Simulated SQL Injection Attack

Date: May 29, 2025

Analyst: Sheniese Aracena-Baez

I wanted to simulate a SQL injection attack from Kali Linux to Metasploitable 2 as the Target machine. During my research, I found that SQL injection attacks are one of the top 3 most common attacks.

This proved to be challenging for me based on my skill level and found myself having to do a lot of troubleshooting and going through hurdles. I did research for different references on how to recreate this type of attack while getting as much data as possible to provide a full report.

A SQL attack = SQL injection, is a type of cyberattack that targets databases/mysql servers through vulnerable web applications. The adversary is tricking a system by inputting malicious Structured Query

Language commands to gain access to that database. Ref:OWASP SQL Injection, What Is SQL Injection (SQLi)

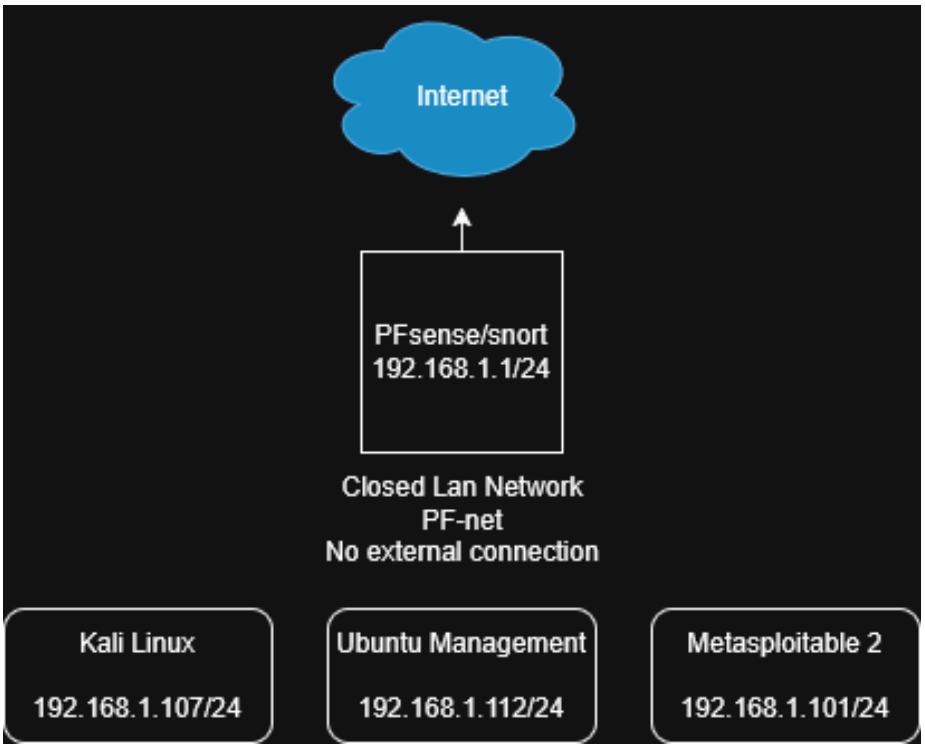
In creating this lab, I was often reminded of many things I've learned thus far in Phase 1.

- Creating a closed environment (Linux nodes/windows active directory domain controller)
- Understanding networking basics like pinging, lan/wan networks, setting your own network and verifying settings/information
- Cyber security frame works, I was specifically reminded of the cyber kill chain, and researching Common vulnerabilities and exposures.
- Again networking concepts like understanding which ports, and protocols that are being used things like this made looking through wireshark much easier to understand.
- The importance of reporting. In this report, I will take technical language and translate it to the best of my ability so it is easier to digest for anyone that reads this.

This is how my topology was set up for this lab within VirtualBox. The first virtual machine configured was pfSense, which operates as both a router and firewall. pfSense has both a public and a private IP address, with two network adapters attached—one for Network Address Translation (NAT) and another for communication within the local area network (LAN). The LAN includes three additional machines that are isolated from the internet and have no connection to the World Wide Web.

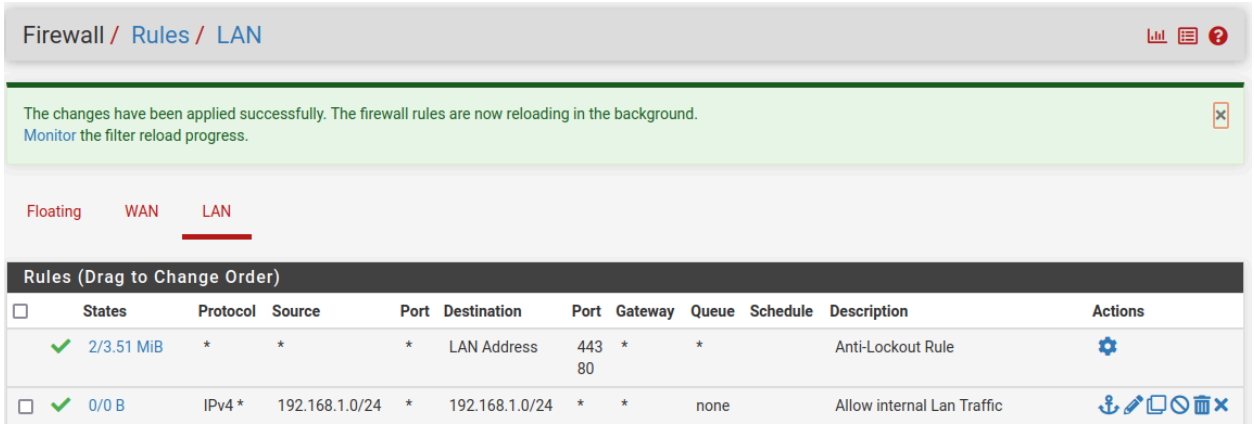
- Topology is in reference to how the network is arranged.

