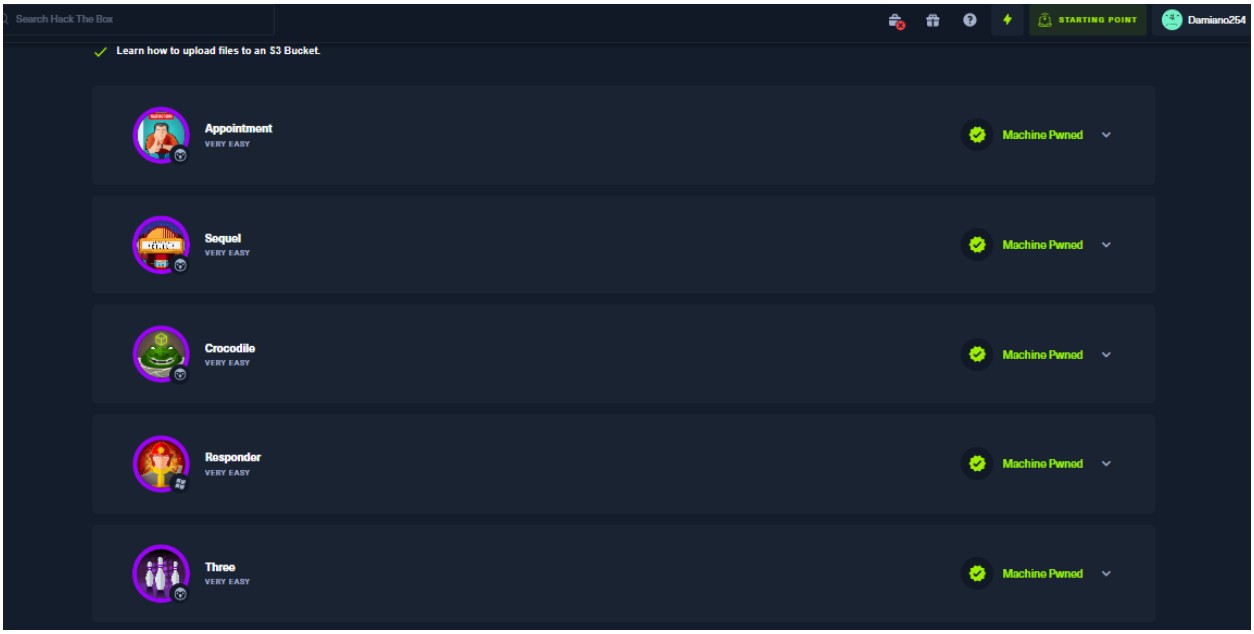


APPOINTMENT

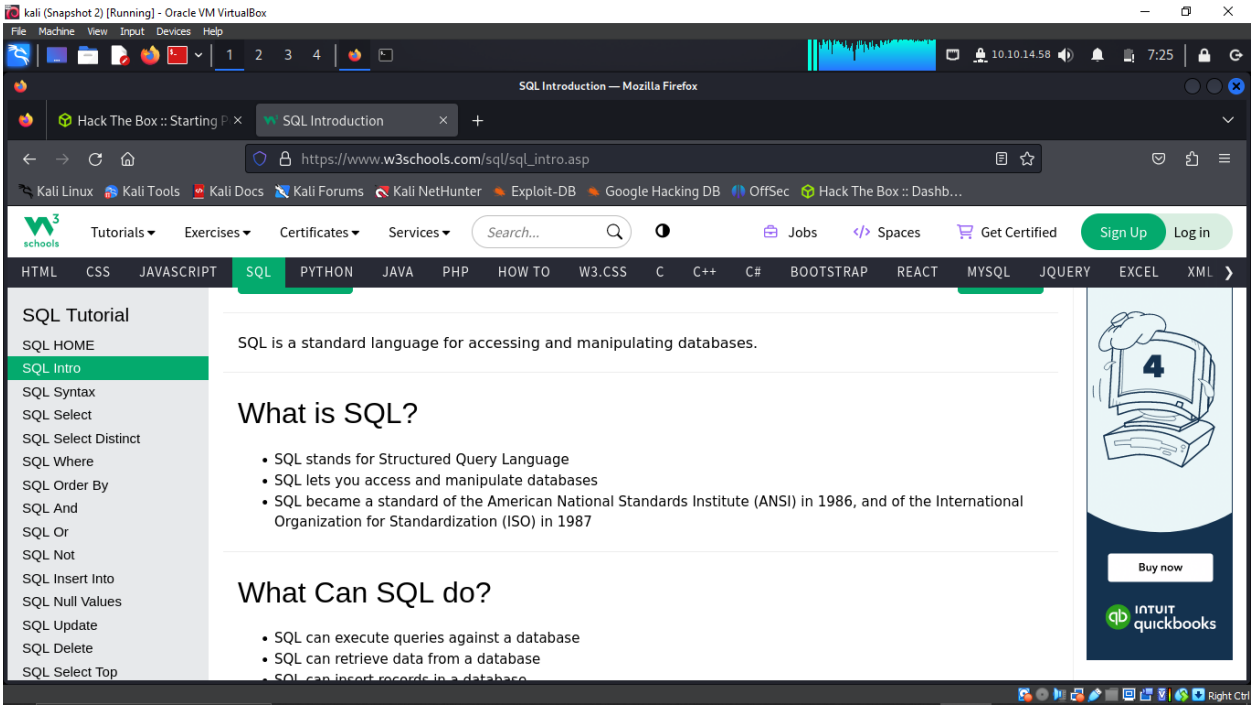
Introduction

The "Appointment" lab is a focused exercise on web application security, specifically targeting SQL vulnerabilities. The lab offers a practical approach to understanding the mechanics of SQL injection and other common web security issues.

Tasks and Findings

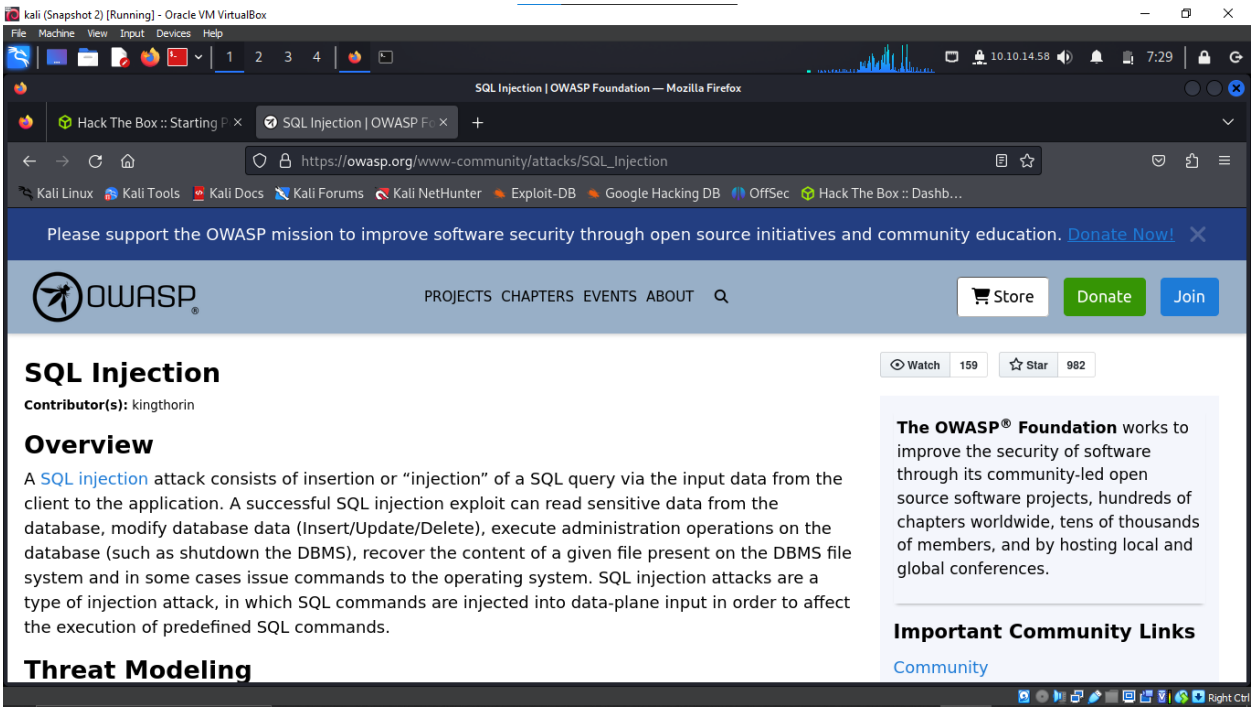
Task 1: SQL Basics

- **Question:** What does SQL stand for?
- **Answer:** Structured Query Language
- **Insight:** Understanding SQL is fundamental in manipulating and querying databases.

- 

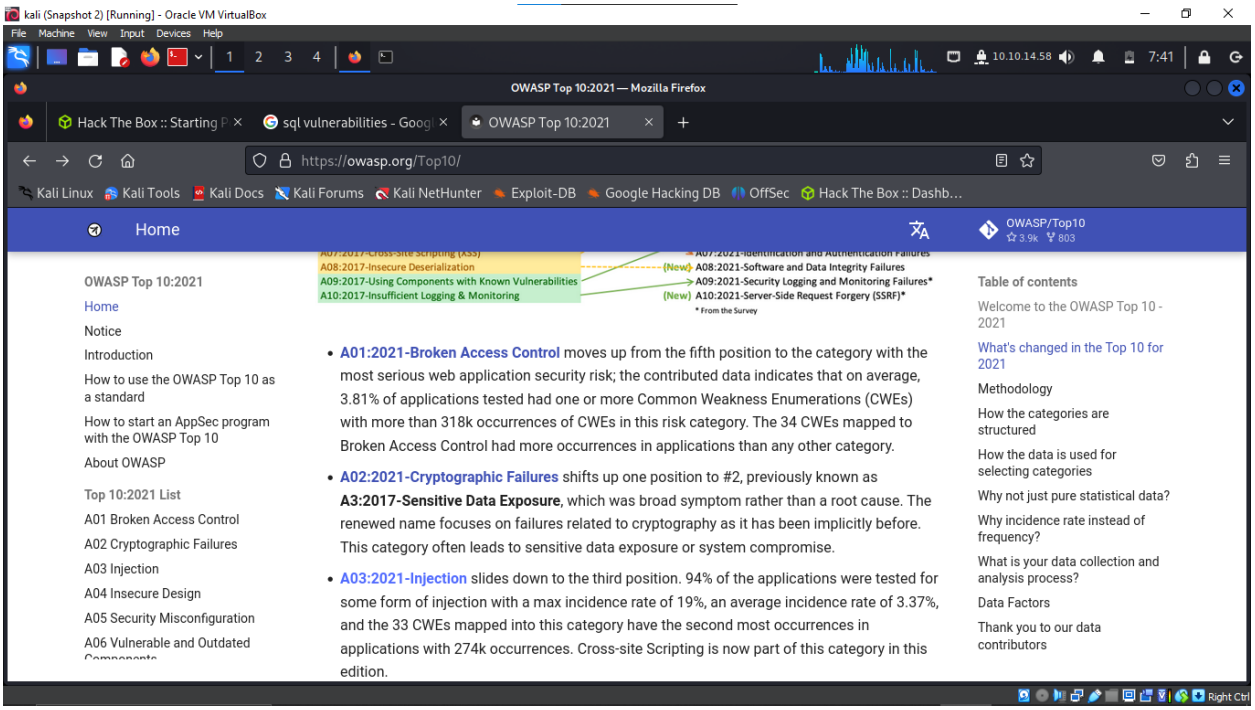
Task 2: Common SQL Vulnerability

- **Question:** Most common type of SQL vulnerability?
- **Answer:** SQL injection
- **Insight:** SQL injection remains a significant threat to web applications, allowing attackers to manipulate queries.

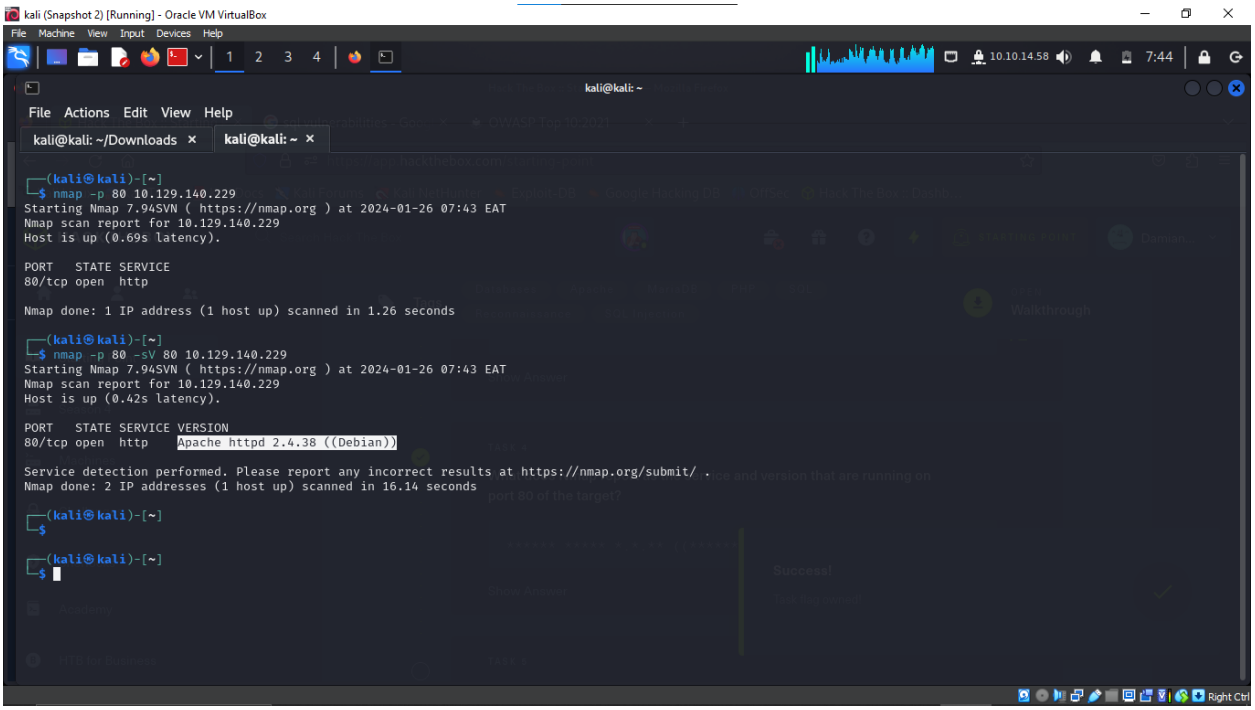
- 

Task 3: OWASP Classification

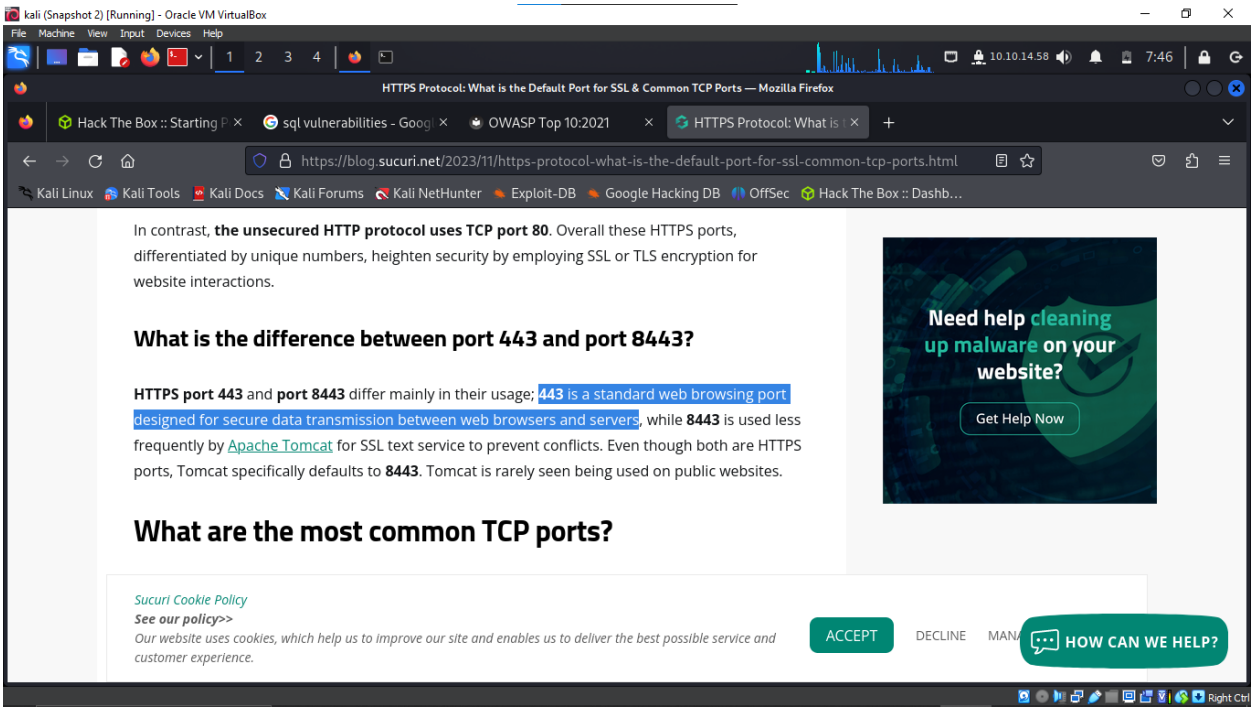
- **Question:** OWASP classification for SQL injection?
- **Answer:** A03:2021-Injection

- **Insight:** Ranked high in OWASP Top 10, indicating its prevalence and impact.
- 

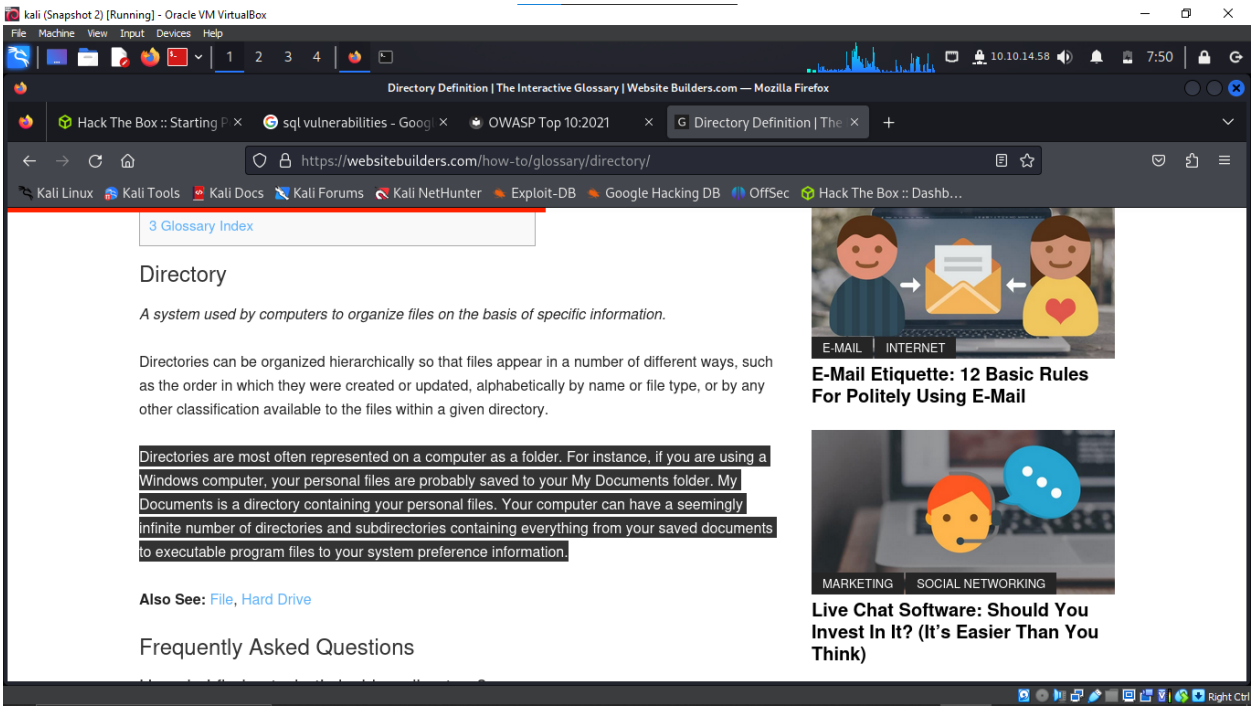
Task 4: Web Server Analysis

- **Question:** Service and version on port 80?
- **Answer:** Apache httpd 2.4.38 ((Debian))
- **Insight:** Identifying server versions is crucial for understanding potential vulnerabilities.
- 

