LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC605NI Ethical Hacking

Assessment Weightage & Type

50% Coursework

Year and Semester

2023 Autumn/Spring

Tittle: Phishing and social engineering techniques

Student Name: Janaki Chaudhary

London Met ID: 20049154

College ID: NP01NT4S210070

Assignment Due Date: 2023/05/03

Assignment Submission Date: 2023/05/03

Word Count (Where Required): 2289

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

Acknowledgement

I would like to express my sincere gratitude to all those who have given me the chance to work on this project. Firstly, I would like to extend my gratitude especially to my module teacher **Mr. Aditya Sharma** for his guidance and support throughout this project. I am also grateful to the college for providing us with the necessary resources required for the project. Additionally, I want to thank my friends and all those who have provided me with the direct or indirect support and shared their knowledge with me during the preparation of this report.

Abstract

In today's world, technology is rapidly evolving and so are the cyber threats. Amon them, phishing and social engineering are one of the most hectic and dangerous type of attack and organization or individual can face. Regardless of how much investments or efforts an organization puts on technical aspects of security, at the end of the day effectiveness of the security ultimately rely on how their employees interact with it. Regarding this project, a short demonstration of spear phishing was conducted, which involved compromising the PC of the IT officer of EHC Bank (assumed Bank) through a phishing email. The attacker lured the officer into downloading a payload file that was mentioned in the mail, which granted the attacker with a backdoor remote access to the system and allowed him to alter the company's official website, thus creating a fake website.

Moreover, the report is structured into various sections, including an introduction that provides a brief overview of the topic and its current situation, a background section that outlines the topic's context, a case study with critical analysis and tools /technologies used to present the proposed demonstration, an attack demonstration section that details the phases of the attack with multiple screenshots and a conclusion section that covers the legal, ethical and social consequences that can result from this demonstration.

Table of Contents

Table of figures

1. Introduction

1.1. Subject matter

With the development of information technology and the spread of social media networks, it has made communication convenient, but it has also led personal information being shared in internet. This has resulted in the emergence of social engineering, which involves exploiting human psychology to manipulate users into divulging sensitive information. One of the common methods of social engineering is phishing, in which the attackers impersonate legitimate sources through email spoofing, fake websites, or instant messages to obtain login credentials or make the victims performs certain actions (Rosencrance, 2023).

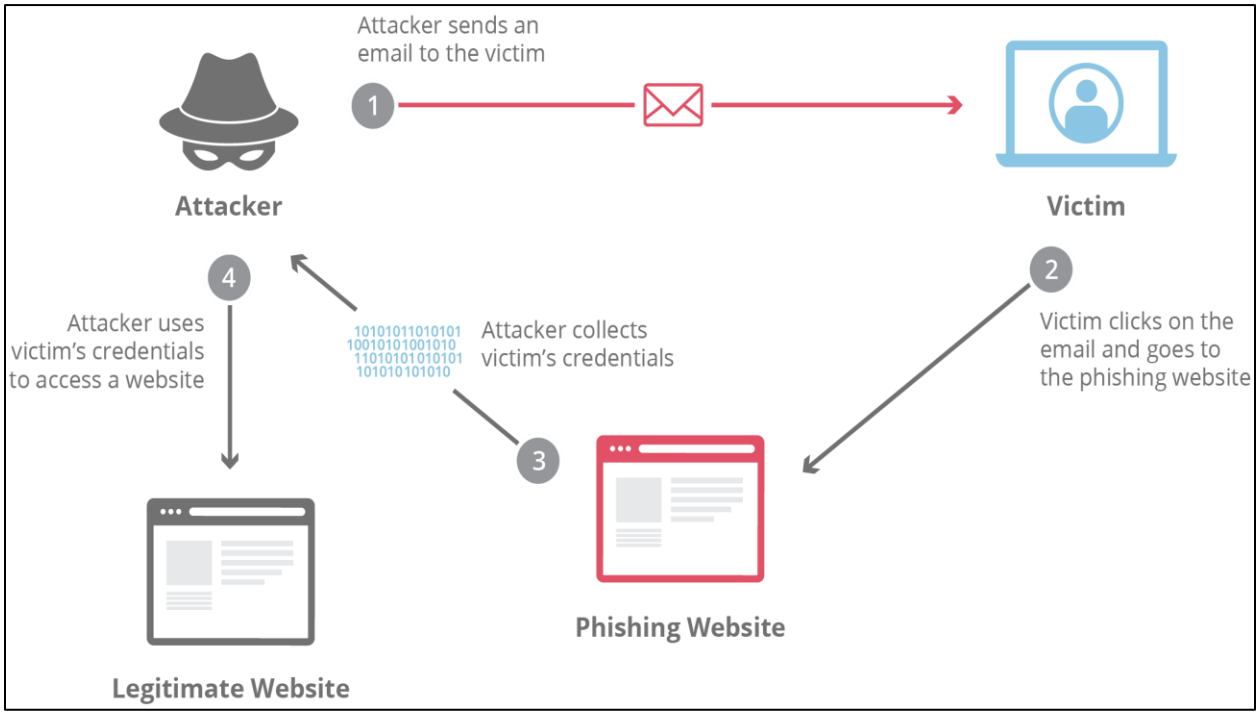


Figure 1 Example of simple email phishing process (Cloudfare, 2023).

Ethical hacking is the legitimate process of attempting unauthorized access to a computer device or data. Ethical hacking involves simulating real world attack-methods and behavior of malicious attackers to identify vulnerabilities and security weaknesses that can be addressed proactively, preventing unauthorized access by real attackers, thus helping organizations to mitigate cyber-attacks (Neagu, 2023).

This report presents a demonstration of a phishing attack that targets a company's domain controller. The attack aims to deceive the company's staff through a phishing email scam. To be precise, an assumed bank's (EHC Bank) sample environment is simulated using virtualization. The Metasploit framework and "VNCinejct" is used for gaining backdoor remote access and control, thus getting full access to the company's servers and computers.

1.2. Current scenario

In recent years, there has been a massive increase in the number and complexity of phishing attacks. The report published by Todd Stanfield, states that the Vade has detected 562.4 million phishing emails in the first quarter of 2023, which is an increase of 248.8 million from the previous quarter, Among the months in Q1, January had the highest volume of phishing emails with 488.5 million, while February and march had significantly lower numbers i.e. 26.6 million and 47.3 million, respectively (Stansfield, 2023).

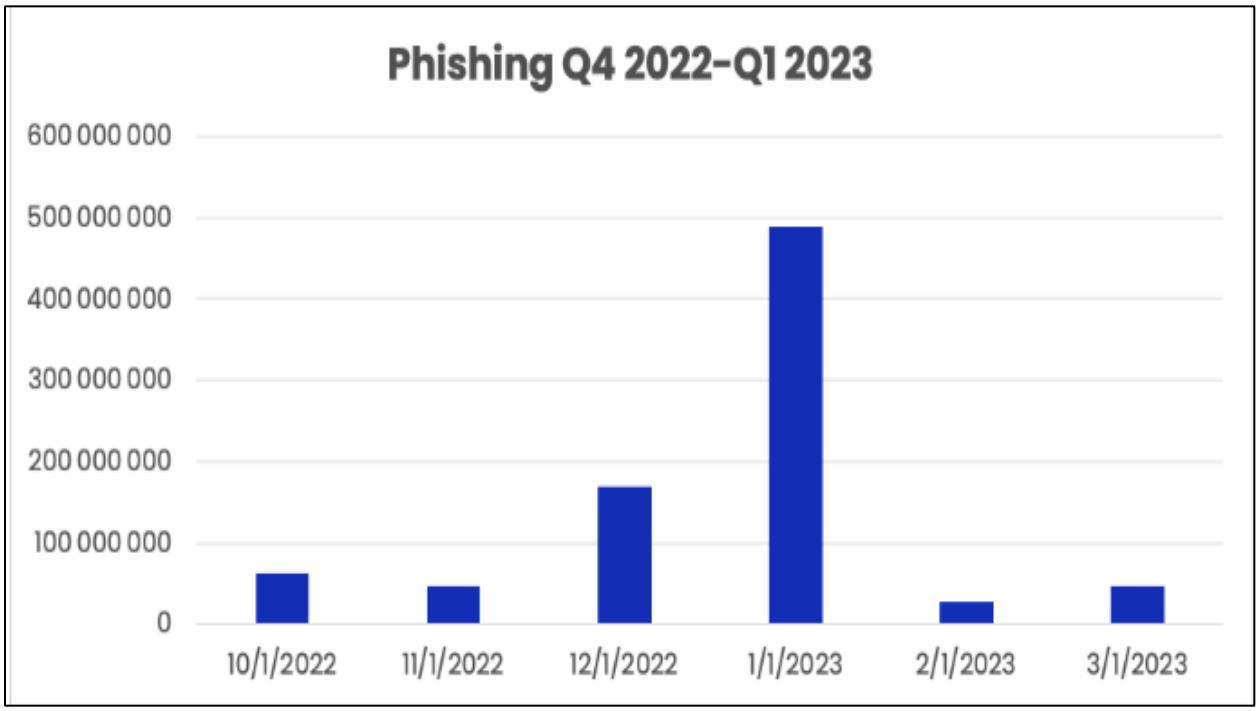


Figure 2 Volume of phishing attack 2022-2023 (Stansfield, 2023).

According to the report published by Anti-Phishing Working Group (APWG), the number one target for phishing attack is financial institution accounting for 23 percent of all attacks, while attacks on SaaS/webmail and social media accounted for 17 and 11 percent respectively, as shown in the figure below. The attackers are also even choosing the other unusual targets such as streaming services as well, online gaming accounts, reward program accounts and GitHub accounts accounting 30 percent of the total targets (Cook, 2023).

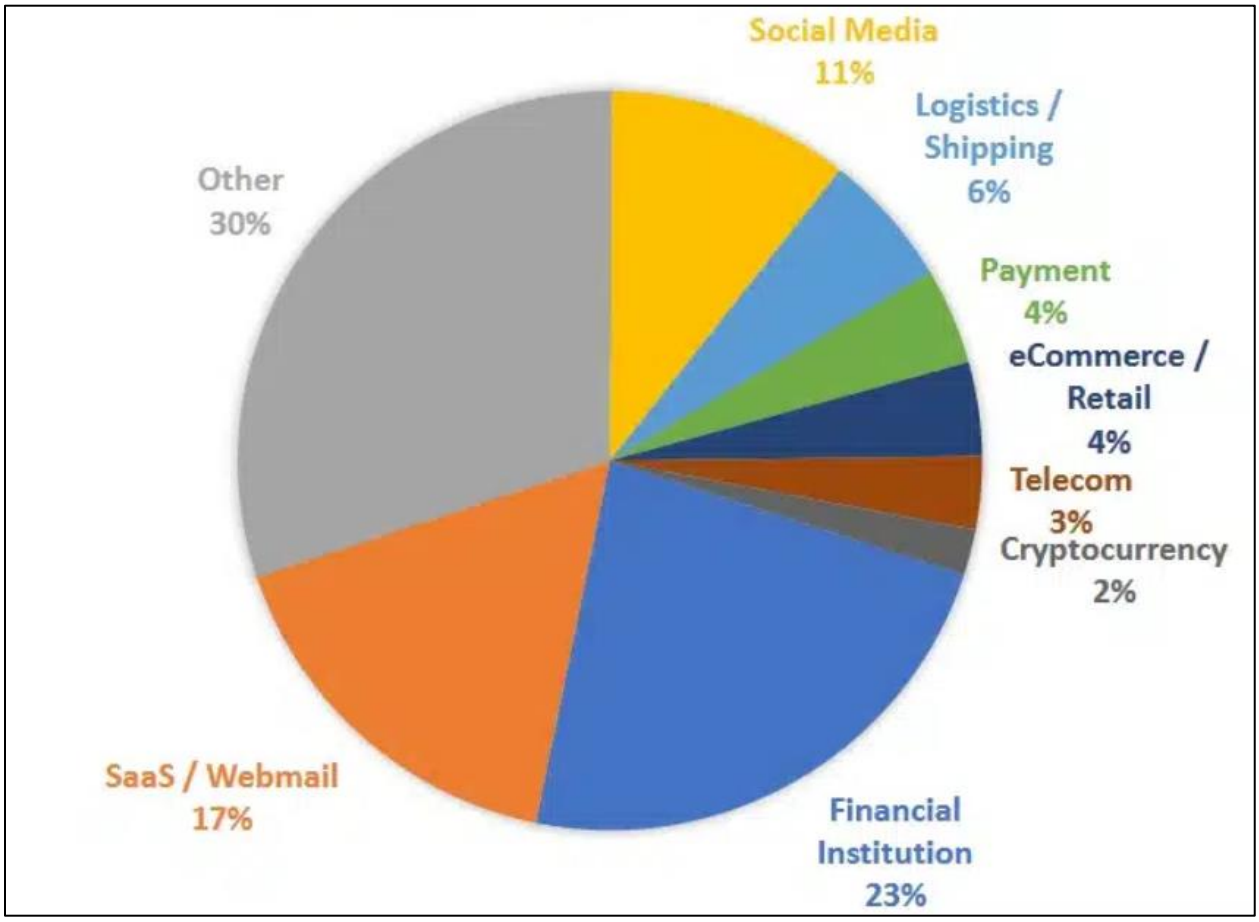


Figure 3 Industries targeted by Phishing, 3Q 2022 (Cook, 2023).

1.3. Aims and Objectives.

1.3.1. Aims

The main aim of this report is to do in-detailed study about the real-world phishing and social engineering techniques and understand its impact with the help of a demonstration.

1.3.2. Objectives

The objectives taken to achieve the aim are given below,

- To conduct extensive research on phishing and social engineering techniques, as well as its life cycles.
- To critically analyze real world phishing attack via case study.
- To setup a virtual environment of a financial organization i.e., assumed Bank.
- To set up a payload and use Metasploit framework to demonstrate remote access and control in the victim's system.
- To set up a phishing mail and deliver it to the victim's PC as an authenticated online forum Gmail account.
- To create a fake website by altering the official website of the bank.
- To evaluate legal, ethical, and social issues of the demonstrated phishing attack.
- To research and provide necessary recommendation to mitigate such attacks.

2. Background and literature review

2.1. Background

2.1.1. Social Engineering

The mechanism by which the social engineering works is manipulating people's emotions to steer them away from logical decision-making and towards emotional decision-making. The target's trust, fear, sympathy and willingness to support are exploited to extract sensitive information such as login credentials and other personal and official credentials. Terror, envy, interest, wrath, intimacy, loyalty, pride, compassion etc. are the examples of emotions used in social engineering (Fan, et al., 2017). A brief explanation of social engineering life cycle is shown below in given diagram,

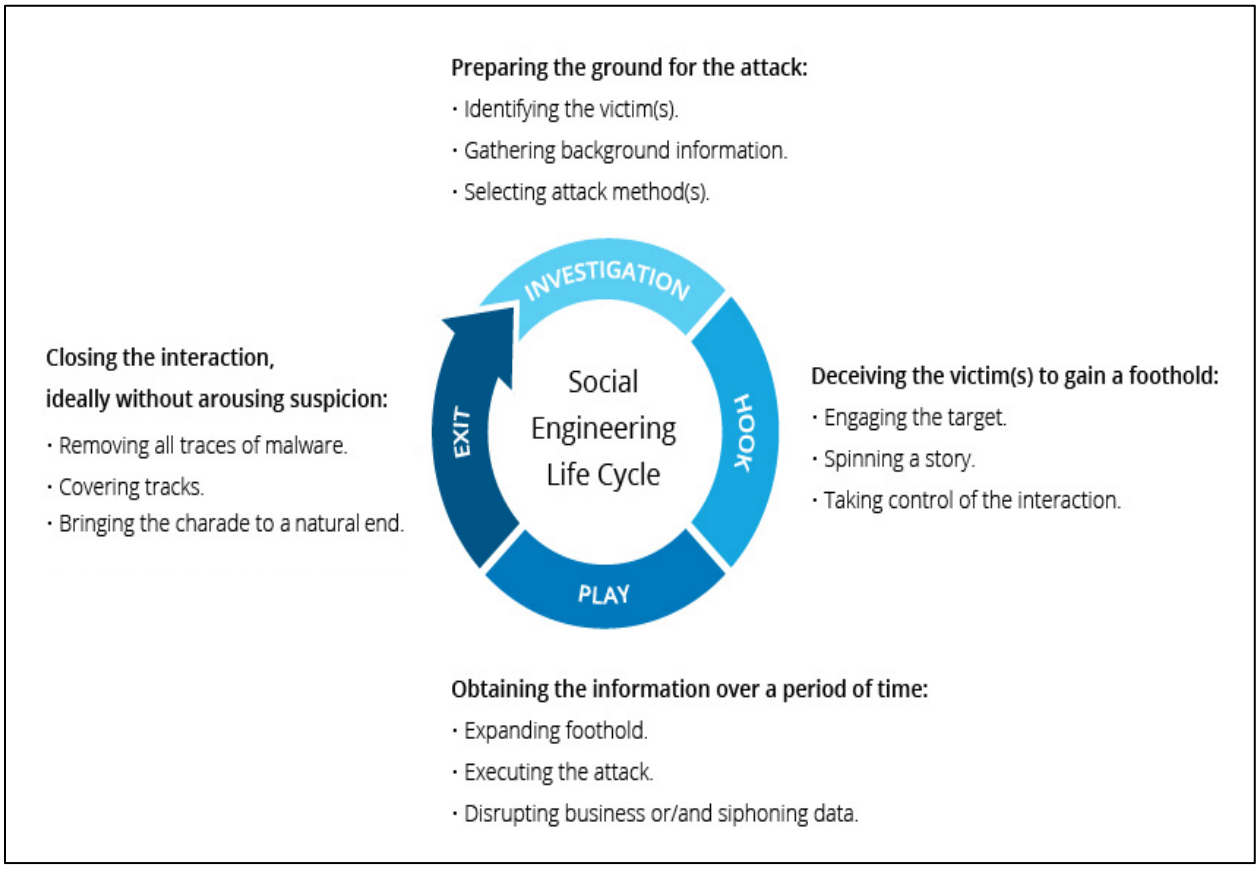


Figure 4 Social Engineering Life Cycle (Website security store, 2021).

Follow Appendix 7.1. for detailed explanation about Phishing and social engineering.

2.1.2. Spear Phishing

Spear phishing is a targeted attack where the attacker sends phishing messaged to specific individuals or groups often with a high level of personalization and customization, tricking them into revealing sensitive information or installing malware. The attack is more sophisticated and harder to detect as it is tailored to the interests and characteristics of the targeted individuals, using publicly available information. It is one of the common tactics used by cybercriminals and state-sponsored actors to gain access to sensitive information system (MohanaKhrishan, 2021).

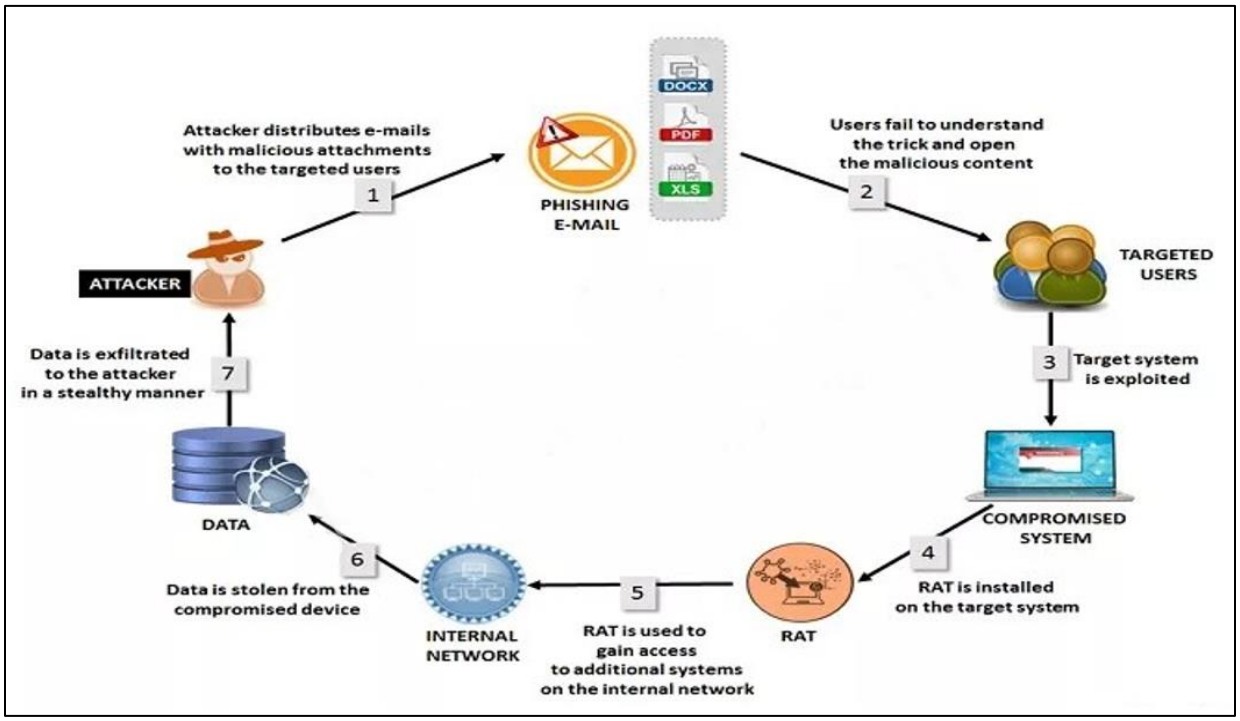


Figure 5 Example of a spear phishing (Bhardwaj, 2023).

Regarding this coursework's demonstration, firstly the official email account of the IT officer of EHC Bank is noted and his interest and characteristic were gathered, then a customized phishing mail was created easily tracking him to install the payload (malware), which enabled attacker with remote access and control. The attacker altered the official website of the bank thus creating a fake website sending alert message "Your account is hacked!", thus causing reputational damage to the organization.

2.2. Literature Review

2.2.1. Case study

Hackers target Russian government with fake windows update pushing RATs.

According to the report by Bill Toulas, Hackers are targeting Russian government agencies with phishing emails that pose as windows security updates and other deceptive tactics to install remote access malwares. The attacks are being conducted by a previously undetected APT (advanced persistent threat) group believed to be operating from China and they have also been linked to four separate spear phishing campaigns also. In all four cases, the ultimate goal of the campaigns was to infect the targets with a custom remote access trojan (RAT) for getting access into the system through the victim. The first phishing campaign was conducted in February 2022 by distributing the RAT named “interactive_map_UA.exe”. The second campaign used a tar.gz archive that was supposed to be a patch update for the Log4Shell vulnerability sent by the Ministry of Digital Development, Telecommunications and Mass communications of Russian Federation. Similarly, the third and fourth campaign, had phishing mails to employees of RT TV station (Toulas, 2022).

2.2.2. Critical analysis of the case study

The case study reports on a previously undetected APT group believed to be operating from China that has been targeting Russian government agencies and media organization with phishing emails. The attackers used deceptive tactics to install remote access malware on the victim’s system with the ultimate goal of gaining access to sensitive information or causing harm. The case study emphasizes the need for the employee education and targeted cybersecurity measures to prevent successful phishing attacks. It servers as a reminder of the ongoing and evolving threat of cyber attacks and the need of organizations to prioritize cybersecurity measures to protect their system and information.

2.3. Tools and technologies

2.3.1. VMware Workstation 16 pro

VMware Workstation 16 pro is a virtualization software developed by VMware enc company and enables users to create and run multiple virtual machines in a single physical machine. It is a type-2 hypervisor. (Afreen, 2023).

2.3.2. Kali Linux

Kali Linux is a Linux distribution designed for digital forensics, penetration testing, and security auditing and is equipped with a wide range of tools for different purposes like password cracking, network mapping, vulnerability scanning and wireless analysis. It is extensively employed by researchers, hackers, and security professionals to carry out diverse security related tasks (Jena, 2022).

2.3.3. Metasploit

Metasploit is one of the world's leading open-source modular penetrating framework which enables us to write, test, execute and exploit codes. It is used by network security professionals, ethical hackers, system administrators for penetration testing, patch installations testing etc. The core of the Metasploit framework is the meterpreter, which is an advanced payload, can be used to remotely control a compromised system. The meterpreter supplies numerous powerful features including the ability to sun arbitrary command, transfer files, access, and control victim's system (Buckbee, 2022). It consists different libraries and components i.e.,

- MSF core: It is the core library that includes the exploitation engine, payload etc.
- MSF Base: It is the set of modules and tools like exploit modules, encoders etc.
- MSF UI: It is the user interface of the framework i.e., GUI and CLI.

Follow Appendix 7.2. for detailed explanation of Metasploit framework.

2.3.4. Windows server 2019

Windows server 2019 is an operating system developed by Microsoft for enterprise-level applications and services in data centers and other environments. Its core uses include hosting websites and web applications, running virtual machines and containers, managing, and storing data, etc (Stenger, 2021). Regarding this coursework, two windows servers are used as domain controller and web server respectively.

2.3.5. Windows 7 enterprise

Windows 7 enterprise is an OS designed for business and corporate environments, with advanced features for managing and securing devices and data. In this coursework, it has been used as an PC for the staff i.e. IT officer of EHC Bank.

3. Attack Demonstration

There are plenty of attacks that can be used to export the malicious file and infect/harm a victim's system. Regarding this report's demonstration, a virtual environment is created to simulate an attack on a typical bank system. Firstly, two windows servers are configured as Domain controller and Web server respectively for the EHC bank. Moreover, a html website is created and hosted as the bank's official website using web server. Similarly, an ITofficer user is created as an Ad user with all the administrative privileges and run on windows 7 PC. Finally, an exe payload is created in kali Linux which is delivered through a phishing mail as a patch update to ITofficer system. Once, the victim downloads it and opens the file, the payload is executed, thus allowing backdoor remote access and control. With this access, the attacker alters the HTML script of the bank's official website hosted on web server, thus causing reputational damage to the company.

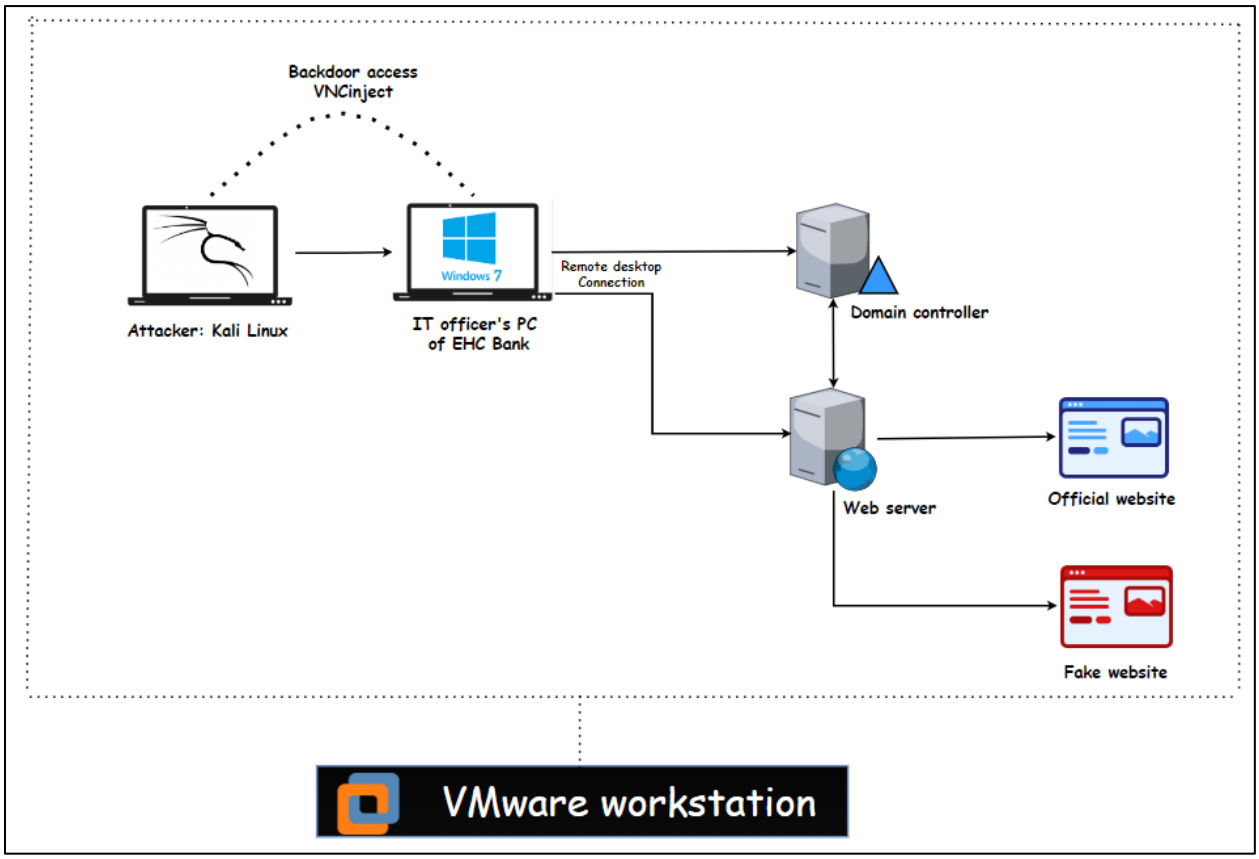


Figure 6 Proposed demonstration of EHC Bank.

3.1. Phases of Attack

The phases of an attack can differ depending upon the type of attack and the attacker's objectives. However, here are some common phases of the attack that is demonstrated for this report,

3.1.1. Reconnaissance

The attacker first gathers the information about the Bank and the IT officer of the bank by doing a thorough research from social media profiles and collected official mail of the officer.

Follow Appendix 7.3. to see the information gathered about the employee.

3.1.2. Weaponization

The attacker creates a payload named "update.exe" with VNC injected for backdoor remote access and created a phishing mail for windows patch update.

3.3.3. Delivery

The attacker delivers the malicious exe payload through a windows update phishing mail to the victim as an authenticated Microsoft windows customer support team.

3.3.4. Exploitation

After, the IT officer downloads the file, the exe payload is executed on the system, thus allowing backdoor remote access and control to attacker.

3.3.5. Installation

The attacker does not want any persistent or long-term access to the victim's system in future, thus eliminating the need for an installation phase.

3.3.6. Command and Control

The attacker uses Metasploit framework to establish a command-and-control channel with the victim's system. The multihandler module listens incoming connections whereas the VNCinject injects a VNC server into the victim system's memory.

3.3.7. Actions and objectives

The attacker's main motive was to alter the company's official website and create a fake website for reputational damage. To fulfill this, the attacker gained access to IT officer PC, since it has all administrative privileges.

3.2. Demonstration

The demonstration steps that were carried out during the attack are given below,

3.2.1. Installing and configuring domain controller.

Firstly, a windows server 2019 was installed and configured as Domain controller. An user named “IT officer” was added in AD users.

