CTF Challenge Proposal

Created by Yehuda Gurovich

Stage 1: Setup & Start

Description & Purpose

In this initial stage, participants are introduced to the challenge by visiting the provided website to gather background information.

Steps Taken

1. **Step 1**: Navigate to ctf.yehudagurovich.com to access the starting page of the CTF.

Result

Participants can view the homepage of the website and begin their exploration.

Relevant Course Material & Other Tools and Techniques Used

- **Topic 1**: Basics of a *Python HTTP server*
- **Topic 2**: Understanding *sockets* used in HTTP servers
- **Topic 3**: *Self-hosted websites and domains*
- **Topic 4**: *Google Cloud Platform*
- **Topic 5**: *Docker* containers for hosting websites

Stage 2: Finding the Secret Route

Description & Purpose

This stage involves discovering a hidden route on the website and downloading an executable file essential for the next stage.

Steps Taken

1. **Step 1**: Examine the "Our Services" section on the homepage. Noting that each line starts with a capital letter, combine these letters to form the word "CURL."
2. **Step 2**: Use the `curl` command on the website to reveal a hidden message. The message contains words with extra spacing. Combining these words reveals: "route is secret mission". This indicates the secret route: ctf.yehudagurovich.com/secretmission.
3. **Step 3**: Access the hidden route to download the necessary executable file.

Result

Participants obtain the executable file required for the subsequent stage.

Relevant Course Material & Other Tools and Techniques Used

- **Topic 1**: Basics of a *Python HTTP server*
- **Topic 2**: Understanding *sockets* used in HTTP servers
- **Topic 3**: Techniques for *self-hosting websites and domains*, using Google Cloud Platform
- **Topic 4**: Utilizing *curl* to interact with web servers
- **Topic 5**: Analyzing *HTTP user agents* and headers

Stage 3: Executing the File & MITM Attack

Description & Purpose

This stage involves running the executable file, observing network traffic, and performing a Man-in-the-Middle (MITM) attack to capture a transmitted message.

Steps Taken

1. **Step 1**: Execute the downloaded file and monitor network traffic to observe packet transmissions.
2. **Step 2**: Use Wireshark to capture and analyze the network packets.
3. **Step 3**: Follow the UDP stream for the packets in Wireshark to extract the transmitted message.

Result

Participants obtain an encrypted message from the network traffic.

Relevant Course Material & Other Tools and Techniques Used

- **Topic 1**: Creating *executable* files using *pyinstaller* in python
- **Topic 2**: Using *Wireshark* for network analysis
- **Topic 3**: Understanding the *UDP* protocol and packet analysis
- **Topic 4**: Performing *MITM attacks* to capture network traffic
- **Topic 5**: *Threading* to handle client and server at the same time when packets get sent in the executable
- **Topic 6**: *Sockets* for the client and server
- **Topic 7**: *Scapy* to generate all the packets

Stage 4: Decrypting the Message & Final Message

Description & Purpose

In this final stage, participants must decrypt the message obtained from the previous stage and decode it to reveal the final message.

Steps Taken

1. **Step 1**: Analyze the length, cipher type, key, and encoding of the captured message.
2. **Step 2**: Figure out what parts of the message are useful and need to be ordered, in our case we need the last 21 characters if it ends with ctfXX where XX are the numbers for the order of the packet
3. **Step 3**: Use Python to decrypt the message using the Columnar Transposition Cipher and Base64 decoding.

4. **Step 4**: Visit ctf.yehudagurovich.com/finalmessage to access the final message.

Result

Participants successfully complete the CTF challenge by decrypting and decoding the final message and then visiting the designated website to view the result.

Relevant Course Material & Other Tools and Techniques Used

- **Topic 1**: Understanding and applying *ciphers*
- **Topic 2**: Techniques for *encryption and decryption*
- **Topic 3**: *Python programming* for cryptographic tasks
- **Topic 4**: *Regex* for filtering data