Ahmed Kasteer

20F-0336  BCS-7C

Information security

**SQLmap**

**INTRODUCTION**:

A powerful tool designed specifically for finding and exploiting security flaws in web applications that use databases is SQL MAP. Its main purpose is to identify and take advantage of SQL injection vulnerabilities, which, if ignored, can be used to access databases without authorization and retrieve private information. For penetration testers, SQL MAP is a vital tool that makes the process of finding vulnerabilities easier. It uses several tags to determine if a website is vulnerable to injection attacks.

**TASK DESCRIPTION:**

You can practice SQL Map techniques in accordance with the penetration testing methodology by taking on the task at TryHackMe. Using a VPN to establish a safe and encrypted connection is the first step in the process. After that, the data collection stage is carried out, and SQL Map is used to examine and scan the target for SQL injection vulnerabilities. Data is extracted from the database as a result of SQL Map's automated detection and exploitation of these vulnerabilities. Passwords, usernames, and other sensitive information may be included in this data. Retrieving particular flags or sensitive data from the web application or database is the task's goal.

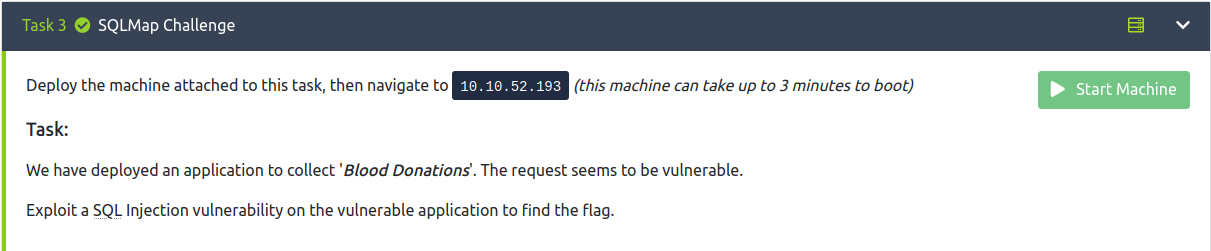
**INSIGHTS:**

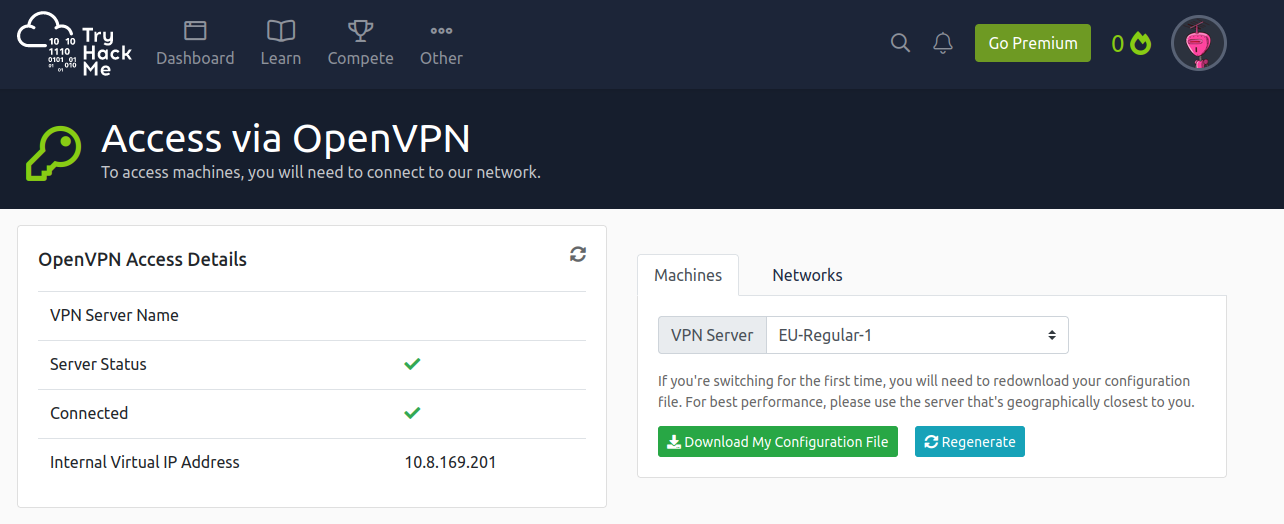
SQL Map shows up as a powerful utility that makes it easier to find and take advantage of SQL injection vulnerabilities in web applications. It gives security experts the tools they need to quickly find vulnerabilities and retrieve information from databases. Within the task at hand, SQL Map has demonstrated its efficacy in extracting confidential data and modifying the actions of susceptible web applications.

