Title: Pen Test on [redacted], [redacted], and [redacted]
Name: Rafik Tarbari
Date: September 29, 2022

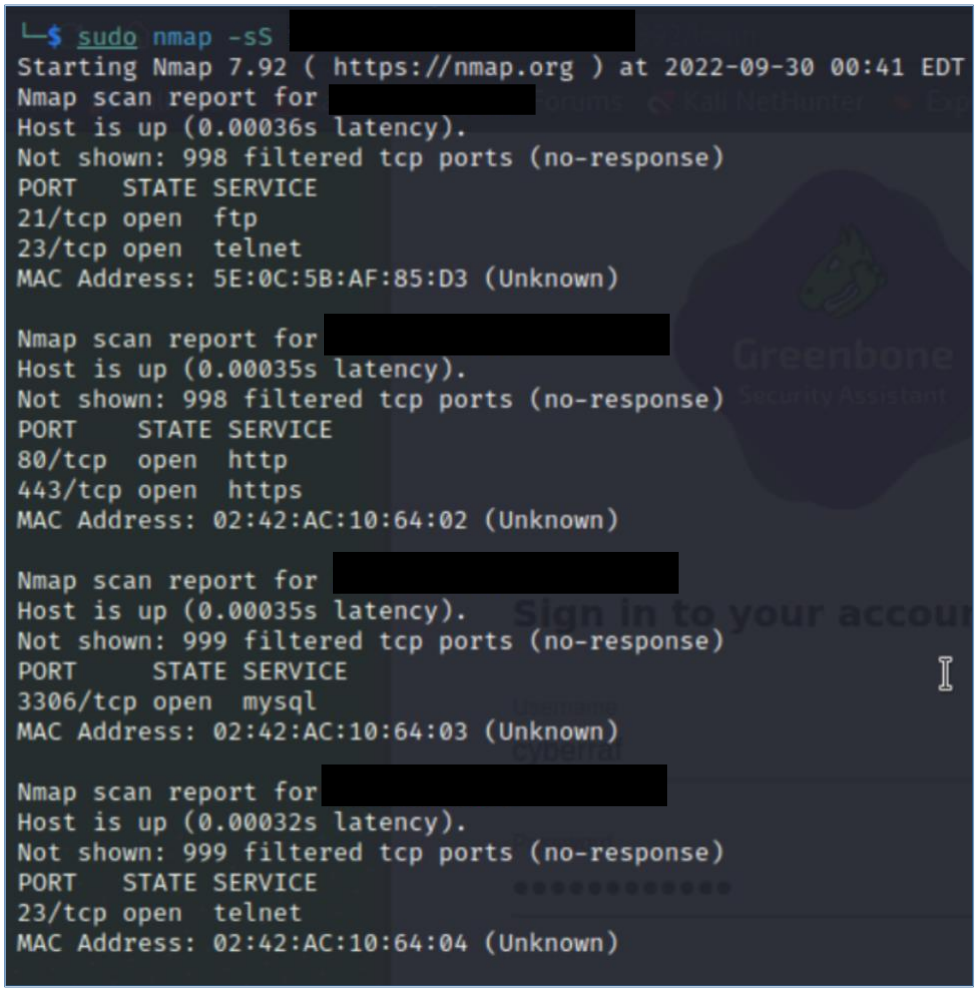
Introduction:

In this report, we are conducting a recon on [redacted], [redacted], and [redacted]. We will be gathering general information (hosts up that are up, open ports, vulnerabilities) on the hosts.

Using nmap:
sudo nmap -sS [redacted]

** *-sS* establishes a stealth TCP connection when *-sT* does for a simple TCP connection (meaning that the firewall can detect and block the connection). Doing the 2 different scans, we obtain the same result of number of hosts that are up.

