Scan Report

May 13, 2019

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.0.0/24". The scan started at Mon May 13 15:38:46 2019 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.0.1 _gateway	0	1	1	5	0
192.168.0.2	0	0	0	0	0
192.168.0.3	0	0	0	0	0
192.168.0.4	0	0	0	0	0
192.168.0.5	0	0	0	0	0
192.168.0.6	0	0	0	0	0
192.168.0.7	0	0	0	0	0
192.168.0.8	0	0	0	0	0
192.168.0.9	0	0	0	0	0
192.168.0.10	0	0	0	0	0
192.168.0.11	0	0	0	0	0
192.168.0.12	0	0	0	0	0
192.168.0.13	0	0	0	0	0
192.168.0.14	0	0	0	0	0
192.168.0.15	0	0	0	0	0
192.168.0.16	0	0	0	0	0
192.168.0.17	0	0	0	0	0
192.168.0.18	0	0	0	0	0
192.168.0.19	0	0	0	0	0
192.168.0.20	0	0	0	0	0
192.168.0.21	0	0	0	0	0
192.168.0.22	0	0	0	0	0
192.168.0.23	0	0	0	0	0
192.168.0.24	0	0	0	0	0
192.168.0.25	0	0	0	0	0
192.168.0.26	0	0	0	0	0
192.168.0.27	0	0	0	0	0
192.168.0.28	0	0	0	0	0
192.168.0.29	0	0	0	0	0
192.168.0.30	0	0	0	0	0
192.168.0.31	0	0	0	0	0
192.168.0.32	0	0	0	0	0
192.168.0.33	0	0	0	0	0
192.168.0.34	0	0	0	0	0
192.168.0.35	0	0	0	0	0
192.168.0.36	0	0	0	0	0
192.168.0.37	0	0	0	0	0
192.168.0.38	0	0	0	0	0
192.168.0.39	0	0	0	0	0
192.168.0.40	0	0	0	0	0
192.168.0.41	0	0	0	0	0
192.168.0.42	0	0	0	0	0

. . . (continues) . . .

... (continued) ...

Host	High	Medium	Low	Log	False Positive
192.168.0.43	0	0	0	0	0
192.168.0.44	0	0	0	0	0
192.168.0.45	0	0	0	0	0
192.168.0.46	0	0	0	0	0
192.168.0.47	0	0	0	0	0
192.168.0.48	0	0	0	0	0
192.168.0.49	0	0	0	0	0
192.168.0.50	0	0	0	0	0
192.168.0.51	0	0	0	0	0
192.168.0.52	0	0	0	0	0
192.168.0.53	0	0	0	0	0
192.168.0.54	0	0	0	0	0
192.168.0.55	0	0	0	0	0
192.168.0.56	0	0	0	0	0
192.168.0.57	0	0	0	0	0
192.168.0.58	0	0	0	0	0
192.168.0.59	0	0	0	0	0
192.168.0.60	0	0	0	0	0
192.168.0.61	0	0	0	0	0
192.168.0.62	0	0	0	0	0
192.168.0.63	0	0	0	0	0
192.168.0.64	0	0	0	0	0
192.168.0.65	0	0	0	0	0
192.168.0.66	0	0	0	0	0
192.168.0.67	0	0	0	0	0
192.168.0.68	0	0	0	0	0
192.168.0.69	0	0	0	0	0
192.168.0.70	0	0	0	0	0
192.168.0.71	0	0	0	0	0
192.168.0.72	0	0	0	0	0
192.168.0.73	0	0	0	0	0
192.168.0.74	0	0	0	0	0
192.168.0.75	0	0	0	0	0
192.168.0.76	0	0	0	0	0
192.168.0.77	0	0	0	0	0
192.168.0.78	0	0	0	0	0
192.168.0.79	0	0	0	0	0
192.168.0.80	0	0	0	0	0
192.168.0.81	0	0	0	0	0
192.168.0.82	0	0	0	0	0
192.168.0.83	0	0	0	0	0
192.168.0.84	0	0	0	0	0
192.168.0.85	0	0	0	0	0
192.168.0.86	0	0	0	0	0

... (continues) ...

... (continued) ...

Host	High	Medium	Low	Log	False Positive
192.168.0.87	0	0	0	0	0
192.168.0.88	0	0	0	0	0
192.168.0.89	0	0	0	0	0
192.168.0.90	0	0	0	0	0
192.168.0.91	0	0	0	0	0
192.168.0.92	0	0	0	0	0
192.168.0.93	0	0	0	0	0
192.168.0.94	0	0	0	0	0
192.168.0.95	0	0	0	0	0
192.168.0.96	0	0	0	0	0
192.168.0.97	0	0	0	0	0
192.168.0.98	0	0	0	0	0
192.168.0.99	0	0	0	0	0
192.168.0.100	0	0	0	0	0
192.168.0.101	0	0	0	0	0
192.168.0.102	0	0	0	0	0
192.168.0.103	0	1	1	9	0
192.168.0.104	0	0	0	0	0
192.168.0.105	0	0	0	0	0
192.168.0.106	0	0	0	0	0
192.168.0.107	0	0	0	0	0
192.168.0.108	0	0	0	4	0
192.168.0.109	0	0	0	0	0
192.168.0.110	0	0	0	0	0
192.168.0.111	0	0	0	0	0
192.168.0.112	0	0	0	0	0
192.168.0.113	0	0	0	0	0
192.168.0.114	0	0	0	0	0
192.168.0.115	0	2	0	7	0
192.168.0.116	0	0	0	0	0
192.168.0.117	4	1	1	9	0
192.168.0.118	0	0	0	0	0
192.168.0.119	0	0	0	0	0
192.168.0.120	0	0	0	0	0
192.168.0.121	0	0	0	0	0
192.168.0.122	0	0	0	0	0
192.168.0.123	0	0	0	0	0
192.168.0.124	0	0	0	0	0
192.168.0.125	0	0	0	0	0
192.168.0.126	0	0	0	0	0
192.168.0.127	0	0	0	0	0
192.168.0.128	0	0	0	0	0
192.168.0.129	0	0	0	0	0
192.168.0.130	0	0	0	0	0

... (continues) ...

... (continued) ...

Host	High	Medium	Low	Log	False Positive
192.168.0.131	0	0	0	0	0
192.168.0.132	0	0	0	0	0
192.168.0.133	0	0	0	0	0
192.168.0.134	0	0	0	0	0
192.168.0.135	0	0	0	0	0
192.168.0.136	0	0	0	0	0
192.168.0.137	0	0	0	0	0
192.168.0.138	0	0	0	0	0
192.168.0.139	0	0	0	0	0
192.168.0.140	0	0	0	0	0
192.168.0.141	0	0	0	0	0
192.168.0.142	0	0	0	0	0
192.168.0.143	0	0	0	0	0
192.168.0.144	0	0	0	0	0
192.168.0.145	0	0	0	0	0
192.168.0.146	0	0	0	0	0
192.168.0.147	0	0	0	0	0
192.168.0.148	0	0	0	0	0
192.168.0.149	0	0	0	0	0
192.168.0.150	0	0	0	0	0
192.168.0.151	0	0	0	0	0
192.168.0.152	0	0	0	0	0
192.168.0.153	0	0	0	0	0
192.168.0.154	0	0	0	0	0
192.168.0.155	0	0	0	0	0
192.168.0.156	0	0	0	0	0
192.168.0.157	0	0	0	0	0
192.168.0.158	0	0	0	0	0
192.168.0.159	0	0	0	0	0
192.168.0.160	0	0	0	0	0
192.168.0.161	0	0	0	0	0
192.168.0.162	0	0	0	0	0
192.168.0.163	0	0	0	0	0
192.168.0.164	0	0	0	0	0
192.168.0.165	0	0	0	0	0
192.168.0.166	0	0	0	0	0
192.168.0.167	0	0	0	0	0
192.168.0.168	0	0	0	0	0
192.168.0.169	0	0	0	0	0
192.168.0.170	0	0	0	0	0
192.168.0.171	0	0	0	0	0
192.168.0.172	0	0	0	0	0
192.168.0.173	0	0	0	0	0
192.168.0.174	0	0	0	0	0

... (continues) ...

... (continued) ...

Host	High	Medium	Low	Log	False Positive
192.168.0.175	0	0	0	0	0
192.168.0.176	0	0	0	0	0
192.168.0.177	1	19	1	30	0
192.168.0.178	0	0	0	0	0
192.168.0.179	0	0	0	0	0
192.168.0.180	0	0	0	0	0
192.168.0.181	0	0	0	0	0
192.168.0.182	0	0	0	0	0
192.168.0.183	0	0	0	0	0
192.168.0.184	0	0	0	0	0
192.168.0.185	0	0	0	0	0
192.168.0.186	0	0	0	0	0
192.168.0.187	0	0	0	0	0
192.168.0.188	0	0	0	0	0
192.168.0.189	0	0	0	0	0
192.168.0.190	0	0	0	0	0
192.168.0.191	0	0	0	0	0
192.168.0.192	0	0	0	0	0
192.168.0.193	0	0	0	0	0
192.168.0.194	0	0	0	0	0
192.168.0.195	0	0	0	0	0
192.168.0.196	0	0	0	0	0
192.168.0.197	0	0	0	0	0
192.168.0.198	0	0	0	0	0
192.168.0.199	0	0	0	0	0
192.168.0.200	0	0	0	0	0
192.168.0.201	0	0	0	0	0
192.168.0.202	0	0	0	0	0
192.168.0.203	0	0	0	0	0
192.168.0.204	0	0	0	0	0
192.168.0.205	0	0	0	0	0
192.168.0.206	0	0	0	0	0
192.168.0.207	0	0	0	0	0
192.168.0.208	0	0	0	0	0
192.168.0.209	0	0	0	0	0
192.168.0.210	0	0	0	0	0
192.168.0.211	0	0	0	0	0
192.168.0.212	0	0	0	0	0
192.168.0.213	0	0	0	0	0
192.168.0.214	0	0	0	0	0
192.168.0.215	0	0	0	0	0
192.168.0.216	0	0	0	0	0
192.168.0.217	0	0	0	0	0
192.168.0.218	0	0	0	0	0

... (continues) ...

... (continued) ...

Host	High	Medium	Low	Log	False Positive
192.168.0.219	0	0	0	0	0
192.168.0.220	0	0	0	0	0
192.168.0.221	0	0	0	0	0
192.168.0.222	0	0	0	0	0
192.168.0.223	0	0	0	0	0
192.168.0.224	0	1	1	12	0
192.168.0.225	0	0	0	0	0
192.168.0.226	0	0	0	0	0
192.168.0.227	0	0	0	0	0
192.168.0.228	0	0	0	0	0
192.168.0.229	0	0	0	0	0
192.168.0.230	0	0	0	0	0
192.168.0.231	0	0	0	0	0
192.168.0.232	0	0	0	0	0
192.168.0.233	0	0	0	0	0
192.168.0.234	0	0	0	0	0
192.168.0.235	0	0	0	0	0
192.168.0.236	0	0	0	0	0
192.168.0.237	0	0	0	0	0
192.168.0.238	0	0	0	0	0
192.168.0.239	0	0	0	0	0
192.168.0.240	0	0	0	0	0
192.168.0.241	0	0	0	0	0
192.168.0.242	0	0	0	0	0
192.168.0.243	0	0	0	0	0
192.168.0.244	0	0	0	0	0
192.168.0.245	0	0	0	0	0
192.168.0.246	0	0	0	0	0
192.168.0.247	0	0	0	0	0
192.168.0.248	0	0	0	0	0
192.168.0.249	0	0	0	0	0
192.168.0.250	0	0	0	0	0
192.168.0.251	0	0	0	0	0
192.168.0.252	0	0	0	0	0
192.168.0.253	0	0	0	0	0
192.168.0.254	0	0	0	0	0
Total: 254	5	25	5	76	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.

