**Pentest Report on 192.168.1.100**

Ashutosh Joshi- (A20438752)

Vulnerability Analysis and Ctrl

Illinois Institute of Technology

Date: 12/10/2020

**Abstract**

The report contains the methods, approach and the tools for the penetration testing of the provided IP that is 192.168.1.100. When there is a high vulnerability and it can be exploited than I rated its severity as “HIGH” and rated “Medium”, if there is an exploit possible on our target which happens most of the time but there are also some security measures there to protect it from being happening in the first place. And at the last, the “LOW” severity includes some very low security services or features that needs to turn off or running on some different permissions or with extra privileges that needs to be changed to make it more secure machine. The securing involves changing the permission of protected files and apply remediations actions actively.

**Content**

1. Executive Summary
2. Methodology
3. Planning
4. Exploitation
5. Reporting
6. Detailed Finding
7. Threat Level: HIGH
8. Threat Level: Medium
9. Threat Level: Low
10. List of Tools
11. Remediation
12. References

**Executive Summary**

The purpose of the testing was to find the vulnerability in the provided IP, so as to gain better knowledge of the penetration testing and its tools. The target machine details are OS: Windows 6.1 (Samba 4.3.11-ubuntu), Computer name: acme, NetBIOS computer name: ACME\x00, FQDN: acme. The tools used in this penetration testing are Nmap, Nessus and Metasploit. These are the most used tools but it changed according to the problem and the exploits. These tools were able to provide 8 vulnerability to the required target which can be exploited. There were less high-level threats on the target but still had some issues which needs remediations.

I have identified areas where security policy is not being adhered to, this introduces a risk to the organization and therefore we must declare the system as insecure*.*

**Methodology**

1. Planning

My planning for this penetration testing was based upon the results I get from the Nmap and Nessus scans. Which includes the following, like the services which are running on the server, which ports are open and which services the are responding to if any request has been made and at last, I observed the vulnerability provided by these tools and try to exploit them all.

1. Exploitation

Exploitation is done with the help of above planning output obtained. With the help of obtained results are used in Metasploit to execute the payloads for the required services and ports. Metasploit provides variety of attacks and scripts which are used according with the open ports and services.

Metasploit is used in this penetration testing but it depends upon the exploiter approach too. For example, to scan the present directories on the target I used the “Dirbuster” to get the details of all the directory present on the target machine which can be exploited with the help of Metasploit or any preferred tool.

1. Reporting

It involves the testing based on the results. Which appears as low, high and medium.

