NAME: **AIKPOKPODION ENOCH E**.

MATRC NO: **15/ENG02/003**

COURSE NAME: **COMPUTER SECURITY TECHNIQUES**

Table of Contents

[QUESTION 1 3](#_Toc37521202)

[QUESTION 2 7](#_Toc37521203)

[(a) HOW TO CARRY OUT AN ATTACK WITHOUT BEING NOTICED 8](#_Toc37521204)

[(b) SECURITY MEASURES TO PREVENT THE LIKELIHOOD OF OTHER HACKERS PERFORMING THE ACTION IN THE FUTURE 17](#_Toc37521205)

[QUESTION 3 21](#_Toc37521206)

[(a) DECRYPT THE FOLLOWING CODES 21](#_Toc37521207)

[(b) ‘DECRYPT SING THAT RAP FALL’ 21](#_Toc37521208)

[QUESTION 4 22](#_Toc37521209)

# QUESTION 1

Understanding that in an organization, mobile devices are the most vulnerable technological items one can possess and move around with, they are devices which can easily be exploited by hackers. Organizations need to put a strong and solid security policy in place for this technology items, this is important because of its vulnerability.

Mobile devices used in an organization is either provided by the organization itself or it is purchased by the employee, this in one way benefits the user by means of accessibility and comfortability, using the preferred mobile phone and also the organization by reduction of expenses.

On the other way, it exposes the organization to risk (it makes the company vulnerable). This is because employees use their devices for personal, recreational activities, and other activities not relating to the business of their organization.

Since to a reasonable amount of restriction and strictness, it would be okay for a company to allow its users to use mobile phones of their choice to allow accessibility. The security policy which I would be proposing includes practice of the following methods:

1. Use of a secure PIN (Personal Identification Number) or password.
2. Regular backup of data on the device.
3. Restriction of connection to public networks.
4. Regular software version check to keep software up to date.
5. Storing MAC (Media Access Control) address of devices for each user.
6. Reporting immediately if mobile device is lost or mobile device is stolen.
7. Encryption of the mobile device against intruders.
8. Restriction of access to data according to location defined by the organization
9. **USE OF A SECURE PIN (PERSONAL IDENTIFICATION NUMBER)**

PIN (Personal Identification Number) is a security code used to verify one’s identity, it is similar to a password, it should be confidential and should be kept secret because it can allow access to sensitive information about the organization such as financial transactions. Since security would always be a concern, it would be wise to use a pin that is difficult to guess.

* Avoid using simple pins sequence like 1234,0000
* Significant dates such as date of birth, spouse birthday
* Any part of home address
* Any part of phone number

It is useful to understand that longer PINS are safer than shorter PINS (if one uses a 4-digit PIN, there 10,000 possible variations but with a 6-digit PIN, there are 1 million possible codes.)

1. **REGULAR BACKUP OF DATA ON THE DEVICE**

Backing up data on mobile phones used for an organization are essential because they seem to wear out and one might lose data, also, the internet harbors many potential threats to data on a mobile phone. Malwares like viruses and trojans do not just steal data they also erase them in some cases. Also, threats from ransomware where a hacker puts a virus in a mobile phone that encrypts the data, making it useless. The organization might have to pay a ransom to unencrypt the data with no guarantee if it would be recovered or not.

1. **RESTRICTION OF CONNECTION TO PUBLIC NETWORKS**

Considering the massive flaw of WPA2 (Wi-Fi Protective Access), it is not advisable to make use of a public network with a mobile phone which has sensitive information about an organization. This is because information can be easily understood and even if it is encrypted. One of the biggest threats is the ability of hackers to position themselves between the connection point and the mobile phone, it could end up to sending information to the hacker.

1. **REGULAR SOFTWARE UPDATE CHECK TO KEEP SOFTWARE UP-TO-DATE**

Software updates are so important because they often include critical patches to security holes in software or operating system. Many or more harmful malware attacks take advantage of vulnerability in software. These big problems require updates to be kept safe and stable.

1. **STORING MAC ADDRESS OF EACH USER**

MAC (Media Access Control) addresses are present in every mobile device and what they do is that they allow user connect to a network, they allow the network device to attract the attention of a single directly connected device. Network cards each have a unique MAC address. Packets that are sent on the ethernet are always coming from a MAC address and sent to a MAC address. If a network adapter is receiving a packet, it is comparing the packet's destination MAC address to the adapter's own MAC address. If the addresses match, the packet is processed, otherwise it is discarded. This means that if MAC address of a mobile phone is stored, it can be used for access control in an organization to limit the availability of information to the user and whereas, there can be a fixed computer that would have full access.