This report contains all 111 results selected by the filtering described above. Before filtering there were 111 results.

2 Results per Host

2.1 192.168.0.1

Host scan start Mon May 13 15:38:50 2019 UTC
Host scan end Mon May 13 15:45:42 2019 UTC

Service (Port)	Threat Level
general/tcp	Medium
general/tcp	Low
53/tcp	Log
general/icmp	Log
general/tcp	Log
general/CPE-T	Log

2.1.1 Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Solution type: VendorFix
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS
TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details: `TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815

. . . continues on next page . . .

... continued from previous page ...

Version used: $Revision: 11066 $

References

CVE: CVE-2004-0230
BID:10183
Other:
URL:http://xforce.iss.net/xforce/xfdb/15886
URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

[return to 192.168.0.1]

2.1.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1001708423
Packet 2: 1001708535

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`
`URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152`

[return to 192.168.0.1]

2.1.3 Log 53/tcp

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result
`Nmap service detection (unknown) result for this port: domain`

Log Method
Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References
`Other:`
`URL:https://community.greenbone.net/c/vulnerability-tests`

[return to 192.168.0.1]

2.1.4 Log general/icmp

Log (CVSS: 0.0) NVT: ICMP Timestamp Detection
Summary The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Log Method Details: `ICMP Timestamp Detection` OID:1.3.6.1.4.1.25623.1.0.103190 Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

[return to 192.168.0.1]

2.1.5 Log general/tcp

Log (CVSS: 0.0) NVT: OS Detection Consolidation and Reporting
Summary This script consolidates the OS information detected by several NVTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
`Best matching OS:`
`OS: Linux Kernel`
`CPE: cpe:/o:linux:kernel`

... continues on next page ...

... continued from previous page ...

```
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.0.177 to 192.168.0.1:
192.168.0.177
192.168.0.1
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

[return to 192.168.0.1]

2.1.6 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
192.168.0.1|cpe:/o:linux:kernel

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 14324 $

References
Other:
URL:http://cpe.mitre.org/

[return to 192.168.0.1]

2.2 192.168.0.2

Host scan start Mon May 13 15:38:50 2019 UTC
Host scan end Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.3 192.168.0.3

Host scan start Mon May 13 15:38:50 2019 UTC
Host scan end Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.4 192.168.0.4

Host scan start Mon May 13 15:38:50 2019 UTC
Host scan end Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.5 192.168.0.5

Host scan start Mon May 13 15:38:50 2019 UTC
Host scan end Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.6 192.168.0.6

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.7 192.168.0.7

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.8 192.168.0.8

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.9 192.168.0.9

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.10 192.168.0.10

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.11 192.168.0.11

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.12 192.168.0.12

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.13 192.168.0.13

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.14 192.168.0.14

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.15 192.168.0.15

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.16 192.168.0.16

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.17 192.168.0.17

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.18 192.168.0.18

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.19 192.168.0.19

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.20 192.168.0.20

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:38:53 2019 UTC

Service (Port)	Threat Level

2.21 192.168.0.21

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.22 192.168.0.22

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.23 192.168.0.23

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.24 192.168.0.24

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.25 192.168.0.25

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.26 192.168.0.26

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.27 192.168.0.27

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.28 192.168.0.28

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.29 192.168.0.29

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:41:53 2019 UTC

Service (Port)	Threat Level

2.30 192.168.0.30

Host scan start	Mon May 13 15:38:50 2019 UTC
Host scan end	Mon May 13 15:40:53 2019 UTC

Service (Port)	Threat Level

2.31 192.168.0.31

Host scan start	Mon May 13 15:38:53 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.32 192.168.0.32

Host scan start	Mon May 13 15:38:53 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.33 192.168.0.33

Host scan start	Mon May 13 15:38:53 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.34 192.168.0.34

Host scan start	Mon May 13 15:38:53 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.35 192.168.0.35

Host scan start	Mon May 13 15:38:53 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.36 192.168.0.36

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:57 2019 UTC

Service (Port)	Threat Level

2.37 192.168.0.37

Host scan start	Mon May 13 15:38:53 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.38 192.168.0.38

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.39 192.168.0.39

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:57 2019 UTC

Service (Port)	Threat Level

2.40 192.168.0.40

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.41 192.168.0.41

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.42 192.168.0.42

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.43 192.168.0.43

Host scan start	Mon May 13 15:38:54 2019 UTC
Host scan end	Mon May 13 15:38:56 2019 UTC

Service (Port)	Threat Level

2.44 192.168.0.44

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.45 192.168.0.45

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.46 192.168.0.46

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.47 192.168.0.47

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.48 192.168.0.48

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.49 192.168.0.49

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.50 192.168.0.50

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.51 192.168.0.51

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.52 192.168.0.52

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.53 192.168.0.53

Host scan start	Mon May 13 15:38:56 2019 UTC
Host scan end	Mon May 13 15:38:58 2019 UTC

Service (Port)	Threat Level

2.54 192.168.0.54

Host scan start	Mon May 13 15:38:57 2019 UTC
Host scan end	Mon May 13 15:38:59 2019 UTC

Service (Port)	Threat Level

2.55 192.168.0.55

Host scan start	Mon May 13 15:38:57 2019 UTC
Host scan end	Mon May 13 15:38:59 2019 UTC

Service (Port)	Threat Level

2.56 192.168.0.56

Host scan start	Mon May 13 15:38:57 2019 UTC
Host scan end	Mon May 13 15:38:59 2019 UTC

Service (Port)	Threat Level

2.57 192.168.0.57

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.58 192.168.0.58

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.59 192.168.0.59

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.60 192.168.0.60

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.61 192.168.0.61

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.62 192.168.0.62

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.63 192.168.0.63

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.64 192.168.0.64

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.65 192.168.0.65

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.66 192.168.0.66

Host scan start	Mon May 13 15:38:58 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.67 192.168.0.67

Host scan start	Mon May 13 15:38:59 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.68 192.168.0.68

Host scan start	Mon May 13 15:38:59 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.69 192.168.0.69

Host scan start	Mon May 13 15:38:59 2019 UTC
Host scan end	Mon May 13 15:39:01 2019 UTC

Service (Port)	Threat Level

2.70 192.168.0.70

Host scan start	Mon May 13 15:39:01 2019 UTC
Host scan end	Mon May 13 15:39:04 2019 UTC

Service (Port)	Threat Level

2.71 192.168.0.71

Host scan start	Mon May 13 15:39:01 2019 UTC
Host scan end	Mon May 13 15:39:04 2019 UTC

Service (Port)	Threat Level

2.72 192.168.0.72

Host scan start	Mon May 13 15:39:01 2019 UTC
Host scan end	Mon May 13 15:39:04 2019 UTC

Service (Port)	Threat Level

2.73 192.168.0.73

Host scan start	Mon May 13 15:39:01 2019 UTC
Host scan end	Mon May 13 15:39:04 2019 UTC

Service (Port)	Threat Level

2.74 192.168.0.74

Host scan start	Mon May 13 15:39:01 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.75 192.168.0.75

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.76 192.168.0.76

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.77 192.168.0.77

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.78 192.168.0.78

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.79 192.168.0.79

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.80 192.168.0.80

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.81 192.168.0.81

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.82 192.168.0.82

Host scan start	Mon May 13 15:39:02 2019 UTC
Host scan end	Mon May 13 15:39:06 2019 UTC

Service (Port)	Threat Level

2.83 192.168.0.83

Host scan start	Mon May 13 15:39:05 2019 UTC
Host scan end	Mon May 13 15:39:08 2019 UTC

Service (Port)	Threat Level

2.84 192.168.0.84

Host scan start	Mon May 13 15:39:04 2019 UTC
Host scan end	Mon May 13 15:39:08 2019 UTC

Service (Port)	Threat Level

2.85 192.168.0.85

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:08 2019 UTC

Service (Port)	Threat Level

2.86 192.168.0.86

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.87 192.168.0.87

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:08 2019 UTC

Service (Port)	Threat Level

2.88 192.168.0.88

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:08 2019 UTC

Service (Port)	Threat Level

2.89 192.168.0.89

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.90 192.168.0.90

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.91 192.168.0.91

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.92 192.168.0.92

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.93 192.168.0.93

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.94 192.168.0.94

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.95 192.168.0.95

Host scan start	Mon May 13 15:39:06 2019 UTC
Host scan end	Mon May 13 15:39:09 2019 UTC

Service (Port)	Threat Level

2.96 192.168.0.96

Host scan start	Mon May 13 15:39:08 2019 UTC
Host scan end	Mon May 13 15:39:10 2019 UTC

Service (Port)	Threat Level

2.97 192.168.0.97

Host scan start	Mon May 13 15:39:08 2019 UTC
Host scan end	Mon May 13 15:39:10 2019 UTC

Service (Port)	Threat Level

2.98 192.168.0.98

Host scan start	Mon May 13 15:39:09 2019 UTC
Host scan end	Mon May 13 15:39:12 2019 UTC

Service (Port)	Threat Level

2.99 192.168.0.99

Host scan start	Mon May 13 15:39:09 2019 UTC
Host scan end	Mon May 13 15:39:12 2019 UTC

Service (Port)	Threat Level

2.100 192.168.0.100

Host scan start	Mon May 13 15:39:09 2019 UTC
Host scan end	Mon May 13 15:39:12 2019 UTC

Service (Port)	Threat Level

2.101 192.168.0.101

Host scan start	Mon May 13 15:39:09 2019 UTC
Host scan end	Mon May 13 15:39:12 2019 UTC

Service (Port)	Threat Level

2.102 192.168.0.102

Host scan start	Mon May 13 15:39:09 2019 UTC
Host scan end	Mon May 13 15:39:14 2019 UTC

Service (Port)	Threat Level

2.103 192.168.0.103

Host scan start	Mon May 13 15:39:09 2019 UTC
Host scan end	Mon May 13 15:44:51 2019 UTC

Service (Port)	Threat Level
general/tcp	Medium
general/tcp	Low
general/CPE-T	Log
general/icmp	Log
8000/tcp	Log
8080/tcp	Log
general/tcp	Log

2.103.1 Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Solution type: VendorFix
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS
TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details: `TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: `$Revision: 11066 $`

References
`CVE: CVE-2004-0230`
`BID:10183`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/15886`
`URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006`
`URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx`
`URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`

[return to 192.168.0.103]

2.103.2 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
`It was detected that the host implements RFC1323.`
`The following timestamps were retrieved with a delay of 1 seconds in-between:`
`Packet 1: 375003174`
`Packet 2: 375004298`

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

... continues on next page ...

... continued from previous page ...

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`
`URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152`

[return to 192.168.0.103]

2.103.3 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
`192.168.0.103|cpe:/o:linux:kernel`

Log Method
Details: `CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 14324 $`

References
`Other:`
`URL:http://cpe.mitre.org/`

[return to 192.168.0.103]

2.103.4 Log general/icmp

Log (CVSS: 0.0) NVT: ICMP Timestamp Detection
Summary The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Log Method Details: `ICMP Timestamp Detection` OID:1.3.6.1.4.1.25623.1.0.103190 Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

[return to 192.168.0.103]

2.103.5 Log 8000/tcp

Log (CVSS: 0.0) NVT: LDAP Detection
Summary A LDAP Server is running at this host. The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Log Method Details: `LDAP Detection` OID:1.3.6.1.4.1.25623.1.0.100082 Version used: `$Revision: 13541 $`

[return to 192.168.0.103]

2.103.6 Log 8080/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "192.168.0.103" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://192.168.0.103:8080/
http://192.168.0.103:8080/upnpdev/pres/uuid_175181e0-1dd2-11b2-bf93-c677af100e95
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://192.168.0.103:8080/upnpdev/pres/uuid_175181e0-1dd2-11b2-bf93-c677af100e95
↪/ (type [dms] )
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038

. . . continues on next page . . .

... continued from previous page ...

Version used: $Revision: 13679 $

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result
Missing Headers

Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection

Log Method
Details: HTTP Security Headers Detection
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: $Revision: 10899 $

References
Other:
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
URL:https://securityheaders.io/

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port

... continues on next page ...

. . . continued from previous page . . .

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

[return to 192.168.0.103]

2.103.7 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: Traceroute

Summary

. . . continues on next page . . .

... continued from previous page ...

A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.0.177 to 192.168.0.103:
192.168.0.177
192.168.0.103
```

