LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework 02

Year and Semester

2021 -22 Spring Semester

Student Name: Sarthak Bikram Rana

London Met ID: 20049228

College ID: NP01NT4S210129

Assignment Due Date: 5th May 2022

Assignment Submission Date: 5th May 2022

Word Count (Where Required): 4949

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgement

This is the second coursework in the Security in the Computing module, in which we were given the task to to research, describe, analyse, evaluate, to demonstrate and to provide mitigation techniques and cases related to information and network security.I choose Brute Force attacks on Information Technology devices and systems as the topic for my coursework. I also had to undertake research on the issue for my coursework by looking at a variety of related articles, journals, reports and websites.

Finally, I would like to thank Mr. Akchayat Bikram Dhoj Joshi, our recognized module leader, for exposing me to the topic of different network-based attacks and guiding me by guiding me through the brute force attack and reviewing my coursework at various stages. I would also like to thank my parents for their encouragement and support towards me. Also, I would also like to thank my friends for their assistance in completing this coursework

Abstract

The primary goal of this course is to undertake an attack on a vulnerable system and then offer a research-based analysis, evaluation and mitigation measures for the attack. An thorough investigation on the topic Brute Force attack on Information Technology devices and systems is undertaken through many studies, journals, articles and websites to get fundamental understanding on the topic.

The attack on Metasploitable was carried out utilizing the Kali operating system, which is a vulnerable operating system. This attack was conducted in compliance with ethical principles. The precautions or mitigation methods outlined in the following sections of the documentation have been tested and implemented on the system.

Overall, this report includes an introduction section on cyber attacks, a background section on the topic, a demonstration section that includes the steps of the attack, a mitigation section that includes the topic's preventive measures, an evaluation section that includes pros, cons, and cost benefit analysis and finally the report's conclusion.

Table of Contents

List of Figures

1. Introduction

Over the last few decades, the term "internet" has expanded dramatically from a modest networking medium to a global network with more than two billion users. It has become a vital part of many people's daily lives all across the world, changing the way we live, talk, and work, from our personal ties to our job routines. Though the internet has provided us with various advantages and opportunities, it has also increased the level of risks and risk to mankind, as the number of malwares, hackers, and other undesired malicious activities continues to rise on a daily basis.

Cyber attacks and other illegal activities on the internet are the biggest potential drawbacks or the dark side of the internet. Spam, computer viruses and worms, hacking, denial-of-service attacks, online scams, identity theft, violations of digital property rights and privacy, online bullying, and other unethical online behaviours are only a few examples (Kim, et al., 2011).

Connecting our devices to the internet has numerous advantages, but it also exposes them to cyber-attacks such as SQL injection, phishing, and stealing, man-in-the-middle, drive-by assault, cross-site scripting attack, brute force attack and multiple web-based attacks. These attacks have a wide range of consequences, from discomfort to posing a significant threat to the country or any individual. As a result, the security of information technology is a critical issue (faq-ans, 2021).

The classification of the different types of cyber attacks are demonstrated on the diagram below,

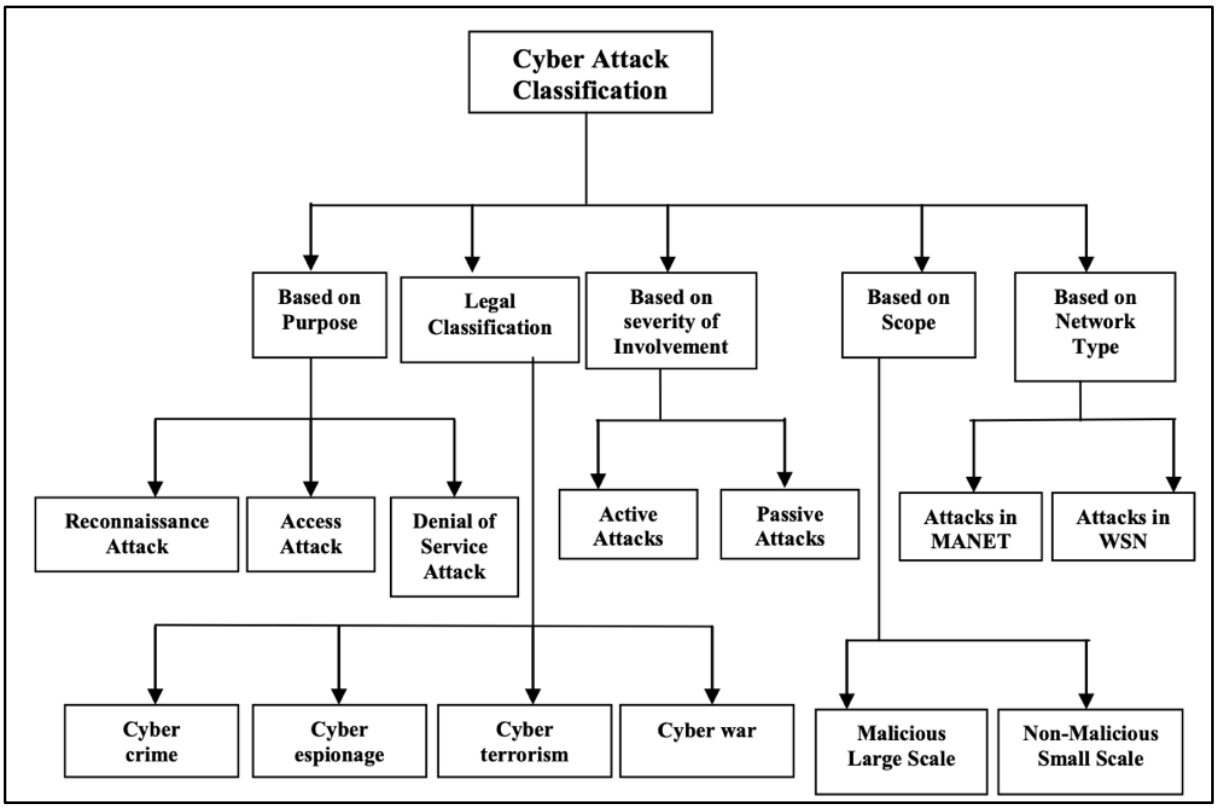

Figure 1: Classification of Cyber Attack (M. Uma, 2011).

1.1 Current Scenario

According to a recent survey done by a group of statisticians, there were 4.66 billion active internet users globally in January 2021, accounting for 59.5 percent of the global population. 92.6 percent (4.32 billion) of this total used mobile devices to access the internet (Johnson, 2021).

It is difficult to imagine a future without the internet, which connects billions of people around the world and serves as a central foundation of the modern information society. The global internet penetration rate is 59%, with Northern Europe leading the way with a population internet penetration rate of 95%. The UAE, Denmark, and South Korea have the highest internet penetration rates in the world (Johnson, 2021).

Asia had the most online users in 2019, with over 2.3 billion according to the most recent count. With about 728 million internet users, Europe came in second. In terms of internet users, China, India, and the United States lead all other countries. China has about 854 million internet users, whereas India has around 560 million. Large swaths of the populace in both countries remain unconnected (Johnson, 2021).

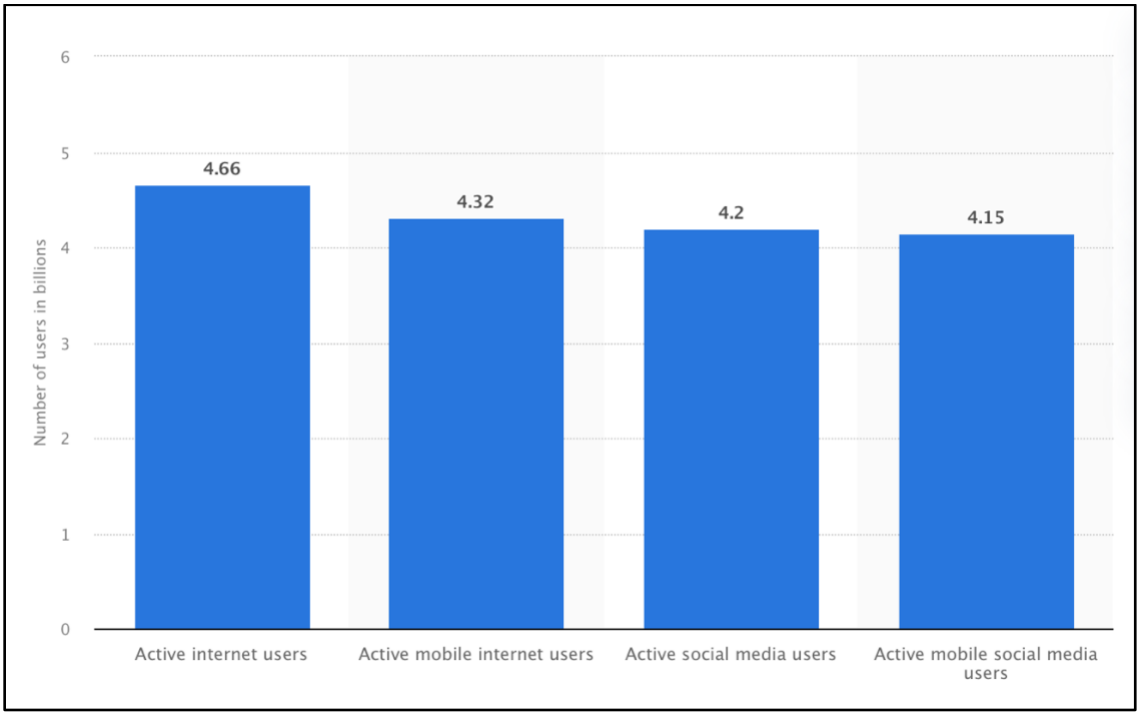

Figure 2: Worldwide digital population as of January 2021 (Statista, 2021).

Because the growth and use of the internet has expanded in the current world scenario, it has also resulted in one of many cybercrimes. The global pandemic COVID-19 has driven enterprises to work remotely, requiring employees to utilize more IoT devices, which has resulted in an increase in data hacking and breaches due to poor security protocols.

In the current scenario, as cyber attacks have increased, cyber security concerns in IoT devices, mobile phones, and the workplace have risen considerably, resulting in a surge in data hacking and breaches. According to the survey, 95 percent of cyber attacks are caused by human error, and there have been a total of 11,762 data breaches between January 1st, 2015 and May 31st, 2020, with 45 percent involving hacking, 17 percent involving malware, 22 percent involving phishing, and the remaining 16 percent involving other types of network-based attacks. (Sobers, 2021).

When it comes to the statistics of various sorts of network-based attacks, Google has detected roughly 600-800 malware-affected sites per week, causing the largest financial damages to enterprises. Similarly, ransomware was responsible for 25% of data breaches that cost roughly $20 billion in 2021. Google has also spotted around $2 million phishing sites in 2020 and it has also revealed that 5% of emails on the internet are phishing. By 2022, the number of DDoS attacks is estimated to reach $14.5 million (Parachute, 2022).

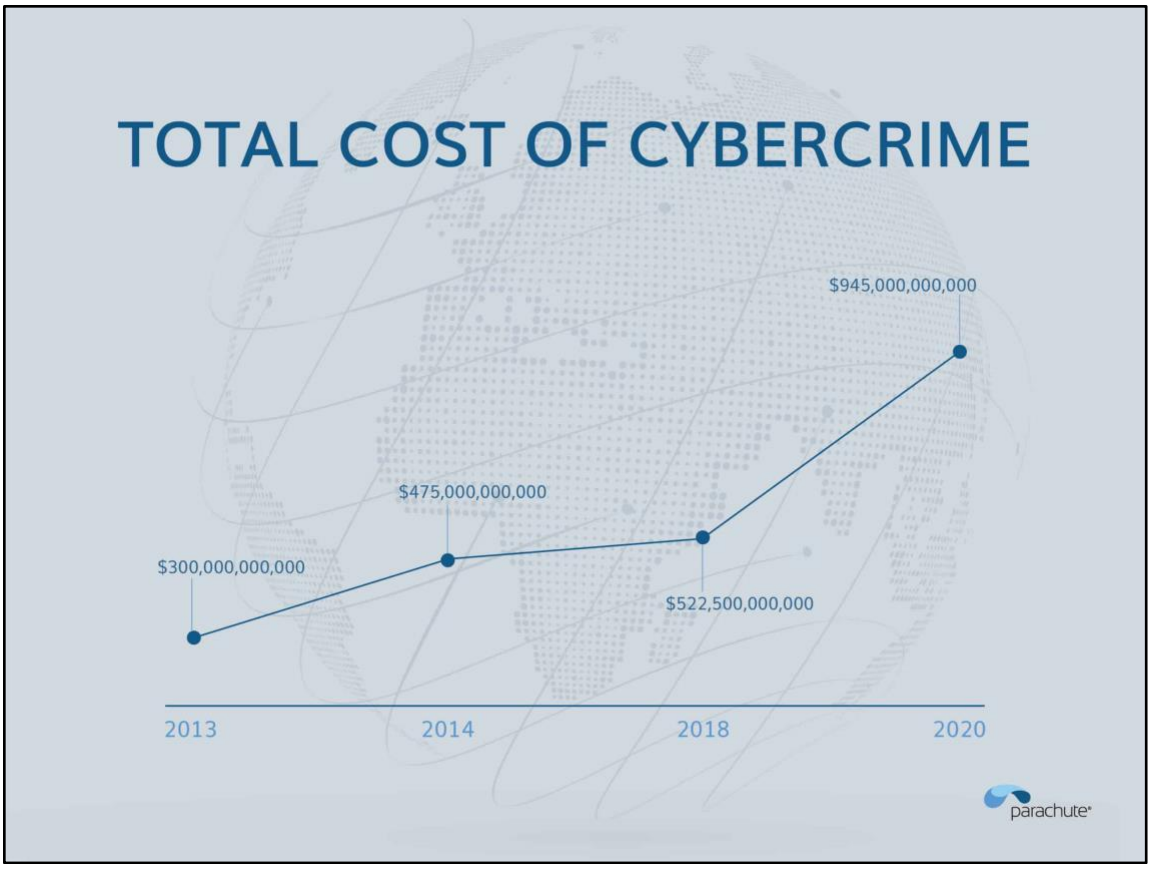

Figure 3: Graph of Total cost of Cybercrime (Parachute, 2022).

Over the last few years, the global cost of cybercrime has risen over $1 trillion, which is 50% higher than the estimate for 2018 and more than 1% of global GDP. The average cost of a data breach for organizations that have completely implemented security automation was $2.45 million, compared to $6.03 million for those that lag behind in security automation. Organizations that use successful cyber attack prevention strategies can save up to $1.4 million each avoided attack (Parachute, 2022).

Using a few historical examples of network-based attacks, In 2020, a Twitter breach that targeted 130 accounts, including those of former presidents and Elon Musk, resulted in attackers stealing $121,000 in Bitcoin in roughly 300 transactions. In the same year, Marriott announced a security compromise that affected the data of over 5.2 million hotel guests. The Equifax breach affected 147.9 million consumers in 2017, costing the firm over $4 billion in total (Sobers, 2021). Similarly, throughout these few years many organizations had been victim of different kinds of network based attacks.

1.2 Problem Statement

Hackers or intruders can easily compromise computer and networking devices such as IoT devices, webservers, firewalls, IDS/IPS, routers and switches by conducting a brute-force attack. Since anyone is permitted to attempt SSH access on the remote web server or any type of networking device, there are various vulnerabilities in SSH auxiliary. Because these services continue to function, the associated port stays open, allowing hackers or attackers to undertake brute force assaults.

By completing this project, we will have a comprehensive understanding of network-based attacks as well as the issue of Brute Force attacks on information technology devices and systems. Also, by launching a brute force attack on the shh auxiliary, we may gain an awareness of all of its faults and provide preventive measures.

1.3 Aims and Objectives

The main aim of this coursework is to provide relevant and in-depth knowledge about Brute Force attacks on information technology and systems by conducting a Brute Force attack over SSH from Kali Linux as an attacker pc to Metaspoitable2 as the victim pc. Finally, after the attack has been successfully carried out, the various possible vulnerabilities need to be demonstrated, as well as their mitigation.

To fulfill this aim the following objectives are required:

- To conduct research on the topic of Brute Force attacks on Information Technology devices and systems.
- To gain the fundamental knowledge about the topic through using a variety of related news, journals, papers and websites.
- To study the common vulnerabilities in the Metaspoitable2 system, which represents any other vulnerable system.
- To perform vulnerability scanning and port scanning of the target using Nmap.
- To conduct a Brute Force attack in ethical norms from Kali Linux OS to Metaspoitable2.
- To provide an overall analysis beginning with an attack, stating vulnerabilities, implementing mitigations and finally presenting an evaluation.

2. Background

2.1 Introduction to Brute Force attack

The term Brute Force attack is a type of network based attack in which an intruder tries to guess a username and password combination by a trial-and-error method used by application programs to decode login information and encryption keys in order to gain unauthorized access to a system or data (Hanna, 2022). This is a type of attack that cannot be avoided because there is no way to safeguard the system from a brute force attack.