|  |  |  |
| --- | --- | --- |
| L | LOW | 3 |
| M | MEDIUM | 2 |
| H | HIGH | 3 |

**Detailed Finding**

1. **Threat Level: HIGH**
2. FTP Exploit

Port 21

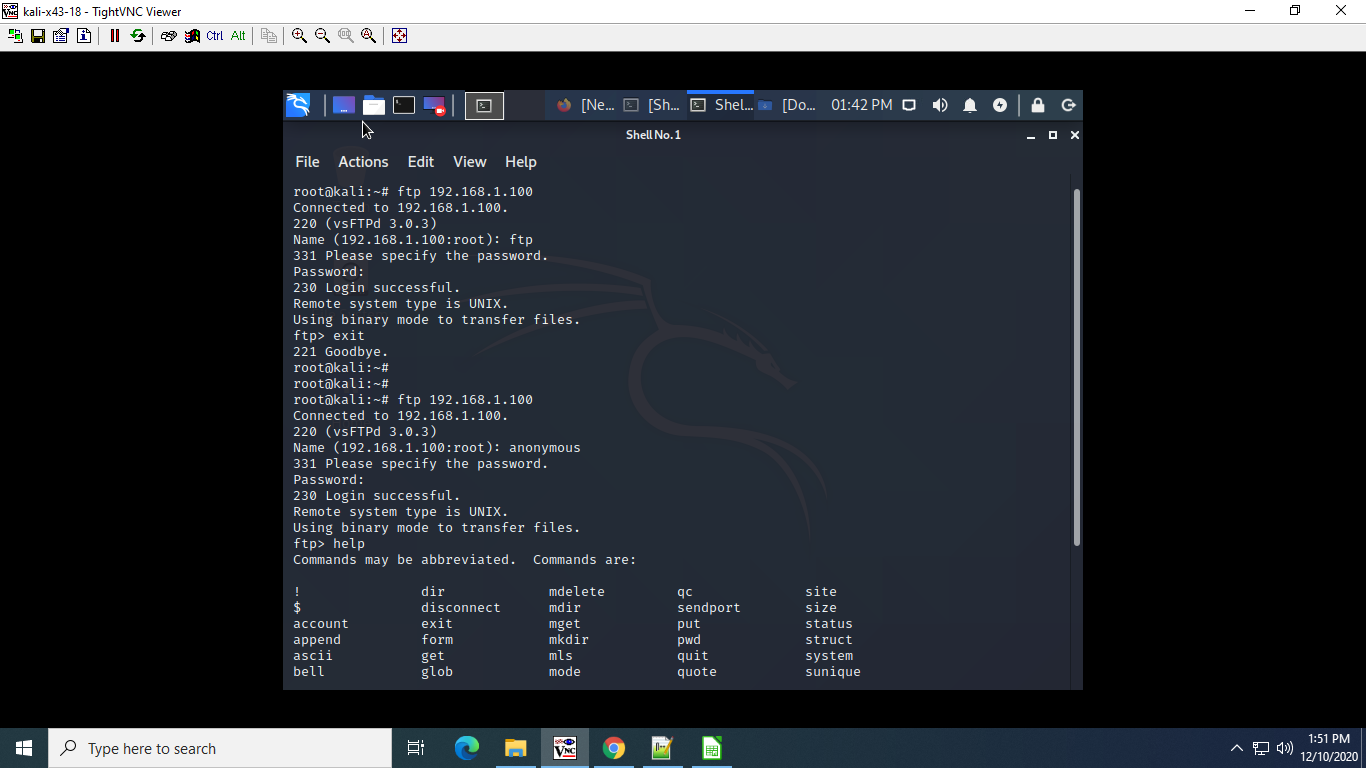
Version: vsftpd 3.0.3

Doing a namp scan on the specific port

Sudo nmap -T4 -p21 -A 192.168.1.100

The result of the scan shows that the FTP logins are allowed with

Anonymous Login allowed



1. Ftp 192.168.1.100

USERNAME: ftp

PASS: anonymous

1. Ftp 192.168.1.100

USER: anonymous

PASS: anonymous

With these credentials I was able to login into the FTP port 21.