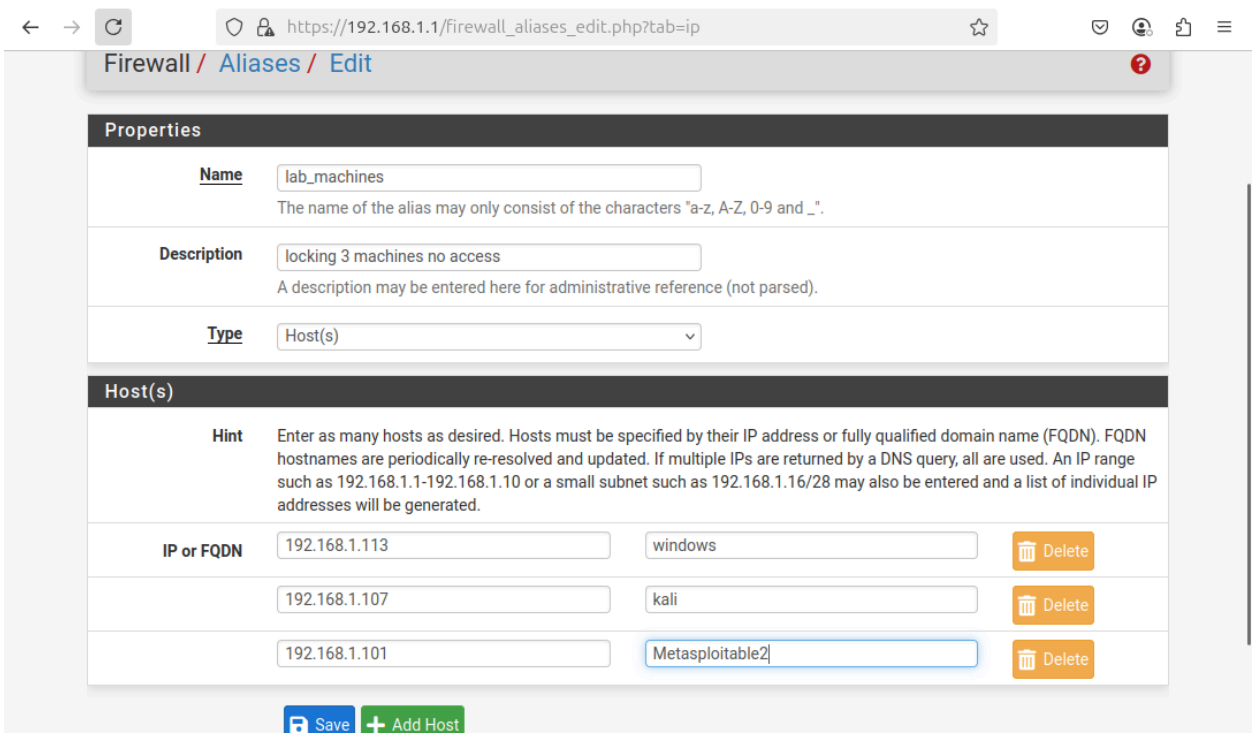
- A firewall is a system that in this case will monitor and control incoming and out going communications/traffic within this network.
- A virtual machine is a software based computer. It digitally replicates hardware, allowing multiple virtual computers of even different operating systems to run on



Virtual Environment and System configuration

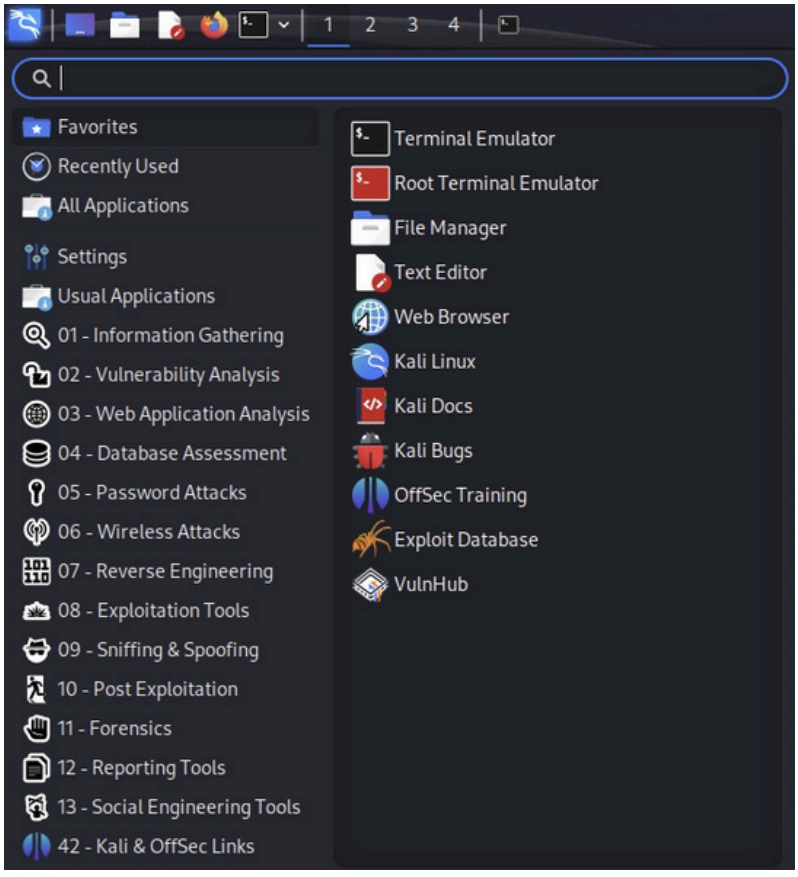
- PFSense:
    - Working as the gateway/router
    - Configured with firewall rules to close off Kali Linux, Ubuntu Management, Metasploitable 2. These 3 machines can communicate with each other but cannot ping anything outside the local area network like pinging or attempting communication with google.com
    - Assigned both a Public and Private IP address. Public IP 10.0.2.15/24 Private 192.168.1.1/24





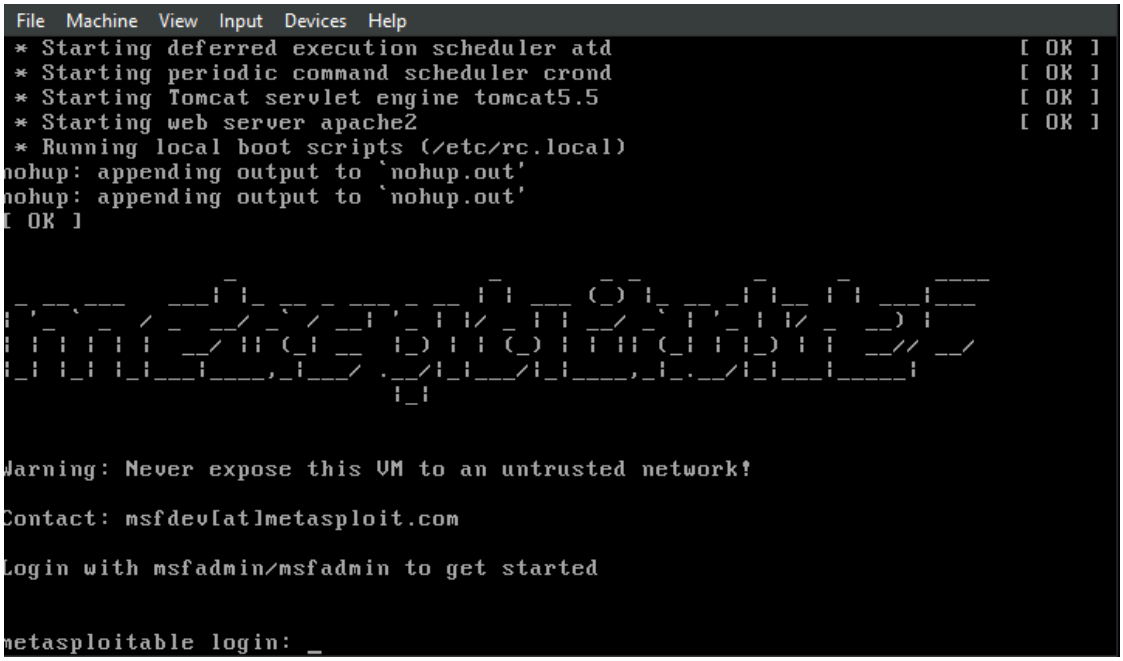
- Kali Linux
    - Working as the hacker/attacking machine

- Using readily installed open source tools for all things Cybersecurity for both Blue team and Red team tactics. In this lab the following tools were used SQLmap, BurpSuite, Nikto, Nmap, Wireshark
- IP configuration done through Dynamic Host Control Protocol from PFsense, IP assigned 192.168.1.107
- Recommended only as a tool for learning purposes and should always be used in a closed environment, within a virtual machine



