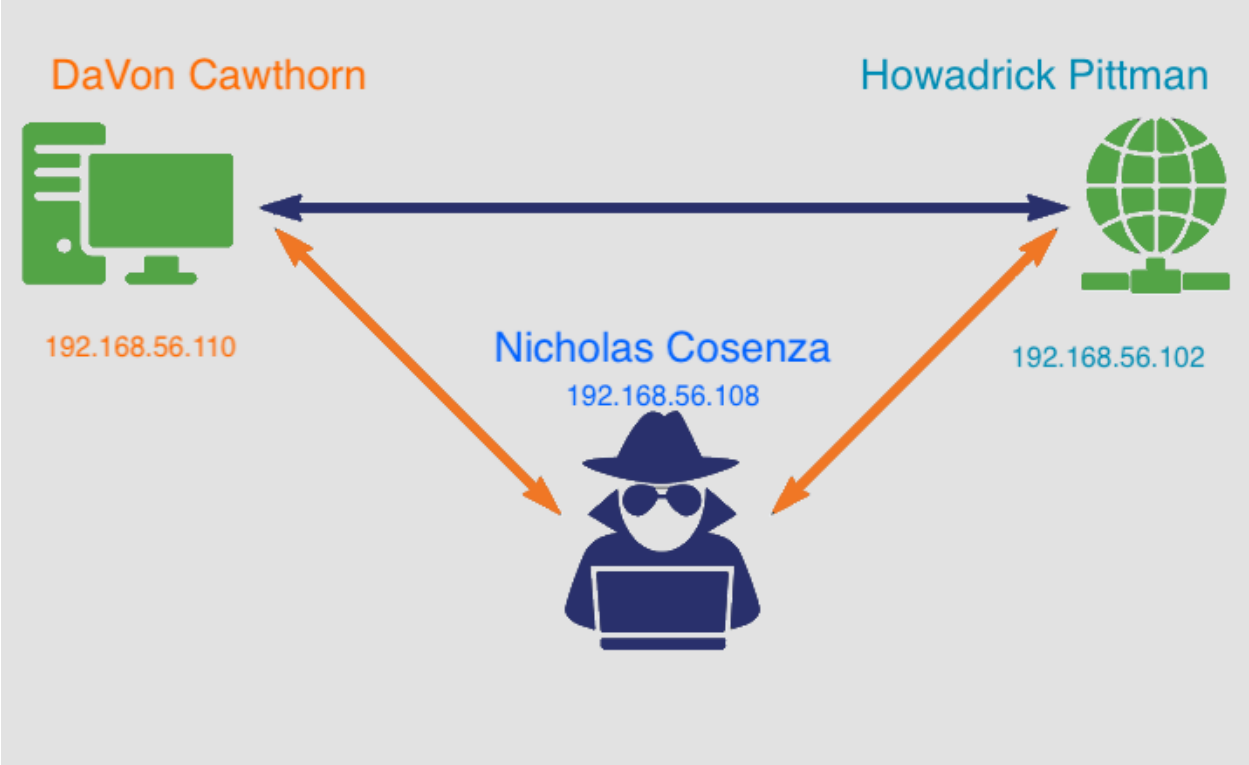
MIGHTY EXECUTIONERS

PITM Credential Stealer via BetterCAP



This is an overview of how to steal credentials using a Linux command line tool, called BetterCap.

Basics of PITM

1. **Attackers inject false information into this system to trick your computer to think the attacker's computer is the network gateway. From your perspective, everything is normal. The attacker is able to see all of your packets.**
2. **DNS cache poisoning can occur when the attacker gives you a fake DNS entry that leads to a different website. It might look like Google, but it's not Google.**
3. **HTTPS is one of the ways users know that their data is "safe." The S stands for secure. At least that is what an attacker wants you to think. Attackers set up HTTPS websites that look like legitimate sites with valid authentication certificates, but the URL will be just a bit different.**
4. **Attackers listen to traffic on public or unsecured Wi-Fi networks, or they create Wi-Fi networks with common names to trick people into connecting so they can steal credentials or credit card numbers or whatever other information users send on that network.**

What is a PITM Attack?

According to Wikipedia:

In cryptography and computer security, a person-in-the-middle attack (often abbreviated to PITM, MitM, MIM, PiM attack or PITMA) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.A man-in-the-middle attack is a similar strategy and can be used against many cryptographic protocols. One example of person-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle.

