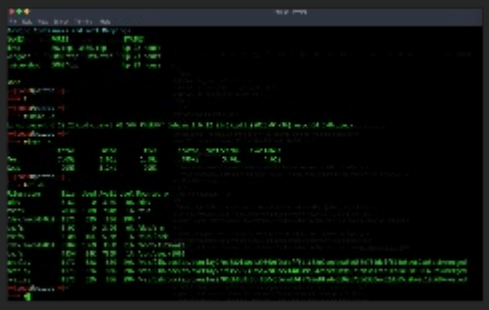
RaspberryPi4-WebSploit

Lab Enviroment

- Lab Setup:
  - Equipment:
    - Model:
      - Raspberry Pi 4 Model B
    - Operating System:
      - Linux parrot 6.12.25+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.12.25-1+rpt1 (2025-04-30) aarch64 GNU/Linux
    - Memory:
      - 8G
    - Storage:
      - 128G
    - InfoGraphic:
      - 
      - cmdline:

```
┌─[root@parrot]─[~]
└──╼ #uname -a
Linux parrot 6.12.25+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.12.25-1+rpt1 (2025-04-30) aarch64
GNU/Linux
┌─[root@parrot]─[~]
└──╼ #free -h
               total        used        free      shared  buff/cache   available
Mem:           7.6Gi       3.0Gi       1.5Gi       486Mi       3.7Gi       4.6Gi
Swap:           99Mi        512Ki        99Mi
┌─[root@parrot]─[~]
└──╼ #df -h
Filesystem             Size  Used Avail Use% Mounted on
udev                   3.6G     0  3.6G   0% /dev
tmpfs                  783M  1.8M  781M   1% /run
/dev/mmcblk0p2  117G   32G   80G  29% /
tmpfs                  3.9G     0  3.9G   0% /dev/shm
tmpfs                  5.0M   16K  5.0M   1% /run/lock
/dev/mmcblk0p1  510M  156M  355M  31% /boot/firmware
tmpfs                  783M   84K  783M   1% /run/user/1000
overlay                117G   32G   80G  29% /var/lib/docker/overlay2/
ed680fa0ce29360f2cbcff3d1632e2debeea5d656e754deff51308c9c2a05d1b/merged
overlay                117G   32G   80G  29% /var/lib/docker/
overlay2/7e4559539a5a7c09ae0f40149a342beef3b9b675cb3a17ad1ee8a138158325f3/merged
overlay                117G   32G   80G  29% /var/lib/docker/
overlay2/866b8c8f7df850453ebab6f9799e8fede3109b733d380ee62db85c2be9c19d69/merged
┌─[root@parrot]─[~]
└──╼ #
```

  - Installation:
    - Download Operating System (Parrot or Kali):
      - Download ParrotOS for RaspberryPi 4 here:
        - https://www.parrotsec.org/
      - Download Kali Linux for RaspberryPi 4 here:

- n/a

- Flash image to disk using RaspberryPi Imager:
  - 

  - Download RaspberryPi Imager here:
    - https://www.raspberrypi.org/
- Boot Pi with Parrot or Kali OS default login's:
  - ParrotOS:
    - pi
    - parrot
  - Kali Linux:
    - n/a
    - n/a
- Download and install Websploit Labs:

https://websploit.or...

  - Installation Script:

```
curl -sSL https://websploit.org/install.sh | sudo bash
```

  - 

  - Updating Websploit Docker containers to support ARM arch:
    - From the cmdline login into root

```
sudo su
```

    - Move to Root's root directory to find the Websploit home directory ~/h4cker

```
cd ~/
```

    - Stay in the root directory & shutdown & remove all running conatiners
      - 1. Stop All Containers

```
docker stop $(docker ps -aq)
```

      - 2. Remove All Containers

```
docker rm $(docker ps -aq)
```

- 3. (Optional) Clean Up Volumes and Networks

```
docker volume prune -f
docker network prune -f
```

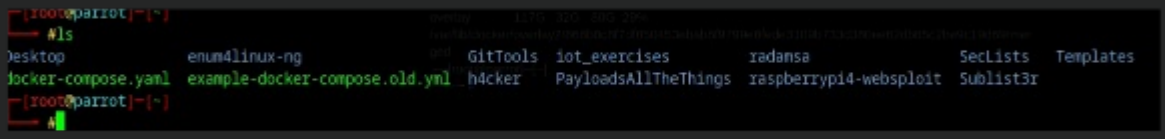
- 4. (Optional) Verify Clean State

```
docker ps -a
```

- Copy provider docker-compose file & keep as referance

```
cp docker-compose.yml example-docker-compose.yml
```

-



- Create/Edit docker-compose file that supports ARM arch

```
nano docker-compose.yml
```

-

- New docker-compose.yml file that supports ARM arch & recreates networks
  - docker-compose.yaml