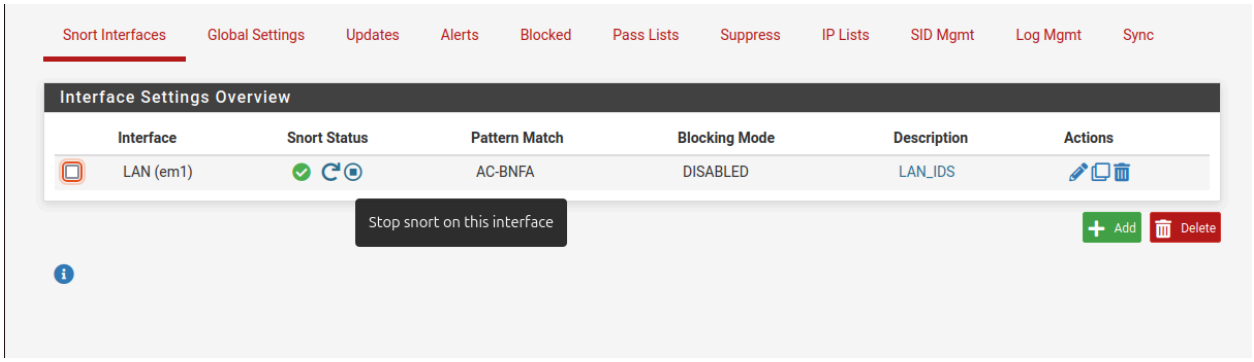
- Metasploitable 2
  - Configured to be a target/vulnerable machine
  - Programmed with outdated and vulnerable services
  - Cannot be upgraded or patched
  - Ideal for simulating cyberattacks for learning purposes

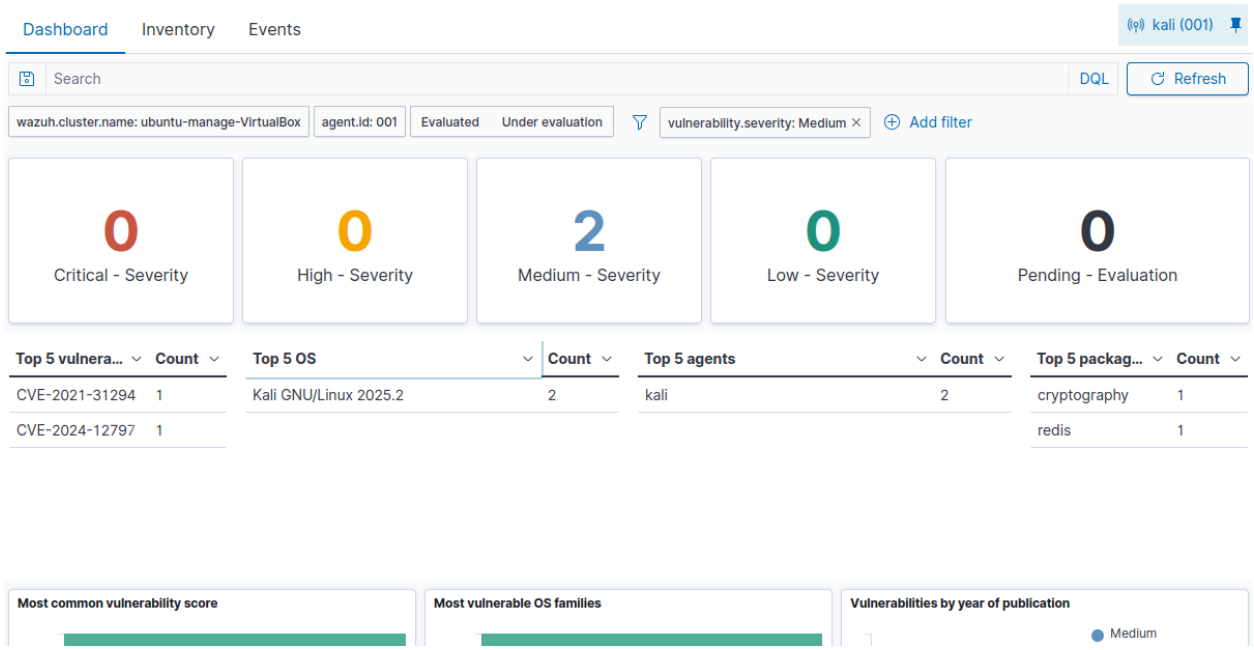
- Should never have direct access to the internet due to its vulnerability. Should only be used within a virtual machine



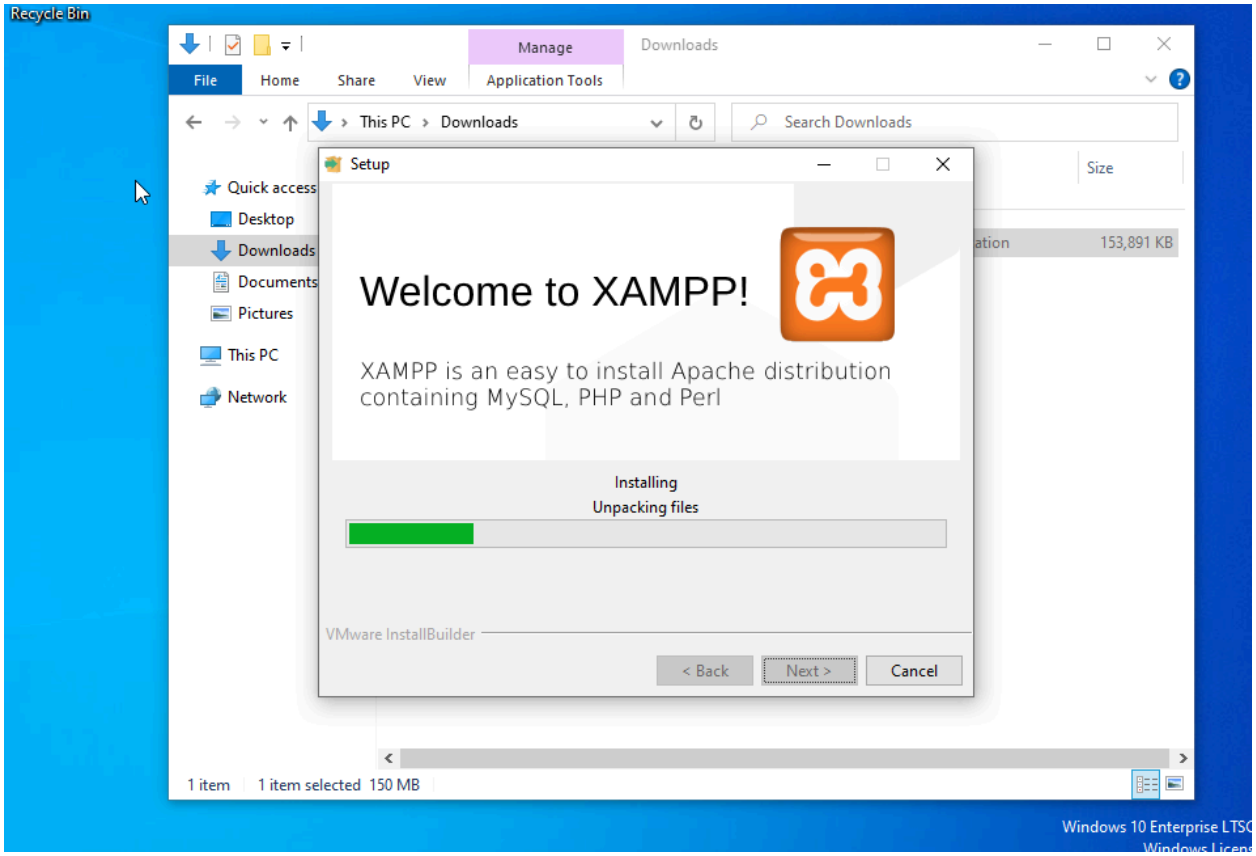
- Ubuntu Management Machine
    - Function solely to monitor, set alerts and manage our firewall
    - Initial access to the internet in order to set up pfSense, Snort, and Wazuh

