description

The remote host seems to be enabled to do Internet Key Exchange (IKE).
This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.
Make sure that the use of this VPN endpoint is done in accordance with your corporate security policy.
Note that if the remote host is not configured to allow the Nessus host to perform IKE/IPSEC negotiations, Nessus won't be able to detect the IKE service.
Also note that this plugin does not run over IPv6.

Solution

If this service is not needed, disable it or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 2012/10/24, Modification date: 2016/02/15

Ports

udp/500

192.168.10.10

Scan Information

Start time:	Sat Dec 9 13:09:35 2017
End time:	Sat Dec 9 13:18:26 2017

Host Information

DNS Name:	rodc.ldil.de
Netbios Name:	RODC
IP:	192.168.10.10
MAC Address:	00:50:56:01:29:92
OS:	Microsoft Windows Server 2008 R2 Standard Service Pack 1

Results Summary

Critical	High	Medium	Low	Info	Total
3	0	1	0	52	56

Results Details

0/tcp

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.
There are several possible reasons for this :
- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.
This might be an availability problem related to the following :
- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.
In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.
- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information:

Publication date: 2002/03/19, Modification date: 2014/06/04

Ports

tcp/0

```
Port 3269 was detected as being open but is now closed
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Microsoft Windows Server 2008 R2 Standard Service Pack 1
Confidence level : 99
Method : MSRPC

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

NTP:!:unknown


The remote host is running Microsoft Windows Server 2008 R2 Standard Service Pack 1
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2017/04/14

Ports

tcp/0

```
192.168.10.10 resolves as rodc.ldil.de.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:09 EET
Scan duration : 520 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

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

Description

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

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.
If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Publication date: 2007/03/12, Modification date: 2013/01/07

Ports

tcp/0

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```

The following card manufacturers were identified :

00:50:56:01:29:92 : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_server_2008:r2:sp1 -> Microsoft Windows Server 2008 R2 Service Pack 1
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

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

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.10.234 to 192.168.10.10 :
192.168.10.234
192.168.10.10

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

53/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/53

```
Port 53/tcp was found to be open
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2003/02/13, Modification date: 2017/05/16

Ports

tcp/53

72779 - DNS Server Version Detection

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:

Publication date: 2014/03/03, Modification date: 2014/11/05

Ports

tcp/53

```
DNS server answer for "version" (over TCP) :

  Microsoft DNS 6.1.7601 (1DB1446A)
```

53/udp

72836 - MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)

Synopsis

The DNS server running on the remote host has multiple vulnerabilities.

Description

According to its self-reported version number, the Microsoft DNS Server running on the remote host has the following vulnerabilities :
- A memory corruption vulnerability exists that can be triggered by an attacker sending a specially crafted NAPTR query. This could result in arbitrary code execution. (CVE-2011-1966)
- A denial of service vulnerability exists related to the improper handling of uninitialized memory. This may result in the DNS service becoming unresponsive.
(CVE-2011-1970)

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-058

Solution

Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	49012
BID	49019
CVE	CVE-2011-1966
CVE	CVE-2011-1970
MSKB	2562485
XREF	OSVDB:74399
XREF	OSVDB:74400
XREF	MSFT:MS11-058

Exploitable with

Core Impact (true)

Plugin Information:

Publication date: 2014/03/05, Modification date: 2017/08/30

Ports

udp/53

```
  Installed version : 6.1.7601.17514
  Fixed version     : 6.1.7601.17639
```

72837 - MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)

Synopsis

The DNS server running on the remote host is susceptible to a denial of service attack.

Description

According to its self-reported version number, the Microsoft DNS server running on the remote host does not properly handle objects in memory when looking up the resource record of a domain. By sending a specially crafted DNS query an attacker may be able to exploit this flaw and cause the DNS server on the remote host to stop responding and eventually restart.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms12-017

Solution

Microsoft has released a set of patches for Windows 2003, 2008, and 2008 R2.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	52374
CVE	CVE-2012-0006
MSKB	2647170
XREF	OSVDB:80005
XREF	MSFT:MS12-017

Plugin Information:

Publication date: 2014/03/05, Modification date: 2017/08/30

Ports

udp/53

```
Installed version : 6.1.7601.17514
Fixed version     : 6.1.7601.17750
```

72780 - Microsoft DNS Server Version Detection

Synopsis

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

Description

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

See Also

http://technet.microsoft.com/en-us/library/cc772069.aspx

Solution

The command 'dnscmd /config /EnableVersionQuery 0' can be used to disable version queries if desired.

Risk Factor

None

Plugin Information:

Publication date: 2014/03/03, Modification date: 2014/03/03

Ports

udp/53

```
Reported version : Microsoft DNS 6.1.7601 (1DB1446A)
Extended version : 6.1.7601.17514
```

88/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/88

```
Port 88/tcp was found to be open
```

43829 - Kerberos Information Disclosure

Synopsis

The remote Kerberos server is leaking information.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/01/08, Modification date: 2015/09/24

Ports

tcp/88

```
Nessus gathered the following information :

  Server time  : 2017-12-09 11:15:01 UTC
  Realm        : LDIL.DE
```

123/udp

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

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

See Also

http://www.ntp.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/03/20, Modification date: 2017/05/31

Ports

udp/123

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

  No sensitive information has been disclosed.

  Version : unknown
```