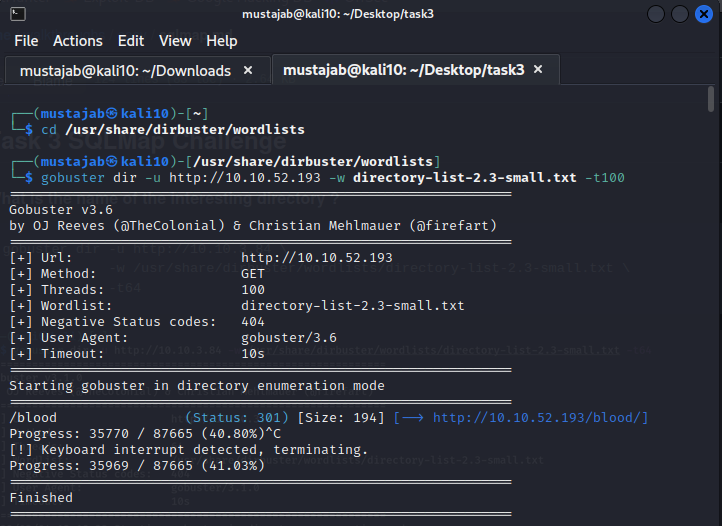
**LIMITATIONS OR CONSIDERATIONS:**

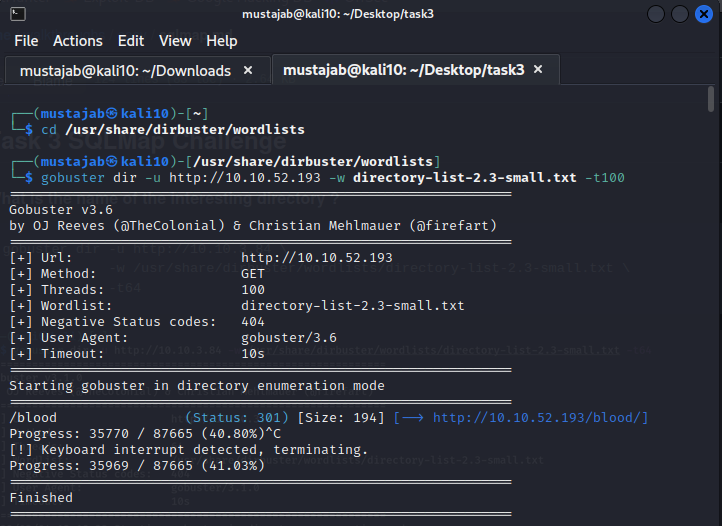
Despite its strength, SQL MAP is not without its limitations. It was discovered during testing that this tool might have difficulties processing complex queries. Sometimes it took the use of an extra tool, like "gobuster," to find a vulnerable parameter. However, SQL Map is very good at listing databases and retrieving important data elements—like active users—from these databases.

**SCREENSHOTS:**









**REQUEST CAPTURE**

This request was captured where a parameter if id was observed in the URL and the whole request was saved in a file to apply different SQL Map commands on it to find sensitive information.

GET /blood/view.php?id=1 HTTP/1.1

Host: 10.10.52.193

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

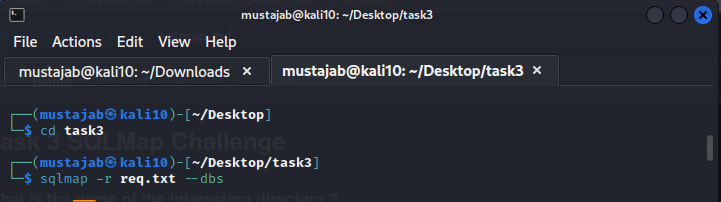
Accept-Encoding: gzip, deflate

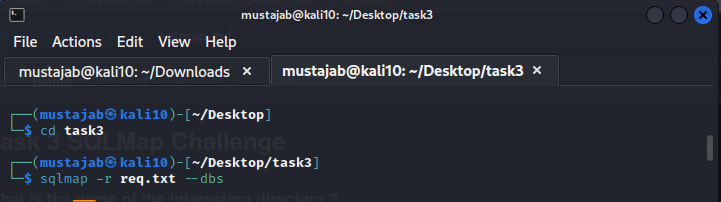
Connection: keep-alive

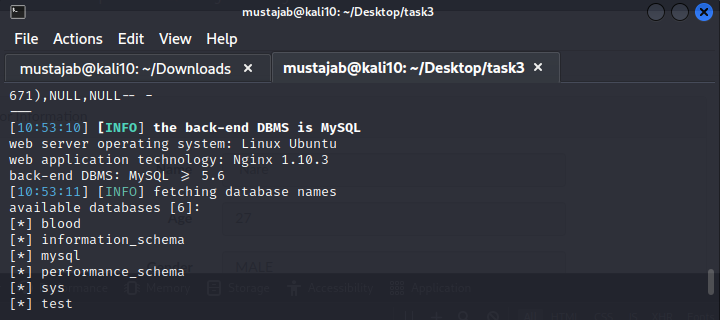
Referer: http://10.10.52.193/blood/blood.php

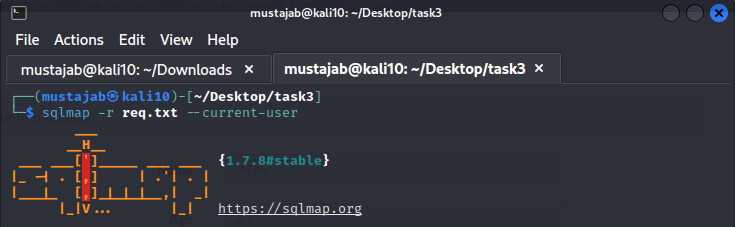
Cookie: PHPSESSID=jq1k688v8qlgc9fbbnd6aespv0

