Network Security Audit

14 April, 2015

Affected Items

Scan of testasp.vulnweb.com

Scan details

Scan information	
Start time	4/14/2015 12:17:58 PM
Finish time	4/14/2015 1:25:21 PM
Scan time	1 hours, 7 minutes

Server information	
Responsive	True

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	25
High	0
Medium	11
Low	0
Informational	14

Affected items

1032/tcp	
Alert group	**Possible Trojan horse(s) detected**
Severity	**Medium**
Description	An unknown service runs on this port. This port is also known to be used by Trojan horses. Check the system if you do not know what service might be opening the port.
Recommendations	Identify the process that is using the port (using netstat or simliar). If a Trojan horse is identified, scan the system for other malware
Alert variants	
Details	An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): Lixy Unless you know what service is opening the port, you'd better check your system Note: It may have been dynamically allocated to some service (e.g. RPC) Solution: If a Trojan horse is identified, scan the system for any other malware

1033/tcp	
Alert group	**Possible Trojan horse(s) detected**
Severity	**Medium**
Description	An unknown service runs on this port. This port is also known to be used by Trojan horses. Check the system if you do not know what service might be opening the port.
Recommendations	Identify the process that is using the port (using netstat or simliar). If a Trojan horse is identified, scan the system for other malware

Alert variants	
Details	An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): Lixy Unless you know what service is opening the port, you'd better check your system Note: It may have been dynamically allocated to some service (e.g. RPC) Solution: If a Trojan horse is identified, scan the system for any other malware

135/tcp

Alert group	**DCE Services Enumeration**
Severity	**Medium**
Description	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.
Recommendations	filter incoming traffic to this port.
Alert variants	
Details	
Details	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: 1032/tcp UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:87.230.29.167[1032] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access Port: 1033/tcp UUID: 82ad4280-036b-11cf-972c-00aa006887b0, version 2 Endpoint: ncacn_ip_tcp:87.230.29.167[1033] Solution : filter incoming traffic to this port(s).

139/tcp

Alert group	**SMB on port 445**
Severity	**Informational**
Description	This script detects wether port 445 and 139 are open and if thet are running SMB servers.
Alert variants	
Details	An SMB server is running on this port

3389/tcp

Alert group	**Microsoft RDP Server Private Key Information Disclosure Vulnerability**
Severity	**Medium**
Description	This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.
Recommendations	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.
Alert variants	
Details	

Alert group	**Microsoft Remote Desktop Protocol Detection**
Severity	**Informational**
Description	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.
Alert variants	
Details	

69/udp

Alert group	**Hillstone Software TFTP Write/Read Request Server Denial Of Service Vulnerability**
Severity	**Medium**
Description	This host is running Hillstone Software TFTP Server and is prone to denial of service vulnerability.
Recommendations	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.
Alert variants	
Details	

80/tcp

Alert group	**Microsoft ASP.NET Information Disclosure Vulnerability (2418042)**
Severity	**Medium**
Description	This host is missing a critical security update according to Microsoft Bulletin MS10-070.
Recommendations	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
Alert variants	
Details	

Alert group	**Microsoft IIS Tilde Character Information Disclosure Vulnerability**
Severity	**Medium**
Description	This host is running Microsoft IIS Webserver and is prone to information disclosure vulnerability.
Recommendations	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.
Alert variants	
Details	

Alert group	**Directory Scanner**
Severity	**Informational**
Description	This plugin attempts to determine the presence of various common dirs on the remote web server
Alert variants	
Details	The following directories were discovered: /cgi-bin, /Templates, /html, /images, /templates While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Alert group	**Microsoft IIS Tilde Character Information Disclosure Vulnerability**
Severity	**Informational**
Description	This host is running Microsoft IIS Webserver and is prone to information disclosure vulnerability.
Recommendations	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.
Alert variants	
Details	File/Folder name found on server starting with :acufor

Alert group	**Microsoft IIS Webserver Version Detection**
Severity	**Informational**
Description	This script detects the installed MS IIS Webserver and sets the result in KB.
Alert variants	
Details	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

Alert group	**robot(s).txt exists on the Web Server**
Severity	**Informational**
Description	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.
Recommendations	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.
Alert variants	
Details	The file 'robots.txt' contains the following: User-agent: * Disallow: /

Alert group	**Web mirroring**
Severity	**Informational**
Description	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.
Alert variants	
Details	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])

Alert group	**Windows SharePoint Services detection**
Severity	**Informational**
Description	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.
Recommendations	It's recommended to allow connection to this host only from trusted hosts or networks.
Alert variants	
Details	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

8443/tcp

Alert group	**Check for SSL Weak Ciphers**
Severity	**Medium**
Description	This routine search for weak SSL ciphers offered by a service.
Recommendations	The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.
Alert variants	
Details	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

Alert group	POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
Severity	**Medium**
Description	This host is installed with OpenSSL and is prone to information disclosure vulnerability.
Recommendations	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
Alert variants	
Details	

Alert group	Check for SSL Medium Ciphers
Severity	**Informational**
Description	This Plugin reports about SSL Medium Ciphers.
Alert variants	
Details	Medium ciphers offered by this service: SSL3_RSA_DES_192_CBC3_SHA TLS1_RSA_DES_192_CBC3_SHA

Alert group	Microsoft IIS Webserver Version Detection
Severity	**Informational**
Description	This script detects the installed MS IIS Webserver and sets the result in KB.
Alert variants	
Details	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

Alert group	SSL Certificate - Subject Common Name Does Not Match Server FQDN
Severity	**Informational**
Description	The SSL certificate contains a common name (CN) that does not match the hostname.
Alert variants	
Details	Hostname: testasp.vulnweb.com Common Name: *.kundenadmin.hosteurope.de

Alert group	Windows SharePoint Services detection
Severity	**Informational**
Description	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.
Recommendations	It's recommended to allow connection to this host only from trusted hosts or networks.
Alert variants	
Details	Server: Microsoft-IIS/6.0 Operating System Type: Windows Server 2003 / Windows XP Professional x64 X-AspNet-Version: 1.1.4322 X-Powered-By: ASP.NET

general/icmp

Alert group	ICMP Timestamp Detection
Severity	**Informational**
Description	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.
Alert variants	
Details	

general/tcp

Alert group	OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)

Severity	**Medium**
Description	This host is installed with OpenSSL and is prone to man in the middle attack.
Recommendations	Remove support for EXPORT_RSA cipher suites from the service. Update to version 0.9.8zd or 1.0.0p or 1.0.1k or later For updates refer to https://www.openssl.org
Alert variants	
Details	EXPORT_RSA cipher suites supported by the remote server: SSLv3: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) SSLv3: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003) TLSv1.0: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) TLSv1.0: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003) TLSv1.1: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) TLSv1.1: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003) TLSv1.2: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0006) TLSv1.2: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0003)

Alert group	**OS fingerprinting**
Severity	**Informational**
Description	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.
Alert variants	
Details	ICMP based OS fingerprint results: (71% confidence) Microsoft Windows