

Scan Report

April 13, 2016

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 192.168.116.167”. The scan started at Wed Apr 13 22:30:39 2016 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	2
2	Results per Host	2
2.1	192.168.116.167	2
2.1.1	Medium 8443/tcp	2
2.1.2	Medium 443/tcp	6
2.1.3	Low general/tcp	10
2.1.4	Log 8443/tcp	11
2.1.5	Log 443/tcp	14
2.1.6	Log general/tcp	23
2.1.7	Log general/icmp	24
2.1.8	Log 8080/tcp	25
2.1.9	Log 80/tcp	26
2.1.10	Log 631/tcp	41
2.1.11	Log 515/tcp	45
2.1.12	Log 4567/tcp	46
2.1.13	Log 2555/tcp	48

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.116.167	0	8	1	96	0
Total: 1	0	8	1	96	0

Vendor security updates are not trusted.

Overrides are on. When a result has an override, this report uses the threat of the override.

Notes are included in the report.

This report might not show details of all issues that were found.

It only lists hosts that produced issues.

Issues with the threat level “Debug” are not shown.

Issues with the threat level “False Positive” are not shown.

This report contains all 105 results selected by the filtering described above. Before filtering there were 106 results.

2 Results per Host

2.1 192.168.116.167

Host scan start Wed Apr 13 22:30:45 2016 UTC

Host scan end

Service (Port)	Threat Level
8443/tcp	Medium
443/tcp	Medium
general/tcp	Low
8443/tcp	Log
443/tcp	Log
general/tcp	Log
general/icmp	Log
8080/tcp	Log
80/tcp	Log
631/tcp	Log
515/tcp	Log
4567/tcp	Log
2555/tcp	Log

2.1.1 Medium 8443/tcp

... continues on next page ...

...continued from previous page ...

Medium (CVSS: 6.8)

NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary

OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution**Solution type:** VendorFix

Updates are available.

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

Details:OpenSSL CCS Man in the Middle Security Bypass Vulnerability

OID:1.3.6.1.4.1.25623.1.0.105042

Version used: \$Revision: 1369 \$

References

CVE: CVE-2014-0224

BID:67899

Other:

URL:<http://www.securityfocus.com/bid/67899>URL:<http://openssl.org/>

Medium (CVSS: 4.3)

NVT: Check for SSL Weak Ciphers

Summary

This routine search for weak SSL ciphers offered by a service.

... continues on next page ...

...continued from previous page ...

Vulnerability Detection Result

Weak ciphers offered by this service:

SSL2_RC4_128_MD5
 SSL2_RC4_128_EXPORT40_WITH_MD5
 SSL2_RC2_CBC_128_CBC_WITH_MD5
 SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
 SSL3_RSA_RC4_128_MD5
 SSL3_RSA_RC4_128_SHA
 SSL3_RSA_DES_64_CBC_SHA
 TLS1_RSA_RC4_128_MD5
 TLS1_RSA_RC4_128_SHA
 TLS1_RSA_DES_64_CBC_SHA

Solution

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS j 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method

Details: Check for SSL Weak Ciphers

OID: 1.3.6.1.4.1.25623.1.0.103440

Version used: \$Revision: 2012 \$

Medium (CVSS: 4.3)

NVT: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv2 and SSL ↪v3 protocols and supports one or more ciphers.

Impact

...continues on next page ...

...continued from previous page ...
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Solution It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws.
Vulnerability Detection Method Check the used protocols of the services provided by this system. Details:Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: \$Revision: 1183 \$
References Other: URL: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithm-key-sizes-and-parameters-report URL: https://bettercrypto.org/

Medium (CVSS: 4.3) NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
Summary This host is installed with OpenSSL and is prone to information disclosure vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application
Solution Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE: The only correct way to fix POODLE is to disable SSL v3.0
Affected Software/OS ... continues on next page ...

...continued from previous page ...
OpenSSL through 1.0.1i
Vulnerability Insight The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code
Vulnerability Detection Method Send a SSLv3 request and check the response. Details:POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability OID:1.3.6.1.4.1.25623.1.0.802087 Version used: \$Revision: 2249 \$
References CVE: CVE-2014-3566 BID:70574 Other: URL:http://osvdb.com/113251 URL:https://www.openssl.org/~bodo/ssl-poodle.pdf URL:https://www.imperialviolet.org/2014/10/14/poodle.html URL:https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html URL:http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit ↪ing-ssl-30.html

[[return to 192.168.116.167](#)]

2.1.2 Medium 443/tcp

Medium (CVSS: 6.8) NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
Summary OpenSSL is prone to security-bypass vulnerability.
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.
Solution Solution type: VendorFix Updates are available.
Affected Software/OS OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h ... continues on next page ...

