Scan Report

May 22, 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 172.16.93.132". The scan started at Sun May 22 17:26:15 2016 UTC and ended at Sun May 22 18:03:16 2016 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
172.16.93.132	6	7	2	45	0
Total: 1	6	7	2	45	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 60 results selected by the filtering described above. Before filtering there were 89 results.

Results per Host

172.16.93.132

Host scan start	Sun May 22 17:28:05 2016 UTC
Host scan end	Sun May 22 18:02:32 2016 UTC

Service (Port)	Threat Level
1524/tcp	High
3632/tcp	High
5432/tcp	High
3306/tcp	High
22/tcp	High
445/tcp	High
3306/tcp	Medium
22/tcp	Medium
25/tcp	Medium
512/tcp	Medium
22/tcp	Low
general/tcp	Low
1524/tcp	Log
3632/tcp	Log
5432/tcp	Log
3306/tcp	Log
22/tcp	Log
445/tcp	Log
25/tcp	Log

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
general/tcp	Log
general/icmp	Log
general/SMBClient	Log
general/CPE-T	Log
8787/tcp	Log
8009/tcp	Log
80/tcp	Log
6667/tcp	Log
5900/tcp	Log
514/tcp	Log
513/tcp	Log
23/tcp	Log
2121/tcp	Log
21/tcp	Log
2049/tcp	Log
111/tcp	Log
1099/tcp	Log

High 1524/tcp

High (CVSS: 10.0)
NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host
Attackers can exploit this issue to execute arbitrary commands in the context of the application.
Successful attacks will compromise the affected isystem.

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

Solution
Solution type: Workaround

Vulnerability Detection Method
Details:`Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `$Revision: 3062 $`

[return to 172.16.93.132]

High 3632/tcp

High (CVSS: 9.3)
NVT: distcc Remote Code Execution Vulnerability

Summary
distcc 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

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

Solution
Vendor updates are available. Please see the references for more information.

Vulnerability Detection Method
Details:`distcc Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: `$Revision: 3062 $`

References
```
CVE: CVE-2004-2687
Other:
  URL:http://distcc.samba.org/security.html
   URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2687
   URL:http://www.osvdb.org/13378
   URL:http://archives.neohapsis.com/archives/bugtraq/2005-03/0183.html
```

[return to 172.16.93.132]

High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Summary
It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result
`It was possible to login as user postgres with password "postgres".`

Solution
Change the password as soon as possible.

Vulnerability Detection Method
Details:`PostgreSQL weak password`
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: `$Revision: 3062 $`

[return to 172.16.93.132]

High 3306/tcp

High (CVSS: 9.0) NVT: MySQL weak password
Summary It was possible to login into the remote MySQL as root using weak credentials.
Vulnerability Detection Result `It was possible to login as root with an empty password.`
Solution Change the password as soon as possible.
Vulnerability Detection Method Details:`MySQL weak password` OID:1.3.6.1.4.1.25623.1.0.103551 Version used: `$Revision: 3046 $`

[return to 172.16.93.132]

High 22/tcp

High (CVSS: 9.0) NVT: SSH Brute Force Logins with default Credentials
Summary A number of known default credentials is tried for log in via SSH protocol.

Vulnerability Detection Result
`It was possible to login with the following credentials <User>:<Password>`
`user:user`

Solution Change the password as soon as possible.
Vulnerability Detection Method Details:`SSH Brute Force Logins with default Credentials` OID:1.3.6.1.4.1.25623.1.0.103239 Version used: `$Revision: 2435 $`

[return to 172.16.93.132]

High 445/tcp

High (CVSS: 7.5) NVT: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
Summary The host is running SMB/NETBIOS and prone to authentication bypass Vulnerability
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact Successful exploitation could allow attackers to use shares to cause the system to crash. Impact Level: System
Solution **Solution type:** WillNotFix No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A workaround is to, - Disable null session login. - Remove the share. - Enable passwords on the share.
Affected Software/OS Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT
Vulnerability Insight The flaw is due to an SMB share, allows full access to Guest users. If the Guest account is enabled, anyone can access the computer without a valid user account or password.
Vulnerability Detection Method Details:`Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability` OID:1.3.6.1.4.1.25623.1.0.801991 Version used: `$Revision: 3100 $`

References
`CVE: CVE-1999-0519`
`Other:`
`URL:http://xforce.iss.net/xforce/xfdb/2`
`URL:http://seclab.cs.ucdavis.edu/projects/testing/vulner/38.html`

[return to 172.16.93.132]

Medium 3306/tcp

Medium (CVSS: 6.8)
NVT: MySQL Denial Of Service and Spoofing Vulnerabilities

Product detection result
cpe:/a:mysql:mysql:5.0.51a
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary
The host is running MySQL and is prone to Denial Of Service and Spoofing Vulnerabilities

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

Impact
Successful exploitation could allow users to cause a Denial of Service and man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate. Impact Level: Application

Solution
Upgrade to MySQL version 5.0.88 or 5.1.41 For updates refer to http://dev.mysql.com/downloads

Affected Software/OS
MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 on all running platform.

