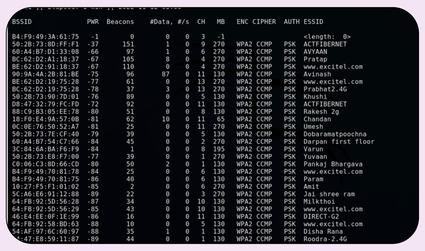
Exploring Ethical Hacking and Methods of Cyber Security

Internship Report, Cluster Innovation Centre, Nikunj Saini

Abstract

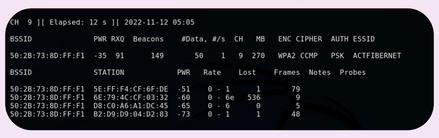
All of us use internet for the most of our works, may it be office work, personal work, social media, or any other platform. We often download files, which include all formats like a document, picture, audio, video or even a software upgrades. To download such files, we often visit torrents or unauthorized websites, where the available software may contain virus which are capable of stealing your data and even granting a third person to operate your entire device. Such people who use data for malicious purposes are called 'Black Hat Hackers'. People who use such viruses to test server security, are called 'White Hat Hackers'. In this project, I have explored numerous ways in which the data can be stolen from your devices and the hacker may get access to your devices. I had also tried to implement methods through which a successful backdoor can be generated for data theft. In the end, I explored the counter measures for such attacks so that our device stays secure from such attacks.

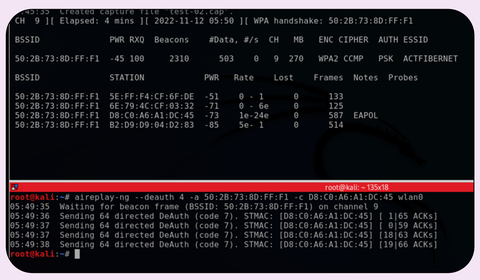
Network Hacking



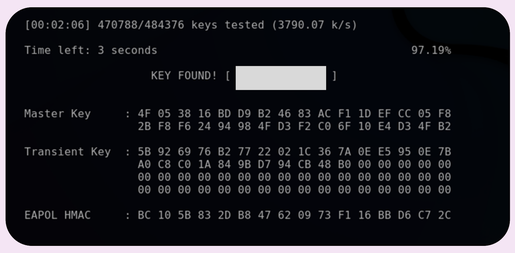
Detecting networks using airodump-ng command on the Linux Terminal.
This shows all the available networks in the vicinity of the router in monitor mode.
The next step is to perform targeted sniffing of the netwrok and capture traffic.

Targetted sniffing shows all the devices that are connected to the network
We then perform deauth attacks to capture the handshake packet





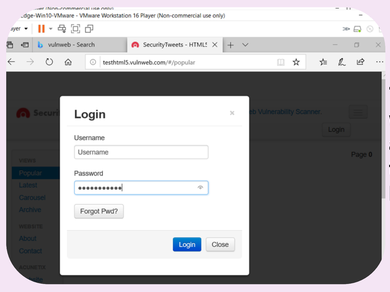
Using the captured handshake packet, we can find the key of the network by genrating MIC using wordlist of possible passwords.



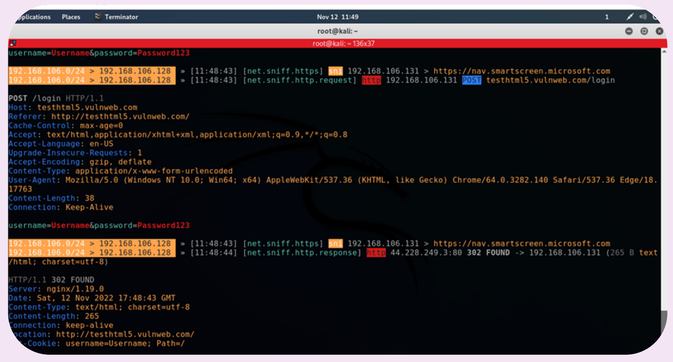
Once the Password is captured, we can connect to the netwrok and perform MITM attacks on the target.

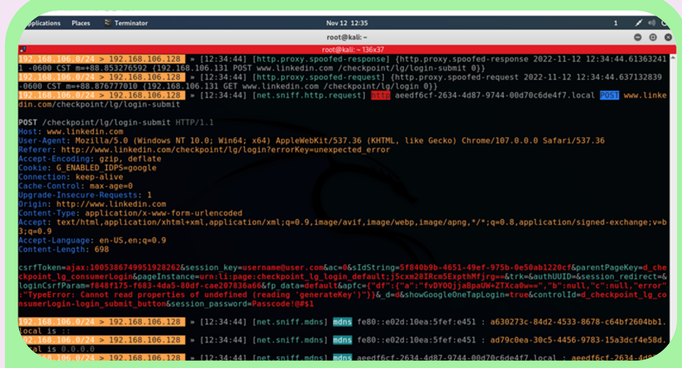
Data Capturing

Webpages basically have 3 protocols (HTTP, HTTPS and HSTS). The least secure is the http protocol. To capture data from such websites, we simply use packet sniffers to get the data. To capture the data from websites, we the Bettercap framework of the Kali Linux machine.

