7

Your attack team has run initial reconnaissance on the target: Throwback Hacks Security. They find that there are 3 machines that are publicly facing: THROWBACK-PROD, THROWBACK-FW01, and THROWBACK-MAIL. Your team has informed you that these assets are publicly accessible, it is your job to perform additional reconnaissance on these machines and find the way in. To accomplish this, we'll be learning to use the tool nmap.

Scanning the World with nmap

nmap is a commonly used port scanning tool that is an industry standard that is both fast and comes with NSE scripts. nmap also supports CIDR notation so we can specify a /24 to specify 254 hosts.
We can specify how we want to scan the hosts using switches.

- sV determines service and version of open ports
- sC runs a script scan against the found ports
- -p- scans all ports 0-65535
- -v runs the scan in verbose mode

1.) nmap -sV -sC -p- -v 10.200.x.0/24 --min-rate 5000
This nmap command is fairly stable and will scan the entire network in a couple of minutes. You may need to specify the min rate to be lower, as it affects the minimum number of packets that nmap sends. If too high it can miss ports or cause false positives.

```
cryillic@human-eater:/$ nmap -sV -sC -p- -v 10.200.3.0/24 --min-rate 5000
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-15 18:23 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Initiating Ping Scan at 18:23
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 18:23, 0.97s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 18:23
Completed Parallel DNS resolution of 256 hosts. at 18:23, 0.05s elapsed
Nmap scan report for 10.200.3.0 [host down]
Nmap scan report for 10.200.3.1 [host down]
Nmap scan report for 10.200.3.2 [host down]
```

Scanning the network with nmap

Identifying Assets and Finding the Attack Surface

Enumerating THROWBACK-PROD Scans

When enumerating the nmap scan we find many open ports as well as a leaked domain name.

```
445/tcp   open  microsoft-ds? syn-ack ttl 126
3389/tcp  open  ms-wbt-server syn-ack ttl 126 Microsoft Terminal Services
| ssl-cert: Subject: commonName=THROWBACK-PROD.[redacted]
| Issuer: commonName=THROWBACK-PROD.[redacted]
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-27T22:26:10
| Not valid after:  2021-01-26T22:26:10
| MD5:   5ea4 baab f267 132f 37a0 9c26 6be5 3bec
| SHA-1: b058 ec84 df89 f60d 8c99 705a dbca e5c5 e0be b825
```

Enumerating nmap scans port 445 + 3389

We also find that port 80 is running an IIS server this is good to note to visit and enumerate later.

```
80/tcp    open  http          syn-ack ttl 126 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: [redacted]
```

Enumerating nmap scans on port 80

Enumerating THROWBACK-MAIL Scans

We find that THROWBACK-MAIL is a Linux box running an Apache server on port 80 running a login page.

```
80/tcp  open  http    syn-ack ttl 62 Apache httpd [redacted] ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 2D267521ED544C817FADA219E66C0CCC
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/[redacted] (Ubuntu)
| http-title: [redacted]
|_Requested resource was src/login.php
```

Enumerating nmap scans on port 80

Enumerating THROWBACK-FW01 Scans

When looking at the scans we see that the box is more than likely running a pfSense firewall with a public pfSense login.

```
80/tcp  open  http     syn-ack ttl 62 nginx
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://10.200.3.138/
443/tcp open  ssl/http syn-ack ttl 62 nginx
|_http-title: [redacted]
| ssl-cert: Subject: commonName=pfSense-5f099cf870c18/organizationName=pfSense webConfigurator Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-5f099cf870c18
| Issuer: commonName=pfSense-5f099cf870c18/organizationName=pfSense webConfigurator Self-Signed Certificate
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-11T11:05:28
| Not valid after:  2021-08-13T11:05:28
| MD5:   fe06 fa47 4d83 8454 e67a 1840 7ea8 d101
| SHA-1: 672e 5f8f 9b28 7cad 5789 c5be cb1c f3f2 6c63 dfb2
```

Enumerating THROWBACK-FW01 scans

Answer the questions below

What is the domain name?

Correct Answer

What is the HTTP title of the web server running on THROWBACK-PROD?

Correct Answer

How many ports are open on THROWBACK-MAIL?

Correct Answer

What service is running on THROWBACK-FW01?

Correct Answer

What version of Apache is running on THROWBACK-MAIL?

Correct Answer