Scan Report

February 20, 2018

Summary

This document reports on the results of an automatic security scan. The scan started at Tue Feb 20 13:42:54 2018 UTC and ended at Tue Feb 20 13:56:42 2018 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
192.168.1.10 (rome.secnet)	Severity: High	3	3	1	60	0
Total: 1		3	3	1	60	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 67 results selected by the filtering described above. Before filtering there were 67 results.

2 Results per Host

2.1 192.168.1.10

Host scan start	Tue Feb 20 13:43:00 2018 UTC
Host scan end	Tue Feb 20 13:56:41 2018 UTC

Service (Port)	Threat Level
http-alt (8080/tcp)	High
imap (143/tcp)	High
pop3 (110/tcp)	High
general/tcp	Medium
imaps (993/tcp)	Medium
pop3s (995/tcp)	Medium
domain (53/tcp)	Low
http-alt (8080/tcp)	Log
imap (143/tcp)	Log
pop3 (110/tcp)	Log
general/tcp	Log
imaps (993/tcp)	Log
pop3s (995/tcp)	Log
domain (53/tcp)	Log
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/icmp	Log
http (80/tcp)	Log
microsoft-ds (445/tcp)	Log

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
netbios-ssn (139/tcp)	Log
ssh (22/tcp)	Log

2.1.1 High http-alt (8080/tcp)

High (CVSS: 6.8)
NVT: Apache Tomcat servlet/JSP container default files

```
Default files, such as documentation, default Servlets and JSPs were found on
the Apache Tomcat servlet/JSP container.
Remove default files, example JSPs and Servlets from the Tomcat
Servlet/JSP container.
These files should be removed as they may help an attacker to guess the
exact version of Apache Tomcat which is running on this host and may provide
other useful information.
The following default files were found :
/examples/servlets/index.html
/examples/jsp/snp/snoop.jsp
/examples/jsp/index.html
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.12085

[return to 192.168.1.10]

2.1.2 High imap (143/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References

```
CVE: CVE-2014-0224
BID:67899
Other:
  URL:http://www.securityfocus.com/bid/67899
   URL:http://openssl.org/
```

[return to 192.168.1.10]

2.1.3 High pop3 (110/tcp)

High (CVSS: 6.8)
NVT: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)

OID of test routine: 1.3.6.1.4.1.25623.1.0.105043

References
CVE: CVE-2014-0224
BID:67899
Other:
URL:http://www.securityfocus.com/bid/67899
URL:http://openssl.org/

[return to 192.168.1.10]

2.1.4 Medium general/tcp

Medium (CVSS: 2.6)
NVT: TCP timestamps

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 363780014
Paket 2: 363780122
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

References
Other:
URL:http://www.ietf.org/rfc/rfc1323.txt

[return to 192.168.1.10]

2.1.5 Medium imaps (993/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

[return to 192.168.1.10]

2.1.6 Medium pop3s (995/tcp)

Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

```
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
```

... continues on next page ...

... continued from previous page ...

```
TLS1_RSA_RC2_40_MD5
TLS1_RSA_DES_40_CBC_SHA
TLS1_EDH_RSA_DES_40_CBC_SHA
TLS1_ADH_RC4_40_MD5
TLS1_ADH_RC4_128_MD5
TLS1_ADH_DES_40_CBC_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103440

[return to 192.168.1.10]

2.1.7 Low domain (53/tcp)

Low (CVSS: 5.0)
NVT: Determine which version of BIND name daemon is running

```
BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
The BIND based NAMED 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.
The remote bind version is : 9.7.0-P1
Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 192.168.1.10]

2.1.8 Log http-alt (8080/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log NVT:
Open port. OID of test routine: 0

Log NVT:
Open port. OID of test routine: 0

Log NVT:
Open port. OID of test routine: 0

[return to 192.168.1.10]

2.1.9 Log imap (143/tcp)

Log NVT:
Open port. OID of test routine: 0

Log NVT:
Open port.

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: IMAP STARTTLS Detection

```
Summary:
The remote IMAP Server supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105007

[return to 192.168.1.10]

2.1.10 Log pop3 (110/tcp)

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: POP3 STARTTLS Detection

```
Summary:
The remote POP3 Server supports the STARTTLS command.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.105008

[return to 192.168.1.10]

2.1.11 Log general/tcp

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 192.168.1.1 to 192.168.1.10:
192.168.1.1
192.168.1.10
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: Simple TCP portscan in NASL

```
Host have 10 TCP port(s) open in given port range.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80112

