Scan Report

October 15, 2025

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 "grav wizard 2". The scan started at Wed Oct 15 17:36:51 2025 UTC and ended at Wed Oct 15 18:06:39 2025 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
127.0.0.1 localhost	2	3	0	29	0
Total: 1	2	3	0	29	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 34 results selected by the filtering described above. Before filtering there were 34 results.

Results per Host

127.0.0.1

Host scan start	Wed Oct 15 17:36:57 2025 UTC
Host scan end	Wed Oct 15 18:06:39 2025 UTC

Service (Port)	Threat Level
25/tcp	High
9390/tcp	High
443/tcp	Medium
25/tcp	Medium
9390/tcp	Medium
443/tcp	Log
25/tcp	Log
9390/tcp	Log
general/CPE-T	Log
general/tcp	Log

High 25/tcp

High (CVSS: 7.5)
NVT: SMTP too long line

Summary
Some antivirus scanners dies when they process an email with a too long string without line breaks.

. . . continues on next page . . .

... continued from previous page ...

Such a message was sent. If there is an antivirus on your MTA, it might have crashed. Please check its status right now, as it is not possible to do it remotely.

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

Solution
Solution type: VendorFix
Contact the vendor of the antivirus scanner to get an update.

Vulnerability Detection Method
Details: `SMTP too long line`
OID:1.3.6.1.4.1.25623.1.0.11270
Version used: `$Revision: 13470 $`

[return to 127.0.0.1]

High 9390/tcp

High (CVSS: 10.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials

Product detection result
```
cpe:/a:openvas:openvas_manager:7.0
Detected by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.
↪1.25623.1.0.103825)
```

Summary
The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result
```
It was possible to login using the following credentials (username:password:role
↪):
admin:admin:Admin
```

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution
Solution type: Workaround
Change the password of the mentioned account(s).

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

Vulnerability Detection Method
Try to login with default credentials via the OMP/GMP protocol.
Details: `OpenVAS / Greenbone Vulnerability Manager Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.108554
Version used: `$Revision: 13944 $`

Product Detection Result
Product: `cpe:/a:openvas:openvas_manager:7.0`
Method: `OpenVAS / Greenbone Vulnerability Manager Detection`
OID: 1.3.6.1.4.1.25623.1.0.103825)

[return to 127.0.0.1]

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):
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.

... continues on next page ...

... continued from previous page ...

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 127.0.0.1]

Medium 25/tcp

Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result
`'VRFY root' produces the following answer: 252 2.0.0 root`

Solution
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: `Check if Mailserver answer to VRFY and EXPN requests`
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: `$Revision: 13470 $`

References
`Other:`
`URL:http://cr.yp.to/smtp/vrfy.html`

[return to 127.0.0.1]

Medium 9390/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):
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 127.0.0.1]

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)

... continues on next page ...

... continued from previous page ...

- 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 "localhost" 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://localhost/
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?/)"
https://localhost/css
https://localhost/img
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
https://localhost/omp (cmd [login] text [/omp?r=1] login [] password [] )
```

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: 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
```
Header Name                Header Value
-----------                ------------
Content-Security-Policy  : default-src 'self' 'unsafe-inline'; img-src 'self' bl
↪ob:; frame-ancestors 'self'
X-Frame-Options          : SAMEORIGIN
Missing Headers
---------------
Referrer-Policy
X-Content-Type-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

. . . continues on next page . . .

... continued from previous page ...

```
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 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.

... continues on next page ...

... continued from previous page ...

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: HTTP Public Key Pinning (HPKP) Missing

Summary

The remote web server is not enforcing HPKP.

Vulnerability Detection Result

```
The remote web server is not enforcing HPKP.
HTTP-Banner:
HTTP/1.1 303 See Other
Connection: close
Content-Length: ***replaced***
Content-Security-Policy: default-src 'self' 'unsafe-inline'; img-src 'self' blob
↪:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Expires: ***replaced***
Location: https://localhost/login/login.html
Date: ***replaced***
```

Solution

Solution type: Workaround
Enable HPKP or add / configure the required directives correctly following the guides linked in the references.

Log Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing
OID:1.3.6.1.4.1.25623.1.0.108247
Version used: $Revision: 7391 $

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#hpkp
   URL:https://tools.ietf.org/html/rfc7469
   URL:https://securityheaders.io/
```

Log (CVSS: 0.0)
NVT: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing

Summary
The remote web server is not enforcing HSTS.

Vulnerability Detection Result

```
The remote web server is not enforcing HSTS.
HTTP-Banner:
HTTP/1.1 303 See Other
Connection: close
Content-Length: ***replaced***
Content-Security-Policy: default-src 'self' 'unsafe-inline'; img-src 'self' blob
↪:; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Expires: ***replaced***
Location: https://localhost/login/login.html
Date: ***replaced***
```

Solution
Solution type: Workaround
Enable HSTS or add / configure the required directives correctly following the guides linked in the references.

Log Method
Details: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing
OID:1.3.6.1.4.1.25623.1.0.105879
Version used: $Revision: 7391 $

References

```
Other:
  URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
   URL:https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Shee
↪t
```

... continues on next page ...

