Plugin ID,CVE,CVSS v2.0 Base Score,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output,CVSS v3.0 Base Score,Risk Factor

"10180","","","None","10.0.2.10","tcp","0","Ping the remote host","It was possible to identify the status of the remote host (alive or

dead).","Nessus was able to determine if the remote host is alive using one or

more of the following ping types :

- An ARP ping, provided the host is on the local subnet

and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host

a packet with the flag SYN, and the host will reply with

a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).","n/a","","The remote host is up

The host replied to an ARP who-is query.

Hardware address : 08:00:27:08:4b:9b","","None"

"11219","","","None","10.0.2.10","tcp","22","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 22/tcp was found to be open","","None"

"19506","","","None","10.0.2.10","tcp","0","Nessus Scan Information","This plugin displays information about the Nessus scan.","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- Whether the display of superseded patches is enabled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.","n/a","","Information about this scan :

Nessus version : 10.1.2

Nessus build : 20068

Plugin feed version : 202204221540

Scanner edition used : Nessus Home

Scanner OS : LINUX

Scanner distribution : debian6-x86-64

Scan type : Normal

Scan name : host discovery

Scan policy used : Host Discovery

Scanner IP : 10.0.2.15

Port scanner(s) : nessus\_syn\_scanner

Port range : 1-65535

Ping RTT : 96.437 ms

Thorough tests : no

Experimental tests : no

Paranoia level : 1

Report verbosity : 1

Safe checks : yes

Optimize the test : yes

Credentialed checks : no

Patch management checks : None

Display superseded patches : yes (supersedence plugin launched)

CGI scanning : disabled

Web application tests : disabled

Max hosts : 256

Max checks : 5

Recv timeout : 5

Backports : None

Allow post-scan editing: Yes

Scan Start Date : 2022/4/22 12:48 MDT

Scan duration : 18 sec

","","None"

"10180","","","None","10.0.2.8","tcp","0","Ping the remote host","It was possible to identify the status of the remote host (alive or

dead).","Nessus was able to determine if the remote host is alive using one or

more of the following ping types :

- An ARP ping, provided the host is on the local subnet

and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host

a packet with the flag SYN, and the host will reply with

a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).","n/a","","The remote host is up

The host replied to an ARP who-is query.

Hardware address : 08:00:27:ea:75:a3","","None"

"11219","","","None","10.0.2.8","tcp","135","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 135/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","139","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 139/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","445","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 445/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","3389","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 3389/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","5357","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 5357/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","49152","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 49152/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","49153","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 49153/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","49154","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 49154/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","49155","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 49155/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","49156","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 49156/tcp was found to be open","","None"

"11219","","","None","10.0.2.8","tcp","49157","Nessus SYN scanner","It is possible to determine which TCP ports are open.","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.","Protect your target with an IP filter.","","Port 49157/tcp was found to be open","","None"

"19506","","","None","10.0.2.8","tcp","0","Nessus Scan Information","This plugin displays information about the Nessus scan.","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.","n/a","","Information about this scan :

Nessus version : 10.1.2

Nessus build : 20068

Plugin feed version : 202204221540

Scanner edition used : Nessus Home

Scanner OS : LINUX

Scanner distribution : debian6-x86-64

Scan type : Normal

Scan name : host discovery

Scan policy used : Host Discovery

Scanner IP : 10.0.2.15

Port scanner(s) : nessus\_syn\_scanner

Port range : 1-65535

Ping RTT : 97.287 ms

Thorough tests : no

Experimental tests : no

Paranoia level : 1

Report verbosity : 1

Safe checks : yes

Optimize the test : yes

Credentialed checks : no

Patch management checks : None

Display superseded patches : yes (supersedence plugin launched)

CGI scanning : disabled

Web application tests : disabled

Max hosts : 256

Max checks : 5

Recv timeout : 5

Backports : None

Allow post-scan editing: Yes

Scan Start Date : 2022/4/22 12:48 MDT

Scan duration : 62 sec

","","None"