Solution

Block unwanted packets from escaping your network.

Log Method

Details: `Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 10411 $`

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary

This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://community.greenbone.net/c/vulnera
↪bility-tests:
Banner: SERVER: BH
Identified from: HTTP Server banner on port 8080/tcp
```

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 192.168.0.103]

2.104 192.168.0.104

Host scan start Mon May 13 15:39:09 2019 UTC
Host scan end Mon May 13 15:39:12 2019 UTC

Service (Port)	Threat Level

2.105 192.168.0.105

Host scan start Mon May 13 15:39:09 2019 UTC
Host scan end Mon May 13 15:39:14 2019 UTC

Service (Port)	Threat Level

2.106 192.168.0.106

Host scan start Mon May 13 15:39:09 2019 UTC
Host scan end Mon May 13 15:39:14 2019 UTC

Service (Port)	Threat Level

2.107 192.168.0.107

Host scan start Mon May 13 15:39:10 2019 UTC
Host scan end Mon May 13 15:39:13 2019 UTC

Service (Port)	Threat Level

2.108 192.168.0.108

Host scan start Mon May 13 15:39:10 2019 UTC
Host scan end Mon May 13 15:40:32 2019 UTC

Service (Port)	Threat Level
general/icmp	Log
general/tcp	Log
general/CPE-T	Log

2.108.1 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

[return to 192.168.0.108]

2.108.2 Log general/tcp

Log (CVSS: 0.0)
NVT: Check for enabled / working Port scanner plugin

Summary
The script reports if:
- a custom scan configuration is in use without having a Port scanner from the 'Port scanners' family enabled.
- a port scanner plugin was running into a timeout.
- a required port scanner (e.g. nmap) is not installed.

Vulnerability Detection Result
```
The host wasn't scanned due to the following possible reasons:
 - No Port scanner plugin from the "Port scanners" family is included in this sc
↪an configuration. Recommended: Nmap (NASL wrapper).
 - The Port scanner plugin reached a timeout during the port scanning phase. Ple
↪ase either choose a port range for this target containing less ports or raise
↪the "scanner_plugins_timeout" scanner preference to a higher timeout.
```

Solution
Based on the script output please:

... continues on next page ...

... continued from previous page ...

- add a Port scanner plugin from the 'Port scanners' family to this scan configuration. Recommended: Nmap (NASL wrapper).
- either choose a port range for this target containing less ports or raise the 'scanner_plugins_timeout' scanner preference to a higher timeout.
- install the 'nmap' binary/package or make it accessible to the scanner.

Log Method
Details: `Check for enabled / working Port scanner plugin`
OID:1.3.6.1.4.1.25623.1.0.108323
Version used: `$Revision: 10122 $`

References
```
Other:
  URL:http://docs.greenbone.net/GSM-Manual/gos-4/en/performance.html#scan-perfor
↪mance
   URL:http://docs.greenbone.net/GSM-Manual/gos-4/en/vulnerabilitymanagement.htm
↪l?highlight=scanner_plugins_timeout#general-preferences
```

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
```

Log Method
Details: `OS Detection Consolidation and Reporting`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `2019-05-02T04:45:21+0000`

References
```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 192.168.0.108]

2.108.3 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.
Vulnerability Detection Result 192.168.0.108|cpe:/o:linux:kernel
Log Method Details: CPE Inventory OID:1.3.6.1.4.1.25623.1.0.810002 Version used: $Revision: 14324 $
References Other: URL:http://cpe.mitre.org/

[return to 192.168.0.108]

2.109 192.168.0.109

Host scan start	Mon May 13 15:39:10 2019 UTC
Host scan end	Mon May 13 15:39:14 2019 UTC

Service (Port)	Threat Level

2.110 192.168.0.110

Host scan start	Mon May 13 15:39:10 2019 UTC
Host scan end	Mon May 13 15:39:14 2019 UTC

Service (Port)	Threat Level

2.111 192.168.0.111

Host scan start	Mon May 13 15:39:12 2019 UTC
Host scan end	Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.112 192.168.0.112

Host scan start Mon May 13 15:39:12 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.113 192.168.0.113

Host scan start Mon May 13 15:39:12 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.114 192.168.0.114

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.115 192.168.0.115

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:44:12 2019 UTC

Service (Port)	Threat Level
80/tcp	Medium
general/tcp	Medium
80/tcp	Log
general/CPE-T	Log
general/tcp	Log

2.115.1 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
The following URLs requires Basic Authentication (URL:realm name):
http://192.168.0.115/:"USER LOGIN"

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: $Revision: 10726 $

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

[return to 192.168.0.115]

2.115.2 Medium general/tcp

Medium (CVSS: 5.0)
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability

Summary
The host is running TCP services and is prone to denial of service vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to guess sequence numbers and cause a denial of service to persistent TCP connections by repeatedly injecting a TCP RST packet.

Solution
Solution type: VendorFix
Please see the referenced advisories for more information on obtaining and applying fixes.

Affected Software/OS
TCP/IP v4

Vulnerability Insight
The flaw is triggered when spoofed TCP Reset packets are received by the targeted TCP stack and will result in loss of availability for the attacked TCP services.

Vulnerability Detection Method
A TCP Reset packet with a different sequence number is sent to the target. A previously open connection is then checked to see if the target closed it or not.
Details: `TCP Sequence Number Approximation Reset Denial of Service Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902815
Version used: `$Revision: 11066 $`

References
`CVE: CVE-2004-0230`
`BID:10183`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/15886`
`URL:http://www.us-cert.gov/cas/techalerts/TA04-111A.html`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950`
`URL:http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006`
`URL:http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx`
`URL:http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`
`URL:http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html`

[return to 192.168.0.115]

2.115.3 Log 80/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "192.168.0.115" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.0.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories require authentication and are tested by the script "H
↪TTP Brute Force Logins with default Credentials (OID: 1.3.6.1.4.1.25623.1.0.10
↪8041)":
http://192.168.0.115/
The following directories were used for CGI scanning:
http://192.168.0.115/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 13679 $

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
`The remote web server type is :`
`HTTPD`

Solution
- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method
Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 11585 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

[return to 192.168.0.115]

2.115.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary

. . . continues on next page . . .

... continued from previous page ...

This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
192.168.0.115|cpe:/o:netbsd:netbsd

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 14324 $

References
Other:
URL:http://cpe.mitre.org/

[return to 192.168.0.115]

2.115.5 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: OpenBSD
CPE: cpe:/o:openbsd:openbsd
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: HP UX
CPE: cpe:/o:hp:hp-ux
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
OS: Cisco IOS
CPE: cpe:/o:cisco:ios
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint
```

... continues on next page ...

... continued from previous page ...

OS: NetBSD
CPE: cpe:/o:netbsd:netbsd
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (ICMP based OS Fingerprinting)
Concluded from ICMP based OS fingerprint

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 192.168.0.177 to 192.168.0.115:
192.168.0.177
192.168.0.115

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

Log (CVSS: 0.0)
NVT: Unknown OS and Service Banner Reporting

Summary
This NVT consolidates and reports the information collected by the following NVTs:
- Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154)
- Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)
- Service Detection (wrapped) with nmap (OID: 1.3.6.1.4.1.25623.1.0.108525)
- OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

... continues on next page ...

... continued from previous page ...

If you know any of the information reported here, please send the full output to the referenced community portal.

Vulnerability Detection Result

```
Unknown banners have been collected which might help to identify the OS running
↪on this host. If these banners containing information about the host OS please
↪ report the following information to https://community.greenbone.net/c/vulnera
↪bility-tests:
Banner: Server: HTTPD
Identified from: HTTP Server banner on port 80/tcp
```

Log Method

Details: `Unknown OS and Service Banner Reporting`
OID:1.3.6.1.4.1.25623.1.0.108441
Version used: `$Revision: 12934 $`

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

[return to 192.168.0.115]

2.116 192.168.0.116

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.117 192.168.0.117

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:42:10 2019 UTC

Service (Port)	Threat Level
445/tcp	High
general/tcp	High
135/tcp	Medium
general/tcp	Low
general/icmp	Log
445/tcp	Log
135/tcp	Log
139/tcp	Log
general/tcp	Log
general/CPE-T	Log

2.117.1 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2019-05-03T10:54:50+0000`

References
```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

High (CVSS: 10.0)
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS10-012.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
Microsoft Windows 7
Microsoft Windows 2000 Service Pack and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2003 Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Vulnerability Detection Method
Details: `Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)`
OID:1.3.6.1.4.1.25623.1.0.902269
Version used: `2019-05-03T10:54:50+0000`

References
`CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231`
`Other:`
`URL:http://secunia.com/advisories/38510/`
`URL:http://support.microsoft.com/kb/971468`
`URL:http://www.vupen.com/english/advisories/2010/0345`
`URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx`

High (CVSS: 10.0)
NVT: Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability

Summary
This host is missing a critical security update according to Microsoft Bulletin MS09-050.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can exploit this issue to execute code with SYSTEM-level privileges. Failed exploit attempts will likely cause denial-of-service conditions.

Solution
Solution type: VendorFix

Affected Software/OS
- Windows 7 RC
- Windows Vista and
- Windows 2008 Server

Vulnerability Insight
Multiple vulnerabilities exists,
- A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB version 2 (SMBv2) packets.
- Unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Vulnerability Detection Method
Details: `Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.900965
Version used: `$Revision: 12602 $`

References
```
CVE: CVE-2009-2526, CVE-2009-2532, CVE-2009-3103
BID:36299
Other:
  URL:http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx
```

[return to 192.168.0.117]

2.117.2 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/o:microsoft:windows_vista:-:sp2
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)

Summary
OS End Of Life Detection
The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
The "Windows Vista" Operating System on the remote host has reached the end of l
↪ife.
CPE: cpe:/o:microsoft:windows_vista:-:sp2
Installed version,
build or SP: sp2
EOL date: 2017-04-11
EOL info: https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Windows%20Vista&Filter=FilterNO

Solution
Solution type: Mitigation

Vulnerability Detection Method
Details: OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 8927 $

Product Detection Result
Product: cpe:/o:microsoft:windows_vista:-:sp2
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 192.168.0.117]

2.117.3 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49152]
Port: 49153/tcp
     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49153]
     Annotation: Security Center
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49154]
     Annotation: AppInfo
     UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49154]
     Annotation: AppInfo
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49154]
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49154]
     Annotation: IKE/Authip API
     UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49154]
     Annotation: AppInfo
Port: 49155/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49156/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.0.117[49156]
Port: 49177/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.117[49177]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
```

... continues on next page ...