...continued from previous page ...

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

Details: [OpenSSL CCS Man in the Middle Security Bypass Vulnerability](#)

OID: 1.3.6.1.4.1.25623.1.0.105042

Version used: \$Revision: 1369 \$

References

CVE: CVE-2014-0224

BID: 67899

Other:

URL: <http://www.securityfocus.com/bid/67899>

URL: <http://openssl.org/>

Medium (CVSS: 4.3)

NVT: Check for SSL Weak Ciphers

Summary

This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result

Weak ciphers offered by this service:

SSL2_RC4_128_MD5
 SSL2_RC4_128_EXPORT40_WITH_MD5
 SSL2_RC2_CBC_128_CBC_WITH_MD5
 SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
 SSL3_RSA_RC4_128_MD5
 SSL3_RSA_RC4_128_SHA
 SSL3_RSA_DES_64_CBC_SHA
 TLS1_RSA_RC4_128_MD5
 TLS1_RSA_RC4_128_SHA
 TLS1_RSA_DES_64_CBC_SHA

Solution

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.

... continues on next page ...

...continued from previous page ...
<ul style="list-style-type: none"> - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong
Vulnerability Detection Method Details:Check for SSL Weak Ciphers OID:1.3.6.1.4.1.25623.1.0.103440 Version used: \$Revision: 2012 \$
Medium (CVSS: 4.3) NVT: Deprecated SSLv2 and SSLv3 Protocol Detection
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
Vulnerability Detection Result In addition to TLSv1+ the service is also providing the deprecated SSLv2 and SSL ↪v3 protocols and supports one or more ciphers.
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transfered within the secured connection.
Solution It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.
Affected Software/OS All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws.
Vulnerability Detection Method Check the used protocols of the services provided by this system. Details:Deprecated SSLv2 and SSLv3 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.111012 Version used: \$Revision: 1183 \$
References ... continues on next page ...

...continued from previous page ...

Other:

URL:<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithm-key-sizes-and-parameters-report>
 URL:<https://bettercrypto.org/>

Medium (CVSS: 4.3)

NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

Summary

This host is installed with OpenSSL and is prone to information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Impact Level: Application

Solution

Vendor released a patch to address this vulnerability, For updates contact vendor or refer to <https://www.openssl.org>

NOTE: The only correct way to fix POODLE is to disable SSL v3.0

Affected Software/OS

OpenSSL through 1.0.1i

Vulnerability Insight

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Send a SSLv3 request and check the response.

Details:POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability

OID:1.3.6.1.4.1.25623.1.0.802087

Version used: \$Revision: 2249 \$

References

CVE: CVE-2014-3566

BID:70574

Other:

URL:<http://osvdb.com/113251>

URL:<https://www.openssl.org/~bodo/ssl-poodle.pdf>

URL:<https://www.imperialviolet.org/2014/10/14/poodle.html>

URL:<https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html>

URL:<http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploit-ing-ssl-30.html>

[\[return to 192.168.116.167 \]](#)

2.1.3 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: Paket 1: 19917429 Paket 2: 19917529
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution 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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152
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: 787 \$
References Other: URL: http://www.ietf.org/rfc/rfc1323.txt

[\[return to 192.168.116.167 \]](#)

2.1.4 Log 8443/tcp

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin 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 and set the results in the plugins knowledge base.
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: 69 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin 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 and set the results in the plugins knowledge base.
Vulnerability Detection Result A web server is running on this port through SSL
Log Method ... continues on next page ...

...continued from previous page ...

Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: \$Revision: 69 \$

Log (CVSS: 0.0)
NVT: Directories used for CGI Scanning

Summary

The script prints out the directories which are used when CGI scanning is enabled.

Vulnerability Detection Result

The following directories are used for CGI scanning:

/cgi-bin
/scripts
/

Log Method

Details:Directories used for CGI Scanning
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: \$Revision: 1727 \$

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.

Vulnerability Detection Result

wapiti report filename is empty. that could mean that
wrong version of wapiti is used or tmp dir is not accessible.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
In short: check installation of wapiti and OpenVAS

Log Method

Details:wapiti (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: \$Revision: 2227 \$

...continues on next page ...

