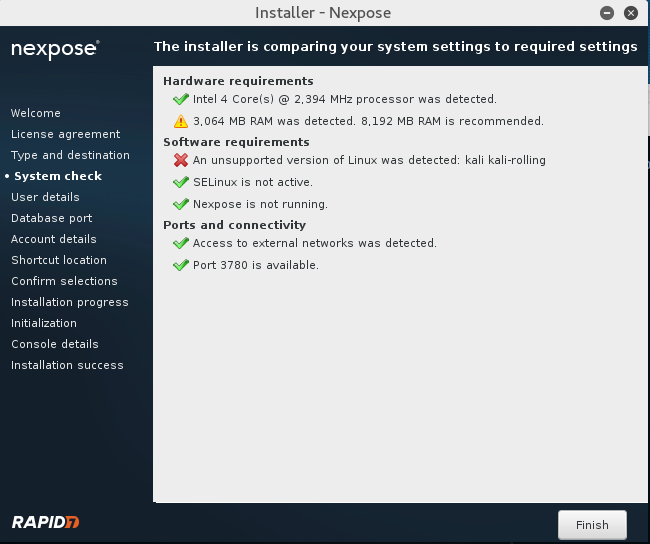
Vulnerability Scanning

By

Note: Attempted to install openvas, many times, but failed. Also it seems installation is different from video that is OLD and from 2013. I had continuing issue that login to greenbone SA failed, even after making new user and deleting old user. Hope you can tell me what to do.

Furthermore, nexpose can’t be installed on kali, proof:

**

# Nessus Scan of two Targets

Using metasploitable2 and Windows 7 64bit, both on host only network with CIDR IP range 192.168.10.0/24. Auto-generated Nessus embedded.



# Sparta Scan of two Targets

While not as nice looking as Nessus it is still practical:

## Target One, metasploitable2:

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.10.133

+ Target Hostname: 192.168.10.133

+ Target Port: 80

+ Start Time: 2016-04-18 12:09:14 (GMT-4)

---------------------------------------------------------------------------

+ Server: Apache/2.2.8 (Ubuntu) DAV/2

+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10

+ 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 agent 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

+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

+ Uncommon header 'tcn' found, with contents: list

+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.

+ OSVDB-3268: /doc/: Directory indexing found.

+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.

+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008

+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3268: /test/: Directory indexing found.

+ OSVDB-3092: /test/: This might be interesting...

+ /phpinfo.php: Output from the phpinfo() function was found.

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3268: /icons/: Directory indexing found.

+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /phpMyAdmin/: phpMyAdmin directory found

+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ 8349 requests: 2 error(s) and 29 item(s) reported on remote host

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-04-18 12:10:55

[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)

[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...

[DATA] max 3 tasks per 1 server, overall 64 tasks, 3 login tries, ~0 tries per task

[DATA] attacking service mysql on port 3306

[3306][mysql] host: 192.168.10.133 login: root

[STATUS] attack finished for 192.168.10.133 (valid pair found)

1 of 1 target successfully completed, 1 valid password found

Hydra (http://www.thc.org/thc-hydra) finished at 2016-04-18 12:11:47

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-04-18 12:13:42

[DATA] max 10 tasks per 1 server, overall 64 tasks, 10 login tries, ~0 tries per task

[DATA] attacking service ftp on port 21

[21][ftp] host: 192.168.10.133 login: ftp password: ftp

[STATUS] attack finished for 192.168.10.133 (valid pair found)

1 of 1 target successfully completed, 1 valid password found

Hydra (http://www.thc.org/thc-hydra) finished at 2016-04-18 12:13:42

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.10.133

+ Target Hostname: 192.168.10.133

+ Target Port: 8180

+ Start Time: 2016-04-18 12:18:21 (GMT-4)

---------------------------------------------------------------------------

+ Server: Apache-Coyote/1.1

+ 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 agent 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

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0xW/21630 0x1228677438000

+ OSVDB-39272: favicon.ico file identifies this server as: Apache Tomcat

+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.

+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ /: Appears to be a default Apache Tomcat install.

+ Cookie JSESSIONID created without the httponly flag

+ OSVDB-376: /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin.

+ OSVDB-3092: /admin/: This might be interesting...

+ OSVDB-3233: /tomcat-docs/index.html: Default Apache Tomcat documentation found.

+ OSVDB-3233: /manager/html-manager-howto.html: Tomcat documentation found.

+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.

+ OSVDB-3092: /webdav/index.html: WebDAV support is enabled.

+ OSVDB-3233: /jsp-examples/: Apache Java Server Pages documentation.

+ /admin/account.html: Admin login page/section found.

+ /admin/controlpanel.html: Admin login page/section found.

+ /admin/cp.html: Admin login page/section found.

+ /admin/index.html: Admin login page/section found.

+ /admin/login.html: Admin login page/section found.

+ /servlets-examples/: Tomcat servlets examples are visible.

+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 'tomcat'). Apache Tomcat.

+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)

+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected)

+ /manager/status: Tomcat Server Status interface found (pass protected)

+ /admin/login.jsp: Tomcat Server Administration interface found

+ 7663 requests: 2 error(s) and 28 item(s) reported on remote host

+ End Time: 2016-04-18 12:20:13 (GMT-4) (112 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

## The Second Target – Windows 7

Anonymous access: <none>

| IPC$:

| warning: Couldn't get details for share: NT\_STATUS\_ACCESS\_DENIED

|\_ Anonymous access: READ

Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds

Checking for MS08-067..

The target is NOT vulnerable!

########## Bruteforcing all users with 'password', blank and username as password

Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2016-04-18 12:11:30

[ERROR] File for logins is empty: /tmp/192.168.10.139-users.txt

To get a shell use:

/usr/local/bin/psexec.py <user>:<password>@192.168.10.139 cmd.exe