



 slington college
(इस्लिंग्टन कलेज)

CC7180NI

Security Auditing and Penetration Testing

Individual

2nd Semester

2024/25 Spring/Autumn

Student Name: Manish Gurung

London Met ID: 17030839

College ID: NP01S7S240020

Assignment Due Date: Thursday, January 16, 2025

Assignment Submission Date: Monday, January 13, 2025

Submitted To: Mr. Suraj Nepal

Word Count (Where required): 3005

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.



17030839 Manish Gurung.docx

 Islington College, Nepal

Document Details

Submission ID

trn:oid::3618:79084947

Submission Date

Jan 13, 2025, 12:54 PM GMT+5:45

Download Date

Jan 13, 2025, 12:57 PM GMT+5:45

File Name

17030839 Manish Gurung.docx

File Size

26.0 KB

29 Pages

3,699 Words

22,673 Characters












9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **27 Not Cited or Quoted 9%**
Matches with neither in-text citation nor quotation marks
-  **0 Missing Quotations 0%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 5%  Internet sources
- 1%  Publications
- 8%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.





Match Groups

- 27 Not Cited or Quoted 9%
Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
Matches that are still very similar to source material
- 0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 5% Internet sources
- 1% Publications
- 8% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	www.coursehero.com	2%
2	Submitted works	University of Greenwich on 2021-11-28	<1%
3	Submitted works	CTI Education Group on 2024-06-24	<1%
4	Submitted works	University of Maryland, Global Campus on 2024-04-22	<1%
5	Internet	theceoviews.com	<1%
6	Submitted works	California State University, San Bernardino on 2024-05-07	<1%
7	Submitted works	islingtoncollege on 2024-12-24	<1%
8	Submitted works	University of Sunderland on 2024-04-08	<1%
9	Submitted works	Arab Open University on 2024-11-07	<1%
10	Publication	Karatoprak, Murat. "Implementation and Comparison of Advanced Encryption St...	<1%





11	Submitted works	Southern New Hampshire University - Continuing Education on 2024-01-22	<1%
12	Submitted works	Queensland University of Technology on 2024-10-20	<1%
13	Submitted works	University of Glamorgan on 2010-04-19	<1%
14	Internet	www.arnold-bergstraesser.de	<1%
15	Submitted works	University of Bradford on 2023-03-14	<1%
16	Internet	studyonline.ecu.edu.au	<1%
17	Submitted works	Johns Hopkins University on 2022-06-09	<1%
18	Submitted works	University of Bradford on 2023-03-15	<1%
19	Submitted works	Osmania University, Hyderabad on 2024-08-28	<1%
20	Submitted works	Thornton Township High School District 205 on 2020-06-10	<1%
21	Submitted works	University of Maryland, Global Campus on 2023-06-28	<1%



Table of Contents

Table of Figures	7
Abstract	8
1) Introduction	9
2) Role 1: Security Analyst Conducting Simulated Incidents.....	10
i. Incidents	10
ii. Detailed Execution Steps	12
iii. Analysis of Security Weaknesses	16
iv. Impact Assessment	18
3) Role 2: CISO Preparing Incident Report and Special IS Audit.....	20
1. Executive Summary	20
2. Detailed Incident Report.....	21
3. Containment and Remediation Measures	23
4. Special IS Audit	25
5. Recommendations for Future Prevention.....	27
4) Conclusion.....	29
5) References	30
6) Appendix.....	31
Incident 1: Phishing Attack (Screenshots)	31
Incident 2: Malware Attack (Screenshots).....	34

Table of Figures

Figure 1: Flow chart of the Phishing attack	13
Figure 2: Flow chart of Malware attack.....	15
Figure 3: Taking Source Code (Script) from the organization's website	31
Figure 4: Creating source code for the fake website	31
Figure 5: Creating Bogus website	32
Figure 6: Crafting a Phishing Email	32
Figure 7: Deploying the phishing email to the employee account	33
Figure 8: User login credentials.....	33
Figure 9: Developing a Test Malware File (Ransomware)	34
Figure 10: Created a Ransomware Malware test file.....	34
Figure 11: Crafting a Phishing email with Malware file attached.	35
Figure 12: Deploying phishing email with malware file attached	35
Figure 13: System encryption.....	36

Abstract

The report covers two simulated incidents phishing and malware infection attacks- which were done to test the readiness and preparedness of an organization in confronting cyber-attacks. The simulations were conducted to find flaws, measure the readiness of existing controls, and make recommendations. Based on critical analysis of the execution and the results of these incidents, this report highlights areas of attention and actionable steps to fix them to improve the security posture of the institution further.

1) Introduction

The report below shows the organization's weakness which led to the Phishing and Malware attack incident. The company was found to have many security flaws as well as having an inexperienced security analyst and response team who were unable to handle the incident at the right time. After analyzing the details of the incidents, the organization needs to implement advanced security and policies, provide required training to the employees, upgrade the technical controls and apply an updated advanced defense system to the company.

2) Role 1: Security Analyst Conducting Simulated Incidents

i. Incidents

Incident 1: Phishing Attack Leading to Unauthorized Access

Objective:

This simulation focuses on an attempt at contextual phishing email campaign crafted to elicit employee login credentials. This simulation will attempt to imitate an attacker attempting to access the Institution's sensitive systems by an unauthorized means by sending an intelligent and convincing phishing email.

