Name: Cristian Barreno

Vulnerability Scanning Exercise 1

Prerequisites

- Linux Ubuntu 22.04 Server
- nmap installed
- git installed

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

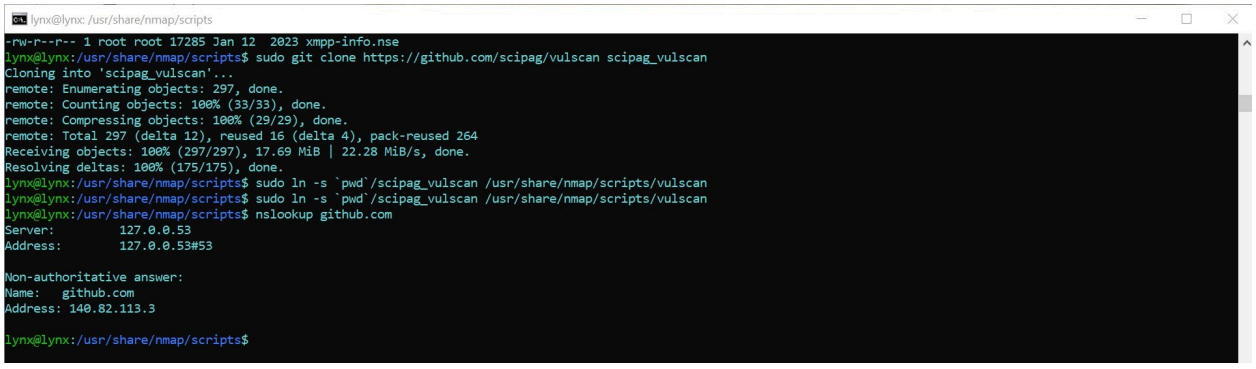
Task 1

Step 1
find -name nmap

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.



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

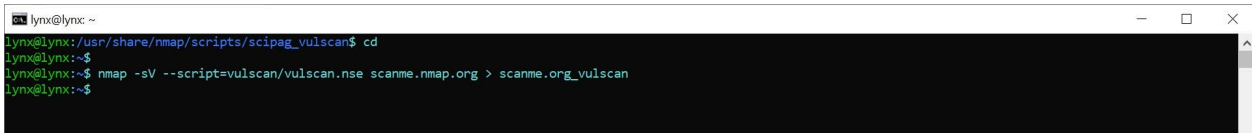
I used ls -l to list the content of /usr/share/nmap/scripts/scipag_vulscan

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

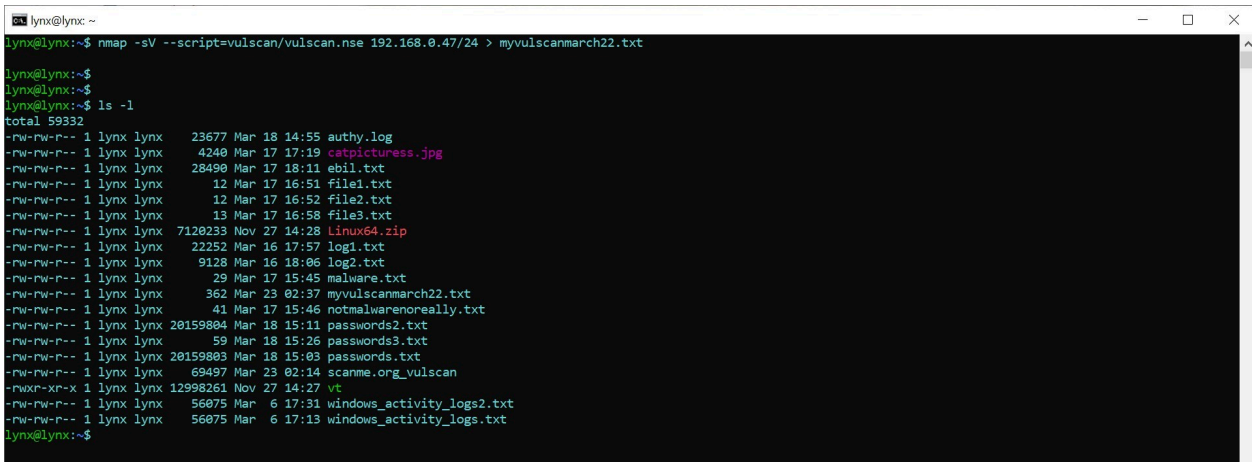


Task 2

Scan your own network for vulnerabilities.

