Branden Barnes

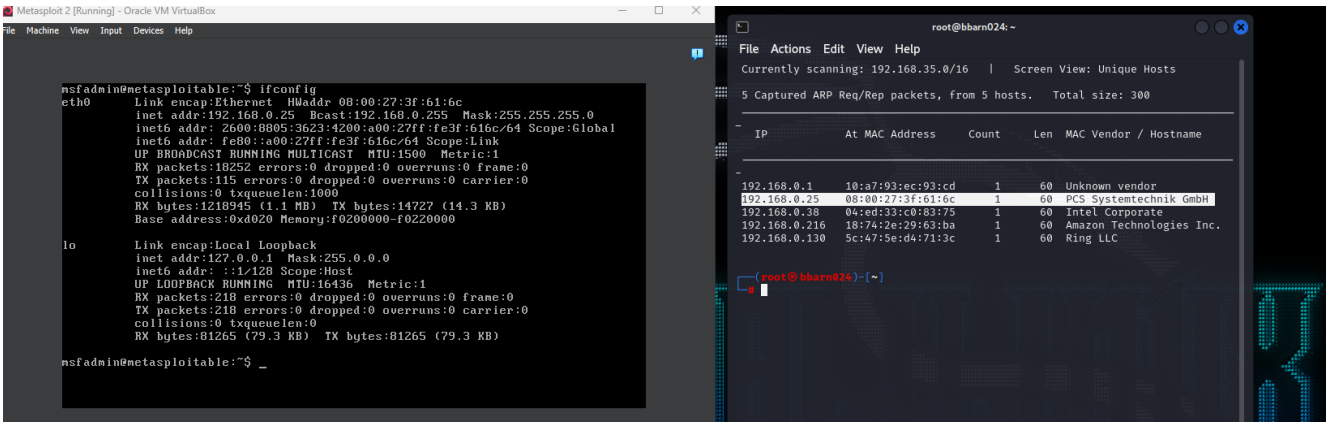
Professor Vatsa

CYSE 450

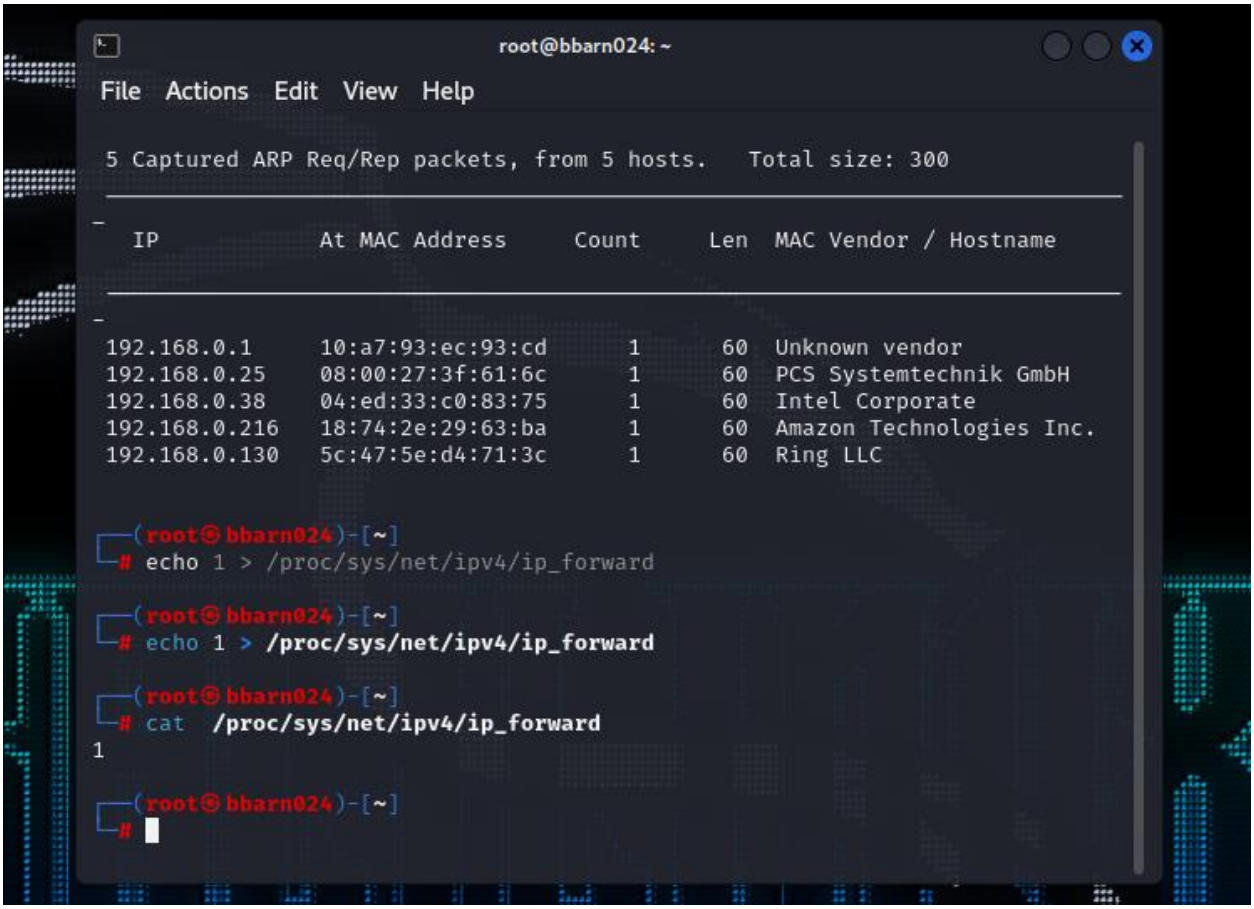
Packet Sniffing

Task: **Performing an ARP Spoofing Attack**

1-2. Power on and login to Kali Linux and Metasploitable2. Open a root terminal on the Kali Linux virtual machine and discover the IP addresses of the other machines on the network to spoof them.

