Berk Emre Mert
bmert24@student.oulu.fi

Task 1:

Privacy and Social Engineering: My Perspective

In our class, we learned about privacy issues and the exploitation of leaked information in social engineering attacks. Social engineering attacks are cunning ways of getting individuals to divulge confidential information or to perform an act that compromises security. The following is my understanding of the importance of leaked information, the success rate of these attacks, and some examples on how the attacks work.

Why Leaked Information is Important

Once people share personal details online, these can be used against them. It is not just people but also businesses and organizations that can be exploited. For example, if someone posts that they are expecting a package delivery, an attacker can send a spoof email indicating that there is a problem with the delivery. This would make the email look genuine and increase the chances that the person will take the bait.

Leaked information helps attackers create realistic situations. They may pose as a person you know or use details about your company to make themselves appear as though they are from the company. This makes it harder for you to tell if the message is legitimate or not.

How Successful Are Social Engineering Attacks?

Such attacks succeed because they are based on emotions like trust, fear, or urgency. Attackers will often pose as someone you know or someone in a position of authority. For instance, they can call and claim to be from your bank and that there is a problem with your account. They will instruct you to act quickly, and in doing so, you might forget to check if the call is legitimate.

In the cyber world, attackers are able to use advanced technology like deep fakes to duplicate voices or faces. This further makes it even harder to ascertain if the person contacting you exists or not.

Examples of Social Engineering

Phishing Emails: These are fake emails that come as though from someone familiar to you. The attackers use leaked information to make them real. For example, they might mention a recent transaction or an upcoming event.

Impersonation: The attackers will impersonate someone familiar to you, for example, a colleague or a delivery person. They utilize what they know about you to make their story believable.

Timing is Everything: Attackers tend to strike when you are most vulnerable. For example, if your business is dealing with a security issue, they might impersonate rescuers at that time.

Psychology and Human Behavior

Social engineers apply psychology to trick people:

Establishing Trust: They seek out personal details to make you comfortable with them. This will make you more inclined to share information or disregard security measures.

Exploiting Ignorance: The majority of people are not sufficiently aware of cybersecurity, and attackers take advantage of this ignorance.

Overconfidence: Some people have too much confidence in technology and overlook that humans can be tricked. Attackers take advantage of this to their advantage.

Conclusion

Leaked information is a powerful instrument for social engineering assaults. They are successful because they use psychology to make people do what they wouldn't normally do. From emails that are counterfeit to impersonation using high-end technology, attackers take advantage of trust and unawareness to obtain their goals.

As students, we need to be aware of these risks and do our part to protect ourselves and our institutions. This means being prudent with personal information online and staying current with cybersecurity.

Task 2:

Task 2A)

General Observations for Workstation 1:

-On the desktop computer there is a critical information page named as ‘Vulnerbilities in Apache’ which is marked as ‘Critical’ as well but it’s left open and anyone seeing the windows or passing by can see that page. What can be seen on that page:

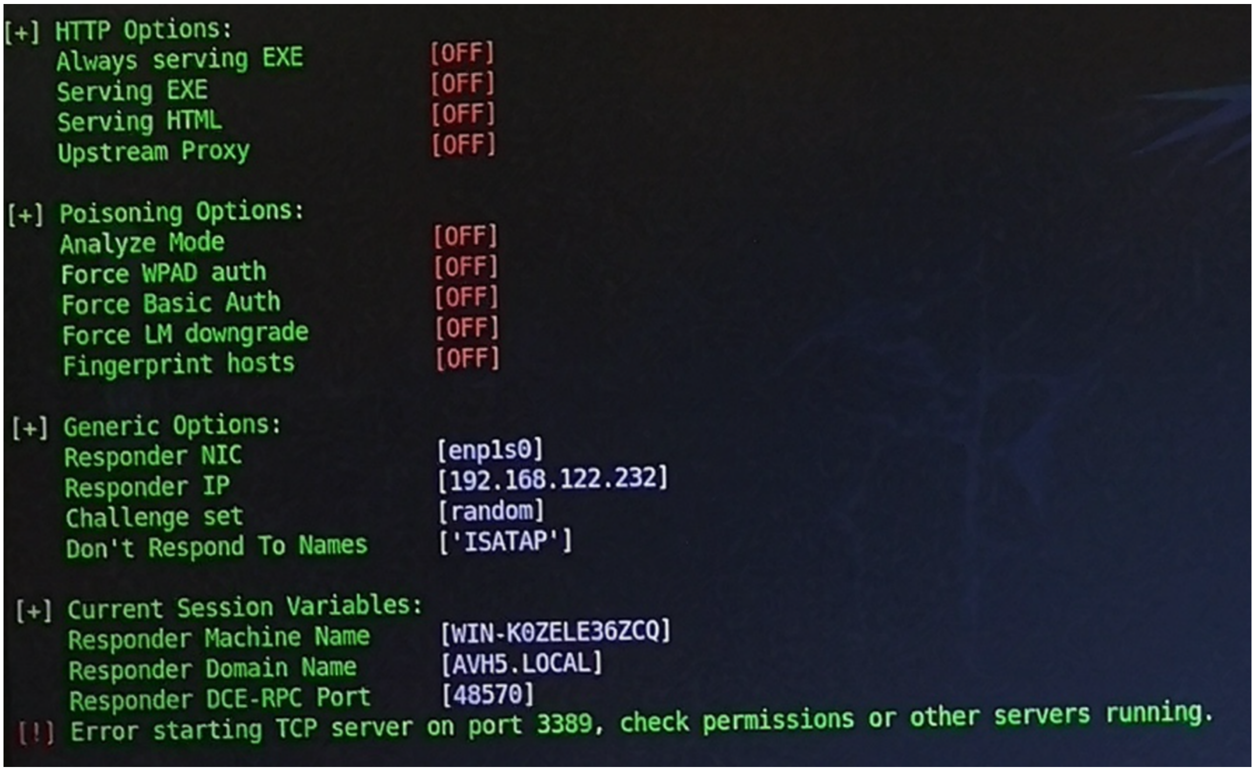
# Advisor ID: Apachi ID of the advisor which is pretty crucial while logging in to the server.

# Summary title on the screen: This part includes very sensitive information about the company. It includes the information that the company uses Apache Log4j2 which doesn’t protect against attacker controlled LDAP and other JNDI related endpoints. From the following link I have reached to more information about the bug and I found further links describing the problem: https://bst.cisco.com/bugsearch/bug/CSCwa47310

From the following link I learned even more information about the bug and it’s leakage: https://www.cve.org/CVERecord?id=CVE-2021-44228

# The template file: On the right side of the screen, a LibreOffice window is open including the file ‘Formal Vulnerability Assesment Template. That file seems like it’s prepared for the supervisor of the worker who observed the Cisco warning and started preparing this file. This file shouldn’t be published publicly but the screen is left open so there is a huge irony here. A person like in the example, can see that screen and take a picture instantly. That file includes ‘Public Water System ID’, so it seems like this server service is most probably for a governmental organization and related to citizens at the first hand. We also soo address details and phone number as well about the population served. We also can see the worker’s information there and most probably that employee has an access to the system.

-On the laptop screen a terminal is open and it’s giving the current information about a server. We see



```
[+] HTTP Options:
    Always serving EXE          [OFF]
    Serving EXE                 [OFF]
    Serving HTML                [OFF]
    Upstream Proxy              [OFF]

[+] Poisoning Options:
    Analyze Mode                [OFF]
    Force WPAD auth             [OFF]
    Force Basic Auth            [OFF]
    Force LM downgrade          [OFF]
    Fingerprint hosts           [OFF]

[+] Generic Options:
    Responder NIC               [enp1s0]
    Responder IP                [192.168.122.232]
    Challenge set               [random]
    Don't Respond To Names      ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name      [WIN-K0ZELE36ZCQ]
    Responder Domain Name       [AVH5.LOCAL]
    Responder DCE-RPC Port      [48570]
[!] Error starting TCP server on port 3389, check permissions or other servers running.
```

I learned the following informations about these data:

1. The current setup allows capturing NTLMv2 hashes from network users who attempt to resolve unknown hostnames.
2. These can be cracked offline using hashcat or John the Ripper.
3. If SMB relay attacks are enabled, captured credentials can be relayed to authenticate against vulnerable systems.
4. If SMB signing is disabled on the network, captured NTLM credentials can be used to gain unauthorized access to systems.

What kind of assumptions can you make about the users of these machines?

What is their possible occupation, operating system, personality/habits they have and what programs they use?