Vulnerability Insight

Vulnerability Detection Method
Details:MySQL Denial Of Service and Spoofing Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.801064
Version used: $Revision: 3238 $

Product Detection Result
Product: cpe:/a:mysql:mysql:5.0.51a
Method: MySQL/MariaDB Detection
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
CVE: CVE-2009-4019, CVE-2009-4028
Other:
URL:http://bugs.mysql.com/47780
URL:http://bugs.mysql.com/47320
URL:http://marc.info/?l=oss-security&m=125881733826437&w=2
URL:http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html

[return to 172.16.93.132]

Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result
```
The following weak client-to-server encryption algorithms are supported by the r
↪emote service:
aes256-cbc
blowfish-cbc
rijndael-cbc@lysator.liu.se
aes128-cbc
aes192-cbc
arcfour
3des-cbc
cast128-cbc
arcfour128
arcfour256
The following weak server-to-client encryption algorithms are supported by the r
↪emote service:
aes256-cbc
blowfish-cbc
rijndael-cbc@lysator.liu.se
aes128-cbc
aes192-cbc
arcfour
3des-cbc
cast128-cbc
arcfour128
arcfour256
```

Solution
Disable the weak encryption algorithms.

Vulnerability Insight
The ‘arcfour‘ cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The ‘none‘ algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.

. . . continues on next page . . .

... continued from previous page ...

Details:SSH Weak Encryption Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: $Revision: 3160 $

References
Other:
URL:https://tools.ietf.org/html/rfc4253#section-6.3
URL:https://www.kb.cert.org/vuls/id/958563

[return to 172.16.93.132]

Medium 25/tcp

Medium (CVSS: 6.8)
NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

Summary
Multiple vendors' implementations of STARTTLS are prone to a vulnerability that lets attackers inject arbitrary commands.

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

Impact
An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.

Solution
Updates are available.

Affected Software/OS
The following vendors are affected:
Ipswitch Kerio Postfix Qmail-TLS Oracle SCO Group spamdyke ISC

Vulnerability Detection Method
Send a special crafted STARTTLS request and check the response.
Details:Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection ...
OID:1.3.6.1.4.1.25623.1.0.103935
Version used: $Revision: 2780 $

References
CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1575, CVE-2011-1926, CVE-2011-2165

... continues on next page ...

... continued from previous page ...

```
BID:46767
Other:
  URL:http://www.securityfocus.com/bid/46767
   URL:http://kolab.org/pipermail/kolab-announce/2011/000101.html
   URL:http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
   URL:http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
   URL:http://www.kb.cert.org/vuls/id/MAPG-8D9M4P
   URL:http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-
↪notes.txt
   URL:http://www.postfix.org/CVE-2011-0411.html
   URL:http://www.pureftpd.org/project/pure-ftpd/news
   URL:http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNot
↪es_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
   URL:http://www.spamdyke.org/documentation/Changelog.txt
   URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?inclu
↪de_text=1
   URL:http://www.securityfocus.com/archive/1/516901
   URL:http://support.avaya.com/css/P8/documents/100134676
   URL:http://support.avaya.com/css/P8/documents/100141041
   URL:http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
   URL:http://inoa.net/qmail-tls/vu555316.patch
   URL:http://www.kb.cert.org/vuls/id/555316
```

Medium (CVSS: 5.0)
NVT: SSL Certification Expired

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

Vulnerability Detection Result

```
Expired Certificates:
The SSL certificate on the remote service expired on 2010-04-16 14:07:45
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
issued by .: 1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F6
↪3616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of
↪Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outsid
↪e US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint: ED093088706603BFD5DC237399B498DA2D4D31C6
```

Solution

... continues on next page ...

... continued from previous page ...

Replace the SSL certificate by a new one.