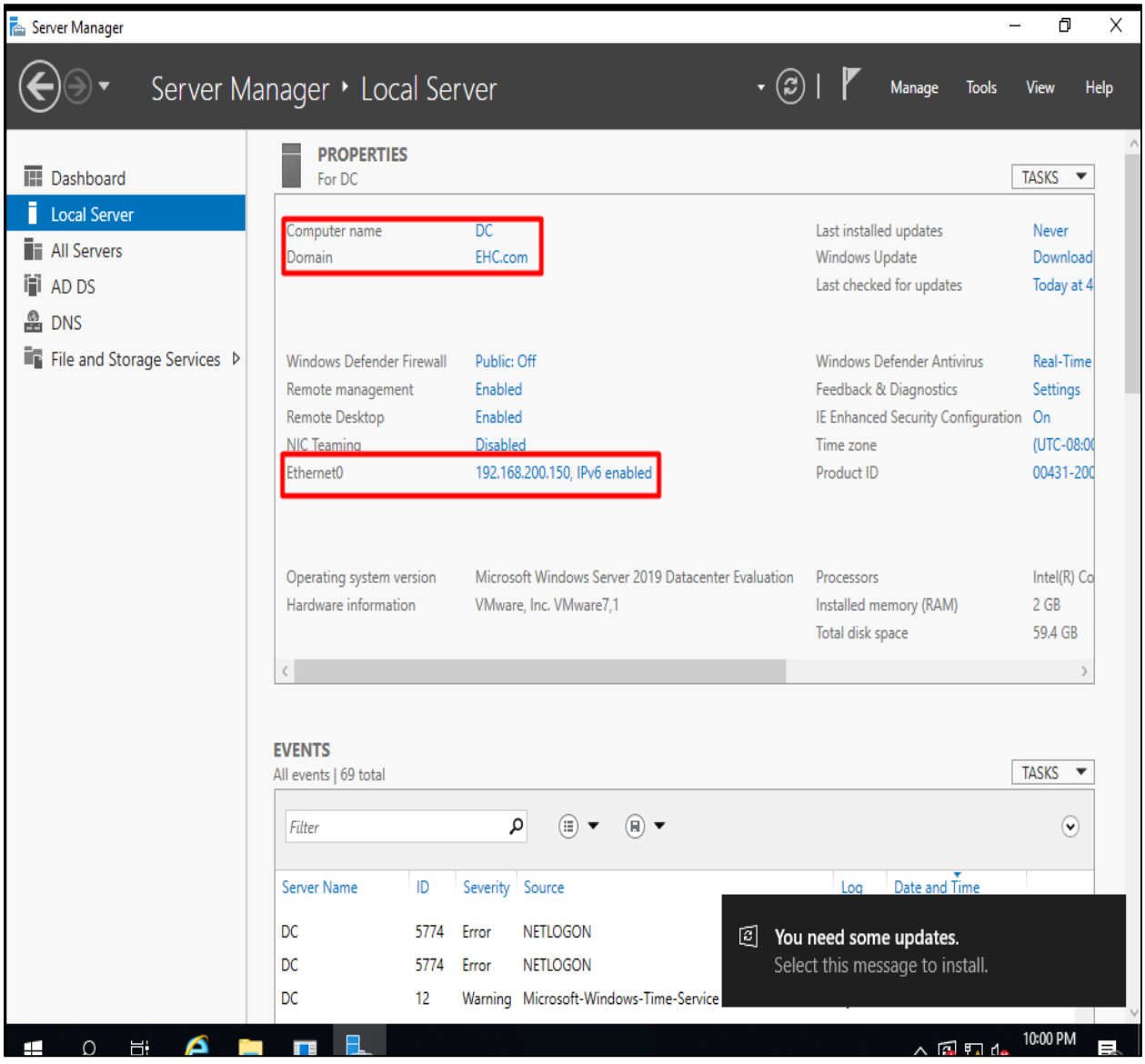


Figure 7 Domain controller configuration.

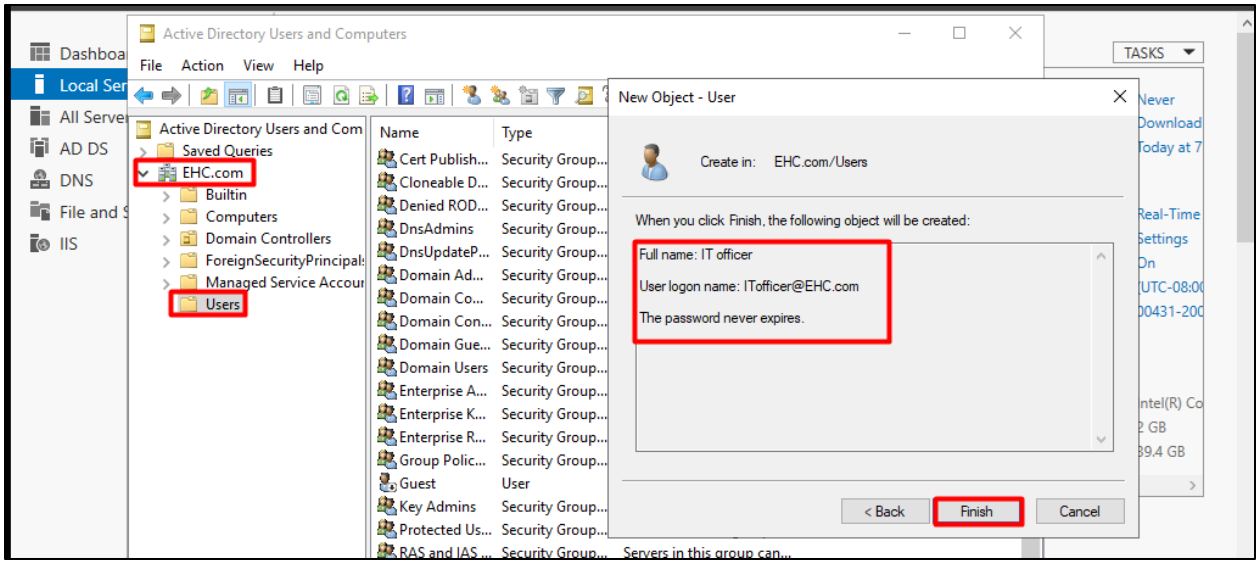


Figure 8 Adding ITofficer user in Active Directory Users.

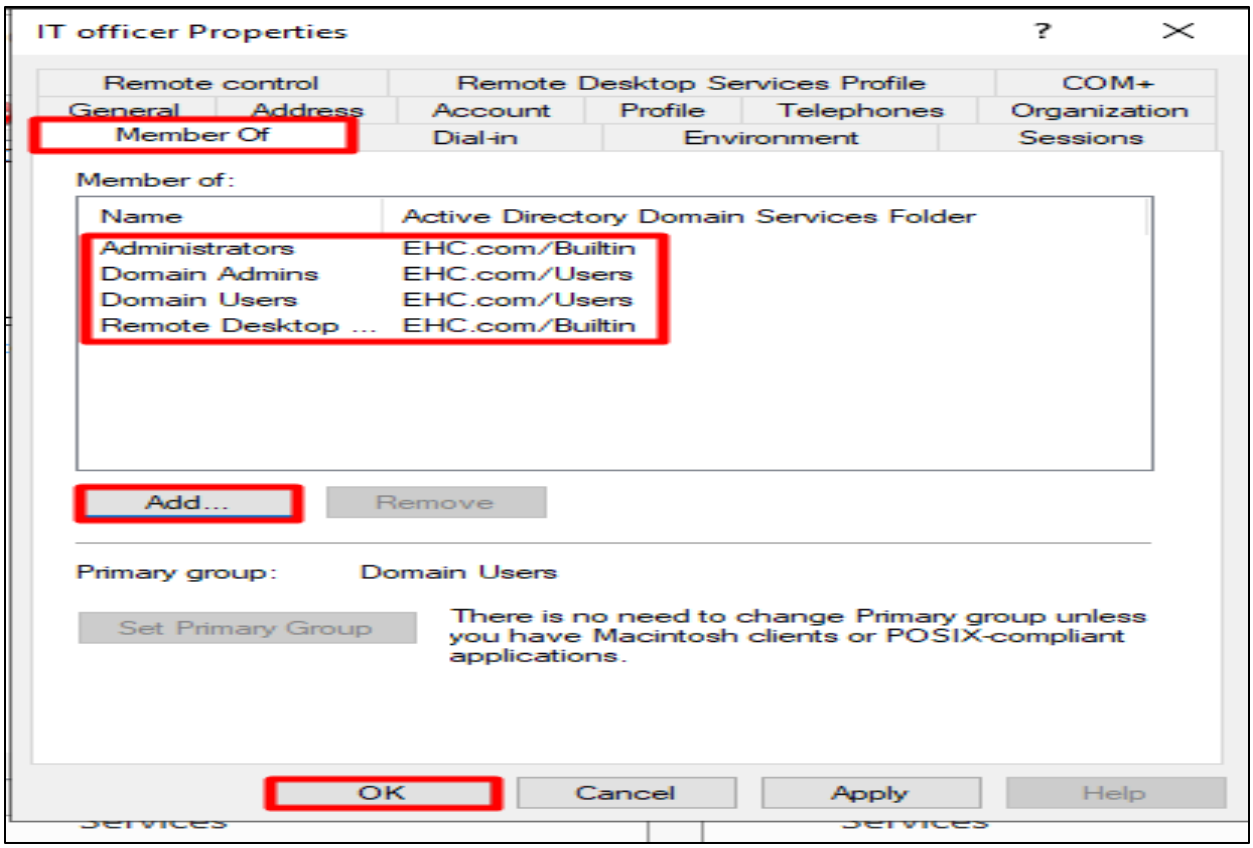


Figure 9 Providing all the administrative privileges to IT Officer user.

[Follow Appendix 7.4 for detailed steps.]

3.2.2. Installing and configuring web server.

As previous, another windows server 2019 is installed and configured as web server. Then, it is kept under EHC.com domain and official website was hosted.

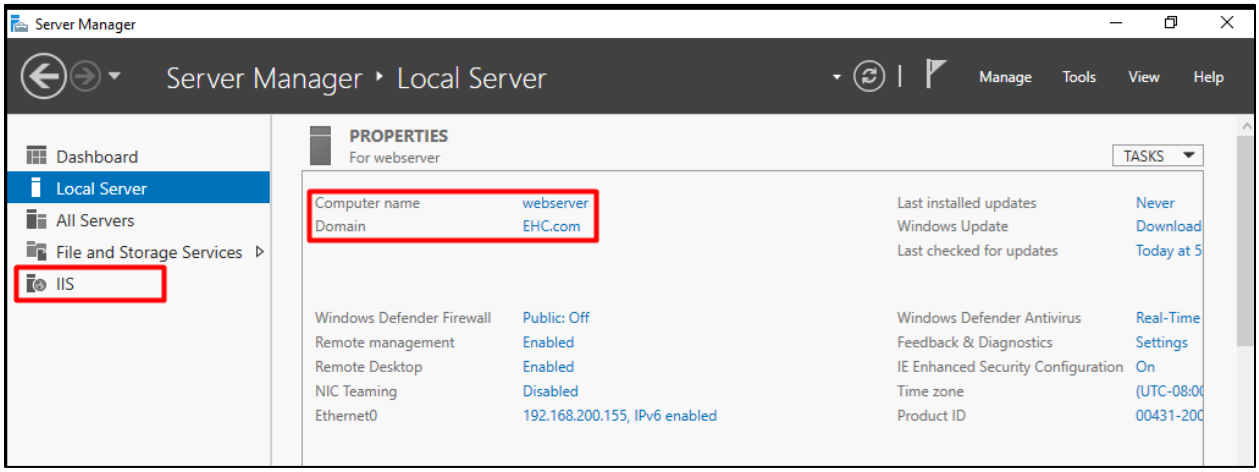


Figure 10 Configuring webserver and keeping it under domain EHC.com.

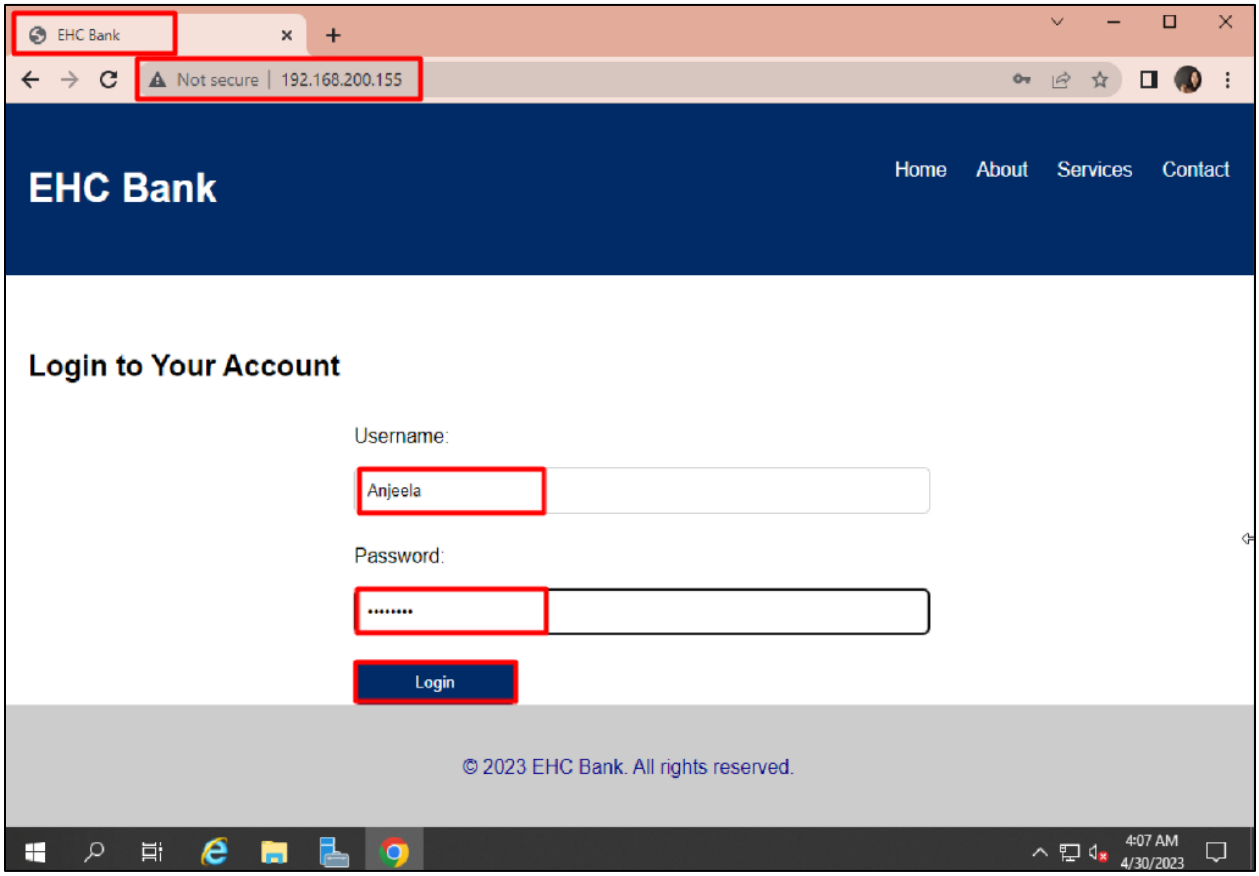


Figure 11 Sample website hosted on webserver.

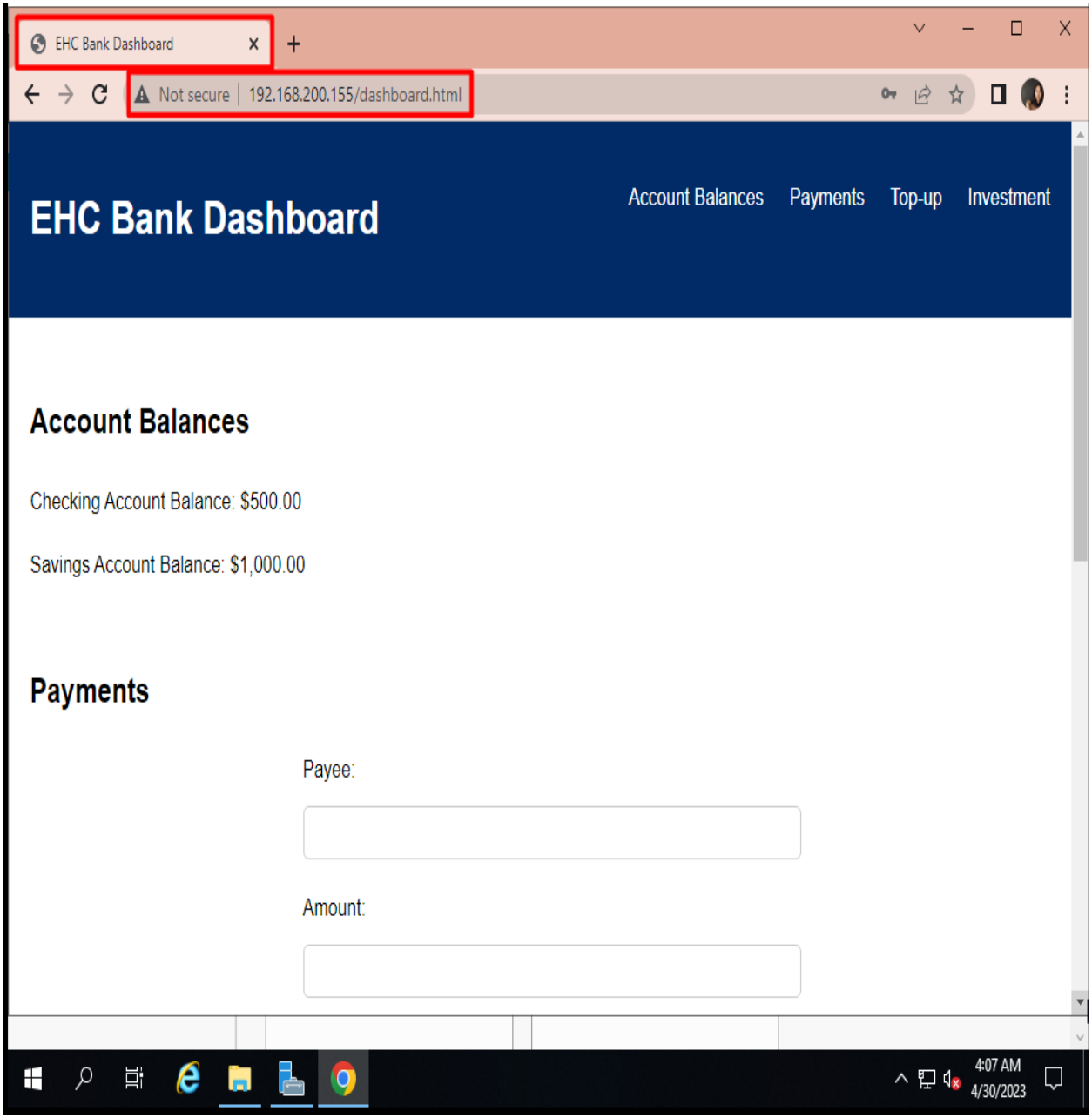


Figure 12 Sample dashboard interface that is shown after giving credentials.

Follow appendix 7.5. for detailed steps.

3.2.3. Installing and configuring windows 7 PC.

The windows 7 enterprise was installed and the PC is used as ITOfficer's PC of EHC bank which is the member of AD users.

Figure 13 Configuration of windows 7

Follow appendix 7.6. for detailed steps.

3.2.4. Creating an exe payload using Metasploit in Kali Linux.

For carrying out the attack, a update.exe payload is generated along with VNCinjection for backdoor remote access and control. The Metasploit is opened using msfconsole command.

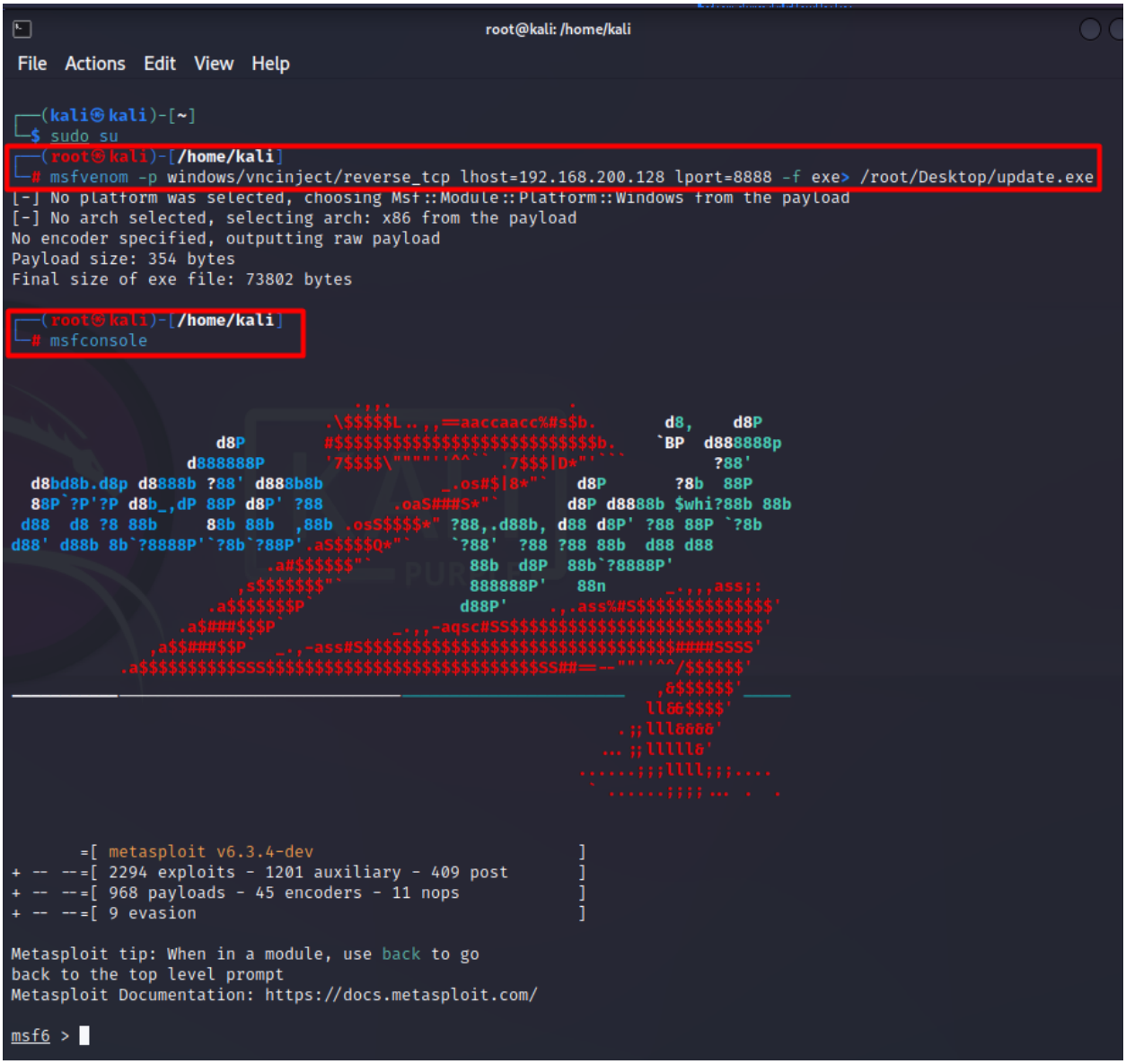


Figure 14 Creating payload.

Follow appendix 7.7. for detained steps.

3.2.5. Delivering the payload through a phishing mail.

To deliver the exe file to the IT officer's PC, social networking technique is used. Firstly, the payload was uploaded to the Mega drive. Then a fraud mail was sent to the victim along with the payload stored drive link. The victim was thus convinced about the fraud update mail and downloaded the file and executed it.

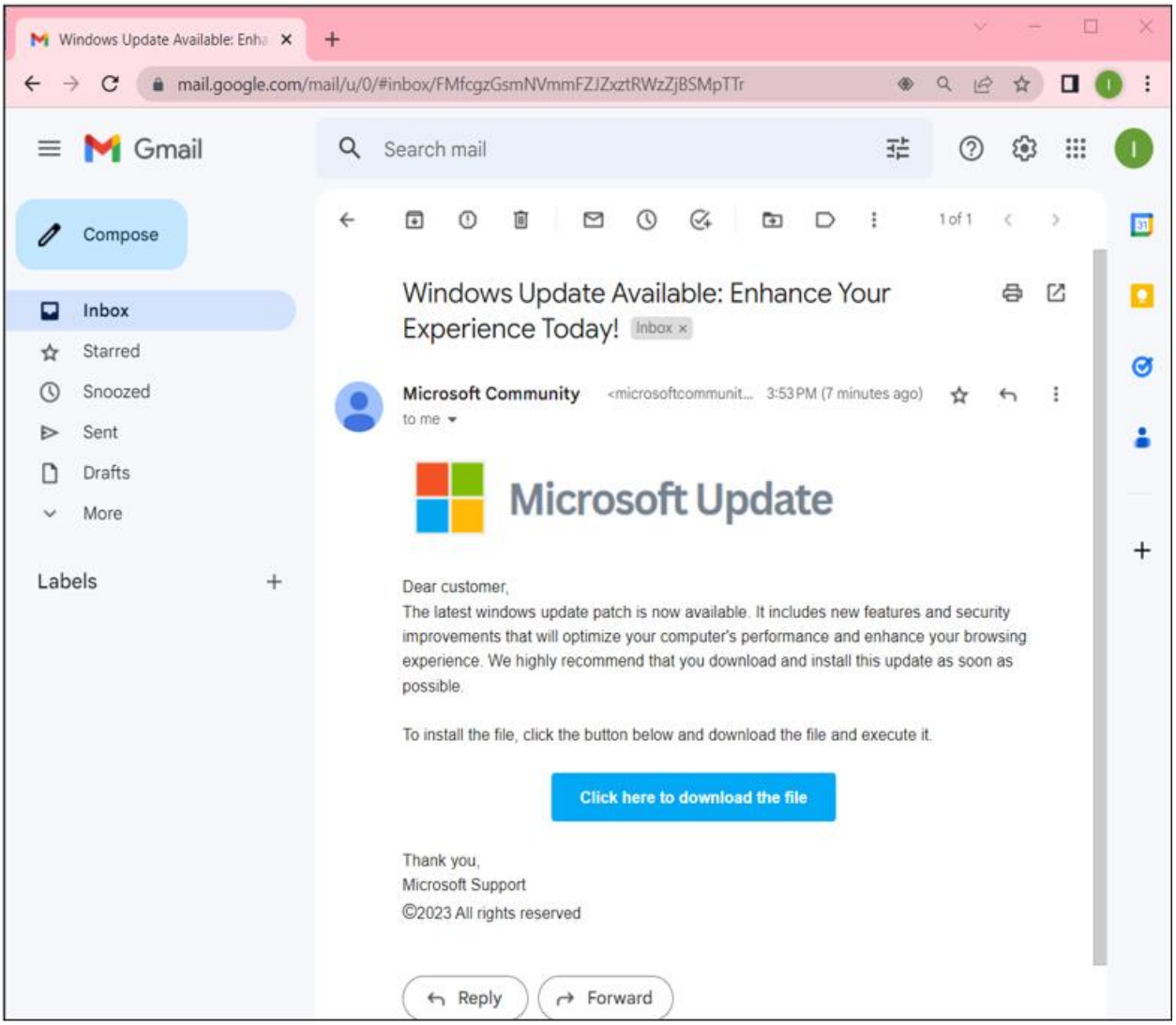


Figure 15 Victim getting fraud mail.

Follow appendix 7.8. for detailed steps

3.2.6. Accessing and controlling the IT officer's PC.

Since, the victim downloaded and executed the payload file, it was running in the background allowing backdoor access and control over the victim's system. The attacker remotely controlled the PC and opened the DC with remote desktop connection feature. Moreover, the attacker exploited the AD computers and found a web server. The attacker pings the webserver with command "ipconfig webserver" thus getting the IP address of the webserver. Then, the attacker remotely accessed the webserver and changed the html code of the website thus creating a fake website for users.

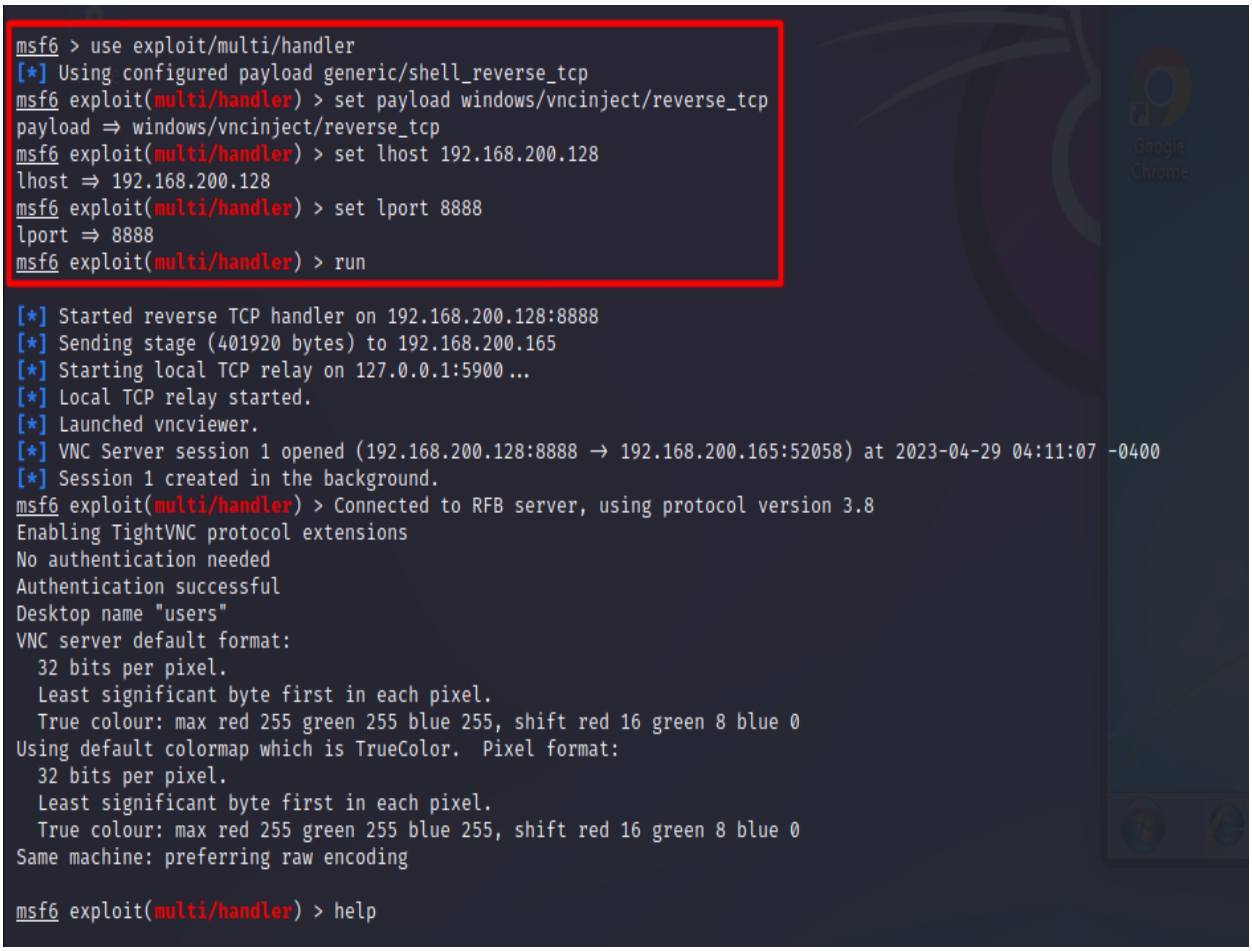


Figure 16 Attacker getting a vnc session for accessing and controlling the system.

