
 Secure Site May-18-2015
Latest Scan Results
My Account
Scan Settings
Upgrade
Security Seal
Contact
News

Show report for host: www.oathkeepersjoco.com (H:0, M:9, L:33)

Scan Results	
Hostname	www.oathkeepersjoco.com
Scan date	2015-05-15
Scan Status	Done
Vulnerability Score	38.74 (F) 
Vulnerability Summary	
High	0
Medium	9 <ul style="list-style-type: none"> Apache Running Version Prior to 2.2.27 Apache Running Version Prior to 2.2.27 Apache Running Version Prior to 2.2.25 Apache Running Version Prior to 2.2.25 Apache Running Version Prior to 2.2.24 Apache Running Version Prior to 2.2.24 Apache Running Version Prior to 2.2.23 Apache Running Version Prior to 2.2.23 Deprecated SSL Protocol Usage
Low	33 <ul style="list-style-type: none"> HTTP CONNECT Proxy Detection FTP Clear Text Authentication TCP Timestamps Retrieval HTTP Packet Inspection HTTP Packet Inspection Supported SSL Ciphers Suites ICMP Echo Request Identify Unknown Services via GET Requests Identify Unknown Services via GET Requests Identify Unknown Services via GET Requests SSL Verification Test TTL Anomaly Detection Rsync Modules Detection rpcinfo -p Information Disclosure rpcinfo -p Information Disclosure rpcinfo -p Information Disclosure rpcinfo -p Information Disclosure Directory Scanner Directory Scanner NTP Variables Reading SSH Detection Nmap HTTP Server Detection HTTP Server Detection SSH Server Detection RPC Portmapper ICMP Timestamp Request Services Services

Scan Results

[Services](#)
[Services](#)
[Services](#)
[Services](#)

Total 42

Vulnerability by Risk Level

Vulnerability by Service

Vulnerability Count

(Displays High and Medium risk vulnerabilities)

Security Testing

Type	Tests	Failed	Passed
Infrastructure Tests	11844	49	11795
Blind SQL Injection	0	0	0
SQL Injection	0	0	0
Cross Site Scripting	0	0	0
Source Disclosure	0	0	0
PHP Code Injection	0	0	0
Windows Command Execution	0	0	0
UNIX Command Execution	0	0	0
UNIX File Disclosure	0	0	0
Windows File Disclosure	0	0	0
Directory Disclosure	0	0	0
Remote File Inclusion	0	0	0
HTTP Header Injection	0	0	0

Medium risk vulnerabilities results for: www.oathkeepersjoco.com

1. **Apache Running Version Prior to 2.2.27 (Medium)** [back](#)

Port: http (80/tcp)

Summary:

Multiple vulnerabilities have been found in Apache:

* The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

* The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

Version source: Server: Apache/2.2.22

Installed version: 2.2.22

Fixed version: 2.2.27

Recommended Solution:

Upgrade to Apache version 2.2.27 or newer.

More information: http://www.apache.org/dist/httpd/CHANGES_2.2.27, and http://httpd.apache.org/security/vulnerabilities_22.html

CVE: [CVE-2013-6438](#)

CVE: [CVE-2014-0098](#)

Test ID: 16698

2. **Apache Running Version Prior to 2.2.27 (Medium)** [back](#)

Port: https (443/tcp)

Summary: Multiple vulnerabilities have been found in Apache: * The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request. * The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation. Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.27
Recommended Solution: Upgrade to Apache version 2.2.27 or newer.
More information: http://www.apache.org/dist/httpd/CHANGES_2.2.27 , and http://httpd.apache.org/security/vulnerabilities_22.html
CVE: CVE-2013-6438
CVE: CVE-2014-0098
Test ID: 16698
3. Apache Running Version Prior to 2.2.25 (Medium) back
Port: https (443/tcp)
Summary: Multiple vulnerabilities have been found in Apache: * mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator. * mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI. Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.25
Recommended Solution: Upgrade to Apache version 2.2.24 or newer.
More information: http://www.apache.org/dist/httpd/CHANGES_2.2.25 , http://httpd.apache.org/security/vulnerabilities_22.html , and http://mail-archives.apache.org/mod_mbox/httpd-announce/201307.mbox/%3C20130710125106.635ba5a2.wrowe@rowe-clan.net%3E
CVE: CVE-2013-1862
CVE: CVE-2013-1896
Test ID: 16103
4. Apache Running Version Prior to 2.2.25 (Medium) back
Port: http (80/tcp)
Summary: Multiple vulnerabilities have been found in Apache: * mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator. * mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI. Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.25
Recommended Solution: Upgrade to Apache version 2.2.24 or newer.
More information: http://www.apache.org/dist/httpd/CHANGES_2.2.25 , http://httpd.apache.org/security/vulnerabilities_22.html , and http://mail-archives.apache.org/mod_mbox/httpd-announce/201307.mbox/%3C20130710125106.635ba5a2.wrowe@rowe-clan.net%3E
CVE: CVE-2013-1862
CVE: CVE-2013-1896
Test ID: 16103
5. Apache Running Version Prior to 2.2.24 (Medium) back

