

**NAME: BOSAN RIYASAI JOY**

**MATRIC. ON: 15/ENG02/012**

**COMPUTER ENGINEERING**

**COE510 ASSIGNMENT**

### **QUESTION 1**

Mobile devices are among the most vulnerable tech items we own, because they're easily exploited and can be quickly compromised by hackers. It's essential for the company to have a solid security policy in place for mobile devices.

Below is a list of best practices for securing a mobile device for its employees:

- Keep the software up to date
- If you lose it or it's stolen, report it immediately
- Use a secure PIN
- Don't connect to public wi-fi networks
- Backup your device
- Encrypt your device

It is important to make sure that XYZ devices can only be used in so-called 'demilitarized zones' within the organization. That is, the devices should not be able to directly access sensitive resources, and access should only be allowed to some organizational resources through VPNs. It is also important to be able to monitor the use of such devices through the network, and keep track of when, where, and how these devices connect.

In order to reap the benefits while mitigating physical and digital security risk, corporate leaders and risk managers must provide an Acceptable Use Policy that specifies how employees can use their own devices to access and process corporate data. This policy should also include which specific applications may be used to share or discuss corporate information. Most importantly, company leadership must hold their employees accountable for following such policy. With 90 percent of all cyberattacks beginning with phishing, organizations are under constant threat of complex attacks targeting employees that can easily bypass gateways and land in email or text inboxes. Since employees use their devices for email and text to conduct business, a secure messaging strategy must be considered an essential component to any initiative.

Company-owned devices are easier to secure, since the organization can control them.

For example, the company can make sure that these devices are not rooted, and can also check which programs the user has installed and is running on the company-owned system. There is also the option of installing security software (such as endpoint monitoring agents) on these company-owned devices. Through the use of mobile device management (MDM), IT departments can limit the application and program options that employees can use in order to restrict downloads, block websites and monitor network traffic for suspicious activity. To keep corporate-owned devices protected from potential security threats, IT departments must ensure that all applications offered on company-owned devices are secure, meet compliance standards and offer encryption. Policies must also be in place to help ensure proper use by employees to protect from the ever-changing hacking landscape."

Some of the potential problems stem from rogue wi-fi in public venues, since a typical user can't easily determine whether the network is authentic and belongs to the organization.

Also, the user can be encouraged to create profiles that are used based on the physical location of the device.

If a mobile device is broken or lost, endpoint and MDM solutions can help. Platforms can provide fencing around work-related emails and documents. These platforms also offer the ability to push a remote system wipe, as a last resort, should a device with confidential or sensitive files go missing. With BYOD, network administrators can only impact company owned information such as e-mails or documents delivered through work systems. With company-owned devices, the entire device can be wiped remotely, removing all data and access."

## **QUESTION 2**

Industrial espionage is the covert and sometimes illegal practice of investigating competitors to gain a business advantage. You've likely heard about phishing scams and other forms of social engineering utilized by hackers. Basic computer security awareness and a bit of common sense in your day-to-day online activities is generally enough to avoid becoming victims. However, these deceptions are not the only tricks of modern-day hackers. As an industrial espionage there are many different techniques I could use to carry out my attack on the XYZ company without being noticed, these techniques are listed and discussed below;

### **1. Trojans**

My intent as a hacker is to get you to install it by making you believe it's safe. Once installed on your computer, a Trojan can do anything from logging your keystrokes, to opening a backdoor and giving the hacker access to your system. There are several ways in which a Trojan can infect your personal computer. The most common infection used is to trick you into

clicking on a file or email attachment. These attachments will come to you like it is an official notice from the IRS, FBI, or your bank.

Email may be a popular delivery vehicle for Trojans, but it's not the only one. Clicking on a malicious link on Facebook or other social media sites can allow a hacker to inject a Trojan into your personal computer. Even though these sites take security seriously and are as vigilant as possible, there have been instances when Trojans have infected users this way.

## **2. Drive-By Downloads**

In a drive-by download attack, you don't have to click on anything to initiate the download and installation of malware – just visiting a website that has been compromised is enough to get your computer infected. By hijacking the users' homepage and search bar, and placed advertisements in the users' "Favorites" folder.

A drive-by download exploits exposed security flaws in your web browser, operating system, or other software that has not been recently updated or patched. Unfortunately, the download and installation of the malware is invisible to the victim. Also, there is no way to tell whether a website is infected just by looking at it.