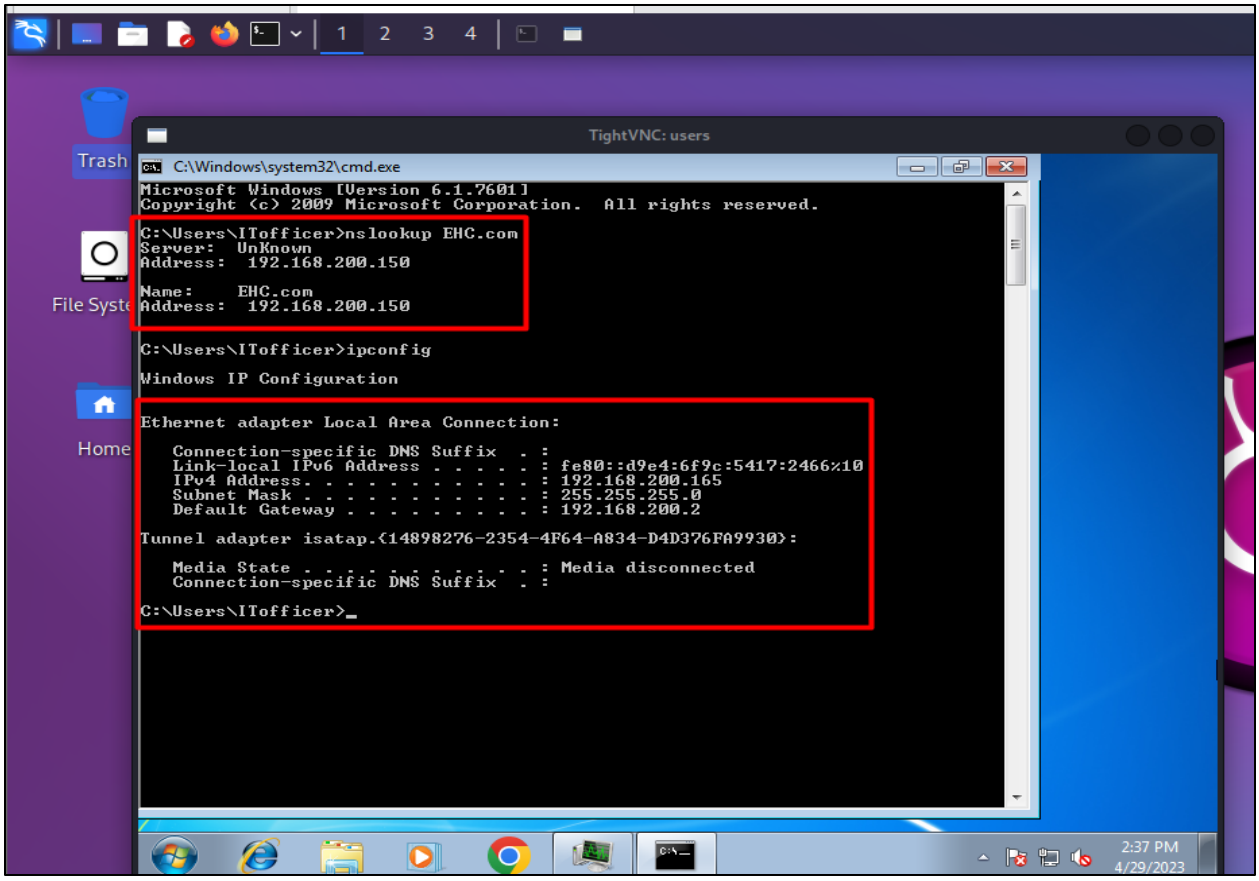


Figure 17 Attacker exploiting the victim's system.

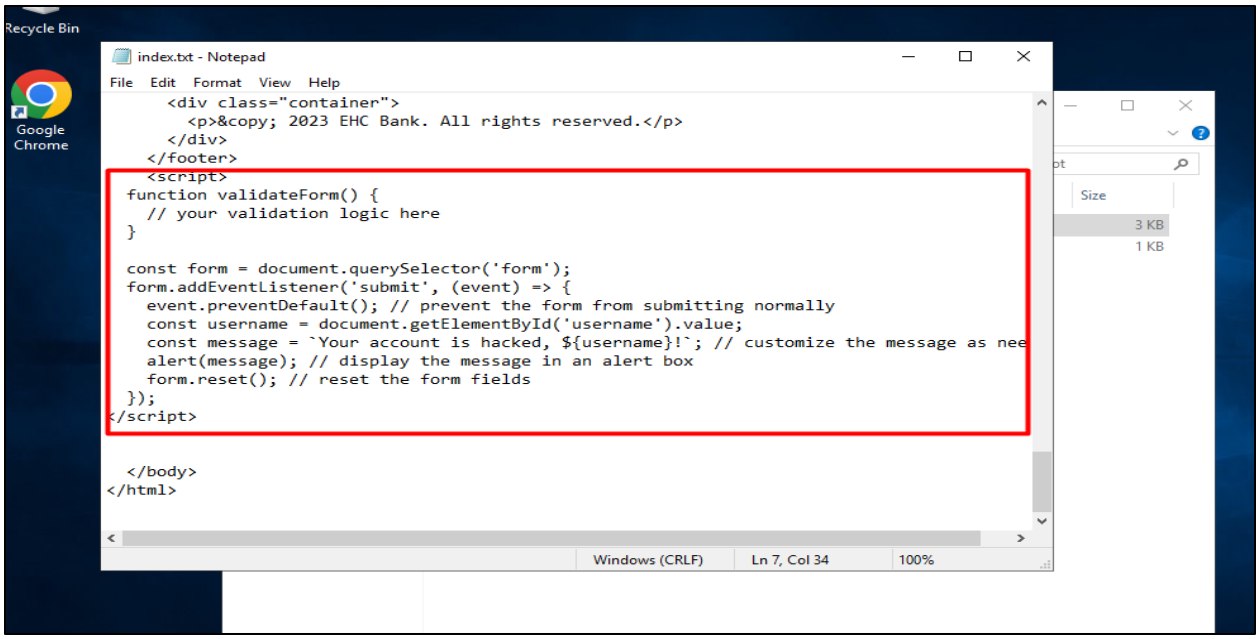


Figure 18 Victim customizing the official website's html file.

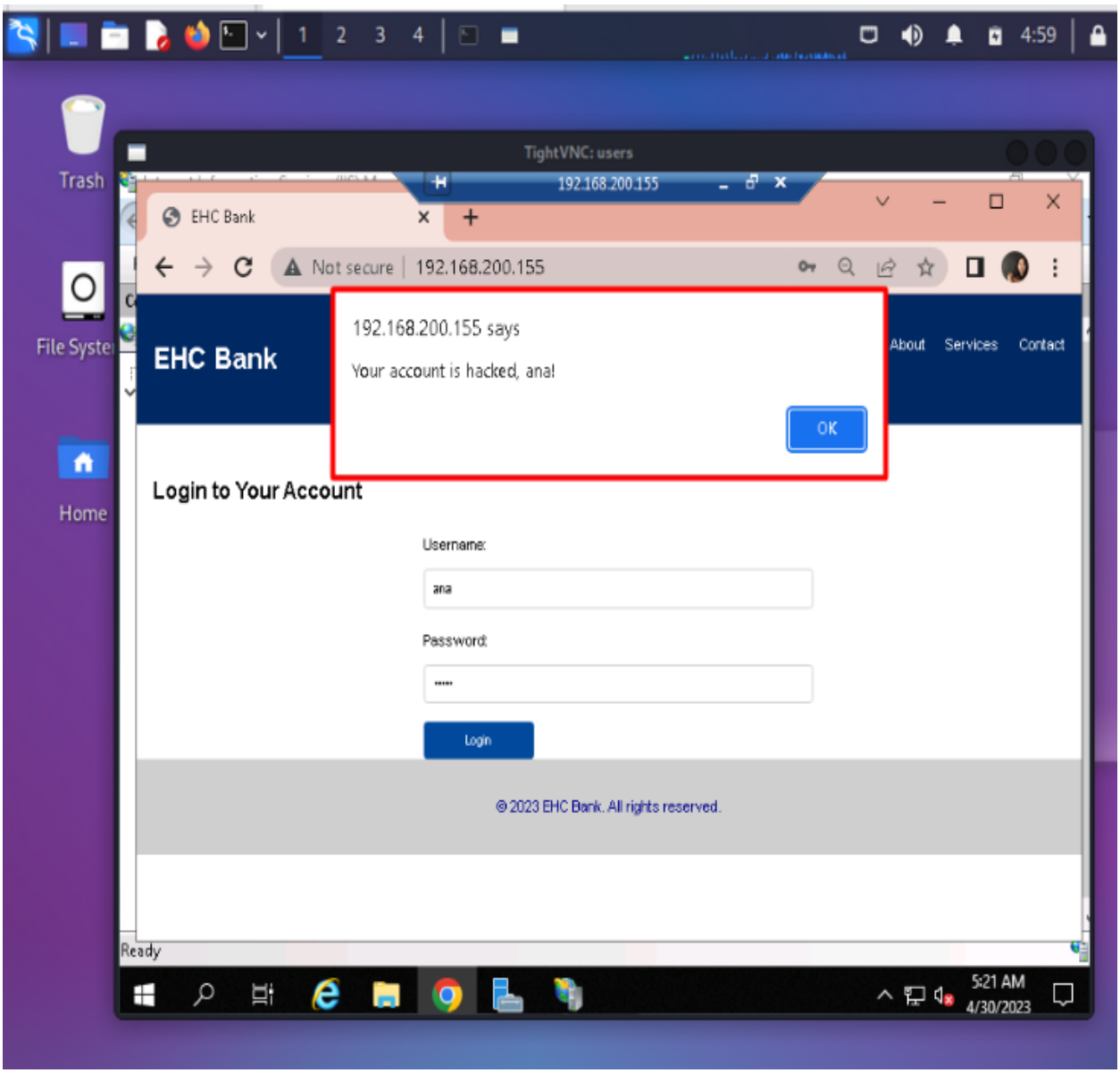


Figure 19 Fake website.

[Follow Appendix 7.9 for detailed steps.]

3.3. Recommendation and Awareness

Phishing and social engineering are annoying and difficult to detect. Since, an attacker just needs a response from a key individual to gain access to sensitive data or systems, the cooperation/organization should be vigilant about all the potential flaws and vulnerabilities in their system to avoid falling as a prey to phishing attacks. Moreover, some of the other recommendations that can be used to help people/organization to be safe from these types of attacks are given below,

- Educate employees about phishing and social engineering.
  Providing employees with training and awareness programs that cover topics such as what these attacks are, how to recognize them and real-world examples of attacks.

- Use anti-phishing tools and software's.
  Implement anti-phishing tools such as Symantec Email security that can detect and block the phishing emails.

- Verify email sender's identity.
  Check the email address and display name, look for digital signatures, verify the domain of the organization by contacting the official company's support team to confirm the legitimacy of the email.

- Conduct regular security audits.
  Regular security audits should be conducted to identify potential vulnerabilities and implement measures to address them.

- Keep the software and servers up to date with latest security patches.

- Install robust email firewalls to analyze incoming and outgoing email-server traffic based in specific set of rules and protocols.

4. Conclusion

4.1. Conclusion of the project

Phishing and social engineering risks have often got increasingly complicated and are now regarded as the deadliest and most significant security dangers that individuals and institutions face. These sorts of attacks can lead an organization to lose not just a large sum of money, but also goodwill and user's trust, which can be worth more than that money. In this report, a brief demonstration based on web server hijacking phishing was shown from which we can see how convenient it is to take over the company's system by targeting and exploiting the specific staff of the company. No matter how much investments or efforts an organization puts on the technical side of the security, at the end of the day everything depends upon interaction of the company's employee with it. Therefore, employee and user awareness is the best defense against phishing and social engineering attacks.

4.2. Legal, ethical, and social issues

Considering legal, ethical, and social issues is an essential aspect while working within a project/coursework that involves cyber-attack-demonstration. It is an imperative to take these issues into an account to avoid negative outcomes that may affect the report or its readers. To be precise, this is an educational report meant to be accomplished for the final year coursework of the module ethical hacking, conducted by Islington college; LMU. While demonstrating the attack, all the guidelines has been strictly adhered as mentioned by our module leader. Despite, there is no surprise that this type of attack comes with different consequences in the form of legal, ethical, and social issues which are briefed below,

4.2.1. Legal issues

Legal issues are caused by violating the laws and regulations of the country. In case of Nepal, legal issues regarding Computer and IT fields come under Nepal Electronic Act 2063. Some of the laws that may hinder/related with this demonstration are,

The Electronic Transaction Act, 2063 (2008) chapter 9 Article 45,46,47 states,

Follow Appendix 7.10. to read the article's statement.

4.2.2. Ethical issues

Ethical issues refer to the dilemma or problem created in people's moral philosophy or principal values. This demonstration has the potential to cause ethical harm to the individuals whose accounts are compromised. Attacker could violate the individual's privacy and exploit their personal information or official information which can have a detrimental impact on their emotional well-being. Unauthorized use of such information raises ethical issues related to autonomy and fairness(equality),

4.2.3. Social Issues

Social issues refer to the problems that is not illegal but affects the society or the perceptions created in the society. If an organization is compromised, it can lead to the exposure of sensitive user data, which can be used for further attacks, causing distress and negative social impact. The spread of misinformation and distrust in institutions can also occur, which can have long-lasting effects on society.. Such attacks can create unforgettable fear and negative perceptions among the people in the society.

5. References

Afreen, S., 2023. *VMware Workstation: Everything You Need to Know.* [Online] Available at: https://www.simplilearn.com/tutorials/cloud-computing-tutorial/vmware-workstation
[Accessed 30 04 2023].

Ahola, M., 2023. *The 8 types of phishing attack that could target your business.* [Online] Available at: https://blog.usecure.io/types-of-phishing-attack
[Accessed 01 05 2023].

Bhardwaj, R., 2023. *Spear Phishing Attack: Cyber Security.* [Online] Available at: https://ipwithease.com/spear-phishing-attack-cyber-security/
[Accessed 01 05 2023].

Buckbee, M., 2022. *What is Metasploit? The Beginner's Guide.* [Online] Available at: https://www.varonis.com/blog/what-is-metasploit
[Accessed 30 04 2023].

Chin, K., 2023. *19 Most Common Types of Phishing Attacks in 2023.* [Online] Available at: https://www.upguard.com/blog/types-of-phishing-attacks
[Accessed 01 05 2023].

Cloudfare, 2023. *What is a phishing attack?.* [Online] Available at: https://www.cloudflare.com/learning/access-management/phishing-attack/
[Accessed 30 04 2023].

Cook, S., 2023. *Phising statistics and facts for 2019–2023.* [Online] Available at: https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/
[Accessed 30 04 2023].

Fan, W., Lwakatare, K. & Rong, R., 2017. *Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigation..* [Online] Available at: https://oa.upm.es/45395/1/Social%20Engineering-IJCNIS-V9-N1-1.pdf
[Accessed 01 05 2023].

imperva, 2023. *Phishing attacks.* [Online] Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/ [Accessed 01 05 2023].

Jena, B. K., 2022. *What Does Kali Linux Mean?.* [Online] Available at: https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-kali-linux [Accessed 30 04 2023].

lawcommision, 2008. [Online] Available at: https://www.lawcommission.gov.np/en/wp-content/uploads/2018/10/electronic-transaction-act-2063-2008.pdf [Accessed 01 05 2023].

Metasploit, 2023. *Metasploit modules.* [Online] Available at: https://docs.metasploit.com/docs/modules.html [Accessed 01 05 2023].

MohanaKhrishan, R., 2021. *What Is a Spear Phishing Attack? Definition, Process, and Prevention Best Practices.* [Online] Available at: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-spear-phishing-attack/ [Accessed 01 05 2023].

Neagu, C., 2023. *What Is Ethical Hacking? An Introduction to the Concept.* [Online] Available at: https://heimdalsecurity.com/blog/ethical-hacking/ [Accessed 25 04 2023].

Rosencrance, L., 2023. *social engineering.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/social-engineering [Accessed 30 04 2023].

Sheldon, R., 2023. *vishing (voice or VoIP phishing).* [Online] Available at: https://www.techtarget.com/searchunifiedcommunications/definition/vishing [Accessed 01 05 2023].

Stansfield, T., 2023. *Q1 2023 Phishing and Malware Report: Phishing Increases 102% QoQ.* [Online]
Available at: https://www.vadesecure.com/en/blog/q1-2023-phishing-and-malware-report-phishing-increases-102-qoq
[Accessed 30 04 2023].

Stenger, B., 2021. *What Is Windows Server and How Is It Different From Windows?.* [Online]
Available at: https://www.makeuseof.com/tag/windows-server-different-windows/
[Accessed 30 04 2023].

Thomas, P., 2021. *Metasploit, History and Usage.* [Online]
Available at: https://hackwarenews.com/metasploit-history-and-usage/
[Accessed 01 05 2023].

Toulas, B., 2022. *Hackers target Russian govt with fake Windows updates pushing RATs.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/hackers-target-russian-govt-with-fake-windows-updates-pushing-rats/
[Accessed 01 05 2023].

Website security store, 2021. *What is social engineering.* [Online]
Available at: https://websitesecuritystore.com/blog/what-is-social-engineering-attack/
[Accessed 01 05 2023].

6.Bibliography

COOPER, S., 2022. *Remote Access Trojans Explained plus 11 Best RAT Software, Scanners, & Detection Tools.* [Online] Available at: https://www.comparitech.com/net-admin/remote-access-trojan-rat/ [Accessed 01 05 2023].

Jefferson, B., 2023. *15 Common Types of Cyber Attacks and How to Mitigate Them.* [Online]
Available at: https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/ [Accessed 01 05 2023].

Rani, S., 2019. PENETRATION TESTING USING METASPLOIT FRAMEWORK: ANETHICAL APPROACH. *International Research Journal of Engineering and Technology (IRJET),* 6(8), pp. 538-532.

Rao, T. V. N. & Shravan, V., 2019. Metasploit Unleashed Tool for Penetration Testing. *International Journal on Recent and innovation Trends in Computing and communication,* 7(4), pp. 16-20.

webroot, 2023. *Email Phishing, Vishing & Other Types of Attacks.* [Online] Available at: https://www.webroot.com/us/en/resources/tips-articles/what-is-phishing [Accessed 01 05 2023].

Yasar, K., 2023. *RAT (Remote Access Trojan).* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan
[Accessed 01 05 2023].

Z, A. K., 2019. A Study on Metasploit Payloads. *International Journal of Cyber-security and Digital Forensics.,* 8(4), pp. 298-307.

7. Appendix

7.1. Types of phishing attack

There are different types of phishing attacks. Sime of the common phishing attacks are briefed below,

- **Email phishing**

  Email phishing is the most common type of phishing attack, where an attacker sends a fake email that looks like its from a legitimate source such as bank, online retailer, or social media platform. The email often includes a link or attachment that, if clicked, takes the victim to a phony website or installs malicious software on their device (imperva, 2023).

- **Spear phishing**

  Spear phishing is a targeted attack where the attacker sends phishing messaged to specific individuals or groups often with a high level of personalization and customization, tricking them into revealing sensitive information or installing malware. The attack is more sophisticated and harder to detect as it is tailored to the interests and characteristics of the targeted individuals, using publicly available information. It is one of the common tactics used by cybercriminals and state-sponsored actors to gain access to sensitive information system (MohanaKhrishan, 2021).

- **Smishing**

  Smishing is a form of phishing that involves sending fraudulent text messages to trick victim into providing sensitive information or clicking on links. Attackers may pretend to be a trusted source and use urgency or rewards to convince the victim to act quickly. These messaged often contain links to fake websites or ask for personal information that can be used for malicious purposes (Chin, 2023).

- **Vishing**

  Vishing is a form of phishing attack where the attacker uses phone calls or voice messages to deceive victims into sharing confidential information such as their credit card details or login credentials. The attacker often pretends to be a trustworthy entity, such as a bank or a government agency, and may manipulate the caller ID to appear authentic (Sheldon, 2023).

- **Clone phishing**

  Clone phishing is a phishing technique where the attacker replicates a genuine email or website and deceives the victim into sharing confidential information. By using stolen credentials, the attacker creates a replica that appears genuine to the victim, leading them to share sensitive information, such as login credentials or financial data. The main objective of clone phishing attacks is to exploit the trust of the victim in the legitimate source to gain access to confidential information (Ahola, 2023).

7.2. About Metasploit

Metasploit was created and conceived by HD More during his working period. He realized that much of his time was spent in confirming and sainting the public exploit code. Thus, in Oct 2003, he published his first version of Perl-based Metasploit having eleven exploits. Later, with the help of Spoon HD and Metasploit team, Metasploit 2.0 in April 2004 and Metasploit 3.0 in April 2007 were released. The 3.0 Metasploit was written in Ruby Programming Language (Thomas, 2021).

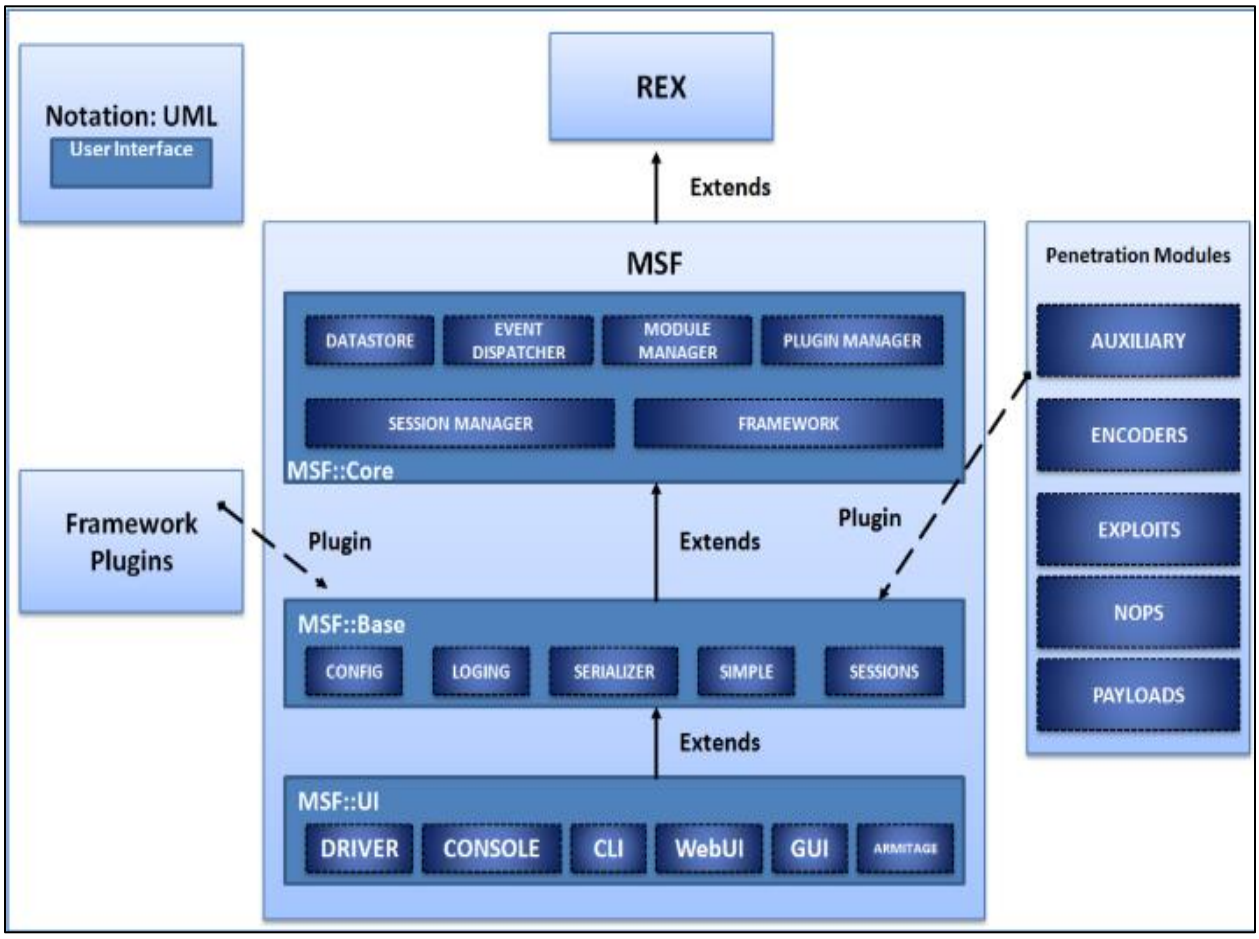


Figure 20 Metasploit Framework.

The meterpreter is the core of the Metasploit framework. Meterpreter is an advanced payload that can be used to remotely control a compromised system. The meterpreter supplies numerous features including ability to run arbitrary commands, transfer files, and access the victim's webcam and microphone. There are different libraries and components in this framework and are given below,

- **MSF core**

  It refers to the core libraries and includes the exploitation engine, meterpreter payload, the database and other core components necessary for the operation of the framework.

- **MSF Base**

  It is the set of modules and tools, including exploit modules, payloads, auxiliary modules, and other components used in penetration testing. The different modules used in this framework are:

  - **Exploit modules.**

    These are scripts that exploit a specific vulnerability in the victim's system.
  - **Auxiliary modules**

    These are the tools that perform a variety of tasks such as scanning for vulnerabilities, sniffing network traffic, or creating a DDOS attack.
  - **Payloads**

    A payload is a piece of code i.e., delivered to a target system as a part of an exploit. They are used for various purposes such as creating reverse shell, spawning a command prompt, or installing a rootkit.
  - **Encoders**

    They are used to encode payloads in order to bypass antivirus and intrusion detection systems.
  - **NOP generators**

    These tools are used to generate "no-operation" (NOP) sled, which aligns payloads in memory in preparation for an exploitation attempt.

- **MSF UI**

  It refers to the user interface of the framework. It includes the CLI as well as GUIs that are available for framework.

7.3. Reconnaissance phase

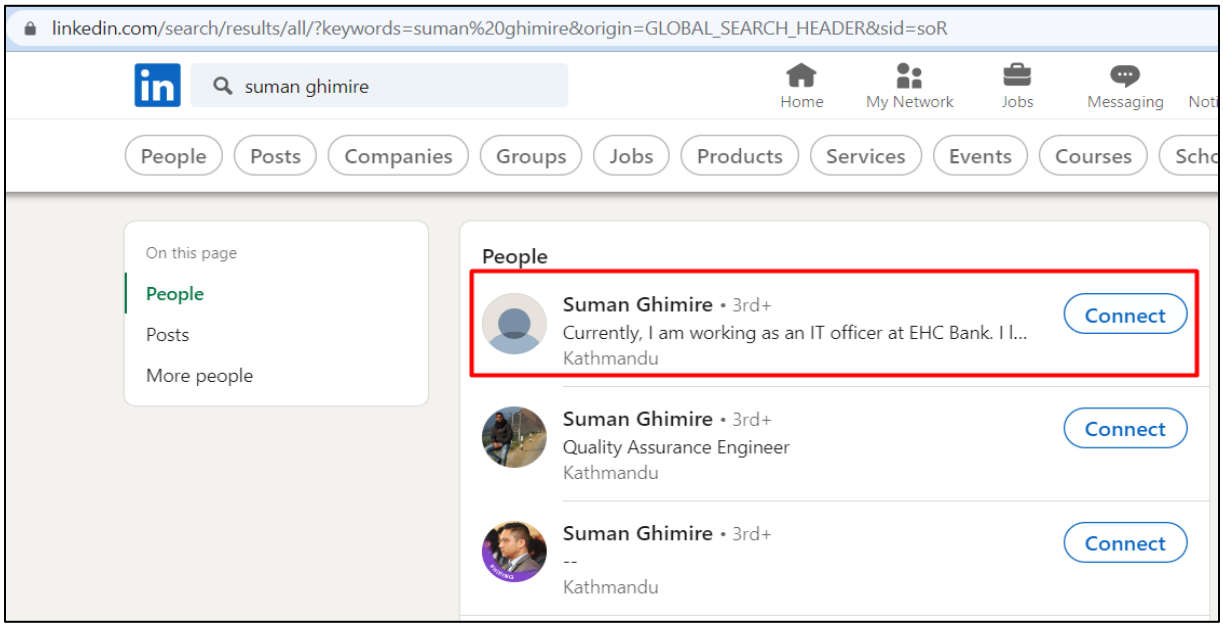


Figure 21 Attacker found the linkedin account of the IT officer of EHC bank.

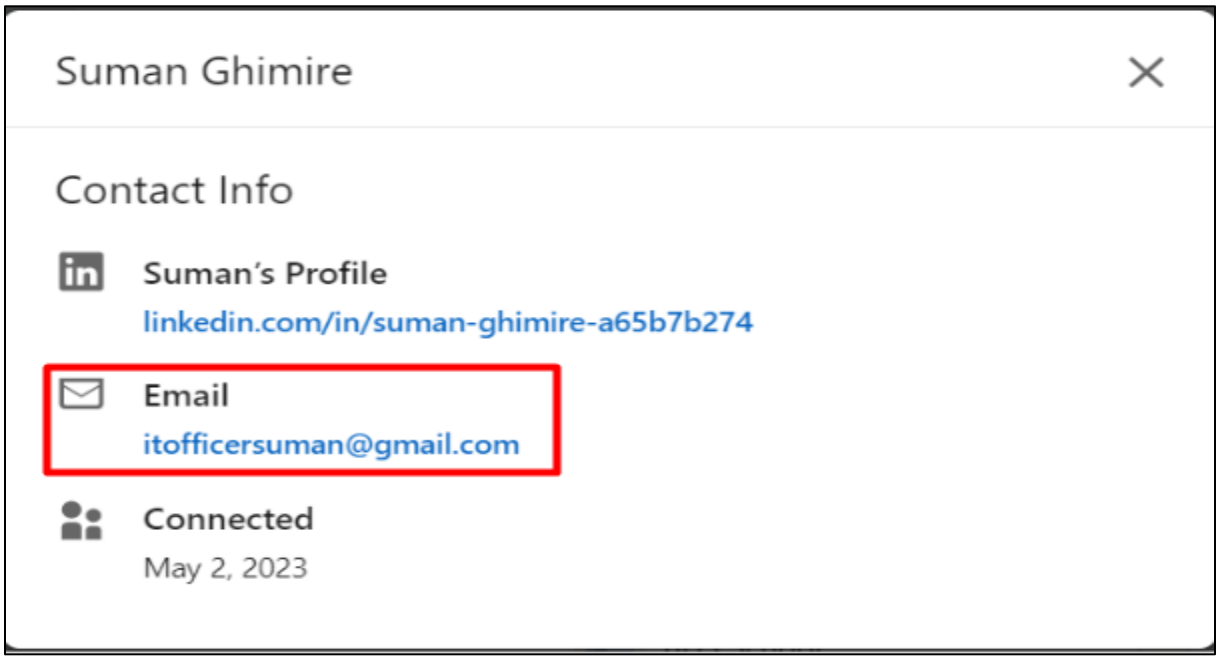


Figure 22 Attacker got the official Gmail account of the IT officer.

7.4. Installing and configuring domain controller.

- At first the IP address of the network is checked using command “ipconfig”.