Port:	http (80/tcp)
Summary:	<p>Multiple vulnerabilities have been found in Apache:</p> <ul style="list-style-type: none"> * Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URLs in the mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, and mod_status modules. * Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string. <p>Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.24</p>
Recommended Solution:	Upgrade to Apache version 2.2.24 or newer.
More information:	http://www.apache.org/dist/httpd/CHANGES_2.2.24 , and http://httpd.apache.org/security/vulnerabilities_22.html
CVE:	CVE-2012-3499
CVE:	CVE-2012-4558
Test ID:	16102
6. Apache Running Version Prior to 2.2.24 (Medium) back	
Port:	https (443/tcp)
Summary:	<p>Multiple vulnerabilities have been found in Apache:</p> <ul style="list-style-type: none"> * Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URLs in the mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, and mod_status modules. * Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string. <p>Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.24</p>
Recommended Solution:	Upgrade to Apache version 2.2.24 or newer.
More information:	http://www.apache.org/dist/httpd/CHANGES_2.2.24 , and http://httpd.apache.org/security/vulnerabilities_22.html
CVE:	CVE-2012-3499
CVE:	CVE-2012-4558
Test ID:	16102
7. Apache Running Version Prior to 2.2.23 (Medium) back	
Port:	https (443/tcp)
Summary:	<p>Multiple vulnerabilities have been discovered in Apache:</p> <ul style="list-style-type: none"> * envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl. * Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list. <p>Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.23</p>
Recommended Solution:	Upgrade to Apache version 2.2.23 or newer.
More information:	http://www.apache.org/dist/httpd/CHANGES_2.2.23 and http://httpd.apache.org/security/vulnerabilities_22.html
CVE:	CVE-2012-0883
CVE:	CVE-2012-2687
Test ID:	15084

8. Apache Running Version Prior to 2.2.23 (Medium) back	
Port:	http (80/tcp)
Summary:	
Multiple vulnerabilities have been discovered in Apache:	
* envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.	
* Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.	
Version source: Server: Apache/2.2.22 Installed version: 2.2.22 Fixed version: 2.2.23	
Recommended Solution:	
Upgrade to Apache version 2.2.23 or newer.	
More information:	http://www.apache.org/dist/httpd/CHANGES_2.2.23 and http://httpd.apache.org/security/vulnerabilities_22.html
CVE:	CVE-2012-0883
CVE:	CVE-2012-2687
Test ID:	15084
9. Deprecated SSL Protocol Usage (Medium) back	
Port:	https (443/tcp)
Summary:	
The remote service accepts connections encrypted using SSLv2 and/or SSLv3, which reportedly suffers from several cryptographic flaws and has been deprecated for several years. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.	
Recommended Solution:	
Consult the application's documentation to disable SSL 2.0 and SSL 3.0, and use TLS 1.0 or newer.	
More information:	http://www.schneier.com/paper-ssl.pdf
Test ID:	9329

Low risk vulnerabilities results for: www.oathkeepersjoco.com	
1. HTTP CONNECT Proxy Detection (Low) back	
Port:	http-alt (8080/tcp)
Summary:	
The remote service supports the HTTP CONNECT method for tunneling connections through an HTTP connection.	
Test ID:	11346
2. FTP Clear Text Authentication (Low) back	
Port:	ftp (21/tcp)
Summary:	
The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.	
Recommended Solution:	
Switch to FTPS (FTP over SSL/TLS) or SFTP (part of the SSH suite).	
Test ID:	11278
3. TCP Timestamps Retrieval (Low) back	
Port:	general/tcp
Summary:	
The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can be sometimes be computed.	
The uptime was estimated to 346187s, i.e. about 4 days. (Note that the clock is running at about 300 Hz and will overflow in about 14316556s, that is 165 days)	
More information:	http://www.ietf.org/rfc/rfc1323.txt
Test ID:	10399

