VULNERABILITY ASSESSMENT REPORT

Project Title: Comprehensive Cybersecurity Threat Detection and Incident Response

Report Date: 14th Dec, 2024

Prepared By: Orji Ngozi Vivian

Contact Information: orjivivian@gmail.com |

https://www.linkedin.com/in/ngozi-vivian-orji

CONFIDENTIALITY STATEMENT

This report and its contents are confidential and intended solely for academic purposes. Unauthorized use, reproduction, or dissemination of this report is strictly prohibited. The findings, conclusions, and recommendations in this report, prepared by Orji Ngozi Vivian are based on a simulated cybersecurity assessment. Any misuse of this information is against ethical and professional standards.

TABLE OF CONTENTS

Executive Summary

This project simulates a cybersecurity incident to enhance practical threat detection and response skills. It focuses on identifying vulnerabilities in a controlled environment using network scanning tools: Nmap and Nessus. It also analyzes the scan with tools like Netcat, enum4linux, and smbclient, followed by remediation strategies to address critical risks.

The assessment identified several vulnerabilities, from open ports exposing critical services to high-severity misconfigurations. This report provides actionable recommendations to mitigate risks.

The most critical vulnerabilities identified were outdated operating systems and the high possibility of uploading malicious files. Immediate action is recommended to address the vulnerabilities and mitigate risk.

Additionally, SQL injection, unprivileged access, and buffer overflow are high-risk activities that should be prevented.

To enhance Stapler 1’s overall security, implement a vulnerability management program, conduct regular security assessments, and prioritize patch management. The application can better withstand attacks by following secure coding practices and implementing strong access controls.

Please note that the overall business impact of the identified vulnerabilities was not assessed in this report. It is recommended to perform a detailed risk assessment, taking into account specific business factors, to prioritize remediation efforts effectively.

Implementing the recommended measures will enhance Stapler 1's security posture, safeguarding data and improving user safety.

1. Technical Summary

1.1 Scope

The scope of this project includes:

Setting up a controlled network environment using virtual machines: Stapler 1 (vulnerable system) which was done in VirtualBox.

Nmap Scanning was performed to check for open ports and services running in the Stapler 1 machine. Also, a Nessus scan was conducted to identify possible vulnerabilities in Stapler 1.

Possible remediation was provided to mitigate the risk of exploitation.

1.2 Risk Ratings

To ensure clarity and consistency in evaluating vulnerabilities, the following risk levels and colors were applied based on the industry-standard framework called CVSS(Common Vulnerability Scoring System). It is important to note that assessing the business impact of these risks is beyond the scope of this report. Therefore some issues that may be considered highly or critically vulnerable from the technical perspective, may be acceptable in the organization risk based on the tolerance or migration that has been put in place.

RISK LEVEL	DESCRIPTION	CVSSV3 SCORE
Low Risk	Indicates a vulnerability or issue with minimal impact that can be easily mitigated.	**0.0 – 3.9**
Medium Risk	Indicates a vulnerability or issue with a moderate impact that requires more effort to address and mitigate.	**4.0 – 6.9**
High Risk	Indicates a vulnerability or issue with a significant threat to security that requires immediate attention and remediation.	**7.0 – 8.9**
Critical Risk	Indicates a vulnerability with the highest severity and imminent threat requiring urgent action.	**9.0 – 10.0**

1.3 Findings Overview

Below are the findings obtained from running the Nmap scan and Nessus. These findings will be covered in detail in Technical Details.

Result Summary from Nmap Scan:

Findings #	Open Ports	Services	Versions
1	21	FTP	Vsftpd 2.0.8 or later
2	22	ssh	OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
3	53	domain	dnsmasq 2.75
4	80	HTTP	PHP cli server 5.5 or later
5	139	NetBIOS-ssn	Samba smbd 4.3.9-Ubuntu
6	666	Doom?	
7	3306	MySQL	MySQL 5.7.12-0ubuntu1
8	12380	HTTP	Apache httpd 2.4.18

Result Summary from Nessus Scan:

Focusing on reporting the critical and high vulnerabilities because they need urgent attention.

FINDINGS #	VULNERABILITIES	RISK
1	Canonical Ubuntu Linux SeoL (16.04.x)	CRITICAL
2	MySQL 5.7.x < 5.7.36 Multiple Vulnerabilities (Oct 2021 CPU)	CRITICAL
3	Ubuntu 16.04 to 24.04 ESM and LTS vulnerabilities	CRITICAL
4	phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities	CRITICAL
5	phpMyAdmin prior to 4.8.6 SQLi vulnerability	CRITICAL
6	Microsoft Windows SMB Shares Unprivileged Access	HIGH
7	MySQL 5.7.x < 5.7.35 Multiple Vulnerabilities (Jul 2021 CPU)	HIGH

8	phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)	HIGH
9	CGI Generic SQL Injection (blind)	HIGH

2. Technical Details

2.1. Setup and Reconnaissance

2.1.1. Environment Setup:

A network environment was created using VirtualBox. I downloaded the stapler Zip file from https://www.vulnhub.com/entry/stapler-1,150/

2.1.2. Reconnaissance:

Information gathered using Nmap.

Stapler 1 (A vulnerable Linux system):

The IP address was determined by running:

sudo nmap -sn -n 10.0.2.0/24

From the output, the IP address is 10.0.2.13.