6 hosts are up on the [redacted]



```
Nmap scan report for [redacted]
Host is up (0.00030s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 02:42:AC:10:64:05 (Unknown)

Nmap scan report for [redacted]
Host is up (0.00055s latency).
All 1000 scanned ports on [redacted] are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 02:42:AC:10:64:06 (Unknown)
```

sudo nmap [redacted]

Ports **22** and **80** are open, this host must be a **web-server.** The OS running on the server is **linux.**
Network Distance: 1 hop

```
└─$ sudo nmap -O [redacted]
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 00:18 EDT
Nmap scan report for [redacted]
Host is up (0.00013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: B2:C0:9A:42:39:2B (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc|firewall|WAP
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X|2.4.X (95%), Synology DiskStation Manager 5.X (90%), WatchGuard Fireware 11.X (89%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/a:synology:diskstation_manager:5.2 cpe:/o:linux:linux_kernel cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.0 - 5.4 (95%), Linux 2.6.32 (95%), Linux 2.6.32 or 3.10 (95%), Linux 4.4 (95%), Linux 5.0 - 5.3 (94%), Linux 5.4 (94%), Linux 2.6.32 - 2.6.35 (93%), Linux 2.6.32 - 2.6.39 (93%), Linux 2.6.32 - 3.0 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.02 seconds
```

sudo nmap [redacted]

This host is down; it is unreachable. We tried ping and nmap but we were uncessful.

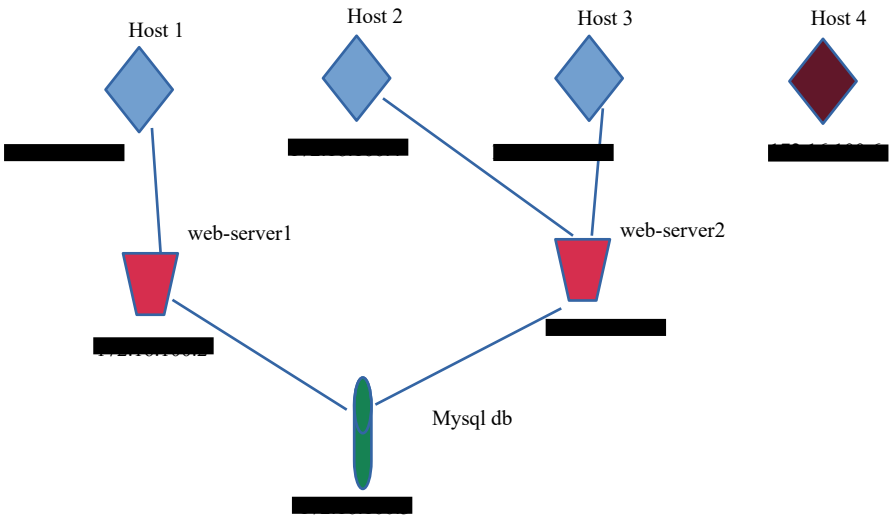
```
┌──(kali㉿kali-ws)-[~]
└─$ sudo nmap -O -sT [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 00:28 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.69 seconds

┌──(kali㉿kali-ws)-[~]
└─$ ping [redacted]
PING [redacted] ([redacted]) 56(84) bytes of data.
From [redacted] icmp_seq=1 Destination Host Unreachable
From [redacted] icmp_seq=2 Destination Host Unreachable
From [redacted] icmp_seq=3 Destination Host Unreachable
From [redacted] icmp_seq=4 Destination Host Unreachable
From [redacted] icmp_seq=5 Destination Host Unreachable
From [redacted] icmp_seq=6 Destination Host Unreachable
^C
--- [redacted] ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 8182ms
pipe 4
```

List of Ips/hosts that are up:

1. [redacted] *(open ports: 21 (ftp), 23 (telnet); OS: Linux)*
2. [redacted] *(web-server; open ports: 80 (http), 443 (https); OS: Linux)*
3. [redacted] *(mysql database; open ports: 3306 (mysql); OS: Linux)*
4. [redacted] *(open ports: 23 (telnet); OS: Linux)*
5. [redacted] *(open ports: 23 (telnet); OS: Linux)*
6. [redacted] *(open ports: None)*
7. [redacted] *(web-server; open ports: 22 (ssh), 80 (http); OS: Linux)*