On a trial-and-error basis, a brute force assault tries a large number of key combinations. It attempts every possible combination to obtain the required information. If the password length is very short, it can be readily cracked. When the key size is huge and the password is strong, a brute force assault takes a long time. A computer program or ready-made software is frequently used to carry out a brute force attack (Mahore & Deorankar, 2017).

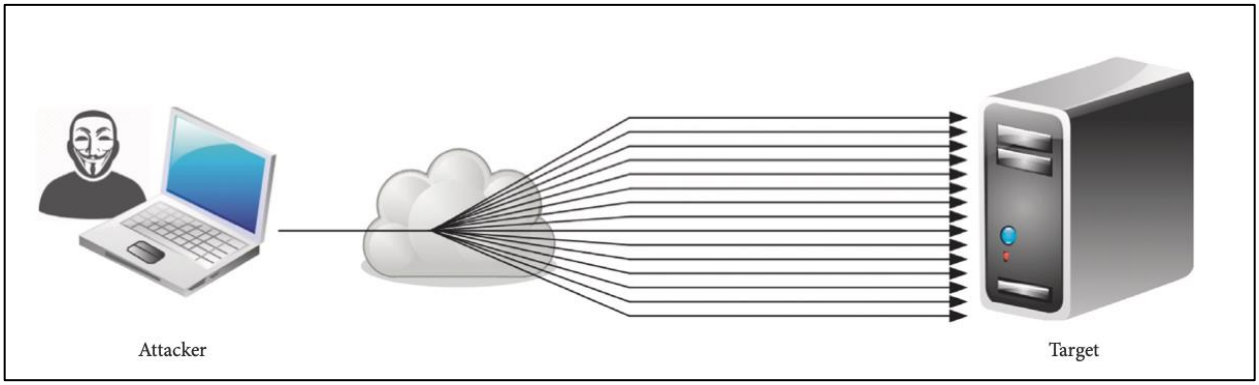

Figure 4: Demonstration of Brute force attack (Stiawan, et al., 2019).

2.2 Classification of Brute Force attack

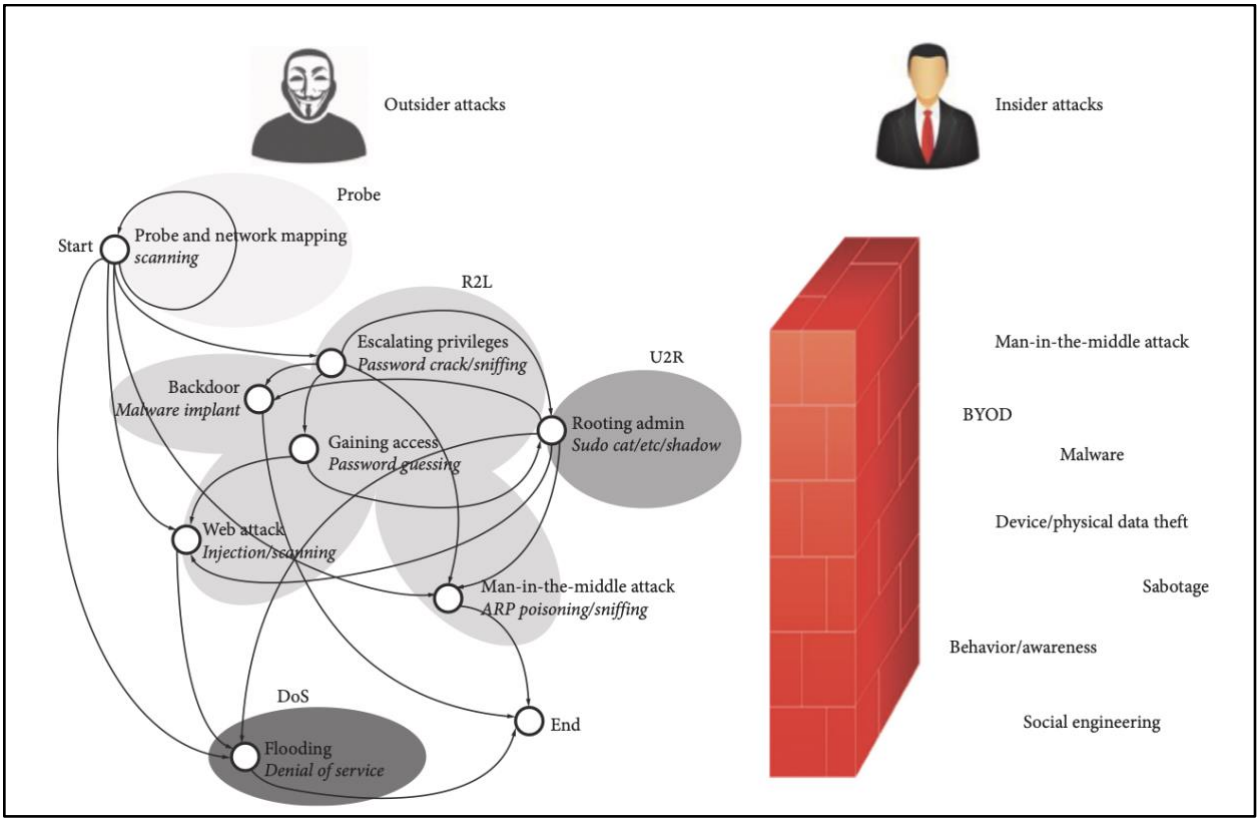

Figure 5: Illustration of Brute Force Attack (Stiawan, et al., 2019).

In general, Brute Force Attacks are classified as either insiders or outsiders where insider attack is usually perceived as a valid user of the organization. According to the researchers, the brute force attack can be classified as either online password hacking or offline password hacking and it can have significant consequences by implying valid passwords on the server (Stiawan, et al., 2019).

The insider attack restricts access to some services that do not have additional coverings on distinct service packages and it also differs from inbound packages from outside the network that are closely inspected by filters with several DMZ services. An insider attack on IoT comes in many different forms and causes a variety of issues connected to purposeful and unintentional security incidents caused by workers and outsources. Because the attacker is inside, they are intimately familiar with technical issues such as the network's backbone, IP address allocations, the virtual local area network (VLAN), the service clustering application and mainly the IT staff members who monitor the network (Stiawan, et al., 2019).

2.3 Pattern of Brute Force attack

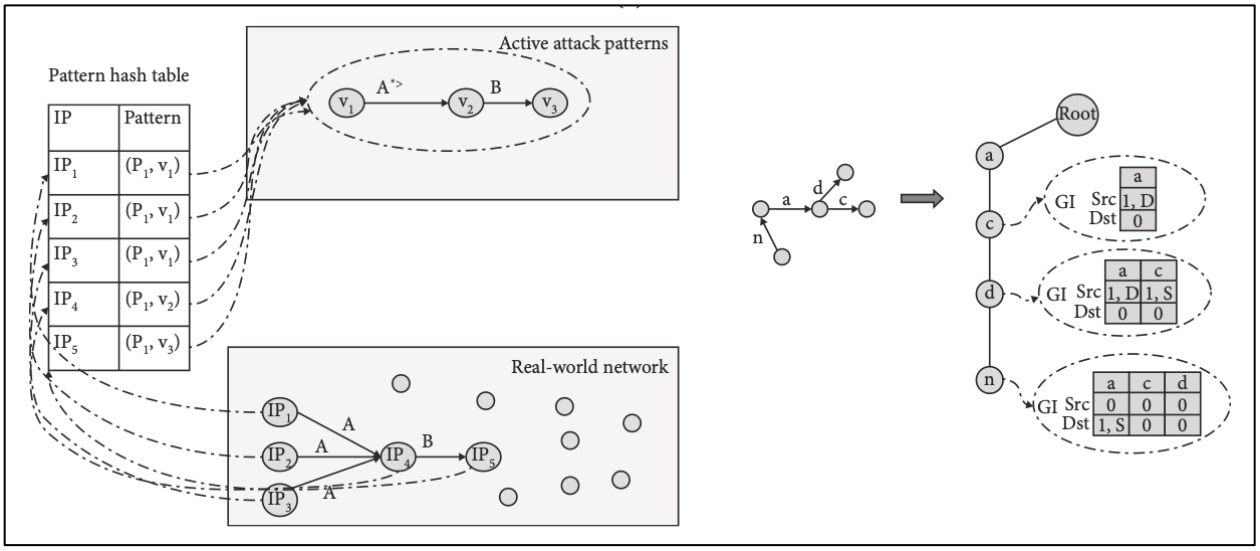

Figure 6: Pattern of attacks based upon the correlation approach (Stiawan, et al., 2019).

The picture above represents brute force attack methodologies and methods, as well as patterns that represent brute force attacks. Some attack patterns were generated using graphinfo's time-sensitive approach to statistical relationships and other patterns were generated using a data set that demonstrated distribution values for the generated patterns, which were an outcome of the attacks stimulated that aligned with the results from the extracted data package (Stiawan, et al., 2019).

The brute force attacks are classified into several different types which includes traditional brute force attacks in which an attacker tries every possible combination of username and password, reverse brute force attacks in which a small number of common passwords are repeatedly tried against many different accounts, credential stuffing attacks in which an attack attempts to use stolen usernames and passwords from sites or services to hijack accounts on other services and applications (Swinhoe, 2020).

Dictionary attacks and Rainbow table attacks are two types of brute force attacks. A dictionary attack cycles over terms in a dictionary or popular passwords from past data breaches. Rainbow table attacks are carried out by employing a pre-computed dictionary containing plaintext passwords and their matching hash values, with the attacker determining passwords by reversing the hashing function (Swinhoe, 2020).

2.4 Motive behind Brute Force attack

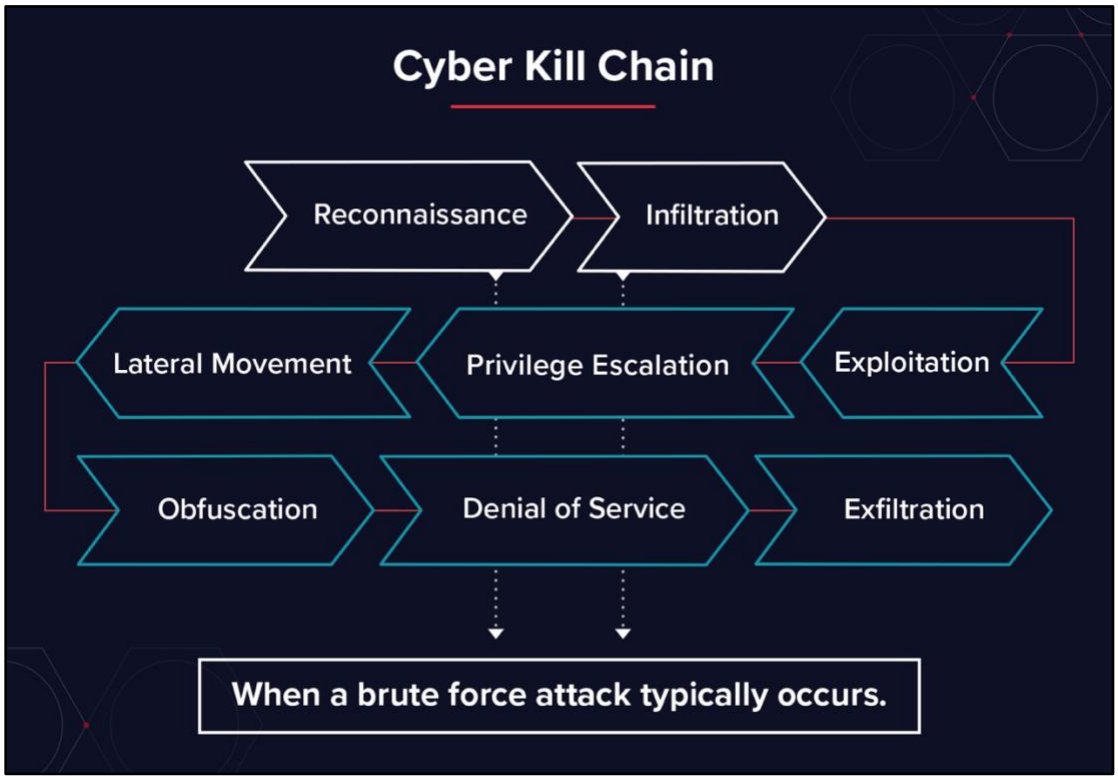

Figure 7: Motive behind brute force attack (Petters, 2021).

Brute force attacks often occur during the investigation and penetration stages of the cyber death chain. Attackers require access or entry points into their targets and brute force approaches are a "set it and forget it" method of acquiring that access. Once within the network, attackers can employ brute force techniques to increase their privileges or carry out encryption downgrade operations (Petters, 2021).

While talking about the different protocols such as FTP, SSH, SMB, telnet, MySQL, Microsoft SQL, SMTP and VNC, we have used SSH protocol to conduct the following brute force attack. Similarly, globally attackers has carried out an SSH brute force attack several time in past few years because it provides shell account access across the network.

2.5 SSH Brute Force attack

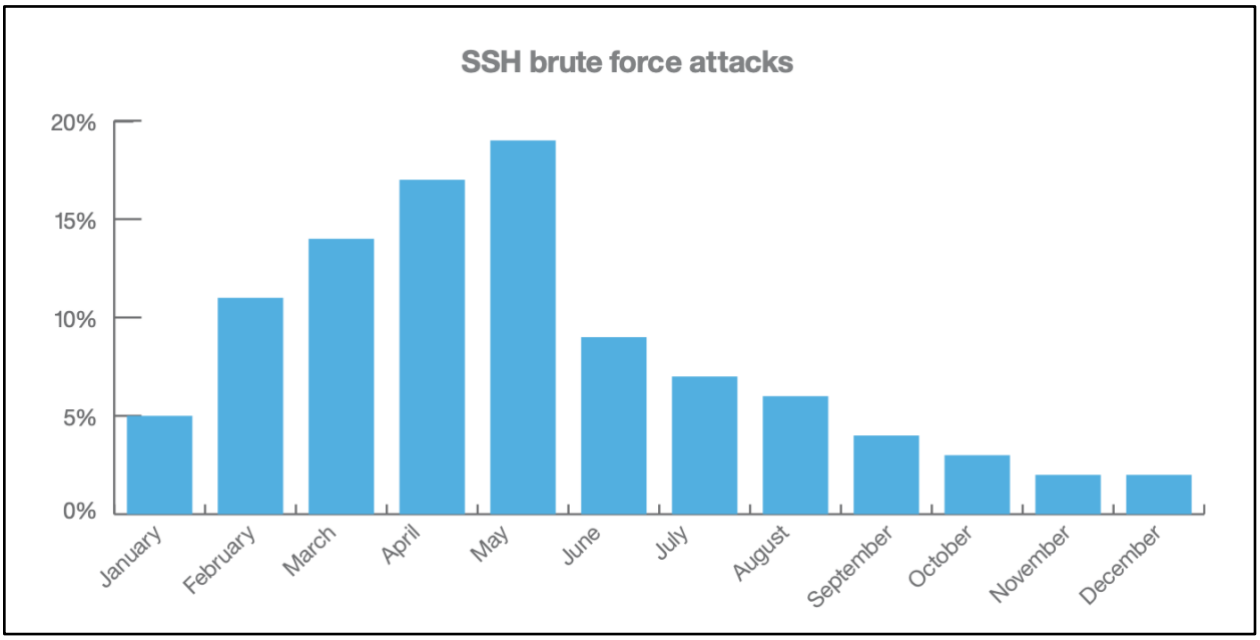

Figure 8: Percentage of SSH brute force attacks for each month in 2015 (Craig, 2016).

From the above stats we can observe that the SSH brute force attack mainly peaked in May of 2015 and drastically decreased for the rest of the year. The malware known as SSH Psychos was most likely responsible for much of the early-year activity and the declining trend in later months reflected attempts by members of the security community to neutralize this danger. In May, the number of distinct attacker IP addresses associated with SSH brute force attacks reached an all-time high. The key message is that SSH brute force attacks aren't restricted to a small group of attackers and securing the systems from them is much important (Craig, 2016).

2.7 Protocols

The brute force uses several kinds of protocols in order to carry out the attack successfully, few of them are:

2.7.1 SSH

The Secure Shell (SSH) Protocol is a network security protocol that allows for secure remote login and other secure network services to be provided across an insecure network. It allows for secure remote system administration as well as file transmission over unsecured network. It is presently utilized in practically all data centers. To provide a secure channel over an unsafe network, Secure Shell employs a client-server architecture (Stackscale, 2021).

