# OpenVas Vulnerability Report

**HackerTarget.com**

HackerTarget.com hosts the worlds most **trusted open source** vulnerability scanners. Allowing easy access to the process of testing and securing Internet facing systems.

⚠ This report is autogenerated using the OpenVas Security Scanner. No guarantee is made to the accuracy of the information found. See https://hackertarget.com/terms/ for full Terms of Service.

CONFIDENTIAL - This report contains sensitive information and should be stored in a secure location

# Table of Contents

# Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

It only lists hosts that produced issues.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started: **Mon Dec 7 12:51:47 2015 UTC**
Scan ended:
Task:  testasp.vulnweb.com

## Vulnerability Summary

| HIGH 2 | MEDIUM 8 | LOW 0 |
|---|---|---|

Any **HIGH** and **MEDIUM** risk vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be stepping stones to High risk attacks.

## Host Summary

| Host | Start | End | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|---|---|
| **87.230.29.167** | Dec 7, 12:51:52 | (not finished) | 2 | 8 | 0 | 23 | 0 |
| Total: 1 | | | 2 | 8 | 0 | 23 | 0 |

# Results per Host

## Host 87.230.29.167

Scanning of this host started at: Mon Dec 7 12:51:52 2015 UTC
Number of results:  33

### Port Summary for Host 87.230.29.167

| Service (Port) | Threat Level |
|---|---|
| 80/tcp | High |
| 139/tcp | Log |
| 3389/tcp | Medium |
| general/SMBClient | Log |
| 135/tcp | Medium |
| general/icmp | Log |
| general/tcp | Log |
| 8443/tcp | Medium |

## Security Issues for Host 87.230.29.167

| **High** (CVSS: 7.5) | 80/tcp |
| NVT: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139) | |

**Summary**

This script attempts to use SQL injection techniques on CGI scripts

More info at : http://en.wikipedia.org/wiki/SQL_injection

**Vulnerability Detection Result**

The following URLs seem to be vulnerable to various SQL injection
techniques :
/Templatize.asp?item='UNION'
/Templatize.asp?item='
/Templatize.asp?item='%22
/Templatize.asp?item=9%2c+9%2c+9
/Templatize.asp?item='bad_bad_value
/Templatize.asp?item=bad_bad_value'
/Templatize.asp?item='+OR+'
/Templatize.asp?item='WHERE
/Templatize.asp?item=%3B
/Templatize.asp?item='OR
An attacker may exploit this flaws to bypass authentication
or to take the control of the remote database.
Solution: Modify the relevant CGIs so that they properly escape arguments
See also : http://www.securiteam.com/securityreviews/5DP0N1P76E.html

**Solution**

Modify the relevant CGIs so that they properly escape arguments.

**Vulnerability Detection Method**

Details: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139)

Version used: $Revision: 421 $

| **High** (CVSS: 7.5) | 80/tcp |
| NVT: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139) | |

| **High** (CVSS: 7.5) | 80/tcp |
| NVT: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139) | |

**Summary**

This script attempts to use SQL injection techniques on CGI scripts

More info at : http://en.wikipedia.org/wiki/SQL_injection

**Vulnerability Detection Result**

The following URLs seem to be vulnerable to various SQL injection
techniques :
/showforum.asp?id='UNION'
/showforum.asp?id='
/showforum.asp?id='%22
/showforum.asp?id=9%2c+9%2c+9
/showforum.asp?id=9%2c+9%2c+9
/showforum.asp?id='bad_bad_value
/showforum.asp?id=bad_bad_value'
/showforum.asp?id='+OR+'
/showforum.asp?id='WHERE
/showforum.asp?id=%3B
/showforum.asp?id=%3B
/showforum.asp?id='OR
An attacker may exploit this flaws to bypass authentication
or to take the control of the remote database.
Solution: Modify the relevant CGIs so that they properly escape arguments
See also : http://www.securiteam.com/securityreviews/5DP0N1P76E.html

**Solution**

Modify the relevant CGIs so that they properly escape arguments.

