X3rror

IOT & Security Sol's

Security Assessment Finding Report

Business Confidential

Scan Report

August 11, 2020

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 "openvas$_l$ib$_s$can$_1$72.162.217.137$_k$cVCaFuH0 36 : 152020$UTCandendedat.Thereportfirstsummarisestheresultsfound.Then, foreachhost, thereportdescribeseveryissuefo$

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
172.162.217.137	22	33	2	85	0
Total: 1	22	33	2	85	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "High" are not shown.
Issues with the threat level "Medium" are not shown.
Issues with the threat level "Low" are not shown.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 142 results selected by the filtering described above. Before filtering there were 408 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
172.162.217.137	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 172.162.217.137

Host scan start
Host scan end

Service (Port)	Threat Level
1524/tcp	High
512/tcp	High
general/tcp	High
80/tcp	High
8009/tcp	High
5432/tcp	High
514/tcp	High

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
6667/tcp	High
22/tcp	High
6200/tcp	High
21/tcp	High
3306/tcp	High
8787/tcp	High
3632/tcp	High
5900/tcp	High
1099/tcp	High
513/tcp	High
80/tcp	Medium
5432/tcp	Medium
445/tcp	Medium
6667/tcp	Medium
22/tcp	Medium
21/tcp	Medium
23/tcp	Medium
25/tcp	Medium
5900/tcp	Medium
2121/tcp	Medium
general/tcp	Low
22/tcp	Low
1524/tcp	Log
512/tcp	Log
general/icmp	Log
general/tcp	Log
80/tcp	Log
8009/tcp	Log
5432/tcp	Log
445/tcp	Log
514/tcp	Log
6667/tcp	Log
22/tcp	Log
general/CPE-T	Log
21/tcp	Log
53/tcp	Log
23/tcp	Log
25/tcp	Log
3306/tcp	Log
8787/tcp	Log
3632/tcp	Log
5900/tcp	Log
139/tcp	Log
1099/tcp	Log

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
2121/tcp	Log
111/tcp	Log
6000/tcp	Log
513/tcp	Log

2.1.1 High 1524/tcp

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

Summary
A backdoor is installed on the remote host.

Vulnerability Detection Result
`The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)`

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution
Solution type: Workaround
A whole cleanup of the infected system is recommended.

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `2020-03-21T13:23:23+0000`

[return to 172.162.217.137]

2.1.2 High 512/tcp

High (CVSS: 10.0)
NVT: rexec Passwordless / Unencrypted Cleartext Login

Summary
This remote host is running a rexec service.

Vulnerability Detection Result
`The rexec service is not allowing connections from this host.`

... continues on next page ...

... continued from previous page ...

Solution
Solution type: Mitigation
Disable the rexec service and use alternatives like SSH instead.

Vulnerability Insight
rexec (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 rexec authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Method
Details: `rexec Passwordless / Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `$Revision: 13541 $`

References
```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0618
```

[return to 172.162.217.137]

2.1.3 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

Product detection result
```
cpe:/o:canonical:ubuntu_linux:8.04
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary
OS End Of Life Detection.
The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
```
The "Ubuntu" Operating System on the remote host has reached the end of life.
CPE:                cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP:        8.04
EOL date:           2013-05-09
EOL info:           https://wiki.ubuntu.com/Releases
```

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Upgrade the Operating System on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method
Details: `OS End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: `2019-10-21T09:55:06+0000`

Product Detection Result
Product: `cpe:/o:canonical:ubuntu_linux:8.04`
Method: `OS Detection Consolidation and Reporting`
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 172.162.217.137]

2.1.4 High 80/tcp

High (CVSS: 7.5)
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.

Summary
PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result
`Vulnerable url: http://172.162.217.137/cgi-bin/php`

Impact
Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.

Solution
Solution type: VendorFix
PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight
When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.
An example of the -s command, allowing an attacker to view the source code of index.php is below:
http://example.com/index.php?-s

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: PHP-CGI-based setups vulnerability when parsing query string parameters from ph.
↪..
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: 2019-11-08T10:10:55+0000

References
CVE: CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:53388
Other:
URL:http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-r
↪isks-Update-1567532.html
URL:http://www.kb.cert.org/vuls/id/520827
URL:http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
URL:https://bugs.php.net/bug.php?id=61910
URL:http://www.php.net/manual/en/security.cgi-bin.php
URL:http://www.securityfocus.com/bid/53388

High (CVSS: 7.5)
NVT: phpinfo() output Reporting

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Result
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://172.162.217.137/mutillidae/phpinfo.php
http://172.162.217.137/phpinfo.php

Impact
Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Solution
Solution type: Workaround
Delete the listed files or restrict access to them.

Vulnerability Detection Method
Details: phpinfo() output Reporting
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: $Revision: 11992 $

High (CVSS: 7.5)
NVT: Test HTTP dangerous methods

Summary
Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.
This script checks if they are enabled and can be misused to upload or delete files.

Vulnerability Detection Result
`We could upload the following files via the PUT method at this web server:`
`http://172.162.217.137/dav/puttest1762786016.html`
`We could delete the following files via the DELETE method at this web server:`
`http://172.162.217.137/dav/puttest1762786016.html`

Impact
- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.
- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution
Solution type: Mitigation
Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method
Details: `Test HTTP dangerous methods`
OID:1.3.6.1.4.1.25623.1.0.10498
Version used: `2019-12-04T13:23:25+0000`

References
`BID:12141`
`Other:`
`OWASP:OWASP-CM-001`

High (CVSS: 10.0)
NVT: TWiki XSS and Command Execution Vulnerabilities

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`
`Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)`

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result
. . . continues on next page . . .

... continued from previous page ...

Installed version: 01.Feb.2003
Fixed version: 4.2.4

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution
Solution type: VendorFix
Upgrade to version 4.2.4 or later.

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight
The flaws are due to,
- %URLPARAM}}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH}}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: TWiki XSS and Command Execution Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.800320
Version used: $Revision: 12952 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2008-5304, CVE-2008-5305
BID:32668, 32669
Other:
URL:http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
URL:http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

[return to 172.162.217.137]

2.1.5 High 8009/tcp

High (CVSS: 7.5)
NVT: Apache JServ Protocol (AJP) Public WAN (Internet) Accessible

Summary
The script checks if the target host is running a service supporting the Apache JServ Protocol (AJP) accessible from a public WAN (Internet).

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

Solution
Solution type: Mitigation
Only allow access to the AJP service from trusted sources / networks.

Vulnerability Insight
When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising (e.g. bypassing security checks, bypassing user authentication among others).

Vulnerability Detection Method
Evaluate if the target host is running a service supporting the Apache JServ Protocol (AJP) accessible from a public WAN (Internet).
Details: `Apache JServ Protocol (AJP) Public WAN (Internet) Accessible`
OID:1.3.6.1.4.1.25623.1.0.108716
Version used: `2020-03-02T11:38:26+0000`

References
```
Other:
  URL:https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff
↪1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
```

High (CVSS: 7.5)
NVT: Apache Tomcat AJP RCE Vulnerability (Ghostcat)

Summary
Apache Tomcat is prone to a remote code execution vulnerability in the AJP connector dubbed 'Ghostcat'.

Vulnerability Detection Result
```
It was possible to read the file "/WEB-INF/web.xml" through the ajp13 connector.
Result:
AB 8  È  OK     Content-Type   text/html;charset=ISO-8859-1 AB ü  ø<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
```

... continues on next page ...

... continued from previous page ...

```
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at
      http://www.apache.org/licenses/LICENSE-2.0
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
   "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
    <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
    /*<![CDATA[*/
      body {
          color: #000000;
          background-color: #FFFFFF;
   font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
      }
    img {
       border: none;
    }

    a:link, a:visited {
        color: blue
    }
    th {
        font-family: Verdana, "Times New Roman", Times, serif;
        font-size: 110%;
        font-weight: normal;
        font-style: italic;
        background: #D2A41C;
        text-align: left;
    }
    td {
        color: #000000;
 font-family: Arial, Helvetica, sans-serif;
    }

    td.menu {
        background: #FFDC75;
    }
```

... continues on next page ...

. . . continued from previous page . . .

```
    .center {
        text-align: center;
    }
    .code {
        color: #000000;
        font-family: "Courier New", Courier, monospace;
        font-size: 110%;
        margin-left: 2.5em;
    }

     #banner {
        margin-bottom: 12px;
     }
     p#congrats {
         margin-top: 0;
         font-weight: bold;
         text-align: center;
     }
     p#footer {
         text-align: right;
         font-size: 80%;
     }
     /*]]>*/
   </style>
</head>
<body>
<!-- Header -->
<table id="banner" width="100%">
    <tr>
      <td align="left" style="width:130px">
        <a href="http://tomcat.apache.org/">
   <img src="tomcat.gif" height="92" width="130" alt="The Mighty Tomcat - MEOW!"
↪/>
 </a>
      </td>
      <td align="left" valign="top"><b>Apache Tomcat/5.5</b></td>
      <td align="right">
        <a href="http://www.apache.org/">
   <img src="asf-logo-wide.gif" height="51" width="537" alt="The Apache Software
↪ Foundation"/>
 </a>
       </td>
     </tr>
</table>
<table>
    <tr>
        <!-- Table of Contents -->
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
        <td valign="top">
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
    <th>Administration</th>
                </tr>
                <tr>
    <td class="menu">
      <a href="manager/status">Status</a><br/>
                    <a href="admin">Tomcat Administration</a><br/>
                    <a href="manager/html">Tomcat Manager</a><br/>
                     
                  </td>
                </tr>
            </table>
     <br />
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
    <th>Documentation</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="RELEASE-NOTES.txt">Release Notes</a><br/>
                    <a href="tomcat-docs/changelog.html">Change Log</a><br/
↪>
                    <a href="tomcat-docs">Tomcat Documentation</a><br/>
↪                      
                     
      </td>
                </tr>
            </table>

            <br/>
            <table width="100%" border="1" cellspacing="0" cellpadding="3">
                <tr>
                  <th>Tomcat Online</th>
                </tr>
                <tr>
                  <td class="menu">
                    <a href="http://tomcat.apache.org/">Home Page</a><br/>
      <a href="http://tomcat.apache.org/faq/">FAQ</a><br/>
                    <a href="http://tomcat.apache.org/bugreport.html">Bug D
↪atabase</a><br/>
                    <a href="http://issues.apache.org/bugzilla/buglist.cgi?bug_s
↪tatus=UNCONFIRMED&amp;bug_status=NEW&amp;bug_status=ASSIGNED&amp;bug_status=RE
↪OPENED&amp;bug_status=RESOLVED&amp;resolution=LATER&amp;resolution=REMIND&amp;
↪resolution=---&amp;bugidtype=include&amp;product=Tomcat+5&amp;cmdtype=doit&amp
↪;order=Importance">Open Bugs</a><br/>
```

. . . continues on next page . . .

... continued from previous page ...

