A green chameleon logo

Description automatically generated

**HTTP-PORT -80 ATTACK**

​​

**TABLE OF CONTENTS**

1-SUMMARY……………………………………………………………………………………..

2-INTRODUCTION……………………………………………………………………………..

3- TOOLS USED………………………………………………………………………………..

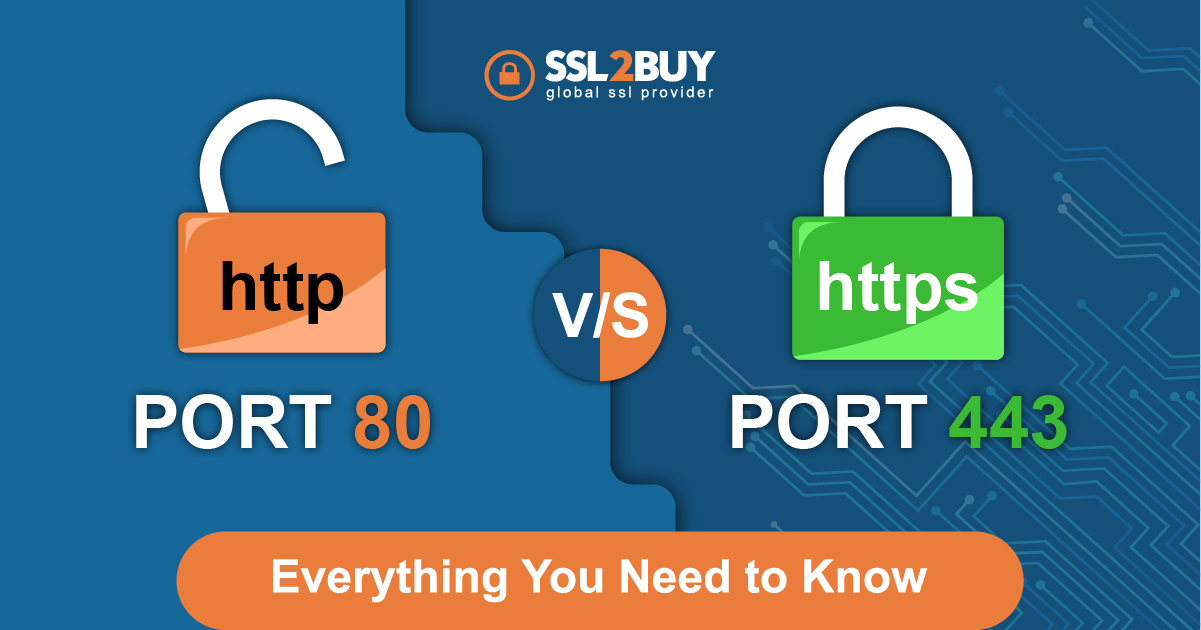
4-SCOPE OF TESTING………………………………………………………………………….

5-RESULTS…………………………………………………………………………………………

6-CONCLUSIONS……………………………………………………………………………….

7-REFERENCES……………………………………………………………………………………

**INTRODUCTION**



Port 80 is a well-known port number used in the context of the Hypertext Transfer Protocol (HTTP), which is the foundation of data communication on the World Wide Web. Here are key points about port 80 and its association with HTTP.

**HTTP (Hypertext Transfer Protocol):**

HTTP is the primary protocol used for transmitting and receiving information on the World Wide Web. It defines how messages are formatted and transmitted between web browsers and web servers.

**Default Port:**

Port 80 is the default port for unencrypted HTTP traffic. When a user enters a URL into a web browser without specifying a port number, the browser automatically assumes port 80 for HTTP.

**HTTP Traffic:**

Web browsers use port 80 to establish connections with web servers when retrieving web pages, images, or other resources. The communication is in plaintext, making it susceptible to interception if not encrypted.

