**Information Security Project Documentation**

**Project Name: WIAM Tool**

**Submitted to: Dr. Qasim Ali Arain**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Names:** | **Inayat Ali** | **Waqar Ali** | **Abdul Jabbar** | **M. Moiz** |
| **Roll Numbers:** | **18SW61** | **18SW82** | **18SW64** | **18SW125** |

****

**Email Spoofing:**

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it’s a name they recognize, they’re more likely to trust it. So they’ll click malicious links, open malware attachments, send sensitive data and even wire corporate funds.

Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review email headers packaged with every message to determine whether the sender address is forged.

**How Email Spoofing Works:**

The goal of spoofing is to trick users into believing the email is from someone they know or can trust—in most cases, a colleague, vendor or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.

**For example:**

an attacker might create an email that looks like it comes from PayPal. The message tells the user that their account will be suspended if they don’t click a link, authenticate into the site and change the account’s password. If the user is successfully tricked and types in credentials, the attacker now has credentials to authenticate into the targeted user’s PayPal account, potentially stealing money from the user.

**How to Protect from Email Spoofing:**

Even with email security in place, some malicious email messages reach user inboxes. Whether you’re an employee responsible for financial decisions or as someone who uses personal email at work, there are several steps you can take to avoid becoming a victim of email fraud:

* Never click links to access a website where you’re asked to authenticate. Always type the official domain in your browser and authenticate directly on the site.
* The steps to view email headers are different for each email client, so first look up how to view email headers for your inbox software. Then, open email headers and look for the Received-SPF section of the headers and look for a PASS or FAIL response.
* Copy and paste the content of an email message into a search engine. Chances are that text used in a common phishing attack has already been reported and published on the Internet.
* Be suspicious of email supposedly from an official source with bad spelling or grammar.
* Avoid opening attachments from suspicious or unknown senders.
* Emails promising riches—or anything else that’s too good to be true—is likely a scam.
* Beware of emails that create a sense of urgency or danger. Phishing and BEC attacks often try to short-circuit recipients’ natural scepticism by suggesting that something bad will happen if they don’t act quickly. Treat email links with extra caution if the message warns of pending account closures, scheduled payment failures or suspicious activity on one of your financial accounts. Visit the website directly through your browser, not the link in the email.

**Reversed Connection**

A reverse connection is usually used to bypass firewall restrictions on open ports. A firewall usually blocks open ports but does not block outgoing traffic. In a normal forward connection, a client connects to an open port on the server. However, in the case of a reverse connection, the client opens a port for the server to connect to.

**Access a computer behind a firewall:**

The remote machine needs to connect to your machine using your IP address and port number, which can be found in the Reverse Connections.

Once the remote computer connects to your machine, Remote Desktop Viewer will establish the reverse connection.

When connecting to a machine which is not on your local network, you will need to provide your externally visible IP address and port number to the remote server.

**Cipher Modes**

**OneTimePad:**

The OneTimePad cipher in this program has the following work pattern:

Generating OneTimePad(key)

The program asks the user to define the number of OneTimePad(Key) the user want to create. The keys can be used to encrypt and decrypt a message.

The program then asks to user to define the length of the OneTimePad(key) where the user has to make sure the length of the OneTimePad must be greater than the message the user wants to encrypt.

The programs the save the OneTimePad in files named (otp0,1,...n)

**Encryption**

The program starts with asking the user to enter the OneTimePad file name the user wants to use(the file must be entered with the extension (.txt) also).

Then the program asks the user to enter the message to encrypt.

Then the program asks the user to enter the name of the file(with .txt, .doc extension) where the ciphertext will be saved and then used to decrypt the original message.

**Decryption**

The program asks the user to enter the name of OneTimePad file which will be used to decrypt the ciphertext.

The program asks the user to enter the name of the file in which the ciphertext is stored.

The program then uses the OneTimePad file to decrypt the ciphertext file and then shows user the original message.

**Advanced Encryption Standard(AES):**

**Encryption:**

The program starts with asking user to enter an Alphanumeric password which will be then converted into a hexadecimal key and will be used to encrypt/decrypt the message.

The program then asks the user to enter the message.

The program then prompts and asks user the enter name for file in which the cipher information will be stored.

**Decryption:**

The programs firstly asks the user to enter the name of file he wants to decrypt.

The programs then asks the user to enter the password which was originally used to encrypt the file.

If the entered password is correct then the program shows the original/correct message otherwise the program will give an “MAC check failed” error in case the password is wrong.