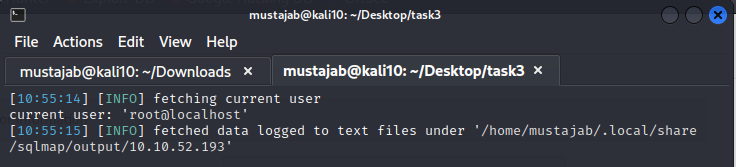
Upgrade-Insecure-Requests: 1



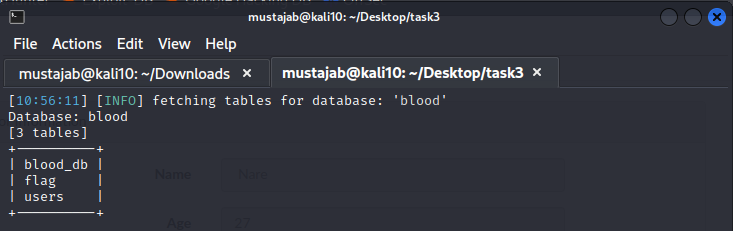


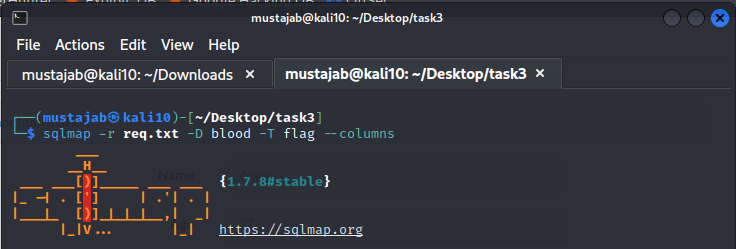


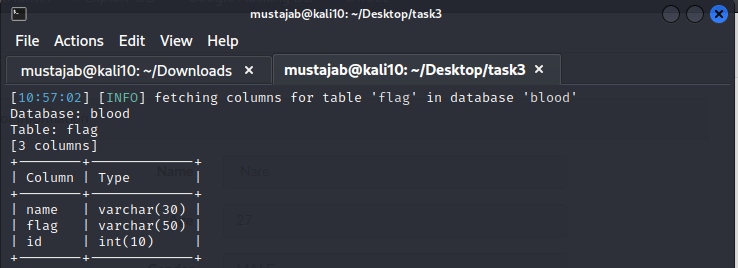




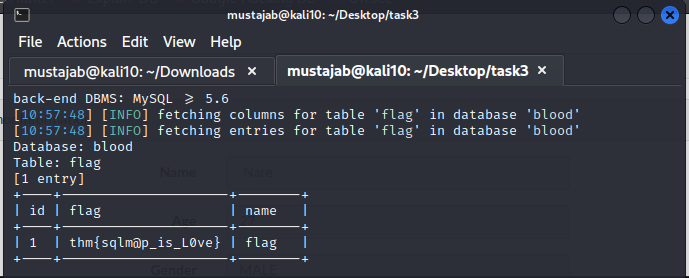












**BrupSuite**

**INTRODUCTION:**

Burp Suite is a powerful cybersecurity tool designed specifically for evaluating web application security. It serves as an electronic tool to assist security experts in identifying and fixing vulnerabilities on webpages. Its main objective is to detect a broad range of vulnerabilities in web applications, from cross-site scripting errors to SQL injections. With its impressive automation features, the tool can automatically scan websites and web services for common security flaws. The feature set of Burp Suite includes the ability to generate thorough vulnerability reports, which aids in efficient communication with stakeholders and developers. Notably, it makes it possible to record and manage HTTP/HTTPS traffic flowing between a web server and a web browser..

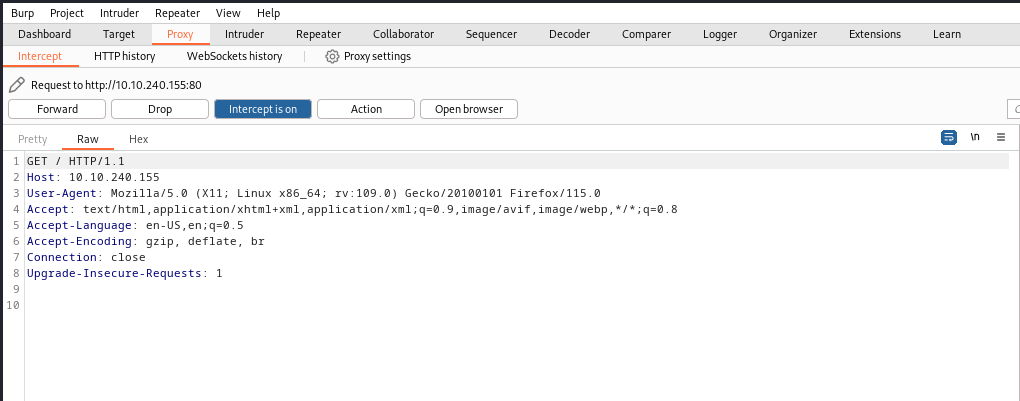
**TASK DESCRIPTION:**

This room covers the basics of using Burp Suite, with an emphasis on exploring different aspects like installation, dashboard features, navigation, and setting up a proxy using FoxyProxy. Participants also learn about site mapping, defining issues, using the Burp Suite browser, and implementing efficient scoping and targeting strategies, such as HTTPS traffic proxies.

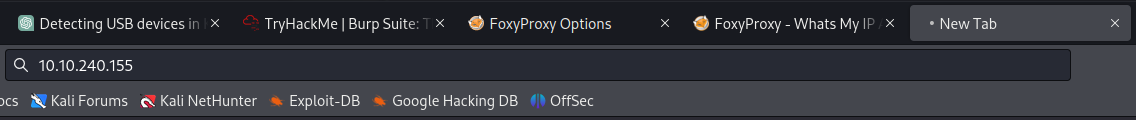
**INSIGHTS**:

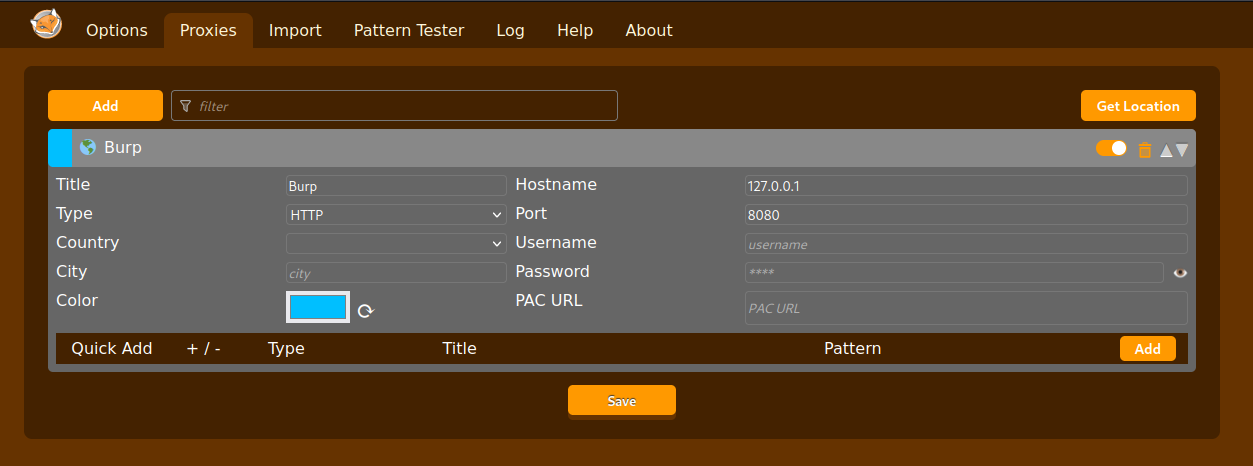
This room's lessons offer important insights into manipulating, observing, and changing web requests. Furthermore, it provides instructions on how to use complementary tools such as FoxyProxy, which facilitates the smooth switching between multiple proxy servers while browsing the internet. The main focus is on introducing users to proxy configurations and request capturing. The images below show particular tasks completed in accordance with the instructions in the room.