**Vulnerability Detection Method**

Details: wpoison (nasl version) (OID: 1.3.6.1.4.1.25623.1.0.11139)

Version used: $Revision: 421 $

| Medium (CVSS: 6.4) | 3389/tcp |
|---|---|
| NVT: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658) | |

**Summary**

This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

Successful exploitation could allow remote attackers to gain sensitive information.

Impact Level: System/Application

**Solution**

**Solution type:** WillNotFix

No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

A Workaround is to connect only to terminal services over trusted networks.

**Affected Software/OS**

All Microsoft-compatible RDP (5.2 or earlier) softwares

**Vulnerability Insight**

The flaw is due to RDP server which stores an RSA private key used for signing a terminal server's public key in the mstlsapi.dll library, which allows remote attackers to calculate a valid signature and further perform a man-in-the-middle (MITM) attacks to obtain sensitive information.

**Vulnerability Detection Method**

Details: Microsoft RDP Server Private Key Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902658)

Version used: $Revision: 1640 $

**References**

CVE:   CVE-2005-1794
BID:   13818
Other: http://secunia.com/advisories/15605/
       http://xforce.iss.net/xforce/xfdb/21954
       http://www.oxid.it/downloads/rdp-gbu.pdf
       http://sourceforge.net/p/xrdp/mailman/message/32732056

## Medium (CVSS: 5.0)
### NVT: IIS Service Pack - 404 (OID: 1.3.6.1.4.1.25623.1.0.11874)

80/tcp

**Summary**

Ensure that the server is running the latest stable Service Pack

**Vulnerability Detection Result**

The remote IIS server *seems* to be Microsoft IIS 6.0 - w2k3 build 3790

**Solution**

**Solution type:** VendorFix

The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk.

Caveat: This test makes assumptions of the remote patch level based on static return values (Content-Length) within the IIS Servers 404 error message. As such, the test can not be totally reliable and should be manually confirmed.

**Vulnerability Detection Method**

Details: IIS Service Pack - 404 (OID: 1.3.6.1.4.1.25623.1.0.11874)

Version used: $Revision: 1782 $

## Medium (CVSS: 5.0)                                                   80/tcp
NVT: Microsoft ASP.NET Information Disclosure Vulnerability (2418042) (OID: 1.3.6.1.4.1.25623.1.0.901161)

**Summary**

This host is missing a critical security update according to Microsoft Bulletin MS10-070.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

Successful exploitation could allow remote attackers to decrypt and gain access to potentially sensitive data encrypted by the server or read data from arbitrary files within an ASP.NET application. Obtained information may aid in further attacks. Impact Level: System/Application

**Solution**

**Solution type:** VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, http://www.microsoft.com/technet/security/bulletin/MS10-070.mspx

**Affected Software/OS**

Microsoft ASP.NET 1.0 Microsoft ASP.NET 4.0 Microsoft ASP.NET 3.5.1 Microsoft ASP.NET 1.1 SP1 and prior Microsoft ASP.NET 2.0 SP2 and prior Microsoft ASP.NET 3.5 SP1 and prior

**Vulnerability Insight**

The flaw is due to an error within ASP.NET in the handling of cryptographic padding when using encryption in CBC mode. This can be exploited to decrypt data via returned error codes from an affected server.

**Vulnerability Detection Method**

Details: Microsoft ASP.NET Information Disclosure Vulnerability (2418042) (OID: 1.3.6.1.4.1.25623.1.0.901161)

Version used: $Revision: 1564 $

**References**

CVE:    CVE-2010-3332
BID:    43316
CERT:  DFN-CERT-2011-0712 , DFN-CERT-2010-1237
Other: http://www.vupen.com/english/advisories/2010/2429
         http://www.microsoft.com/technet/security/bulletin/MS10-070.mspx
         http://www.troyhunt.com/2010/09/fear-uncertainty-and-and-padding-oracle.html
         http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-security-vulnerability.aspx

**Medium** (CVSS: 5.0)                                                     135/tcp
NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

**Summary**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Solution**

filter incoming traffic to this port.

