



pentesting

Report generated by Nessus™

Sun, 30 Jun 2024 21:25:03 IST

TABLE OF CONTENTS

Vulnerabilities by Host

• 172.67.186.112.....	4
-----------------------	---

Nessus Essentials

Vulnerabilities by Host

172.67.186.112



Scan Information

Start time: Sun Jun 30 20:55:13 2024
End time: Sun Jun 30 21:25:02 2024

Host Information

IP: 172.67.186.112
OS: CISCO PIX 7.0

Vulnerabilities

45590 - Common Platform Enumeration (CPE)

Synopsis

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

Description

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

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

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/06/24

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:cisco:pix_firewall:7.0 -> Cisco PIX Firewall Software

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : firewall  
Confidence level : 70
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/80/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/443/www

```
The remote web server type is :  
cloudflare
```


10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2052/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2053/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2083/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2086/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2087/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/2096/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8080/www

```
The remote web server type is :  
cloudflare
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8443/www

```
The remote web server type is :  
cloudflare
```


10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

tcp/8880/www

```
The remote web server type is :  
cloudflare
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sun, 30 Jun 2024 15:38:52 GMT

Content-Type: text/plain; charset=UTF-8

Content-Length: 16

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Server: cloudflare

CF-RAY: 89bf3eeae98881f8-SIN

Response Body :

error code: 1003

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: cloudflare

Date: Sun, 30 Jun 2024 15:38:47 GMT

Content-Type: text/html

Content-Length: 655

Connection: close

CF-RAY: -

Response Body :

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
```

```
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2052/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sun, 30 Jun 2024 15:38:56 GMT

Content-Type: text/plain; charset=UTF-8

Content-Length: 16

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Server: cloudflare

CF-RAY: 89bf3f047cc89c2d-SIN

Response Body :

error code: 1003

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2053/www

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: cloudflare

Date: Sun, 30 Jun 2024 15:38:49 GMT

Content-Type: text/html

Content-Length: 655

Connection: close

CF-RAY: -

Response Body :

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
```

```
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

```
Response Code : HTTP/1.1 400 Bad Request
```

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

```
Server: cloudflare
Date: Sun, 30 Jun 2024 15:38:58 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -
```

```
Response Body :
```

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
```



```
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2086/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sun, 30 Jun 2024 15:38:53 GMT

Content-Type: text/plain; charset=UTF-8

Content-Length: 16

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Server: cloudflare

CF-RAY: 89bf3ef3d96a490c-SIN

Response Body :

error code: 1003

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

```
Response Code : HTTP/1.1 400 Bad Request
```

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

```
Server: cloudflare
Date: Sun, 30 Jun 2024 15:38:57 GMT
Content-Type: text/html
Content-Length: 655
Connection: close
CF-RAY: -
```

```
Response Body :
```

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
```

```
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: cloudflare

Date: Sun, 30 Jun 2024 15:38:46 GMT

Content-Type: text/html

Content-Length: 655

Connection: close

CF-RAY: -

Response Body :

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
```

```
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sun, 30 Jun 2024 15:38:54 GMT

Content-Type: text/plain; charset=UTF-8

Content-Length: 16

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Server: cloudflare

CF-RAY: 89bf3efc2f0d48e2-SIN

Response Body :

error code: 1003

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8443/www

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: cloudflare

Date: Sun, 30 Jun 2024 15:38:50 GMT

Content-Type: text/html

Content-Length: 655

Connection: close

CF-RAY: -

Response Body :

```
<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare</center>
</body>
</html>
```



```
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->  
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8880/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

HTTP/2 TLS Support: No

HTTP/2 Cleartext Support: No

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Sun, 30 Jun 2024 15:39:00 GMT

Content-Type: text/plain; charset=UTF-8

Content-Length: 16

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Server: cloudflare

CF-RAY: 89bf3f1dfc8240f2-SIN

Response Body :

error code: 1003

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/80/www

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

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/443/www

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

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2052/www

```
Port 2052/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2053/www

```
Port 2053/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2083/www

```
Port 2083/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2086/www

```
Port 2086/tcp was found to be open
```


Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2087/www

```
Port 2087/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/2096/www

```
Port 2096/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/8443/www

```
Port 8443/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/8880/www

```
Port 8880/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/06/04

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406300659
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : pentesting
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.226.130
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 85.366 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/6/30 20:55 IST
Scan duration : 1732 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

Plugin Output

tcp/0

```
Remote operating system : CISCO PIX 7.0  
Confidence level : 70  
Method : SinFP
```

```
The remote host is running CISCO PIX 7.0
```


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

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

Plugin Output

tcp/80/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2052/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2053/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2086/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

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


22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8443/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8880/www

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

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.226.130 to 172.67.186.112 :  
192.168.226.130  
192.168.226.2  
172.67.186.112
```

```
Hop Count: 2
```