135/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/135

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

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

```

The following DCERPC services are available locally :

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

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07B840

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

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07B840

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-f57a3f0a334044b229

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
```

```
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc07BA61

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc07BA61

Object UUID : 5d8c0e58-a295-460b-a1fd-e22c6e3d7748
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : OLE7454A2C30D7A4892A761CA8514D5

Object UUID : 5d8c0e58-a295-460b-a1fd-e22c6e3d7748
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-adef088a96c2487121

Object UUID : 00000000-0000-0 [...]
```

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

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

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.
Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/09/27

Ports

udp/137

```
The following 4 NetBIOS names have been gathered :

 RODC              = Computer name
 LDIL              = Workgroup / Domain name
 LDIL              = Domain Controllers
 RODC              = File Server Service

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

   00:50:56:01:29:92
```

139/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/139

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

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

389/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/389

```
Port 389/tcp was found to be open
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/10, Modification date: 2017/05/16

Ports

tcp/389

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/07/12, Modification date: 2012/02/20

Ports

tcp/389

```
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-currentTime:
   |  20171209111638.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=RODC,CN=Servers,CN=StoreBranch,CN=Sites,CN=Configuration,DC=ldil,DC=de
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-defaultNamingContext:
   |  DC=ldil,DC=de
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-configurationNamingContext:
   |  CN=Configuration,DC=ldil,DC=de
[+]-rootDomainNamingContext:
   |  DC=ldil,DC=de
[+]-supportedControl:
   |  1.2.840.113556.1.4.319
   |  1.2.840.113556.1.4.801
   |  1.2.840.113556.1.4.473
   |  1.2.840.113556.1.4.528
   |  1.2.840.113556.1.4.417
   |  1.2.840.113556.1.4.619
   |  1.2.840.113556.1.4.841
   |  1.2.840.113556.1.4.529
   |  1.2.840.113556.1.4.805
   |  1.2.840.113556.1.4.521
   |  1.2.840.113556.1.4.970
   |  1.2.840.113556.1.4.1338
   |  1.2.840.113556.1.4.474
```

```
        |  1.2.840.113556.1.4.1339
        |  1.2.840.113556.1.4.1340
        |  1.2.840.113556.1.4.1413
        |  2.16.840.1.113730.3.4.9
        |  2.16.840.1.113730.3.4.10
        |  1.2.840.113556.1.4.1504
        |  1.2.840.113556.1.4.1852
        |  1.2.840.113556.1.4.802
        |  1.2.840.113556.1.4.1907
        |  1.2.840.113556.1.4.1948
        |  1.2.840.113556.1.4.1974
        |  1.2.840.113556.1.4.1341
        |  1.2.840.113556.1.4.2026
        |  1.2.840.113556.1.4.2064
        |  1.2.840.113556.1.4.2065
        |  1.2.840.113556.1.4.2066
     [+]-supportedLDAPVersion:
        |  3
        |  2
     [+]-supportedLDAPPolicies:
        |  MaxPoolThreads
        |  MaxDatagramRecv
        |  MaxReceiveBuffer
        |  InitRecvTimeout
        |  MaxConnections
        |  MaxConnIdleTime
        |  MaxPageSize
        |  MaxQueryDuration
        |  MaxTempTableSize
        |  MaxResultSetSize
        |   [...]
```

445/tcp

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)
ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

https://technet.microsoft.com/library/security/MS17-010

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

http://www.nessus.org/u?7bec1941

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

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

https://support.microsoft.com/en-us/kb/2696547

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

http://www.nessus.org/u?36fd3072

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

https://github.com/stamparm/EternalRocks/

http://www.nessus.org/u?59db5b5b

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.
For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.5 (CVSS:3.0/E:F/RL:U/RC:X)

CVSS Base Score

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

CVSS Temporal Score

9.5 (CVSS2#E:F/RL:U/RC:ND)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213

MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	OSVDB:153673
XREF	OSVDB:153674
XREF	OSVDB:153675
XREF	OSVDB:153676
XREF	OSVDB:153677
XREF	OSVDB:153678
XREF	OSVDB:155620
XREF	OSVDB:155634
XREF	OSVDB:155635
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2017/03/20, Modification date: 2017/09/07

Ports

tcp/445

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/445

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

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/kb/143474

https://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2017/11/06

Ports

tcp/445

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

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

```

The following DCERPC services are available remotely :

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

```
Netbios name : \\RODC

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

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RODC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\RODC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\RODC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\RODC

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

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

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2017/02/21

Ports

tcp/445

```
The remote Operating System is : Windows Server 2008 R2 Standard 7601 Service Pack 1
The remote native LAN manager is : Windows Server 2008 R2 Standard 6.1
The remote SMB Domain Name is : LDIL
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

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

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

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'
service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/04, Modification date: 2011/03/27

Ports

tcp/445

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

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

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

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

See Also

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

https://support.microsoft.com/en-us/kb/2696547

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

http://www.nessus.org/u?36fd3072

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

Solution

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

Risk Factor

None

References

XREF	OSVDB:151058

Plugin Information:

Publication date: 2017/02/03, Modification date: 2017/02/16

Ports

tcp/445

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

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

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

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.
Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/06/19, Modification date: 2017/06/19

Ports

tcp/445

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

464/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/464

```
Port 464/tcp was found to be open
```

593/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/593

```
Port 593/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/593

```
An http-rpc-epmap is running on this port.
```

636/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/636

```
Port 636/tcp was found to be open
```

3268/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/3268

```
Port 3268/tcp was found to be open
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/02/10, Modification date: 2017/05/16

