# Title: Ethical Hacking for Beginners (Tools, Enumeration and Exploitation)

**********

# * * * * * * DISCLAIM…

**Article** · June 2019

CITATIONS
0

READS
17,465

**2 authors**, including:

Kharim Mchatta
Coventry University
**5** PUBLICATIONS **0** CITATIONS

SEE PROFILE


Author: Kharim Haji Mchatta

Title: Ethical Hacking for Beginners (Tools, Enumeration and Exploitation)

Date: 6/24/2019

**********
*
*
*
* DISCLAIMER: ANY MALICIOUS USE OF THE CONTENTS FROM THIS ARTICLE *
*
* WILL NOT HOLD THE AUTHOR RESPONSIBLE, THE CONTENTS ARE SOLELY FOR *
*
* EDUCATIONAL PURPOSE *
*
*
**********

# Table of Contents

## OBJECTIVE OF THE ARTICLE

The main reasons for writing this article is to help the guys who are starting out in the penetration testing field on ways on how to exploit or enumerate some of the common services like ssh, ftp, dns, smb and many other more.

Most of articles online would show you the theoretical aspect of how a service could be exploited but they don't show practical examples on how the exploits or enumerations are done based on the service.

There are numerous ways on which a system can be attacked, don't be stuck with the methods which are mentioned and shown in this article, do research and learn as many techniques as possible simply because in one system the technique could work but on another system the technique wouldn't work depending on the complexity of the security systems that are put in place by the targeted machine.

## HOW TO SETUP VIRTUAL PENETRATION TESTING LAB

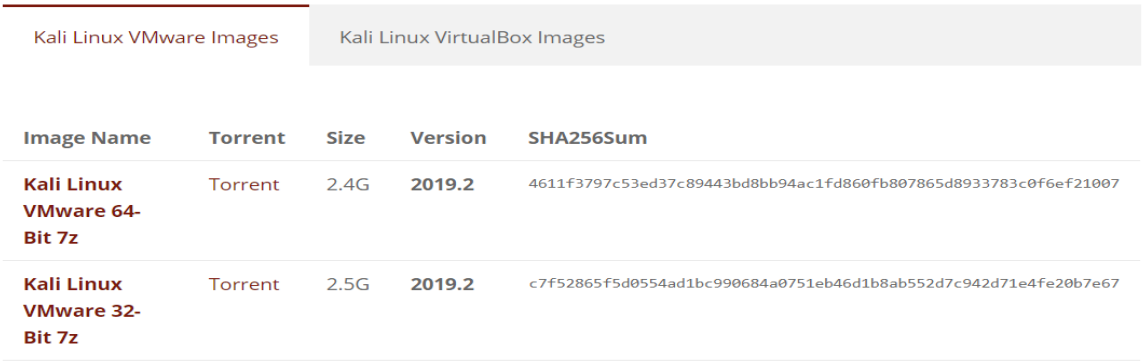
To get started with penetration testing you need to have a virtual environment running on your local host, there are many virtual environment platforms, but the most common ones include **oracle virtual box** and **VMware**. You can download them in

(a) Oracle Virtual Box - https://www.virtualbox.org/wiki/Downloads

(b) VMware - https://www.vmware.com/

Based on my experience I would recommend using Oracle Virtual Box but its all based on preference.

After that the next step is to download an OS system to run on the virtual box and for our case it would be Kali Linux which can be download at https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/




On the top you will see two tabs which all contains ISO's based on the virtual environment your using. Select one then download it.

Once downloaded please follow these YouTube links created by Hackersploit to see how you can setup the OS on the virtual environments

(a) how to install kali Linux on a virtual machine - https://youtu.be/od9jo8tvZUs

(b) how to install kali Linux on VMware - https://youtu.be/ShOb8bQ_h_I

## LINUX DISTRIBUTIONS FOR HACKING AND PENETRATION TESTING

Depending on the goal you want to achieve there are many Linux distributions which can be used for various purposes and the distribution are as follows

(a) Kali Linux – widely known for ethical hacking and penetration testing

(b) Blackbox – it's an ubuntu distro for penetration testing and security assessment purpose

(c) Parrot OS – its for penetration testers who need cloud friendly environment with online anonymity and encrypted system

(d) Black Arch – used for penetration testing and security research

(e) DEFT – also known as Digital Evidence and Forensics Toolkit (DEFT) used for computer forensics with the purpose of running live systems without corrupting and tampering devices connected to the PC where booting takes place

(f) Samurai Web Testing Framework – is used for web penetration testing.

(g) CAINE – also known as Computer Aided Investigative Environment. It is solely focused of Digital forensics

(h) Network Security Toolkit – it provides security professionals and network administrators with a wide range of open source network security tools. It has an advanced Web User Interface for system/network administration, navigation, automation, network monitoring & analysis and configuration of many applications found in Network Security Toolkit distro.

(i) Gugtraq - II -is focused on digital forensics, penetration testing, malware laboratories and GSM forensic. It also has over 500 ethical security hacking tools installed and configured

(j) CYBORG HAWK LINUX – is used for network security and assessment and digital forensics

(k) Weakerthan – used for wireless hacking as it contains plenty of wireless tools

**NOTE:** All the above distributions can be used depending on what you want to achieve, there are many other more distributions apart from the ones listed above. On this article we will focus more on kali Linux as the main and preferable distribution

## PLACES TO LEARN MORE ON PENETRATION TESTING

There are a lot of ways on which a person could learn penetration testing which can differ from person to person. The following are some of the ways you could use to learn penetration testing

(a) Google - In google there are a lot of articles on which you could go through to learn about penetration testing so it's time to do your research and gain the theoretical knowledge on penetration testing, common website to visit and get started with the theoretical aspect of penetration testing, ethical hacking and security include U-demy (https://www.udemy.com/), Null byte (https://null-byte.wonderhowto.com/), cybrary (https://www.cybrary.it/) and Hackersploit (https://hsploit.com/).

(b) YouTube channels – there are a lot of channels on which they teach penetration testing concepts and show practical part of it where individuals could learn a lot from, these channels include hackersploit, IppSec, Null byte, Hak5 and Demmsec, all these channels contain good contents in penetration testing

(c) Mentor – find someone who is skilled and is already in the security world to help you out learn and direct you while you are getting started in the field.

# CHAPTER 1: INTRODUCTION

## 1.1 understanding terminologies

cyber security is a field that is evolving every day, as technology keep's on evolving the more the digital crimes keep on get more popular and growing. As systems keep on getting more sophisticated the more the cyber criminals keep on finding various ways to get to the sensitive information. The motive of each hacker varies from one hacker to another some are motivated by the money they get paid to hack a system, others are just motivated because of the ego and others are motivated by the act of protecting the wellbeing of the people.

Cyber security is the process of protecting organization's assets from unauthorized access but also from potential damages which might be caused by potential security breaches.

In cyber security there are terminologies that need to be understood by various individual's in-terms of careers in this field.

(a) Penetration testing – is the process of looking for weakness in the systems before they are being exploited by hackers

(b) Ethical hacking – is the process of trying to exploit a network by covering all hacking methodologies with other similar hacking techniques as a black hat hacker would do according to EC-COUNCIL

(c) Cyber security – is the process of defending an organization's network from various threats. The cyber security is divided into two teams

   (i) Blue team – they are the individuals who are responsible for implementing the security of the organization and ensuring the security controls are put into place

   (ii) Red team – they are the individuals who are responsible for testing the security that have been implemented by the blue team by trying to hack there way through the system

1.2 Understanding the open system interconnection (OSI) model is an important part of hacking, you need to know and understand how application and systems communicate and function over the system.

## OPEN SYSTEM INTERCONNECTION (OSI) LAYER

Is a reference model on how applications communicate on the network. There are 7 layers of the 0SI model where layer 1 is has a far relationship with the user and layer 7 has a close relation to the user.

### Layer 7: Application layer

This is the layer which involves the user, this is the layer where the user interacts with the systems example applications like the web browsers, email applications like outlook etc.

### Layer 6: Presentation layer

This is the layer where you interact with the operating system example trying to boot your system, or trying to change or add your drivers etc

### Layer 5: Session layer

This is the layer where by when two computers interact with each other successfully they create a session among each other

### Layer 4: Transport Layer

This is all about the transfer of data from one point to, how much amount of data can be sent and received from one point to another

### Layer 3: Network Layer

This is the layer that involves how devices communicate with each other example TCP/IP

### Layer 2: Data-link layer

This layer involves the physical addressing of network devices example mac address

### Layer 1: Physical layer

It's all about how devices are connected to each other physically

1.3 in penetration testing there are various areas of specialties that an individual could get into and these include:

(a) web penetration testing

(b) Network penetration testing

(c) Application penetration testing

(d) Mobile penetration testing

(e) Wireless penetration testing

(f) IoT penetration testing

# CHAPTER 2: HACKING METHODOLOGIES

The process of looking for systems vulnerabilities as well as presenting the evidence of theory attacks to show the vulnerabilities are obvious. Good penetration usually provides suggestions for directing and correcting the issue that was encountered during the analysis, in other terms these techniques are applied to improve the security of the systems against attacks.
The main reason is to identify security issues by applying a methodology, tools and techniques as an attacker. The following are phases of hacking

(a) RECONNAISSANCE
Is the most important phase of the hacking methodology. You can never win a war if you haven't gathered enough information about your enemy. The importance of reconnaissance is to gather information and facts about your target. At this phase each information that is obtained is saved.
At this stage there are two ways of gathering information and this includes.

(i) Passive – this is where the attacker doesn't actively engage the system, they gather information based on online information which they might come across

(ii) Active – this is where the attacker actively engages the system in order to gather information

(b) SCANNING
Is the process of identifying set of active machines, ports and services, discovering operating system architecture of the target, identifying vulnerabilities and threats in the network. Scanning is usually used by hackers to create a profile about the targeted organization.

(c) ENUMERATION
Is the process of extracting user names, machine names, network resources, shares and services from the computer system. Here is where the hacker makes an active connection to the system to perform direct queries to gain more information about the target.

(d) EXPLOITATION
Is the process of executing the attack based on the information that has been gathered in the previous stage. In this stage is where the hacker performs that actual hacking itself using the hacking the tools exposed to him.

(e) PRIVILEGE EXCALATION

Is the process of obtaining privileges that are granted to higher privileged accounts than the attacker broke into originally. The goal of this step is to move from a low-level account all the way up to the administrator account to have full access and control of the system

(f) PRESENCE MAINTANANCE

Is the process of creating an unknown entrance that will allow you to come back into the system anytime the hackers to come back without being detected, this can be achieved by planting a backdoor on to the system

(g) COVERING TRACKS

Is the process of removing any signs of evidence that you were in the system. The hacker would delete log files and remove any other related evidence that need to be deleted so that the system admin wouldn't know that the system was attacked.