In the following example, we use the BetterCap tool and "ARP" option. This protocol is used to gain information on the targets.

ARP

Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).ARP spoofing, also known as ARP poisoning,can be used in a Person in the Middle (PITM) attack that allows attackers to intercept communication between network devices. The attack works as follows: The attacker must have access to the network.
To learn more about ARP poisoning click on the ARP heading above which is also a link.

Installation

Install Bettercap on your chosen VM. We have chosen to use Kali-Linux. To install, open Kali-Linux and enter ‘sudo apt install bettercap’ in the command line. Follow all prompts to finish installation.

```
sudo apt install bettercap
```

Open the Virtual Machines that you are going to perform PITM attack between, in this case we used Metasploitable and SiftWorkstation. To determine IP addresses run ‘ifconfig’ in the command line once you open each machine. IN EACH machine we have found the IP addresses of each VM.Attacker’s IP address is 192.168.56.108, target one machine’s IP address is 192.168.56.102, and the target machine 2 IP address is 192.168.56.110. This will be pivotal in understanding the PITM attack.

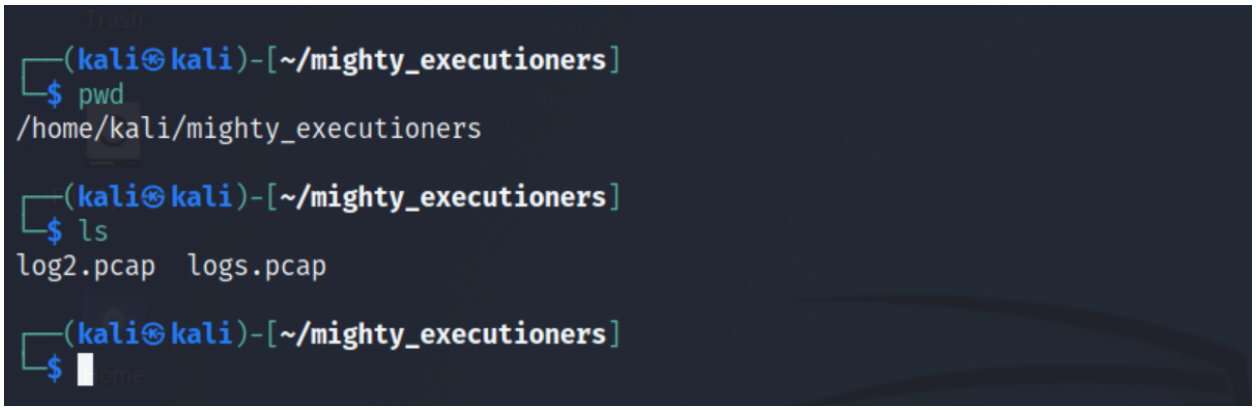
```
ifconfig
```

We will open BetterCap. The command used to open BetterCap is ‘sudo BetterCap –iface and eth1’. We used eth1 because it matches the inet IP address location of the **host only** VM machine(s) which we are targeting.

```
sudo bettercap -iface and eth1
```