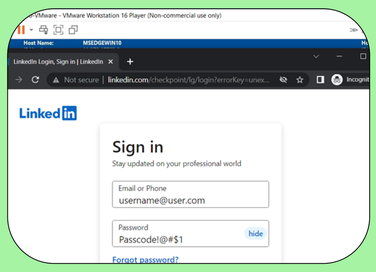


This is how HTTP webpages can be traced and the credentials of the target are being recorded by Kali MAchine





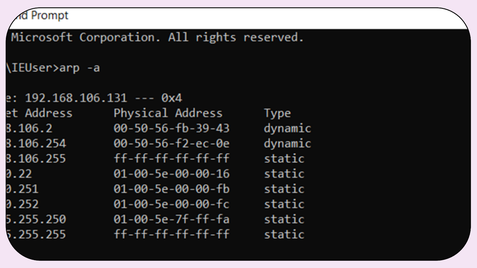
This is how HTTPS webpages can be traced
The webpages are downgraded to HTTP and the credentials of the target are being recorded by Kali MAchine
HSTS webpages can be also captured if redireted through a downgraded HTTP webpage



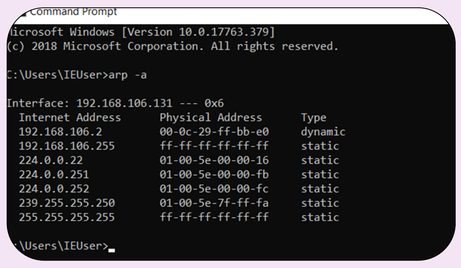
Post Connection Attacks

Once we have gained access to the network, we can easily become 'Man in The Middle'. This means that we interrupt the connection between the client and the host through the router. For the router, we become the client and for the client, we become the router. So, all the data will flow through our system.

The ARP poisoning attacks woill help us to become the MITM.



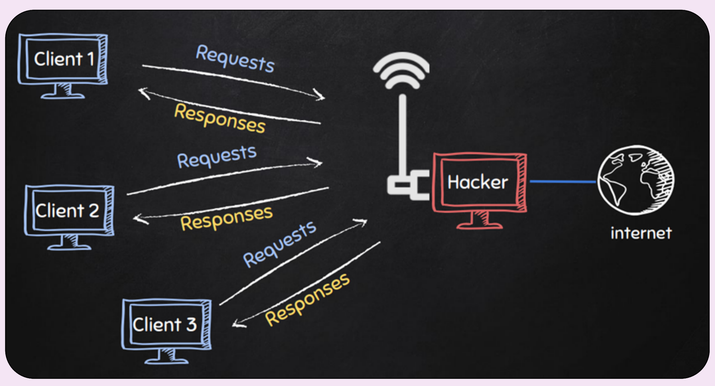
ARP table for the target Windows VM before ARP poisoning attack



ARP table for the target Windows VM after ARP poisoning attack

Honey Pot - Multiple Targets

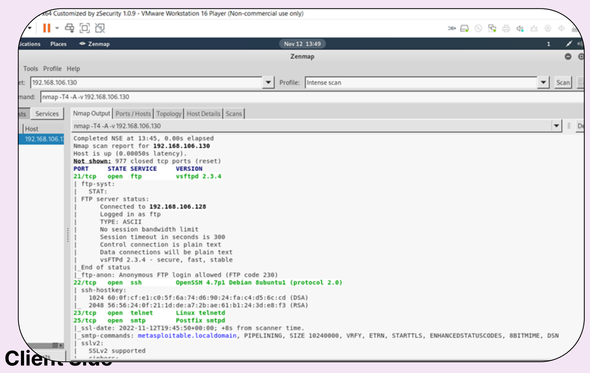
Instead of being MITM for one single target, we can be the MITM for multiple targets at the same time. To perform this, we need to have one of the routers that contain the chipset Atheros AR9271 or Realtek AR8812AU.
We first set the router to monitor mode, so that we can keep track of what traffic is flowing. Then we also have to enable Wi-Fi on the Linux machine. Once we set up the router, the communication will take place as shown below.

