Network Traffic Analysis - Week 5 Project

Course: ITS4211

Student: Isaac Caballero

Date: 10FEB25

Project Objectives

The objective of this week's project is to complete network traffic analysis tasks within the Project Ares Battle School environment. Tasks include analyzing captured packets, identifying IP addresses, and extracting relevant data using tools on the Kali Linux virtual machine.

Tasks Overview:

1. **Network Analysis (Tasks 15-29):**
   - Analyze a PCAP file (NetworkTraffic.pcap) using tools in Kali Linux.
   - Access the Q&A Portal via the QA_Portal.htm link on the Kali desktop.
   - Answer questions related to the PCAP file, including DNS records, SNMP services, database management systems, and IP addresses.

Key Objectives:

- **Objective 15:** Identify the type of DNS record that points between the domain name and IP address for the Exchange server.
- **Objective 16:** Determine the FQDN (Fully Qualified Domain Name) of the WDC exchange server.

- **Objective 17:** Count the number of PTR DNS queries and replies during the capture.
- **Objective 18:** Identify the IP address that the mail application resolves to.
- **Objective 19:** Find the domain name associated with the IP address 18.6.0.9.
- **Objective 20:** Determine the launch IP address of the SNMP service attack.
- **Objective 21:** Identify the SNMP community string enumerated by the attacker.
- **Objective 22:** Determine the version number of the Linux firmware from the SNMP service.
- **Objective 23:** Identify the Linux command used to gather packets on the server based on the SNMP conversation.
- **Objective 24:** Find the intended recipient of the US Tax Policy Enabled Blog document from the SMB service.
- **Objective 25:** Identify the Relational Database Management System (RDBMS) used within the Washington network.
- **Objective 26:** Determine the IP address that hosts the database.
- **Objective 28:** Find the password for the database user in repeated hexadecimal format.
- **Objective 29:** Identify the name of the database where Personal Identifiable Information (PII) is stored.

Approach and Execution

1. Logged into the Project Ares portal and launched the Battle School game.

2. Entered the Battle Room and initiated the Network Traffic Analysis module.

3. Connected to the Kali Linux virtual machine via VNC session.

4. Opened the provided NetworkTraffic.pcap file and used tools such as Wireshark and command-line utilities to extract necessary information.

5. Accessed the Q&A portal and submitted answers for tasks 15-29.

6. Captured screenshots of each completed objective for documentation.

Challenges and Solutions

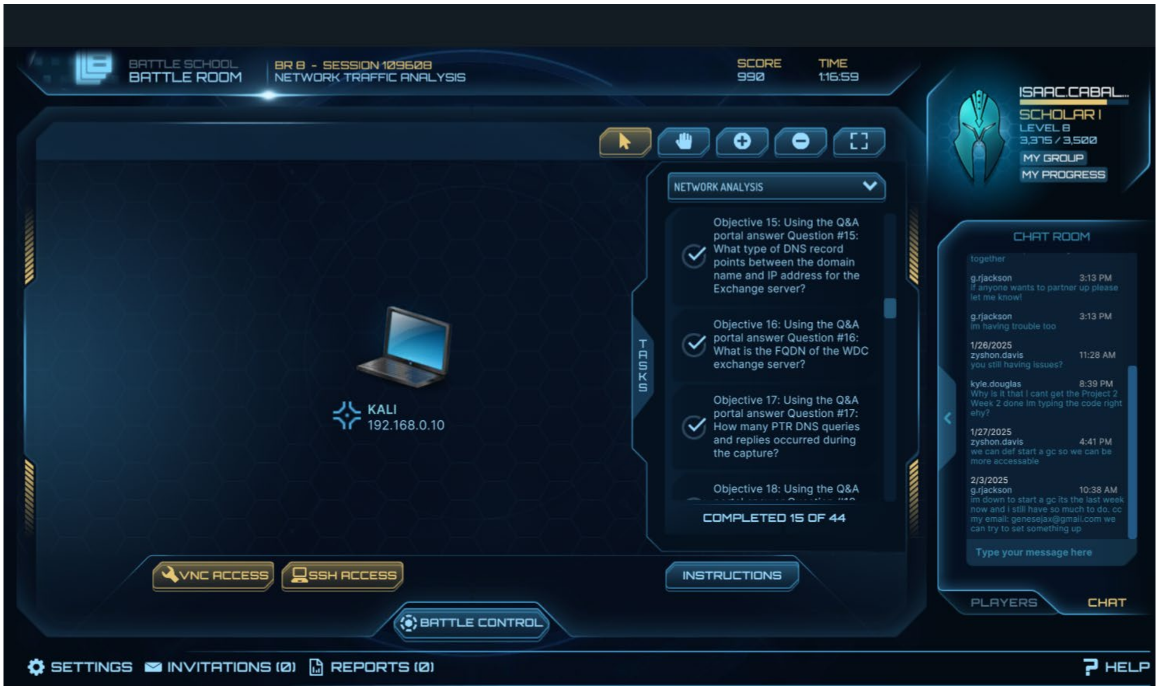
One of the challenges faced was filtering through the network capture to find specific queries. To overcome this, advanced filtering techniques in Wireshark were applied, and command-line tools such as tcpdump and tshark were used to refine searches efficiently.