```
                    <a href="http://mail-archives.apache.org/mod_mbox/tomcat-use
↪rs/">Users Mailing List</a><br/>
                    <a href="http://mail-archives.apache.org/mod_mbox/tomcat-dev
↪/">Developers Mailing List</a><br/>
                    <a href="irc://irc.freenode.net/#tomcat">IRC</a><br/>
       
                  </td>
                </tr>
              </table>

              <br/>
              <table width="100%" border="1" cellspacing="0" cellpadding="3">
                  <tr>
                    <th>Examples</th>
                  </tr>
                  <tr>
                    <td class="menu">
                      <a href="jsp-examples/">JSP Examples</a><br/>
                      <a href="servlets-examples/">Servlet Examples</a><br/>
                      <a href="webdav/">WebDAV capabilities</a><br/>
             
                    </td>
                  </tr>
              </table>

              <br/>
              <table width="100%" border="1" cellspacing="0" cellpadding="3">
                  <tr>
    <th>Miscellaneous</th>
                  </tr>
                  <tr>
                    <td class="menu">
                      <a href="http://java.sun.com/products/jsp">Sun's Java&n
↪bsp;Server Pages Site</a><br/>
                    <a href="http://java.sun.com/products/servlet">Sun's Se
↪rvlet Site</a><br/>
           
                    </td>
                  </tr>
              </table>
        </td>
        <td style="width:20px"> </td>

        <!-- Body -->
        <td align="left" valign="top">
          <p id="congrats">If you're seeing this page via a web browser, it mean
↪s you've setup Tomcat successfully. Congratulations!</p>
```

... continues on next page ...

... continued from previous page ...

```
          <p>As you may have guessed by now, this is the default Tomcat home pag
↪e. It can be found on the local filesystem at:</p>
          <p class="code">$CATALINA_HOME/webapps/ROOT/index.jsp</p>

          <p>where "$CATALINA_HOME" is the root of the Tomcat installation direc
↪tory. If you're seeing this page, and you don't think you should be, then eith
↪er you're either a user who has arrived at new installation of Tomcat, or you'
↪re an administrator who hasn't got his/her setup quite right. Providing the la
↪tter is the case, please refer to the <a href="tomcat-docs">Tomcat Documentati
↪on</a> for more detailed setup and administration information than is found in
↪ the INSTALL file.</p>
            <p><b>NOTE:</b> This page is precompiled. If you change it, this pag
↪e will not change since
                  it was compiled into a servlet at build time.
                  (See <tt>$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml</tt> as t
↪o how it was mapped.)
            </p>
            <p><b>NOTE: For security reasons, using the administration webapp
            is restricted to users with role "admin". The manager webapp
            is restricted to users with role "manager".</b>
            Users are defined in <code>$CATALINA_HOME/conf/tomcat-users.xml</cod
↪e>.</p>
            <p>Included with this release are a host of sample Servlets and JSPs
↪ (with associated source code), extensive documentation (including the Servlet
↪ 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web app
↪lications.</p>
            <p>Tomcat mailing lists are available at the Tomcat project web site
↪:</p>
           <ul>
               <li><b><a href="mailto:users@tomcat.apache.org">users@tomc
```

Solution
Solution type: VendorFix
Update to version 7.0.100, 8.5.51, 9.0.31 or later.

Affected Software/OS
Apache Tomcat versions prior 7.0.100, 8.5.51 or 9.0.31 when the AJP connector is enabled.

Vulnerability Insight
Apache Tomcat server has a file containing vulnerability, which can be used by an attacker to read or include any files in all webapp directories on Tomcat, such as webapp configuration files or source code.

Vulnerability Detection Method
Sends a crafted AJP13 request and checks the response.
Details: `Apache Tomcat AJP RCE Vulnerability (Ghostcat)`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.143545
Version used: 2020-03-25T03:34:54+0000

References
CVE: CVE-2020-1938
Other:
URL:https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E
URL:https://www.chaitin.cn/en/ghostcat
URL:https://www.cnvd.org.cn/flaw/show/CNVD-2020-10487
URL:https://github.com/YDHCUI/CNVD-2020-10487-Tomcat-Ajp-lfi
URL:https://tomcat.apache.org/tomcat-7.0-doc/changelog.html
URL:https://tomcat.apache.org/tomcat-8.5-doc/changelog.html
URL:https://tomcat.apache.org/tomcat-9.0-doc/changelog.html

[return to 172.162.217.137]

2.1.6 High 5432/tcp

High (CVSS: 9.0)
NVT: PostgreSQL weak password

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

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
Solution type: Mitigation
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: 2020-01-28T13:26:39+0000

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

[return to 172.162.217.137]

2.1.7 High 514/tcp

High (CVSS: 7.5)
NVT: rsh Unencrypted Cleartext Login

Summary
This remote host is running a rsh service.

Vulnerability Detection Result
`The rsh service currently has issues with name resolution and is not allowing co`
`↪nnections from this host.`

Solution
Solution type: Mitigation
Disable the rsh service and use alternatives like SSH instead.

Vulnerability Insight
rsh (remote shell) is a command line computer program which can execute shell commands as another user, and on another computer across a computer network.

Vulnerability Detection Method
Details: `rsh Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.100080
Version used: `$Revision: 13010 $`

References
`Other:`
`URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651`

[return to 172.162.217.137]

2.1.8 High 6667/tcp

High (CVSS: 7.5)
NVT: Check for Backdoor in UnrealIRCd

Summary
Detection of backdoor in UnrealIRCd.

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

Solution

. . . continues on next page . . .

... continued from previous page ...

Solution type: VendorFix
Install latest version of unrealircd and check signatures of software you're installing.

Vulnerability Insight
Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.
The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Vulnerability Detection Method
Details: `Check for Backdoor in UnrealIRCd`
OID:1.3.6.1.4.1.25623.1.0.80111
Version used: `$Revision: 13960 $`

References
`CVE: CVE-2010-2075`
`BID:40820`
`Other:`
`URL:http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt`
`URL:http://seclists.org/fulldisclosure/2010/Jun/277`
`URL:http://www.securityfocus.com/bid/40820`

[return to 172.162.217.137]

2.1.9 High 22/tcp

High (CVSS: 7.5)
NVT: SSH Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote SSH server using default credentials.
As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

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

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013).
Details: `SSH Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.103239
Version used: `2020-03-26T13:48:10+0000`

[return to 172.162.217.137]

2.1.10 High 6200/tcp

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution
Solution type: VendorFix
The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 12076 $`

References
```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
```

... continues on next page ...

... continued from previous page ...

URL:https://security.appspot.com/vsftpd.html

[return to 172.162.217.137]

2.1.11 High 21/tcp

High (CVSS: 7.5)
NVT: FTP Brute Force Logins Reporting

Summary
It was possible to login into the remote FTP server using weak/known credentials.
As the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

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

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Reports weak/known credentials detected by the VT 'FTP Brute Force Logins' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: FTP Brute Force Logins Reporting
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: 2020-03-24T12:27:11+0000

High (CVSS: 7.5)
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

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

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method
Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `$Revision: 12076 $`

References
```
BID:48539
Other:
  URL:http://www.securityfocus.com/bid/48539
   URL:http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
↪doored.html
   URL:https://security.appspot.com/vsftpd.html
```

[return to 172.162.217.137]

2.1.12 High 3306/tcp

High (CVSS: 9.0)
NVT: MySQL / MariaDB weak password

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
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
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Details: `MySQL / MariaDB weak password`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.103551
Version used: 2020-04-01T10:41:43+0000

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)

[return to 172.162.217.137]

2.1.13 High 8787/tcp

High (CVSS: 10.0)
NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities

Summary
Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Vulnerability Detection Result
```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice returned the following response:
Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/
↪ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__se
↪nd__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/
↪ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `m
↪ain_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/
↪drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr
↪/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:143
↪0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
↪r/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in
↪`start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not im
↪plemented
```

Impact
By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:
- Implementing taint on untrusted input
- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)
- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method
Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.
Details: `Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: `$Revision: 12338 $`

References
```
BID:47071
Other:
  URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=22750
   URL:http://www.securityfocus.com/bid/47071
   URL:http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_t
↪esters/
   URL:http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html
```

[return to 172.162.217.137]

2.1.14 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
```
It was possible to execute the "id" command.
Result: uid=1(daemon) gid=1(daemon)
```

Impact
DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

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

... continues on next page ...

... continued from previous page ...

For more information about DistCC's security see the references.

Vulnerability Detection Method
Details: `DistCC Remote Code Execution Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: `$Revision: 12032 $`

References
`CVE: CVE-2004-2687`
`Other:`
`URL:https://distcc.github.io/security.html`
`URL:https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80/archives/bugtraq/2005-03/0183.html`

[return to 172.162.217.137]

2.1.15 High 5900/tcp

High (CVSS: 9.0)
NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Vulnerability Detection Result
`It was possible to connect to the VNC server with the password: password`

Solution
Solution type: Mitigation
Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight
This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.
Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.
Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method
Details: `VNC Brute Force Login`
OID:1.3.6.1.4.1.25623.1.0.106056
Version used: `2019-12-03T12:31:12+0000`

[return to 172.162.217.137]

2.1.16 High 1099/tcp

High (CVSS: 10.0)
NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability

Summary
Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

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

Impact
An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Solution
Solution type: Workaround
Disable class-loading.

Vulnerability Insight
The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software.

Vulnerability Detection Method
Check if the target tries to load a Java class via a remote HTTP URL.
Details: `Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.140051
Version used: `$Revision: 13999 $`

References
```
Other:
  URL:https://tools.cisco.com/security/center/viewAlert.x?alertId=23665
```

[return to 172.162.217.137]

2.1.17 High 513/tcp

High (CVSS: 7.5)
NVT: rlogin Passwordless / Unencrypted Cleartext Login

Summary
This remote host is running a rlogin service.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
`The service is misconfigured so it is allowing conntections without a password.`

Solution
Solution type: Mitigation
Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight
rlogin has several serious security problems,
- all information, including passwords, is transmitted unencrypted.
- .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)

Vulnerability Detection Method
Details: `rlogin Passwordless / Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: `$Revision: 13541 $`

References
```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651
   URL:http://en.wikipedia.org/wiki/Rlogin
   URL:http://www.ietf.org/rfc/rfc1282.txt
```

[return to 172.162.217.137]

2.1.18 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: /doc directory browsable

Summary
The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Vulnerability Detection Result
`Vulnerable url: http://172.162.217.137/doc/`

Solution
Solution type: Mitigation
Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:
<Directory /usr/doc> AllowOverride None order deny, allow deny from all allow from localhost </Directory>

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Details: /doc directory browsable
OID:1.3.6.1.4.1.25623.1.0.10056
Version used: 2019-11-22T13:51:04+0000

References
CVE: CVE-1999-0678
BID:318

Medium (CVSS: 4.3)
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Summary
This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

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

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution
Solution type: VendorFix
Upgrade to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight
The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: $Revision: 11857 $

References
CVE: CVE-2012-0053
BID:51706
Other:
URL:http://secunia.com/advisories/47779
URL:http://www.exploit-db.com/exploits/18442
URL:http://rhn.redhat.com/errata/RHSA-2012-0128.html
URL:http://httpd.apache.org/security/vulnerabilities_22.html

... continues on next page ...

... continued from previous page ...

URL:http://svn.apache.org/viewvc?view=revision&revision=1235454
URL:http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.htm
↪l

Medium (CVSS: 5.0)
NVT: awiki Multiple Local File Include Vulnerabilities

Summary
awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result
Vulnerable url: http://172.162.217.137/mutillidae/index.php?page=/etc/passwd

Impact
An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host. Other attacks are also possible.

Solution
Solution type: WillNotFix
No known solution was made available for at least one year since the 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.

Affected Software/OS
awiki 20100125 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method
Details: awiki Multiple Local File Include Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: 2019-12-11T11:26:13+0000

References
BID:49187
Other:
URL:https://www.exploit-db.com/exploits/36047/
URL:http://www.securityfocus.com/bid/49187
URL:http://www.kobaonline.com/awiki/

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary

... continues on next page ...

... continued from previous page ...

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
The following input fields where identified (URL:input name):
http://172.162.217.137/phpMyAdmin/:pma_password
http://172.162.217.137/phpMyAdmin/?D=A:pma_password
http://172.162.217.137/tikiwiki/tiki-install.php:pass
http://172.162.217.137/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: Cleartext Transmission of Sensitive Information via HTTP
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: $Revision: 10726 $

References
Other:
URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
Debugging functions are enabled on the remote web server.

... continues on next page ...

... continued from previous page ...

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
`The web server has the following HTTP methods enabled: TRACE`

Impact
An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server configuration.
Please see the manual of your web server or the references for more information.

Affected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight
It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2019-11-22T13:51:04+0000`

References
```
CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683,
↪CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE
↪-2014-7883
BID:9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995
Other:
  URL:http://www.kb.cert.org/vuls/id/288308
   URL:http://www.kb.cert.org/vuls/id/867593
   URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
   URL:https://www.owasp.org/index.php/Cross_Site_Tracing
```

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

... continues on next page ...

... continued from previous page ...

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

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

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution
Solution type: WillNotFix
No known solution was made available for at least one year since the 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.

Affected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details: `phpMyAdmin 'error.php' Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: `2019-12-05T15:10:00+0000`

Product Detection Result
Product: `cpe:/a:phpmyadmin:phpmyadmin:3.1.1`
Method: `phpMyAdmin Detection`
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
`CVE: CVE-2010-4480`
`Other:`
`URL:http://www.exploit-db.com/exploits/15699/`
`URL:http://www.vupen.com/english/advisories/2010/3133`

Medium (CVSS: 4.3)
NVT: TWiki < 6.1.0 XSS Vulnerability

Product detection result
`cpe:/a:twiki:twiki:01.Feb.2003`

... continues on next page ...

... continued from previous page ...

Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 6.1.0

Solution
Solution type: VendorFix
Update to version 6.1.0 or later.

Affected Software/OS
TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: TWiki < 6.1.0 XSS Vulnerability
OID:1.3.6.1.4.1.25623.1.0.141830
Version used: 2019-03-26T08:16:24+0000

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2018-20212
Other:
URL:https://seclists.org/fulldisclosure/2019/Jan/7
URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Medium (CVSS: 6.0)
NVT: TWiki Cross-Site Request Forgery Vulnerability

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.3.1

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution
Solution type: VendorFix
Upgrade to version 4.3.1 or later.

Affected Software/OS
TWiki version prior to 4.3.1

Vulnerability Insight
Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method
Details: TWiki Cross-Site Request Forgery Vulnerability
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: $Revision: 12952 $

Product Detection Result
Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
CVE: CVE-2009-1339
Other:
URL:http://secunia.com/advisories/34880
URL:http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
URL:http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-di
↪ff-cve-2009-1339.txt

Medium (CVSS: 6.8)
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10

Product detection result
cpe:/a:twiki:twiki:01.Feb.2003
Detected by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

... continues on next page ...

... continued from previous page ...

Summary
The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result
`Installed version: 01.Feb.2003`
`Fixed version: 4.3.2`

Impact
Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution
Solution type: VendorFix
Upgrade to TWiki version 4.3.2 or later.

Affected Software/OS
TWiki version prior to 4.3.2

Vulnerability Insight
Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method
Details: `TWiki Cross-Site Request Forgery Vulnerability - Sep10`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `$Revision: 12952 $`

Product Detection Result
Product: `cpe:/a:twiki:twiki:01.Feb.2003`
Method: `TWiki Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.800399)

References
`CVE: CVE-2009-4898`
`Other:`
`URL:http://www.openwall.com/lists/oss-security/2010/08/03/8`
`URL:http://www.openwall.com/lists/oss-security/2010/08/02/17`
`URL:http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix`
`URL:http://twiki.org/cgi-bin/view/Codev/DownloadTWiki`

[return to 172.162.217.137]

2.1.19 Medium 5432/tcp

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

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

Vulnerability Detection Result
```
The certificate of the remote service expired on 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
subject alternative names (SAN):
None
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 (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