1. **REPORTING IMMEDIATELY IF MOBILE DEVICE IS STOLEN OR LOST**

It is important to always report lost or stolen mobile devices to an organization so that the organization can take proper step such as blocking the device from gaining access to information and also erasing the data on the device if possible.

1. **ENCRYPRTION OF THE MOBILE DEVICE AGAINST INTRUDERS**

It is a good practice to always sensitive and valuable encrypt information because an encrypted data makes an intruder find it difficult to understand and also, it makes it meaningless on sight.

# QUESTION 2

Firstly, an Industrial Espionage is someone who embraces illegal and unethical methods of collecting corporate data. It involves stealing intellectual property, sensitive data and trade secrets to use them for competitive advantage. The theft of economic information sponsored by foreign states is called economic espionage. It’s done not just for profit but for strategic reasons.

The usual targets of an industrial espionage are the following:

* **Trade secrets:** It generally means protected information about existing products or products in development. While definition of “trade secret” varies from country to country, this information may help your rivals make their products more competitive or even bring a similar product to the market faster than you can.
* **Client information**: Data of your clients, including their financial information, can be used to steal business or can be leaked to damage the reputation of your company.
* **Financial information**: Financial information about your company can be used to offer better deals to your clients and partners, win bids, and even make better offers to your valuable employees.
* **Marketing information**: This will allow your competitors to prepare a timely answer for your marketing campaigns, which, in turn, may render them ineffective.

As an industrial espionage hired by XYZ company, the following would be the way to carry out an attack without being noticed.

First of all, these are the tools I would use.

1. I would get an external different NIC (Network Interface Card) which would allow the computer to connect to network is better to be used than the internal network interface card because it can be replaced and it helps anonymity.



1. I would get a laptop which is specifically going to be Kali Linux because it is capable of working on network security, forensic analysis and penetration testing and it makes available the latest tools and updates to have control, access to tools for hacking and to protect hackers from the new known threats.
2. Have versatile knowledge in the various operation of the Linux computer (White hat, Black hat, Grey hat)

## HOW TO CARRY OUT AN ATTACK WITHOUT BEING NOTICED

The method I would for the attack is going to be Social Engineering, Dumpster Diving, Penetration testing and some other methods. Social Engineering involves attempting to trick system users or administrators into doing something in the interest of the social engineer, but beyond the engineer’s access or rights. Social Engineering attacks are normally harmful to the information system or user. I would use people’s inherent need to help others to compromise the information system. Common Social Engineering techniques include trying to get help desk analysts to reset user account passwords or have end users reveal their passwords enabling the

Social Engineer to log in to accounts they are not authorized. This technique includes phishing and spear phishing.

* **Phishing** is when the social engineer attempts to get the targeted individual to disclose personal information like user names, account numbers, and passwords. This is often done by using authentic looking, but fake, emails from corporations, banks, and customer support staff. Other forms of phishing attempt to get users to click on phony hyperlinks that will allow malicious code to be installed on the target computer without their knowledge. This malware will then be used to remove data from the computer or use the computer to attack others. Phishing normally is not targeted at specific users but may be everyone on a mailing list or with a specific email address extension
* **Spear phishing** is a form of phishing in which the target users are specifically identified. For example, the attacker may research to find the email addresses of the Chief Executive Officer (CEO) of a company and other executives and only phish these people.

**Dumpster Diving**: In Dumpster Diving, the assessor filters through trash discarded by system users and administrators looking for information that will lead to further understanding of the target. This information could be system configurations and settings, network diagrams, software versions and hardware components, and even user names and passwords. The term refers to entering a large trash container, however “diving” small office garbage cans if given the opportunity can lead to lucrative information as well.

Also, other methods for intrusion includes attacking the network of XYZ organization from the outside by first configuring the network interfaces.

This can be done by the following commands

 ‘ifconfig -a’ this shows the list of all available network cards on the computer.

Then DHCP (Direct Host Configuration Protocol) is configured using the next command

nano /etc/networking/interfaces

#add the following lines##

auto eth0

iface eth0 inet static

address {IP\_Address}

netmask {netmask}

gateway {Gateway\_IP\_Address}

Many times, the penetration tester will not want to use the actual MAC address of the adapter that is being used on the computer. This may be done to bypass simple security procedures such as MAC address filtering where only systems with specific MAC addresses are allowed to connect to the network. This can also be done to masquerade your wireless adapter to appear

to be from another manufacturer to match those wireless cards being used on the wireless network.