4. HTTP Packet Inspection (Low)	back
Port: http (80/tcp)	
Summary:	
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.	
Protocol version: HTTP/1.1 SSL: no Pipelining: yes Keep-Alive: yes Options allowed: (Not implemented) Headers: Date: Fri, 15 May 2015 22:29:23 GMT Server: Apache/2.2.22 (Debian) X-Powered-By: PHP/5.5.20-1~dotdeb.1 Vary: Accept-Encoding Keep-Alive: timeout=15, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html X-Pad: avoid browser bug	
Test ID: 10209	
5. HTTP Packet Inspection (Low)	back
Port: https (443/tcp)	
Summary:	
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.	
Protocol version: HTTP/1.1 SSL: yes Pipelining: yes Keep-Alive: yes Options allowed: (Not implemented) Headers: Date: Fri, 15 May 2015 22:29:23 GMT Server: Apache/2.2.22 (Debian) X-Powered-By: PHP/5.5.20-1~dotdeb.1 Vary: Accept-Encoding Keep-Alive: timeout=15, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html X-Pad: avoid browser bug	
Test ID: 10209	
6. Supported SSL Ciphers Suites (Low)	back
Port: https (443/tcp)	
Summary:	
This test detects which SSL ciphers are supported by remote service for encrypting communications.	
Here is the list of SSL ciphers supported by the remote server:	
- High Strength Ciphers (>= 112-bit key)	
* SSLv3 - EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1	
* SSLv3 - DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1	
* SSLv3 - RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1	
* TLSv1 - EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1	
* TLSv1 - DHE-RSA-AES128-SHA Kx=DH Au=RSA Enc=AES(128) Mac=SHA1	
* TLSv1 - DHE-RSA-AES256-SHA Kx=DH Au=RSA Enc=AES(256) Mac=SHA1	
* TLSv1 - n/a Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1	
* TLSv1 - n/a Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1	
* TLSv1 - n/a Kx=DH Au=RSA Enc=SEED(128) Mac=SHA1	
* TLSv1 - n/a Kx=ECDH Au=RSA Enc=3DES(168) Mac=SHA1	
* TLSv1 - n/a Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1	
* TLSv1 - n/a Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1	
* TLSv1 - n/a Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1	
* TLSv1 - DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1	
* TLSv1 - AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1	
* TLSv1 - AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1	
* TLSv1 - n/a Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1	
* TLSv1 - n/a Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1	
* TLSv1 - RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1	
* TLSv1 - n/a Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1	
The fields above are:	

* {OpenSSL ciphername}
 * Kx={key exchange}
 * Au={authentication}
 * Enc={symmetric encryption method}
 * Mac={message authentication code}
 * {export flag}

More information: <http://www.openssl.org/docs/apps/ciphers.html>

Test ID: 9819

7. ICMP Echo Request (Low) [back](#)

Port: general/icmp

Summary:

The remote host answers an ICMP echo request (ping).

Recommended Solution:

Filter out the ICMP echo requests (8)

Impact:

The remote host answers ping, an attacker can use this to determine the host is running.

Test ID: 9507

8. Identify Unknown Services via GET Requests (Low) [back](#)

Port: https (443/tcp)

Summary:

This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

A web server is running on this port

Test ID: 8434

9. Identify Unknown Services via GET Requests (Low) [back](#)

Port: http (80/tcp)

Summary:

This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

A web server is running on this port

Test ID: 8434

10. Identify Unknown Services via GET Requests (Low) [back](#)

Port: ssh (22/tcp)

Summary:

This test is a complement of Service test, as it tries recognize more banners and use an HTTP request if necessary.

A SSH server is running on this port

Test ID: 8434

11. SSL Verification Test (Low) [back](#)

Port: https (443/tcp)

Summary:

This test connects to a SSL server, and checks its certificate and the available (shared) SSLv2 ciphers. Weak (export version) ciphers are reported as problematic.