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

Vulnerability Detection Method
Details:SSL Certification Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: $Revision: 2937 $

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_DES_192_EDE3_CBC_WITH_MD5
  SSL2_DES_64_CBC_WITH_MD5
  SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
  SSL2_RC2_CBC_128_CBC_WITH_MD5
  SSL2_RC4_128_EXPORT40_WITH_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_RC4_40_MD5
  SSL3_ADH_DES_64_CBC_SHA
  SSL3_ADH_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_64_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_RSA_DES_64_CBC_SHA
  SSL3_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_128_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_RC4_40_MD5
  TLS1_ADH_DES_64_CBC_SHA
  TLS1_ADH_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_64_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

TLS1_RSA_DES_64_CBC_SHA
TLS1_RSA_DES_40_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 ¡ 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: 3061 $

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. Those supported ciphers can be
↪found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

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 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

... continues on next page ...

... continued from previous page ...

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: 2699 $`

References
```
Other:
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
```

[return to 172.16.93.132]

Medium 512/tcp

Medium (CVSS: 5.0)
NVT: Check for rexecd Service

Summary
Rexecd Service is running at this Host. Rexecd (Remote Process Execution) has the same kind of functionality that rsh has : you can execute shell commands on a remote computer.
The main difference is that rexecd authenticate by reading the username and password *unencrypted* from the socket.

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

Solution
Disable rexec Service.

Vulnerability Detection Method
Details:`Check for rexecd Service`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `$Revision: 2244 $`

[return to 172.16.93.132]

Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result
```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-sha1-96
hmac-md5-96
hmac-md5
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-sha1-96
hmac-md5-96
hmac-md5
```

Solution
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details:`SSH Weak MAC Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `$Revision: 3157 $`

[return to 172.16.93.132]

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: 4055421
Paket 2: 4055459
```

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

Solution

. . . continues on next page . . .

. . . continued from previous page . . .

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See 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 172.16.93.132]

Log 1524/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: shell`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 3632/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: distccd`
Log Method Details:`Identify unknown services with nmap` OID:1.3.6.1.4.1.25623.1.0.66286 Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 5432/tcp

Log (CVSS: 0.0) NVT: PostgreSQL Detection
Summary Detection of PostgreSQL, a open source object-relational database system (http://www.postgresql.org). The script sends a connection request to the server (user:postgres, DB:postgres) and attempts to extract the version number from the reply.

Vulnerability Detection Result
`Detected PostgreSQL`
`Version: unknown`
`Location: 5432/tcp`
`CPE: cpe:/a:postgresql:postgresql`
`Concluded from version identification result:`
`Rv`

Log Method Details:`PostgreSQL Detection` OID:1.3.6.1.4.1.25623.1.0.100151 Version used: `$Revision: 2664 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for Postgres
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3210 $`

[return to 172.16.93.132]

Log 3306/tcp

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

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

Vulnerability Detection Result
```
Detected MySQL
Version: 5.0.51a-3ubuntu5
Location: 3306/tcp
CPE: cpe:/a:mysql:mysql:5.0.51a
Concluded from version identification result:
5.0.51a-3ubuntu5     Gu8U%Wds ,ª                5L_zi|TmLolO
```

Log Method
Details:`MySQL/MariaDB Detection`
OID:1.3.6.1.4.1.25623.1.0.100152
Version used: `$Revision: 2611 $`

Log (CVSS: 0.0)
NVT: Services

Summary

. . . continues on next page . . .

... continued from previous page ...

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

Vulnerability Detection Result

```
An unknown service is running on this port.
It is usually reserved for MySQL
```

Log Method

Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3210 $`

Log (CVSS: 0.0)
NVT: Database Open Access Vulnerability

Summary

The host is running a Database server and is prone to information disclosure vulnerability.

Vulnerability Detection Result

```
MySQL can be accessed by remote attackers
```

Impact

Successful exploitation could allow an attacker to obtain the sensitive information of the database.
Impact Level: Application

Affected Software/OS

MySQL IBM DB2 PostgreSQL IBM solidDB Oracle Database Microsoft SQL Server
Workaround: Restrict Database access to remote systems.

Vulnerability Insight

Do not restricting direct access of databases to the remote systems.

Log Method

Details:`Database Open Access Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.902799
Version used: `$Revision: 3060 $`

References

```
Other:
  URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_d
↪ss_v1-2.pdf
```

[return to 172.16.93.132]

Log 22/tcp

Log (CVSS: 0.0)
NVT: SSH Protocol Versions Supported

Summary
Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service.
The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Vulnerability Detection Result
```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
```

Log Method
Details:`SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `$Revision: 2817 $`

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

Summary
This detects the SSH Server's type and version by connecting to the server and processing the buffer received.
This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result
```
Detected SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Remote SSH supported authentication: password,publickey
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:4.7p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