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

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

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

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
. . . continues on next page . . .

... continued from previous page ...

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2020-03-31T06:57:15+0000`

References

```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Summary

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Result

```
In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 proto
↪col and supports one or more ciphers. Those supported ciphers can be found in
↪the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.8
↪02067) 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

Solution type: Mitigation

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 like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method

Check the used protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2020-03-31T06:57:15+0000

References

```
CVE: CVE-2016-0800, CVE-2014-3566
Other:
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://drownattack.com/
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

... continues on next page ...

... continued from previous page ...

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
`Server Temporary Key Size: 1024 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2020-03-31T06:57:15+0000`

References
```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

Medium (CVSS: 5.8)
NVT: SSL/TLS: 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.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Updates are available. Please see the references for more information.

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: `SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.105042
Version used: `2020-03-31T06:57:15+0000`

References
```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:https://www.openssl.org/news/secadv/20140605.txt
   URL:http://www.securityfocus.com/bid/67899
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
```
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
```

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

... continues on next page ...

... continued from previous page ...

Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- 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: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `2020-03-31T06:57:15+0000`

References
```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an 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.

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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

Vulnerability Detection Method
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2020-03-31T06:57:15+0000

References
CVE: CVE-2014-3566
BID:70574
Other:
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 172.162.217.137]

2.1.20 Medium 445/tcp

Medium (CVSS: 6.0)
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)

Product detection result
cpe:/a:samba:samba:3.0.20
Detected by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary
Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

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

Impact
An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution
Solution type: VendorFix
Updates are available. Please see the referenced vendor advisory.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
This issue affects Samba 3.0.0 to 3.0.25rc3.

Vulnerability Detection Method
Send a crafted command to the samba server and check for a remote command execution.
Details: `Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)`
OID:1.3.6.1.4.1.25623.1.0.108011
Version used: `$Revision: 10398 $`

Product Detection Result
Product: `cpe:/a:samba:samba:3.0.20`
Method: `SMB NativeLanMan`
OID: 1.3.6.1.4.1.25623.1.0.102011)

References
```
CVE: CVE-2007-2447
BID:23972
Other:
  URL:http://www.securityfocus.com/bid/23972
   URL:https://www.samba.org/samba/security/CVE-2007-2447.html
```

[return to 172.162.217.137]

2.1.21 Medium 6667/tcp

Medium (CVSS: 6.8)
NVT: UnrealIRCd Authentication Spoofing Vulnerability

Product detection result
```
cpe:/a:unrealircd:unrealircd:3.2.8.1
Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)
```

Summary
This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.

Vulnerability Detection Result
```
Installed version: 3.2.8.1
Fixed version:     3.2.10.7
```

Impact
Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

Affected Software/OS
UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight
The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `UnrealIRCd Authentication Spoofing Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.809883
Version used: `$Revision: 11874 $`

Product Detection Result
Product: `cpe:/a:unrealircd:unrealircd:3.2.8.1`
Method: `UnrealIRCd Detection`
OID: 1.3.6.1.4.1.25623.1.0.809884)

References
```
CVE: CVE-2016-7144
BID:92763
Other:
  URL:http://seclists.org/oss-sec/2016/q3/420
   URL:http://www.openwall.com/lists/oss-security/2016/09/05/8
   URL:https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf8
↪6bc50ba1a34a766
   URL:https://bugs.unrealircd.org/main_page.php
```

[return to 172.162.217.137]

2.1.22 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:
```

... continues on next page ...

... continued from previous page ...

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

Solution
Solution type: Mitigation
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.
Details: `SSH Weak Encryption Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: `2020-03-26T13:48:10+0000`

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

[return to 172.162.217.137]

2.1.23 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result
`It was possible to login to the remote FTP service with the following anonymous ↪account(s):`
`anonymous:anonymous@example.com`
`ftp:anonymous@example.com`

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2020-03-24T12:27:11+0000`

References
`Other:`
`URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497`

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command ↪. Response(s):
Anonymous sessions: 331 Please specify the password.
Non-anonymous sessions: 331 Please specify the password.

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: FTP Unencrypted Cleartext Login
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: 2020-03-24T12:27:11+0000

[return to 172.162.217.137]

2.1.24 Medium 23/tcp

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

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

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method
Details: Telnet Unencrypted Cleartext Login

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.108522
Version used: 2019-06-06T07:39:31+0000

[return to 172.162.217.137]

2.1.25 Medium 25/tcp

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

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

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

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

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

Vulnerability Detection Method
Details: Check if Mailserver answer to VRFY and EXPN requests
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: 2020-03-23T13:51:29+0000

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

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.

... continues on next page ...

... continued from previous page ...

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
Solution type: VendorFix
Updates are available. Please see the references for more information.

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: `2020-03-23T13:51:29+0000`

References
```
CVE: CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1506,
↪CVE-2011-1575, CVE-2011-1926, CVE-2011-2165
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
```

... continues on next page ...

... continued from previous page ...

URL:http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_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: 4.3)
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)

Summary
This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result
'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Impact
Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution
Solution type: VendorFix
- Remove support for 'DHE_EXPORT' cipher suites from the service
- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

Affected Software/OS
- Hosts accepting 'DHE_EXPORT' cipher suites
- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight
Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)
OID:1.3.6.1.4.1.25623.1.0.805188

... continues on next page ...

... continued from previous page ...

Version used: 2020-03-31T06:57:15+0000

References

```
CVE: CVE-2015-4000
BID:74733
Other:
  URL:https://weakdh.org
   URL:https://weakdh.org/imperfect-forward-secrecy.pdf
   URL:http://openwall.com/lists/oss-security/2015/05/20/8
   URL:https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained
   URL:https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-change
↪s
```

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

Summary

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

Vulnerability Detection Result

```
The certificate of the remote service expired on 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
subject alternative names (SAN):
None
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 (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

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

... continues on next page ...