(h) REPORT WRITING

Is the process of documenting all the findings that you made during your exploitation of the system on how you managed to exploit it, and also recommend some solutions on how they could stop that to occur in the future.

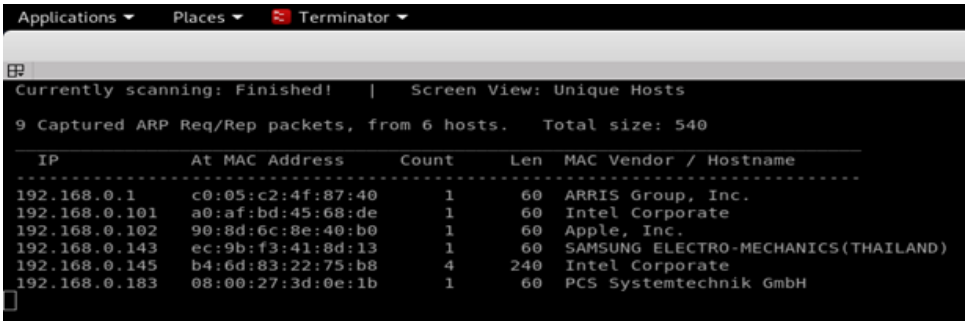
# CHAPTER 3: TOOLS TO BE USED IN ETHICAL HACKING

The tools mentioned in this article are solely based on the authors preference but there are other tools which a user could use to exploit the same service. Please take time and research on other tools and look for the tool that works better for you. More options of tools could be found on kali Linux's website https://tools.kali.org/tools-listing where there are a lot of options of tools which you could look at and practice on but also other tools could be found on GitHub.

Hackers are exposed to different type of tools that can be used to gather information, enumerate and exploit a system. Each tool serve's a specific function to a hacker. The following is a list of tools that could be used by a hacker to attack a system:

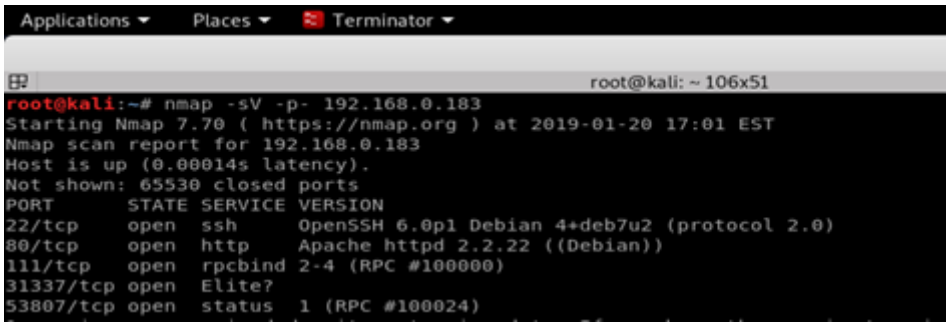
## (a) Netdiscover

Is a tool that is being used to help find and identify hosts on either a wireless or switched network. It can be used in either active or passive mode. Netdiscover will also provide the mac address of a host on the network



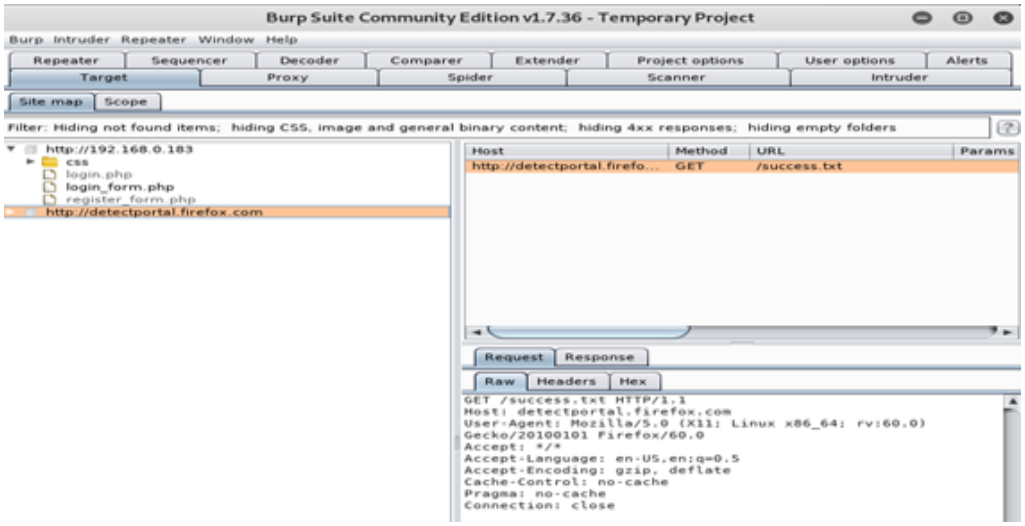

## (b) Nmap

Is a port scanning tool. It sends ICMP packets to check whether the port is open or closed. It also helps find the operating system running on a host



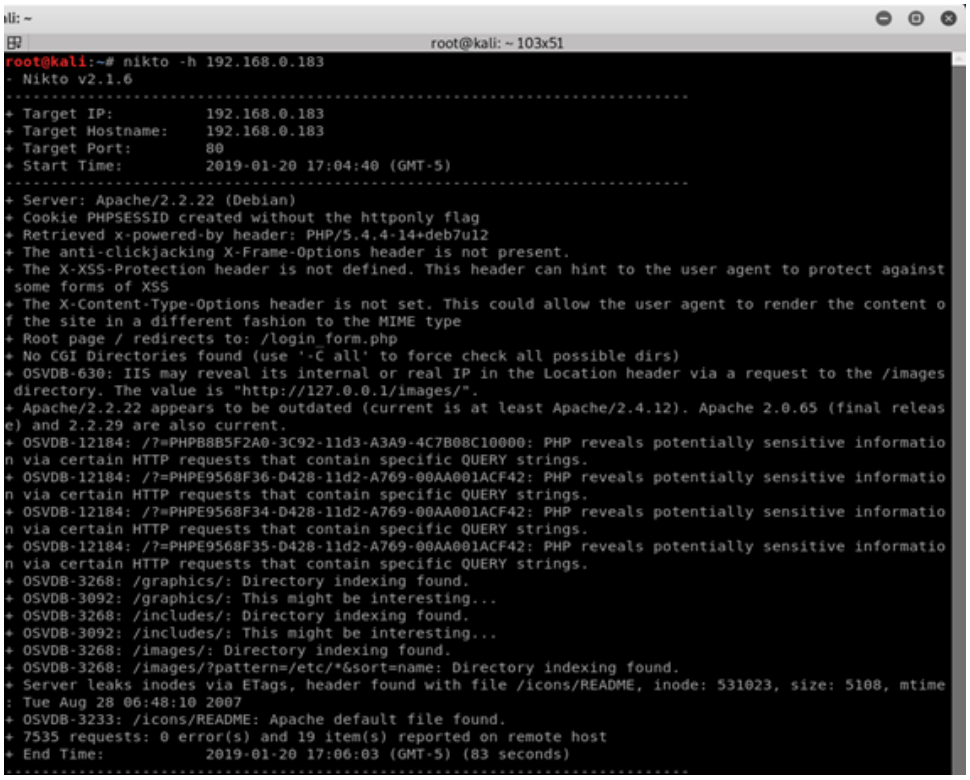
(c) Burp suite

Is a hacking tool that is being used to perform security testing of web applications. It has various features that work together to support the entire testing process from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities



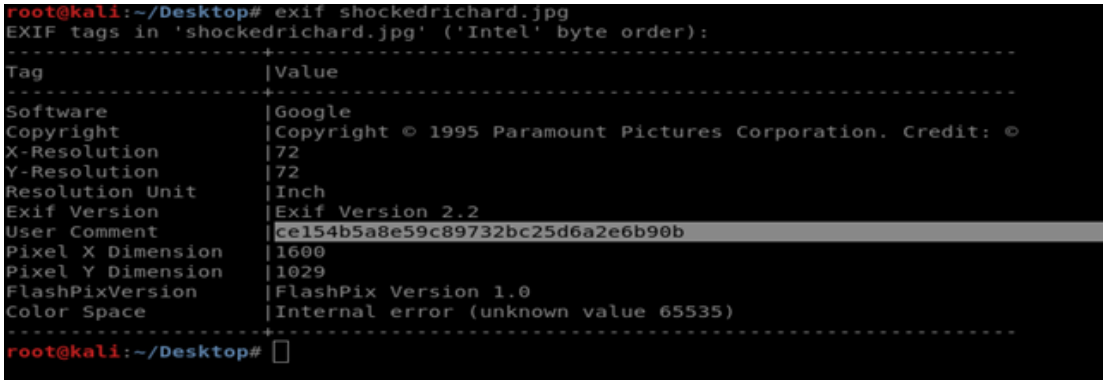

(d) Nikto

This is a web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, but also it checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers



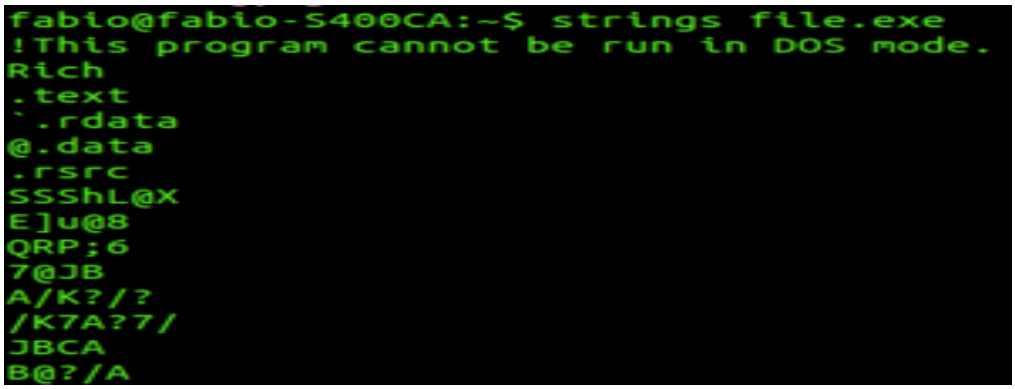
## (e) Exif

This is an information gathering tool that can be used for reading, writing and manipulating image, audio and video metadata.