Log Method
Details:`SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `$Revision: 2902 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
`An ssh server is running on this port`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3210 $`

Log (CVSS: 0.0)
NVT: SSH Protocol Algorithms Supported

Summary
This script detects which algorithms and languages are supported by the remote SSH Service

Vulnerability Detection Result
```
The following options are supported by the remote ssh service:
kex_algorithms:
diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-h
↪ellman-group14-sha1,diffie-hellman-group1-sha1
server_host_key_algorithms:
ssh-rsa,ssh-dss
encryption_algorithms_client_to_server:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
encryption_algorithms_server_to_client:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes19
↪2-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
mac_algorithms_client_to_server:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client:
hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com
↪,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server:
none,zlib@openssh.com
compression_algorithms_server_to_client:
none,zlib@openssh.com
```

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details:SSH Protocol Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: $Revision: 2828 $

[return to 172.16.93.132]

Log 445/tcp

Log (CVSS: 0.0)
NVT: Microsoft SMB Signing Disabled

Summary
Checking for SMB signing is disabled.
The script logs in via smb, checks the SMB Negotiate Protocol response to confirm SMB signing is disabled.

Vulnerability Detection Result
SMB signing is disabled on this host

Log Method
Details:Microsoft SMB Signing Disabled
OID:1.3.6.1.4.1.25623.1.0.802726
Version used: $Revision: 2576 $

[return to 172.16.93.132]

Log 25/tcp

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

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

Vulnerability Detection Result
Remote SMTP server banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

Solution
Change the login banner to something generic.

Log Method
Details:SMTP Server type and version

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.10263
Version used: `$Revision: 2599 $`

Log (CVSS: 0.0)
NVT: SMTP STARTTLS Detection

Summary
Check if the remote Mailserver supports the STARTTLS command.

Vulnerability Detection Result
`The remote Mailserver supports the STARTTLS command.`

Log Method
Details:`SMTP STARTTLS Detection`
OID:1.3.6.1.4.1.25623.1.0.103118
Version used: `$Revision: 2558 $`

Log (CVSS: 0.0)
NVT: SSL Certificate - Self-Signed Certificate Detection

Summary
The SSL certificate on this port is self-signed.

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

Log Method
Details:`SSL Certificate - Self-Signed Certificate Detection`
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: `$Revision: 2603 $`

References
```
Other:
  URL:http://en.wikipedia.org/wiki/Self-signed_certificate
```

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
An SMTP server is running on this port
Here is its banner :
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Log Method
Details:Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: $Revision: 3210 $

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

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

Vulnerability Detection Result

```
Detected Postfix
Version: unknown
Location: 25/tcp
CPE: cpe:/a:postfix:postfix
Concluded from version identification result:
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

Log Method
Details:Postfix SMTP Server Detection
OID:1.3.6.1.4.1.25623.1.0.111086
Version used: $Revision: 2598 $

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.
Service does not support TLSv1.1 ciphers.
Service does not support TLSv1.2 ciphers.
Medium ciphers offered by this service:
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_ADH_WITH_AES_128_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
```

... continues on next page ...

... continued from previous page ...

```
  SSL3_ADH_DES_192_CBC_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_ADH_WITH_AES_128_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_RSA_WITH_AES_128_SHA
  TLS1_ADH_DES_192_CBC_SHA
Weak ciphers offered by this service:
  SSL2_RC4_128_MD5
  SSL2_DES_192_EDE3_CBC_WITH_MD5
  SSL2_DES_64_CBC_WITH_MD5
  SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
  SSL2_RC2_CBC_128_CBC_WITH_MD5
  SSL2_RC4_128_EXPORT40_WITH_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_RC4_40_MD5
  SSL3_ADH_DES_64_CBC_SHA
  SSL3_ADH_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_64_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_RSA_DES_64_CBC_SHA
  SSL3_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_128_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_RC4_40_MD5
  TLS1_ADH_DES_64_CBC_SHA
  TLS1_ADH_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_64_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_RSA_DES_64_CBC_SHA
  TLS1_RSA_DES_40_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: 2827 $`

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_EDH_RSA_DES_192_CBC3_SHA
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_ADH_WITH_AES_128_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_DES_192_CBC_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_ADH_WITH_AES_128_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_RSA_WITH_AES_128_SHA
  TLS1_ADH_DES_192_CBC_SHA
```

Log Method
Details:`Check for SSL Medium Ciphers`
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: `$Revision: 3060 $`

[return to 172.16.93.132]

Log general/tcp

Log (CVSS: 0.0)
NVT: SSH OS Identification

Summary
This script performs SSH based OS detection.