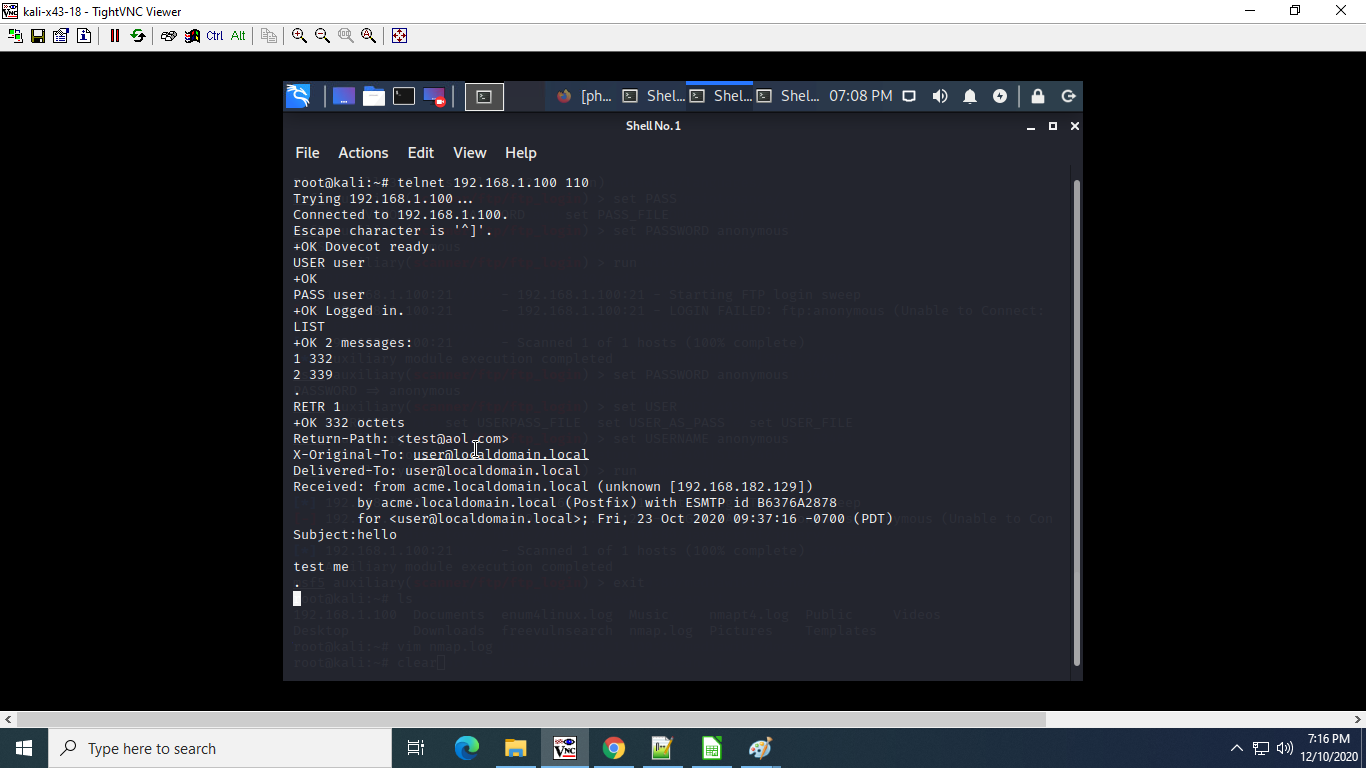
1. POP3 Exploit

Used Nmap default scripts and freevulnscripts to find out the vulnerability in the port 110 which is POP3

nmap -p 110,995 --script pop3-ntlm-info <target>

nmap -p 110 --script pop3-ntlm-info 192.168.1.100

which provides the USERNAME user and the PASSWORD can be exploited with Metasploit using its wordlist attack. Which results in PASSWORD user