Benefits of Additional Resources

The resources in the Media Center provided useful background on packet analysis techniques, which helped in interpreting network traffic data. The Game Room activities were beneficial for honing hands-on skills with various network security tools.

Screenshots and Results

Screenshot: w5 br 4.png



✓ Objective 15: Using the Q&A portal answer Question #15: What type of DNS record points between the domain name and IP address for the Exchange server?

✓ Objective 16: Using the Q&A portal answer Question #16: What is the FQDN of the WDC exchange server?

✓ Objective 17: Using the Q&A portal answer Question #17: How many PTR DNS queries and replies occurred during the capture?

Objective 18: Using the Q&A

together

g.rjackson 3:13 PM
If anyone wants to partner up please let me know!

g.rjackson 3:13 PM
im having trouble too

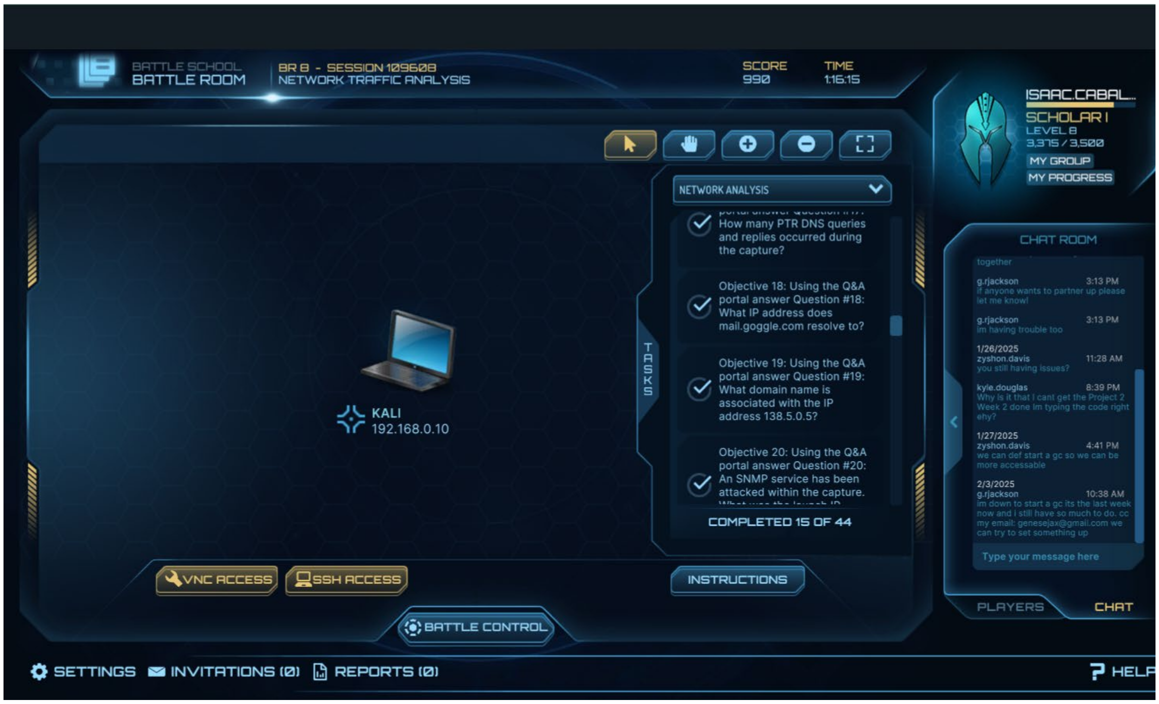
1/26/2025
zyshon.davis 11:28 AM
you still having issues?