... continued from previous page ...

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

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result
```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173
↪652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complic
↪ation of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thi
↪ng outside US,C=XX
Signature Algorithm:  sha1WithRSAEncryption
```

Solution
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight
The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: 2020-03-31T06:57:15+0000

References
Other:
URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Medium (CVSS: 4.3)
NVT: SSL/TLS: 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 TLSv1.0+ the service is also providing the deprecated SSLv2 and SSLv3 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) 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
Solution type: Mitigation
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 like:
- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)
- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method
Check the used protocols of the services provided by this system.
Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.111012
Version used: 2020-03-31T06:57:15+0000

... continues on next page ...

... continued from previous page ...

References

```
CVE: CVE-2016-0800, CVE-2014-3566
Other:
  URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/delivera
↪bles/algorithms-key-sizes-and-parameters-report
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://drownattack.com/
   URL:https://www.imperialviolet.org/2014/10/14/poodle.html
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2020-03-31T06:57:15+0000`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

Medium (CVSS: 4.3)
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)

Summary
This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result
'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact
Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution
Solution type: VendorFix
- Remove support for 'RSA_EXPORT' cipher suites from the service.
- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS
- Hosts accepting 'RSA_EXPORT' cipher suites
- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight
Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method
Check previous collected cipher suites saved in the KB.
Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)
OID:1.3.6.1.4.1.25623.1.0.805142
Version used: 2020-03-31T06:57:15+0000

References
CVE: CVE-2015-0204
BID:71936
Other:
URL:https://freakattack.com

... continues on next page ...

... continued from previous page ...

URL:http://secpod.org/blog/?p=3818
URL:http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-f
↪actoring-nsa.html

Medium (CVSS: 4.3)
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Summary
This host is prone to an 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.

Solution
Solution type: Mitigation
Possible Mitigations are:
- Disable SSLv3
- Disable cipher suites supporting CBC cipher modes
- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

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
Evaluate previous collected information about this service.
Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability .
↪..
OID:1.3.6.1.4.1.25623.1.0.802087
Version used: 2020-03-31T06:57:15+0000

References
CVE: CVE-2014-3566
BID:70574
Other:
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 172.162.217.137]

2.1.26 Medium 5900/tcp

Medium (CVSS: 4.8)
NVT: VNC Server Unencrypted Data Transmission

Summary
The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

Vulnerability Detection Result
```
The VNC server provides the following insecure or cryptographically weak Securit
↪y Type(s):
2 (VNC authentication)
```

Impact
An attacker can uncover sensitive data by sniffing traffic to the VNC server.

Solution
Solution type: Mitigation
Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

Vulnerability Detection Method
Details: `VNC Server Unencrypted Data Transmission`
OID:1.3.6.1.4.1.25623.1.0.108529
Version used: `$Revision: 13014 $`

References
```
Other:
  URL:https://tools.ietf.org/html/rfc6143#page-10
```

[return to 172.162.217.137]

2.1.27 Medium 2121/tcp

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
```

... continues on next page ...

... continued from previous page ...

```
↪. Response(s):
Anonymous sessions:     331 Password required for anonymous
Non-anonymous sessions: 331 Password required for openvas-vt
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method
Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2020-03-24T12:27:11+0000`

[return to 172.162.217.137]

2.1.28 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 463774
Packet 2: 463896
```

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

Solution
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

... continues on next page ...

... continued from previous page ...

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-03-21T13:23:23+0000`

References
```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 172.162.217.137]

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

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
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: `2020-03-26T13:48:10+0000`

[return to 172.162.217.137]

2.1.30 Log 1524/tcp

Log (CVSS: 0.0)
NVT: Service Detection with 'GET' Request

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

Vulnerability Detection Result
`A root shell of Metasploitable seems to be running on this port.`

Log Method
Details: `Service Detection with 'GET' Request`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `2020-03-25T13:50:09+0000`

[return to 172.162.217.137]

2.1.31 Log 512/tcp

Log (CVSS: 0.0)
NVT: Service Detection with 'BINARY' Request

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

Vulnerability Detection Result
`A rexec service seems to be running on this port.`

Log Method

... continues on next page ...

... continued from previous page ...

Details: Service Detection with 'BINARY' Request
OID:1.3.6.1.4.1.25623.1.0.108204
Version used: 2020-02-20T07:23:20+0000

[return to 172.162.217.137]

2.1.32 Log general/icmp

Log (CVSS: 0.0)
NVT: ICMP Timestamp Detection

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

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

Log Method
Details: ICMP Timestamp Detection
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: $Revision: 10411 $

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

[return to 172.162.217.137]

2.1.33 Log general/tcp

Log (CVSS: 0.0)
NVT: OpenSSH Detection Consolidation

Summary
The script reports a detected OpenSSH including the version number.

Vulnerability Detection Result
Detected OpenSSH Server
Version: 4.7p1

... continues on next page ...

... continued from previous page ...

```
Location:       22/tcp
CPE:            cpe:/a:openbsd:openssh:4.7p1
Concluded from version/product identification result:
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Log Method
Details: OpenSSH Detection Consolidation
OID:1.3.6.1.4.1.25623.1.0.108577
Version used: 2019-05-23T06:42:35+0000

References
Other:
URL:https://www.openssh.com/

Log (CVSS: 0.0)
NVT: OS Detection Consolidation and Reporting

Summary
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the referenced community portal.

Vulnerability Detection Result

```
Best matching OS:
OS:             Ubuntu
Version:        8.04
CPE:            cpe:/o:canonical:ubuntu_linux:8.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (SSH OS Identification)
Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Setting key "Host/runs_unixoide" based on this information
Other OS detections (in order of reliability):
OS:             Linux/Unix
CPE:            cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 21/tcp: 220 (vsFTPd 2.3.4)
OS:             Debian GNU/Linux
CPE:            cpe:/o:debian:debian_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.105355 (FTP OS Identification)
Concluded from FTP banner on port 2121/tcp: 220 ProFTPD 1.3.1 Server (Debian) [:
↪:ffff:172.162.217.137]
OS:             Debian GNU/Linux
CPE:            cpe:/o:debian:debian_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
Concluded from SMB/Samba banner on port 445/tcp:
```

... continues on next page ...

... continued from previous page ...

```
OS String:  Unix
SMB String: Samba 3.0.20-Debian
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from PHP Server banner on port 80/tcp: X-Powered-By: PHP/5.2.4-2ubuntu
↪5.10
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.2.8 (Ubuntu)
↪DAV/2
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.111068 (SMTP/POP3/IMAP Server OS Identificat
↪ion)
Concluded from SMTP banner on port 25/tcp: 220 metasploitable.localdomain ESMTP
↪Postfix (Ubuntu)
OS:           Ubuntu
Version:      8.04
CPE:          cpe:/o:canonical:ubuntu_linux:8.04
Found by NVT: 1.3.6.1.4.1.25623.1.0.111069 (Telnet OS Identification)
Concluded from Telnet banner on port 23/tcp:                  _
↪_       - -        -     -      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
OS:           Ubuntu
CPE:          cpe:/o:canonical:ubuntu_linux
Found by NVT: 1.3.6.1.4.1.25623.1.0.108192 (MySQL/MariaDB Server OS Identificati
↪on)
Concluded from MySQL/MariaDB server banner on port 3306/tcp: 5.0.51a-3ubuntu5
```

Log Method

Details: OS Detection Consolidation and Reporting

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105937
Version used: 2020-04-01T10:41:43+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: SSL/TLS: Hostname discovery from server certificate

Summary
It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.

Vulnerability Detection Result
The following additional but not resolvable hostnames were detected:
ubuntu804-base.localdomain

Log Method
Details: SSL/TLS: Hostname discovery from server certificate
OID:1.3.6.1.4.1.25623.1.0.111010
Version used: $Revision: 13774 $

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 172.162.217.1 to 172.162.217.137:
172.162.217.1
172.162.217.137

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: 2020-03-21T13:23:23+0000

[return to 172.162.217.137]

2.1.34 Log 80/tcp

Log (CVSS: 0.0)
NVT: Apache HTTP/Web Server Detection (HTTP)

Summary
Checks whether Apache HTTP/Web Server is present on the target system.

Vulnerability Detection Result
```
Detected Apache HTTP/Web Server
Version:       2.2.8
Location:      80/tcp
CPE:           cpe:/a:apache:http_server:2.2.8
Concluded from version/product identification result:
Server: Apache/2.2.8
```

Log Method
Details: `Apache HTTP/Web Server Detection (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.900498
Version used: `2020-03-04T13:56:06+0000`

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)
- Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032)
- The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use
- The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use
If you think any of this information is wrong please report it to the referenced community portal.

Vulnerability Detection Result
```
The Hostname/IP "172.162.217.137" was used to access the remote host.
Generic web application scanning is disabled for this host via the "Enable gener
↪ic web application scanning" option within the "Global variable settings" of t
↪he scan config in use.
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
```

... continues on next page ...

... continued from previous page ...

```
This service seems to be NOT able to host ASP scripts.
The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)" was used to access
↪the remote host.
Historic /scripts and /cgi-bin are not added to the directories used for CGI sca
↪nning. You can enable this again with the "Add historic /scripts and /cgi-bin
↪to directories for CGI scanning" option within the "Global variable settings"
↪of the scan config in use.
The following directories were used for CGI scanning:
http://172.162.217.137/
http://172.162.217.137/cgi-bin
http://172.162.217.137/dav
http://172.162.217.137/doc
http://172.162.217.137/dvwa
http://172.162.217.137/mutillidae
http://172.162.217.137/mutillidae/documentation
http://172.162.217.137/oops/TWiki
http://172.162.217.137/phpMyAdmin
http://172.162.217.137/rdiff/TWiki
http://172.162.217.137/test
http://172.162.217.137/test/testoutput
http://172.162.217.137/tikiwiki
http://172.162.217.137/tikiwiki/lib
http://172.162.217.137/twiki
http://172.162.217.137/twiki/pub
http://172.162.217.137/twiki/pub/TWiki/FileAttachment
http://172.162.217.137/twiki/pub/TWiki/TWikiDocGraphics
http://172.162.217.137/twiki/pub/TWiki/TWikiLogos
http://172.162.217.137/twiki/pub/TWiki/TWikiPreferences
http://172.162.217.137/twiki/pub/TWiki/TWikiTemplates
http://172.162.217.137/twiki/pub/icn
http://172.162.217.137/view/TWiki
While this is not, in and of itself, a bug, you should manually inspect these di
↪rectories to ensure that they are in compliance with company security standard
↪s
The following directories were excluded from CGI scanning because the "Regex pat
↪tern to exclude directories from CGI scanning" setting of the NVT "Global vari
↪able settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\
↪.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|p
↪icture|bilder|thumbnail|media/|skins?/)"
http://172.162.217.137/icons
http://172.162.217.137/mutillidae/images
http://172.162.217.137/mutillidae/javascript
http://172.162.217.137/mutillidae/javascript/ddsmoothmenu
http://172.162.217.137/mutillidae/styles
http://172.162.217.137/mutillidae/styles/ddsmoothmenu
http://172.162.217.137/phpMyAdmin/themes/original/img
http://172.162.217.137/tikiwiki/img/icons
```

... continues on next page ...

