**EXPERIMENT- 01**

**HACKING TOOLS AND SKILLS**

**AIM:**

To learn about various hacking tools and skills required to hacking.

**INTRODUCTION:**

There are various definitions one can get to know about hackers. The term hacker was used in the early 1990s and it was to describe someone who could be a great programmer and had the ability to solve complex problems. Now the definition of the hacker changed from time to time as it started to gain a negative vibe by the media.

The media started to refer to this hacker as someone who finds loopholes and tries to gain access into the system to steal information that could be important for the victims. This was the picture created by the media to only show the negative aspect, but they didn’t show the positive aspect. The positive aspect was someone who was exposing the vulnerabilities found in the system and protecting organizations and multiple users.

In short, we can define a hacker as someone who is able to be creative, solve problems that can be complex, and more. Due to this reason, the term has been broken into three different categories :

**White Hat Hacker**

They are the hackers referred to as security professionals. This type of hacker is employed by organizations, and they are permitted to attack an organization. They can attack the organization because their main job is to find the vulnerabilities which can be used by the attacker.

**Black Hat Hacker**

They are one type of hackers who uses the knowledge for malicious purposes. They are someone whom we can call a cracker. The way they use the knowledge is to gain access to the information of the user which might be dangerous for the victims.

**Grey Hat Hacker**

They are the type of hacker who acts as both the white Hat Hacker and the Black Hat Hacker. For example: - A grey hat hacker can work as a security profession for any organization and finds the vulnerabilities that still exist in the system. But they can leave a backdoor, by which they can access and can sell confidential information to the competitors of a company.

**Script Kiddie**

They are someone who doesn’t have the experience or lack knowledge.  The experience or the knowledge they lack is how an exploit works. They mostly rely on those exploits which are already created by someone. They are someone who can compromise the target, but they can’t modify or debug the exploit if it does not work.

**Elite Hacker**

They are someone who has efficient knowledge of how the exploit takes place, or they can create exploits. They are someone who can also modify the codes that someone else has written. In short, we can say that they have skills that are elite.

**Ethical Hacker**

Ethical hackers are those who are hired and are given permission to attack the system. They can attack the system just to expose the vulnerabilities, that an attacker can take advantage of.

**Hacktivists**   
They are actually a group of hackers. They usually hack into the computer systems because they have some reason, or they have some purpose. Now the purpose can be of anything like freedom of speech and so on.

**Ethical Hacking**

[Ethical Hacking](https://www.geeksforgeeks.org/introduction-to-ethical-hacking/) is compromising computer systems for assessing security and acting in good faith by informing the vulnerable party. Ethical hacking is a key skill for many job roles related to securing the online assets of an organization. The professionals working on these job roles maintain the organization’s computers, servers, and other components of its infrastructure in working conditions preventing unauthorized access through non-physical channels.

 Ethical hacking is to scan vulnerabilities and to find potential threats on a computer or network. An ethical hacker finds the weak points or loopholes in a computer, web applications, or network and reports them to the organization.

**SKILLS REQUIRED**

**1. Computer Networking Skills**

One of the most important skills to become an ethical hacker is networking skills. The computer network is nothing but the interconnection of multiple devices, generally termed as Hosts connected using multiple paths to send/receive data or media. Understanding networks like DHCP, Supernetting, Subnetting, and more will provide ethical hackers to explore the various interconnected computers in a network and the potential security threats that this might create, as well as how to handle those threats.

**2. Computer Skills**

Computer skills are knowledge and ability which allow one to use computers and related technology. Typically, basic computer skills include data processing, managing computer files, and creating presentations. Advanced computer skills include managing databases, programming, and running calculations in spreadsheets. Some of the most essential computer skills are MS Office, Spreadsheets, Email, Database Management, social media, Web, Enterprise systems, etc. An ethical hacker needs to be a computer systems expert.

**3. Linux Skills**

Linux is a community of open-source Unix like operating systems that are based on the Linux Kernel. It is a free and open-source operating system and the source code can be modified and distributed to anyone commercially or non-commercially under the GNU General Public License. The main reason to learn Linux for an ethical hacker is, in terms of security, Linux is more secure than any other operating system. It does not mean that Linux is 100 percent secure it has some malware for it but is less vulnerable than any other operating system. So, it does not require any anti-virus software.