TOPOLOGY



Checking Vulnerabilities:

** [redacted]

No vulnerabilities found.

```
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.0 - 5.4 (95%
), Linux 5.0 - 5.3 (94%), Linux 2.6.32 or 3.10 (94%), Linux 5.4 (93
x 2.6.32 - 2.6.39 (93%), Linux 4.0 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.13 ms [redacted]

OS and Service detection performed. Please report any incorrect res
Nmap done: 1 IP address (1 host up) scanned in 16.74 seconds
zsh: segmentation fault  sudo nmap -A [redacted]
```

Traceroute:
1 Hop 0.13 seconds

** [redacted]
The web-server is running Apache httpd 2.4.41

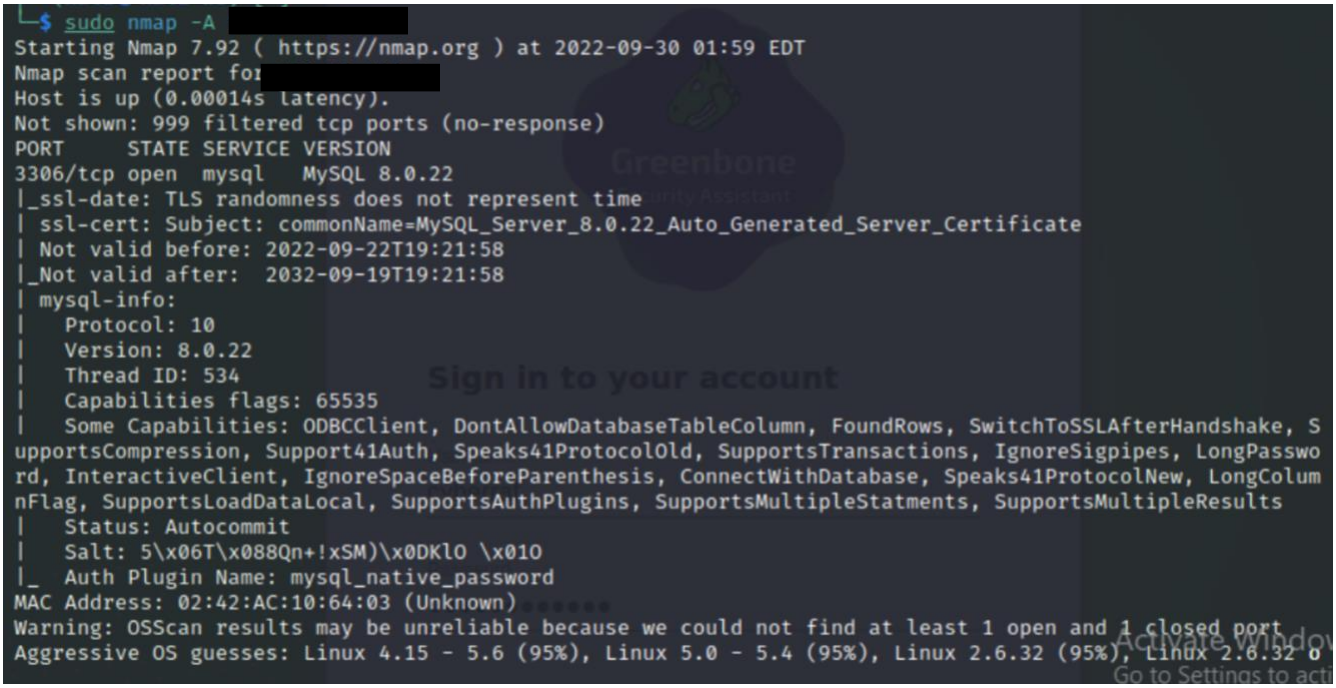
```
└─$ sudo nmap -A [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 01:49 EDT
Nmap scan report for [redacted]
Host is up (0.00013s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
443/tcp open  http    Apache httpd 2.4.41
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 02:42:AC:10:64:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 2.6.32 (95%), Linux 2.6.32 or 3.10 (95%), Linu
 (95%), Linux 5.0 - 5.3 (94%), Linux 5.4 (94%), Linux 5.0 - 5.4 (94%), Linux 2.6.32 - 2.6.35 (93%),
x 2.6.32 - 2.6.39 (93%), Linux 4.0 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: localhost

TRACEROUTE
HOP RTT     ADDRESS
1   0.13 ms [redacted]

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 20.54 seconds
zsh: segmentation fault  sudo nmap -A [redacted]
```