... continued from previous page ...

```
http://172.162.217.137/tikiwiki/styles
http://172.162.217.137/tikiwiki/styles/transitions
Directory index found at:
http://172.162.217.137/dav/
http://172.162.217.137/mutillidae/documentation/
http://172.162.217.137/test/
http://172.162.217.137/test/testoutput/
http://172.162.217.137/twiki/TWikiDocumentation.html
http://172.162.217.137/twiki/bin/view/TWiki/TWikiDocumentation
http://172.162.217.137/twiki/bin/view/TWiki/TWikiInstallationGuide
Extraneous phpinfo() script found at:
http://172.162.217.137/mutillidae/phpinfo.php
http://172.162.217.137/phpinfo.php
PHP script discloses physical path at:
http://172.162.217.137/tikiwiki/tiki-install.php (/var/www/tikiwiki/lib/adodb/dr
↪ivers/adodb-mysql.inc.php)
The "Number of pages to mirror" setting (Current: 200) of the NVT "Web mirroring
↪" (OID: 1.3.6.1.4.1.25623.1.0.10662) was reached. Raising this limit allows to
↪ mirror this host more thoroughly but might increase the scanning time.
NOTE: The 'Maximum number of items shown for each list' setting has been reached
↪. There are 368 additional entries available for the following truncated list.
The following CGIs were discovered:
Syntax : cginame (arguments [default value])
http://172.162.217.137/dav/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://172.162.217.137/mutillidae/ (page [add-to-your-blog.php] )
http://172.162.217.137/mutillidae/documentation/ (C=S;O [A] C=N;O [D] C=M;O [A]
↪C=D;O [A] )
http://172.162.217.137/mutillidae/index.php (username [anonymous] do [toggle-hin
↪ts] page [home.php] )
http://172.162.217.137/oops/TWiki/TWikiHistory (template [oopsrev] param1 [1.10]
↪ )
http://172.162.217.137/phpMyAdmin/index.php (phpMyAdmin [10c872efcb2672315313e37
↪674665772a51ba440] token [967fff0a6019a99ebab5383c0de6db92] pma_username [] ta
↪ble [] lang [] server [1] db [] convcharset [utf-8] pma_password [] )
http://172.162.217.137/phpMyAdmin/phpmyadmin.css.php (token [967fff0a6019a99ebab
↪5383c0de6db92] js_frame [right] lang [en-utf-8] nocache [2457687151] convchars
↪et [utf-8] )
http://172.162.217.137/rdiff/TWiki/TWikiHistory (rev1 [1.10] rev2 [1.9] )
http://172.162.217.137/test/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A] )
http://172.162.217.137/test/testoutput/ (C=S;O [A] C=N;O [D] C=M;O [A] C=D;O [A]
↪ )
http://172.162.217.137/tikiwiki/tiki-install.php (host [localhost] dbinfo [] pas
↪s [] name [] db [] restart [1] resetdb [] user [] )
http://172.162.217.137/twiki/bin/attach/TWiki/FileAttachment (filename [Sample.t
↪xt] revInfo [1] )
http://172.162.217.137/twiki/bin/edit/Know/ReadmeFirst (t [1597179074] )
http://172.162.217.137/twiki/bin/edit/Know/WebChanges (t [1597178841] )
```

... continues on next page ...

... continued from previous page ...

```
http://172.162.217.137/twiki/bin/edit/Know/WebHome (t [1597178777] )
http://172.162.217.137/twiki/bin/edit/Know/WebIndex (t [1597179076] )
http://172.162.217.137/twiki/bin/edit/Know/WebNotify (t [1597179077] )
http://172.162.217.137/twiki/bin/edit/Know/WebPreferences (t [1597178854] )
http://172.162.217.137/twiki/bin/edit/Know/WebSearch (t [1597178852] )
http://172.162.217.137/twiki/bin/edit/Know/WebStatistics (t [1597179079] )
http://172.162.217.137/twiki/bin/edit/Know/WebTopicList (t [1597179077] )
http://172.162.217.137/twiki/bin/edit/Main/BillClinton (topicparent [Main.TWikiU
↪sers] )
http://172.162.217.137/twiki/bin/edit/Main/CharleytheHorse (t [1597179093] )
http://172.162.217.137/twiki/bin/edit/Main/ChristopheVermeulen (topicparent [Mai
↪n.TWikiUsers] )
http://172.162.217.137/twiki/bin/edit/Main/DavidWarman (topicparent [Main.TWikiU
↪sers] )
http://172.162.217.137/twiki/bin/edit/Main/EngineeringGroup (topicparent [Main.T
↪WikiGroups] )
http://172.162.217.137/twiki/bin/edit/Main/GoodStyle (topicparent [Main.WebHome]
↪ )
http://172.162.217.137/twiki/bin/edit/Main/JohnAltstadt (topicparent [Main.TWiki
↪Users] )
http://172.162.217.137/twiki/bin/edit/Main/JohnTalintyre (t [1597179093] )
http://172.162.217.137/twiki/bin/edit/Main/LondonOffice (t [1597179104] )
http://172.162.217.137/twiki/bin/edit/Main/MartinRaabe (topicparent [TWiki.TWiki
↪UpgradeGuide] )
http://172.162.217.137/twiki/bin/edit/Main/NicholasLee (t [1597179094] )
http://172.162.217.137/twiki/bin/edit/Main/OfficeLocations (t [1597178788] )
http://172.162.217.137/twiki/bin/edit/Main/PeterFokkinga (topicparent [Main.TWik
↪iUsers] )
http://172.162.217.137/twiki/bin/edit/Main/PeterThoeny (t [1597178959] )
http://172.162.217.137/twiki/bin/edit/Main/SanJoseOffice (t [1597179103] )
http://172.162.217.137/twiki/bin/edit/Main/SupportGroup (topicparent [Main.TWiki
↪Groups] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiAdminGroup (t [1597179099] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiGroups (t [1597178786] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiGuest (t [1597179095] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiPreferences (topicparent [Main.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiRegistration (topicparent [Main.
↪TWikiUsers] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiUsers (t [1597178784] )
http://172.162.217.137/twiki/bin/edit/Main/TWikiWeb (topicparent [Main.WebHome]
↪)
http://172.162.217.137/twiki/bin/edit/Main/TestArea (topicparent [Main.WebHome]
↪)
http://172.162.217.137/twiki/bin/edit/Main/TextFormattingFAQ (topicparent [Main.
↪WebHome] )
http://172.162.217.137/twiki/bin/edit/Main/TextFormattingRules (topicparent [Mai
```

... continues on next page ...

... continued from previous page ...

```
↪n.WebHome] )
http://172.162.217.137/twiki/bin/edit/Main/TokyoOffice (t [1597179105] )
http://172.162.217.137/twiki/bin/edit/Main/WebChanges (t [1597178790] )
http://172.162.217.137/twiki/bin/edit/Main/WebHome (t [1597178758] )
http://172.162.217.137/twiki/bin/edit/Main/WebIndex (t [1597178798] )
http://172.162.217.137/twiki/bin/edit/Main/WebNotify (t [1597178867] )
http://172.162.217.137/twiki/bin/edit/Main/WebPreferences (t [1597178803] )
http://172.162.217.137/twiki/bin/edit/Main/WebSearch (t [1597178799] )
http://172.162.217.137/twiki/bin/edit/Main/WebStatistics (t [1597178869] )
http://172.162.217.137/twiki/bin/edit/Main/WebTopicEditTemplate (topicparent [Ma
↪in.WebPreferences] )
http://172.162.217.137/twiki/bin/edit/Main/WebTopicList (t [1597178866] )
http://172.162.217.137/twiki/bin/edit/Main/WelcomeGuest (topicparent [Main.WebHo
↪me] )
http://172.162.217.137/twiki/bin/edit/Main/WikiName (topicparent [Main.TWikiUser
↪s] )
http://172.162.217.137/twiki/bin/edit/Main/WikiNotation (topicparent [Main.TWiki
↪Users] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic1 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic2 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic3 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic4 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic5 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic6 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic7 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/TestTopic8 (topicparent [Sandbox.W
↪ebHome] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebChanges (t [1597178856] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebHome (t [1597178780] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebIndex (t [1597179082] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebNotify (t [1597179089] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebPreferences (t [1597178863] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebSearch (t [1597178861] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebStatistics (t [1597179090] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebTopicEditTemplate (topicparent
↪[Sandbox.WebPreferences] )
http://172.162.217.137/twiki/bin/edit/Sandbox/WebTopicList (t [1597179088] )
http://172.162.217.137/twiki/bin/edit/TWiki/ (topic [] topicparent [TWikiFAQ] on
↪lywikiname [on] templatetopic [TWikiFaqTemplate] )
http://172.162.217.137/twiki/bin/edit/TWiki/AppendixFileSystem (t [1597179060] )
```

... continues on next page ...

... continued from previous page ...

```
http://172.162.217.137/twiki/bin/edit/TWiki/BumpyWord (t [1597179107] )
http://172.162.217.137/twiki/bin/edit/TWiki/DefaultPlugin (t [1597178999] )
http://172.162.217.137/twiki/bin/edit/TWiki/FileAttachment (t [1597178991] )
http://172.162.217.137/twiki/bin/edit/TWiki/FormattedSearch (t [1597179034] )
http://172.162.217.137/twiki/bin/edit/TWiki/GnuGeneralPublicLicense (t [15971790
↪69] )
http://172.162.217.137/twiki/bin/edit/TWiki/GoodStyle (t [1597178944] )
http://172.162.217.137/twiki/bin/edit/TWiki/InstalledPlugins (t [1597179066] )
http://172.162.217.137/twiki/bin/edit/TWiki/InstantEnhancements (t [1597179006]
↪)
http://172.162.217.137/twiki/bin/edit/TWiki/InterWikis (t [1597179001] )
http://172.162.217.137/twiki/bin/edit/TWiki/InterwikiPlugin (t [1597179000] )
http://172.162.217.137/twiki/bin/edit/TWiki/ManagingTopics (t [1597179055] )
http://172.162.217.137/twiki/bin/edit/TWiki/ManagingWebs (t [1597179058] )
http://172.162.217.137/twiki/bin/edit/TWiki/MeaningfulTitle (topicparent [TWiki.
↪TextFormattingFAQ] )
http://172.162.217.137/twiki/bin/edit/TWiki/NewTopic (topicparent [TWiki.TWikiSh
↪orthand] )
http://172.162.217.137/twiki/bin/edit/TWiki/NotExistingYet (topicparent [TWiki.T
↪extFormattingRules] )
http://172.162.217.137/twiki/bin/edit/TWiki/PeterThoeny (t [1597179068] )
http://172.162.217.137/twiki/bin/edit/TWiki/SiteMap (t [1597179067] )
http://172.162.217.137/twiki/bin/edit/TWiki/StartingPoints (t [1597178807] )
http://172.162.217.137/twiki/bin/edit/TWiki/TWikiAccessControl (t [1597179024] )
http://172.162.217.137/twiki/bin/edit/TWiki/TWikiAdminCookBook (t [1597179003] )
```

Log Method
Details: CGI Scanning Consolidation
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: 2019-09-23T09:25:24+0000

References
Other:
URL:https://community.greenbone.net/c/vulnerability-tests

Log (CVSS: 0.0)
NVT: Fingerprint web server with favicon.ico

Summary
The remote web server contains a graphic image that is prone to information disclosure.