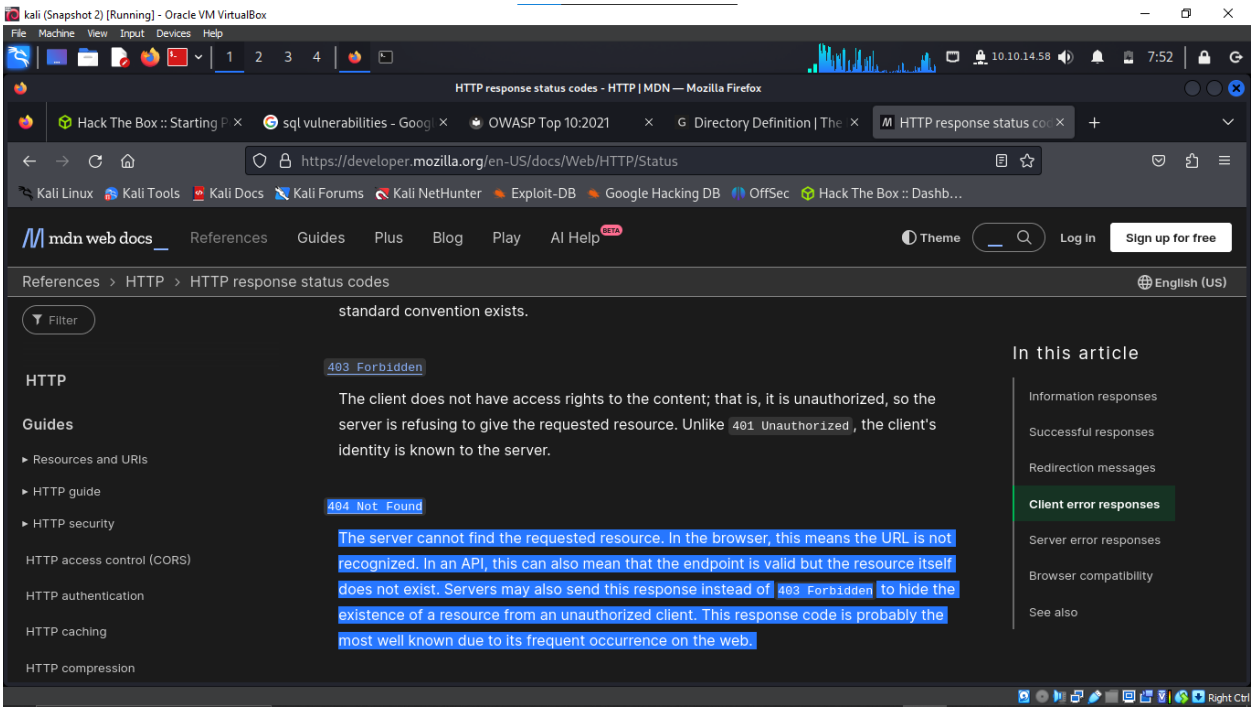
Task 5: HTTPS Protocol

- **Question:** Standard port for HTTPS?
- **Answer:** 443
- **Insight:** Secure communication via HTTPS is vital for web security.
- 

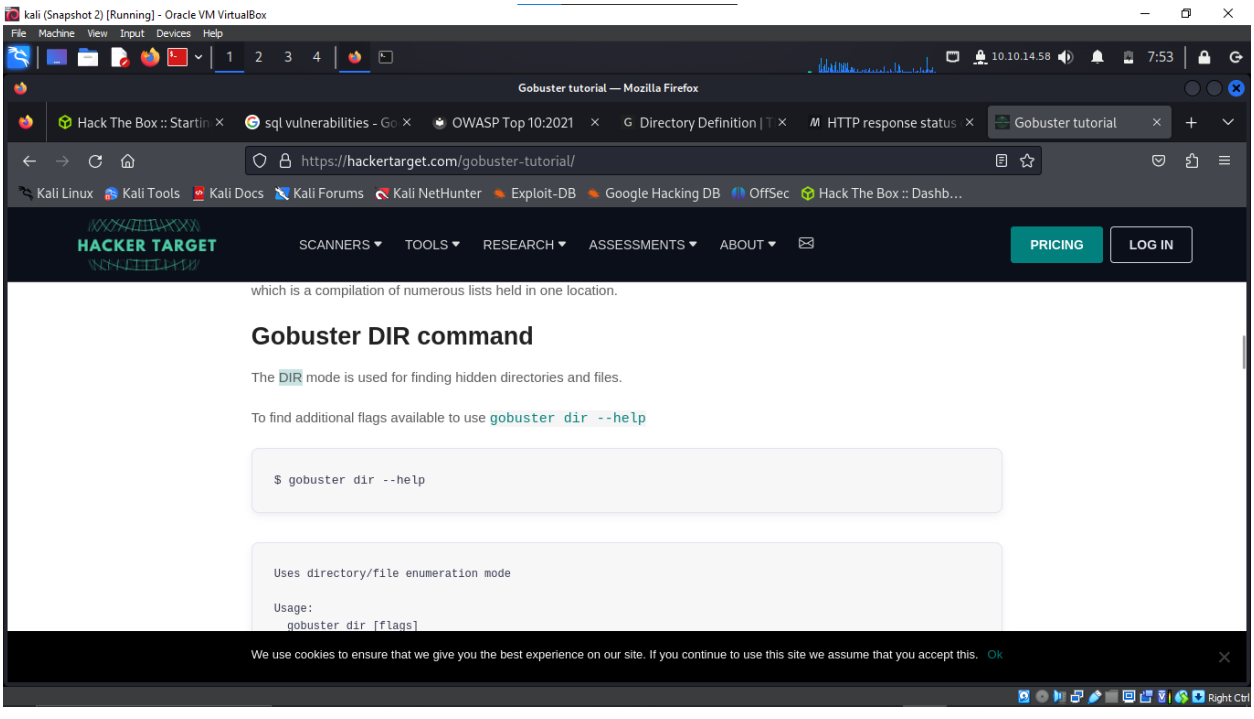
Task 6: Web Application Terminology

- **Question:** What is a folder in web-app terminology?
- **Answer:** Directory
- **Insight:** Directories structure the content and paths in web applications.
- 

Task 7: HTTP Response Codes

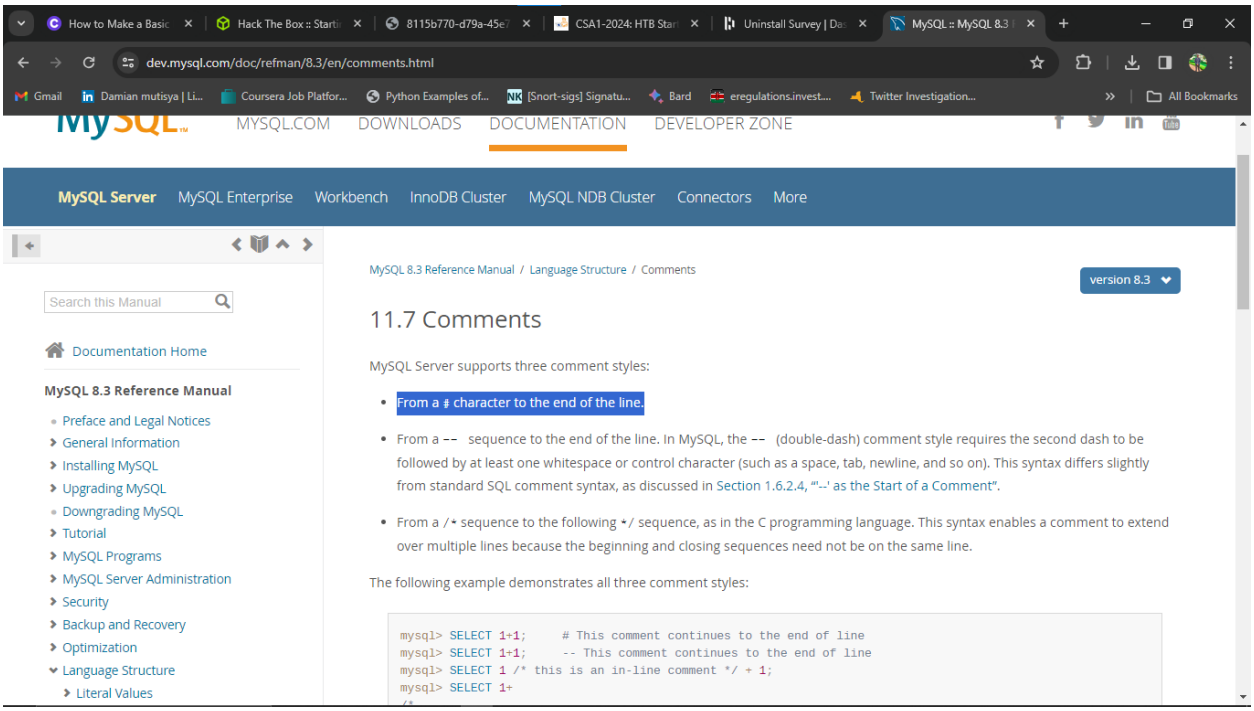
- **Question:** 'Not Found' error code?
- **Answer:** 404
- **Insight:** HTTP status codes provide insights into web server responses.
- 

Task 8: Brute Forcing Directories

- **Question:** Gobuster switch for directories?
- **Answer:** dir
- **Insight:** Tools like Gobuster are essential for uncovering hidden paths in web apps.
- 

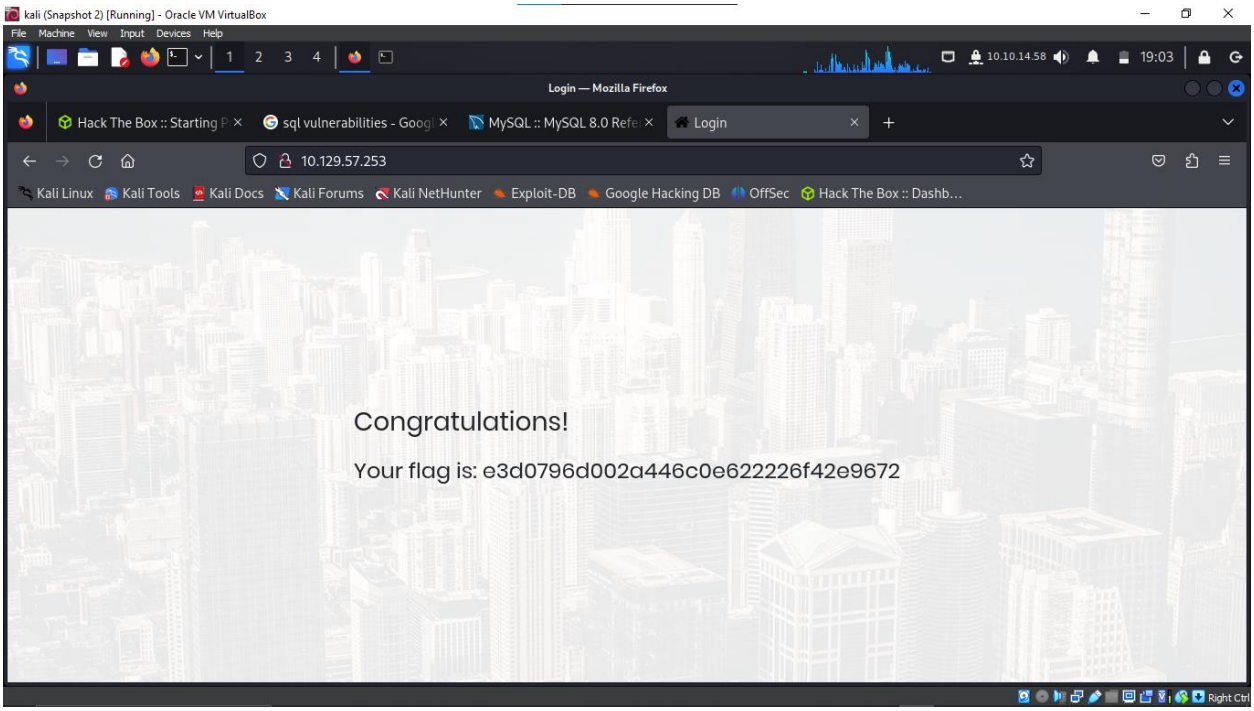
Task 9: MySQL Comments

- **Question:** Character for commenting in MySQL?
- **Answer:** #
- **Insight:** Understanding SQL syntax, including comments, is key in identifying injection points.



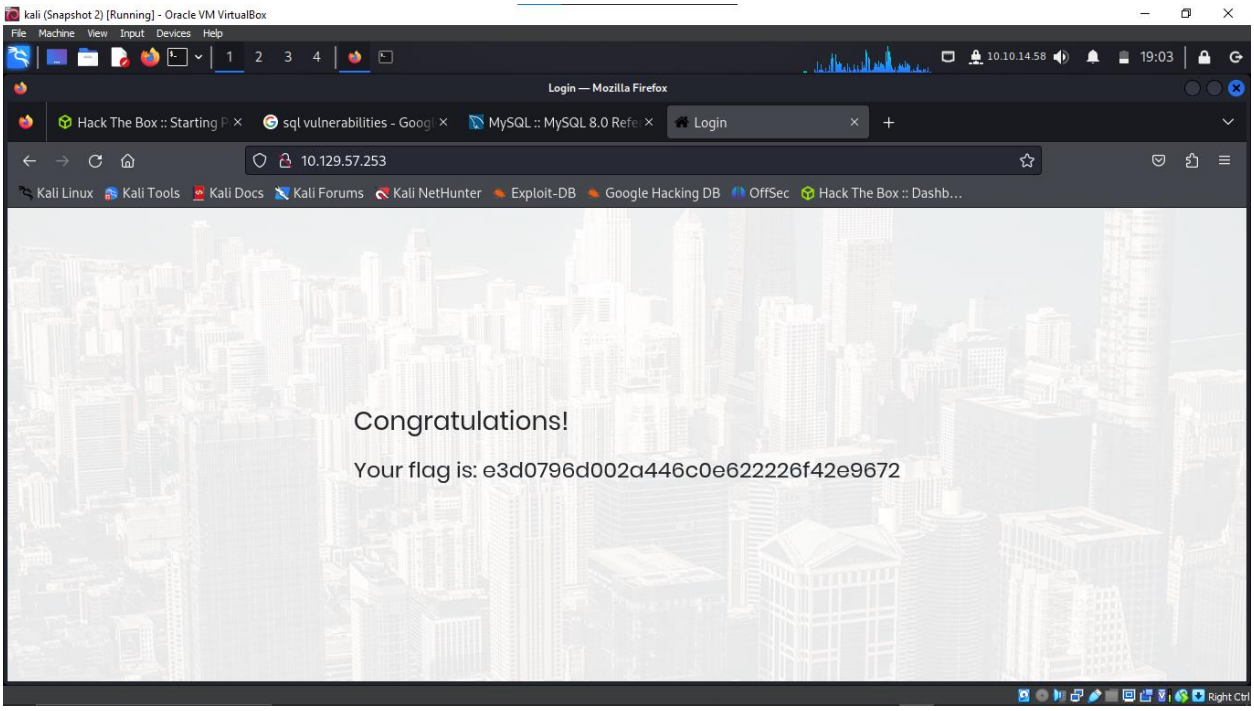
Task 10: SQL Injection Exploit

- **Question:** First word on the webpage after SQL injection?
- **Answer:** Congratulations
- **Insight:** Demonstrates how SQL injection can lead to unauthorized access.



Submit Root Flag

- **Flag:** e3d0796d002a446c0e622226f42e9672
- **Insight:** Successful exploitation and completion of the lab objectives.



Conclusion

The "Appointment" lab is an insightful journey into the world of web application security, highlighting the critical need for robust measures against SQL injection and the importance of secure web server configurations.

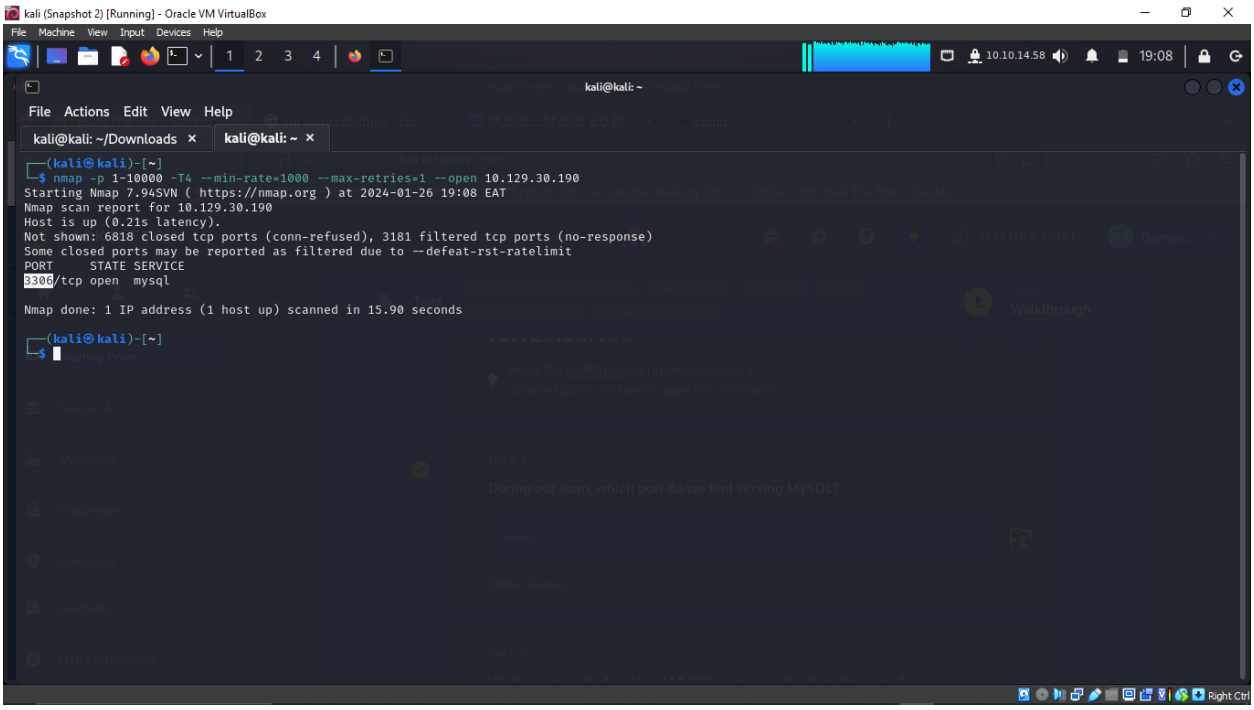
SEQUEL

Introduction

The "Sequel" lab in Hack The Box offers an in-depth exploration of MySQL databases, specifically MariaDB, a popular community-developed version of MySQL. This lab emphasizes database enumeration, login techniques, and data retrieval.