Ports

tcp/3268

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/07/12, Modification date: 2012/02/20

Ports

tcp/3268

```
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-currentTime:
   |  20171209111638.0Z
[+]-subschemaSubentry:
   |  CN=Aggregate,CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-dsServiceName:
   |  CN=NTDS Settings,CN=RODC,CN=Servers,CN=StoreBranch,CN=Sites,CN=Configuration,DC=ldil,DC=de
[+]-namingContexts:
   |  DC=ldil,DC=de
   |  CN=Configuration,DC=ldil,DC=de
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
   |  DC=DomainDnsZones,DC=ldil,DC=de
   |  DC=ForestDnsZones,DC=ldil,DC=de
[+]-defaultNamingContext:
   |  DC=ldil,DC=de
[+]-schemaNamingContext:
   |  CN=Schema,CN=Configuration,DC=ldil,DC=de
[+]-configurationNamingContext:
   |  CN=Configuration,DC=ldil,DC=de
[+]-rootDomainNamingContext:
   |  DC=ldil,DC=de
[+]-supportedControl:
   |  1.2.840.113556.1.4.319
   |  1.2.840.113556.1.4.801
   |  1.2.840.113556.1.4.473
   |  1.2.840.113556.1.4.528
   |  1.2.840.113556.1.4.417
   |  1.2.840.113556.1.4.619
   |  1.2.840.113556.1.4.841
   |  1.2.840.113556.1.4.529
   |  1.2.840.113556.1.4.805
   |  1.2.840.113556.1.4.521
   |  1.2.840.113556.1.4.970
   |  1.2.840.113556.1.4.1338
   |  1.2.840.113556.1.4.474
   |  1.2.840.113556.1.4.1339
   |  1.2.840.113556.1.4.1340
   |  1.2.840.113556.1.4.1413
   |  2.16.840.1.113730.3.4.9
   |  2.16.840.1.113730.3.4.10
   |  1.2.840.113556.1.4.1504
   |  1.2.840.113556.1.4.1852
   |  1.2.840.113556.1.4.802
   |  1.2.840.113556.1.4.1907
   |  1.2.840.113556.1.4.1948
   |  1.2.840.113556.1.4.1974
   |  1.2.840.113556.1.4.1341
   |  1.2.840.113556.1.4.2026
   |  1.2.840.113556.1.4.2064
   |  1.2.840.113556.1.4.2065
   |  1.2.840.113556.1.4.2066
[+]-supportedLDAPVersion:
   |  3
   |  2
[+]-supportedLDAPPolicies:
   |  MaxPoolThreads
   |  MaxDatagramRecv
   |  MaxReceiveBuffer
   |  InitRecvTimeout
   |  MaxConnections
   |  MaxConnIdleTime
```

```
    |  MaxPageSize
    |  MaxQueryDuration
    |  MaxTempTableSize
    |  MaxResultSetSize
    |   [...]
```

3269/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/3269

```
Port 3269/tcp was found to be open
```

5355/udp

53514 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Synopsis

Arbitrary code can be executed on the remote host through the installed Windows DNS client.

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.
Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

See Also

http://technet.microsoft.com/en-us/security/bulletin/ms11-030

Solution

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

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

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

STIG Severity

I

References

BID	47242
CVE	CVE-2011-0657
MSKB	2509553

XREF	OSVDB:71780
XREF	IAVA:2011-A-0039
XREF	MSFT:MS11-030

Exploitable with

Core Impact (true)Metasploit (true)

Plugin Information:

Publication date: 2011/04/21, Modification date: 2017/08/30

Ports

udp/5355

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

Synopsis

The remote device supports LLMNR.

Description

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

See Also

http://www.nessus.org/u?85beb421

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports

udp/5355

```
According to LLMNR, the name of the remote host is 'RODC'.
```

5722/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/5722

```
The following DCERPC services are available on TCP port 5722 :
```

```
Object UUID : 5bc1ed07-f5f5-485f-9dfd-6fd0acf9a23c
UUID : 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1.0
Description : Unknown RPC service
Annotation : Frs2 Service
Type : Remote RPC service
TCP Port : 5722
IP : 192.168.10.10
```

49152/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49152

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.10.10
```

49153/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49153

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
```

```
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.10.10
```

49154/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49154

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
```

```
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo [...]
```

49155/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49155

```
The following DCERPC services are available on TCP port 49155 :
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4.0
Description : Active Directory Replication Interface
Windows process : unknown
Annotation : MS NT Directory DRS Interface
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ab, version 0.0
Description : Local Security Authority
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.10.10

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-01234567cffb, version 1.0
Description : Network Logon Service
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.10.10
```

61238/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/61238

```
The following DCERPC services are available on TCP port 61238 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 61238
IP : 192.168.10.10

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

```
TCP Port : 61238
IP : 192.168.10.10
```

61272/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/61272

```
The following DCERPC services are available on TCP port 61272 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 61272
IP : 192.168.10.10
```

61279/tcp

10736 - DCE Services Enumeration

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/61279

```
The following DCERPC services are available on TCP port 61279 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5.0
Description : DNS Server
Windows process : dns.exe
Type : Remote RPC service
TCP Port : 61279
IP : 192.168.10.10
```

192.168.10.20

Scan Information

Start time:	Sat Dec 9 13:09:35 2017
End time:	Sat Dec 9 13:12:15 2017

Host Information

IP:	192.168.10.20
MAC Address:	00:50:56:01:29:98
OS:	Linux Kernel 2.6 on CentOS Linux release 6