kyle.douglas 8:39 PM
Why is it that I cant get the Project 2 Week 2 done Im typing the code right ehy?

1/27/2025
zyshon.davis 4:41 PM
we can def start a gc so we can be more accessable

2/3/2025
g.rjackson 10:38 AM
im down to start a gc its the last week now and i still have so much to do. cc my email: genesejax@gmail.com we can try to set something up

Screenshot: w5 br 3.png



✓ How many PTR DNS queries and replies occurred during the capture?

✓ Objective 18: Using the Q&A portal answer Question #18: What IP address does mail.goggle.com resolve to?

✓ Objective 19: Using the Q&A portal answer Question #19: What domain name is associated with the IP address 138.5.0.5?

✓ Objective 20: Using the Q&A portal answer Question #20: An SNMP service has been attacked within the capture.

together

g.rjackson 3:13 PM
If anyone wants to partner up please let me know!

g.rjackson 3:13 PM
im having trouble too

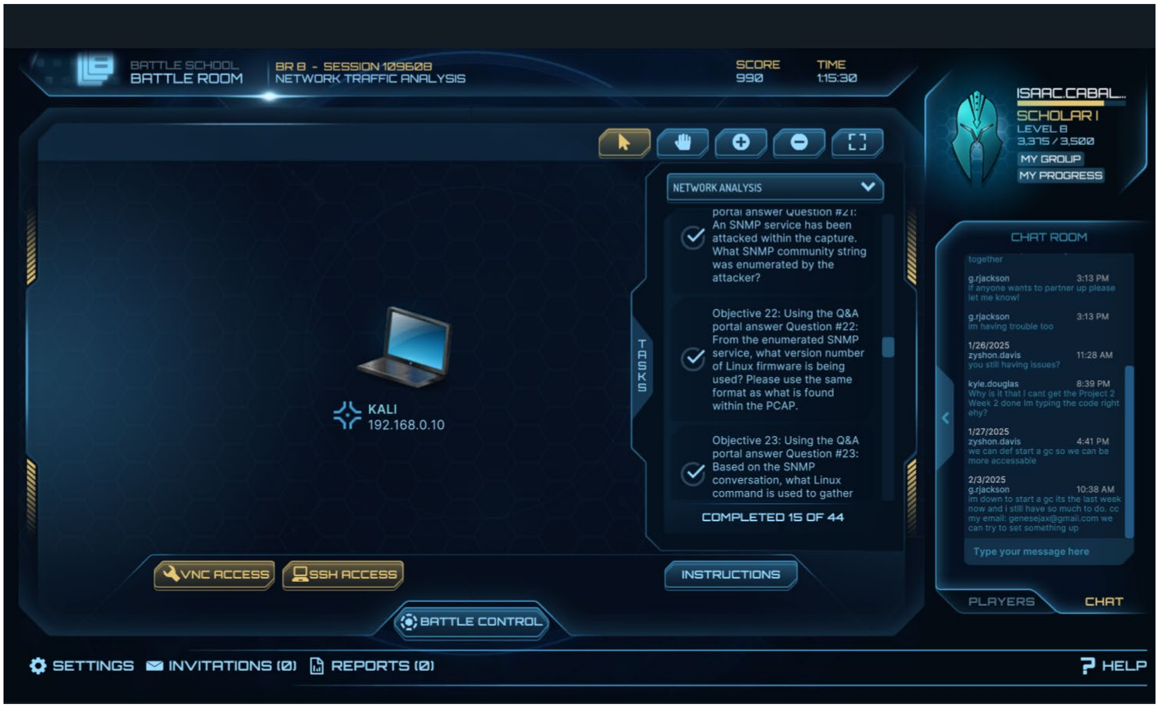
1/26/2025
zyshon.davis 11:28 AM
you still having issues?