Vulnerability Detection Result

```
Detected OS: Ubuntu
Version: 8.04
CPE: cpe:/o:canonical:ubuntu_linux:8.04
Concluded from SSH banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Log Method
Details:`SSH OS Identification`
OID:1.3.6.1.4.1.25623.1.0.105586
Version used: `$Revision: 2927 $`

Log (CVSS: 0.0)
NVT: OS Detection

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.

Vulnerability Detection Result
```
Best matching OS:
cpe:/o:canonical:ubuntu_linux:8.04
Found by NVT 1.3.6.1.4.1.25623.1.0.105586 (Ubuntu 8.04)
Other OS detections (in order of reliability):
OS: cpe:/o:canonical:ubuntu_linux found by 1.3.6.1.4.1.25623.1.0.10267 (SSH Serv
↪er type and version)
OS: cpe:/o:linux:kernel found by 1.3.6.1.4.1.25623.1.0.111068 (Linux)
OS: cpe:/o:linux:kernel found by 1.3.6.1.4.1.25623.1.0.102002 (Detects remote op
↪erating system version)
```

Log Method
Details:`OS Detection`
OID:1.3.6.1.4.1.25623.1.0.105937
Version used: `$Revision: 2709 $`

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
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: 3117 $`

. . . continues on next page . . .

. . . continued from previous page . . .

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 172.16.93.131 to 172.16.93.132:
172.16.93.131
172.16.93.132
```

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: 2837 $`

[return to 172.16.93.132]

Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

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

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

Log Method
Details:`ICMP Timestamp Detection`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `$Revision: 3115 $`

References

. . . continues on next page . . .

... continued from previous page ...

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

[return to 172.16.93.132]

Log general/SMBClient

Log (CVSS: 0.0)
NVT: SMB Test

Summary
Test remote host SMB Functions

Vulnerability Detection Result
`Error getting SMB-Data -> PROTOCOL NEGOTIATION FAILED: NT_STATUS_IO_TIMEOUT`

Log Method
Details:`SMB Test`
OID:1.3.6.1.4.1.25623.1.0.90011
Version used: `$Revision: 2251 $`

[return to 172.16.93.132]

Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result

```
172.16.93.132|cpe:/a:mysql:mysql:5.0.51a
172.16.93.132|cpe:/a:postfix:postfix
172.16.93.132|cpe:/a:postgresql:postgresql
172.16.93.132|cpe:/a:openbsd:openssh:4.7p1
172.16.93.132|cpe:/o:canonical:ubuntu_linux:8.04
```

Log Method
Details:`CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 2837 $`

[return to 172.16.93.132]

Log 8787/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: drb`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 8009/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: ajp13`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

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:
http://172.16.93.132:80/
```

Log Method
Details:`DIRB (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: `$Revision: 3117 $`

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for HTTP
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3210 $`

Log (CVSS: 0.0)
NVT: No 404 check

Summary
Remote web server does not reply with 404 error code.

Vulnerability Detection Result
```
The remote web server is very slow - it took 76 seconds to
execute the plugin no404.nasl (it usually only takes a few seconds).
In order to keep the scan total time to a reasonable amount, the remote web serv
↪er
has not been tested.
If you want to test the remote server, either fix it to have it reply to OpenVAS
↪'s requests
```

...continues on next page ...

... continued from previous page ...

```
in a reasonable amount of time, or set the global option 'Thorough tests' to 'ye
↪s'
```

Vulnerability Insight
This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map, search page or authentication page instead.
OpenVAS enabled some counter measures for that, however they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate

Log Method
Details:`No 404 check`
OID:1.3.6.1.4.1.25623.1.0.10386
Version used: `$Revision: 2837 $`

Log (CVSS: 0.0)
NVT: Directory Scanner

Summary
This plugin attempts to determine the presence of various common dirs on the remote web server

Vulnerability Detection Result

```
The following directories were discovered:
/cgi-bin, /test
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

Log Method
Details:`Directory Scanner`
OID:1.3.6.1.4.1.25623.1.0.11032
Version used: `$Revision: 2837 $`

References

```
Other:
  OWASP:OWASP-CM-006
```

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

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

... continues on next page ...

. . . continued from previous page . . .

