Scan Report

June 8, 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 "Network Vulnerability Scan". The scan started at Sat Jun 8 13:47:40 2024 UTC and ended at Sat Jun 8 14:17:22 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
172.28.224.1	0	3	1	23	0
Total: 1	0	3	1	23	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 27 results selected by the filtering described above. Before filtering there were 27 results.

Results per Host

172.28.224.1

Host scan start	Sat Jun 8 13:47:52 2024 UTC
Host scan end	Sat Jun 8 14:17:22 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium
general/tcp	Medium
443/tcp	Medium
general/tcp	Low
135/tcp	Log
general/SMBClient	Log
445/tcp	Log
general/tcp	Log
443/tcp	Log
5357/tcp	Log
139/tcp	Log
general/CPE-T	Log

Medium 135/tcp

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

Summary

. . . continues on next page . . .

... continued from previous page ...

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: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:172.28.224.1[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49665]
Port: 49666/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49667]
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49667]
Port: 49668/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49668]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[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:172.28.224.1[49668]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:172.28.224.1[49668]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
```

... continues on next page ...

... continued from previous page ...

```
     Endpoint: ncacn_ip_tcp:172.28.224.1[49668]
Port: 49670/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.28.224.1[49670]
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 172.28.224.1]

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

... continues on next page ...

... continued from previous page ...

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 172.28.224.1]

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
```

... continues on next page ...

... continued from previous page ...

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 172.28.224.1]

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: 3601232467
Packet 2: 3601233906

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 172.28.224.1]

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

... continues on next page ...

. . . continued from previous page . . .

Version used: $Revision: 11885 $

[return to 172.28.224.1]

Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test with 'smbclient'

Summary
This script reports information about the SMB server of the remote host collected with the 'smbclient' tool.

Vulnerability Detection Result
Error getting SMB-Data -> PROTOCOL NEGOTIATION FAILED: NT_STATUS_CONNECTION_DISC
↪ONNECTED

Log Method
Details: SMB Test with 'smbclient'
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: $Revision: 13274 $

[return to 172.28.224.1]

Log 445/tcp

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
Only SMBv2 is 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 $

. . . continues on next page . . .

. . . continued from previous page . . .

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 172.28.224.1]

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: Microsoft Windows
CPE: cpe:/o:microsoft:windows
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 5357/tcp: Server: Microsoft-HTTPAPI/2.
↪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
```

. . . continues on next page . . .

... continued from previous page ...

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 172.28.224.1:`
`172.17.0.2`
`172.28.224.1`

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 172.28.224.1]

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 "172.28.224.1" 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://172.28.224.1/
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: /
```

... continues on next page ...

... continued from previous page ...

CPE: cpe:/a:greenbone:greenbone_security_assistant:7.0.3
Concluded from version/product identification result:
Version 7.0.3

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.

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

... continues on next page ...

... continued from previous page ...

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
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.

... continues on next page ...

... continued from previous page ...

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:
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

... continues on next page ...

... continued from previous page ...

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.
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 $

... continues on next page ...

... continued from previous page ...

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 172.28.224.1]

Log 5357/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

... continues on next page ...

... continued from previous page ...

```
The Hostname/IP "172.28.224.1" 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.
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://172.28.224.1:5357/
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 :
Microsoft-HTTPAPI/2.0
```

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: Nikto (NASL wrapper)

Summary
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
---------------------------------------------------------------------------
+ Target IP:          172.28.224.1
+ Target Hostname:    172.28.224.1
+ Target Port:        5357
+ Start Time:         2024-06-08 14:00:59 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
↪gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
↪to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7553 requests: 1 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-06-08 14:04:47 (GMT0) (228 seconds)
---------------------------------------------------------------------------
+ 1 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 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 $`

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 172.28.224.1]

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

... 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 172.28.224.1]

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
172.28.224.1|cpe:/a:greenbone:greenbone_security_assistant:7.0.3
172.28.224.1|cpe:/o:microsoft:windows

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 172.28.224.1]