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

52:28:f5:26:7d:a8:0b:1a:03:92:0f:49:b4:70:0a:39

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA

Validity

Not Before: Apr 10 00:00:00 2015 GMT

Not After : Apr 9 23:59:59 2016 GMT

Subject: OU=Domain Control Validated, OU=PositiveSSL, CN=www.oathkeepersjoco.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c1:1b:dc:db:06:85:70:6c:82:bd:67:12:88:17:

19:48:3f:90:e5:55:2c:24:05:ad:29:c6:7e:35:51:

77:24:40:35:47:03:6f:74:cf:cd:e0:ec:af:1e:a5:
a2:97:1d:26:87:26:89:7e:29:31:a9:2f:99:9b:cd:
15:3a:16:c5:a9:f5:89:20:c2:70:cf:c2:fa:4d:b2:
ac:33:f4:c3:f0:e2:e0:ea:d1:a8:b2:c3:41:2c:72:
b3:76:12:61:91:f0:56:04:aa:7e:a1:51:a2:bc:2c:
aa:f7:7c:86:04:76:6d:2a:93:27:bf:1c:1a:31:91:
52:e5:71:c7:be:c6:8b:18:53:5d:05:40:04:91:e2:
fd:36:2d:71:1e:91:ec:97:b1:17:a0:af:2f:a1:b8:
25:a7:a2:4c:82:70:23:55:a2:3f:60:e2:52:3e:25:
f6:94:aa:d1:a9:c7:33:2e:58:9e:2b:be:ce:ee:ee:
a4:3a:94:db:f4:05:63:4e:ef:dd:13:19:f1:cf:b6:
73:49:32:6e:1c:fd:0c:84:bd:24:b0:31:a4:56:5c:
7b:8c:1b:1f:7d:d0:b7:35:87:b3:db:d3:26:db:48:
99:4c:88:cc:96:b0:29:bc:93:45:28:a7:61:62:e6:
98:61:b1:9f:8a:47:00:9e:eb:df:bc:19:b7:97:83:
d6:f3

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:90:AF:6A:3A:94:5A:0B:D8:90:EA:12:56:73:DF:43:B4:3A:28:DA:E7

X509v3 Subject Key Identifier:

2D:0F:99:19:12:75:40:00:14:CA:76:B3:D0:39:D2:74:80:10:D5:FE

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.6449.1.2.2.7

CPS: https://secure.comodo.com/CPS

Policy: 2.23.140.1.2.1

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl

Authority Information Access:

CA Issuers - URI:http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt

OCSP - URI:http://ocsp.comodoca.com

X509v3 Subject Alternative Name:

DNS:www.oathkeepersjoco.com, DNS:oathkeepersjoco.com

Signature Algorithm: sha256WithRSAAEncryption

5e:12:06:f5:12:2e:3b:d8:4d:56:9a:99:d0:cf:53:7e:0f:ab:
ea:ad:ed:5b:ce:6a:e1:cc:13:f9:02:75:f2:2c:fd:04:43:e2:
32:83:06:56:d4:23:11:fd:0c:06:c8:c3:d0:8b:43:a7:fb:08:
29:34:13:67:1c:17:bf:cd:03:84:ce:67:fe:0d:71:7e:b0:bd:
40:88:97:5f:6f:48:45:4d:4a:34:1a:89:4a:f6:5e:c3:e7:a2:
b2:fe:56:0f:db:52:5c:03:95:03:d8:cd:71:f6:f4:0a:0b:6b:
e7:10:3c:ea:23:0a:80:f2:d1:8d:37:2d:13:32:b4:bb:35:72:
d7:25:21:8f:07:fc:ef:2e:42:bf:0c:29:80:32:81:a0:2a:52:
43:82:b0:db:12:d0:19:3d:1a:db:4e:cf:92:53:9a:78:a5:8f:
76:70:23:7b:43:72:87:f6:3a:82:da:eb:2c:2c:08:25:8f:cb:
fa:0a:bb:13:db:aa:03:9c:08:70:e6:35:07:0c:67:5b:ef:00:
46:f9:30:43:7b:9c:b8:33:9c:ca:1b:f5:01:8b:66:f6:64:4a:
78:77:a7:a7:bf:68:60:d6:5e:54:88:13:ac:d0:6c:23:4f:6a:
10:1f:d2:6e:73:1e:9b:86:0d:70:13:a3:39:fc:87:19:2e:21:
56:19:c6:0e

This SSLv2 server also accepts SSLv3 connections.

This SSLv2 server also accepts TLSv1 connections.