...continued from previous page ...

Log (CVSS: 0.0)

NVT: Check for SSL Ciphers

Summary

This routine search for SSL ciphers offered by a service.

Vulnerability Detection Result

Service supports SSLv2 ciphers.

Service supports SSLv3 ciphers.

Service supports TLSv1 ciphers.

Medium ciphers offered by this service:

SSL3_RSA_DES_192_CBC3_SHA

TLS1_RSA_DES_192_CBC3_SHA

Weak ciphers offered by this service:

SSL2_RC4_128_MD5

SSL2_RC4_128_EXPORT40_WITH_MD5

SSL2_RC2_CBC_128_CBC_WITH_MD5

SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5

SSL3_RSA_RC4_128_MD5

SSL3_RSA_RC4_128_SHA

SSL3_RSA_DES_64_CBC_SHA

TLS1_RSA_RC4_128_MD5

TLS1_RSA_RC4_128_SHA

TLS1_RSA_DES_64_CBC_SHA

No non-ciphers are supported by this service

Log Method

Details:Check for SSL Ciphers

OID:1.3.6.1.4.1.25623.1.0.802067

Version used: \$Revision: 2012 \$

Log (CVSS: 0.0)

NVT: Check for SSL Medium Ciphers

Summary

This Plugin reports about SSL Medium Ciphers.

Vulnerability Detection Result

Medium ciphers offered by this service:

SSL3_RSA_DES_192_CBC3_SHA

TLS1_RSA_DES_192_CBC3_SHA

Log Method

Details:Check for SSL Medium Ciphers

OID:1.3.6.1.4.1.25623.1.0.902816

Version used: \$Revision: 2012 \$

[\[return to 192.168.116.167 \]](#)

2.1.5 Log 443/tcp

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:2555/ http://192.168.116.167:631/ https://192.168.116.167:443/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:2555/ https://192.168.116.167:443/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
...continues on next page ...

...continued from previous page ...
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:4567/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:4567/</code> <code>http://192.168.116.167:2555/</code> <code>https://192.168.116.167:443/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:4567/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code>
Log Method ... continues on next page ...

...continued from previous page ...	
Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/ https://192.168.116.167:443/	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:631/ https://192.168.116.167:443/	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
...continues on next page ...	

...continued from previous page ...
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:2555/</code> <code>https://192.168.116.167:443/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:4567/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code>
... continues on next page ...

...continued from previous page ...

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

<https://192.168.116.167:8443/><http://192.168.116.167:8080/><http://192.168.116.167:4567/><http://192.168.116.167:2555/><https://192.168.116.167:443/>**Log Method**

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

<https://192.168.116.167:8443/><http://192.168.116.167:8080/><http://192.168.116.167:4567/><http://192.168.116.167:631/><https://192.168.116.167:443/>**Log Method**

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:4567/</code> <code>https://192.168.116.167:443/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> ... continues on next page ...

...continued from previous page ...	
https://192.168.116.167:443/	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ https://192.168.116.167:443/	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: Services	
Summary This plugin 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 and set the results in the plugins knowledge base.	
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: 69 \$	
Log (CVSS: 0.0) NVT: Services	
Summary ...continues on next page ...	

...continued from previous page ...
This plugin 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 and set the results in the plugins knowledge base.
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: 69 \$

Log (CVSS: 0.0) NVT: Directories used for CGI Scanning
Summary The script prints out the directories which are used when CGI scanning is enabled.
Vulnerability Detection Result The following directories are used for CGI scanning: /cgi-bin /scripts /
Log Method Details:Directories used for CGI Scanning OID:1.3.6.1.4.1.25623.1.0.111038 Version used: \$Revision: 1727 \$

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Vulnerability Detection Result wapiti report filename is empty. that could mean that wrong version of wapiti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapiti 1.x is not supported. In short: check installation of wapiti and OpenVAS
...continues on next page ...

...continued from previous page ...

Log Method

Details:wapiti (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.80110
Version used: \$Revision: 2227 \$

Log (CVSS: 0.0)

NVT: Check for SSL Ciphers

Summary

This routine search for SSL ciphers offered by a service.

Vulnerability Detection Result

Service supports SSLv2 ciphers.

Service supports SSLv3 ciphers.

Service supports TLSv1 ciphers.