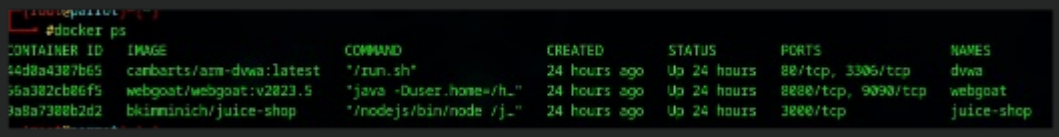
```
services:
  webgoat:
            container_name: webgoat
            image: webgoat/webgoat:v2023.5
            restart: unless-stopped
            networks:
            websploit:
            ipv4_address: 10.6.6.11

  juice-shop:
            container_name: juice-shop
            image: bkimminich/juice-shop
            restart: unless-stopped
            networks:
            websploit:
            ipv4_address: 10.6.6.12

  dvwa:
            container_name: dvwa
            image: cambarts/arm-dvwa:latest
            restart: unless-stopped
            networks:
            websploit:
            ipv4_address: 10.6.6.13

networks:
  websploit:
            driver: bridge
            ipam:
            config:
            - subnet: 10.6.6.0/24
            gateway: 10.6.6.1
```

- Build & start new docker containers & network

```
docker-compose up -d
```

- Confirm containers and network are working properly

```
docker ps
```



- Use Websploit built in container scanner

```
containers
```

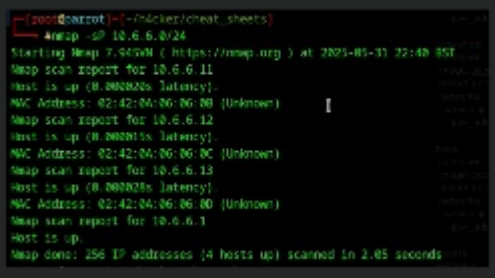
Recon

- Phase 1: Network Recon (Nmap)

Nmap (Network Mapp...

- What I did:
  - I began by scanning the internal RaspberryPi4-WebSploit network (10.6.6.0/24) using Nmap to identify live hosts and open TCP ports. This provided a broad view of available services and gave me three target IPs with interesting ports, including web-facing services on ports 80, 8080, 3000, and 9090.
- Why I did it:
  - To enumerate active hosts and map the attack surface
  - Identify potential web services to investigate further
- Started with a scan using Nmap on network 10.6.6.0/24

```
nmap -sP 10.6.6.0/24
```



- cmdline:

```
┌─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nmap -sP 10.6.6.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 22:40 BST
Nmap scan report for 10.6.6.11
Host is up (0.000020s latency).
MAC Address: 02:42:0A:06:06:0B (Unknown)
Nmap scan report for 10.6.6.12
Host is up (0.000015s latency).
MAC Address: 02:42:0A:06:06:0C (Unknown)
Nmap scan report for 10.6.6.13
Host is up (0.000028s latency).
MAC Address: 02:42:0A:06:06:0D (Unknown)
Nmap scan report for 10.6.6.1
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.05 seconds
```

- DIscovered Host :
  - Host-1
    - IP Address
      - 10.6.6.11
    - MAC Address
      - 02:42:0A:06:06:0B
    - PORT
      - 8080/tcp
      - 9090/tcp
    - STATE
      - open
      - open
    - SERVICE
      - http-proxy
      - zues-admin
  - Host-2
    - IP Address
      - 10.6.6.12
    - MAC Address
      - 02:42:0A:06:06:0C
    - PORT
      - 3000/tcp
    - STATE
      - open
    - SERVICE
      - ppp
  - Host-3
    - IP Address
      - 10.6.6.13
    - MAC Address
      - 02:42:0A:06:06:0D
    - PORT
      - 80/tcp
      - 3306/tcp
    - STATE
      - open
      - open
    - SERVICE
      - http
      - mysql
- Scanned the network host with defualt Nmap scripts

```
nmap -sC 10.6.6.0/24
```

- cmdline:

```
┌──[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nmap -sC 10.6.6.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 22:49 BST
Nmap scan report for 10.6.6.11
Host is up (0.000027s latency).
Not shown: 998 closed tcp ports (reset)
PORT        STATE SERVICE
8080/tcp open  http-proxy
|_http-title: Site doesn't have a title.
9090/tcp open  zeus-admin
MAC Address: 02:42:0A:06:06:0B (Unknown)

Nmap scan report for 10.6.6.12
Host is up (0.000027s latency).
Not shown: 999 closed tcp ports (reset)
PORT        STATE SERVICE
3000/tcp open  ppp
MAC Address: 02:42:0A:06:06:0C (Unknown)

Nmap scan report for 10.6.6.13
Host is up (0.000026s latency).
Not shown: 998 closed tcp ports (reset)
PORT        STATE SERVICE
80/tcp   open  http
| http-title: Setup :: Damn Vulnerable Web Application (DVWA) v1.9
|_Requested resource was setup.php
| http-cookie-flags:
|   /:
|           PHPSESSID:
|_          httponly flag not set
| http-robots.txt: 1 disallowed entry
|_/
3306/tcp open  mysql
MAC Address: 02:42:0A:06:06:0D (Unknown)

Nmap scan report for 10.6.6.1
Host is up (0.000026s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
| dns-nsid:
|_  bind.version: dnsmasq-2.90

Nmap done: 256 IP addresses (4 hosts up) scanned in 17.64 seconds
```

- Phase 2: Web Recon (Nikto)

Nikto is an open-s...

