Scan Report

December 28, 2024

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 10.0.2.15". The scan started at Sat Dec 28 12:51:18 2024 UTC and ended at Sat Dec 28 13:05:55 2024 UTC. 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

Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.2.15	0	1	1	16	0
Total: 1	0	1	1	16	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 18 results selected by the filtering described above. Before filtering there were 18 results.

Results per Host

10.0.2.15

Host scan start	Sat Dec 28 12:52:08 2024 UTC
Host scan end	Sat Dec 28 13:05:55 2024 UTC

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

Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Summary
The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

```
The certificate of the remote service expired on 2020-08-20 19:18:24.
Certificate details:
subject ...: C=DE,L=Osnabrueck,O=OpenVAS Users,CN=218ffb30ff7a
subject alternative names (SAN):
```

... continues on next page ...

... continued from previous page ...

```
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for 218f
↪fb30ff7a
serial ....: 5B7C65801F8422EBBDAD2299
valid from : 2018-08-21 19:18:24 UTC
valid until: 2020-08-20 19:18:24 UTC
fingerprint (SHA-1): 6B34D170BC2D0EAE4DB2D6122E2DA7E94F0ADF6F
fingerprint (SHA-256): A672ACF69BB0944271599E210BF04BF20736E3CCB5862FAF3EFAC9872
↪41BC4B9
```

Solution
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Vulnerability Insight
This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.

Vulnerability Detection Method
Details: `SSL/TLS: Certificate Expired`
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: `$Revision: 11103 $`

[return to 10.0.2.15]

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: 2814762215
Packet 2: 2814763379
```

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.

... continues on next page ...

... continued from previous page ...

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
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 10.0.2.15]

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 $`

... continues on next page ...

... continued from previous page ...

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

[return to 10.0.2.15]

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
10.0.2.15|cpe:/a:greenbone:greenbone_security_assistant:7.0.3
10.0.2.15|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 10.0.2.15]

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.

... continues on next page ...

... continued from previous page ...

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: `$Revision: 14244 $`

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 172.17.0.2 to 10.0.2.15:
172.17.0.2
10.0.2.15
```

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 10.0.2.15]

Log 443/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 "10.0.2.15" 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:
https://10.0.2.15/
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
```

. . . continues on next page . . .

... continued from previous page ...

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.
Note: The plugin needs the 'dirb' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result
`This are the directories/files found with brute force:`
`https://10.0.2.15:443/`

Log Method
Details: `DIRB (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: `$Revision: 13985 $`

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: Nikto (NASL wrapper)

Summary

... continues on next page ...

... continued from previous page ...

This plugin uses nikto to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.
Note: The plugin needs the 'nikto' or 'nikto.pl' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 10.0.2.15:443
---------------------------------------------------------------------------
+ 0 host(s) tested
```

Log Method
Details: `Nikto (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: `$Revision: 13985 $`

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 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

... continues on next page ...

... continued from previous page ...

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=218ffb30ff7a
subject alternative names (SAN):
None
issued by .: C=DE,L=Osnabrueck,O=OpenVAS Users,OU=Certificate Authority for 218f
↪fb30ff7a
serial ....: 5B7C65801F8422EBBDAD2299
valid from : 2018-08-21 19:18:24 UTC
valid until: 2020-08-20 19:18:24 UTC
fingerprint (SHA-1): 6B34D170BC2D0EAE4DB2D6122E2DA7E94F0ADF6F
fingerprint (SHA-256): A672ACF69BB0944271599E210BF04BF20736E3CCB5862FAF3EFAC9872
↪41BC4B9

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: $Revision: 13434 $

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

... continues on next page ...

... continued from previous page ...

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 TLSv1.1 protocol:
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
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_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 TLSv1.1 protocol:
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol:

... 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_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 TLSv1.1 protocol.
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_AES_256_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.
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
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_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.
```

... continues on next page ...

... continued from previous page ...

```
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 $`

Log (CVSS: 0.0)
NVT: wapiti (NASL wrapper)

Summary
This plugin uses wapiti to find web security issues.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
See the preferences section for wapiti options.
Note that the scanner is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Note: The plugin needs the 'wapiti' binary found within the PATH of the user running the scanner and needs to be executable for this user. The existence of this binary is checked and reported separately within 'Availability of scanner helper tools' (OID: 1.3.6.1.4.1.25623.1.0.810000).

Vulnerability Detection Result

```
The wapiti report filename is empty. That could mean that a wrong version of wap
↪iti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapi
↪ti 1.x is not supported.
In short: Check the installation of wapiti and the scanner.
```

Log Method
Details: `wapiti (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: `$Revision: 13985 $`

[return to 10.0.2.15]