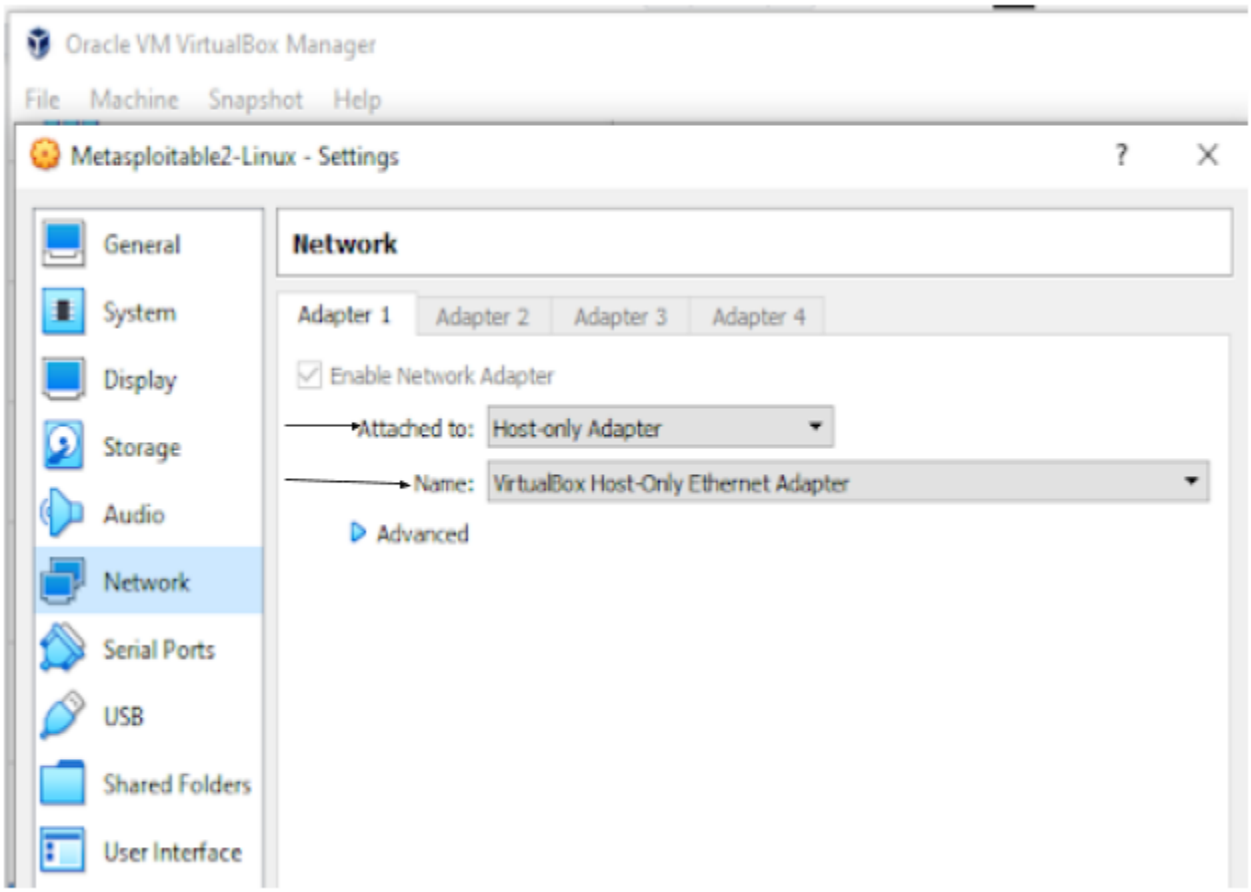
Creating Pcap File Destination

In order to utilize the BetterCap tool to its full potential, we created a destination Pcap file. In order to place the traffic which we are intercepting during the attack. By creating a Pcap file we will be able view the intercepted traffic in Wireshark as well as save to view later. This Pcap file will save the information in which you have intercepted so that the PITM will be able to properly investigate the information stolen.
Bettercap needs a destination file as previously used in the configuration rules.
The rule in which we used was `set net.sniff.output /home/kali/mighty_executioners/log2.pcap` We created a working directory named the mighty_executioners, as well as a pcap file called "log2.pcap". WE ADVISE YOU TO DO THE SAME.



Network Set-Up

To minimize our host network from being vulnerable to attacks.We recommend you set all VMs to **host only** network in your Oracle VirtualBox setting under network.