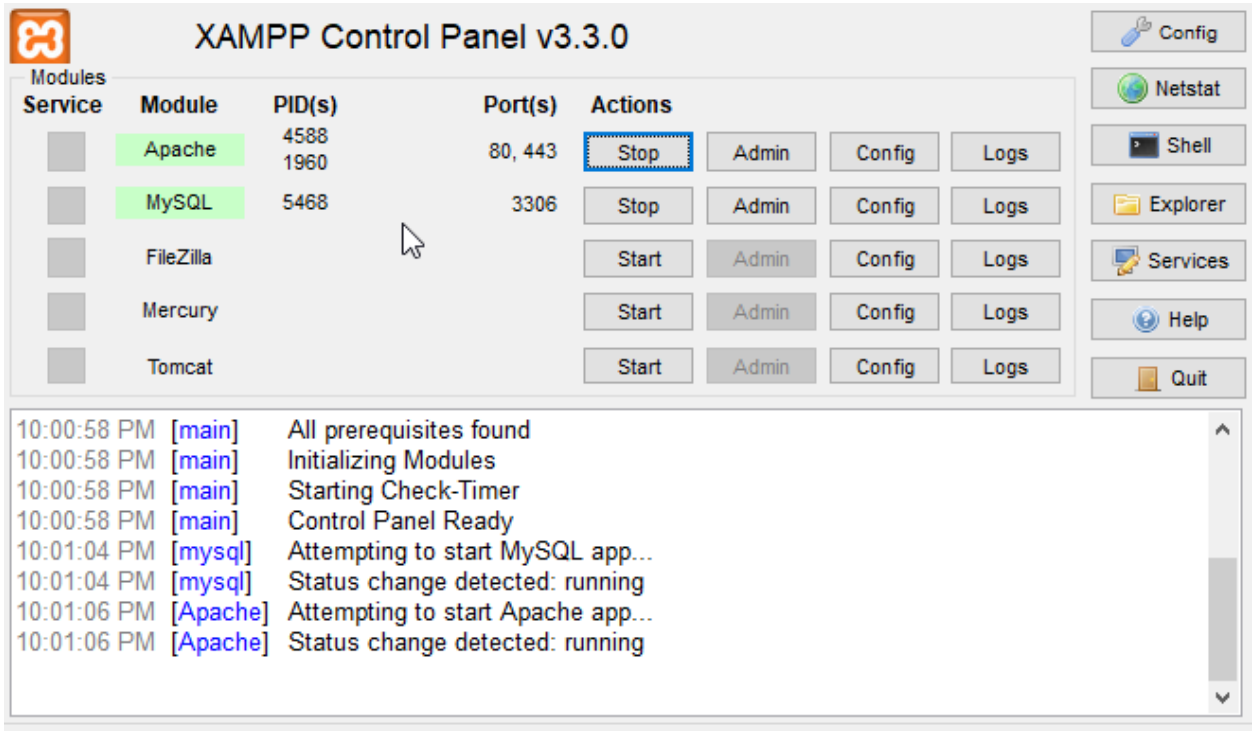
```
< x-amz-server-side-encryption: AES256
< x-amz-version-id: S6vrBinshb9PNe1U2.bGdhznQ1VmyEGJ
< accept-ranges: bytes
< server: AmazonS3
< date: Thu, 29 May 2025 15:29:56 GMT
< etag: "15ac555bcb3ec32405eabf5b86e9c967"
< x-cache: Hit from cloudfront
< via: 1.1 0146c8129cacdacca96753291cf27ec4.cloudfront.net (CloudFront)
< x-amz-cf-pop: EWR53-P1
< x-amz-cf-id: 4xQrWvXEkh2lOOI21q-kAmgx45FXNDd0KiythQruaqTr3-vcNY0RFw==
< age: 52841
<
{ [8192 bytes data]
100  192k  100  192k    0     0   558k      0 --:--:-- --:--:-- --:--:--  558k
* Connection #0 to host packages.wazuh.com left intact
manage@manage-VirtualBox:~/Desktop$ chmod +x wazuh-install.sh
manage@manage-VirtualBox:~/Desktop$ sudo ./wazuh-install.sh -a
30/05/2025 02:10:45 INFO: Starting Wazuh installation assistant. Wazuh version:
4.12.0
30/05/2025 02:10:45 INFO: Verbose logging redirected to /var/log/wazuh-install.l
og
30/05/2025 02:10:50 INFO: --- Dependencies ----
30/05/2025 02:10:50 INFO: Installing gawk.
```





Honorable mention to Windows 10 that was created for this honey pot project but was not used due to how many resources were needed to use this machine and others at the same time. This machine required too many resources and slowed down the processe for the other virtual machines and the host machine. Windows 10 was configured with XAMPP and DVWA in order to simulate web based vulnerability testing.


Recycle Bin
Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Size
153,891 KB
Setup
Welcome to XAMPP!
XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl
Installing
Unpacking files
VMware InstallBuilder
< Back
Next >
Cancel
1 item
1 item selected 150 MB
Windows 10 Enterprise LTSC


XAMPP Control Panel v3.3.0
Modules
Service
Module
PID(s)
Port(s)
Actions
Apache
4588
1960
80, 443
Stop
Admin
Config
Logs
MySQL
5468
3306
Stop
Admin
Config
Logs
FileZilla
Start
Admin
Config
Logs
Mercury
Start
Admin
Config
Logs
Tomcat
Start
Admin
Config
Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
10:00:58 PM [main] All prerequisites found
10:00:58 PM [main] Initializing Modules
10:00:58 PM [main] Starting Check-Timer
10:00:58 PM [main] Control Panel Ready
10:01:04 PM [mysql] Attempting to start MySQL app...
10:01:04 PM [mysql] Status change detected: running
10:01:06 PM [Apache] Attempting to start Apache app...
10:01:06 PM [Apache] Status change detected: running

Kali Linux Tools used to Simulate SQL Injection Attack

5 different tools were used that can typically be found within Kali Linux

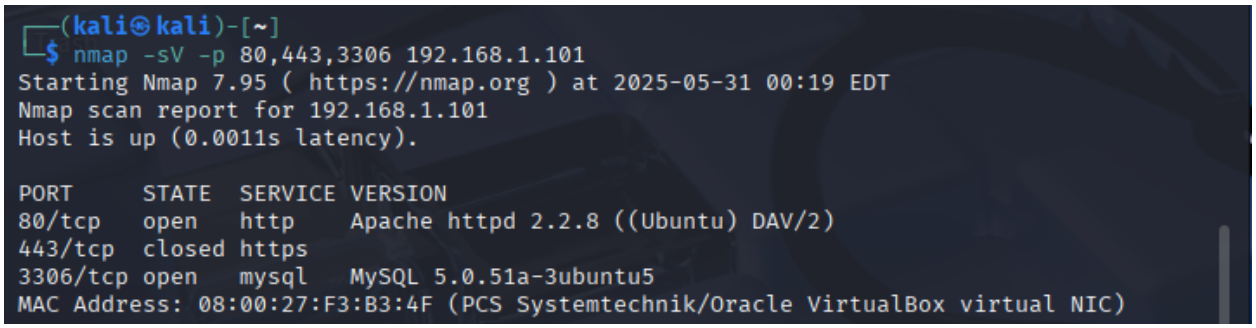
- Nmap
- Nikto
- BurpSuite
- Wireshark (This tool was installed into the Ubuntu management machine for live packet analyzation)
- SQLmap

The tools were used following some of the steps attackers must complete in order to complete their goal.

