

Name: Cristian Barreno

## Vulnerability Scanning Exercise 1

### Prerequisites

- Linux Ubuntu 22.04 Server
- nmap installed
- git installed



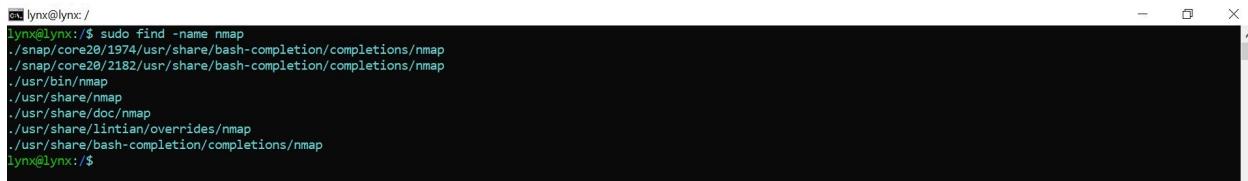
```
crux:~ lynx@lynx:~  
lynx@lynx:~$ git --version  
git version 2.34.1  
lynx@lynx:~$
```

By typing `git --version` i can see that git is installed and the current version.

### Task 1

#### Step 1

`find -name nmap`

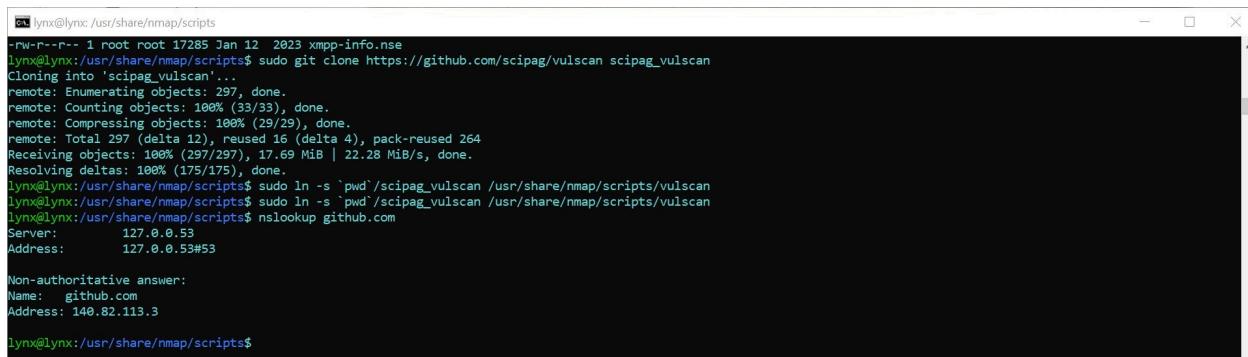


```
crux:~ lynx@lynx:~  
lynx@lynx:~$ sudo find -name nmap  
./snap/core20/1974/usr/share/bash-completion/completions/nmap  
./snap/core20/2182/usr/share/bash-completion/completions/nmap  
./usr/bin/nmap  
./usr/share/nmap  
./usr/share/doc/nmap  
./usr/share/lintian/overrides/nmap  
./usr/share/bash-completion/completions/nmap  
lynx@lynx:~$
```

I used `sudo find` to locate nmap. From the screenshot above i see that nmap lives in `./usr/share/nmap`

#### Step 2

Installing Vulnerability scanner built within the nmap application.



```
crux:~ lynx@lynx:/usr/share/nmap/scripts  
-rw-r--r-- 1 root root 17285 Jan 12 2023 xmpp-info.nse  
lynx@lynx:/usr/share/nmap/scripts$ sudo git clone https://github.com/scipag/vulscan scipag_vulscan  
Cloning into 'scipag_vulscan'...  
remote: Enumerating objects: 297, done.  
remote: Counting objects: 100% (33/33), done.  
remote: Compressing objects: 100% (29/29), done.  
remote: Total 297 (delta 12), reused 16 (delta 4), pack-reused 264  
Receiving objects: 100% (297/297), 17.69 MiB | 22.28 MiB/s, done.  
Resolving deltas: 100% (175/175), done.  
lynx@lynx:/usr/share/nmap/scripts$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan  
lynx@lynx:/usr/share/nmap/scripts$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan  
lynx@lynx:/usr/share/nmap/scripts$ nslookup github.com  
Server: 127.0.0.53  
Address: 127.0.0.53#53  
  
Non-authoritative answer:  
Name: github.com  
Address: 140.82.113.3  
lynx@lynx:/usr/share/nmap/scripts$
```