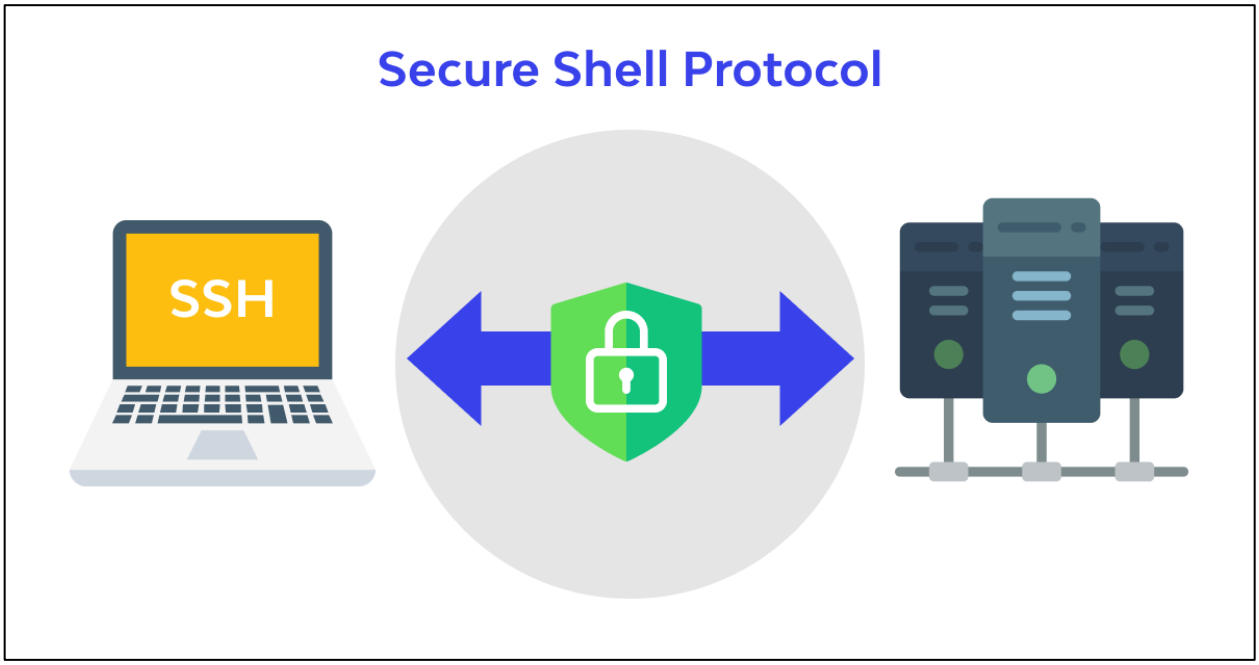

Figure 9: How SSH protocol works (wallaram, 2022).

2.7.2 TCP

The Transfer Control Protocol (TCP) is a transport protocol that is used on top of the Internet Protocol (IP) to ensure reliable packet transmission. TCP includes means for dealing with many of the issues associated with packet-based messaging, such as missing packets, out-of-order packets, duplicate transmissions and malformed packets. Because TCP is the most commonly used protocol on top of IP, the Internet protocol stack is also known as TCP/IP (Khan Academy, 2022).

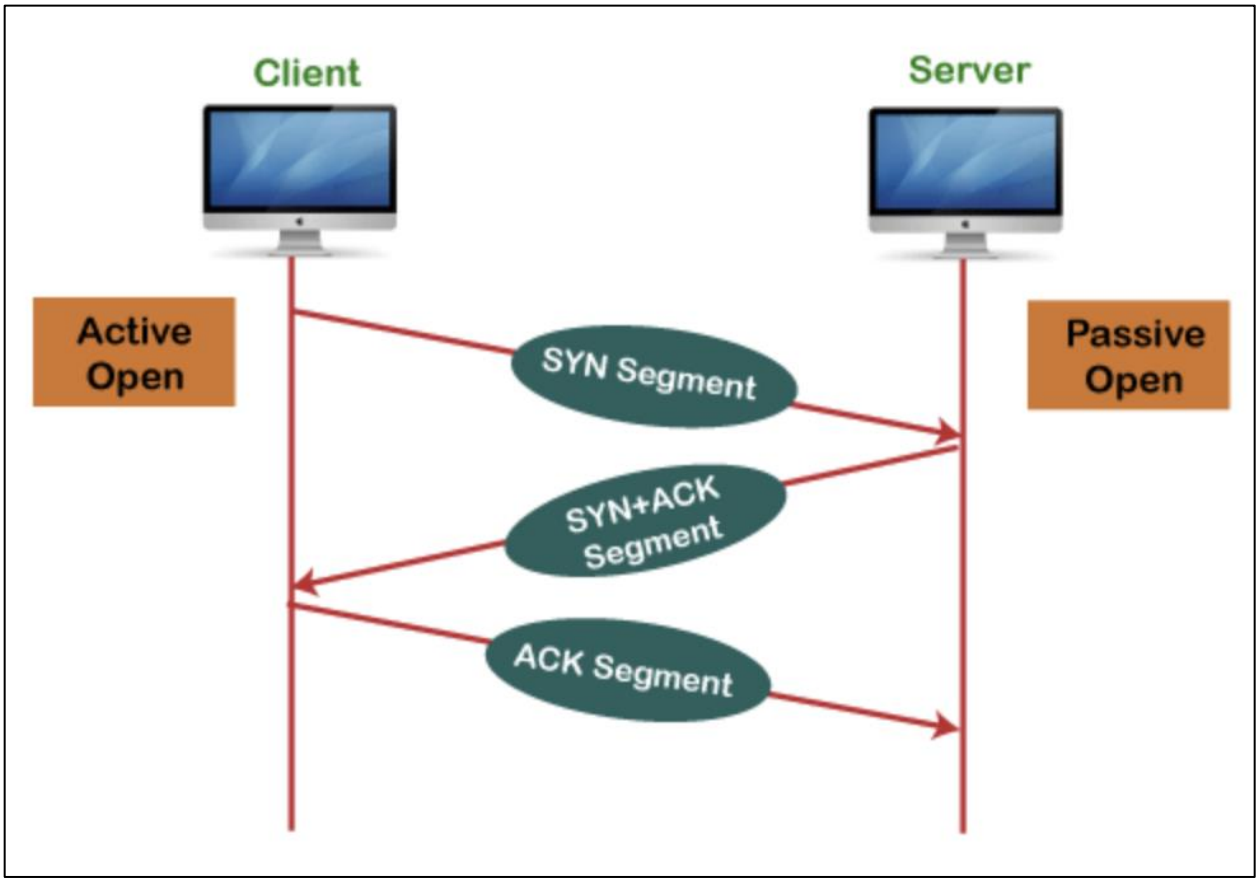

Figure 10: How TCP protocol works (javapoint, 2022).

2.7.3 Telnet

Telnet is a protocol that provides a command line interface for communicating with a distant device or server. It is sometimes used for remote management, but it is also used for initial device setup, such as network hardware. Telnet can be used to test or debug remote web or mail servers, as well as access MUDs (multi-user dungeon games) and trusted internal networks (ExtraHop, 2022).

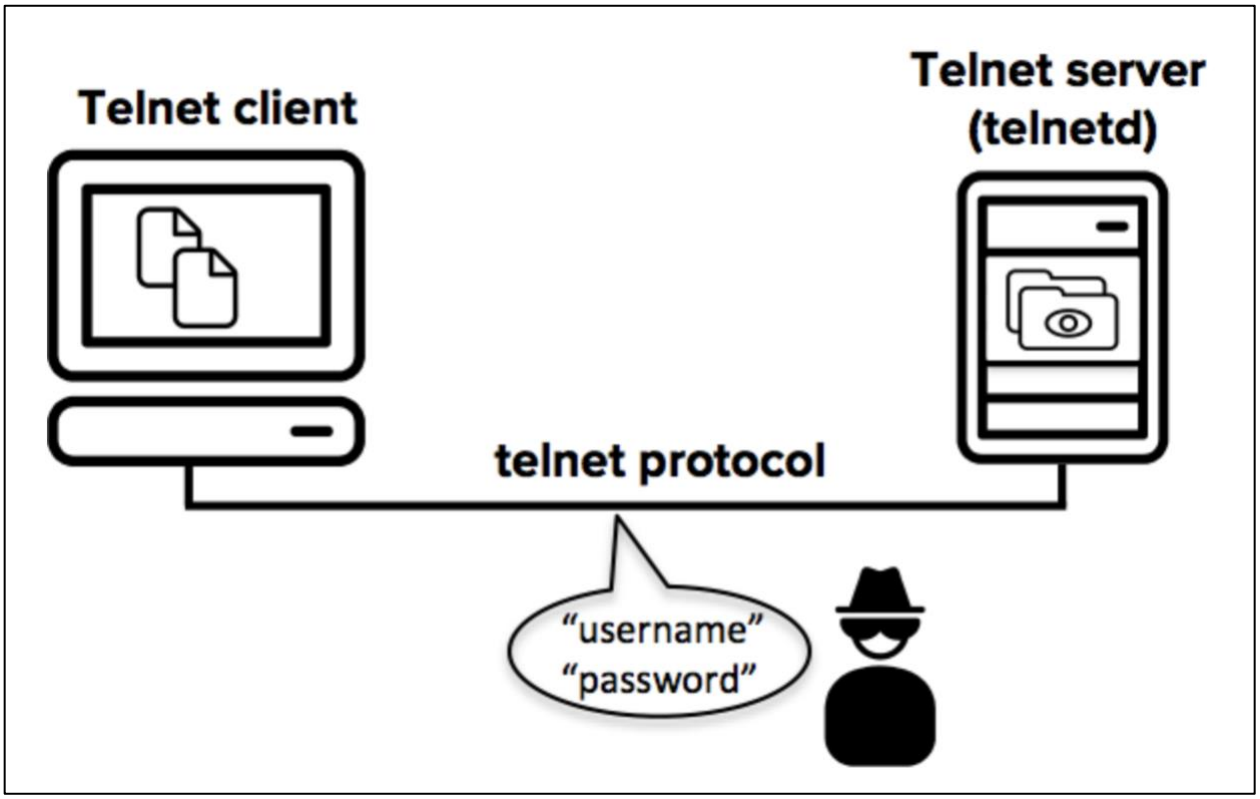

Figure 11: How telnet protocol works (SSH, 2022).

2.8 Methodology

First, a network architecture for the attack was developed using Cisco packet tracer, which comprises of a core router, core switch, Kali Linux as the attacker PC and Metaspoitable2 as the victim PC, demonstrating the entire attack scenario. To carry out the attack, Kali Linux and Metaspoitable2 were launched in VMware and their network adapters were adjusted to NAT to let the guest machines to connect to the internet.

The terminals of both were then launched, where the following commands were typed in order to successfully carry out the attack. The IP addresses of both systems were obtained using the 'ifconfig' command and the connection between them was verified using the 'ping' function. Then, in the Kali Linux terminal, the 'nmap' command was used to do port scanning, from which we chose port number 22 'SSH' for the attack.

The 'msfconsole' command was used to launch the Metasploit framework. Then ssh was searched in the auxiliar and it was logged using the auxiliary scanner. The options were then loaded and RHOST was selected. Inside Kali Linux, a 'password.txt' file was created with the gedit command, which has a hundred distinct possible passwords and usernames, including 'msfadmin' which is the actual username and password of metaspoitable2.

The RHOSTS configuration was then set in Kali with Metasploitable's IP address as the victim. The user pass file was configured to point to the newly produced password.txt file. This command was executed and the brute force assault was successful since one of the user password pairs matched 'msfadmin msfadmin'. Following the completion of the auxiliary module execution, a session was formed in order to get access to Metasploitable. Finally, Metasploitable was launched from Kali, and the 'id' command was used to determine user and group names, as well as the 'ls' command to list the vulnerabilities.

2.9 Required Tools

The several required tools which is needed to carry out the brute force attack to gain SSH access are as,

2.8.1 VMware

VMware, founded in 1998 is a virtualization and cloud computing software development company based in Palo Alto, California. VMware's virtualization solutions are based on its bare-metal hypervisor ESX/ESXi in x86 architecture. A hypervisor is installed on the physical server with VMware server virtualization to allow multiple virtual machines (VMs) to run on the same physical server. Each virtual machines can run its own operating system, allowing many operating systems to coexist on a single physical server (Suse-Defines, 2022).

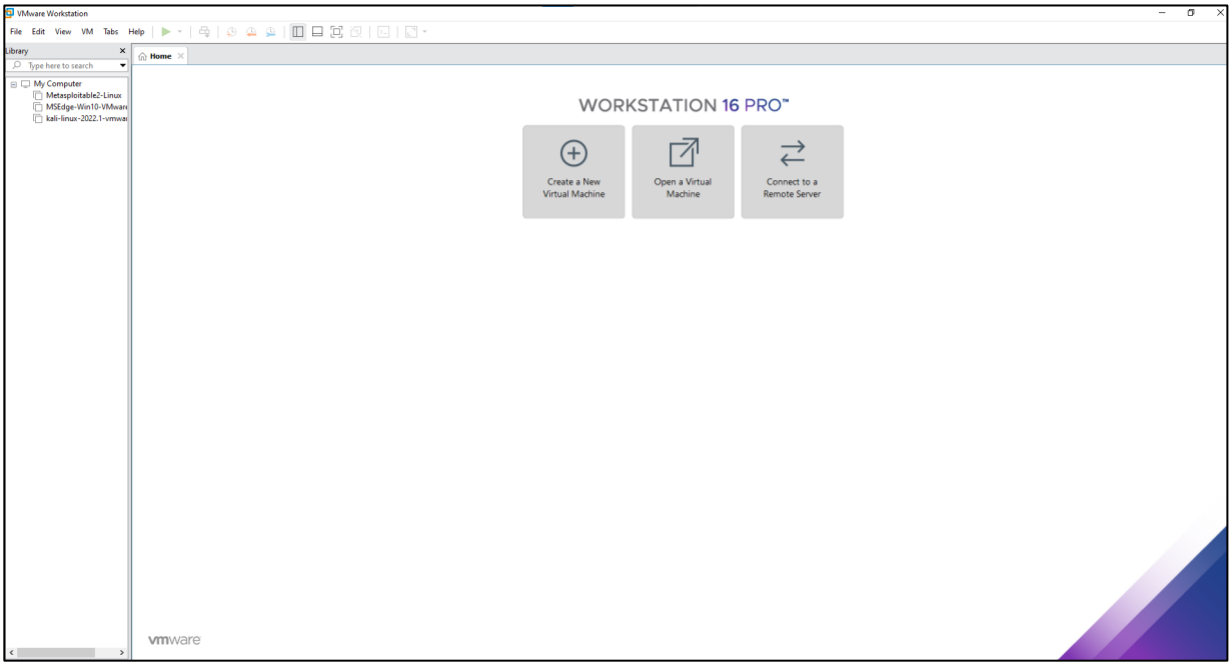

Figure 12: VMware Interface.

2.8.2 Kali Linux

Kali Linux is a Linux security system based on Debian that was created primarily for computer forensics and advanced penetration testing. Kali Linux has hundreds of tools that are well-suited to a variety of information security activities, such as penetration testing, security research, computer forensics and reverse engineering (Williams, 2022).

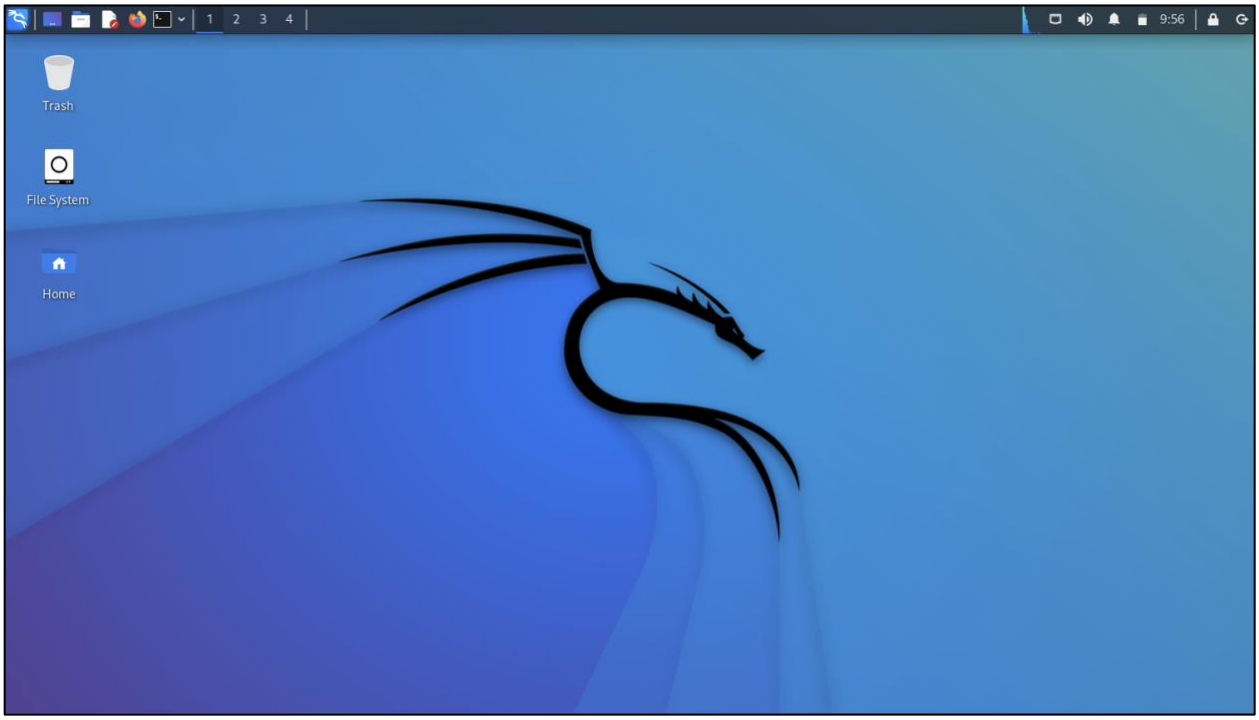

Figure 13: Kali Linux in VMware.

