**Scanning Networks**

**Tools:**

Nmap, Netdiscover, Masscan, and Apache2

Download:

This all tools are pre-installed in pentesting linux distro

NMAP: <https://nmap.org/download>

Masscan: <https://github.com/robertdavidgraham/masscan>

Netdiscover: [https://github.com/netdiscover- scanner/netdiscover](https://github.com/netdiscover-%20scanner/netdiscover)

Apache 2: <https://httpd.apache.org/download.cgi>

* **Performing network scanning and device discovery**

Nmap :Network mapper

Syntax: nmap [options] [target(url) or (ip)]

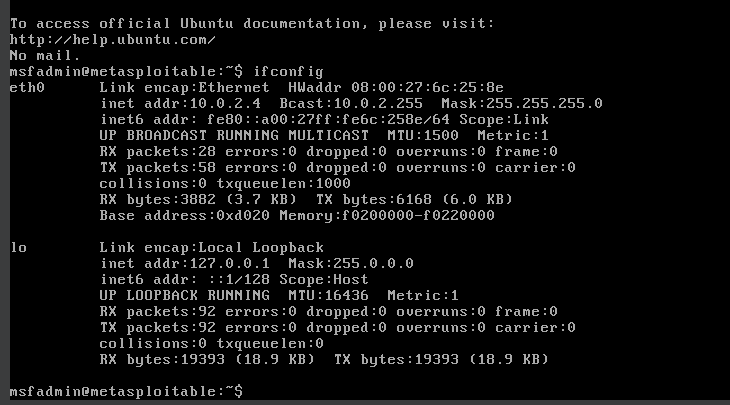
NOTICE:

Here we are using the metasploitable machine as a target because we don’t have any right or permissions to pentesting on any website available on internet

Some are the organization is provide websites for penetration tester to penetrate on it like acunetix,portswwiger etc..

But Metasploitable is vulnerable machine and the website is also configured in it so we get all on one plateform

Metasploitable IP [10.0.2.4] :different for all device



Nmap results :

Results of nmap for metasploitable

Command : nmap -sV -sC -A -p- -v 10.0.2.4

[-sV service version detection

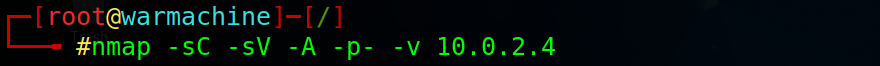
-sC default script scan

-A- aggressive scan

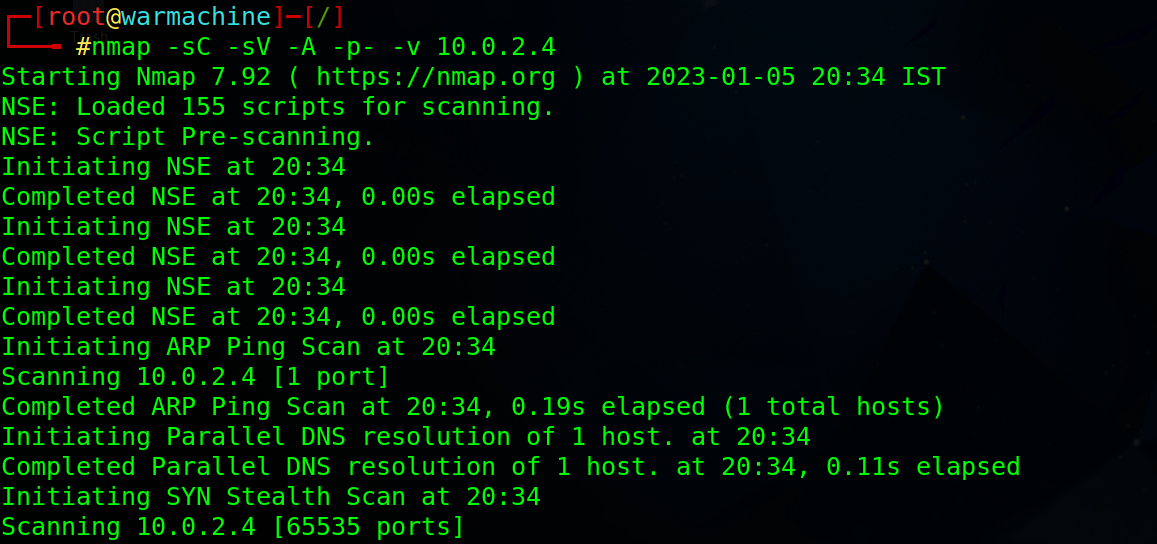
-p- scanning all ports

-v verbose]

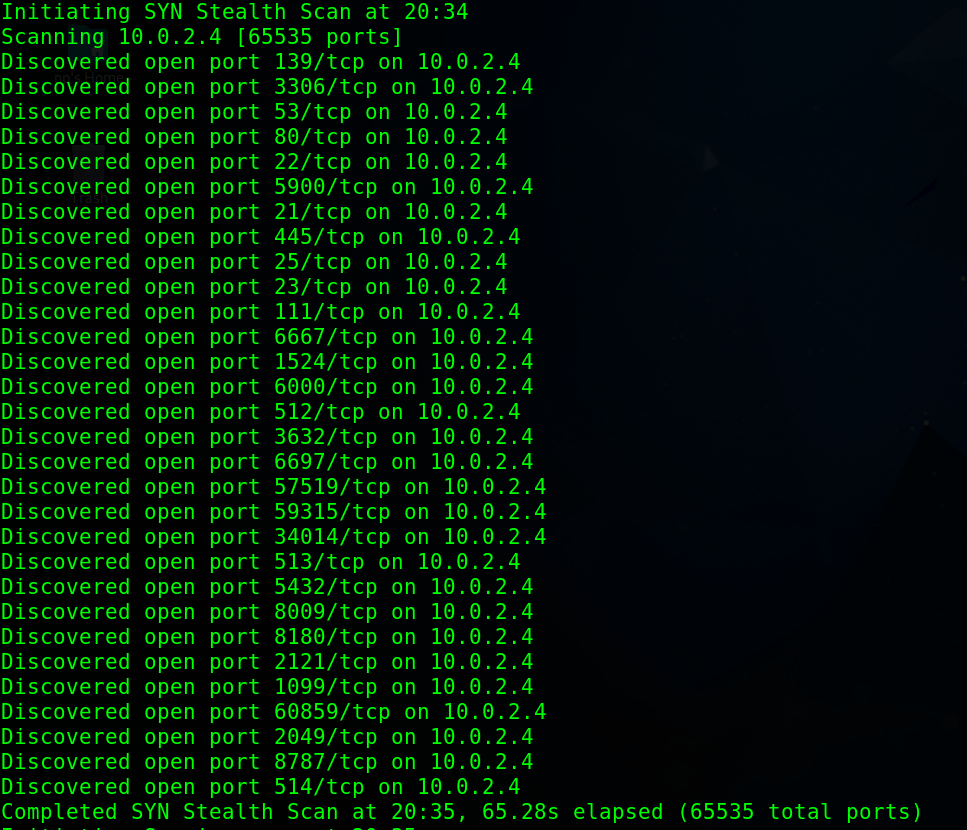
Syntax:



Scanning:

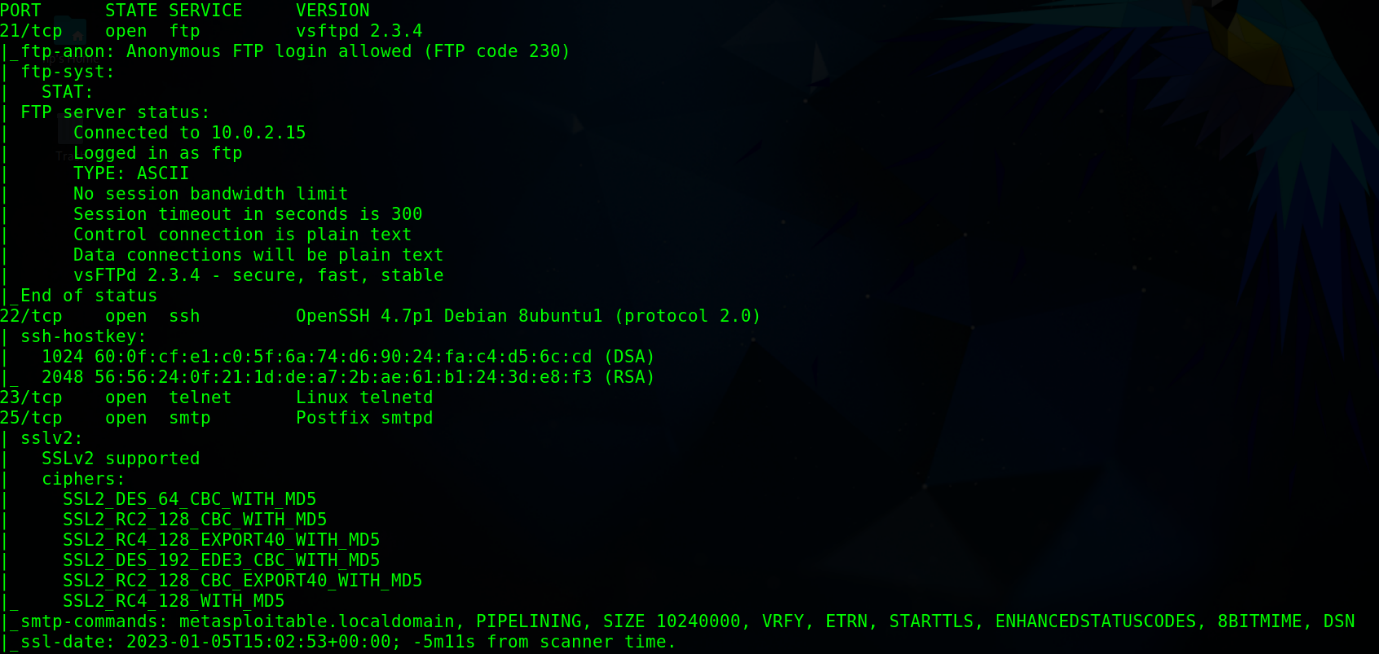


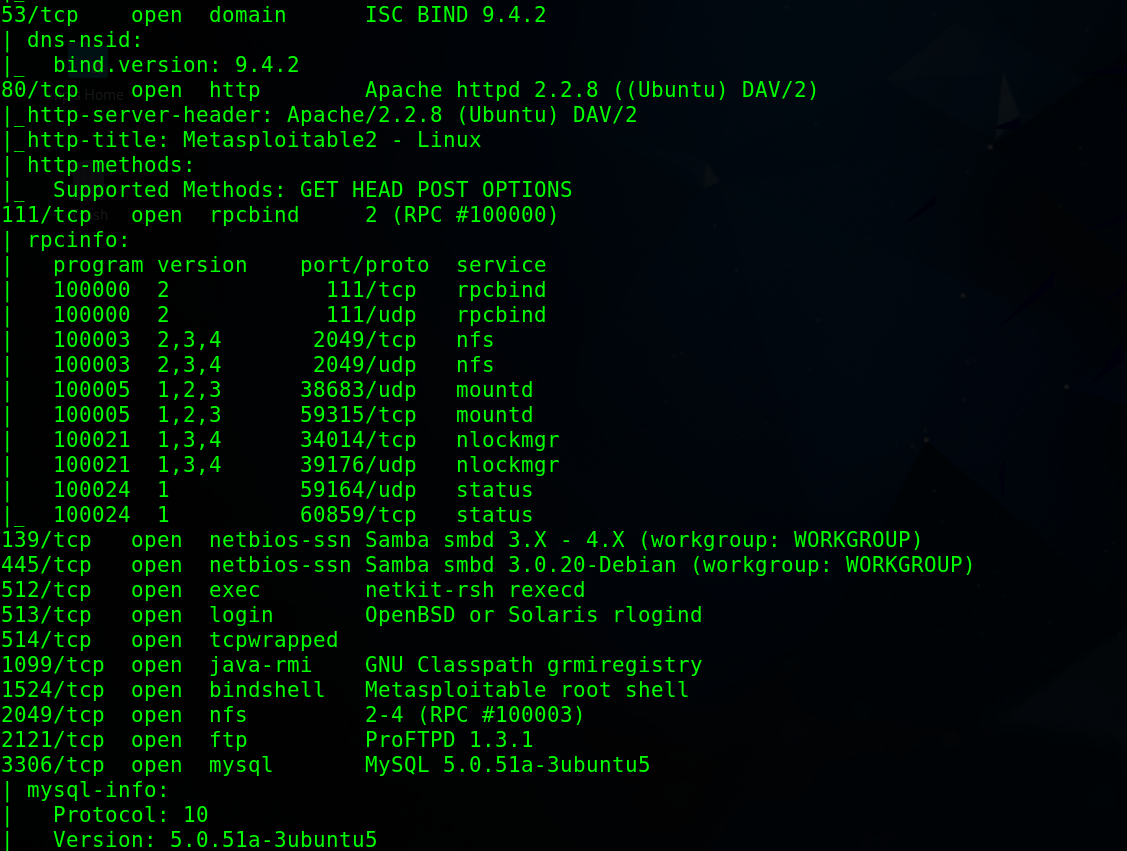
**Open ports:**

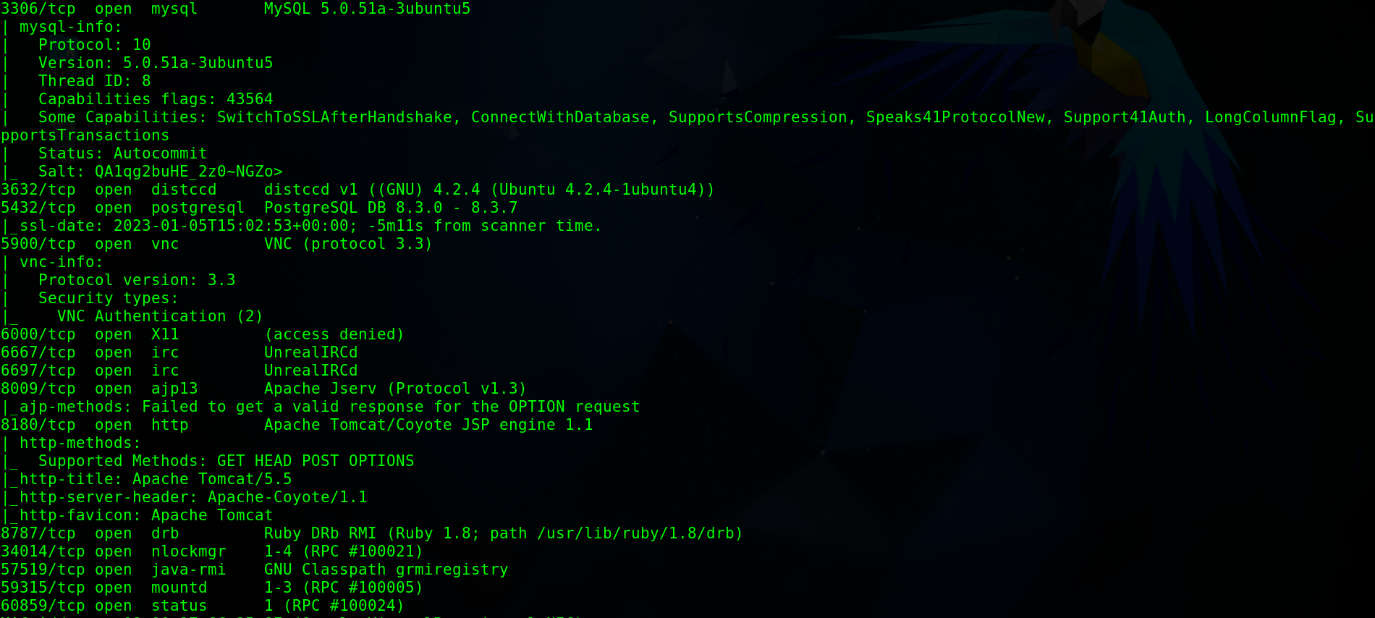


We scan all 65535 ports and get the all open ports from 0 to 65535

**Service and Service version:**







We got the sevices and the versions of service are running on different ports

**Port /Services**

21:ftp

22:ssh

23:telnet

25:smtp

53:domain

80:http

111:rpcbind