... continued from previous page ...

URL:https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#hsts
URL:https://tools.ietf.org/html/rfc6797
URL:https://securityheaders.io/

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 TLSv1.1 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

... continues on next page ...

... continued from previous page ...

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:
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
```

... continues on next page ...

... continued from previous page ...

```
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.
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

... continues on next page ...

. . . continued from previous page . . .

Version used: $Revision: 13985 $

[return to 127.0.0.1]

Log 25/tcp

Log (CVSS: 0.0)
NVT: Postfix SMTP Server Detection

Summary
The script checks the SMTP server banner for the presence of Postfix.

Vulnerability Detection Result

```
Detected Postfix
Version:  unknown
Location: 25/tcp
CPE:      cpe:/a:postfix:postfix
Concluded from version/product identification result:
220 9c89ef55d1a6.localdomain ESMTP Postfix
```

Log Method
Details: Postfix SMTP Server Detection
OID:1.3.6.1.4.1.25623.1.0.111086
Version used: $Revision: 13461 $

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 SMTP server is running on this port
Here is its banner :
220 9c89ef55d1a6.localdomain ESMTP Postfix
```

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

Log (CVSS: 7.2)
NVT: SMTP antivirus scanner DoS

Summary
This script sends the 42.zip recursive archive to the mail server. If there is an antivirus filter, it may start eating huge amounts of CPU or memory.

Vulnerability Detection Result
`For some reason, we could not send the 42.zip file to this MTA.`

Solution
Solution type: Mitigation
Reconfigure your antivirus / upgrade it.

Vulnerability Detection Method
Details: `SMTP antivirus scanner DoS`
OID:1.3.6.1.4.1.25623.1.0.11036
Version used: `$Revision: 13470 $`

References
`BID:3027`

Log (CVSS: 0.0)
NVT: SMTP Missing Support For STARTTLS

Summary
The remote SMTP server does not support the 'STARTTLS' command.

Vulnerability Detection Result
`The remote SMTP server does not support the 'STARTTLS' command.`

Log Method
Details: `SMTP Missing Support For STARTTLS`
OID:1.3.6.1.4.1.25623.1.0.105091
Version used: `$Revision: 13153 $`

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

Summary
This detects the SMTP Server's type and version by connecting to the server and processing the buffer received.

Vulnerability Detection Result
`Remote SMTP server banner:`
`220 9c89ef55d1a6.localdomain ESMTP Postfix`

... continues on next page ...

... continued from previous page ...

```
The remote SMTP server is announcing the following available ESMTP commands (EHL
↪O response) via an unencrypted connection:
8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY
```

Log Method
Details: SMTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10263
Version used: $Revision: 14004 $

[return to 127.0.0.1]

Log 9390/tcp

Log (CVSS: 0.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Detection

Summary
The script sends a connection request to the server and attempts to determine if it is a OpenVAS Manager (openvasmd) or Greebone Vulnerability Manager (gmvd).

Vulnerability Detection Result

```
Detected OpenVAS Manager
Version:  7.0
Location: 9390/tcp
CPE:      cpe:/a:openvas:openvas_manager:7.0
Concluded from version/product identification result:
OMP protocol version request '<GET_VERSION/>', response: <version>7.0</version>
```

Log Method
Details: OpenVAS / Greenbone Vulnerability Manager Detection
OID:1.3.6.1.4.1.25623.1.0.103825
Version used: $Revision: 13874 $

Log (CVSS: 0.0)
NVT: Service Detection with '<xml/>' Request

Summary
This plugin performs service detection.
This plugin is a complement of find_service.nasl. It sends a '<xml/>' request to the remaining unknown services and tries to identify them.

Vulnerability Detection Result

```
A OpenVAS / Greenbone Vulnerability Manager supporting the OMP/GMP protocol seem
↪s to be running on this port.
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: `Service Detection with '<xml/>' Request`
OID:1.3.6.1.4.1.25623.1.0.108198
Version used: `$Revision: 13874 $`

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: 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`

... continues on next page ...

... continued from previous page ...

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
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
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

... continues on next page ...

... continued from previous page ...

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
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

... continues on next page ...

... continued from previous page ...

```
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.
'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
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 127.0.0.1]

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

```
127.0.0.1|cpe:/a:greenbone:greenbone_security_assistant:7.0.3
127.0.0.1|cpe:/a:openvas:openvas_manager:7.0
127.0.0.1|cpe:/a:postfix:postfix
127.0.0.1|cpe:/o:linux:linux_kernel:2.6.32
```

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 127.0.0.1]

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 2.6.32
CPE: cpe:/o:linux:linux_kernel:2.6.32
Found by NVT: 1.3.6.1.4.1.25623.1.0.108021 (Nmap OS Identification (NASL wrapper
↪))
Concluded from Nmap TCP/IP fingerprinting:
OS details: Linux 2.6.32
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
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
```

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

. . . 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 127.0.0.1 to 127.0.0.1:
127.0.0.1
```

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 127.0.0.1]