**Vulnerability Detection Method**

Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

Version used: $Revision: 41 $

**Medium** (CVSS: 5.0)                                                     135/tcp
NVT: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

**Summary**

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

**Vulnerability Detection Result**

Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Here is the list of DCE services running on this host:
Port: 1031/tcp
    UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
    Endpoint: ncacn_ip_tcp:87.230.29.167[1031]
    Named pipe : lsass
    Win32 service or process : lsass.exe
    Description : SAM access
Port: 1032/tcp
    UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2
    Endpoint: ncacn_ip_tcp:87.230.29.167[1032]
Solution : filter incoming traffic to this port(s).

**Solution**

filter incoming traffic to this port.

**Vulnerability Detection Method**

Details: DCE Services Enumeration (OID: 1.3.6.1.4.1.25623.1.0.10736)

Version used: $Revision: 41 $

## Medium (CVSS: 4.3)                    8443/tcp
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

**Summary**

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

**Vulnerability Detection Result**

Weak ciphers offered by this service:
  SSL2_RC4_128_MD5
  SSL2_RC4_128_EXPORT40_WITH_MD5
  SSL2_RC2_CBC_128_CBC_WITH_MD5
  SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_64_CBC_SHA
  SSL3_RSA_EXPORT1024_WITH_DES_CBC_SHA, weak authentication
  SSL3_RSA_EXPORT1024_WITH_RC4_56_SHA, weak authentication
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_64_CBC_SHA
  TLS1_RSA_EXPORT1024_WITH_DES_CBC_SHA, weak authentication
  TLS1_RSA_EXPORT1024_WITH_RC4_56_SHA, weak authentication

**Solution**

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

**Vulnerability Insight**

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

- Any SSL/TLS using no cipher is considered weak.

- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.

- RC4 is considered to be weak.

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak.

- 1024 bit RSA authentication is considered to be insecure and therefore as weak.

- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks

- Any cipher considered to be secure for only the next 10 years is considered as medium

- Any other cipher is considered as strong

**Vulnerability Detection Method**

Details: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

Version used: $Revision: 733 $

## Medium (CVSS: 4.3)                                    8443/tcp
## NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

**Summary**

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

**Vulnerability Detection Result**

In addition to TLSv1+ the service is also providing the deprecated SSLv2 and SSLv3 protoco↵
ls and supports one or more ciphers.

**Impact**

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transfered within the secured connection.

**Solution**

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

**Affected Software/OS**

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

**Vulnerability Insight**

The SSLv2 and SSLv3 protocols containing known cryptographic flaws.

**Vulnerability Detection Method**

Check the used protocols of the services provided by this system.

Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Version used: $Revision: 1183 $

**References**

 Other: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-
        parameters-report
        https://bettercrypto.org/

| **Medium** (CVSS: 4.3)<br>NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087) | 8443/tcp |
|---|---|

**Summary**

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

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**

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

Impact Level: Application

**Solution**

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

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

**Affected Software/OS**

OpenSSL through 1.0.1i

**Vulnerability Insight**

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

**Vulnerability Detection Method**

Send a SSLv3 request and check the response.

Details: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087)

Version used: $Revision: 1152 $

**References**

CVE:    CVE-2014-3566

BID:    70574

CERT:   DFN-CERT-2015-1431 , DFN-CERT-2015-1075 , DFN-CERT-2015-1026 , DFN-CERT-2015-0664 , DFN-CERT-2015-0548 , DFN-CERT-2015-0404 , DFN-CERT-2015-0396 , DFN-CERT-2015-0259 , DFN-CERT-2015-0254 , DFN-CERT-2015-0245 , DFN-CERT-2015-0118 , DFN-CERT-2015-0114 , DFN-CERT-2015-0083 , DFN-CERT-2015-0082 , DFN-CERT-2015-0081 , DFN-CERT-2015-0076 , DFN-CERT-2014-1717 , DFN-CERT-2014-1680 , DFN-CERT-2014-1632 , DFN-CERT-2014-1564 , DFN-CERT-2014-1542 , DFN-CERT-2014-1414 , DFN-CERT-2014-1366 , DFN-CERT-2014-1354

Other: http://osvdb.com/113251

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

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

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

        http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

**Log** (CVSS: 0.0)
NVT: OS fingerprinting (OID: 1.3.6.1.4.1.25623.1.0.102002)
general/tcp

**Summary**

This script performs ICMP based OS fingerprinting (as described by Ofir Arkin and Fyodor Yarochkin in Phrack #57). It can be used to determine remote operating system version.

