

SIMPLE WEB SCANNER

Prepared by: Noemi Mateo
NoemiM@genstudents.org

**Generation Singapore
Cloud Support & DevOps
2025 - Cohort 04**



Project Summary

Schedule a Cron Job at regular intervals, such as every 10 minutes, to initiate an nmap scan of the network and save the results to a text file. Additionally, incorporate several enhancements and display the findings in a web browser.

TASK A

- Set up a Virtual Machine and install Ubuntu.
- Install Apache2, PHP, and nmap.
- Adjust Ownership and Permissions accordingly.

```
noemi@noemi-VirtualBox:~$  
noemi@noemi-VirtualBox:~$ sudo apt-get install apache2  
Reading package lists... Done  
  
noemi@noemi-VirtualBox:~$ sudo apt-get install php  
Reading package lists... Done  
  
noemi@noemi-VirtualBox:~$ php -v  
PHP 8.3.6 (cli) (built: Mar 19 2025 10:08:38) (NTS)  
Copyright (c) The PHP Group  
Zend Engine v4.3.6, Copyright (c) Zend Technologies  
    with Zend OPcache v8.3.6, Copyright (c), by Zend Technologies  
noemi@noemi-VirtualBox:~$ sudo apt-get install nmap  
Reading package lists... Done  
  
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...  
noemi@noemi-VirtualBox:~$ sudo service apache2 restart  
noemi@noemi-VirtualBox:~$
```

```
noemi@noemi-VirtualBox:~$ sudo chown noemi /var/www/html  
noemi@noemi-VirtualBox:~$ sudo chmod 744 /var/www/html  
noemi@noemi-VirtualBox:~$ ll /var/www/html  
total 20  
drwxr--r-- 2 noemi root 4096 Apr 3 21:23 ./  
drwxr-xr-x 3 root root 4096 Apr 3 21:23 ../  
-rw-r--r-- 1 root root 10671 Apr 3 21:23 index.html  
noemi@noemi-VirtualBox:~$ sudo crontab -e  
no crontab for root - using an empty one  
  
Select an editor. To change later, run 'select-editor'.  
1. /bin/nano      <---- easiest  
2. /usr/bin/vim.basic  
3. /usr/bin/vim.tiny  
4. /bin/ed  
  
Choose 1-4 [1]: 2  
  
# m h dom mon dow   command  
  
*/10 * * * * nmap 192.168.1.0/24 -O -oN /var/www/html/nmap.html
```

TASK B

- Configure the Cron Job.
- Develop the network.php file.

Learning Objectives

- Install and navigate a Linux distribution.
- Gain insight into the User Interface (UI) and Command Line Interface (CLI) of Linux (Ubuntu).
- Create Cron Jobs for scheduled tasks (crontab).
- Become familiar with NMAP.
- Understand basic file and folder permission changes and ownership (chmod, chown, members, groups).

The Virtual Box was already set up with a bridged connection to the internet.

The Linux distribution in use is Ubuntu 24.04.2 LTS.

For TASK A, my first step was to execute the command sudo apt-get update

to update the package management system. Subsequently, I successfully installed apache2, php, and nmap, and to apply all changes, I needed to restart apache2 using

sudo service apache2 restart

I modified the ownership of the html directory located within the www directory, which is under var, to my user account with the command

sudo chown noemi /var/www/html.

Additionally, I adjusted the permissions to 777, granting full access to all users with

sudo chmod 777 /var/www/html

Moving on to TASK B, I set up a Cron Job to initiate a web scan every 10 minutes, every hour, every day, every month, and every day of the week using the command:

**/10 * * * * nmap 192.168.1.0/24 -O -oN /var/www/html/nmap.html*

The Cron Job was configured to examine the devices on the network, determine the operating system (-O) running on each device, along with all the additional information typically gathered by nmap, and to format this output as standard text (-oN) prior to saving it in nmap.html. This file would serve as the foundation for the website content displayed by the apache2 server when requests are made from the browser.

Before the content could be presented, I needed to produce a PHP file that would structure it in a way that is more user-friendly and visually appealing for those seeking the information. The network.php file was developed using



A screenshot of a code editor window titled "network.php" located at "/var/www/html". The code is as follows:

```
<?php  
  
date_default_timezone_set("Asia/Singapore");  
  
echo "Server Timestamp: ";  
echo date("h:i:sa");  
  
echo "<pre>";  
include("nmap.html");  
echo "</pre>";  
  
?>
```

a text editor and was subsequently saved in the /var/www/html/ directory.

