Scan Report

October 30, 2018

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 "scan2". The scan started at Tue Oct 30 10:41:20 2018 UTC and ended at Tue Oct 30 11:33:40 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	High	Medium	Low	Log	False Positive
172.16.0.22	4	14	1	0	0
172.16.0.23	2	3	1	0	0
172.16.0.8	3	8	3	0	0
172.16.0.16	0	13	6	0	0
172.16.0.20	0	2	1	0	0
172.16.0.11	0	1	2	0	0
172.16.0.1 _gateway	0	0	1	0	0
172.16.0.21	0	0	1	0	0
Total: 8	9	41	16	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 66 results selected by the filtering described above. Before filtering there were 803 results.

1.1 Host Authentications

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

2 Results per Host

2.1 172.16.0.22

Host scan start Tue Oct 30 10:41:31 2018 UTC
Host scan end Tue Oct 30 11:21:30 2018 UTC

Service (Port)	Threat Level
80/tcp	High
445/tcp	High

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
9/tcp	High
7/tcp	Medium
135/tcp	Medium
22/tcp	Medium
17/tcp	Medium
443/tcp	Medium
3389/tcp	Medium
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

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

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and install the hotfixes from the referenced advisory.

Affected Software/OS
Microsoft Windows 8 x32/x64
Microsoft Windows 8.1 x32/x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: `MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)`
OID:1.3.6.1.4.1.25623.1.0.105257

... continues on next page ...

... continued from previous page ...

Version used: $Revision: 11872 $

References
CVE: CVE-2015-1635
Other:
URL:https://support.microsoft.com/kb/3042553
URL:https://technet.microsoft.com/library/security/MS15-034
URL:http://pastebin.com/ypURDPc4

[return to 172.16.0.22]

2.1.2 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

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

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

... continues on next page ...

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.810676
Version used: $Revision: 11874 $

References
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, ↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
URL:https://support.microsoft.com/en-in/kb/4013078
URL:https://technet.microsoft.com/library/security/MS17-010
URL:https://github.com/rapid7/metasploit-framework/pull/8167/files

High (CVSS: 7.5)
NVT: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability

Summary
The host is running SMB/NETBIOS and prone to an authentication bypass vulnerability

Vulnerability Detection Result
It was possible to login at the share 'IPC$' with an empty login and password.

Impact
Successful exploitation could allow attackers to use shares to cause the system to crash.

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.
A workaround is to,
- Disable null session login.
- Remove the share.
- Enable passwords on the share.

Affected Software/OS
Microsoft Windows 95,
Microsoft Windows 98,
Microsoft Windows NT.
Other Windows implementations / versions might be affected as well.

Vulnerability Insight
The flaw is due to an SMB share, allows full access to Guest users. If the Guest account is enabled, anyone can access the computer without a valid user account or password.

Vulnerability Detection Method
Details: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability

... continues on next page ...

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.801991
Version used: $Revision: 11997 $

References
CVE: CVE-1999-0519
Other:
URL:http://xforce.iss.net/xforce/xfdb/2
URL:http://seclab.cs.ucdavis.edu/projects/testing/vulner/38.html

[return to 172.16.0.22]

2.1.3 High 9/tcp

High (CVSS: 10.0)
NVT: Check for Discard Service

Summary
The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.
This service is unused these days, so it is advised that you disable it.

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

Solution
Solution type: Mitigation
- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard
Then launch cmd.exe and type :
net stop simptcp net start simptcp
To restart the service.

Vulnerability Detection Method
Details: Check for Discard Service
OID:1.3.6.1.4.1.25623.1.0.11367
Version used: $Revision: 11015 $

References
Other:
URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0636

[return to 172.16.0.22]

2.1.4 Medium 7/tcp

Medium (CVSS: 5.0)
NVT: echo Service Reporting (TCP + UDP)

Summary
An echo Service is running at this Host via TCP and/or UDP.
The echo service is an Internet protocol defined in RFC 862. It was originally proposed for testing and measurement of round-trip times in IP networks. While still available on most UNIX-like operating systems, testing and measurement is now performed with the Internet Control Message Protocol (ICMP), using the applications ping and traceroute.

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

Solution
Solution type: Mitigation
Disable the echo Service.

Vulnerability Detection Method
Details: `echo Service Reporting (TCP + UDP)`
OID:1.3.6.1.4.1.25623.1.0.100075
Version used: `$Revision: 12037 $`

References
```
Other:
  URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0635
```

[return to 172.16.0.22]

2.1.5 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.22[49152]
```

... continues on next page ...

... continued from previous page ...

```
Port: 49153/tcp
      UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49153]
      Annotation: NRP server endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49153]
      Annotation: DHCP Client LRPC Endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49153]
      Annotation: DHCPv6 Client LRPC Endpoint
      UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49153]
      Annotation: Wcm Service
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49153]
      Annotation: Event log TCPIP
Port: 49154/tcp
      UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: IdSegSrv service
      UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: Proxy Manager provider server endpoint
      UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: IP Transition Configuration endpoint
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: IKE/Authip API
      UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: Proxy Manager client server endpoint
      UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: Adh APIs
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49154]
      Annotation: Impl friendly name
```

... continues on next page ...

... continued from previous page ...

```
Port: 49155/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Annotation: KeyIso
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Annotation: Impl friendly name
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:172.16.0.22[49155]
      Annotation: MS NT Directory DRS Interface
Port: 49157/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:172.16.0.22[49157]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49157]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:172.16.0.22[49157]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49157]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
```

... continues on next page ...

... continued from previous page ...

```
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:172.16.0.22[49157]
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:172.16.0.22[49157]
      Annotation: MS NT Directory DRS Interface
Port: 49158/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_http:172.16.0.22[49158]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_http:172.16.0.22[49158]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_http:172.16.0.22[49158]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_http:172.16.0.22[49158]
      Annotation: KeyIso
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_http:172.16.0.22[49158]
      Annotation: MS NT Directory DRS Interface
Port: 49159/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49159]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49159]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49159]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49159]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.22[49159]
Port: 49170/tcp
      UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
      Endpoint: ncacn_ip_tcp:172.16.0.22[49170]
      Named pipe : dnsserver
      Win32 service or process : dns.exe
      Description : DNS Server
Port: 49179/tcp
```

... continues on next page ...

... continued from previous page ...

```
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.16.0.22[49179]
Port: 49182/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.22[49182]
     Annotation: Remote Fw APIs
Port: 49194/tcp
     UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.22[49194]
     Annotation: Frs2 Service
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

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

Solution
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: $Revision: 6319 $

[return to 172.16.0.22]

2.1.6 Medium 22/tcp

Medium (CVSS: 5.0)
NVT: OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)

Product detection result
cpe:/a:openbsd:openssh:7.4
Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to security bypass vulnerability.

Vulnerability Detection Result
Installed version: 7.4
Fixed version: 7.6

Impact

... continues on next page ...

... continued from previous page ...

Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution
Solution type: VendorFix
Upgrade to OpenSSH version 7.6 or later.

Affected Software/OS
OpenSSH versions before 7.6 on Windows

Vulnerability Insight
The flaw exists in the 'process_open' function in sftp-server.c script which does not properly prevent write operations in readonly mode.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH 'sftp-server' Security Bypass Vulnerability (Windows)`
OID:1.3.6.1.4.1.25623.1.0.812050
Version used: `$Revision: 11983 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
`CVE: CVE-2017-15906`
`BID:101552`
`Other:`
`URL:https://www.openssh.com/txt/release-7.6`
`URL:https://github.com/openbsd/src/commit/a6981567e8e`
`URL:http://www.openssh.com`

Medium (CVSS: 5.0)
NVT: OpenSSH User Enumeration Vulnerability-Aug18 (Windows)

Product detection result
`cpe:/a:openbsd:openssh:7.4`
`Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)`

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

```
Installed version: 7.4
Fixed version:     NoneAvailable
Installation
path / port:       22/tcp
```

Impact
Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution
Solution type: NoneAvailable
No known solution is available as of 21st August, 2018. Information regarding this issue will be updated once solution details are available. For updates refer to Reference links.

Affected Software/OS
OpenSSH version 7.7 and prior on Windows.

Vulnerability Insight
The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `OpenSSH User Enumeration Vulnerability-Aug18 (Windows)`
OID:1.3.6.1.4.1.25623.1.0.813863
Version used: `$Revision: 12116 $`

Product Detection Result
Product: `cpe:/a:openbsd:openssh:7.4`
Method: `SSH Server type and version`
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
```
CVE: CVE-2018-15473
Other:
  URL:http://www.openssh.com
   URL:https://0day.city/cve-2018-15473.html
   URL:https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a
↪7d1e0
```

Medium (CVSS: 5.0)
NVT: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Windows)

Product detection result
`cpe:/a:openbsd:openssh:7.4`

... continues on next page ...

... continued from previous page ...

Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)

Summary
This host is installed with openssh and is prone to user enumeration vulnerability.

Vulnerability Detection Result
Installed version: 7.4
Fixed version: NoneAvailable
Installation
path / port: 22/tcp

Impact
Successfully exploitation will allow remote attacker to harvest valid user accounts, which may aid in brute-force attacks.

Solution
Solution type: NoneAvailable
No known solution is available as of 05th September, 2018. Information regarding this issue will be updated once solution details are available.

Affected Software/OS
OpenSSH version 5.9 to 7.8 on Windows.

Vulnerability Insight
The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) component is used on an affected system.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: OpenSSH 'auth2-gss.c' User Enumeration Vulnerability (Windows)
OID:1.3.6.1.4.1.25623.1.0.813887
Version used: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:openbsd:openssh:7.4
Method: SSH Server type and version
OID: 1.3.6.1.4.1.25623.1.0.10267)

References
CVE: CVE-2018-15919
Other:
URL:http://www.openssh.com
URL:https://bugzilla.novell.com/show_bug.cgi?id=1106163
URL:https://seclists.org/oss-sec/2018/q3/180

[return to 172.16.0.22]

2.1.7 Medium 17/tcp

Medium (CVSS: 5.0)
NVT: Check for Quote of the day Service (TCP)

Summary
The quote service (qotd) is running on this host.
Description :
A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.

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

Impact
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution
Solution type: Mitigation
- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd
Then launch cmd.exe and type :
net stop simptcp net start simptcp
To restart the service.

Vulnerability Detection Method
Details: `Check for Quote of the day Service (TCP)`
OID:1.3.6.1.4.1.25623.1.0.10198
Version used: `$Revision: 4827 $`

References
`Other:`
`URL:https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0103`

[return to 172.16.0.22]

2.1.8 Medium 443/tcp

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: `$Revision: 11402 $`

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-exploiting-ssl-30.html
```

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: `$Revision: 5547 $`

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: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

... continues on next page ...

... continued from previous page ...

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_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
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: $Revision: 11135 $

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: 4.0)
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 https://weakdh.org/sysadmin.html).
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: `$Revision: 11524 $`

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

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:`

... continues on next page ...

... continued from previous page ...

```
Subject:              CN=GRU
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: `$Revision: 8810 $`

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

[return to 172.16.0.22]

2.1.9 Medium 3389/tcp

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.

... continues on next page ...

... continued from previous page ...

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 TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
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: `$Revision: 11135 $`

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: 4.0)

NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

... continues on next page ...

... continued from previous page ...

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 https://weakdh.org/sysadmin.html).
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: `$Revision: 11524 $`

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

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:              CN=GRU.minions.galactic
Signature Algorithm:  sha1WithRSAEncryption
```

... continues on next page ...

... continued from previous page ...

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: `$Revision: 8810 $`

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

[return to 172.16.0.22]

2.1.10 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.`

... continues on next page ...

... continued from previous page ...

```
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3302404
Packet 2: 3302508
```

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

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

[return to 172.16.0.22]

2.2 172.16.0.23

Host scan start Tue Oct 30 10:41:31 2018 UTC
Host scan end Tue Oct 30 11:00:13 2018 UTC

Service (Port)	Threat Level
445/tcp	High
general/tcp	High
135/tcp	Medium

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
3389/tcp	Medium
general/tcp	Low

2.2.1 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

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

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS
Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `$Revision: 11874 $`

References
`CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,`
`↪CVE-2017-0148`
`BID:96703, 96704, 96705, 96707, 96709, 96706`

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:https://support.microsoft.com/en-in/kb/4013078
   URL:https://technet.microsoft.com/library/security/MS17-010
   URL:https://github.com/rapid7/metasploit-framework/pull/8167/files
```

[return to 172.16.0.23]

2.2.2 High general/tcp

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

Product detection result
cpe:/o:microsoft:windows_7:-:-:
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 "Windows 7" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:microsoft:windows_7:-:-:
EOL date: 2013-04-09
EOL info: https://support.microsoft.com/en-us/lifecycle/search?sort=PN&
↪alpha=Windows%207&Filter=FilterNO

Solution
Solution type: Mitigation

Vulnerability Detection Method
Details: OS End Of Life Detection
OID:1.3.6.1.4.1.25623.1.0.103674
Version used: $Revision: 8927 $

Product Detection Result
Product: cpe:/o:microsoft:windows_7:-:-:
Method: OS Detection Consolidation and Reporting
OID: 1.3.6.1.4.1.25623.1.0.105937)

[return to 172.16.0.23]

2.2.3 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49152]
Port: 49153/tcp
     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49153]
     Annotation: Security Center
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.16.0.23[49154]
```

... continues on next page ...

... continued from previous page ...

```
      Annotation: Impl friendly name
Port: 49155/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:172.16.0.23[49155]
Port: 49156/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:172.16.0.23[49156]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

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

Solution
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: $Revision: 6319 $

[return to 172.16.0.23]

2.2.4 Medium 3389/tcp

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 TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

Solution
Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

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: `$Revision: 11135 $`

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: 4.0)
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:              CN=PC-helen.jerry.land
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

... continues on next page ...

... continued from previous page ...

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: `$Revision: 8810 $`

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

[return to 172.16.0.23]

2.2.5 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: 3008819
Packet 2: 3008921
```

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

... continues on next page ...

... continued from previous page ...

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

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

[return to 172.16.0.23]

2.3 172.16.0.8

Host scan start Tue Oct 30 10:41:28 2018 UTC
Host scan end Tue Oct 30 11:19:38 2018 UTC

Service (Port)	Threat Level
512/tcp	High
513/tcp	High
514/tcp	High
80/tcp	Medium
21/tcp	Medium
443/tcp	Medium
22/tcp	Medium
general/tcp	Low
443/tcp	Low

... (continues) ...

... (continued) ...

Service (Port)	Threat Level
22/tcp	Low

2.3.1 High 512/tcp

High (CVSS: 10.0)
NVT: Check for rexecd Service

Summary
Rexecd Service is running at this Host. Rexecd (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 rexecd authenticate by reading the username and password *unencrypted* from the socket.

Vulnerability Detection Result
`The rexecd Service is not allowing connections from this host.`

Solution
Solution type: Mitigation
Disable rexec Service.

Vulnerability Detection Method
Details: `Check for rexecd Service`
OID:1.3.6.1.4.1.25623.1.0.100111
Version used: `$Revision: 6849 $`

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

[return to 172.16.0.8]

2.3.2 High 513/tcp

High (CVSS: 7.5)
NVT: Check for rlogin Service

Summary
This remote host is running a rlogin service.

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

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Disable rlogin service and use 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)
Impact Level: System

Vulnerability Detection Method
Details: `Check for rlogin Service`
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: `$Revision: 11997 $`

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 172.16.0.8]

2.3.3 High 514/tcp

High (CVSS: 7.5)
NVT: rsh Service Reporting

Summary
A rsh service is running at this Host. 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 Result
`The rsh service is not allowing connections from this host.`

Solution
Solution type: Mitigation
Disable rsh and use SSH instead.

Vulnerability Detection Method
Details: `rsh Service Reporting`
OID:1.3.6.1.4.1.25623.1.0.100080
Version used: `$Revision: 12037 $`

References
`Other:`

... continues on next page ...

... continued from previous page ...

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

[return to 172.16.0.8]

2.3.4 Medium 80/tcp

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

Summary
Debugging functions are enabled on the remote web server.
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: $Revision: 10828 $

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

... continues on next page ...

... continued from previous page ...

URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
URL:https://www.owasp.org/index.php/Cross_Site_Tracing

[return to 172.16.0.8]

2.3.5 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:openvas-vt@example.com
ftp:openvas-vt@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
drwxr-xr-x    2 0        0            4096 May 11  2016 pub
Account "ftp":
drwxr-xr-x    2 0        0            4096 May 11  2016 pub
```

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: `$Revision: 12030 $`

... continues on next page ...

... continued from previous page ...

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

[return to 172.16.0.8]

2.3.6 Medium 443/tcp

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

Summary
Debugging functions are enabled on the remote web server.
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: $Revision: 10828 $

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

... continues on next page ...

... continued from previous page ...

```
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: 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 2018-01-11 07:26:13.
Certificate details:
subject ...: 1.2.840.113549.1.9.1=#726F6F74406B6576696E2E6D696E696F6E732E67616C6
↪163746963,CN=kevin.minions.galactic,OU=SomeOrganizationalUnit,O=SomeOrganizati
↪on,L=SomeCity,ST=SomeState,C=--
subject alternative names (SAN):
None
issued by .: 1.2.840.113549.1.9.1=#726F6F74406B6576696E2E6D696E696F6E732E67616C6
↪163746963,CN=kevin.minions.galactic,OU=SomeOrganizationalUnit,O=SomeOrganizati
↪on,L=SomeCity,ST=SomeState,C=--
serial ....: 3E67
valid from : 2017-01-11 07:26:13 UTC
valid until: 2018-01-11 07:26:13 UTC
fingerprint (SHA-1): B932004BEEBA1F627E0D0B279CC6C71553456D6F
fingerprint (SHA-256): B9B75A201CD05CF08694A232C74AA2FA9999C0CE7F2B64AB282829077
↪BE9E4CB
```

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 $`

... continues on next page ...

... continued from previous page ...

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
```
'Vulnerable' cipher suites accepted by this service via the SSLv3 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

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

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `$Revision: 5232 $`

References
`CVE: CVE-2016-2183, CVE-2016-6329`
`Other:`

... continues on next page ...

... continued from previous page ...

URL:https://bettercrypto.org/
URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
URL:https://sweet32.info/

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 SSLv3 protocol 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: $Revision: 5547 $

References
CVE: CVE-2016-0800, CVE-2014-3566
Other:
URL:https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

... continues on next page ...

... continued from previous page ...

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: 4.3)
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_ECDHE_RSA_WITH_RC4_128_SHA
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_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
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

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: $Revision: 11135 $

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/

[return to 172.16.0.8]

2.3.7 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 remote service:
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 remote service:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256

... continues on next page ...

... continued from previous page ...

```
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: `$Revision: 4490 $`

References

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

[return to 172.16.0.8]

2.3.8 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: 32416542
Packet 2: 32417580
```

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

... continues on next page ...

... continued from previous page ...

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

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

[return to 172.16.0.8]

2.3.9 Low 443/tcp

Low (CVSS: 2.6)
NVT: SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability

Summary
This host is installed with OpenSSL and is prone to padding oracle attack.

Vulnerability Detection Result
```
It was possible to send an encrypted data with malformed padding and receive Rec
↪ord Overflow alert from the SSL Server
```

Impact
Exploiting this vulnerability allows remote attackers to obtain sensitive cleartext information via a padding oracle attack against an AES CBC session.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
OpenSSL 1.0.2 users should upgrade to 1.0.2h.
OpenSSL 1.0.1 users should upgrade to 1.0.1t.

Affected Software/OS
OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h.

Vulnerability Insight
The vulnerability is due to not considering memory allocation during a certain padding check.

Vulnerability Detection Method
Send an encrypted padded message and check the returned alert (Record Overflow if vulnerable, Bad Record Mac if no vulnerable.
Details: `SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.107141
Version used: `$Revision: 11874 $`

References
`CVE: CVE-2016-2107`
`Other:`
`URL:https://www.openssl.org/news/secadv/20160503.txt`

[return to 172.16.0.8]

2.3.10 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
```

... continues on next page ...

. . . continued from previous page . . .

Solution
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: `$Revision: 4490 $`

[return to 172.16.0.8]

2.4 172.16.0.16

Host scan start Tue Oct 30 10:41:28 2018 UTC
Host scan end Tue Oct 30 11:25:42 2018 UTC

Service (Port)	Threat Level
443/tcp	Medium
587/tcp	Medium
22/tcp	Medium
25/tcp	Medium
21/tcp	Medium
10000/tcp	Medium
443/tcp	Low
587/tcp	Low
22/tcp	Low
25/tcp	Low
10000/tcp	Low
general/tcp	Low

2.4.1 Medium 443/tcp

Medium (CVSS: 6.8)
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

. . . continues on next page . . .

... continued from previous page ...

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.

Solution
Solution type: VendorFix
Updates are available.

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: `$Revision: 11186 $`

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

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: `SSL/TLS: Report Vulnerable Cipher Suites for HTTPS`
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: `$Revision: 5232 $`

References
```
CVE: CVE-2016-2183, CVE-2016-6329
Other:
  URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://sweet32.info/
```

[return to 172.16.0.16]

2.4.2 Medium 587/tcp

Medium (CVSS: 6.8)
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.

Solution
Solution type: VendorFix
Updates are available.

... continues on next page ...

. . . continued from previous page . . .

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: `$Revision: 11186 $`

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

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 TLSv1.0 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_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

. . . continues on next page . . .

... continued from previous page ...

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: $Revision: 11135 $

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/

[return to 172.16.0.16]

2.4.3 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 remote service:
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 remote 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
```

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: `$Revision: 4490 $`

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

[return to 172.16.0.16]

2.4.4 Medium 25/tcp

Medium (CVSS: 6.8)
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Summary
OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

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.

Solution
Solution type: VendorFix
Updates are available.

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: `$Revision: 11186 $`

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

[return to 172.16.0.16]

2.4.5 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:openvas-vt@example.com
```

... continues on next page ...

... continued from previous page ...

ftp:openvas-vt@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: $Revision: 12030 $

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

[return to 172.16.0.16]

2.4.6 Medium 10000/tcp

Medium (CVSS: 6.8)
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.

Solution

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Updates are available.

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: `$Revision: 11186 $`

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

Medium (CVSS: 6.4)
NVT: SSL/TLS: Missing 'secure' Cookie Attribute

Summary
The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

Vulnerability Detection Result
```
The cookies:
Set-Cookie: redirect=***replaced***; path=/
are missing the "secure" attribute.
```

Solution
Solution type: Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Affected Software/OS
Server with SSL/TLS.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The flaw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Vulnerability Detection Method
Details: `SSL/TLS: Missing 'secure' Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.902661
Version used: `$Revision: 11374 $`

References
```
Other:
  URL:https://www.owasp.org/index.php/SecureFlag
   URL:http://www.ietf.org/rfc/rfc2965.txt
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-
↪002)
```

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result
```
The cookies:
Set-Cookie: redirect=***replaced***; path=/
Set-Cookie: testing=***replaced***; path=/; secure
are missing the "httpOnly" attribute.
```

Solution
Solution type: Mitigation
Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS
Application with session handling in cookies.

Vulnerability Insight
The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: `Missing 'httpOnly' Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `$Revision: 5270 $`

References

... continues on next page ...

... continued from previous page ...

```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
↪002)
```

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

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

Affected Software/OS
Services accepting vulnerable SSL/TLS cipher suites via HTTPS.

Vulnerability Insight
These rules are applied for the evaluation of the vulnerable cipher suites:
- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Vulnerability Detection Method
Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
OID:1.3.6.1.4.1.25623.1.0.108031
Version used: $Revision: 5232 $

References
CVE: CVE-2016-2183, CVE-2016-6329
Other:
  URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
   URL:https://sweet32.info/

Medium (CVSS: 5.0)
NVT: Webmin 1.880 Information Disclosure Vulnerability

... continues on next page ...

... continued from previous page ...

Product detection result
cpe:/a:webmin:webmin:1.831
Detected by Check for Webmin / Usermin (OID: 1.3.6.1.4.1.25623.1.0.10757)

Summary
Webmin is prone to an information disclosure vulnerability that allows non-privileged users to access arbitrary files.

Vulnerability Detection Result
Installed version: 1.831
Fixed version: Please see the solution tag for an available Mitigation

Impact
Successful exploitation would allow an attacker to access any file on the system, ranging from sensitive documents to administrator passwords.

Solution
Solution type: Mitigation
No patch is available as of 15th March, 2018. As a mitigation technique, the setting 'Can view any file as a log file' can be disabled, effectively stopping a user from exploiting this vulnerability.

Affected Software/OS
Webmin through version 1.880

Vulnerability Insight
An issue was discovered in Webmin when the default Yes setting of 'Can view any file as a log file' is enabled. As a result of weak default configuration settings, limited users have full access rights to the underlying Unix system files, allowing the user to read sensitive data from the local system (using Local File Include) such as the '/etc/shadow' file via a 'GET /syslog/save_log.cgi?view=1&file=/etc/shadow' request.

Vulnerability Detection Method
The script checks if a vulnerable version is present on the target host.
Details: Webmin 1.880 Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.113135
Version used: $Revision: 12116 $

Product Detection Result
Product: cpe:/a:webmin:webmin:1.831
Method: Check for Webmin / Usermin
OID: 1.3.6.1.4.1.25623.1.0.10757)

References
CVE: CVE-2018-8712
Other:

... continues on next page ...

... continued from previous page ...

URL:https://www.7elements.co.uk/resources/technical-advisories/webmin-1-840-1-
↪880-unrestricted-access-arbitrary-files-using-local-file-include/
URL:http://www.webmin.com/changes.html

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 TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_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: $Revision: 11135 $

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/

[return to 172.16.0.16]

2.4.7 Low 443/tcp

Low (CVSS: 2.6) NVT: SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability
Summary This host is installed with OpenSSL and is prone to padding oracle attack.

Vulnerability Detection Result
`It was possible to send an encrypted data with malformed padding and receive Rec`
`↪ord Overflow alert from the SSL Server`

Impact Exploiting this vulnerability allows remote attackers to obtain sensitive cleartext information via a padding oracle attack against an AES CBC session.
Solution **Solution type:** VendorFix OpenSSL 1.0.2 users should upgrade to 1.0.2h. OpenSSL 1.0.1 users should upgrade to 1.0.1t.
Affected Software/OS OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h.
Vulnerability Insight The vulnerability is due to not considering memory allocation during a certain padding check.
Vulnerability Detection Method Send an encrypted padded message and check the returned alert (Record Overflow if vulnerable, Bad Record Mac if no vulnerable. Details: `SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability` OID:1.3.6.1.4.1.25623.1.0.107141 Version used: `$Revision: 11874 $`

References
`CVE: CVE-2016-2107`
`Other:`
`URL:https://www.openssl.org/news/secadv/20160503.txt`

[return to 172.16.0.16]

2.4.8 Low 587/tcp

Low (CVSS: 2.6)
NVT: SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability

Summary
This host is installed with OpenSSL and is prone to padding oracle attack.

Vulnerability Detection Result
`It was possible to send an encrypted data with malformed padding and receive Rec`
`↪ord Overflow alert from the SSL Server`

Impact
Exploiting this vulnerability allows remote attackers to obtain sensitive cleartext information via a padding oracle attack against an AES CBC session.

Solution
Solution type: VendorFix
OpenSSL 1.0.2 users should upgrade to 1.0.2h.
OpenSSL 1.0.1 users should upgrade to 1.0.1t.

Affected Software/OS
OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h.

Vulnerability Insight
The vulnerability is due to not considering memory allocation during a certain padding check.

Vulnerability Detection Method
Send an encrypted padded message and check the returned alert (Record Overflow if vulnerable, Bad Record Mac if no vulnerable.
Details: `SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.107141
Version used: `$Revision: 11874 $`

References
`CVE: CVE-2016-2107`
`Other:`
`URL:https://www.openssl.org/news/secadv/20160503.txt`

[return to 172.16.0.16]

2.4.9 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.

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
```

Solution
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: `$Revision: 4490 $`

[return to 172.16.0.16]

2.4.10 Low 25/tcp

Low (CVSS: 2.6)
NVT: SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability

Summary
This host is installed with OpenSSL and is prone to padding oracle attack.

Vulnerability Detection Result

```
It was possible to send an encrypted data with malformed padding and receive Rec
↪ord Overflow alert from the SSL Server
```

Impact
Exploiting this vulnerability allows remote attackers to obtain sensitive cleartext information via a padding oracle attack against an AES CBC session.

... continues on next page ...

... continued from previous page ...

Solution
Solution type: VendorFix
OpenSSL 1.0.2 users should upgrade to 1.0.2h.
OpenSSL 1.0.1 users should upgrade to 1.0.1t.

Affected Software/OS
OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h.

Vulnerability Insight
The vulnerability is due to not considering memory allocation during a certain padding check.

Vulnerability Detection Method
Send an encrypted padded message and check the returned alert (Record Overflow if vulnerable, Bad Record Mac if no vulnerable.
Details: `SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.107141
Version used: `$Revision: 11874 $`

References
`CVE: CVE-2016-2107`
`Other:`
`URL:https://www.openssl.org/news/secadv/20160503.txt`

[return to 172.16.0.16]

2.4.11 Low 10000/tcp

Low (CVSS: 2.6)
NVT: SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability

Summary
This host is installed with OpenSSL and is prone to padding oracle attack.

Vulnerability Detection Result
`It was possible to send an encrypted data with malformed padding and receive Rec`
`↪ord Overflow alert from the SSL Server`

Impact
Exploiting this vulnerability allows remote attackers to obtain sensitive cleartext information via a padding oracle attack against an AES CBC session.

Solution
Solution type: VendorFix
OpenSSL 1.0.2 users should upgrade to 1.0.2h.
OpenSSL 1.0.1 users should upgrade to 1.0.1t.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h.

Vulnerability Insight
The vulnerability is due to not considering memory allocation during a certain padding check.

Vulnerability Detection Method
Send an encrypted padded message and check the returned alert (Record Overflow if vulnerable, Bad Record Mac if no vulnerable.
Details: `SSL/TLS: OpenSSL 'CVE-2016-2107' Padding Oracle Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.107141
Version used: `$Revision: 11874 $`

References
`CVE: CVE-2016-2107`
`Other:`
`URL:https://www.openssl.org/news/secadv/20160503.txt`

[return to 172.16.0.16]

2.4.12 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: 8164949
Packet 2: 8165207
```

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.
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.

... continues on next page ...

... continued from previous page ...

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

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

[return to 172.16.0.16]

2.5 172.16.0.20

Host scan start Tue Oct 30 10:41:28 2018 UTC
Host scan end Tue Oct 30 11:33:40 2018 UTC

Service (Port)	Threat Level
21/tcp	Medium
general/tcp	Low

2.5.1 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:openvas-vt@example.com
ftp:openvas-vt@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
```

... continues on next page ...

... continued from previous page ...

```
-rw-r--r--   1 0        0             170 May 19  2015 welcome.msg
Account "ftp":
-rw-r--r--   1 0        0             170 May 19  2015 welcome.msg
```

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: `$Revision: 12030 $`

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

Medium (CVSS: 5.0)
NVT: FTP Writeable Directories

Summary
The remote FTP server contains world-writeable files.
By crawling through the remote FTP server, several directories where marked as being world writeable.

Vulnerability Detection Result
- /

Impact
An attacker may use this misconfiguration problem to use the remote FTP server to host arbitrary data, including possibly illegal content (ie: Divx movies, etc...).

Solution

... continues on next page ...

... continued from previous page ...

Solution type: Mitigation
Configure the remote FTP directories so that they are not world-writeable.

Vulnerability Detection Method
Details: `FTP Writeable Directories`
OID:1.3.6.1.4.1.25623.1.0.19782
Version used: `$Revision: 9541 $`

[return to 172.16.0.20]

2.5.2 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: 8256334
Packet 2: 8256591
```

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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

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

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

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: `$Revision: 10411 $`

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

[return to 172.16.0.20]

2.6 172.16.0.11

Host scan start Tue Oct 30 10:41:28 2018 UTC
Host scan end Tue Oct 30 11:19:06 2018 UTC

Service (Port)	Threat Level
22/tcp	Medium
general/tcp	Low
22/tcp	Low

2.6.1 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:
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:
```

... 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
```

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: `$Revision: 4490 $`

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

[return to 172.16.0.11]

2.6.2 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

... continues on next page ...

... continued from previous page ...

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 9468086
Packet 2: 9468412
```

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

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

[return to 172.16.0.11]

2.6.3 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.

... continues on next page ...

. . . continued from previous page . . .

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
hmac-sha2-256-96
hmac-sha2-512-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

Solution
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: `$Revision: 4490 $`

[return to 172.16.0.11]

2.7 172.16.0.1

Host scan start Tue Oct 30 10:41:28 2018 UTC
Host scan end Tue Oct 30 11:11:31 2018 UTC

Service (Port)	Threat Level
general/tcp	Low

2.7.1 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

. . . continues on next page . . .

... continued from previous page ...

```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 956617703
Packet 2: 956618759
```

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

References

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

[return to 172.16.0.1]

2.8 172.16.0.21

Host scan start	Tue Oct 30 10:41:31 2018 UTC
Host scan end	Tue Oct 30 11:19:51 2018 UTC

Service (Port)	Threat Level
general/tcp	Low

2.8.1 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: 8038180
Packet 2: 8038440
```

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.
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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

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: `$Revision: 10411 $`

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

[return to 172.16.0.21]

This file was automatically generated.