Traceroute:
1 Hop 0.13 seconds

** [redacted]
This database is running mysql version 8.0.22; we can also explore the capabilities of the database; authentication plugin



Traceroute:
1 Hop 0.14 seconds

**[redacted]

Traceroute
1 Hop 0.18 seconds

** [redacted]

Traceroute
1 Hop 0.14 seconds

** [redacted]

Traceroute
1 Hop 0.18 seconds

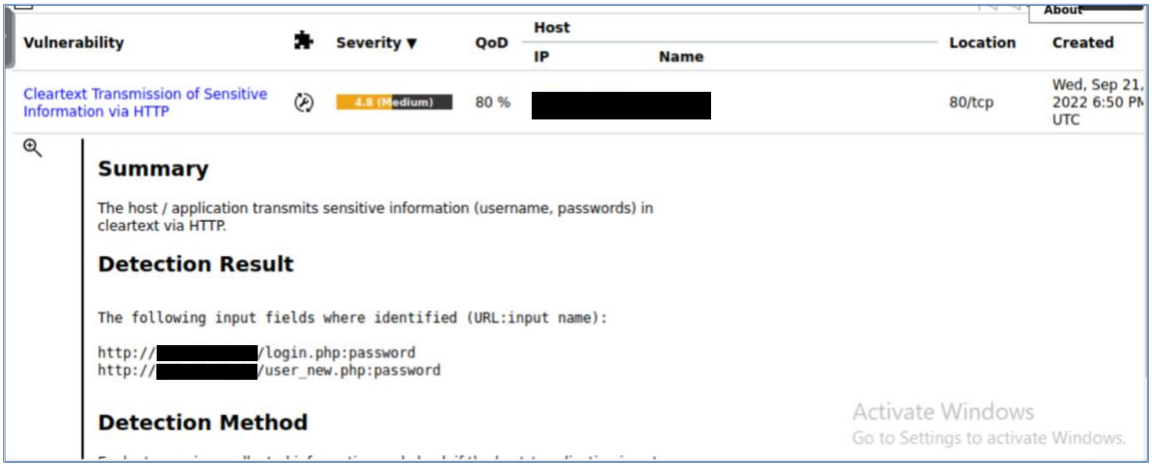
** [redacted]

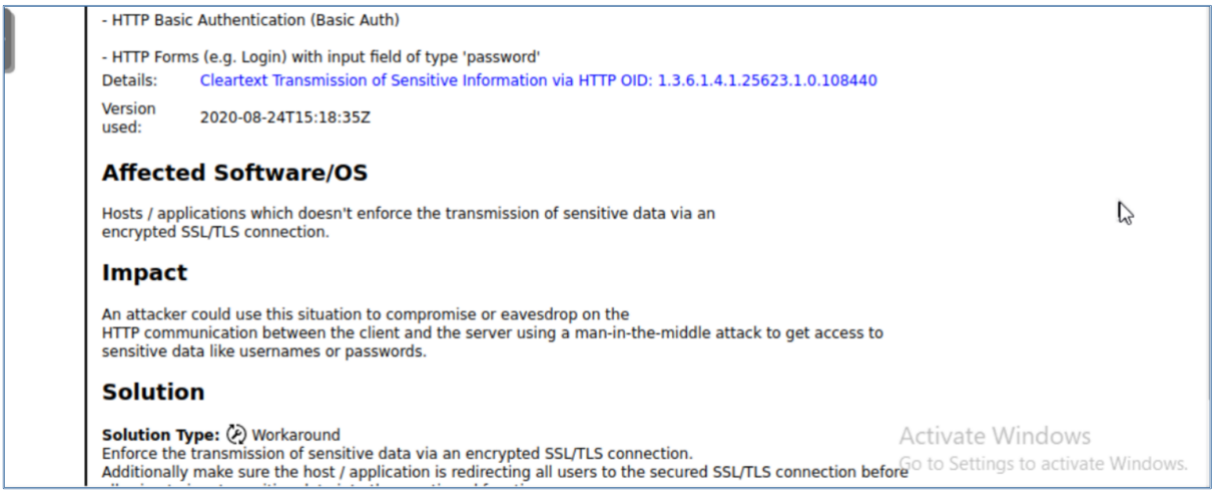
There are many vulnerabilities on the open port 80 of the web-server which is running Apache httpd 2.4.41