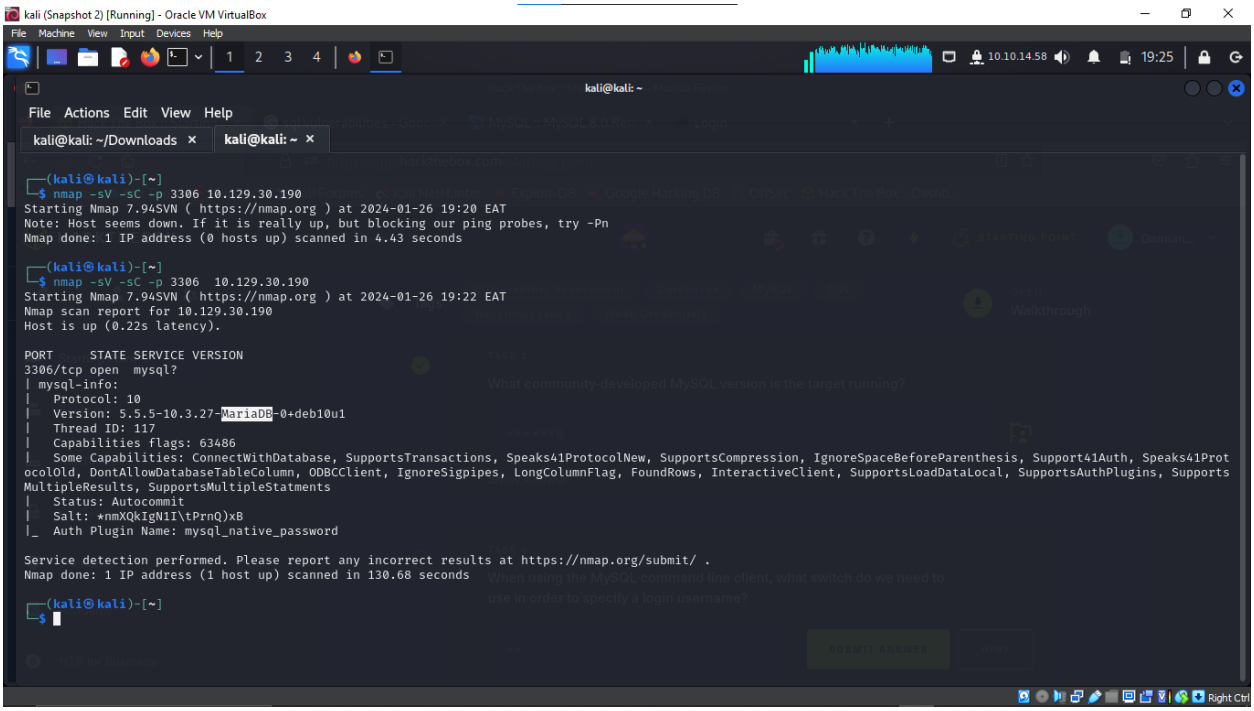
Tasks and Findings

Task 1: Identifying MySQL Port

- **Question:** Port serving MySQL?
- **Answer:** 3306
- **Details:** Port 3306 is the default for MySQL services, critical for database communication.
- 

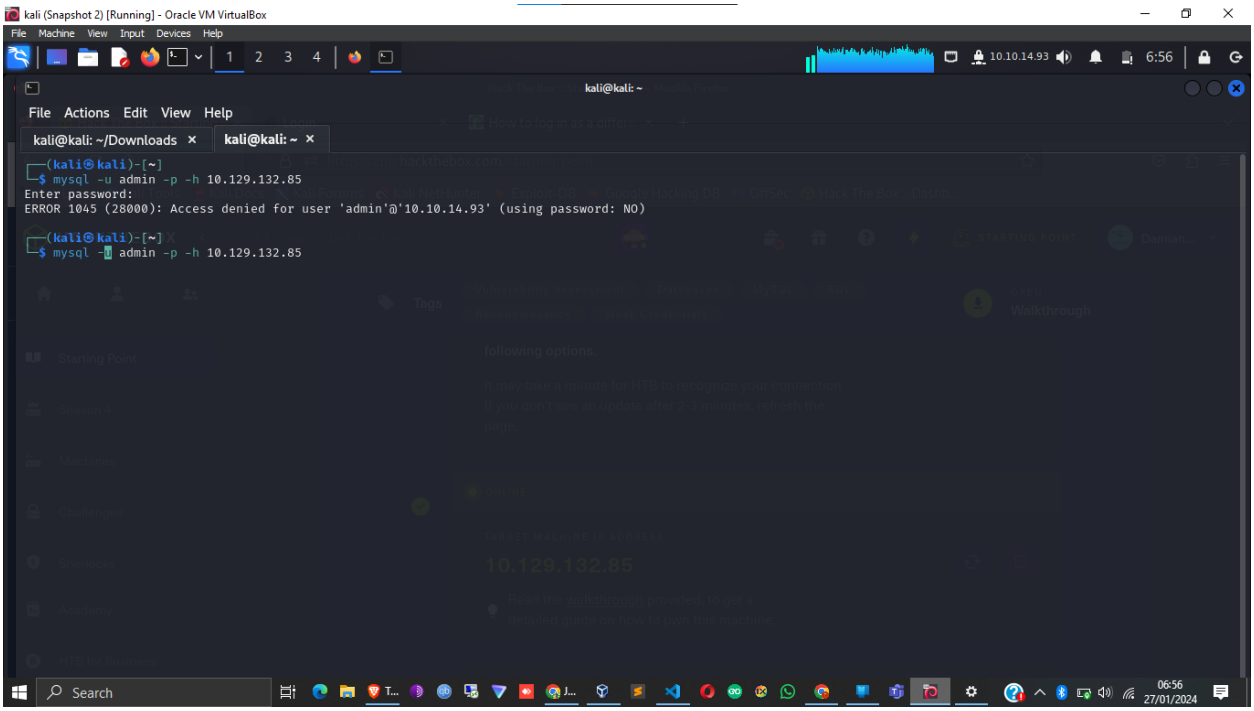
Task 2: MySQL Version

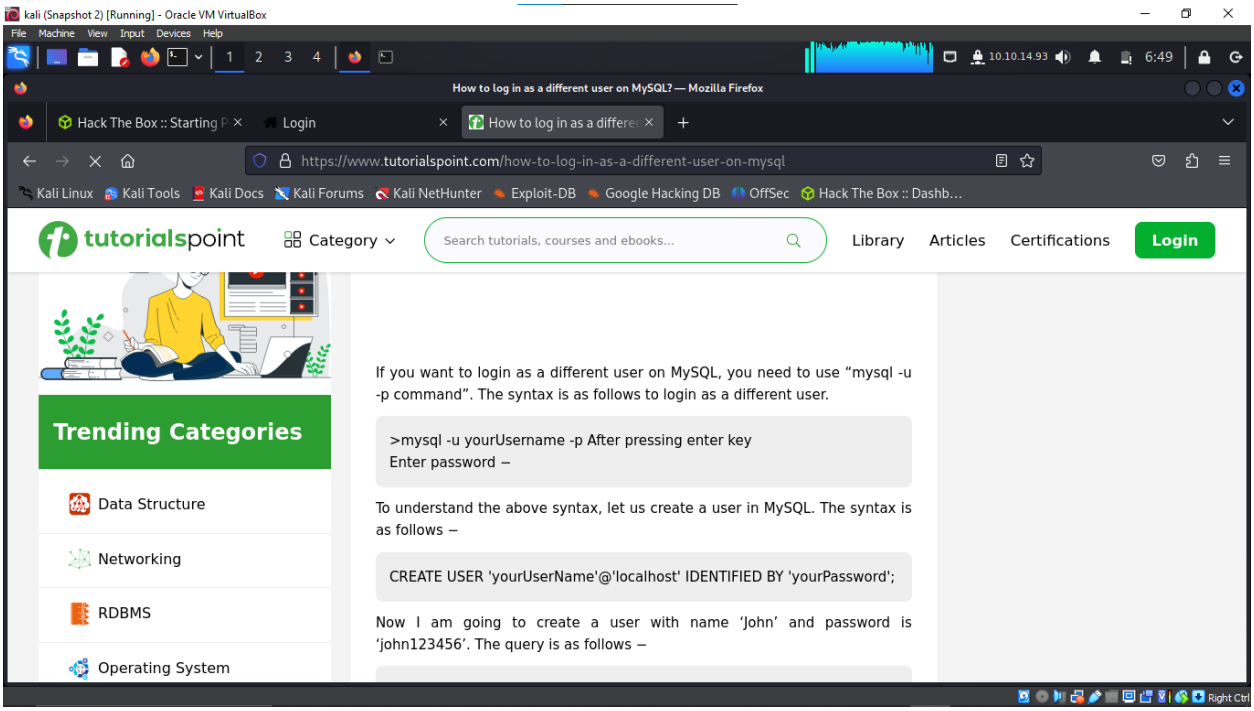
- **Question:** MySQL version running on the target?
- **Answer:** MariaDB
- **Details:** MariaDB is a community-developed fork of the MySQL relational database management system.

- 

Task 3: MySQL Login

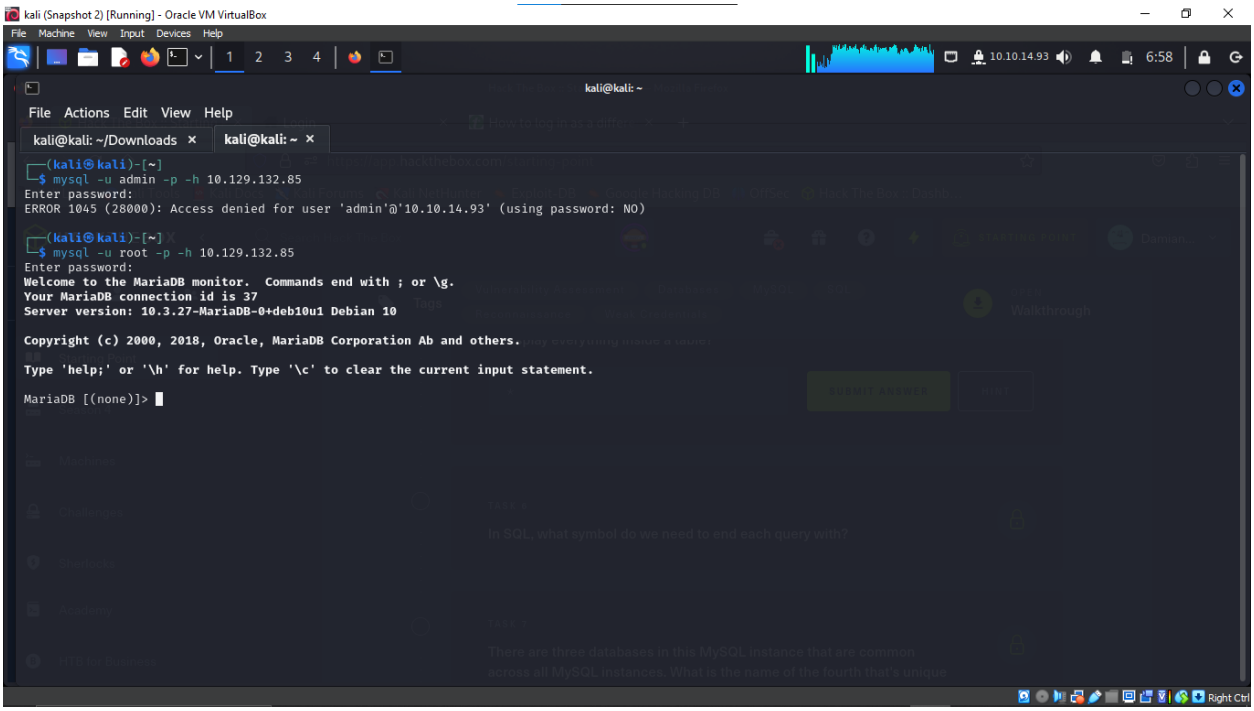
- **Question:** Switch for login username in MySQL client?
- **Answer:** -u
- **Details:** The **-u** switch is used to specify the username when logging into MySQL.

- 

- 

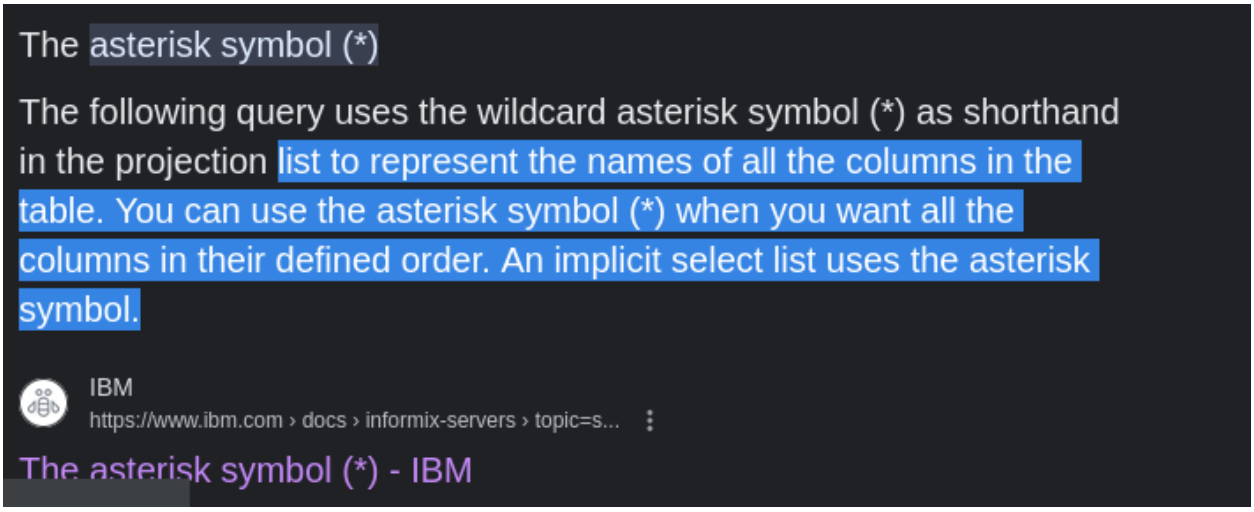
Task 4: Username for MariaDB Login

- **Question:** Username for MariaDB login without a password?
- **Answer:** root
- **Details:** The 'root' username allows access without a password, indicating a potential security risk.

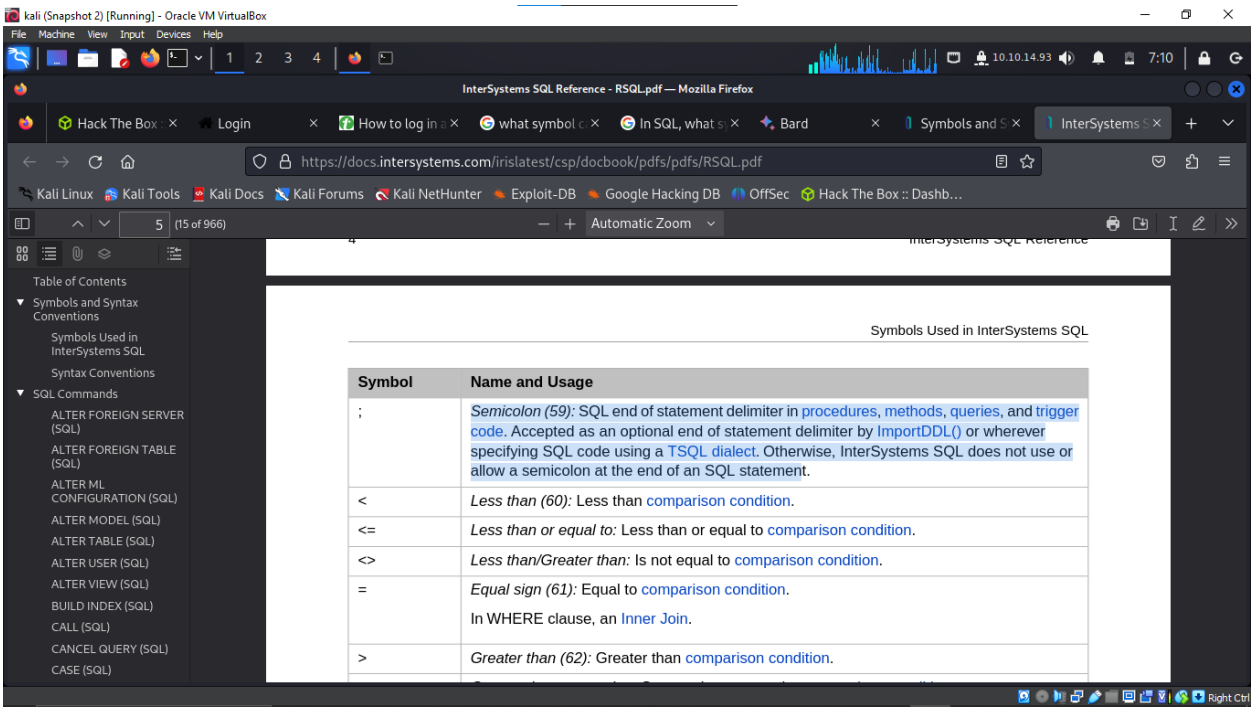
- 

Task 5: SQL Query Symbol

- **Question:** Symbol to display everything in a table?
- **Answer:** *

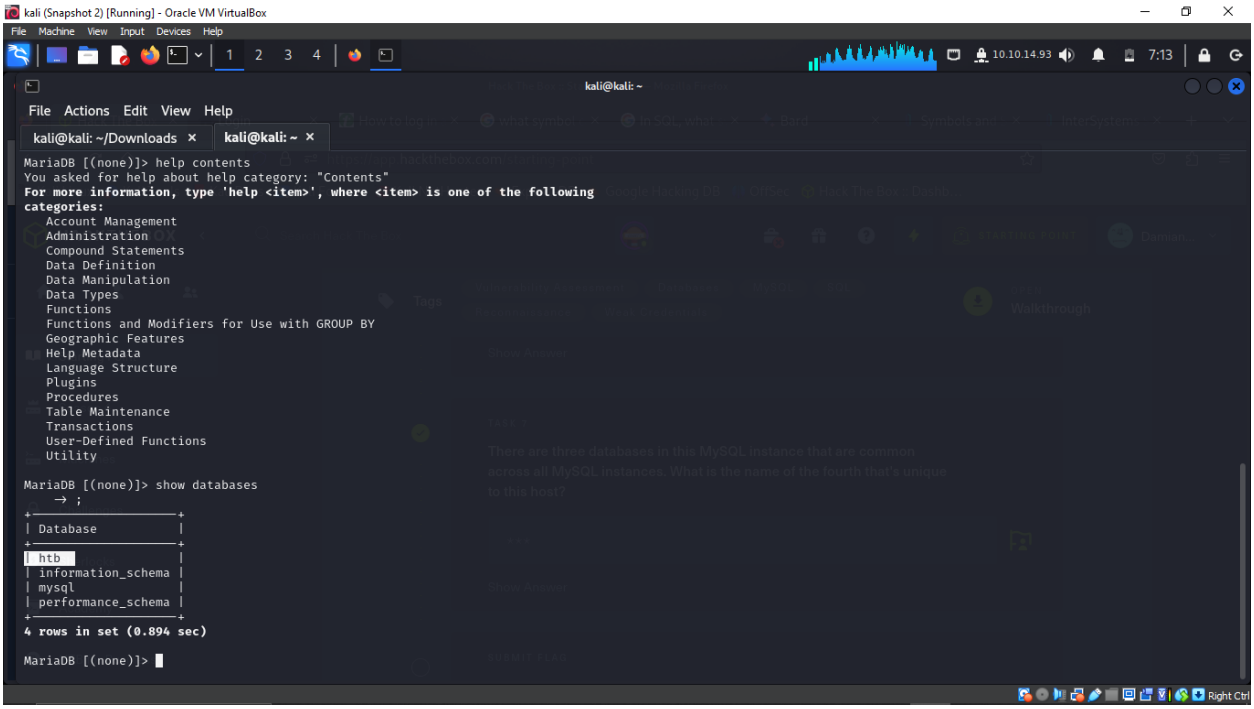
- **Details:** The asterisk (*) is used in SQL to select all records from a table.
- 

Task 6: SQL Query Termination

- **Question:** Symbol to end an SQL query?
- **Answer:** ;
- **Details:** Each SQL query is terminated with a semicolon (;).
- 

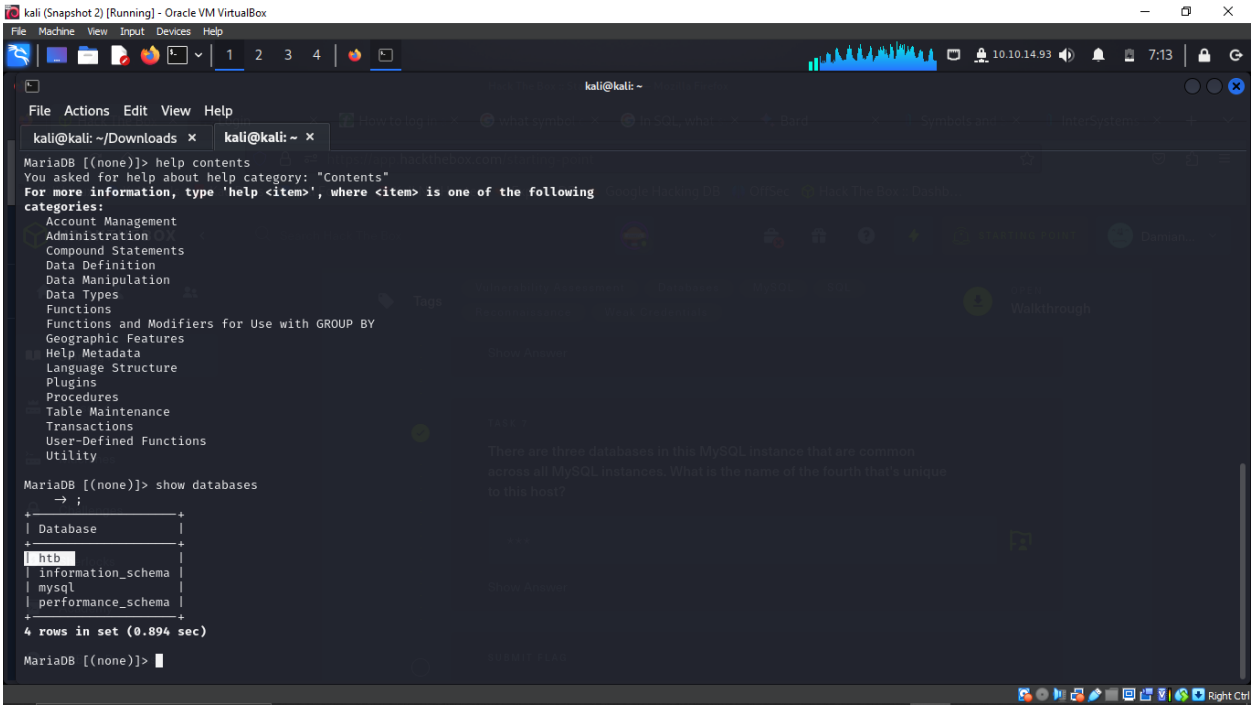
Task 7: Unique Database Name

- **Question:** Name of the unique database in this MySQL instance?
- **Answer:** htb
- **Details:** The 'htb' database is unique to this host, distinguishing it from standard MySQL installations.

- 

Submit Root Flag

- **Flag:** 7b4bec00d1a39e3dd4e021ec3d915da8
- **Details:** Successfully retrieved the root flag, indicating successful data retrieval and control over the MySQL instance.

- 

Conclusion

The "Sequel" lab provided valuable insights into MySQL/MariaDB database management, emphasizing the importance of secure configurations and thorough enumeration techniques. Understanding and interacting with databases is crucial in modern cybersecurity practices.