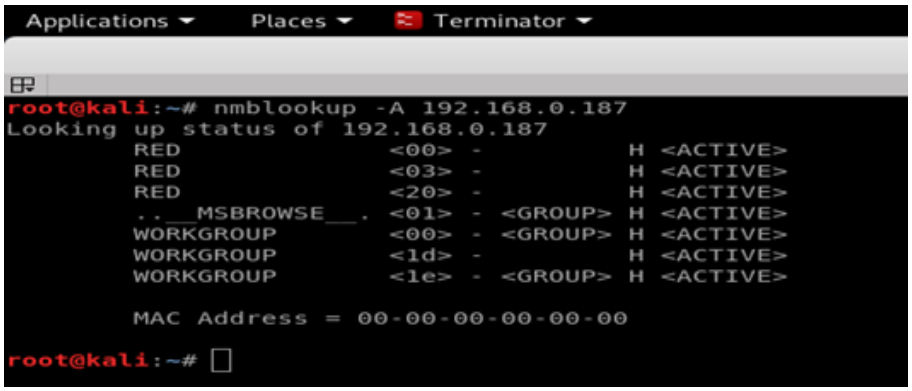

## (f) Strings

This is a tool that makes it possible for the humans to be able to read characters with any file. The purposed of this tool is to be able to know what type of file your looking at and it can be used to extract text



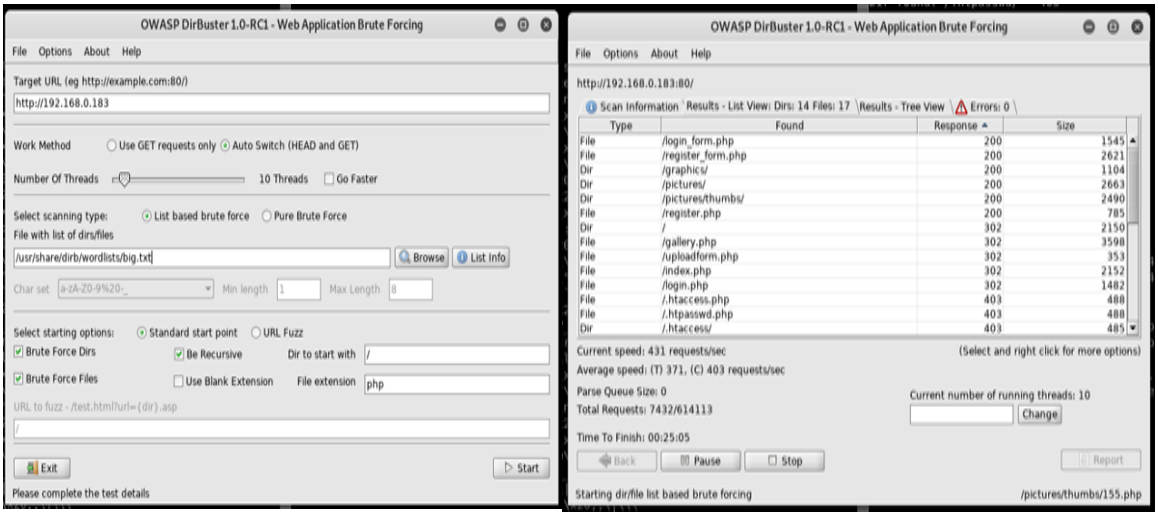

## (g) Nmblookup

Is a tool that can be used to get several meaningful information. It shows relevant information about the workstation like what's the name of the workgroup and sometimes who the users are



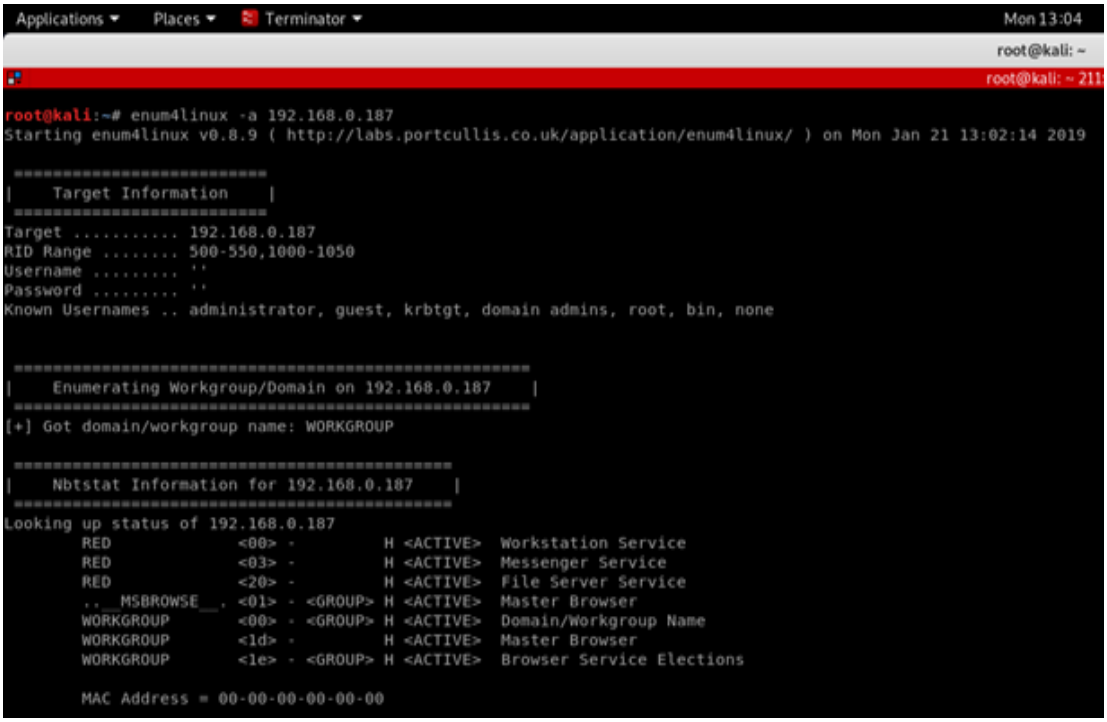
## (h) Dirb, Dirbuster, Gobuster

These are web scanners that look for web content. They basically look for web objects. It works by launching a dictionary-based attack against the webserver and analyzing the response. They all come with preconfigured attack wordlists for smooth usage, but you can use your custom wordlists



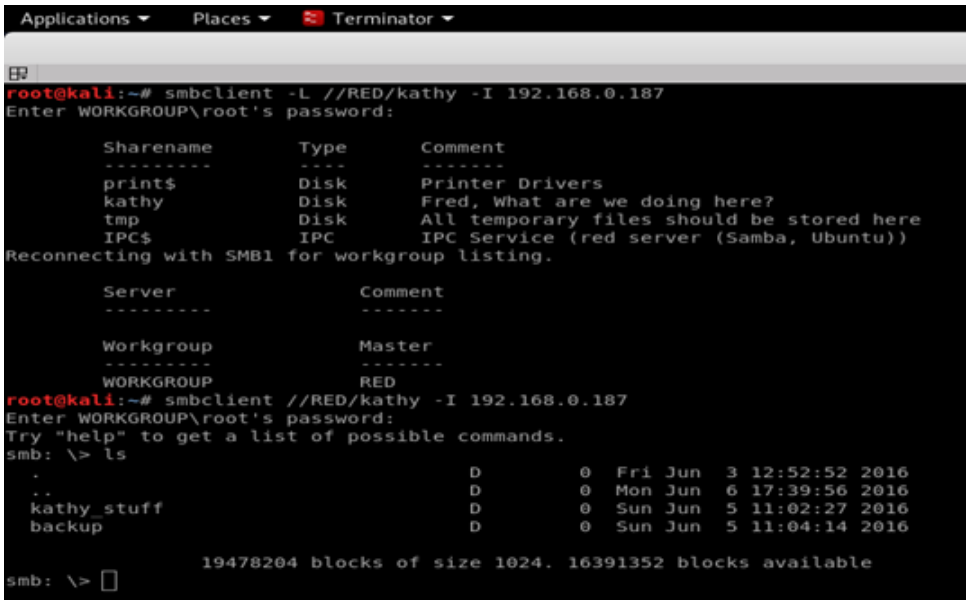

## (i) Enum4linux

Is a tool used for enumerating data from windows hosts which contain samba systems. It could do user listing, listing of group membership information, share enumeration, detecting if a host is in a workgroup or a domain, identifying the operating system and password policy retrieval



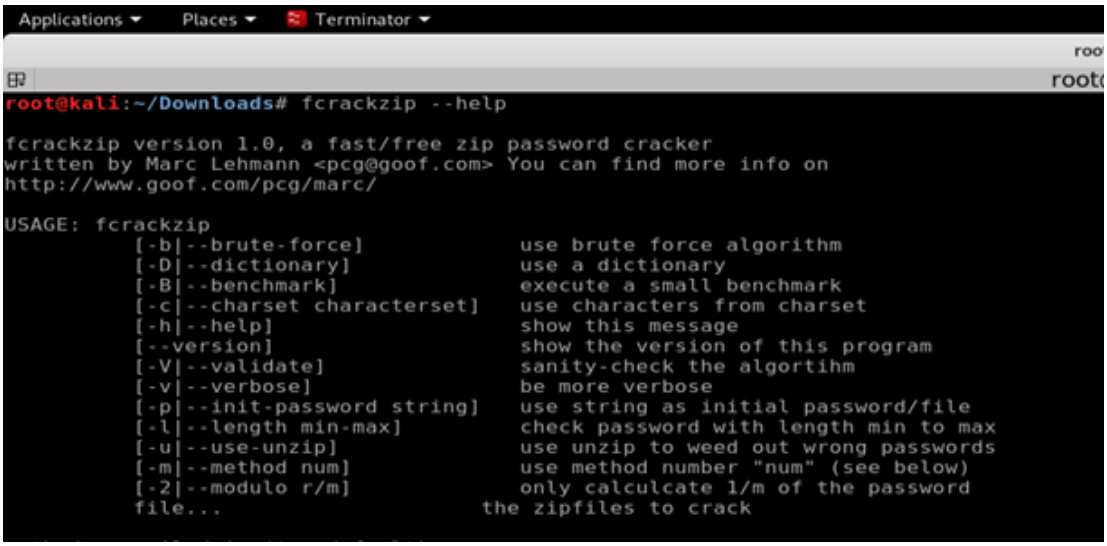
## (j) Smbclient

It's a samba client with an ftp-like interface. It is a tool that is used to test connectivity with a window share machine. It can also be used for transferring files or it can be used to look at share names




## (k) Fcrackzip

This is a tool that can be used to crack zipped files encrypted with zipcrypto through brute force and dictionary-based attacks

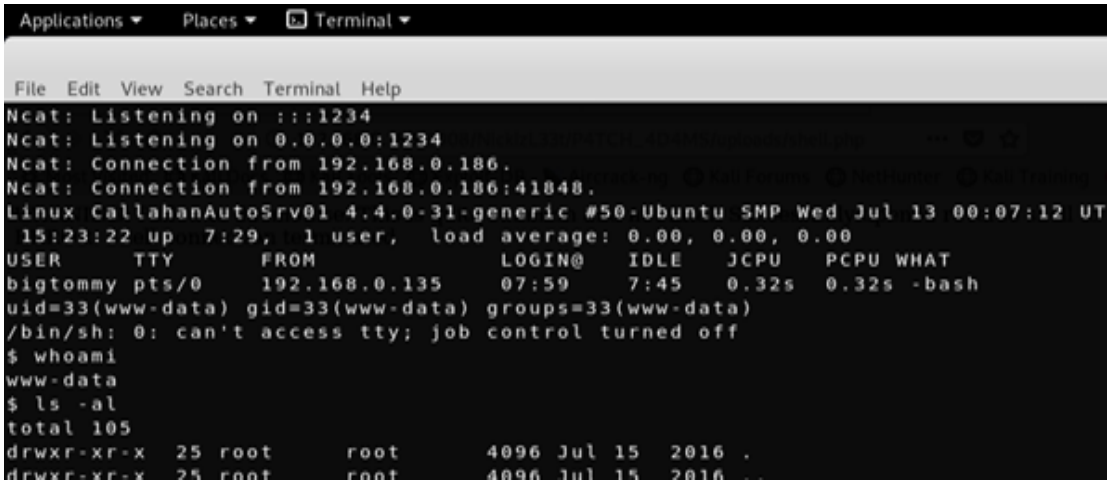


## (l) Pdfcrack

Is a tool that is being used for recovering passwords and content from a pdf file.

