Complete_OS_Scan

Report generated by Nessus™ Tue, 21 Jul 2020 06:25:35 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.43.1.....4
- MishaDey.....9

Vulnerabilities by Host

192.168.43.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	3

Scan Information

Start time: Tue Jul 21 06:01:51 2020
End time: Tue Jul 21 06:25:33 2020

Host Information

IP: 192.168.43.1

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: 2020/06/12

Plugin Output

tcp/53

```
Port 53/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.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2020/06/12

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.11.0
Plugin feed version : 202007201559
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Host Discovery
Scanner IP : 192.168.43.114
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/7/21 6:01 India Standard Time
Scan duration : 1419 sec
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

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).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2020/06/12

Plugin Output

tcp/0

```
The remote host is up
The host replied to an ARP who-is query.
Hardware address : 32:78:a4:f6:f0:a7
```

MishaDey

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	2

Scan Information

Start time: Tue Jul 21 06:04:16 2020
End time: Tue Jul 21 06:04:23 2020

Host Information

DNS Name: MishaDey
IP: 192.168.43.114

Vulnerabilities

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2020/06/12

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.11.0
Plugin feed version : 202007201559
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Host Discovery
Scanner IP : 192.168.43.114
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/7/21 6:04 India Standard Time
Scan duration : 7 sec
```

10180 - Ping the remote host

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

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).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2020/06/12

Plugin Output

tcp/0

```
The remote host is up
The host is the local scanner.
```