Vulnerability Detection Result
The following apps/services were identified:
"phpmyadmin (2.11.8.1 - 4.2.x)" fingerprinted by the file: "http://172.162.217.1
↪37/phpMyAdmin/favicon.ico"

Impact

... continues on next page ...

... continued from previous page ...

The 'favicon.ico' file found on the remote web server belongs to a popular webserver/application. This may be used to fingerprint the webserver/application.

Solution
Solution type: Mitigation
Remove the 'favicon.ico' file or create a custom one for your site.

Log Method
Details: `Fingerprint web server with favicon.ico`
OID:1.3.6.1.4.1.25623.1.0.20108
Version used: `2020-02-26T12:57:19+0000`

Log (CVSS: 0.0)
NVT: HTTP Security Headers Detection

Summary
All known security headers are being checked on the host. On completion a report will hand back whether a specific security header has been implemented (including its value) or is missing on the target.

Vulnerability Detection Result

```
Missing Headers                   | More Information
----------------------------------------------------------------------------------
↪-----------------------------------
Content-Security-Policy           | https://owasp.org/www-project-secure-headers
↪/#content-security-policy
Feature-Policy                    | https://owasp.org/www-project-secure-headers
↪/#feature-policy
Referrer-Policy                   | https://owasp.org/www-project-secure-headers
↪/#referrer-policy
X-Content-Type-Options            | https://owasp.org/www-project-secure-headers
↪/#x-content-type-options
X-Frame-Options                   | https://owasp.org/www-project-secure-headers
↪/#x-frame-options
X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies
X-XSS-Protection                  | https://owasp.org/www-project-secure-headers
↪/#x-xss-protection
```

Log Method
Details: `HTTP Security Headers Detection`
OID:1.3.6.1.4.1.25623.1.0.112081
Version used: `2020-03-18T09:31:42+0000`

References
`Other:`
`URL:https://owasp.org/www-project-secure-headers/`

... continues on next page ...

... continued from previous page ...

URL:https://owasp.org/www-project-secure-headers/#div-headers
URL:https://securityheaders.io/

Log (CVSS: 0.0)
NVT: HTTP Server Banner Enumeration

Summary
This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).

Vulnerability Detection Result

```
It was possible to enumerate the following HTTP server banner(s):
Server banner                       | Enumeration technique
--------------------------------------------------------------------------------
↪-
Server: Apache/2.2.8 (Ubuntu) DAV/2 | Valid HTTP 0.9 GET request to '/index.html
↪'
X-Powered-By: PHP/5.2.4-2ubuntu5.10 | Valid HTTP 0.9 GET request to '/index.php'
```

Log Method
Details: HTTP Server Banner Enumeration
OID:1.3.6.1.4.1.25623.1.0.108708
Version used: 2020-02-25T12:12:27+0000

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

Summary
This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Vulnerability Detection Result

```
The remote HTTP Server banner is:
Server: Apache/2.2.8 (Ubuntu) DAV/2
```

Log Method
Details: HTTP Server type and version
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: 2020-02-06T14:44:42+0000

Log (CVSS: 0.0)
NVT: jQuery Detection (HTTP)

Summary

... continues on next page ...

... continued from previous page ...

Detection of jQuery.
The script sends a connection request to the server and attempts to detect jQuery and to extract its version.

Vulnerability Detection Result

```
Detected jQuery
Version:        unknown
Location:       /mutillidae/javascript/ddsmoothmenu
CPE:            cpe:/a:jquery:jquery
```

Log Method

Details: jQuery Detection (HTTP)
OID:1.3.6.1.4.1.25623.1.0.141622
Version used: 2020-03-27T07:32:24+0000

References

```
Other:
  URL:https://jquery.com/
```

Log (CVSS: 0.0)
NVT: PHP Version Detection (Remote)

Summary

Detects the installed version of PHP. This script sends an HTTP GET request and tries to get the version from the response.

Vulnerability Detection Result

```
Detected PHP
Version:        5.2.4
Location:       80/tcp
CPE:            cpe:/a:php:php:5.2.4
Concluded from version/product identification result:
X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

Log Method

Details: PHP Version Detection (Remote)
OID:1.3.6.1.4.1.25623.1.0.800109
Version used: 2019-12-17T14:07:10+0000

Log (CVSS: 0.0)
NVT: phpMyAdmin Detection

Summary

Detection of phpMyAdmin.

... continues on next page ...

... continued from previous page ...

The script sends a connection request to the server and attempts to extract the version number from the reply.

Vulnerability Detection Result

```
Detected phpMyAdmin
Version:       3.1.1
Location:      /phpMyAdmin
CPE:           cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Concluded from version/product identification result:
Version 3.1.1
Concluded from version/product identification location:
http://172.162.217.137/phpMyAdmin/README
Extra information:
- Protected by Username/Password
```

Log Method

Details: `phpMyAdmin Detection`
OID:1.3.6.1.4.1.25623.1.0.900129
Version used: `2019-12-04T13:23:25+0000`

Log (CVSS: 0.0)
NVT: Services

Summary

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

Vulnerability Detection Result

```
A web server is running on this port
```

Log Method

Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

Log (CVSS: 0.0)
NVT: TWiki Version Detection

Summary

Detection of TWiki.
The script sends a HTTP connection request to the server and attempts to detect the presence of TWiki and to extract its version.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Detected TWiki
Version:       01.Feb.2003
Location:      /twiki/bin
CPE:           cpe:/a:twiki:twiki:01.Feb.2003
Concluded from version/product identification result:
This site is running TWiki version <strong>01 Feb 2003</strong>
```

Log Method
Details: `TWiki Version Detection`
OID:1.3.6.1.4.1.25623.1.0.800399
Version used: `2019-12-04T13:23:25+0000`

[return to 172.162.217.137]

2.1.35 Log 8009/tcp

Log (CVSS: 0.0)
NVT: Apache JServ Protocol (AJP) v1.3 Detection

Summary
The script detects a service supporting the Apache JServ Protocol (AJP) version 1.3.

Vulnerability Detection Result

```
A service supporting the Apache JServ Protocol (AJP) v1.3 seems to be running on
↪ this port.
```

Log Method
Details: `Apache JServ Protocol (AJP) v1.3 Detection`
OID:1.3.6.1.4.1.25623.1.0.108082
Version used: `2020-03-02T11:38:26+0000`

[return to 172.162.217.137]

2.1.36 Log 5432/tcp

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

```
PostgreSQL database can be accessed by remote attackers
```

... continues on next page ...

... continued from previous page ...

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

Solution
Solution type: Workaround
Restrict Database access to remote systems.

Affected Software/OS
- MySQL/MariaDB
- IBM DB2
- PostgreSQL
- IBM solidDB
- Oracle Database
- Microsoft SQL Server

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: `2020-03-21T13:23:23+0000`

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

Log (CVSS: 0.0)
NVT: PostgreSQL Detection

Summary
Detection of PostgreSQL, a open source object-relational database system.
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:       8.3.1
Location:      5432/tcp
CPE:           cpe:/a:postgresql:postgresql:8.3.1
Concluded from version/product identification result:
8.3.1
```

Log Method
Details: `PostgreSQL Detection`

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.100151
Version used: 2020-02-26T09:22:27+0000

References
Other:
URL:https://www.postgresql.org/

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: 2019-07-08T14:12:44+0000

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

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

Vulnerability Detection Result
The certificate of the remote service is self signed.
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
subject alternative names (SAN):
None
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

... continues on next page ...

... continued from previous page ...

```
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 8981 $

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary
This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: 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
subject alternative names (SAN):
None
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 (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2019-04-04T13:38:03+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: PostgreSQL SSL/TLS Support Detection

Product detection result
cpe:/a:postgresql:postgresql:8.3.1
Detected by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary
Checks if the remote PostgreSQL server supports SSL/TLS.

Vulnerability Detection Result
The remote PostgreSQL server supports SSL/TLS.

Log Method
Details: SSL/TLS: PostgreSQL SSL/TLS Support Detection
OID:1.3.6.1.4.1.25623.1.0.105013
Version used: 2020-01-28T13:26:39+0000

Product Detection Result
Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection
OID: 1.3.6.1.4.1.25623.1.0.100151)

References
Other:
URL:https://www.postgresql.org/docs/current/static/ssl-tcp.html

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_AES_256_CBC_SHA

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: SSL/TLS: Report Medium Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

```
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
No 'Anonymous' cipher suites accepted by this service via the SSLv3 protocol.
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol.

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2020-03-31T06:57:15+0000

[return to 172.162.217.137]

2.1.37 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: 11003 $

Log (CVSS: 0.0)
NVT: Microsoft Windows SMB Accessible Shares

Summary
The script detects the Windows SMB Accessible Shares and sets the result into KB.

Vulnerability Detection Result
The following shares were found
IPC$

Log Method
Details: Microsoft Windows SMB Accessible Shares
OID:1.3.6.1.4.1.25623.1.0.902425
Version used: $Revision: 11420 $

Log (CVSS: 0.0)
NVT: SMB log in

Summary
This script attempts to logon into the remote host using login/password credentials.

Vulnerability Detection Result
`It was possible to log into the remote host using the SMB protocol.`

Log Method
Details: `SMB log in`
OID:1.3.6.1.4.1.25623.1.0.10394
Version used: `2019-10-16T06:21:07+0000`

Log (CVSS: 0.0)
NVT: SMB Login Successful For Authenticated Checks

Summary
It was possible to login using the provided SMB credentials. Hence authenticated checks are enabled.

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

Log Method
Details: `SMB Login Successful For Authenticated Checks`
OID:1.3.6.1.4.1.25623.1.0.108539
Version used: `$Revision: 13248 $`

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
```
Detected Samba
Version:       3.0.20
Location:      445/tcp
CPE:           cpe:/a:samba:samba:3.0.20
Concluded from version/product identification result:
Samba 3.0.20-Debian
Extra information:
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2019-12-12T09:38:57+0000

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

Summary
It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.