To login into POP3 on 110 port

telnet 192.168.1.100 110

USER user

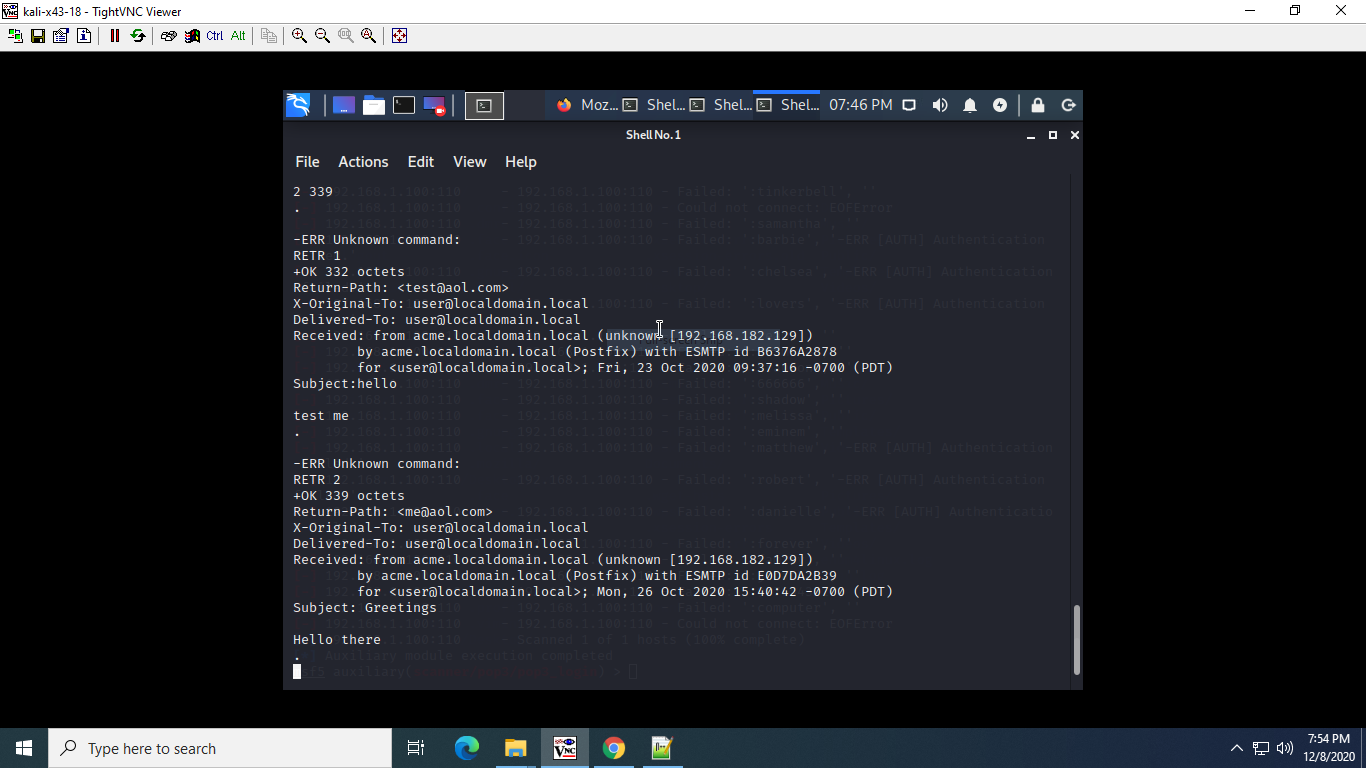
PASS user

LIST (To check the present items in the server)

1) 332

2) 339

Which are the messages that are present in the POP3 server