It essentially presents a timestamp followed by the scan details as specified in the crontab, including the scan type, target IP addresses, and the file designated to hold the scan output. Subsequently, the file displays all the scan results in an organized format. Clearly, the use of the <pre></pre> tags enhances the text's layout; without them, the information would appear as a continuous block. I included a line at the top to adjust the time to the Asia/Singapore timezone.

Bonus Task A

As previously stated, I initially assigned 777 harmful choice available permissions to the html directory.

This configuration granted me root permissions, privileges required to along with identical access to any users in the same group and everyone else.

In terms of security, this permission configuration stands as the most To protect your data and systems effectively, it is essential to grant users only the minimum privileges required to complete their tasks. The value 7 corresponds to read (4), write (2), and execute (1) permissions. Since directories require executable permissions, I opted to modify the setting to 755, as other permission combinations would restrict my access to the nmap output, despite my attempts with various values.

 Chrome File Edit View History Bookmarks Profiles Tab Window Help

Server Timestamp: 11:44:09pm

```
# Nmap 7.94SVN scan initiated Thu Apr  3 23:40:01 2025 as: nmap -oN /var/www/html/nmap.html 192.168.1.106
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
Warning: 192.168.1.109 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
1185/tcp  open  catchpole
3000/tcp  open  ppp
3001/tcp  open  nessus
7778/tcp  open  interwise
9880/tcp  open  glrp
9998/tcp  open  distinct32
MAC Address: C8:08:E9:35:F4:D2 (LG Electronics)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Network Distance: 1 hop

Nmap scan report for 192.168.1.2
Host is up (0.050s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: BC:FF:4D:05:04:E9 (Espressif)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
Device type: specialized/general purpose
Running: Espressif embedded, lwIP, NodeMCU embedded
OS CPE: cpe:a:lwip_project:lwip cpe:/o:nodemcu:nodemcu
OS details: Espressif esp8266 firmware (lwIP stack), NodeMCU firmware (lwIP stack)
Network Distance: 1 hop

Nmap scan report for 192.168.1.6
Host is up (0.024s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
9100/tcp  open  jettdirect
MAC Address: E0:B8:9E:FC:D1:7E (Seiko Epson)
Device type: phone/general purpose
Running: Google Android 4.1.X, Linux 4.X
OS CPE: cpe:/o:google:android:4.1.2 cpe:/o:linux:linux_kernel:4.4.2
OS details: Android 4.1.2, DD-WRT v3.0 (Linux 4.4.2)
Network Distance: 1 hop

Nmap scan report for _gateway (192.168.1.8)
Host is up (0.011s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
443/tcp   open  https
5443/tcp  open  https
5631/tcp  open  ipp
59100/tcp open  jettdirect
MAC Address: 00:0C:29:4B:0A:00 (Huawei)
Device type: general purpose
Running: Linux 4.1.X, Linux 4.4.2
OS CPE: cpe:/o:huawei:firmware:4.1.2 cpe:/o:linux:linux_kernel:4.4.2
OS details: Linux 4.1.2, Linux 4.4.2
Network Distance: 1 hop

Nmap scan report for _gateway (192.168.1.8)
Host is up (0.011s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
443/tcp   open  https
5443/tcp  open  https
5631/tcp  open  ipp
59100/tcp open  jettdirect
MAC Address: 00:0C:29:4B:0A:00 (Huawei)
Device type: general purpose
Running: Linux 4.1.X, Linux 4.4.2
OS CPE: cpe:/o:huawei:firmware:4.1.2 cpe:/o:linux:linux_kernel:4.4.2
OS details: Linux 4.1.2, Linux 4.4.2
Network Distance: 1 hop

Nmap scan report for 192.168.1.106
Host is up (0.0063s latency).
All 1000 scanned ports on 192.168.1.106 are in ignored states.
Warning: 192.168.1.109 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
1185/tcp  open  catchpole
3000/tcp  open  ppp
3001/tcp  open  nessus
7778/tcp  open  interwise
9880/tcp  open  glrp
9998/tcp  open  distinct32
MAC Address: C8:08:E9:35:F4:D2 (LG Electronics)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Network Distance: 1 hop

Nmap scan report for 192.168.1.2
Host is up (0.050s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: BC:FF:4D:05:04:E9 (Espressif)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
Device type: specialized/general purpose
Running: Espressif embedded, lwIP, NodeMCU embedded
OS CPE: cpe:a:lwip_project:lwip cpe:/o:nodemcu:nodemcu
OS details: Espressif esp8266 firmware (lwIP stack), NodeMCU firmware (lwIP stack)
Network Distance: 1 hop

Nmap scan report for 192.168.1.6
Host is up (0.024s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
9100/tcp  open  jettdirect
MAC Address: E0:B8:9E:FC:D1:7E (Seiko Epson)
Device type: phone/general purpose
Running: Google Android 4.1.X, Linux 4.X
OS CPE: cpe:/o:google:android:4.1.2 cpe:/o:linux:linux_kernel:4.4.2
OS details: Android 4.1.2, DD-WRT v3.0 (Linux 4.4.2)
Network Distance: 1 hop

Nmap scan report for _gateway (192.168.1.8)
Host is up (0.011s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
443/tcp   open  https
5443/tcp  open  https
5631/tcp  open  ipp
59100/tcp open  jettdirect
MAC Address: 00:0C:29:4B:0A:00 (Huawei)
Device type: general purpose
Running: Linux 4.1.X, Linux 4.4.2
OS CPE: cpe:/o:huawei:firmware:4.1.2 cpe:/o:linux:linux_kernel:4.4.2
OS details: Linux 4.1.2, Linux 4.4.2
Network Distance: 1 hop
```