... continued from previous page ...

```
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `$Revision: 6319 $`

[return to 192.168.0.117]

2.117.4 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1274206
Packet 2: 1274316
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `$Revision: 14310 $`

References
`Other:`
`URL:http://www.ietf.org/rfc/rfc1323.txt`
`URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152`

[return to 192.168.0.117]

2.117.5 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

Summary
The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details: `ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 10411 $`

References
`CVE: CVE-1999-0524`
`Other:`
`URL:http://www.ietf.org/rfc/rfc0792.txt`

[return to 192.168.0.117]

2.117.6 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
`Detected SMB workgroup: WORKGROUP`
`Detected SMB server: Windows Vista (TM) Home Premium 6.0`
`Detected OS: Windows Vista (TM) Home Premium 6002 Service Pack 2`

Log Method
Details: `SMB NativeLanMan`
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: `2019-04-24T11:06:32+0000`

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
`SMBv1 and SMBv2 are enabled on remote target`

Log Method
Details: `SMB Remote Version Detection`
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: `$Revision: 10898 $`

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
`A CIFS server is running on this port`

Log Method
. . . continues on next page . . .

... continued from previous page ...

Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

[return to 192.168.0.117]

2.117.7 Log 135/tcp

Log (CVSS: 0.0)
NVT: DCE/RPC and MSRPC Services Enumeration

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)

Vulnerability Detection Result
A DCE endpoint resolution service seems to be running on this port.

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this port.

Log Method
Details: DCE/RPC and MSRPC Services Enumeration
OID:1.3.6.1.4.1.25623.1.0.108044
Version used: $Revision: 11885 $

[return to 192.168.0.117]

2.117.8 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A SMB server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

[return to 192.168.0.117]

2.117.9 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Windows Vista (TM) Home Premium 6002 Service Pack 2
CPE: cpe:/o:microsoft:windows_vista:-:sp2
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows Vista (TM) H
↪ome Premium 6002 Service Pack 2; SMB String: Windows Vista (TM) Home Premium 6
↪.0
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
Other:

... continues on next page ...

... continued from previous page ...

URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 192.168.0.177 to 192.168.0.117:
192.168.0.177
192.168.0.117

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

[return to 192.168.0.117]

2.117.10 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
192.168.0.117|cpe:/o:microsoft:windows_vista:-:sp2

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 14324 $

References
Other:

... continues on next page ...

... continued from previous page ...

URL:http://cpe.mitre.org/

[return to 192.168.0.117]

2.118 192.168.0.118

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.119 192.168.0.119

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.120 192.168.0.120

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:39:16 2019 UTC

Service (Port)	Threat Level

2.121 192.168.0.121

Host scan start Mon May 13 15:39:14 2019 UTC
Host scan end Mon May 13 15:39:18 2019 UTC

Service (Port)	Threat Level

2.122 192.168.0.122

Host scan start Mon May 13 15:39:16 2019 UTC
Host scan end Mon May 13 15:39:18 2019 UTC

Service (Port)	Threat Level

2.123 192.168.0.123

Host scan start	Mon May 13 15:39:16 2019 UTC
Host scan end	Mon May 13 15:39:20 2019 UTC

Service (Port)	Threat Level

2.124 192.168.0.124

Host scan start	Mon May 13 15:39:16 2019 UTC
Host scan end	Mon May 13 15:39:21 2019 UTC

Service (Port)	Threat Level

2.125 192.168.0.125

Host scan start	Mon May 13 15:39:16 2019 UTC
Host scan end	Mon May 13 15:39:20 2019 UTC

Service (Port)	Threat Level

2.126 192.168.0.126

Host scan start	Mon May 13 15:39:16 2019 UTC
Host scan end	Mon May 13 15:39:20 2019 UTC

Service (Port)	Threat Level

2.127 192.168.0.127

Host scan start	Mon May 13 15:39:18 2019 UTC
Host scan end	Mon May 13 15:39:20 2019 UTC

Service (Port)	Threat Level

2.128 192.168.0.128

Host scan start	Mon May 13 15:39:18 2019 UTC
Host scan end	Mon May 13 15:39:20 2019 UTC

Service (Port)	Threat Level

2.129 192.168.0.129

Host scan start	Mon May 13 15:39:18 2019 UTC
Host scan end	Mon May 13 15:39:20 2019 UTC

Service (Port)	Threat Level

2.130 192.168.0.130

Host scan start	Mon May 13 15:39:18 2019 UTC
Host scan end	Mon May 13 15:39:21 2019 UTC

Service (Port)	Threat Level

2.131 192.168.0.131

Host scan start	Mon May 13 15:39:18 2019 UTC
Host scan end	Mon May 13 15:39:21 2019 UTC

Service (Port)	Threat Level

2.132 192.168.0.132

Host scan start	Mon May 13 15:39:20 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.133 192.168.0.133

Host scan start	Mon May 13 15:39:20 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.134 192.168.0.134

Host scan start	Mon May 13 15:39:20 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.135 192.168.0.135

Host scan start	Mon May 13 15:39:20 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.136 192.168.0.136

Host scan start	Mon May 13 15:39:21 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.137 192.168.0.137

Host scan start	Mon May 13 15:39:21 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.138 192.168.0.138

Host scan start	Mon May 13 15:39:21 2019 UTC
Host scan end	Mon May 13 15:39:24 2019 UTC

Service (Port)	Threat Level

2.139 192.168.0.139

Host scan start	Mon May 13 15:39:21 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.140 192.168.0.140

Host scan start	Mon May 13 15:39:21 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.141 192.168.0.141

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:27 2019 UTC

Service (Port)	Threat Level

2.142 192.168.0.142

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.143 192.168.0.143

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.144 192.168.0.144

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.145 192.168.0.145

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.146 192.168.0.146

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:26 2019 UTC

Service (Port)	Threat Level

2.147 192.168.0.147

Host scan start	Mon May 13 15:39:24 2019 UTC
Host scan end	Mon May 13 15:39:27 2019 UTC

Service (Port)	Threat Level

2.148 192.168.0.148

Host scan start	Mon May 13 15:39:26 2019 UTC
Host scan end	Mon May 13 15:39:28 2019 UTC

Service (Port)	Threat Level

2.149 192.168.0.149

Host scan start	Mon May 13 15:39:26 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.150 192.168.0.150

Host scan start	Mon May 13 15:39:26 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.151 192.168.0.151

Host scan start	Mon May 13 15:39:26 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.152 192.168.0.152

Host scan start	Mon May 13 15:39:26 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.153 192.168.0.153

Host scan start	Mon May 13 15:39:26 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.154 192.168.0.154

Host scan start	Mon May 13 15:39:27 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.155 192.168.0.155

Host scan start	Mon May 13 15:39:27 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.156 192.168.0.156

Host scan start	Mon May 13 15:39:27 2019 UTC
Host scan end	Mon May 13 15:39:29 2019 UTC

Service (Port)	Threat Level

2.157 192.168.0.157

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.158 192.168.0.158

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.159 192.168.0.159

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.160 192.168.0.160

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.161 192.168.0.161

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.162 192.168.0.162

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.163 192.168.0.163

Host scan start	Mon May 13 15:39:30 2019 UTC
Host scan end	Mon May 13 15:39:32 2019 UTC

Service (Port)	Threat Level

2.164 192.168.0.164

Host scan start	Mon May 13 15:39:30 2019 UTC
Host scan end	Mon May 13 15:39:32 2019 UTC

Service (Port)	Threat Level

2.165 192.168.0.165

Host scan start	Mon May 13 15:39:29 2019 UTC
Host scan end	Mon May 13 15:39:31 2019 UTC

Service (Port)	Threat Level

2.166 192.168.0.166

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:33 2019 UTC

Service (Port)	Threat Level

2.167 192.168.0.167

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:33 2019 UTC

Service (Port)	Threat Level

2.168 192.168.0.168

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:33 2019 UTC

Service (Port)	Threat Level

2.169 192.168.0.169

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:33 2019 UTC

Service (Port)	Threat Level

2.170 192.168.0.170

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:33 2019 UTC

Service (Port)	Threat Level

2.171 192.168.0.171

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:33 2019 UTC

Service (Port)	Threat Level

2.172 192.168.0.172

Host scan start	Mon May 13 15:39:31 2019 UTC
Host scan end	Mon May 13 15:39:34 2019 UTC

Service (Port)	Threat Level

2.173 192.168.0.173

Host scan start	Mon May 13 15:39:32 2019 UTC
Host scan end	Mon May 13 15:39:34 2019 UTC

Service (Port)	Threat Level

2.174 192.168.0.174

Host scan start	Mon May 13 15:39:32 2019 UTC
Host scan end	Mon May 13 15:39:34 2019 UTC

Service (Port)	Threat Level

2.175 192.168.0.175

Host scan start	Mon May 13 15:39:33 2019 UTC
Host scan end	Mon May 13 15:39:35 2019 UTC

Service (Port)	Threat Level

2.176 192.168.0.176

Host scan start	Mon May 13 15:39:33 2019 UTC
Host scan end	Mon May 13 15:39:35 2019 UTC

Service (Port)	Threat Level

2.177 192.168.0.177

Host scan start Mon May 13 15:39:33 2019 UTC
Host scan end

Service (Port)	Threat Level
general/tcp	High
21/tcp	Medium
4000/tcp	Medium
445/tcp	Medium
80/tcp	Medium
general/tcp	Medium
general/tcp	Low
21/tcp	Log
3306/tcp	Log
4000/tcp	Log
445/tcp	Log
80/tcp	Log
general/tcp	Log
139/tcp	Log

2.177.1 High general/tcp

High (CVSS: 7.2)
NVT: Apache HTTP Server < 2.4.39 Privilege Escalation Vulnerability (Linux)

Summary
In Apache HTTP Server, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.39`

Solution
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP server version 2.4.38 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.39 Privilege Escalation Vulnerability (Linux)`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.142219
Version used: 2019-04-15T07:08:44+0000

References
CVE: CVE-2019-0211
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

[return to 192.168.0.177]

2.177.2 Medium 21/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↪. Response(s):
Anonymous sessions: 331 Please specify the password.
Non-anonymous sessions: 331 Please specify the password.

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: $Revision: 13611 $

[return to 192.168.0.177]

2.177.3 Medium 4000/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: $Revision: 5232 $

References
CVE: CVE-2016-2183, CVE-2016-6329
Other:
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://sweet32.info/

[return to 192.168.0.177]

2.177.4 Medium 445/tcp

Medium (CVSS: 4.0)
NVT: Samba 'AD LDAP' Information Disclosure Vulnerability - Aug18

... continues on next page ...

... continued from previous page ...

Summary
This host is running Samba and is prone to an information disclosure vulnerability.

Vulnerability Detection Result
```
Installed version: 4.7.6
Fixed version:     4.7.9 or apply patch
Installation
path / port:       445/tcp
```

Impact
Successful exploitation will allow an attacker to gain access to confidential attribute values.

Solution
Solution type: VendorFix
Upgrade to Samba 4.8.4 or 4.7.9 or 4.6.16 or later. Please see the references for more information.

Affected Software/OS
All versions of Samba from 4.0.0 onwards

Vulnerability Insight
The flaw exists due to a missing access control checks.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba 'AD LDAP' Information Disclosure Vulnerability - Aug18`
OID:1.3.6.1.4.1.25623.1.0.813784
Version used: `2019-05-03T08:55:39+0000`

References
```
CVE: CVE-2018-10919
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-10919.html
   URL:https://www.samba.org/samba/history/samba-4.8.4.html
   URL:https://www.samba.org/samba/history/samba-4.7.9.html
   URL:https://www.samba.org/samba/history/samba-4.6.16.html
   URL:https://www.samba.org
```

Medium (CVSS: 6.5)
NVT: Samba 'libsmbclient' Heap Buffer Overflow Vulnerability - Aug18

Summary
This host is running Samba and is prone to a heap based buffer overflow vulnerability.

Vulnerability Detection Result
```
Installed version: 4.7.6
Fixed version:     4.7.9 or apply patch
```

... continues on next page ...

... continued from previous page ...