Ref: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

In this case Reconnaissance was done with Nmap and Nikto.

- Nmap: Is a network discovery tool. It can identify what hosts are currently available and which ports are accessible through the host.

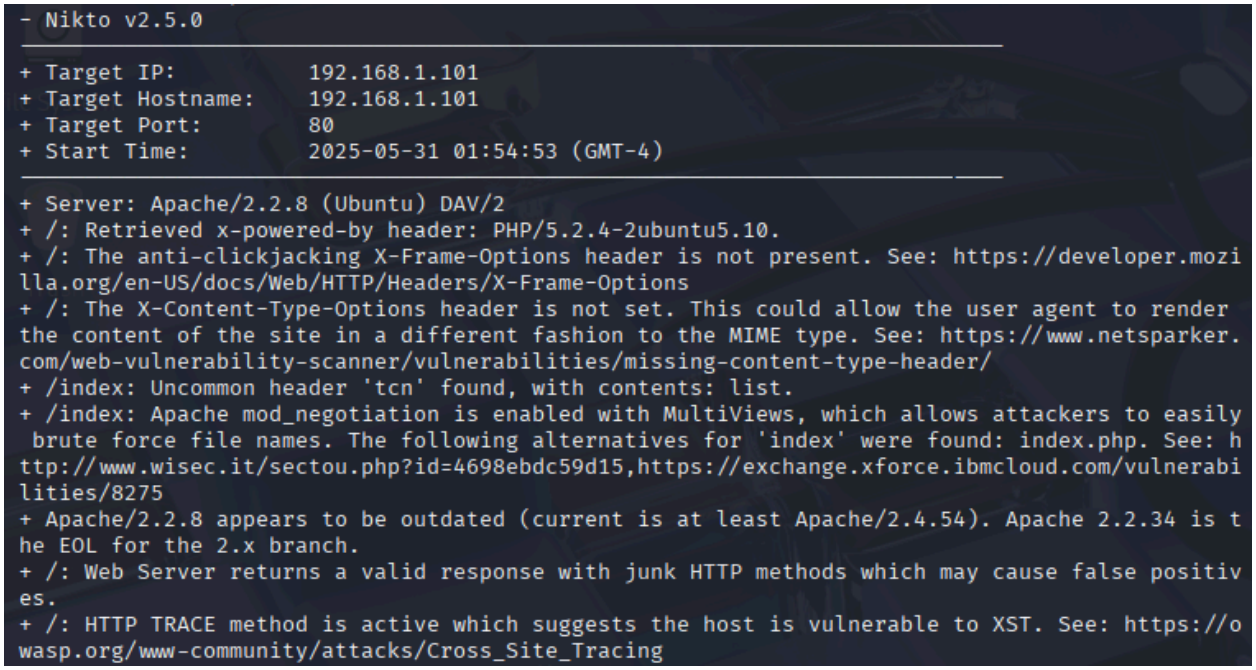


Nmap was used to scan what services are being used in ports 80 (HTTP), 443 (HTTPS), and 3306

(MySQL) instead of all 65,535 ports. This showed us that port 80, and 3306 were open using services HTTP with version Apache httpd 2.2.8 and MySQL version 5.0.51a-3ubuntu5

Reason why this is important in simulating a SQL injection attack is because attackers will scan for ports 80, and 443 due to these being associated with web traffic. Normally, we are using these ports whenever we are accessing a web page through a browser.
Port 3306 is scanned because it is the MySql communication port for example this will be a webpage that requires input like on a form or user login, that input is taken then travels from the webserver into the SQL server hence the SQL injection attack.

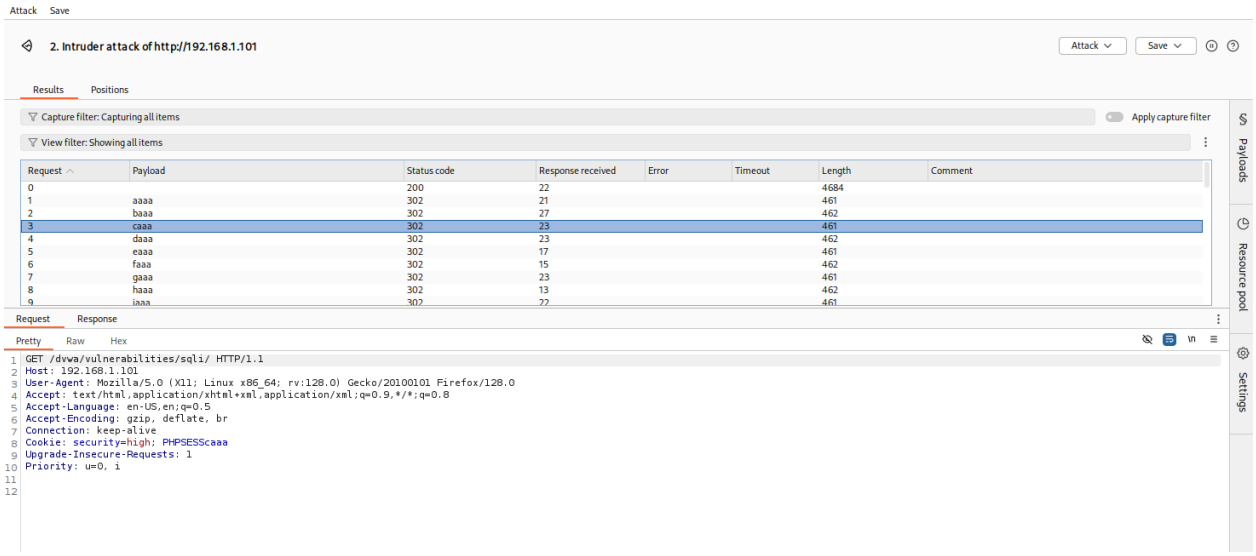
- Nikto is used in this lab to scan web servers for known vulnerabilities that could lead to or support SQL injection attacks. In this case, Nikto gave us a break-down of the server and attacks is can be vulnerable to.