In the screenshot above i navigate to `./usr/share/nmap/scripts`. Then in the script folder I cloned the Github repository like this:

`git clone https://github.com/scipag/vulscan scipag_vulscan`  
`ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan`

I used ls -l to list the content of /usr/share/nmap/scripts/scipag\_vulscan

```
lynx@lynx:/usr/share/nmap/scripts/scipag_vulscan$ ls -l
total 40420
-rw-r--r-- 1 root root    27 Mar 23 01:46 _config.yml
-rw-r--r-- 1 root root  70364 Mar 23 01:46 COPYING.TXT
-rw-r--r-- 1 root root 16756993 Mar 23 01:46 cve.csv
-rw-r--r-- 1 root root 1864748 Mar 23 01:46 exploitdb.csv
-rw-r--r-- 1 root root   53779 Mar 23 01:46 logo.png
-rw-r--r-- 1 root root 1524310 Mar 23 01:46 openvas.csv
-rw-r--r-- 1 root root  6718903 Mar 23 01:46 osvdb.csv
-rw-r--r-- 1 root root   5817 Mar 23 01:46 README.md
lrwxrwxrwx 1 root root     38 Mar 23 01:46 scipag_vulscan -> /usr/share/nmap/scripts/scipag_vulscan
-rw-r--r-- 1 root root  683851 Mar 23 01:46 scipvuldb.csv
-rw-r--r-- 1 root root 7227028 Mar 23 01:46 securityfocus.csv
-rw-r--r-- 1 root root 1826158 Mar 23 01:46 securitytracker.csv
-rw-r--r-- 1 root root   361 Mar 23 01:46 update.ps1
-rw-r--r-- 1 root root   320 Mar 23 01:46 update.sh
drwxr-xr-x 4 root root   4096 Mar 23 01:46 utilities
-rw-r--r-- 1 root root  17230 Mar 23 01:46 vulscan.nse
-rw-r--r-- 1 root root 4576711 Mar 23 01:46 xforce.csv
lynx@lynx:/usr/share/nmap/scripts/scipag_vulscan$
```

## Step 3

Vulnerabilities on scanme.nmap.org

I redirected the vulnerabilities found on scanme.nmap.org and redirected the output to a file by using linux redirection

nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org > scanme.nmap.org\_vulnscan

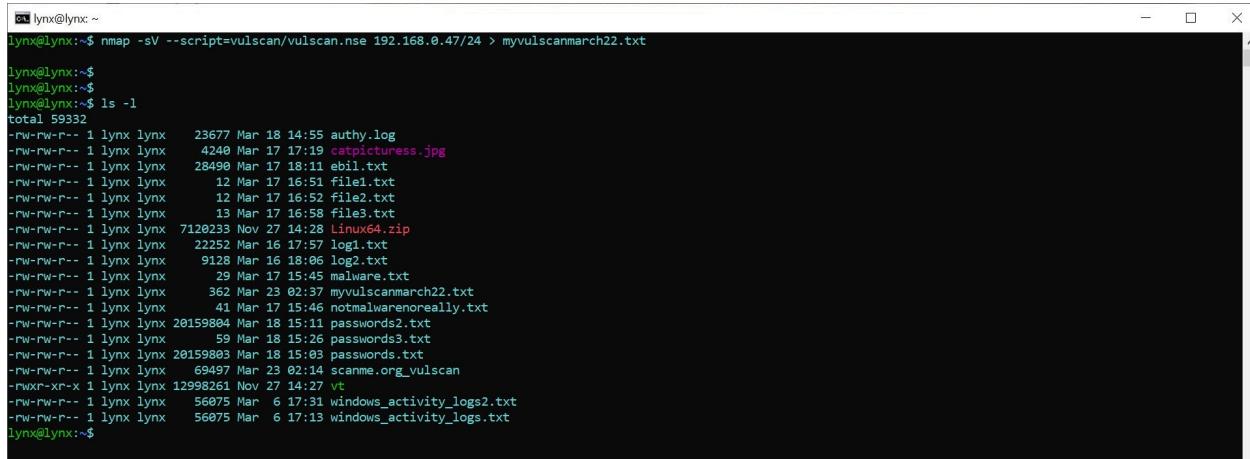
```
lynx@lynx:~
lynx@lynx:/usr/share/nmap/scripts/scipag_vulscan$ cd
lynx@lynx:~$ nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org > scanme.org_vulscan
lynx@lynx:~$
```

## Task 2

Scan your own network for vulnerabilities.