Expected Outcomes:

- **Evaluate the Effectiveness of Email Filtering Systems:** The testbed will analyze how effectively the organization's security for e-mails is set up to detect and block phishing attempts before they ever reach its employees. It looks into spam filters, URL scanners, and other forms of protective measures.
- **Assess the Impact of Compromised Credentials:** Describe how unauthorized access to sensitive data and systems would be used, then go on to describe possible damage following that access. This outcome also considers the sufficiency of multi-factor authentication and incident response to mitigate such risks.

(Broadcom, 2016)

Incident 2: Malware Infection Targeting Critical Systems

Objective:

The simulation involves a ransomware attack that demonstrates how the malware can infect all key systems of an organization and then spread. It aims to simulate real-world scenarios where malware disrupts operations, encrypts sensitive data, and demands payments in ransom, therefore showing the preparedness of an organization and its response.

Expected Outcomes:

- **Assess the Organization's Ability to Detect and Respond to Malware Infections:** The speed with which an organization's security systems and teams can detect and respond to malware infections should be estimated. They should also consider the effectiveness of antivirus tools, intrusion detection systems, and incident response protocols.
- **Identify Vulnerabilities That Enable Malware to Spread Within the Network:** Identify weaknesses in network configuration segmentation, unsupported software and weak endpoint protections that allow malware to spread. This helps gain insight into those weaknesses, and support those defenses to be prepared against the next attack.

(Headquarters, 2005)

ii. Detailed Execution Steps

Incident 1: Phishing Attack

1. Craft a Phishing Email:

- Design an email as realistic as possible, sourced from a place where employees have learned to trust, such as an internal HR update or an IT notification, to maximize employee interaction.
- Embedded in the email was a phishing link leading targets to a spoofed login page resembling some sort of internal company portal.

2. Simulated Credential Capture:

- Spoofed a login page, which is similar in appearance to the real login interface of the organization, for credential harvesting.
- The collected login attempts were stored in a captured credential storehouse that was secured for post-simulation analysis, ensuring that no actual data breach took place during the exercise.

3. Test Unauthorized Access:

- Used captured credentials to simulate unauthorized access attempts to internal systems, testing the effectiveness of access controls concerning the reach of compromised accounts.

4. Monitor Detection and Response:

- Assessed the organization's ability to detect and respond to phishing emails, including the time taken to mark the email as suspicious.
- Evaluated account lockout mechanisms and incident response processes for speed and effectiveness in case unauthorized access attempts took place.

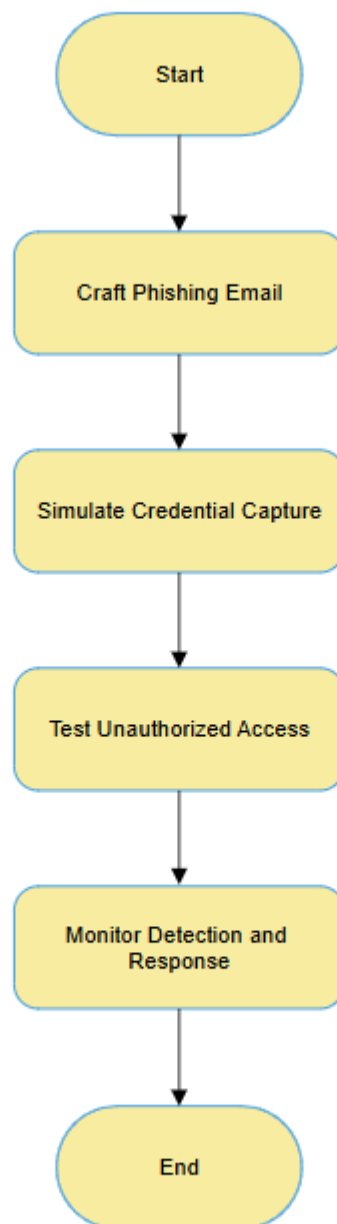


Figure 1: Flow chart of the Phishing attack

Incident 2: Malware Infection

1. Developing a Test Malware File:

- Designed a harmless script that simulates all the activities of how the ransomware works, even down to encrypting a set of dummy files, without touching the organization's systems or data.
- Ensured that the script would be developed to precisely replicate the very encryption patterns and behaviors common in actual ransomware for realistic simulation.

2. Deliver Malware:

- Spread malware along various attack vectors: one from a phishing email with an attachment disguised as a real document, another from a USB drive planted within the organization's premises.
- Conducted analyses of the likelihood of staff experiencing such delivery formats to infer if user awareness training is effective.

3. Simulation Propagation:

- Performed exploitation of known but unpatched vulnerabilities in the network to simulate lateral spread across systems by malware.
- Monitored the malware communicating via shared drives, attached devices, and unsecured endpoints, and highlighted possible network segmentation and security gaps in security posture.

4. Simulate Operational Disruption:

- Carried out the encryption of non-critical files on targeted systems to simulate an actual ransomware attack and left the operational systems and sensitive data intact.
- Monitored the response team's incident actions regarding malware detection, its prevention of spread, and kick-starting recovery processes efficiently.