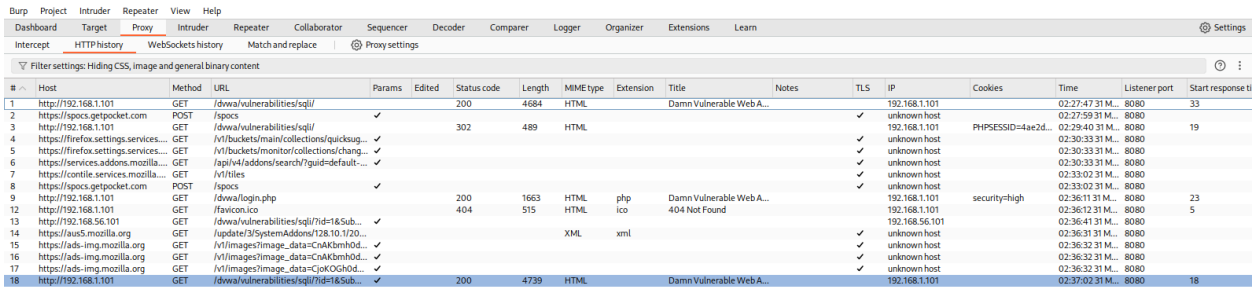


Apache HTTPD 2.2.8 CVE ref: https://nvd.nist.gov/vuln/detail/CVE-2007-6388

https://www.cve.org/CVERecord?id=CVE-2007-6388

- Burp Suite was used to analyze and exploit SQL injection weaknesses in DVWA (Damn Vulnerable Web Application), which was hosted on metasploitable 2 this is done by Interception of HTTP traffic from the DVWA login and SQL Injection pages within the vulnerable web application that is used for testing attacks like these.



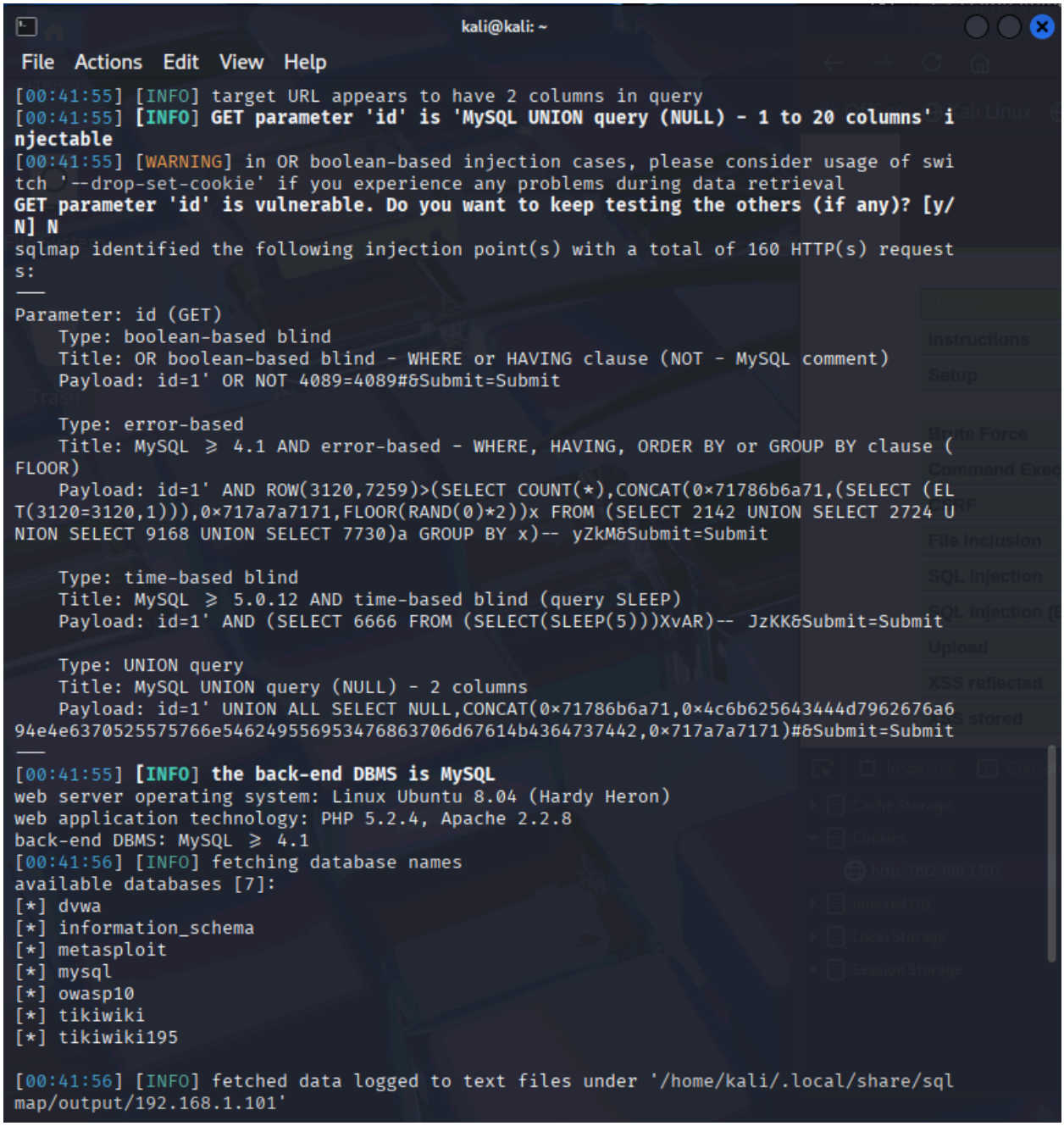


- SQLmap: Automates the process of detecting and exploiting SQL injection weaknesses as well.

  We identified the vulnerability manually with Burp Suite, then used SQLmap to automate the attack.

  SQLmap was able to test and confirm multiple SQL injection techniques. It was able to fetch the

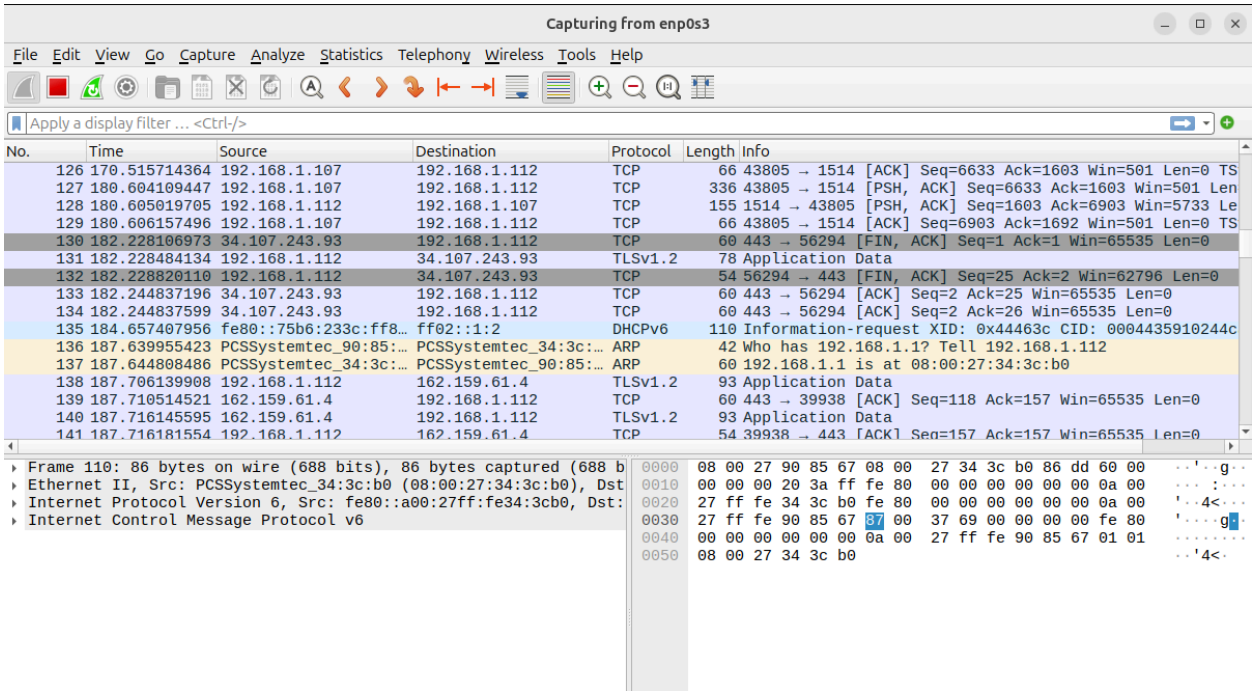
names of the SQL databases.