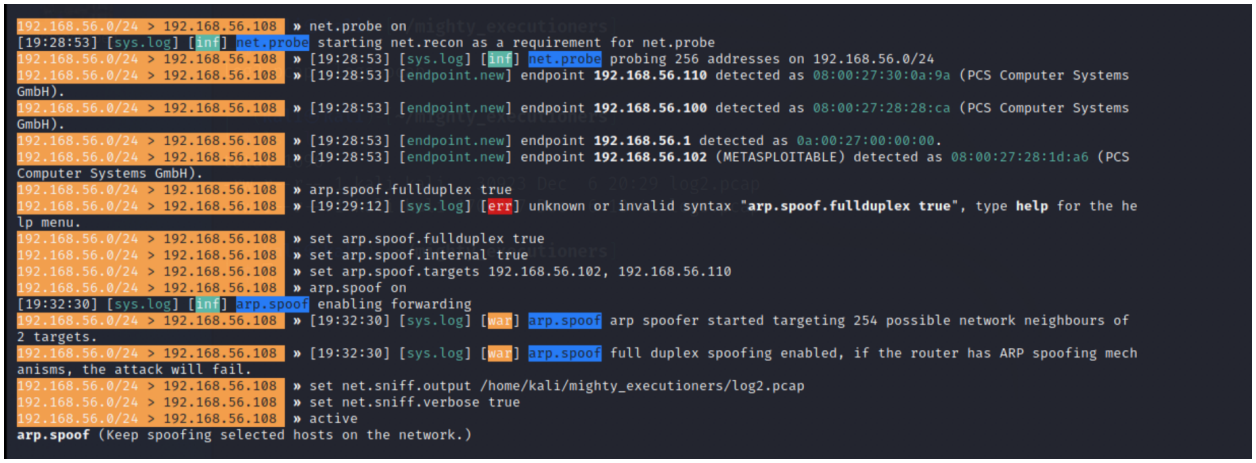


BetterCap Configuration

The next steps involve the configuration of BetterCap. These rules will make our tool run smoothly and will deliver the results in which we are looking for.

The rules were used in this order to configure properly:

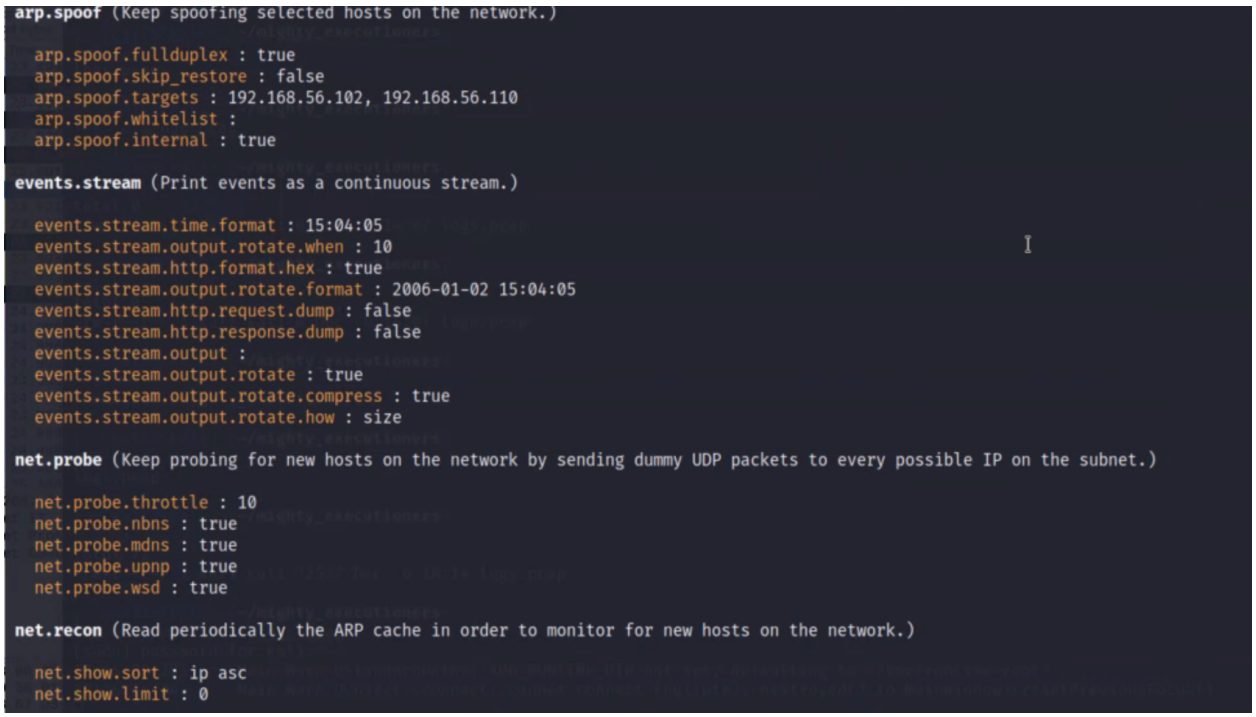
1. net.probe on
2. set arp.spoof.fullduplex true
3. set arp.spoof.internal true
4. Set arp.spoof.targets `192.168.56.102, 192.168.56.110`(target ip address)
5. arp.spoof on
6. set net.sniff.output.output /home/kali/mighty_executioners/log2.pcap
7. set net.sniff.verbose true
8. net.sniff on
9. At any point in the configuration process, you can use either ‘Help’ or ‘Active’ to view both the configurations you have added and what your options within those are set to.