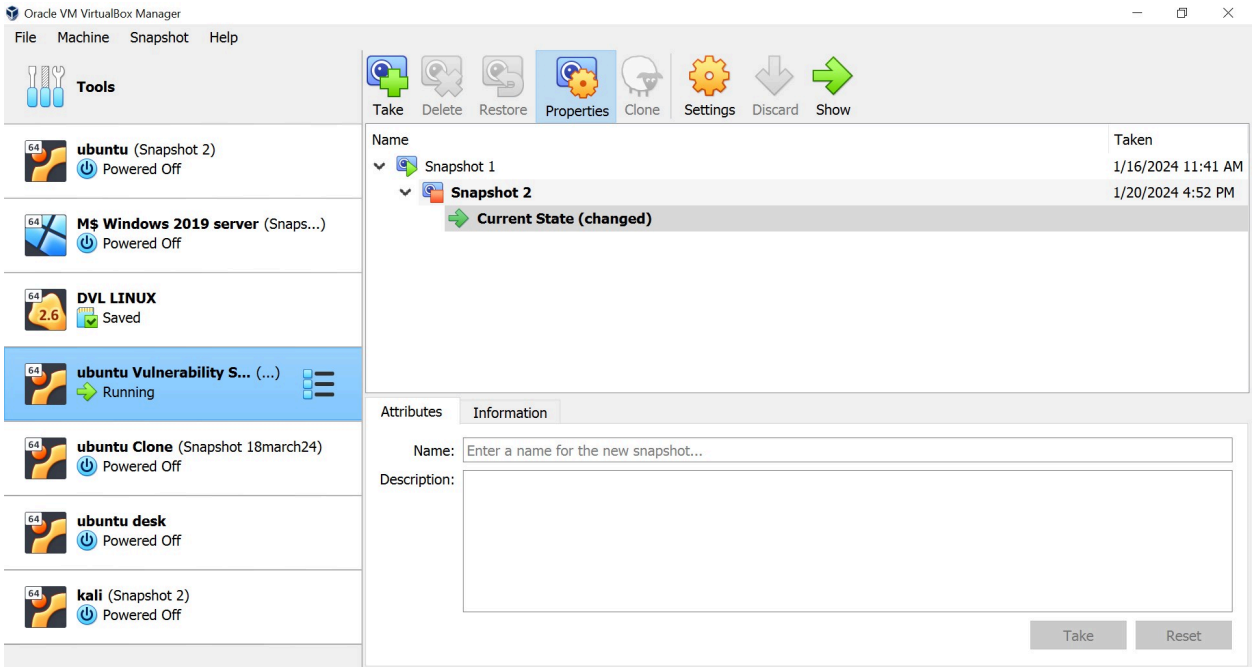
Once I found my network id and CIDR i used the following command to redirect the output to a folder:

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



Task 3

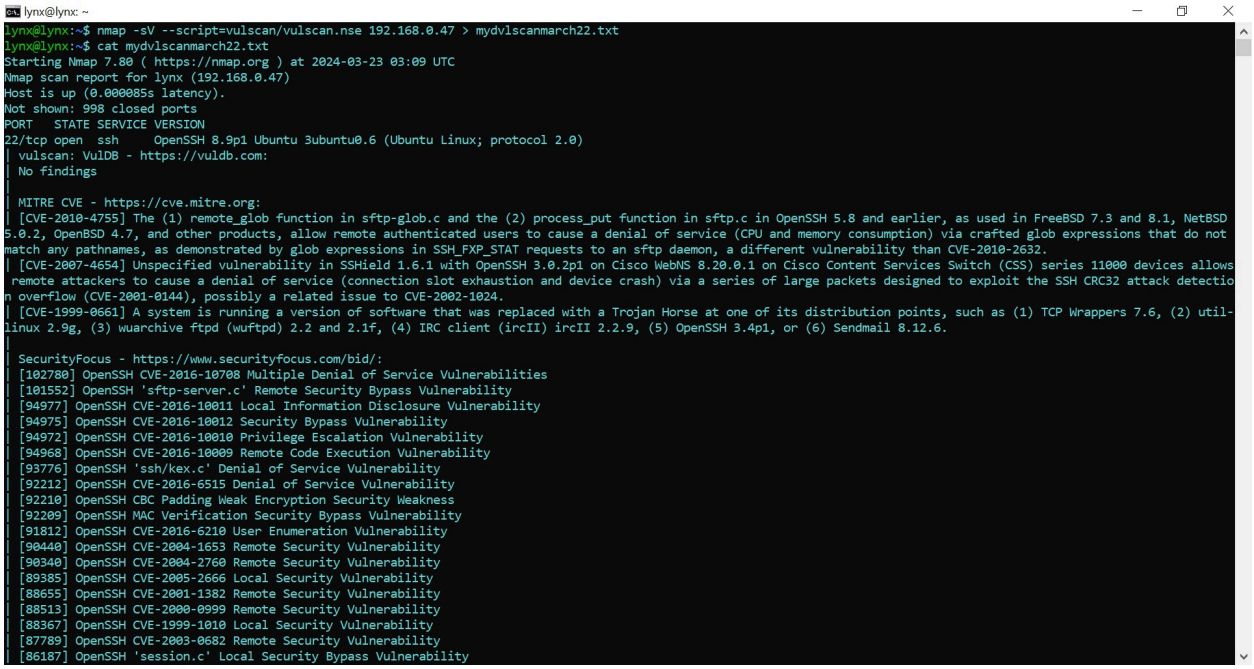
Download a version of Linux called “DamnVulnerableLinux”



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.



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.