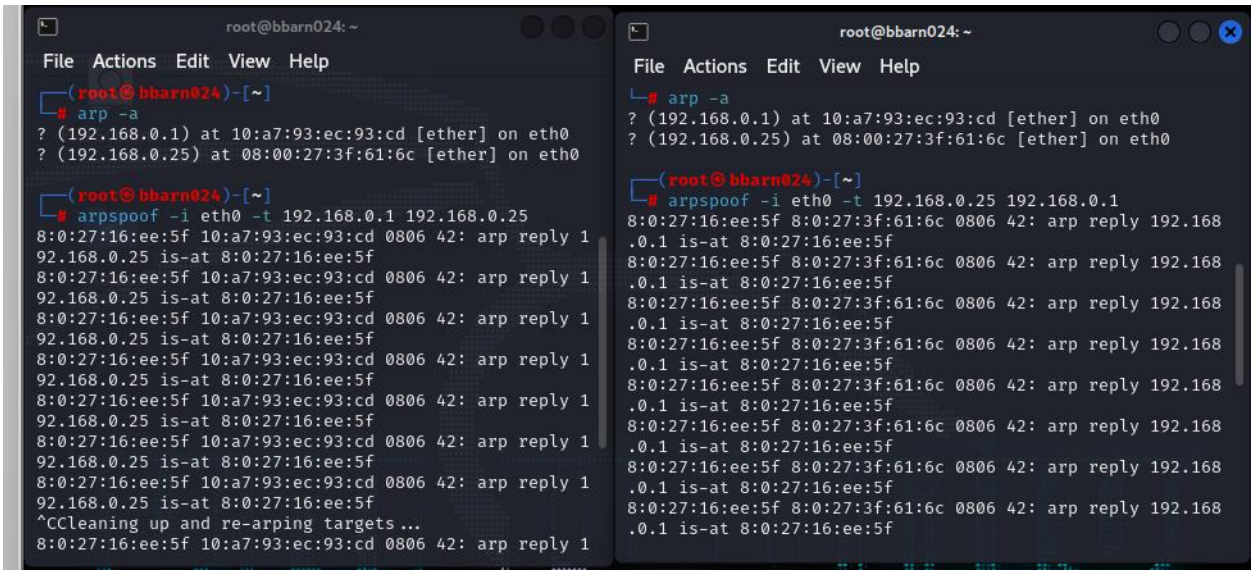


3. Enable IP forwarding.

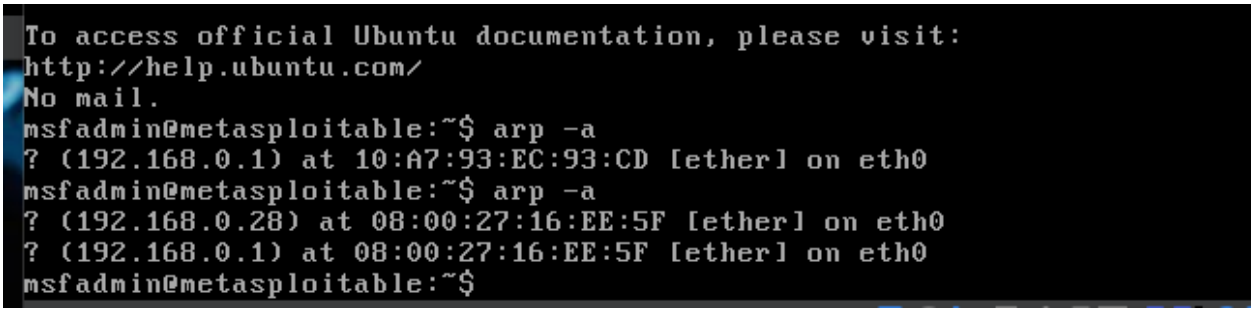


4-5. Generate multiple fake ARP replies. Also, trick the router into believing you are the victim so that you can intercept incoming internet

traffic on the victim's behalf.