130:netbios-ssn

445:netbios-ssn

512:exec

513:login

514:tcpwrapped

1099:java-rmi

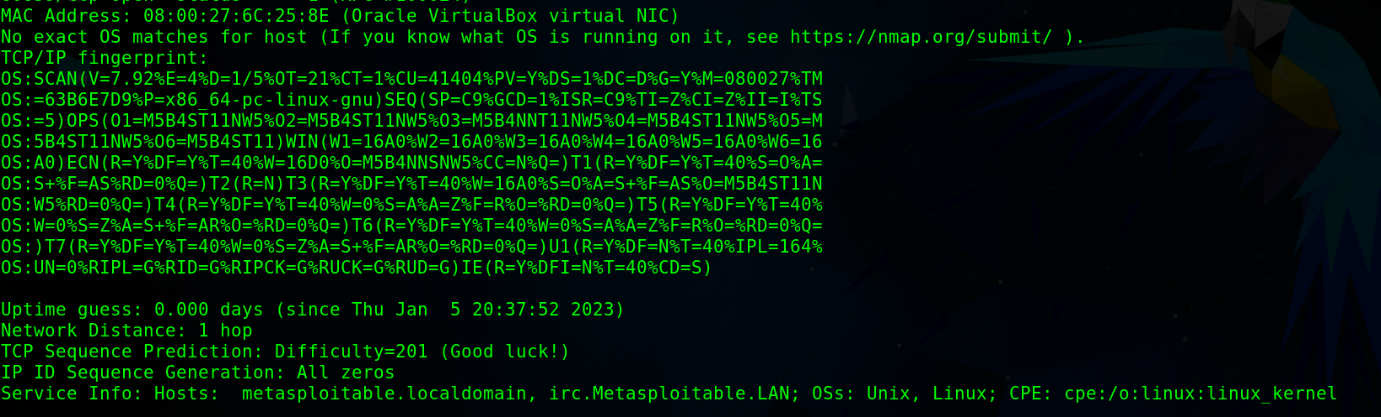
1524:bindshell

2049:nfs

2121:ftp

3306:mysql

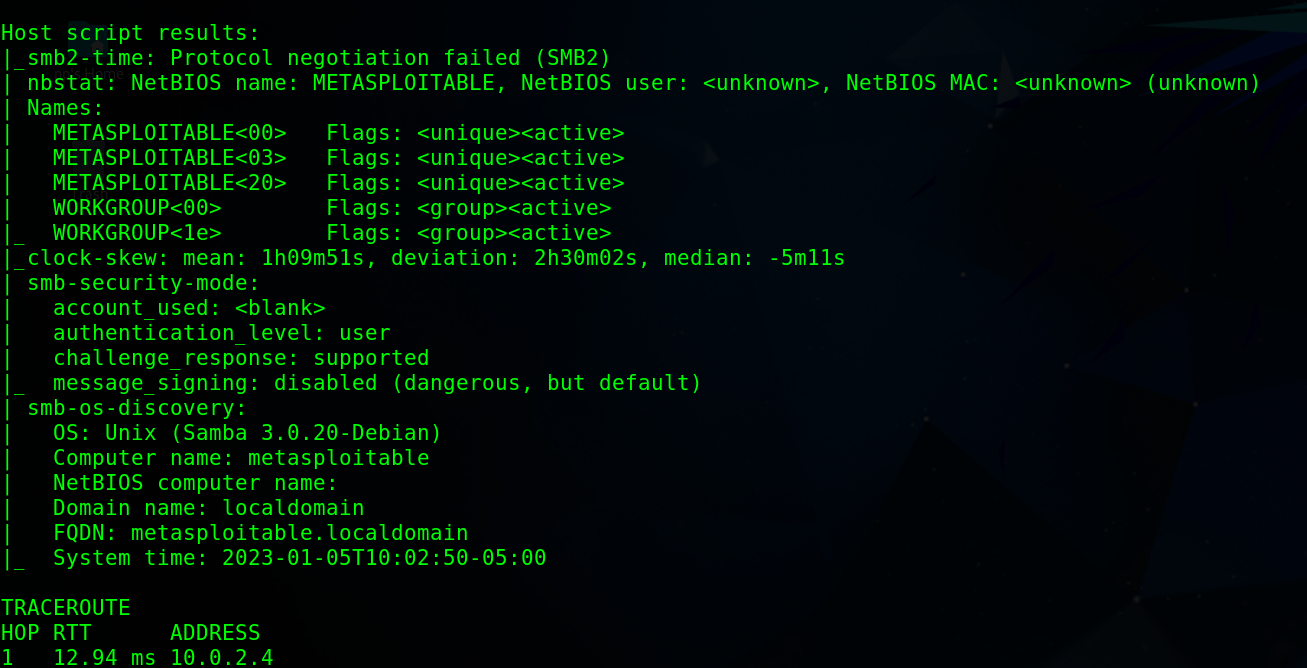
**Os Detection:**



We got the os of target

Os:Linux

**Host and Traceroute:**



We got the host and traceroute

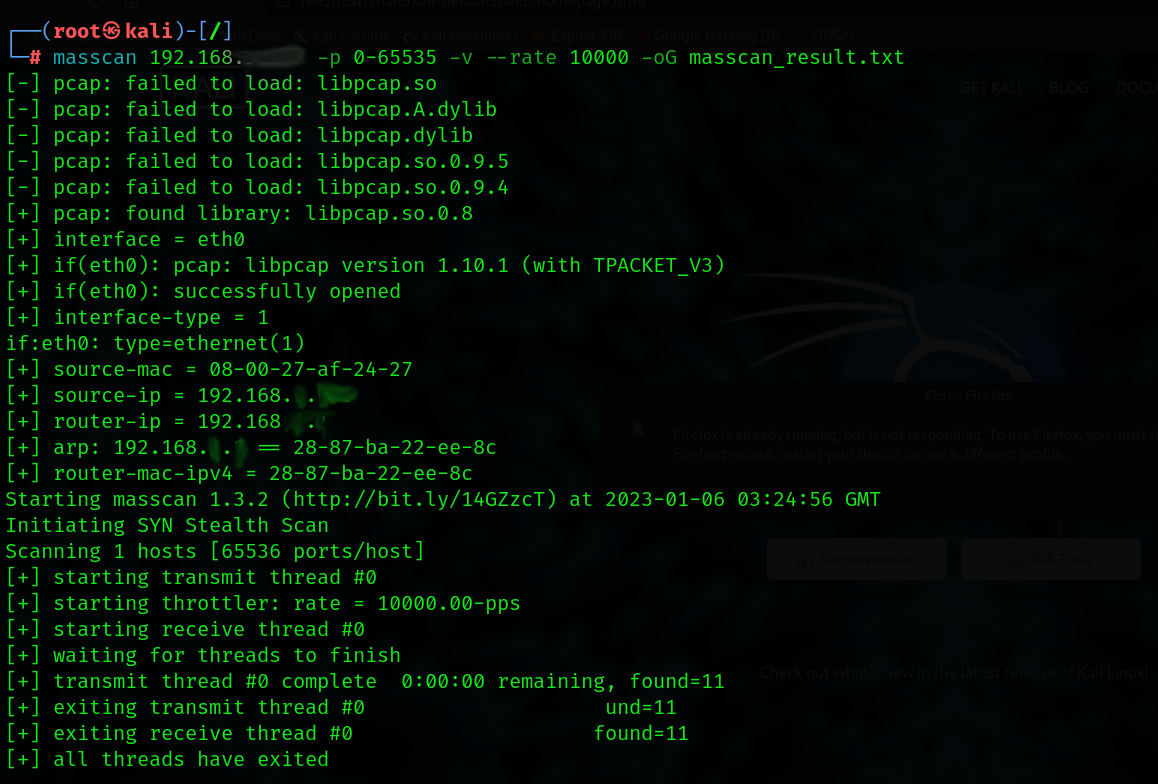
We got the nsb,os name ,domain and domain name and ip address