kyle.douglas 8:39 PM
Why is it that I cant get the Project 2 Week 2 done Im typing the code right ehy?

1/27/2025
zyshon.davis 4:41 PM
we can def start a gc so we can be more accessable

2/3/2025
g.rjackson 10:38 AM
im down to start a gc its the last week now and i still have so much to do. cc my email: genesejax@gmail.com we can try to set something up

Screenshot: w5 br 2.png



portal answer Question #21: An SNMP service has been attacked within the capture. What SNMP community string was enumerated by the attacker?

Objective 22: Using the Q&A portal answer Question #22: From the enumerated SNMP service, what version number of Linux firmware is being used? Please use the same format as what is found within the PCAP.

Objective 23: Using the Q&A portal answer Question #23: Based on the SNMP conversation, what Linux command is used to gather

COMPLETED 15 OF 44

together

g.rjackson 3:13 PM
if anyone wants to partner up please let me know!

g.rjackson 3:13 PM
im having trouble too

1/26/2025
zyshon.davis 11:28 AM
you still having issues?

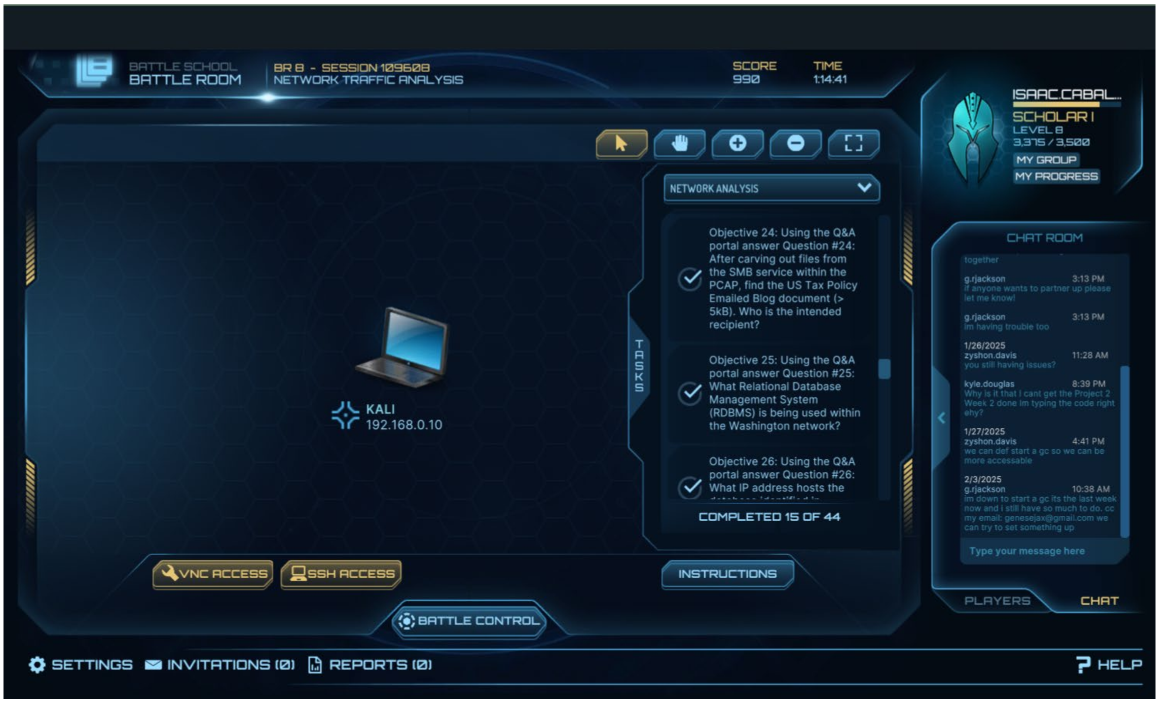
kyle.douglas 8:39 PM
Why is it that I cant get the Project 2 Week 2 done Im typing the code right ehy?