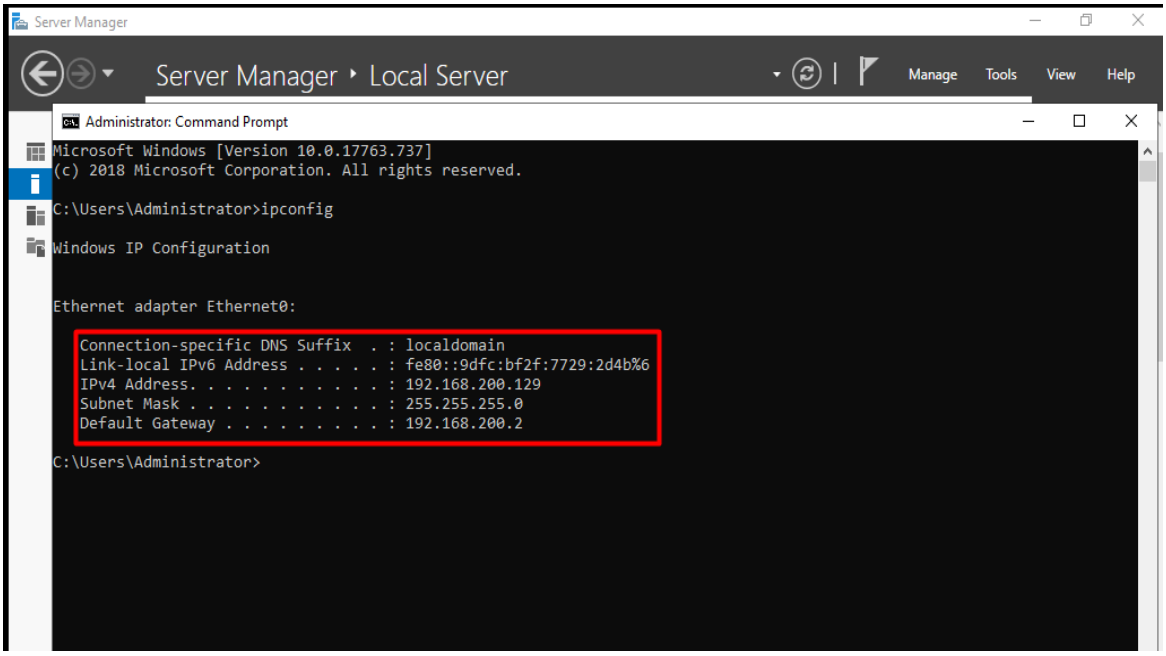


Figure 23 Checking IP address pf the network.

- The name of the server is changed to “DC” (Domain Controller) and is kept in a workgroup as shown in figure below,

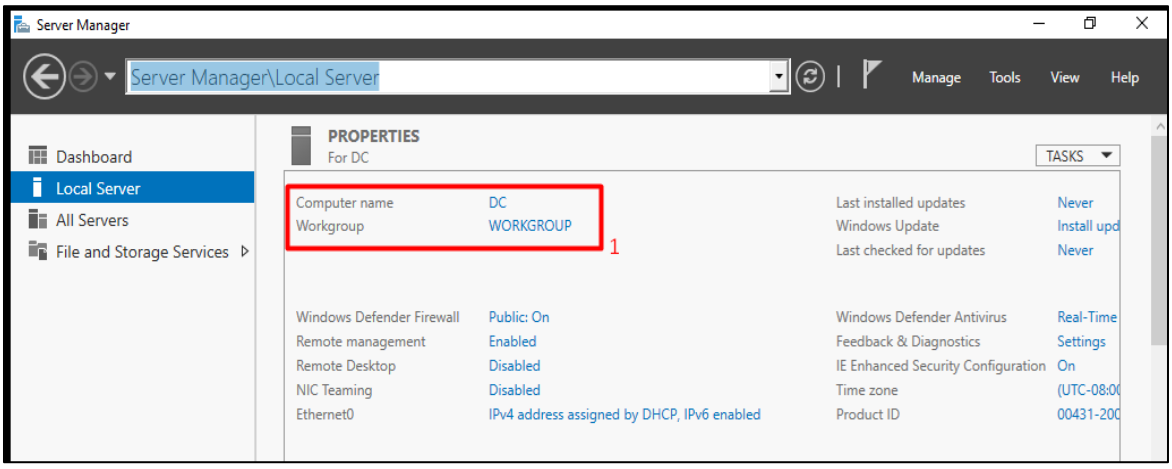


Figure 24 Changing the name of the server.

- Static IP address, default gateway and DNS is assigned as shown in the figure below,

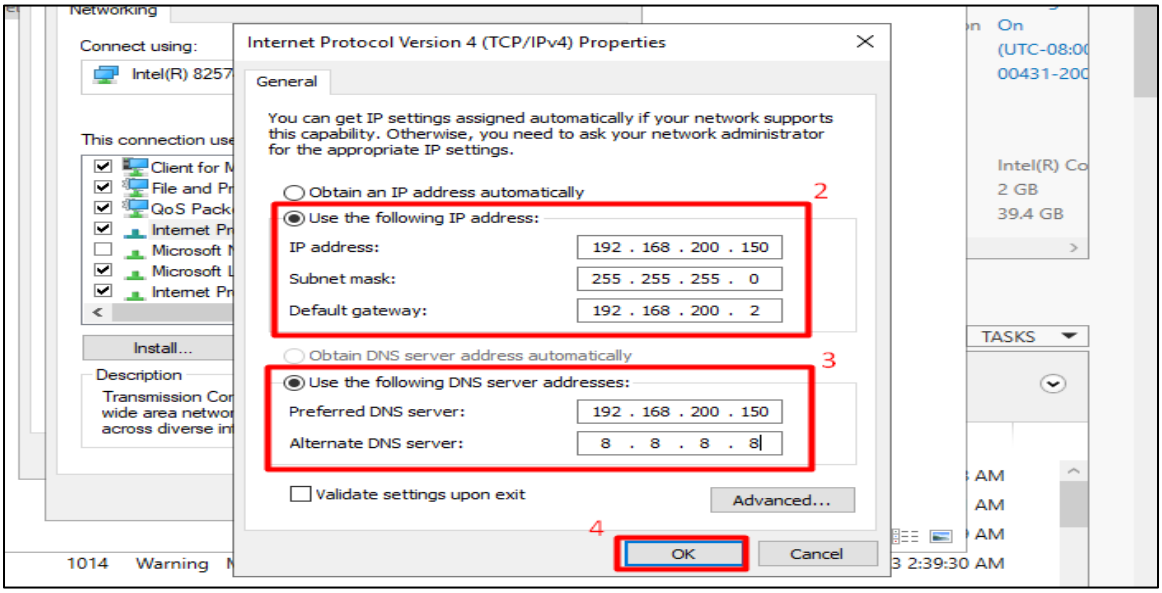


Figure 25 Assigning static IP address, default gateway and DNS.

- The active directory services role is added for further configuration.

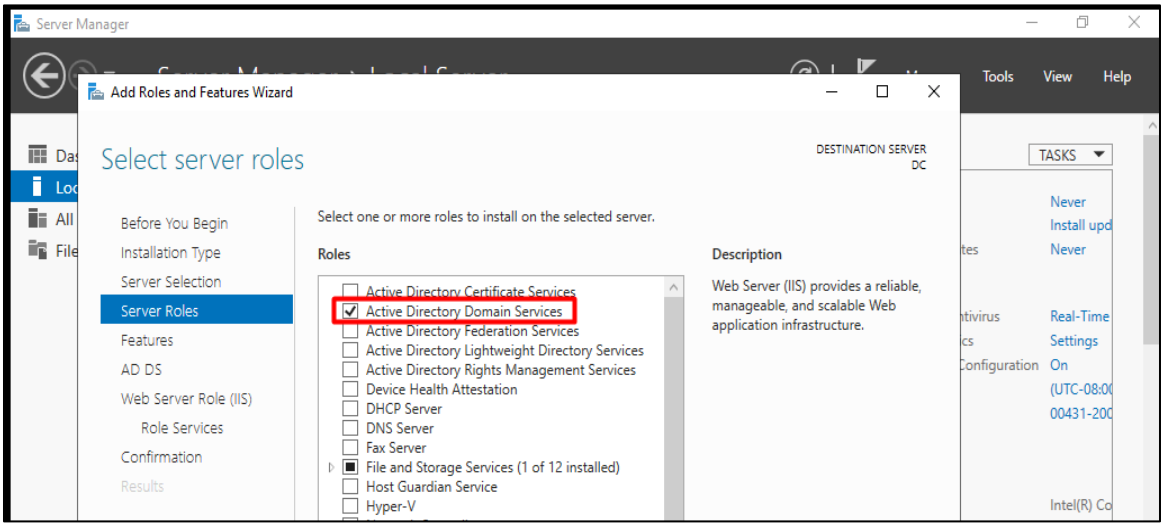


Figure 26 Adding AD services role.

- After addition of the ADDS role, the servier is promoted to domain controller by creating a new forest as “EHC.com”

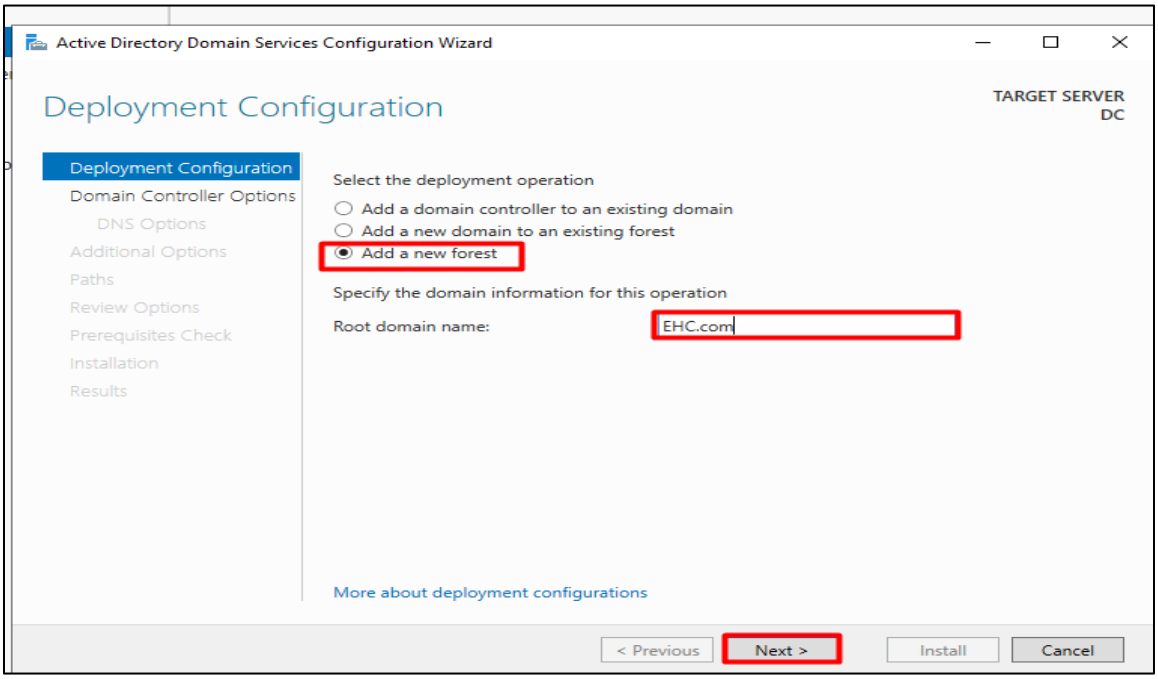


Figure 27 Adding a new forest.

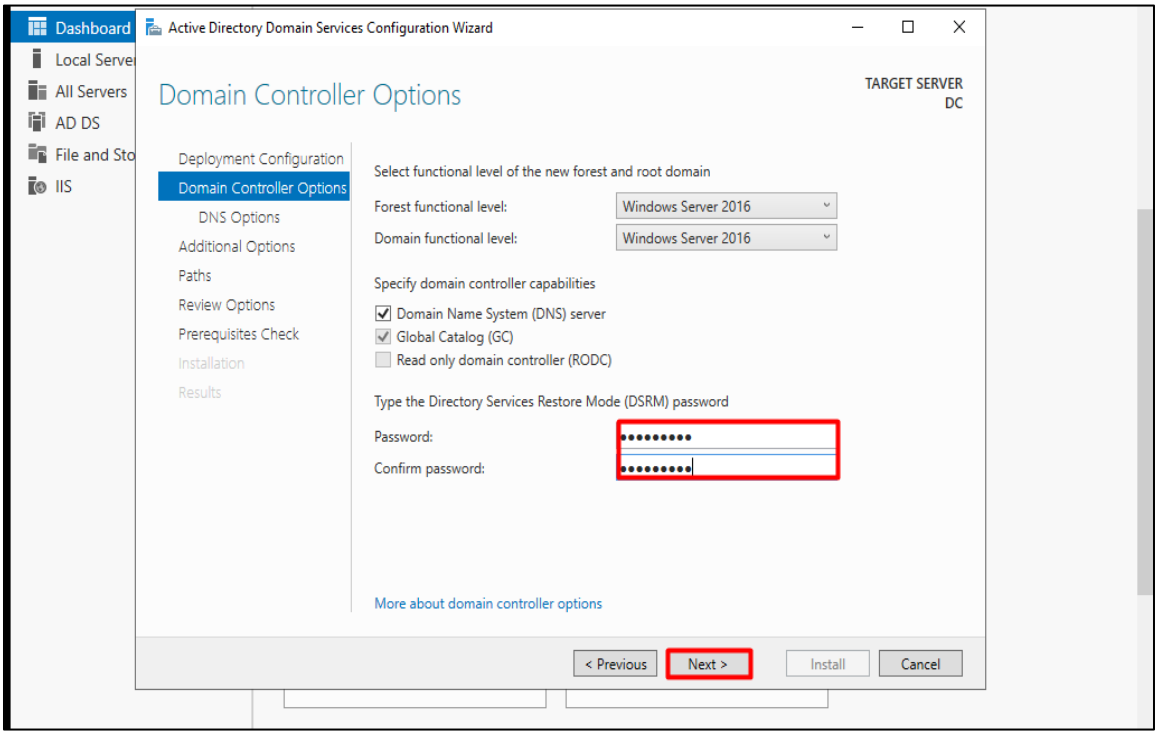


Figure 28 Giving credentials to access the new forest.

- Finally, the domain controller is configured.

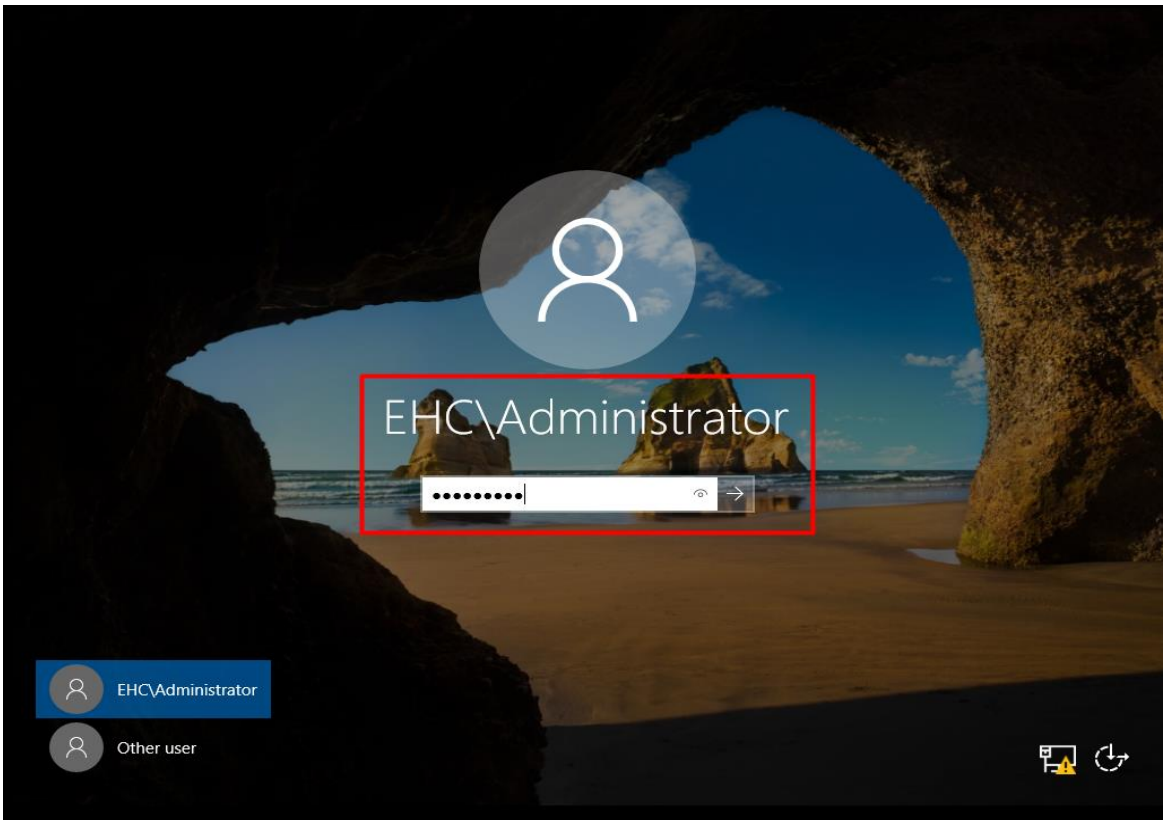


Figure 29 Domain controller of EHC Bank.

- Adding a user “IT officer” in active directory users list.

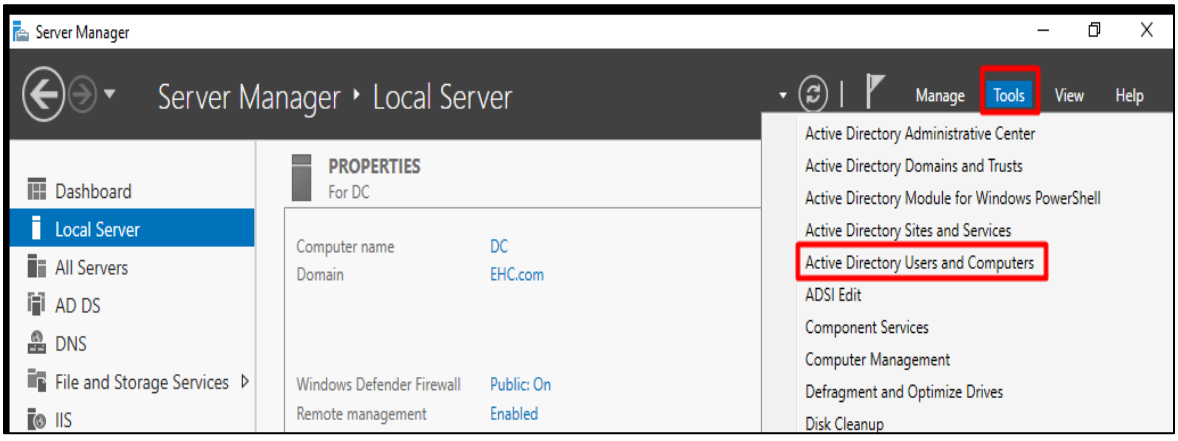


Figure 30 Selecting AD users and computers tool to create a user.

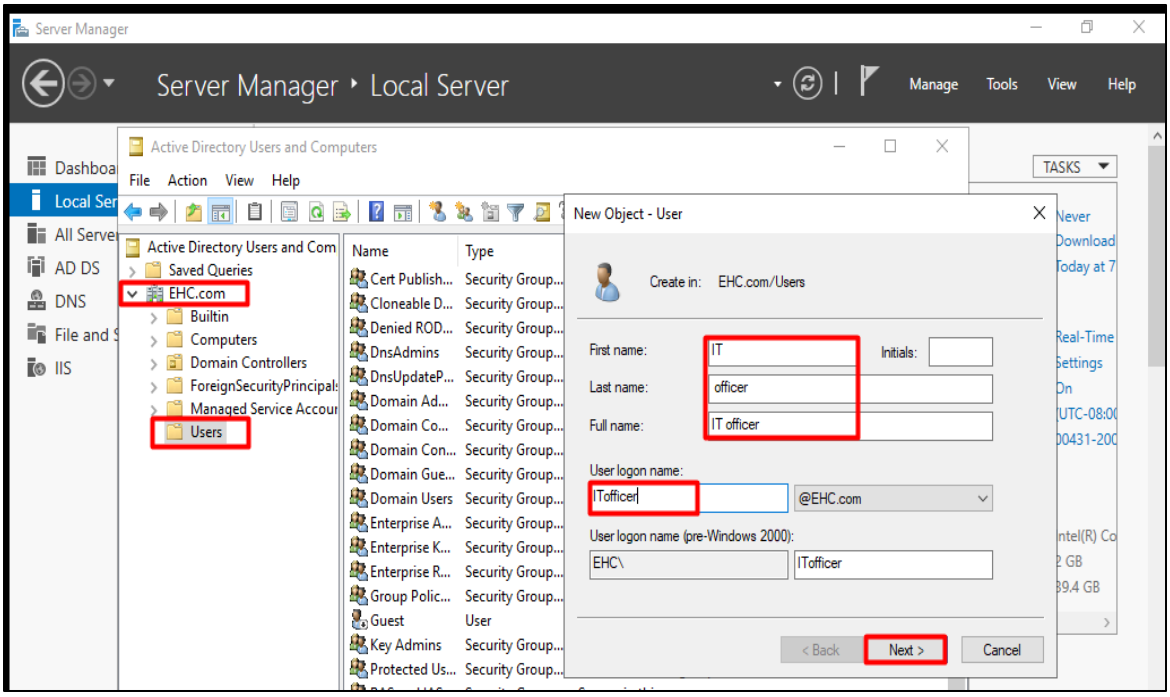


Figure 31 Created user named "ITofficer".

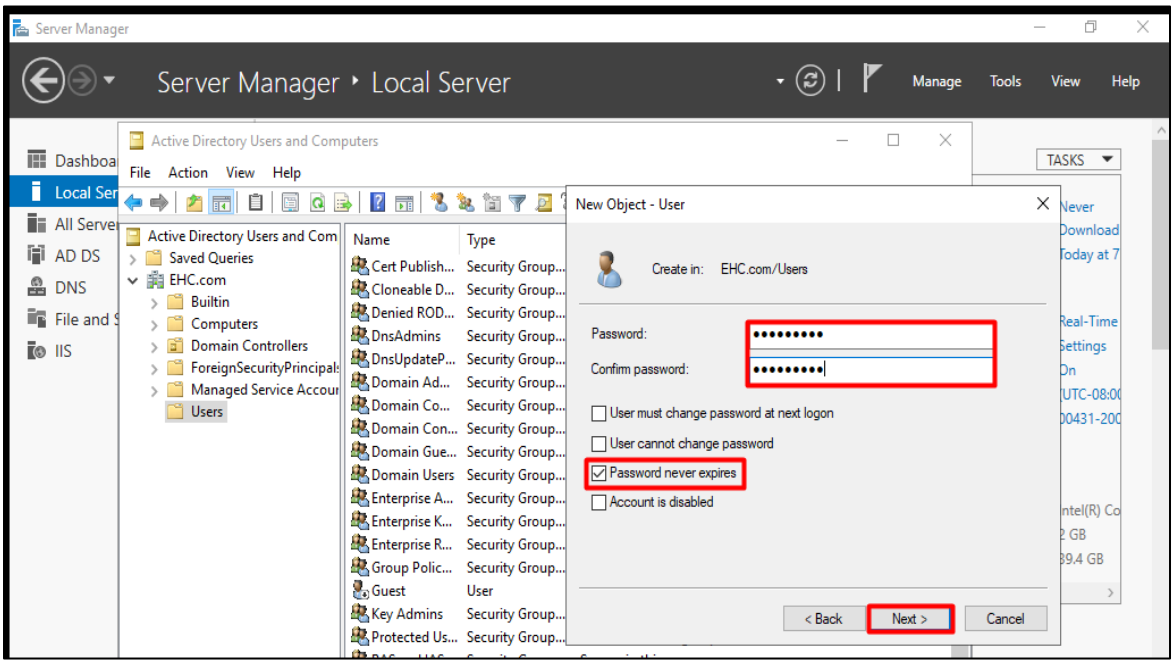


Figure 32 Setting credential for the user.

- Providing all the administrative privileges to the ITofficer.

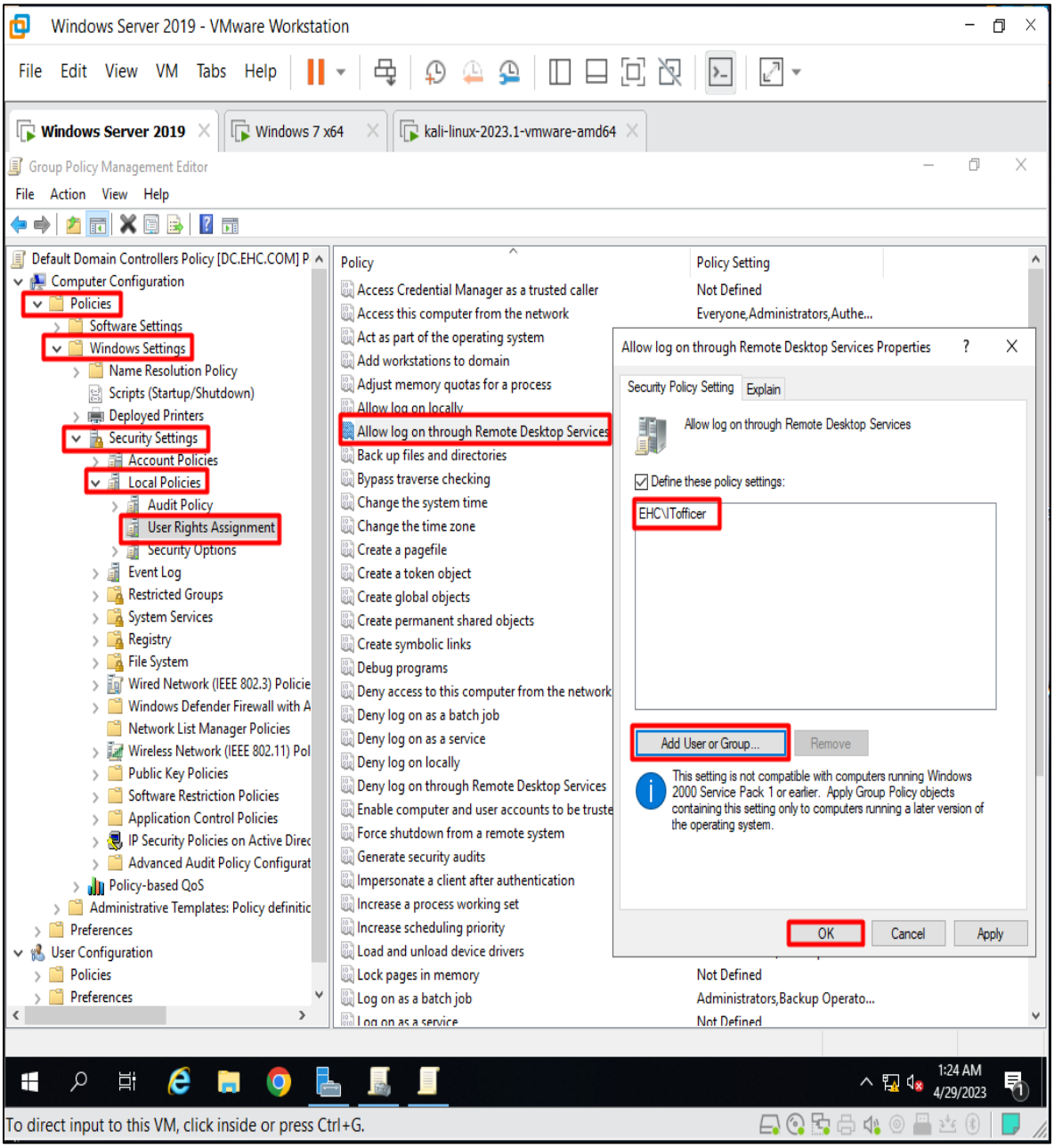


Figure 33 Configuration to allow remote desktop connection and control to ITofficer.

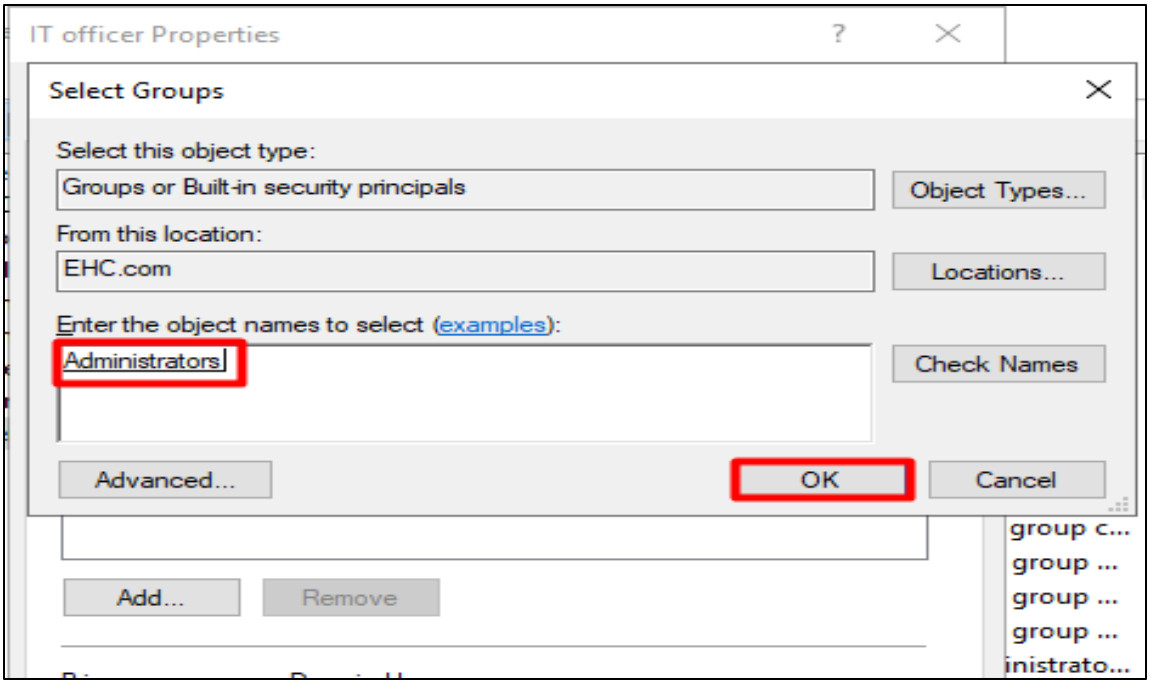


Figure 34 Adding the user to administrator group.