**Vulnerability Detection Result**

ICMP based OS fingerprint results: (100% confidence)
Microsoft Windows

**Log Method**

Details: OS fingerprinting (OID: 1.3.6.1.4.1.25623.1.0.102002)

Version used: $Revision: 1739 $

**References**

 Other: http://www.phrack.org/issues.html?issue=57&amp;id=7#article

**Log** (CVSS: 0.0)
NVT: ICMP Timestamp Detection (OID: 1.3.6.1.4.1.25623.1.0.103190)
general/icmp

**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: 13 $

**References**

 CVE:    CVE-1999-0524
 CERT:  DFN-CERT-2014-0658
 Other: http://www.ietf.org/rfc/rfc0792.txt

**Log** (CVSS: 0.0)
NVT: Traceroute (OID: 1.3.6.1.4.1.25623.1.0.51662)

general/tcp

**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 45.79.134.130 to 87.230.29.167:
45.79.134.130
207.99.53.41
209.123.10.102
209.123.11.142
195.66.225.173
176.28.4.2
176.28.4.114
46.163.104.39
87.230.29.167

**Solution**

Block unwanted packets from escaping your network.

**Log Method**

Details: Traceroute (OID: 1.3.6.1.4.1.25623.1.0.51662)

Version used: $Revision: 975 $

**Log** (CVSS: 0.0)
NVT: SMB Test (OID: 1.3.6.1.4.1.25623.1.0.90011)

general/SMBClient

**Summary**

Test remote host SMB Functions

**Vulnerability Detection Result**

The tool "smbclient" is not available for openvasd.
Therefore none of the tests using smbclient are executed.

**Log Method**

Details: SMB Test (OID: 1.3.6.1.4.1.25623.1.0.90011)

Version used: $Revision: 16 $

**Log** (CVSS: 0.0)                                          80/tcp
NVT: Windows SharePoint Services detection (OID: 1.3.6.1.4.1.25623.1.0.101018)

**Summary**

The remote host is running Windows SharePoint Services. Microsoft SharePoint products and technologies include browser-based collaboration and a document-management platform. These can be used to host web sites that access shared workspaces and documents from a browser.

**Vulnerability Detection Result**

Server: Microsoft-IIS/6.0
Operating System Type: Windows Server 2003 / Windows XP Professional x64
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET

**Solution**

It's recommended to allow connection to this host only from trusted hosts or networks.

**Log Method**

Details: Windows SharePoint Services detection (OID: 1.3.6.1.4.1.25623.1.0.101018)

Version used: $Revision: 1776 $

**Log** (CVSS: 0.0)                                          80/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

**Summary**

This detects the HTTP Server's type and version.

**Vulnerability Detection Result**

The remote web server type is :
Microsoft-IIS/6.0

**Solution**

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

**Log Method**

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 229 $

**Log** (CVSS: 0.0)                                                                          80/tcp
NVT: robot(s).txt exists on the Web Server (OID: 1.3.6.1.4.1.25623.1.0.10302)

**Summary**

Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.

**Vulnerability Detection Result**

The file 'robots.txt' contains the following:
User-agent: *
Disallow: /

**Solution**

Review the content of the robots file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.

**Vulnerability Insight**

Any serious web search engine will honor the /robot(s).txt file and not scan the files and directories listed there.

Any entries listed in this file are not even hidden anymore.