Once I found my network id and CIDR i used the following command to redirect the output to a folder:

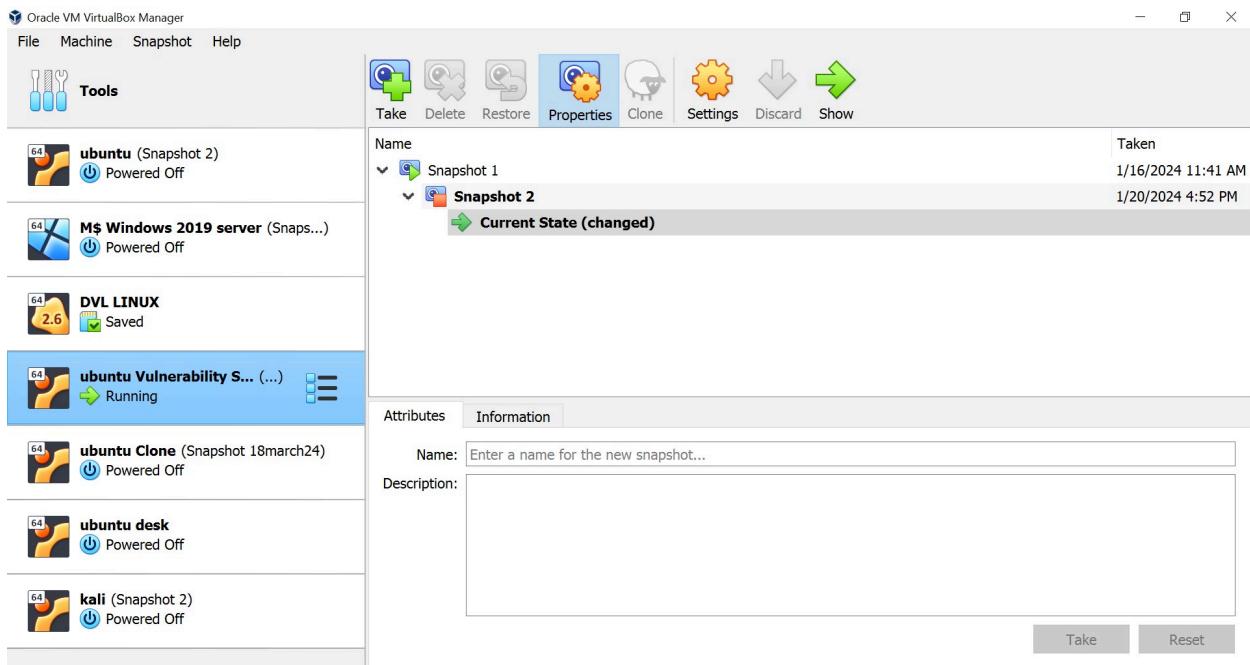
```
nmap -sV --script=vulscan/vulscan.nse 192.168.0.27/24 > myvulscanmarch22
```



```
lynx@lynx:~$ nmap -sV --script=vulscan/vulscan.nse 192.168.0.47/24 > myvulscanmarch22.txt
lynx@lynx:~$ ls -l
total 5932
-rw-rw-r-- 1 lynx lynx 23677 Mar 18 14:55 authy.log
-rw-rw-r-- 1 lynx lynx 4240 Mar 17 17:19 catpicturess.jpg
-rw-rw-r-- 1 lynx lynx 28490 Mar 17 18:11 ebil.txt
-rw-rw-r-- 1 lynx lynx 12 Mar 17 16:51 file1.txt
-rw-rw-r-- 1 lynx lynx 12 Mar 17 16:52 file2.txt
-rw-rw-r-- 1 lynx lynx 13 Mar 17 16:54 file3.txt
-rw-rw-r-- 1 lynx lynx 7128233 Nov 27 14:28 Linux64.zip
-rw-rw-r-- 1 lynx lynx 22252 Mar 16 17:57 log1.txt
-rw-rw-r-- 1 lynx lynx 9128 Mar 16 18:06 log2.txt
-rw-rw-r-- 1 lynx lynx 29 Mar 17 15:45 malware.txt
-rw-rw-r-- 1 lynx lynx 362 Mar 23 02:37 myvulscanmarch22.txt
-rw-rw-r-- 1 lynx lynx 41 Mar 17 15:40 notmalwareoreally.txt
-rw-rw-r-- 1 lynx lynx 20159804 Mar 18 15:11 passwords2.txt
-rw-rw-r-- 1 lynx lynx 59 Mar 18 15:24 passwords3.txt
-rw-rw-r-- 1 lynx lynx 20159803 Mar 18 15:03 passwords.txt
-rw-rw-r-- 1 lynx lynx 69497 Mar 23 02:14 scanme.org_vulscan
-rw-r--r-- 1 lynx lynx 12998261 Nov 27 14:27 vt
-rw-rw-r-- 1 lynx lynx 56075 Mar 6 17:31 windows_activity_logs2.txt
-rw-rw-r-- 1 lynx lynx 56075 Mar 6 17:13 windows_activity_logs.txt
lynx@lynx:~$
```