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	2	31	36

Results Details

0/icmp

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	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 11 seconds.
```

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 2.6 on CentOS Linux release 6
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 2.6 on CentOS Linux release 6
```

18261 - Apache Banner Linux Distribution Disclosure

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:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - CentOS 6
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan : 

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:09 EET
Scan duration : 156 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:29:98 : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:centos:centos:6 -> CentOS-6

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

```
cpe:/a:openbsd:openssh:5.3 -> OpenBSD  OpenSSH 5.3
cpe:/a:apache:http_server:2.2.15 -> Apache Software Foundation Apache HTTP Server 2.2.15
cpe:/a:php:php:5.3.3 -> PHP 5.3.3
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.10.234 to 192.168.10.20 :
192.168.10.234
192.168.10.20

Hop Count: 1
```

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

22/tcp

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:

Publication date: 2016/04/04, Modification date: 2016/12/14

Ports

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
```

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

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Publication date: 2013/10/28, Modification date: 2016/05/12

Ports

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:

Publication date: 2013/11/22, Modification date: 2016/12/14

Ports

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
```

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:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_5.3
SSH supported authentication : publickey,password
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/22

```
Port 22/tcp was found to be open
```

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:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

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:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/22

```

Give Nessus credentials to perform local checks.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

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
```

80/tcp

11213 - HTTP TRACE / TRACK Methods Allowed

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

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

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

http://download.oracle.com/sunalerts/1000718.1.html

Solution

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:H/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	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/11/23

Ports

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 /Nessus1074406023.html HTTP/1.1
Connection: Close
Host: 192.168.10.20
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: Sat, 09 Dec 2017 11:11:35 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1074406023.html HTTP/1.1
Connection: Close
Host: 192.168.10.20
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 ------------------------------
```

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:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.15 (CentOS)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/80

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

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

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/80

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Sat, 09 Dec 2017 11:11:38 GMT
  Server: Apache/2.2.15 (CentOS)
  X-Powered-By: PHP/5.3.3
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  Content-Length: 1026
  Connection: close
  Content-Type: text/html; charset=UTF-8

Response Body :

<html>
<head>
  <title>POS</title>
  <style type="text/css">
    body {
      background-color: #ece5ce;
      color: #774f38;
      font-family: tahoma,verdana;
      font-size: 14px;
    }
    h2 {
      padding: 5px;
    }
    .err {
      background-color: #e08e79;
    }
    .ok {
      background-color: #c5e0c9;
    }
    tr td:first-child {
      text-align: right;
    }
  </style>
</head>
<body>
  <form method="post" action="maksu.php">
  <input type="hidden" name="session" value="4adplk2jo1vbeosrlqhpe6stj4">
  <input type="hidden" name="amount" value="25.99">
  <h1>POS</h1>
```

```
    <table>
      <tr><td>Amount:</td><td><input type="number" name="amount"></td></tr>
      <tr><td>Card number:</td><td><input type="text" size="20" maxlength="19" name="card"></td></
  tr>
      <tr><td>Security code:</td><td><input type="password" size="5" maxlength="4"
   name="card_code"></td></tr>
      <tr><td></td><td><input type="submit" value="Confirm"></td></tr>
    </table>
    </form>
  </body>
  </html>
```

39521 - Backported Security Patch Detection (WWW)

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:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/80

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

48243 - PHP Version Detection

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:

Publication date: 2010/08/04, Modification date: 2017/07/07

Ports

tcp/80

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.3
  Source  : X-Powered-By: PHP/5.3.3
```

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:

Publication date: 2015/07/07, Modification date: 2015/07/07

Ports

tcp/80

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

443/tcp

11213 - HTTP TRACE / TRACK Methods Allowed

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

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

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

http://download.oracle.com/sunalerts/1000718.1.html

Solution

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.3 (CVSS2#E:H/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	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/11/23

Ports

tcp/443

```
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 /Nessus1624588890.html HTTP/1.1
Connection: Close
Host: 192.168.10.20
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: Sat, 09 Dec 2017 11:11:35 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1624588890.html HTTP/1.1
Connection: Close
Host: 192.168.10.20
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 ------------------------------
```

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:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/443

```
The remote web server type is :

Apache/2.2.15 (CentOS)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/443

```
Port 443/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/443

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

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

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

tcp/443

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Sat, 09 Dec 2017 11:11:38 GMT
  Server: Apache/2.2.15 (CentOS)
  X-Powered-By: PHP/5.3.3
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
  Pragma: no-cache
  Content-Length: 1026
  Connection: close
  Content-Type: text/html; charset=UTF-8

Response Body :

<html>
<head>
  <title>POS</title>
  <style type="text/css">
    body {
      background-color: #ece5ce;
      color: #774f38;
      font-family: tahoma,verdana;
      font-size: 14px;
    }
    h2 {
      padding: 5px;
    }
    .err {
      background-color: #e08e79;
    }
    .ok {
      background-color: #c5e0c9;
    }
    tr td:first-child {
      text-align: right;
    }
  </style>
</head>
<body>
  <form method="post" action="maksu.php">
  <input type="hidden" name="session" value="51te18b4el42skoskpru2e50d2">
  <input type="hidden" name="amount" value="25.99">
  <h1>POS</h1>
```

```
    <table>
      <tr><td>Amount:</td><td><input type="number" name="amount"></td></tr>
      <tr><td>Card number:</td><td><input type="text" size="20" maxlength="19" name="card"></td></
  tr>
      <tr><td>Security code:</td><td><input type="password" size="5" maxlength="4"
   name="card_code"></td></tr>
      <tr><td></td><td><input type="submit" value="Confirm"></td></tr>
    </table>
    </form>
  </body>
  </html>
```

