RFID Vuln Scan

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
10287	Traceroute Information	Info	10.10.10.15	UDP	0	No

Plugin Output:

Plugin Output: For your information, here is the traceroute from 10.6.6.205 to 10.10.10.15 :
10.6.6.205
10.6.6.244
10.254.254.10
?
10.10.10.15

Hop Count: 4

Synopsis: It was possible to obtain traceroute information.

Description: Makes a traceroute to the remote host.

Solution:

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
10919	Open Port Re-check	Info	10.10.10.15	TCP	0	No

Plugin Output:

Plugin Output: Port 443 was detected as being open initially but was found unresponsive later.
It is now open.
Port 5000 was detected as being open but is now unresponsive
Port 80 was detected as being open but is now unresponsive

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: - Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
11154	Unknown Service Detection: Banner Retrieval	Info	10.10.10.15	TCP	5000	No

Plugin Output:

Plugin Output:
If you know what this service is and think the banner could be used to

identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

Port : 5000
Type : get_http
Banner :
0x00: B9 9B 00 0A FE 00 23 F4 0D 0A ......#...

Synopsis: There is an unknown service running on the remote host.

Description: Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution:

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
11219	Nessus SYN scanner	Info	10.10.10.15	TCP	80	No

Plugin Output:
Plugin Output: 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.

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
11219	Nessus SYN scanner	Info	10.10.10.15	TCP	443	No

Plugin Output:
Plugin Output: 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.

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
11219	Nessus SYN scanner	Info	10.10.10.15	TCP	5000	No

Plugin Output:
Plugin Output: Port 5000/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.

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
11936	OS Identification	Info	10.10.10.15	TCP	0	No

Plugin Output:
Plugin Output:
Remote operating system : Microsoft Windows Server 2008 R2
Confidence level : 56
Method : MLSinFP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,

please email them to os-signatures@nessus.org. Be sure to include a brief description of the host itself, such as the actual operating system or product / model names.

SinFP:!:
P1:B11013:F0x12:W1024:O0204ffff:M556:
P2:B11013:F0x12:W1024:O0204ffff:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:181310_7_p=80R

The remote host is running Microsoft Windows Server 2008 R2

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:

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
19506	Nessus Scan Information	Info	10.10.10.15	TCP	0	No

Plugin Output:

Plugin Output: Information about this scan :

Nessus version : 8.13.1
Nessus build : 20257
Plugin feed version : 202108161759
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : a57787e0-570e-5de7-a819-c997fcc6d63d-903141/Chunk 1.
Scan policy used : a57787e0-570e-5de7-a819-c997fcc6d63d-903141/Full plug policy
Scanner IP : 10.6.6.205
Port scanner(s) : nessus_syn_scanner
Port range : 1-5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-59,61-224,242-248,256-268,280-287,308-322,333,344-700,702,704-707,709-711,721,723,729-731,737,740-742,744,747-754,758-765,767,769-777,779-783,786,787,799-801,808,810,828,829,847,848,860,871,873,886-888,898,900-904,911-913,927,950,953,975,989-1002,1005,1008,1010,1012,1023-1036,1040,1042,1045,1047-1112,1114-1117,1119,1120,1122-1127,1139,1154,1155,1161,1162,1167-1170,1178,1180,1181,1183-1188,1192,1194,1199-1231,1233-1286,1288-1774,1776-2028,2030,2032-2035,2037,2038,2040-2065,2067-2083,2086,2087,2089-2152,2155,2159-2167,2170-2177,2180,2181,2190,2191,2199-2202,2207,2213,2220-2224,2232-2246,2248-2255,2260,2273,2279-2289,2294-2311,2313-2371,2381-2824,2826-2854,2856-3096,3098-3403,3405-3545,3547-3707,3709-3765,3767-3800,3802,3845-3871,3875,3876,3885,3900,3928,3929,3939,3959,3970,3971,3984-3987,3994,3996-4036,4040-4042,4045,4080,4081,4092,4096-4100,4105,4111,4114,4132-4134,4138,4141-4145,4154,4160,4199-4201,4242,4274,4300,4321,4333,4343-4351,4353-4358,4369,4400,4442-4457,4480,4500,4501,4545-4547,4555,4557,4559,4567-4569,4600,4601,4658-4662,4665,4672,4711,4747,4752,4800-4802,4827,4837-4839,4848,4849,4868,4869,4885,4888,4894,4899,4950,4983,4987-4989,4998,5000-5011,5020-5025,5031,5042,5050-5057,5060,5061,5064-5066,5069,5071,5081,5093,5099-5102,5108,5137,5145,5150-5152,5154,5165,5168,5177,5178,5190-5193,5200-5203,5222,5223,5225,5226,5232,5236,5250,5251,5264,5265,5269,5272,5282,5300-5311,5314,5315,5321,5347,5351-5355,5400-5432,5435,5444,5454-5456,5461-5463,5465,5485,5500-5504,5510,5520,5521,5530,5540,5550,5553-5556,5566,5569,5595-5605,5631,5632,5666,5673-5680,5688,5690,5713-5717,5720,5727,5729,5730,5741,5742,5745,5746,5755,5757,5766-5768,5771,5800-5803,5813,5858,5859,5881,5882,5888,5889,5900-5903,5968,5969,5977-5979,5987-5991,5997-6073,6080,6085,6100-6112,6123,6129,6141-6150,6175-6177,6200,6253,6255,6257,6270,6284,6300,6321,6322,6343,6346,6347,6373,6382,6389,6400-6402,6404-6406,6443,6455,6456,6471,6500-6503,6505-6510,6543,6547-6550,6558,6566,6580-6582,6588,6620,6621,6623,6628,6631,6660,6665-6670,6672,6673,6680,6688,6699-6701,6714,6723,6767,6768,6776-6778,6788-6790,6831,6841,6842,6850,6881-6889,6891,6900,6901,6939,6961-6966,6969,6970,6998-7015,7020,7021,7030,7070,7080,7099-7101,7111,7121,7144,7161,7170,7174,7200,7201,7205,7210,7211,7269,7273,7280,7281,7283,7300-7308,7320,7323,7326,7391,7392,7395,7426-7431,7437,7461,7464,7491,7500,7501,7505,7510,7511,7544,7545,7560,7566,7570,7575,7580,7585,7588,7597,7624,7626,7627,7633,7634,7648-7651,7666,7674-7676,7743,7775-7779,7781,7786,7789,7797,7798,7800,7801,7845,7846,7875,7902,7913,7932,7933,7938,7955,7967,7979,7980,7999-8005,8007-8010,8019,8022,8028,8030,8032,8033,8044,8060,8074,8077,8080-8083,8088-8090,8098,8100,8115,8116,8118,8121-8123,8129-8132,8160,8161,8180-8194,8199-8201,8204-8208,8216,8224,8225,8245,8300,8302,8310,8311,8351,8376-8380,8383,8390,8400-8403,8416,8417,8431,8443-8445,8450,8473,8484,8500,8530,8554,8555,8649,8733,8763-8765,8786,8787,8804,8834,8863,8864,8866,8875,8880,8887-8894,8900,8901,8910,8911,8954,8987,8989,8999-9002,9006,9009,9020-9026,9043,9050,9080,9090,9091,9099-9103,9110,9111,9131,9152,9160-9164,9200-9207,9210,9211,9216,9217,9281-9285,9287,9292,9321,9343,9344,9346,9359,9370,9374,9390-9393,9396,9397,9400,9418,9433,9443,9495,9500,9535-9537,9593-9595,9600,9612,9704,9747,9753,9797,9800-9802,9872,9875,9876,9888,9889,9898-9901,9909,9911,9943,9945,9950-9952,9990-10012,10051,10067,10080-10083,10101-10103,10113-10116,10128,10167,10168,10202-10204,10252,10260,10288,10607,10616,10617,10626,10628,10666,10752,10990,11000,11001,11111,11201,11211,11223,11319-11321,11367,11371,11600,11720,11751,11965,11967,11999-12006,12076,12109,12168,12172,12174,12223,12321,12345,12346,12361,12362,12468,12701,12753,12754,13160,13223,13224,13324,13325,13666,13701,13702,13705,13706,13708-13718,13720-13722,13724,13782,13783,