1/27/2025
zyshon.davis 4:41 PM
we can def start a gc so we can be more accessable

2/3/2025
g.rjackson 10:38 AM
im down to start a gc its the last week now and i still have so much to do. cc my email: genesejax@gmail.com we can try to set something up

Type your message here

Screenshot: w5 br 1.png



Objective 24: Using the Q&A portal answer Question #24: After carving out files from the SMB service within the PCAP, find the US Tax Policy Emailed Blog document (> 5kB). Who is the intended recipient?

Objective 25: Using the Q&A portal answer Question #25: What Relational Database Management System (RDBMS) is being used within the Washington network?

Objective 26: Using the Q&A portal answer Question #26: What IP address hosts the

COMPLETED 15 OF 44

together

g.rjackson 3:13 PM
if anyone wants to partner up please let me know!

g.rjackson 3:13 PM
im having trouble too

1/26/2025
zyshon.davis 11:28 AM
you still having issues?

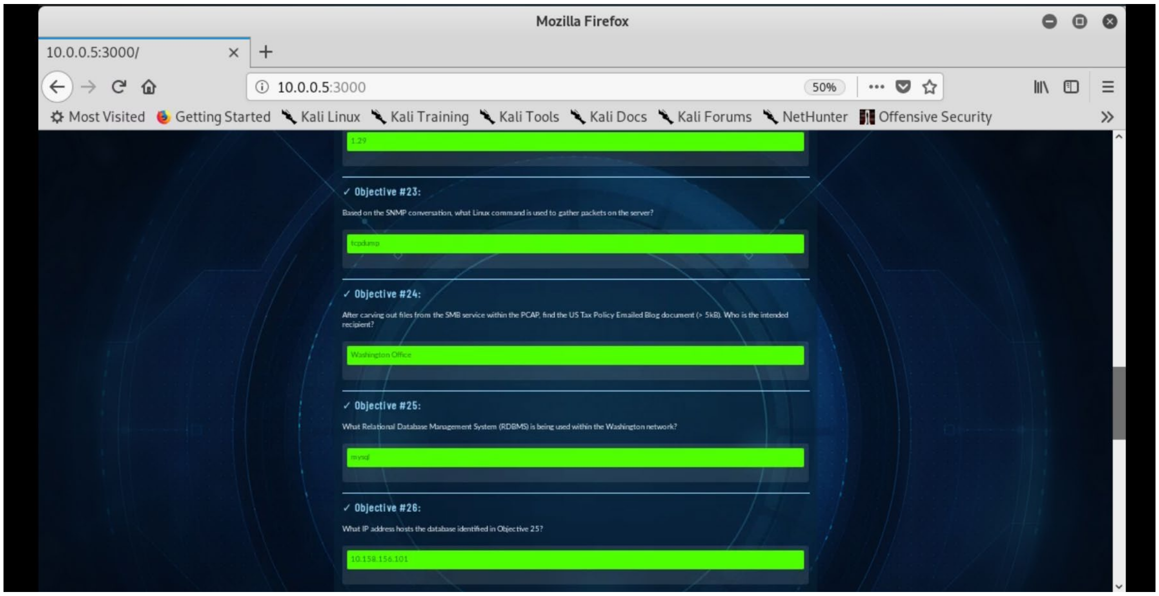
kyle.douglas 8:39 PM
Why is it that I cant get the Project 2 Week 2 done Im typing the code right ehy?

