

scan website learn

Wed, 24 Jan 2024 14:09:51 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 172.67.185.142

Vulnerabilities by Host

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

172.67.185.142



Host Information

IP: 172.67.185.142
OS: Linux Kernel 2.2, Linux Kernel 2.4, Linux Kernel 2.6

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: 2023/12/27

Plugin Output

tcp/0

The remote operating system matched the following CPE :

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

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 54
```

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/2082/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

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/2095/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

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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 403 Forbidden
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
Date: Wed, 24 Jan 2024 08:24:32 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: 84a6e175f99b3fe5-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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/443/www

Response Code : HTTP/1.1 400 Bad Request

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

Server: cloudflare
Date: Wed, 24 Jan 2024 08:24:30 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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2052/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Wed, 24 Jan 2024 08:24:35 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: 84a6e182e9024c03-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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2053/www

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

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

Server: cloudflare
Date: Wed, 24 Jan 2024 08:24:32 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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2082/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Wed, 24 Jan 2024 08:24:30 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: 84a6e1698f00602d-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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2083/www

Response Code : HTTP/1.1 400 Bad Request

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

Server: cloudflare
Date: Wed, 24 Jan 2024 08:24:36 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 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

Plugin Output

tcp/2086/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Wed, 24 Jan 2024 08:24:33 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: 84a6e1798c243fa7-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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2087/www

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

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

Server: cloudflare
Date: Wed, 24 Jan 2024 08:24:35 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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2095/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Wed, 24 Jan 2024 08:24:34 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: 84a6e17feb5d6bf4-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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/2096/www

Response Code : HTTP/1.1 400 Bad Request

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: cloudflare

Date: Wed, 24 Jan 2024 08:24:30 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 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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/8080/www

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1

SSL : no

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

Date: Wed, 24 Jan 2024 08:24:33 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
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Server: cloudflare
CF-RAY: 84a6e17c68f546c1-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 and HTTP pipelining are enabled, etc...

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

Solution

n/a

Risk Factor

None

Flight information

Published: 200

Page 3 of 3 | Submitter: HTTRD (1-1-1-100-B-1-B) | Date: 10/10/2019

卷之三十一

Protocol CSI

SSL : no
Keep Alive : no

Keep-Alive : no
Options allowed : (Not implemented)

options &
Headers :

Server: cloudflare

Server: Cloudflare
Date: Wed, 24 Jan 2024 08:24:32 GMT

Date: Wed, 24 Jan 2024
Content-Type: text/html

Content-Type: text/
Content-Length: 655

Content Ecosystem Connection:

CF-RAT: -

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

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/8880/www

```
Response Code : HTTP/1.1 403 Forbidden

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

Date: Wed, 24 Jan 2024 08:24:36 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: 84a6e18b9c47ab43-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: 2023/09/25

Plugin Output

Port 80/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/443/www

Port 443/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/2052/www

Port 2052/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/2053/www

Port 2053/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/2082/www

Port 2082/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/2083/www

Port 2083/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/2086/www

Port 2086/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

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: 2023/09/25

Plugin Output

tcp/2095/www

Port 2095/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: 2023/09/25

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: 2023/09/25

Plugin Output

tcp/8080/www

Port 8080/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

tcp/8443/www

Port 8443/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/09/25

Plugin Output

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 credentialled or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

Information about this scan :

Nessus version : 10.6.4
Nessus build : 20005
Plugin feed version : 202401240348
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : scan website learn
Scan policy used : Advanced Scan
Scanner IP : 10.15.192.220
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 212.553 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialled checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/1/24 13:33 India Standard Time

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.x
Confidence level : 54
Method : SinFP
```

```
The remote host is running Linux Kernel 2.x
```

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: 2023/07/10

Plugin Output

tcp/443/www

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

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2052/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2053/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2082/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2083/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2086/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2087/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2095/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2096/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8443/www

A web server seems to be running on this port.

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8880/www

A web server seems to be 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 10.15.192.220 to 172.67.185.142 :
10.15.192.220
10.15.192.10
115.242.182.201
?
103.198.140.64
103.198.140.89

Hop Count: 6

© 2024 Tenable™, Inc. All rights reserved.