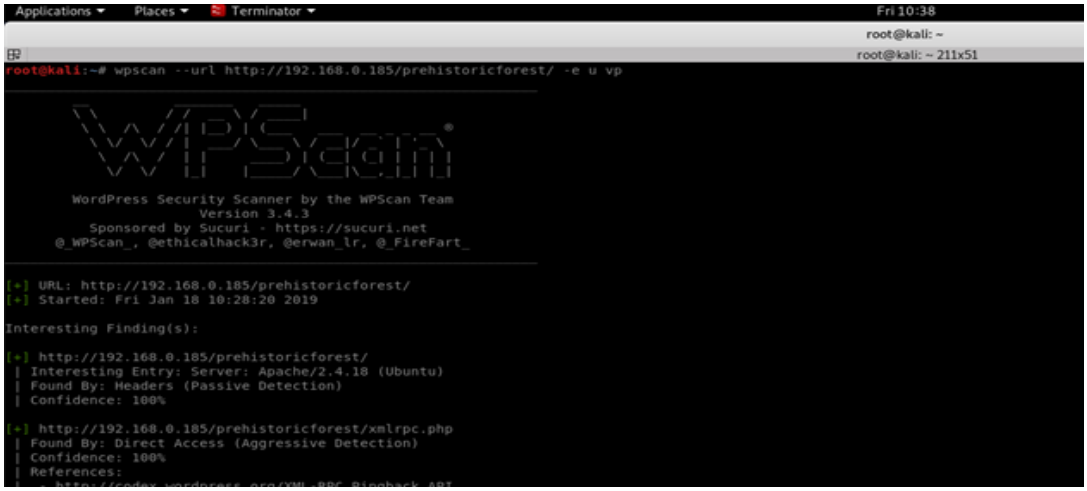

## (m) Netcat

This is a tool that is also known as the swiss army. It's a tool that is being used for reading and writing from a network connection using TCP or UDP.



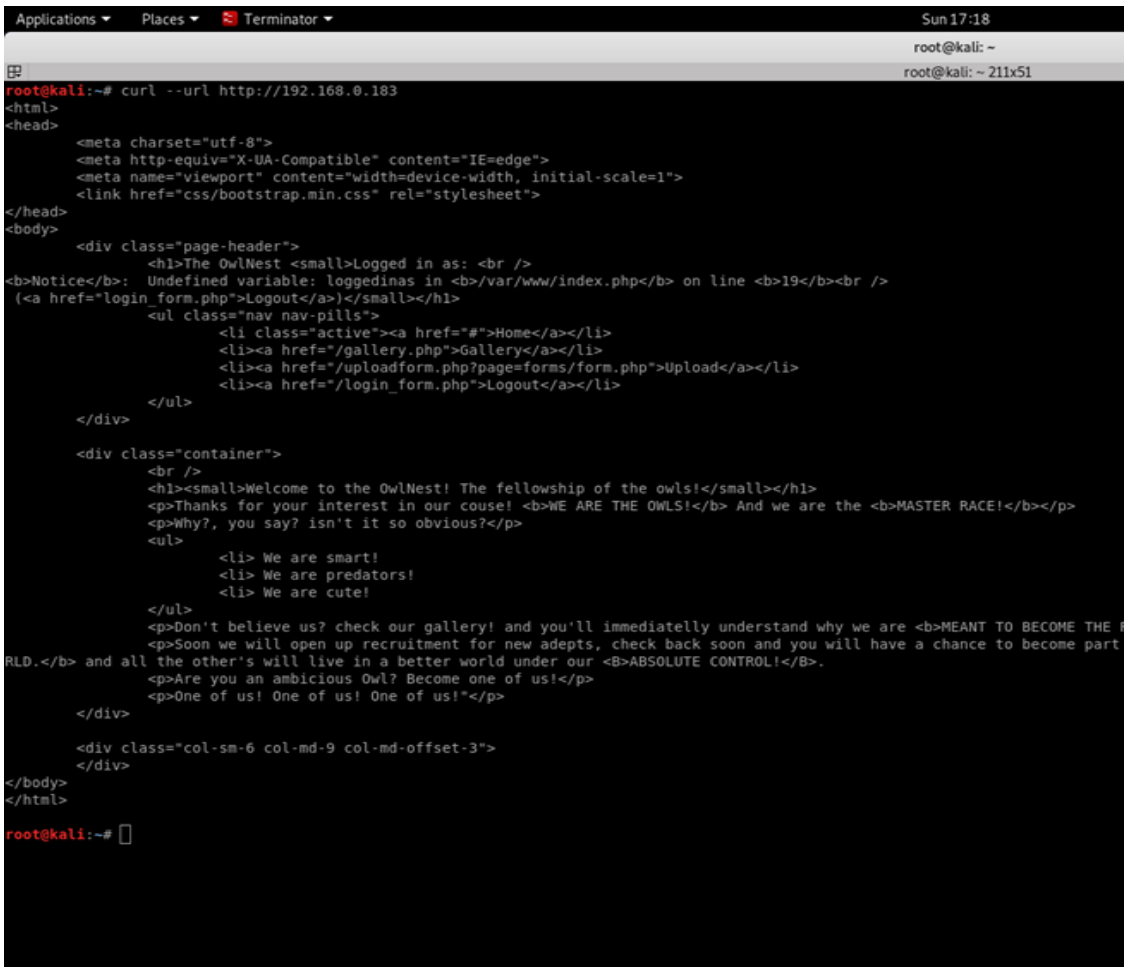
## (n) Wpscan

Is a vulnerability scanning tool that is used by the hacker to scan remote WordPress for vulnerable plugins, usernames and passwords



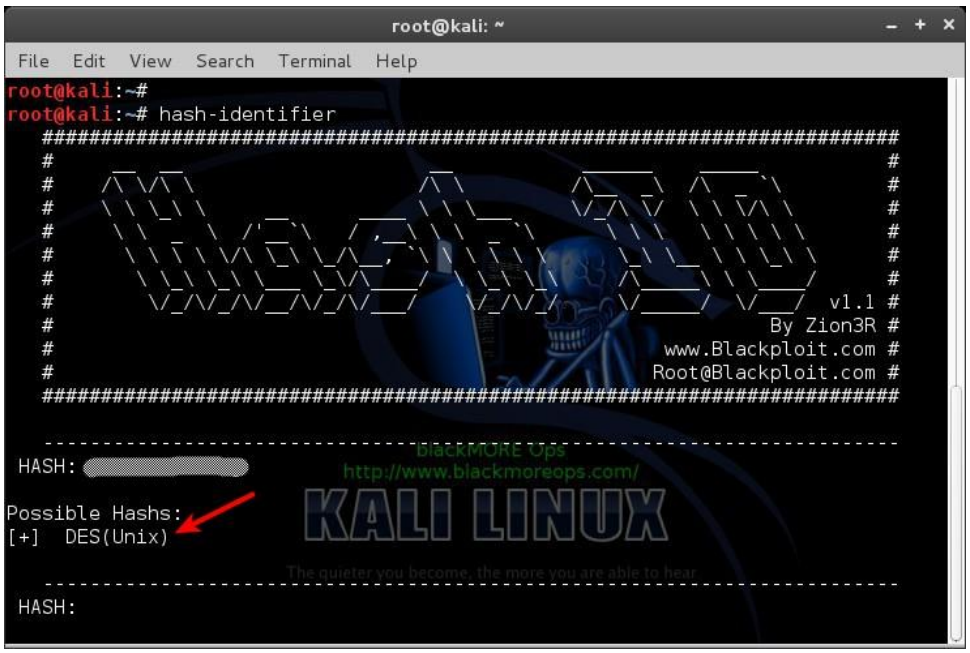

## (o) Curl

Is a tool that helps an attacker to view the source code of a web page and what contents it entails



## (p) Hash identifier

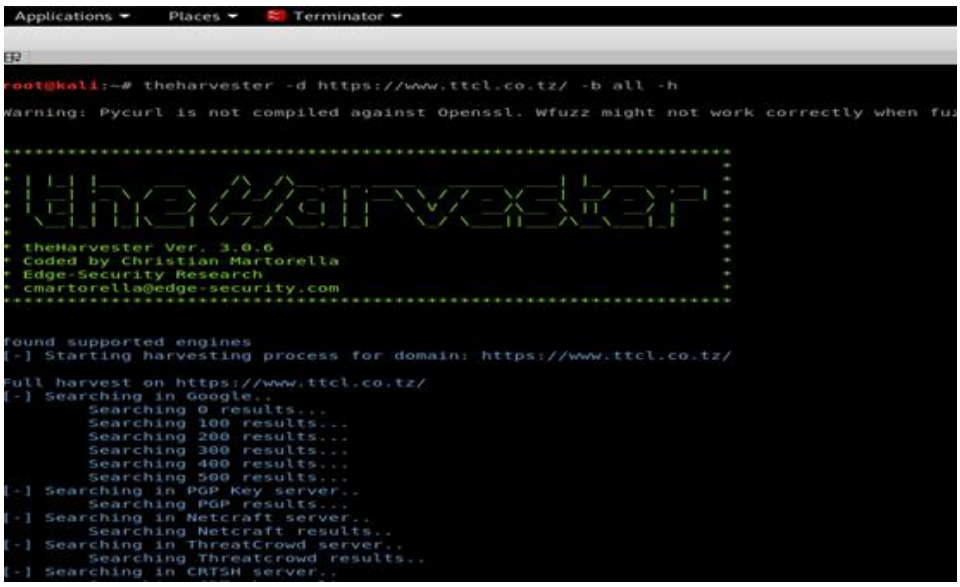
There are many types of hashes that are being used by many applications for example MD5, SHA1, CRC8 and others. some hashes are being generated through source data of a file. The tool helps you identify what type a hash is.