**4. Programming Skills**

“The act of writing code understood by a computational device to perform various instructions.”  Before one write code, he/she must choose the best programming language for his/her programming. Here is the list of programming languages used by ethical hackers

 Python, SQL, C, JavaScript, PHP, Java, Ruby, Perl, C++

**5. Basic Hardware Knowledge**

Computer hardware comprises the physical parts of a computer, like the central processing unit (CPU), monitor, mouse, keyboard, computer data storage, graphics card, sound card, speakers and motherboard, etc. By contrast, the software is the set of instructions that can be stored and run by hardware. For example, suppose one wants to hack a machine that is controlled by a computer. Firstly, he/she needs to know about the machine or how it works. Last, he has to get access to the computer that controls the machine. Now, the machine will have a very good software security system; however, hackers don’t care about hardware security, so he can play with the hardware if he can access it. If one doesn’t know about hardware, then how will he/she know how the motherboard works, how USBs to transfer data, or how CMOS or BIOS work together, etc.? So, one must have basic hardware knowledge also to become an ethical hacker.

**6. Reverse Engineering**

Reverse Engineering is a process of recovering the design, requirement specifications, and functions of a product from an analysis of its code. It builds a program database and generates information from this. The objective of reverse engineering is to expedite the maintenance work by improving the understandability of a system and to produce the necessary documents for a legacy system. In software security, reverse engineering is widely used to ensure that the system lacks any major security flaws or vulnerabilities. It helps to make a system robust, thereby protecting it from hackers and spyware. Some developers even go as far as hacking their system to identify vulnerabilities – a system referred to as ethical hacking.

**7. Cryptography Skills**

Cryptography is the study and application of techniques for reliable communication in the presence of third parties called adversaries. It deals with developing and analysing protocols that prevent malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Cryptography deals with converting a normal text/message known as plain text to a non-readable form known as ciphertext during the transmission to make it incomprehensible to hackers. An ethical hacker must assure that communication between different people within the organization does not leak.

**8. Database Skills**

DBMS is the crux of creating and managing all databases. Accessing a database where all the information is stored can put the company in a tremendous threat, so ensuring that this software is hack-proof is important. An ethical hacker must have a good understanding of this, along with different database engines and data schemas to help the organization build a strong DBMS.

**9. Problem-solving Skills**

Problem-solving skills help one to determine the source of a problem and find an effective solution. Apart from the technical skills pointed above, an ethical hacker also must be a critical thinker and dynamic problem solver. They must be wanting to learn new ways and ensure all security breaches are thoroughly checked. This requires tons of testing and an ingenious penchant to device new ways of problem-solving.  
**TOOLS USED FOR HACKING**

**Kali Linux** is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts,

The official website of Kali Linux is Kali.org. It gained its popularity when it was practically used in Mr. Robot Series. It was not designed for general purposes; it is supposed to be used by professionals or by those who know how to operate Linux/Kali.

Sometimes we have to automate our tasks while performing penetration testing or hacking as there could be thousands of conditions and payloads to test and testing them manually is a difficult task, so to increase the time efficiency we use tools that come pre-packed with Kali Linux. These tools not only save our time but also captures the accurate data and output the specific result. Kali Linux comes packed with **more than 350 tools** which could be useful for hacking or penetration testing.

**1. Nmap**

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyses the responses in order to produce the desired results. It could even be used for host discovery, operating system detection, or scanning for open ports. It is one of the most popular reconnaissance tools.

**To use nmap:**

Ping the host with ping command to get the IP address

*ping hostname*

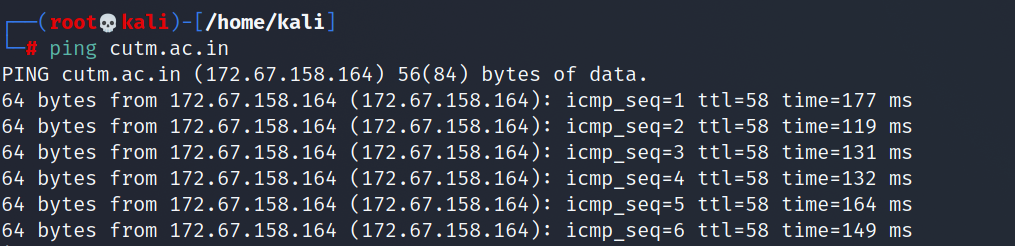
**

Figure 1.1

* Open the terminal and enter the following command there:

*nmap -sV ipaddress*

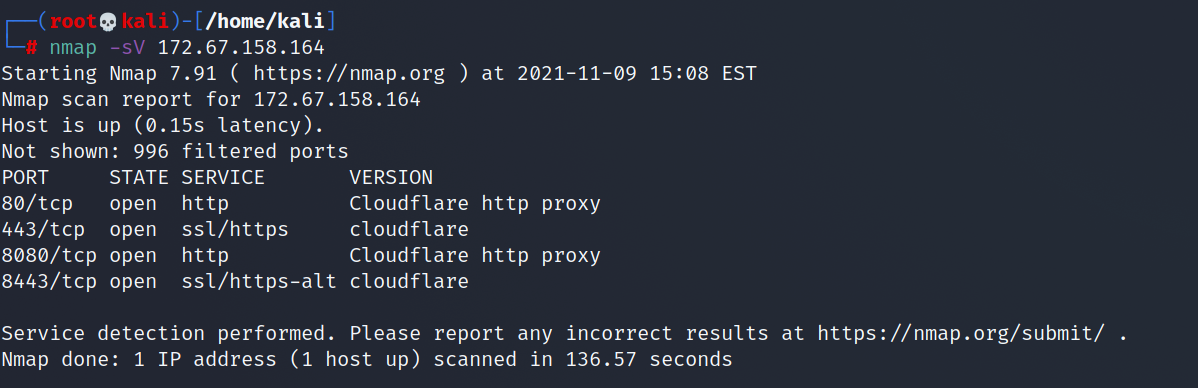
**

Figure 1.2

* Replace the IP address with the IP address of the host you want to scan.
* It will display all the captured details of the host.

**2. Burp Suite**

Burp Suite is one of the most popular web application security testing software. It is used as a proxy, so all the requests from the browser with the proxy pass through it. And as the request passes through the burp suite, it allows us to make changes to those requests as per our need which is good for testing vulnerabilities like XSS or SQLi or even any vulnerability related to the web.  
Kali Linux comes with burp suite community edition which is free but there is a paid edition of this tool known as burp suite professional which has a lot many functions as compared to burp suite community edition.

**To use burpsuite:**

* Open terminal and type “**burpsuite**” there.

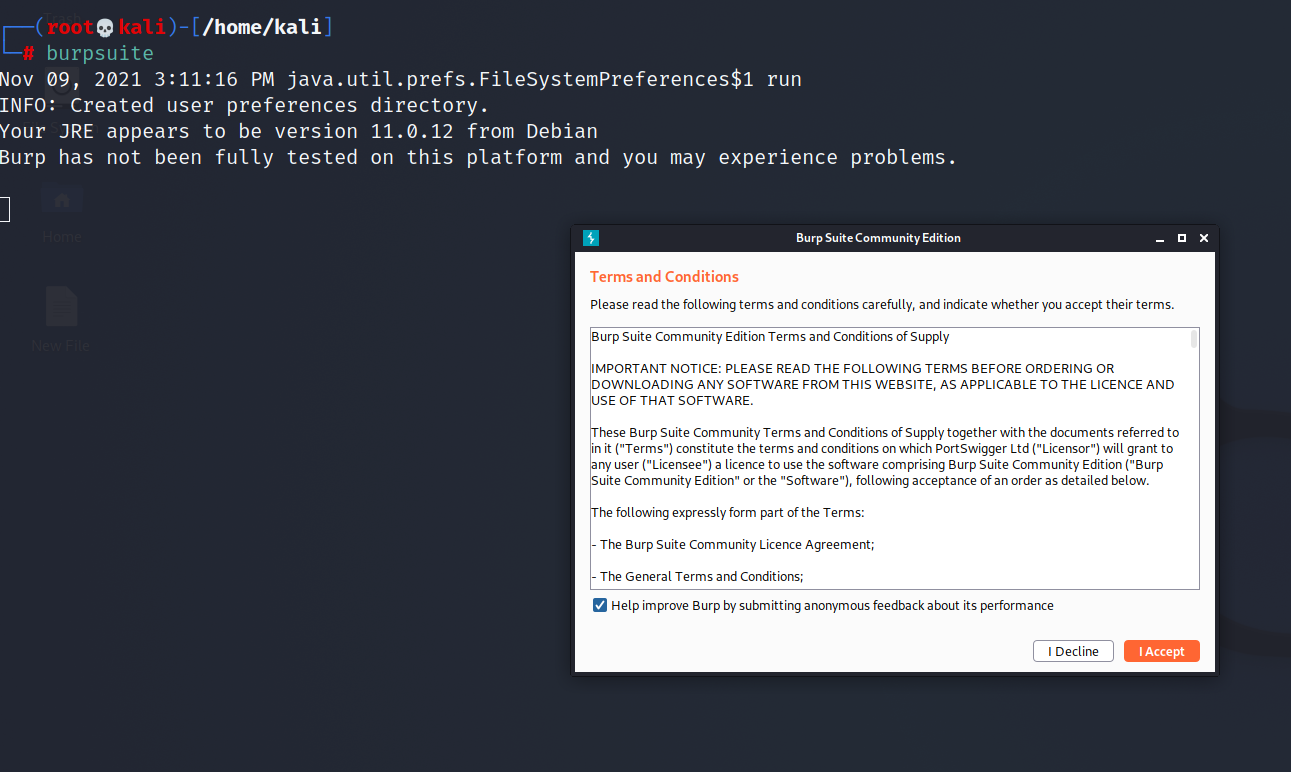


Figure 1.3

* Go to the Proxy tab and turn the interceptor switch to on.