```
Installation
path / port:        445/tcp
```

Impact
Successful exploitation will allow an attacker to conduct a denial of service attack.

Solution
Solution type: VendorFix
Upgrade to Samba 4.6.16, 4.7.9 or 4.8.4 or later. Please see the references for more information.

Affected Software/OS
Samba versions 3.2.0 through 4.8.3

Vulnerability Insight
The flaw exists due to insufficient input validation on client directory listing in libsmbclient.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba 'libsmbclient' Heap Buffer Overflow Vulnerability - Aug18`
OID:1.3.6.1.4.1.25623.1.0.813782
Version used: `2019-05-03T08:55:39+0000`

References

```
CVE: CVE-2018-10858
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-10858.html
   URL:https://www.samba.org/samba/history/samba-4.6.16.html
   URL:https://www.samba.org/samba/history/samba-4.7.9.html
   URL:https://www.samba.org/samba/history/samba-4.8.4.html
   URL:https://www.samba.org
```

Medium (CVSS: 4.0)
NVT: Samba 4.x Multiple DoS Vulnerabilities

Summary
Samba is prone to multiple vulnerabilities.

Vulnerability Detection Result

```
Installed version: 4.7.6
Fixed version:     4.7.12
Installation
path / port:       445/tcp
```

Solution
Solution type: VendorFix
Update to version 4.7.12, 4.8.7, 4.9.3 or later.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
Samba version 4.x.x.

Vulnerability Insight
Samba is prone to multiple vulnerabilities:
- CNAME loops can cause DNS server crashes, and CNAMEs can be added by unprivileged users. (CVE-2018-14629)
- A user able to read more than 256MB of LDAP entries can crash the Samba AD DC's LDAP server. (CVE-2018-16851)

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba 4.x Multiple DoS Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.141732
Version used: `$Revision: 13517 $`

References
```
CVE: CVE-2018-14629, CVE-2018-16851
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-14629.html
   URL:https://www.samba.org/samba/security/CVE-2018-16851.html
```

Medium (CVSS: 4.0)
NVT: Samba DoS Vulnerability (CVE-2018-16841)

Summary
Samba is prone to a denial of service vulnerability.

Vulnerability Detection Result
```
Installed version: 4.7.6
Fixed version:     4.7.12
Installation
path / port:       445/tcp
```

Solution
Solution type: VendorFix
Update to version 4.7.12, 4.8.7, 4.9.3 or later.

Affected Software/OS
Samba 4.3.0 and later.

Vulnerability Insight
A user with a valid certificate or smart card can crash the Samba AD DC's KDC.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Samba DoS Vulnerability (CVE-2018-16841)
OID:1.3.6.1.4.1.25623.1.0.141734
Version used: $Revision: 13517 $

References
CVE: CVE-2018-16841
Other:
URL:https://www.samba.org/samba/security/CVE-2018-16841.html

Medium (CVSS: 4.3)
NVT: Samba DoS Vulnerability (CVE-2018-16853)

Summary
Samba is prone to a denial of service vulnerability.

Vulnerability Detection Result
Installed version: 4.7.6
Fixed version: 4.7.12
Installation
path / port: 445/tcp

Solution
Solution type: VendorFix
Update to version 4.7.12, 4.8.7, 4.9.3 or later.

Affected Software/OS
Samba 4.7.0 and later.

Vulnerability Insight
A user in a Samba AD domain can crash the MIT KDC by requesting an S4U2Self ticket.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Samba DoS Vulnerability (CVE-2018-16853)
OID:1.3.6.1.4.1.25623.1.0.141733
Version used: $Revision: 13517 $

References
CVE: CVE-2018-16853
Other:
URL:https://www.samba.org/samba/security/CVE-2018-16853.html

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 4.3)
NVT: Samba Multiple Vulnerabilities - Aug18

Summary
This host is running Samba and is prone to multiple vulnerabilities.

Vulnerability Detection Result
```
Installed version: 4.7.6
Fixed version:     4.7.9 or apply patch
Installation
path / port:       445/tcp
```

Impact
Successful exploitation will allow an attacker to conduct a denial of service attack and authenticate using NTLMv1 over an SMB1 transport.

Solution
Solution type: VendorFix
Upgrade to Samba 4.8.4 or 4.7.9 or later. Please see the references for more information.

Affected Software/OS
All versions of Samba from 4.7.0 onwards

Vulnerability Insight
Multiple flaws exists due to
- A missing database output checks on the returned directory attributes from the LDB database layer.
- An error which allows authentication using NTLMv1 over an SMB1 transport (either directory or via NETLOGON SamLogon calls from a member server), even when NTLMv1 is explicitly disabled on the server.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba Multiple Vulnerabilities - Aug18`
OID:1.3.6.1.4.1.25623.1.0.813783
Version used: `2019-05-03T08:55:39+0000`

References
```
CVE: CVE-2018-10918, CVE-2018-1139
Other:
  URL:https://www.samba.org/samba/security/CVE-2018-10918.html
   URL:https://www.samba.org/samba/security/CVE-2018-1139.html
   URL:https://www.samba.org/samba/history/samba-4.7.9.html
   URL:https://www.samba.org/samba/history/samba-4.8.4.html
   URL:https://www.samba.org
```

Medium (CVSS: 5.5)
NVT: Samba Path/Symlink Traversal Vulnerability (CVE-2019-3880)

Summary
Samba is prone to a path/symlink traversal vulnerability.

Vulnerability Detection Result
```
Installed version: 4.7.6
Fixed version:     4.8.11
Installation
path / port:       445/tcp
```

Solution
Solution type: VendorFix
Update to version 4.8.11, 4.9.6, 4.10.2 or later.

Affected Software/OS
Samba 3.2.0 and later.

Vulnerability Insight
A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Samba Path/Symlink Traversal Vulnerability (CVE-2019-3880)`
OID:1.3.6.1.4.1.25623.1.0.142391
Version used: `2019-05-09T14:21:05+0000`

References
```
CVE: CVE-2019-3880
Other:
  URL:https://www.samba.org/samba/security/CVE-2019-3880.html
```

[return to 192.168.0.177]

2.177.5 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Apache /server-status accessible

Summary
Requesting the URI /server-status provides information on the server activity and performance.

Vulnerability Detection Result
. . . continues on next page . . .

... continued from previous page ...

Vulnerable url: http://bavo-GL62M-7RD/server-status

Impact
Requesting the URI /server-status gives throughout information about the currently running Apache to an attacker.

Solution
Solution type: Mitigation
- If this feature is unused commenting out the appropriate section in the web servers configuration is recommended.
- If this feature is used restricting access to trusted clients is recommended.

Affected Software/OS
All Apache installations with an enabled 'mod_status' module.

Vulnerability Insight
server-status is a Apache HTTP Server handler provided by the 'mod_status' module and used to retrieve the server's activity and performance.

Vulnerability Detection Method
Checks if the /server-status page of Apache is accessible.
Details: Apache /server-status accessible
OID:1.3.6.1.4.1.25623.1.0.10677
Version used: 2019-04-26T12:19:11+0000

References
Other:
URL:https://httpd.apache.org/docs/current/mod/mod_status.html

Medium (CVSS: 5.0)
NVT: Apache HTTP Server 'HTTP/2 connection' DoS Vulnerability

Summary
This host is running Apache HTTP Server and is prone to denial-of-service vulnerability

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.34
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to cause a denial of service (DoS) condition on a targeted system.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Upgrade to Apache HTTP Server 2.4.34 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP Server versions 2.4.18 through 2.4.30 and 2.4.33.

Vulnerability Insight
The flaw is due to an error in the handling of specially crafted HTTP/2 requests.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server 'HTTP/2 connection' DoS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.813812
Version used: `2019-05-03T08:55:39+0000`

References
```
CVE: CVE-2018-1333
Other:
  URL:https://httpd.apache.org
   URL:http://seclists.org/oss-sec/2018/q3/39
   URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

Medium (CVSS: 4.3)
NVT: Apache HTTP Server Denial of Service Vulnerability Apr18 (Linux)

Summary
The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.

Vulnerability Detection Result
```
Installed version: 2.4.29
Fixed version:     2.4.30
Installation
path / port:       80/tcp
```

Impact
Successful exploitation will allow an attacker to destroy an HTTP/2 stream, resulting in a denial of service condition.