## (q) The harverster

This is an information gathering tool that provides us with information about e-mail accounts, user names and hosts/subdomains from different public sources

Like search engines and PGP key server, the sources supported are google, bing etc.

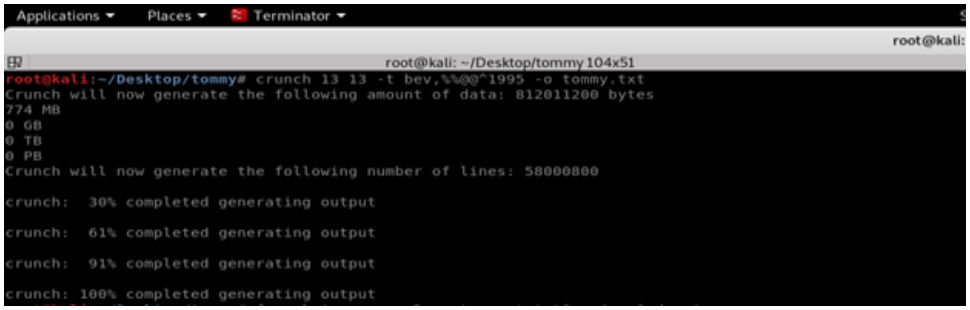


(r) Metasploit

Is a platform that provides exploits for a wide range of applications, services, operating systems and platforms. it comes with modules like payloads, exploits, auxiliary, encoders and posts which in combination can create a potential exploit

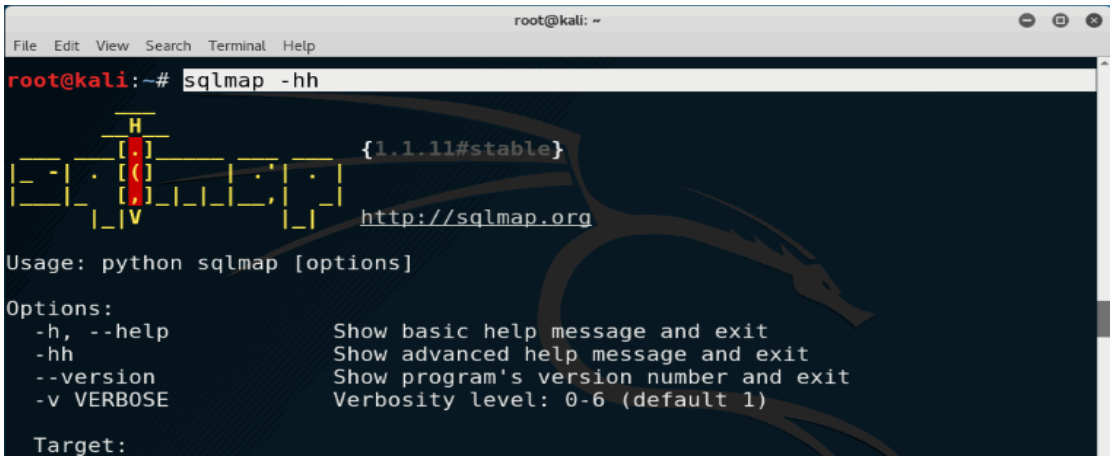

(s) crunch

Is a tool that generates wordlists where you could specify a standard ser of character or a character set you specify. Crunch can generate all possible combinations and permutations.



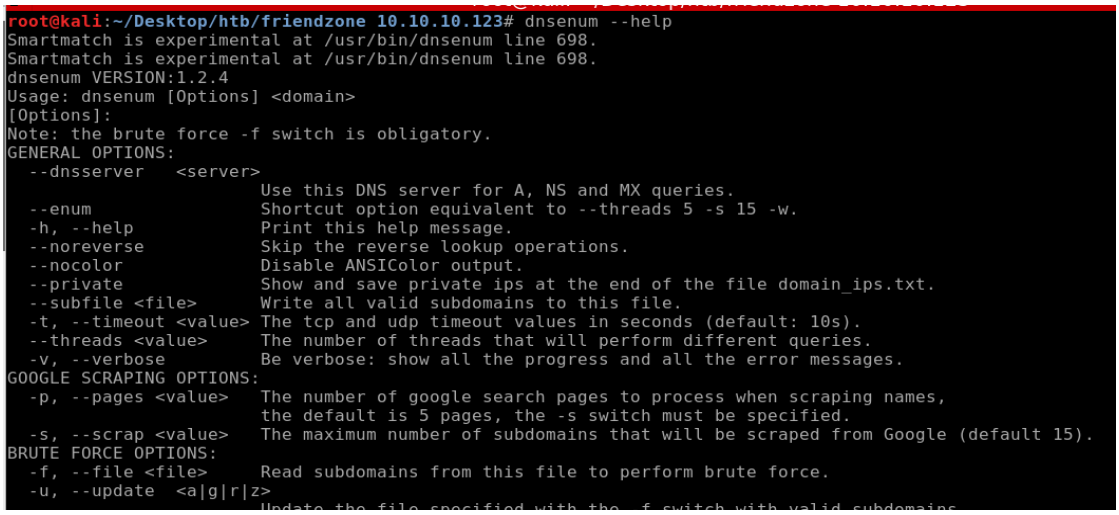

(t) sqlmap

Is a tool that automates the discovery and exploitation of vulnerabilities to SQL injection attacks. It has many functions and included features such as detecting DBMS, databases, tables, columns, retrieve data and even take control of a database



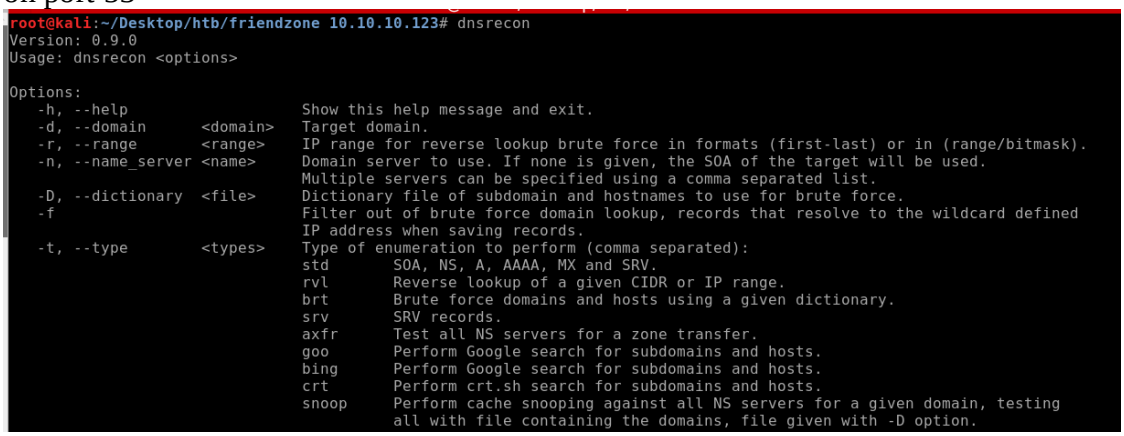
(u) dnsenum

this is a tool that is being used to enumerate a dns server, it enumerates services on port 53




(v) dnsrecon

this is another tool that is being used to enumerate a dns server, it enumerates services on port 53




**NOTE:** The commands used on the different tools shown above aren't the only commands to be used for that tool, to get more options and technique's, type the name of the tool with the word help at the end example

**Nmap help** or **Nmap - -help**

Don't stick to the options only specified here in this article, go to google and do some research about the tool's and see how other techniques that could be used with the tool.

# CHAPTER 4: NETWORK PORTS, SERVICES AND HOW TO EXPLOIT THEM

All electronic devices have specific services which run on specific ports, each service has its functionality on the computer, these services are what hackers usually look for especially the vulnerable services or misconfigured services so that they could exploit them to gain access to the system. Some of the common services that a hacker could exploit include the following:

(a) Port 21 FTP

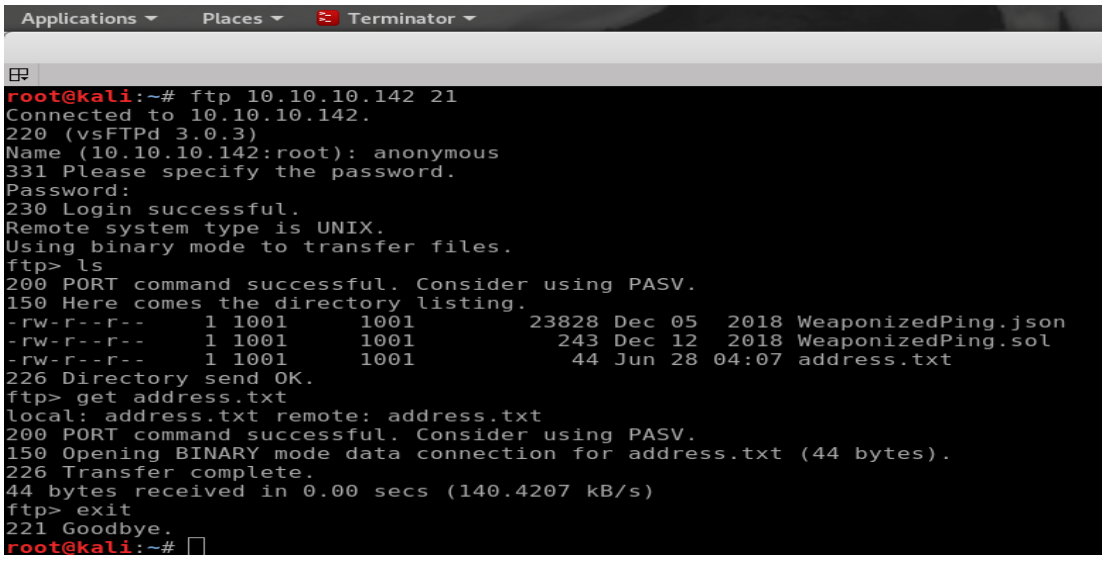
It's a file transfer protocol that allows a user to transfer (download) files from the server to the local machine. To login the ftp server to download the files you use the following command

ftp (ip address of the target machine) (port number of the service running) example:

ftp 192.168.0.101 21

it would ask you for username and password, sometimes the username and password could be **anonymous** (default login) or anonymous as the user name and for the password just press enter

once your logged in successful the first command that is recommended to use is the **help** command so as to see all the available and usable commands after that the next command to use is **dir** - to list the files, **cd** – to move from one directory to another, cd **..** – to get out of a directory and **get** – to download the desired file.