From the above message we can see that the we are able to access the pop3 server message that is stored in target IP that is 192.168.1.100

1. Port: 445

Microsoft Windows SMB Shares Unprivileged Access

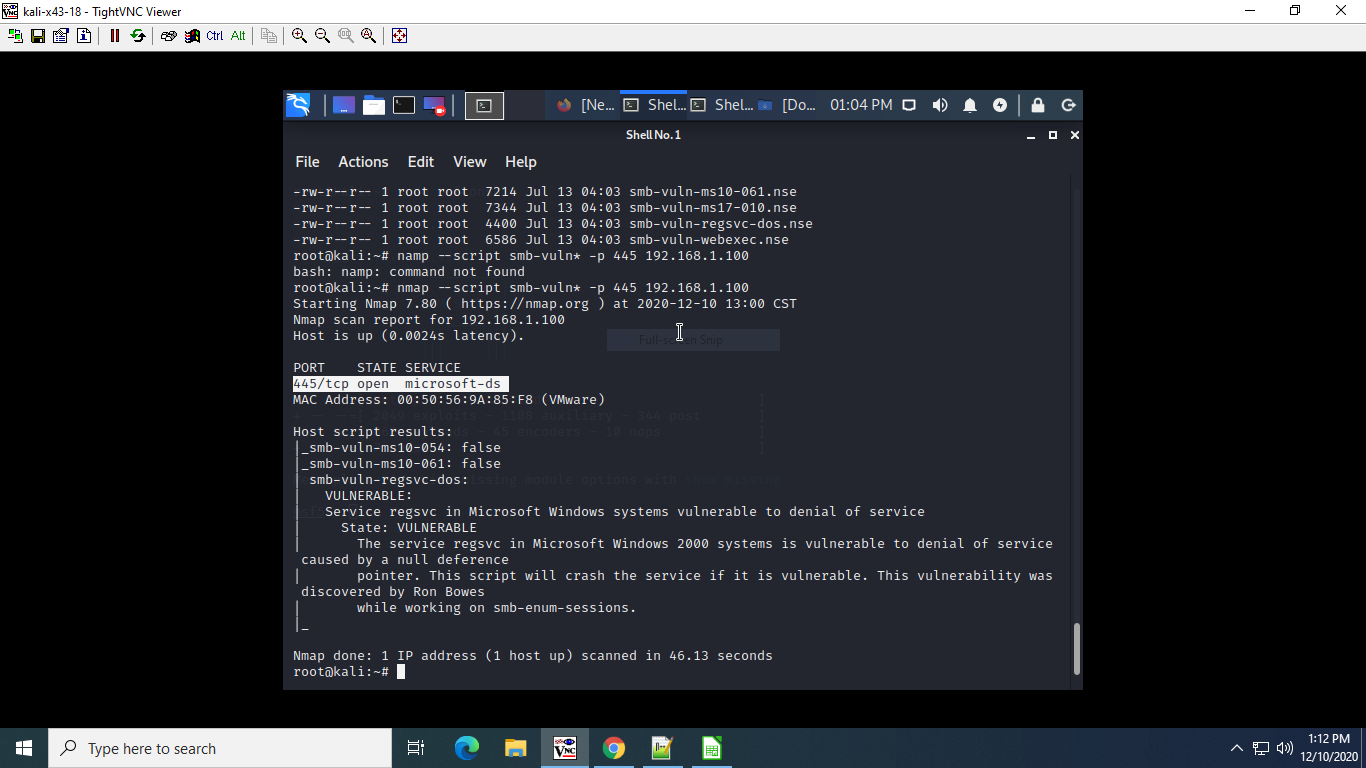
It is possible to access a network share.