Solution
Solution type: VendorFix
Upgrade to version 2.4.30 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP server versions 2.4.17, 2.4.18, 2.4.20, 2.4.23 and from 2.4.25 to 2.4.29 on Linux.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw exists as the Apache HTTP Server writes a NULL pointer potentially to an already freed memory.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server Denial of Service Vulnerability Apr18 (Linux)`
OID:1.3.6.1.4.1.25623.1.0.812845
Version used: `2019-05-03T08:55:39+0000`

References
`CVE: CVE-2018-1302`
`BID:103528`
`Other:`
`URL:https://httpd.apache.org/download.cgi`
`URL:http://www.openwall.com/lists/oss-security/2018/03/24/8`
`URL:http://www.openwall.com/lists/oss-security/2018/03/24/2`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)

Summary
The host is installed with Apache HTTP server and is prone to a denial of service vulnerability.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.30`
`Installation path / port: 80/tcp`

Impact
Successful exploitation will allow an attacker to crash the Apache HTTP Server resulting in denial of service condition.

Solution
Solution type: VendorFix
Upgrade to version 2.4.30 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP server versions 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 through 2.4.18, 2.4.20, 2.4.23, and 2.4.25 through 2.4.29 on Linux.

Vulnerability Insight
The flaw exists as the Apache HTTP Server fails to sanitize against a specially crafted HTTP request header.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.812849
Version used: 2019-05-03T08:55:39+0000

References
CVE: CVE-2018-1303
BID:103522
Other:
URL:https://httpd.apache.org/download.cgi
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 6.8)
NVT: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)

Summary
The host is installed with Apache HTTP server and is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.30
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution
Solution type: VendorFix
Upgrade to version 2.4.30 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP server versions from 2.4.1 to 2.4.4, 2.4.6, 2.4.7, 2.4.9, 2.4.10, 2.4.12, 2.4.16 to 2.4.18, 2.4.20, 2.4.23, 2.4.25 to 2.4.29 on Linux.

Vulnerability Insight
Multiple flaws exists due to,
- Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks.
- Misconfigured mod_session variable, HTTP_SESSION.
- Apache HTTP Server fails to sanitize the expression specified in '<FilesMatch>'.
- An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig.
- Apache HTTP Server fails to sanitize against a specially crafted request.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)
OID:1.3.6.1.4.1.25623.1.0.812844
Version used: 2019-05-03T08:55:39+0000

References
CVE: CVE-2018-1312, CVE-2018-1283, CVE-2017-15715, CVE-2017-15710, CVE-2018-1301
BID:103524, 103520, 103525, 103512, 103515
Other:
URL:https://httpd.apache.org/download.cgi
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 4.3)
NVT: Apache HTTPD HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Linux)

Summary
This host is running Apache HTTP Server and is prone to denial-of-service vulnerability

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.35
Installation
path / port: 80/tcp

Impact
Successful exploitation will allow remote attackers to cause a denial of service (DoS) condition on a targeted system.

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server 2.4.35 or later. Please see the references for more information.

Affected Software/OS
Apache HTTP Server versions 2.4.34, 2.4.33, 2.4.30, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18.

Vulnerability Insight
The flaw is due to an improper processing of specially crafted and continuous SETTINGS data for an ongoing HTTP/2 connection to cause the target service to fail to timeout.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTPD HTTP/2 'SETTINGS' Data Processing DoS Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.814056
Version used: 2019-05-03T08:55:39+0000

... continues on next page ...

... continued from previous page ...

References
CVE: CVE-2018-11763
Other:
URL:https://httpd.apache.org
URL:https://securitytracker.com/id/1041713
URL:https://httpd.apache.org/security/vulnerabilities_24.html

[return to 192.168.0.177]

2.177.6 Medium general/tcp

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Linux)

Summary
By sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

Vulnerability Detection Result
Installed version: 2.4.29
Fixed version: 2.4.38

Solution
Solution type: VendorFix
Update to version 2.4.38 or later.

Affected Software/OS
Apache HTTP server version 2.4.37 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Linux)
OID:1.3.6.1.4.1.25623.1.0.141966
Version used: $Revision: 13547 $

References
CVE: CVE-2018-17189
Other:
URL:https://httpd.apache.org/security/vulnerabilities_24.html

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)

... continues on next page ...

... continued from previous page ...

Summary
In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.38`

Solution
Solution type: VendorFix
Update to version 2.4.38 or later.

Affected Software/OS
Apache HTTP server version 2.4.37 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.141964
Version used: `$Revision: 13750 $`

References
`CVE: CVE-2018-17199`
`Other:`
`URL:https://httpd.apache.org/security/vulnerabilities_24.html`

Medium (CVSS: 6.0)
NVT: Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux)

Summary
In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.39`

Solution
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP server version 2.4.38 and prior.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability. ↪..`
OID:1.3.6.1.4.1.25623.1.0.142220
Version used: `2019-04-15T07:08:44+0000`

References
`CVE: CVE-2019-0217`
`Other:`
`URL:https://httpd.apache.org/security/vulnerabilities_24.html`

Medium (CVSS: 5.0)
NVT: Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Linux)

Summary
Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

Vulnerability Detection Result
`Installed version: 2.4.29`
`Fixed version: 2.4.39`

Solution
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP server version 2.4.38 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.39 mod_http2 DoS Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.142226
Version used: `2019-04-08T15:50:06+0000`

References
`CVE: CVE-2019-0196`
`Other:`
`URL:https://httpd.apache.org/security/vulnerabilities_24.html`

[return to 192.168.0.177]

2.177.7 Low general/tcp

Low (CVSS: 1.7)
NVT: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)

Summary
When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

Vulnerability Detection Result
```
Installed version: 2.4.29
Fixed version:     2.4.39
```

Solution
Solution type: VendorFix
Update to version 2.4.39 or later.

Affected Software/OS
Apache HTTP server version 2.4.38 and prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)`
OID:1.3.6.1.4.1.25623.1.0.142228
Version used: `2019-04-08T15:50:06+0000`

References
```
CVE: CVE-2019-0220
Other:
  URL:https://httpd.apache.org/security/vulnerabilities_24.html
```

[return to 192.168.0.177]

2.177.8 Log 21/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects and reports a FTP Server Banner.

Vulnerability Detection Result
```
Remote FTP server banner:
220 (vsFTPd 3.0.3)
This is probably:
```

... continues on next page ...

... continued from previous page ...

- vsFTPd

Log Method
Details: FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: 2019-05-02T04:45:21+0000

Log (CVSS: 0.0)
NVT: FTP Missing Support For AUTH TLS

Summary
The remote FTP server does not support the 'AUTH TLS' command.

Vulnerability Detection Result
The remote FTP server does not support the 'AUTH TLS' command.

Log Method
Details: FTP Missing Support For AUTH TLS
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: $Revision: 13863 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
An FTP server is running on this port.
Here is its banner :
220 (vsFTPd 3.0.3)

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: vsFTPd FTP Server Detection

Summary

... continues on next page ...

... continued from previous page ...

The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Vulnerability Detection Result

```
Detected vsFTPd
Version:  3.0.3
Location: 21/tcp
CPE:      cpe:/a:beasts:vsftpd:3.0.3
Concluded from version/product identification result:
220 (vsFTPd 3.0.3)
```

Log Method

Details: `vsFTPd FTP Server Detection`
OID:1.3.6.1.4.1.25623.1.0.111050
Version used: `$Revision: 13499 $`

[return to 192.168.0.177]

2.177.9 Log 3306/tcp

Log (CVSS: 0.0)
NVT: MySQL/MariaDB Detection

Summary

Detects the installed version of MySQL/MariaDB.
Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner and store the information in KB.

Vulnerability Detection Result

```
Detected MySQL
Version:  unknown
Location: 3306/tcp
CPE:      cpe:/a:oracle:mysql
Extra information:
Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MySQL server.
Some tests may fail. Allow the scanner to access the remote MySQL server for bet
↪ter results.
```

Log Method

Details: `MySQL/MariaDB Detection`
OID:1.3.6.1.4.1.25623.1.0.100152
Version used: `$Revision: 10929 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A MySQL server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

[return to 192.168.0.177]

2.177.10 Log 4000/tcp

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "bavo-GL62M-7RD" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be NOT able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
```

... continues on next page ...

... continued from previous page ...

```
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
https://bavo-GL62M-7RD:4000/
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 13679 $

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Greenbone Security Assistant (GSA) Detection

Summary
The script sends a connection request to the server and attempts to determine if it is a GSA from the reply.

Vulnerability Detection Result

```
Detected Greenbone Security Assistant
Version:  7.0.3
Location: /
CPE:      cpe:/a:greenbone:greenbone_security_assistant:7.0.3
Concluded from version/product identification result:
<span class="version">Version 7.0.3</span>
```

Log Method
Details: Greenbone Security Assistant (GSA) Detection
OID:1.3.6.1.4.1.25623.1.0.103841
Version used: $Revision: 13882 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A TLScustom server answered on this port

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A web server is running on this port through SSL

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result
```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=bavo-GL62M-7RD
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for bavo
↪-GL62M-7RD
serial ....: 5CD985222AC0F5A61129036A
valid from : 2019-05-13 14:54:26 UTC
valid until: 2021-05-12 14:54:26 UTC
fingerprint (SHA-1): FE505BEC397900DC02AD1B7E31D5C51F3E9A957D
fingerprint (SHA-256): 4B8E03FA40CF4D4AD288ABFFF7455A9620B1C7FE26E0D69A4403EE155
```

... continues on next page ...

... continued from previous page ...

↪360B473

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2019-04-04T13:38:03+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing

Summary
The remote service is missing support for SSL/TLS cipher suites supporting Perfect Forward Secrecy.

Vulnerability Detection Result
The remote service does not support perfect forward secrecy cipher suites.

Log Method
Details: SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing
OID:1.3.6.1.4.1.25623.1.0.105092
Version used: $Revision: 4736 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: $Revision: 4743 $

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
```

Log Method
Details: `SSL/TLS: Report Non Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: `$Revision: 4736 $`

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

```
No 'Strong' cipher suites accepted by this service via the TLSv1.0 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol.
No 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol.
```

... continues on next page ...

... continued from previous page ...

'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: $Revision: 11108 $

[return to 192.168.0.177]

2.177.11 Log 445/tcp

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result
The following shares were found
IPC$

Log Method
Details: Microsoft Windows SMB Accessible Shares
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: $Revision: 11420 $

Log (CVSS: 0.0)
NVT: SMB log in

Summary
This script attempts to logon into the remote host using login/password credentials.

Vulnerability Detection Result
`It was possible to log into the remote host using the SMB protocol.`

Log Method
Details: `SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `$Revision: 13247 $`

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks

Summary
It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Log Method
Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `$Revision: 13248 $`

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
```
Detected Samba
Version:  4.7.6
Location: 445/tcp
CPE:      cpe:/a:samba:samba:4.7.6
Concluded from version/product identification result:
Samba 4.7.6-Ubuntu
Extra information:
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 4.7.6-Ubuntu
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2019-04-24T11:06:32+0000

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 4.7.6-Ubuntu
Detected OS: Ubuntu 18.04

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2019-04-24T11:06:32+0000

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
SMBv1 and SMBv2 are enabled on remote target

Log Method
Details: SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: $Revision: 10898 $

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A CIFS server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

[return to 192.168.0.177]

2.177.12 Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache Web Server Detection

Summary
Detects the installed version of Apache Web Server
The script detects the version of Apache HTTP Server on remote host and sets the KB.