Vulnerability Detection Result
Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.0.20-Debian
Detected OS: Debian GNU/Linux

Log Method
Details: SMB NativeLanMan
OID:1.3.6.1.4.1.25623.1.0.102011
Version used: 2019-12-12T09:38:57+0000

Log (CVSS: 0.0)
NVT: SMB Remote Version Detection

Summary
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.

Vulnerability Detection Result
Only SMBv1 is enabled on remote target

Log Method
Details: SMB Remote Version Detection
OID:1.3.6.1.4.1.25623.1.0.807830
Version used: 2019-05-16T07:13:31+0000

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A CIFS server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: SMBv1 enabled (Remote Check)

Summary
The host has enabled SMBv1 for the SMB Server.

Vulnerability Detection Result
SMBv1 is enabled for the SMB Server

Log Method
Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:
- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).
Details: SMBv1 enabled (Remote Check)
OID:1.3.6.1.4.1.25623.1.0.140151
Version used: 2019-05-20T06:24:13+0000

References
Other:
URL:https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices
URL:https://support.microsoft.com/en-us/kb/2696547
URL:https://support.microsoft.com/en-us/kb/204279

[return to 172.162.217.137]

2.1.38 Log 514/tcp

Log (CVSS: 0.0)
NVT: rsh Service Detection

Summary
Checks if the remote host is running a rsh service.
Note: The reporting takes place in a separate VT 'rsh Unencrypted Cleartext Login' (OID: 1.3.6.1.4.1.25623.1.0.100080).

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Result
A rsh service is running at this port.

Log Method
Details: rsh Service Detection
OID:1.3.6.1.4.1.25623.1.0.108478
Version used: 2019-09-17T06:05:09+0000

Log (CVSS: 0.0)
NVT: Service Detection with 'GET' Request

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

Vulnerability Detection Result
A rsh service seems to be running on this port.

Log Method
Details: Service Detection with 'GET' Request
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: 2020-03-25T13:50:09+0000

[return to 172.162.217.137]

2.1.39 Log 6667/tcp

Log (CVSS: 0.0)
NVT: IRC Server Banner Detection

Summary
This script tries to detect the banner of an IRC server.

Vulnerability Detection Result
The IRC server banner is:
:irc.Metasploitable.LAN 351 FCEAAIJEG Unreal3.2.8.1. irc.Metasploitable.LAN :Fhi
↪XOoE [*=2309]

Log Method
Details: IRC Server Banner Detection
OID:1.3.6.1.4.1.25623.1.0.11156
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: Service Detection with 'GET' Request

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

Vulnerability Detection Result
`An IRC server seems to be running on this port.`

Log Method
Details: `Service Detection with 'GET' Request`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `2020-03-25T13:50:09+0000`

Log (CVSS: 0.0)
NVT: UnrealIRCd Detection

Summary
Detection of UnrealIRCd Daemon. This script sends a request to the server and gets the version from the response.

Vulnerability Detection Result
```
Detected UnrealIRCd
Version:        3.2.8.1
Location:       6667/tcp
CPE:            cpe:/a:unrealircd:unrealircd:3.2.8.1
Concluded from version/product identification result:
Unreal3.2.8.1
```

Log Method
Details: `UnrealIRCd Detection`
OID:1.3.6.1.4.1.25623.1.0.809884
Version used: `$Revision: 10987 $`

[return to 172.162.217.137]

2.1.40 Log 22/tcp

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 ssh server is running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

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

Summary
This script detects which algorithms 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
Details: `SSH Protocol Algorithms Supported`
OID:1.3.6.1.4.1.25623.1.0.105565
Version used: `2020-03-26T13:48:10+0000`

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
SSHv2 Fingerprint(s):
ssh-dss: 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd
ssh-rsa: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
```

Log Method
Details: `SSH Protocol Versions Supported`
OID:1.3.6.1.4.1.25623.1.0.100259
Version used: `2020-03-26T13:48:10+0000`

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
```
Remote SSH server banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Remote SSH supported authentication: password,publickey
Remote SSH text/login banner: (not available)
This is probably:
- OpenSSH
Concluded from remote connection attempt with credentials:
Login:    OpenVAS-VT
Password: OpenVAS-VT
```

Log Method
Details: `SSH Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10267
Version used: `2020-03-26T13:48:10+0000`

[return to 172.162.217.137]

2.1.41 Log general/CPE-T

Log (CVSS: 0.0) NVT: CPE Inventory
Summary This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.
Vulnerability Detection Result 172.162.217.137|cpe:/a:apache:http_server:2.2.8 172.162.217.137|cpe:/a:beasts:vsftpd:2.3.4 172.162.217.137|cpe:/a:isc:bind:9.4.2 172.162.217.137|cpe:/a:jquery:jquery 172.162.217.137|cpe:/a:mysql:mysql:5.0.51a 172.162.217.137|cpe:/a:openbsd:openssh:4.7p1 172.162.217.137|cpe:/a:php:php:5.2.4 172.162.217.137|cpe:/a:phpmyadmin:phpmyadmin:3.1.1 172.162.217.137|cpe:/a:postfix:postfix 172.162.217.137|cpe:/a:postgresql:postgresql:8.3.1 172.162.217.137|cpe:/a:proftpd:proftpd:1.3.1 172.162.217.137|cpe:/a:samba:samba:3.0.20 172.162.217.137|cpe:/a:twiki:twiki:01.Feb.2003 172.162.217.137|cpe:/a:unrealircd:unrealircd:3.2.8.1 172.162.217.137|cpe:/a:x.org:x11:11.0 172.162.217.137|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: 2019-10-24T11:29:24+0000
References Other: URL:https://nvd.nist.gov/products/cpe

[return to 172.162.217.137]

2.1.42 Log 21/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects and reports a FTP Server Banner.

Vulnerability Detection Result

```
Remote FTP server banner:
220 (vsFTPd 2.3.4)
This is probably:
- vsFTPd
Server operating system information collected via "SYST" command:
215 UNIX Type: L8
Server status information collected via "STAT" command:
211-FTP server status:
     Connected to 172.162.217.1
     Logged in as ftp
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     vsFTPd 2.3.4 - secure, fast, stable
211 End of status
```

Log Method
Details: `FTP Banner Detection`
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: `2020-03-24T12:27:11+0000`

Log (CVSS: 0.0)
NVT: FTP Missing Support For AUTH TLS

Summary
The remote FTP server does not support the 'AUTH TLS' command.

Vulnerability Detection Result

```
The remote FTP server does not support the 'AUTH TLS' command.
```

Log Method
Details: `FTP Missing Support For AUTH TLS`
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: `$Revision: 13863 $`

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 FTP server is running on this port.
Here is its banner :
220 (vsFTPd 2.3.4)
```

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

Log (CVSS: 0.0)
NVT: vsFTPd FTP Server Detection

Summary
The script is grabbing the banner of a FTP server and attempts to identify a vsFTPd FTP Server and its version from the reply.

Vulnerability Detection Result
```
Detected vsFTPd
Version:       2.3.4
Location:      21/tcp
CPE:           cpe:/a:beasts:vsftpd:2.3.4
Concluded from version/product identification result:
220 (vsFTPd 2.3.4)
```

Log Method
Details: vsFTPd FTP Server Detection
OID:1.3.6.1.4.1.25623.1.0.111050
Version used: 2020-03-24T12:27:11+0000

[return to 172.162.217.137]

2.1.43 Log 53/tcp

Log (CVSS: 0.0)
NVT: DNS Server Detection (TCP)

Summary

. . . continues on next page . . .

... continued from previous page ...

A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.

Vulnerability Detection Result

```
The remote DNS server banner is:
9.4.2
```

Log Method

Details: `DNS Server Detection (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108018
Version used: `$Revision: 13541 $`

Log (CVSS: 0.0)
NVT: ISC BIND 'named' Detection (Remote)

Summary

BIND 'named' is an open-source DNS server from isc.org. Many proprietary DNS servers are based on BIND source code.

Vulnerability Detection Result

```
Detected ISC BIND
Version:       9.4.2
Location:      53/tcp
CPE:           cpe:/a:isc:bind:9.4.2
Concluded from version/product identification result:
9.4.2
```

Solution

Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts.

Vulnerability Insight

The BIND based name servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source.

Log Method

Details: `ISC BIND 'named' Detection (Remote)`
OID:1.3.6.1.4.1.25623.1.0.10028
Version used: `2019-12-10T15:03:15+0000`

References

```
Other:
  URL:https://www.isc.org/bind/
```

[return to 172.162.217.137]

2.1.44 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
`A telnet server seems to be running on this port`

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

Log (CVSS: 0.0)
NVT: Telnet Banner Reporting

Summary
This scripts reports the received banner of a Telnet service.

Vulnerability Detection Result
Remote Telnet banner:

```
                  _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

Log Method

... continues on next page ...

... continued from previous page ...

Details: Telnet Banner Reporting
OID:1.3.6.1.4.1.25623.1.0.10281
Version used: 2020-03-20T10:26:01+0000

Log (CVSS: 0.0)
NVT: Telnet Service Detection

Summary
This scripts tries to detect a Telnet service running at the remote host.

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

Log Method
Details: Telnet Service Detection
OID:1.3.6.1.4.1.25623.1.0.100074
Version used: 2020-03-21T13:23:23+0000

References
Other:
URL:https://tools.ietf.org/html/rfc854

[return to 172.162.217.137]

2.1.45 Log 25/tcp

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

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

Vulnerability Detection Result
Detected Postfix
Version: unknown
Location: 25/tcp
CPE: cpe:/a:postfix:postfix
Concluded from version/product identification result:
220 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: 2020-03-23T13:51:29+0000

Log (CVSS: 0.0)
NVT: Services

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

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

Log Method
Details: `Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `2019-07-08T14:12:44+0000`

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

Log Method
Details: `SMTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10263
Version used: `2020-03-27T07:53:12+0000`

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

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

Vulnerability Detection Result
```
The certificate of the remote service is self signed.
```

... continues on next page ...

... continued from previous page ...

```
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
subject alternative names (SAN):
None
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 (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method

Details: SSL/TLS: Certificate - Self-Signed Certificate Detection
OID:1.3.6.1.4.1.25623.1.0.103140
Version used: $Revision: 8981 $

References

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

Log (CVSS: 0.0)
NVT: SSL/TLS: Collect and Report Certificate Details

Summary

This script collects and reports the details of all SSL/TLS certificates.
This data will be used by other tests to verify server certificates.

Vulnerability Detection Result

```
The following certificate details of the remote service were collected.
Certificate details:
subject ...: 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
subject alternative names (SAN):
None
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
```

... continues on next page ...

... continued from previous page ...

```
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436
↪DE813CC
```

Log Method
Details: SSL/TLS: Collect and Report Certificate Details
OID:1.3.6.1.4.1.25623.1.0.103692
Version used: 2019-04-04T13:38:03+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Medium Cipher Suites

Summary
This routine reports all Medium SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result

```
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
```

Vulnerability Insight
Any cipher suite considered to be secure for only the next 10 years is considered as medium

Log Method
Details: SSL/TLS: Report Medium Cipher Suites

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.902816
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Non Weak Cipher Suites

Summary
This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Vulnerability Detection Result
'Non Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA

Log Method
Details: SSL/TLS: Report Non Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103441
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites

... continues on next page ...