  - What I did:
    - I then ran Nikto on the discovered web services to detect common vulnerabilities, misconfigurations, and hidden directories. This revealed accessible paths like /dump.tgz, /database.tgz, and /config/, as well as outdated Apache and PHP versions.
  - Why I did it:

- To find low-hanging fruit like open directories, outdated versions
- Nikto is fast and automated, making it great for early recon

Scaned host indivisual with Nikto

`nikto -h http://10.6.6.13`

- cmdline:

```
┌─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nikto -h http://10.6.6.13
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.6.6.13
+ Target Hostname:    10.6.6.13
+ Target Port:        80
+ Start Time:         2025-06-01 00:44:16 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.29.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://
developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://
www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-
US/docs/Web/HTTP/Cookies
+ Root page / redirects to: login.php
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the
EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-
access-to-iconsreadme/
+ 8881 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2025-06-01 00:44:41 (GMT1) (25 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[✗]─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nikto -h http://10.6.6.13 -p 9090
- Nikto v2.5.0
---------------------------------------------------------------------------
- ERROR: The -port option cannot be used with a full URI
┌─[✗]─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nikto -h http://10.6.6.13:9090
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested
┌─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nikto -h http://10.6.6.11:9090
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.6.6.11
+ Target Hostname:    10.6.6.11
+ Target Port:        9090
+ Start Time:         2025-06-01 00:47:39 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://
developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://
www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8073 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-06-01 00:47:59 (GMT1) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[✗]─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nikto -h http://10.6.6.11:8080
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.6.6.11
+ Target Hostname:    10.6.6.11
+ Target Port:        8080
+ Start Time:         2025-06-01 00:48:47 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://
developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://
www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8073 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2025-06-01 00:49:05 (GMT1) (18 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[✗]─[root@parrot]─[~/h4cker/cheat_sheets]
└──╼ #nikto -h http://10.6.6.12:3000
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.6.6.12
+ Target Hostname:    10.6.6.12
+ Target Port:        3000
+ Start Time:         2025-06-01 03:47:33 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: /#/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See:
https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://
developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: 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. See: https://
www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /10.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /archive.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /10.6.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /6.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /1066.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /106612.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /1066.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /106.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /dump.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /site.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /6.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /backup.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /106612.tar.bz2: Potentially interesting backup/cert file found. . See: https://
cwe.mitre.org/data/definitions/530.html
+ /site.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /10_6_6_12.tar.bz2: Potentially interesting backup/cert file found. . See: https://
cwe.mitre.org/data/definitions/530.html
+ /106612.tar.lzma: Potentially interesting backup/cert file found. . See: https://
cwe.mitre.org/data/definitions/530.html
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /database.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
+ /106.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/
definitions/530.html
+ /dump.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/
data/definitions/530.html
```

- Interesting Finds per host
  - Host-1
    - Target Port
      - 8080
      - 9090
    - Server
      - No banner retrieved
      - No banner retrieved
    - Header
      - not set
      - not set
  - Host-2
    - Target Port
      - 3000
    - Server
      - No banner retrieved
    - Header
      - not set
    - DIrectories Discovered
      - See cli print out fo...
      - /dump.tgz
      - /database.tgz
      - /ftp/
      - /public/
  - Host-3
    - Target Port
      - 80
    - Server
      - Apache/2.4.7 (Ubuntu)
    - Header
      - PHP/5.5.9-1ubuntu4.29
    - Root Page
      - redirects to: login.php
    - DIrectories Discovered
      - See cli print out fo...
      - /config/
      - /docs/
      - /icons/REAME
- Phase 3: Web App Assessment (ZAP)
  - OWASP ZAP is an op...
  - What I did:

- Based on the Nikto results, I progressed to OWASP ZAP for a more in-depth and interactive analysis of the web application. I chose ZAP to perform both passive and active scans, observe requests in real time, and explore site structure using spidering tools.

- Why I did it:
  - Unlike Nikto, ZAP allows manual interaction, auth testing, and deeper scan customization
  - I can inspect HTTP headers, cookies, authentication flows, and inject test payloads
  - ZAP supports proxying a browser, ideal for dynamic and client-heavy web apps

Attack

ExFil & Reporting

References