[REPORT TITLE]

[SUBTITLE]

student@youremailaddress.com, [Other info, e.g. OSID]

2023-07-07

Contents

1 Enumeration

1.1 TCP services - common

```
nmap -sC -sV -oA nmap/jupiter 10.10.11.216 # scan for top 1000 default ports
```

testing for label match: 1 testing for basename match: 1 testing for extension match: 1 label: basename: nmap-scan-leaking-domain-name extension: png altText: nmap scan leaking domain name

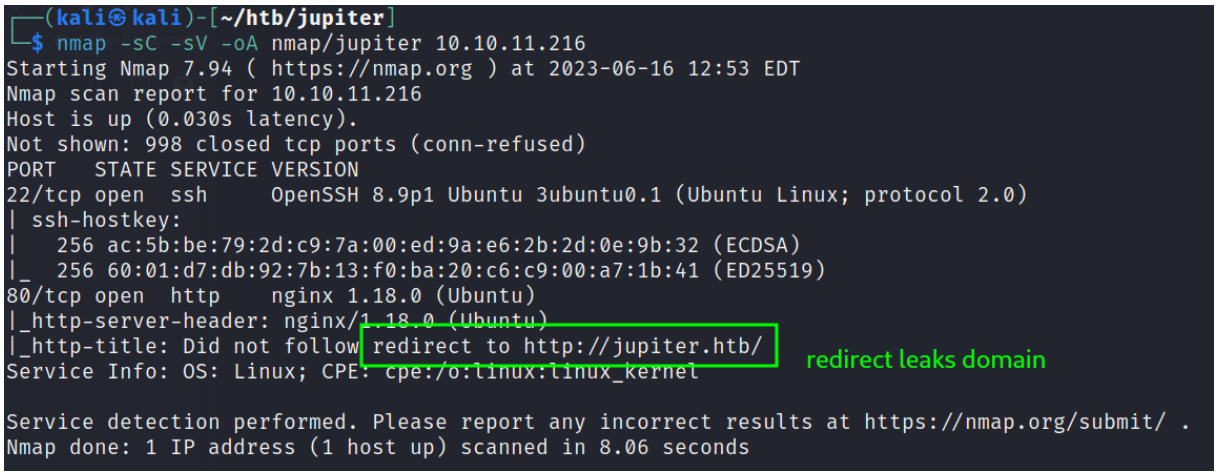

Figure 1.1: nmap scan leaking domain name

An nmap scan of the 1000 most common TCP ports reveals a web server running on Port 80, with a leaked domain name of `jupiter.htb`. See Figure 1.1 Right away, notice that there is an HTTP port open, hosting an nginx server. The `http-title` NSE script identified a redirect to `http://jupiter.htb`

testing for label match: 0 testing for basename match: 1 testing for extension match: 1 label: basename: test-test-test extension: png altText: test test test

Figure 1.2: test test test