... continued from previous page ...

Summary
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Vulnerability Detection Result
```
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this serv
↪ice via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
```

Log Method
Details: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.105018
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 0.0)
NVT: SSL/TLS: Report Supported Cipher Suites

Summary
This routine reports all SSL/TLS cipher suites accepted by a service.
As the NVT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result
```
'Strong' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

... continues on next page ...

... continued from previous page ...

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the SSLv3 protocol.
'Anonymous' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5
'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol.
```

... continues on next page ...

... continued from previous page ...

'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_RC4_128_MD5

Log Method
Details: SSL/TLS: Report Supported Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.802067
Version used: 2020-03-31T06:57:15+0000

Log (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher sui
↪tes on port 25/tcp is reported. If too strong cipher suites are configured for
↪ this service the alternative would be to fall back to an even more insecure c
↪leartext communication.
'Weak' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_RC4_128_SHA

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- 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: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2020-03-31T06:57:15+0000

References
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/

Log (CVSS: 0.0)
NVT: SSL/TLS: SMTP 'STARTTLS' Command Detection

Summary
Checks if the remote SMTP server supports SSL/TLS with the 'STARTTLS' command.

Vulnerability Detection Result
The remote SMTP server supports SSL/TLS with the 'STARTTLS' command.
The remote SMTP server is announcing the following available ESMTP commands (EHLO response) before sending the 'STARTTLS' command:
8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, STARTTLS, VRFY
The remote SMTP server is announcing the following available ESMTP commands (EHLO response) after sending the 'STARTTLS' command:
8BITMIME, DSN, ENHANCEDSTATUSCODES, ETRN, PIPELINING, SIZE 10240000, VRFY

Log Method

... continues on next page ...

... continued from previous page ...

Details: SSL/TLS: SMTP 'STARTTLS' Command Detection
OID:1.3.6.1.4.1.25623.1.0.103118
Version used: 2020-03-23T13:51:29+0000

References
Other:
URL:https://tools.ietf.org/html/rfc3207

[return to 172.162.217.137]

2.1.46 Log 3306/tcp

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.

Solution
Solution type: Workaround
Restrict Database access to remote systems.

Affected Software/OS
- MySQL/MariaDB
- IBM DB2
- PostgreSQL
- IBM solidDB
- Oracle Database
- Microsoft SQL Server

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: 2020-03-21T13:23:23+0000

References
Other:

... continues on next page ...

... continued from previous page ...

URL:https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

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

Summary
Detects the installed version of MySQL/MariaDB.
Detect a running MySQL/MariaDB by getting the banner, extract the version from the banner.

Vulnerability Detection Result
Detected MySQL
Version: 5.0.51a-3ubuntu5
Location: 3306/tcp
CPE: cpe:/a:mysql:mysql:5.0.51a
Concluded from version/product identification result:
5.0.51a-3ubuntu5

Log Method
Details: MySQL/MariaDB Detection
OID:1.3.6.1.4.1.25623.1.0.100152
Version used: 2019-11-05T16:13:01+0000

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 MySQL

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

[return to 172.162.217.137]

2.1.47 Log 8787/tcp

Log (CVSS: 0.0)
NVT: Service Detection with 'GET' Request

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

Vulnerability Detection Result
`A Distributed Ruby (dRuby/DRb) service seems to be running on this port.`

Log Method
Details: `Service Detection with 'GET' Request`
OID:1.3.6.1.4.1.25623.1.0.17975
Version used: `2020-03-25T13:50:09+0000`

[return to 172.162.217.137]

2.1.48 Log 3632/tcp

Log (CVSS: 0.0)
NVT: DistCC Detection

Summary
Tries to detect if the remote host is running a DistCC service.

Vulnerability Detection Result
`A DistCC service is running at this port.`

Log Method
Details: `DistCC Detection`
OID:1.3.6.1.4.1.25623.1.0.12638
Version used: `$Revision: 13541 $`

[return to 172.162.217.137]

2.1.49 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

... continues on next page ...

... continued from previous page ...

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: 13541 $

Log (CVSS: 0.0)
NVT: VNC Server and Protocol Version Detection

Summary
The remote host is running a remote display software (VNC) which permits a console to be displayed remotely.
This allows authenticated users of the remote host to take its control remotely.

Vulnerability Detection Result
A VNC server seems to be running on this port.
The version of the VNC protocol is : RFB 003.003

Solution
Make sure the use of this software is done in accordance with your corporate security policy, filter incoming traffic to this port.

Log Method
Details: VNC Server and Protocol Version Detection
OID:1.3.6.1.4.1.25623.1.0.10342
Version used: $Revision: 13541 $

[return to 172.162.217.137]

2.1.50 Log 139/tcp

Log (CVSS: 0.0)
NVT: SMB/CIFS Server Detection

Summary
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Vulnerability Detection Result
A SMB server is running on this port

Log Method
Details: SMB/CIFS Server Detection
OID:1.3.6.1.4.1.25623.1.0.11011

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 13541 $

[return to 172.162.217.137]

2.1.51 Log 1099/tcp

Log (CVSS: 0.0)
NVT: RMI-Registry Detection

Summary
This Script detects the RMI-Registry Service

Vulnerability Detection Result
The RMI-Registry Service is running at this port

Log Method
Details: RMI-Registry Detection
OID:1.3.6.1.4.1.25623.1.0.105839
Version used: $Revision: 13541 $

[return to 172.162.217.137]

2.1.52 Log 2121/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects and reports a FTP Server Banner.

Vulnerability Detection Result
Remote FTP server banner:
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.162.217.137]
This is probably:
- ProFTPD
Server operating system information collected via "SYST" command:
215 UNIX Type: L8

Log Method
Details: FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: 2020-03-24T12:27:11+0000

Log (CVSS: 0.0)
NVT: FTP Missing Support For AUTH TLS

Summary
The remote FTP server does not support the 'AUTH TLS' command.

Vulnerability Detection Result
`The remote FTP server does not support the 'AUTH TLS' command.`

Log Method
Details: `FTP Missing Support For AUTH TLS`
OID:1.3.6.1.4.1.25623.1.0.108553
Version used: `$Revision: 13863 $`

Log (CVSS: 0.0)
NVT: ProFTPD Server Version Detection (Remote)

Summary
This script detects the installed version of ProFTP Server.

Vulnerability Detection Result
```
Detected ProFTPD
Version:       1.3.1
Location:      2121/tcp
CPE:           cpe:/a:proftpd:proftpd:1.3.1
Concluded from version/product identification result:
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.162.217.137]
```

Log Method
Details: `ProFTPD Server Version Detection (Remote)`
OID:1.3.6.1.4.1.25623.1.0.900815
Version used: `2020-03-24T12:27:11+0000`

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 FTP server is running on this port.
Here is its banner :
220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.162.217.137]
```

... continues on next page ...

... continued from previous page ...

Log Method
Details: Services
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: 2019-07-08T14:12:44+0000

[return to 172.162.217.137]

2.1.53 Log 111/tcp

Log (CVSS: 0.0)
NVT: Obtain list of all port mapper registered programs via RPC

Summary
This script calls the DUMP RPC on the port mapper, to obtain the list of all registered programs.

Vulnerability Detection Result

```
These are the registered RPC programs:
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪TCP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/TCP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/TCP
RPC program #100021 version 1 'nlockmgr' on port 51548/TCP
RPC program #100021 version 3 'nlockmgr' on port 51548/TCP
RPC program #100021 version 4 'nlockmgr' on port 51548/TCP
RPC program #100005 version 1 'mountd' (mount showmount) on port 54227/TCP
RPC program #100005 version 2 'mountd' (mount showmount) on port 54227/TCP
RPC program #100005 version 3 'mountd' (mount showmount) on port 54227/TCP
RPC program #100024 version 1 'status' on port 55364/TCP
RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) on port 111/
↪UDP
RPC program #100003 version 2 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 3 'nfs' (nfsprog) on port 2049/UDP
RPC program #100003 version 4 'nfs' (nfsprog) on port 2049/UDP
RPC program #100005 version 1 'mountd' (mount showmount) on port 33986/UDP
RPC program #100005 version 2 'mountd' (mount showmount) on port 33986/UDP
RPC program #100005 version 3 'mountd' (mount showmount) on port 33986/UDP
RPC program #100024 version 1 'status' on port 40851/UDP
RPC program #100021 version 1 'nlockmgr' on port 55765/UDP
RPC program #100021 version 3 'nlockmgr' on port 55765/UDP
RPC program #100021 version 4 'nlockmgr' on port 55765/UDP
```

Log Method
Details: Obtain list of all port mapper registered programs via RPC
OID:1.3.6.1.4.1.25623.1.0.11111
Version used: $Revision: 13541 $

Log (CVSS: 0.0)
NVT: RPC portmapper (TCP)

Summary
This script performs detection of RPC portmapper on TCP.

Vulnerability Detection Result
`RPC portmapper is running on this port.`

Log Method
Details: `RPC portmapper (TCP)`
OID:1.3.6.1.4.1.25623.1.0.108090
Version used: `2020-03-26T06:41:35+0000`

[return to 172.162.217.137]

2.1.54 Log 6000/tcp

Log (CVSS: 0.0)
NVT: X Server Detection

Summary
This plugin detects X Window servers.
X11 is a client - server protocol. Basically, the server is in charge of the screen, and the clients connect to it and send several requests like drawing a window or a menu, and the server sends events back to the clients, such as mouse clicks, key strokes, and so on...
An improperly configured X server will accept connections from clients from anywhere. This allows an attacker to make a client connect to the X server to record the keystrokes of the user, which may contain sensitive information, such as account passwords. This can be prevented by using xauth, MIT cookies, or preventing the X server from listening on TCP (a Unix sock is used for local connections)

Vulnerability Detection Result
```
Detected X Windows Server
Version:       11.0
Location:      6000/tcp
CPE:           cpe:/a:x.org:x11:11.0
Concluded from version/product identification result:
11.0
Extra information:
Server answered with: Client is not authorized
```

Log Method
Details: `X Server Detection`
OID:1.3.6.1.4.1.25623.1.0.10407
Version used: `$Revision: 10123 $`

[return to 172.162.217.137]

2.1.55 Log 513/tcp

Log (CVSS: 0.0) NVT: Service Detection with 'BINARY' Request
Summary This plugin performs service detection. This plugin is a complement of find_service.nasl. It sends a 'BINARY' request to the remaining unknown services and tries to identify them.
Vulnerability Detection Result `A rlogin service seems to be running on this port.`
Log Method Details: `Service Detection with 'BINARY' Request` OID:1.3.6.1.4.1.25623.1.0.108204 Version used: `2020-02-20T07:23:20+0000`

[return to 172.162.217.137]