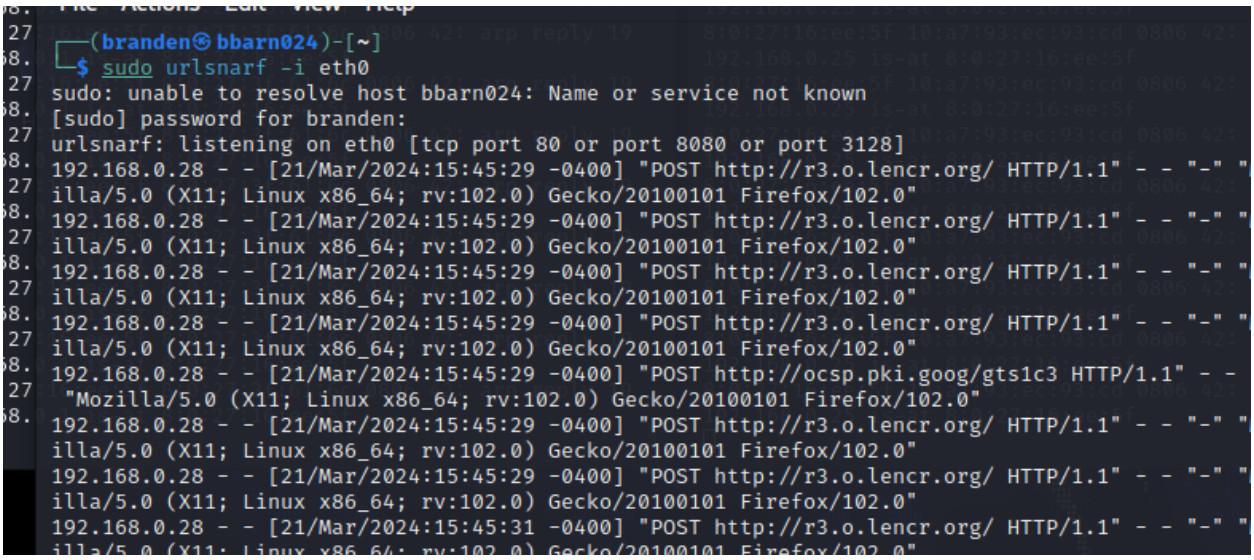


6. Check the Arp table in the target Machine.



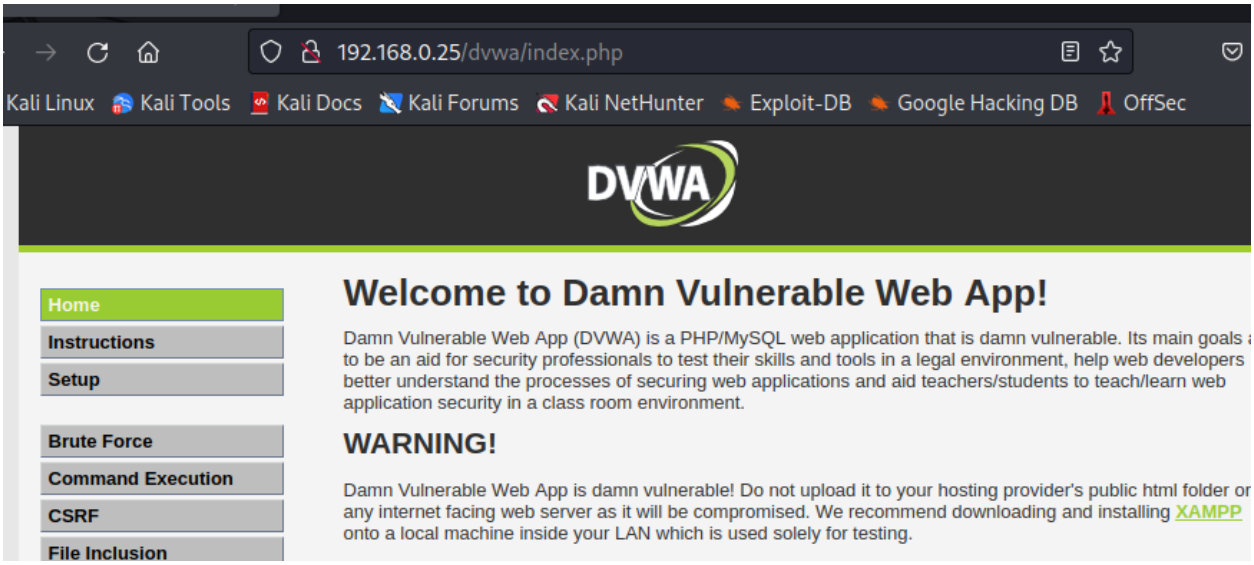
The MAC address changed to the Kali MAC address.

7. Extract the URLs running.