**SCOPE OF TESTING**

A hand holding a glowing circle with text

Description automatically generated

The scope of testing for HTTP port 80 involves a thorough examination of the web server and its interactions with clients over the HTTP protocol. This testing is essential for ensuring the security, performance, and proper functioning of web applications. Here are key areas within the scope of testing for HTTP port 80:

Security Testing:

Vulnerability Scanning: Conduct vulnerability scans to identify potential security weaknesses, misconfigurations, and known vulnerabilities in the web server and its associated applications.

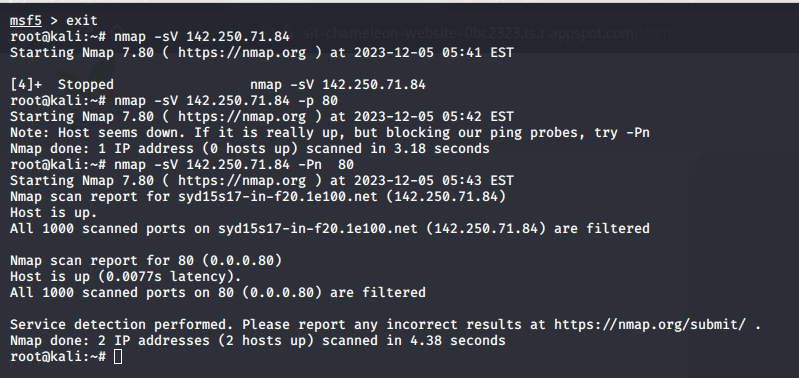
Penetration Testing: Perform penetration testing to simulate attacks and assess the security posture of the web server. This includes testing for common vulnerabilities like SQL injection, cross-site scripting (XSS), and security misconfigurations.

HTTP Methods and Headers:

HTTP Methods Testing: Verify that the web server handles common HTTP methods (GET, POST, PUT, DELETE) appropriately and securely.

Header Analysis: Examine HTTP headers for proper configuration, including security headers such as Content Security Policy (CSP) and HTTP Strict Transport Security (HSTS)