Vulnerability Detection Result
Detected Apache
Version: 2.4.29
Location: 80/tcp
CPE: cpe:/a:apache:http_server:2.4.29
Concluded from version/product identification result:
Server: Apache/2.4.29

Log Method
Details: Apache Web Server Detection
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: $Revision: 10290 $

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use

... continues on next page ...

... continued from previous page ...

- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result

```
The Hostname/IP "bavo-GL62M-7RD" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://bavo-GL62M-7RD/
http://bavo-GL62M-7RD/client
http://bavo-GL62M-7RD/server-status
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://bavo-GL62M-7RD/icons
```

Log Method

Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: $Revision: 13679 $

References

```
Other:
  URL:https://community.greenbone.net/c/vulnerability-tests
```

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary

... continues on next page ...

... continued from previous page ...

All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers
---------------
Content-Security-Policy
Referrer-Policy
X-Content-Type-Options
X-Frame-Options
X-Permitted-Cross-Domain-Policies
X-XSS-Protection
```

Log Method

Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `$Revision: 10899 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: HTTP Server type and version

Summary

This detects the HTTP Server's type and version.

Vulnerability Detection Result

```
The remote web server type is :
Apache/2.4.29 (Ubuntu)
Solution : You can set the directive "ServerTokens Prod" to limit
the information emanating from the server in its response headers.
```

Solution

- Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display'
- Be sure to remove common logos like apache_pb.gif.
- With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

Log Method

Details: `HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 11585 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

[return to 192.168.0.177]

2.177.13 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Linux/Unix
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 3.0.3)
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS: Ubuntu 18.04
Version: 18.04
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Ubuntu 18.04; SMB St
↪ring: Samba 4.7.6-Ubuntu
OS: Ubuntu 18.04
Version: 18.04
```

. . . continues on next page . . .

... continued from previous page ...

```
CPE: cpe:/o:canonical:ubuntu_linux:18.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.29 (Ubuntu)
OS: Ubuntu
CPE: cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server default page on port 80/tcp: <title>Apache2 Ubuntu De
↪fault Page
```

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result

```
Here is the route from 192.168.0.177 to 192.168.0.177:
192.168.0.177
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

[return to 192.168.0.177]

2.177.14 Log 139/tcp

Log (CVSS: 0.0) NVT: SMB/CIFS Server Detection
Summary This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Vulnerability Detection Result `A SMB server is running on this port`
Log Method Details: `SMB/CIFS Server Detection` OID:1.3.6.1.4.1.25623.1.0.11011 Version used: `$Revision: 13541 $`

[return to 192.168.0.177]

2.178 192.168.0.178

Host scan start Mon May 13 15:39:33 2019 UTC
Host scan end Mon May 13 15:39:36 2019 UTC

Service (Port)	Threat Level

2.179 192.168.0.179

Host scan start Mon May 13 15:39:33 2019 UTC
Host scan end Mon May 13 15:39:36 2019 UTC

Service (Port)	Threat Level

2.180 192.168.0.180

Host scan start Mon May 13 15:39:34 2019 UTC
Host scan end Mon May 13 15:39:36 2019 UTC

Service (Port)	Threat Level

2.181 192.168.0.181

Host scan start Mon May 13 15:39:34 2019 UTC
Host scan end Mon May 13 15:39:36 2019 UTC

Service (Port)	Threat Level

2.182 192.168.0.182

Host scan start	Mon May 13 15:39:34 2019 UTC
Host scan end	Mon May 13 15:39:37 2019 UTC

Service (Port)	Threat Level

2.183 192.168.0.183

Host scan start	Mon May 13 15:39:34 2019 UTC
Host scan end	Mon May 13 15:39:37 2019 UTC

Service (Port)	Threat Level

2.184 192.168.0.184

Host scan start	Mon May 13 15:39:35 2019 UTC
Host scan end	Mon May 13 15:39:38 2019 UTC

Service (Port)	Threat Level

2.185 192.168.0.185

Host scan start	Mon May 13 15:39:35 2019 UTC
Host scan end	Mon May 13 15:39:38 2019 UTC

Service (Port)	Threat Level

2.186 192.168.0.186

Host scan start	Mon May 13 15:39:36 2019 UTC
Host scan end	Mon May 13 15:39:38 2019 UTC

Service (Port)	Threat Level

2.187 192.168.0.187

Host scan start	Mon May 13 15:39:37 2019 UTC
Host scan end	Mon May 13 15:39:39 2019 UTC

Service (Port)	Threat Level

2.188 192.168.0.188

Host scan start	Mon May 13 15:39:36 2019 UTC
Host scan end	Mon May 13 15:39:38 2019 UTC

Service (Port)	Threat Level

2.189 192.168.0.189

Host scan start	Mon May 13 15:39:37 2019 UTC
Host scan end	Mon May 13 15:39:39 2019 UTC

Service (Port)	Threat Level

2.190 192.168.0.190

Host scan start	Mon May 13 15:39:37 2019 UTC
Host scan end	Mon May 13 15:39:39 2019 UTC

Service (Port)	Threat Level

2.191 192.168.0.191

Host scan start	Mon May 13 15:39:37 2019 UTC
Host scan end	Mon May 13 15:39:39 2019 UTC

Service (Port)	Threat Level

2.192 192.168.0.192

Host scan start	Mon May 13 15:39:38 2019 UTC
Host scan end	Mon May 13 15:39:40 2019 UTC

Service (Port)	Threat Level

2.193 192.168.0.193

Host scan start	Mon May 13 15:39:38 2019 UTC
Host scan end	Mon May 13 15:39:40 2019 UTC

Service (Port)	Threat Level

2.194 192.168.0.194

Host scan start	Mon May 13 15:39:38 2019 UTC
Host scan end	Mon May 13 15:39:40 2019 UTC

Service (Port)	Threat Level

2.195 192.168.0.195

Host scan start	Mon May 13 15:39:38 2019 UTC
Host scan end	Mon May 13 15:39:40 2019 UTC

Service (Port)	Threat Level

2.196 192.168.0.196

Host scan start	Mon May 13 15:39:39 2019 UTC
Host scan end	Mon May 13 15:39:41 2019 UTC

Service (Port)	Threat Level

2.197 192.168.0.197

Host scan start	Mon May 13 15:39:39 2019 UTC
Host scan end	Mon May 13 15:39:41 2019 UTC

Service (Port)	Threat Level

2.198 192.168.0.198

Host scan start	Mon May 13 15:39:39 2019 UTC
Host scan end	Mon May 13 15:39:41 2019 UTC

Service (Port)	Threat Level

2.199 192.168.0.199

Host scan start	Mon May 13 15:39:39 2019 UTC
Host scan end	Mon May 13 15:39:41 2019 UTC

Service (Port)	Threat Level

2.200 192.168.0.200

Host scan start	Mon May 13 15:39:40 2019 UTC
Host scan end	Mon May 13 15:39:43 2019 UTC

Service (Port)	Threat Level

2.201 192.168.0.201

Host scan start	Mon May 13 15:39:40 2019 UTC
Host scan end	Mon May 13 15:39:43 2019 UTC

Service (Port)	Threat Level

2.202 192.168.0.202

Host scan start	Mon May 13 15:39:40 2019 UTC
Host scan end	Mon May 13 15:39:43 2019 UTC

Service (Port)	Threat Level

2.203 192.168.0.203

Host scan start	Mon May 13 15:39:40 2019 UTC
Host scan end	Mon May 13 15:39:43 2019 UTC

Service (Port)	Threat Level

2.204 192.168.0.204

Host scan start	Mon May 13 15:39:41 2019 UTC
Host scan end	Mon May 13 15:39:44 2019 UTC

Service (Port)	Threat Level

2.205 192.168.0.205

Host scan start	Mon May 13 15:39:42 2019 UTC
Host scan end	Mon May 13 15:39:44 2019 UTC

Service (Port)	Threat Level

2.206 192.168.0.206

Host scan start	Mon May 13 15:39:42 2019 UTC
Host scan end	Mon May 13 15:39:44 2019 UTC

Service (Port)	Threat Level

2.207 192.168.0.207

Host scan start	Mon May 13 15:39:43 2019 UTC
Host scan end	Mon May 13 15:39:45 2019 UTC

Service (Port)	Threat Level

2.208 192.168.0.208

Host scan start	Mon May 13 15:39:43 2019 UTC
Host scan end	Mon May 13 15:39:45 2019 UTC

Service (Port)	Threat Level

2.209 192.168.0.209

Host scan start	Mon May 13 15:39:43 2019 UTC
Host scan end	Mon May 13 15:39:45 2019 UTC

Service (Port)	Threat Level

2.210 192.168.0.210

Host scan start	Mon May 13 15:39:43 2019 UTC
Host scan end	Mon May 13 15:39:45 2019 UTC

Service (Port)	Threat Level

2.211 192.168.0.211

Host scan start	Mon May 13 15:39:43 2019 UTC
Host scan end	Mon May 13 15:39:45 2019 UTC

Service (Port)	Threat Level

2.212 192.168.0.212

Host scan start	Mon May 13 15:39:44 2019 UTC
Host scan end	Mon May 13 15:39:46 2019 UTC

Service (Port)	Threat Level

2.213 192.168.0.213

Host scan start	Mon May 13 15:39:44 2019 UTC
Host scan end	Mon May 13 15:39:46 2019 UTC

Service (Port)	Threat Level

2.214 192.168.0.214

Host scan start	Mon May 13 15:39:44 2019 UTC
Host scan end	Mon May 13 15:39:46 2019 UTC

Service (Port)	Threat Level

2.215 192.168.0.215

Host scan start	Mon May 13 15:39:45 2019 UTC
Host scan end	Mon May 13 15:39:47 2019 UTC

Service (Port)	Threat Level

2.216 192.168.0.216

Host scan start	Mon May 13 15:39:45 2019 UTC
Host scan end	Mon May 13 15:39:47 2019 UTC

Service (Port)	Threat Level

2.217 192.168.0.217

Host scan start	Mon May 13 15:39:45 2019 UTC
Host scan end	Mon May 13 15:39:47 2019 UTC

Service (Port)	Threat Level

2.218 192.168.0.218

Host scan start	Mon May 13 15:39:45 2019 UTC
Host scan end	Mon May 13 15:39:47 2019 UTC

Service (Port)	Threat Level

2.219 192.168.0.219

Host scan start	Mon May 13 15:39:45 2019 UTC
Host scan end	Mon May 13 15:39:48 2019 UTC

Service (Port)	Threat Level

2.220 192.168.0.220

Host scan start	Mon May 13 15:39:46 2019 UTC
Host scan end	Mon May 13 15:39:49 2019 UTC

Service (Port)	Threat Level

2.221 192.168.0.221

Host scan start	Mon May 13 15:39:46 2019 UTC
Host scan end	Mon May 13 15:39:49 2019 UTC

Service (Port)	Threat Level

2.222 192.168.0.222

Host scan start	Mon May 13 15:39:46 2019 UTC
Host scan end	Mon May 13 15:39:49 2019 UTC

Service (Port)	Threat Level

2.223 192.168.0.223

Host scan start	Mon May 13 15:39:47 2019 UTC
Host scan end	Mon May 13 15:39:50 2019 UTC

Service (Port)	Threat Level

2.224 192.168.0.224

Host scan start	Mon May 13 15:39:47 2019 UTC
Host scan end	Mon May 13 15:43:14 2019 UTC

Service (Port)	Threat Level
135/tcp	Medium
general/tcp	Low
139/tcp	Log
general/CPE-T	Log
902/tcp	Log
135/tcp	Log
912/tcp	Log
445/tcp	Log
general/tcp	Log

2.224.1 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.224[49664]
Port: 49665/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.224[49665]
     Annotation: Event log TCPIP
Port: 49666/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.224[49666]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.224[49666]
Port: 49667/tcp
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.224[49667]
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.0.224[49668]
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49668]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49668]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49668]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49668]
Port: 49671/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.0.224[49671]
Port: 49672/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49672]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49672]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.0.224[49672]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.0.224[49672]
      Annotation: KeyIso
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `$Revision: 6319 $`

[return to 192.168.0.224]

2.224.2 Low general/tcp

Low (CVSS: 2.6) NVT: Relative IP Identification number change
Summary The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.
Vulnerability Detection Result `The target host was found to be vulnerable`
Impact An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are: 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.
Solution **Solution type:** VendorFix Contact your vendor for a patch
Vulnerability Detection Method Details: `Relative IP Identification number change` OID:1.3.6.1.4.1.25623.1.0.10201 Version used: `$Revision: 10411 $`

[return to 192.168.0.224]

2.224.3 Log 139/tcp

Log (CVSS: 0.0) NVT: SMB/CIFS Server Detection
Summary This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Vulnerability Detection Result

. . . continues on next page . . .

... continued from previous page ...

A SMB server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

[return to 192.168.0.224]

2.224.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
192.168.0.224|cpe:/o:microsoft:windows_10:1803:cb:pro

Log Method
Details: CPE Inventory
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: $Revision: 14324 $

References
Other:
URL:http://cpe.mitre.org/

[return to 192.168.0.224]

2.224.5 Log 902/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
A VMWare authentication daemon is running on this port:

... continues on next page ...

... continued from previous page ...