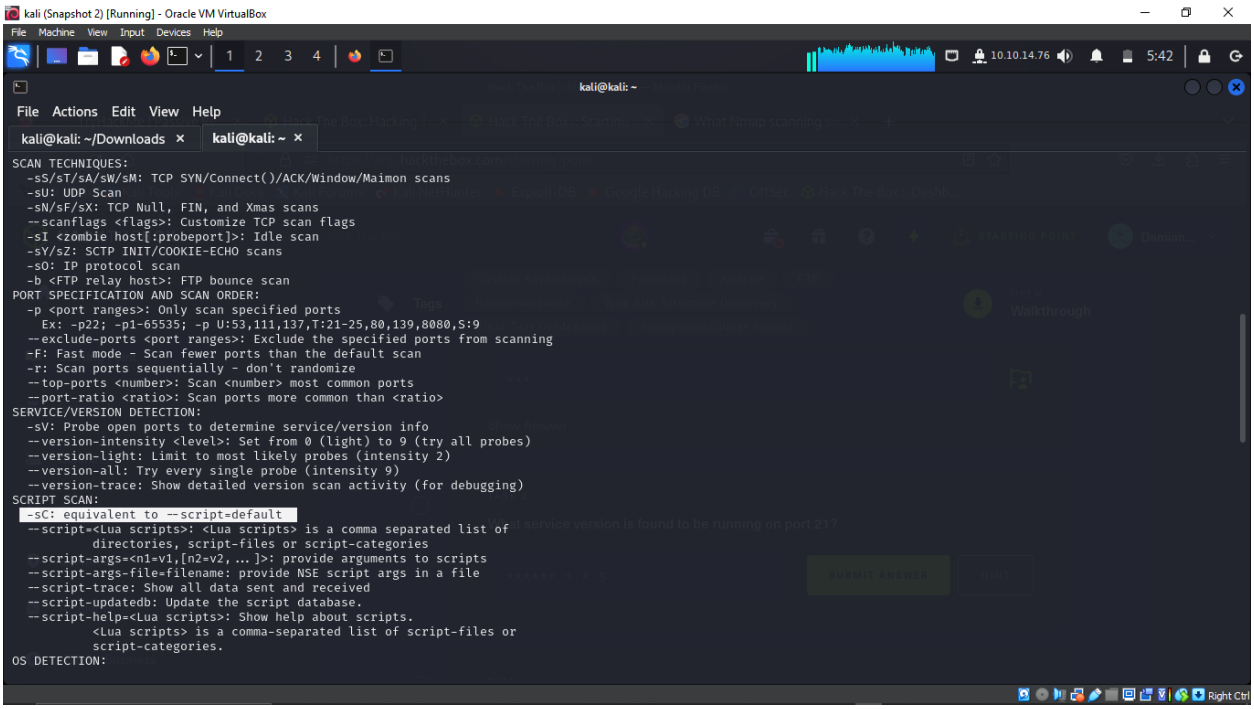
CROCODILE

Introduction

The "Crocodile" lab focuses on network and web application security, particularly involving FTP (File Transfer Protocol) and HTTP services. Key areas include exploiting misconfigurations in these services and understanding their operation and vulnerabilities.

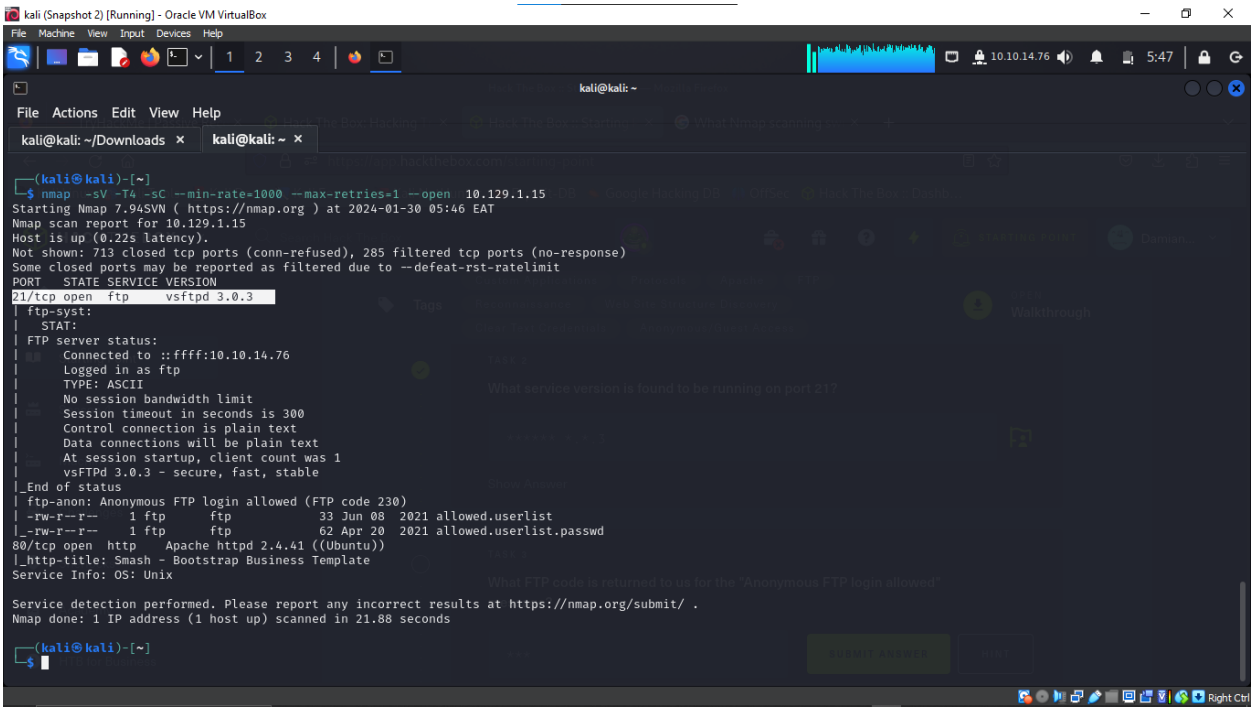
Tasks and Findings

Task 1: Nmap Script Scanning

- **Question:** Nmap scanning switch for default scripts?
- **Answer:** -sC
- **Details:** This switch is essential for automated script scanning, providing deeper insights into detected services.
- 

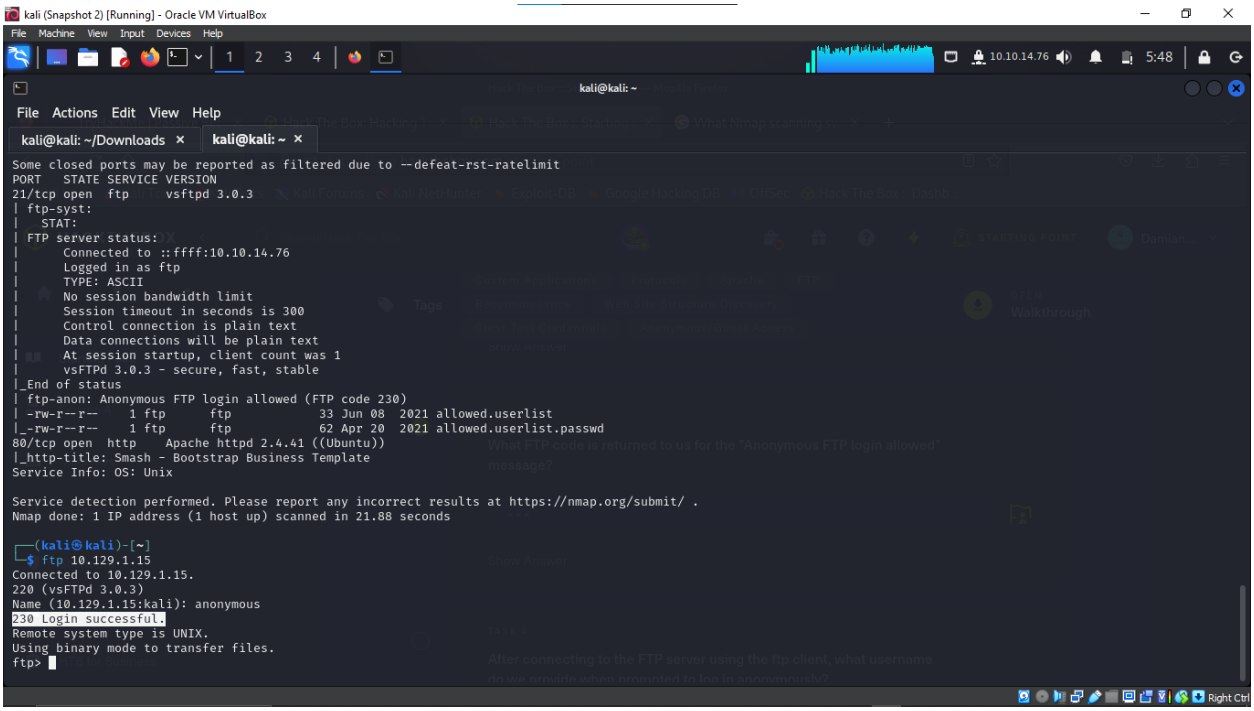
Task 2: FTP Service Version

- **Question:** Service version on port 21?
- **Answer:** vsftpd 3.0.3
- **Details:** Identifying service versions like vsftpd 3.0.3 is crucial for pinpointing potential vulnerabilities.

- 

Task 3: FTP Anonymous Login Code

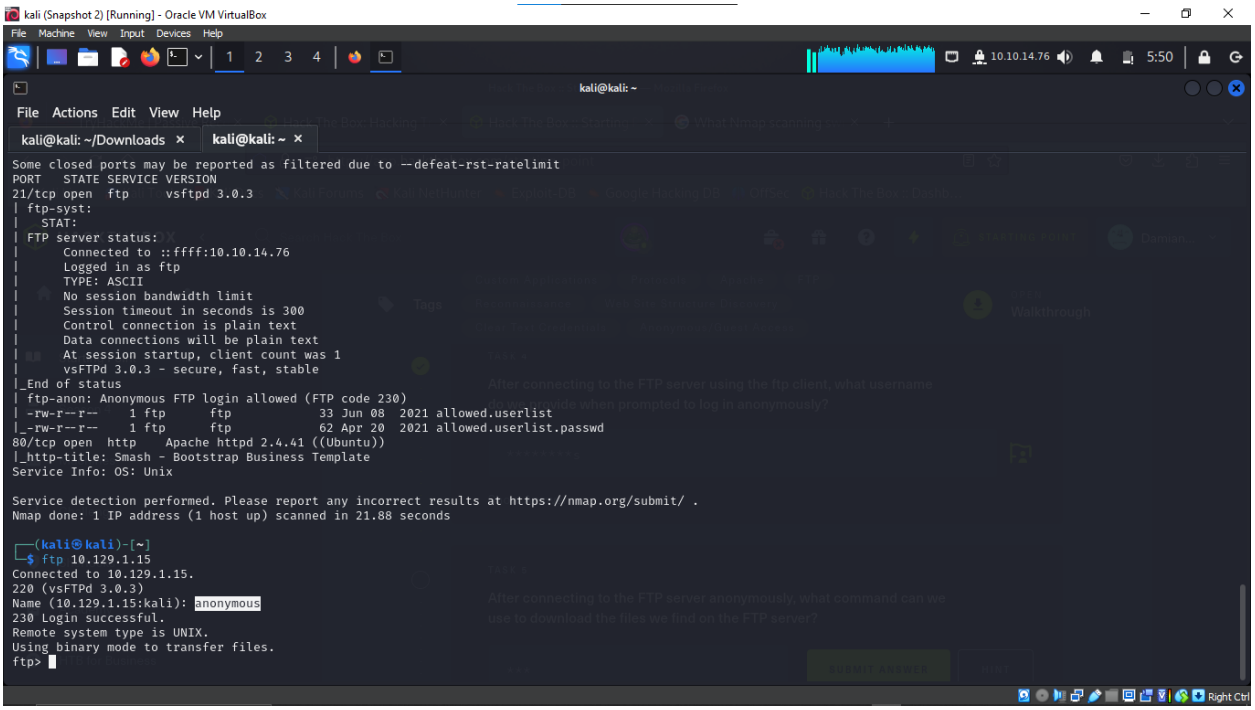
- **Question:** FTP code for "Anonymous FTP login allowed"?
- **Answer:** 230
- **Details:** This indicates that the FTP server permits anonymous logins, a potential security risk.

- 

Task 4: FTP Anonymous Login Username

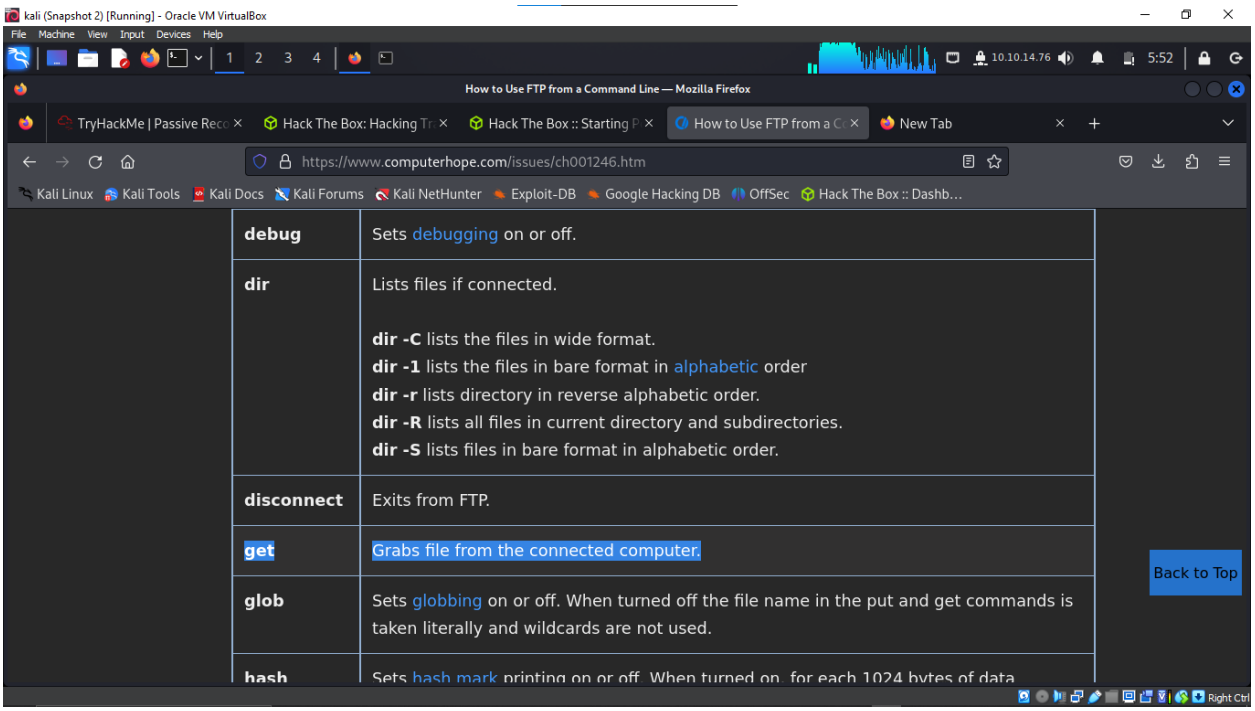
- **Question:** Username for anonymous FTP login?
- **Answer:** anonymous

- **Details:** 'anonymous' is a default username for accessing FTP servers without specific credentials.

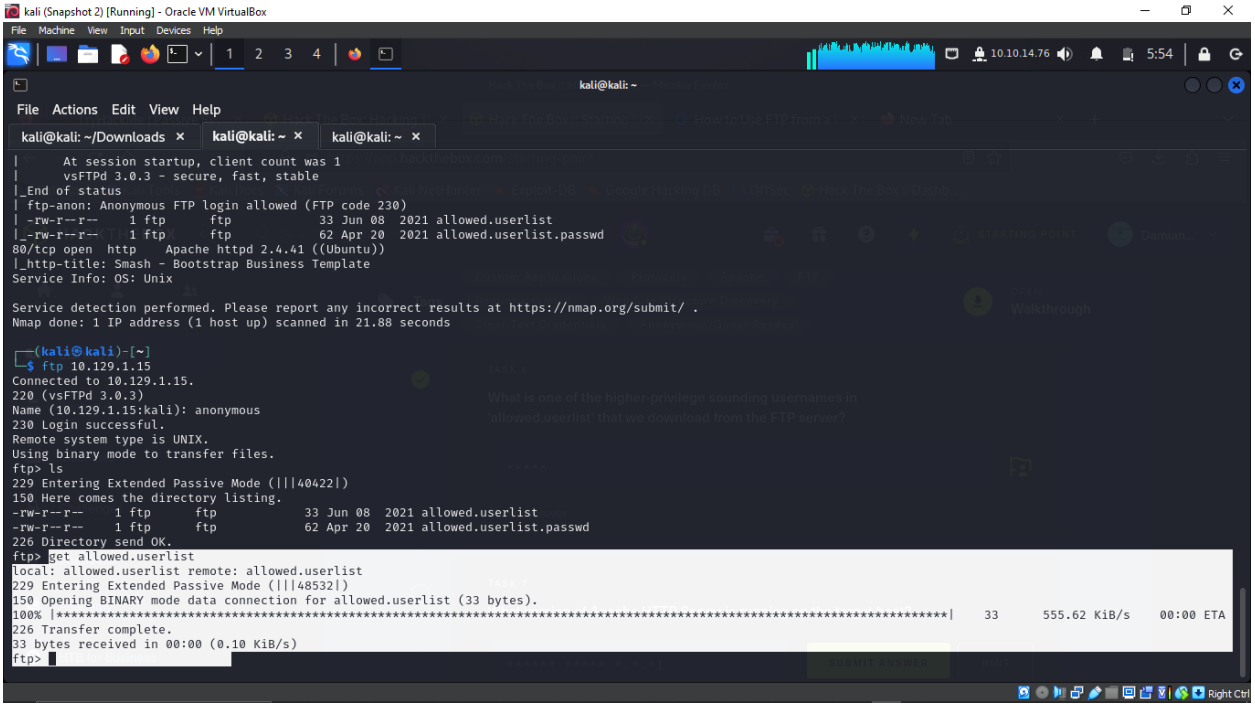


Task 5: FTP File Download Command

- **Question:** Command to download files on FTP server?
- **Answer:** get
- **Details:** 'get' is used for downloading files from FTP servers, crucial for data exfiltration.

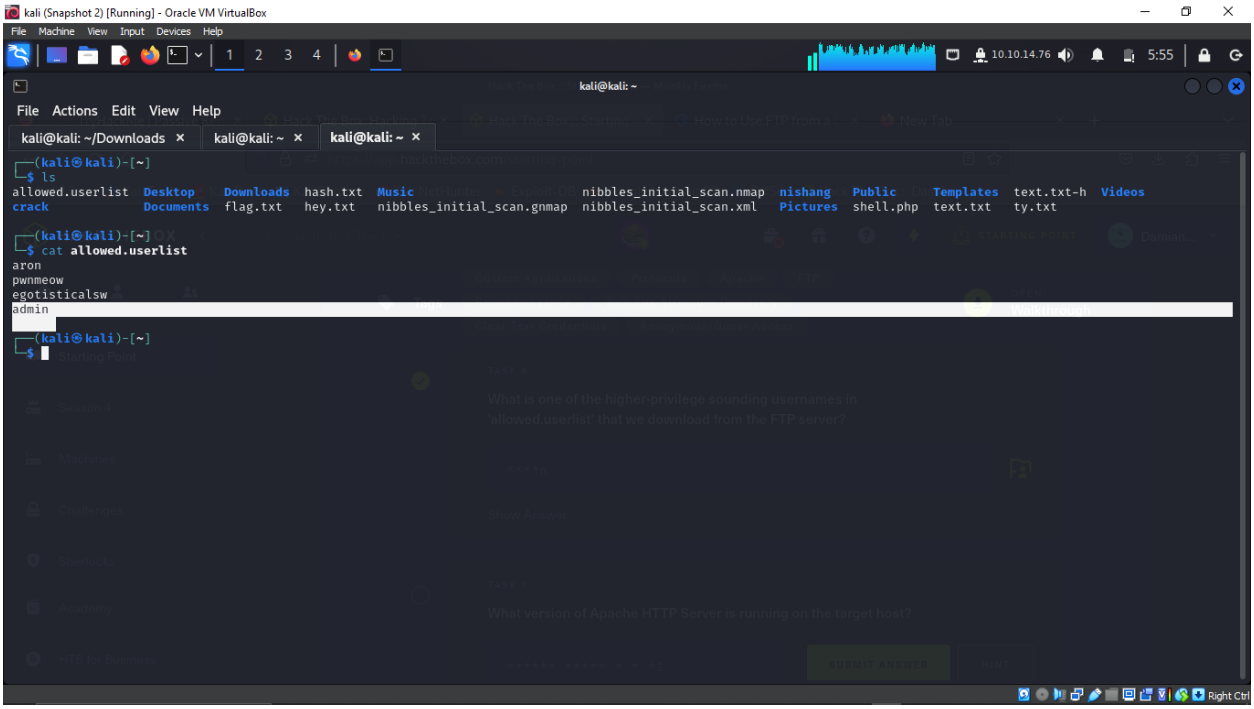


Task 6: Privileged Username in Userlist

- **Question:** Higher-privilege username in 'allowed.userlist'?
- **Answer:** admin
- **Details:** Identifying usernames like 'admin' can lead to potential privilege escalation opportunities.
- 