1/27/2025
zyshon.davis 4:41 PM
we can def start a gc so we can be more accessable

2/3/2025
g.rjackson 10:38 AM
im down to start a gc its the last week now and i still have so much to do. cc my email: genesejax@gmail.com we can try to set something up

Type your message here

Screenshot: w5 br.png



1.29

✓ Objective #23:

Based on the SNMP conversation, what Linux command is used to gather packets on the server?

tcpdump

✓ Objective #24:

After carving out files from the SMB service within the PCAP, find the US Tax Policy Emailed Blog document (> 5kB). Who is the intended recipient?

Washington Office

✓ Objective #25:

What Relational Database Management System (RDBMS) is being used within the Washington network?

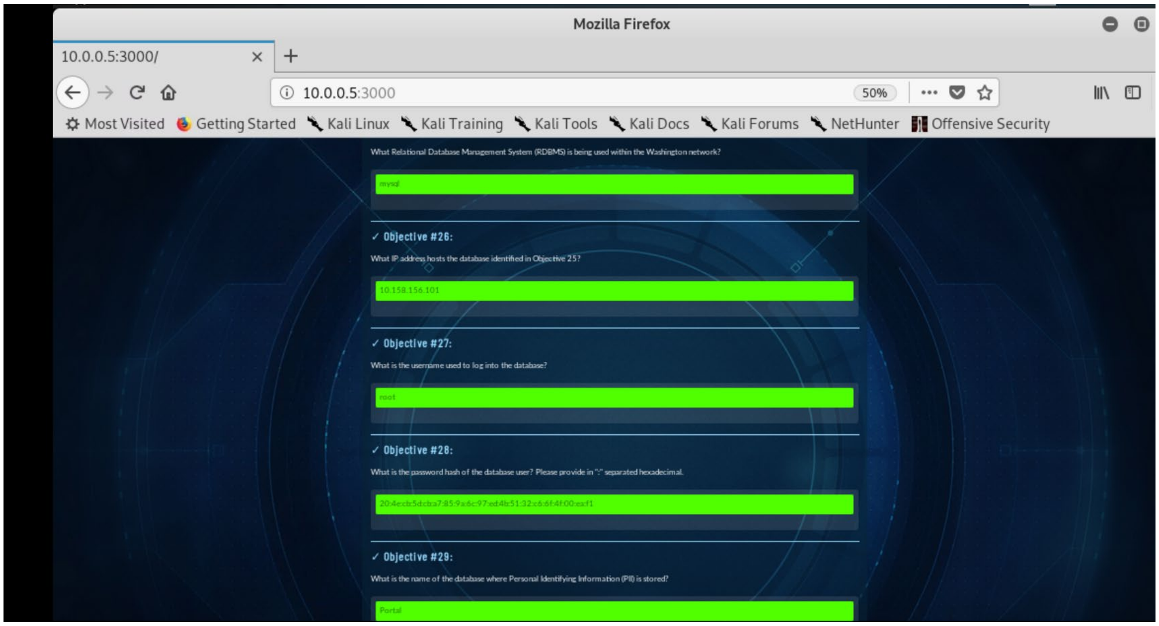
mysql

✓ Objective #26:

What IP address hosts the database identified in Objective 25?

10.158.156.101

Screenshot: w5 project 4.png



What Relational Database Management System (RDBMS) is being used within the Washington network?

mysql

✓ Objective #26:

What IP address hosts the database identified in Objective 25?

10.158.156.101

✓ Objective #27:

What is the username used to log into the database?

root

✓ Objective #28:

What is the password hash of the database user? Please provide in ":" separated hexadecimal.