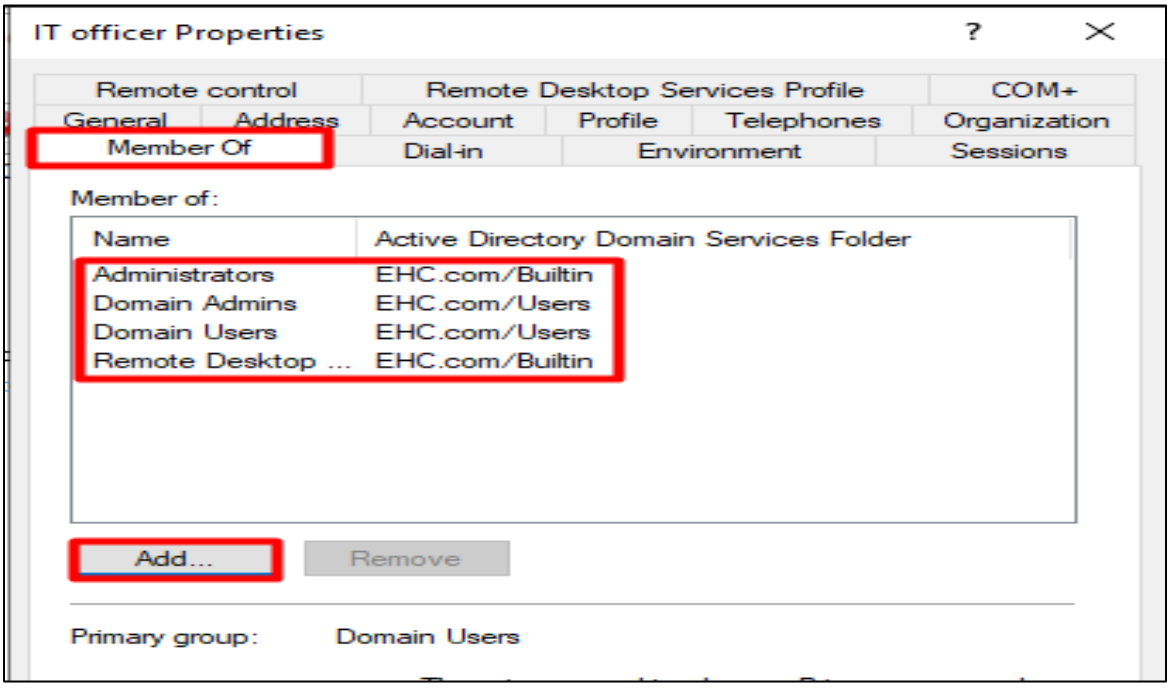


Figure 35 ITofficer having all the admin privileges.

7.5. Installing and configuring webserver.

- Firstly, the we server was installed in VMware and the static IP address and DNS are assigned and the name of the server was changed to “webserver” as shown in figure below,

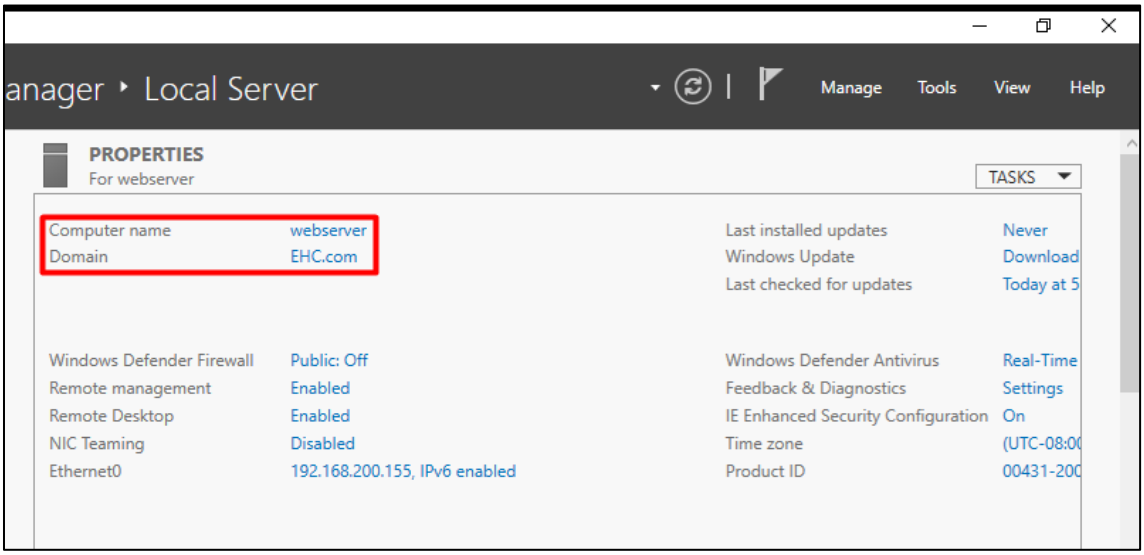


Figure 36 Changing the name of the server and assigning static IP address.

- Then the default website and default html pages are deleted. The path for the default html pages was “C drive/inetpub/wwwroot”. Then, new txt files named “index.txt” and “dashboard.txt” were created and filled with simple html codes for a sample bank HTML page. Additionally, a simple CSS code was also written and saved as style.css to present simple layout of the webpage.

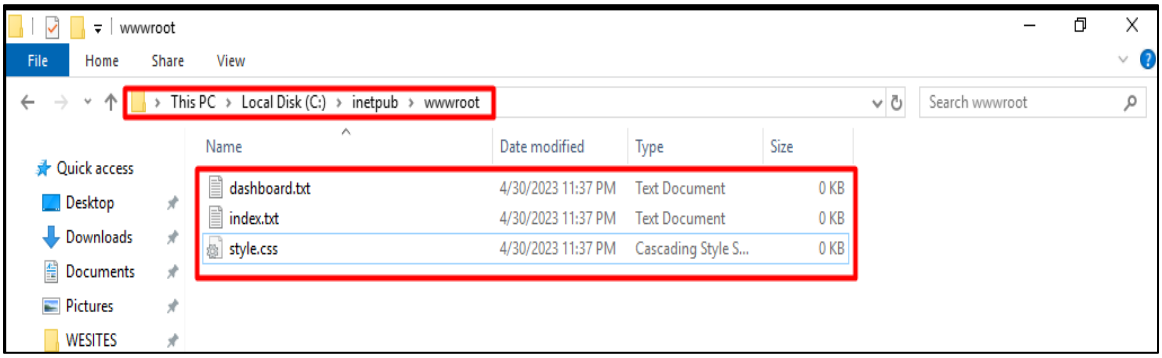


Figure 37 creating txt and CSS file.

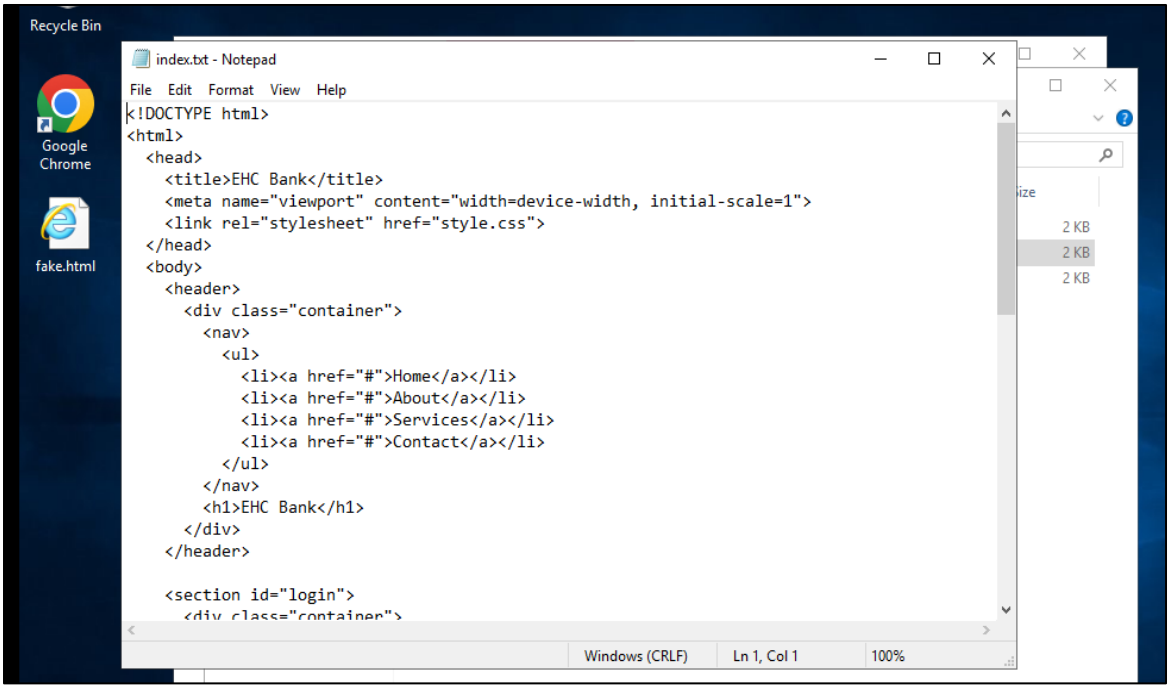


Figure 38 Adding html code in the index.txt file.

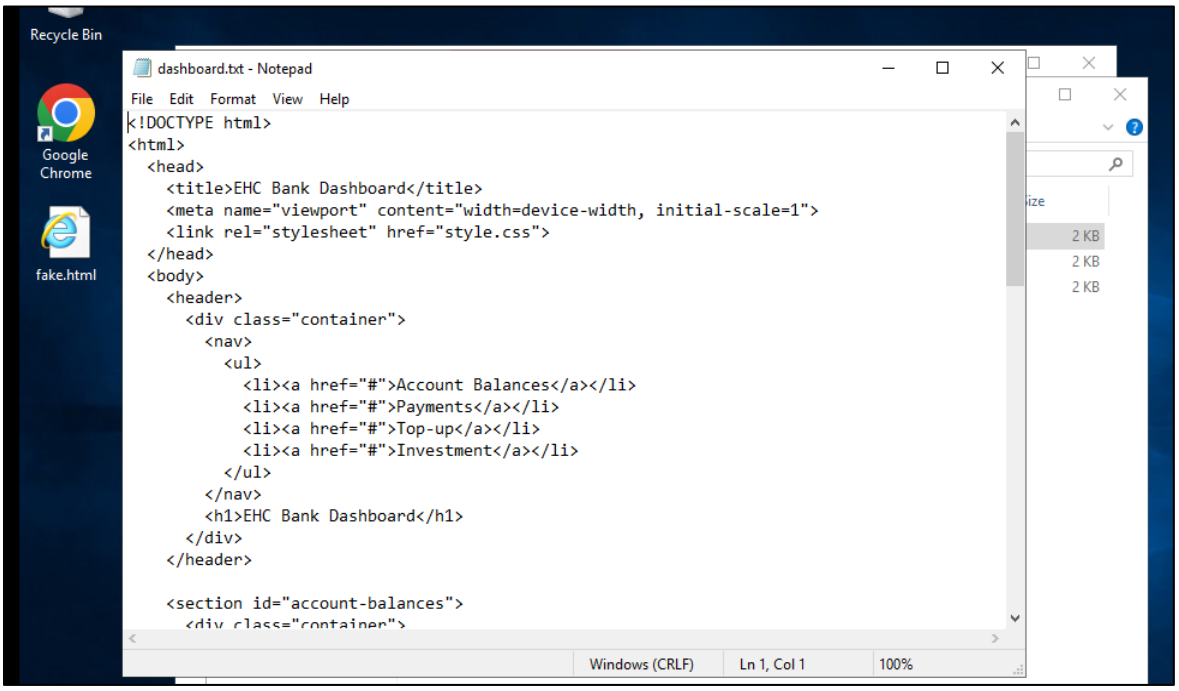


Figure 39 Adding html code in the dashboard.txt file.

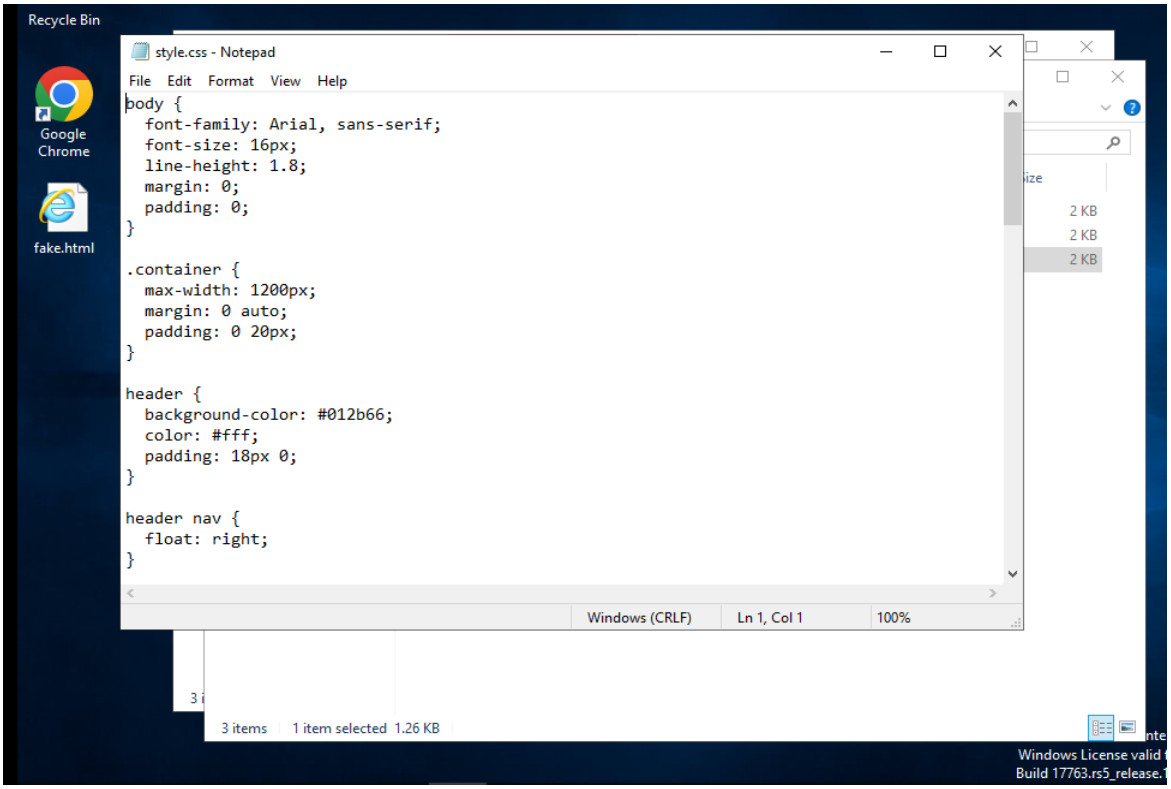


Figure 40 Adding CSS code in the style.css file.

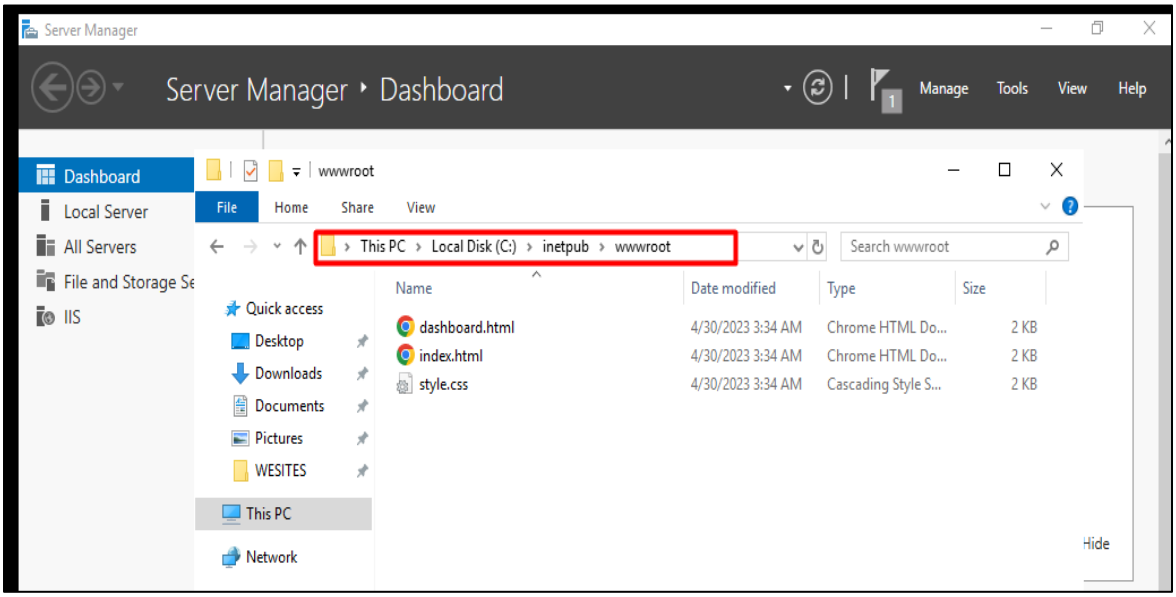


Figure 41 Changing the .txt extension of the files to .html extension.

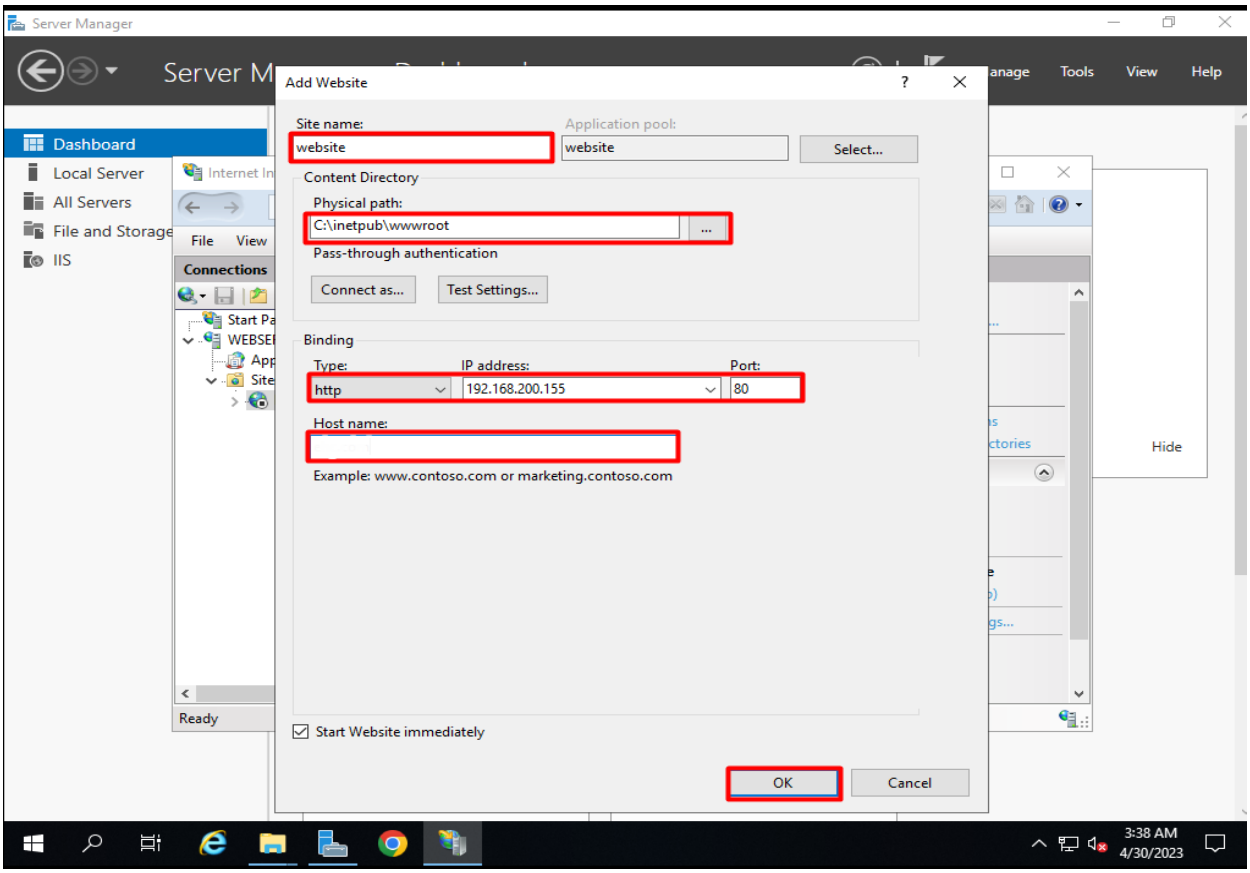


Figure 42 Creating an official website and binding it with the IP address of the server.

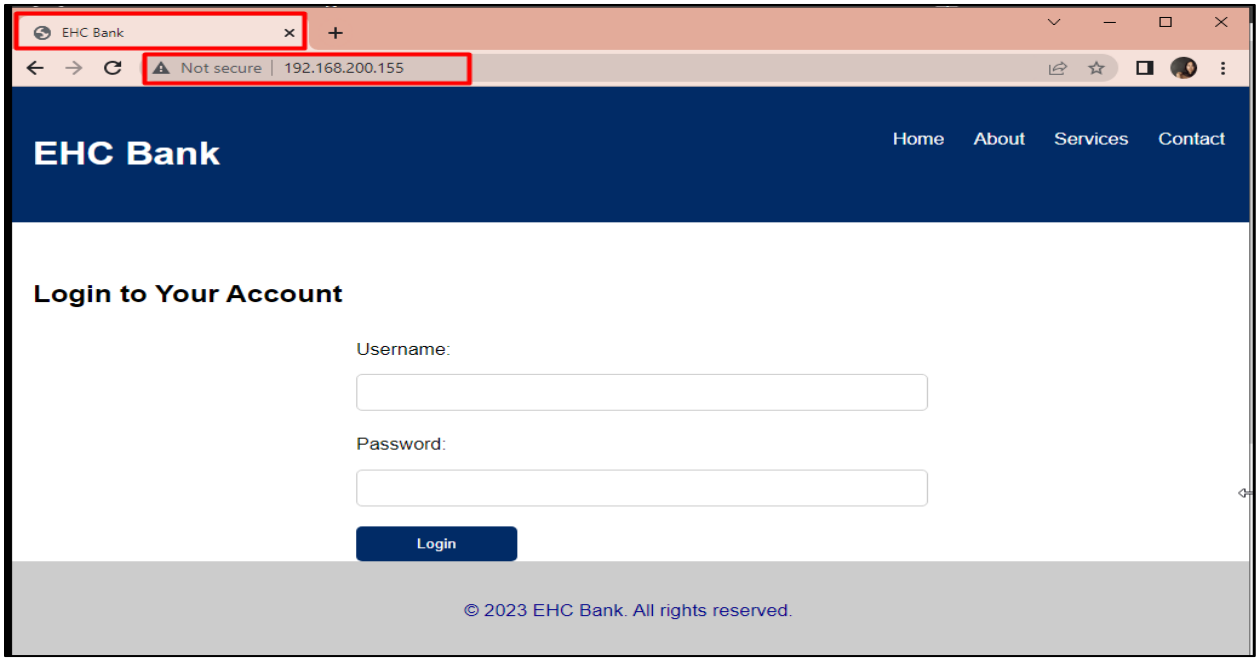


Figure 43 The website is hosted and is accessible for the users now.

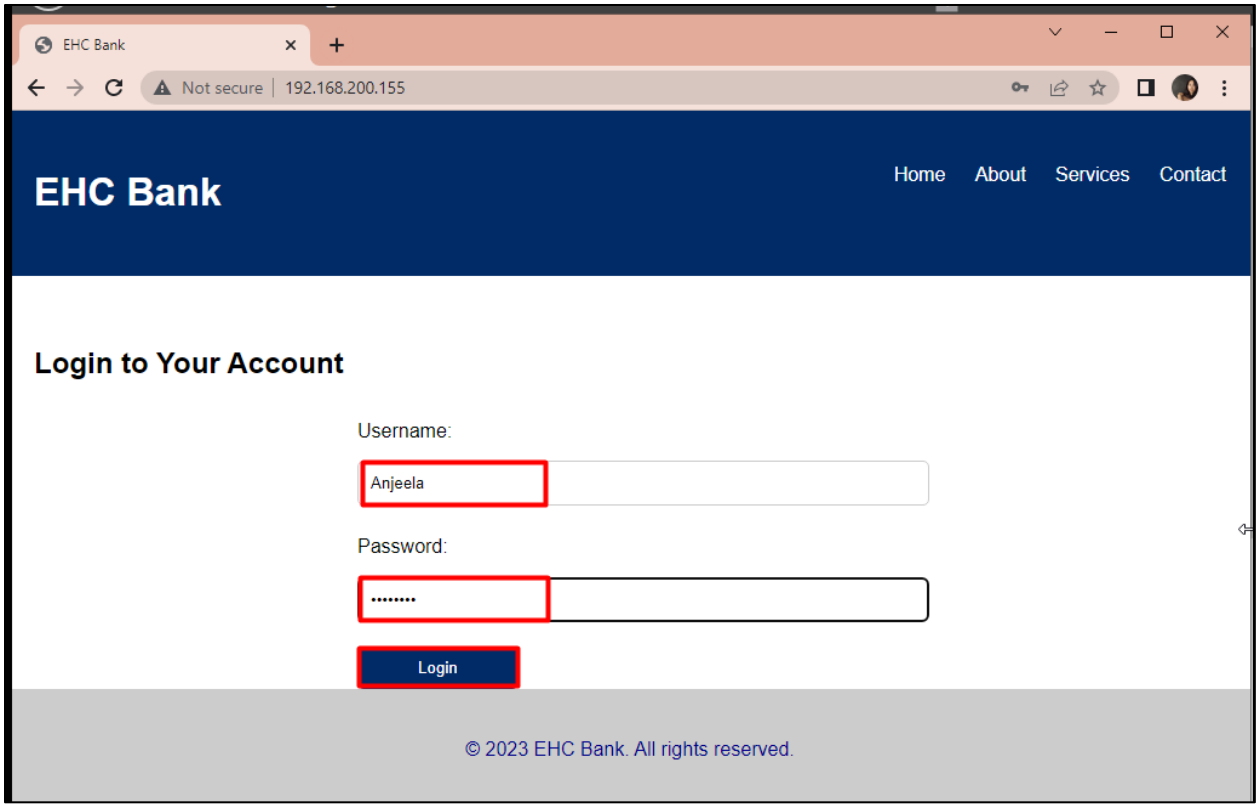


Figure 44 Testing if the dashboard page is opened after giving the credentials by the users.

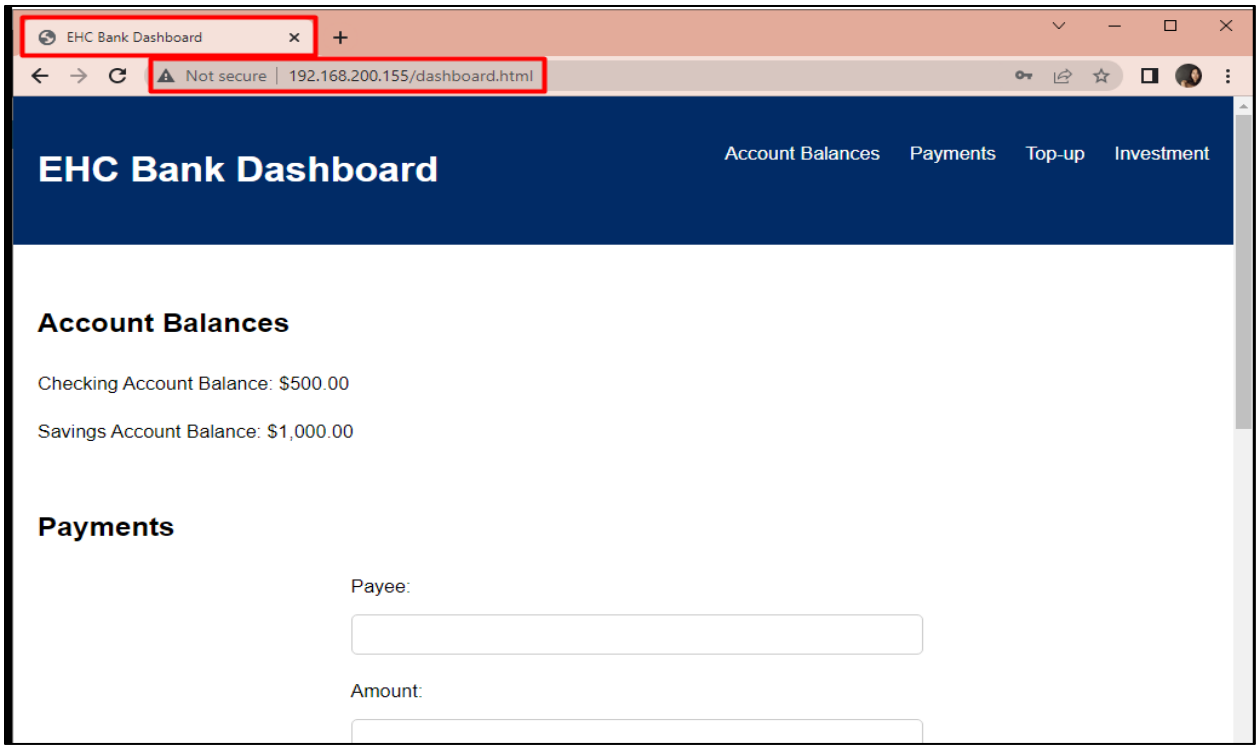


Figure 45 The dashboard page is also now accessible by the users.

7.6. Installing and configuring windows 7.

- The static IP address and DNS of the windows 7 is set after installation.

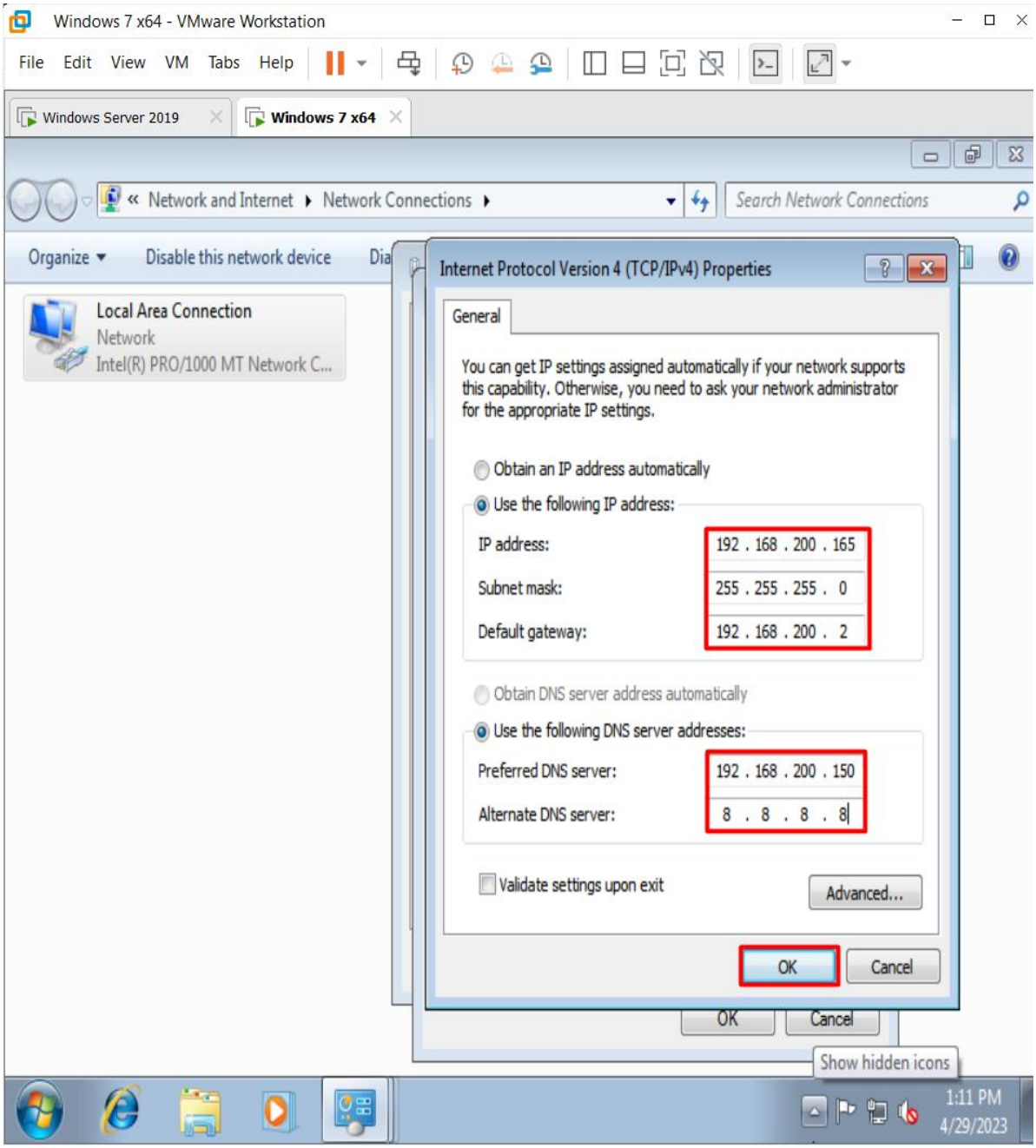


Figure 46 Assigning static IP address and DNS.