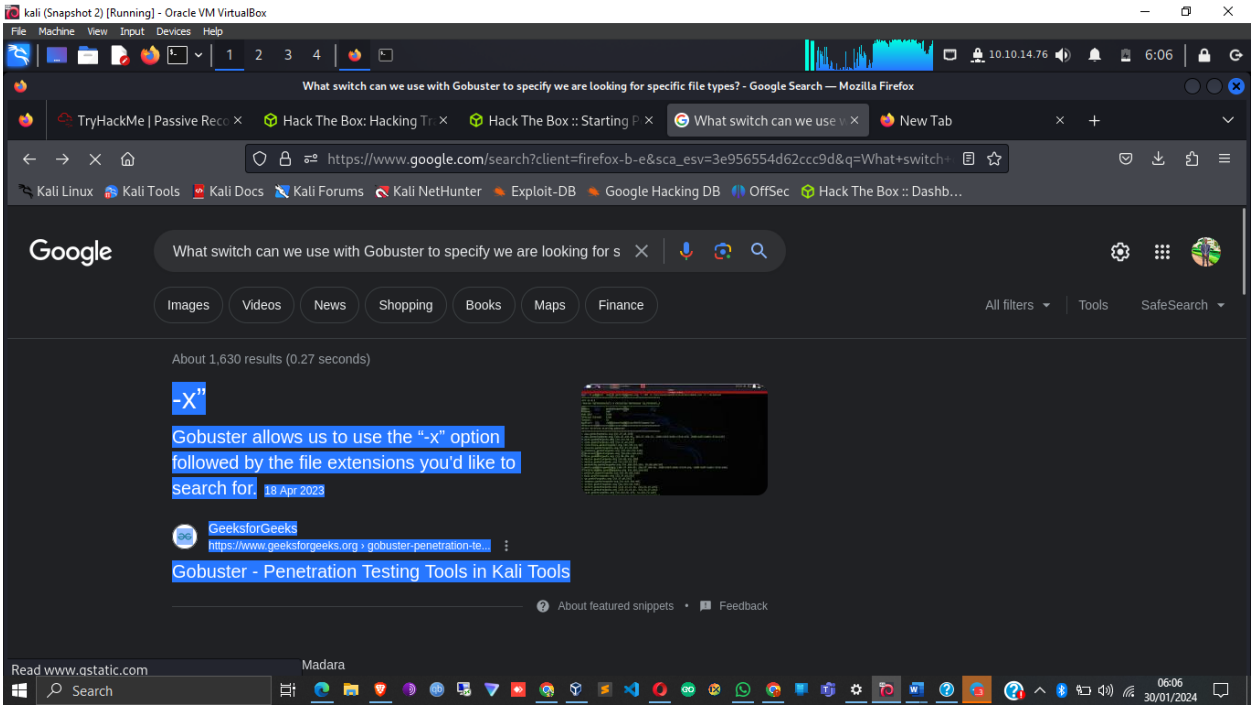
Task 7: Apache HTTP Server Version

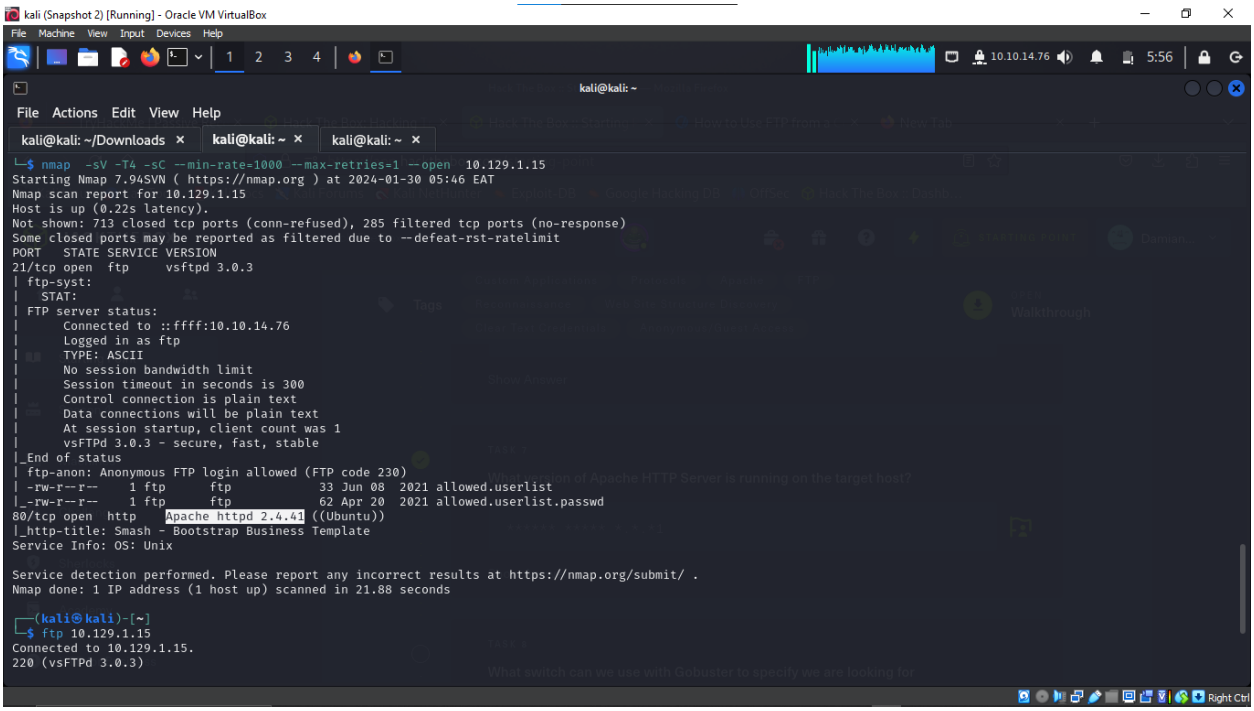
- **Question:** Apache HTTP Server version?
- **Answer:** Apache httpd 2.4.41
- **Details:** Knowing exact versions like Apache httpd 2.4.41 helps in targeting specific vulnerabilities.

- 

Task 8: Gobuster Filetype Search

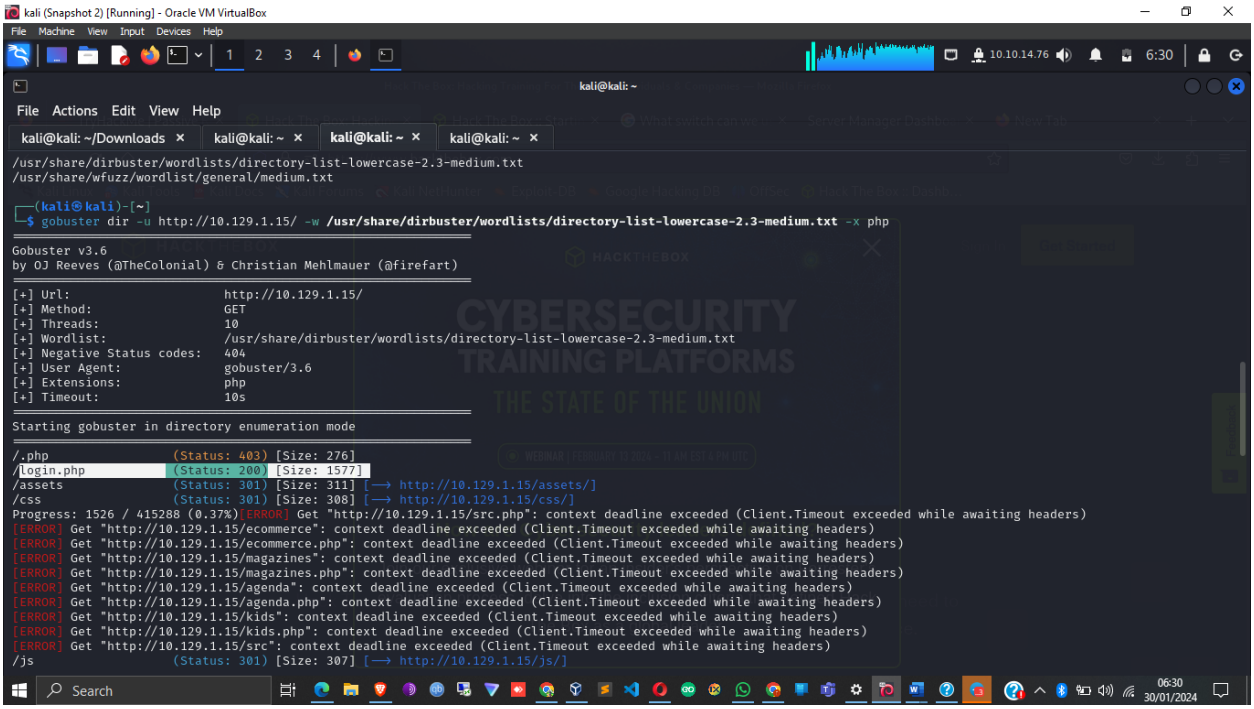
- **Question:** Gobuster switch for filetypes?
- **Answer:** -x
- **Details:** The -x switch in Gobuster is used for specifying file extensions, aiding in targeted directory brute-forcing.

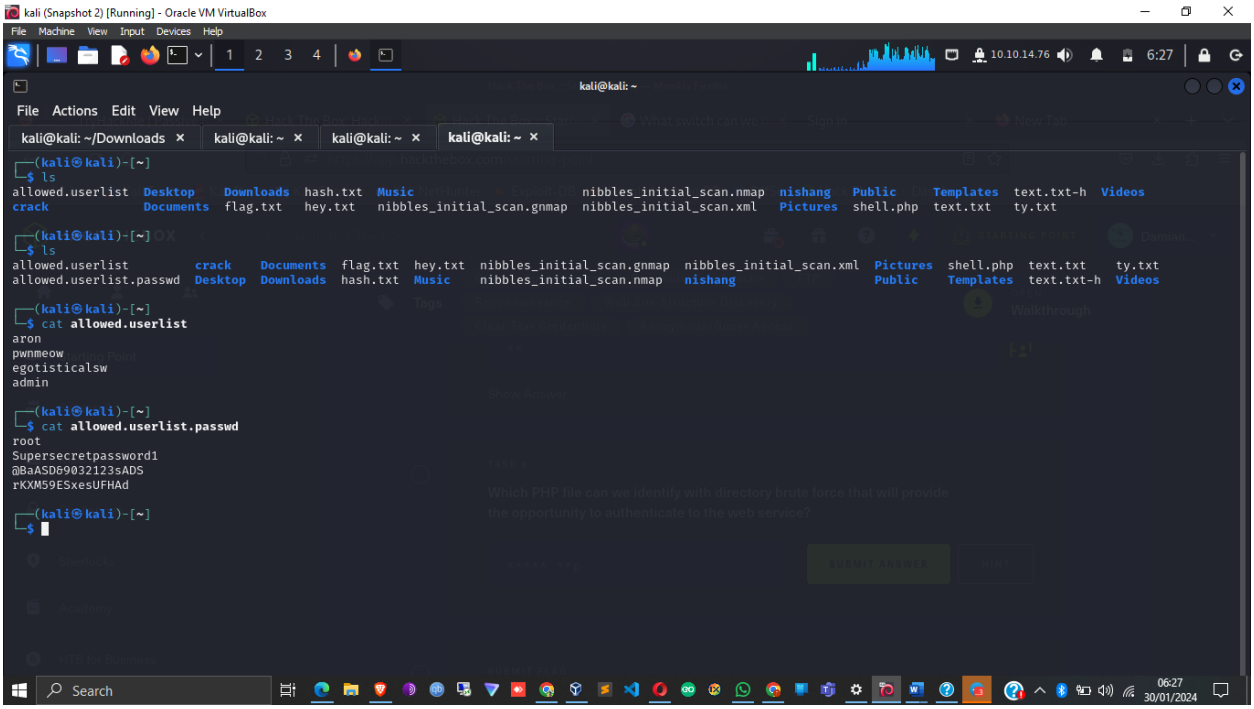
- 

- 

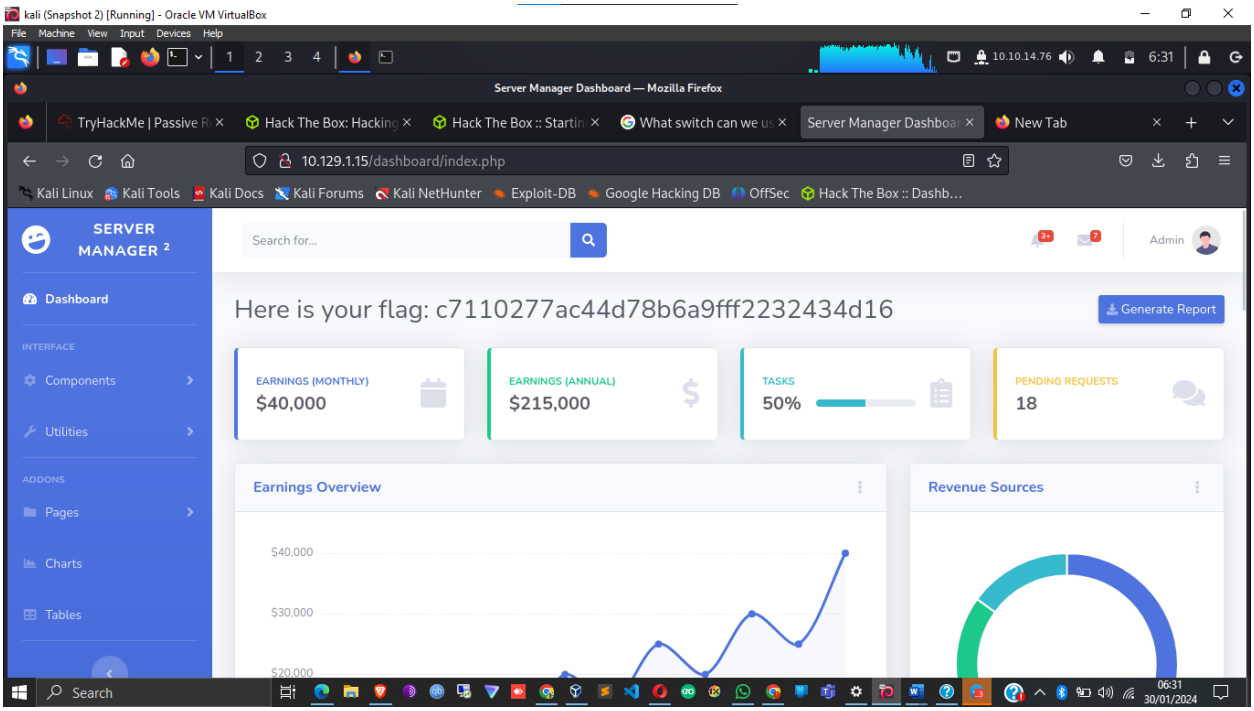
Task 9: PHP File Identification

- **Question:** PHP file identified for web service authentication?
- **Answer:** login.php
- **Details:** Discovering files like 'login.php' can lead to authentication bypasses and further exploitation.

- 

- 

Submit Root Flag

- **Flag:** c7110277ac44d78b6a9fff2232434d16
- **Details:** Successfully retrieved the root flag, demonstrating effective exploitation of the target services.
- 

Conclusion

The "Crocodile" lab provides an insightful journey into exploiting common network services like FTP and HTTP. It underscores the importance of

understanding service configurations, employing effective scanning techniques, and exploiting service vulnerabilities for successful penetration testing.

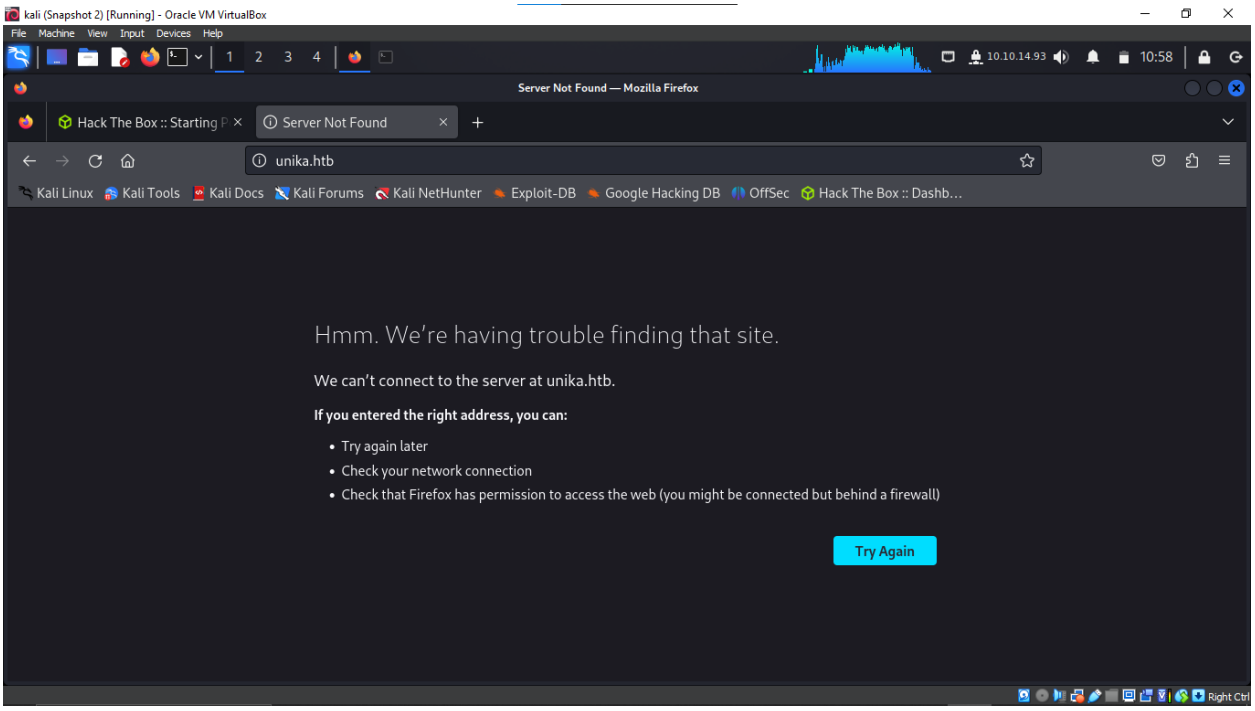
RESPONDER

Introduction

The "Responder" lab is an extensive exercise focusing on exploiting file inclusion vulnerabilities and leveraging the Windows Remote Management (WinRM) service. The lab demonstrates how vulnerabilities in web applications can lead to deeper network intrusions.