**SCREENSHOTS:**

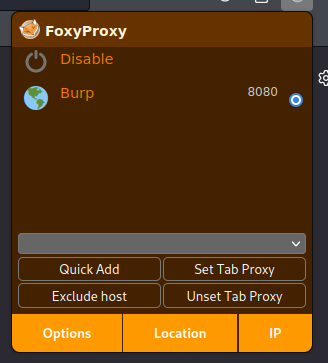
****

***Intercepting a request***

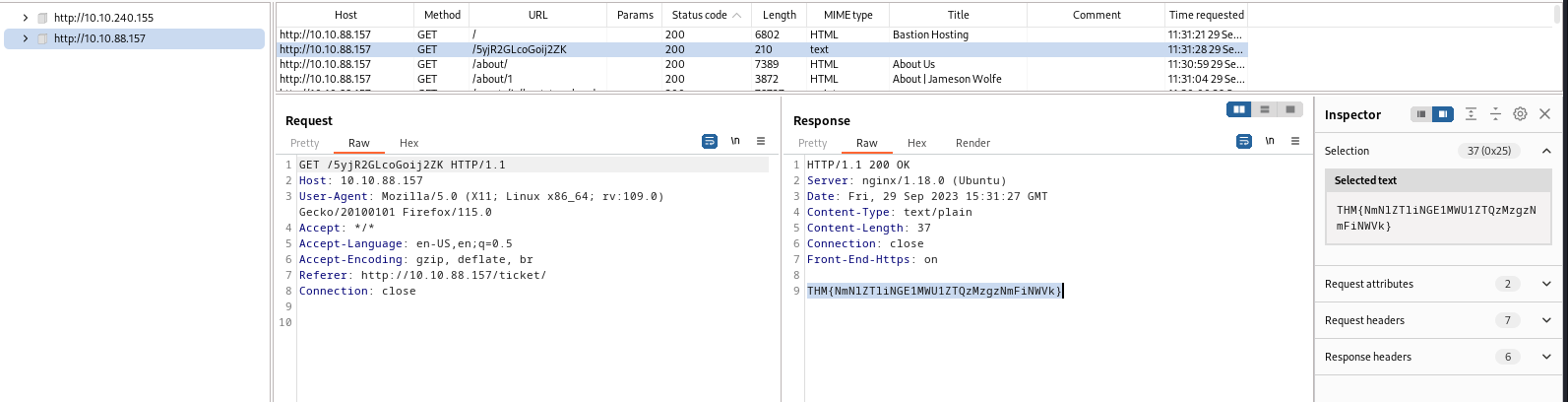
****

****

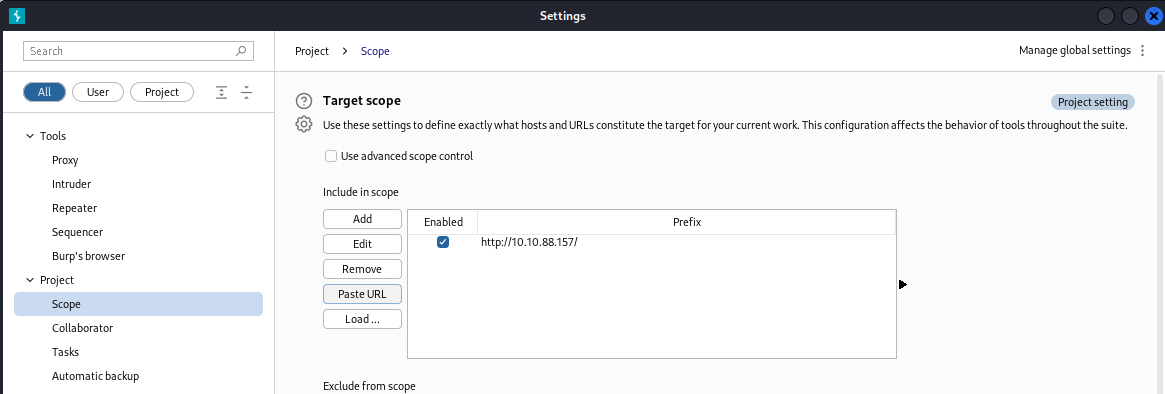
***Installation Froxy Proxy***

****

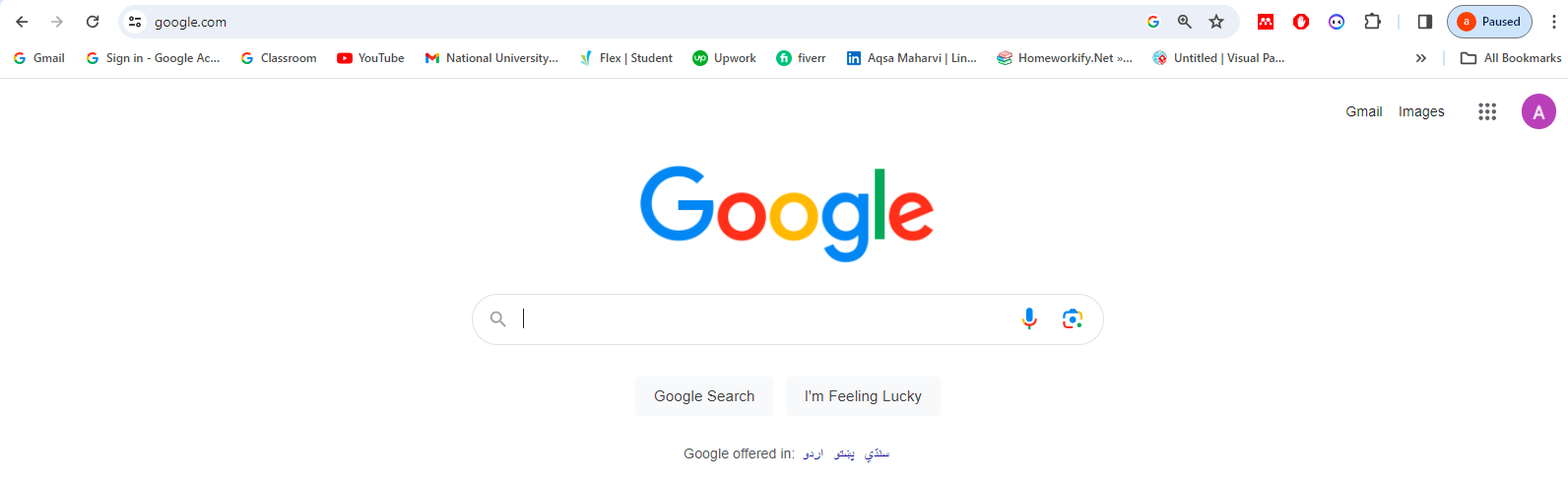
***Setting up a proxy***

****

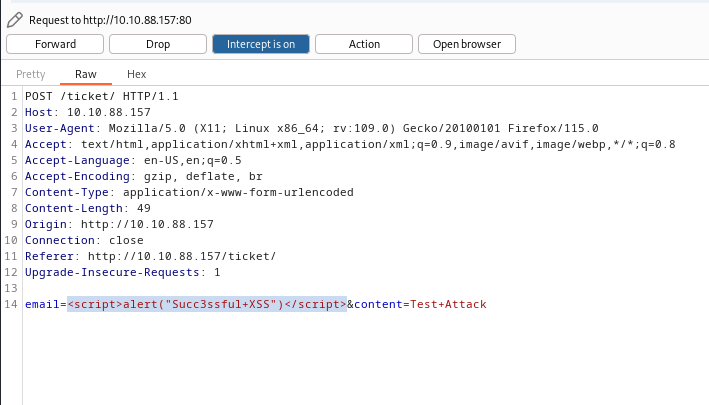
***Irregular URL and related flag***

****

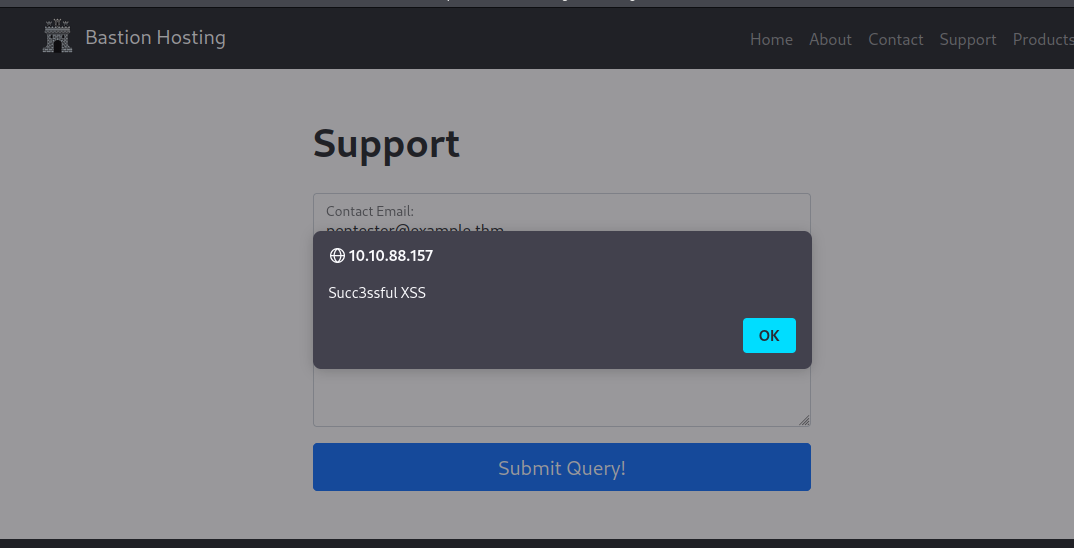
***Added request in scope***



***Accessing site after certification***

****

***Intercepting for XSS attack***

****

**Nmap**

**INTRODUCTION:**

Nmap is a particularly useful tool for network administrators and cybersecurity specialists. An extensive view of network architectures, online hosts, open ports, running services, and even the underlying operating systems is offered by this free and open-source network scanning tool. Because of its incredible versatility, users can use the Nmap Scripting Engine, NSE, to run customized scripts and perform scans using a wide range of methodologies. When it comes to network troubleshooting, vulnerability identification, and ethical hacking, Nmap's versatility and accuracy make it an invaluable tool that empowers users to carry out in-depth assessments and strengthen network security.

