Bucket - 11th Nov 20

10.10.10.212

Scanning

We start by nmaping it, as usual, and it turns out that runs a Nexacut, Identifier-pare ports, and that clients should port port 5 or 80 by default, and port 5 is unknown and port 80 is Apache Jetty/9.4.18.dev.

```
$ nmap -sV -sC -p- -vvv -oN nmap/initial 10.10.10.212
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-10 21:17 EST
Initiating Ping Scan at 21:17
Scanning 10.10.10.212 [4 ports]
Completed Ping Scan at 21:17, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:17
Completed Parallel DNS resolution of 1 host. at 21:17, 0.13s elapsed
DNS resolution for 10.10.10.212 [ip6.arpa]
Initiating SYN Stealth Scan at 21:17
Scanning bucket.htb (10.10.10.212) [65535 ports] at 21:17
Discovered open port 80/tcp on 10.10.10.212
Discovered open port 5/tcp on 10.10.10.212
Completed SYN Stealth Scan at 21:17, 12.07s elapsed (65535 total ports)
Nmap scan report for bucket.htb (10.10.10.212)
Host is up, received echo-reply (0.07s latency).
Scanned at 2020-11-10 21:17:08 EST for 12s
PORT   STATE SERVICE REASON         VERSION
5/tcp  open  rtip    syn-ack ttl 63 Nexacut Identifier-pare
80/tcp open  http    syn-ack ttl 63 Apache Jetty/9.4.18.dev (Unknown Title)
Service Info: Device: broadband router; CPE: cpe:/h:nexacut:identifier-pare
Read data files from: /usr/bin/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
           Raw packets sent: 65535 (2.621MB) | Rcvd: 65535 (2.621MB)
```

Nmap shows the hostnames **bucket.htb** and **s3.bucket.htb** in the `ssl/tls` SANs. The `ssl/tls` SANs, `http-title`:

```
$ nmap -sV -sC -p- -vvv -oN nmap/initial 10.10.10.212
...
| ssl-cert: Subject: commonName=s3.bucket.htb/organizationalUnitName=Development/stateOrProvinceName=Oregon/country=US
| Subject Alternative Name: DNS:s3.bucket.htb
| Issuer: commonName=s3.bucket.htb/organizationalUnitName=Development/stateOrProvinceName=Oregon/country=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-14T17:47:40
| Not valid after: 2021-07-14T17:47:40
| MD5: 3c2b:ed0a:ba0a:f0a0:a0a0:a0a0:a0a0:a0a0
| SHA-256: 2f0f:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a:0a0a
| -----BEGIN CERTIFICATE-----
| MIIDUTCCAjmgAwIBAgIUNzMzMzMzMzMzMzMzMzMzMzMzMzMwDQYJKoZIhvcNAQEL
| BQAwMTEUMBIGA1UEAwwLczMuYnVja2V0LmhidjEgMCAGA1UECwwZRGV2ZWxvcG1l
| bnQgVW5pdCAgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNv
| bnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRh
| Y3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3Q
| gIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGN
| vbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnRhY3QgIGNvbnR
| hY
```