Medium ciphers offered by this service:

SSL3_RSA_DES_192_CBC3_SHA

TLS1_RSA_DES_192_CBC3_SHA

Weak ciphers offered by this service:

SSL2_RC4_128_MD5

SSL2_RC4_128_EXPORT40_WITH_MD5

SSL2_RC2_CBC_128_CBC_WITH_MD5

SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5

SSL3_RSA_RC4_128_MD5

SSL3_RSA_RC4_128_SHA

SSL3_RSA_DES_64_CBC_SHA

TLS1_RSA_RC4_128_MD5

TLS1_RSA_RC4_128_SHA

TLS1_RSA_DES_64_CBC_SHA

No non-ciphers are supported by this service

Log Method

Details:Check for SSL Ciphers
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: \$Revision: 2012 \$

Log (CVSS: 0.0)

NVT: Check for SSL Medium Ciphers

Summary

This Plugin reports about SSL Medium Ciphers.

Vulnerability Detection Result

Medium ciphers offered by this service:

SSL3_RSA_DES_192_CBC3_SHA

...continues on next page ...

...continued from previous page ...
TLS1_RSA_DES_192_CBC3_SHA
Log Method Details:Check for SSL Medium Ciphers OID:1.3.6.1.4.1.25623.1.0.902816 Version used: \$Revision: 2012 \$

[\[return to 192.168.116.167 \]](#)

2.1.6 Log general/tcp

Log (CVSS: 0.0) NVT: OS fingerprinting
Summary This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack 57). It can be used to determine remote operating system version.
Vulnerability Detection Result ICMP based OS fingerprint results: (100% confidence) Linux Kernel
Log Method Details:OS fingerprinting OID:1.3.6.1.4.1.25623.1.0.102002 Version used: \$Revision: 2246 \$
References Other: URL: http://www.phrack.org/issues.html?issue=57&id=7#article

Log (CVSS: 0.0) NVT: arachni (NASL wrapper)
Summary This plugin uses arachni ruby command line to find web security issues. See the preferences section for arachni options. Note that OpenVAS is using limited set of arachni options. Therefore, for more complete web assessment, you should use standalone arachni tool for deeper/customized checks.
Vulnerability Detection Result Arachni could not be found in your system path. OpenVAS was unable to execute Arachni and to perform the scan you requested. Please make sure that Arachni is installed and that arachni is
...continues on next page ...

...continued from previous page ...
available in the PATH variable defined for your environment.
Log Method Details:arachni (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.110001 Version used: \$Revision: 2204 \$

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 192.168.1.6 to 192.168.116.167: 192.168.1.6 192.168.116.167
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: 975 \$

[\[return to 192.168.116.167 \]](#)

2.1.7 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.
... continues on next page ...

...continued from previous page ...

Log Method

Details:ICMP Timestamp Detection

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: \$Revision: 2169 \$

References

CVE: CVE-1999-0524

Other:

URL:http://www.ietf.org/rfc/rfc0792.txt

[\[return to 192.168.116.167 \]](#)**2.1.8 Log 8080/tcp**

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:8080/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: Services

Summary

This plugin 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 and set the results in the plugins knowledge base.

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

...continues on next page ...

...continued from previous page ...

Version used: \$Revision: 69 \$

Log (CVSS: 0.0)

NVT: Directories used for CGI Scanning

Summary

The script prints out the directories which are used when CGI scanning is enabled.

Vulnerability Detection Result

The following directories are used for CGI scanning:

```
/cgi-bin
/scripts
/
```

Log Method

Details:Directories used for CGI Scanning

OID:1.3.6.1.4.1.25623.1.0.111038

Version used: \$Revision: 1727 \$

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.

Vulnerability Detection Result

```
wapiti report filename is empty. that could mean that
wrong version of wapiti is used or tmp dir is not accessible.
Make sure to have wapiti 2.x as wapiti 1.x is not supported.
In short: check installation of wapiti and OpenVAS
```

Log Method

Details:wapiti (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.80110

Version used: \$Revision: 2227 \$

[\[return to 192.168.116.167 \]](#)

2.1.9 Log 80/tcp

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code> <code>http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> ...continues on next page ...

...continued from previous page ...

http://192.168.116.167:2555/
http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/
http://192.168.116.167:2555/
https://192.168.116.167:443/
http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/
http://192.168.116.167:4567/
http://192.168.116.167:2555/
http://192.168.116.167:631/
http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:2555/ http://192.168.116.167:631/ https://192.168.116.167:443/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:2555/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: ...continues on next page ...

