Project website scan 2

Tue, 17 Oct 2023 19:06:37 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

182.73.197.23

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	4

Show

Project website scan 2

Tue, 17 Oct 2023 19:06:37 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

182.73.197.23

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	4

Scan Information

Start time: Tue Oct 17 18:52:09 2023

End time: Tue Oct 17 19:06:37 2023

Host Information

IP: 182.73.197.23

Vulnerabilities

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

```
Port 443/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- Whether the display of superseded patches is enabled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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310170357
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Project website scan 2
Scan policy used : Basic Network Scan
Scanner IP : 192.168.207.155
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 179.339 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
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 : 2023/10/17 18:52 India Standard Time
Scan duration : 793 sec
Scan for malware : no
```

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

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 443 was detected as being open initially but was found unresponsive later.
It is now unresponsive
```

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: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.207.155 to 182.73.197.23 :
192.168.207.155

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
```

```
An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

ttl was greater than 50 - Completing Traceroute.
192.168.207.111
?

Hop Count: 2
```

Project website scan 2

Tue, 17 Oct 2023 19:06:37 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

182.73.197.23

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	4

Host Information

IP: 182.73.197.23

Vulnerabilities

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

```
Port 443/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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310170357
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Project website scan 2
Scan policy used : Basic Network Scan
Scanner IP : 192.168.207.155
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 179.339 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
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 : 2023/10/17 18:52 India Standard Time
Scan duration : 793 sec
Scan for malware : no
```

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

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 443 was detected as being open initially but was found unresponsive later.
It is now unresponsive
```

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: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.207.155 to 182.73.197.23 :
192.168.207.155

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
```

```
An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

ttl was greater than 50 - Completing Traceroute.
192.168.207.111
?

Hop Count: 2
```

Project website scan 2

Tue, 17 Oct 2023 19:06:37 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

Collapse All | Expand All

10287 (1) - 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: 2023/06/26

Plugin Output

182.73.197.23 (udp/0)

```
For your information, here is the traceroute from 192.168.207.155 to 182.73.197.23 :
192.168.207.155

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
```

```
An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

ttl was greater than 50 - Completing Traceroute.
192.168.207.111
?

Hop Count: 2
```


10919 (1) - 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

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

182.73.197.23 (tcp/0)

```
Port 443 was detected as being open initially but was found unresponsive later.
It is now unresponsive
```

11219 (1) - 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

182.73.197.23 (tcp/443)

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

19506 (1) - 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: 2023/07/31

Plugin Output

182.73.197.23 (tcp/0)

```
Information about this scan :

Nessus version : 10.6.1
Nessus build : 20021
Plugin feed version : 202310170357
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Project website scan 2
Scan policy used : Basic Network Scan
Scanner IP : 192.168.207.155
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 179.339 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
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 : 2023/10/17 18:52 India Standard Time
Scan duration : 793 sec
```

```
Scan for malware : no
```