2.8.3 Metaspoitable 2

Metaspoitable 2 is a virtual machine that runs on a VMware image and contains a large number of vulnerabilities. It also provides a secure environment for penetration testing and security research. It was designed to be a vulnerable target for learning about security breaches by conducting Brute force attacks to collect the current passwords in the system (RAPID7, 2012).

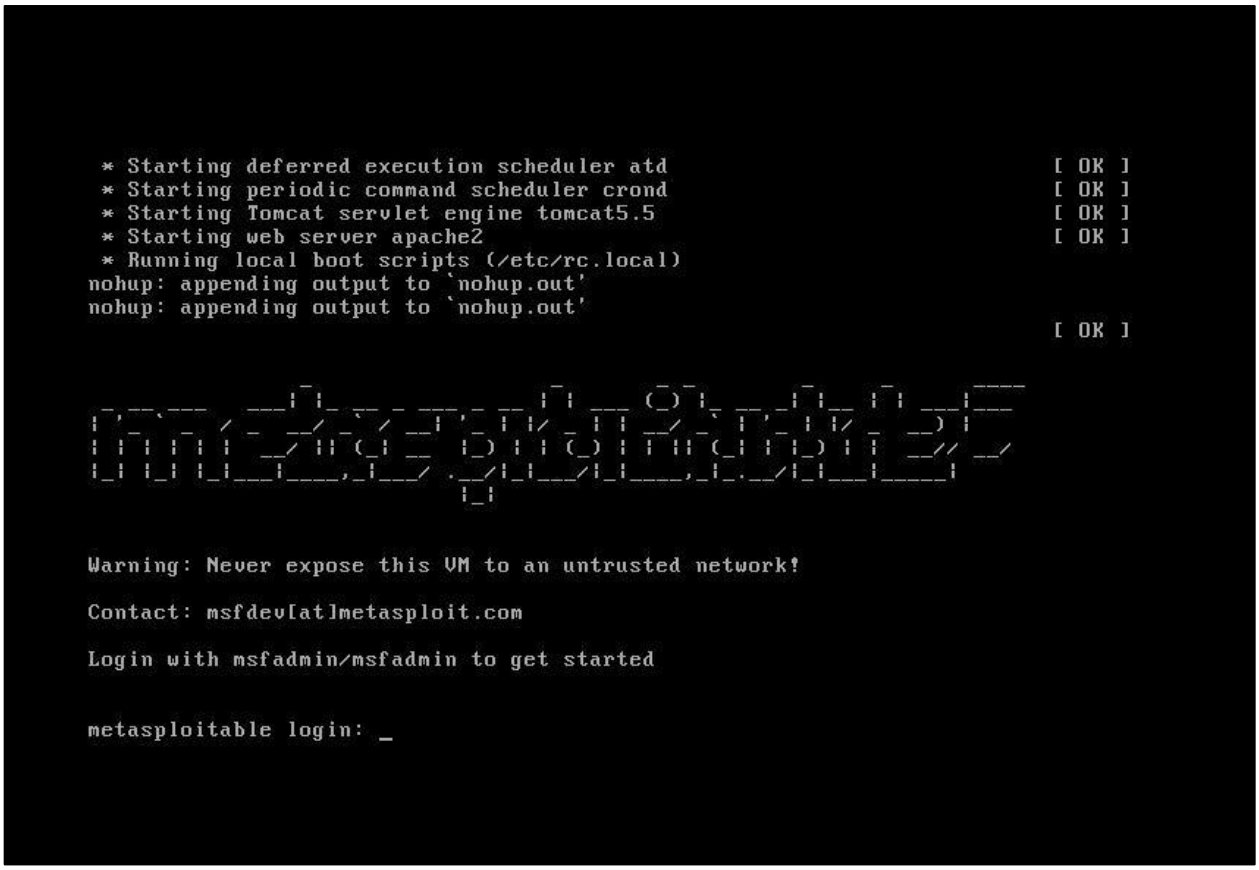

Figure 14: Metaspoitable 2 in VMware.

2.8.4 Nmap

Nmap, which stands for Network Mapper is a free and open-source vulnerability detection and network discovery application. Nmap is used by network administrators to determine what devices are running on their systems, discover available hosts and the services they provide, find open port, and detect security problems. Nmap may be used to monitor individual hosts as well as large networks with hundreds of thousands of devices and subnets (Ferranti, 2018).

```
[mjrod@creoda-fedora ~]$ nmap -p 1-7000
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-06 13:08 EDT
Nmap scan report for
Host is up (0.014s latency).
Not shown: 5969 closed ports, 1020 filtered ports
PORT     STATE SERVICE
1957/tcp open  unix-status
1958/tcp open  dxadmind
5111/tcp open  taep-as-svc
5239/tcp open  unknown
5247/tcp open  capwap-data
5275/tcp open  unknown
5602/tcp open  a1-msc
5613/tcp open  unknown
5662/tcp open  unknown
5665/tcp open  unknown
6379/tcp open  redis

Nmap done: 1 IP address (1 host up) scanned in 3.60 seconds
[mjrod@creoda-fedora ~]$
```

Figure 15: Using Nmap for scanning (mjrod, 2021).

3. Demonstration

The demonstration section contains all of the steps that were taken for the brute force attack, and it is divided into two parts: one for designing a network architecture for the attack and the other for explaining the entire attack.

3.1 Creating a network architecture for the attack

This is the initial step in carrying out the attack, in which a generic network architecture is established using Cisco packet tracer, which will serve as the foundation for the entire attack. A Core Router, a Core Switch, Kali Linux as the attacker PC and Metaspoitable2 as the target PC comprise the topology.

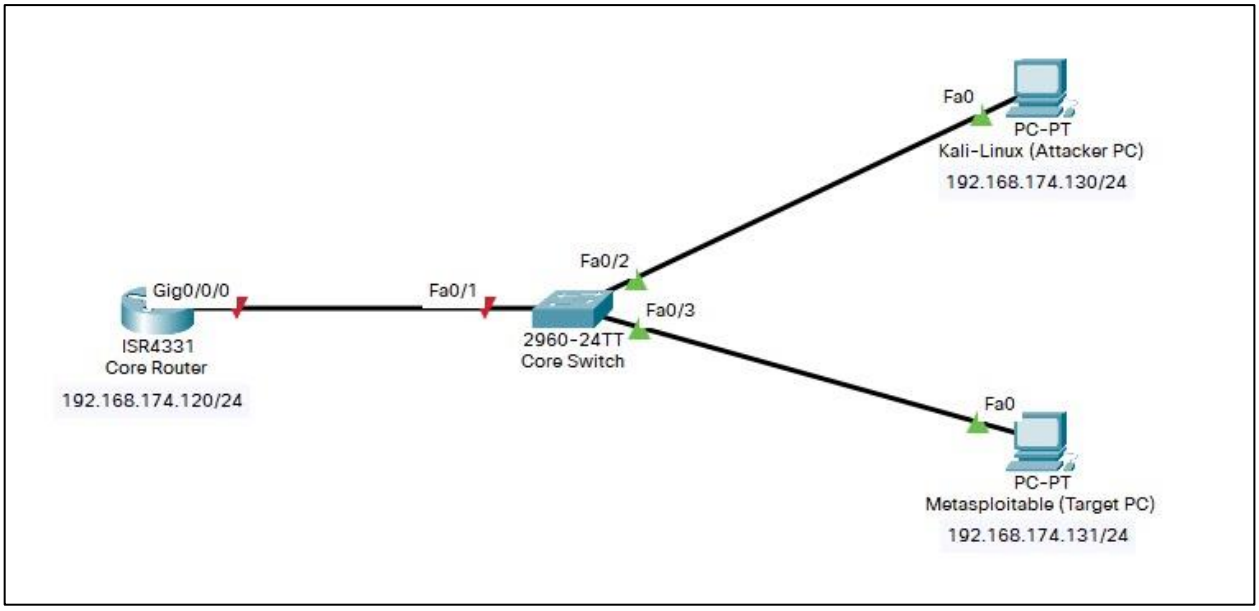

Figure 16: Network Architecture for the attack.

As assigned in the figure above the IP address of the Core Router is 192.168.174.120/24, Kali Linux which the Attacker PC is 192.168.174.130/24 and Metaspoitable2 which is the Target PC is 192.168.174.131/24.

3.2 Steps for demonstration

The steps used to demonstrate the brute force attack are below and each step has been explained.

<u>Step 1:</u> Setting up the network adapter to NAT

Before beginning the attack, the network adapters of both Kali Linux and Metaspoitable2 were set to **"NAT"** in order to allow the guest machines to connect to the internet. It also ensures that the system cannot receive an IP address from the host machine dynamically. As a result, a static IP address must be configured.

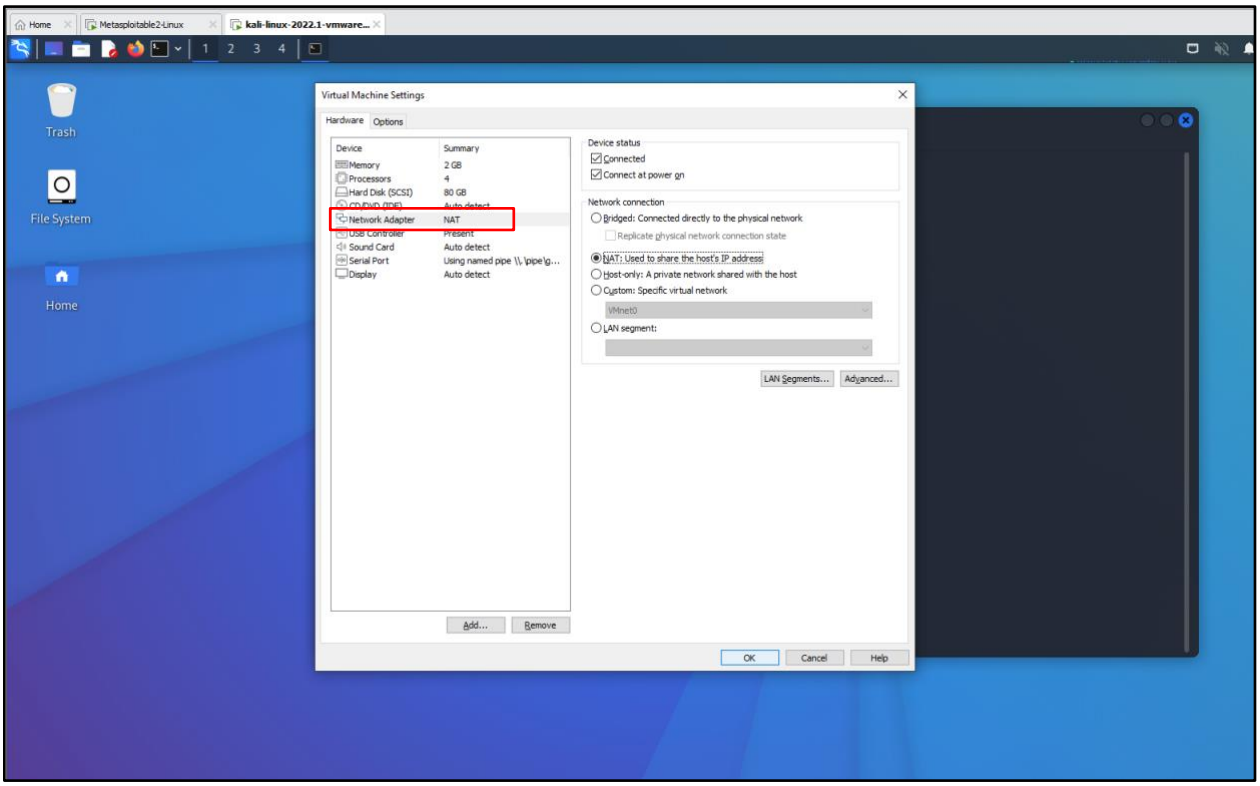

Figure 17: Setting up the network adapter to NAT in Kali Linux.

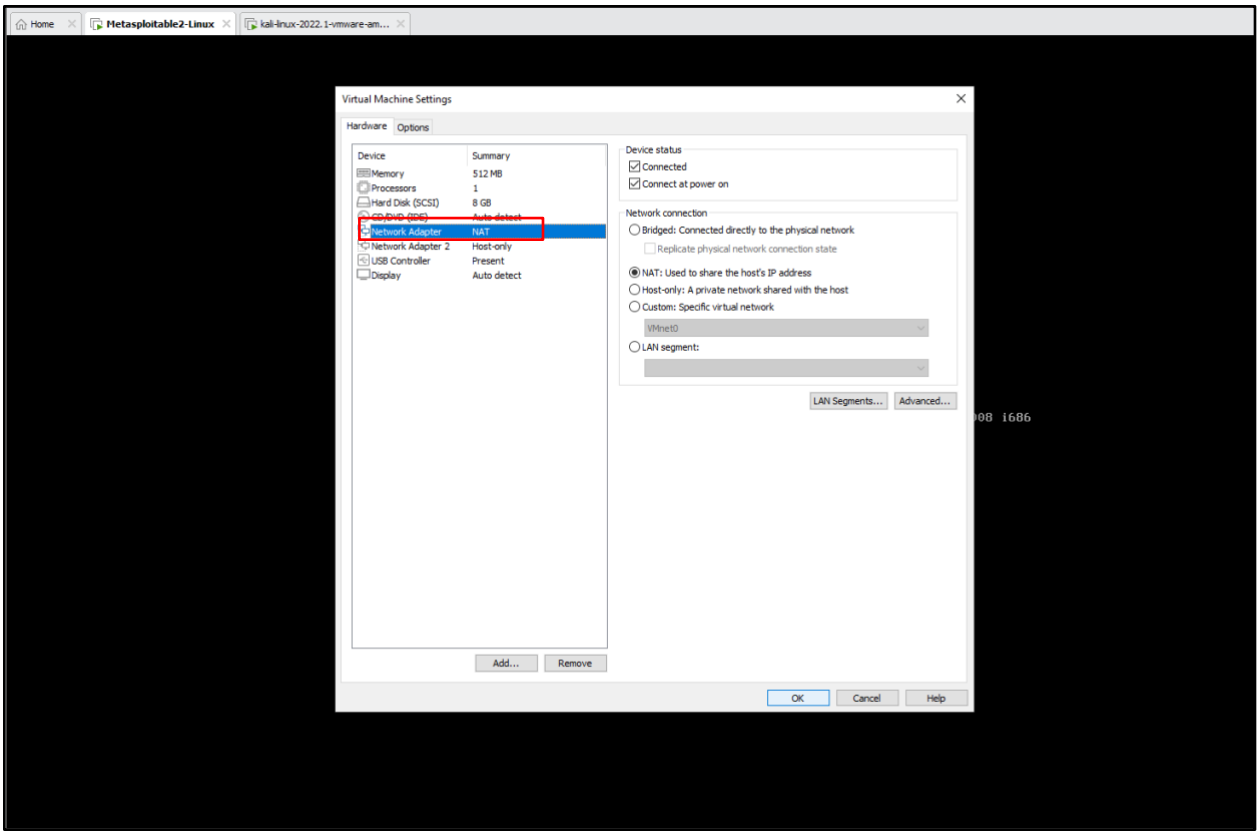

Figure 18: Setting up the network adapter to NAT in Metaspoitable2.

Step 2: Using the ifconfig command to obtain IP address

The terminals of Kali Linux and Metaspoitable2 were launched and the command **"ifconfig"** was run to obtain the IP addresses of the attacker and target computers, respectively which will be used in the further next steps.