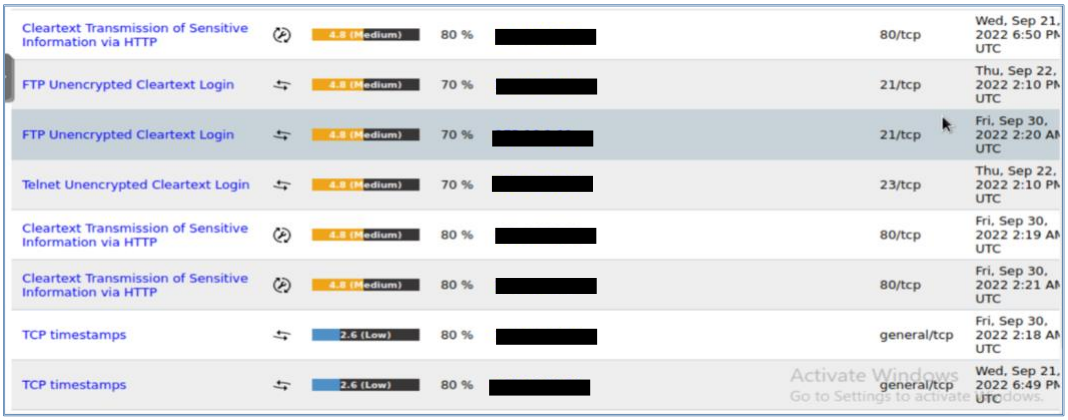
```
┌──(kali㉿kali-ws)-[~]
└─$ sudo nmap -A [redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 02:23 EDT
Nmap scan report for [redacted]
Host is up (0.00015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 8f:25:f2:29:ef:d6:36:8a:4c:bd:65:ee:2b:23:90:e5 (RSA)
|   256 66:ea:c5:9f:cd:26:ca:84:4f:f7:ab:88:da:e6:90:30 (ECDSA)
|_  256 00:3b:da:0a:a6:63:3d:1f:69:c5:80:dc:16:72:ea:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 5 disallowed entries
|_/ /admin/ /documents/ /images/ /passwords/
| http-title: bWAPP - Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: B2:C0:9A:42:39:2B (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 2.6.32 (95%), Linux 2.6.32 or 3.10 (95%), Linux 4.4
 (95%), Linux 5.0 - 5.3 (94%), Linux 5.4 (94%), Linux 5.0 - 5.4 (94%), Linux 2.6.32 - 2.6.35 (93%), Linu
```

Traceroute:
1 Hop 0.15 seconds

Openvas Scanning Results on [redacted] and [redacted]







Conclusion:

Using main tools/commands such as nmap, traceroute, ping, and the openvas software, we have collected 7 hosts that are up : 4 host computers, 2 web-servers, and 1 mysql database. We have found one main vulnerability on the web-servers (.100.2 and .22.58). The port 80 are opened and the hosts/applications are exchanging sensitive data in plain text. We have also found some vulnerabilities on the mysql database (.100.3)