13818-13822,14001,14002,14033,14034,14141,14145,14149,14194,14237,14238,14936,14937,14942,15000,15104,15126,15345,15363,
15858,16360,16361,16367,16368,16384,16660,16661,16959,16969,16991,17007,17185,17219,17300,17770-17772,17990,18000,18181-
18187,18190,18241,18264,18463,18769,18888,18889,19191,19194,19226,19283,19315,19398,19410-19412,19540,19541,19638,19726,
20000,20001,20005,20011,20012,20020,20031,20034,20168,20200,20202,20203,20221,20222,20670,20999,21000,21064,21065,21071,
21227,21300,21317,21490,21544,21554,21590,21700,21800,21845-21849,22000-22003,22222,22273,22289,22305,22321,22370,22555,
22800,22951,23456,23945,24000-24006,24242,24249,24345-24347,24386,24554,24677,24678,24922,25000-25009,25378,25445,25544,
25793,25867,25901,25903,26000,26208,26260-26264,26274,26740,26900,27000-27010,27015-27050,27345,27374,27444,27500,27504,
27665,27901,27910,27960,27961,27999,28001,28017,28070,28431,28910,29559,29760,29891,30001,30002,30100-30102,30303,30999,
31333,31335,31337-31339,31416,31457,31554,31556,31620,31666,31765,31785-31787,31789-31791,32000,32123,32261,32666,32768-
32780,32786,32787,32896,33270,33331,33434,33567,33568,33911,34012,34249,34324,34567,34952,36079,36794,36865,37475,37651,
38037,38201,38292,38293,39213,39681,40001,40412,40421-40426,40841-40843,41002,41080,41111,41170,41443,41508,41794,41795,
42508-42510,42800,43118,43188-43190,44321,44322,44333,44334,44337,44442,44443,44818,45000,45054,45678,45966,47000,47262,
47557,47624,47806,47808,47891,48000-48003,48556,49400,50000-50004,50013,50123,50505,50776,51051,51210,53001,54320,54321,
54345,56768,57341,59595,60008,60177,60179,61439-61441,61446,62078,65000,65301,65534,4433
Ping RTT : 31.250 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 : 30
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/8/17 15:04 Eastern Standard Time
Scan duration : 1197 sec

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:

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
22964	Service Detection	Info	10.10.10.15	TCP	80	No

Plugin Output:

Plugin Output: A web server is running on this port.

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:

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
45590	Common Platform Enumeration (CPE)	Info	10.10.10.15	TCP	0	No

Plugin Output:

Plugin Output:
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_server_2008:r2 -> Microsoft Windows Server 2008 R2

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.

Solution:

Plugin	Plugin Name	Severity	IP Address	Protocol	Port	Exploit?
54615	Device Type	Info	10.10.10.15	TCP	0	No

Plugin Output:

Plugin Output: Remote device type : unknown
Confidence level : 56

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: