Scan Report

November 15, 2016

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 "Immediate scan of IP 192.168.1.1,192.168.1,147,192.168.1.159,192.168.1.174,192.168.1.199,192.168.1.220,192.168 The scan started at Tue Nov 15 14:53:33 2016 UTC and ended at Tue Nov 15 14:57:20 2016 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
192.168.1.1	0	0	1	10	0
Total: 1	0	0	1	10	0

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

This report contains all 11 results selected by the filtering described above. Before filtering there were 14 results.

2 Results per Host

2.1 192.168.1.1

Host scan start	Tue Nov 15 14:53:42 2016 UTC
Host scan end	Tue Nov 15 14:57:20 2016 UTC

Service (Port)	Threat Level
general/tcp	Low
3128/tcp	Log
general/CPE-T	Log
general/tcp	Log

2.1.1 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.`

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 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: 4408 $`

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

[return to 192.168.1.1]

2.1.2 Log 3128/tcp

Log (CVSS: 0.0)
NVT: HTTP Proxy Server Detection

Summary
A HTTP proxy server is running at this Host and accepts unauthenticated requests from the OpenVAS Scanner.

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

Solution
Solution type: Mitigation
Limit access to the proxy to valid users and/or valid hosts.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
An open proxy is a proxy server that is accessible by any Internet user. Generally, a proxy server allows users within a network group to store and forward Internet services such as DNS or web pages to reduce and control the bandwidth used by the group. With an open proxy, however, any user on the Internet is able to use this forwarding service.

Log Method
Details:`HTTP Proxy Server Detection`
OID:1.3.6.1.4.1.25623.1.0.100083
Version used: `$Revision: 3467 $`

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

Summary
This detects the HTTP Server's type and version.

Vulnerability Detection Result
```
The remote web server type is :
squid/3.1.10
```

Solution

Log Method
Details:`HTTP Server type and version`
OID:1.3.6.1.4.1.25623.1.0.10107
Version used: `$Revision: 3564 $`

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

Summary
This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result
```
This are the directories/files found with brute force:
http://192.168.1.1:3128/
```

Log Method
Details:`DIRB (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.103079
Version used: `$Revision: 4290 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`A web server is running on this port`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3923 $`

Log (CVSS: 0.0)
NVT: Services

Summary
This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.

Vulnerability Detection Result
`An HTTP proxy is running on this port`

Log Method
Details:`Services`
OID:1.3.6.1.4.1.25623.1.0.10330
Version used: `$Revision: 3923 $`

Log (CVSS: 0.0)
NVT: Info / Options concerning CGI Scanning

Summary
The script prints out various options and the directories used when CGI scanning is enabled.

Vulnerability Detection Result
```
The host seems to be NOT able to host PHP scripts.
The host seems to be NOT able to host ASP scripts.
The following directories are used for CGI scanning:
http://192.168.1.1:3128/cgi-bin
http://192.168.1.1:3128/scripts
http://192.168.1.1:3128/
```

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Insight
The information printed out is based on the following scripts / settings:
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)

- Various OS fingerprinting methods

Log Method
Details:`Info / Options concerning CGI Scanning`
OID:1.3.6.1.4.1.25623.1.0.111038
Version used: `$Revision: 4334 $`

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

Summary
This plugin uses nikto(1) to find weak CGI scripts and other known issues regarding web server security. See the preferences section for configuration options.

Vulnerability Detection Result

```
Here is the Nikto report:
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.1
+ Target Hostname:    192.168.1.1
+ Target Port:        3128
+ Start Time:         2016-11-15 14:55:31 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
↪gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
↪to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ 26172 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2016-11-15 14:57:19 (GMT0) (108 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Log Method
Details:`Nikto (NASL wrapper)`
OID:1.3.6.1.4.1.25623.1.0.14260
Version used: `$Revision: 4288 $`

Log (CVSS: 0.0)
NVT: Squid Proxy Server Detection

Summary
Detection of installed version of squid.
This script sends HTTP GET request and try to get the version from the response, and sets the result in KB.

Vulnerability Detection Result
```
Detected Squid Proxy Server
Version: 3.1.10
Location: 3128/tcp
CPE: cpe:/a:squid-cache:squid:3.1.10
Concluded from version identification result:
Server: squid/3.1.10
```

Log Method
Details:`Squid Proxy Server Detection`
OID:1.3.6.1.4.1.25623.1.0.900611
Version used: `$Revision: 2554 $`

[return to 192.168.1.1]

2.1.3 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

Summary
This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.

Vulnerability Detection Result
```
192.168.1.1|cpe:/a:squid-cache:squid:3.1.10
```

Log Method
Details:`CPE Inventory`
OID:1.3.6.1.4.1.25623.1.0.810002
Version used: `$Revision: 2837 $`

[return to 192.168.1.1]

2.1.4 Log general/tcp

Log (CVSS: 0.0)
NVT: Traceroute

Summary
A traceroute from the scanning server to the target system was conducted. This traceroute is provided primarily for informational value only. In the vast majority of cases, it does not represent a vulnerability. However, if the displayed traceroute contains any private addresses that should not have been publicly visible, then you have an issue you need to correct.

Vulnerability Detection Result
```
Here is the route from 10.20.232.41 to 192.168.1.1:
10.20.232.41
192.168.1.1
```

Solution
Block unwanted packets from escaping your network.

Log Method
Details:`Traceroute`
OID:1.3.6.1.4.1.25623.1.0.51662
Version used: `$Revision: 4048 $`

[return to 192.168.1.1]