After all these are done, I would build a LAB which basically means an environment for work, this is done with VirtualBox, VMWare player. The two software have their advantages and disadvantages.

**PENETRATION TESTING**

Most people assume that all a penetration tester, or hacker, needs to do is sit down in front of a computer and begin typing an obscure string of code and voila any computer in the world is instantly opened. This stereotype based in movies is far from the truth. Professionals in the field of penetration testing are very meticulous in the approach used when uncovering and exploiting vulnerabilities in computer systems. Over time a proven framework has emerged that is used by professional ethical hackers. The four phases of this framework guide the penetration tester through the process of empirically exploiting information systems in a way that results in a well-documented report that can be used if needed to repeat portions of the testing engagement. This process not only provides a structure for the tester but also is used to develop high-level plans for penetration testing activities. Each phase builds on the previous step and provides detail to the step that follows. While the process is sequential, many testers return to earlier phases to clarify discoveries and validate findings.

The Phases include

1. Reconnaissance
2. Scanning
3. Exploitation
4. Maintaining access
5. Reporting

Using military strategy and scenario to explain these different phases

**Reconnaissance**: In a small room with dim lights, analysts and officers scan and inspect maps of hostile territory. Across the room others watch television channels across the globe frantically taking notes. The final group in this room prepares a detailed assessment of everything about the target being investigated. While this scenario details what would normally be done in a military reconnaissance of a possible target, however, it is analogous to what the penetration tester will do during the reconnaissance phase of the penetration testing lifecycle.

This illustrates the type of work done during the reconnaissance phase of the pentesting lifecycle. This phase focuses on learning anything and everything about the network and organization that is the target of the engagement. This is done by searching the Internet and conducting passive scans of the available connections to the targets network. In this phase, the tester does not actually penetrate the network defenses but rather identifies and documents as much information about the target as possible.

**Scanning**: Imagine a hilltop deep behind enemy lines, a single soldier crouches hidden among a thicket of bushes and trees. The report being sent back informs others about the location of the camp being observed, the mission of the camp, and types of work that is being done in each building. The report also notes the routes in and out of the camp and types of security that can be seen.

The soldier in this example had a mission defined by the analysis conducted during the reconnaissance phase. This is true of the second phase of the penetration testing lifecycle. The tester will use information gained in phase 1 to start actually scanning the targets network and information system. Using tools in this phase, a better definition of the network and system infrastructure of the information system will be targeted for exploitation. The information gained in this phase will be used in the exploitation phase.

**Exploitation**: Four soldiers rush through an open field, the moon is only a sliver and obscured by clouds, however, the soldiers see everything is an eerie green glow. They rush the building slipping through a gap in the fence and then through an open back door. After just moments on the target they are on the way back out with vital information about future troop movements and

plans for the coming months.

Again, this matches what the ethical hacker will do in the exploitation phase. The intent of this phase is to get into the target system and back out with information without being noticed, using system vulnerabilities and proven techniques.

**Maintaining access**: Based on drawings provided by the raid team, a group of skilled engineers excavate earth from deep in the tree line under the room that held the vital information taken earlier. The purpose of this tunnel is to provide easy access to the room for continued exploitation of the enemy. This is the same for the tester, once the system is exploited backdoors and rootkits are left on the systems to allow access in the future.

**Reporting**: The raid team commander stands in front of a group of generals and admirals explaining the details of the raid. Each step is explained in great detail expanding on each detail that allowed the exploitation to take place. The penetration tester too must develop detailed reports to explain each step in the hacking process, vulnerabilities exploited, and systems that were actually compromised. Additionally, in many cases one member of the team, and sometimes more, may be required to provide a detailed briefing to senior leadership and technical staff of the target information system.

During reconnaissance, the following can be acquired from XYZ company

* organizational structure including detailed high-level, departmental, and team organizational charts;
* organizational infrastructure including IP space and network topology;
* technologies used, including hardware platforms and software packages;
* employee email addresses;
* organizational partners;
* physical locations of the organizational facilities;
* phone numbers

Another method I would use is **DNS attack on the company’s network**;

Domain Name Services, or DNS, provides addressing help for the Internet. Generally, people have a better time remembering and using names, like Google.com, while computers have an easier time using numbers like 173.194.46.19 (one of Google’s addresses). The hierarchical structure of the Internet also makes the use of numbered octets more efficient. This creates a

problem where the best addressing scheme for people does not match the best scheme for computers. Name servers help to solve this problem by serving as translators between computers and people.