Recommended Solution:

Usage of weak ciphers should be avoided.

Test ID: 2804

12. TTL Anomaly Detection (Low)

[back](#)

Port: general/tcp

Summary:

The remote host, when queried on open ports, replies with differing TTL values. This could be an indicator that a transparent proxy is on the way, or that this host is a forwarding router, honeypot, etc...

Recommended Solution:

Contact vendor for information on closing up this information leak.

Impact:

An attacker may use this information to find critical systems on your network.

Test ID:	2711
13. Rsync Modules Detection (Low) back	
Port:	rsync (873/tcp)
Summary:	rsync is an open source utility that provides fast incremental file transfer. This test is able to extract rsync modules available on a remote server.
Recommended Solution:	If the rsync server contains sensitive information/modules/files, access to it should be limited.
Test ID:	2358
14. rpcinfo -p Information Disclosure (Low) back	
Port:	unknown (53695/udp)
Summary:	This test calls the DUMP RPC on the port mapper, to obtain the list of all registered programs. This is what we found: RPC program #100024 version 1 'status' is running on this port
Impact:	Attackers can gain critical information about the host.
Test ID:	1898
15. rpcinfo -p Information Disclosure (Low) back	
Port:	sunrpc (111/udp)
Summary:	This test calls the DUMP RPC on the port mapper, to obtain the list of all registered programs. This is what we found: RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
Impact:	Attackers can gain critical information about the host.
Test ID:	1898
16. rpcinfo -p Information Disclosure (Low) back	
Port:	unknown (34404/tcp)
Summary:	This test calls the DUMP RPC on the port mapper, to obtain the list of all registered programs. This is what we found: RPC program #100024 version 1 'status' is running on this port
Impact:	Attackers can gain critical information about the host.
Test ID:	1898
17. rpcinfo -p Information Disclosure (Low) back	
Port:	sunrpc (111/tcp)
Summary:	This test calls the DUMP RPC on the port mapper, to obtain the list of all registered programs. This is what we found: RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
Impact:	Attackers can gain critical information about the host.
Test ID:	1898
18. Directory Scanner (Low) back	
Port:	http (80/tcp)
Summary:	We found some common directories on the web server: The following directories were discovered: /downloads, /icons
Recommended Solution:	Check if those directories contain any sensitive information, if they do, prevent unauthorized access to them.
Impact:	

This is usually not a security vulnerability, only an information gathering. Nevertheless, you should manually inspect these directories to ensure that they are in compliance with accepted security standards.

Test ID: 1822

19. Directory Scanner (Low)

[back](#)

Port: https (443/tcp)

Summary:

We found some common directories on the web server:
The following directories were discovered:
/downloads, /icons

Recommended Solution:

Check if those directories contain any sensitive information, if they do, prevent unauthorized access to them.

Impact:

This is usually not a security vulnerability, only an information gathering. Nevertheless, you should manually inspect these directories to ensure that they are in compliance with accepted security standards.

Test ID: 1822

20. NTP Variables Reading (Low)

[back](#)

Port: ntp (123/udp)

Summary:

It is possible to determine a lot of information about the remote host by querying the NTP variables - these include OS descriptor, and time settings.

Theoretically one could work out the NTP peer relationships and track back network settings from this.

Recommended Solution:

Set NTP to restrict default access to ignore all info packets: restrict default ignore

Impact:

Attackers can gain critical information about the host.

Test ID: 1653

21. SSH Detection (Low)

[back](#)

Port: ssh (22/tcp)

Summary:

The remote SSH daemon supports the following versions of the SSH protocol:
. 1.99
. 2.0

Test ID: 1642

22. Nmap (Low)

[back](#)

Port: general/tcp

Summary:

Nmap found that this host has an uptime of 3.953 days

(Note that operating system guessing is not completely accurate, and is meant to give a picture of what the attacker may see)

Recommended Solution:

Make sure you applied the latest patches/service pack to your operating system.

Test ID: 1043

23. HTTP Server Detection (Low)

[back](#)

Port: https (443/tcp)

Summary:

We were able to detect your web server type and version.

Recommended Solution:

Configure your server to use an alternate name like:
'Wintendo httpd with Dotmatrix display'. See the URL below for more information.

For Apache, add the lines:
ServerSignature Off
ServerTokens Prod
in httpd.conf

For IIS, you can use URLScan to hide the IIS version number.