## Task 3

Download a version of Linux called “DamnVulnerableLinux”



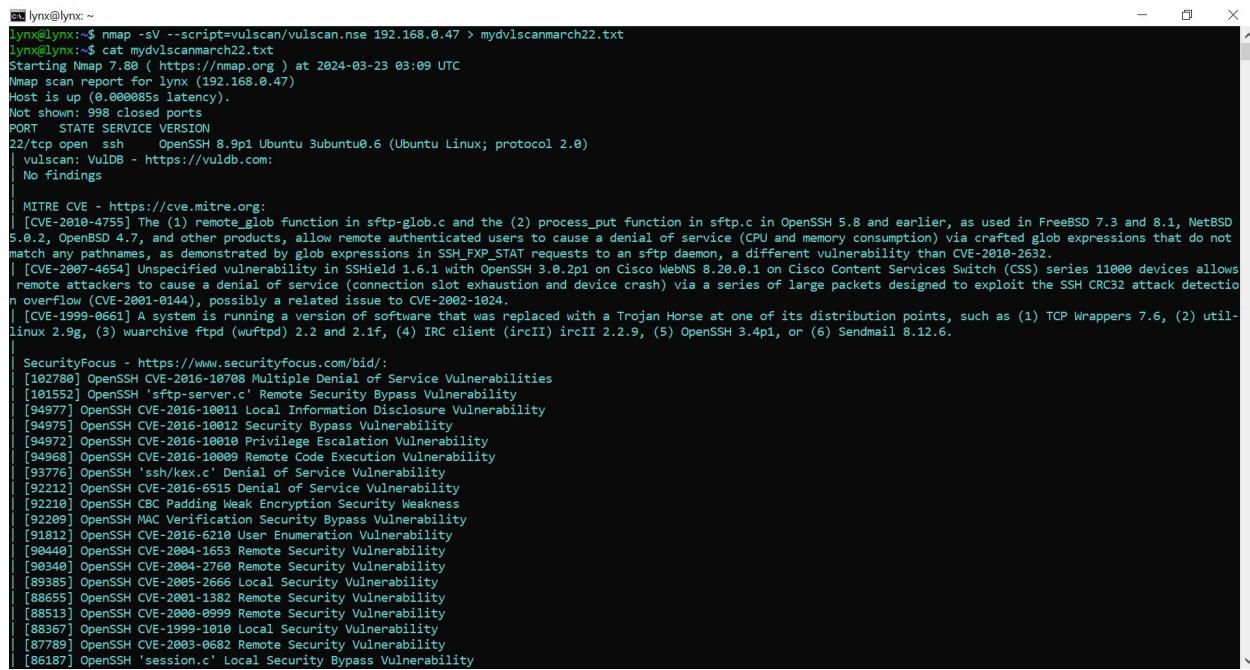
I installed “DamnVulnerableLinux” on VirtualBox. This version of linux is vulnerable to things.

I ran the ifconfig command in my DVL machine to obtain the IP address, then I opened a CMD prompt on my Host OS, and I SSH into the Linux Server – Vulnerability Scanner.