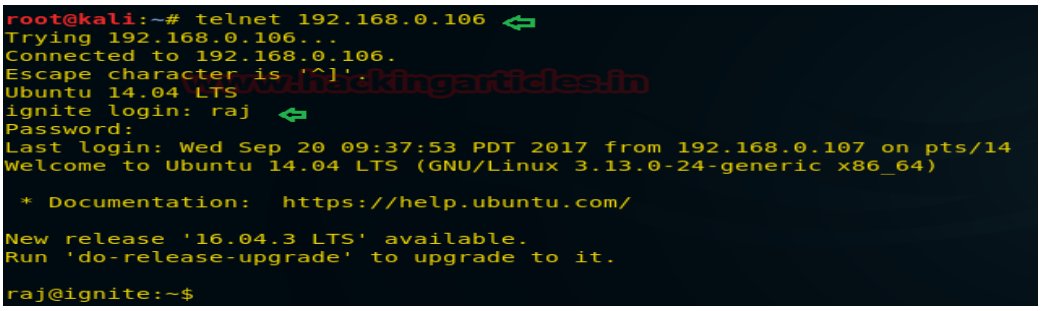


(b) Port 23 Telnet

It's a command that allows users to access remote computers, it allows the attacker to login the computer as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

To gain access to the computer through the telnet protocol you need to use the following commands

telnet (ip address of the target machine) (port number of the service running) example: telnet 192.168.0.8 23




(c) Port 22 SSH

It is also known as a secure shell. It is the process where by an individual try to connect to the server remotely from another computer, it was created as an alternative method of the non-secure protocol login method such as telnet and rlogin and also the insecure file transfer method such as FTP. To make a connection to the server through port 22 you type in the following command

**Method 1:**

Ssh (ip address of the target machine) (port number of the service running) example:

Ssh 192.168.0.8 22

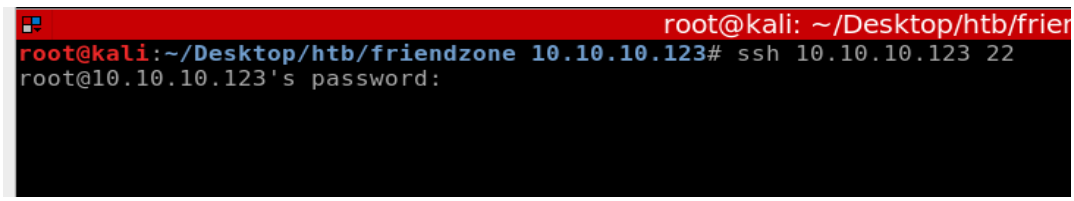
Or

**Method 2:**

Ssh (username)@ (ip address of the target machine) (port number of the service running) example:

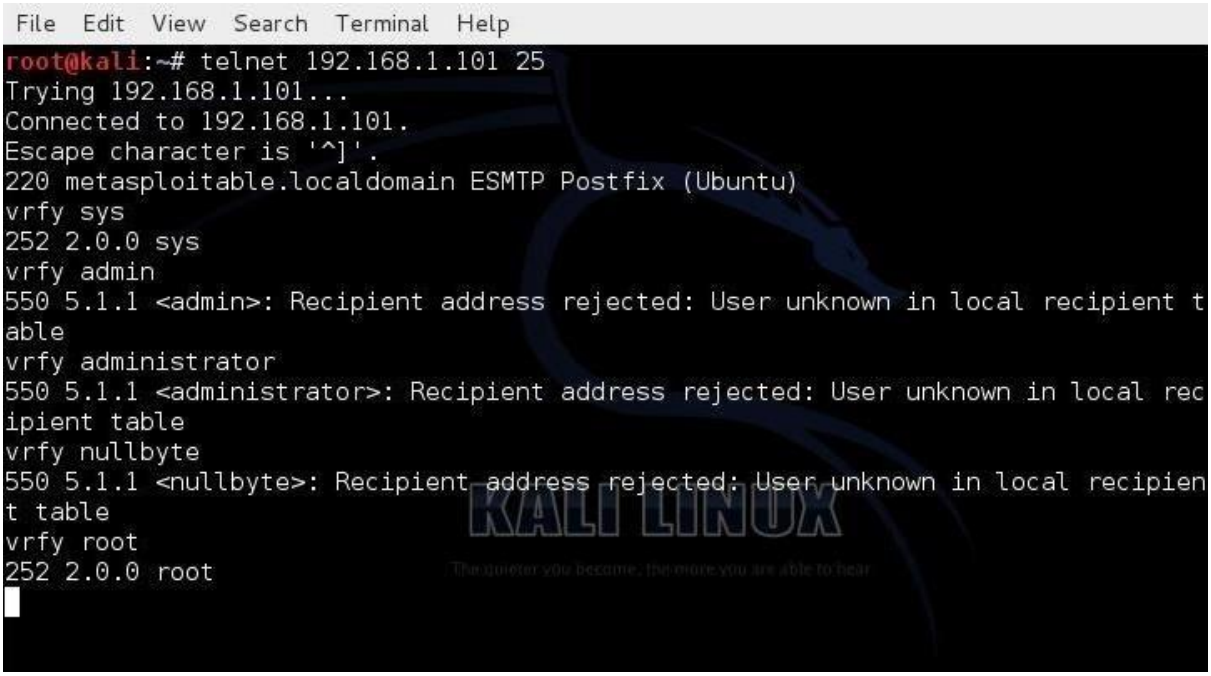
Ssh john.smith@192.168.0.101 22

From method 1 you are login in as root (administrator) and from method 2 you are login in as a user



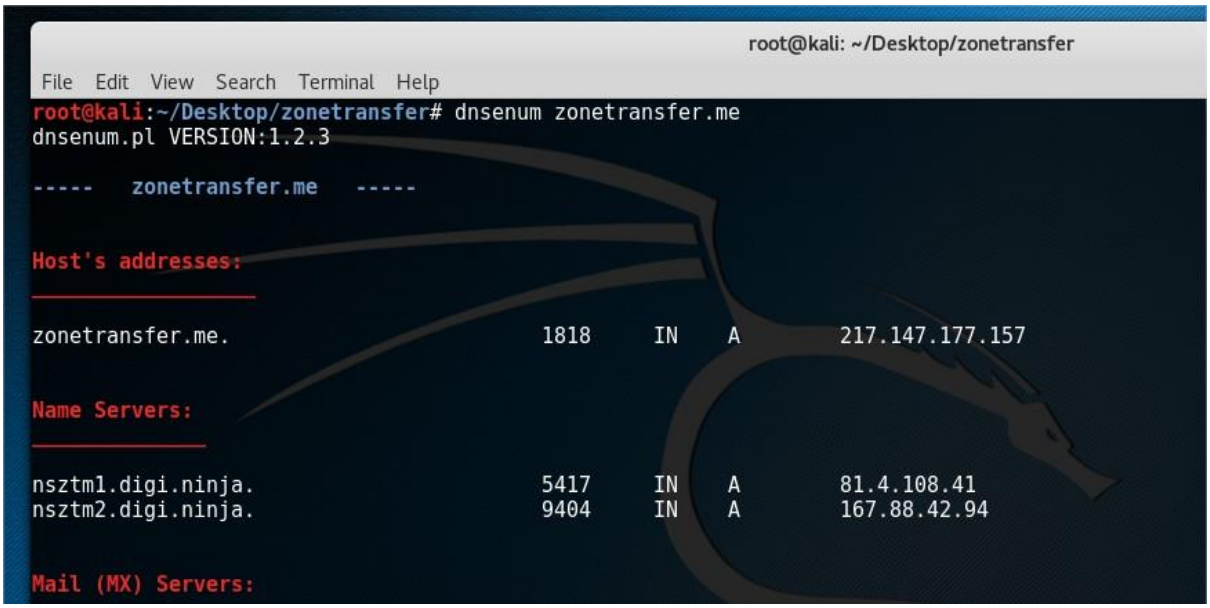
(d) Port 25 SMTP

it is also known as simple mail transfer protocol. It provides the ability to send and receive emails messages over the internet. The tool you use to login smtp is telnet




(e) Port 53 DNS Zone Transfer

It's the process where by the DNS server gives a copy of part of its database (which is known as zone) to another DNS server. A hacker could get information about your topology and about your internal network. Here to enumerate a dns server you are going to use a tool called dnsrecon or dnsenum



(f) Port 80 HTTP

Its also known as hypertext transfer protocol. It is used by the world wide web and its how messages are being formatted and transmitted, and what actions web servers and browsers should take in response to various commands. There are many tools that can be used to enumerate port 50 this includes **Gobuster, Dirbuster, dirb, Nikto, curl, burp suite and owasp-zap**. Each tool has it specific functions

(a) Curl is used for examining the contents (source codes) of a web page

(b) Gobuster, Dirbuster, dirb, Nikto, burpsuite and owasp -zap is used for directory discovery

(c) Burpsuite and owasp -zap can perform spidering on the webpage, intercepting requests and editing them, discover the web page directories encoding and decoding of data and intercepting and editing of cookies. These two tools offer many more functionalities than listed here

(g) Port 110 POP3

It's the most common and recent standard protocol for receiving e-mail. An attacker could use this service to his/her advantage to read the emails from the server once successfully logged in

The tool being used to connect to the port is telnet which will help you with the remote connection

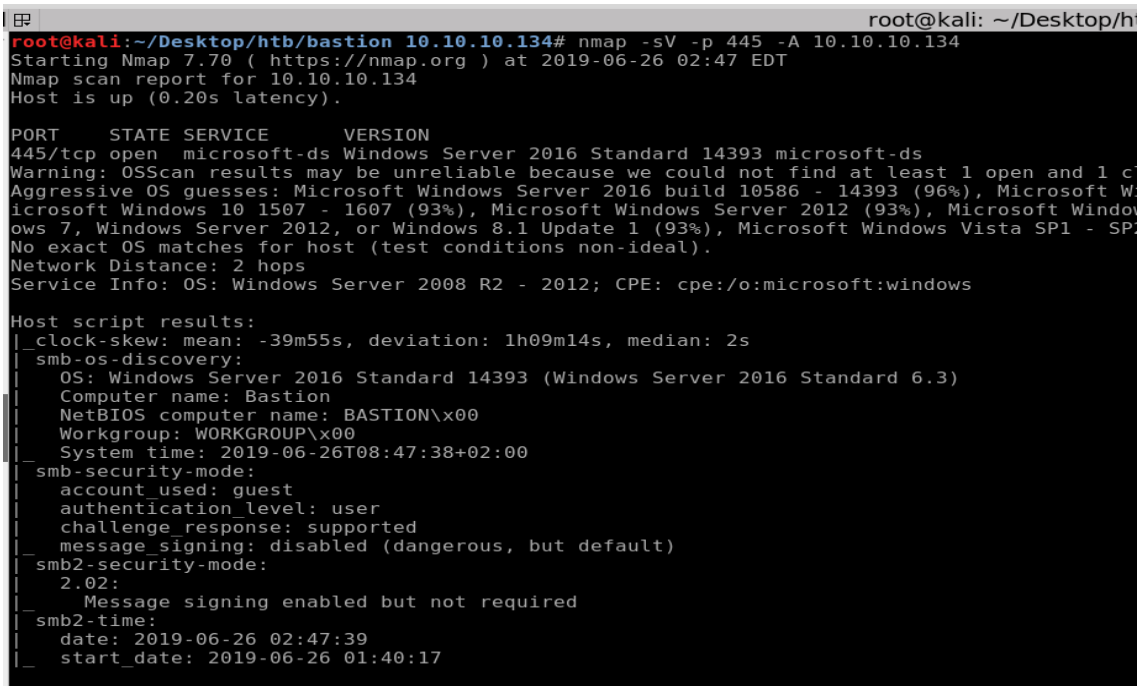
(h) Port 161/162 SNMP

It is also known as simple network management protocol. It is used to monitor network connected devices. It is mainly used for collecting and organizing information about managed devices on the network and it can also be used to change information to change the way the devices work.