Impact:

Attackers can gain critical information about the host.

More information:	http://www.securiteam.com/securitynews/5RP0L1540K.html
Test ID:	1035
24. HTTP Server Detection (Low) back	
Port:	http (80/tcp)
Summary:	
We were able to detect your web server type and version.	
Recommended Solution:	
Configure your server to use an alternate name like: 'Wintendo httpd with Dotmatrix display'. See the URL below for more information.	
For Apache, add the lines: ServerSignature Off ServerTokens Prod in httpd.conf	
For IIS, you can use URLScan to hide the IIS version number.	
Impact:	
Attackers can gain critical information about the host.	
More information:	http://www.securiteam.com/securitynews/5RP0L1540K.html
Test ID:	1035
25. SSH Server Detection (Low) back	
Port:	ssh (22/tcp)
Summary:	
An SSH daemon was detected and the following banner was received: SSH version: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2 SSH supported authentication: publickey,password,hostbased	
Recommended Solution:	
Make sure this doesn't include information about the server's type or version. Change it to something generic like 'welcome'.	
Test ID:	942
26. RPC Portmapper (Low) back	
Port:	sunrpc (111/udp)
Summary:	
The RPC portmapper (portmap(8)) is a server that converts RPC program numbers into TCP/IP (or UDP/IP) protocol port numbers.	
Recommended Solution:	
If RPC services are not used on this machine, close this service. Otherwise filter traffic to this port to allow access only from trusted machines.	
Impact:	
An attacker may use it to enumerate RPC services.	
CVE:	CVE-1999-0632
CVE:	CVE-1999-0189
Test ID:	901
27. ICMP Timestamp Request (Low) back	
Port:	general/icmp
Summary:	
The remote host answers to an ICMP timestamp request. This allows an attacker to know the time and date on your host.	
Recommended Solution:	
See solution provided at: http://www.beyondsecurity.com/faq/questions/54/how-can-i-mitigate-icmp-timestamp	
Impact:	
This may help attackers to defeat time based authentications schemes.	
CVE:	CVE-1999-0524
Test ID:	811
28. Services (Low) back	
Port:	https (443/tcp)
Summary:	
A web server is running on this port through SSL	
Test ID:	772

29. Services (Low)	back
Port: https (443/tcp)	
Summary:	
A SSLv2 server answered on this port	
Test ID: 772	
30. Services (Low)	back
Port: rsync (873/tcp)	
Summary:	
An rsync server is running on this port	
Test ID: 772	
31. Services (Low)	back
Port: http (80/tcp)	
Summary:	
A web server is running on this port	
Test ID: 772	
32. Services (Low)	back
Port: ssh (22/tcp)	
Summary:	
An ssh server is running on this port	
Test ID: 772	
33. Services (Low)	back
Port: ftp (21/tcp)	
Summary:	
An FTP server is running on this port. Here is its banner :	
220 (vsFTPD 2.3.5)	
Test ID: 772	

None risk vulnerabilities results for: www.oathkeepersjoco.com

1. Scan Information (None)	back
Port: general/tcp	
Summary:	
Scanner IP: 10.69.177.153 Target IP: 50.116.23.136 Target Hostname: www.oathkeepersjoco.com	
Test ID: 9162	
2. Open Port (None)	back
Port: ssh (22/tcp)	
Summary:	
Test ID: 719	
3. Open Port (None)	back
Port: ftp (21/tcp)	
Summary:	
Test ID: 719	
4. Open Port (None)	back
Port: http (80/tcp)	
Summary:	
Test ID: 719	
5. Open Port (None)	back
Port: rsync (873/tcp)	
Summary:	
Test ID: 719	

6. Open Port (None) back	
Port:	https (443/tcp)
Summary:	
Test ID:	719
7. Open Port (None) back	
Port:	rpcbind (111/tcp)
Summary:	
Test ID:	719

DISCLAIMER: This report is not meant as an exhaustive analysis of the level of security now present on the tested host, and the data shown here should not be used exclusively to judge the security level of any computer system. This scan was performed automatically, and unlike a manual penetration test it does not reveal all the possible security holes present in the system. Some vulnerabilities that were found might be 'false alarms'. The information in this report is provided "as is" and no liability for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages will be accepted.

Review our [Privacy Policy](#), [Terms of Use](#) © Copyright 1998-2015 Beyond Security. All rights reserved.