**Enumeration and Evasion Scans:**

Within the domain of network scanning, Nmap offers several scan types tailored for enumeration and evasion purposes. These include:

1. **TCP Connect Scan (-sT):**

Serving as Nmap's default scan, it initiates full TCP connections to each port, enabling the determination of whether a port is open, closed, or obstructed by a firewall.

1. **Syn Stealth Scan (-sS):**

Commonly referred to as a SYN scan, this method dispatches SYN packets to the target ports and interprets the responses to ascertain the state of the ports. Its covert nature lies in its avoidance of the full TCP handshake process.

1. **UDP Scan (-sU):**

Utilized to inspect open UDP ports, this scan type is often characterized by slower and less reliable results than its TCP counterpart due to the connectionless nature of UDP.

1. **ACK Scan (-sA):**

The ACK scan is instrumental in uncovering stateful firewall rules. It sends ACK packets and evaluates responses to establish whether ports are filtered by a firewall.

1. **FIN Scan (-sF):**

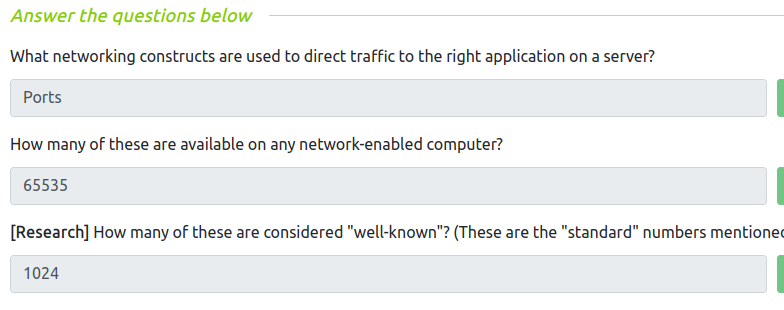
By transmitting FIN packets to target ports, this scan method identifies closed ports, expecting a response in the form of an RST packet. The absence of response indicates that the port is either open or filtered.

1. **Null Scan (-sN):**

Employing packets devoid of TCP flags, the null scan detects closed ports, which should respond with an RST packet. Similar to FIN and Xmas scans, it serves the purpose of evading firewall or intrusion detection system detection.

1. **Xmas Scan (-sX):**

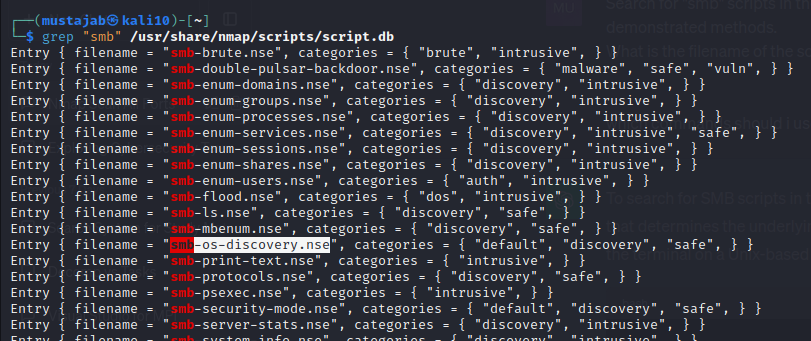
This scan deploys packets with the FIN, URG, and PSH flags set, akin to the NULL and FIN scans. Its primary use lies in evading detection by firewalls or intrusion detection systems.

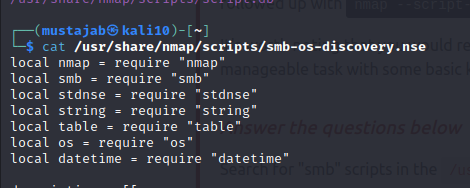
****

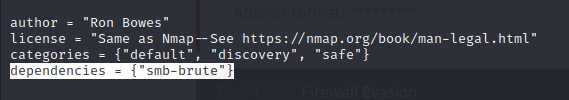
**In Task#03  
Different Switches were:**

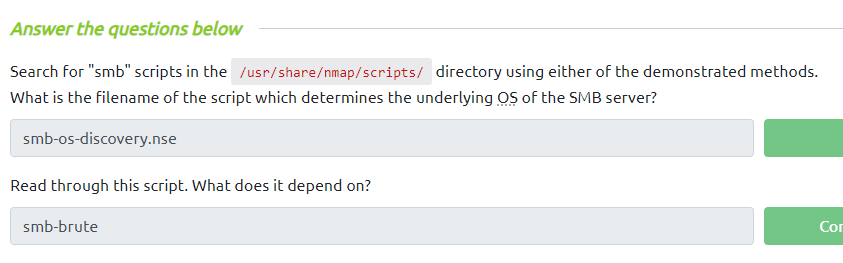
-sS, -sU, -O, -sV, -v, -vv, -oA, -oN, -oG, -A, -T5, -p 80, -p 1000, 1500, -p-, --script, --script-vuln