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.93.132
+ Target Hostname:    172.16.93.132
+ Target Port:        80
+ Start Time:         2016-05-22 17:38:13 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ 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
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apach
↪e 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
↪asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59
↪d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
↪se positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
↪ST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the ph
↪pinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potential
↪ly sensitive information via certain HTTP requests that contain specific QUERY
↪ strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databa
↪ses, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, i
↪node: 92462, size: 40540, mtime: Tue Dec  9 17:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases,
↪ and should be protected or limited to authorized hosts.
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpin
↪fo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output fr
↪om the phpinfo() function was found.
+ /phpinfo.php?cx[]=VgPnAPp2XgUqtHRE7czwSiUKCTxjhN8vkLFBfDB8tKwVderJPUM2ts6VodEU
↪0fVG2zY6AlX6wK5QqPyGkwGZbFqc4xwivCsth5jaaV54chNKw2OYSdcK18N52j43OzMIv8YlpxI8fJ
↪BTxkyTyqFlKIHzQoCzPqx6ZrVFOMcXPQJbYIr6ll9qJnlCfB3FCJwTTfQaZuZ5ugWE8exuT3UuVpXL
↪OpRWuvWMo8VdfqvRShZSwhrnEXTsuRVbjKAmg10Et9Aj0GV9IYSQIPVQRNzNCNUiLItFoomyKRSCvP
↪uqiuiQizIvSWuBZJOCizsMkzHySW8UBNAYqWQMfQKtjhrvhRL5wy7aDcnK3C0kMBneUiswuAxFuoep
↪tvVUSZggqP7a6ALudEjfhQDDJY0mKo098qlwnmlJu7CRzT9v433sgMKdB9u28SmTudBnootRJfwTBe
↪qbPnmnpgk11B7tOJNsAzwJNinHpk0yDaTmUwkItFlKQHvjUX5t2NE995NuDbSiSQGegWFs0hsFRNHz
↪4hXk11QchP2HxWl6LzZPl0ldy9fjRvnMAVH7QKCMTbMoQ64u4WBGUN3DeoswdAxb094bH2vAyI4hbm
↪9VZNWnjVl7PLfDzYflpP6O13lgHAFUzYgUWJ9rBTswixkYQoTWhSgt1ksK14xKNQIsnoY75jGbKHgo
↪sfzZQJtbRiJaWiAl02Gf7pArLRDXQuxl2RY6eGwtWsN2oTEe4gocU68c61XBLeSNY9gpQdgrV3O3DV
↪NbaCuHsJkcPtX3uteILJFiJbioKewYADGYgfe9zEHoYpzbEs9vaeYW88mzrBYhYvoBLo1pQQVrUoun
↪KXFUXcDC2fizYylVZbgZUmIkABOYLboEWhGPHbSKTCBIPLyN3za7xMdf4klfE6pv7OQL2mrRd6C8Ds
↪VfLZPNzNSD5DoLuoLmFET1Ypm9CnoUy3Cp3mEBJDhG1yu6q5wMpGuCKVa2wL2JHkczAvoB64DXUXgC
↪XQH7lZzYBXlkk9NUh7WfnrynRcG4ddXyImcepwbadg7fhEDAOtaoyPwxTahuDZzVLHokc0H73AveRt
↪Bs5lpmkrmMDdi8rd5OMaoXFrNlgCNANszMdQFRjDxjAJnnYjptzeVjFzvxC82KzLSFdOoJO68PhsTD
↪GDeOxR2uEVdJXCeyGjfRO9BPxl4YRMOugUIFAYe362JoBap4drFGMnGtpBK91jMnnbcrLfCE63cXqY
↪qtk8zzD1ndBuN2Fl4CpzsJt5kXKDcuJRBn1ATDU7raI29fPLLnQDa0rW2vCbByUy8lJixWwCvvotkO
↪sFQHOxXrdPL11iEhR2oLdzDM5WxGOj0RnzorZLyWr8IAvJMS6xRSpt9A6nzEDnBWYnPuPBzYxxpeWv
↪JWQC4ku9vWLz1141yJkHhKdlnSpvVsVnhtDX7ILNoc11j2bdfhXaOog8CVlCm9SEmJRdfG1Jtb9zZy
↪hULBQZVVGuNMXvpqekMyZtW3wgBrBR9RKioWnwXxeDuMwScQxsfJHY4vxLIIlRxqOhGii5BeJhLx2M
↪czxXbKuhCjxj7SxjJENTADKMqbco2sYarWbEFCvItvMDQ5Fh6ihSYihCwZzrczAPKVDFa6BpHgLK1o
↪VDT7Ld9fPu7bosecUej392zVJkWB1DqCdyZchSTmREjofB6Xr4g54VNqydijAReEm0ReptxFmUNZeM
↪4FlHEoxGRjjlkg4aE2MmaNoamx3lInQsfxu0iStJrI58wVgQUWxMAswnbSlPqDhIIhTuaEbmUk5NWd
↪lkeqRQgNBUhjCUvVVrMu5DBme7WZwChyHnYaS0spPMpghDE8hHQUOqX7Xkreso3kgBKo2aTFGnd70J
↪Hrdtm2Hgf9i47h8shxwwWfxbcAayIdSCF1tdpCgZ83bjt6oRmNXUXuzr9t7Se0DSXBB5oqOmVPhzlR
↪CcgugR1zzlZwUPgXSwmi9VnTOuSlmEKkzw0u0TCUdTse5aZCmJnchKva3RAKRYwQXWwLWVuNueYZBj
↪zycmsnxb1ThkEjcT9bNfEHKknlneycNT8lfUjqemqvEAj2kFiTuiFgIKcZRXPFX5AnjpezOIeaHEBU
↪RqCGJtQWxO0ellNDVrXRzvDlVdSc2VjPxOnd9GBt4OqOnEIUWmOzQDjDsyaoC8p6lw8RMEFesCQ8Y8
↪GJAX6L2razgTVtLSpLSylV8JOIV90a1xqMdLVUt8DzQfaCF79oju3ZjRDn99wsuJFNcFTxjdohLIud
↪HcvKJitsB8QIcLDSxeOqOIpT01UL2hVvfSxP2eDl5ALH0eVhzR9FUkvLKLkq4i6ylRxW5lXmNx5nAb
↪pS8dqA66A4Po4jSNQ3Giu2BWR3UZ1Wy4oEIsPt29HClKOaziWxAOw3hKjnnQJOArLpuFrrS8RDrKbG
↪ixElnBICt2tfD6Vo3i9TPFatXHGu5QSEoA55xUTLgo7CSH3CGaqzVrQGOCdcorrpV2oKpzMP8tirgA
↪qjnm3n2Sdi6k70nytWBu1jF69xQpO9EfYoXWRbUjML8gUVnywnS4ubiKjl5aM9rx1DdUymNcErezCd
↪N3neDorWiZEEjE2IO3GyOZMNIDgzyrwQAV8ZRmaS17sw9HMR7CaLrGQde63P02i04qsl2zi3anMjjH
↪UMCsMlWO0WtX46p0aqosQSuv73kVCERlD5uqSPFooQKfrQNpBSo11qnfY6nqclYRNL1Xq8FkyNj8UE
↪5wXp9GbJO9k9dGqGfisPb5B5f6CkPK4uIMwPQeAXsTT8wGxLfxdDq3VWnkZQRBP4IILSnwTlfvlcKE
↪W2N7I9F9qumCOS8tsRQ6QDclMTKQgf9GbUrRZAM8qboZV2VQSj20eC4rv0wZxk4jaJGsX70JkJolrZ
↪VLDKU3QcSLxd754mjArCexI3XPWNPQX1wg0iEz0DnEe28bQIFeLOg3YVGNVgBftQwgLFX47mbpzCNn
↪nbzaNMCWo5apDq07GJ34eUlqa3sIVJN2BGWaYUO0OiTThNW7c2daRZtAIOTqZuusSs5Zz0lppLUBiY
```

. . . continues on next page . . .

... continued from previous page ...