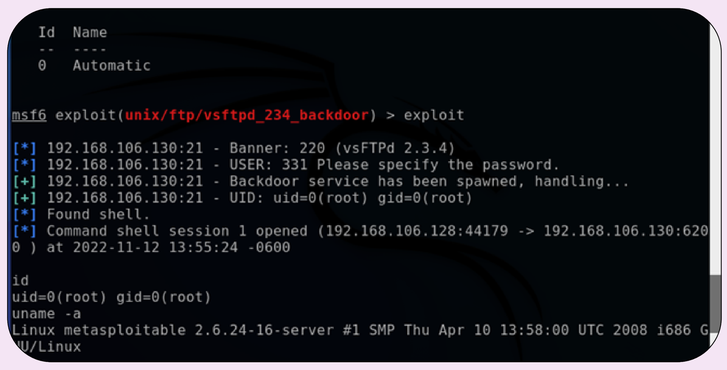


Web Server Hacking - Backdoors

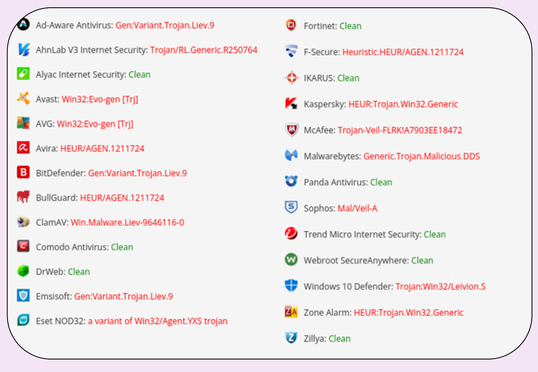
We can also exploit different frameworks of a website using the Zenmap framework. This framework is used to detect the backdoors in the web services so that they can be exploited. Zenmap is only used to gather information about the backdoors. To exploit them, we still have to use the Linux terminal.

Server Side





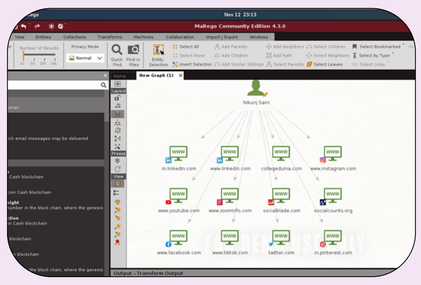
Client Side

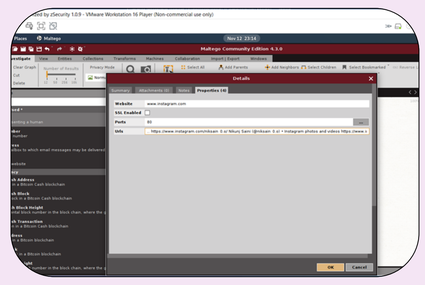


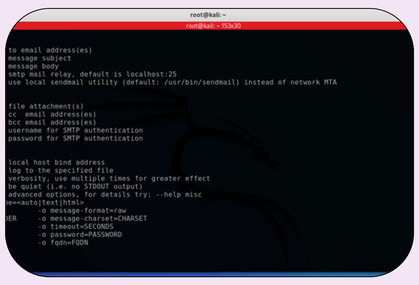
To create the backdoor, we can use Veil framework.
This framework is capable of generating backdoors that can even bypass antivirus tests. One such backdoor created was tested on 26 antivirus and it was detected by 16 of them.
The tested backdoor was one of the simplest backdoor with minimal features.
The test results are shown below in the snip.
These backdoors can be sent to the target machine in two ways.
1) By creating a fake update on any of the services of the target machine. This requires the hacker to be in the MITM first and then this attack can be performed.
2) The second method is by Social Engineering. This is a very strong method and does not require the attacker to be the MITM.

Social Engineering

In this method, we find a target user and find his/her most visited webpages. Then, we search for the people who are associated with the target. These people include family members, co-workers, etc. Once we find them, we can create a network with which we can directly approach the target and send the trojan.





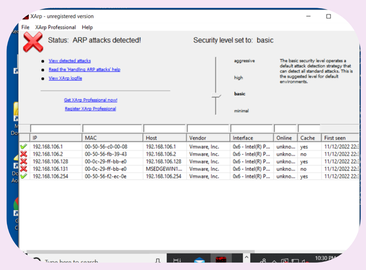


Results

We have come to the conclusion that data can be stolen in many different ways. The steps to steal data are:
1) Gain the network access
2) Be the MITM
3) Detect the target
4) Prepare a map for the type of attacks that need to be run
5) Exploit the target
It is illegal to keep a check on other people's data, so it is not recommended to perform any of the attacks on any person without their consent. All the attacks run in the above test were run on a windows virtual machine.
To protect yourself from such attacks, make sure to follow the following steps:
1) Use difficult passwords with combination of upper case, lower case, numbers and symbols
2) Use ARP-Poisoning attack detectors like XARP
3) Be careful with sites that operate on HTTP protocol
4) Use HTTPS Everywhere and VPN for maximum online security
5) Keep your Anti-virus active all the time
Once we make sure of these 5 things, we can be safe on the internet from black hat hackers and protect ourselves.

Methods of Prevention

To check for ARP Poisoning/MITM attacks, XARP software can be used. This software is capable of detecting the change in the router IP address so that the target can get aware that someone is trying to steal its data.



Online Data Protection
1. Using HTTPS Everywhere extension for browsrers
2. USing a VPN
3. Keep Antivirus updated and check mails carefully before opening

	Pros	Cons
HTTPS Everywhere	- Free	- Only works with HTTPS websites - Visited domains still visible - DNS spoofing still possible
VPN	- Encrypts everything - Protects from all types of MITM attacks	- Not free - VPN provider can still see the data
HTTPS Everywhere + VPN	- Encrypts everything - Protects from all types	- Not Free