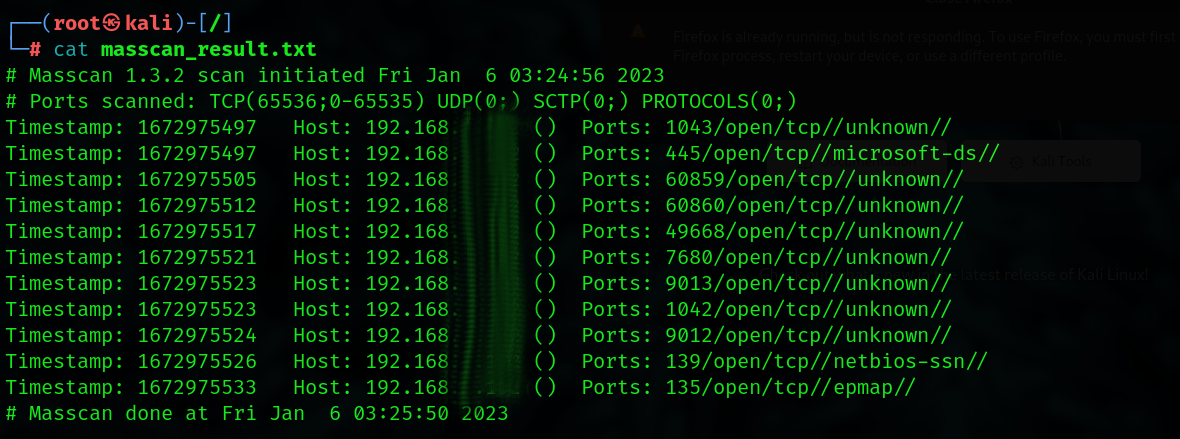
**Masscan:**Faster network scanning

Syntax: masscan [target] [option]

Command :masscan <ip> -p 0-65535 -v –rate 10000 -oG masscan\_result.txt

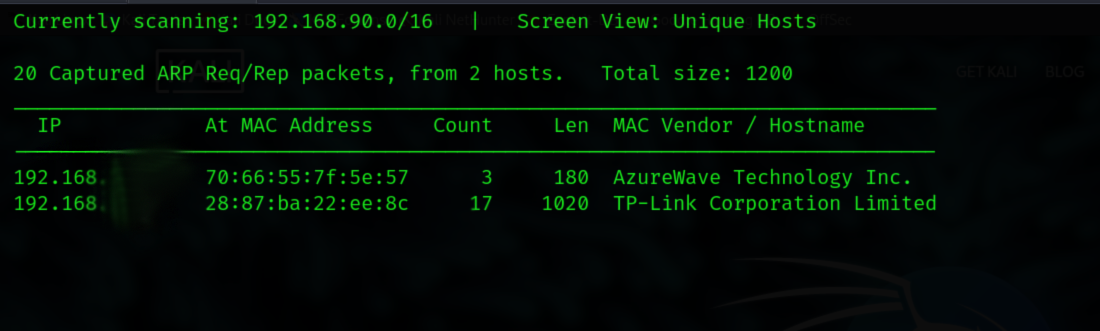
-p<port> , -v<verbose> , --rate<speed> -oG <output format >





**Netdiscover :** Scan the whole network

Command :netdiscover



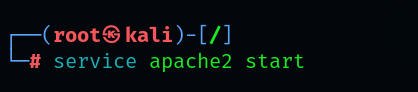
* **launch a website on the personal system using the Apache2 server**

In this we are going with the default apache server which is pre-installed in kali linux

Apache server

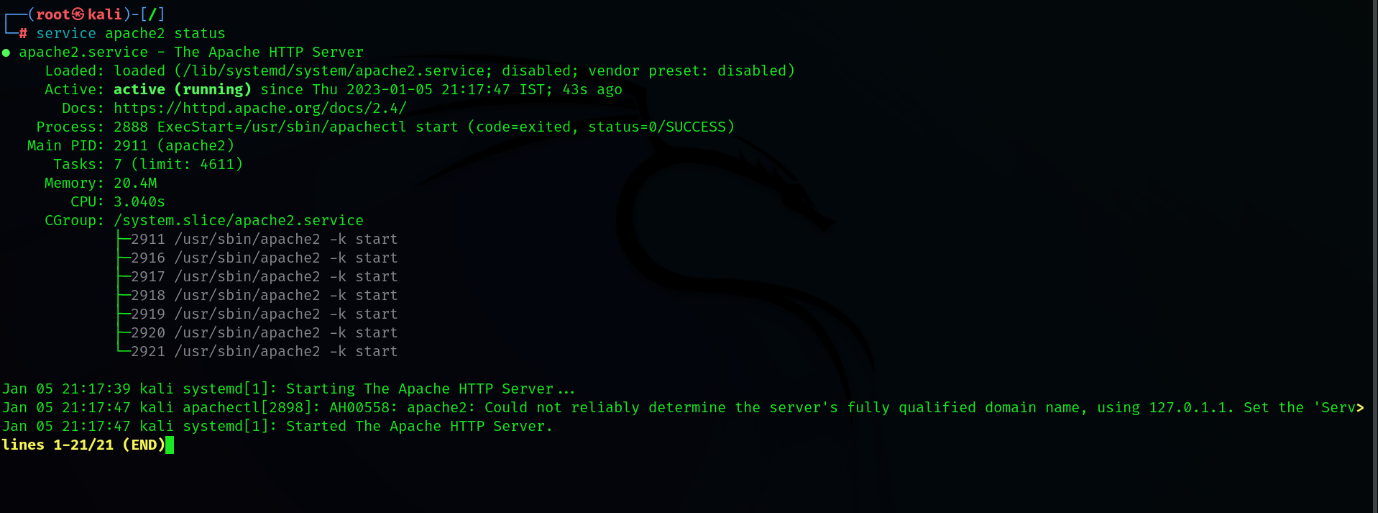
Starting apache server

Command :service apache2 start



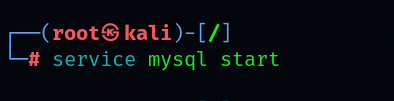
Cheking Status:

Command:service apache2 status



We also have to start mysql server

Command :service mysql start

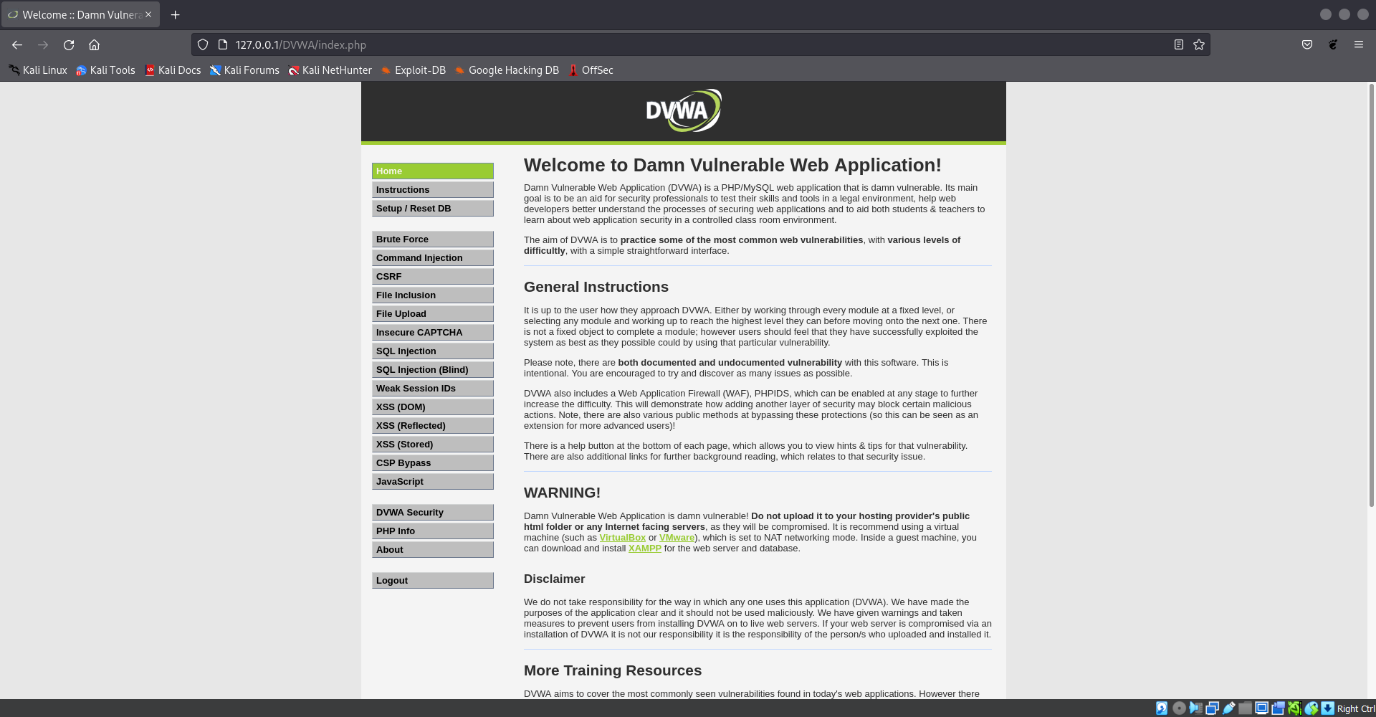


Cheking status

Command :service mysql status



We have configure our web on localhost. For access web we have to type [ 127.0.0.1/DVWA/ ] in web browser url.

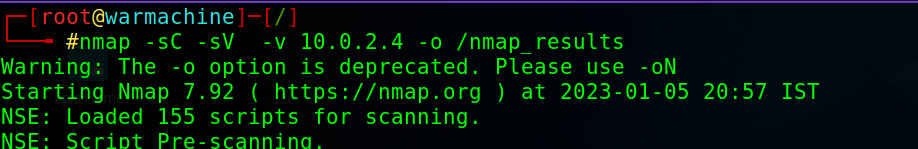


* **get the output of the network scanning and device discovery tools into the specified format.**

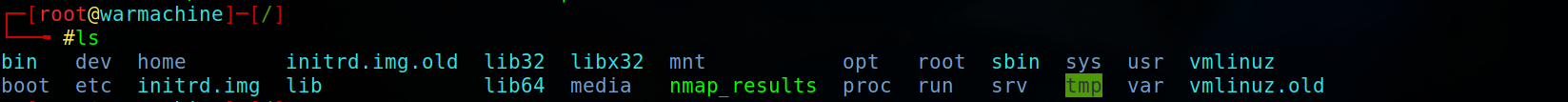
We can get the different types of options for saving the results in different format