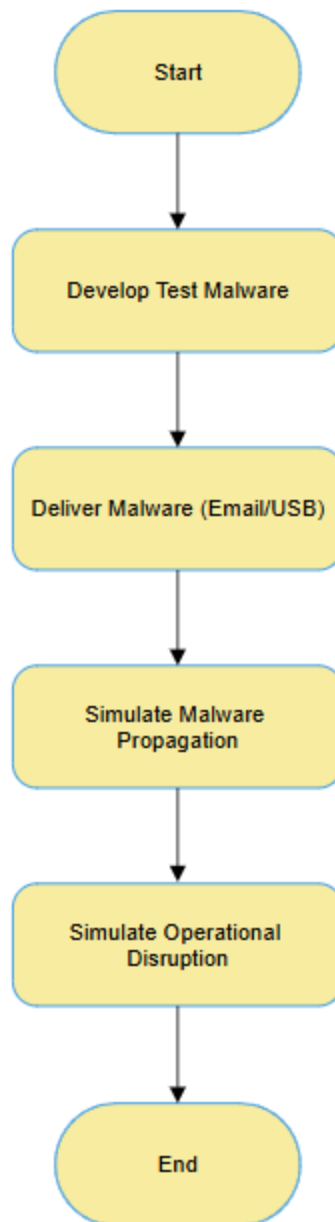


Figure 2: Flow chart of Malware attack

(Institute, 2021)

iii. Analysis of Security Weaknesses

Incident 1: Phishing Attack

Weaknesses Identified:

- **Insufficient Employee Awareness of Phishing Threats:** It was determined that many employees didn't recognize the simulated phishing email sent to test them.
- **Ineffective Email Filtering System:** An inadequate mechanism of the security mail facility within the organization allowed the phishing mail to sail through to the employee's inboxes.
- **Lack of Multi-Factor Authentication (MFA):** Most of the compromised users did not have MFA, and thus were susceptible to unauthorized access.

Suggested Improvements:

- **Conduct Regular Phishing Awareness Training:** The routine training familiarizes users with how to identify and react to such phishing attempts with minimal chances of being attacked.
- **Implement AI-Based Email Filtering:** AI and Machine Learning-based advanced email filtering solutions need to be deployed that can identify and block complex phishing before it ever reaches the user.
- **Enforce MFA Across All User Accounts:** Strong access controls would require multi-factor authentication on all user accounts; this means if an account is breached due to compromised credentials cannot be leveraged further without another layer of verification.

Incident 2: Malware Infection

Weaknesses Identified:

- **Outdated Endpoint Protection Software: Antivirus** software did not detect and block more modern, advanced malware, hence they left the endpoint open to infections.
- **Poor Network Segmentation:** On vulnerable systems, malware can propagate without anything stopping it across the network, which increases the attack surface and amplifies the impact.
- **Failure to Patch Known Vulnerabilities:** Systems that had not been updated with the latest patches were still vulnerable to exploits, thus allowing malware to enter through known vulnerabilities.

Suggested Improvements:

- **Deploy Updated Antivirus Software with the Latest Threat Signatures:** Current endpoint protection solutions ensure that new and emerging threats are detected and mitigated properly.
- **Implement Robust Network Segmentation:** This could mean the isolation of critical systems from less trustworthy networks and will help confine malware spread and/or reduce lateral movement inside a network.
- **Establish a Patch Management Program:** Regular patching and deployment of those patches to all systems will ensure that newly discovered vulnerabilities are patched before they can be exploited by malware.

(Stallings, 2005)

iv. Impact Assessment

Incident 1: Phishing Attack

Financial Impact

Major concerns include fraud as a result of theft or unauthorized access to sensitive financial information, which could involve intellectual property information of business value. In the case of such a breach, fraud might result in various forms: direct monetary loss, or legal and regulatory liabilities, apart from higher operational costs to manage the damage and fix security loopholes.

Operational Impact

The accounts compromised might amount to immense hours of downtime, disrupting critical business operations and/or time-sensitive product or service delivery. Such disruption would not only hamper productivity but will also engage important business hours to manage incidents and recovery, and that's going to further load the organization's workflow.

Reputational Impact

It could also cause irreparable damage to the reputation of the organization in terms of loss of faith by the clients, partners, and stakeholders. The news will go like a bushfire, and becomes hard to regain their trust. Due to loss of confidence, customer loyalty will fall, along with strained partnerships and lowered competitive advantages in the market.

Incident 2: Malware Infection**Financial Impact**

Organizations can pay significant amounts over time, including lost revenue and lost operations. In addition, there may be costs associated with paying ransom if a ransom is issued, as well as legal fees, forensic investigations, and the implementation of strict security measures.

Operational Impact

Business-critical processes will be heavily affected, with resultant delays in service delivery and general inefficiency. It may also shift internal attention to the restoration process. Productivity would thus be affected, and more stress would be put on teams for the resolution of these issues.

Reputational Impact

A cybersecurity incident has the capability of permanently destroying customers', partners', and stakeholders' trust in the organization. Concerns about security and how safe the organization can keep customer data may make people move to other organizations; it may strain the relationship with partners. It follows, after some time, into the brand and a smear on the organization's reputation in enterprise competitiveness.

3) Role 2: CISO Preparing Incident Report and Special IS Audit

1. Executive Summary

Having attended two cybersecurity events, one on phishing and one on malware, we understand the challenges and risks our organization faces. Phishing threats identified significant gaps in our email analysis and employee community technical training, which allowed malicious actors to access and gain unauthorized access to information.

However, malware exposes weaknesses in endpoint protection, patch management, and network segmentation that may potentially cause enterprise-wide operational disruption and loss of data. These incidents have identified a dire need to strengthen our security controls through advanced technical controls, strong policy updates, and employee training on a large scale. The financial impact ranges from costs related to downtime to potential regulatory fines, culminating in reputational damage; therefore, proactive steps are of utmost importance to secure the organization. This report forms the basis on which the necessary changes will be implemented to mitigate future risks effectively.

2. Detailed Incident Report

Incident 1: Phishing Attack

Affected Systems:

- **Email Systems:** These are the email systems whereby the phishing attack was aimed, delivering malicious emails and having employees interact with these emails.
- **Local Network:** It was then able to propagate inside the local network after credentials were harvested and thus compromised other systems.
- **User Accounts:** Those providing credentials had their user accounts directly targeted, which caused the risks of unauthorized access.