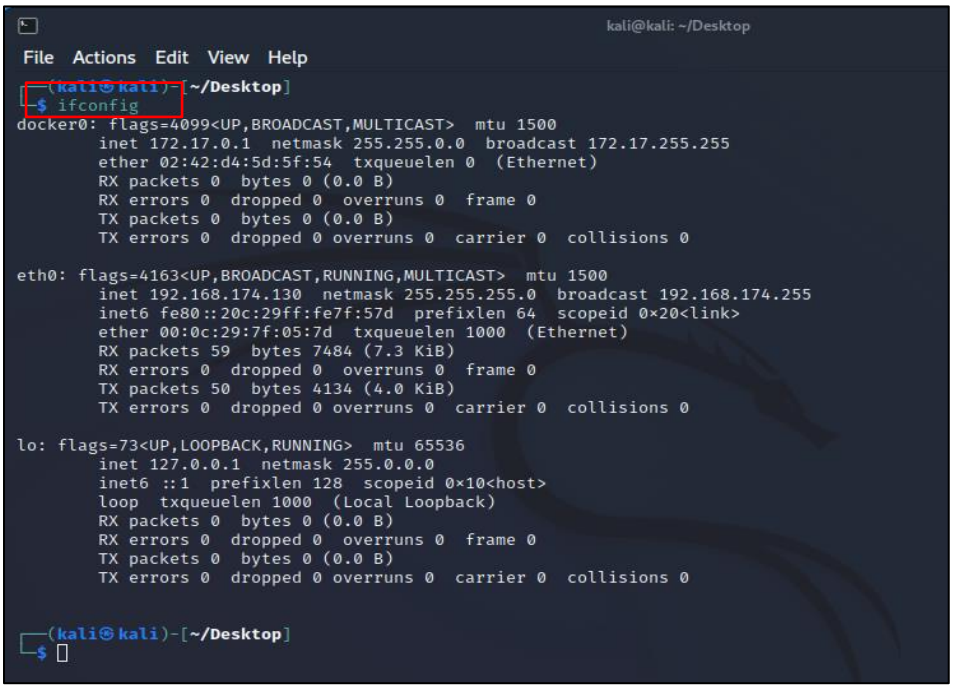

Figure 19: Obtaining the IP address of Kali Linux.

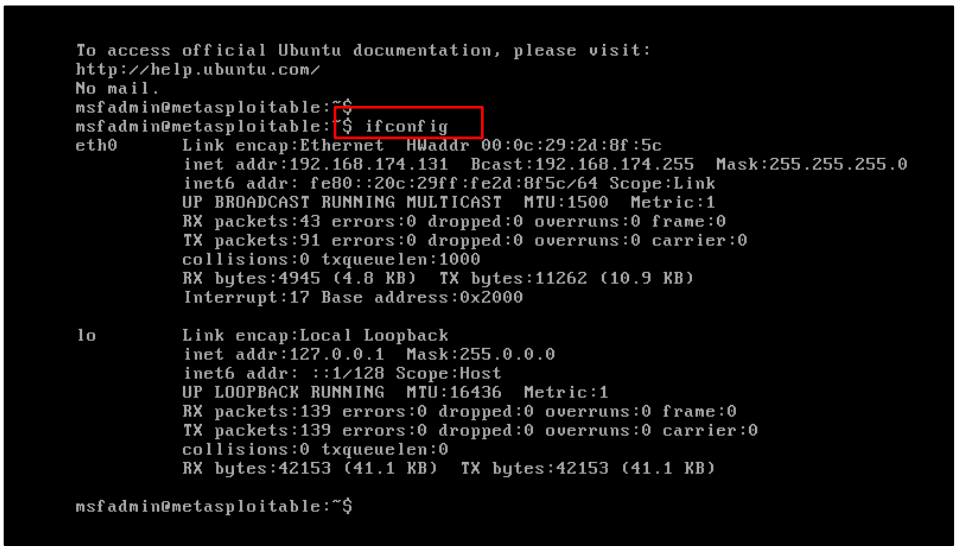

Figure 20: Obtaining the IP address of Metaspoitable2.

Step 3: Using the ping command to establish connection between both PC

Using the IP address obtained in **Step 3**, the connection between the two computers was tested with the **"ping"** command. The corresponding command **"ping 192.168.174.131"** which is the IP address of the Metaspoitable2, is run in the terminal of Kali Linux and the command **"ping 192.168.174.130"** which is the IP address of the Metaspoitable2, is run in the terminal of Metaspoitable2, and the connection is confirmed as successful between both of them.

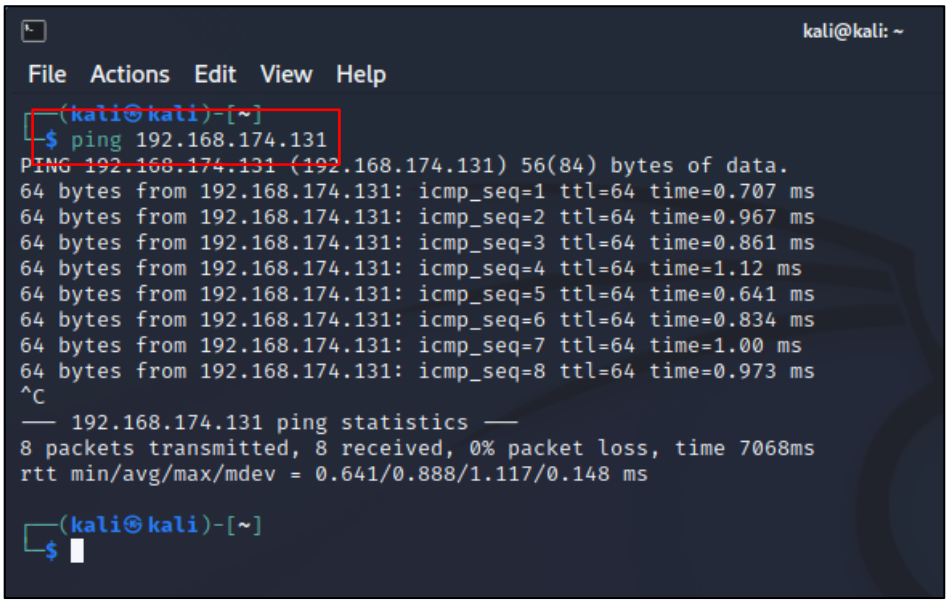

Figure 21: Pinging Metaspoitable2 from Kali Linux.

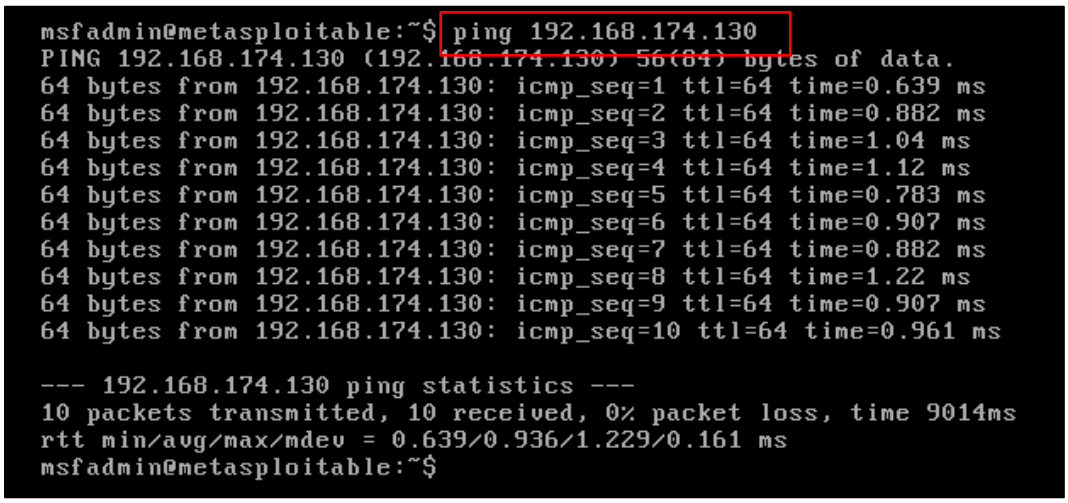

Figure 22: Pinging Kali Linux from Metaspoitable2.

Step 4: Performing port scan on Kali Linux using Nmap

In order to examine the status of the active ports, the following command **"nmap -sV 192.168.174.131"** was used from where the IP address is of Metaspoitable2. When the execution was finished, it displayed a number of open ports, one of which being port 22 for SSH, which was ideal for the brute force attack.

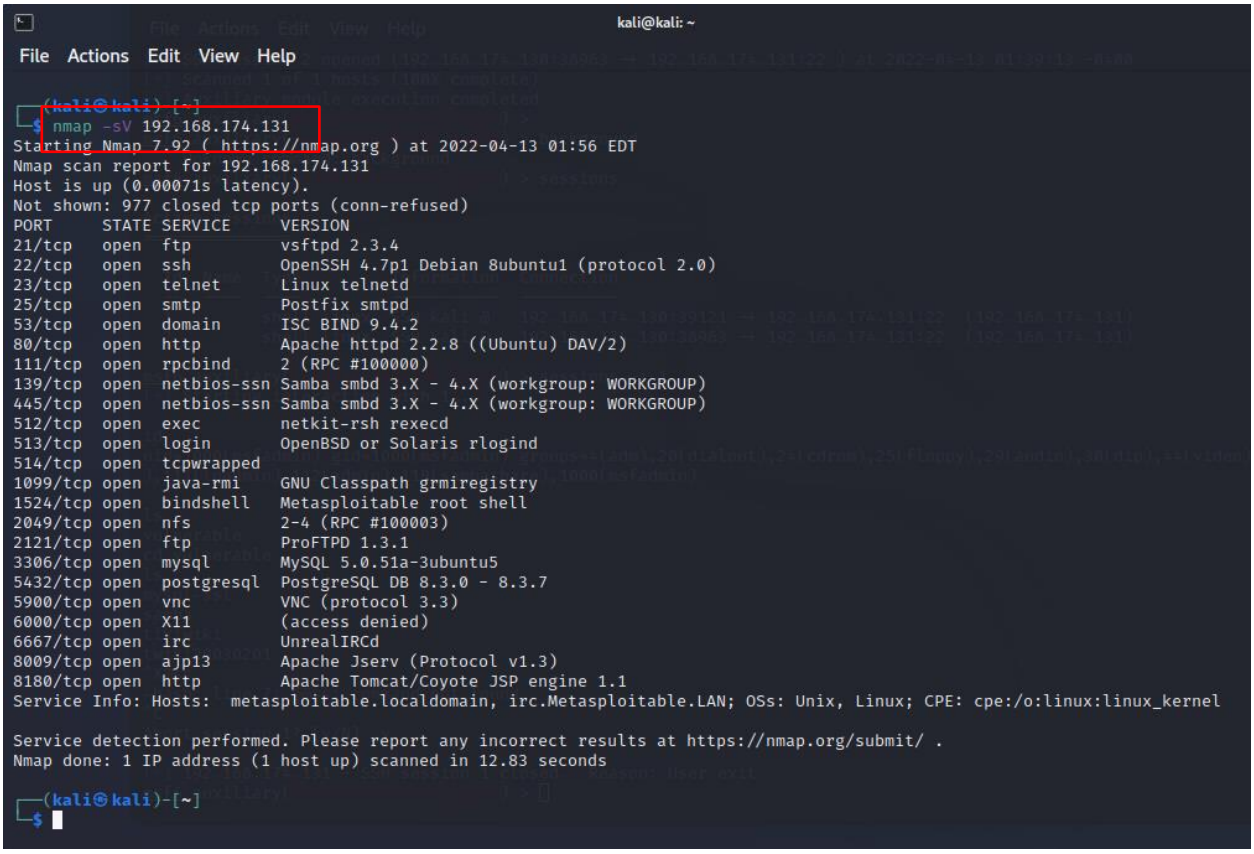

Figure 23: Performing port scanning on Kali Linux using nmap.

Step 5: Starting up the Metasploit framework

To launch the Metasploit framework within Kali Linux, we entered the command **"msfconsole"** in the terminal, which boots up the environment. During the time of execution it also listed out the number of modules that are available in the Metasploit framework such as 2196 exploits, 1162 auxiliary, 400 post, 596 payloads, 45 encoders, 10 nops and 9 evasion. Then it directly redirects to **"msf6"** the most recent version of Metasploitable2, which has the advantage of supplying users with the most recent exploits and tools.

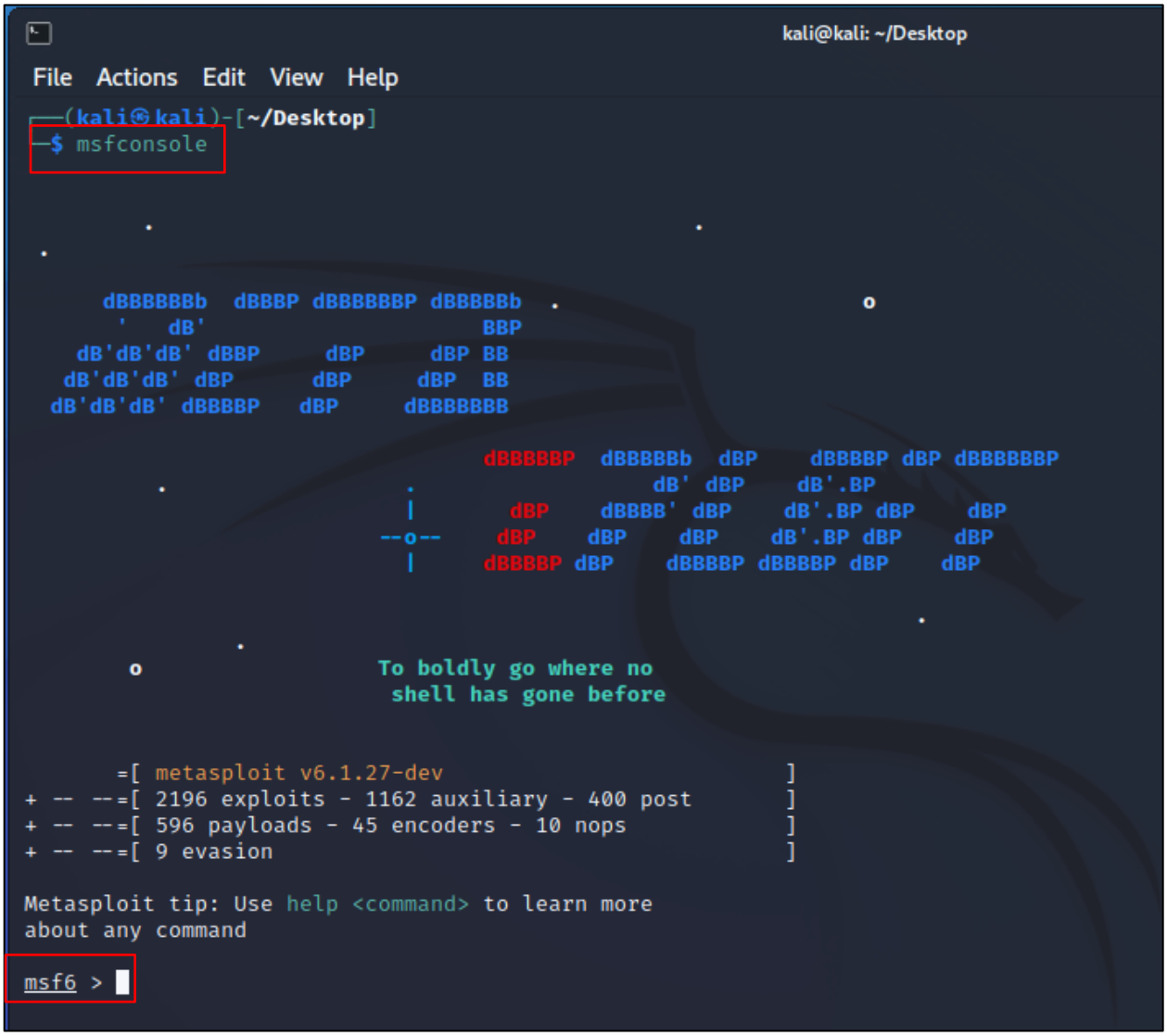

Figure 24: Starting Metasploitable framework console.

Step 6: Searching for SSH auxiliary in the Metasploit Framework

To find out the different possible auxiliaries present in the Metasploit framework **"SSH"** module was used with the following command **"search ssh"** was run which listed 60 different present auxiliaries in the framework. Amongst all we used the auxiliary number 46 which is **"ssh_login"** to carry out the attack.

```
msf6 > search ssh

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                    2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Cod
e Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal     No     Apache Karaf Default Credential
s Command Execution
   2   auxiliary/scanner/ssh/karaf_login                                      normal     No     Apache Karaf Login Utility
   3   exploit/apple_ios/ssh/cydia_default_ssh               2007-07-02       excellent  No     Apple iOS Default SSH Password
Vulnerability
   4   exploit/unix/ssh/arista_tacplus_shell                 2020-02-02       great      Yes    Arista restricted shell escape
(with privesc)
   5   exploit/unix/ssh/array_vxag_vapv_privkey_privesc      2014-02-03       excellent  No     Array Networks vAPV and vxAG Pr
ivate Key Privilege Escalation Code Execution
   6   exploit/linux/ssh/ceragon_fibeair_known_privkey       2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Priva
te Key Exposure
   7   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal     No     Cerberus FTP Server SFTP Userna
me Enumeration
   8   auxiliary/dos/cisco/cisco_7937g_dos                   2020-06-02       normal     No     Cisco 7937G Denial-of-Service A
ttack
   9   auxiliary/admin/http/cisco_7937g_ssh_privesc          2020-06-02       normal     No     Cisco 7937G SSH Privilege Escal
ation
   10  auxiliary/scanner/http/cisco_firepower_login                           normal     No     Cisco Firepower Management Cons
ole 6.0 Login
   40  exploit/linux/ssh/quantum_vmpro_backdoor              2014-03-17       excellent  No     Quantum vmPRO Backdoor Command
   41  auxiliary/fuzzers/ssh/ssh_version_15                                   normal     No     SSH 1.5 Version Fuzzer
   42  auxiliary/fuzzers/ssh/ssh_version_2                                    normal     No     SSH 2.0 Version Fuzzer
   43  auxiliary/fuzzers/ssh/ssh_kexinit_corrupt                              normal     No     SSH Key Exchange Init Corruptio
n
   44  post/linux/manage/sshkey_persistence                                   excellent  No     SSH Key Persistence
   45  post/windows/manage/sshkey_persistence                                 good       No     SSH Key Persistence
   46  auxiliary/scanner/ssh/ssh_login                                        normal     No     SSH Login Check Scanner
   47  auxiliary/scanner/ssh/ssh_identify_pubkeys                             normal     No     SSH Public Key Acceptance Scann
er
   48  auxiliary/scanner/ssh/ssh_login_pubkey                                 normal     No     SSH Public Key Login Scanner
   49  exploit/multi/ssh/sshexec                             1999-01-01       manual     No     SSH User Code Execution
   50  auxiliary/scanner/ssh/ssh_enumusers                                    normal     No     SSH Username Enumeration
   51  auxiliary/fuzzers/ssh/ssh_version_corrupt                              normal     No     SSH Version Corruption
   52  auxiliary/scanner/ssh/ssh_version                                      normal     No     SSH Version Scanner
   53  post/multi/gather/saltstack_salt                                       normal     No     SaltStack Salt Information Gath
erer
```

Figure 25: Searching for different auxiliaries inside the framework.