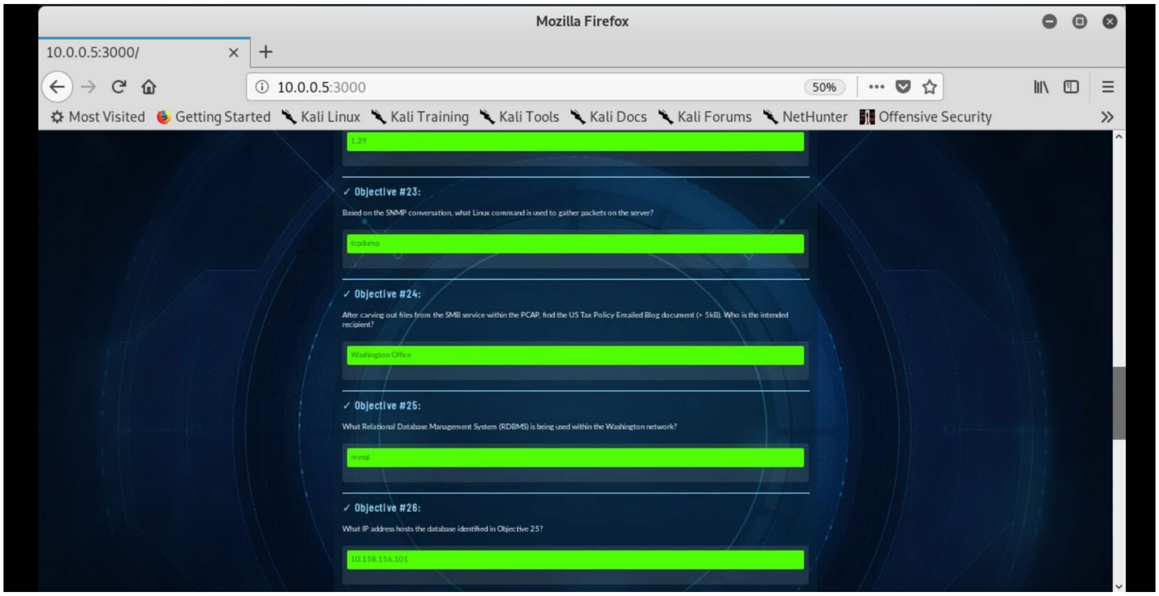
20:4e:cb:5d:cb:a7:85:9a:6c:97:ed:4b:51:32:c6:6f:4f:00:ea:f1

✓ Objective #29:

What is the name of the database where Personal Identifying Information (PII) is stored?

Portal

Screenshot: w5 project 3.png



1.29

✓ Objective #23:

Based on the SNMP conversation, what Linux command is used to gather packets on the server?

tcpdump

✓ Objective #24:

After carving out files from the SMB service within the PCAP, find the US Tax Policy Emailed Blog document (> 5kB). Who is the intended recipient?

Washington Office

✓ Objective #25:

What Relational Database Management System (RDBMS) is being used within the Washington network?

