
[REPORT TITLE]

[SUBTITLE]

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

2023-07-07

Contents

1 Enumeration	1
1.1 TCP services - common	1

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

```
(kali㉿kali)-[~/htb/jupiter]
└─$ nmap -sC -sV -oA nmap/jupiter 10.10.11.216
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 12:53 EDT
Nmap scan report for 10.10.11.216
Host is up (0.030s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 ac:5b:be:79:2d:c9:7a:00:ed:9a:e6:2b:2d:0e:9b:32 (ECDSA)
|_ 256 60:01:d7:db:92:7b:13:f0:ba:20:c6:c9:00:a7:1b:41 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://jupiter.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds
```

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

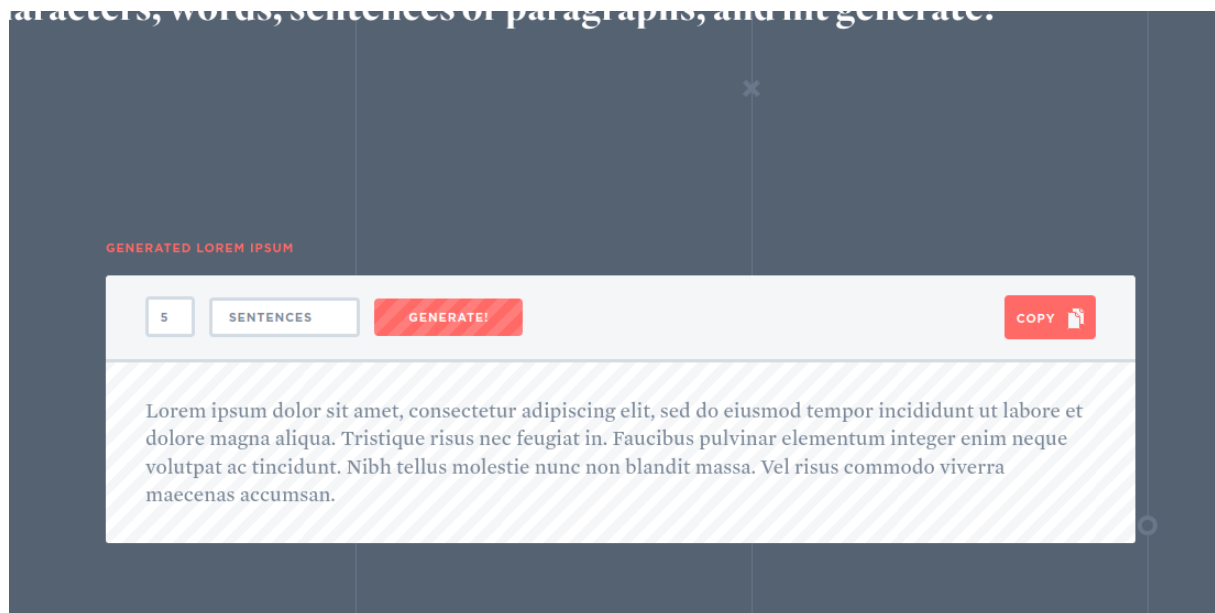


Figure 1.2: test test test