532 Corp Report: **Tyler O'Hare**

● Scenario:

532 Corp is a large multinational corporation whose primary source of revenue is from its research and development activities. 532 Corp has concerns that their employees are leaking company secrets and actively trying to bring 532Corp down. 532Corp is also at severe risk of being exploited since their cybersecurity engineer just left the company.

Sarah, the former cybersecurity engineer at 532 Corp was in charge of securing all the company data and ensuring that hackers could not take advantage of any potential vulnerabilities. Unfortunately, she left the company and hasn't really left much information behind.

The CEO of 532Corp hired you to access any vulnerabilities that Sarah "forgot" to document. Let's just say she didn't really leave 532 Corporation on the best terms (cough cough she was fired) and hence her work wasn't really documented well.She didn't really leave much behind as to what she found, but we're hoping that you can figure out all the vulnerabilities. For all we know, 532Corp could be hacked already.

Your task is to perform an assessment on what Sarah left behind and perform penetration tests where necessary to see if any aspects of the 532Corporation network are susceptible to being exploited. Anything you find sketchy or can essentially "hack" is important for us to know

● Executive Summary:

It is undeniable that Sarah left 532 corp in a ruined state after her departure. I found that overall 532 corp is at risk for several high impact vulnerabilities that need to be addressed immediately. In the network's current state, several user accounts are compromised meaning that 532 corp runs the risk of having information leaked. Any information sent throughout the network using telnet is at risk of being eavesdropped on. I found a few out of date software running on the network along with an out of date wordpress website that is susceptible to high risk attacks. These problems need to be remediated immediately to stop anyone who tries, or already has hacked into 532 corp. Failure to do so may lead to significant financial loss to 532 corp.

● **Issues Identified**:

Footprinting:

a. The first step I conducted was footprinting of 532 corp. I visited https://532corp.hackerville.org and the bios for the employees at 532 corps are very personal and can be used to form a custom wordlist for a bruteforce attack. So I created a custom wordlist for every word on the site by copying and pasting the text on the site into a space delimited wordlist creator. **Strategic Recommendation:** To avoid attacks like this from being possible I recommend removing the personal bios from the public as they are easily accessible for attackers.
b. I was also able to create an account at https://532corp.hackerville.org with no validation that I needed to work for the company. Along with this, I was able to use a relatively low security password when signing up for the account. **Strategic Recommendation:** It should be made a requirement to have strong passwords associated with all employee accounts and to limit who can create an account to just employees.
c. Continuing on with my 532 corp footprinting I found that https://532corp.hackerville.org is run using wordpress. Wordpress is known to be susceptible to attacks so I decided to run a vulnerability scan on the site. It was quickly found that the site has multiple wordpress related vulnerabilities on it.Here are the following vulnerabilities I was able to find:

   – https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24698

   – https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0233

   Strategic Recommendation: It is highly recommended to update all wordpress plugins so they can have the latest patches for these vulnerabilities. If possible, moving the site away from wordpress may be useful as well.

Scanning:

The next step I took was scanning the given network IP range with nmap. 12 Hosts were found in the NMAP Scan using the following command:

sudo nmap -sSV -O --script vuln 82.46.91.0/24 > resultsMAX2.txt

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-20 14:03 CDT
```

```
Nmap scan report for cpc87219-aztw31-2-0-cust9.18-1.cable.virginm.net
(82.46.91.10)
Host is up (0.0019s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10
(96%), Linux 2.6.32 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS
210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation
Manager 5.2-5644 (94%), Linux 2.6.32 - 3.5 (94%), Linux 3.4 - 3.10
(93%), Linux 2.6.32 - 2.6.35 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust99.18-1.cable.virginm.net (82.46.91.100)
Host is up (0.0018s latency).
All 1000 scanned ports on
cpc87219-aztw31-2-0-cust99.18-1.cable.virginm.net (82.46.91.100) are
filtered
Too many fingerprints match this host to give specific OS details