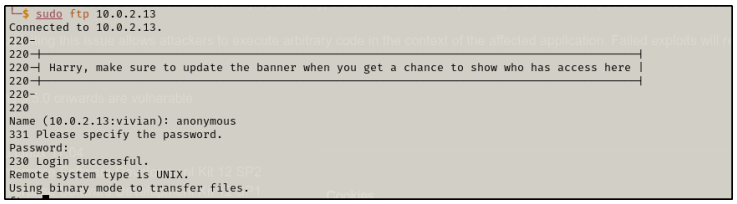
Next, a Nmap scan was performed to discover common ports and services running.

sudo nmap -p- -A 10.0.2.13

1. **Ftp (21):** File transfer protocol is a network protocol used for the transfer of files between a client and a server over a network.

   Information gathered from the Nmap scan shows that ftp is running on port 21. Ftp service allows for anonymous login and allows easy/fast download or upload of files. Files, commands, and credentials can be transmitted without encryption.

   I was able to connect to ftp as an anonymous user.



   I reviewed the data available in FTP and discovered a note file, which I downloaded.

```
ftp> ls -la
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jun 04  2016 .
drwxr-xr-x    2 0        0            4096 Jun 04  2016 ..
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp>
```

```
ftp> get note
local: note remote: note
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
100% |*****************************************|   107       2.85 KiB/s    00:00 ETA
226 Transfer complete.
107 bytes received in 00:00 (2.57 KiB/s)
```

```
└─$ cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your
 are done, John.
```

From the above information, three names were gathered: Harry, Elly, and John.

Potential Vulnerabilities: 1. FTP is outdated and linked to known vulnerability exploits (see resources for links).

2. Files can be uploaded or downloaded easily, making them vulnerable to exploitation because malicious actors can decide to alter the file or upload malware.

Recommendations: 1. Ensure regular patching and updating of the service version to avoid being exploitable.

2. If possible close the port or restrict access to only authorized users.

2. **Netbios-ssn(139):** It is a service that operates over TCP/IP protocol used for file sharing, printer sharing, and other network services in Microsoft Windows-based networks. Stapler1 is using samba. Samba allows Unix/Linux systems to interact with Windows systems seamlessly, implementing Server Message Block(SMB).

   Running a searchsploit shows there is a possibility of is_known_pipename exploitation.

```
┌──(vivian㉿kali)-[~]
└─$ sudo searchsploit Samba 4.
---------------------------------------------------------------- ---------------------------------
 Exploit Title                                                  |  Path
---------------------------------------------------------------- ---------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasp | osx/remote/9924.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Sh | linux/local/23674.txt
Samba 3.0.4 - SWAT Authorisation Buffer Overflow        | linux/remote/364.pl
Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy AuditE | linux/remote/21850.rb
Samba 3.4.5 - Symlink Directory Traversal               | linux/remote/33599.txt
Samba 3.4.5 - Symlink Directory Traversal (Metasploit)  | linux/remote/33598.rb
Samba 3.4.7/3.5.1 - Denial of Service                   | linux/dos/12588.txt
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename( | linux/remote/42084.rb
Samba 3.5.11/3.6.3 - Remote Code Execution              | linux/remote/37834.py
Samba 3.5.22/3.6.17/4.0.8 - nttrans Reply Integer Overf | linux/dos/27778.txt
Samba 4.5.2 - Symlink Race Permits Opening Files Outsid | multiple/remote/41740.txt
Sambar FTP Server 6.4 - 'SIZE' Remote Denial of Service | windows/dos/2934.php
Sambar Server 4.1 Beta - Admin Access                   | cgi/remote/20570.txt
Sambar Server 4.2 Beta 7 - Batch CGI                    | windows/remote/19761.txt
Sambar Server 4.3/4.4 Beta 3 - Search CGI               | windows/remote/20223.txt
Sambar Server 4.4/5.0 - 'pagecount' File Overwrite      | multiple/remote/21026.txt
Sambar Server 4.x/5.0 - Insecure Default Password Prote | multiple/remote/21027.txt
Sambar Server 5.x - Information Disclosure              | windows/remote/22434.txt
Sambar Server 5.x/6.0/6.1 - 'results.stm' indexname Cro | windows/remote/25694.txt
```

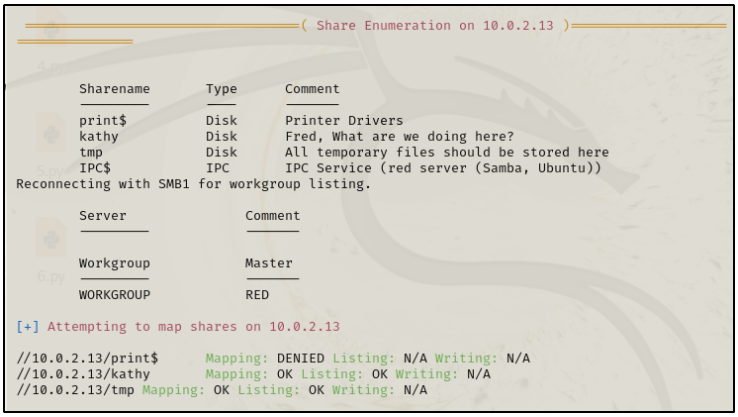
Now, using smbclient and enum4linux to enumerate for shares, users, and groups.