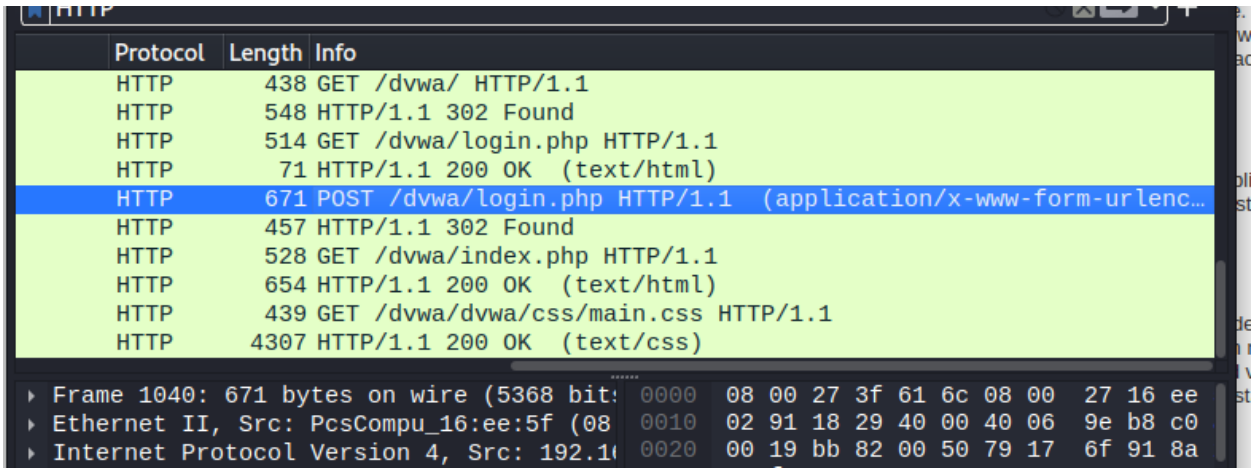


8. Open a browser in kali Linux and type the IP address of Metasploitable2 (Target Machine). Then go to DVWA page which would look like the following screenshot.