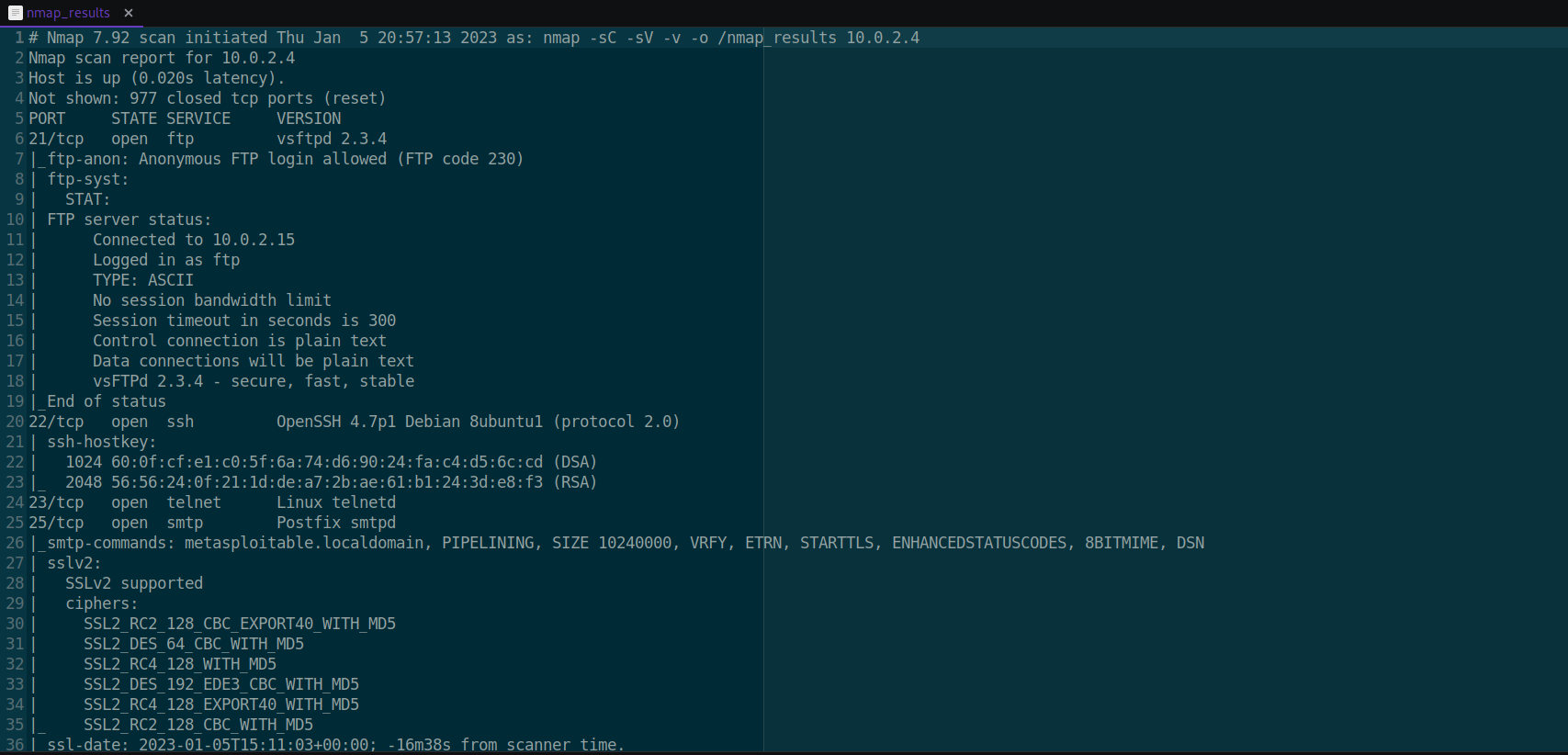
-o=saving output

Command :nmap -sC -sV -A -o , nmap -sC -sV -A -oA

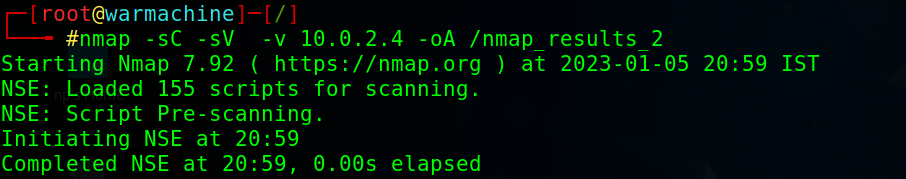


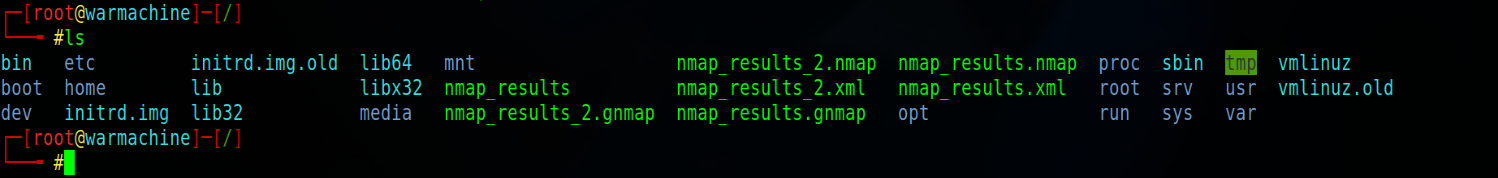
Result file :nmap\_results



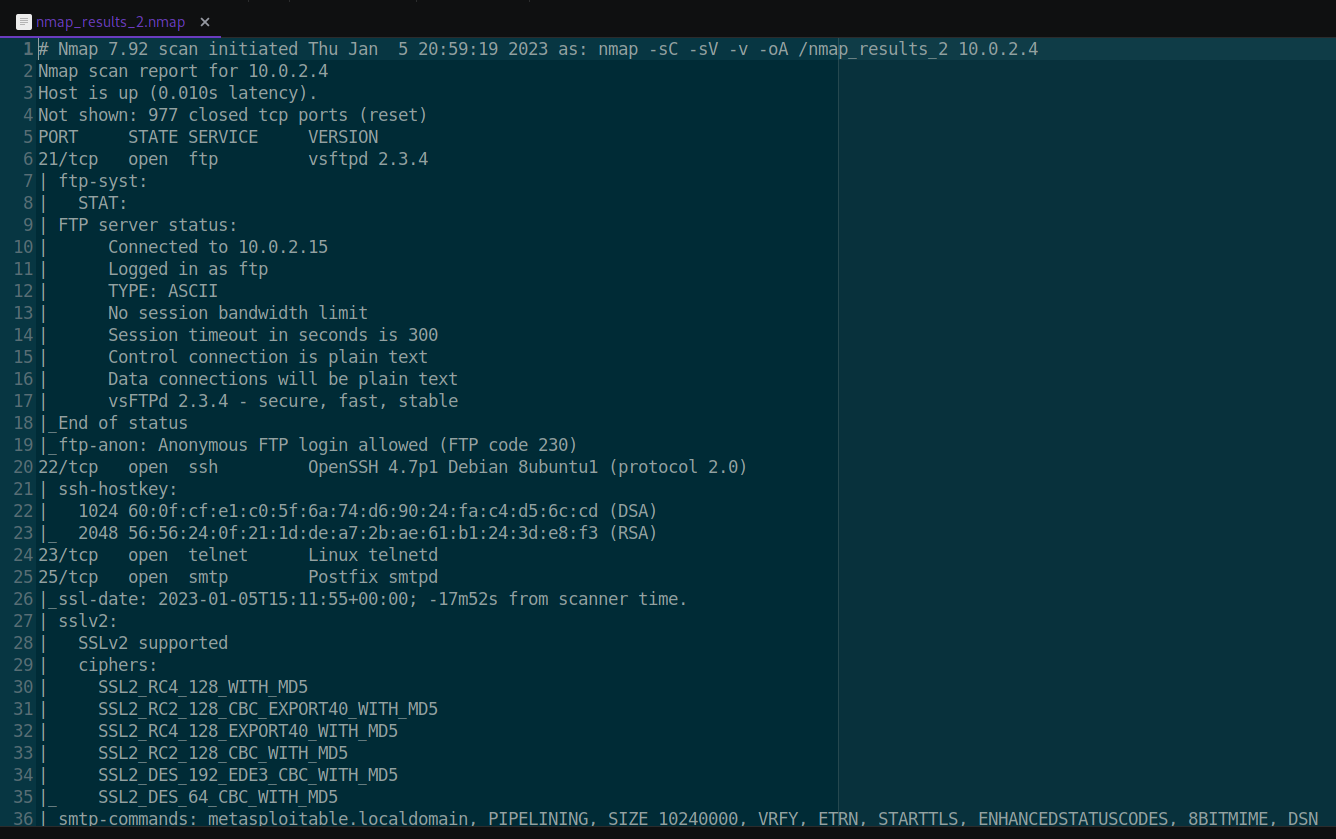


This create the files in different files simple,xml,gnmap

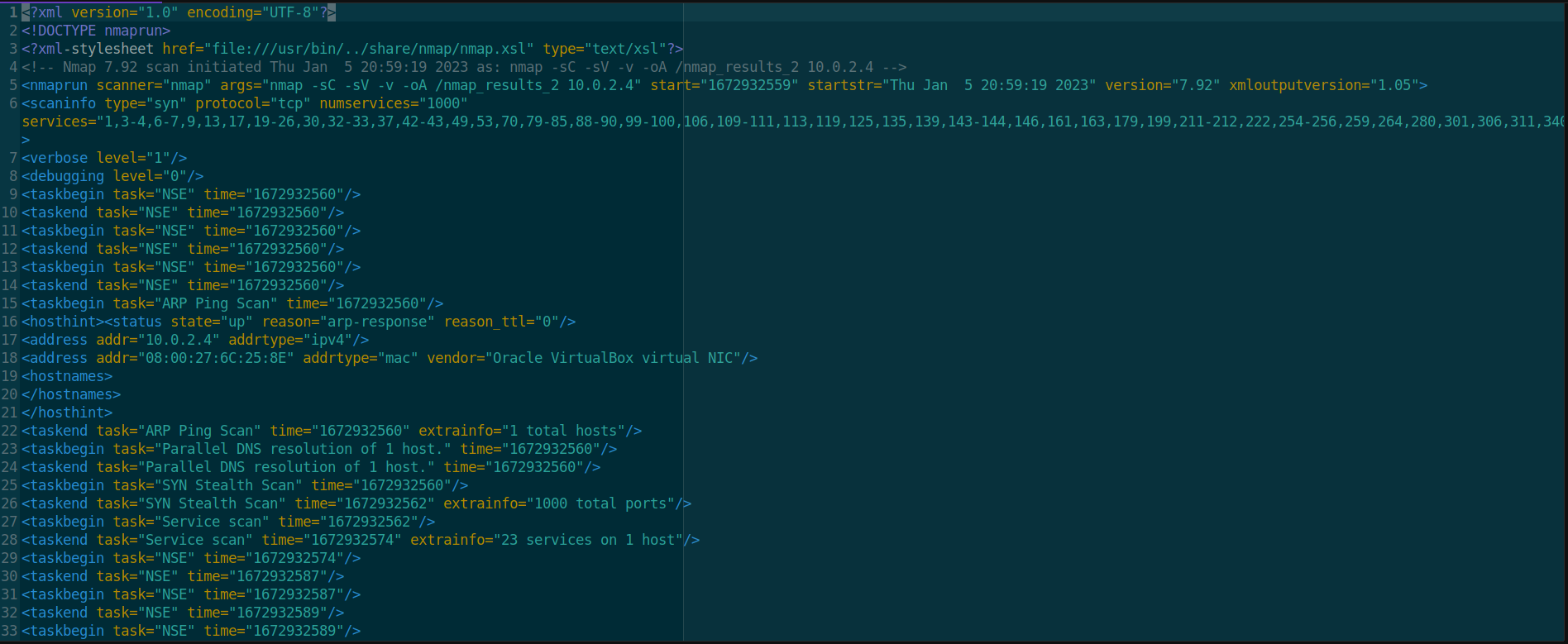