**Log Method**

Details: robot(s).txt exists on the Web Server (OID: 1.3.6.1.4.1.25623.1.0.10302)

Version used: $Revision: 673 $

**Log** (CVSS: 0.0)                                                                          80/tcp
NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

**Summary**

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

**Vulnerability Detection Result**

A web server is running on this port

**Log Method**

Details: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

Version used: $Revision: 69 $

**Log** (CVSS: 0.0)                                                          80/tcp
NVT: Web mirroring (OID: 1.3.6.1.4.1.25623.1.0.10662)

**Summary**

This script makes a mirror of the remote web site and extracts the list of CGIs that are used by the remote host.

It is suggested you allow a long-enough timeout value for this test routine and also adjust the setting on the number of pages to mirror.

**Vulnerability Detection Result**

The following CGI have been discovered :
Syntax : cginame (arguments [default value])
/Login.asp (RetURL [%2FDefault%2Easp%3F] )
/Templatize.asp (item [html/about.html] )
/Register.asp (RetURL [%2FDefault%2Easp%3F] )
/showforum.asp (id [0] )
The following directories have been discovered :
/Images

**Log Method**

Details: Web mirroring (OID: 1.3.6.1.4.1.25623.1.0.10662)

Version used: $Revision: 1825 $

**Log** (CVSS: 0.0)                                                          80/tcp
NVT: Directories used for CGI Scanning (OID: 1.3.6.1.4.1.25623.1.0.111038)

**Summary**

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

**Vulnerability Detection Result**

The following directories are used for CGI scanning:
/scripts
/cgi-bin
/Images
/

**Log Method**

Details: Directories used for CGI Scanning (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 1727 $

**Log** (CVSS: 0.0)     80/tcp
NVT: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

**Summary**

This script detects the installed MS IIS Webserver and sets the result in KB

**Vulnerability Detection Result**

Detected Microsoft IIS Webserver
Version: 6.0
Location: 80/tcp
CPE: cpe:/a:microsoft:iis:6.0
Concluded from version identification result:
IIS/6.0

**Log Method**

Details: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

Version used: $Revision: 1166 $

**Log** (CVSS: 0.0)     139/tcp
NVT: SMB on port 445 (OID: 1.3.6.1.4.1.25623.1.0.11011)

**Summary**

This script detects wether port 445 and 139 are open and if thet are running SMB servers.

**Vulnerability Detection Result**

An SMB server is running on this port

**Log Method**

Details: SMB on port 445 (OID: 1.3.6.1.4.1.25623.1.0.11011)

Version used: $Revision: 41 $

**Log** (CVSS: 0.0)     3389/tcp
NVT: Microsoft Remote Desktop Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.100062)

**Summary**

The Microsoft Remote Desktop Protocol (RDP) is running at this host. Remote Desktop Services, formerly known as Terminal Services, is one of the components of Microsoft Windows (both server and client versions) that allows a user to access applications and data on a remote computer over a network.

**Vulnerability Detection Result**

Vulnerability was detected according to the Vulnerability Detection Method.

**Log Method**

Details: Microsoft Remote Desktop Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.100062)

Version used: $Revision: 15 $

**Log** (CVSS: 0.0)                                                            3389/tcp
NVT: Identify unknown services with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

**Summary**

This plugin performs service detection by launching nmap's service probe against ports running unidentified services.

Description :

This plugin is a complement of find_service.nasl. It launches nmap -sV (probe requests) against ports that are running unidentified services.

**Vulnerability Detection Result**

Nmap service detection result for this port: ms-wbt-server

**Log Method**

Details: Identify unknown services with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286)

Version used: $Revision: 329 $

**Log** (CVSS: 0.0)                                                            8443/tcp
NVT: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

**Summary**

This detects the HTTP Server's type and version.

**Vulnerability Detection Result**

The remote web server type is :
Microsoft-IIS/6.0

**Solution**

Configure your server to use an alternate name like 'Wintendo httpD w/Dotmatrix display' Be sure to remove common logos like apache_pb.gif. With Apache, you can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

**Log Method**

Details: HTTP Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10107)

Version used: $Revision: 229 $

**Log** (CVSS: 0.0)                                                            8443/tcp
NVT: SSL Certificate - Subject Common Name Does Not Match Server FQDN (OID: 1.3.6.1.4.1.25623.1.0.103141)

**Summary**

The SSL certificate contains a common name (CN) that does not match the hostname.