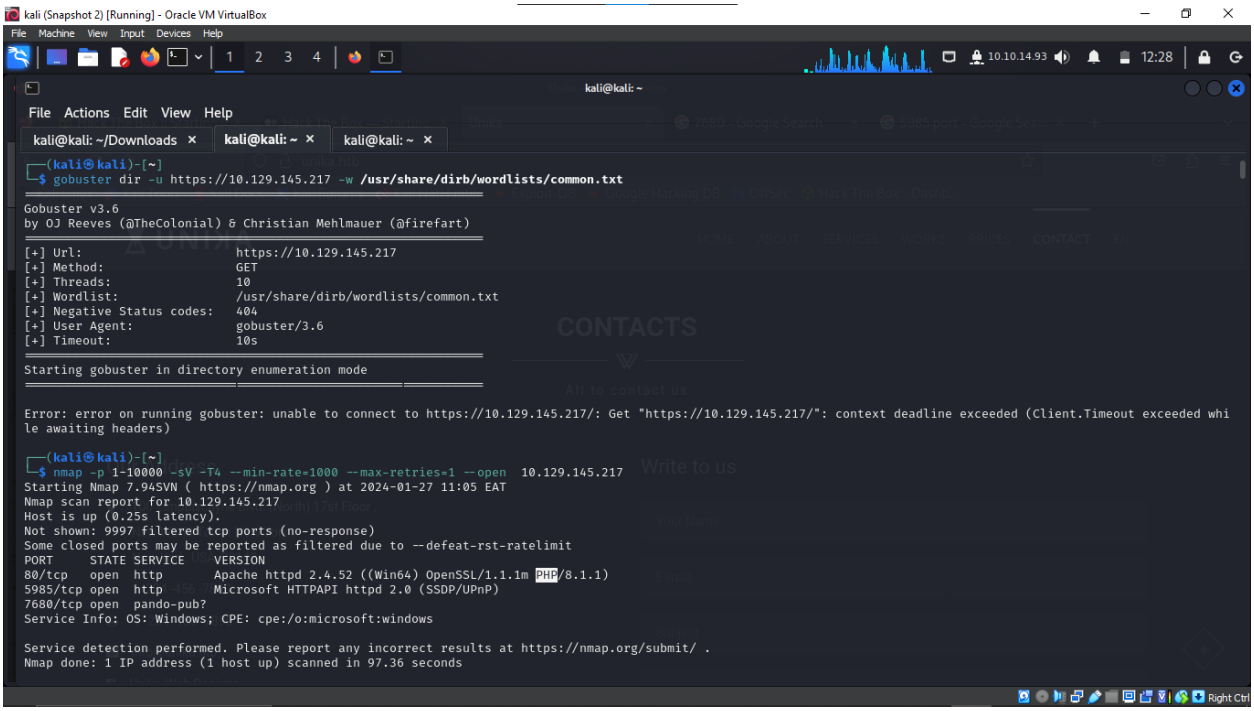
Tasks and Findings

Task 1: Web Service Redirection

- **Question:** Domain redirected to when visiting the web service?
- **Answer:** unika.htb
- **Details:** The redirection to a specific domain is crucial for understanding the webserver's configuration.
- 

Task 2: Server Scripting Language

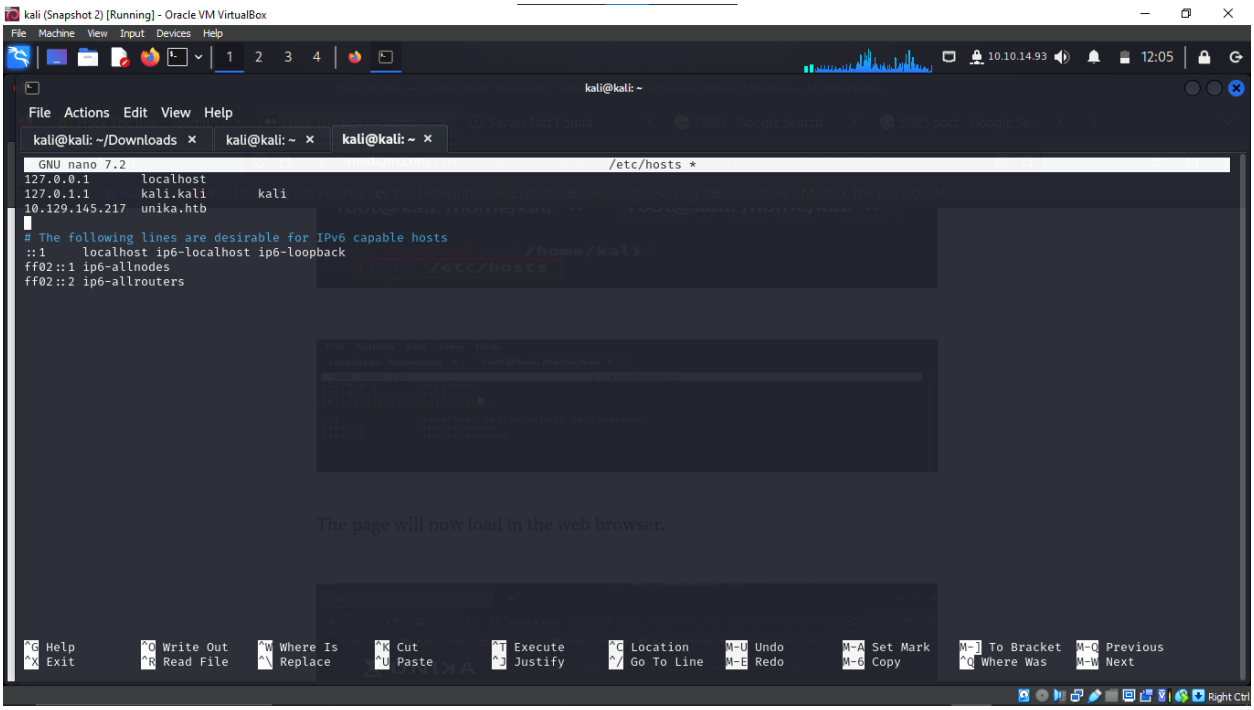
- **Question:** Scripting language used on the server?
- **Answer:** PHP
- **Details:** Identifying PHP usage is essential for assessing potential vulnerabilities.

- 

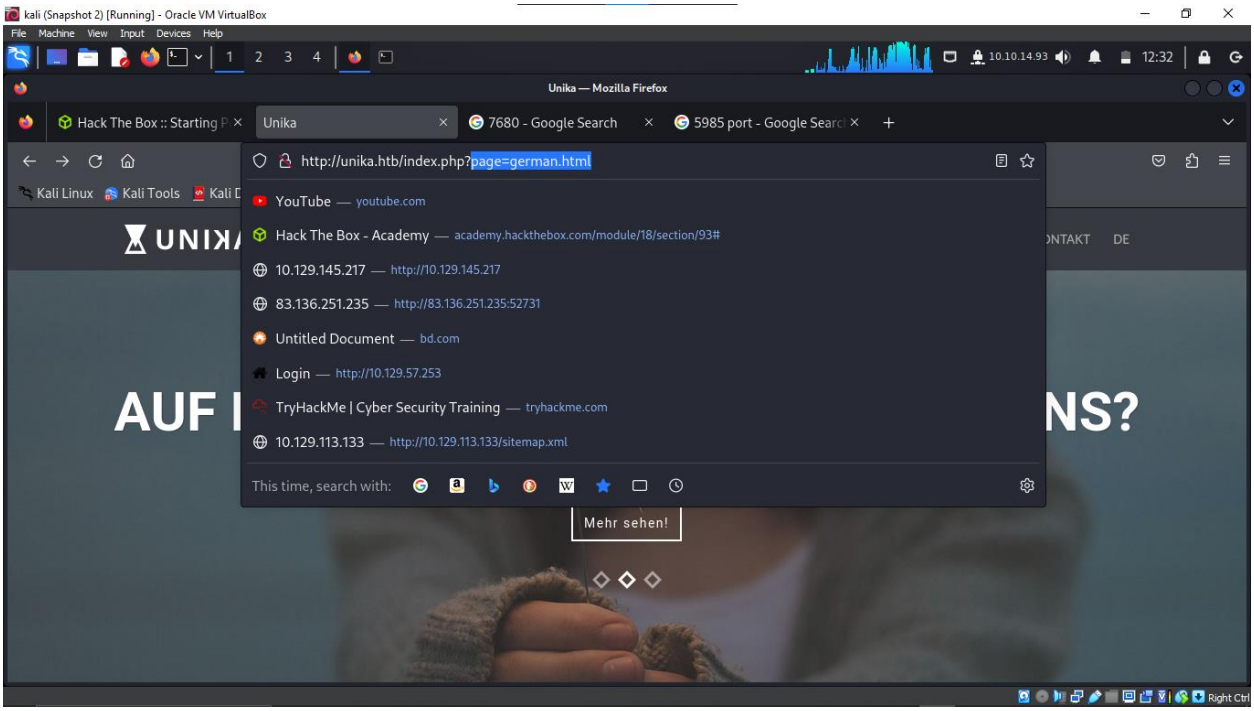
-

Task 3: Webpage Language Selection

- **Question:** URL parameter for different language versions?
- **Answer:** page
- **Details:** The 'page' parameter is a potential vector for file inclusion attacks.

- 

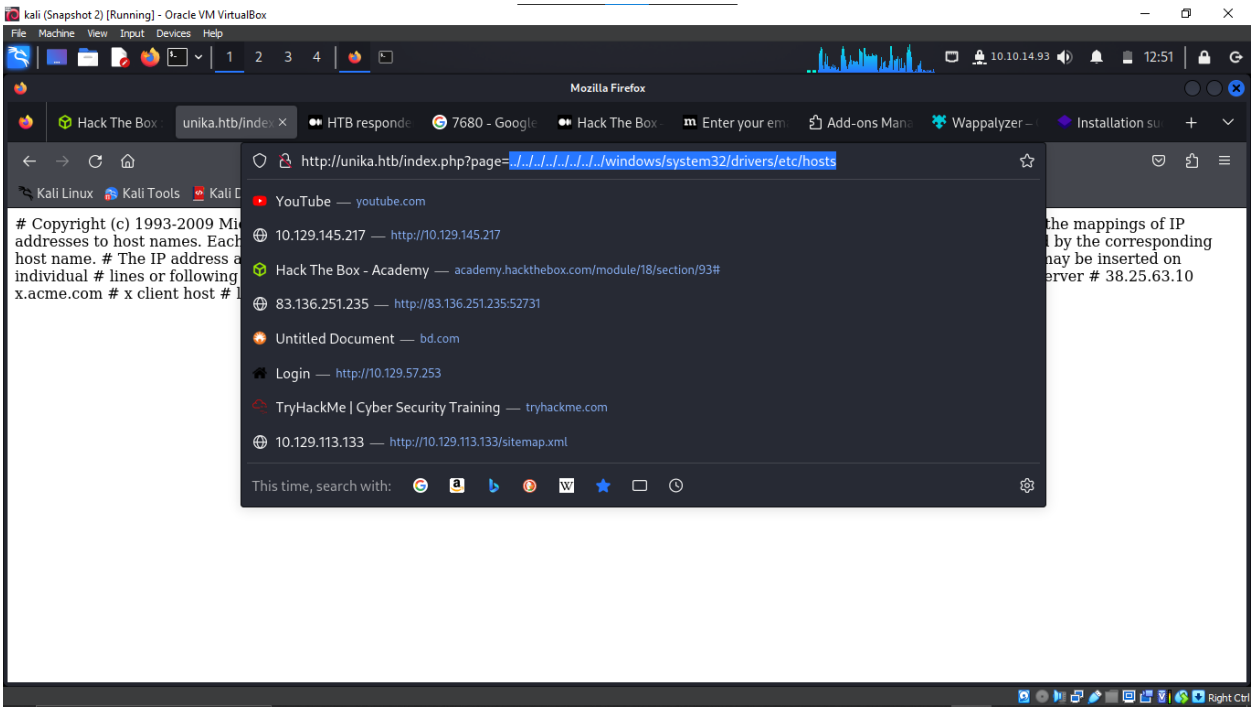
-

- 

-

Task 4: Local File Inclusion (LFI) Exploit

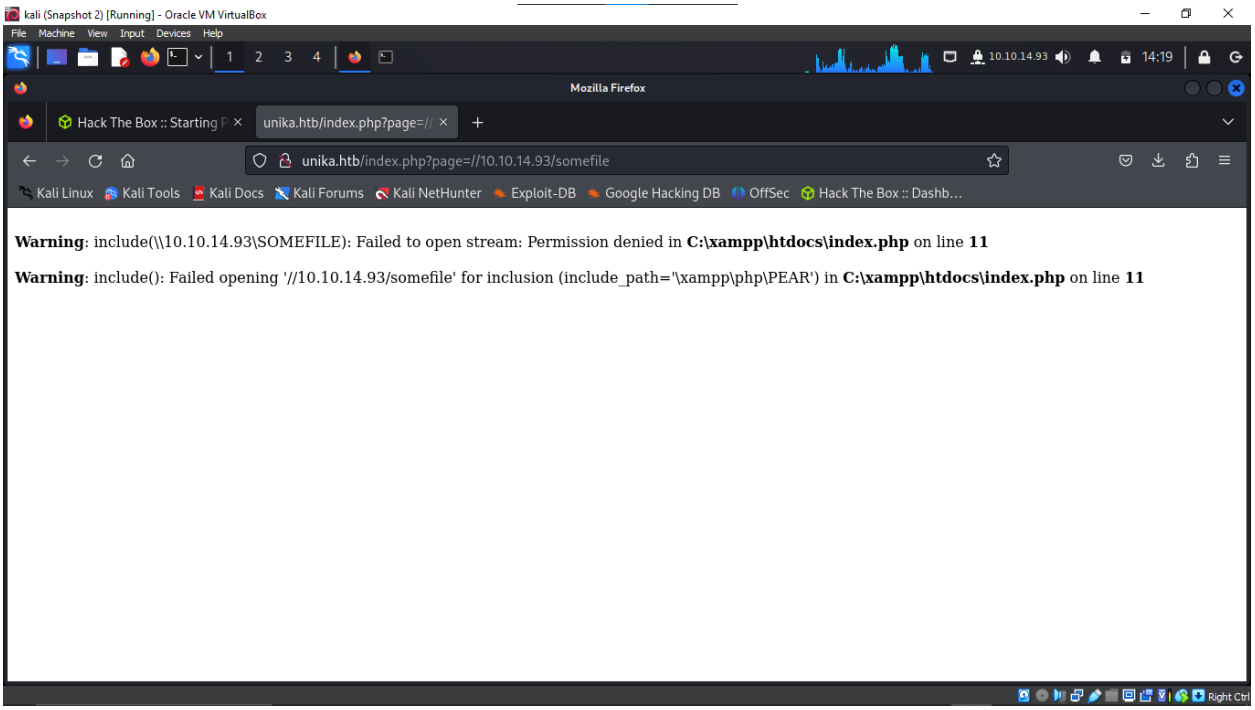
- **Question:** Example of LFI exploitation?
- **Answer:** ../../../../../../../../windows/system32/drivers/etc/hosts
- **Details:** LFI vulnerabilities allow unauthorized file access, posing significant security risks.

- 

Task 5: Remote File Inclusion (RFI) Exploit

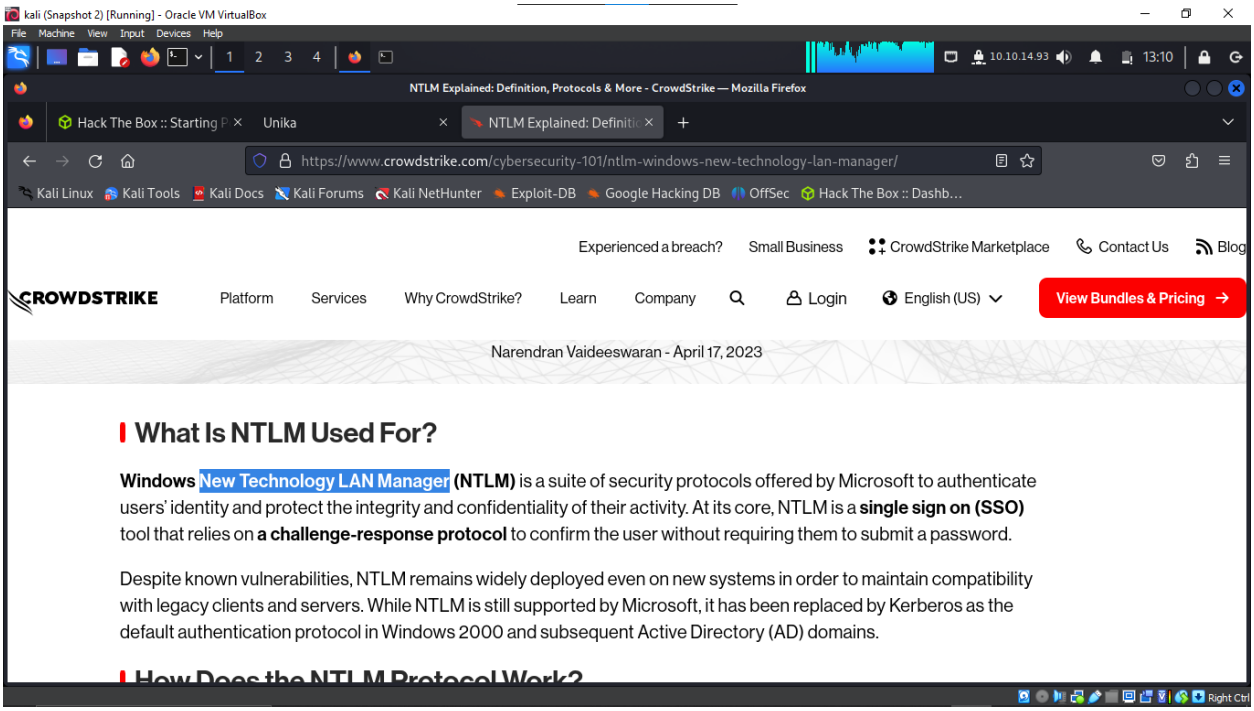
- **Question:** Example of RFI exploitation?

- **Answer:** //10.10.14.6/somefile
- **Details:** RFI enables external file inclusion, leading to remote code execution.



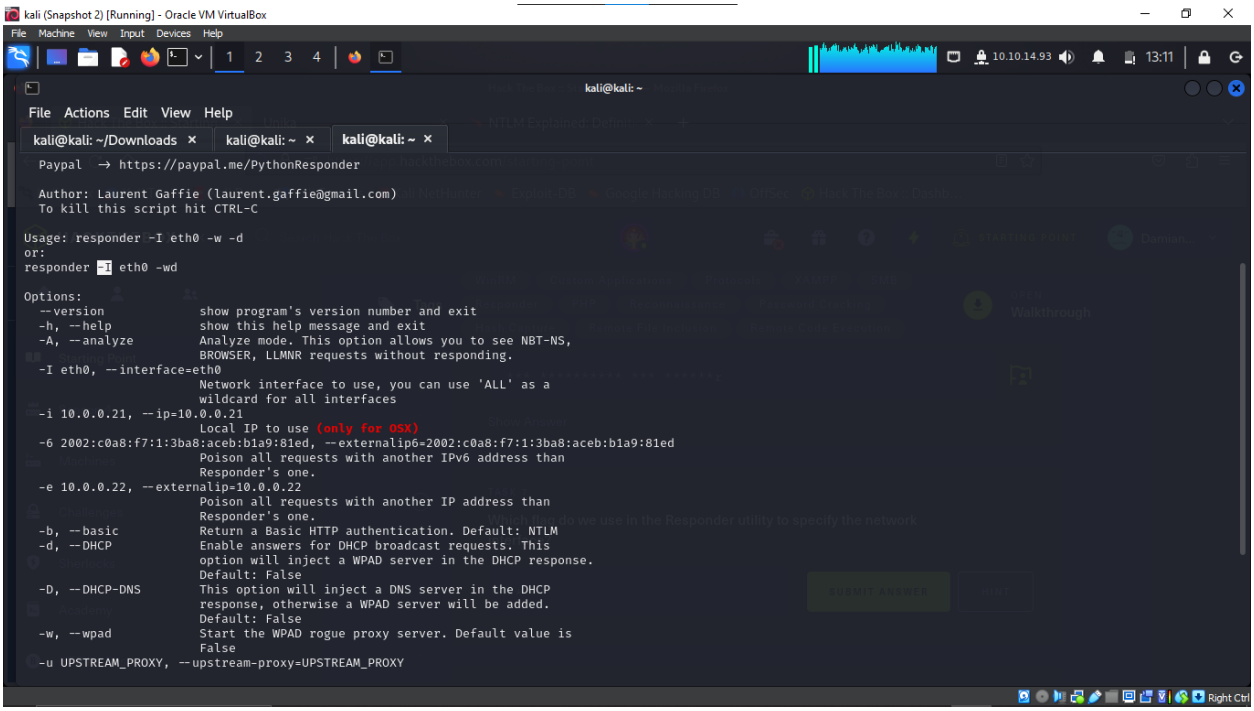
Task 6: NTLM Authentication

- **Question:** What does NTLM stand for?
- **Answer:** New Technology Lan Manager
- **Details:** NTLM is a suite of Microsoft security protocols providing authentication, integrity, and confidentiality to users.

- 

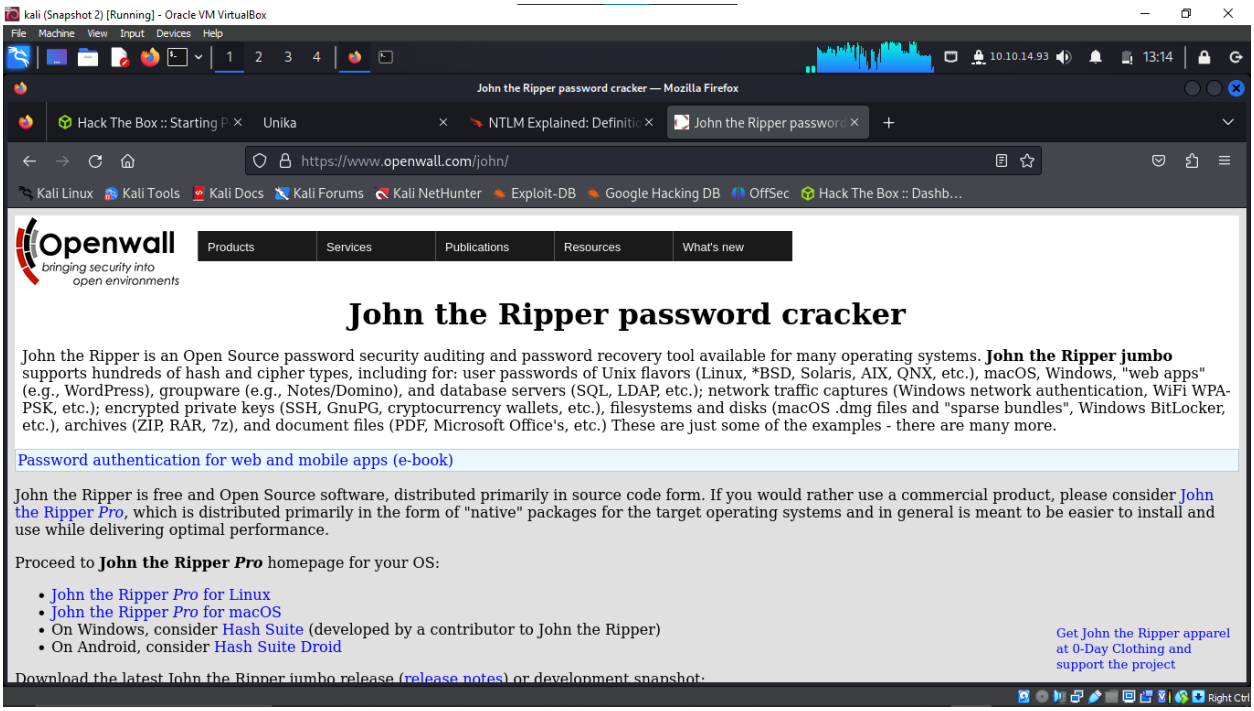
Task 7: Responder Utility Flag

- **Question:** Flag for network interface in Responder?
- **Answer:** -I
- **Details:** The -I flag specifies the network interface for capturing authentication hashes.