Data at Risk:

- **User Credentials:** Attackers can gain unauthorized access to systems and data by way of compromised login credentials.
- **Sensitive Organizational Data:** This could be personal data, financial records, or intellectual property that may be accessed through the hacking and theft of sensitive information.

Severity:

- **Medium:** The incident containment is quite good; however, it can escalate in severity up to unauthorized access and data breaches if security controls to that effect are not implemented.

Business Impact:

- **Disruption of Workflows:** There has been an operational disruption to employees affected by phishing, which hinders productivity and the performance of major tasks.
- **Potential Data Theft:** Exposed sensitive data can result in financial losses, loss of goodwill, and even possible legal liabilities, especially in the case of critical data being leaked or misused.

Incident 2: Malware Infection

Affected Systems:

- **File Servers:** Centralized repositories of critical business data, as well as customer information, were attacked and encrypted, hence lost.
- **Networked Endpoints:** The malware infected several workstations and networked devices, allowing it to laterally move and affect many different systems.
- **Shared Drives:** The malware accessed shared storage areas for massive encryption to disrupt access to critical data.

Data at Risk:

- **Operational Data:** Critical data for operations that is continuously encrypted, without limitation to all files, databases, and system configurations, becomes unreadable.
- **Customer Data:** Sensitive and personal information about customers on compromised systems may be stolen or disclosed.

Severity:

- **Critical:** This was because of the high impact of system downtime, disruption of operation processes, and considerable financial losses from lost productivity, recovery efforts, and possible ransom threats.

Business Impact:

- **Severe Disruption to Key Business Processes:** The attack resulted in widespread service disruption, disrupting customer service lines, ordering processes, and other key business operations.
- **Loss of Client Trust:** The breach exposed client trust in the secured way of data handling and thus may lead to potential customer loss and a weaker competitive posture.

3. Containment and Remediation Measures

Phishing Attack

Containment:

- **Disable Compromised Accounts:** The immediate action taken on compromised accounts is to disable them, which limits any further access, thus reducing the attack surface.
- **Block the Phishing Domain:** No more phishing emails from this domain need to be relayed to the employee base, hence reducing any more attacks.

Remediation:

- **Reset System Passwords:** Requiring users to reset their passwords can help prevent hackers from using compromised credentials to access other systems.
- **Enhance Email Filtering Capabilities:** Implementing a strong email filtering system, including artificial intelligence tools, will help identify and block suspicious emails before they reach the user.

Recovery:

- **Implement MFA (Multi-Factor Authentication):** Multi-factor authentication reduces even a single factor being compromised to afford any unauthorized access.
- **Conduct Phishing Awareness Training:** Continuous training arms your workers with the necessary knowledge on how to identify phishing attempts. This makes people less vulnerable to such kinds of attacks and enhances security.

Malware Infection

Containment:

- **Isolate Infected Devices from the Network:** It can prevent malware from propagating itself to other systems by keeping infected systems off the network and containing the eventual impact of the infection.
- **Terminate Malicious Processes:** Identifying and killing active malware processes would stop further encryption and damage to important files and systems.

Remediation:

- **Restore Encrypted Files from Backups:** Restoring data from a safe, regular backup ensures that an organization can recover important files without paying a ransom or losing data permanently.
- **Update Antivirus Definitions:** Ensure that antivirus software is updated with the latest definitions to enable the detection and removal of new viruses.

Recovery:

- **Perform a Forensic Analysis and Patch Vulnerabilities:** As detailed a forensic analysis as possible will reveal how the malware entered the system and what kind of vulnerabilities were exploited; fixing those very vulnerabilities will prevent similar attacks soon.
- **Patching Vulnerabilities:** Patching systems and software ensures that known security weaknesses are fixed, thus preventing similar attacks quickly.

(Simon, 2002)

4. Special IS Audit

Vulnerability Assessment

Phishing Attack:

- **Email Filtering Misconfigurations:** Most of the email misconfiguration gave way to malicious emails to bypass defenses and render employees towards phishing attacks.

Malware Infection:

- **Exploited Unpatched Software and Insufficient Endpoint Monitoring:** Out-of-date or unpatched software at the endpoints, coupled with poor endpoint monitoring, allowed the malware to enter the network and spread.

Effectiveness of Security Controls

- **Ineffective Email Filtering and Antivirus Software:** The inability of the currently deployed email filtering and antivirus solutions to identify and block phishing attempts and malware has led to the compromise of endpoints and systems.
- **Lack of Real-Time Threat Detection Capabilities:** The lack of real-time threat detection and monitoring systems reduced the ability of the organization to quickly identify and respond to the attacks.

Policy Evaluation

- **Absence of Consistent Security Policies Across Systems:** Inconsistent security policies and procedures across different parts of the organization result in different security levels, making some systems more vulnerable to attack than others.
- **Weak Incident Response Plans:** Inadequate or unclear disaster response plans can hinder an organization's ability to effectively detect, contain, and remediate incidents, leading to extended downtime and data loss.

In conclusion, the audit provided weaknesses which hampered the company in different ways which led to data loss, damage to social image, financial loss and many more. The company can avoid these incidents if the proper security policy is applied to each department. Likewise, providing proper knowledge to the employees about these attacks can make more impact on being secure. Being updated on every step is necessary for the company like upgrading the security controls providing advanced antivirus software for the devices, real-time threat detection and end-point monitoring. Being secure in today's world is hard but with the correct information and implementation of appropriate training, enhancing security policies and other security measures can help the company on reducing these types of attacks in the upcoming days.