- Changing computer name to “USERS” and keeping under EHC.com domain.

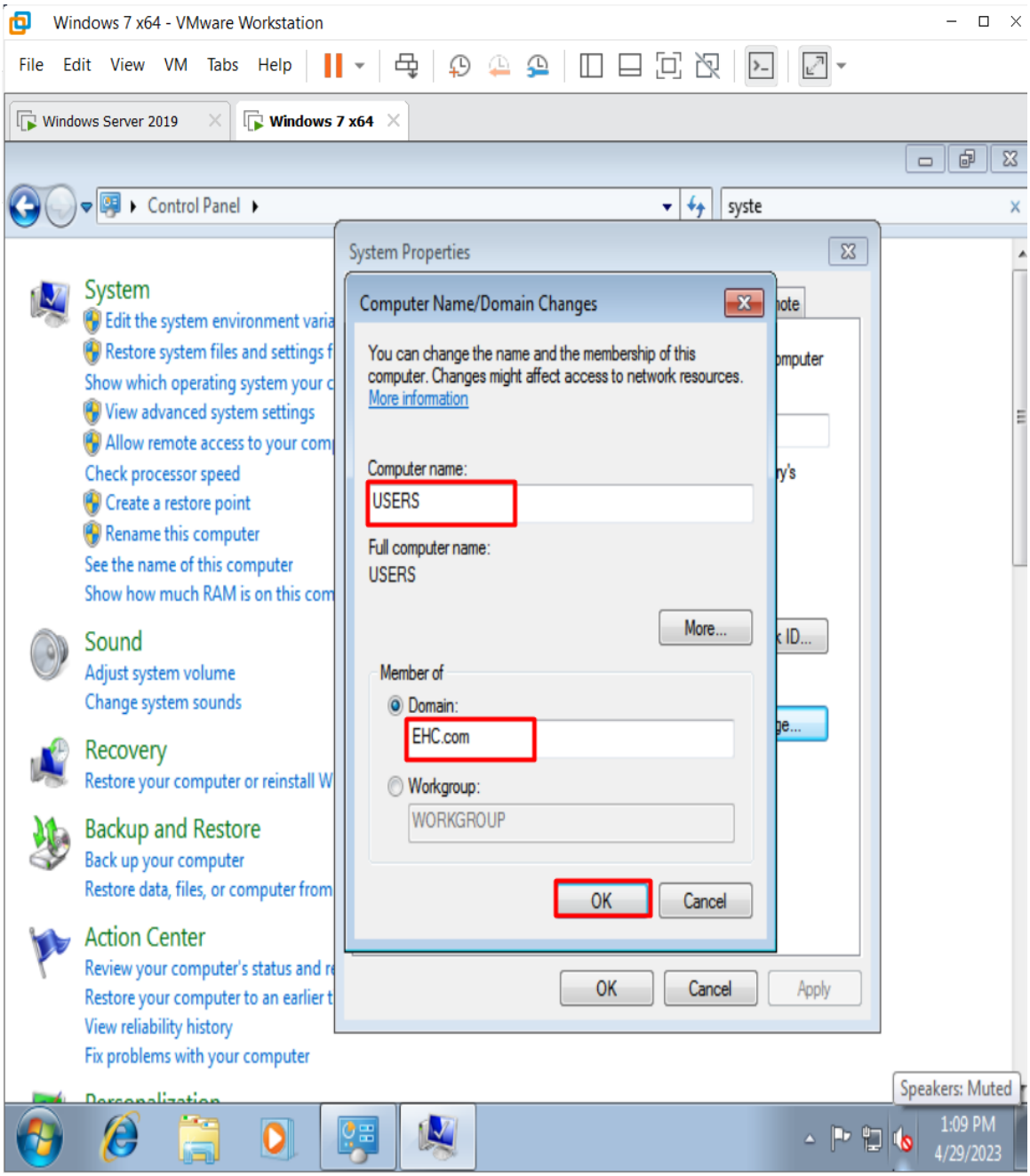


Figure 47 Changing the computer name and keeping under EHC.com domain.

- Logging windows 7 as an IT officer user.

Figure 48 Logging in as ITofficer.

7.7. Creating an exe payload using Metasploit in kali Linux.

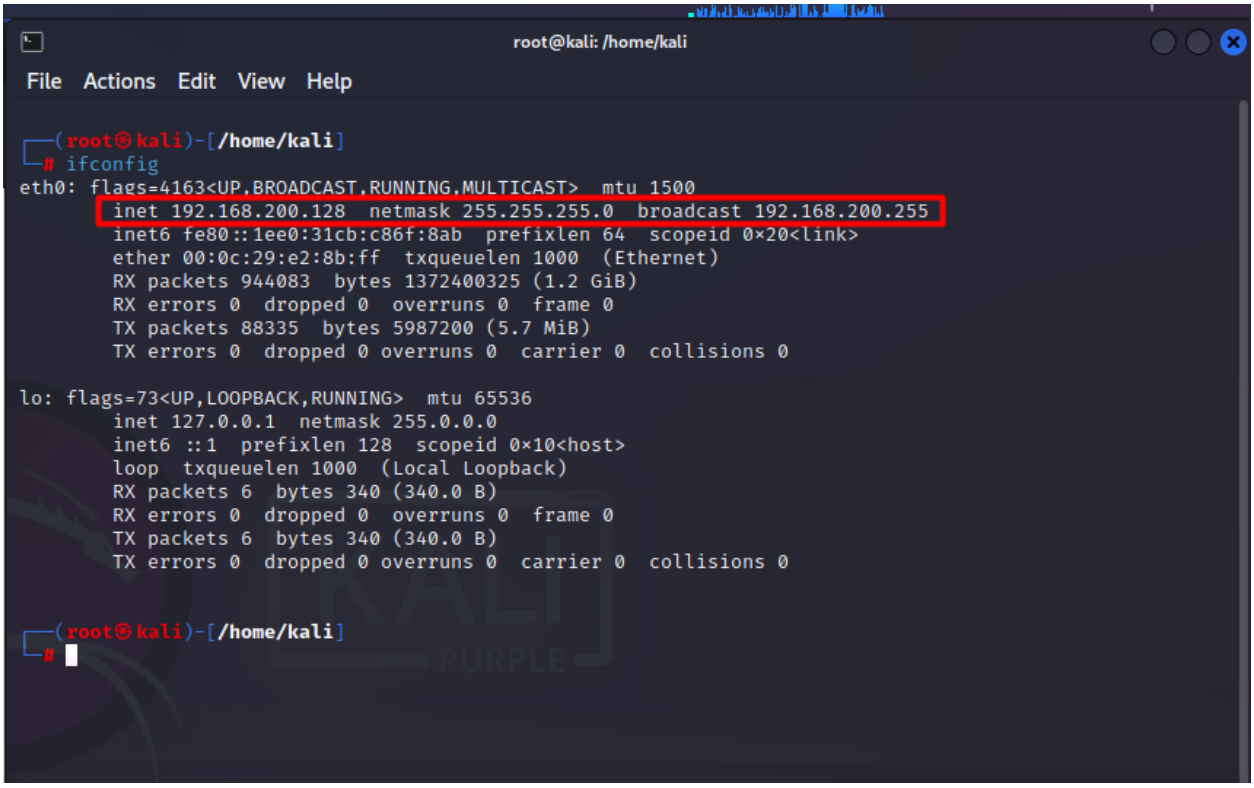


Figure 49 Checking IP address of the Kali Linux.

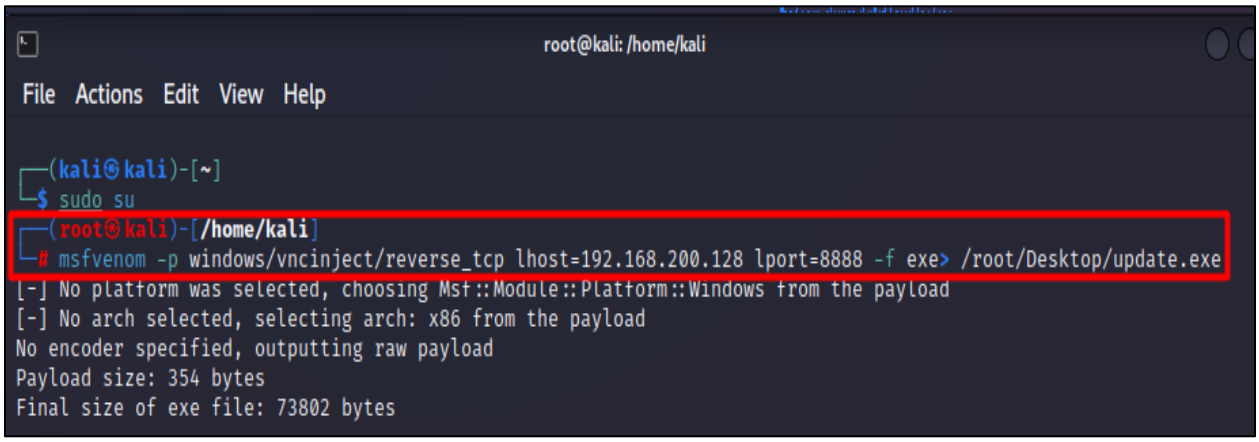


Figure 50 Creating payload for backdoor remote access and control.

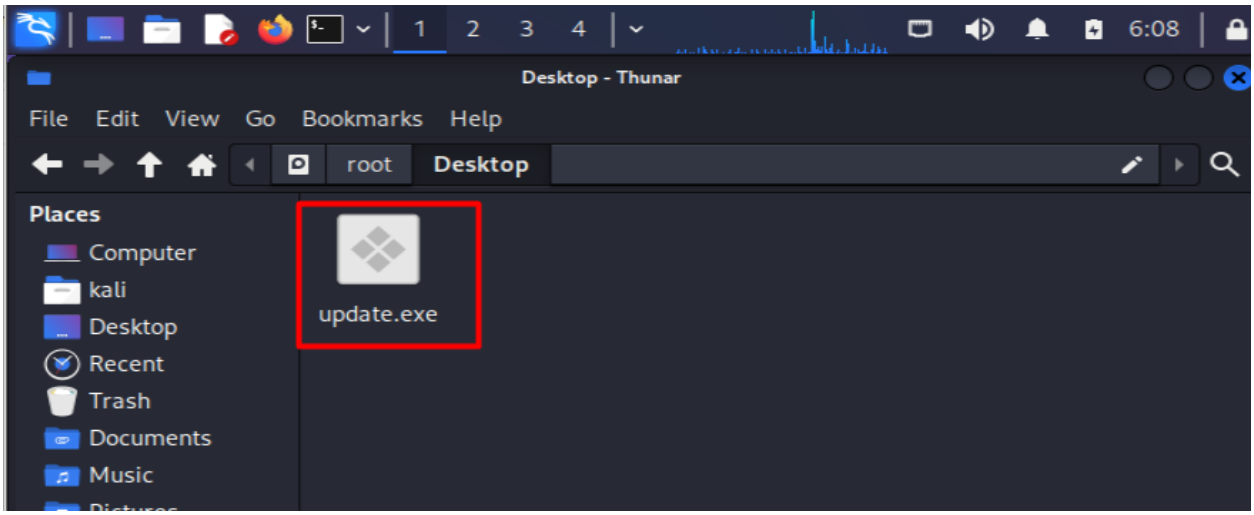


Figure 51 update.exe payload.

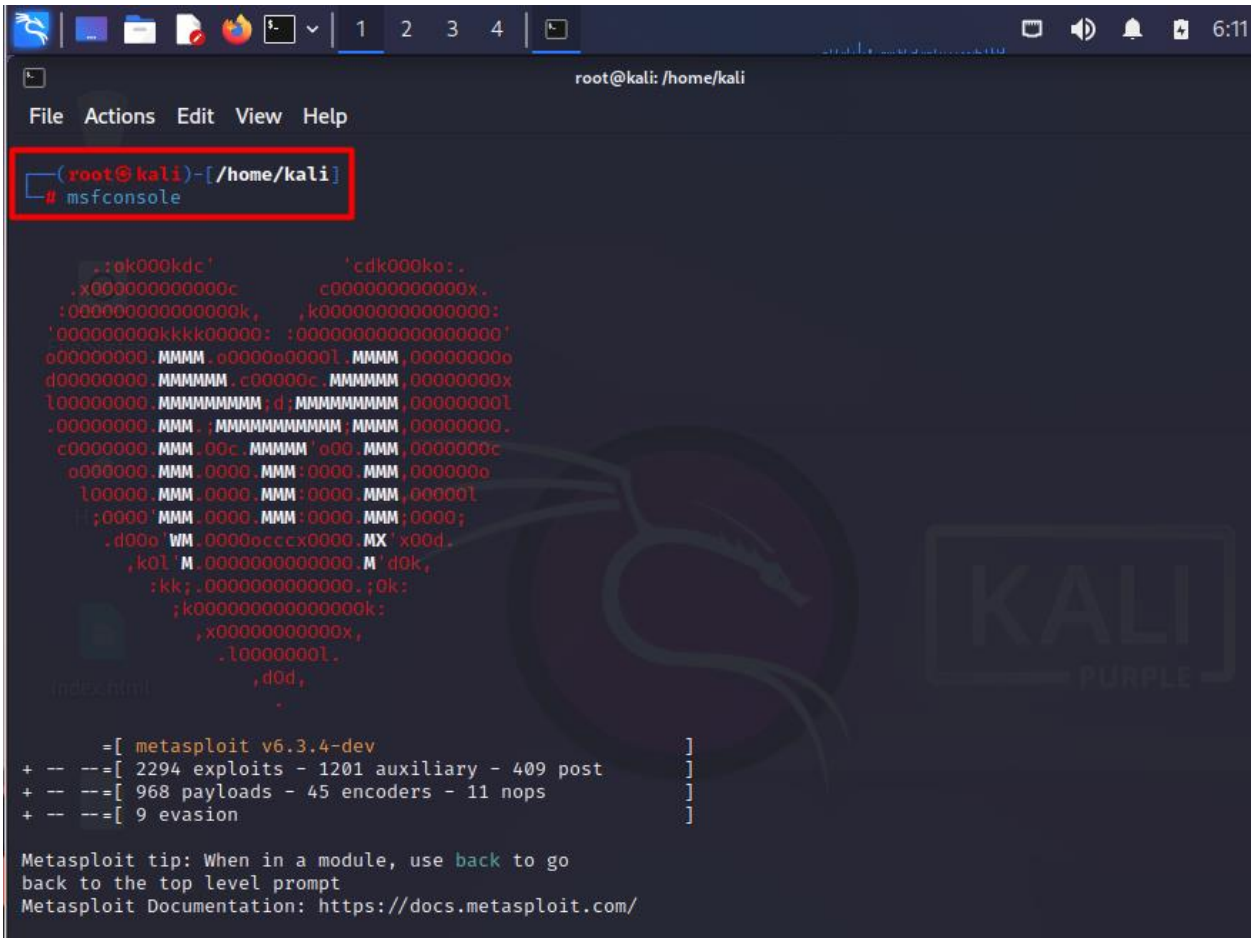


Figure 52 Running "msfconsole" command to start Metasploit framework.

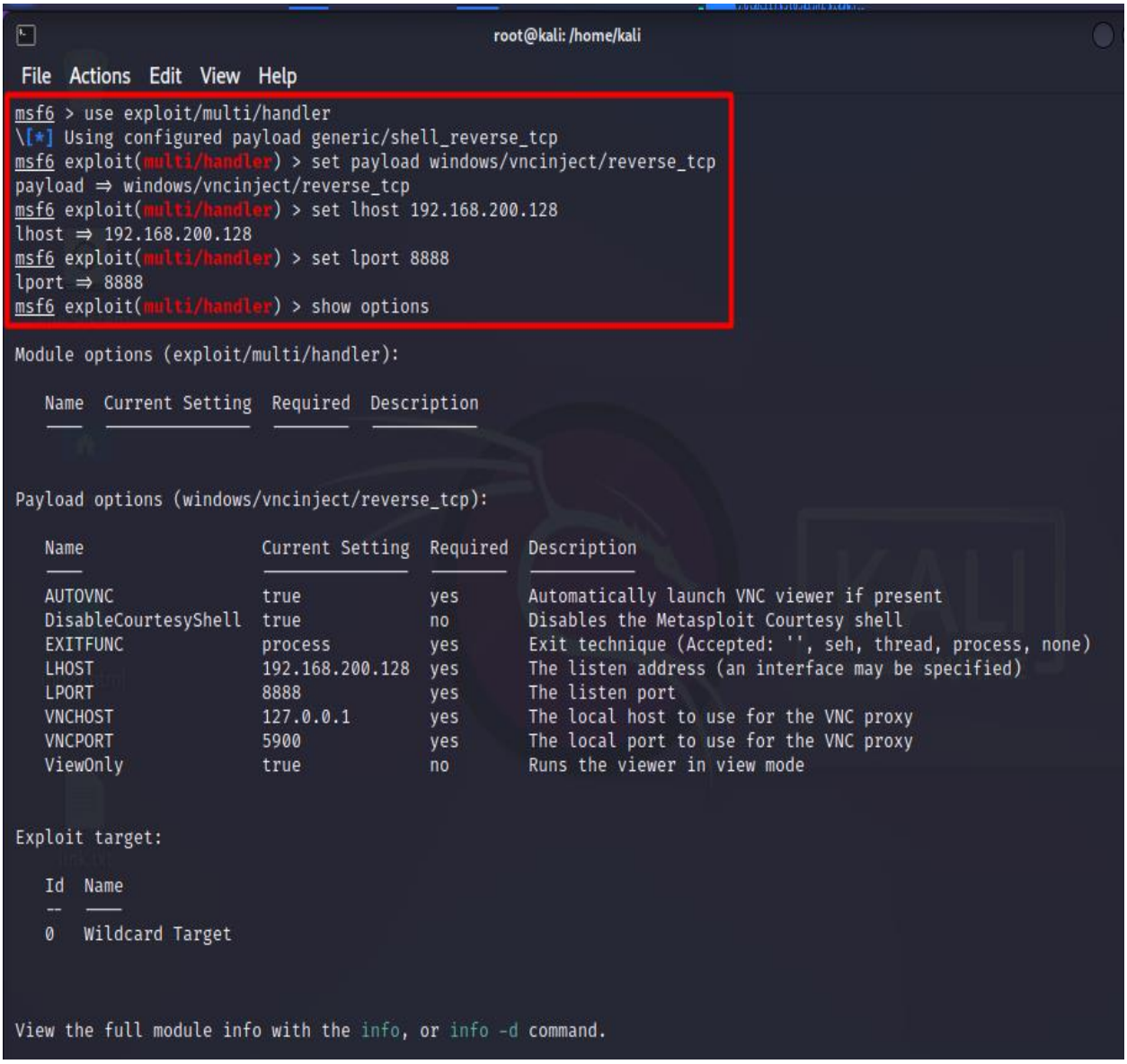


Figure 53 Using multihandler command to set the reverse TCP payload, lhost and port as well.

7.8. Delivering the payload through a phishing mail.

- The update.exe was uploaded to the mega drive.

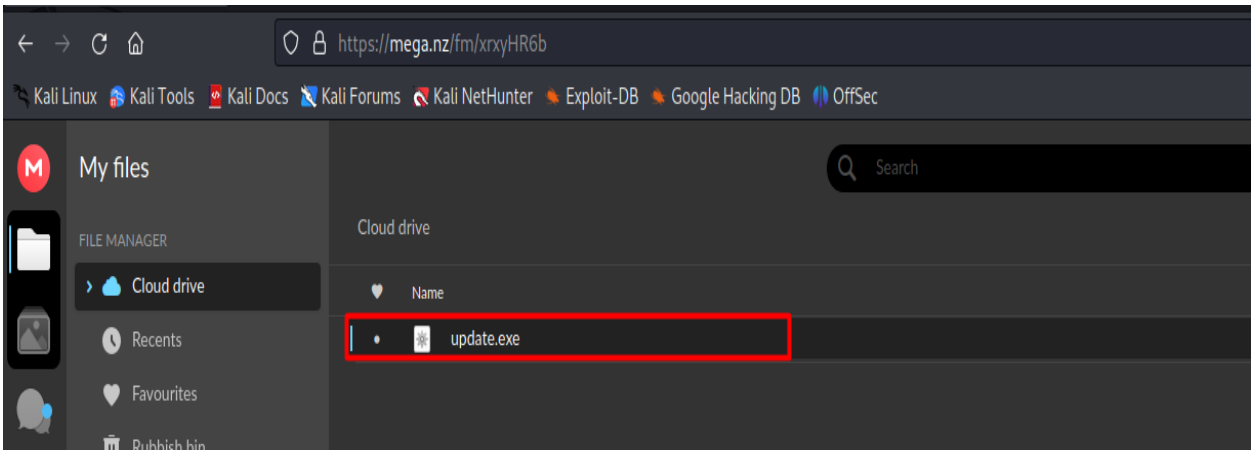


Figure 54 Uploading the update.exe payload in mega drive.

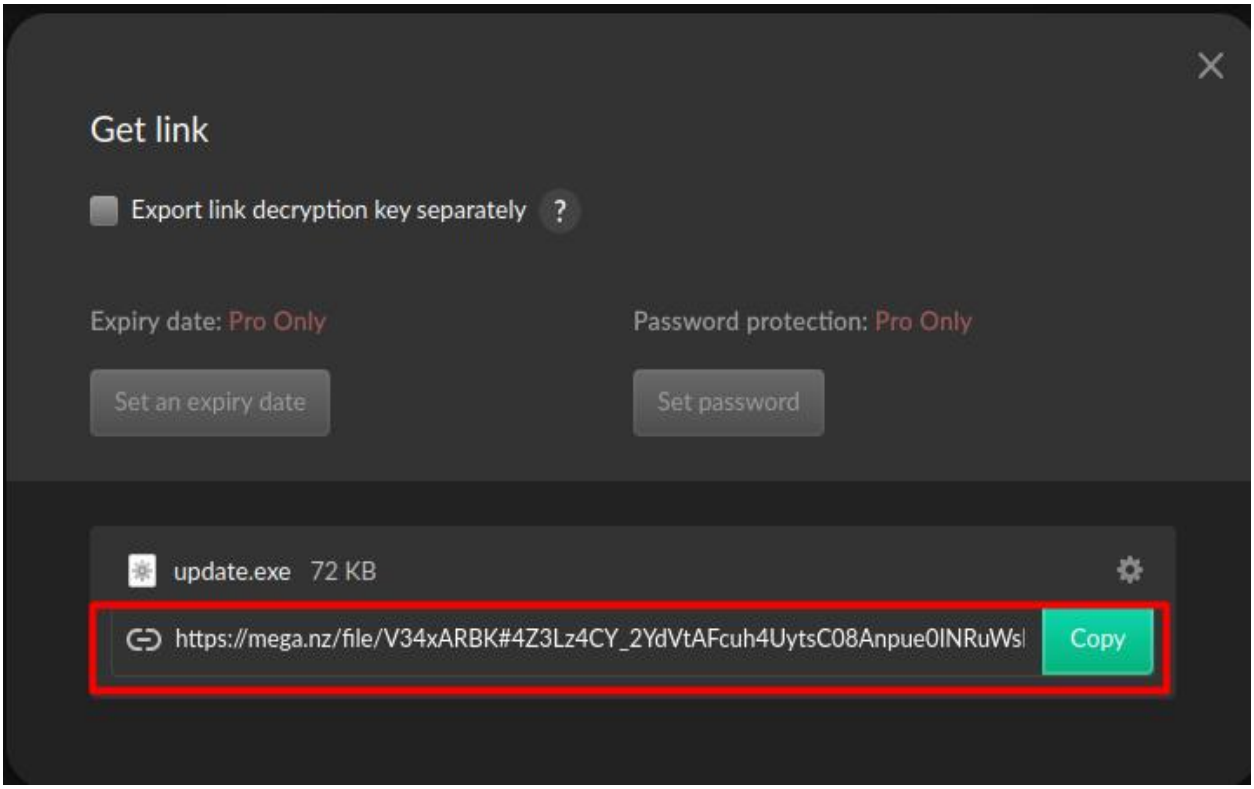


Figure 55 Getting the link of the uploaded file.

- Creating a fake mail from a fake Gmail Microsoft community account.

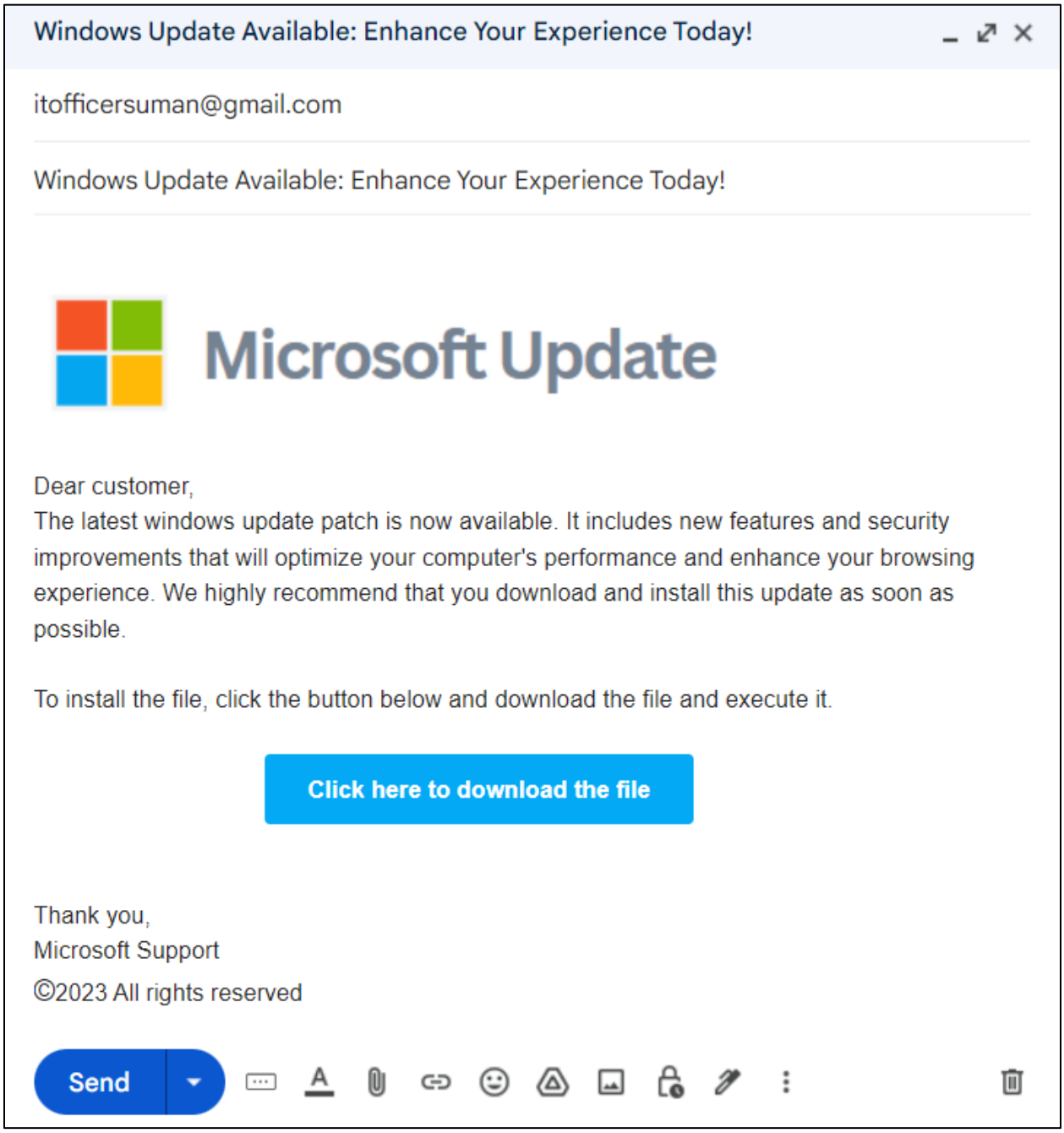


Figure 56 Creating fraud mail.

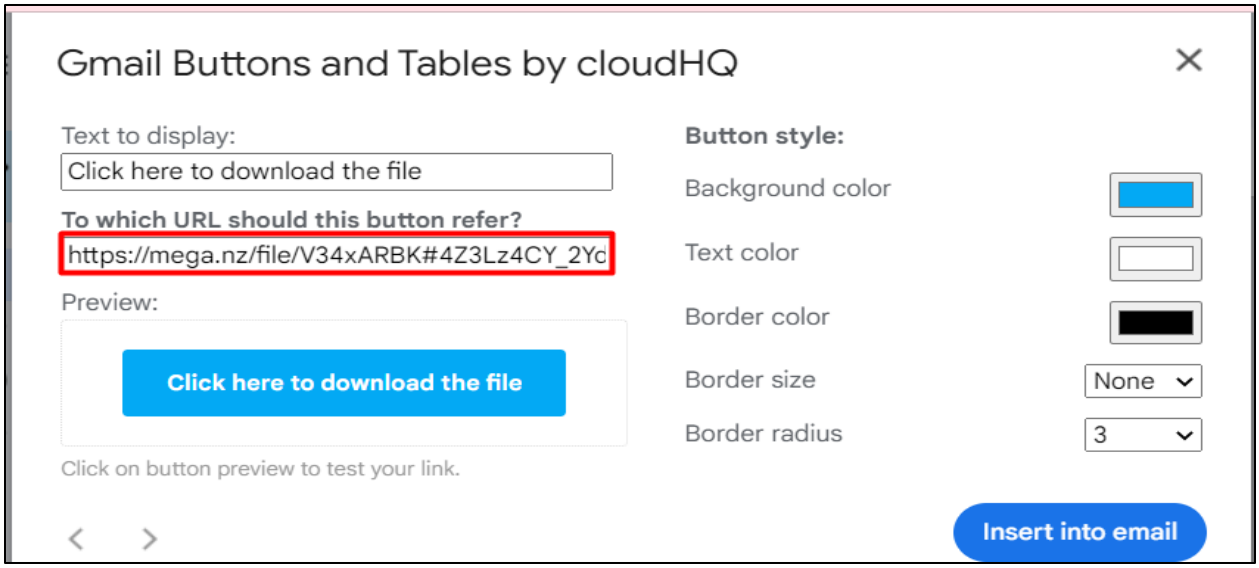


Figure 57 Adding link to the button of the fraud mail.