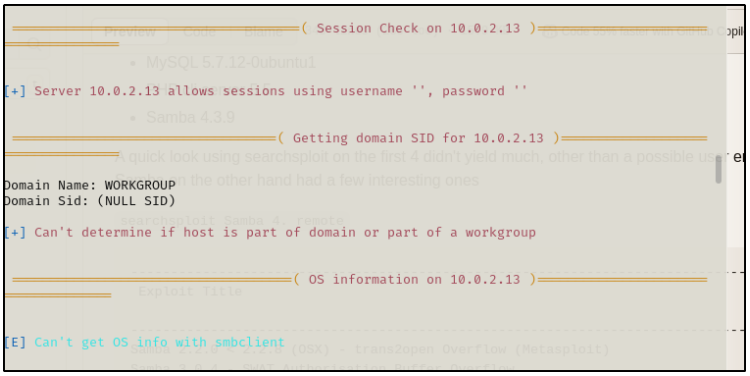
First, smbclient was used to list the shares by logging in with the password “root”.

```
└─$ sudo smbclient -L //10.0.2.13
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            RED
```

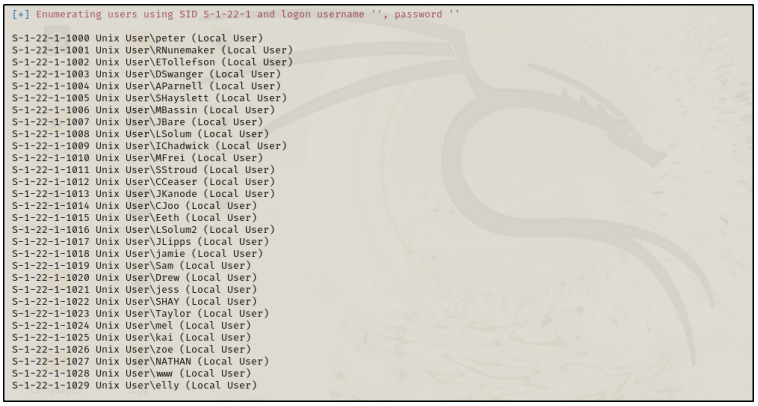
Enum4linux was used to display information on shares, users, OS, and groups.

```
└─$ sudo enum4linux -a 10.0.2.13
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon
 Dec 16 13:17:15 2024

 =========================================( Target Information )=========================================

Target ........... 10.0.2.13
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.0.2.13 )============================


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 10.0.2.13 )================================
```


(Share Enumeration on 10.0.2.13)
Sharename Type Comment
print$ Disk Printer Drivers
kathy Disk Fred, What are we doing here?
tmp Disk All temporary files should be stored here
IPC$ IPC IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
WORKGROUP RED
[+] Attempting to map shares on 10.0.2.13
//10.0.2.13/print$ Mapping: DENIED Listing: N/A Writing: N/A
//10.0.2.13/kathy Mapping: OK Listing: OK Writing: N/A
//10.0.2.13/tmp Mapping: OK Listing: OK Writing: N/A


(Session Check on 10.0.2.13)
[+] Server 10.0.2.13 allows sessions using username '', password ''
(Getting domain SID for 10.0.2.13)
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
(OS information on 10.0.2.13)
[E] Can't get OS info with smbclient

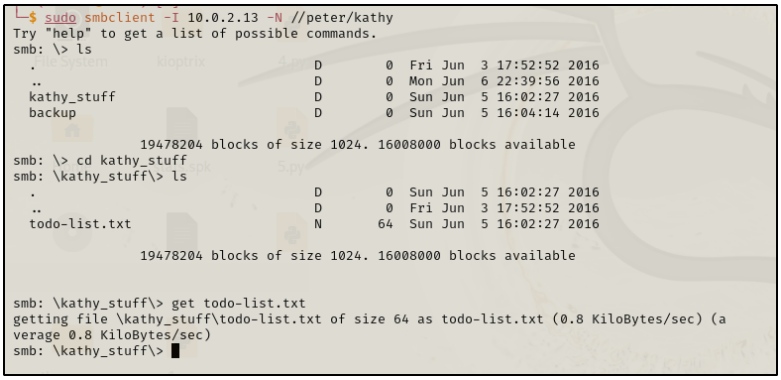

(OS information on 10.0.2.13)
[E] Can't get OS info with smbclient
[+] Got OS info for 10.0.2.13 from srvinfo:
RED Wk Sv PrQ Unx NT SNT red server (Samba, Ubuntu)
platform_id : 500
os version : 6.1
server type : 0x809a03

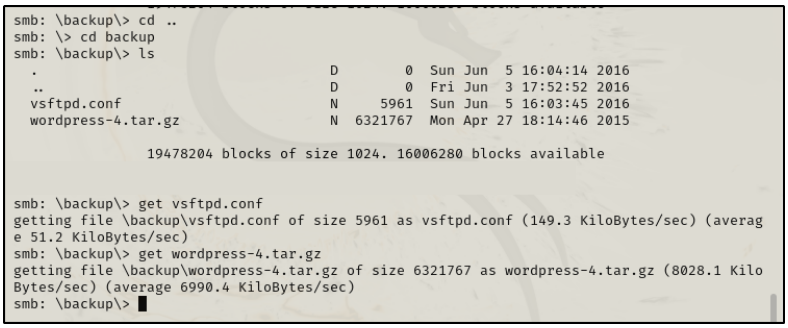

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\ww (Local User)
S-1-22-1-1029 Unix User\elly (Local User)


[+] Enumerating users using SID S-1-5-21-864226560-67800430-3082388513 and logon username '', password ''
S-1-5-21-864226560-67800430-3082388513-501 RED\nobody (Local User)
S-1-5-21-864226560-67800430-3082388513-513 RED\None (Domain Group)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
(Getting printer info for 10.0.2.13)
No printers returned.

With the above result, try logging into all the shares using one of the usernames and no password options.