39521 - Backported Security Patch Detection (WWW)

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:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/443

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

48243 - PHP Version Detection

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:

Publication date: 2010/08/04, Modification date: 2017/07/07

Ports

tcp/443

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.3
  Source  : X-Powered-By: PHP/5.3.3
```

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:

Publication date: 2015/07/07, Modification date: 2015/07/07

Ports

tcp/443

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

192.168.10.30

Scan Information

Start time: Sat Dec 9 13:09:35 2017

End time: Sat Dec 9 13:17:37 2017

Host Information

IP: 192.168.10.30

MAC Address: 00:50:56:01:1a:ae

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

0/tcp

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:10 EET
Scan duration : 455 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:1a:ae : VMware, Inc.
```

0/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

192.168.10.51

Scan Information

Start time:	Sat Dec 9 13:09:35 2017
End time:	Sat Dec 9 14:28:48 2017

Host Information

IP:	192.168.10.51
MAC Address:	00:50:56:01:18:7e
OS:	Linux Kernel 3.1, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	18	19

Results Details

0/icmp

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	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 11 seconds.
```

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.1
Linux Kernel 3.3
Confidence level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.1
Linux Kernel 3.3
```

18261 - Apache Banner Linux Distribution Disclosure

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:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - Debian 7.0 (wheezy)
 - Debian unstable (sid)
 - Debian testing (wheezy)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_udp_scanner nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:09 EET
Scan duration : 4749 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:18:7e : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:linux:linux_kernel:3.1
  cpe:/o:linux:linux_kernel:3.3

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server 2.2.22
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.10.234 to 192.168.10.51 :
192.168.10.234
192.168.10.51

Hop Count: 1
```

23/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/23

```
Port 23/tcp was found to be open
```

80/tcp

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	6939
CVE	CVE-2003-1418
XREF	OSVDB:60395
XREF	CWE:200

Plugin Information:

Publication date: 2016/01/22, Modification date: 2016/08/01

Ports

tcp/80

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "22c9b-fc-5050e9c759908"
  Inode number           : 142491
  File size              : 252 bytes
  File modification time : Oct. 10, 2014 at 09:59:56 GMT
```

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:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.22 (Debian)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/80

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

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

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

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: Sat, 09 Dec 2017 12:27:33 GMT
  Server: Apache/2.2.22 (Debian)
  Last-Modified: Fri, 10 Oct 2014 09:59:56 GMT
  ETag: "22c9b-fc-5050e9c759908"
  Accept-Ranges: bytes
  Content-Length: 252
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<body>

<h2>I-Spy IP Camera 0.9</h2>

<img src="/cgi-bin/video.cgi">

<p><a href="/cgi-bin/video.cgi">Plain image</a></p>
<p><a href="cgi-bin/video_full.cgi">Plain image (High resolution)</a></p>

<p>I-SPY FW Version 7.87B-55-R2.6B</p>

</body>
```

39521 - Backported Security Patch Detection (WWW)

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:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/80

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

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

1072/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/1072

```
Port 1072/udp was found to be open
```

192.168.10.52

Scan Information

Start time:	Sat Dec 9 13:09:35 2017
End time:	Sat Dec 9 14:28:52 2017

Host Information

IP:	192.168.10.52
MAC Address:	00:50:56:01:18:7d
OS:	Linux Kernel 3.1, Linux Kernel 3.3

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	18	19

Results Details

0/icmp

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	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 11 seconds.
```

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.1
Linux Kernel 3.3
Confidence level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.1
Linux Kernel 3.3
```

18261 - Apache Banner Linux Distribution Disclosure

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:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - Debian 7.0 (wheezy)
 - Debian unstable (sid)
 - Debian testing (wheezy)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan : 

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_udp_scanner nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:09 EET
Scan duration : 4753 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```

The following card manufacturers were identified :

00:50:56:01:18:7d : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:linux:linux_kernel:3.1
  cpe:/o:linux:linux_kernel:3.3

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server 2.2.22
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 59
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.10.234 to 192.168.10.52 :
192.168.10.234
192.168.10.52

Hop Count: 1
```

23/tcp

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/23

```
Port 23/tcp was found to be open
```

80/tcp

88098 - Apache Server ETag Header Information Disclosure

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	6939
CVE	CVE-2003-1418
XREF	OSVDB:60395
XREF	CWE:200

Plugin Information:

Publication date: 2016/01/22, Modification date: 2016/08/01

Ports

tcp/80

```
Nessus was able to determine that the Apache Server listening on
port 80 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                 : ETag: "22c9b-fc-5050e9c759908"
  Inode number           : 142491
  File size              : 252 bytes
  File modification time : Oct. 10, 2014 at 09:59:56 GMT
```

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:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Apache/2.2.22 (Debian)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/80

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

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

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

Ports

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: Sat, 09 Dec 2017 12:27:34 GMT
  Server: Apache/2.2.22 (Debian)
  Last-Modified: Fri, 10 Oct 2014 09:59:56 GMT
  ETag: "22c9b-fc-5050e9c759908"
  Accept-Ranges: bytes
  Content-Length: 252
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html>
<body>