The stealth and effectiveness of a drive-by download makes it one of the best methods in a hacker's arsenal today. As a result, this form of attack has been on the rise and will only continue to get worse unless computer users take the proper precautions. Updating your software and using the latest version of your favorite web browser is a good start since it will close any newly discovered security holes these infected sites can exploit.

### **3. Rootkits**

A rootkit is not exactly malware like a virus or Trojan. It is something much more insidious: a malicious segment of code injected into your computer system, designed to hide any unauthorized activity taking place. Since rootkits grant administrative control to the attacker, your computer can be used without restrictions and without your knowledge.

A rootkit can attack and replace important operating system files, allowing it to hide or disguise itself and other malware. Once a rootkit has buried itself deep within your system, it can cover an intruder's tracks (by altering system logs), cover up evidence of malicious processes running in the background, hide files of all types, and open a port to create a backdoor.

Some rootkits are designed to infect a computer's BIOS (basic input/output system), which is a type of firmware that initializes the hardware when your computer is powered on. When rootkits invade this part of your system, it makes even operating system reinstallation or disk replacement an ineffective strategy to neutralize the rootkit infection.

Many of the worst, most destructive kinds of malware use rootkit technology. Since rootkits can infect different areas and different files, it is very difficult for even moderately experienced users to deal with them. Unfortunately, you will not even know whether you have this type of malware since it is designed to hide itself so effectively. That is why avoiding questionable sites, diligently updating your antivirus software, avoiding dubious email attachments, and generally protecting your system is a good way to make sure you never fall victim to this type of ingeniously malicious infection.

Once access I've gained to the XYZ company, using one of techniques and technologies outlined above. I would transform their computer into a zombie, a zombie, or "bot," is a computer under the control of a hacker without the knowledge of the computer user. The infecting malware is called a bot program, and a variety of combinations and techniques can be used to get it onto the target system. Quite often, it is delivered as a Trojan, activated by clicking a malicious email attachment or link, and remains hidden from the user because it has built-in rootkit technology. The main objective of the hacker in this sort of attack is to make the compromised computer part of a robot network or botnet.

A hacker in charge of a botnet is sometimes referred to as a "bot herder." The newly installed bot program opens a backdoor to the system and reports back to the bot herder. This is done through command-and-control (C&C) servers. Using these C&C servers, the bot herder controls the entire botnet, having all the zombie computers acting as one unit. Botnets have a tremendous amount of processing power with sometimes up to hundreds of thousands of zombies worldwide.

Once your computer becomes part of a botnet, the i can use it in a number of ways. It can be used to send spam and viruses, steal your personal data, or it can be used in click fraud scams to fraudulently boost web traffic. Some bot herders even rent out the processing power of their botnets to other hackers.

This type of cybercrime is a big problem in many parts of the world.

Then I'll perform extortion through encryption, imagine if hackers could hold your personal computer hostage and extort a cash payment from you. Unfortunately, this scenario is quite

possible and has been playing out very successfully for quite a few years now. The security threat is classified as ransomware, and it is an extremely profitable endeavor for cybercriminals.

Injecting itself into your system by way of a drive-by download or similar method, ransomware usually does one of two things: it either locks your computer, or encrypts all your personal files. In both cases it displays a message stating that you must pay a ransom or you will never have access to your files again.

### **QUESTION 3**

A. 3 HAMLETS – M (M is the 3<sup>rd</sup>)

1 ORACLE – O (O is the 1<sup>st</sup> letter and so on...)

9 MESSENGERS – R

1 SHELL – S

4 RODENTS – E

1 CALABASH – C

3 PROPHECIES – O

1 DESTINY – D

6 COWRIES – E

Using the key of the words before the words to decode each letter the above letters were decoded which gives the decrypted information as

Decrypted text – MORSECODE.

B. SING THAT RAP FALL – THINGS FALL APART

(using transposition patten with a particular key pattern)

## QUESTION 4

Using creaser substitution cipher key 5 (left)

T – O

S – N

J – E

S – N

F – A

R – M

H – C

G – B

T – O

J – E

Q – L

T – O

N – I

Z – U

S – N

Using columnar transposition cipher



1 2 3 4 5  
O N C E I  
N A B L U  
E M O O N

Decrypted text – ONCEINABLUEMOON

ONCE IN A BLUE MOON