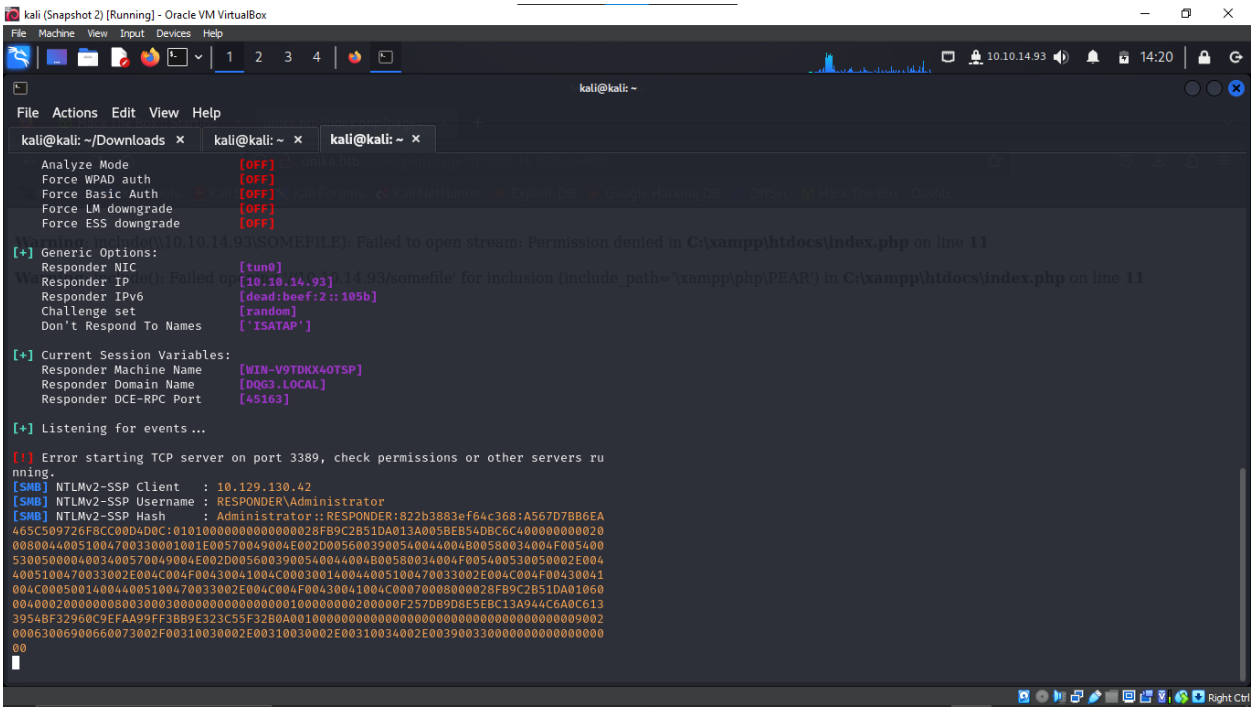
- 

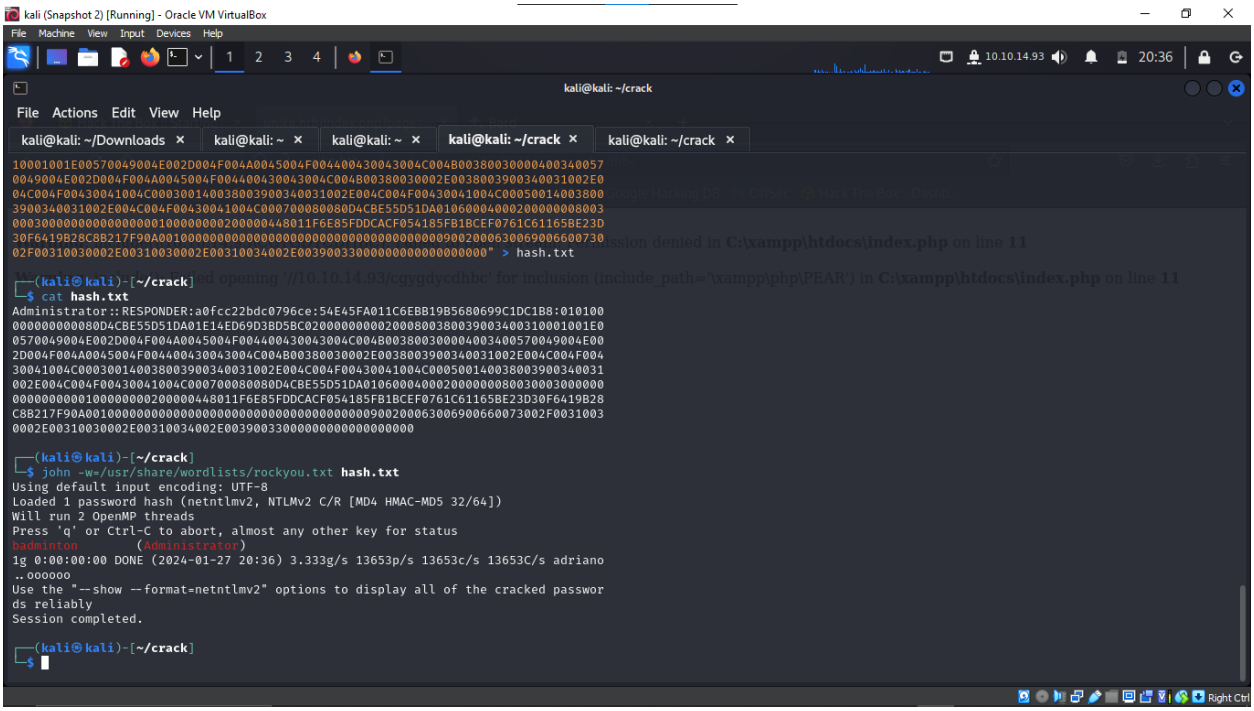
Task 8: Hash Cracking Tool

- **Question:** Full name of the **john** hash-cracking tool?
- **Answer:** John The Ripper

- **Details:** John The Ripper is a widely-used tool for password hash cracking.
- 

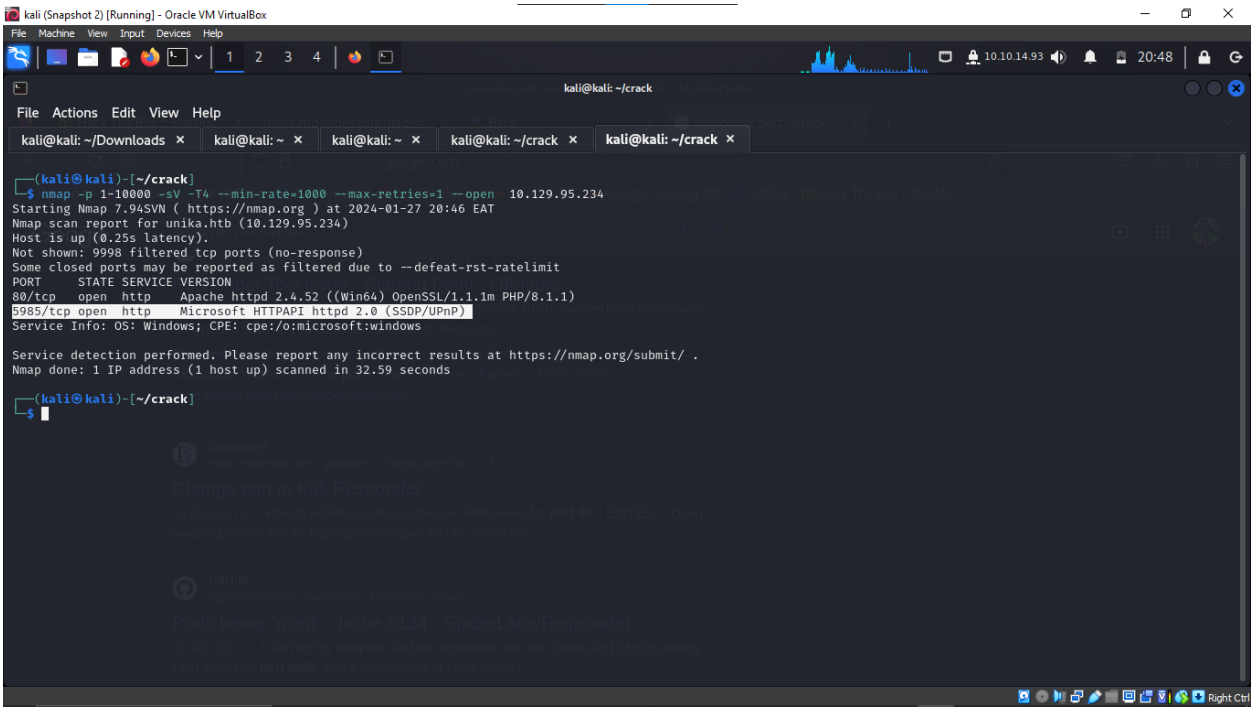
Task 9: Administrator Password

- **Question:** Password for the administrator user?
- **Answer:** badminton
- **Details:** Cracking this password is key for accessing higher-privileged areas of the network.
- 

- 

Task 10: Remote Access Service Port

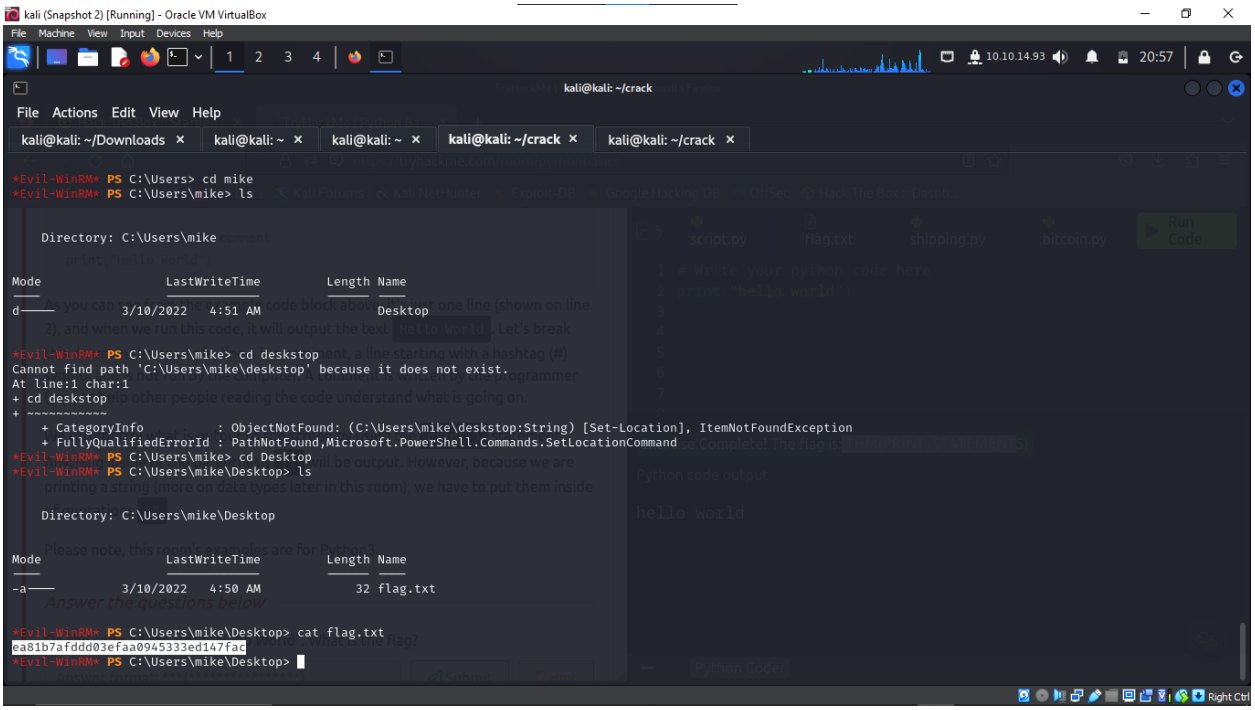
- **Question:** Port for Windows Remote Management (WinRM)?
- **Answer:** 5985
- **Details:** Port 5985 is used by WinRM for remote management and command execution.

- 

Submit Root Flag

- **Flag:** ea81b7afddd03efaa0945333ed147fac

- **Details:** Successful exploitation of the target system and retrieval of the root flag.



Conclusion

The "Responder" lab provides a hands-on experience in exploiting web application vulnerabilities and leveraging network services for deeper system access. It highlights the importance of understanding web application security and the potential implications of compromised network services.

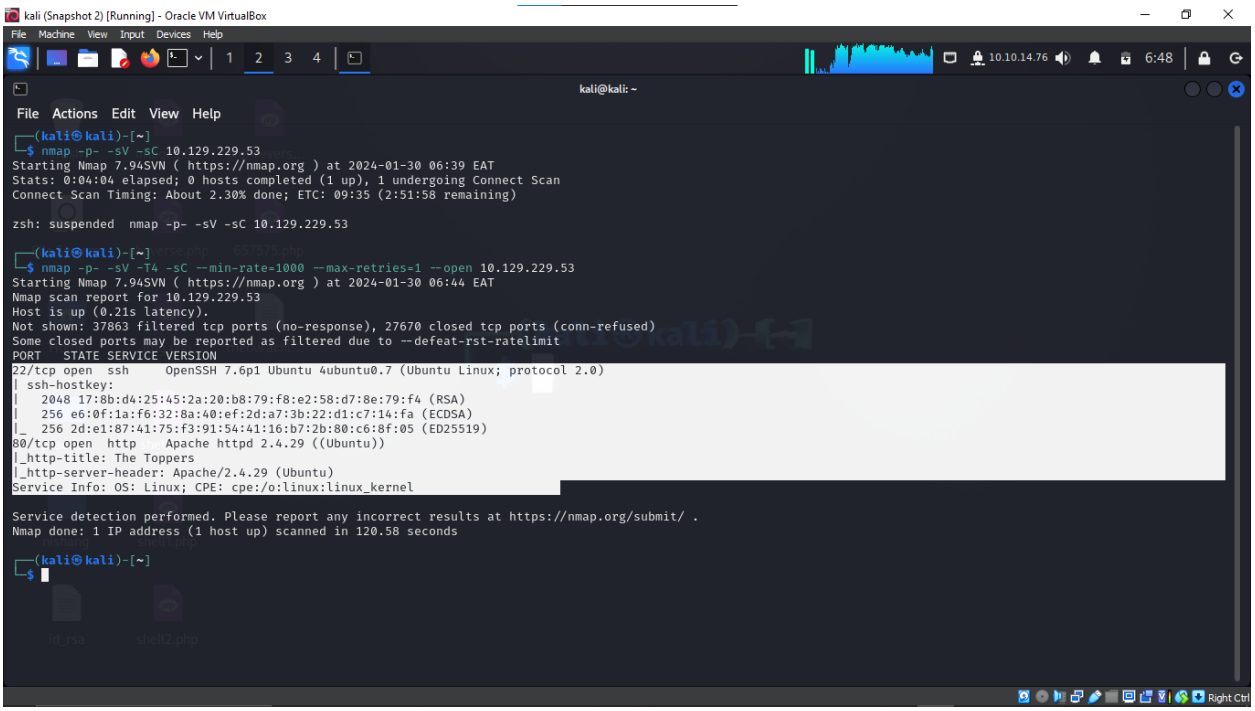
THREE

Introduction

The "Three" lab centers around a scenario involving web and cloud infrastructure, focusing on AWS services and web scripting vulnerabilities. It offers hands-on experience in exploiting misconfigured AWS S3 buckets and leveraging these for further system access.

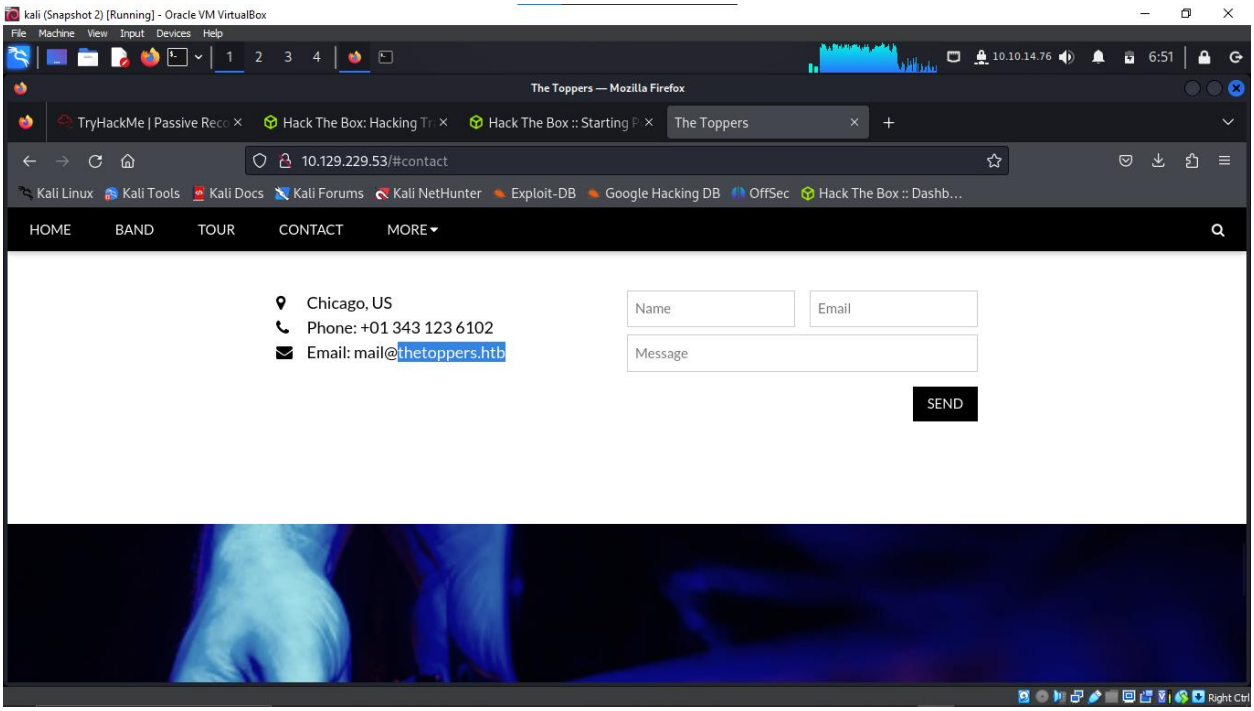
Tasks and Findings

Task 1: Open TCP Ports

- **Question:** Number of open TCP ports?
- **Answer:** 2
- **Details:** Identifying open TCP ports is crucial for determining potential points of entry.
- 

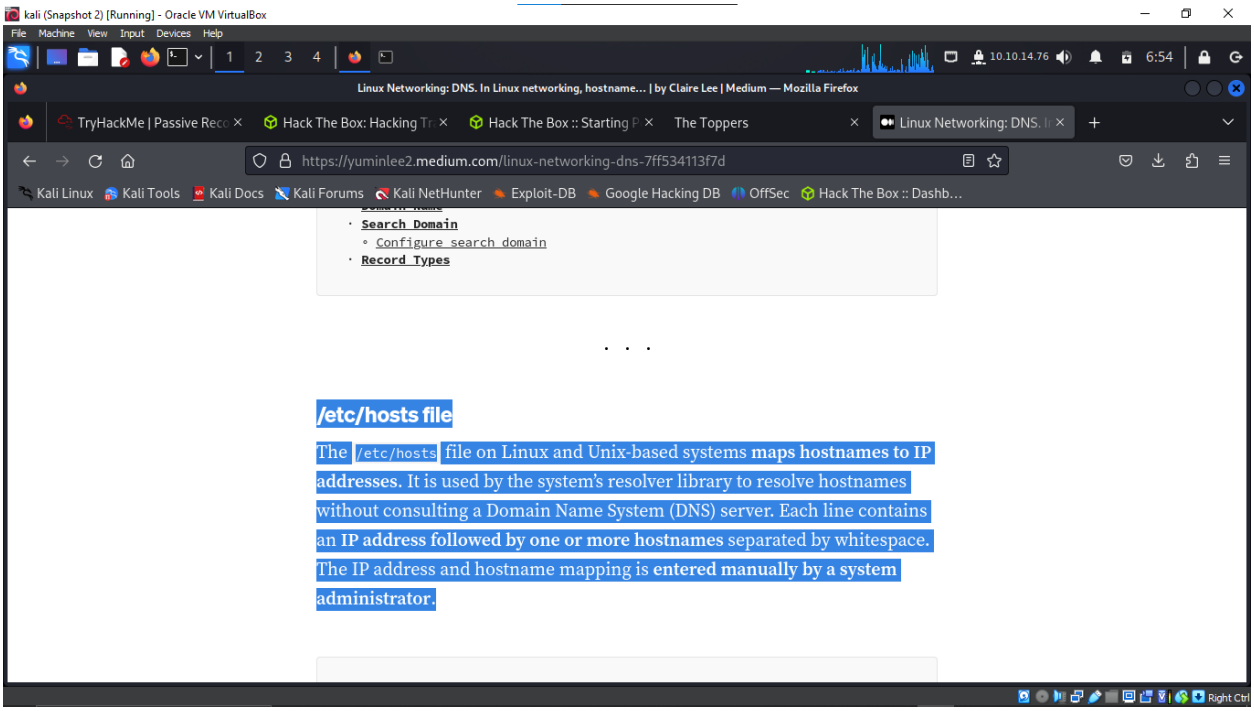
Task 2: Email Domain

- **Question:** Domain of the email in the "Contact" section?
- **Answer:** thetoppers.htb
- **Details:** This information is useful for understanding the domain structure and potential subdomains.