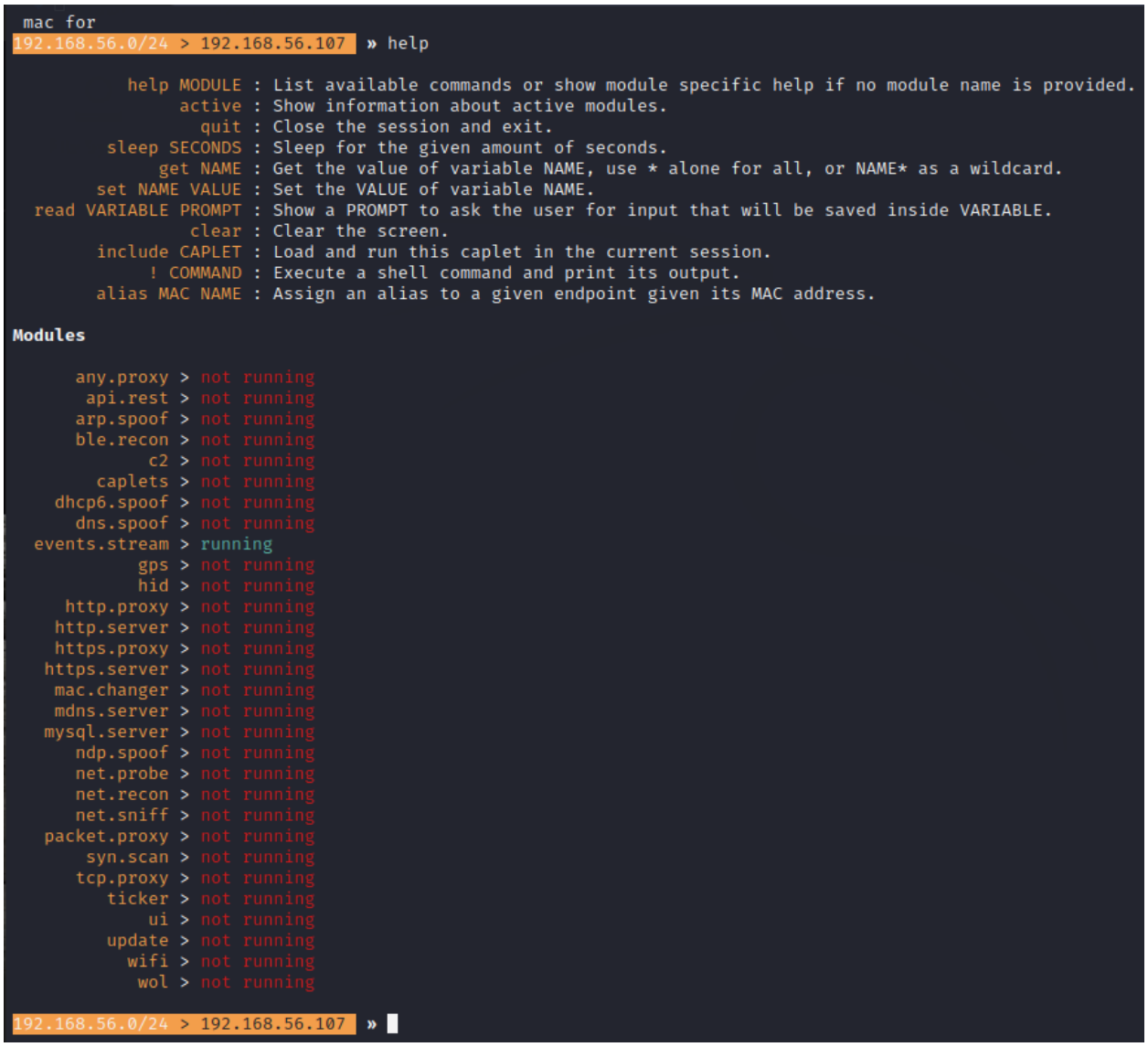
parameter	default	description
Sudo Bettercap -iface wlan0	<entire subnet>	Selecting the interface of wlan0 i.e Wi-Fi. You can also try it with LAN(local area network), It will work the same as with Wi-Fi. -iface command is used for selecting the interface. You can use the command ifconfig to get all the interfaces
net.show		To show all the devices that are connected to the same network with their IP, MAC, Name, etc. Now we need to copy the IP address of the devices on which we want to sniff. This is done with set arp.spoof.targets
help	True	This will provide you with the modules of BetterCap with their status.
arp.spoof.full duplex	TRUE	If true, both the targets and the gateway will be attacked, otherwise only the target (if the router has ARP spoofing protections in place this will make the attack fail).
Net.probe on	ON	This will send various probe packets to each IP in order and in the present subnet so that net.recon module may detect them with ease
set arp.spoof.targets 192.168.56.102,192.168.56.110(IP address of the target Device)	SET	Set the target to the IP you can add any number of IPs here by using “,”. For example 192.168.56.102 ,192.168.56.110
set arp.spoof on	ON	Start the ARP spoofer
Set net.sniff.local	True	Setting it to true will consider packets from/to this computer, otherwise it will skip them. As we are MITM (man in the middle) that means all the data is transferring from our computer

net.sniff on	ON	Turning on the sniffing and catching the packets.