5. Recommendations for Future Prevention

Technical Controls

- **Deploy Advanced AI-driven Email Filtering and Endpoint Monitoring Systems:** Advanced AI-based solutions, whether in email filtering or endpoint monitoring, will make giant strides in detecting and blocking phishing emails and malware before they reach an organization.
- **Conduct Regular Vulnerability Assessments and Patch Management:** Continuous vulnerability assessment coupled with proper patch management will go a long way toward discovering and closing security gaps, thereby reducing exploitation opportunities.

Policy Enhancements

- **Mandate Phishing Simulation Exercises for Employees:** Run periodic phishing simulation exercises among employees to make them aware of how to identify and avoid such emails that could lead to credential compromise.
- **Implement a Comprehensive Incident Response Plan:** The constant revision of the incident response plan guarantees timeliness and effectiveness in detecting and responding to, as well as recovering from, information security-related incidents.

Employee Training

- **Regularly Train Employees to Recognize Phishing Attempts and Handle Suspicious Emails:** These ongoing training programs on phishing awareness and best practices for safe emailing will harden the human link in security and make organizations less vulnerable to phishing attacks.

System Improvements

- **Strengthen Network Segmentation to Limit Malware Spread:** Malware is confined to just one part of the network.
- **Ensure Robust Backup Systems for Quick Recovery:** The backup systems should be reliable and secure, which guarantees fast recovery of critical data in case of an infection by malware; this will help minimize downtime or disruption of operations.

(Technology, 2018)

4) Conclusion

These simulated incidents, therefore, have identified serious gaps in the organizational setup concerning cybersecurity, like email filtering, endpoint protection, and vulnerability management, which have easily made the organization a target for phishing attacks and malware infections. To minimize such risks, more emphasis should be placed on enhancing the technical controls of AI-driven email filtering, endpoint monitoring, periodic vulnerability assessment, and patch management. In addition, implementing comprehensive policies such as incident response plans and regularly training employees to recognize phishing attempts will increase the effectiveness of anti-terrorism efforts. Addressing these vulnerabilities will help protect sensitive data, improve security, and retain customers and partners.

5) References

- Broadcom, 2016. *Broadcom*. [Online]
Available at:
<https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=9ab0c6de-926c-4e7f-861f-fcd86b3fe992&CommunityKey=8af7f28f-02f1-4107-8639-93a60b6546d4&tab=librarydocuments>
[Accessed 12 2024].
- GettyImage, 1995. *iStock*. [Online]
Available at: <https://www.istockphoto.com/vector/ransomware-encryption-lock-virus-gm1388154033-445878312>
[Accessed 02 01 2025].
- Headquarters, S. W., 2005. *Detecting Advanced Threats and Evasive Malware with Symantec Cynic*, Mountain View, USA: s.n.
- Institute, S., 2021. *Incident Handling and Response*. [Online]
Available at: <https://www.sans.org/white-papers/>
[Accessed 12 2024].
- Simon, K. D. M. & W. L., 2002. *THE ART OF DECEPTION Controlling the Human Element of Security*. s.l.:Wiley.
- Stallings, W., 2005. *Cryptography and Network Security Principles and Practices*. 4th Edition ed. USA: Prentice Hall.
- Technology, N. I. o. S. a., 2018. *NIST*. [Online]
Available at: <https://csrc.nist.gov/pubs/cswp/6/cybersecurity-framework-v11/final>
[Accessed 12 2024].

Incident 1: Phishing Attack (Screenshots)

- Taking the source code (Script) of an organization's website and creating new source code (Script) to create a fake website.



- Creating bogus website using the source code (Script) of the website.