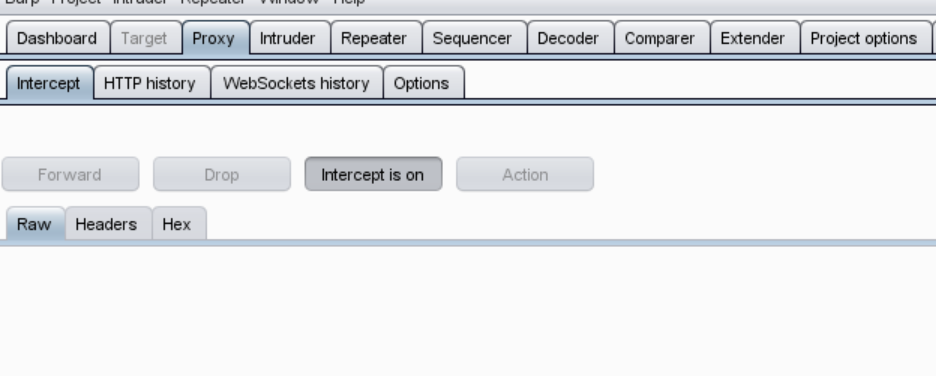


Figure 1.4

* Now visit any URL and it could be seen that the request is captured.

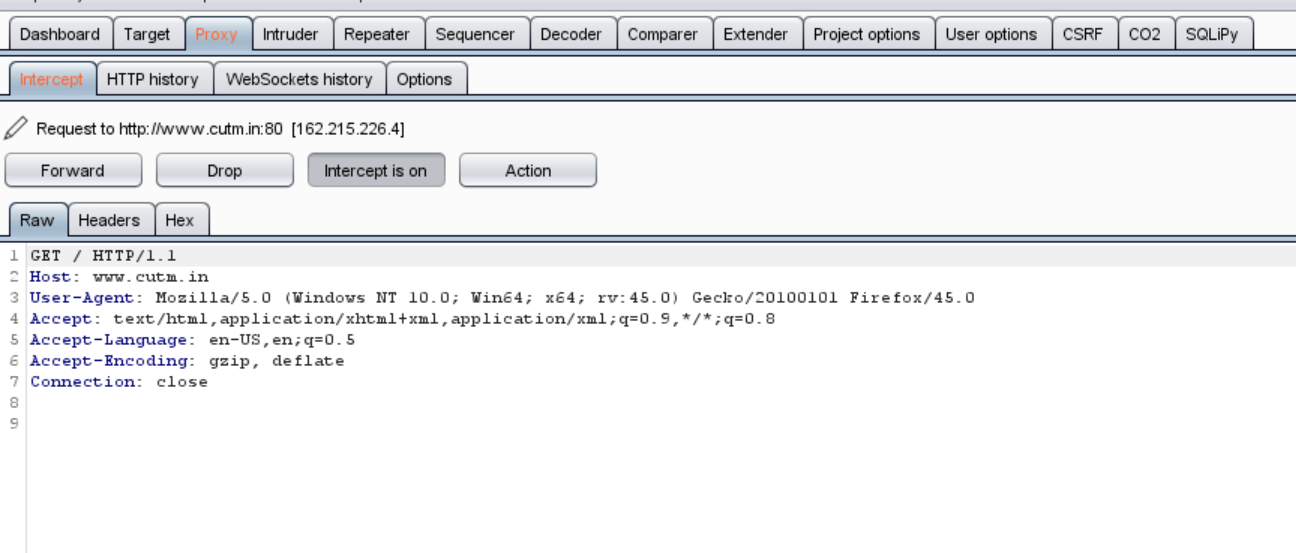


Figure 1.5

**3. Wireshark**

Wireshark is a network security tool used to analyze or work with data sent over a network. It is used to analyze the packets transmitted over a network. These packets may have information like the source IP and the destination IP, the protocol used, the data, and some headers. The packets generally have an extension of “**.pcap**” which could be read using the Wireshark tool.

**To use wireshark:**

Open Wireshark and download a demo pcap file

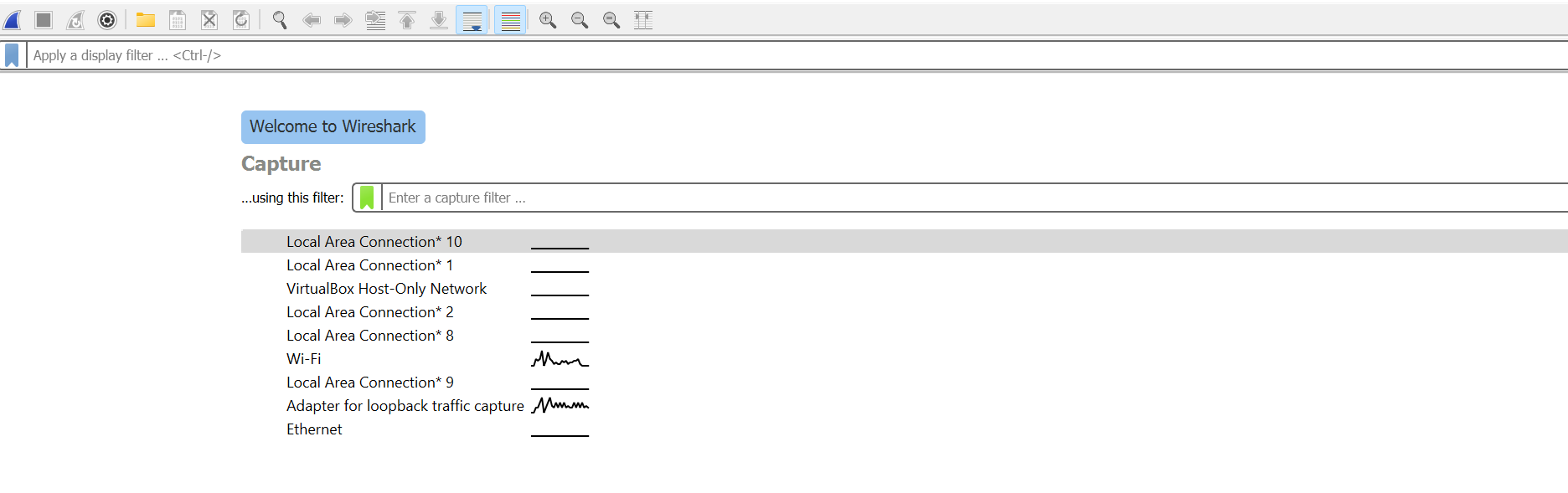


Figure 1.6

* Press”**ctrl+o**” to open a pcap file in wireshsark.

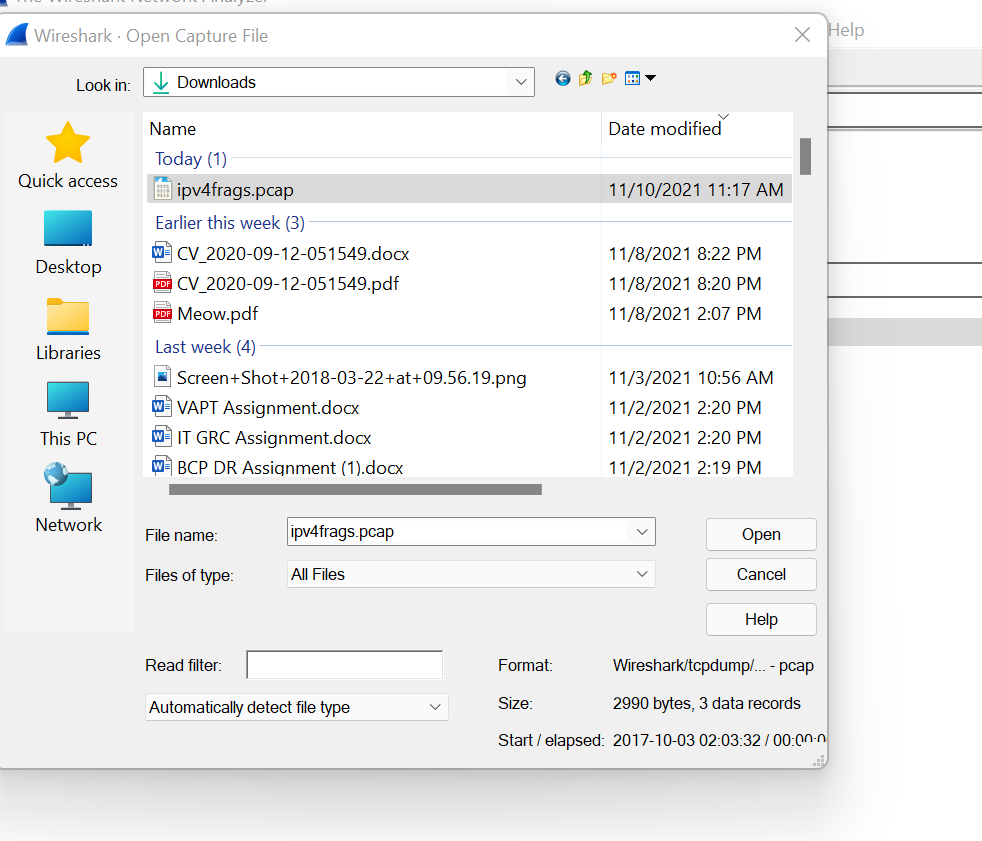


Figure 1.7

* Now it can be seen that it displays the list of packets along with the headers of these packets.

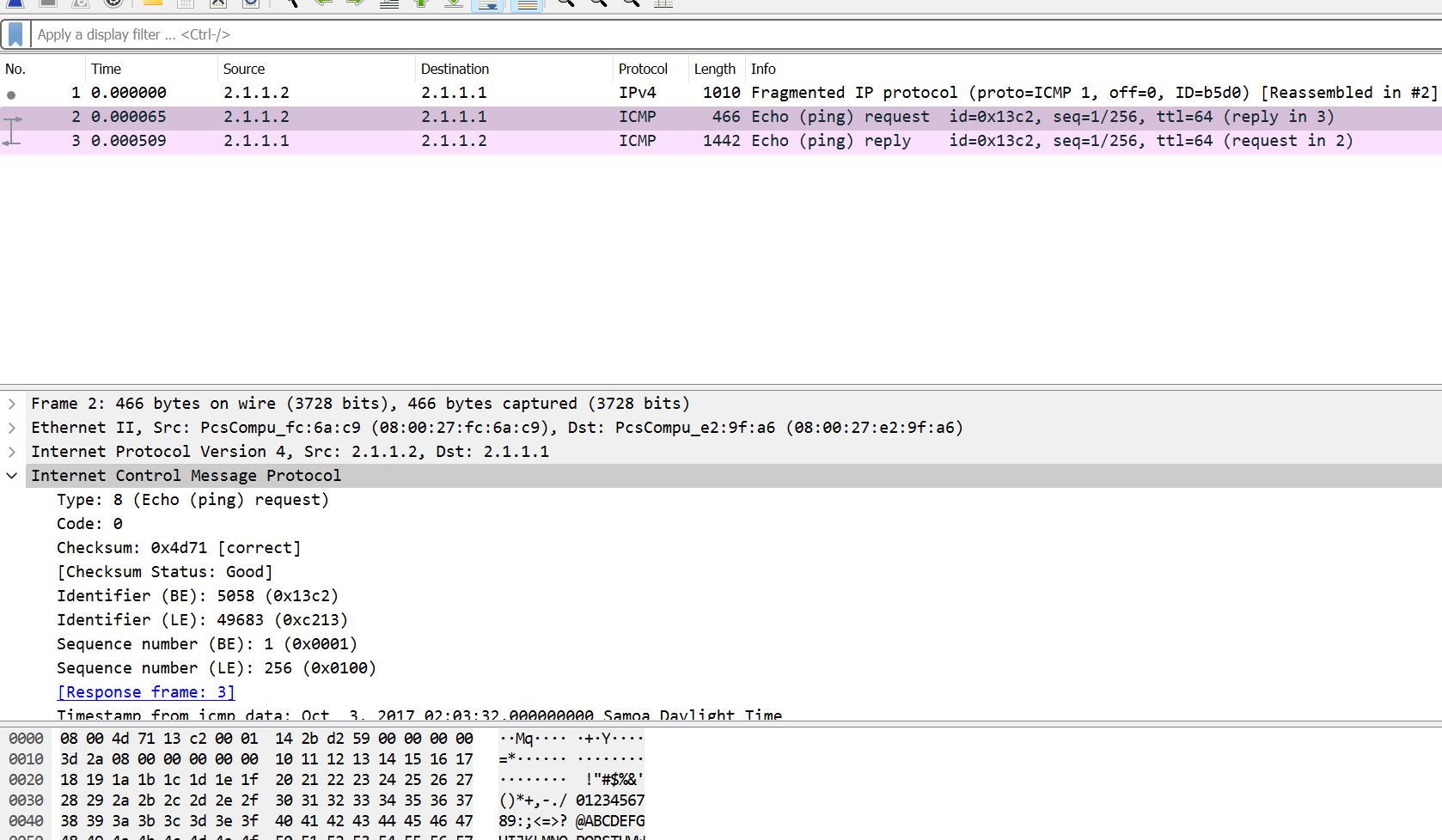


Figure 1.8

**4. Metasploit Framework**

Metasploit is an open-source tool that was designed by Rapid7 technologies. It is one of the world’s most used penetration testing frameworks. It comes packed with a lot of exploits to exploit the vulnerabilities over a network or operating systems. Metasploit generally works over a local network but we can use Metasploit for hosts over the internet using “**port forwarding** “. Metasploit is a CLI based tool but it even has a GUI package called “**armitage**” which makes the use of Metasploit more convenient and feasible.

**To use metasploit:**

* Metasploit comes pre-installed with Kali Linux
* Just enter “**msfconsole**” in the terminal.



Figure 1.9

**5. aircrack-ng**

Aircrack is an all-in-one packet sniffer, WEP and WPA/WPA2 cracker, analysing tool and a hash capturing tool. It is a tool used for Wi-Fi hacking. It helps in capturing the package and reading the hashes out of them and even cracking those hashes by various attacks like dictionary attacks. It supports almost all the latest wireless interfaces.

**To use aircrack-ng:**

aircrack-ng comes pre-compiled with Kali Linux.

* Simply type aircrack-ng in the terminal to use it.

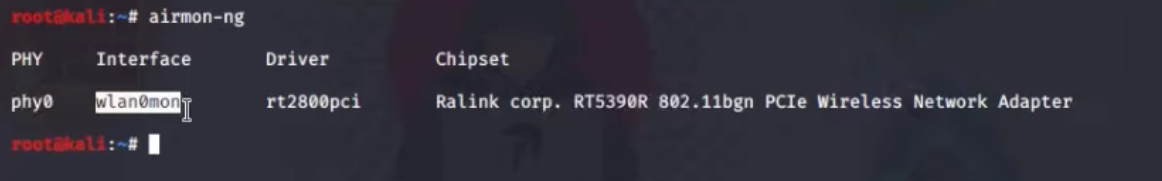


Figure 1.10

**6. Netcat**

Netcat is a networking tool used to work with ports and performing actions like port scanning, port listening, or port redirection. This command is even used for Network Debugging or even network daemon testing. This tool is considered as the Swiss army knife of networking tools. It could even be used to do the operating related to TCP, UDP, or UNIX-domain sockets or to open remote connections and much more.

**To use netcat:**

Netcat comes pre-installed with Kali Linux.

* Just type “**nc**” or “**netcat**” in the terminal to use the tool.
* To perform port listening type the following commands in 2 different terminals.

*nc -nvlp 1234*

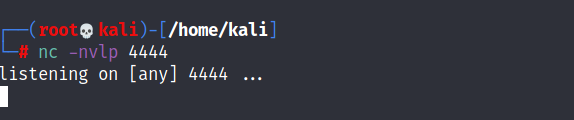
**

Figure 1.11

*nc -nvz ip 1234*

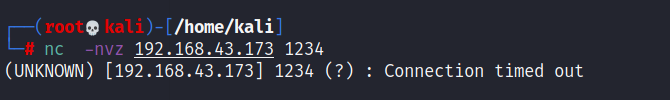
**

Figure 1.12

**7. John the Ripper**

John the Ripper is a great tool for cracking passwords using some famous brute for attacks like dictionary attack or custom wordlist attack etc. It is even used to crack the hashes or passwords for the zipped or compressed files and even locked files as well. It has many available options to crack hashes or passwords.

**To use John the Ripper:**

* John the ripper comes pre-installed in Kali Linux.
* Just type “**john**” in the terminal to use the tool.