```
↪T248KJ5oQQ29ylvnnjI0UpVbu8j7UT4Vi3btnuQrCDvfS8m5XLyq3WNJxZDYVx3sPy1kpieOG2aIts
↪rASh6Aml2ozO1jOgW3OhmwMRQGPCJTc9N3z8QClRfqv8Wtz0tVF9bQpmmZm5wB4vBYREeiZhMhUU80
↪nfauw8Ct9iGozkXdjPq9oXNLpAO1STN7mWKRR268QXprN51xfXjVUM640ADfJ0SWiEuXgitb4pKkne
↪9Mx17bjsD5q56OVhgpMddC8wsq0TVO1xfiZdIHz8ogVYjayTa3ADibMiXZOOWPd31zRTpdtfyJIWkk
↪dM8eky8eazKLbeLj15sULyhOiZNhy6gxsgupkPVLbkXWKL1vUzGmVcF53cGAn8lCsjmQQOEtCP2fu8
↪YEWkOkawCBUiIrgslRwKXkvHpsvdw8S3792xrsdDx77tpaeU1MzfIg3v57mD6GdOX0y5SdKrD64073
↪zmQhB6wPicfsDGGuF9wVX92EFAI4USRWU0QI5QLCouqt4rIhcQTrQKj1cdK6cqKPRnFqiGCbpCA6qP
↪pyeBHR2rRqh2KkenGKkaL5IK134Z4aVuhMyGpj0ZVlDpuuqUrssPPybaXQRHBO8YHNJJDriaFmdInr
↪c05yhOiAfVnEmRS9CCBHIrqgvBUvizlR2TPrSJaVgAuCOY7cYycW6sjF5LqV0zQN7Q7um2RrCKIM80
↪l3Ft1TyVr9ENfioINqZYdhlNmsKuQ2Sttu7uNFOuv7gInm3qIDNp6ZaLpcilYwMfbERPImTROp8szd
↪ddGXIsILDL4w0rKXpuFcJAByWKSsm3uTnVGaRcxlCgdER9bw7a2D6fkhcuvDZU3CwLEghZEC16tbOL
↪UyiKLZooddCXbac8ZfEISbAu0qFN29SQZWPtxHm0KkBgYmNQHs8O9LCwclAGZrNw3jSNsUL96LuAPm
↪IJhekRhEKsuFbGq60qfMVrsPV9bd3Vi92qOZRYlh9wjmM0c1eHeA4z1Hr4lrGZH6Sf0RjvkMRuWh6p
↪lFmv4kDCiJXUAsMOESOIMUzVu9DpOj8r95XIj5Tgoy5QABLN9L9ltnyT0a<script>alert(foo)</
↪script>: Output from the phpinfo() function was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL d
↪atabases, and should be protected or limited to authorized hosts.
+ 8347 requests: 0 error(s) and 29 item(s) reported on remote host
+ End Time:           2016-05-22 17:39:06 (GMT0) (53 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: 2837 $`