Log (CVSS: 0.0)
NVT: Simple TCP portscan in NASL

```
This portscanner is EXPERIMENTAL and you should NOT RELY ON it if you don't know
↪ what you're doing. If you are sure what you're doing - you should turn on exp
↪erimental_scripts option in preferences in order to turn off this warning.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80112

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

```
Open TCP ports: 80, 110, 445, 993, 22, 8080, 995, 139, 53, 143
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 192.168.1.10]

2.1.12 Log imaps (993/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Check for SSL Ciphers

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Log (CVSS: 0.0)
NVT: Check for SSL Medium Ciphers

```
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.13 Log pop3s (995/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: Check for SSL Ciphers

```
Service supports SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
Weak ciphers offered by this service:
  SSL3_RSA_RC4_40_MD5
  SSL3_RSA_RC4_128_MD5
  SSL3_RSA_RC4_128_SHA
  SSL3_RSA_RC2_40_MD5
  SSL3_RSA_DES_40_CBC_SHA
  SSL3_EDH_RSA_DES_40_CBC_SHA
  SSL3_ADH_RC4_40_MD5
  SSL3_ADH_RC4_128_MD5
  SSL3_ADH_DES_40_CBC_SHA
  TLS1_RSA_RC4_40_MD5
  TLS1_RSA_RC4_128_MD5
  TLS1_RSA_RC4_128_SHA
  TLS1_RSA_RC2_40_MD5
```

... continues on next page ...

... continued from previous page ...

```
  TLS1_RSA_DES_40_CBC_SHA
  TLS1_EDH_RSA_DES_40_CBC_SHA
  TLS1_ADH_RC4_40_MD5
  TLS1_ADH_RC4_128_MD5
  TLS1_ADH_DES_40_CBC_SHA
No non-ciphers are supported by this service
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.802067

Log (CVSS: 0.0)
NVT: Check for SSL Medium Ciphers

```
Medium ciphers offered by this service:
  SSL3_RSA_DES_192_CBC3_SHA
  SSL3_EDH_RSA_DES_192_CBC3_SHA
  SSL3_ADH_DES_192_CBC_SHA
  SSL3_DHE_RSA_WITH_AES_128_SHA
  SSL3_ADH_WITH_AES_128_SHA
  TLS1_RSA_DES_192_CBC3_SHA
  TLS1_EDH_RSA_DES_192_CBC3_SHA
  TLS1_ADH_DES_192_CBC_SHA
  TLS1_DHE_RSA_WITH_AES_128_SHA
  TLS1_ADH_WITH_AES_128_SHA
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.902816

[return to 192.168.1.10]

2.1.14 Log domain (53/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.15 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 192.168.1.10]

2.1.16 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
192.168.1.10|cpe:/a:samba:samba:3.4.7
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 192.168.1.10]

2.1.17 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:192.168.1.1,192.168.1.10
TCP ports:80,110,445,993,22,8080,995,139,53,143
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 192.168.1.10]

2.1.18 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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103190

References

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

[return to 192.168.1.10]

2.1.19 Log http (80/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

. . . continues on next page . . .

... continued from previous page ...

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

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

```
The remote web server type is :
Apache/2.2.14 (Ubuntu)
Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10107

Log (CVSS: 0.0)
NVT: Directory Scanner

```
The following directories were discovered:
/cgi-bin, /icons
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
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.11032

References

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

[return to 192.168.1.10]

2.1.20 Log microsoft-ds (445/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log (CVSS: 0.0)
NVT: SMB NativeLanMan

. . . continues on next page . . .

... continued from previous page ...

```
 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.Detected SMB workgroup: WORKGROUP
Detected SMB server: Samba 3.4.7
Detected OS: Unix
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102011

[return to 192.168.1.10]

2.1.21 Log netbios-ssn (139/tcp)

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log
NVT:

```
Open port.
```

OID of test routine: 0

Log NVT:
Open port. OID of test routine: 0

[return to 192.168.1.10]

2.1.22 Log ssh (22/tcp)

Log NVT:
Open port. OID of test routine: 0

Log NVT:
Open port. OID of test routine: 0

Log NVT:
Open port. OID of test routine: 0

Log NVT:
Open port.

. . . continues on next page . . .

. . . continued from previous page . . .

OID of test routine: 0

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

```
The remote SSH Server supports the following SSH Protocol Versions:
1.99
2.0
SSHv2 Fingerprint: 0c:d8:26:b3:dd:f0:d4:83:57:95:78:f8:5a:0c:ae:53
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100259

[return to 192.168.1.10]