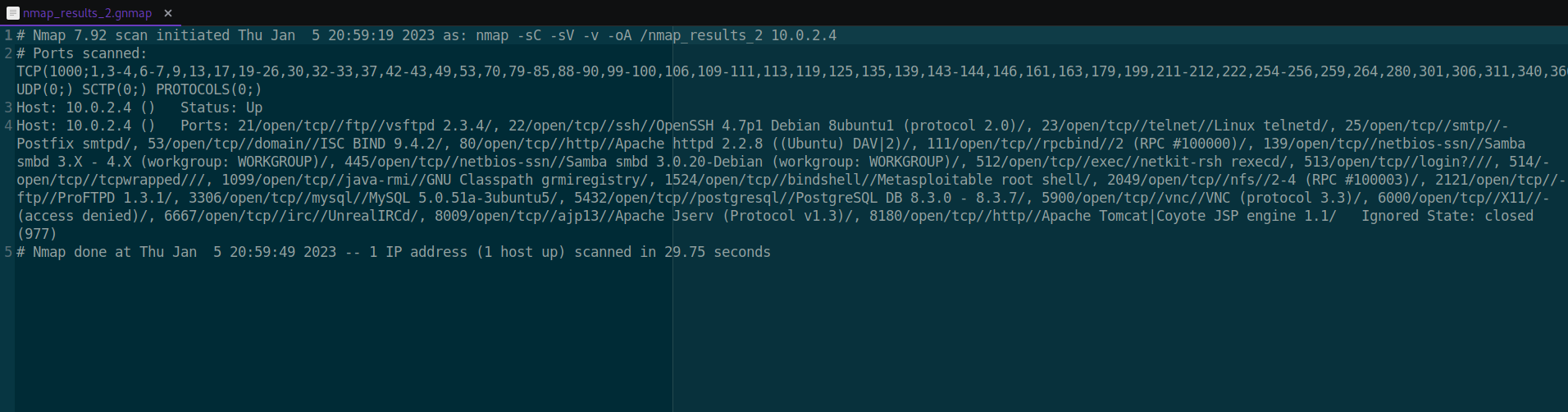
**Simple file**



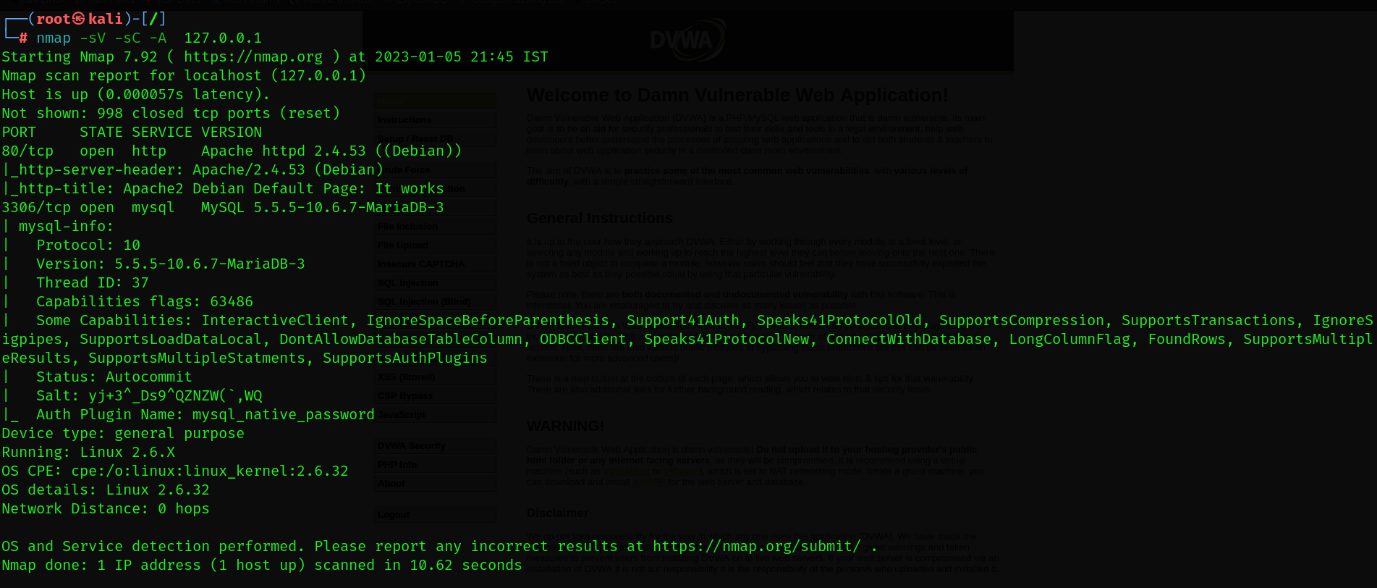
**Xml file**



**Gnmap file**

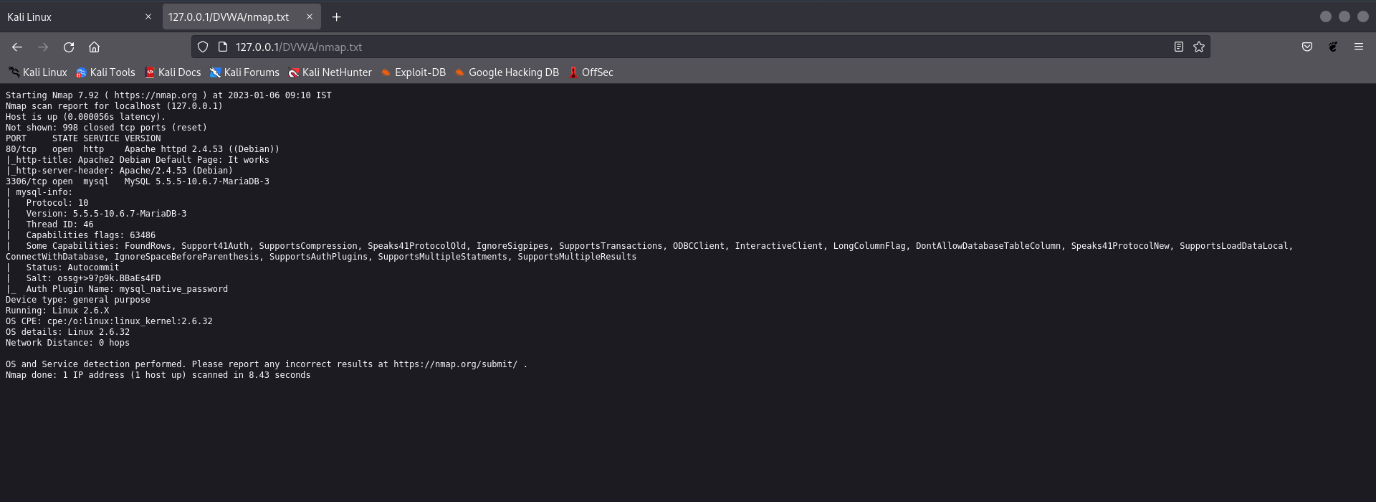


**● The out-of-the-network scanning and device discovery tools on the web page hosted on the Apache2 server**



* **Automate the process of embedding the network scanning and device discovery output result into the active web page.**