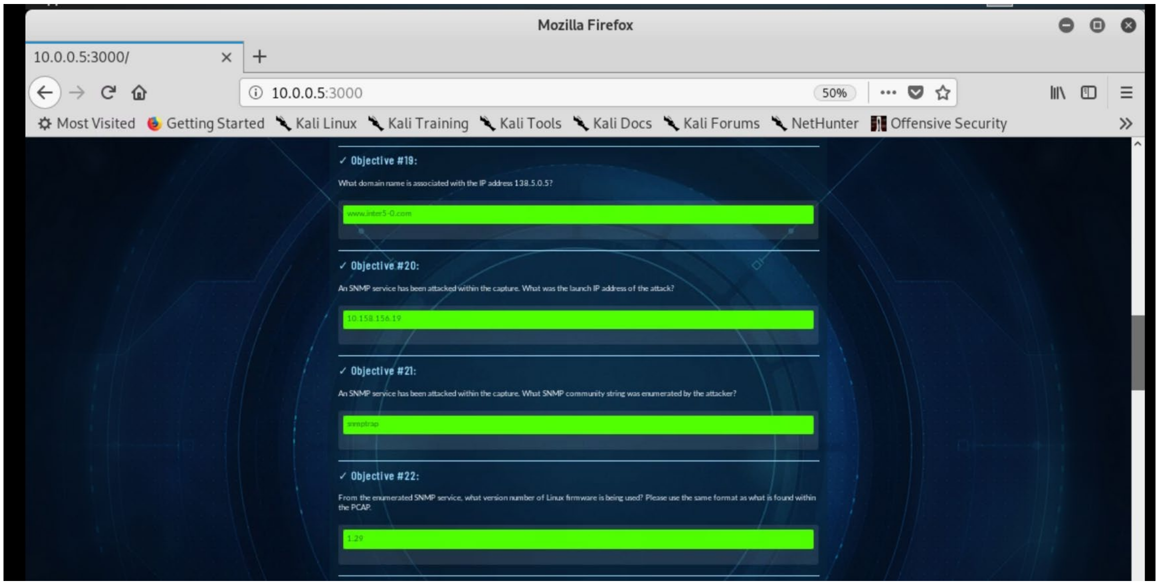
mysql

✓ Objective #26:

What IP address hosts the database identified in Objective 25?

10.158.156.101

Screenshot: w5 project 2.png



✓ Objective #19:

What domain name is associated with the IP address 138.5.0.5?

www.inter5-0.com

✓ Objective #20:

An SNMP service has been attacked within the capture. What was the launch IP address of the attack?

10.158.156.19

✓ Objective #21:

An SNMP service has been attacked within the capture. What SNMP community string was enumerated by the attacker?

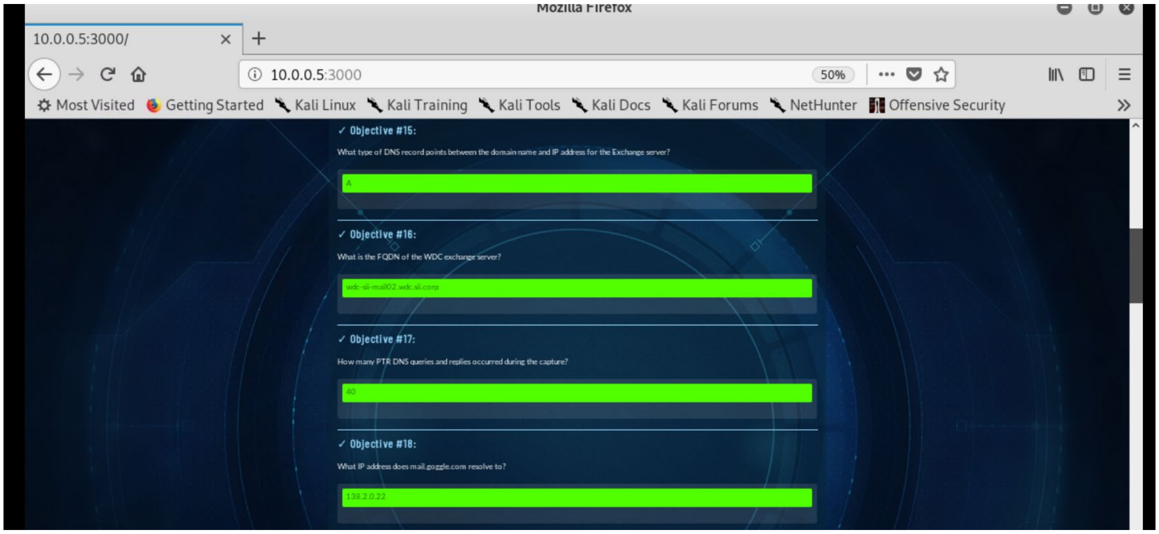
snmptrap

✓ Objective #22:

From the enumerated SNMP service, what version number of Linux firmware is being used? Please use the same format as what is found within the PCAP.

1.29

Screenshot: week 5 project .png



✓ Objective #15:

What type of DNS record points between the domain name and IP address for the Exchange server?

A

✓ Objective #16:

What is the FQDN of the WDC exchange server?

wdc-sii-mail02.wdc.sii.corp

✓ Objective #17:

How many PTR DNS queries and replies occurred during the capture?

40

✓ Objective #18:

What IP address does mail.goggle.com resolve to?

138.2.0.22