**Searching for Scripts:**

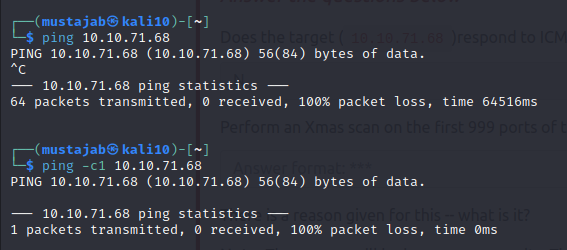


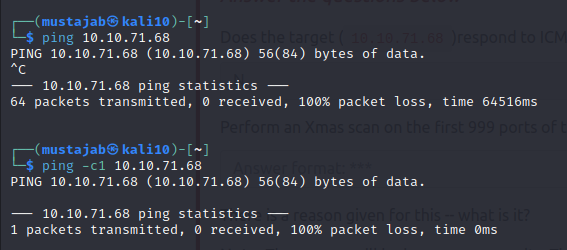


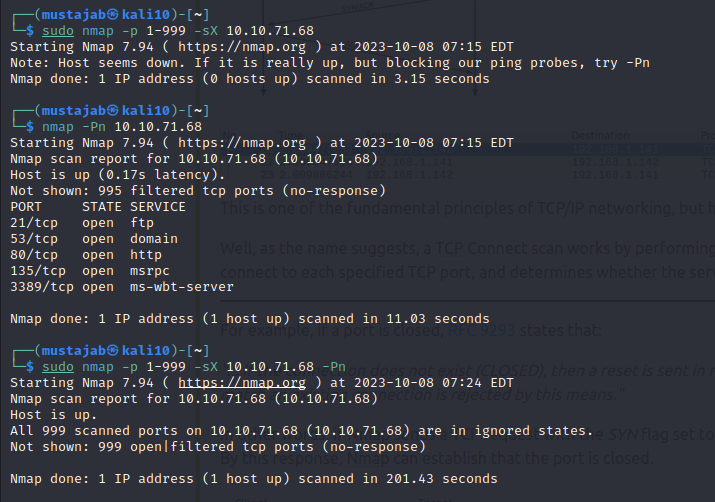


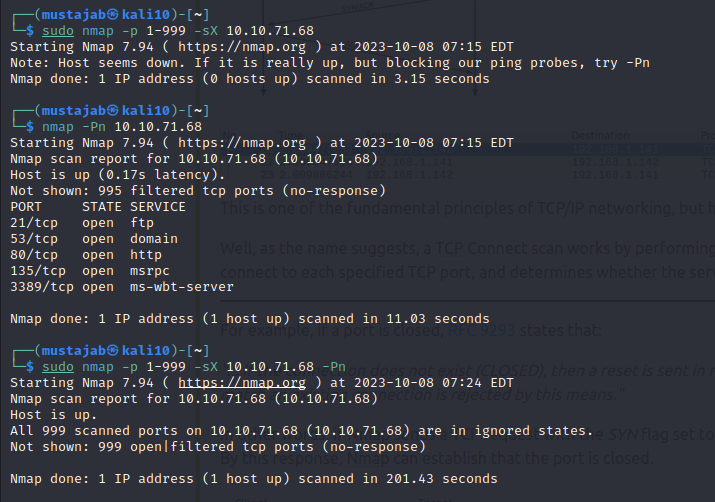


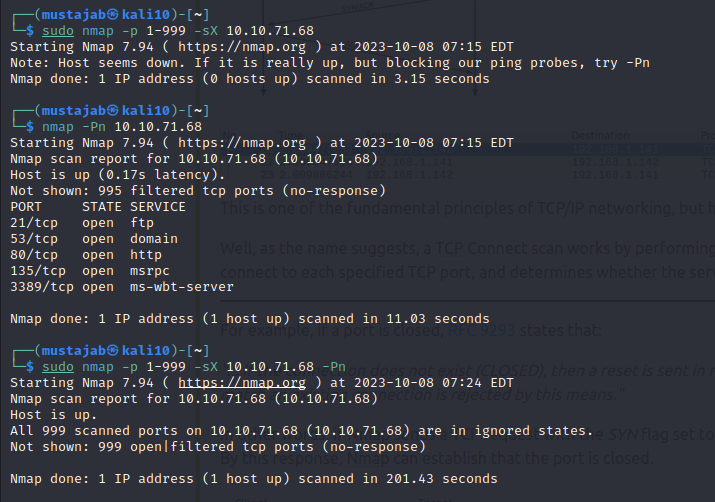
**PRACTICAL**

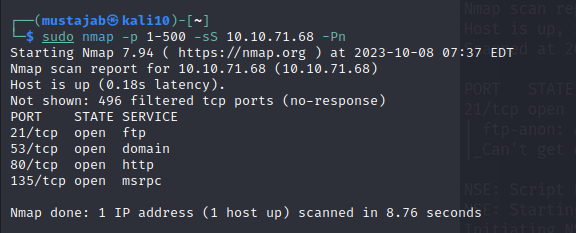


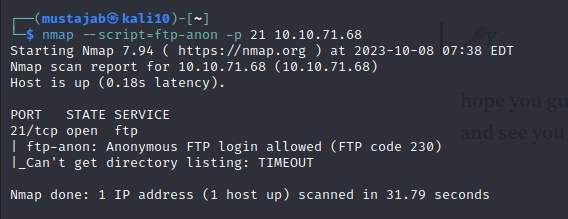


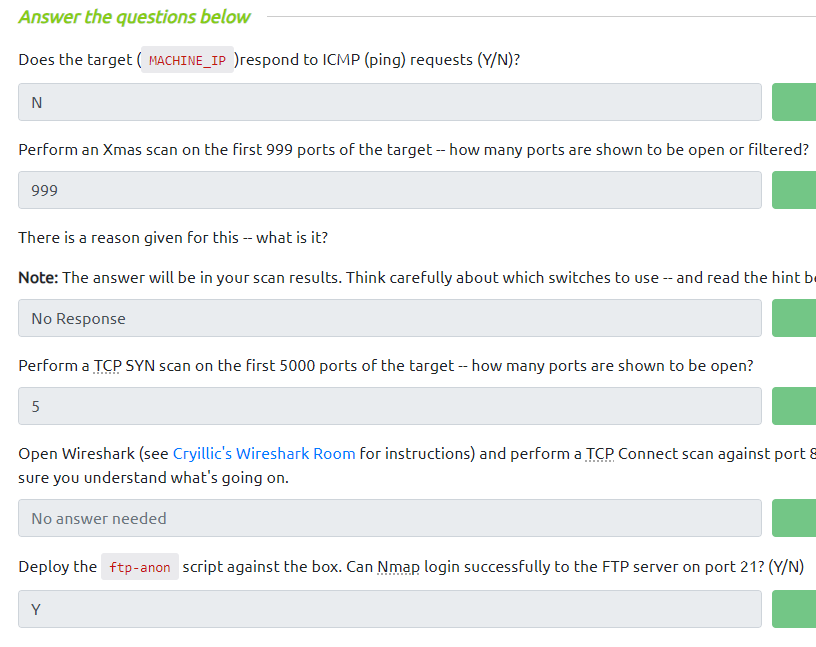












**GNU Debugger**

**Introduction:**

GDB, which stands for "GNU Debugger," is a potent tool that lets you explore the code, set breakpoints, examine and change variables, and more. It also gives you insights into how your program is being executed. Installing gcc/g++ on Linux and other operating systems, like MacOS and Windows, makes this debugger available..

**-Description:**

GDB offers a range of commands to debug C/C++ programs, including:

**- run:**

Initiates the program from the beginning. If a breakpoint is set, the program will halt at that specific breakpoint.