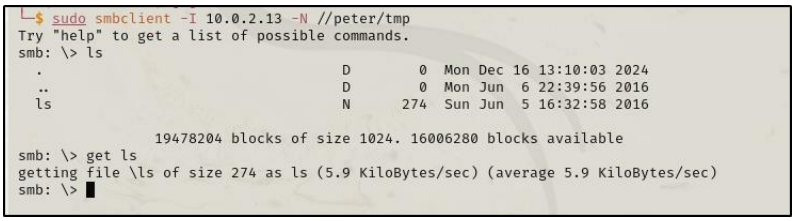
Let’s start with Kathy:

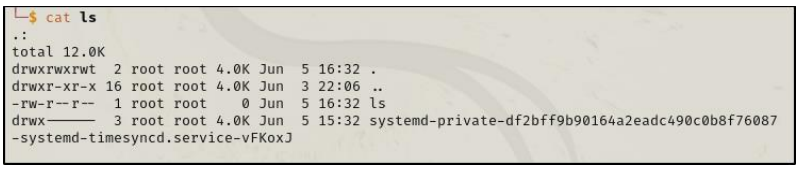




The WordPress-4.tar.gz contains lists of WordPress websites, the todo-list contains the text “I'm making sure to backup anything important for Initech, Kathy”, while vsftpd.conf contains information about ftp server.

Now let’s check the tmp share:





This displays some content in the root directory.

Potential Vulnerabilities: 1. The service version is outdated and it is associated with some known attacks (links to the known attacks listed in the resources section).

2. It allows read and write access, which attackers can exploit to modify or upload malicious data.

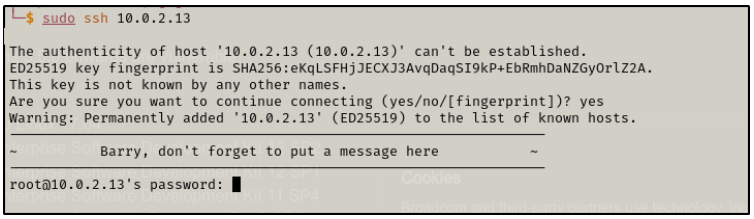
Recommendations: 1. Update the service version to the latest version to help mitigate the risk of attack.

2. Restrict shared access to only authorized users.

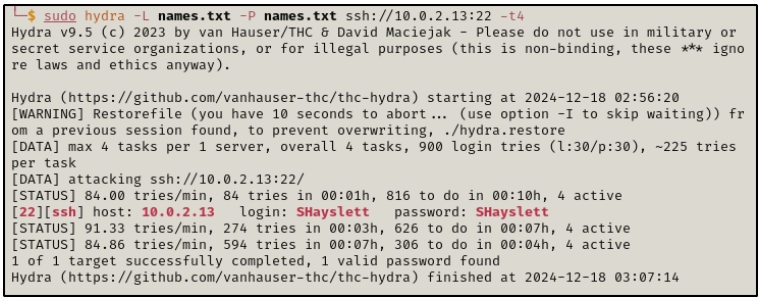
3. **SSH (22):** A secure shell is a protocol that allows for secure remote access between two computers over an unsecured network.

From the Nmap scan it shows that it is using OpenSSH 7.2p2 Ubuntu 4 and uses SSH hotkeys.

When I try to connect to SSH, it takes me to a login page, asking for a password which I don't have access to. So I was not able to log in.



I ran a brute force attack using the list of users provided from my findings above.



I logged in and went through the account and couldn't find anything of interest.

Possible vulnerabilities: 1. Outdated OpenSSH version which is known to link to known vulnerabilities.

2. Brute force attack due to weak credentials and exposed credentials.

3. Attackers can impersonate the server if the host keys are weak/ compromised.

Recommendations: 1. Ensure regular updates and patching of service.

2. Use an Intrusion Detection System (IDS) to monitor SSH traffic and mitigate brute-force attacks.

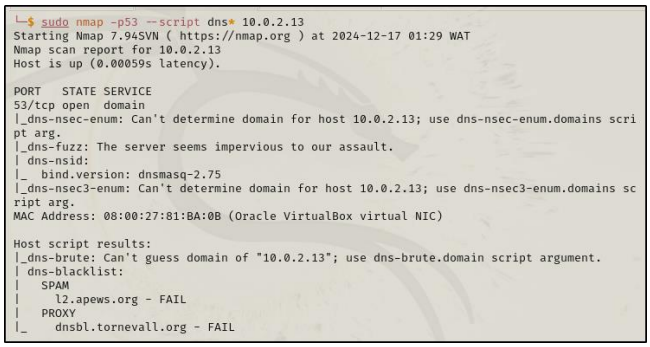
3. Educate employees/ executives on the importance of using standard passwords.

4. Ensure regular regeneration and replacement of the host key.

5. Disable root login access and use key-based access instead of password.

4. **Domain (53):** A Domain Name System (DNS) is used to translate human-readable domain names into IP addresses that the computer understands and can use to communicate across networks and the internet.

   From the Nmap scan, bind. The version indicates that it is responding to dnsmasq-2.75.



   There isn't anything of interest found.

   Possible Vulnerabilities: The service version is outdated and it is known to be associated with known vulnerabilities like heap-based buffer overflow attacks.

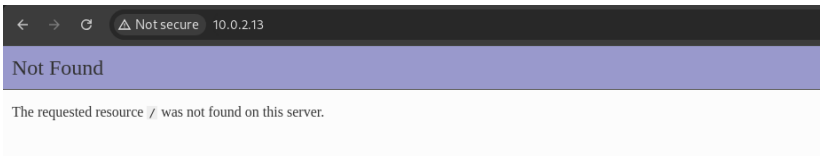
   Recommendations: 1. Close the port or restrict access to only authorized users.