Active tells you all of the modules which you have active in BetterCap, at the current time. It will show the options set at that given moment in which you have inputted.

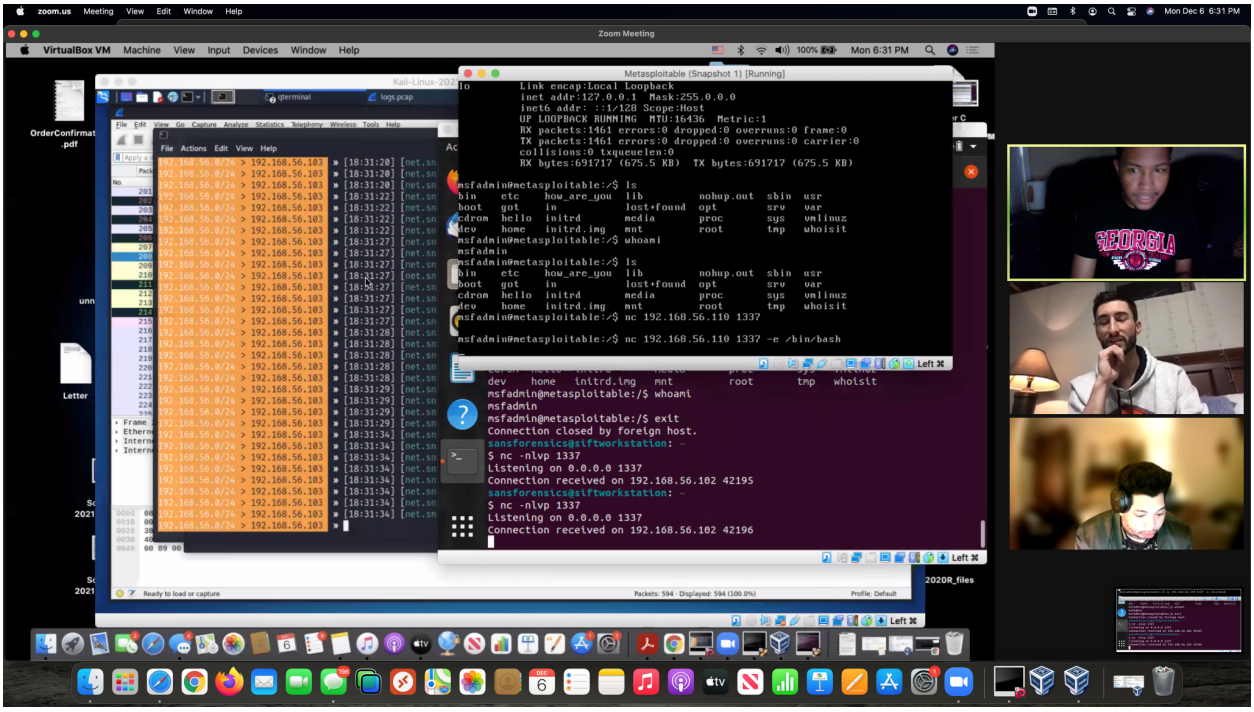


Help lists available commands or shows modules specific to what you are trying to achieve.