```
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtoco
↪l:SOAP, MKSDisplayProtocol:VNC , , NFCSSL supported/t
```

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: VMware ESX/GSX Server detection

Summary
The remote host appears to be running VMware ESX or GSX Server.
Description :
According to its banner, the remote host appears to be running a VMWare server authentication daemon, which likely indicates the remote host is running VMware ESX or GSX Server.

Vulnerability Detection Result

```
A VMware Authentication Daemon in Version: 1.10 is running on this port
```

Log Method
Details: VMware ESX/GSX Server detection
OID:1.3.6.1.4.1.25623.1.0.20301
Version used: $Revision: 13541 $

References

```
Other:
  URL:http://www.vmware.com/
```

[return to 192.168.0.224]

2.224.6 Log 135/tcp

Log (CVSS: 0.0)
NVT: DCE/RPC and MSRPC Services Enumeration

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)

Vulnerability Detection Result

```
A DCE endpoint resolution service seems to be running on this port.
```

... continues on next page ...

... continued from previous page ...

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Solution type: Mitigation
Filter incoming traffic to this port.

Log Method
Details: `DCE/RPC and MSRPC Services Enumeration`
OID:1.3.6.1.4.1.25623.1.0.108044
Version used: `$Revision: 11885 $`

[return to 192.168.0.224]

2.224.7 Log 912/tcp

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
```
A VMWare authentication daemon is running on this port:
220 VMware Authentication Daemon Version 1.0, ServerDaemonProtocol:SOAP, MKSDisp
↪layProtocol:VNC , ,
```

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: VMware ESX/GSX Server detection

Summary
The remote host appears to be running VMware ESX or GSX Server.
Description :
According to its banner, the remote host appears to be running a VMWare server authentication daemon, which likely indicates the remote host is running VMware ESX or GSX Server.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

A VMware Authentication Daemon in Version: 1.0 is running on this port

Log Method
Details: VMware ESX/GSX Server detection
OID:1.3.6.1.4.1.25623.1.0.20301
Version used: $Revision: 13541 $

References
Other:
URL:http://www.vmware.com/

[return to 192.168.0.224]

2.224.8 Log 445/tcp

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
Detected SMB workgroup: WORKGROUP
Detected SMB server: Windows 10 Pro 6.3
Detected OS: Windows 10 Pro 17134

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2019-04-24T11:06:32+0000

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
SMBv1 and SMBv2 are enabled on remote target

Log Method
Details: SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 10898 $

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
A CIFS server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

[return to 192.168.0.224]

2.224.9 Log general/tcp

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result
```
Best matching OS:
OS: Windows 10 Pro 17134
CPE: cpe:/o:microsoft:windows_10:1803:cb:pro
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp: OS String: Windows 10 Pro 17134
↪; SMB String: Windows 10 Pro 6.3
Setting key "Host/runs_windows" based on this information
Other OS detections (in order of reliability):
OS: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.108044 (DCE/RPC and MSRPC Services Enumerati
↪on)
```

... continues on next page ...

... continued from previous page ...

Concluded from DCE/RPC and MSRPC Services Enumeration on port 135/tcp

Log Method
Details: OS Detection Consolidation and Reporting
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2019-05-02T04:45:21+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
Here is the route from 192.168.0.177 to 192.168.0.224:
192.168.0.177
192.168.0.224

Solution
Block unwanted packets from escaping your network.

Log Method
Details: Traceroute
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: $Revision: 10411 $

[return to 192.168.0.224]

2.225 192.168.0.225

Host scan start	Mon May 13 15:39:48 2019 UTC
Host scan end	Mon May 13 15:39:51 2019 UTC

Service (Port)	Threat Level

2.226 192.168.0.226

Host scan start	Mon May 13 15:39:48 2019 UTC
Host scan end	Mon May 13 15:39:51 2019 UTC

Service (Port)	Threat Level

2.227 192.168.0.227

Host scan start	Mon May 13 15:39:48 2019 UTC
Host scan end	Mon May 13 15:39:50 2019 UTC

Service (Port)	Threat Level

2.228 192.168.0.228

Host scan start	Mon May 13 15:39:49 2019 UTC
Host scan end	Mon May 13 15:39:51 2019 UTC

Service (Port)	Threat Level

2.229 192.168.0.229

Host scan start	Mon May 13 15:39:49 2019 UTC
Host scan end	Mon May 13 15:39:51 2019 UTC

Service (Port)	Threat Level

2.230 192.168.0.230

Host scan start	Mon May 13 15:39:49 2019 UTC
Host scan end	Mon May 13 15:39:51 2019 UTC

Service (Port)	Threat Level

2.231 192.168.0.231

Host scan start	Mon May 13 15:39:50 2019 UTC
Host scan end	Mon May 13 15:39:52 2019 UTC

Service (Port)	Threat Level

2.232 192.168.0.232

Host scan start	Mon May 13 15:39:50 2019 UTC
Host scan end	Mon May 13 15:39:52 2019 UTC

Service (Port)	Threat Level

2.233 192.168.0.233

Host scan start	Mon May 13 15:39:51 2019 UTC
Host scan end	Mon May 13 15:39:53 2019 UTC

Service (Port)	Threat Level

2.234 192.168.0.234

Host scan start	Mon May 13 15:39:51 2019 UTC
Host scan end	Mon May 13 15:39:53 2019 UTC

Service (Port)	Threat Level

2.235 192.168.0.235

Host scan start	Mon May 13 15:39:51 2019 UTC
Host scan end	Mon May 13 15:39:53 2019 UTC

Service (Port)	Threat Level

2.236 192.168.0.236

Host scan start	Mon May 13 15:39:51 2019 UTC
Host scan end	Mon May 13 15:39:53 2019 UTC

Service (Port)	Threat Level

2.237 192.168.0.237

Host scan start	Mon May 13 15:39:51 2019 UTC
Host scan end	Mon May 13 15:39:53 2019 UTC

Service (Port)	Threat Level

2.238 192.168.0.238

Host scan start	Mon May 13 15:39:52 2019 UTC
Host scan end	Mon May 13 15:39:54 2019 UTC

Service (Port)	Threat Level

2.239 192.168.0.239

Host scan start	Mon May 13 15:39:52 2019 UTC
Host scan end	Mon May 13 15:39:55 2019 UTC

Service (Port)	Threat Level

2.240 192.168.0.240

Host scan start	Mon May 13 15:39:53 2019 UTC
Host scan end	Mon May 13 15:39:55 2019 UTC

Service (Port)	Threat Level

2.241 192.168.0.241

Host scan start	Mon May 13 15:39:53 2019 UTC
Host scan end	Mon May 13 15:39:55 2019 UTC

Service (Port)	Threat Level

2.242 192.168.0.242

Host scan start	Mon May 13 15:39:53 2019 UTC
Host scan end	Mon May 13 15:39:56 2019 UTC

Service (Port)	Threat Level

2.243 192.168.0.243

Host scan start	Mon May 13 15:39:54 2019 UTC
Host scan end	Mon May 13 15:39:56 2019 UTC

Service (Port)	Threat Level

2.244 192.168.0.244

Host scan start	Mon May 13 15:39:54 2019 UTC
Host scan end	Mon May 13 15:39:56 2019 UTC

Service (Port)	Threat Level

2.245 192.168.0.245

Host scan start	Mon May 13 15:39:54 2019 UTC
Host scan end	Mon May 13 15:39:57 2019 UTC

Service (Port)	Threat Level

2.246 192.168.0.246

Host scan start	Mon May 13 15:39:55 2019 UTC
Host scan end	Mon May 13 15:39:57 2019 UTC

Service (Port)	Threat Level

2.247 192.168.0.247

Host scan start	Mon May 13 15:39:55 2019 UTC
Host scan end	Mon May 13 15:39:58 2019 UTC

Service (Port)	Threat Level

2.248 192.168.0.248

Host scan start	Mon May 13 15:39:56 2019 UTC
Host scan end	Mon May 13 15:39:58 2019 UTC

Service (Port)	Threat Level

2.249 192.168.0.249

Host scan start	Mon May 13 15:39:56 2019 UTC
Host scan end	Mon May 13 15:39:58 2019 UTC

Service (Port)	Threat Level

2.250 192.168.0.250

Host scan start	Mon May 13 15:39:56 2019 UTC
Host scan end	Mon May 13 15:39:58 2019 UTC

Service (Port)	Threat Level

2.251 192.168.0.251

Host scan start	Mon May 13 15:39:56 2019 UTC
Host scan end	Mon May 13 15:39:58 2019 UTC

Service (Port)	Threat Level

2.252 192.168.0.252

Host scan start	Mon May 13 15:39:57 2019 UTC
Host scan end	Mon May 13 15:39:59 2019 UTC

Service (Port)	Threat Level

2.253 192.168.0.253

Host scan start	Mon May 13 15:39:57 2019 UTC
Host scan end	Mon May 13 15:39:59 2019 UTC

Service (Port)	Threat Level

2.254 192.168.0.254

Host scan start	Mon May 13 15:39:58 2019 UTC
Host scan end	Mon May 13 15:40:00 2019 UTC

Service (Port)	Threat Level