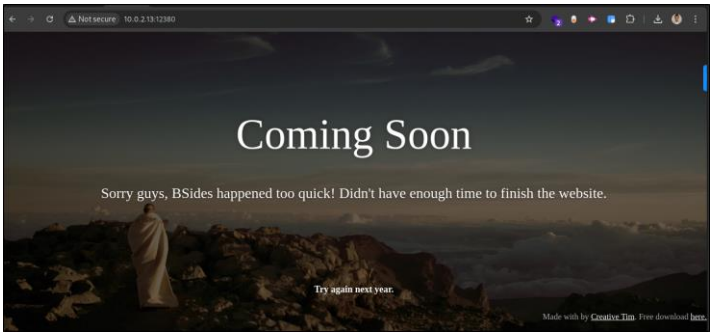
   2. Ensure regular updates and patching of service.

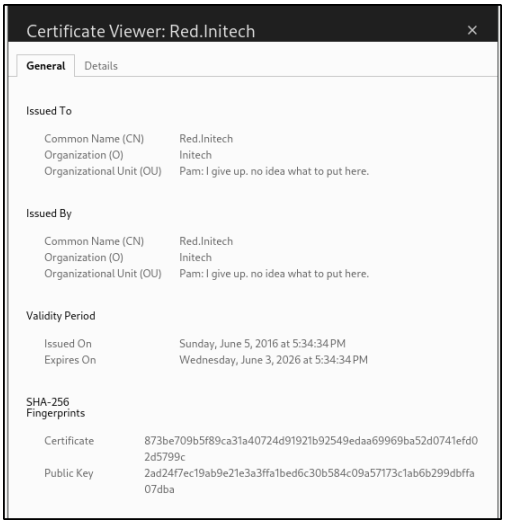
5. **Http (80/12380):** Hypertext Transfer Protocol is a protocol for worldwide web use to communicate between a client and a server.

   From the Nmap scan, port 80 is using PHP CLI server 5.5 or later and port 12380 is using Apache httpd 2.4.18.

On my browser when I inputed http://10.0.2.13, http://10.0.2.13:12380, https://10.0.2.13:12380 I got







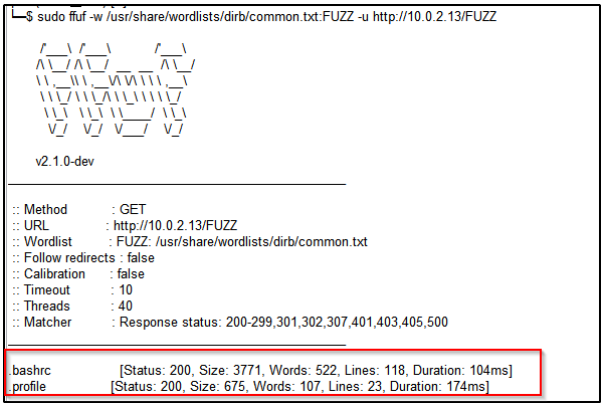
I viewed the source code of port 80 and didn't get anything interesting but port 12380 showed some names "Tim, Zoe".

Then, I decided to run a ffuf scan to check for the possibilities of other directories that might be available.

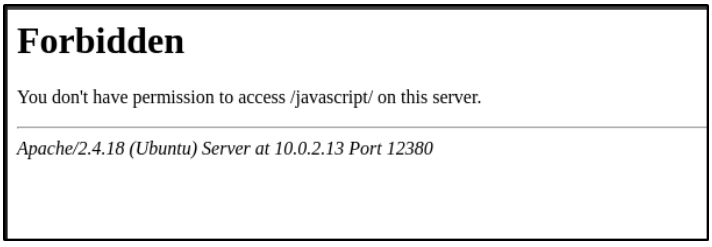
http://10.0.2.13 showed two downloadable files but nothing of interest was found in it.

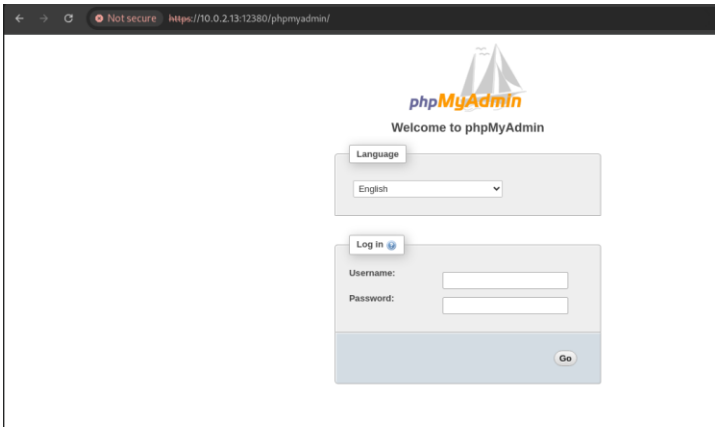
http://10.0.2.13:12380 didn't have any known directory.

https://10.0.2.13:12380 has some directories.