1. Possible Occupation:

- The users are likely IT security professionals, penetration testers, system administrators, or cybersecurity analysts.
- Given the presence of a vulnerability assessment template and exposure of Log4j2 security flaws, they are likely involved in cybersecurity auditing or risk assessment.
- The inclusion of "Public Water System ID" suggests they may work in a government agency or a company providing IT services to public infrastructure.

2. Operating System:

- The desktop likely runs Linux.
- The laptop is running a terminal with server information possibly running security tools.

3. Personality/Habits:

- The users are likely technical and knowledgeable about cybersecurity.
- However, they exhibit poor operational security (OpSec) by leaving sensitive data visible on screens.
- They may be overconfident or careless, not following best practices like screen locking or securing sensitive documents.
- They might work under high stress, causing them to overlook basic security measures.

4. Programs They Use:

- LibreOffice
- Terminal

- Web browser (probably Firefox because it has Pocket extension)
- Network security tools

What kind of attack vectors can you identify and what other observations can you make from these snapshots?

1. Shoulder Surfing / Visual Hacking:

- The open vulnerability page and LibreOffice document can be photographed or read by unauthorized individuals.
- Can be gathered information about server vulnerabilities, network setups, and employee details, leading to social engineering attacks.

2. Credential Exposure & NTLM Hash Capture:

- The laptop's terminal displays NTLMv2 hashes, which can be captured and cracked using tools like *Hashcat or John the Ripper*.
- If SMB signing is disabled, could be relayed credentials to gain unauthorized access.
- The system appears vulnerable to *SMB* relay attacks, which allow to escalate privileges.

3. Log4j2 Exploitation:

- The company uses Apache Log4j2, which is vulnerable to JNDI injection attacks.
- If someone exploits CVE-2021-44228, they could achieve remote code execution (RCE) and take control of affected servers.

4. Government Infrastructure Targeting:

- The presence of a Public Water System ID suggests a link to critical infrastructure.
- Targeting this system could compromise water management services, impacting public safety.

Additional Observations & Recommendations

- Users should lock their screens when leaving their workstation.
- Use screen privacy filters to prevent shoulder surfing.
- Enable SMB signing to prevent relay attacks.
- Mitigate Log4j vulnerabilities by updating to a secure version or disabling JNDI lookups.
- Use multi-factor authentication (MFA) to reduce the risk of credential-based attacks.
- Ensure security awareness training to prevent careless exposure of sensitive information.

General Observations for Workstation 2:

-On the computer screen we see a browser is open with several tabs and the current tab is the information page of AutoDesk's website.

# On AutoDesk's website: Current part is including 'Education Program' prepared freely for students and educators.

# On tabs part: Outlook is open with the current user's email's first part (maksuto…).
Spotify is open with the song's name's first part (Verkkoso…). I found this album online from Spotify: Verkkosukkatyttö EP - EP by Scoogie Bros.
Youtube is open without any video playing.
CNN International and Twitter are there as well.
A Zoom Error page is open.
A weather page is open for the city Lahti (I looked up at it and it's a city in Finland, I'm not from there so don't judge me please).

-On the right side of the monitor there are several sticky notes are attached:

# The first note includes the information for Work Hours (I assume it means Company's own system) username and password, database username and password, Windows 10 username and password.

# Second note includes the information with some candidates (probably for the company's new workers) and their phone numbers. Also the meeting time (I assume for the interview) of Zoom and the password.

# On the third note, there is contact information for the Java related problems. The mail address is technical-support@. Rest of @ is not written so I assume that email address is within the scope of the company.

-On the keyboard a card is attached.

# That card looks mostly like the employee's entry card for the company. The barcode on the card has a number and it's 60040708237607316.

What kind of assumptions can you make about the users of these machines?

What is their possible occupation, operating system, personality/habits they have and what programs they use?

1. Possible Occupation:

- The user is likely a student, educator, HR personnel, or office worker.
- The presence of AutoDesk's Education Program suggests they might be involved in engineering, architecture, or design.
- The sticky notes with candidate details and interview times indicate that they might have HR responsibilities.

2. Operating System:

- The sticky notes mention Windows 10 credentials, meaning this system runs Windows 10.