**Vulnerability Detection Result**

Hostname: testasp.vulnweb.com
Common Name: *.kundenadmin.hosteurope.de

**Log Method**

Details: SSL Certificate - Subject Common Name Does Not Match Server FQDN (OID: 1.3.6.1.4.1.25623.1.0.103141)

Version used: $Revision: 1279 $

**Log** (CVSS: 0.0)          8443/tcp
NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

**Summary**

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

**Vulnerability Detection Result**

A TLScustom server answered on this port

**Log Method**

Details: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

Version used: $Revision: 69 $

**Log** (CVSS: 0.0)          8443/tcp
NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

**Summary**

This plugin attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 and set the results in the plugins knowledge base.

**Vulnerability Detection Result**

A web server is running on this port through SSL

**Log Method**

Details: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)

Version used: $Revision: 69 $

**Log** (CVSS: 0.0)          8443/tcp
NVT: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

**Summary**

Remote web server does not reply with 404 error code.

**Vulnerability Detection Result**

This web server is [mis]configured in that it does not return '404 Not Found'
error codes when a non-existent file is requested, perhaps returning
a site map, search page or authentication page instead.
CGI scanning will be disabled for this host.

**Vulnerability Insight**

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

**Log Method**

Details: No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)

Version used: $Revision: 1048 $

**Log** (CVSS: 0.0)                                                                    8443/tcp
NVT: Directories used for CGI Scanning (OID: 1.3.6.1.4.1.25623.1.0.111038)

### Summary

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

### Vulnerability Detection Result

The following directories are used for CGI scanning:
/scripts
/cgi-bin
/

### Log Method

Details: Directories used for CGI Scanning (OID: 1.3.6.1.4.1.25623.1.0.111038)

Version used: $Revision: 1727 $

**Log** (CVSS: 0.0)                                                                    8443/tcp
NVT: Check for SSL Ciphers (OID: 1.3.6.1.4.1.25623.1.0.802067)

### Summary

This routine search for SSL ciphers offered by a service.

### Vulnerability Detection Result

Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  TLS1_RSA_DES_192_CBC3_SHA
Weak ciphers offered by this service:
  SSL2_RC4_128_MD5
  SSL2_RC4_128_EXPORT40_WITH_MD5
  SSL2_RC2_CBC_128_CBC_WITH_MD5
  SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_64_CBC_SHA
  SSL3_RSA_EXPORT1024_WITH_DES_CBC_SHA, weak authentication
  SSL3_RSA_EXPORT1024_WITH_RC4_56_SHA, weak authentication
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_64_CBC_SHA
  TLS1_RSA_EXPORT1024_WITH_DES_CBC_SHA, weak authentication
  TLS1_RSA_EXPORT1024_WITH_RC4_56_SHA, weak authentication
No non-ciphers are supported by this service

### Log Method

Details: Check for SSL Ciphers (OID: 1.3.6.1.4.1.25623.1.0.802067)

Version used: $Revision: 312 $

**Log** (CVSS: 0.0)      8443/tcp
NVT: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

**Summary**

This script detects the installed MS IIS Webserver and sets the result in KB

**Vulnerability Detection Result**

Detected Microsoft IIS Webserver
Version: 6.0
Location: 8443/tcp
CPE: cpe:/a:microsoft:iis:6.0
Concluded from version identification result:
IIS/6.0

**Log Method**

Details: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

Version used: $Revision: 1166 $

**Log** (CVSS: 0.0)      8443/tcp
NVT: Check for SSL Medium Ciphers (OID: 1.3.6.1.4.1.25623.1.0.902816)

**Summary**

This Plugin reports about SSL Medium Ciphers.

**Vulnerability Detection Result**

Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  TLS1_RSA_DES_192_CBC3_SHA

**Log Method**

Details: Check for SSL Medium Ciphers (OID: 1.3.6.1.4.1.25623.1.0.902816)

Version used: $Revision: 12 $

This file was automatically generated.