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)`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.80110
Version used: `$Revision: 3207 $`

[return to 172.16.93.132]

Log 6667/tcp

Log (CVSS: 0.0)
NVT: Check for Telnet Server

Summary
A telnet Server is running at this host.
Experts in computer security, such as SANS Institute, and the members of the comp.os.linux.security newsgroup recommend that the use of Telnet for remote logins should be discontinued under all normal circumstances, for the following reasons:
Telnet, by default, does not encrypt any data sent over the connection (including passwords), and so it is often practical to eavesdrop on the communications and use the password later for malicious purposes anybody who has access to a router, switch, hub or gateway located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login and password information (and whatever else is typed) with any of several common utilities like tcpdump and Wireshark.
Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle.
Commonly used Telnet daemons have several vulnerabilities discovered over the years.

Vulnerability Detection Result
`A telnet server seems to be running on this port`

Log Method
Details:`Check for Telnet Server`
OID:1.3.6.1.4.1.25623.1.0.100074
Version used: `$Revision: 2837 $`

Log (CVSS: 0.0)
NVT: Detect Server type and version via Telnet

Summary
This detects the Telnet Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Vulnerability Detection Result
```
Remote telnet banner :
ERROR :Closing Link: [172.16.93.131] (Throttled: Reconnecting too fast) -Email a
↪dmin@Metasploitable.LAN for more information.
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution
Change the login banner to something generic.

Log Method
Details:`Detect Server type and version via Telnet`
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: `$Revision: 2837 $`

[return to 172.16.93.132]

Log 5900/tcp

Log (CVSS: 0.0)
NVT: VNC security types

Summary
This script checks the remote VNC protocol version and the available 'security types'.

Vulnerability Detection Result
`The remote VNC server chose security type #2 (VNC authentication)`

Log Method
Details:`VNC security types`
OID:1.3.6.1.4.1.25623.1.0.19288
Version used: `$Revision: 1318 $`

[return to 172.16.93.132]

Log 514/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: tcpwrapped`

Log Method

. . . continues on next page . . .

... continued from previous page ...

Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 513/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: login
This is a guess. A confident identification of the service was not possible.
```

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 23/tcp

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for Telnet
```

Log Method
Details:`Services`

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3210 $`

[return to 172.16.93.132]

Log 2121/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: ftp`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 21/tcp

Log (CVSS: 0.0)
NVT: Services

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

Vulnerability Detection Result
```
An unknown service is running on this port.
It is usually reserved for FTP
```

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3210 $`

[return to 172.16.93.132]

Log 2049/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: nfs`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 111/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: rpcbind`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]

Log 1099/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: rmiregistry`

Log Method
Details:`Identify unknown services with nmap`
OID:1.3.6.1.4.1.25623.1.0.66286
Version used: `$Revision: 2752 $`

[return to 172.16.93.132]