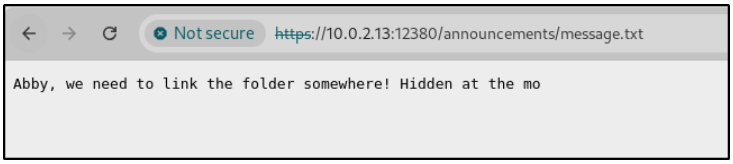


Output of other directories in https://10.0.2.13:12380

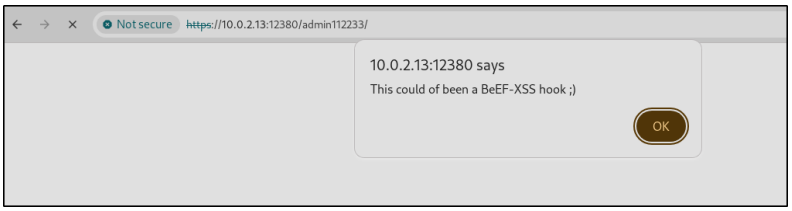


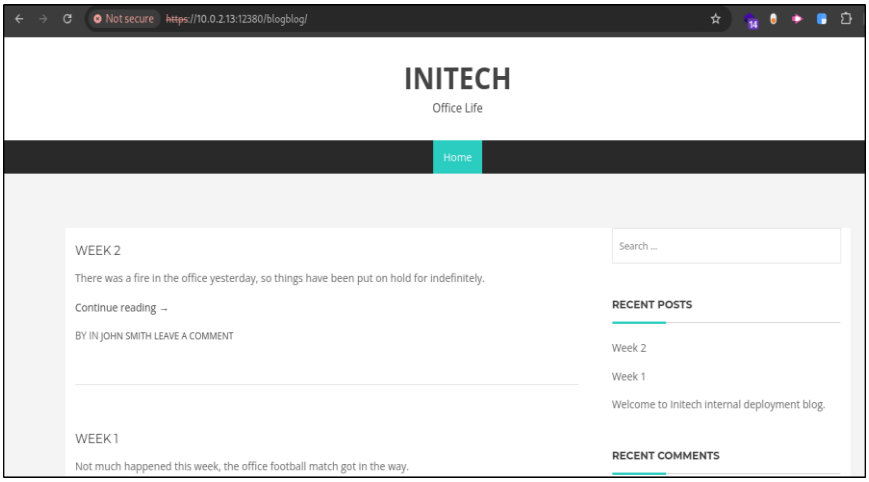

Not secure https://10.0.2.13:12380/phpmyadmin/
phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Username:
Password:
Go


Not secure https://10.0.2.13:12380/announcements/
Index of /announcements
Name Last modified Size Description
Parent Directory -
message.txt 2016-06-04 00:10 61
Apache/2.4.18 (Ubuntu) Server at 10.0.2.13 Port 12380


Not secure https://10.0.2.13:12380/announcements/message.txt
Abby, we need to link the folder somewhere! Hidden at the mo


Not secure https://10.0.2.13:12380/robots.txt
User-agent: *
Disallow: /admin112233/
Disallow: /blogblog/


Not secure https://10.0.2.13:12380/admin112233/
10.0.2.13:12380 says
This could of been a BeEF-XSS hook ;)
OK

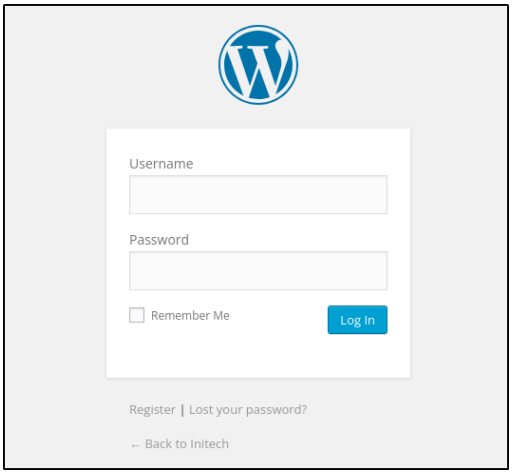


The SSL certificate for https://10.0.2.13 is insecure.

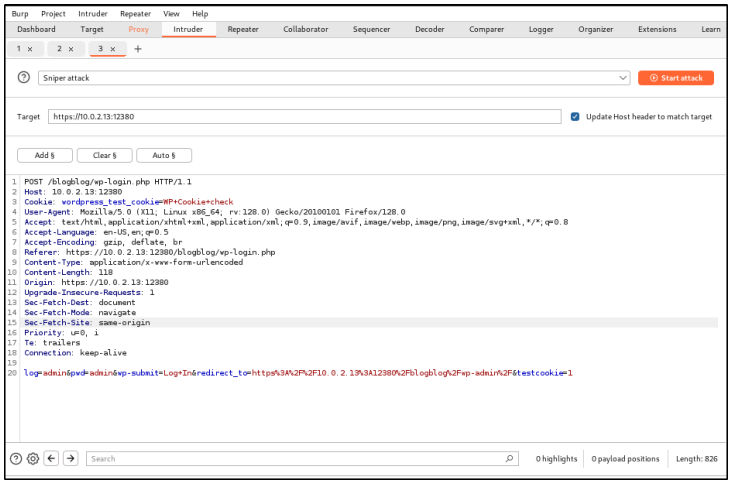
Out of all the pages, https://10.0.2.13/blogblog seems to have some interesting directories.

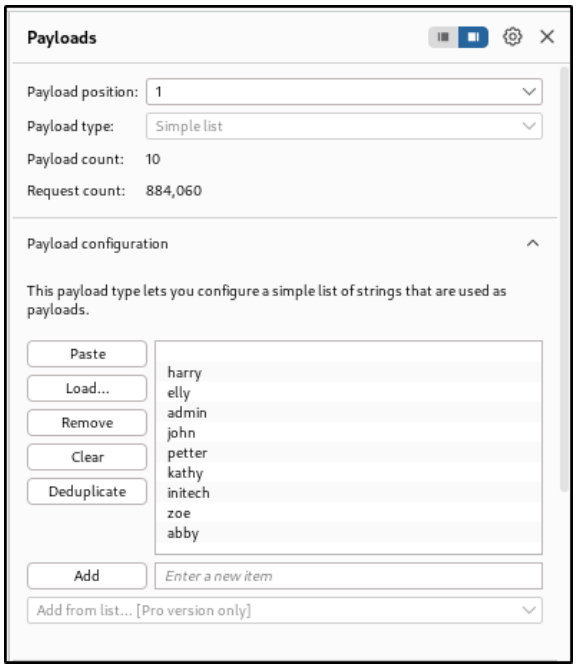
It contains a link to a register page which prompts you to input a username and an email. Once you click send, it sends a popup message indicating the password being sent to your email but it doesn't send anything.