These name servers are set up in a hierarchical order with top-level domain (TLD) servers, serving main domains, such as .com, .gov, .edu, and many others. At the other end of the name server hierarchy each network can have its own name server that allows local services and computers to be accessed by name instead of by IP address.

Name servers contain a lot of useful information, well beyond web pages. For example, the name server will contain the mail server, or MX record, for the domain, other named computers or “A” records and other helpful information.

By querying a domain name server, one has to do the following in Kali Linux:

The following command entered in the Kali Linux terminal will query the name server assigned to the local computer.

‘nslookup’

This will result in a carrot (>) being displayed in the terminal indicating the system is awaiting input. Type the following command to query the local name server to determine the IP address of the Google web page.

> www.google.com

This will return a number of IP addresses both authoritative (the first responses) and nonauthoritative, those following the nonauthoritative note. Nonauthoritative answers are a great source of information as this term only indicates the information is provided from the server’s cache.

To exit from nslookup use the following command.

>exit

The nslookup command will use the name server defined for the local machine. To display the name servers being used for the current nslookup commands use the following command.

nslookup

>server

The command nslookup can return other information as well. For example, to search for all of the mail servers type the following commands.

>set type5MX

>google.com

This will return all of the known mail servers for the Google domain. Identifying the different types of records about the target can be an important part of completing reconnaissance. As stated earlier the nslookup command, by default, uses the locally defined name server. In Kali Linux, the name server is defined in the resolv.conf file located in the /etc directory. Use the

following commands to identify the locally defined name server.

cat/etc/resolv.conf

The name server used by nslookup can be changed to the target domains

name server. First identify the targets name server with the following

command.

**r**

nslookup

>set type= ns

>google.com

In Scanning, it mostly deals with networks and their protocols, one has to understand the network traffic, the firewall in place to protect the network, understanding the Internet Protocols (IP) including TCP (Transfer Control Protocol) and UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol).

Using traceroute to know the different computers initiating communication. This command works by manipulating the packets time to live value or TTL. The TTL is the number of times the packet can be rebroadcast by the next host encountered on the network or hops. The command will start with a TTL value of 1 indicating the packet can only go as far as the next device between the initiator and the target. The receiving device will send back an ICMP type 11, code 0 packet (time exceeded), and the packet is logged. The sender increases the TTL by 1 and sends the next series of packets. The packets will reach their expected time to live at the next hop along the network; which in turn, causes the receiving router to send another time exceeded reply. This continues until the target is reached, and all hops along the way have been recorded, creating a listing of all devices between the initiating computer and the target. This can be helpful for a penetration tester when determining what devices are on a network. Windows platforms have a

default TTL of 128, Linux platforms start with a TTL of 64, and Cisco networking devices have a whopPing TTL of 255.

Exploiting a computer, networking device, or web service is great; however, the goal of most penetration tests is to maintain access to the compromised system. There are a number of methodologies for maintaining access to exploited victim systems; however, the overarching conclusion of every methodology is not to steal information but to reduce the time-consuming and exhaustive efforts required to keep attacking the same machine over and over after it’s already been compromised. If a security tester is working with a team, remote collocated servers or is in need of a secondary access point for a later access to the computer system, then efforts and expectation can be easily managed and further attacks can be more precise. Maintaining access is a secondary art form that involves just as much, if not

more, thought than the exploitation of a system. This chapter covers the basic concepts of security testers and hackers alike use to maintain access and keep the compromised session going.