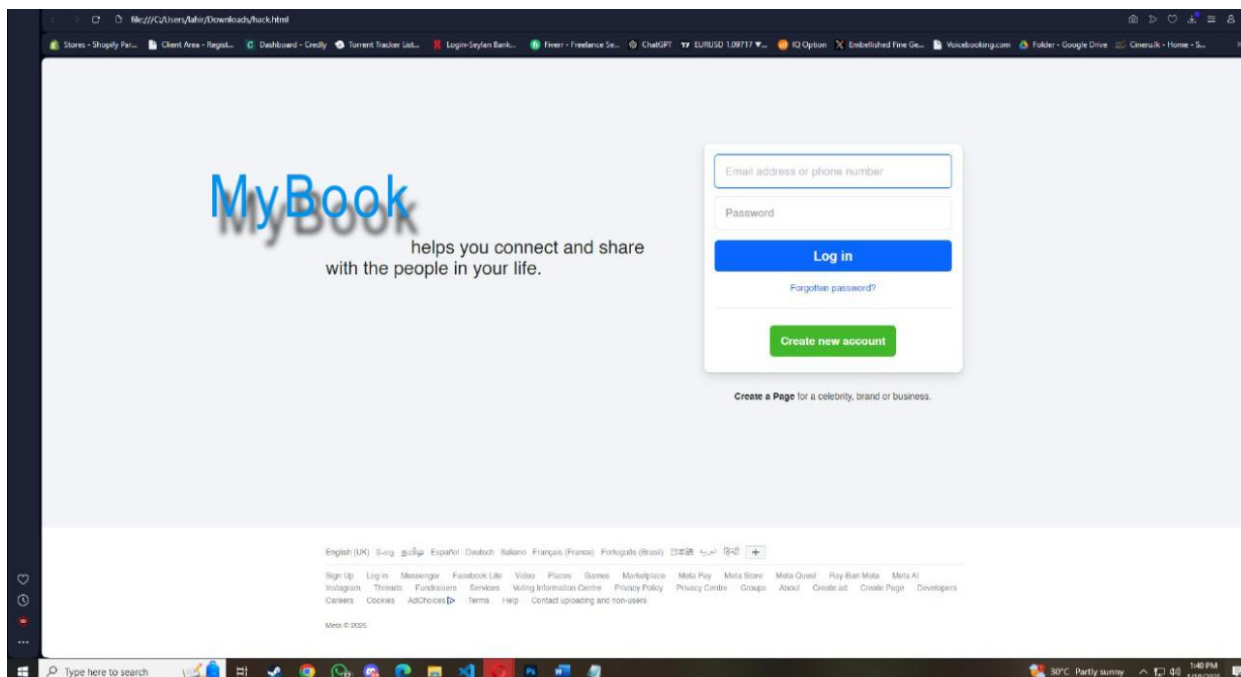


Figure 5: Creating Bogus website

- Crafting a phishing email to send to the employee's device.

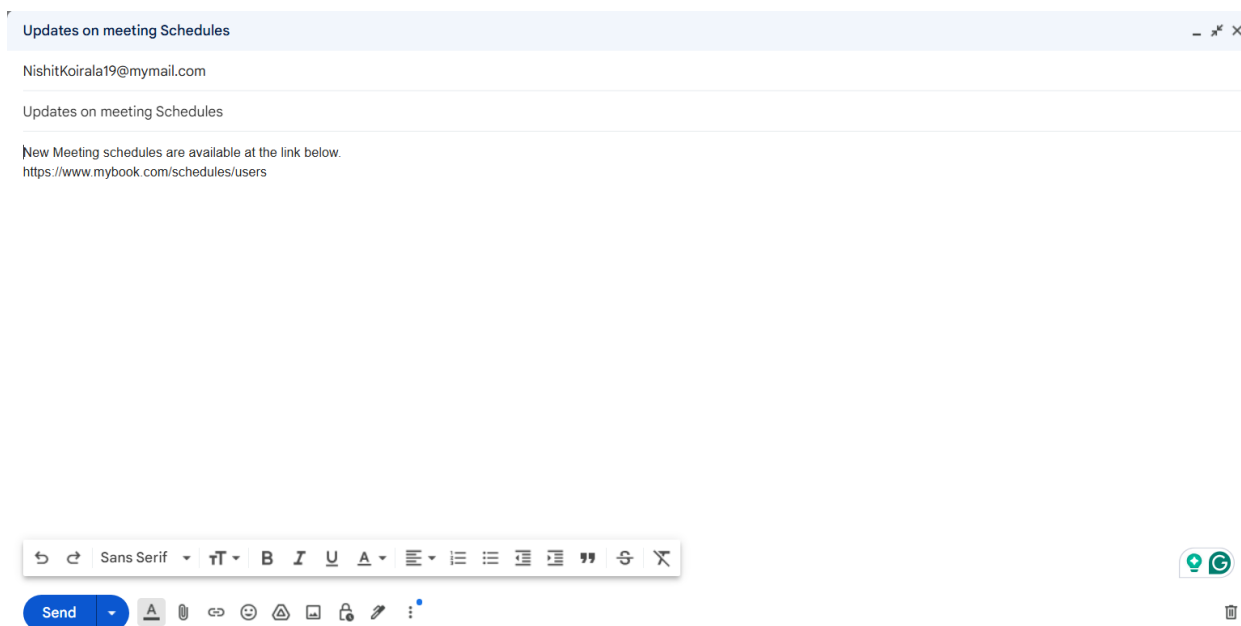


Figure 6: Crafting a Phishing Email

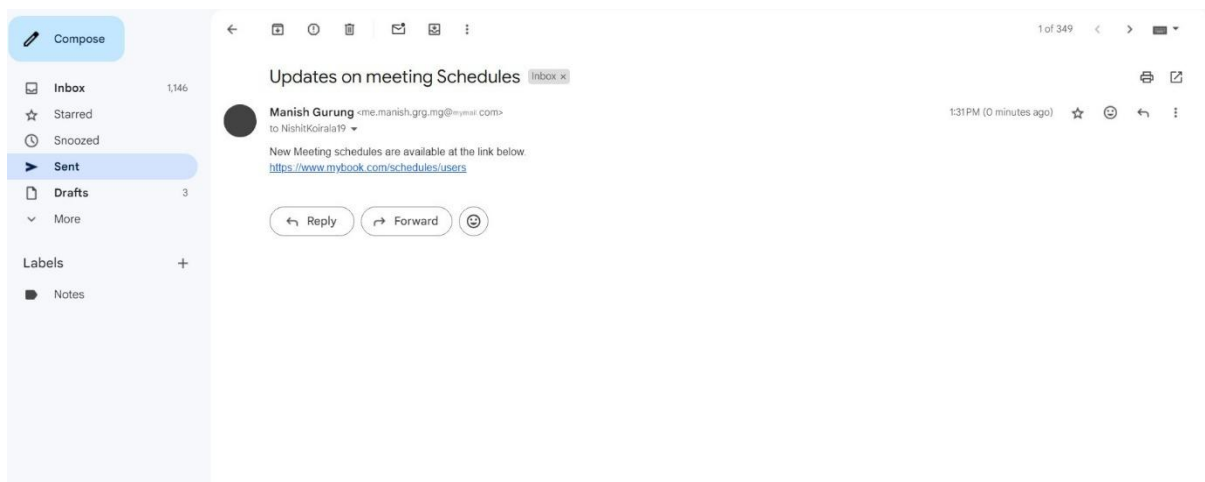


Figure 7: Deploying the phishing email to the employee account

After deploying the phishing email, the employee clicks the link where he/she has to enter their login credentials.

