Basic Cybersecurity Report

1. Ping Test Result

PING example.com (93.184.216.34) 56(84) bytes of data. 64

bytes from 93.184.216.34: icmp_seq=1 ttl=56 time=10.3 ms 64

bytes from 93.184.216.34: icmp_seq=2 ttl=56 time=10.2 ms 64

bytes from 93.184.216.34: icmp_seq=3 ttl=56 time=10.1 ms

2. Nmap Scan Details

Starting Nmap 7.93 (https://nmap.org) at 2025-06-17 12:00

UTC Nmap scan report for example.com (93.184.216.34)

Host is up (0.010s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

Service Info: OS: Unix

3. Open Ports and Services

22/tcp - SSH

80/tcp - HTTP

443/tcp - HTTPS

4. Vulnerabilities Found

- Port 22 (SSH): No specific vulnerabilities found, but brute-force attacks are common. - Port 80

(HTTP): Could be vulnerable to outdated software (e.g., Apache or Nginx vulnerabilities). - Port

443 (HTTPS): Ensure SSL/TLS configurations are up-to-date to avoid known vulnerabilities.

5. Critical Assets

- Web Server (HTTP/HTTPS): Serves content to users and handles sensitive data. -

SSH Service: Provides remote administrative access; critical for maintaining the server.

6. Threat Hunting Commentary

Based on the scan results, the web server (example.com) is running HTTP and HTTPS services along with

SSH.

These are common targets for attackers. It's recommended to:

- Ensure strong password policies and possibly use key-based SSH authentication.

- Keep the web server and its software dependencies up to date.

- Regularly scan for SSL/TLS vulnerabilities.

- Monitor access logs for suspicious activity.

```
1 # Nmap 7.94SVN scan initiated Tue Jun 17 17:04:34 2025 as: nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
2 Nmap scan report for demo.owasp-juice.shop (81.169.145.156)
3 Host is up (0.11s latency).
4 Other addresses for demo.owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
5 rDNS record for 81.169.145.156: w9c.rzone.de
6 Not shown: 993 closed tcp ports (reset)
7 PORT     STATE    SERVICE     VERSION
8 21/tcp   open     ftp         ftpd.bin round-robin file server 3.4.0r16
9 25/tcp   filtered smtp
10 80/tcp   open     http-proxy  F5 BIG-IP load balancer http proxy
11 |_http-csrf: Couldn't find any CSRF vulnerabilities.
12 | http-enum:
13 |   /blog/: Blog
14 |   /weblog/: Blog
15 |   /weblogs/: Blog
16 |   /wordpress/: Blog
17 |   /wiki/: Wiki
18 |   /mediawiki/: Wiki
19 |   /wiki/Main_Page: Wiki
20 |   /tikiwiki/: Tikiwiki
21 |   /cgi-bin/mj_wwwusr: Majordomo2 Mailing List
22 |   /majordomo/mj_wwwusr: Majordomo2 Mailing List
23 |   /j2ee/examples/servlets/: Oracle j2ee examples
24 |   /j2ee/examples/jsp/: Oracle j2ee examples
25 |   /dsc/: Trend Micro Data Loss Prevention Virtual Appliance
26 |   /reg_1.htm: Polycom IP phone
27 |   /adr.htm: Snom IP Phone
```

Top terminal (Parrot Terminal - nmap vuln scan output):

```
                    https://www.securityfocus.com/bid/49303
                    https://seclists.org/fulldisclosure/2011/Aug/175
|_                  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|_   /blog/: Blog
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-vuln-cve2010-0738:
|_   /jmx-console/: Authentication was not required
445/tcp  filtered microsoft-ds
8080/tcp open     http-proxy    F5 BIG-IP load balancer http proxy
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-server-header: BigIP
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 504.75 seconds
┌─[user@parrot]─[~/Desktop]
└─ $sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
```

juice_scan.txt editor (top window):
```
1 # Nmap 7.94SVN scan init
  nmap -sV -sC --script vul
  juice.shop
2 Nmap scan report for demo
3 Host is up (0.11s latency
4 Other addresses for demo.
  2a01:238:20a:202:1156::
5 rDNS record for 81.169.1
6 Not shown: 993 closed tcp
7 PORT     STATE    SERVICE
8 21/tcp   open     ftp
  server 3.4.0r16
9 25/tcp   filtered smtp
10 80/tcp   open     http-p
   proxy
```

Bottom terminal (Parrot Terminal - nmap scan output):
```
┌─[user@parrot]─[~/Desktop]
└─ $sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-17 17:04 UTC
Nmap scan report for demo.owasp-juice.shop (81.169.145.156)
Host is up (0.11s latency).
Other addresses for demo.owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::
rDNS record for 81.169.145.156: w9c.rzone.de
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
21/tcp   open     ftp           ftpd.bin round-robin file server 3.4.0r16
25/tcp   filtered smtp
80/tcp   open     http-proxy    F5 BIG-IP load balancer http proxy
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /blog/: Blog
|   /weblog/: Blog
|   /weblogs/: Blog
|   /wordpress/: Blog
|   /wiki/: Wiki
|   /mediawiki/: Wiki
|   /wiki/Main_Page: Wiki
|   /tikiwiki/: Tikiwiki
|   /cgi-bin/mj_wwwusr: Majordomo2 Mailing List
|   /majordomo/mj_wwwusr: Majordomo2 Mailing List
```