It also contains a login page and some other pages.

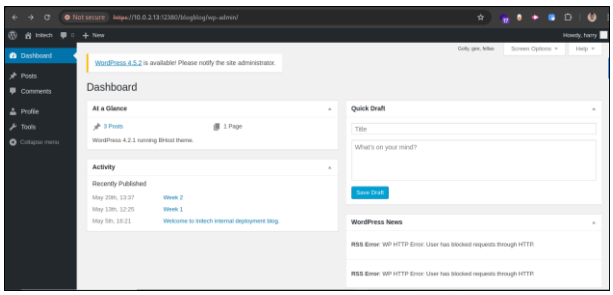


I ran a dictionary brute force attack on the login page using Burp Suite. I use some of the disclosure names from earlier findings and word lists.





Some login credentials were found and was able to log in.



Possible Vulnerabilities: 1. The service is outdated.

2. Weak passwords allowed for brute force attacks.

3. HTTP is not secured and data can be stolen easily.

4. Links disclosing sensitive information were found.

5. Use of false SSL certificate.

Recommendations: 1. Switch all communications to HTTPS to ensure secure data transmission.

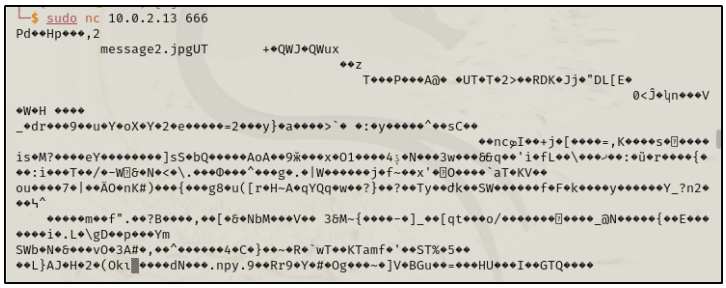
2. Update the PHP version to the latest version.

3. Restrict directory listing.

4. Restrict access to sensitive data to authorized users only.

6. **Port 666:** Nmap was not able to tell for sure what service and version is running. It guessed it was a doom service.

   Manual connection to the port using Netcat. This outputs a result that indicates it is listening but the message is encrypted.



I saved the file and extracted its contents.

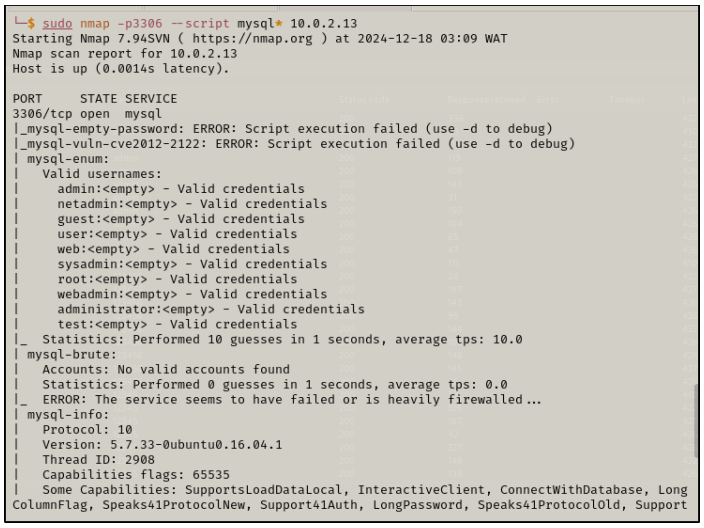
The above image shows that there is an image file called message2.jpg. Which displays:

Possible Vulnerability: It allows for the download of files that can be exploited.

Recommendation: Close unnecessary open ports to reduce the attack surface and prevent exploitation.

7. **MySQL (3306):** MySQL uses structured query language(SQL) to manage and organize data in a structured manner.

From the Nmap scan, MySQL is using MySQL 5.7.12-0ubuntu1.



```
└─$ sudo nmap -p3306 --script mysql* 10.0.2.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 03:09 WAT
Nmap scan report for 10.0.2.13
Host is up (0.0014s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
| mysql-enum:
|   Valid usernames:
|     admin:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     root:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
| mysql-info:
|   Protocol: 10
|   Version: 5.7.33-0ubuntu0.16.04.1
|   Thread ID: 2908
|   Capabilities flags: 65535
|   Some Capabilities: SupportsLoadDataLocal, InteractiveClient, ConnectWithDatabase, Long
ColumnFlag, Speaks41ProtocolNew, Support41Auth, LongPassword, Speaks41ProtocolOld, Support
```

Possible Vulnerabilities: 1. The service version is outdated and known to be associated with known vulnerabilities.

2. Possible brute force attack due to disclosure of username and the fact that is using a native password plugin.

3. Autocommit is enabled, meaning changes are committed immediately, increasing the risk of accidental or unauthorized modifications.

4. The salt is exposed, which, when combined with a weak password, increases the likelihood of brute-force attacks on the password hash.

Recommendations: 1. Ensure regular updates and patches of the service.

2. Restrict access to MySQL (Port 3306) to only authorized users through proper firewall rules.

3. Educate users on the importance of creating standard passwords and implement a policy enforcing strong password rules.

4. Enable and monitor MySQL logs, such as error logs and slow query logs, to identify suspicious activity.

2.1.3. Nessus scan report:

The report contains information about the critical and high-risk level vulnerabilities. For detailed information about the vulnerabilities, refer to the resources section.