- Obtaining the login/password credentials of the employee.

```
2PHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:1028
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 127.0.0.1
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : NishitKoirala19@mymail.com
[-] Password : Nishithero4321
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. []
```

Figure 8: User login credentials

Detailed steps on how the ransomware attack was done.

- Developing a Test Malware File (Ransomware)

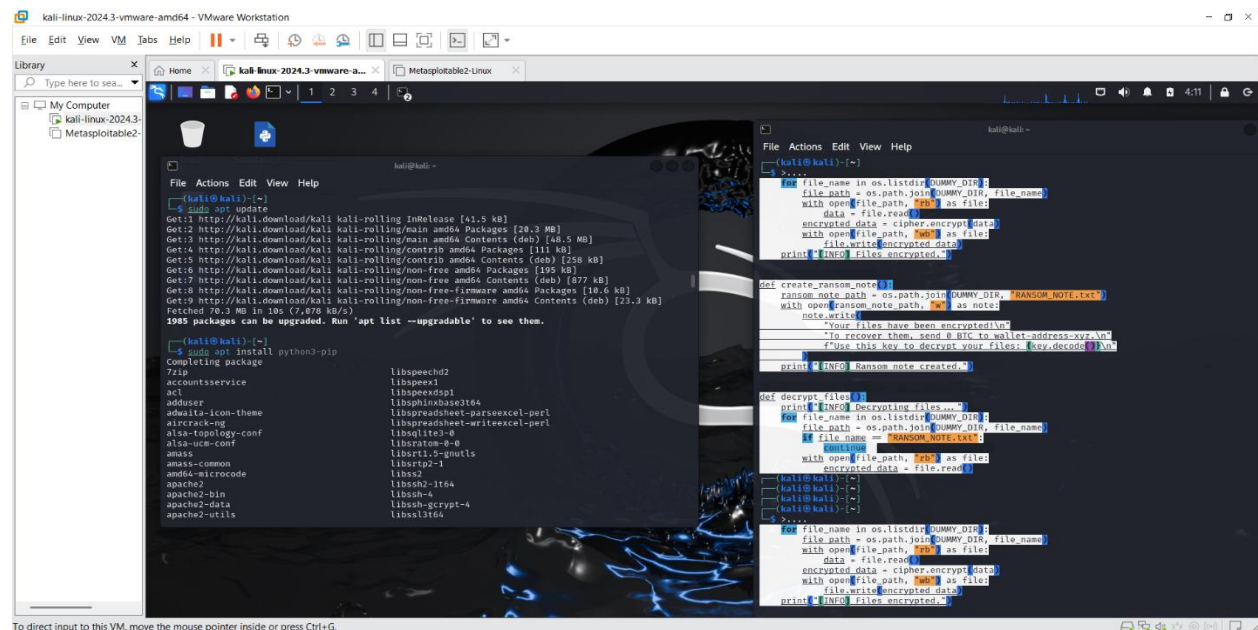


Figure 9: Developing a Test Malware File (Ransomware)

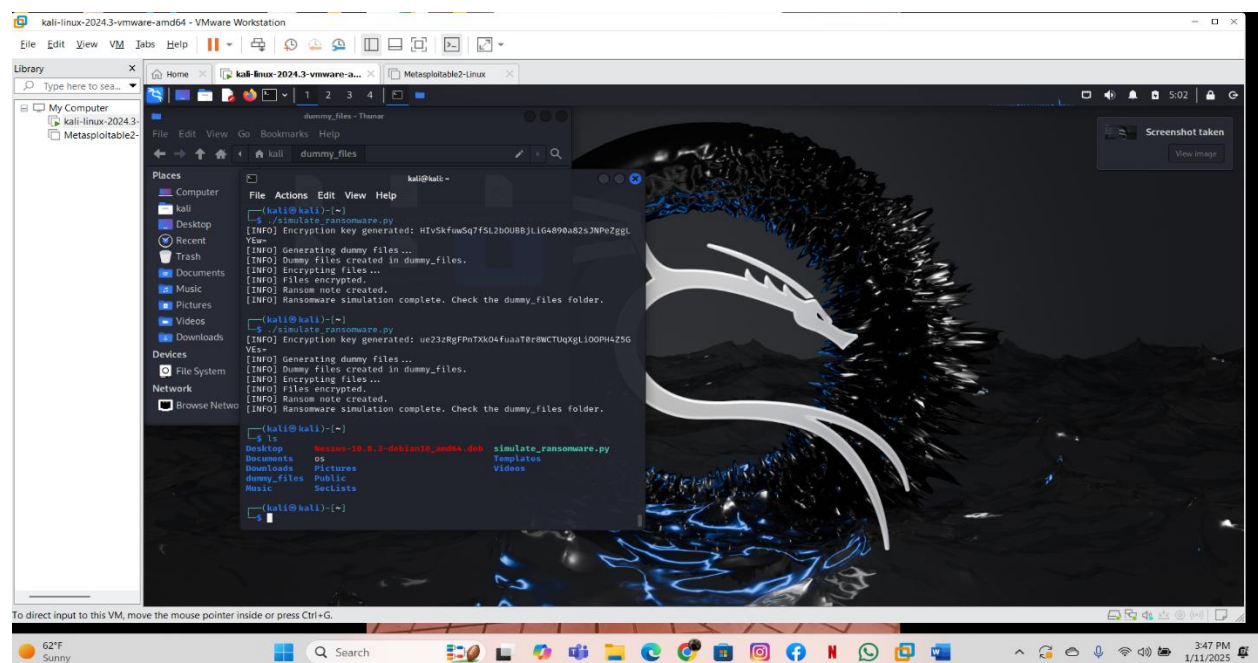


Figure 10: Created a Ransomware Malware test file

- Spread the malware file through phishing emails with an attachment disguised as an organization's document.