**- continue:**

Resumes program execution until the next breakpoint is reached or until the program concludes.

**- next:**

Executes the next line of source code. In the case of a function call, it proceeds to execute the entire function without interruption.

**-backtrace:**

Provides a back-trace of the call stack, illustrating the sequence of function calls that led to the current program point.

**-step:**

Facilitates stepping into a function call, allowing you to enter the function and execute it line by line.

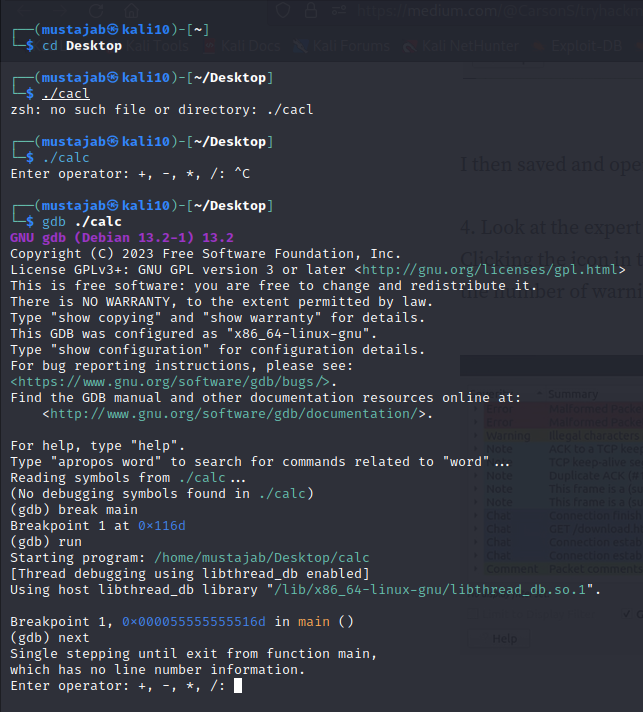
**- print:**

Outputs the value of a variable or expression.

**- quit:**

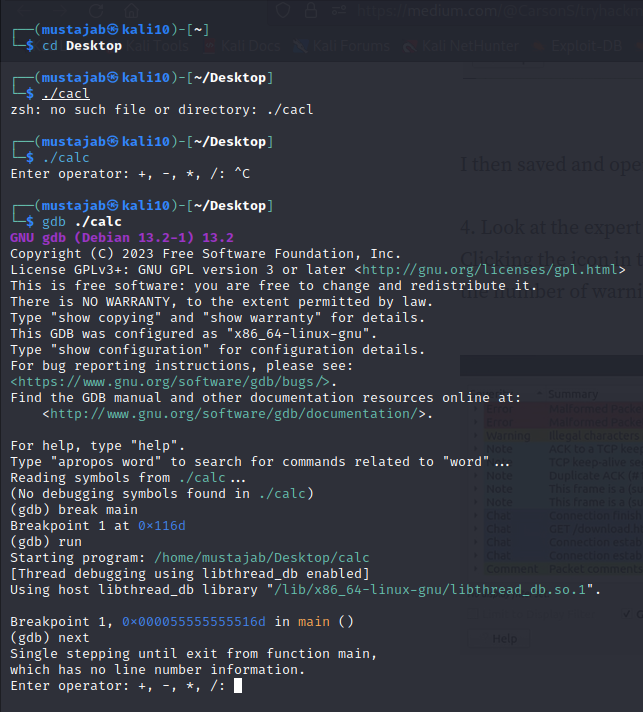
Exits GDB.

**SCREENSHOTS**



A screenshot of a computer program

Description automatically generated



A screenshot of a computer program

Description automatically generated