In the screenshot below i ran:

```
nmap -sV --script=vulscan/vulscan.nse 192.168.0.47 > mydvlscanmarch22.txt
```

To redirect the scan to a file.



```
lynx@lynx: ~
lynx@lynx: ~$ nmap -sV --script=vulscan/vulscan.nse 192.168.0.47 > mydvlscanmarch22.txt
lynx@lynx: ~$ cat mydvlscanmarch22.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-23 03:09 UTC
Nmap scan report for lynx (192.168.0.47)
Host is up (0.000085s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
|_ vulscan: VulDB - https://vuldb.com/
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2010-4755] The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.
| [CVE-2007-4654] Unspecified vulnerability in SSHield 1.6.1 with OpenSSH 3.0.2p1 on Cisco WebNS 8.20.0.1 on Cisco Content Services Switch (CSS) series 11000 devices allows remote attackers to cause a denial of service (connection slot exhaustion and device crash) via a series of large packets designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144), possibly a related issue to CVE-2002-1024.
| [CVE-1999-0661] A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.
|
| SecurityFocus - https://www.securityfocus.com/bid:
[102780] OpenSSH CVE-2016-10788 Multiple Denial of Service Vulnerabilities
[101552] OpenSSH sftp-server.c Remote Security Bypass Vulnerability
[94977] OpenSSH CVE-2016-10011 Local Information Disclosure Vulnerability
[94975] OpenSSH CVE-2016-10012 Security Bypass Vulnerability
[94972] OpenSSH CVE-2016-10018 Privilege Escalation Vulnerability
[94968] OpenSSH CVE-2016-10009 Remote Code Execution Vulnerability
[93776] OpenSSH 'ssh/kex.c' Denial of Service Vulnerability
[92212] OpenSSH CVE-2016-6515 Denial of Service Vulnerability
[92210] OpenSSH CBC Padding Weak Encryption Security Weakness
[92209] OpenSSH MAC Verification Security Bypass Vulnerability
[91812] OpenSSH CVE-2016-6210 User Enumeration Vulnerability
[90440] OpenSSH CVE-2004-1653 Remote Security Vulnerability
[90348] OpenSSH CVE-2004-2760 Remote Security Vulnerability
[89385] OpenSSH CVE-2005-2666 Local Security Vulnerability
[88655] OpenSSH CVE-2001-1382 Remote Security Vulnerability
[88513] OpenSSH CVE-2000-0999 Remote Security Vulnerability
[88367] OpenSSH CVE-1999-1010 Local Security Vulnerability
[87789] OpenSSH CVE-2003-0682 Remote Security Vulnerability
[86187] OpenSSH 'session.c' Local Security Bypass Vulnerability
```

## Identify 3 vulnerabilities and generate a short executive summary on each.

**1 [CVE-1999-0661]** A system is running a version of software that was replaced with a Trojan Horse at one of its distribution points, such as (1) TCP Wrappers 7.6, (2) util-linux 2.9g, (3) wuarchive ftpd (wuftpd) 2.2 and 2.1f, (4) IRC client (ircII) ircII 2.2.9, (5) OpenSSH 3.4p1, or (6) Sendmail 8.12.6.

CVE-1999-0661 has a CVSS base score of 10, high severity, exploitability score of 10, and an impact score of 10. Published in 01/01/1999, and last modified in 10/17/2016.

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Currently there is no Common weakness enumeration number.

NIST NVD references links to Advisories, Solutions, and Tools for this CVE.

**2 [CVE-2012-4558]** Multiple cross-site scripting (XSS) vulnerabilities in the balancer\_handler function in the manager interface in mod\_proxy\_balancer.c in the mod\_proxy\_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

Cross-site scripting vulnerabilities occur when untrusted data enters a web application, from web request. A victim visits the website that contains a malicious script. Once the malicious script is injected, the attacker gains control and could do many malicious activities. There are many potential mitigation phases from architecture and design to environmental hardening.

CVE-2012-4558 has a CVSS base score of 4.3, medium severity, exploitability score of 8.6, and an impact score of 2.9. Published on 02/26/2013, and last modified on 11/06/2023.

**3 [CVE-2013-2249]** mod\_session\_dbd.c in the mod\_session\_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

CVE-2013-2249 has a CVSS base score of 7.5, high severity, exploitability score of 10, and an impact score of 6.4. Published on 07/23/2013, and last modified on 11/06/2023.

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Currently there is no Common weakness enumeration number.