...continued from previous page ...
<code>https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:2555/ https://192.168.116.167:443/ http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:631/ http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:631/ https://192.168.116.167:443/ http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) ...continues on next page ...

...continued from previous page ...	
OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:80/	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/ https://192.168.116.167:443/ http://192.168.116.167:80/	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
...continues on next page ...	

...continued from previous page ...

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:631/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:631/

https://192.168.116.167:443/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code> <code>https://192.168.116.167:443/</code> <code>http://192.168.116.167:80/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
<p>This are the directories/files found with brute force:</p> <pre>https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:2555/ http://192.168.116.167:80/</pre>
<p>Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$</p>

<p>Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)</p>
<p>Summary This script uses DIRB to find directories and files on web applications via brute forcing.</p>
<p>Vulnerability Detection Result This are the directories/files found with brute force:</p> <pre>https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:2555/ https://192.168.116.167:443/ http://192.168.116.167:80/</pre>
<p>Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$</p>

<p>Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)</p>
<p>Summary This script uses DIRB to find directories and files on web applications via brute forcing.</p>
<p>Vulnerability Detection Result This are the directories/files found with brute force:</p> <pre>https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ http://192.168.116.167:2555/ http://192.168.116.167:631/ http://192.168.116.167:80/</pre>
<p>... continues on next page ...</p>

...continued from previous page ...

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:8080/

http://192.168.116.167:4567/

http://192.168.116.167:2555/

http://192.168.116.167:631/

https://192.168.116.167:443/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:8080/

http://192.168.116.167:4567/

http://192.168.116.167:2555/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ http://192.168.116.167:2555/ https://192.168.116.167:443/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ http://192.168.116.167:631/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result ... continues on next page ...

...continued from previous page ...
This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ http://192.168.116.167:631/ https://192.168.116.167:443/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ https://192.168.116.167:443/ http://192.168.116.167:80/
...continues on next page ...

...continued from previous page ...

Log Method

Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/
http://192.168.116.167:8080/
http://192.168.116.167:631/
http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/
http://192.168.116.167:8080/
http://192.168.116.167:631/
https://192.168.116.167:443/
http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: \$Revision: 2161 \$

...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.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:8080/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

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

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:8080/

https://192.168.116.167:443/

http://192.168.116.167:80/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

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

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

...continues on next page ...

...continued from previous page ...
https://192.168.116.167:443/ http://192.168.116.167:80/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin 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 and set the results in the plugins knowledge base.
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: 69 \$

Log (CVSS: 0.0) NVT: Directories used for CGI Scanning
Summary The script prints out the directories which are used when CGI scanning is enabled.
Vulnerability Detection Result The following directories are used for CGI scanning: /cgi-bin /scripts /
Log Method Details:Directories used for CGI Scanning OID:1.3.6.1.4.1.25623.1.0.111038 Version used: \$Revision: 1727 \$

Log (CVSS: 0.0) NVT: wapiti (NASL wrapper)
...continues on next page ...

...continued from previous page ...

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.

Vulnerability Detection Result

wapiti report filename is empty. that could mean that

wrong version of wapiti is used or tmp dir is not accessible.

Make sure to have wapiti 2.x as wapiti 1.x is not supported.

In short: check installation of wapiti and OpenVAS

Log Method

Details:wapiti (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.80110

Version used: \$Revision: 2227 \$

[\[return to 192.168.116.167 \]](#)

2.1.10 Log 631/tcp

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:2555/

http://192.168.116.167:631/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

...continues on next page ...

...continued from previous page ...

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:4567/

http://192.168.116.167:2555/

http://192.168.116.167:631/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:4567/

http://192.168.116.167:631/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:631/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:4567/</code> <code>http://192.168.116.167:2555/</code> <code>http://192.168.116.167:631/</code>
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> ...continues on next page ...

...continued from previous page ...	
<code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:4567/</code> <code>http://192.168.116.167:631/</code>	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)	
Summary This script uses DIRB to find directories and files on web applications via brute forcing.	
Vulnerability Detection Result This are the directories/files found with brute force: <code>https://192.168.116.167:8443/</code> <code>http://192.168.116.167:8080/</code> <code>http://192.168.116.167:631/</code>	
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$	
Log (CVSS: 0.0) NVT: Services	
Summary This plugin 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 and set the results in the plugins knowledge base.	
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: 69 \$	
...continues on next page ...	

...continued from previous page ...