To restrict access under Windows, open Explorer, do a right click on

each share, go to the 'sharing' tab, and click on 'permissions'.

1. **THREAT LEVEL: Medium**
2. SMB PORT 445

To exploit this port used I nmap default scripts which provides the result showing the target IP which is 192.168.1.100 is vulnerable to the DOS attack.

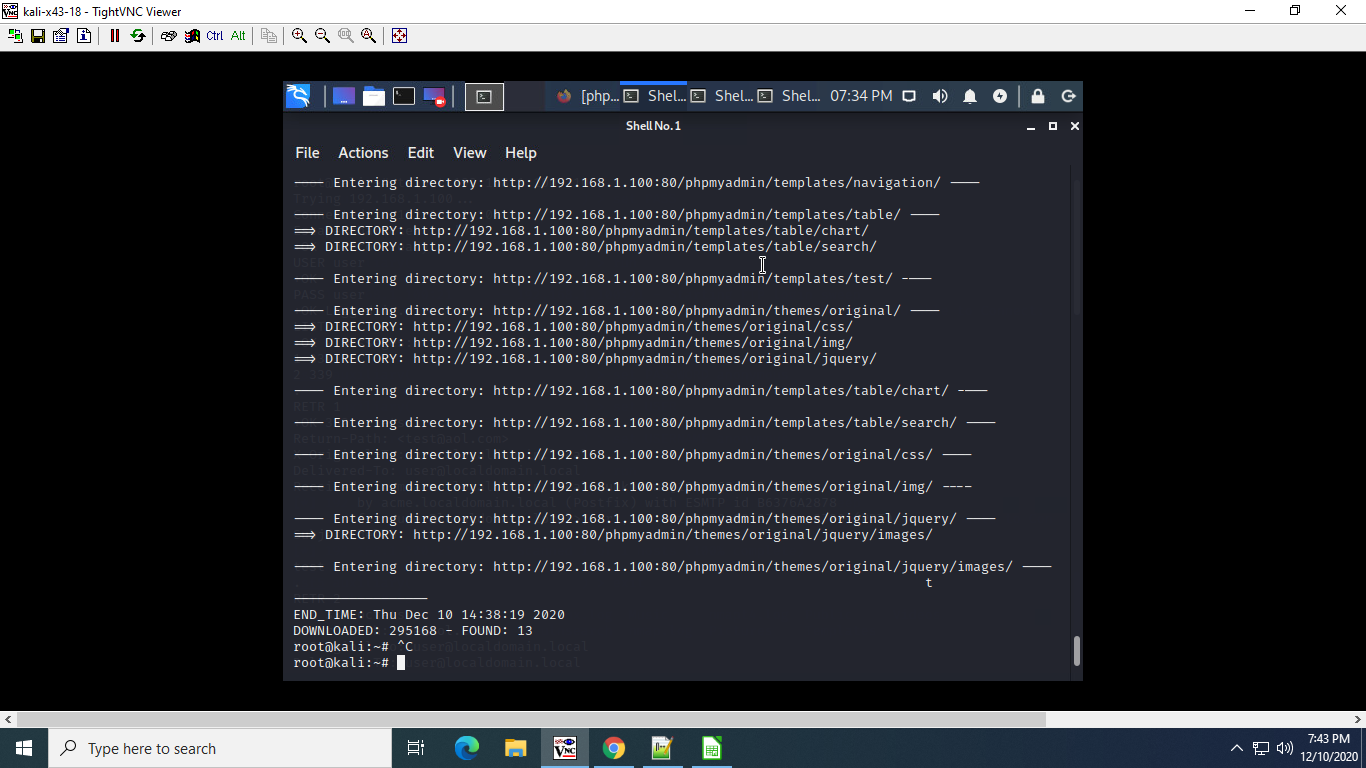


1. Getting Directory and its Structure knowledge using “DIRBUSTER”

DirBuster is a multi-threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within.

dirb hostname

dirb <https://192.168.1.100>



DirBuster report shows 13 vulnerability in its output report and it is able to access all the database present in the target machine like PHPMYADMIN.

1. **Threat Level: LOW**

Port: 110

POP3 Cleartext Logins Permitted

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:7.2p2:

| CVE-2016-8858 7.8 https://vulners.com/cve/CVE-2016-8858

|\_ CVE-2017-15906 5.0 <https://vulners.com/cve/CVE-2017-15906>

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|\_http-server-header: Apache/2.4.18 (Ubuntu)

MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/HTTP/APACHE\_OPTIONSBLEED \*EXPLOIT\*

| EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0 https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D \*EXPLOIT\*

| EXPLOITPACK:2666FB0676B4B582D689921651A30355 5.0 https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355 \*EXPLOIT\*

| EDB-ID:40909 5.0 <https://vulners.com/exploitdb/EDB-ID:40909>

**List of Tools**

1. Nmap (Scanning and Recommence)
2. Nessus (Scanning and Recommence)
3. Metasploit (Exploiting and for scanning also. Used Nmap with Metsploit)
4. DirBuster (To brute force Directory)
5. Hydra (To bruteforce passwords on SSH and PHPMYADMIN)

**Remediation**

1. PORT 21 FTP

When using the FTP protocol this can be done using implicit FTPS running on port 990 or by using explicit FTPS running on port 21. Both of these protocols use SSL/TLS to **secure** both the command and data channels protecting both the commands and data exchanged between the client and server.

1. PORT 110 POP3

Many mail clients now support this as an extension to standard POP3 support, since the SSL encrypts everything and prevents eavesdropping of the connection (but not man-in-the-middle attacks). Secure POP3, or pop3s runs on port 995 of the server instead of the plaintext port 110 and demands an SSL-capable client on the other end.

1. SMB Exploit

Enable firewall, install VPN, implement the VLANs and use MAC address filtering to prevent the SMB exploit.

1. DirBuster Exploit

The rules should be made in your server to block people for a set amount of time if they request more than 100 requests in a minute or something. This breaks it severely, but not forever. A permanent ban isn't suggested, but not the worst idea either. Sort of like password guess limitations that lock you out for 5 minutes.

**References**

Attaching Nmap vulnerability report which is used as a reference to exploit target.

<https://www.offensive-security.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/>

<https://nmap.org/nsedoc/scripts/pop3-capabilities.html>

<https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b>