Timestamp: 11:43:59pm

```
0:45VN scan initiated Thu Apr  3 23:40:01 2025 as: nmap -oN /var/www/html/rmap.html 192.168.1.0/24
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
as grown to over 2.3 seconds, decreasing to 2.0
192.168.1.101 giving up on port because retransmission cap hit (10).
tcp  192.168.1.101
up (0.0003s latency)
n: 994 closed tcp ports (reset)
STATE SERVICE
open httpd-ssl
open https
open ppp
open nessus
open interwise
open
open
open distinct32
ess: C8:0B:89:35:F4:D2 (LG Electronics)
ype: general purpose
Linux
cpu: /0linux/linux kernel:3
ls: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Distance: 1 hop

nmap-report for 192.168.1.2
```

```
Recycle Bin
Map Career Noemil 192.168.1.106: http://192.168.1.106/phpinfo + - d

Server Timestamp: 11:44:12pm

# Map 7.04GW scan initiated Thu Apr 3 23:46:01 2025 ss: nmap -o -n /var/www/html
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
RTTVar has grown to over 2.3 seconds, decreasing to 2.0
Warning: 192.168.1.106 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 994 closed tcp ports (reset)
      PORT      STATE SERVICE
115/tcp    open  catchpole
3080/tcp   open  ppp
3001/tcp   open  nessus
7778/tcp   open  interwise
9080/tcp   open  grlpc
9993/tcp   open  distict32
MAC Address: C8:EE:A9:35:F4:D2 (LG Electronics)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10, Linux 3.2 - 3.16
Network Distance: 1 hop

Nmap scan report for 192.168.1.2
Host is up (0.005s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 0F:EE:AA:91:EA (Microsoft Corporation)
```

```
noemi_m@Natee: ~
```

Bonus Task B

After conducting research and learning how to modify the /etc/netplan/01-network-manager-all.yaml file with the new configuration in vim, I confirmed that my Ubuntu was already connected via a bridged connection. I then attempted to access the network.php file on Ubuntu using the Safari browser on my host system, which was a MacBook Pro. Additionally, I was able to view the scan results from my Windows laptop, and the open WSL window serves as evidence that the connection was successfully established through the Edge browser on the Windows device.

```
noemi@noemi-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.106  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a027:fffe%enp0s3  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:3b:9e:31  txqueuelen 1000  (Ethernet)
            RX packets 103204  bytes 102995290 (102.9 MB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 21745  bytes 7058630 (7.0 MB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          ether 00:00:00:00:00:00  txqueuelen 1000  (Local Loopback)
            RX packets 2320  bytes 272240 (272.2 KB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 2320  bytes 272240 (272.2 KB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: false
      dhcp6: false
      addresses: [192.168.1.106/24]
      routes:
        - to: default
          via: 192.168.1.8
      nameservers:
        addresses: [192.168.1.254]
~
```

Recommendations

- Opt for permissions other than 777. Create users with minimal privileges, and add to the sudoers group for elevated access if needed.
- Utilize tools like nmap solely within your personal network and avoid their use on secure systems to prevent alerts. Refrain from using such tools at work to avoid triggering alarms or logs of suspicious activity.

Note: snapshot of nmap's impact on Windows laptop.