Log (CVSS: 0.0) NVT: Directories used for CGI Scanning
Summary The script prints out the directories which are used when CGI scanning is enabled.
Vulnerability Detection Result The following directories are used for CGI scanning: /cgi-bin /scripts /
Log Method Details:Directories used for CGI Scanning OID:1.3.6.1.4.1.25623.1.0.111038 Version used: \$Revision: 1727 \$

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Vulnerability Detection Result wapiti report filename is empty. that could mean that wrong version of wapiti is used or tmp dir is not accessible. Make sure to have wapiti 2.x as wapiti 1.x is not supported. In short: check installation of wapiti and OpenVAS
Log Method Details:wapiti (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.80110 Version used: \$Revision: 2227 \$

[\[return to 192.168.116.167 \]](#)

2.1.11 Log 515/tcp

Log (CVSS: 0.0) NVT: Identify unknown services with nmap
Summary This plugin performs service detection by launching nmap's service probe against ports running unidentified services. Description :
Vulnerability Detection Result Nmap service detection result for this port: printer
Log Method Details:Identify unknown services with nmap OID:1.3.6.1.4.1.25623.1.0.66286 Version used: \$Revision: 329 \$

[\[return to 192.168.116.167 \]](#)

2.1.12 Log 4567/tcp

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ ...continues on next page ...

...continued from previous page ...
http://192.168.116.167:8080/ http://192.168.116.167:4567/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin 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 and set the results in the plugins knowledge base.
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: 69 \$

Log (CVSS: 0.0) NVT: Directories used for CGI Scanning
Summary The script prints out the directories which are used when CGI scanning is enabled.
Vulnerability Detection Result The following directories are used for CGI scanning: /cgi-bin /scripts /
Log Method Details:Directories used for CGI Scanning OID:1.3.6.1.4.1.25623.1.0.111038 Version used: \$Revision: 1727 \$

Log (CVSS: 0.0) NVT: wapiti (NASL wrapper)
...continues on next page ...

...continued from previous page ...

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.

Vulnerability Detection Result

wapiti report filename is empty. that could mean that

wrong version of wapiti is used or tmp dir is not accessible.

Make sure to have wapiti 2.x as wapiti 1.x is not supported.

In short: check installation of wapiti and OpenVAS

Log Method

Details:wapiti (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.80110

Version used: \$Revision: 2227 \$

[\[return to 192.168.116.167 \]](#)

2.1.13 Log 2555/tcp

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

This are the directories/files found with brute force:

https://192.168.116.167:8443/

http://192.168.116.167:2555/

Log Method

Details:DIRB (NASL wrapper)

OID:1.3.6.1.4.1.25623.1.0.103079

Version used: \$Revision: 2161 \$

Log (CVSS: 0.0)

NVT: DIRB (NASL wrapper)

Summary

This script uses DIRB to find directories and files on web applications via brute forcing.

Vulnerability Detection Result

...continues on next page ...

...continued from previous page ...
This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:4567/ http://192.168.116.167:2555/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:2555/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing.
Vulnerability Detection Result This are the directories/files found with brute force: https://192.168.116.167:8443/ http://192.168.116.167:8080/ http://192.168.116.167:4567/ http://192.168.116.167:2555/
Log Method Details:DIRB (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.103079 Version used: \$Revision: 2161 \$

Log (CVSS: 0.0) NVT: Services
Summary This plugin 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 and set the results in the plugins knowledge base.
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: 69 \$

Log (CVSS: 0.0) NVT: Directories used for CGI Scanning
Summary The script prints out the directories which are used when CGI scanning is enabled.
Vulnerability Detection Result The following directories are used for CGI scanning: /cgi-bin /scripts /
Log Method Details:Directories used for CGI Scanning OID:1.3.6.1.4.1.25623.1.0.111038 Version used: \$Revision: 1727 \$

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 OpenVAS is using limited set of wapiti options. Therefore, for more complete web assessment, you should use standalone wapiti tool for deeper/customized checks.
Vulnerability Detection Result wapiti report filename is empty. that could mean that wrong version of wapiti is used or tmp dir is not accessible. ...continues on next page ...

...continued from previous page ...
Make sure to have wapiti 2.x as wapiti 1.x is not supported. In short: check installation of wapiti and OpenVAS
Log Method Details:wapiti (NASL wrapper) OID:1.3.6.1.4.1.25623.1.0.80110 Version used: \$Revision: 2227 \$

[\[return to 192.168.116.167 \]](#)

This file was automatically generated.