

NehamStore: Recon

Introduction

The recognition phase is almost the most important face at the moment to do web penetration testing, because it will give us a wider attack surface than just the domain that has been assigned to us.

In this phase we are going to perform OSINT recognition, such as subdomain identification, and Active Recognition such as directory listing.

Subdomain Enumeration

The first recon action that I did was Subdomain enumeration. To this purpose Nahamsec has provided an internet domain so that we can conduct these tests, the domain is **nahamstore.com**. The goal is that, once the subdomains are identified, they are added to the **/etc/hosts** file of our attacking machine, changing the **.com** to **.thm**.

The tool that i used was **subfinder**:

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ subfinder -d nahamstore.com > subdomains.txt

[INFO] Current subfinder version v2.6.0 (outdated)
[INFO] Loading provider config from the default location: /home/kali/.config/subfinder/provider-config.yaml
[INFO] Enumerating subdomains for nahamstore.com
[INFO] Found 5 subdomains for nahamstore.com in 25 seconds 992 milliseconds
```

And these were with identified subdomains:

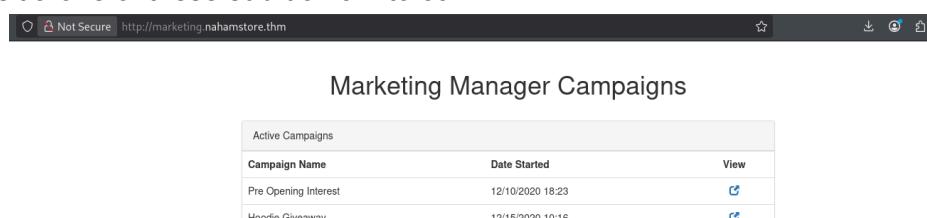
```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ cat subdomains.txt
www.nahamstore.com
nahamstore-2020.nahamstore.com
stock.nahamstore.com
marketing.nahamstore.com
shop.nahamstore.com
```

Then i added to my file **etc/host**:

```
GNU nano 8.7
/etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali.kali      kali

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.65.170.203      nahamstore.thm shop.nahamstore.thm marketing.nahamstore.thm stock.nahamstore.thm nahamstore-2020.nahamstore.thm
```

We can visit a one of these sub domain to confirm:



The screenshot shows a browser window with the URL <http://marketing.nahamstore.thm>. The page title is "Marketing Manager Campaigns". Below the title is a table titled "Active Campaigns" with three rows of data:

Campaign Name	Date Started	View
Pre Opening Interest	12/10/2020 18:23	
Hoodie Giveaway	12/15/2020 10:16	

⌚ Nmap: Ports and Services

The full nmap port scan gives us three open ports:

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ sudo nmap -sS -n -Pn -T4 nahamstore.thm
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-23 08:19 AST
Nmap scan report for nahamstore.thm (10.65.170.203)
Host is up (0.071s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 33.80 seconds
```

And when we did a service scan we received this:

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ sudo nmap -sCV -n -T4 -p22,80,8000 nahamstore.thm
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-23 08:36 AST
Nmap scan report for nahamstore.thm (10.65.170.203)
Host is up (0.059s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-keykey:
|_ 2048 84:6e:52:ca:db:9e:df:0a:ae:b5:70:3d:07:d6:91:78 (RSA)
|_ 256 1a:1d:db:ca:99:8a:64:b1:8b:10:df:a9:39:d5:c3:d3 (EDDSA)
|_ 256 f6:36:16:d7:66:8e:7b:35:09:07:cb:90:c9:84:63:38 (ED25519)
80/tcp    open  http     nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: NahamStore - Home
|_http-cookie-flags:
|_ session:
|   httponly flag not set
8000/tcp  open  http     nginx 1.18.0 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_admin
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 14.14 seconds
```

In summary, the nmap scan revealed that the website has three open ports: an ssh connection on port 22, an HTTP server on port 80, and another HTTP service on **port 8000**, along with a **/robots.txt** directory and a **/admin** directory.

📁 Directory bruteforcing

To perform a directory brute force, use feroxbuster, but with a **"one-liner" in bash** to perform the process on all subdomains, not just the main domain, but also those saved in the subdomains.txt file. The one liner was:

```
for domain in $(cat subdomains.txt); do feroxbuster -u http://$domain -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -t 100 --time-limit 1m -o Ferox_$domain.txt; done
```

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ for domain in $(cat subdomains.txt); do feroxbuster -u http://$domain -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -t 100 --time-limit 1m -o Ferox_$domain.txt; done
[ERRIC_OXIDE]
by Ben "epi" Risher • ver. 2.19.0
● Target Url          http://nahamstore.thm/
● In-Scope Url        nahamstore.thm
● Threads             100
● Wordlist            /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
● Status Codes        All Status Codes
● Timeout (secs)      /
● User-Agent          Feroxbuster/2.19.0
● Config File         /etc/feroxbuster/ferox-config.toml
● Timeout (secs)      10
● Output File         Ferox_nahamstore.thm.txt
● HTTP methods        [GET]
● Recursion Depth    1m
● Time Limit          1m
● New Version Available https://github.com/epi052/feroxbuster/releases/latest
▶ Press [ENTER] to use the Scan Management Menu
```

