**COE 510 ASSIGNMENT**

**COMPUTER SECURITY TECHNIQUES**

**OHAJI JUDE-THADDEUS**

**15/ENG02/040**

**COMPUTER ENGINEERING**

**Q1:**

**SECURITY POLICY ON THE USE OF MOBILE PHONES**

* Stolen or lost mobile devices must be reported as soon as possible.
* Downloading and installation of materials from untrusted sources are prohibited.
* Mobile devices must not be connected to a PC which does not have up to date and enabled malware protection.
* Corporate data essential to their role should not be loaded into private mobile devices by users.
* Remote lock and data wipe option on the mobile device must be enabled in case of theft.
* Mobile phone users must not load pirated software or illegal contents into their devices.
* Mobile devices must be protected with an undisclosed strong password.
* Practice safe disposal techniques when getting rid of mobile device Only devices managed by IT will be allowed to connect directly to the internal corporate network.
* Users are responsible for the backup of his/her own personal data and the company will accept no responsibility for the loss of files due to non-compliant device being wiped for security reasons.
* All mobile devices must be kept up to date with manufacturer or network provided patches to increase security.

**Q2:**

Industrial espionage is the practice (most times illegal) of investigating competitors to gain a business advantage. In most times industrial spies are simply seeking any data that their organization can exploit to its advantage.

The first step is to infiltrate using social engineering tactics whereby interaction is key. Getting close to a high ranking employee and investigating the target and trying to gather all necessary background information.

After establishing a little bit of trust, with few weeks of familiarity and interaction, the target gets comfortable with the spy (me) and they tend to hang out together during weekends and free time as the case may be. The spy gets close enough to access his PC maybe at home or during hangouts, and after that the spy goes on to plant a bug in the system to monitor traffics and diverse information to his own system so as to monitor activities and obtain information and of course creating a backdoor which gives him access to the target files without having to be in the same location.

Also as an investigation spy I can make use of spywares which is a malware utilized by attackers for background undetectable lifting of valuable information from the target, such as credit card details, pictures, password, secured folders etc.

Another method can be utilizing the Remote Access Trojan whereby after successful installation of the malware, access is granted to the attacker (me) to be able to control certain areas such as hard drives and installing key loggers for undetectable access which can be later used as the case may be.

I can also make use of the Denial of Service (DOS) attack whereby the targets internet service is disrupted by unwanted information thereby increasing traffic and also increasing amount of attempts to log in. These are means for diversion of attention for the threat to be carried out.

After all attempts and infiltration, as an attacker I must follow the protocol of erasing any trace that can point to me.

First of all, to carry out the above intended attacks I must have a Virtual Private Network (VPN) to erase all trace and footprint, clearing and erasing logs and after carrying out all these activities, ensuring that all files and folders created during the course of the infiltration are discarded. If at all I can implicate someone else by purposely leaving an item which can be traced to his colleague although it might not be necessary as the case maybe.

**Q3:**

1. 3 HAMLETS - M

1 ORACLE- O

9 MESSENGERS-R

1 SHELL- S

4 RODENTS- E

1 CALABASH- C

3 PROPHECIES- O

1 DESTINY- D

6 COWRIES- E

Result = **MORSE CODE**

1. **SING THAT RAP FALL**

An anagram (re-arranged words) of **THINGS FALL APART**

**Q4:**

Encrypted Message TSJSFRHGTJQTNZS

1. Using Caesar Substitution Cipher (key 5)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the above letters Caesar shift of 5 =**VWXYZABCDEFGHIJKLMNOPQRSTU**

Decrypted message = **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 message is = **ONCE IN A BLUE MOON**