- Fake Gmail account used for delivering the mail.

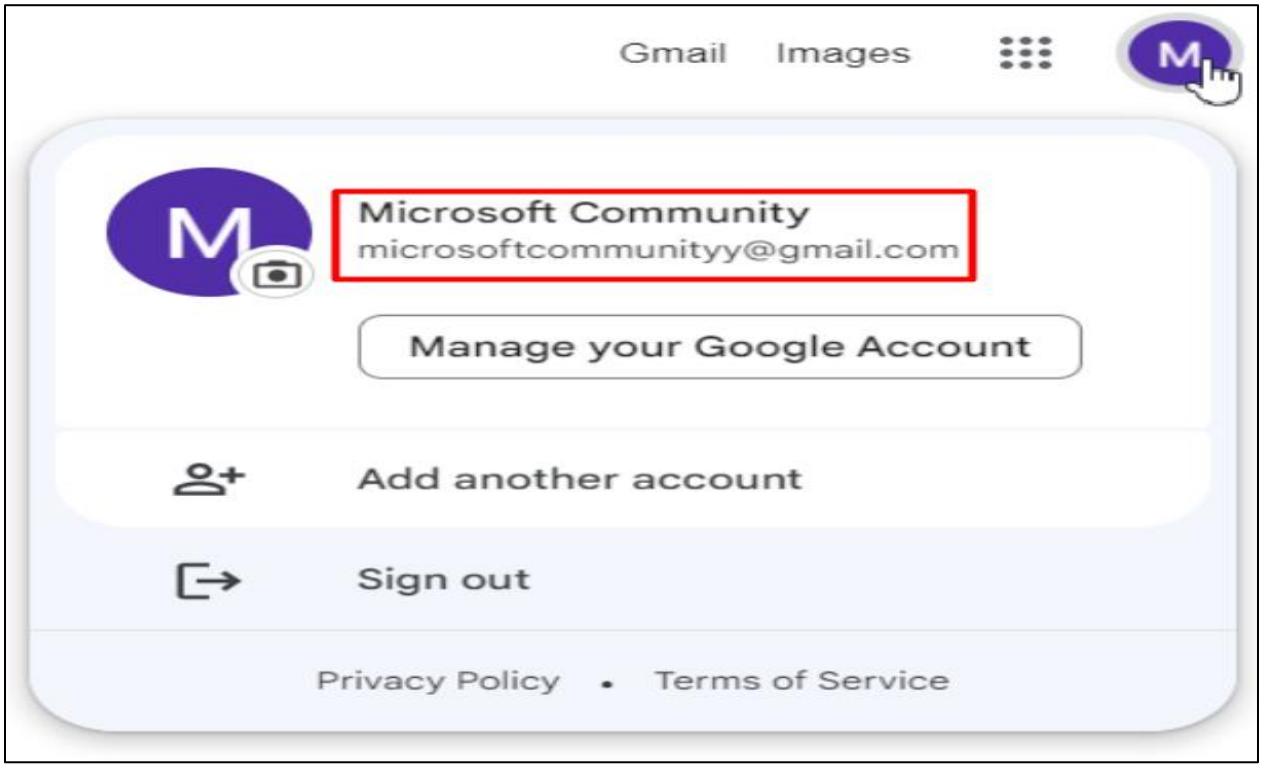


Figure 58 Fake Gmail account used for delivering the mail.

- Victim getting the mail.

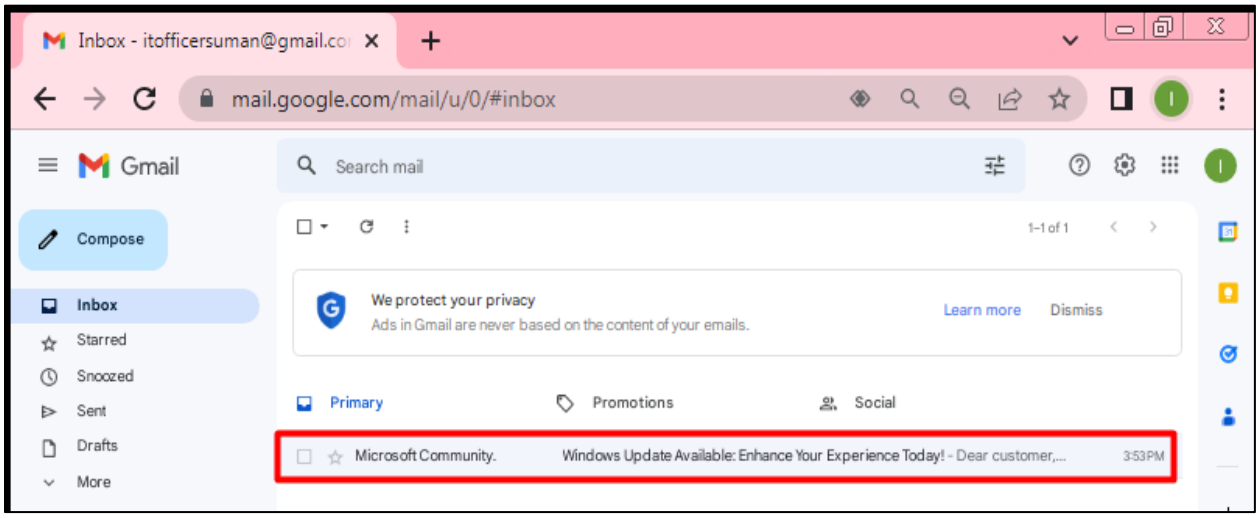


Figure 59 Victim getting the mail.

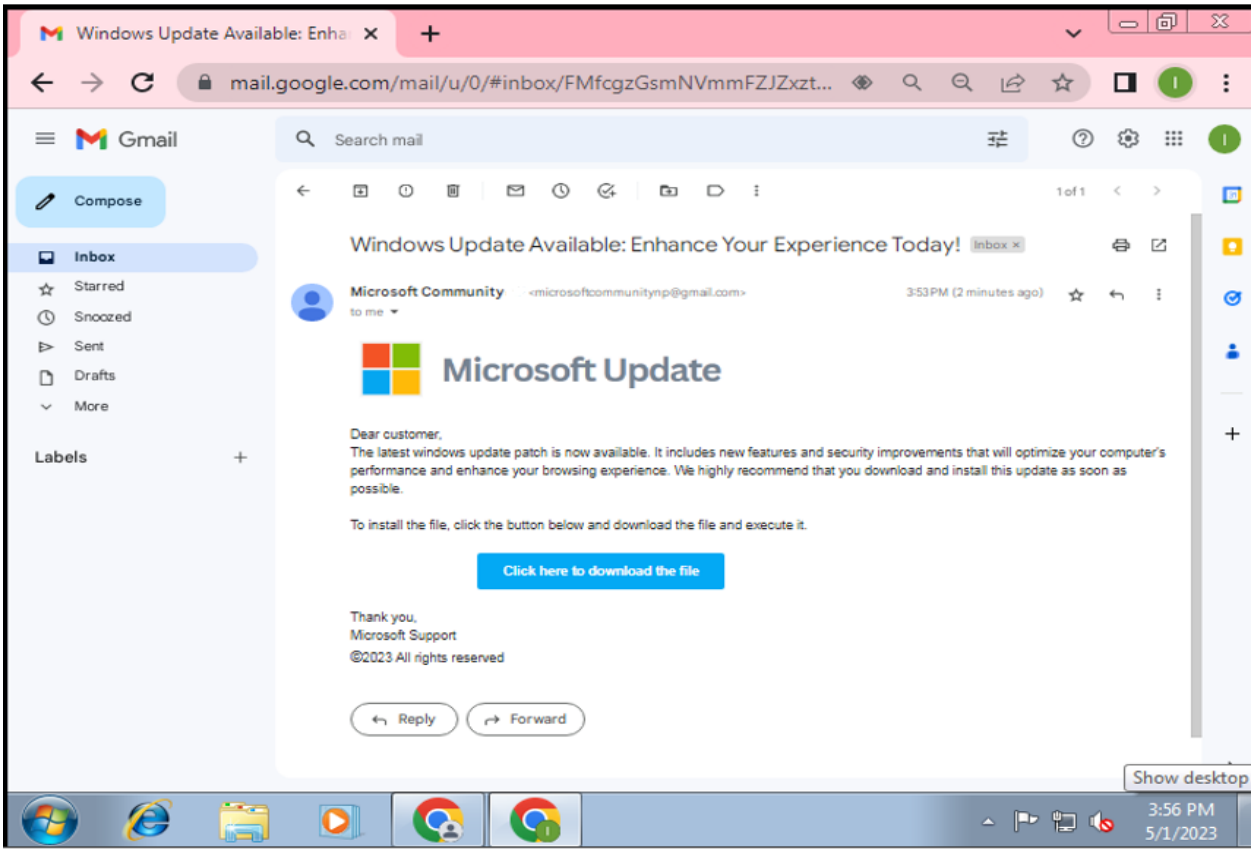


Figure 60 Victim opened the mail and downloaded the file.

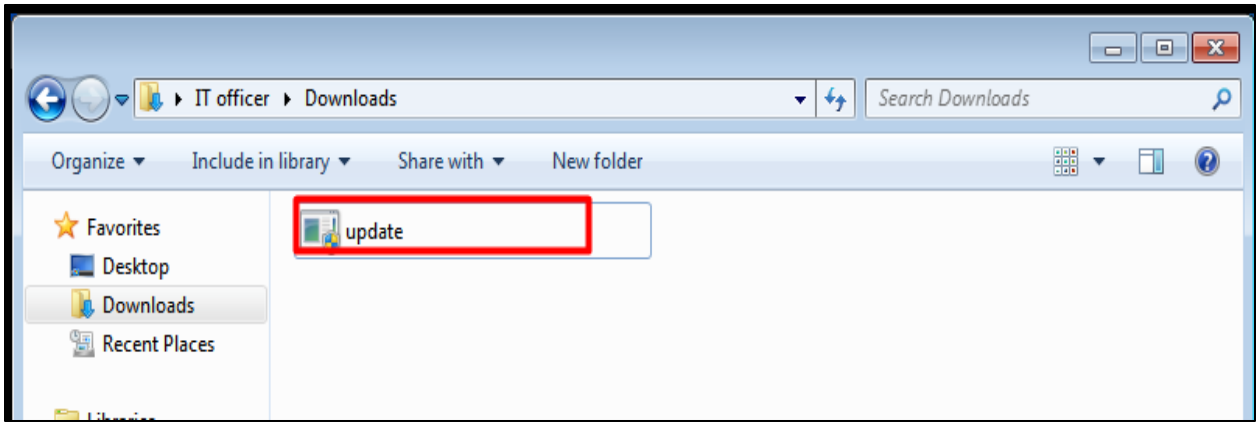


Figure 61 Downloaded file.

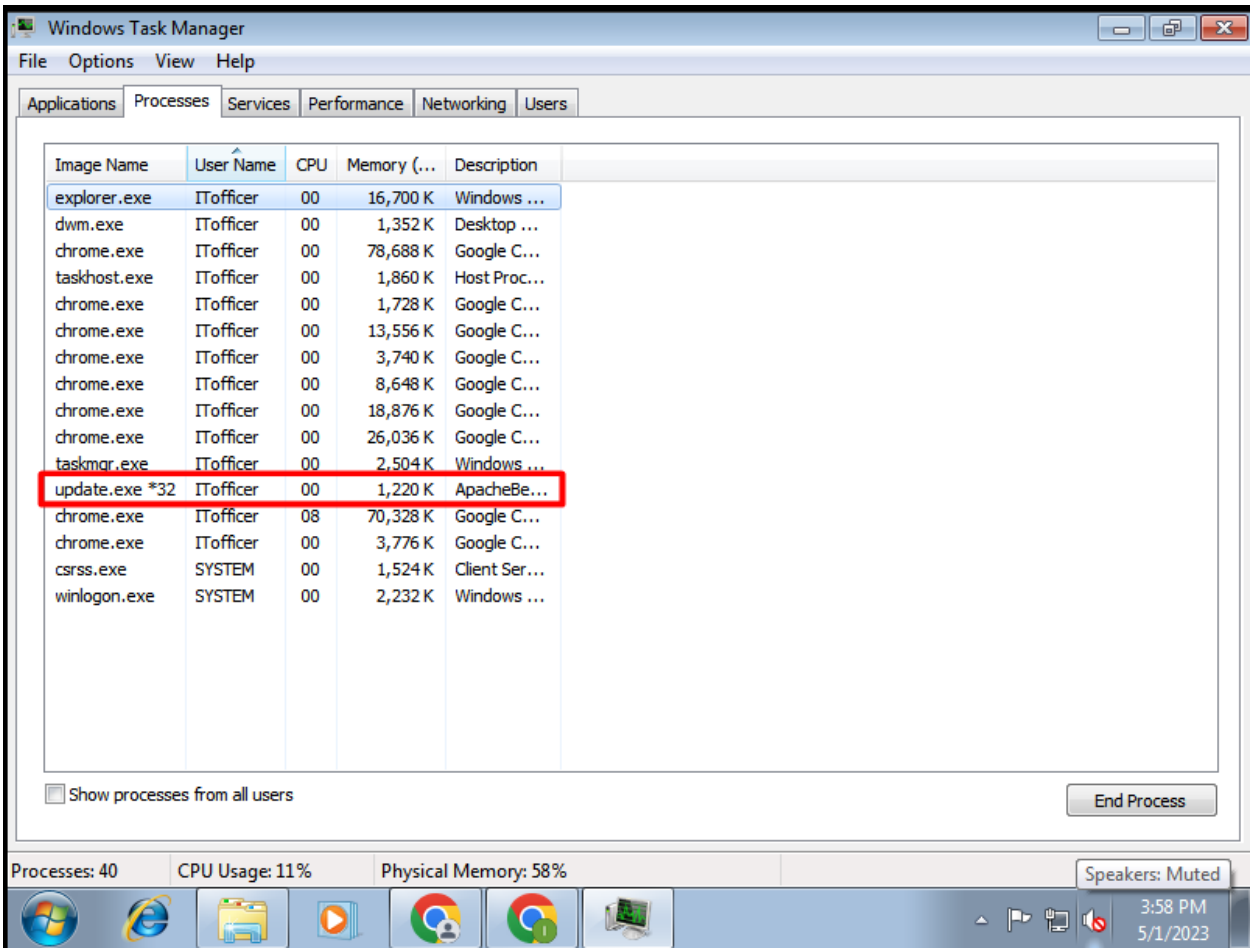


Figure 62 Payload running in background.

7.9. Accessing and controlling the victim's PC.

- After the execution of the file by victim, a vnc session is started in Metasploit.

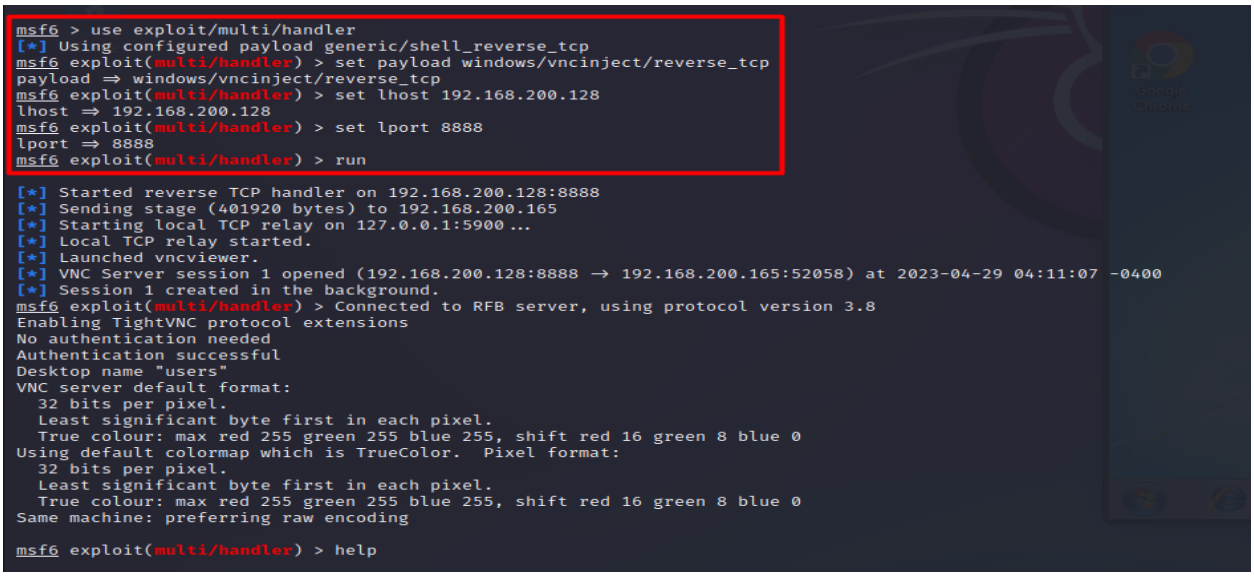


Figure 63 Attacker getting VNC session for remote access and control.

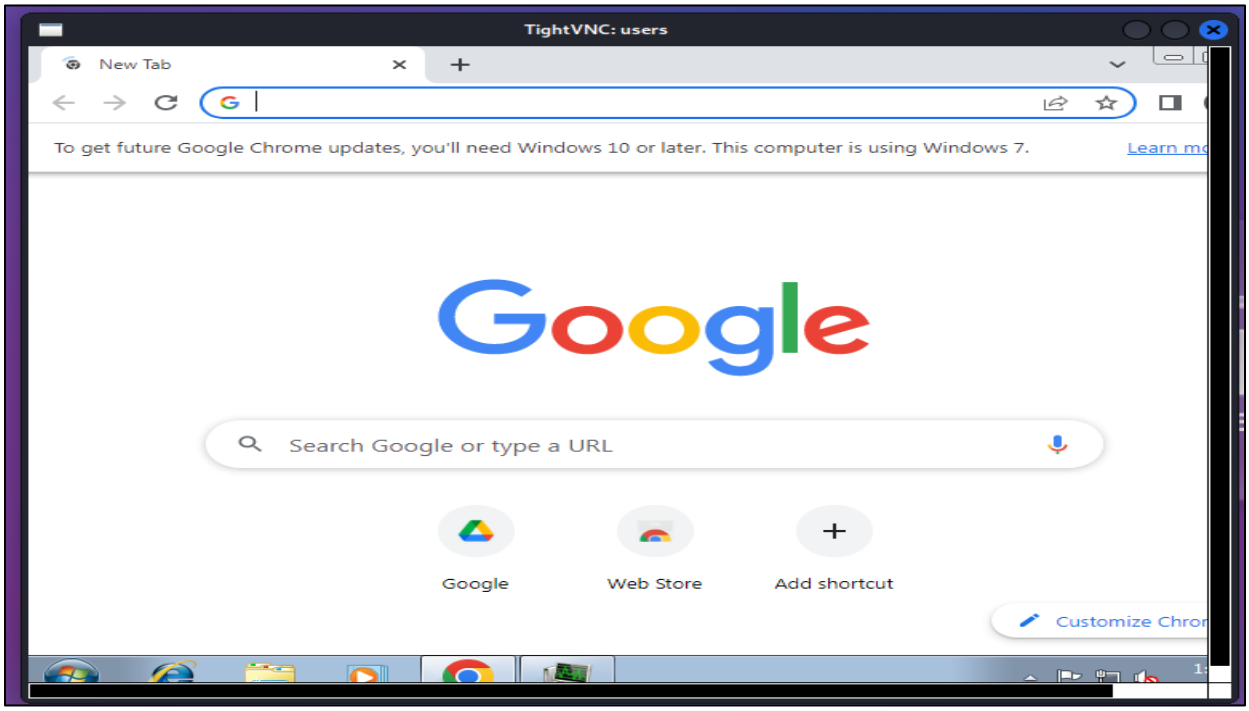
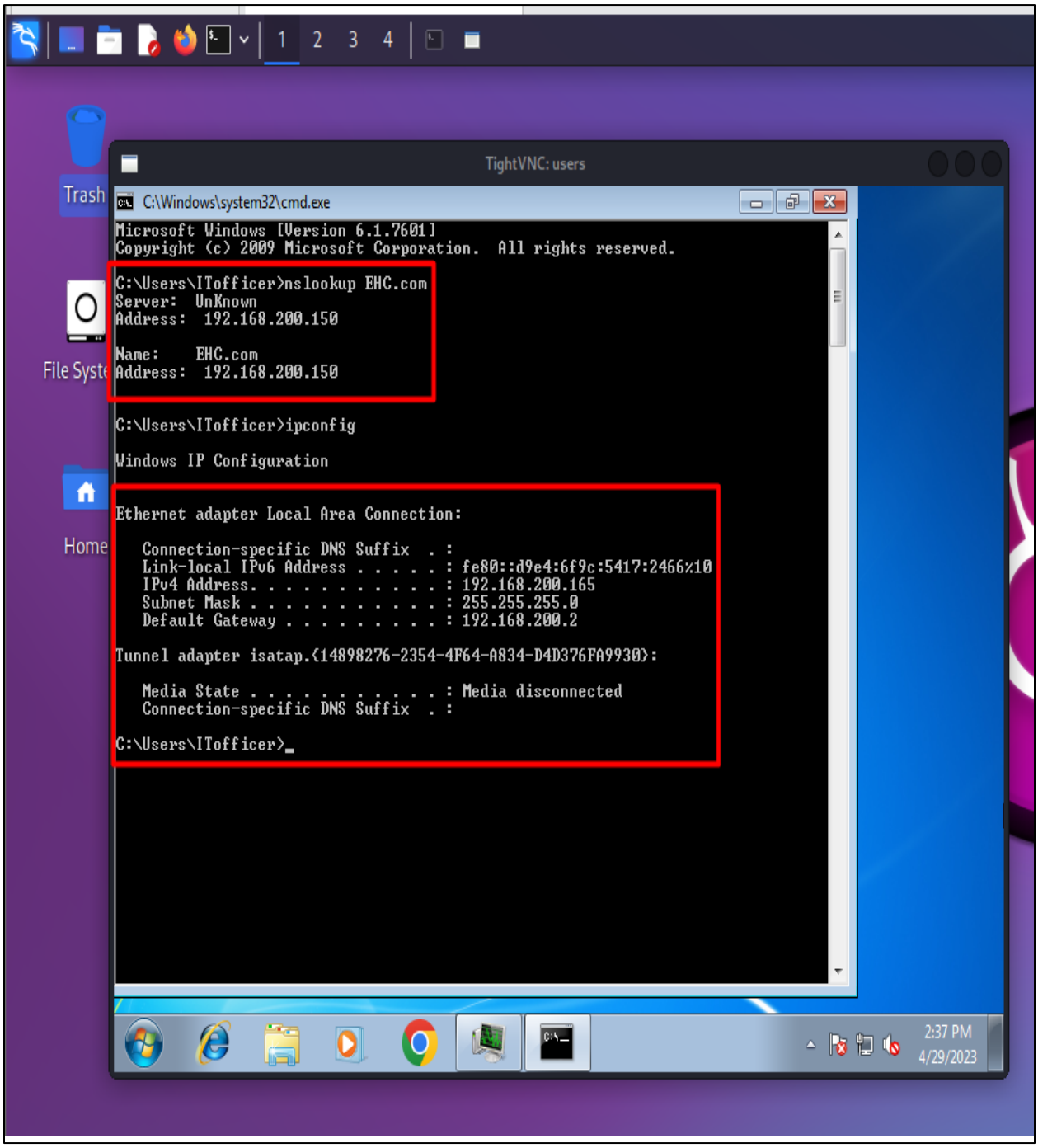


Figure 64 Attacker remotely accessing and controlling victim's PC.

- The attacker thus run “nslookup” command in CLI to see the Domain Controller server details and found out that this pc is under EHC.com domain and the IP address of the DC server is 192.168.100.150.



- The attacker then found a file “RemoteAccess” which contained the password for remote desktop connection to the other computers.

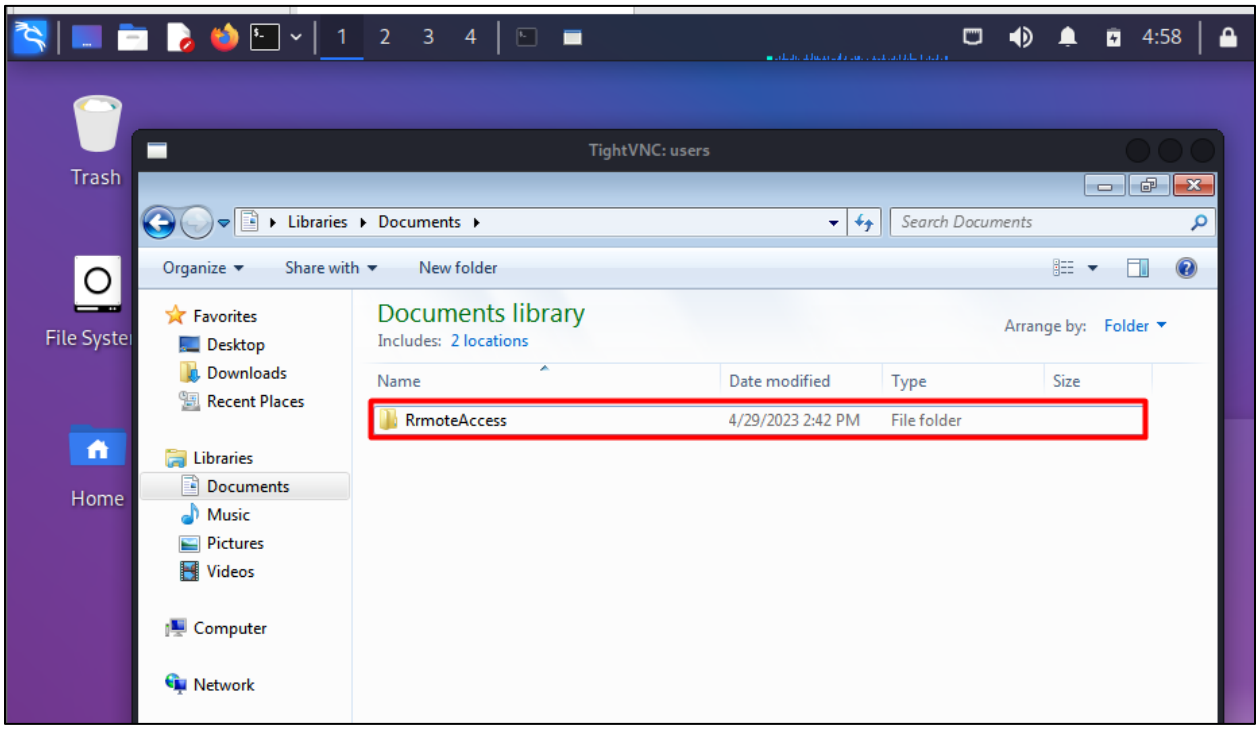


Figure 65 Attacker found a file named “RemoteAccess”

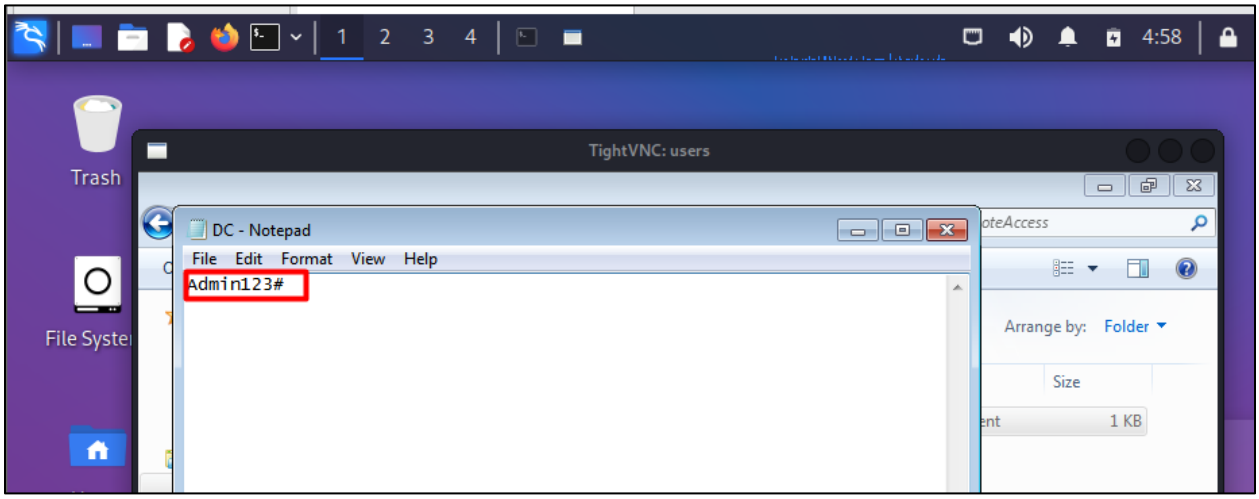


Figure 66 Attacker getting password for remote desktop connection.

- Now, the attacker remotely accessed domain controller.

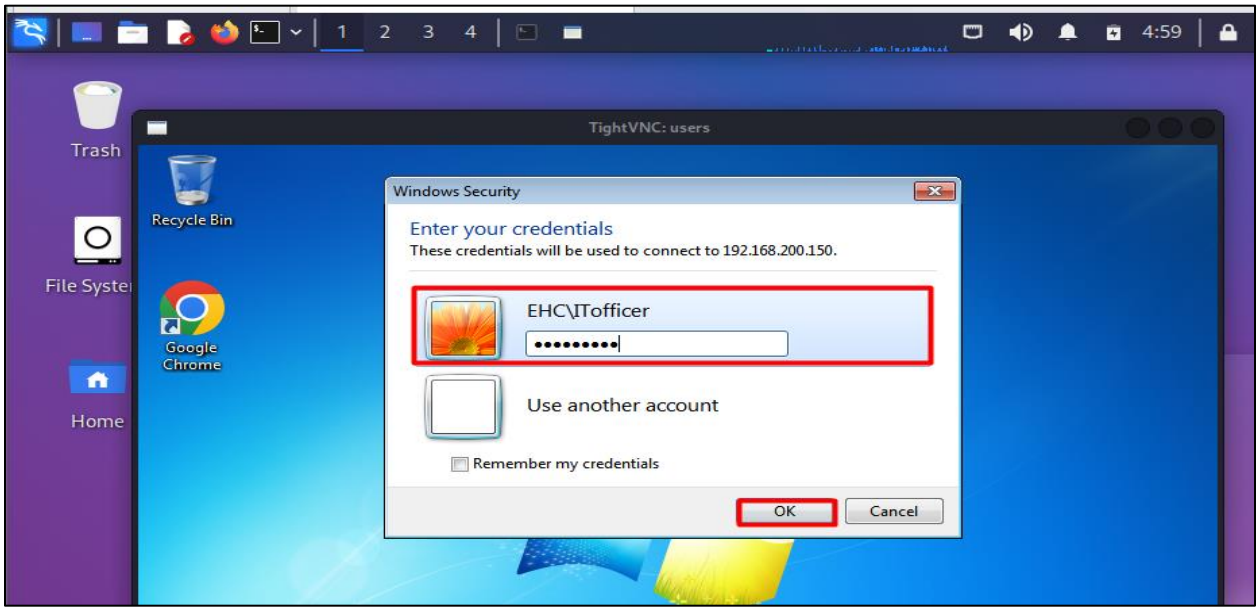


Figure 67 Attacker trying to access DC remotely from victim's PC.