<h2>I-Spy IP Camera 0.9</h2>

<img src="/cgi-bin/video.cgi">

<p><a href="/cgi-bin/video.cgi">Plain image</a></p>
<p><a href="cgi-bin/video_full.cgi">Plain image (High resolution)</a></p>

<p>I-SPY FW Version 7.87B-55-R2.6B</p>

</body>
```

39521 - Backported Security Patch Detection (WWW)

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:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/80

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

43111 - HTTP Methods Allowed (per directory)

Synopsis

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

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

1072/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/1072

```
Port 1072/udp was found to be open
```

192.168.10.234

Scan Information

Start time:	Sat Dec 9 13:09:42 2017
End time:	Sat Dec 9 13:09:52 2017

Host Information

DNS Name:	kali
IP:	192.168.10.234
MAC Address:	00:50:56:01:32:f5 00:50:56:01:32:fa 00:50:56:01:32:f4 00:50:56:01:32:f9 00:50:56:01:32:f6 00:50:56:01:32:f7 00:50:56:01:32:f8
OS:	Linux Kernel 4.12.0-kali1-amd64

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	31	31

Results Details

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```

Remote operating system : Linux Kernel 4.12.0-kali1-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 4.12.0-kali1-amd64
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2017/04/14

Ports

tcp/0

```
192.168.10.234 resolves as kali.
```

12634 - Authenticated Check : OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet, or local commands and extracts the list of installed packages.
If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/07/06, Modification date: 2017/11/17

Ports

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Linux kali 4.12.0-kali1-amd64 #1 SMP Debian 4.12.6-1kali6 (2017-08-30) x86_64 GNU/Linux

Local security checks have NOT been enabled because the remote Linux
distribution is not supported.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
```

```
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:09 EET
Scan duration : 10 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

21745 - Authentication Failure - Local Checks Not Run

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:

Publication date: 2006/06/23, Modification date: 2017/05/30

Ports

tcp/0

```
Additional failure information from ssh_get_info2.nasl :
Debian version does not match known patterns
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2017/01/26

Ports

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - fe80::250:56ff:fe01:32f4 (on interface eth0)
 - fe80::90f4:2d78:8dc6:1282 (on interface eth1)
 - fe80::6561:631c:86eb:a5e6 (on interface eth2)
 - fe80::ff46:ee3e:87a2:9753 (on interface eth3)
 - fe80::35d6:ae07:7359:e655 (on interface eth4)
 - fe80::6e4c:90ef:a2f2:a8ec (on interface eth5)
 - fe80::fcda:cc39:e730:eea4 (on interface eth6)
 - ::1 (on interface lo)
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2007/05/11, Modification date: 2017/01/26

Ports

tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 10.99.0.234 (on interface eth0)
 - 10.10.10.234 (on interface eth1)
 - 10.0.100.234 (on interface eth2)
 - 10.10.0.10 (on interface eth3)
 - 172.20.0.234 (on interface eth4)
 - 192.168.10.234 (on interface eth5)
 - 192.168.20.234 (on interface eth6)
 - 127.0.0.1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information:

Publication date: 2008/06/30, Modification date: 2017/01/26

Ports

tcp/0

```

The following MAC addresses exist on the remote host :

  - 00:50:56:01:32:f5 (interface eth1)
  - 00:50:56:01:32:fa (interface eth6)
  - 00:50:56:01:32:f4 (interface eth0)
  - 00:50:56:01:32:f9 (interface eth5)
  - 00:50:56:01:32:f6 (interface eth2)
  - 00:50:56:01:32:f7 (interface eth3)
  - 00:50:56:01:32:f8 (interface eth4)
```

34098 - BIOS version (SSH)

Synopsis

The BIOS version could be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to get the BIOS vendor and version.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/08, Modification date: 2017/08/28

Ports

tcp/0

```
Version      : 6.00
Vendor       : Phoenix Technologies LTD
Release Date : 09/17/2015
UUID         : 4204D3C5-5DF6-9C4C-5D0B-7A6E24E5AD02
```

35351 - System Information Enumeration (via DMI)

Synopsis

Information about the remote system's hardware can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/01/12, Modification date: 2016/08/17

Ports

tcp/0

```
Chassis Information
  Serial Number : None
  Version       : N/A
```

```
    Manufacturer  : No Enclosure
    Lock          : Not Present
    Type          : Other

  System Information
    Serial Number : VMware-42 04 d3 c5 5d f6 9c 4c-5d 0b 7a 6e 24 e5 ad 02
    Version       : None
    Manufacturer  : VMware, Inc.
    Product Name  : VMware Virtual Platform
    Family        : Not Specified
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:32:f8 : VMware, Inc.
00:50:56:01:32:f7 : VMware, Inc.
00:50:56:01:32:f6 : VMware, Inc.
00:50:56:01:32:f9 : VMware, Inc.
00:50:56:01:32:f4 : VMware, Inc.
00:50:56:01:32:fa : VMware, Inc.
00:50:56:01:32:f5 : VMware, Inc.
```

45432 - Processor Information (via DMI)

Synopsis

Nessus was able to read information about the remote system's processor.