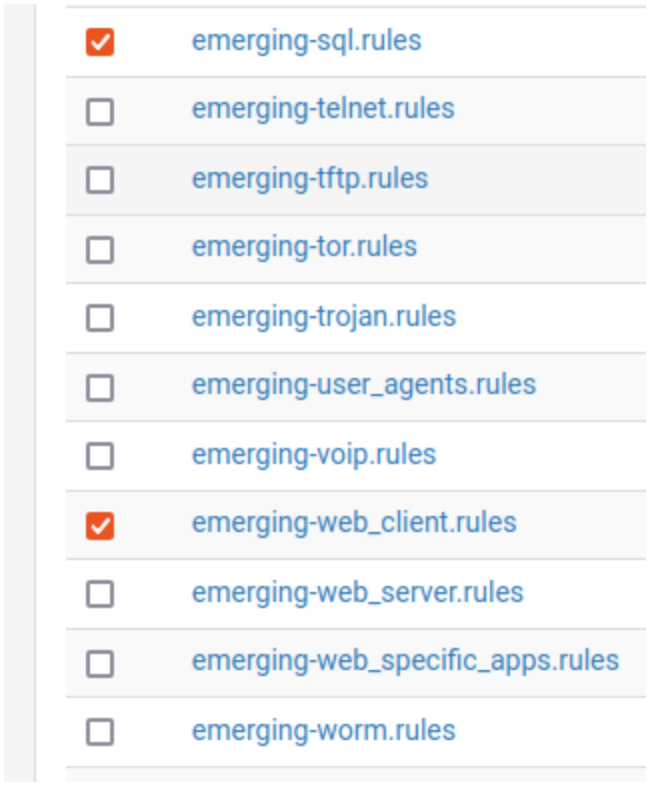
SQLmap is also able to extract user credentials for the users table in the DVWA database, and was able to crack the hash and give the password in plain text.

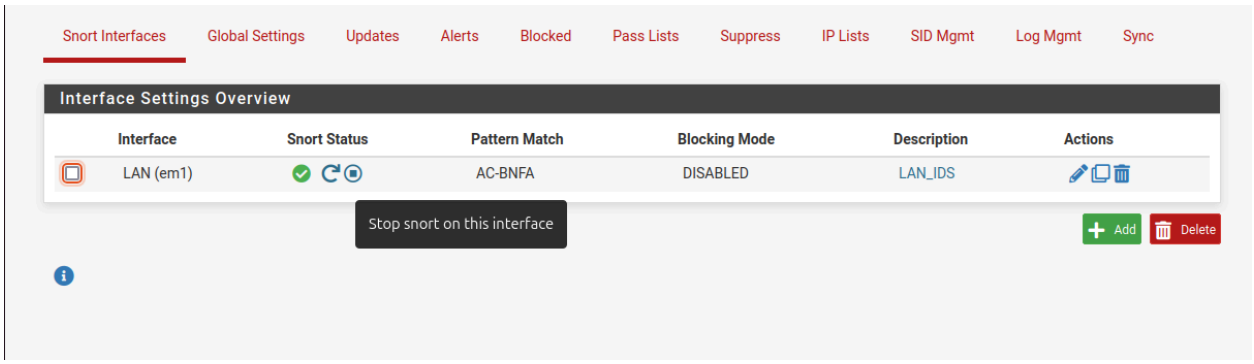
- Wireshark is a tool that lets me see all the network traffic going in and out of a machine or within a network with the right filters and parameters in place. In my lab, I use it on the network to analyze the network traffic.

  It allows for real time packet analyzation and inspection of protocols being used.



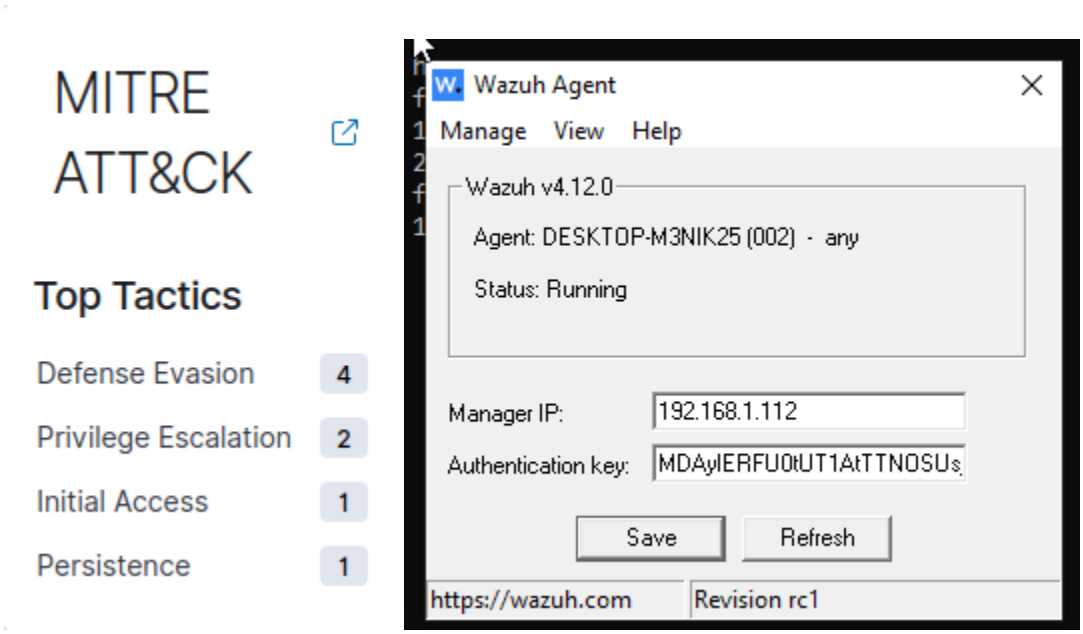
- Snort is an Intrusion Detection System (IDS) it watches traffic passing through pfSense and raises alerts when it sees something suspicious and monitors for anything we set rules for, like a SQL injection attack. This is installed within the services of pfsense and managed through PFsenses gui. We created alerts within Snort looking for any SQL attacks with the selected rules activated for the selected network interface