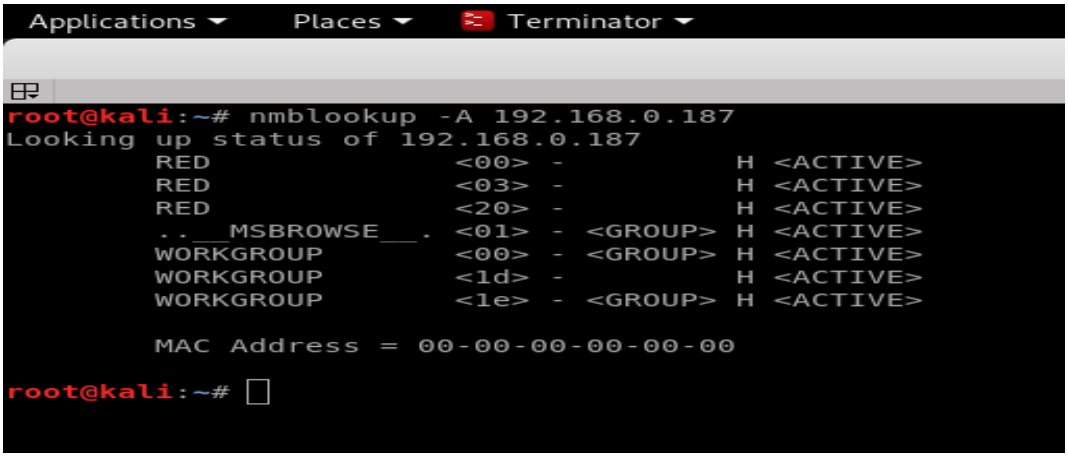
The tool being used to connect to the port is telnet which will help you with the remote connection

(i) Port 445 SMB

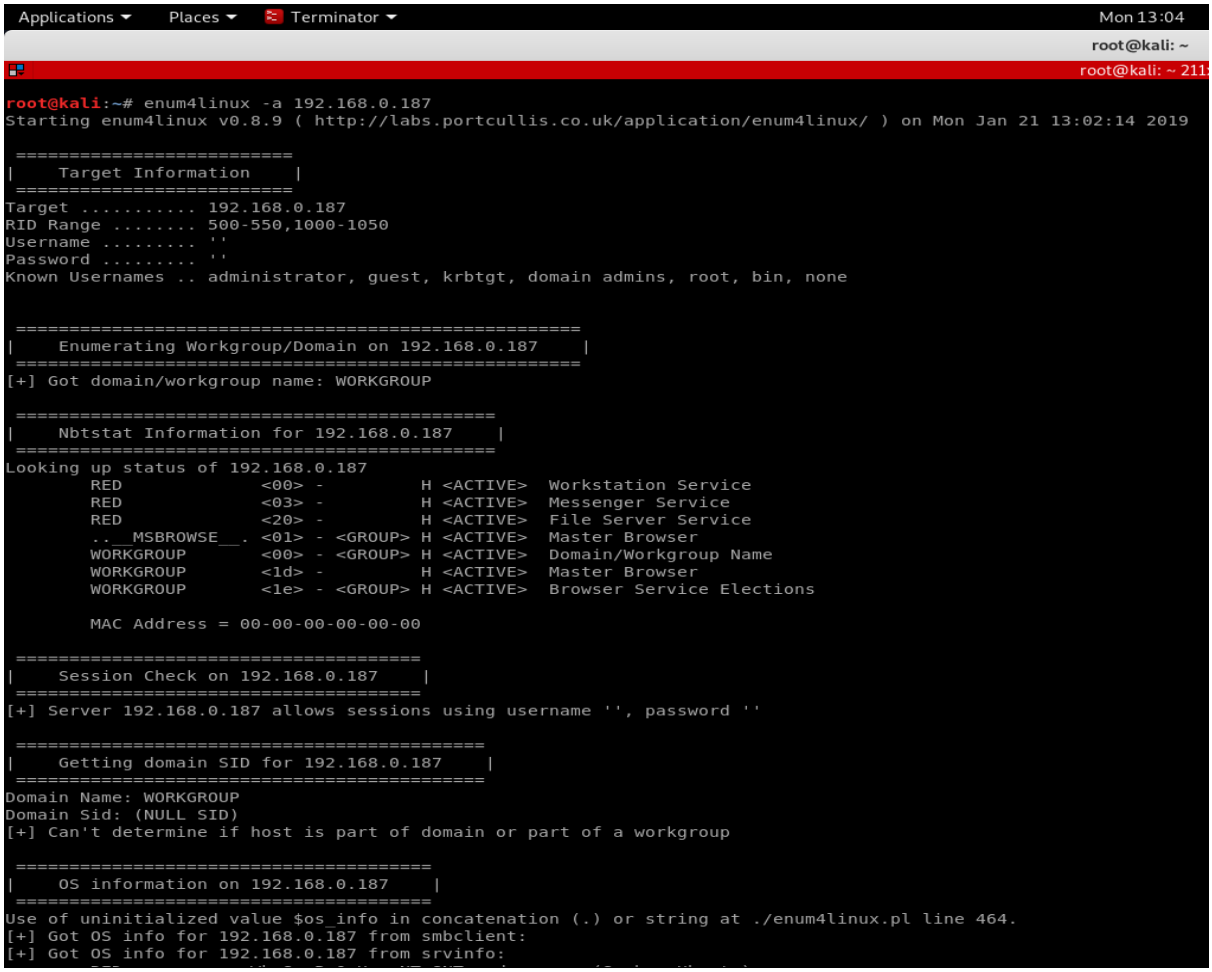
also know as server message block. It is a sharing service protocol, it is used to share resources from the network like files, printers, serial ports and other resources. Nmap as a tool can be used to enumerate the protocol to get to know about the configurations



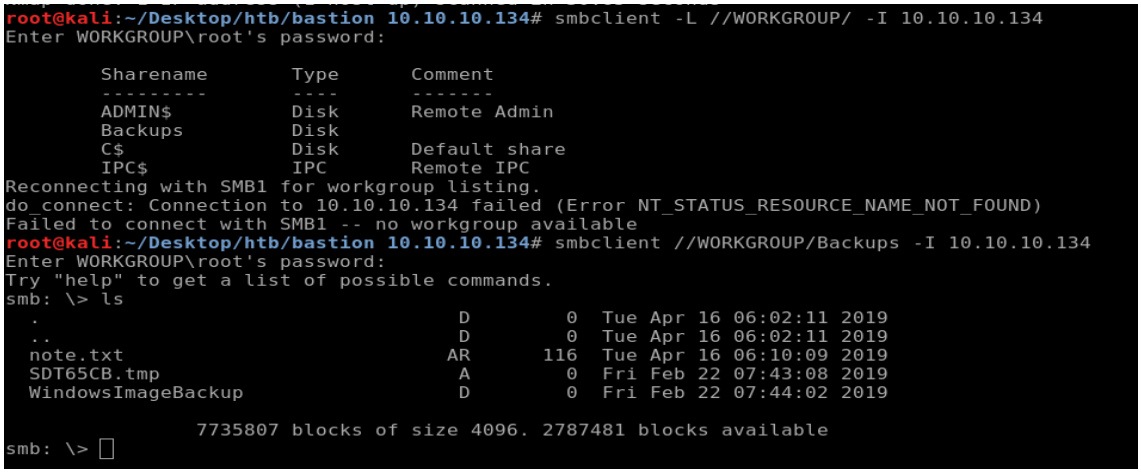

Nmblookup can be used to find out the name of the computers connected to the network



Enum4linux is another tool that can be used to interrogate the machine and get possible usernames, domains, passwords, NetBIOS information and other relevant information




Smbclient is used for creating the remote connection to the targeted computer that are visible on the network, once access you can download a copy of the files from the computer.



# CHAPTER 5: OTHER HACKING TECHNIQUES

## (a) Robots/web crawlers/Spidering

is a program or automated script which browses the World Wide Web in a methodical, automated manner. This process is called Web crawling or spidering. Many legitimate sites, search engines, use spidering as a means of providing up-to-date data. This can be achieved using burp suite which has an option to spider a host.

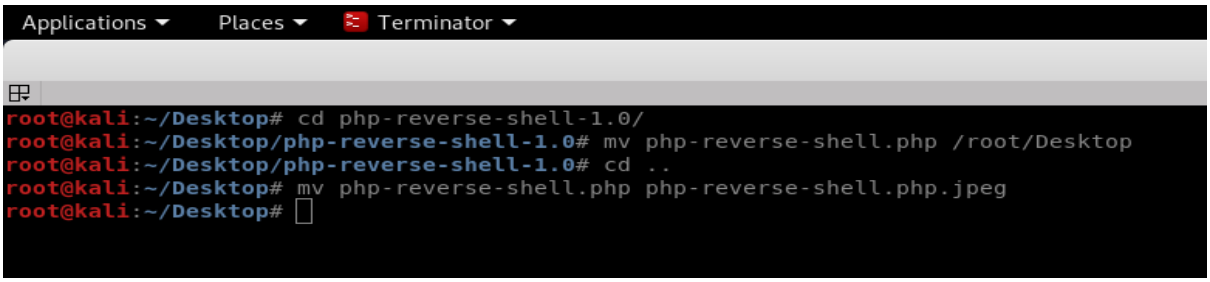

Other tools that you could use to perform spidering is the wget command from the terminal, you could use the -S or - -spider or - - server-response to perform spidering using the wget command.