Open browser and visit your nmap result file



**● Access the webpage within the network with the result of network scanning and device discovery updated every 10 minutes with the time stamp**

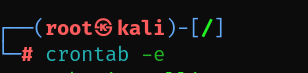
We can achieve automation using crontab in linux

Crontab

Commands: crontab -l

Crontab -e

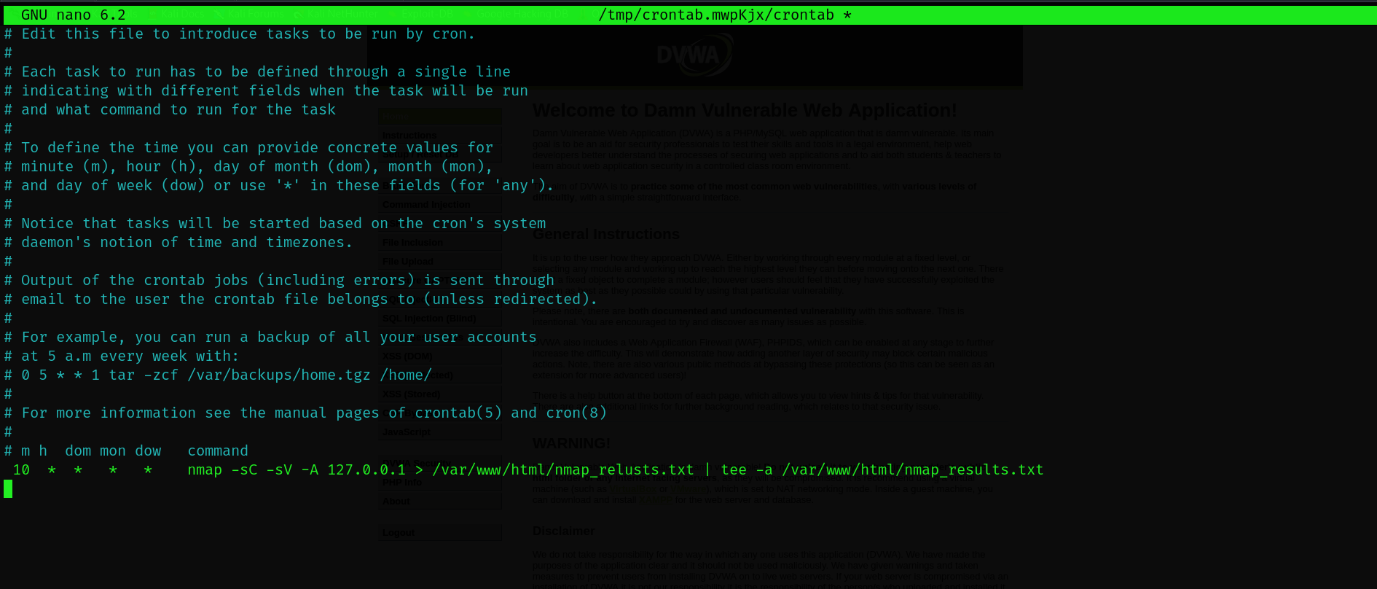
Crontab -e for crating new task



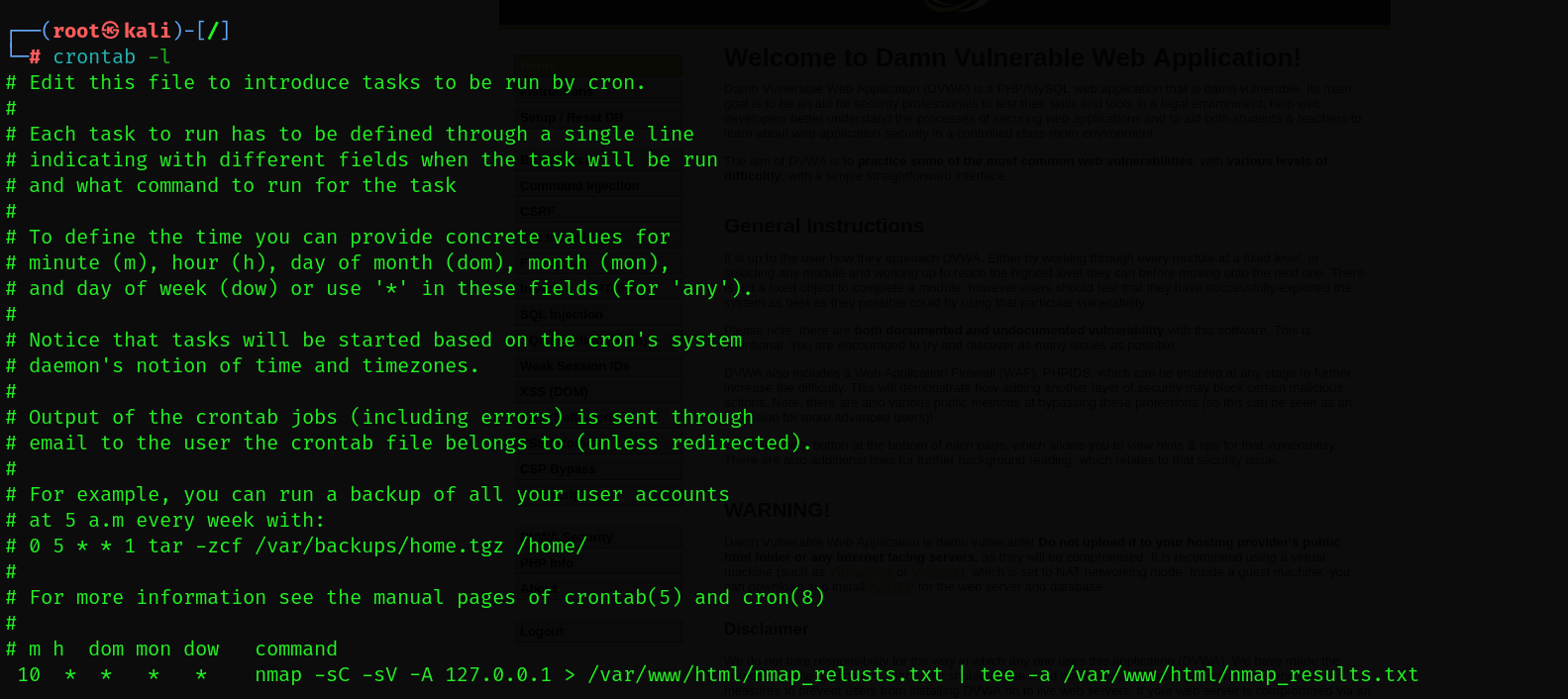
m(minute), h(hour), dom (day of month),mon (month), dow(day of weak)

command:

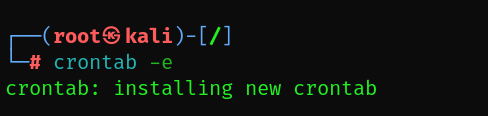
nmap -sC -sV -A 127.0.0.1 > /var/www/html/nmap\_results.txt | tee -a /var/www/html/nmap\_results.txt



List of crontab



Crontab installing…



Output:

