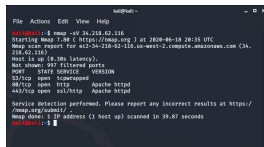


## Assignment 2

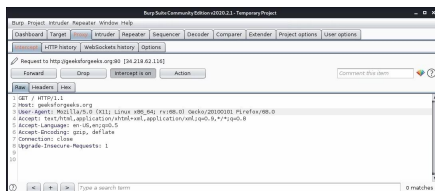
### Tool 1 Nmap

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 analyzes 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.



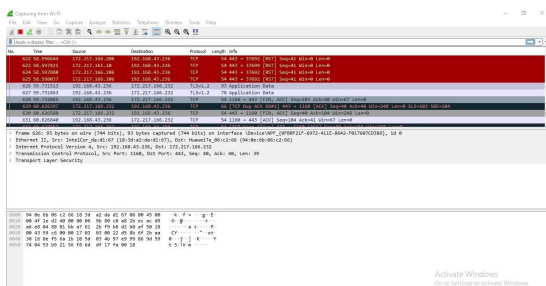
### Tool 2 Burp Suite

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.



### Tool 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



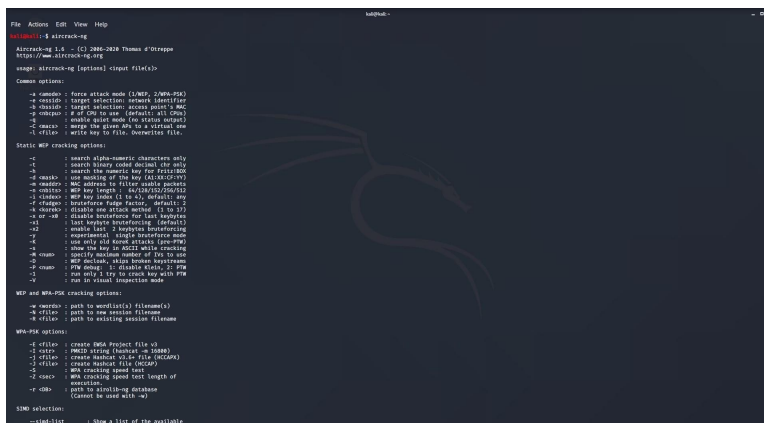
## Tool 4 Metasploit framework

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". Basically 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.

A screenshot of the Metasploit framework terminal interface. The window title is 'msfconsole'. The prompt is 'msf5>'. The terminal shows the Metasploit version '2.0.0-dev (2018-08-14)' and the 'msf5' command being entered. The terminal also shows the 'msf5' command being entered, which displays the Metasploit version and the 'msf5' command being entered. The terminal also shows the 'msf5' command being entered, which displays the Metasploit version and the 'msf5' command being entered.

## Tool 5 aircrack-ng

Aircrack is an all in one packet sniffer, WEP and WPA/WPA2 cracker, analyzing tool and a hash capturing tool. It is a tool used for wifi 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

A screenshot of the aircrack-ng terminal interface. The window title is 'aircrack-ng'. The prompt is 'aircrack-ng 1.0 - (C) 2000-2020 Thomas d'Otreppe'. The terminal shows the 'aircrack-ng' command being entered, which displays the aircrack-ng version and the 'aircrack-ng' command being entered. The terminal also shows the 'aircrack-ng' command being entered, which displays the aircrack-ng version and the 'aircrack-ng' command being entered.

## Tool 6 Netcat

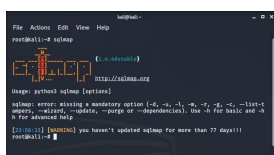
Netcat is a networking tool used to work with ports and performing actions like port scanning, port listening, or port redirection. This command is even used for Network Debugging or even network daemon testing. This tool is considered as the Swiss army knife of networking tools. It

```
msf5(msf5-17101@msf5) $ nc 127.0.0.1 1234
```

John the Ripper is a great tool for cracking passwords using some famous brute force 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.

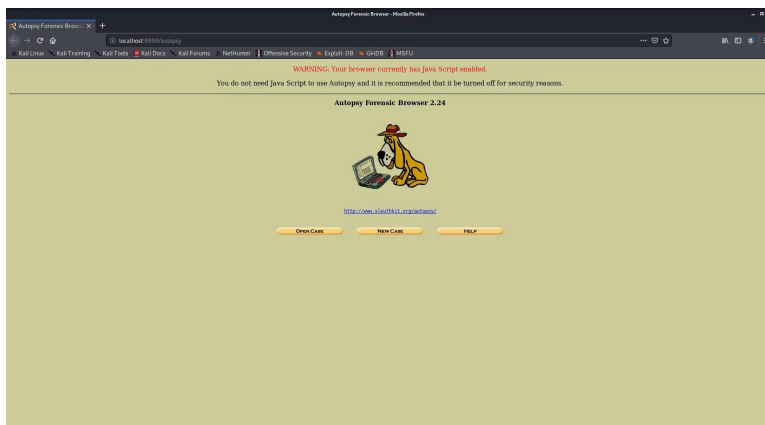
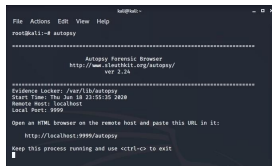


sqlmap is one of the best tools to perform SQL injection attacks. It just automates the process of testing a parameter for SQL injection and even automates the process of exploitation of the vulnerable parameter. It is a great tool as it detects the database on its own so we just have to provide a URL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



## Tool 9 Autopsy

Autopsy is a digital forensics tool that is used to gather information from forensics. Or in other words, this tool is used to investigate files or logs to learn about what exactly was done with the system. It could even be used as a recovery software to recover files from a memory card or a pen drive



## Tool 10 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