3. Personality/Habits:

- Disorganized and careless about security, given the presence of credentials on sticky notes.
- They seem to multitask, having multiple browser tabs open.
- Likely distracted or casual at work, as they have Spotify, YouTube, Twitter, and news sites open.
- Forgetful or reliant on physical notes, as they store login information on sticky notes.
- Might be livin in Lahti, Finland.

4. Programs They Use:

- Outlook
- Spotify
- YouTube
- Twitter
- CNN International
- Zoom
- AutoDesk software

What kind of attack vectors can you identify and what other observations can you make from these snapshots?

1. Credential Exposure (Sticky Notes):

- The username and password for multiple systems are physically exposed.
- With access to the workspace, can be easily stolen these credentials.
- If passwords are reused, this could allow access to multiple company systems.

2. Email & Social Engineering Attacks:

- The first part of the user's email (maksuto…) is visible in Outlook.
- Could be guessed or phish the user via email by pretending to be an official contact.

- Candidate details & Zoom meeting password are exposed, making it possible to impersonate HR staff or intercept interviews.

3. Physical Security Risks (Employee Card):

- The barcode on the employee card could be scanned and cloned to gain physical access to the building.
- Could be taken a picture of the barcode and create a duplicate badge.

4. Potential for Credential Stuffing Attacks:

- If the Windows 10 credentials are the same across multiple devices, could be logged into their computer remotely.
- If these passwords are reused on personal accounts, could be gained unauthorized access elsewhere.

5. Zoom Exploitation:

- The Zoom meeting password is written down, allowing an unauthorized person to join the meeting.
- If it's an interview or company discussion, could be eavesdropped on confidential company conversations.

6. Social Media & Web-Based Threats:

- Twitter and news sites suggest the user may be vulnerable to phishing links or social engineering attempts.
- If AutoDesk's Education Program account is linked to company email, might be targeted their AutoDesk account for additional compromise.

Additional Observations & Recommendations

- Remove or encrypt physical sticky notes with credentials.
- Use a password manager instead of writing down passwords.
- Secure the employee entry card—do not leave it exposed.
- Enable multi-factor authentication (MFA) for all critical accounts.
- Monitor email for phishing attempts, as partial email exposure makes them a target.
- Be cautious with Zoom meeting links and passwords to avoid unauthorized attendees.
- Avoid storing sensitive information on publicly accessible desktops.

Task 2B)

E-mail I created:

From: "IT Support" <it.support@cisco.com>
To: [Email On The Screen]
Subject: Urgent: Account Verification Needed

Dear [Name On The Screen],

We have detected unusual activity in your account, and for security purposes, we need to verify your information. To prevent any interruption in service, please follow the instructions below and confirm your identity immediately.

Click the link below to begin the verification process:
https://fake-verification-link.com

If you do not complete the verification within 24 hours, your account will be temporarily suspended.

If you have any questions, please do not hesitate to contact us.

Sincerely,
IT Support Team
Cisco Support Team

Notice: This is an automated message, please do not reply to this email.

ChatGPT link: https://chatgpt.com/share/67e7b758-b870-800c-b5ef-d1c678ebbc54

SpamAssasin Score: 2.6, **The report:**

```
 pts rule                       description
---- ----------------------    --------------------------------------------------
---
 0.1 TO_MALFORMED               To: has a malformed address
 0.0 URIBL_DBL_BLOCKED_OPENDNS ADMINISTRATOR NOTICE: The query to
                                dbl.spamhaus.org was blocked due to usage of an
                                open resolver. See
                                https://www.spamhaus.org/returnc/pub/ [URIs:
                                fake-verification-link.com]
-0.0 NO_RELAYS                  Informational: message was not relayed via SMTP
 0.0 URIBL_BLOCKED              ADMINISTRATOR NOTICE: The query to URIBL was
                                blocked.  See

http://wiki.apache.org/spamassassin/DnsBlocklists…
                                #dnsbl-block for more information. [URIs:
                                fake-verification-link.com]
 0.1 MISSING_MID                Missing Message-Id: header
 1.4 MISSING_DATE               Missing Date: header
 0.0 TVD_PH_BODY_ACCOUNTS_PRE   The body matches phrases such as "accounts
```

```
                                   suspended", "account credited", "account
                                   verification"
    -0.0 NO_RECEIVED               Informational: message has no Received headers
     1.0 SYSADMIN                  Supposedly from your IT department
     0.0 URI_PHISH                 Phishing using web form
```

You can file the .eml file in the repository as well.