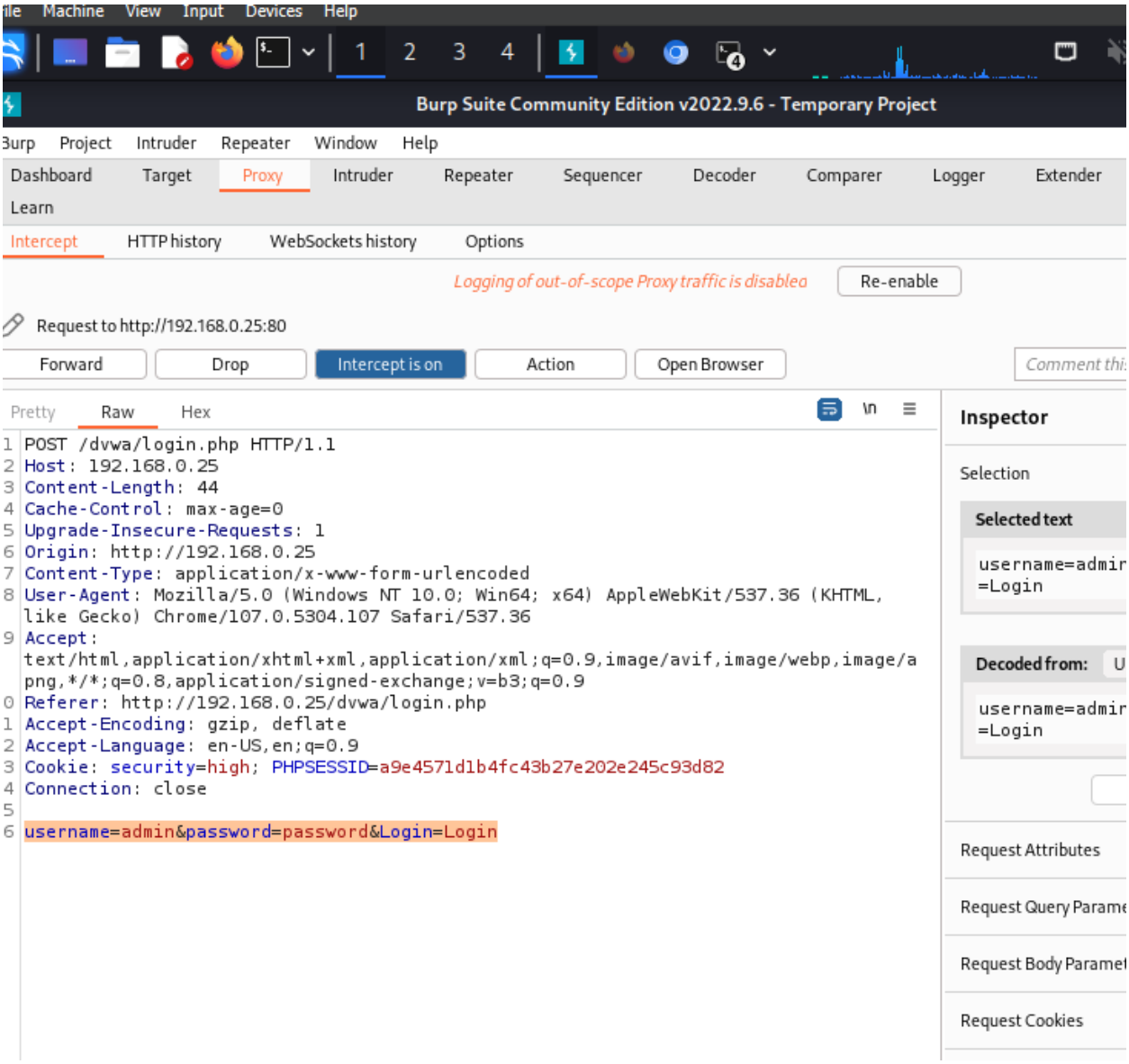
Login using username : admin and password : password.



9. Now open Wireshark and analyze HTTP POST packet to capture the credentials you used to login to DVWA page in Metasploitable2 VM.



10. Open Burp Suite in Kali Linux to harvest the credentials.


ile Machine View Input Devices Help
1 2 3 4
Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Learn
Intercept HTTP history WebSockets history Options
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Request to http://192.168.0.25:80
Forward Drop Intercept is on Action Open Browser
Comment this
Pretty Raw Hex
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.0.25
3 Content-Length: 44
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.0.25
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.0.25/dvwa/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=high; PHPSESSID=a9e4571d1b4fc43b27e202e245c93d82
14 Connection: close
15
16 username=admin&password=password&Login=Login
Inspector
Selection
Selected text
username=admin
=Login
Decoded from:
username=admin
=Login
Request Attributes
Request Query Parame
Request Body Paramet
Request Cookies