Description

Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/06, Modification date: 2016/02/25

Ports

tcp/0

```
Nessus detected 2 processors :
```

```
Current Speed   : 3000 MHz
Version         : Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status          : Populated, Enabled
Family          : Unknown
Type            : Central Processor

Current Speed   : 3000 MHz
Version         : Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz
Manufacturer    : GenuineIntel
External Clock  : Unknown
Status          : Populated, Enabled
Family          : Unknown
Type            : Central Processor
```

45433 - Memory Information (via DMI)

Synopsis

Information about the remote system's memory devices can be read.

Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/06, Modification date: 2011/03/21

Ports

tcp/0

```
Total memory : 8192 MB
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

```
The remote operating system matched the following CPE :
  cpe:/o:linux:linux_kernel:4.12

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:7.5
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

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

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/06/30, Modification date: 2017/11/06

Ports

tcp/0

```

  Hostname : kali
    kali (hostname command)
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/10/12, Modification date: 2015/08/21

Ports

tcp/0

```
  reboot   system boot  4.12.0-kali1-amd Wed Nov 22 21:45   still running
  reboot   system boot  4.12.0-kali1-amd Mon Nov 20 14:15   still running
  reboot   system boot  4.12.0-kali1-amd Mon Nov 20 13:27 - 14:15  (00:48)
  reboot   system boot  4.12.0-kali1-amd Mon Nov 20 13:18 - 14:15  (00:57)

  wtmp begins Mon Nov 20 13:18:34 2017
```

58651 - Netstat Active Connections

Synopsis

Active connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/04/10, Modification date: 2015/06/02

Ports

tcp/0

```
Netstat output :
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:49954         127.0.0.1:8834          ESTABLISHED
tcp        0      0 10.99.0.234:8834        77.74.137.114:35571     TIME_WAIT
tcp        0      0 192.168.10.234:47798    192.168.10.51:80        ESTABLISHED
tcp        0      0 192.168.10.234:58844    192.168.10.52:23        ESTABLISHED
tcp        0      0 127.0.0.1:8834          127.0.0.1:49954         ESTABLISHED
tcp        0      0 10.99.0.234:8834        77.74.137.114:11892     TIME_WAIT
tcp        0      0 192.168.10.234:59244    192.168.10.52:80        ESTABLISHED
tcp        0      0 10.99.0.234:22          77.74.137.114:11311     ESTABLISHED
tcp        0      1 192.168.10.234:55622    192.168.10.1:8009       SYN_SENT
tcp        0      0 10.99.0.234:8834        77.74.137.114:61431     TIME_WAIT
tcp        0      1 192.168.10.234:50762    192.168.10.1:81         SYN_SENT
tcp        0      0 192.168.10.234:60198    192.168.10.51:23        ESTABLISHED
tcp        0      0 10.99.0.234:8834        77.74.137.114:35939     TIME_WAIT
tcp        0      0 10.99.0.234:8834        77.74.137.114:61527     TIME_WAIT
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::8834                 :::*                    LISTEN
udp        0      0 192.168.10.234:40972    192.168.10.30:161       ESTABLISHED
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 192.168.10.234:46021    192.168.10.20:137       ESTABLISHED
udp        0      0 192.168.10.234:46087    192.168.10.10:161       ESTABLISHED
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*          [...]
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/13, Modification date: 2016/08/05

Ports

tcp/0

```
tcp4 (listen)
  src: [host=0.0.0.0, port=22]
  dst: [host=0.0.0.0, port=*]

tcp4 (listen)
  src: [host=0.0.0.0, port=8834]
  dst: [host=0.0.0.0, port=*]

tcp4 (established)
  src: [host=127.0.0.1, port=49954]
  dst: [host=127.0.0.1, port=8834]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=35571]

tcp4 (established)
  src: [host=192.168.10.234, port=47798]
  dst: [host=192.168.10.51, port=80]

tcp4 (established)
  src: [host=192.168.10.234, port=58844]
  dst: [host=192.168.10.52, port=23]

tcp4 (established)
  src: [host=127.0.0.1, port=8834]
  dst: [host=127.0.0.1, port=49954]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=11892]

tcp4 (established)
  src: [host=192.168.10.234, port=59244]
  dst: [host=192.168.10.52, port=80]

tcp4 (established)
  src: [host=10.99.0.234, port=22]
  dst: [host=77.74.137.114, port=11311]

tcp4 (established)
  src: [host=192.168.10.234, port=55622]
  dst: [host=192.168.10.1, port=8009]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=61431]

tcp4 (established)
  src: [host=192.168.10.234, port=50762]
  dst: [host=192.168.10.1, port=81]

tcp4 (established)
  src: [host=192.168.10.234, port=60198]
  dst: [host=192.168.10.51, port=23]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=35939]

tcp4 (established)
  src: [host=10.99.0.234, port=8834]
  dst: [host=77.74.137.114, port=61527]

tcp6 (listen)
  src: [host=::, port=22]
  dst: [host=::, port=*]
```

```
tcp6 (listen)
  src: [host=::, port=8834]
  dst: [host=::, port=*]

udp4 (established)
  src: [host=192.168.10.234, port=40972]
  dst: [host=192.168.10.30, port=161]

udp4 (listen)
  src: [host=0.0.0.0, port=68]
  dst: [host=0.0.0.0, port=*]

udp4 (established)
  src: [host=192.168.10.234, port=46021]
  dst: [host=192.168.10.20, port=137]

udp4 (established)
  src: [host=192.168.10.234, port=46087]
  dst: [host=192.168.10.10, port=161]

udp6 (listen)
  src: [host=::, port=58 [...]
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/05/30, Modification date: 2017/11/17

Ports

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Linux kali 4.12.0-kali1-amd64 #1 SMP Debian 4.12.6-1kali6 (2017-08-30) x86_64 GNU/Linux

We are able to run commands on the remote host, but are unable to
currently identify it in this plugin.

Runtime : 0.28478 seconds
```