- 

Task 3: Hostname Resolution

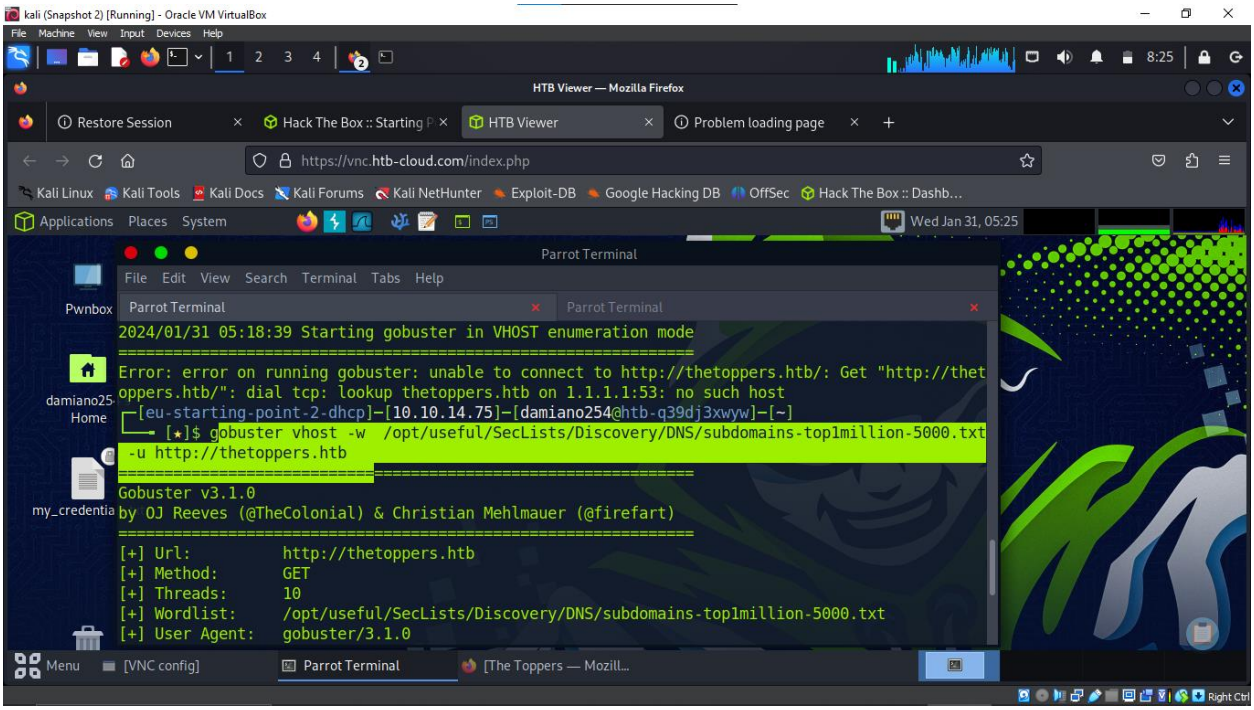
- **Question:** Linux file for hostname resolution without DNS?
- **Answer:** /etc/hosts
- **Details:** Modifying /etc/hosts enables access to specific domains and subdomains without DNS resolution.

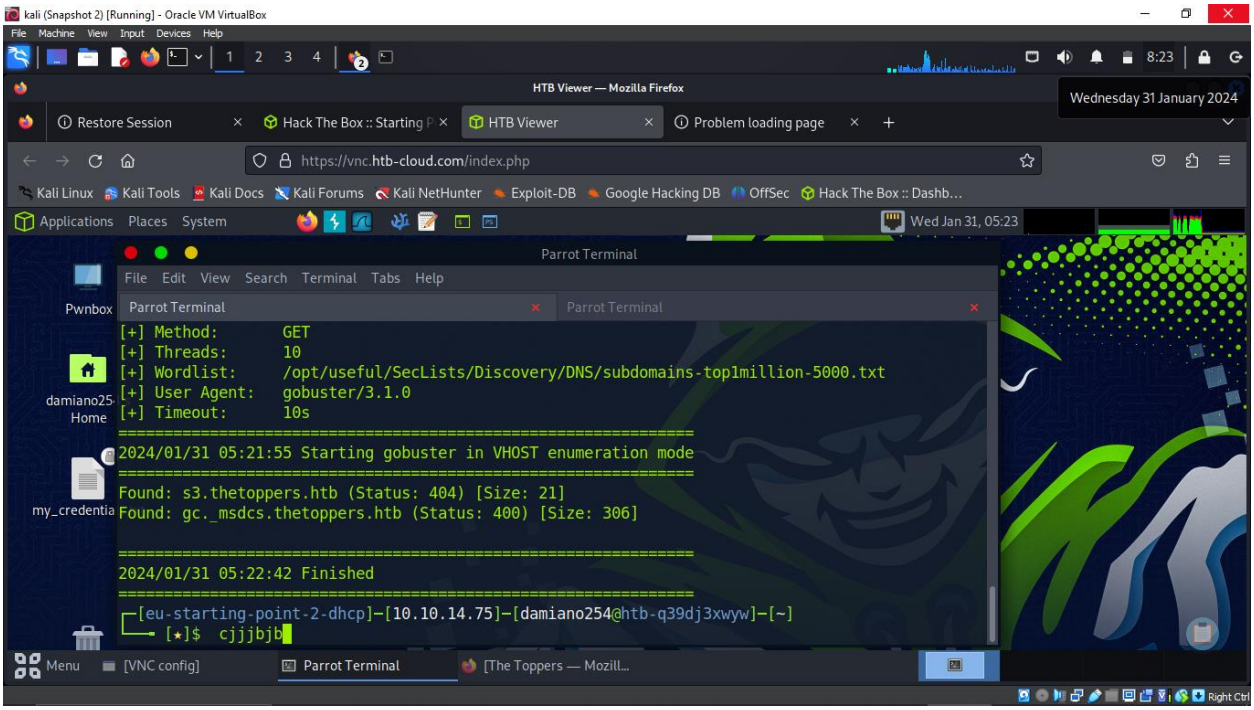
- 

Task 4: Sub-domain Discovery

- **Question:** Discovered sub-domain during enumeration?
- **Answer:** s3.thetoppers.htb

- **Details:** Discovering sub-domains can reveal additional services or entry points.





Task 5: Service on Sub-domain

- **Question:** Service running on discovered sub-domain?
- **Answer:** Amazon S3
- **Details:** The presence of an Amazon S3 service indicates potential cloud storage vulnerabilities.

Amazon S3

Article Talk

From Wikipedia, the free encyclopedia

The technical content of this article relies largely or entirely on docum
Amazon.com. Relevant discussion may be found on the talk page. Ple
article by introducing citations to additional sources.

Find sources: "Amazon S3" – news · newspapers · books · scholar · JSTOR *(Nover*

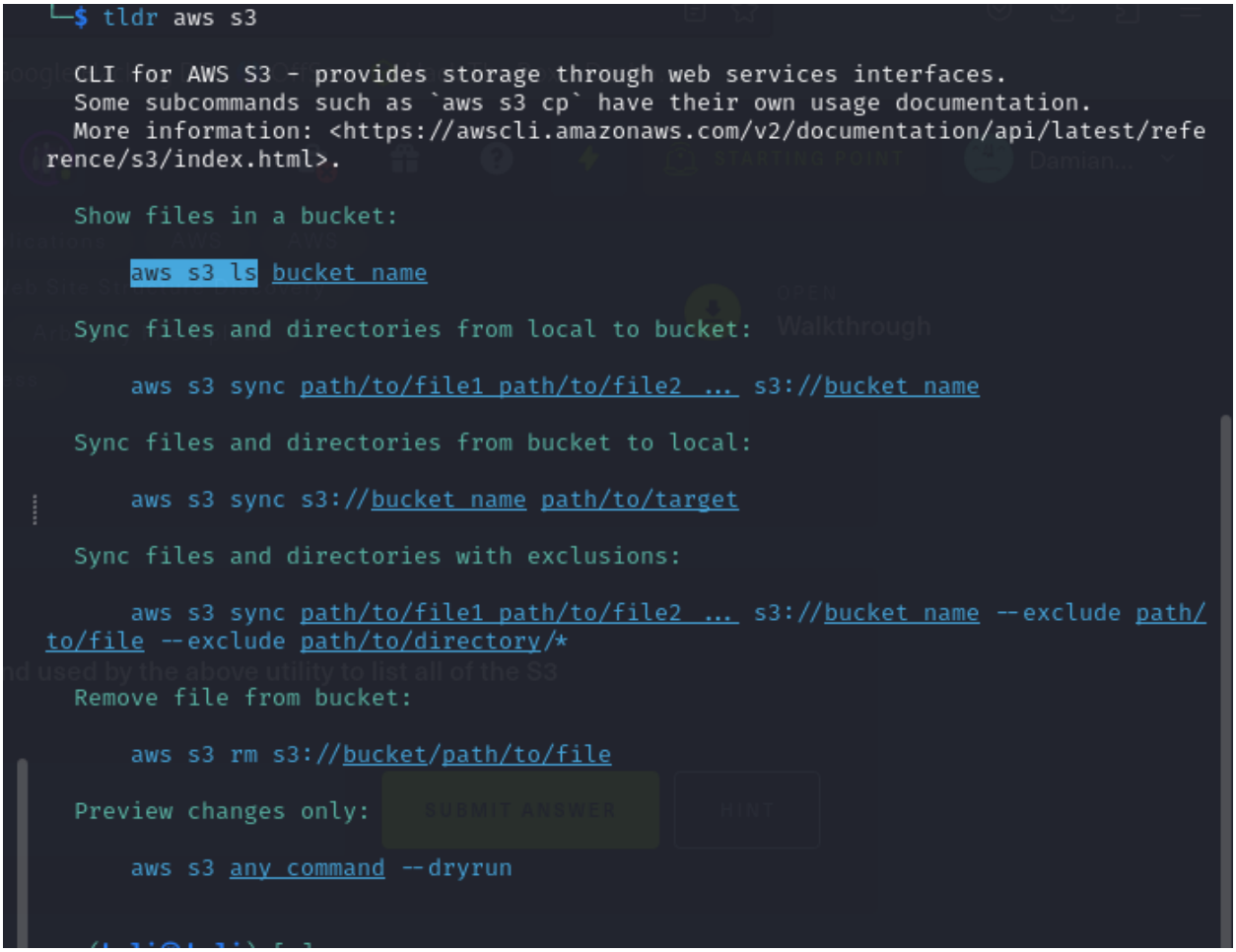
Amazon S3 or **Amazon Simple Storage Service** is a service offered by Amazon Web Services (AWS) that provides object storage through a web service interface.[1][2] Amazon S3 uses the same scalable storage infrastructure that Amazon.com uses to run its e-commerce network.[3] Amazon S3 can store any type of object, which allows uses like storage for Internet applications, backups, disaster recovery, data archives, data lakes for analytics, and hybrid cloud storage. AWS launched Amazon S3 in the United States on March 14, 2006,[1][4] then in Europe in November 2007.[5]

Task 6: AWS CLI Utility

- **Question:** Command line utility for interacting with Amazon S3?
- **Answer:** awscli
- **Details:** awscli is a vital tool for interacting with AWS services, enabling various operations like listing and transferring files.

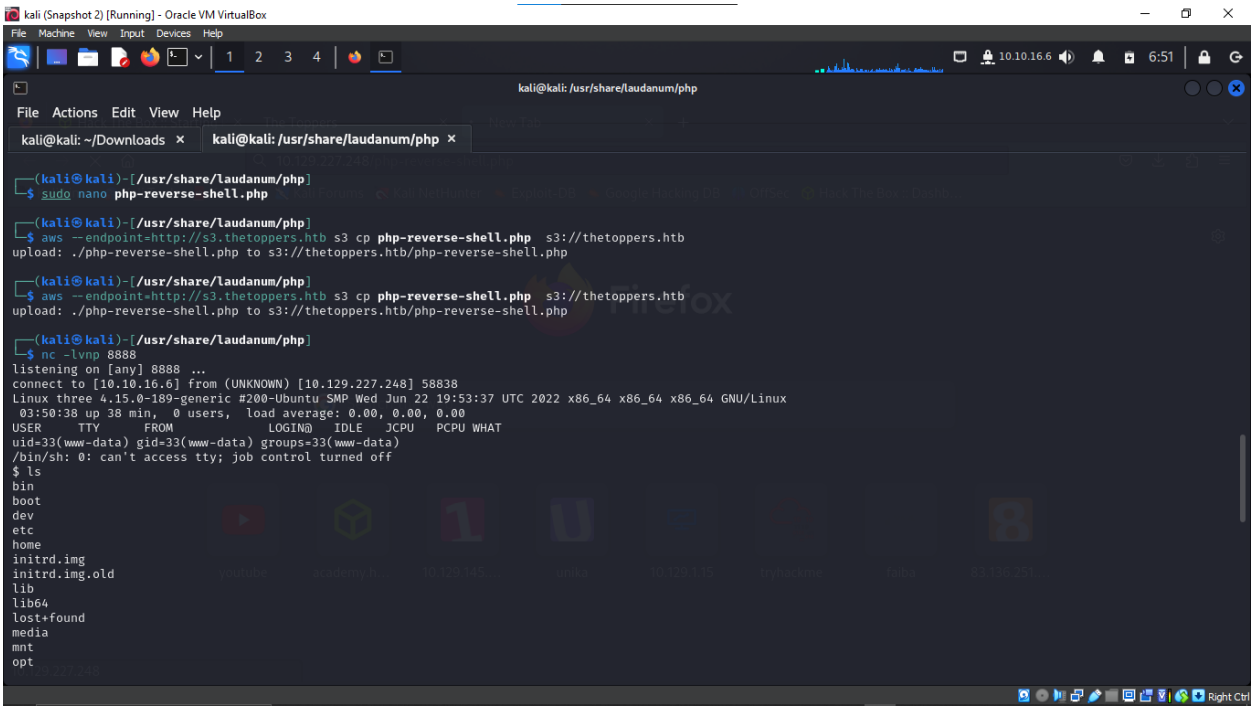
Task 7: AWS CLI Setup

- **Question:** Command to set up AWS CLI?
- **Answer:** aws configure
- **Details:** Proper configuration of awscli is essential for interacting with AWS services.

- 

Task 8: Listing S3 Buckets

- **Question:** Command to list S3 buckets?
- **Answer:** aws s3 ls
- **Details:** This command lists all S3 buckets, aiding in enumeration and potential exploitation.

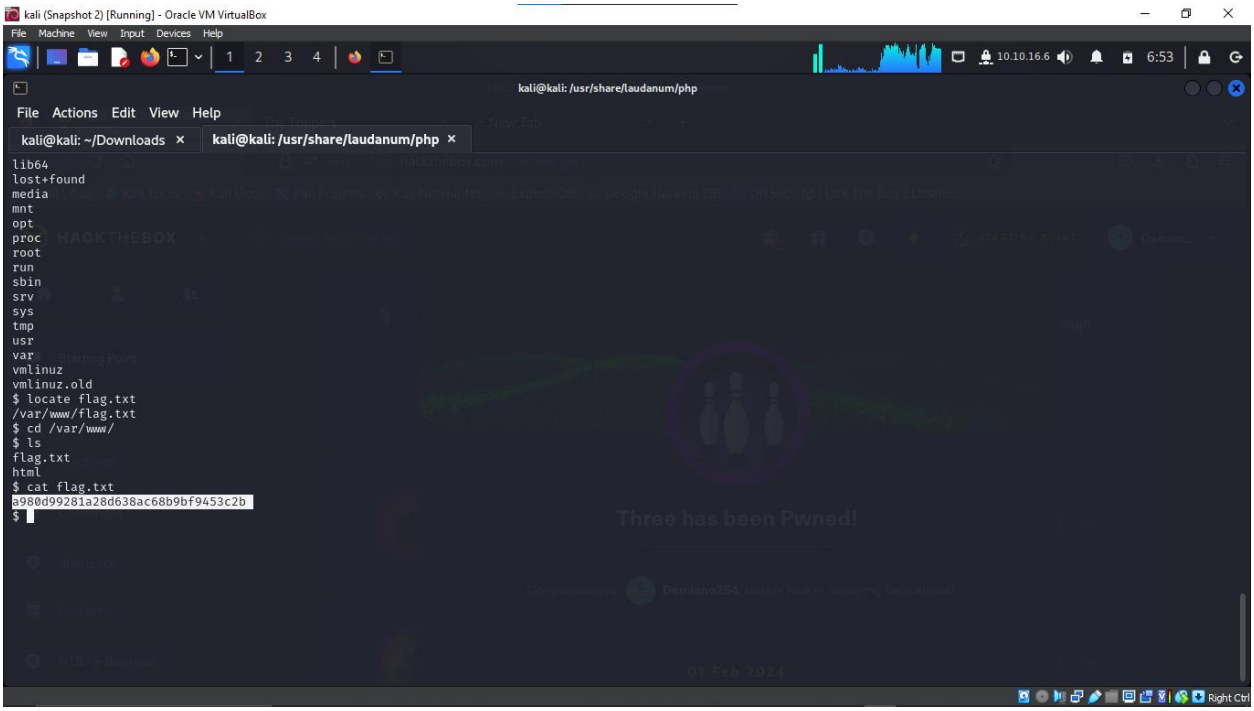
- 

Task 9: Server Scripting Language

- **Question:** Scripting language on the server?
- **Answer:** PHP
- **Details:** PHP is a widely used language for web development, often with its own set of vulnerabilities.
-

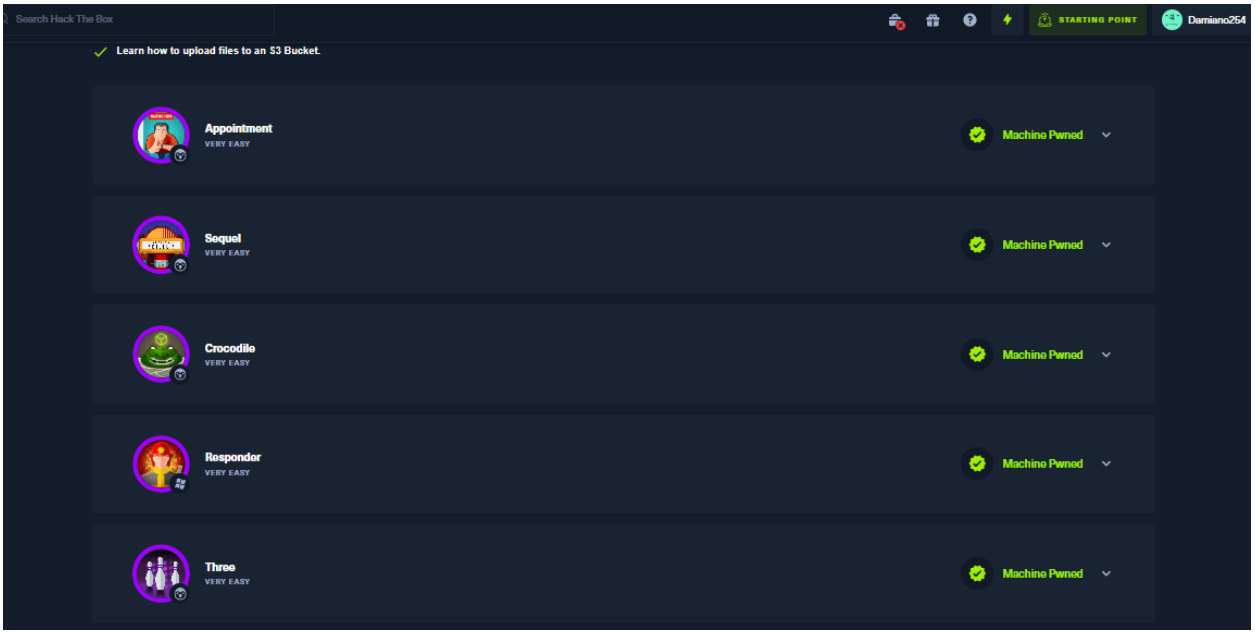
Submit Root Flag

- **Flag:** a980d99281a28d638ac68b9bf9453c2b
- **Details:** Successful retrieval of the root flag indicates effective exploitation and access control.
-



Conclusion

The "Three" lab provides critical insights into exploiting cloud-based infrastructures and web applications. It underscores the need for secure cloud configurations and demonstrates the potential vulnerabilities in web applications, especially those integrating with cloud services.


Search Hack The Box
STARTING POINT
Damiano254
Learn how to upload files to an S3 Bucket.
Appointment
VERY EASY
Machine Pwned
Sequel
VERY EASY
Machine Pwned
Crocodile
VERY EASY
Machine Pwned
Responder
VERY EASY
Machine Pwned
Three
VERY EASY
Machine Pwned