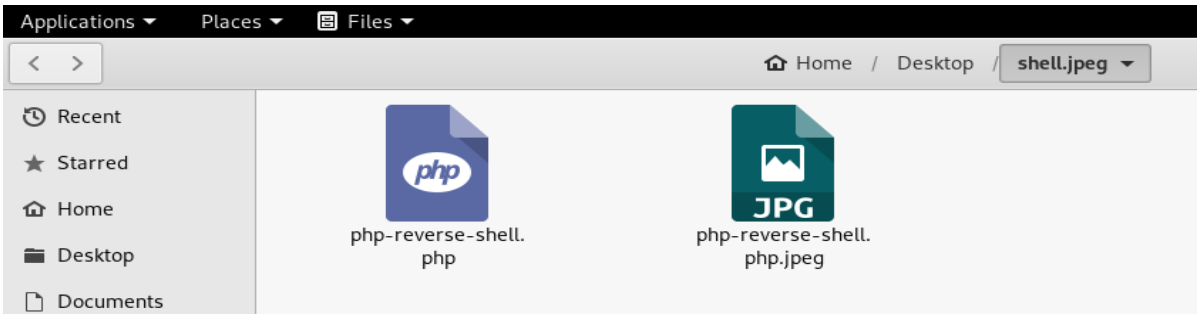
```
root@kali:~# wget -S nmap.org
--2019-06-27 03:34:38--  http://nmap.org/
Resolving nmap.org (nmap.org)... 45.33.49.119, 2600:3c01::f03c:91ff:fe98:ff4e
Connecting to nmap.org (nmap.org)|45.33.49.119|:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 301 Moved Permanently
  Date: Thu, 27 Jun 2019 07:34:41 GMT
  Server: Apache/2.4.6 (CentOS)
  Location: https://nmap.org/
  Content-Length: 298
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1
Location: https://nmap.org/ [following]
--2019-06-27 03:34:42--  https://nmap.org/
Connecting to nmap.org (nmap.org)|45.33.49.119|:443... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Date: Thu, 27 Jun 2019 07:34:43 GMT
  Server: Apache/2.4.6 (CentOS)
  Strict-Transport-Security: max-age=31536000; preload
  Accept-Ranges: bytes
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=utf-8
Length: unspecified [text/html]
Saving to: 'index.html.3'

index.html.3                                [  <=>

2019-06-27 03:34:43 (61.6 KB/s) - 'index.html.3' saved [22371]
```

The purpose of spidering a host is to be able to get information about the target system especially web page resources like index and folders

(b) Changing file extensions

To make a file look like an image all you need to do is change the extension using the mv command




The purpose of changing the file extension is to trick the content filet when trying to upload the shell that the file your uploading isn't malicious. Sometimes you may find that when your trying to upload a shell on a webpage, the page will filter out anything that has an extension of .php so to bypass this content filter you will be required to change the file extension to successfully upload the shell.

(c) Port knocking

port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports (use nmap)

The primary advantage of this method is that the ports protected by Port Knocking will be shown unavailable for a usual port scan. The main purpose of port knocking is to create a connection with the port.

# CHAPTER 6: WHAT IS CAPTURE THE FLAG

Capture the flag is a cyber security game that involves challenging individual to try and hack a vulnerable machine and try to get the flag's that are stored in various places into the system. The aim of these games is to teach an individual about security problems, how services could be exploited and how to protect yourself against such attacks. You can play these games either as a an individual or you could play in teams whereby teams would be playing attack and defend.

## 6.1 PLATFORM FOR CTF'S

There are many platforms out there where you can practice your penetration testing skills without getting on the illegal side of the law since when you do penetration testing without the consent of the owners you might end up in jail no matter what intentions you have Good or bad. The most famous and reputable platform to practice your skills in **hack the box** and **tryhackme** but apart from these two you could download virtual machines from **vulnhub**.

## 6.2 TYPES OF CHALLENGES

There are many challenges that are involved in capture the flag competitions which an individual can try to get themselves involved with; each challenge teaches an individual about the specific area of expertise. The challenges involved in capture the flag are as follows

(a) programming – these types of challenges usually involve programming to solve the challenge. Most of the time it would in cooperate a mixture of programming and reverse engineering

(b) cryptography – these challenges are usually real-world challenges that usually include the most popular ransomware type of malware

(c) forensics – these types of challenge would usually require you to examine network packets to look for evidence

(d) Exploitation - these types of challenges usually will require you to determine how to exploit a provided running process on the target machine

(e) reverse engineering – for this type of challenge it would require you to reverse engineer an executable that the server would have sent to you

## 6.3 AIM OF CTF'S

Not everything that you do in capture the flag is applicable in real life scenario's, for example in capture the flag you must gain access to the system to retrieve the flag but in a real-life scenario there is no such thing as a flag.

The aim of CTF's is to teach an individual technique which can help them in learning or improving their penetration testing skills. Each challenge that you will get has its lesson that it teaches an individual and each challenge can be applicable in real life systems for example you might learn SQL injection

The following are some of the lessons that you will learn from each challenge:

(a) programming challenges helps an individual enhance their Whitebox testing skills for example the source code analysis where u find loopholes by reading code

(b) cryptography challenges help an individual enhance their cryptography testing skills for example. They will teach you on how to gain access to poorly configured communication systems.

(c) forensics challenges help an individual enhance their forensics skills for example the packets that you would examine could help you determine if a port scan has been done on your system. This could be applicable on real systems to determine the activities tat happened before getting hacked or to determine if someone was doing any malicious activities with the network.

(d) exploitation challenges help an individual enhance their service enumeration and hacking skills for example when port 21 is open here you will know how to access to the remote system and how to exploit the service.

# CONCLUSION

This article is intended to help people who are getting into penetration testing, there are a lot of topics which are not covered but it's the authors belief that the individuals who are going to read this article will do more research on other topics which haven't been covered in this article which they are going to meet along their career line while progressing their skills from beginner to Intermediate and finally to advanced level hacking.

There is no easy way to success. The key to become a good penetration tester is to understand what you're doing, practice more and do more research, nothing comes easy.

Google is your best friend, there are a lot of information that can be found on google so make use of google if you don't understand a certain topic or don't understand what a certain port service is and how it could be exploited go to google and do research on the service.

# References


Akash. (n.d.). *TechTric*. Retrieved from TechTric: http://www.techtrick.in/description/4581-website-hacking-sql-injections-sqlmap-introduction

ALex. (June, 6 2018). *ethical hacking and penetration testing* . Retrieved from ethical hacking and penetration testing : https://miloserdov.org/?p=1254

Arms, C. (2015, January 22). *Cybersecurity News and Business Computer Tips*. Retrieved from Cybersecurity News and Business Computer Tips: https://cyberarms.wordpress.com/tag/metasploit/page/4/

Bjacharya. (2016, July 1). *cybrary*. Retrieved from cybrary: https://www.cybrary.it/0p3n/ethical-hacking-kali-linux-part-6-nmap-network-mapper/

Brown, E. (2018, November 28). *AT&T Business*. Retrieved from AT&T Cybersecurity: https://www.alienvault.com/blogs/security-essentials/capture-the-flag-ctf-what-is-it-for-a-newbie

CISCO. (n.d.). *CCNA Security COurse*. Retrieved from Geek University : https://geek-university.com/ccna-security/hacking-methodology/

Day, Z. (2017, April 15). *Zero Day*. Retrieved from Zero Day: https://zero-day.io/dns-zone-transfers/

Forge, S. (n.d.). *Soure Forge.net*. Retrieved from Soure Forge.net: http://pdfcrack.sourceforge.net/

Grotherus, J. ( 2016, January 5). *Cybrary*. Retrieved from Cybrary: https://www.cybrary.it/0p3n/discover-network-hosts-with-netdiscover/

Haas, J. (2019, March 21). *Life wire*. Retrieved from Life wire: https://www.lifewire.com/strings-linux-command-4093452

Hacking-Tutorials.com. (n.d.). *Hacking-Tutorials.com*. Retrieved from Hacking-Tutorials.com: https://www.hacking-tutorial.com/tips-and-trick/information-gathering-using-theharvester-in-kali-linux/#sthash.HSrdEL0T.V4x4MX0W.dpbs

Hofman, M. (2009, November 11). *Internet Storm Center*. Retrieved from Internet Storm Center: https://isc.sans.edu/diary/Cyber+Security+Awareness+Month+-+Day+12+Ports+161162+Simple+Network+Management+Protocol+%28SNMP%29/7327

Ismail, M. H. (2011, June 15). *Mypapit GNU/Linux*. Retrieved from Mypapit GNU/Linux: https://blog.mypapit.net/2011/06/crack-zip-file-password-with-fcrackzip.html

Laureau, J. (2019, May 12). *Secjuice*. Retrieved from Secjuice: https://www.secjuice.com/hacking-methodology-eli5/

linux, K. (n.d.). *Kali Tools*. Retrieved from Kali Tools: https://tools.kali.org/web-applications/burpsuite

Linux, K. (n.d.). *Kali tools*. Retrieved from Kali tools: https://tools.kali.org/password-attacks/crunch

Linux, K. (n.d.). *Kali Tools*. Retrieved from Kali Tools: https://tools.kali.org/web-applications/wpscan

Linux, K. (n.d.). *Kali Tools*. Retrieved from Kali Tools: https://tools.kali.org/information-gathering/enum4linux

Margaret Rouse, A. L. (2006, August). *Whatis.com*. Retrieved from Whatis.com: https://searchnetworking.techtarget.com/definition/Telnet

Margaret Rouse, P. L. (2018, October). *Whatis.com*. Retrieved from Whatis.com: https://searchsecurity.techtarget.com/definition/Secure-Shell

OpenCampus. (n.d.). *OpenCampus*. Retrieved from Ethical Hacking: https://www.greycampus.com/opencampus/ethical-hacking/what-is-scanning

OpenCampus. (n.d.). *OpenCampus*. Retrieved from Ethical Hacking: https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types

Rouse, M. (2007, March). *Whatis.com*. Retrieved from Whatis.com: https://whatis.techtarget.com/definition/POP3-Post-Office-Protocol-3

Techopedia. (n.d.). *Techopedia*. Retrieved from Techopedia: https://www.techopedia.com/definition/1710/simple-mail-transfer-protocol-smtp

Vlajin, B. (2018, October 18). *cloudwards*. Retrieved from cloudwards: https://www.cloudwards.net/what-is-ftp/