Step 7: Creating a username and password list for attack

For the next step in the brute force attack, we used the **"gedit"** command to generate a list called **"password.txt"** that had 100 distinct combinations of usernames and passwords in the Kali desktop environment, including Metasploitable2 actual username and password which is **"msfadmin msfadmin"**.

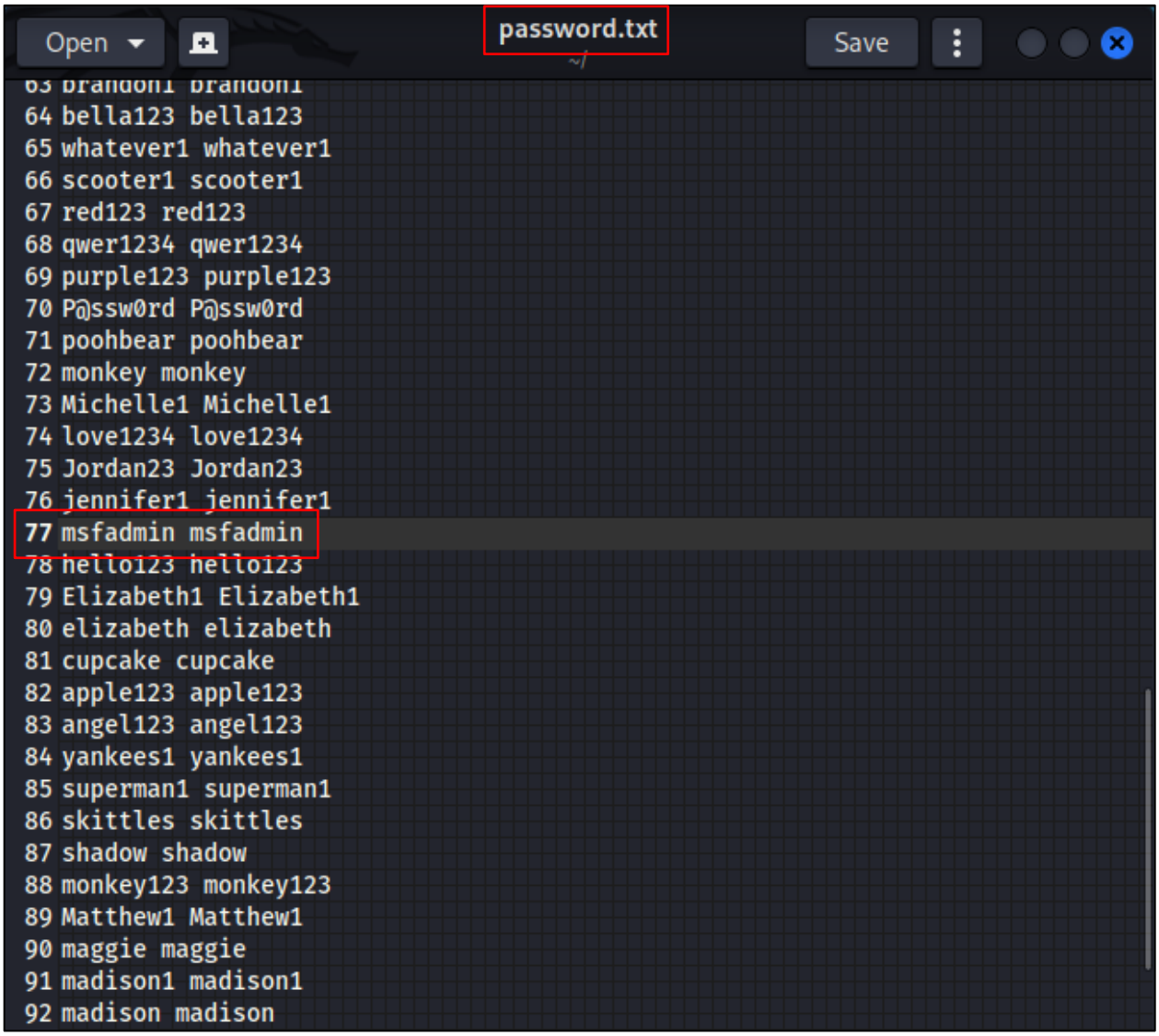

Figure 26: Generating password.txt file.

The following **“password.txt”** file is saved inside the kali desktop environment.

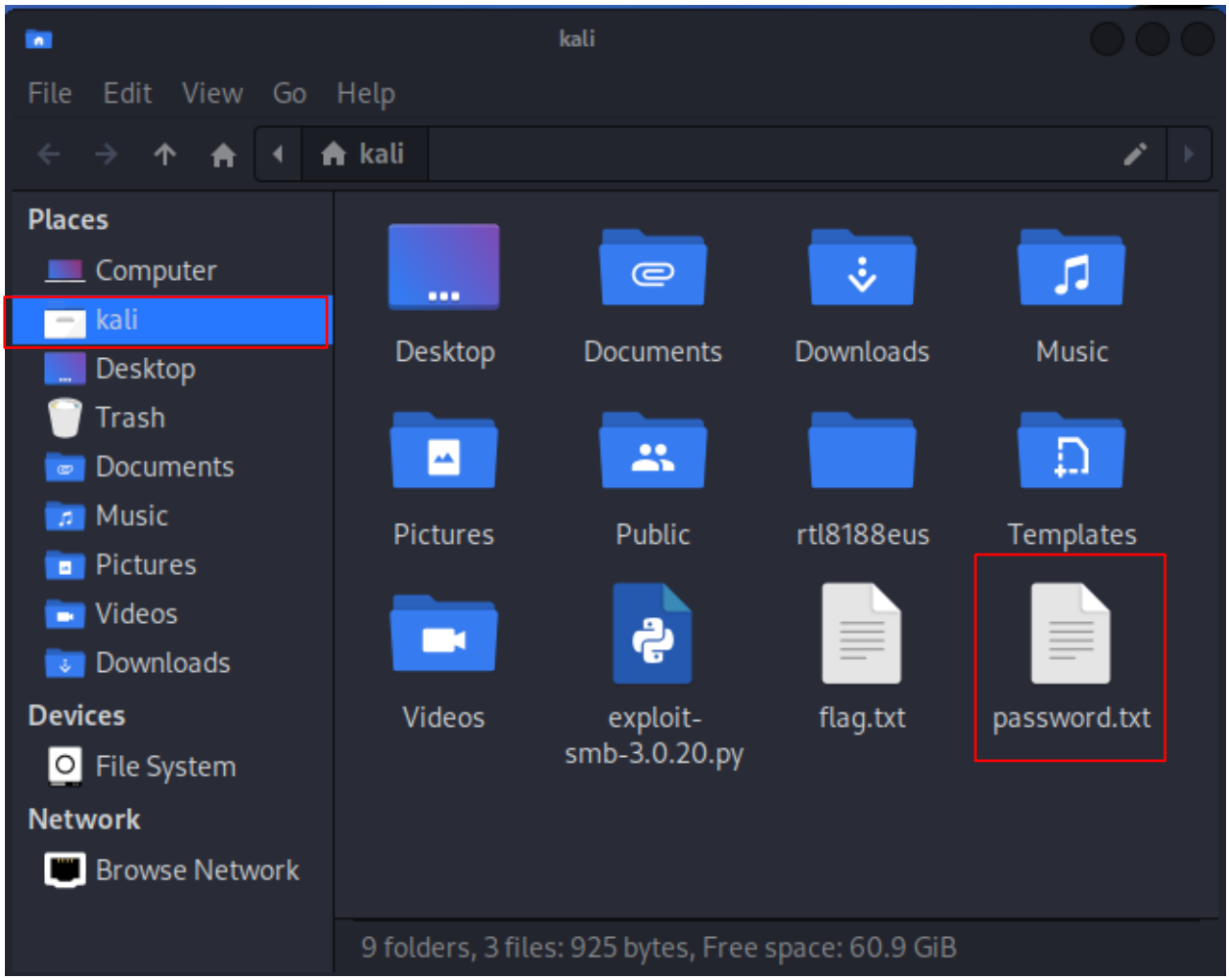

Figure 27: Showing the location of the password.txt file.

Step 8: Searching for ssh vulnerabilities in the web

To carry out the attack successfully we need to use an auxiliary inside the ssh module for which we searched up for the possible exploits of ssh in the web. The search directed us to multiple webpages from which we can find the specific auxiliary for the brute force attack to carry out.

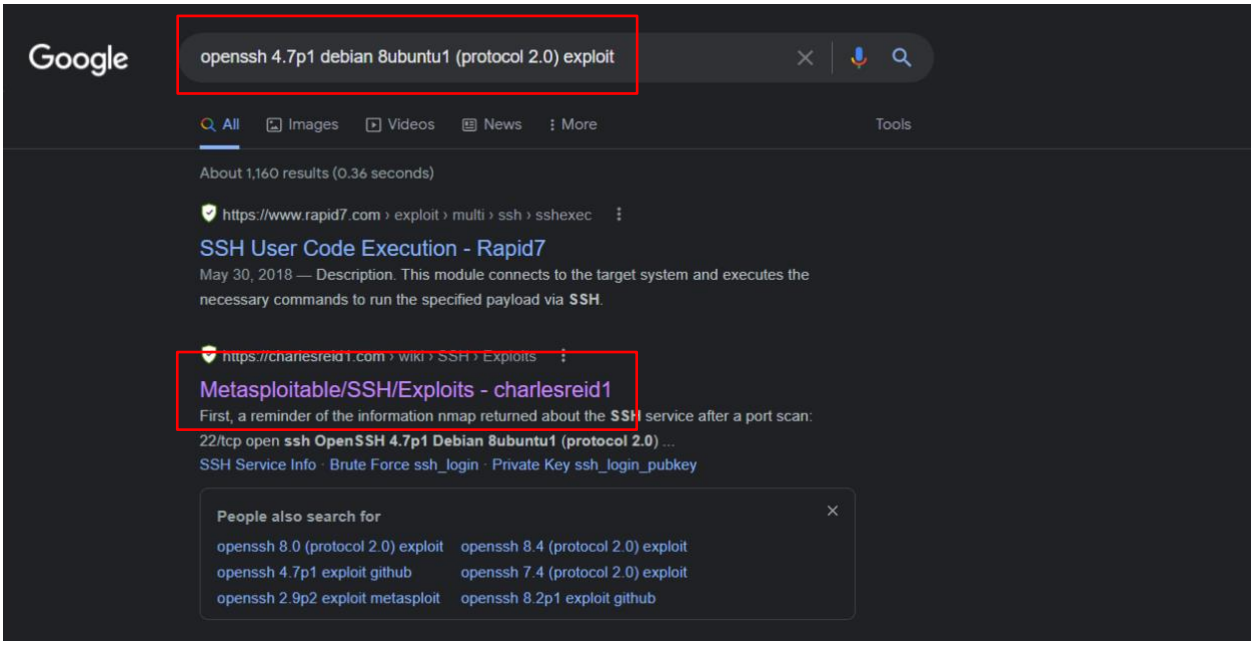

Figure 28: Searching for SSH exploits in the web.

Now, after visiting a specific URL containing various Metasploit SSH exploits, we choose the **"ssh_login**" method with the command **"auxiliary/scanner/ssh/ssh_login"** which is most suited to carrying out the attack in accordance with the requirements of this coursework. This also allows to use Metasploit to brute force guess SSH login credentials.

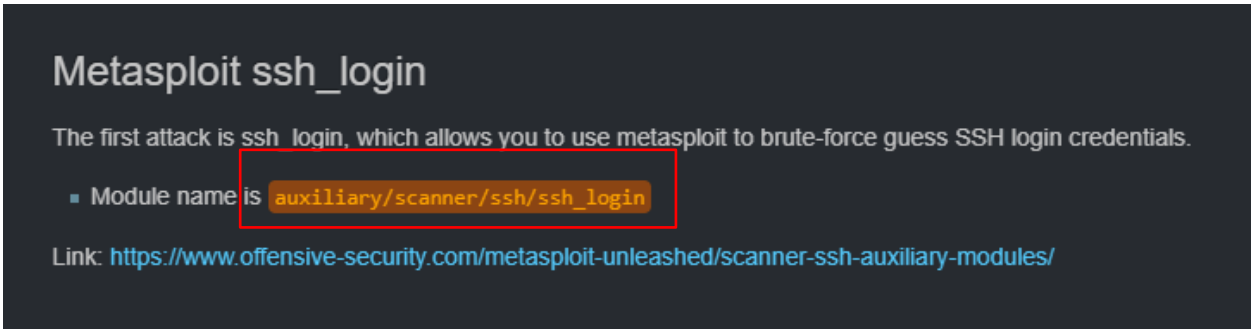

Figure 29: Selecting the auxiliary for the attack.

Step 9: Listing out the different options inside the auxiliary

The next step is to check out all the options available for the **"ssh_login"** module with the command **"show options"**. It provided with a list of options name, their settings, requirement and a brief description as well. Out of which the **"RHOSTS"** options was used to carry out the brute force attack.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all
                                                 users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, fro
                                                m 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password coup
                                                le stored in the current da
                                                tabase
   DB_ALL_PASS       false            no        Add all passwords in the cu
                                                rrent database to the list
   DB_ALL_USERS      false            no        Add all users in the curren
                                                t database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials s
                                                tored in the current databa
                                                se (Accepted: none, user, u
                                                ser&realm)
   PASSWORD                           no        A specific password to auth
                                                enticate with
   PASS_FILE                          no        File containing passwords,
                                                one per line
   RHOSTS                             yes       The target host(s), see htt
                                                ps://github.com/rapid7/meta
                                                sploit-framework/wiki/Using
                                                -Metasploit
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a creden
                                                tial works for a host
   THREADS           1                yes       The number of concurrent th
                                                reads (max one per host)
   USERNAME                           no        A specific username to auth
                                                enticate as
   USERPASS_FILE                      no        File containing users and p
                                                asswords separated by space
                                                , one pair per line
   USER_AS_PASS      false            no        Try the username as the pas
                                                sword for all users
   USER_FILE                          no        File containing usernames,
                                                one per line
   VERBOSE           false            yes       Whether to print output for
                                                 all attempts

msf6 auxiliary(scanner/ssh/ssh_login) >
```

Figure 30: Listing out all the available options.

Step 10: Setting options for the configuration

Firstly, we choose the **"ssh_login"** auxiliary method with the command **"auxiliary/scanner/ssh/ssh_login"** which allows to use the Metasploit environment to brute force guess SSH login credentials. Then the configuration was set using **"set RHOSTS 192.169.174.131"** command where the IP address is of the target pc which is Metasploitable2. Then the location of the file **"password.txt"** was set using **"set USERPASS_FILE /home/kali/password.txt"** which consists hundred different combinations of usernames and passwords.

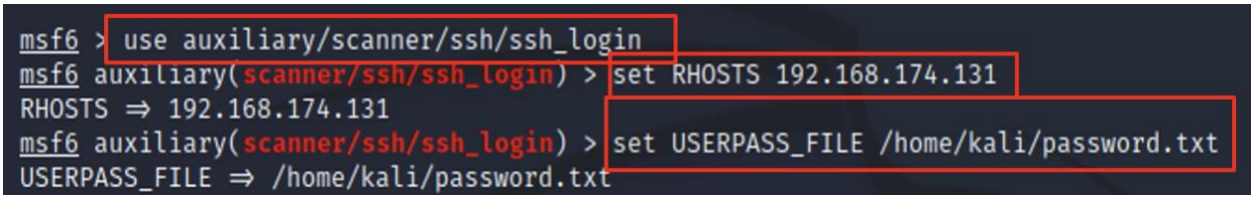

Figure 31: Setting options for the configuration.

Step 11: Verifying the settings for the configuration

After the configuration has been made which has been explained in the above **"Step 10"**, now to check out if the options are set accordingly or not the **"show options"** command was run in the terminal.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting   Required  Description
   ----              ---------------   --------  -----------
   BLANK_PASSWORDS   false             no        Try blank passwords for al
                                                 l users
   BRUTEFORCE_SPEED  5                 yes       How fast to bruteforce, fr
                                                 om 0 to 5
   DB_ALL_CREDS      false             no        Try each user/password cou
                                                 ple stored in the current
                                                 database
   DB_ALL_PASS       false             no        Add all passwords in the c
                                                 urrent database to the lis
                                                 t
   DB_ALL_USERS      false             no        Add all users in the curre
                                                 nt database to the list
   DB_SKIP_EXISTING  none              no        Skip existing credentials
                                                 stored in the current data
                                                 base (Accepted: none, user
                                                 , user&realm)
   PASSWORD                            no        A specific password to aut
                                                 henticate with
   PASS_FILE                           no        File containing passwords,
                                                  one per line
   RHOSTS            192.168.174.131   yes       The target host(s), see ht
                                                 tps://github.com/rapid7/me
                                                 tasploit-framework/wiki/Us
                                                 ing-Metasploit
   RPORT             22                yes       The target port
   STOP_ON_SUCCESS   false             yes       Stop guessing when a crede
                                                 ntial works for a host
   THREADS           1                 yes       The number of concurrent t
                                                 hreads (max one per host)
   USERNAME                            no        A specific username to aut
                                                 henticate as
   USERPASS_FILE     /home/kali/passw  no        File containing users and
                     ord.txt                     passwords separated by spa
                                                 ce, one pair per line
   USER_AS_PASS      false             no        Try the username as the pa
                                                 ssword for all users
   USER_FILE                           no        File containing usernames,
                                                  one per line
   VERBOSE           false             yes       Whether to print output fo
                                                 r all attempts

msf6 auxiliary(scanner/ssh/ssh_login) >
```

Figure 32: Verifying the configuration.