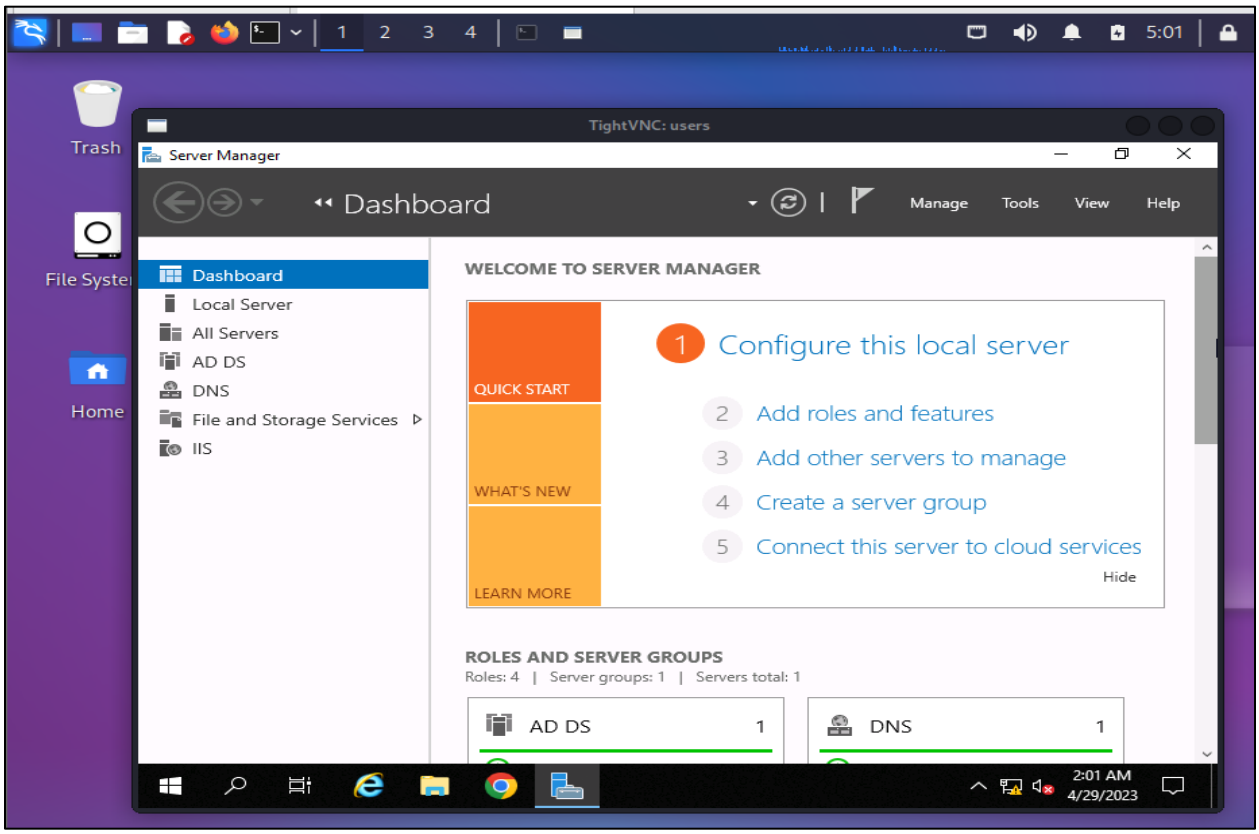


Figure 68 Attacker successfully accessed DC server.

- The attacker checks the users and computer list in AD users and computer list and found out that there is an webserver also in the AD computers list. She pinged the webserver with command “ipconfig webserver” thus getting the IP address of the web server i.e. 192.168.200.155 and tried remote desktop connection to the webserver suing same password thus successfully accessing web server. The attacker the, customizes the html file of the official website thus creating and hosting fake website.

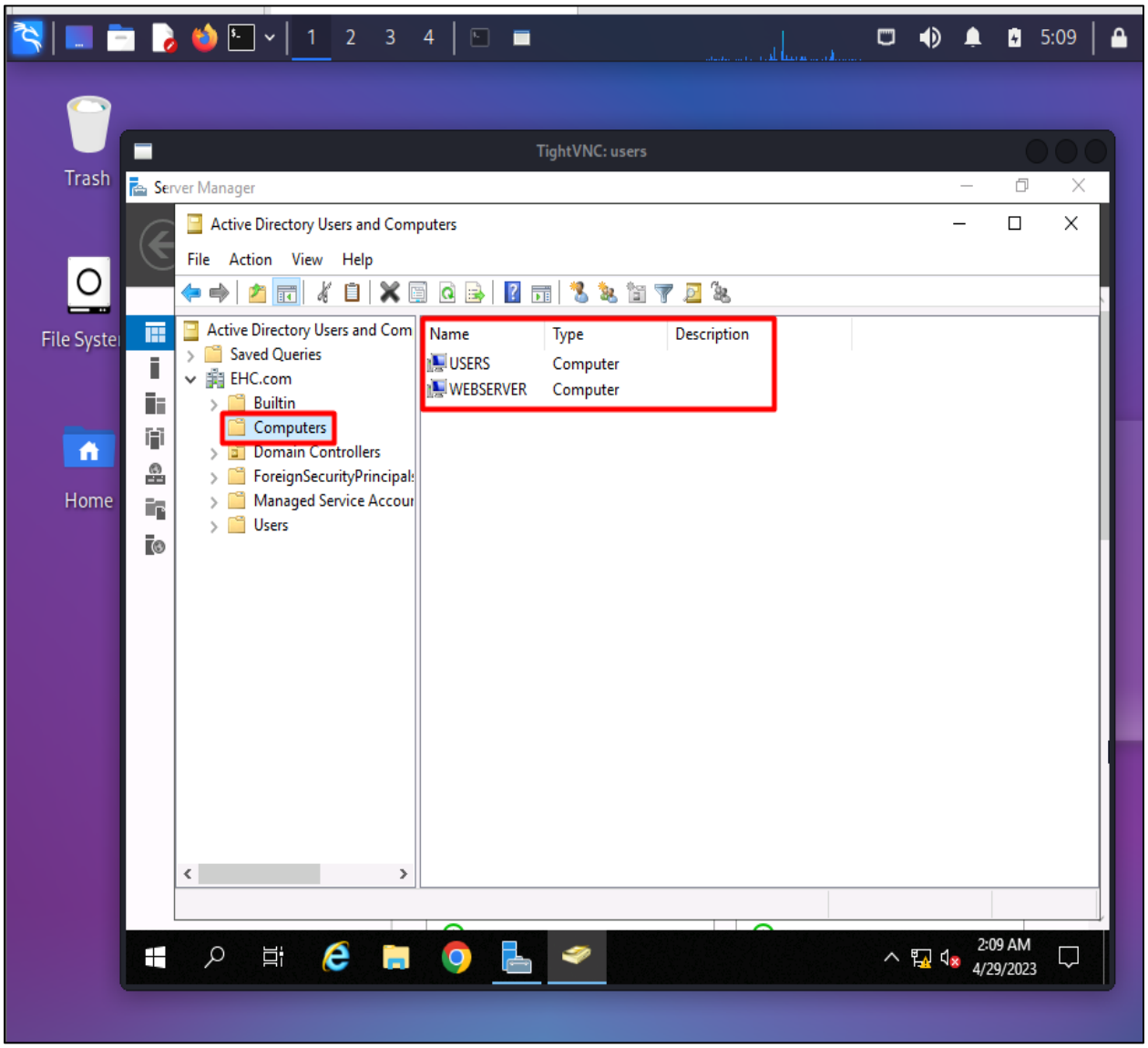


Figure 69 Attacker found a web server AD computer's list.

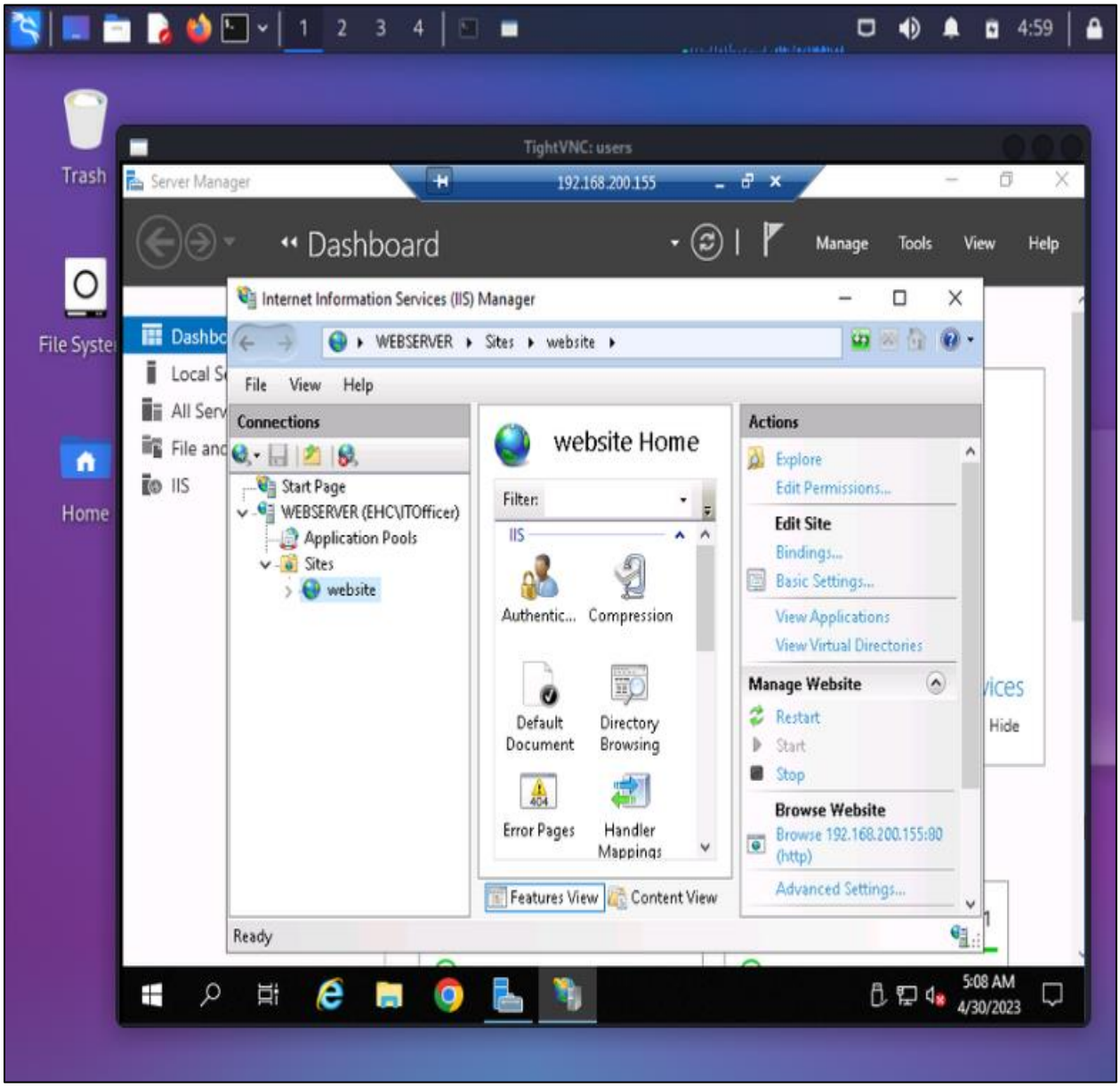


Figure 70 Attacker accessed the web server successfully.

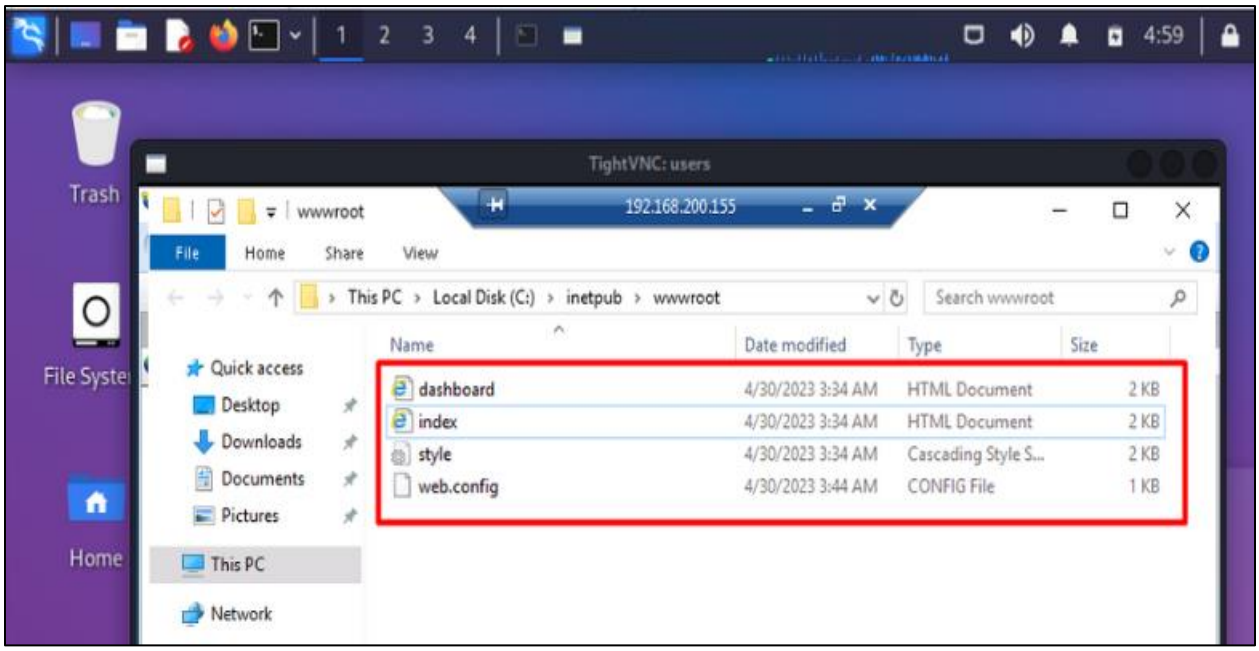


Figure 71 Attacker deleting the official website's files.

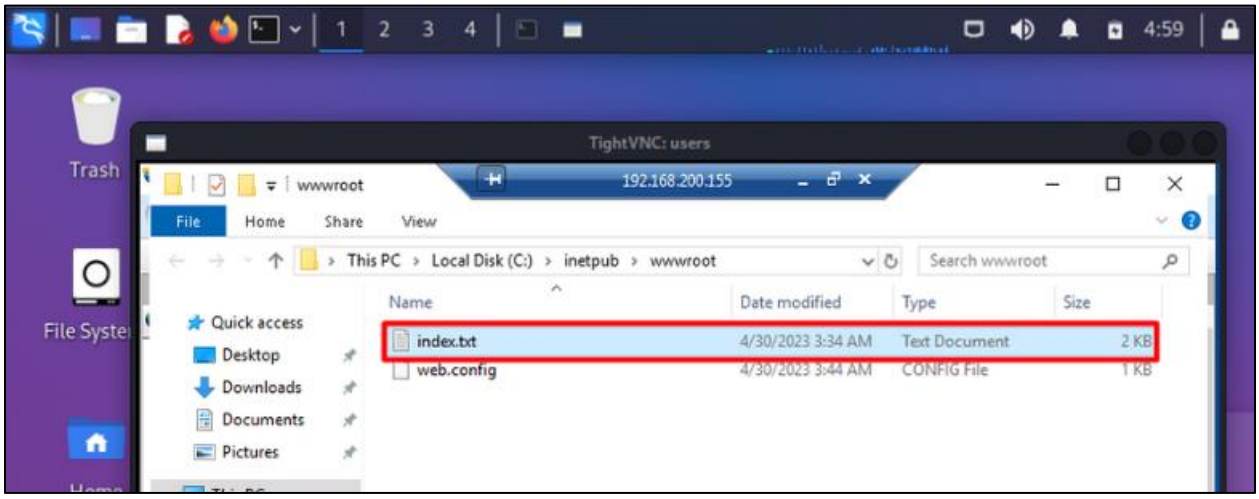


Figure 72Attacker creating a txt file to add html code.

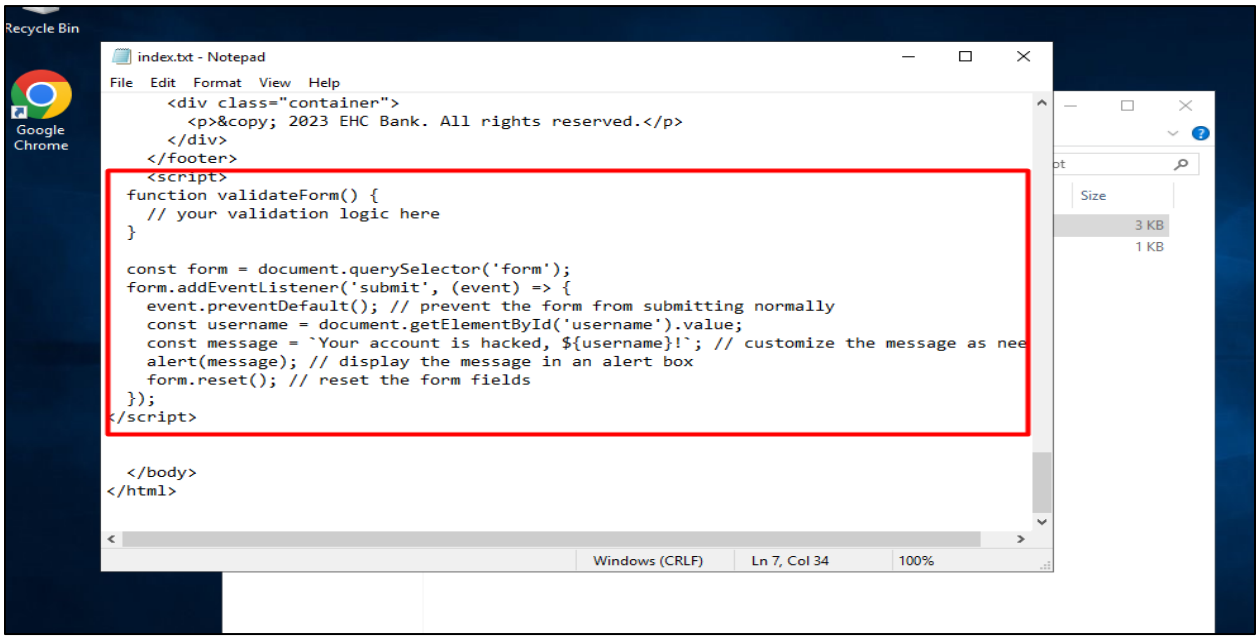


Figure 73 Attacker adding html code in the index.txt file.

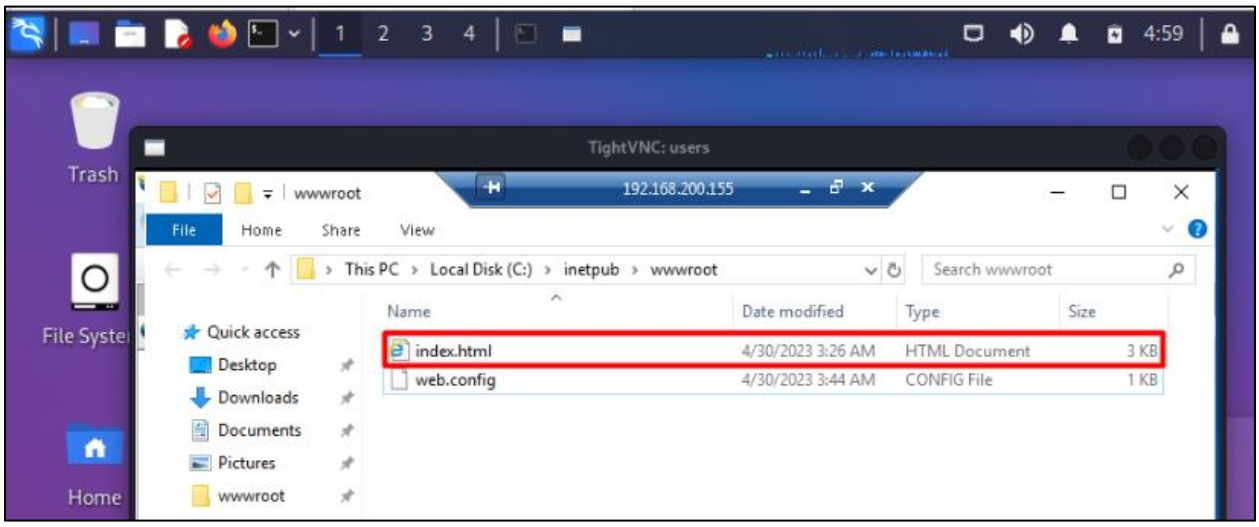


Figure 74 Attacker successfully customized the html files.

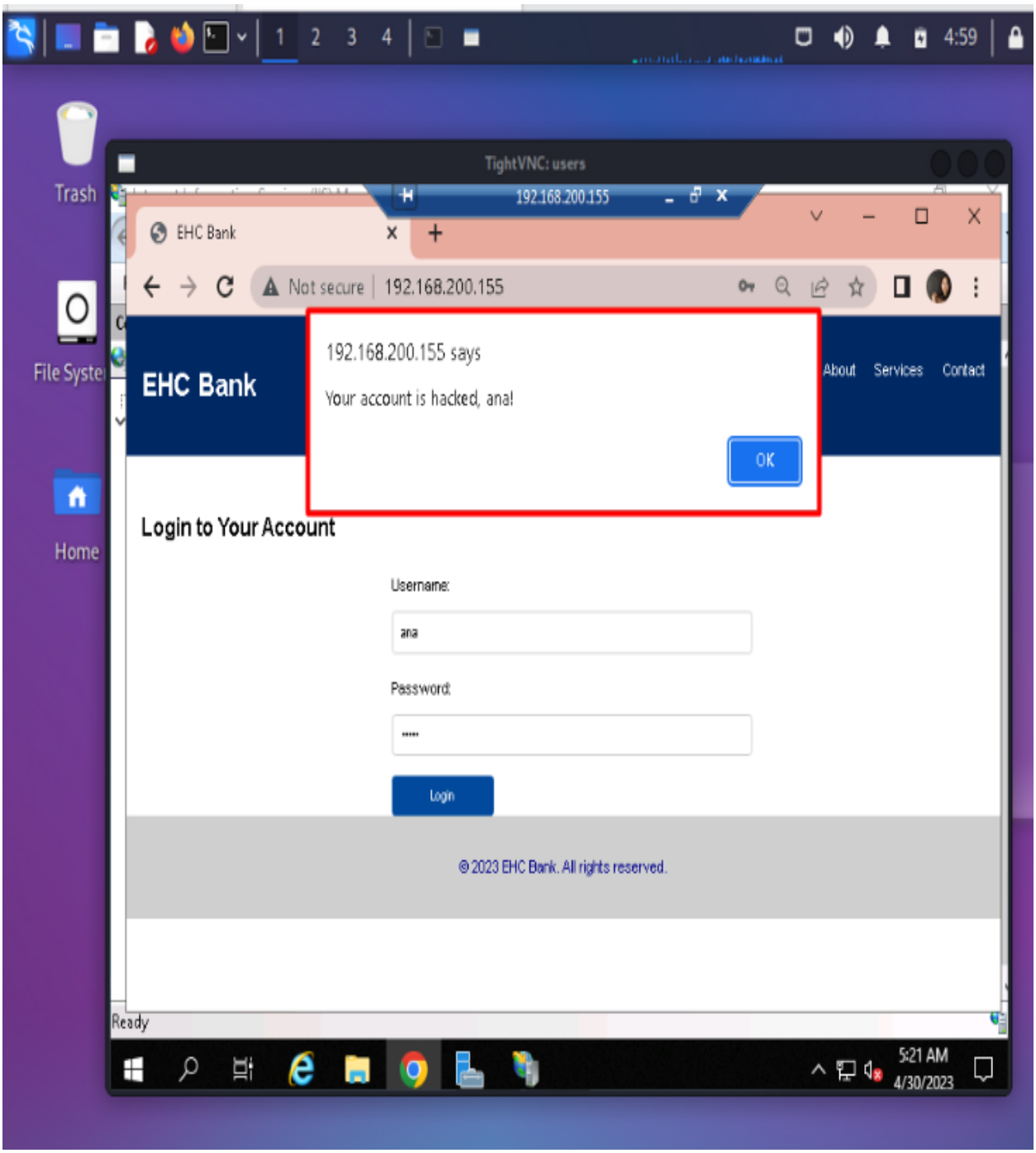


Figure 75 Attacker confirming if the website is behaving as per his configuration or not.

- Finally, the users were unable to login and were directed to the fake website created by attacker thus causing reputational damage to the company.

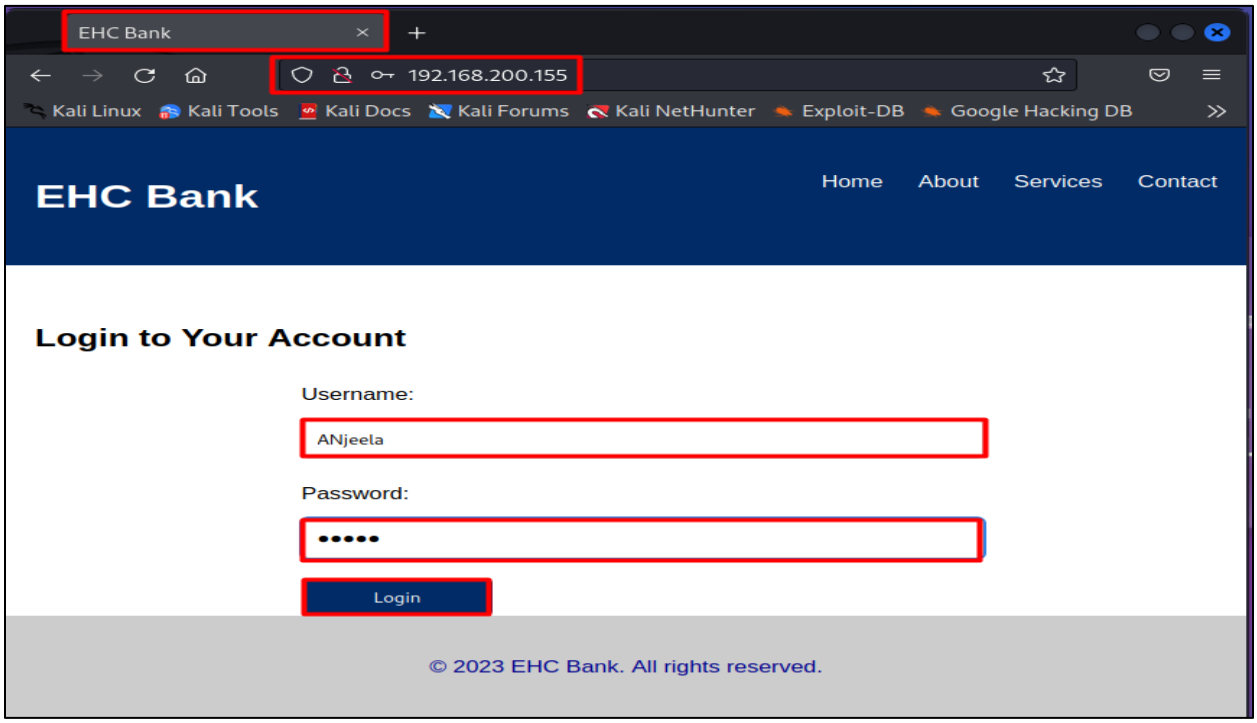


Figure 76 Users trying to log in.

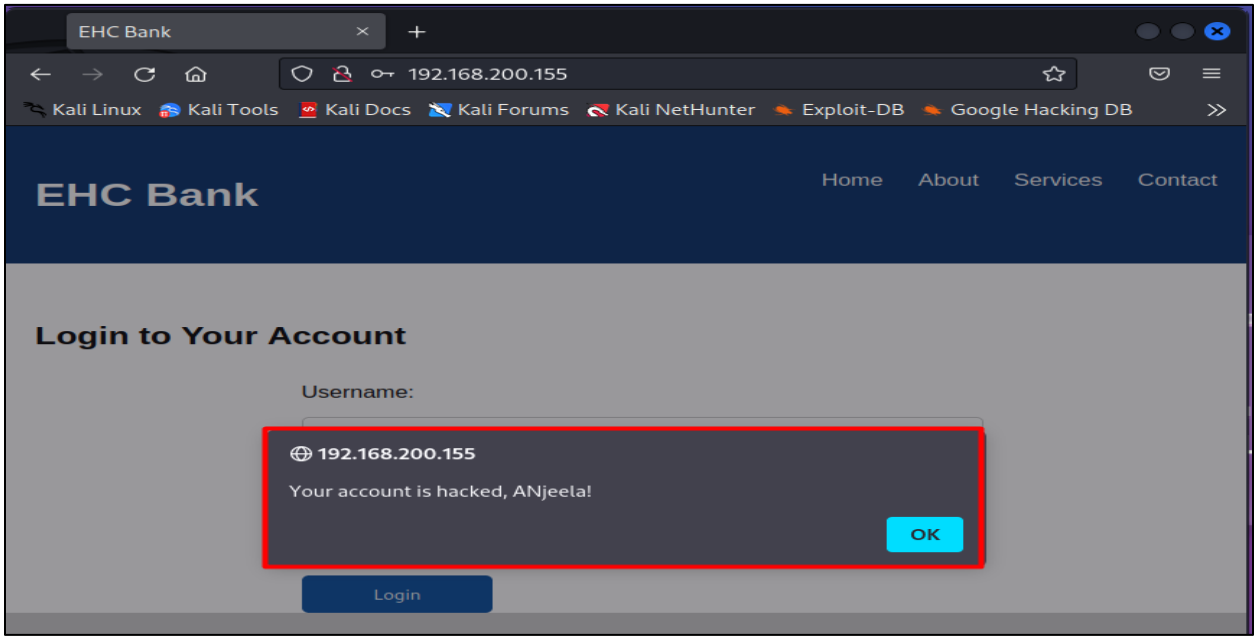


Figure 77 User getting a warning message "Your account is hacked."

7.10. Electronic Transaction Act 2063 (2008) Chapter 9 Article 45,46 and 47.

45. Unauthorized Access in computer Materials: If any person with an intention to have access in any program, information or data of any computer without authorization of the owner of or the person responsible for such a computer or even in the case of authorization, performs any act with an intention to have access in any program, information or data contrary to form such authorization, such a person shall be liable to the punishment with the fine not exceeding three years or with both depending on the severity of offence (lawcommision, 2008).

46. Damage to any computer and information system: If any person knowingly and with a mala fide intention to cause wrongful loss or damage to any institution destroys, damage, deletes, alters, disrupts any information of any computer source by any means or diminishes value and utility of such information or after it injuriously or causes any person to carryout such an act, such person shall be liable to the punishment with the fine not exceeding two thousand rupees and with imprisonment no exceeding three years or both (lawcommision, 2008).

47. Publication of illegal materials in electronic form: (1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes, and communities shall be liable to the punishment with the fine not exceeding one hundred thousand rupees or with the imprisonment not exceeding five years or with both.

(2) If any person commit an offence referred to in subsection (1) time to time he/she shall be liable to the punishment for each time with one and one half percent of the punishment of the previous punishment (lawcommision, 2008).