22/tcp

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:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_7.5p1 Debian-10
SSH supported authentication : publickey,password
```

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:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.
See the section 'plugins options' about configuring this plugin.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2017/08/25

Ports

tcp/22

```
Port 22/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

25221 - Remote listeners enumeration (Linux / AIX)

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:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

tcp/22

```

  Process ID   : 7436
  Executable   : /usr/sbin/sshd
  Command line : /usr/sbin/sshd -D
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

```

Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
```

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

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  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
```

68/udp

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.
See the section 'plugins options' about configuring this plugin.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/08/15, Modification date: 2017/08/25

Ports

udp/68

```
Port 68/udp was found to be open
```

25221 - Remote listeners enumeration (Linux / AIX)

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:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

udp/68

```

  Process ID   : 1784
  Executable   : /sbin/dhclient
  Command line : /sbin/dhclient -d -q -sf /usr/lib/NetworkManager/nm-dhcp-helper -pf /run/
dhclient-eth3.pid -lf /var/lib/NetworkManager/dhclient-cec9324d-e7a6-3273-9745-438b95233ba7-
eth3.lease -cf /var/lib/NetworkManager/dhclient-eth3.conf eth3
```

8834/tcp

25221 - Remote listeners enumeration (Linux / AIX)

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:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

tcp/8834

```

  Process ID   : 7814
  Executable   : /opt/nessus/sbin/nessusd
```

```
Command line : nessusd -q
```

43734/udp

25221 - Remote listeners enumeration (Linux / AIX)

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:

Publication date: 2007/05/16, Modification date: 2017/08/28

Ports

udp/43734

```
Process ID   : 7814
Executable   : /opt/nessus/sbin/nessusd
Command line : nessusd -q
```

192.168.10.245

Scan Information

Start time:	Sat Dec 9 13:09:42 2017
End time:	Sat Dec 9 13:17:29 2017

Host Information

IP:	192.168.10.245
MAC Address:	00:50:56:01:21:ae

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

0/tcp

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2017/12/9 13:10 EET
Scan duration : 441 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:21:ae : VMware, Inc.
```

0/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/0

```
The UDP port scan could not complete: The remote host has remained silent for too long
This might be due to a firewall filtering UDP and/or ICMP packets
```

192.168.10.251

Scan Information

Start time:	Sat Dec 9 13:09:42 2017
End time:	Sat Dec 9 14:27:05 2017

Host Information

IP:	192.168.10.251
MAC Address:	00:50:56:01:32:c9
OS:	Linux Kernel 3.16 on Debian 8.0 (jessie)

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	19	19

Results Details

0/icmp

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	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

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

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.16 on Debian 8.0 (jessie)
Confidence level : 95
Method : SSH


The remote host is running Linux Kernel 3.16 on Debian 8.0 (jessie)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- 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:

Publication date: 2005/08/26, Modification date: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711171815
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.10.234
Port scanner(s) : nessus_udp_scanner nessus_tcp_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 : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
```

```
Scan Start Date : 2017/12/9 13:09 EET
Scan duration : 4639 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2017/11/17

Ports

tcp/0

```
The following card manufacturers were identified :

00:50:56:01:32:c9 : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:debian:debian_linux:8.0 -> Debian Linux 8.0 (Jessie)

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:6.7 -> OpenBSD OpenSSH 6.7
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.10.234 to 192.168.10.251 :
192.168.10.234
192.168.10.251

Hop Count: 1
```

22/tcp

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:

Publication date: 1999/10/12, Modification date: 2017/11/17

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u1
SSH supported authentication : publickey,password
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/10/24

Ports

tcp/22

```
Port 22/tcp was found to be open
```

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:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2017/07/07

Ports

tcp/22

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

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:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/22

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

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

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

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
```

```
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    umac-64@openssh.com

  The server supports the following options for mac_algorithms_server_to_client :

    hmac-sha1
    hmac-sha1-etm@openssh.com
    hmac-sha2-256
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    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
```

69/udp

11819 - TFTP Daemon Detection

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:

Publication date: 2003/08/13, Modification date: 2016/02/22

Ports

udp/69

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/69

```
Port 69/udp was found to be open
```

5353/udp

34277 - Nessus UDP Scanner

Synopsis

It is possible to determine which UDP ports are open.

Description

This plugin runs a UDP port scan against the target. It is possible to determine which UDP ports are open by sending UDP packets on every port. If the port is open, the application will most often keep quiet.
If the port is closed, the TCP/IP stack may send back an ICMP Host unreachable / bad port packet. If the target machine is protected by a firewall, this technique cannot distinguish open ports from filtered ports and fails. As the ICMP rate is often limited, this scan is slow.

Solution

Protect your target with an IP filter or implement ICMP rate limitation.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

udp/5353

```
Port 5353/udp was found to be open
```

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information:

Publication date: 2013/05/31, Modification date: 2013/05/31

Ports

udp/5353

```
Nessus was able to extract the following information :

  - mDNS hostname       : kalics3-2.local.

  - Advertised services :
    o Service name      : kalics3-2 [00:50:56:01:32:c9]._workstation._tcp.local.
      Port number       : 9
    o Service name      : kalics3-2._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```