Step 12: Running the module

The final phase of the assault is to run the module using the **"run"** command. When the execution was finished, it displayed the matches of the hundred different username and password combinations from the **"password.txt"** file and the Metasploitable system, as well as the version of SSH used in the Metasploitable2 and the pair **"msfadmin msfadmin"** as the correct username and password of the victim pc.

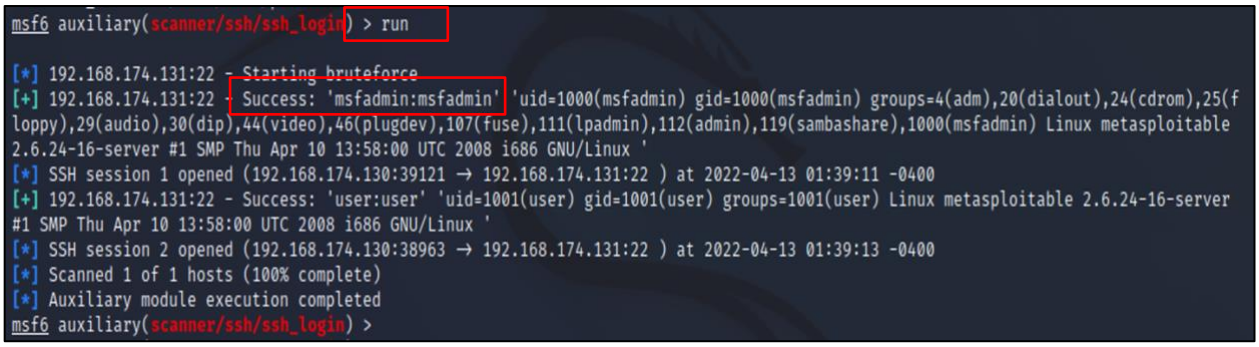

Figure 33: Attack being successful.

Step 13: Opening the session

Then after the completion of the brute force attack using **“ssh”** auxiliary, the module execution **“sessions”** command was run to list all the active sessions present in it. Then to interact with the SSH session **“-i”** flag is used. Then to establish interaction “**session -i 1**” command was run where **“id”** command was used to check the users and its privilege and the **“ls”** command was used to list all the files present on it. This shows that the attempt was successful and the account was successfully compromised.

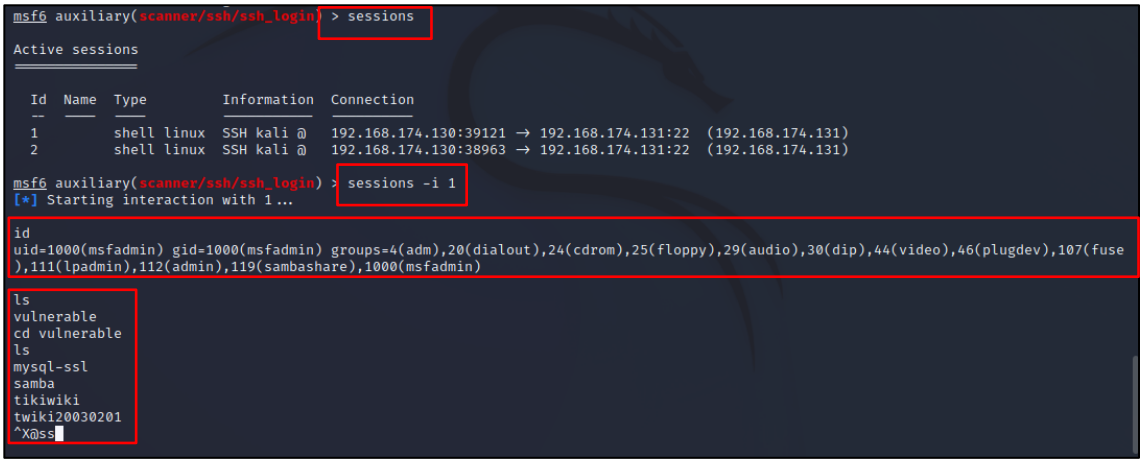

Figure 34: Opening the session and checking it with different commands.

3.3 Login into Metasploitable2 from Kali Linux

After successfully completing the brute force attack from Kali Linux as the attacker pc to Metaspoitable2 as the target pc using the **"ssh login"** auxiliary, Metasploitable2 was logged in from Kali Linux using the Metaspoitable2's IP address. The command **"ssh msfadmin@192.168.100.10"** was run in **root@kali**, and Metasploitable was successfully logged in from kali linux with the password **"msfadmin".** Then, in msfadmin, the **"ls"** command was used to find the vulnerability.

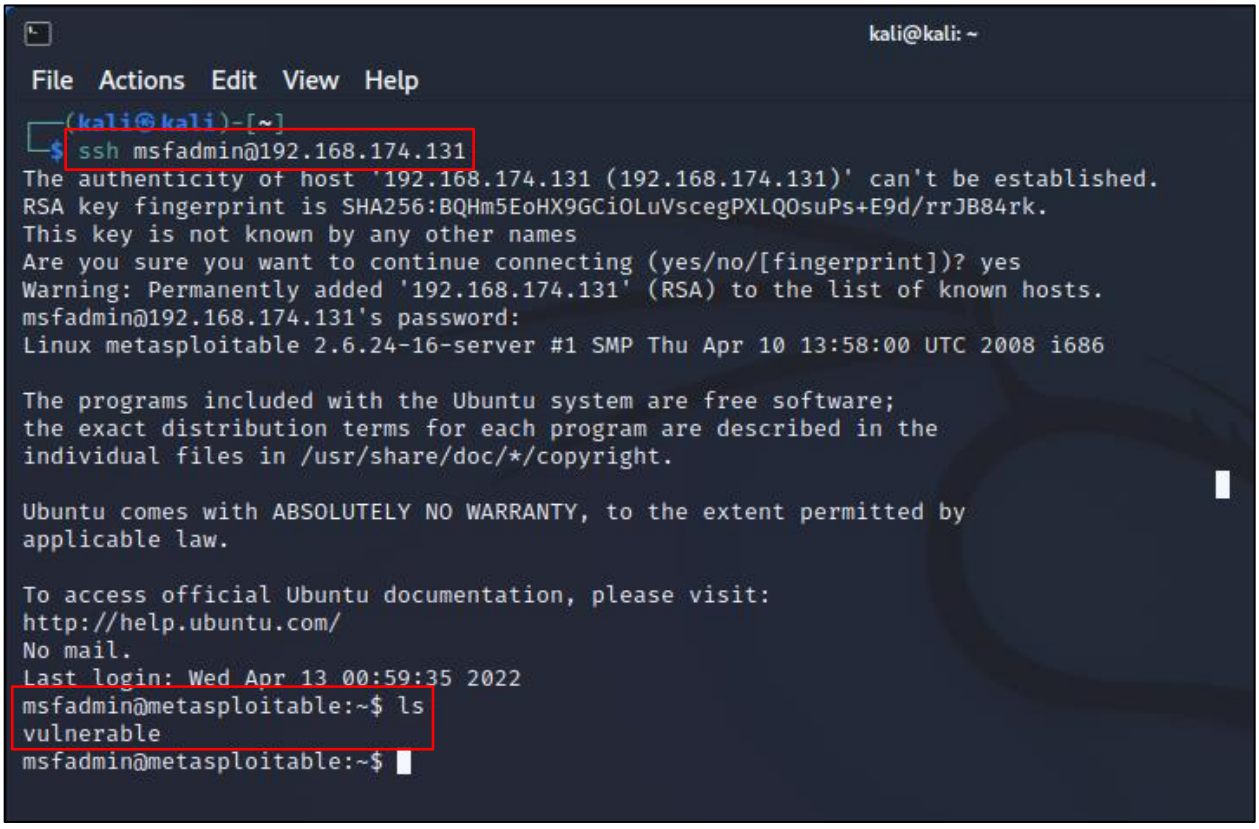

Figure 35: Logging Metaspoitable2 from Kali Linux.

4. Mitigation

The mitigation section contains two different methods that can be taken for the prevention for the brute force attack.

4.1 Changing the password of Metaspoitable2

Step 1: Changing the password

This is one of the method for the mitigation of the brute force attack in which the password for the **"msfadmin"** username was changed to **"coursework_77#"** which is a more secure password which was made up of using different alphabets, numbers and symbols. It was performed by using the **"passwd"** command and then entering the current password to ensure authenticity followed by the new password.

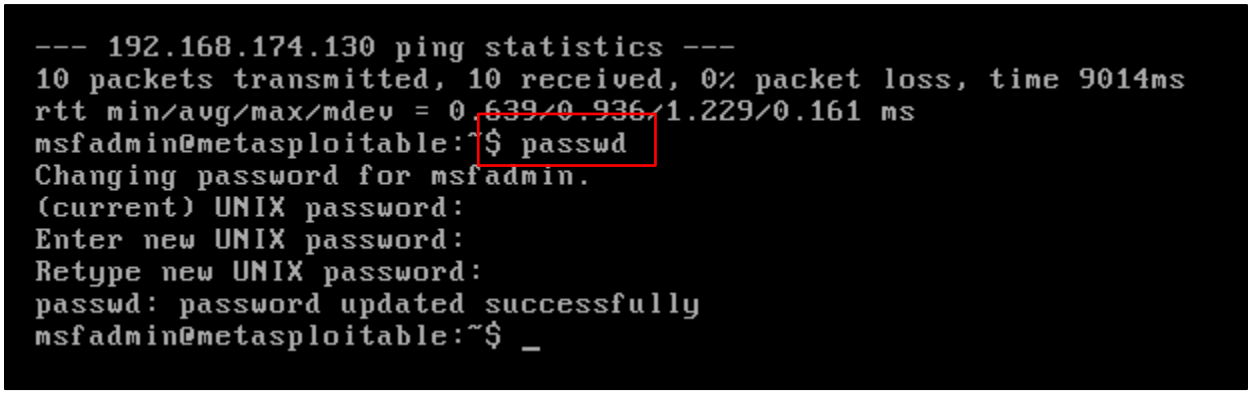

Figure 36: Changing the password of Metaspoitable2.

Step 2: Trying to login Metasploitable2 using both old and new password

The Metasploitable2 was now logged in from Kali Linux using the IP address of the Metasploitable2. The command **"ssh msfadmin@192.168.100.10"** was issued by **root@kali** and when the terminal asked for Metasploitable2 password, the password **"msfadmin"** was wrong. However, when the newly updated password **"coursework 77#"** was used, the user was successfully logged in.

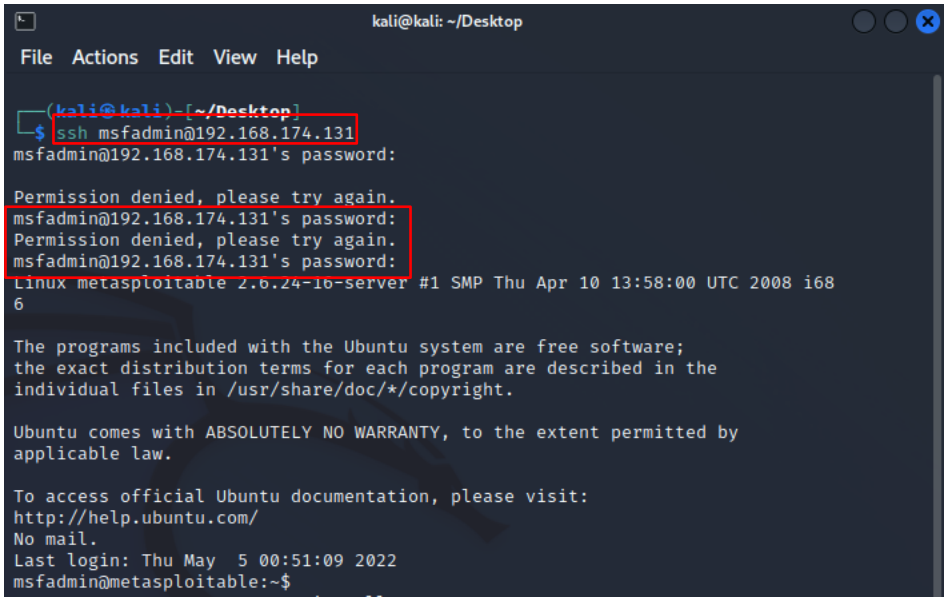

Figure 37: Checking the new password.

4.2 Changing the status of exploited port 22

This is also one of the methods for the mitigation of the brute force attacks in which the status of port 22 (ssh) is changed. The port 22 was open when it was exploited at last this port was closed to unauthorized root login to avoid future attacks of the same type.

Step 1: Scanning port 22 using nmap

Firstly using the command **"nmap -p 22 192.168.174.131"** the status of the port is checked which lists that the post is in **"open"** state.

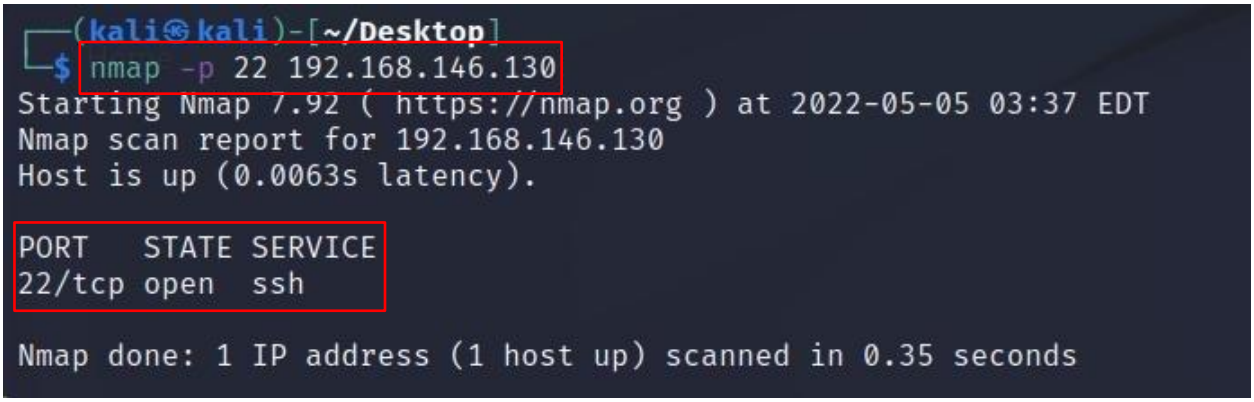

Figure 38: Checking the status of the port 22.

Step 2: Enabling the Uncomplicated Firewall (UFW) in Metaspoitable 2

In default the status of the uncomplicated firewall was disabled. In order to enable it the command **"ufw enable"** was used. After enabling it the status and configuration of the firewall was checked using the command **"ufw verbose status".**

```
root@metasploitable:~# ufw enable
Firewall started and enabled on system startup
root@metasploitable:~# ufw verbose status

Usage: ufw COMMAND

Commands:
  enable                      Enables the firewall
  disable                     Disables the firewall
  default ARG                 set default policy to ALLOW or DENY
  logging ARG                 set logging to ON or OFF
  allow|deny RULE             allow or deny RULE
  delete allow|deny RULE      delete the allow/deny RULE
  status                      show firewall status
  version                     display version information
```

Figure 39: Enabling the Uncomplicated Firewall.