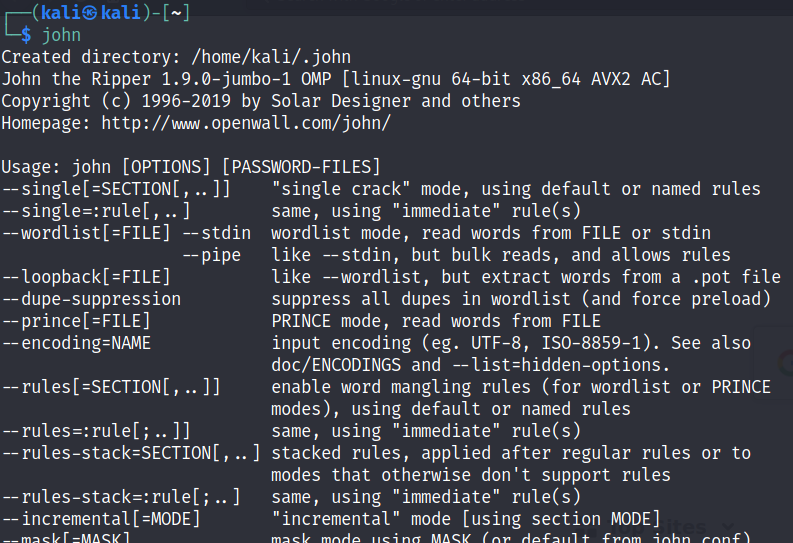


Figure 1.13

**8. sqlmap**

sqlmap is one of the best tools to perform SQL injection attacks. It just automates the process of testing a parameter for SQL injection and even automates the process of exploitation of the vulnerable parameter. It is a great tool as it detects the database on its own so we just have to provide a URL to check whether the parameter in the URL is vulnerable or not, we could even use the requested file to check for POST parameters.

**To use sqlmap tool:**

* sqlmap comes pre-installed in Kali Linux
* Just type sqlmap in the terminal to use the tool.

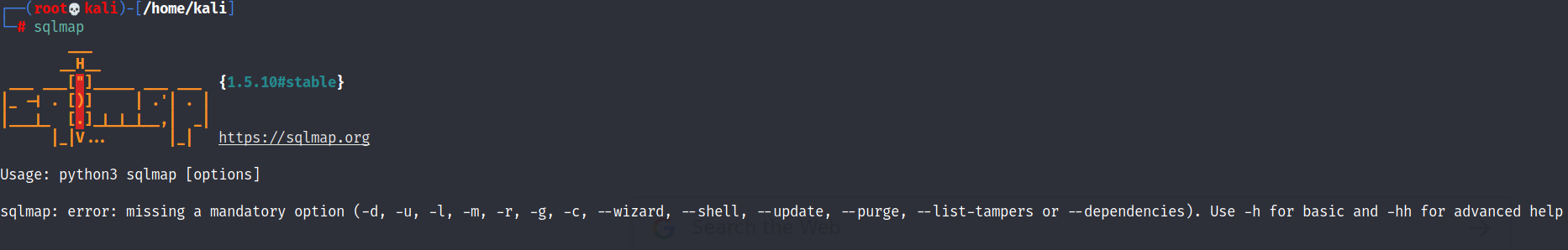


Figure 1.14

**9. Social Engineering Toolkit**

Social Engineering toolkit is a collection of tools that could be used to perform social engineering attacks. These tools use and manipulate human behavior for information gathering. it is a great tool to phish the websites even.

**To use Social Engineering Toolkit (perform experiment and add pics when you submit)**

* Social Engineering Toolkit comes pre-installed with Kali Linux
* Just type “**setoolkit**” in the terminal.

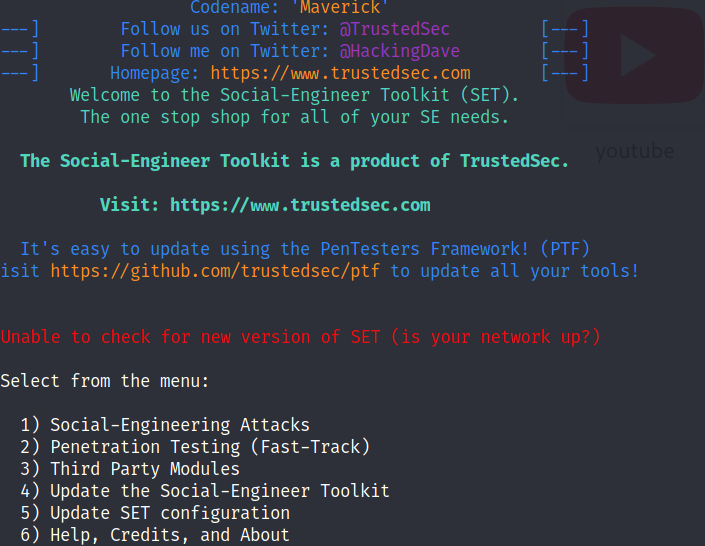
****

Figure 1.15

* Agree to the terms and conditions to start using the social engineering toolkit.

Result: Tools and skills required by an ethical hacker was covered.