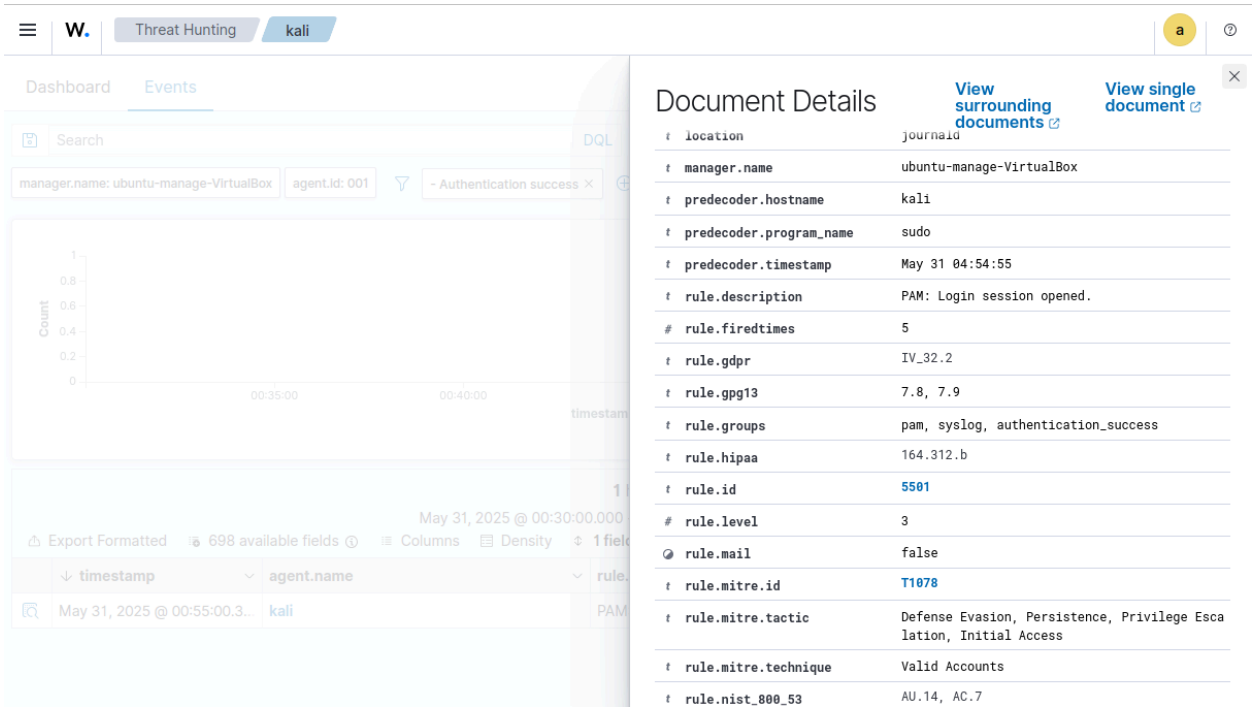


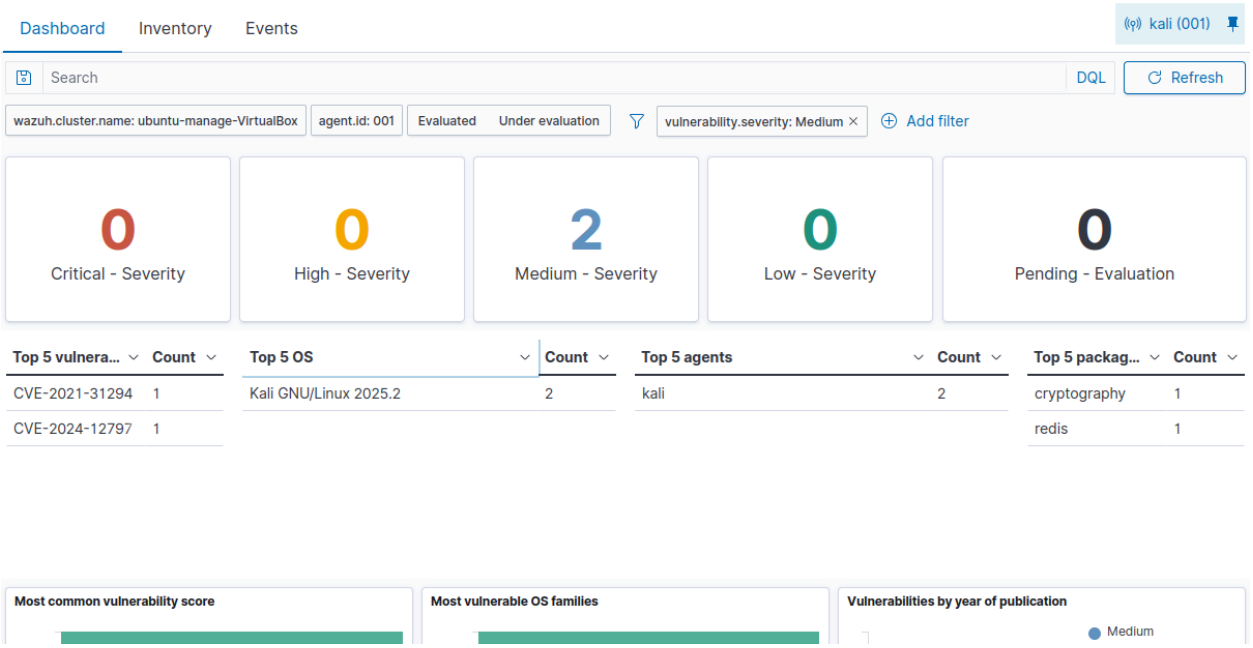


Wazuh is our SIEM/Secuirty Information and Event Management tool it collects logs from all the machines, analyzes them, and gives us a dashboard/gui to see attacks, patterns, and system changes. Metasploitable is too old and out dated (On purpose) to have a tool like this installed. In windows you can just download the msi file and install the wazuh agent then you can simply input the ip address. Initially I had input the authentication code, then on my second attempt I was able to apply this automatically. Lastly, on Kali Linux, Wazuh needed to be installed through the terminal. It became simple when I accessed my Wazuh dashboard on Kali and was able to copy and paste the command into the terminal.

With each attack that was launched from Kali Linux into Metasploitable, we are able to see the type of attack and when it was executed.







This project gave me a deeper understanding of the way actual cyberattacks like SQL injection can happen and the way blue teamers pick up on them through the use of tools like Snort, and Wazuh. I was able to isolate a network to test and monitor the attacks in a safe environment and learn about the way reconnaissance, exploitation, and analysis work with each other with respect to red and blue team operations.

The project tested me, pushed me through technical hurdles, and pushed me to troubleshoot in ways a possible real world SOC can work. It allowed me to use what I've learned in Phase 1 from the fundamentals of networking through security frameworks such as the Cyber Kill Chain and being hands on with what we've been learning..

References

OWASP Foundation. (2021). *OWASP Top Ten Web Application Security Risks – 2021*. https://owasp.org/www-project-top-ten/

PortSwigger Ltd. (n.d.). *SQL injection*. Web Security Academy. https://portswigger.net/web-security/sql-injection

Cisco Talos. (n.d.). *Snort user manual*. https://docs.snort.org/

Netgate. (n.d.). *pfSense documentation*. https://docs.netgate.com/pfsense/en/latest/

The Wireshark Team. (n.d.). *Wireshark user's guide*. https://www.wireshark.org/docs/wsug_html_chunked/

Wazuh, Inc. (n.d.). *Wazuh documentation*. https://documentation.wazuh.com/

MITRE Corporation. (n.d.). *MITRE ATT&CK framework*. https://attack.mitre.org/