All the information was saved in its respective file:

```
(kali㉿kali)-[~/.../Machines/NahamStore/Recon/Directory Listing]
$ ls -l
total 892
-rw-rw-r-- 1 kali kali 5006 Dec 23 18:09 Ferox_marketing.nahamstore.thm.txt
-rw-rw-r-- 1 kali kali 4732 Dec 23 18:07 Ferox_nahamstore-2020.nahamstore.thm.txt
-rw-rw-r-- 1 kali kali 877778 Dec 23 18:07 Ferox_nahamstore.thm.txt
-rw-rw-r-- 1 kali kali 4699 Dec 23 18:09 Ferox_shop.nahamstore.thm.txt
-rw-rw-r-- 1 kali kali 4853 Dec 23 18:08 Ferox_stock.nahamstore.thm.txt
```

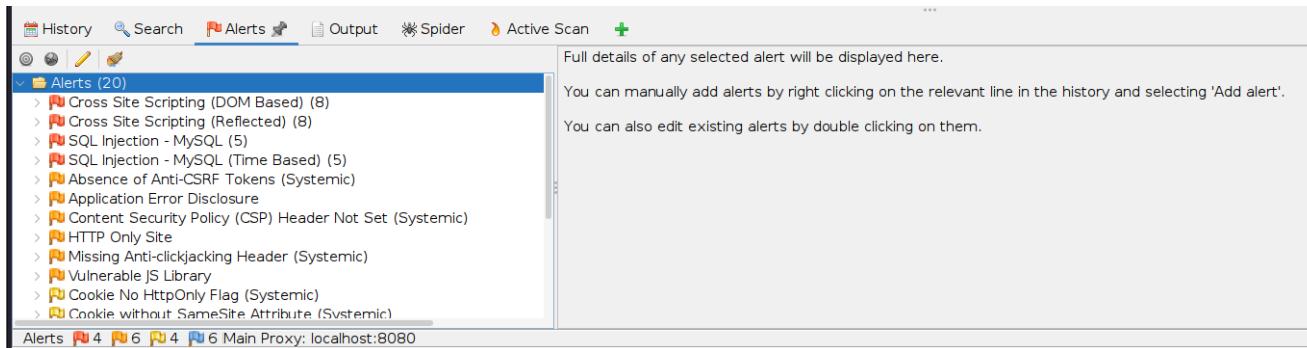
Web technologies

To enumerate the technologies that runs in the web application all its subdomain i used **whatweb**

```
(kali㉿kali)-[~/Desktop/THM/Machines/NahamStore]
$ whatweb -i subdomains.txt --no-errors | tee technologies.txt
http://stock.nahamstore.thm/ [200 OK] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)], IP[10.67.166.47], nginx[1.14.0]
http://shop.nahamstore.thm/ [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)], IP[10.67.166.47], Red
irectLocation[http://nahamstore.thm], Title[301 Moved Permanently], nginx[1.14.0]
http://nahamstore.thm/ [200 OK] Bootstrap[3.3.7], Cookies[session], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)]
, IP[10.67.166.47], JQuery, Script, Title[NahamStore - Home], X-UA-Compatible[IE=edge], nginx[1.14.0]
http://marketing.nahamstore.thm/ [200 OK] Bootstrap[3.3.7], Cookies[session], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)], IP[10.
67.166.47], Title[Marketing Manager - Active Campaigns], X-UA-Compatible[IE=edge], nginx[1.14.0]
http://nahamstore.thm [200 OK] Bootstrap[3.3.7], Cookies[session], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)],
IP[10.67.166.47], JQuery, Script, Title[NahamStore - Home], X-UA-Compatible[IE=edge], nginx[1.14.0]
```

Vulnerability Analysis

To perform the vulnerability analysis I used OWASP Zap Proxy



The screenshot shows the OWASP Zap Proxy interface. On the left, there's a sidebar with icons for History, Search, Alerts, Output, Spider, and Active Scan. The 'Alerts' tab is selected, showing a list of 20 vulnerabilities. The list includes items like 'Cross Site Scripting (DOM Based)' (8), 'Cross Site Scripting (Reflected)' (8), 'SQL Injection - MySQL' (5), etc. To the right of the alert list, there's a large panel with descriptive text and buttons for adding, viewing, and editing alerts.

As we can see, Zap found several **high-risk** vulnerabilities. I saved the report in HTML format to consult it in the future exploitation phase.

And to expand the vulnerability analysis, use **Nuclei**, passing it the list with all subdomains and saving it in a .txt file.

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ nuclei -l subdomains.txt -o VulnAnalisis.txt

projectdiscovery.io
v3.6.1

[WRN] Found 1 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v3.6.1 (latest)
[INF] Current nuclei-templates version: v10.3.5 (latest)
[INF] New templates added in latest release: 57
[INF] Templates loaded for current scan: 8996
[INF] Executing 8994 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 2 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 5
```

Finally i perform a last vulnerability analysis using **Nikto** to the main domain and all subdomain saving the result in a HTML file

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Recon]
$ nikto -h subdomains.txt -o NiktoAnalysis.html -Format html
- Nikto v2.5.0

+ Target IP:          10.66.128.176
+ Target Hostname:    marketing.nahamstore.thm
+ Target Port:        80
+ Start Time:         2025-12-24 10:40:02 (GMT-4)
```

Conclusion

And with all this, we conclude the reconnaissance phase. All this information that we have collected will be used in the previous exploitation phase