Step 3: Denying the SSH client request comping from Kali Linux.

To block the SSH client request coming from the Kali Linux with its IP address the command **"ufw deny from 192.168.146.128 to any port 22"** was executed, which blocks the **"port 22"** of TCP. At last the command **"ufw status verbose"** was executed to verify that if the rule was added correctly or not.

```
root@metasploitable:~# ufw deny from 192.168.146.128 to any port 22
Rule added
root@metasploitable:~# ufw status verbose
Firewall loaded

To                         Action  From
--                         ------  ----
Anywhere                   DENY    192.168.146.128
22:tcp                     DENY    192.168.146.128
22:udp                     DENY    192.168.146.128
```

Figure 40: Blocking SSH client request for Kali Linux.

Step 4: Accepting the SSH client request

In this step the **"ufw allow ssh"** command was executed to accept the SSH client request coming from any other device. Then the **"ufw status verbose"** command was executed to verify that if the rule which was added is correct or not.

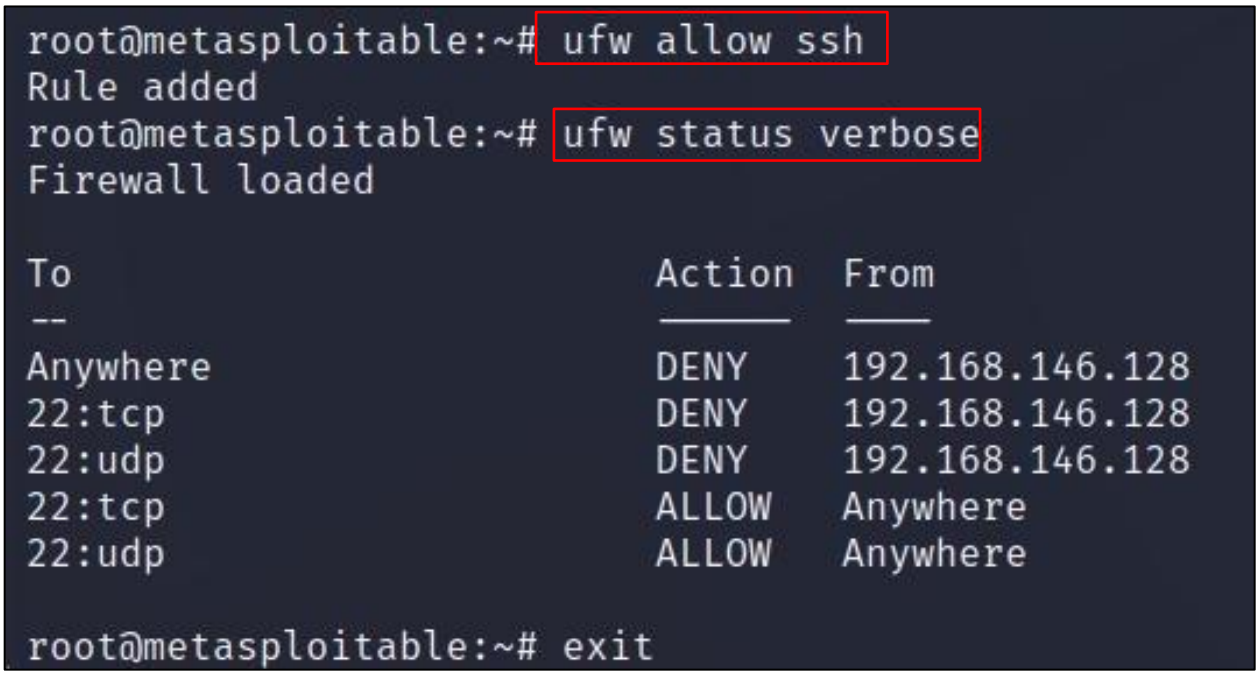

Figure 41: Allowing SSH client request for other hosts.

Step 5: Again scanning port 22 using nmap

At last using the command **"nmap -p 22 192.168.174.130"** the status of the port is checked which lists that the post is in **"filtered"** state, which means that the firewall has been set in port 22.

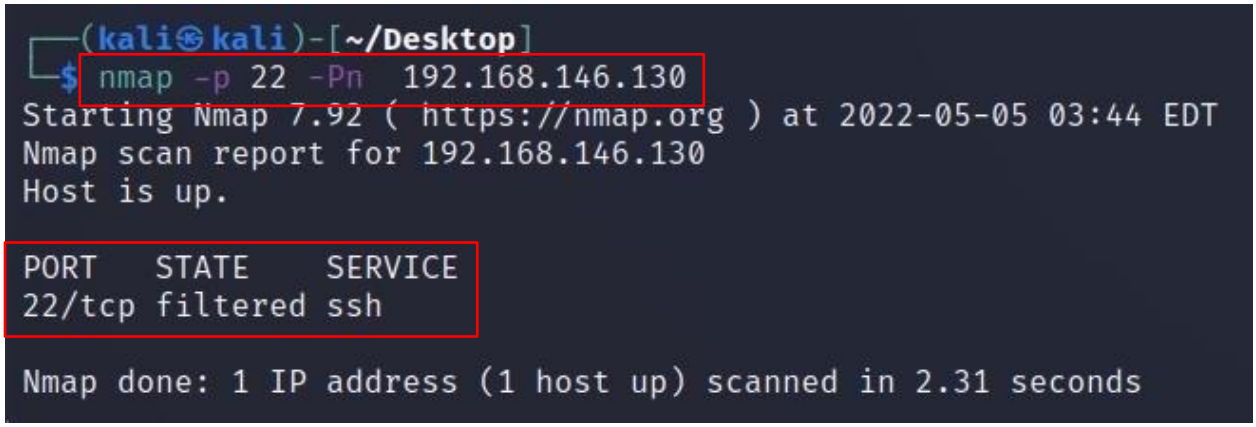

Figure 42: Again checking the status of the port.

5. Evaluation

The Brute Force attack is one of the frequently occurring attacks which doesn't require much tools. There is some procedure which could be followed or a method that could be applied to prevent Brute force attack to certain level. These methodologies can be usefull in order to reduce this cyber-attack.

In this coursework two of the mitigation methods have been demonstrated where one is changing the password of the Metasploitable2 and setting strong password consisting of numbers, alphabets and symbols to prevent the account being compromised. The other mitigation measure that has been applied is changing the status of the exploited port 22 using firewall.

5.1 Pros of the applied mitigation strategy

- The mitigation approach used does not require any new software or hardware components, making it cost-effective.
- The configuration of ssh can be changed as needed and access to unauthorized logins can be prohibited.
- Changing passwords on a regular basis can help to prevent and minimize the probability of a brute force attack.
- Because TCP port 22 is closed, a Brute Force attack from Kali Linux to Metaspoitable 2 via SSH login is not possible.

5.2 Cons of the applied mitigation strategy

- Whether the password of the Metasploitable 2 is changed frequently the hacker can again conduct the brute force attack using different password lists.
- If there is no control measure applied then the account of the victim can be not just compromised but the data stored can be leaked or abused.
- The firewall rule of Metasploitable 2 cab be easily bypassed from Kali Linux by changing its static IP address.

5.3 Cost Benefit analysis

A cost-benefit analysis is a technique that allows organizations to evaluate decisions, systems or initiatives, as well as assign a financial value to intangible assets. The model is constructed by identifying the advantages of an action as well as the costs associated with it and then subtracting the costs from the benefits. A cost benefit analysis produces results that can be utilized to reach reasonable conclusions about the feasibility and advisability of a choice or circumstance (Joe Weller, 2016).

The formula to calculate the Cost Benefit Analysis is:

Cost Benefit Analysis (CBA) = $ALE_{(prior)}$ – $ALE_{(post)}$ – ACS

Where,

$ALE_{(prior)}$ = It is the annual lost expectancy before implementing security on the risk measures.

$ALE_{(post)}$ = It is the annual lost expectancy after implementing security or the risk measures.

ACS = It is the annual cost of applied security or safeguard.

Further, to calculate the ALE the formula is,

ALE = SLE x ARO

Where,

SLE = It is the single lost expectancy which is the amount of lost that can occur in a single event of the attack or damage.

ARO = It is the annual rate of occurrence which is the number of times the incident takes place in a year.

For the calculation of the Cost Benefit Analysis, let us consider an organization XYZ has a system which is vulnerable to SSH brute force. The entire systems network interface is set on NAT which means that they are not vulnerable to outsiders. But an attacker might perfom the brute force attack if he access the devices inside the network physically. It has been estimated that the organization might face the attack once a year which causes a loss of $125000 if the brute force attack occurs which leads the attacker to have access to all of the systems of the organization. For its mitigation the organization installed an external firewall which costs $15000, if the organization did not use the firewall there would have been huge loss of data. After the implementation of the external firewall the Annual Loss Expectancy due to the Brute Force attack was reduced to $65000.

The Cost Benefit Analysis is:
Here,
Single Loss Expectancy (SLE) = $125000
Annual Rate of Occurrence (ARO) = 1 times a year
Annual Loss Expectancy (ALE) = SLE * AR0
= $125000 * 1
= $125000

Annual Loss Expectancy prior ($ALE_{(prior)}$) = $125000
Annual Loss Expectancy post ($ALE_{(post)}$) = $65000
Annual Cost of the Safeguard (ACS) = $15000

Cost Benefit Analysis (CBA) = $ALE_{(prior)} – ALE_{(post)} – ACS$
= $125000 - $65000 - $15000
= $ 45000

Hence, the cost of installing an external firewall is less than the annual lost expectancy due to the Brute Force attack. Thus, installing an external firewall has positive benefits to the organization.

6. Conclusion

Finally, the coursework gave us the opportunity to learn more about network-based attacks, of which I chose the topic Brute Force attacks on Information Technology devices and systems and how it plays a significant role in the aspect of information security, including its types, patterns, motive behind it, and protocols, among other details.

We carried out an attack on a vulnerable Metasploitable2 system running the Kali Linux operating system. The network topology for the attack was presented using packet tracer, which reflects the attack's overview. Other tools have been utilized in this course, including VMware to launch Kali Linux and Metasploitable2 from which we carried out the attack and other tools such as nmap. Each step of the attack has been discussed in detail, and screenshots have been provided to show what was actually done.

The documentation is a technical report to support the conducted attack it has been compiled with allot pf research from valid sources which has been listed in the reference section. The illustrations included have been cited and arranged with captions. Bibliography section has also been included to list all the site that have been consulted in accomplishing this coursework.

This coursework has fulfilled all the objectives as listed above and provided a lot of knowledge about the tools used and has provided an insight on the real-life scenarios. The completion of this coursework improved our research and information-finding abilities as well.

References

faq-ans, 2021. *How Information System influence our daily lives?.* [Online]
Available at: https://faq-ans.com/en/Q%26A/page=ab7a8180406ce8f7ecebc4ed122ebdc9
[Accessed 17 April 2022].

Statista, 2021. • *Internet users in the world 2021 | Statista.* [Online]
Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/
[Accessed 19 April 2022].

Johnson, J., 2021. • *Internet users in the world 2021 | Statista.* [Online]
Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/
[Accessed 19 April 2022].

M. Uma, G. P., 2011. A Survey on Various Cyber Attacks and Their Classifications. *International Journal of Network Security,* 15(5), pp. 390-396.

Hanna, K. T., 2022. *What is a brute-force attack? - Definition from TechTarget.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/brute-force-cracking
[Accessed 23 April 2022].

Mahore, T. R. & Deorankar, P. A., 2017. A survey on various attacks possible in authentication.. *International Journal of Advance Research in Science and Engineering,* 6(4), pp. 891-895.

Sobers, R., 2021. *134 Cybersecurity Statistics and Trends for 2021.* [Online]
Available at: https://www.varonis.com/blog/cybersecurity-statistics
[Accessed 26 April 2022].

Parachute, 2022. *2022 Cyber Attack Statistics, Data, and Trends | Parachute.* [Online]
Available at: https://parachute.cloud/2022-cyber-attack-statistics-data-and-trends/
[Accessed 26 April 2022].

Kim, W., Jeong, O. R., Kim, C. & So, J., 2011. The dark side of the Internet: Attacks, cost and responses. *Information Systems,* 36(3), pp. 675-705.

Stiawan, D. et al., 2019. Investigation Brute Force Attack Patterns in IoT Network. *Journal of Electrical and Computer Engineering,* Volume 2019, pp. 1-13.

Swinhoe, D., 2020. *What is a brute force attack? And why they are on the rise | CSO Online.* [Online]
Available at: https://www.csoonline.com/article/3563352/brute-force-attacks-explained-and-why-they-are-on-the-rise.html
[Accessed 28 April 2022].

Petters, J., 2021. *What is a Brute Force Attack?.* [Online]
Available at: https://www.varonis.com/blog/brute-force-attack
[Accessed 28 April 2022].

Craig, S., 2016. *Beware of older cyber attacks, Footprinting and brute force attacks are still in use,* New York: IBM Security.

Stackscale, 2021. *SSH protocol: usage, versions and implementations | Stackscale.* [Online]
Available at: https://www.stackscale.com/blog/ssh-protocol/
[Accessed 28 April 2022].

Suse-Defines, 2022. *What is VMware? | Answer from SUSE Defines.* [Online]
Available at: https://www.suse.com/suse-defines/definition/vmware/
[Accessed 28 April 2022].

Williams, L., 2022. *Kali Linux Tutorial for Beginners: What is, How to Install & Use.* [Online]
Available at: https://www.guru99.com/kali-linux-tutorial.html
[Accessed 28 April 2022].

RAPID7, 2012. *Metasploitable 2 | Metasploit Documentation.* [Online]
Available at: https://docs.rapid7.com/metasploit/metasploitable-2/
[Accessed 28 April 2022].

Khan Academy, 2022. *Transmission Control Protocol (TCP) (article) | Khan Academy.* [Online]
Available at: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp
[Accessed 28 April 2022].

ExtraHop, 2022. *Telnet Protocol - Definition & How it Works - ExtraHop.* [Online]
Available at: https://www.extrahop.com/resources/protocols/telnet/
[Accessed 28 April 2022].

Ferranti, M., 2018. *What is Nmap? Why you need this network mapper | Network World.* [Online]
Available at: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html
[Accessed 28 April 2022].

wallaram, 2022. *What is SSH Protocol 🔑 All there is to know about it..* [Online]
Available at: https://www.wallarm.com/what/what-is-ssh-protocol
[Accessed 29 April 2022].

javapoint, 2022. *TCP - javatpoint.* [Online]
Available at: https://www.javatpoint.com/tcp
[Accessed 29 April 2022].

SSH, 2022. *Countering Password Stealing Attacks - Replace telnet with SSH..* [Online]
Available at: https://www.ssh.com/academy/ssh/telnet
[Accessed 29 April 2022].

mjrod, 2021. *Scanning with `nmap` CLI Tool.* [Online]
Available at: https://dev.1mrkt.to/scanning-with-nmap-cli-tool/
[Accessed 29 April 2022].

Joe Weller, 2016. *Cost Benefit Analysis: An Expert Guide* | *Smartsheet.* [Online]
Available at: https://www.smartsheet.com/expert-guide-cost-benefit-analysis
[Accessed 3 May 2022].

Bibliography

Tidwell, T., Larson, R., Firtch, K. & Hale, J., 2001. Modeling Internet Attacks. *Workshop on Information Assurance and Security*, 5 June, pp. 54-59.

Raza, M., Iqbal, M., Sharif, M. & Haider, W., 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal,* 19(4), pp. 439-444.

Kumar, N., 2011. Investigations in Brute Force Attack on Cellular Security Based on Des and Aes. *IJCEM International Journal of Computational Engineering & Management,* Volume 14, pp. 50-52.

Melnick, J., 2018. *Top 10 Most Common Types of Cyber Attacks.* [Online]
Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
[Accessed 3 April 2022].

Abomhara, M., 2015. *Cyber Security and the Internet of Things:Vulnerabilities,Threats, Intrudersand Attacks,* Agder: University of Agder.
Embroker, 2022. *2022 Must-Know Cyber Attack Statistics and Trends | Embroker.* [Online]
Available at: https://www.embroker.com/blog/cyber-attack-statistics/
[Accessed 2 May 2022].

purplesec, 2022. *2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends | PurpleSec.* [Online]
Available at: https://purplesec.us/resources/cyber-security-statistics/
[Accessed 3 May 2022].

fortnite, 2022. *Recent Cyber Attacks—News on Data and Security Breaches | Fortinet.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks
[Accessed 3 May 2022].

Stair, R. M. & Reynolds, G. W., 2018. *Fundamental of Information Systems.* 4th Edition ed. Boston: Cengage Learning.

Dave, K. T., 2013. Brute-force Attack “Seeking but Distressing”. *International Journal of Innovations in Engineering and Technology (IJIET),* 2(3), pp. 75-78.

Singh, R., Kumar, H., Singla, R. K. & Ketti, R. R., 2017. Internet Attacks and Intrusion Detection System. 41(2), pp. 171-184.