VULNERABILITIES	DESCRIPTIONS	RISK	RECOMMENDATIONS
Canonical Ubuntu Linux SeoL (16.04.x)	Canonical Ubuntu Linux is 16.04.x.no longer maintained by its vendor or provider. This is vulnerable because the vendor no longer provides security patches for this version.	CRITICAL	Upgrade to a version of Canonical Ubuntu Linux that is currently supported.
MySQL 5.7.x < 5.7.36 Multiple Vulnerabilities (Oct 2021 CPU)	This version of MySQL is affected by multiple vulnerabilities, which include OpenSSL component vulnerabilities that take over the MySQL server, InnoDB component vulnerability that allows a highly privileged attacker to affect the integrity and availability of the MySQL Server, cURL component vulnerabilities that allow an unauthenticated, remote attacker to affect the availability of the MySQL Server.	CRITICAL	Upgrade to MySQL version 5.7.36 or later. Ensure regular patching.
Ubuntu 16.04 to 24.04 ESM and LTS vulnerabilities	It contains commands, software libraries, and tools that are vulnerable. Some of these include Linux kernel, python, Apache HTTP server, curl, OpenSSH, OpenSSL, klibc, git, wget, PHP, and libpng. The vulnerabilities are linked to multiple CVEs, highlighting risks such as resource exhaustion, bypassing security mechanisms, and sensitive data exposure.	CRITICAL	Update the affected package.

phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities	It can cause SQL injection due to improper validation of user-supplied input. Also when the AllowArbitraryServer configuration setting is set to true it affects the arbitrary file. This could lead to reading arbitrary files and disclosing sensitive information.	CRITICAL	Upgrade to phpMyAdmin version 4.8.5 or later. Alternatively, apply the patches referenced in the vendor advisories.
phpMyAdmin prior to 4.8.6 SQLi vulnerability	It is affected by a SQL injection (SQLi) vulnerability that exists in the designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.	CRITICAL	Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories.
Microsoft Windows SMB Shares Unprivileged Access	Windows shares that can be accessed through the network with the given credentials.	HIGH	To restrict access in Windows, open Explorer, right-click on each share, go to the 'Sharing' tab, and adjust the 'Permissions' settings.
MySQL 5.7.x < 5.7.35 Multiple Vulnerabilities (Jul 2021 CPU)	The versions are vulnerable to a heap-based buffer overflow and suffer from user-after-free vulnerabilities. This could lead to remote code execution, corruption of data, and DoS attacks.	HIGH	Upgrade to MySQL version 5.7.35 or later.
phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)	It is affected by a SQL injection (SQLi) vulnerability in the user accounts page. An authenticated, remote attacker can exploit this, by injecting custom SQL in place of their own username, to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.	HIGH	Upgrade to phpMyAdmin version 4.9.4, 5.0.1, or later. Alternatively, apply the patches referenced in the vendor advisories.
CGI Generic SQL Injection (blind)	Nessus identified that specially crafted parameters sent to CGI scripts could modify application behavior and directly access the database. An attacker may be able to exploit this issue to	HIGH	Modify the affected CGI scripts so that they properly escape arguments.

	bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.		

3. Conclusion

The vulnerabilities identified during this simulation highlight significant risks in the Stapler 1 system. Immediate remediation actions, including patching, configuration updates, and access control enhancements, are recommended to prevent potential exploitation. These measures, if implemented effectively, will strengthen the security of the environment.

4. Appendices

4.1 Appendix A: Detailed Methodology

Tools Used:

Nmap for network reconnaissance.

Burp suite and hydra for brute force attack.

Ffuf for directory findings.

Netcat for testing network connections.

Enum4linux for samba enumerations.

Nessus for vulnerability assessment.

Steps Taken:

Setup of virtual machines in a NAT network configuration.

Scanning for open ports and services using Nmap.

Scanning for vulnerabilities with Nessus.

4.2 Appendix B: Resources

Link to view Nmap scan and Nessus scan:

https://drive.google.com/drive/folders/1ltcMCAqAUHOiMjCtGOgrfwGRfVQoeSaY?usp=drive_link

For FTP :

https://www.jscape.com/blog/5-steps-to-a-secure-ftp-server

https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

https://github.com/Hellsender01/vsftpd_2.3.4_Exploit

For SSH:

https://nvd.nist.gov/vuln/search/results?form_type=Advanced&cves=on&cpe_version=cpe:/a:openbsd:openssh:7.2p2

https://www.exploit-db.com/exploits/40136

https://ubuntu.com/security/notices/USN-3538-1

https://vuldb.com/?id.89622

For DNS:

https://askubuntu.com/questions/1310087/how-to-get-the-latest-dnsmasq-version

https://www.cybersecurity-help.cz/vdb/gnu/dnsmasq/2.78/

https://www.exploit-db.com/exploits/42942

https://www.rapid7.com/db/vulnerabilities/dnsmasq-cve-2017-14491/

For HTTP:

https://www.tenable.com/plugins/nessus/76772

https://www.exploit-db.com/exploits/36251

https://gist.github.com/chrisjsimpson/3490250

For Samba:

https://www.rapid7.com/db/modules/exploit/linux/samba/is_known_pipename/

https://www.exploit-db.com/exploits/42084

https://www.samba.org/samba/security/CVE-2017-7494.html

For MySQL:

https://www.exploit-db.com/exploits/40679

https://security.snyk.io/package/linux/ubuntu%3A16.04/mysql-5.7

https://github.com/canonical/ubuntu-security-notices/blob/main/osv/cve/2024/UBUNTU-CVE-2024-21230.json