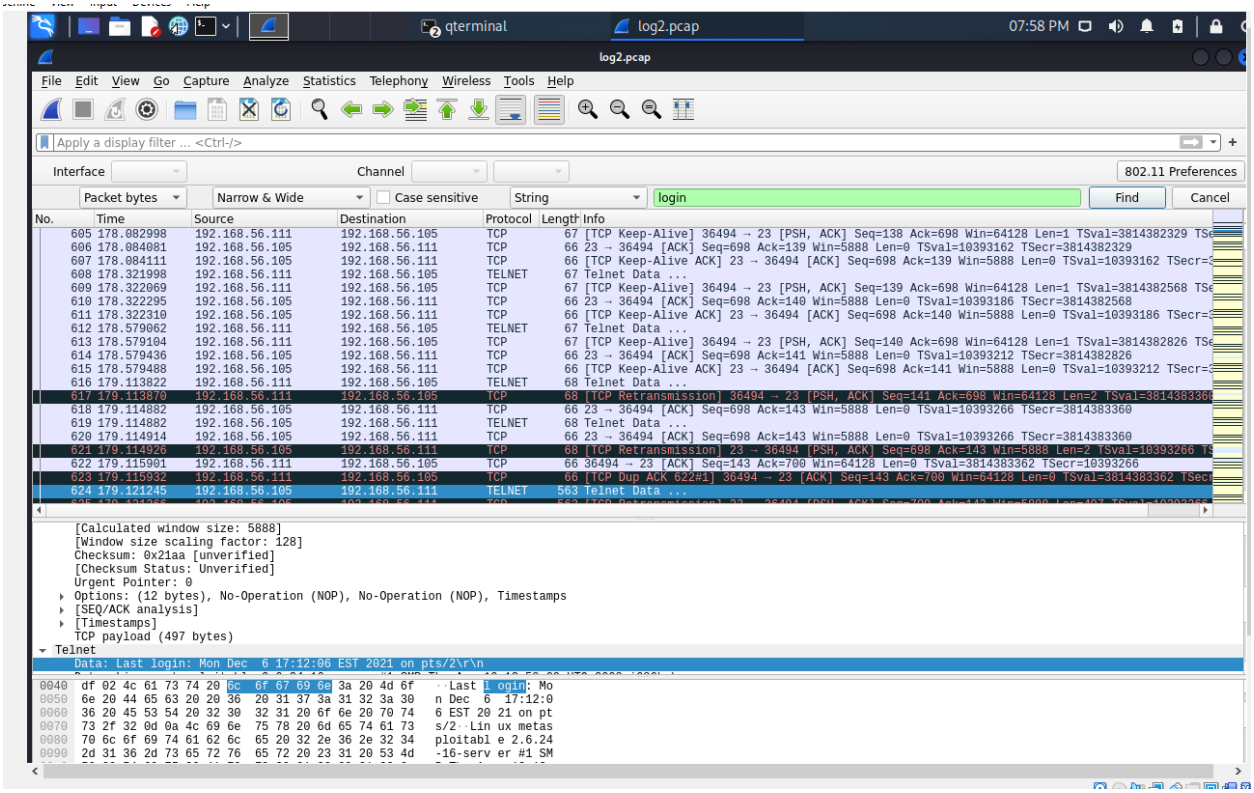
Victim Virtual-Machines

We have decided to create two Virtual Machines to create and simulate the network traffic to intercept as PITM. Machine 1(M1) is called SiftWorkstation. Machine 2(M2) is Metasploitable. We decided to use a telnet login command to network M1 to M2. The command we used to perform this is `telnet 192.168.56.102` to access M2. Once this telnet command is used we have to login to M2. The login information for M2 is User = msfadmin Pwd = msfadmin. You can create a login process of your own, but this is the path which we are demonstrating. At this point we are going to use Wireshark to view the traffic packets we intercepted.



Wireshark Traffic

Upon entering the Wireshark application, we have decided to use ‘ctrl+F’. This command will allow us to search for specific characters in the “Packet bytes” filter; After you have entered the unique characters in which you are searching for in the packets, follow the trail to intercept the information in which you are looking for. In this case, we searched for “login” within the packet bytes because it is the Metasploitable Vm(M2) Username and Password. This was found in packet 151 of the network traffic. We also follow a TCP stream to access the data thoroughly with the packets. We are now ready to intercept traffic as the PITM. In a new command line window, we have entered the command `sudo wireshark log2.pcap`. We will now view intercepted traffic packets.



Future of PITM Attacks

PITM attacks will continue to be a useful tool in attackers' arsenals as long as they can continue to intercept important data like passwords and credit card numbers. It's a perpetual arms race between software developers and network providers to close the vulnerabilities attackers exploit to execute PITM.Take the massive proliferation of the Internet of Things (IoT) over the past few years. IoT devices don't yet adhere to the same security standards or have the same capabilities as other devices, which makes them more vulnerable to PITM attacks. Attackers use them as a way into an organization's network so they can move to other techniques. Who knew

that a new fancy internet-capable thermostat was a security hole? Attackers do!