Lab5 – VulnScanning

You can use this lab manual for your personal documentation. Use screenshots for your own documentation, there will be questions later on that may point to this lab manual. Take care to check if you need to collect some information from the lab for the answers.

\ at the end of the line is used to mark that the command needs to be on one line. Replace **student-id** with your own student-id and **x** or **y** as your VMs correct IP in the labs.

For this lab you will need a local copy of the Target webserver. The target server template can be found in \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\apukoneet. Credentials for the target are **root / root66**

This lab also uses tools from Kali for scanning. Grab the latest Kali image from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\. Credentials for the Kali are **root / toor**

You can use your own Kali if you have own already

NOTE! Set the VMs to use VirtualBox ***Host-Only*** network and check the IP addresses of the VMs. For this lab, DO NOT use Bridged or NAT network, so you don't accidentally scan other targets than the target-server. Double-check target IP addresses for correct results.

Using tools described in the lab, scan the target server for vulnerabilities. Using the results, write a short recommendation to your CTO (Teacher) on what are the most critical vulnerabilities and what mitigation steps should be taken.

Do NOT copy-paste the results or screenshots of the output of the tools. You have to do some digging on what the results actually mean, and what issues are actually relevant.

This lab is graded 4 points, 1 point for a correctly identified vulnerability.

Use the following tools:

- nmap, a generic port scan and OS detection tool

A good starting point for nmap parameters: nmap -A -T4 -p-

- NIKTO, web application scanner
- lynis (https://cisofy.com/lynis/), a host-based security auditing tool. NOTE! Install and run this tool directly ON the Target server

Installing lynis:

```
wget https://downloads.cisofy.com/lynis/lynis-2.7.0.tar.gz
tar -xvf lynis-2.7.0.tar.gz
cd lynis
./lynis audit system
```

You can also use any other tools for further analysis, but these three should point out at least 4 obvbious vulnerabilities/attack vectors.

```
root@kali:~# nmap -sP 192.168.56.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-20 12:22 EET
Nmap scan report for 192.168.56.100
Host is up (0.00025s latency).
MAC Address: 08:00:27:6E:4A:FF (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.00018s latency).
MAC Address: 08:00:27:95:AB:C6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 31.27 seconds
```

```
root@kali:~# nmap -sV -A 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-20 12:25 EET
Nmap scan report for 192.168.56.101
Host is up (0.00037s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 c5:75:64:ef:bf:e4:7c:30:54:eb:94:03:ed:f1:cf:15 (RSA)
|   256 e8:ae:cd:d3:dd:ca:3e:95:a2:89:d4:6a:fb:8d:97:67 (ECDSA)
|_  256 a0:f9:d0:3f:b8:35:e0:e7:6a:18:7b:4a:2e:dc:ae:49 (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|_  100000  2,3,4        111/udp  rpcbind
3306/tcp open  mysql   MySQL 5.5.60-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.60-MariaDB
|   Thread ID: 5
|   Capabilities flags: 63487
|   Some Capabilities: FoundRows, Support41Auth, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, IgnoreSigpipes, ConnectWithDatabase, Speaks41ProtocolOld,
ODBCClient, InteractiveClient, Speaks41ProtocolNew, LongPassword, LongColumnFlag, SupportsCompression, SupportsTransactions, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthP
lugins
|   Status: Autocommit
|   Salt: (8^?Vtct@~{pB5!G!l!\
|_  Auth Plugin Name: 87
MAC Address: 08:00:27:95:AB:C6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

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

admin sivulle pääsy pitäisi olla evätty

/phpindo() sivusto on kaikkien nähtävillä, täältä löytyy kaikenlaista tietoa kohdekoneesta.

sudoers fileen kaikilla kaikki käyttöoikeudet, kuka tahansa joka pääsee koneelle voi lisäät sudo oikeudet kenelle tahansa kättäjälle

Centos Linux release 7.4.1708

```
+ OSVDB-112004: /: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-112004: /index.php: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
```

http trace metodi on aktiivinen, hyökkääjä voi tarkkailla http pyyntöjä, mitä serverille tulee.