## (b) SECURITY MEASURES TO PREVENT THE LIKELIHOOD OF OTHER HACKERS PERFORMING THE ACTION IN THE FUTURE

After all these actions have been performed, the following are preventive measures that I would propose to XYZ company

1. Update the OS (Operating System) used by XYZ company and other software frequently, that is if it is not automatically. This keeps hackers from accessing the computer through vulnerabilities in outdated programs (which can be exploited by malware). Also, consider retiring particularly susceptible software such as Java or Flash when going to the internet, especially as many sites and services continue to move away from them.
2. Download up-to-date security programs, including anti-malware software with multiple technologies for protecting against spyware, ransomware, and exploits, as well as a firewall, if the OS didn’t come pre-packaged with it. (One should check if the OS has both firewall and antivirus built in and enabled by default, and whether those programs are compatible with additional cybersecurity software.)
3. Destroy all traces of the organization's info on hardware is they plan on selling to buy new devices. Consider using a software like as d-ban to erase all data from the hard drive. For those looking to pillage your recycled devices, this makes information much more difficult to recover. If the information the organization is trying to protect is critical enough, removing the platters where the information is stored then destroying them is the way to go.
4. XYZ company should make a security policy that its employees do not use open Wi-Fi on their devices; it makes it too easy for threat actors to steal the connection and download illegal files. Protect the Wi-Fi used with an encrypted password, and consider refreshing the equipment every few years. Some routers have vulnerabilities that are never patched. Newer routers allow you to provide guests with segregated wireless access. Plus, they make frequent password changes easier.
5. Speaking of passwords and mobile devices: password protect all of the devices, including your desktop, laptop, phone, smartwatch, tablet, camera. The ubiquity of mobile devices makes them especially vulnerable. Lock your mobile phones and make the timeout fairly short. Use fingerprint lock for the iPhone and passkey or swipe for Android. “It’s easy to forget that mobile devices are essentially small computers that just happen to fit in your pocket and can be used as a phone,” says Jean-Philippe Taggart, Senior Security Researcher at Malwarebytes. “Your mobile device contains a veritable treasure trove of personal information and, once unlocked, can lead to devastating consequences.”
6. Also, for password, Sensing a pattern here? Create difficult passwords, and never use the same ones across multiple services. If that’s as painful as a stake to a vampire’s heart, use a password manager like LastPass or 1Password. For extra hacker protection, ask about two-step authentication. Several services have only recently started to offer 2FA, and they require the user to initiate the process. Trust us, the extra friction is worth it. Two-factor authentication makes taking over an account that much more difficult, and on the flip side, much easier to reclaim should the worst happen.
7. Come up with creative answers for security questions. People can now figure out your mother’s maiden name or where you graduated from high school with a simple Google search. Consider answering like a crazy person. If Bank of America asks, “What was the name of your first boyfriend/girlfriend?” reply, “Your mom.” Just don’t forget that’s how you answered when they ask you again.
8. Practice smart emailing. Phishing campaigns still exist, but cybercriminals have become much cleverer than that Nigerian prince who needs your money. Hover over links to see their actual URLs (as opposed to just seeing words in hyperlink text). Also, check to see if the email is really from the person or company claiming to have sent it. If you’re not sure, pay attention to awkward sentence construction and formatting. If something still seems fishy, do a quick search on the Internet for the subject line. Others may have been scammed and posted about it online.
9. Make use of VPN connections in the organization because they are more secure.
10. Keep sensitive data off the cloud. “No matter which way you cut it, data stored on the cloud doesn’t belong to you,” says Taggart. “There are very few cloud storage solutions that offer encryption for ‘data at rest.’ Use the cloud accordingly. If it’s important, don’t.”

# QUESTION 3

## (a) DECRYPT THE FOLLOWING CODES

 **3** HAMLETS

 **1** ORACLE

 **9** MESSENGERS

 **1** SHELL

 **4** RODENTS

 **1** CALABASH

 **3** PROPHECIES

 **1** DESTINY

 **6** COWRIES

To decrypt the codes, I noticed that each number before each letter in the column was pointing to the position of the letter in the word (provided that it starts from 1). So, for 3 HAMLETS, M is the word 3 is pointing to.

Therefore, if all the letters in each word are gotten according to the position of numbers, the decrypted code is **MORSECODE**.

## (b) ‘DECRYPT SING THAT RAP FALL’

The decrypted text is **THINGS FALL APART**

# QUESTION 4

1. Caesar substitution cipher (key 5)

Default when in key 0 - **ABCBEFGHIJKLMNOPQRSTUVWXYZ**

With Caesar key 5 – **VWXYZACDEFGHIJKLMNOPQRSTU**

Therefore, the decrypted Caesar cipher is **ONENAMCBOELOIUN**

1. Columnar transposition cipher (key 5)

Using key = abcde

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| a | b | c | d | e |
| 1 | 2 | 3 | 4 | 5 |
| o | n | C | e | i |
| n | a | b | l | u |
| e | m | o | O | n |

The plain text is therefore ‘**ONCE IN A BLUE MOON**’