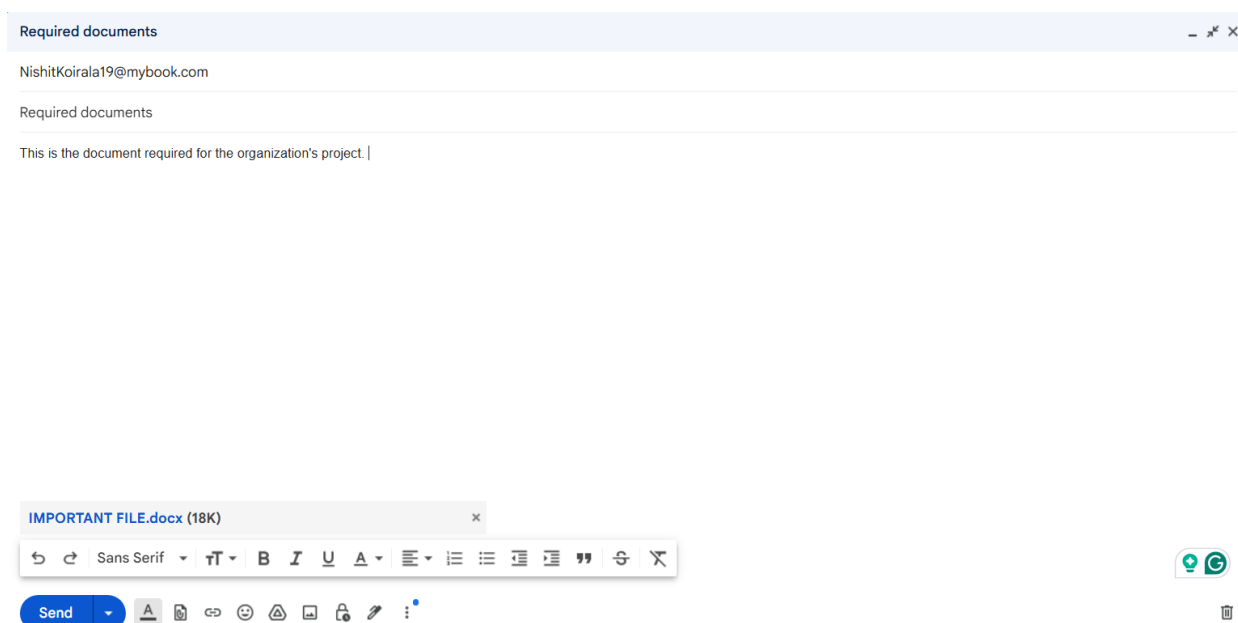


Figure 11: Crafting a Phishing email with Malware file attached.

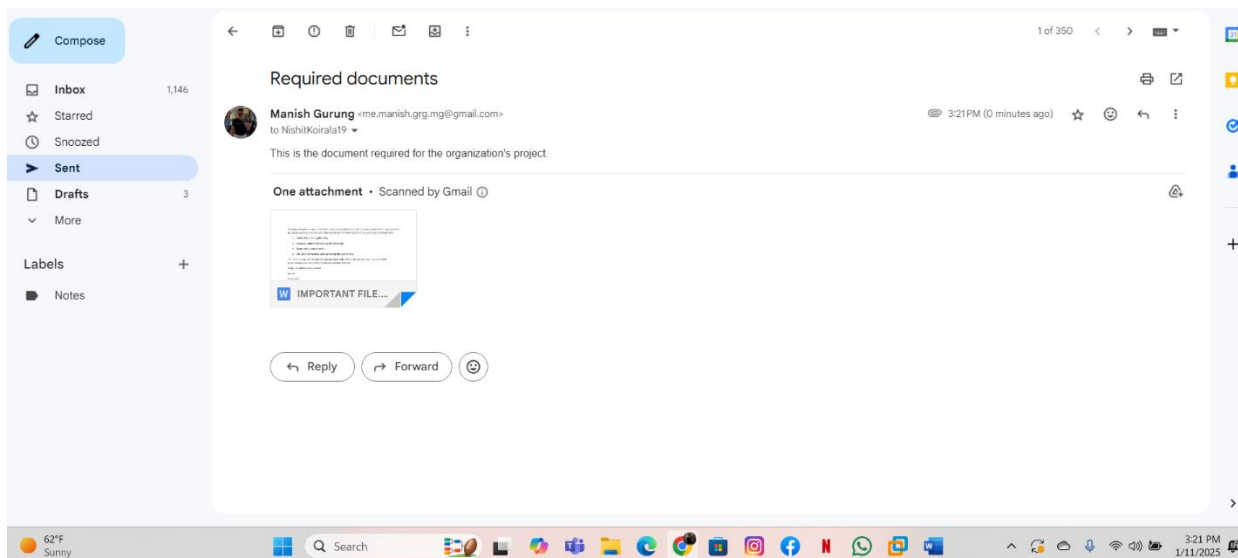


Figure 12: Deploying phishing email with malware file attached

- Activating the malware file as soon as the organization opens the document.

Once the file is opened, the system is locked down, denying access to the user until the ransom is paid.



Figure 13: System encryption

(GettyImage, 1995)