**RESULTS**

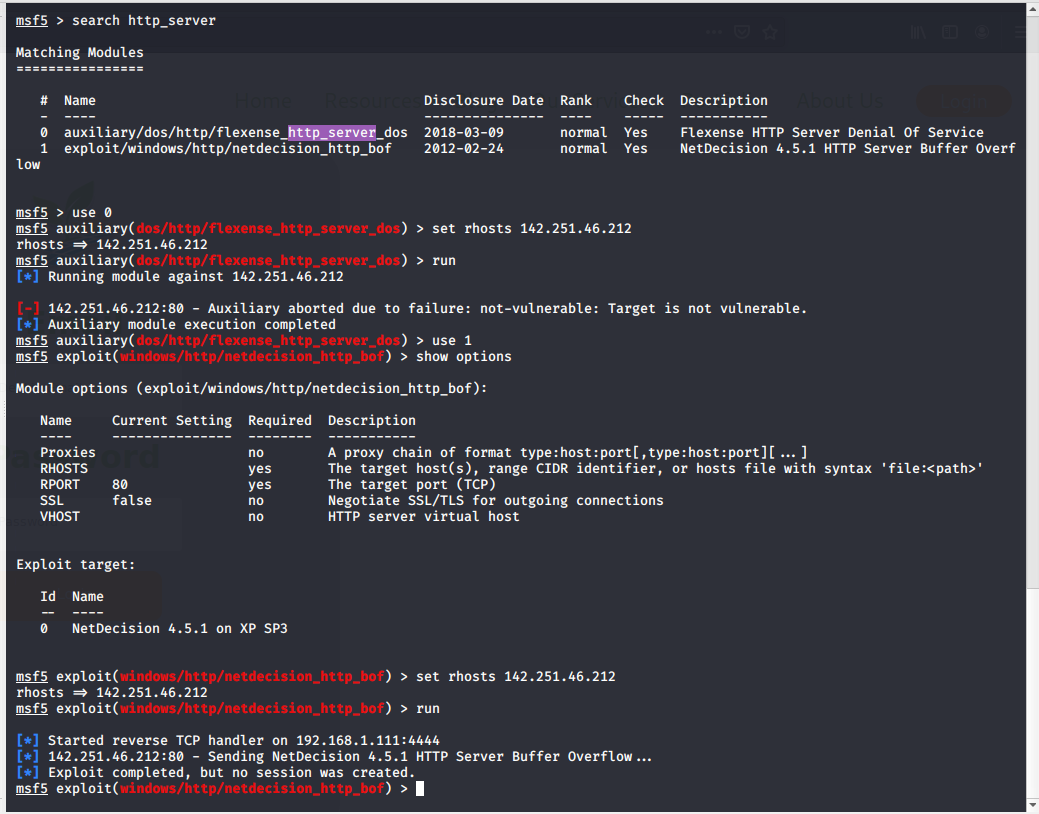


A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

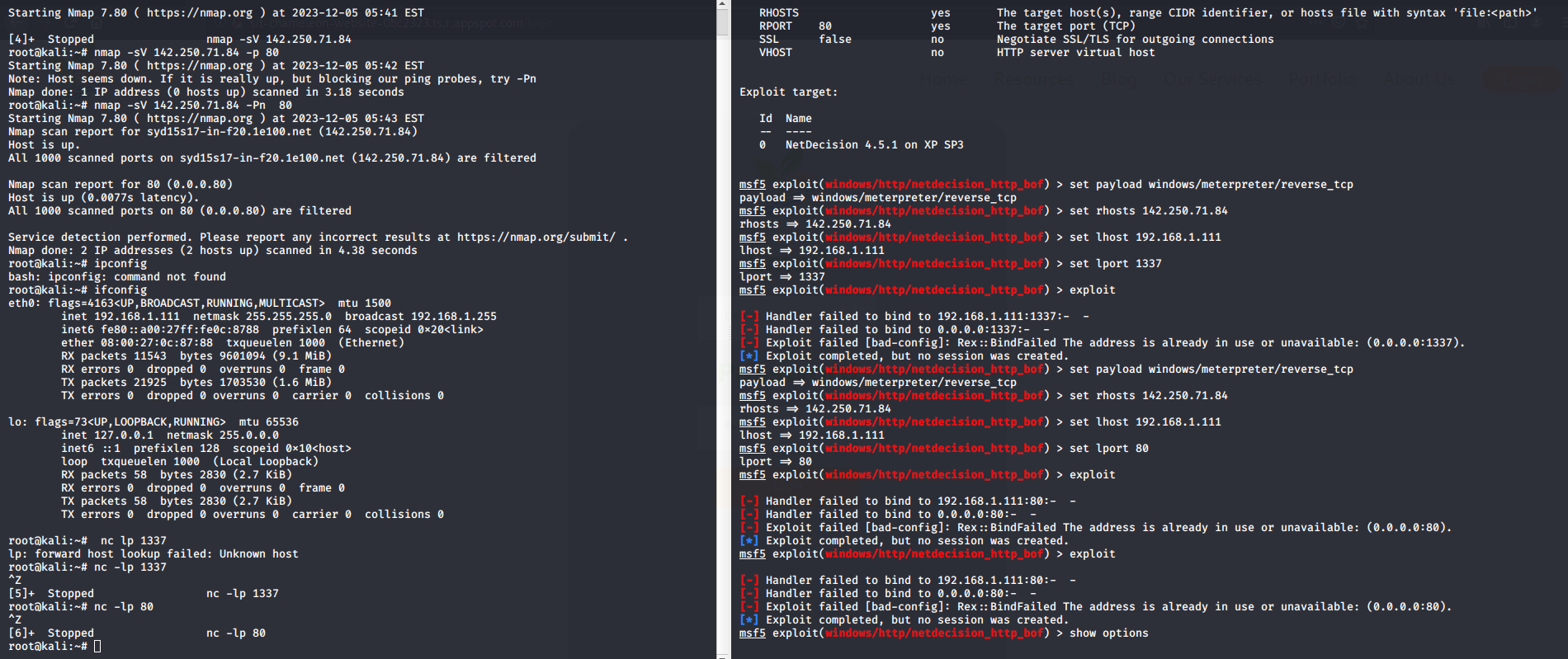


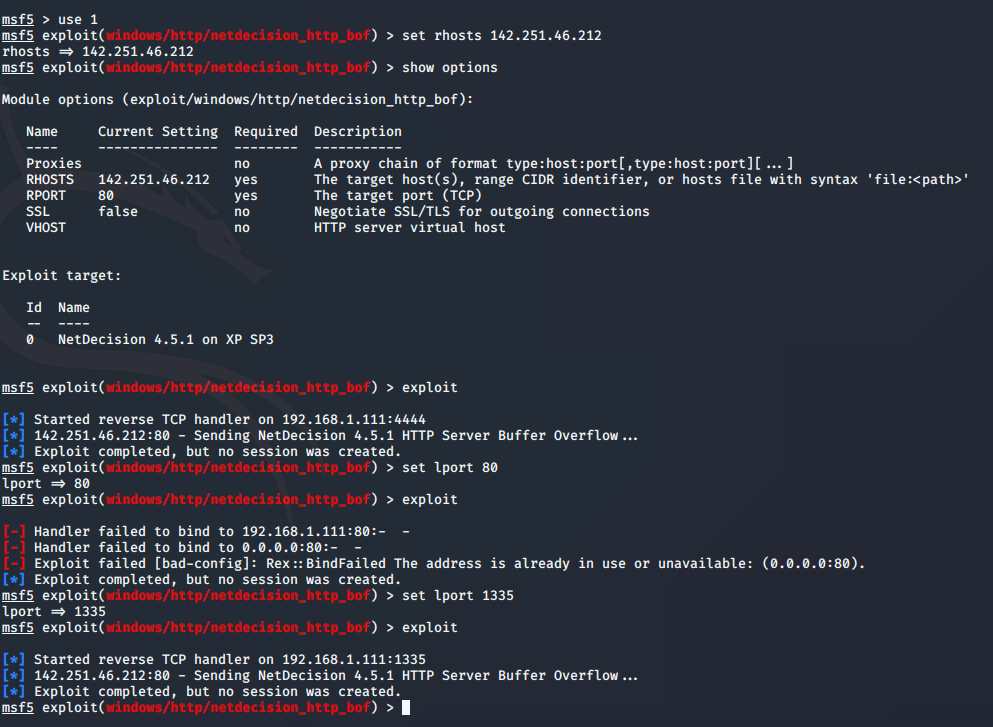
A screen shot of a computer screen

Description automatically generated

**A screenshot of a computer

Description automatically generated**

****

****

IN THE HTTP -80 WHICH IS THE OPNE PORT OF THE CHAMELOEN WEBISTE I HAVE USED THE METAPLOITBLE AND IT CAN BE SEEN FROM THE ABOVE SCREENSHOTS AS WELL.

**CONCLUSION**

On the other hand, the TCP protocol offers an HTTP connection via Port 80. This port allows for an unencrypted connection between the web browser and the web servers, leaving private user information vulnerable to hackers and possibly resulting in serious data misuse. In the event of a data breach, HTTPS Port 443 provides encrypted communication between the web browser and web server, rendering the data unreadable. Therefore, for web browsing, establishing a secure HTTP Port 80 connection is clearly inferior to connecting through HTTPS Port 443.

REFERENCES-

1- SSL2BUY. (n.d.). *Port 80 (HTTP) vs. Port 443 (HTTPS): Everything You Need to Know*. [online] Available at: https://www.ssl2buy.com/wiki/port-80-http-vs-port-443-https#:~:text=Conclusion.

‌