Nmap scan report for
cpc87219-aztw31-2-0-cust198.18-1.cable.virginm.net (82.46.91.199)
Host is up (0.0019s latency).
All 1000 scanned ports on
cpc87219-aztw31-2-0-cust198.18-1.cable.virginm.net (82.46.91.199) are
filtered
Too many fingerprints match this host to give specific OS details

Nmap scan report for
cpc87219-aztw31-2-0-cust199.18-1.cable.virginm.net (82.46.91.200)
Host is up (0.0020s latency).
Not shown: 998 closed ports
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%),
Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%),
Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17)
(94%), Linux 2.6.32 - 2.6.35 (94%), Linux 2.6.32 - 3.5 (94%), Linux
2.6.32 - 3.13 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust200.18-1.cable.virginm.net (82.46.91.201)
Host is up (0.0027s latency).
Not shown: 996 closed ports
PORT  STATE SERVICE   VERSION
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain      ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http        Apache httpd 2.4.41 ((Ubuntu))
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /login.php: Possible admin folder
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|     Slowloris tries to keep many connections to the target web
server open and hold
```

```
|     them open as long as possible.  It accomplishes this by opening
connections to
|     the target web server and sending a partial request. By doing
so, it starves
|     the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_    http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
3389/tcp open  ms-wbt-server xrdp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_rdp-vuln-ms12-020: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (92%), Synology
DiskStation Manager 5.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.4
cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1
Aggressive OS guesses: Linux 2.6.32 or 3.10 (92%), Linux 4.4 (92%),
Linux 2.6.32 (91%), Linux 4.0 (90%), Linux 2.6.32 - 2.6.35 (89%),
Linux 2.6.32 - 2.6.39 (89%), Linux 2.6.32 - 3.0 (87%), Linux 3.11 -
4.1 (87%), Linux 3.2 - 3.8 (87%), Linux 2.6.18 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust202.18-1.cable.virginm.net (82.46.91.203)
Host is up (0.0030s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
```

```
Device type: general purpose
Running (JUST GUESSING): Linux 4.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
Aggressive OS guesses: Linux 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust203.18-1.cable.virginm.net (82.46.91.204)
Host is up (0.0025s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.0 (90%), Linux 2.6.32 or 3.10 (87%),
Linux 2.6.32 (86%), Linux 4.4 (86%), Linux 2.6.32 - 2.6.35 (85%),
Linux 2.6.32 - 2.6.39 (85%), Linux 2.6.31 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net (82.46.91.205)
Host is up (0.0027s latency).
Not shown: 995 closed ports
PORT  STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
23/tcp  open  telnet?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp  open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

```
80/tcp  open  http    Apache httpd 2.4.41
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /: Root directory w/ listing on 'apache/2.4.41 (ubuntu)'
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-sql-injection:
|   Possible sqli for queries:
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dD%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dD%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
```

```
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dD%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dD%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dD%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
```

```
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=D%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=S%3bO
%3dA%27%20OR%20sqlspider
|
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=M%3bO
%3dA%27%20OR%20sqlspider
|_
http://cpc87219-aztw31-2-0-cust204.18-1.cable.virginm.net:80/?C=N%3bO
%3dA%27%20OR%20sqlspider
```

```
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.0 (90%), Linux 2.6.32 (87%), Linux
2.6.32 or 3.10 (87%), Linux 4.4 (87%), Linux 2.6.32 - 2.6.35 (85%),
Linux 2.6.32 - 2.6.39 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: 192.168.1.205; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust205.18-1.cable.virginm.net (82.46.91.206)
Host is up (0.0027s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /login.php: Possible admin folder
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.0 (90%), Linux 2.6.32 (87%), Linux
2.6.32 or 3.10 (87%), Linux 4.4 (87%), Linux 2.6.32 - 2.6.35 (85%),
```

```
Linux 2.6.32 - 2.6.39 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust206.18-1.cable.virginm.net (82.46.91.207)
Host is up (0.0029s latency).
Not shown: 995 closed ports
PORT  STATE SERVICE   VERSION
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain      ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3000/tcp open  http        Node.js (Express middleware)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|    Couldn't find a file-type field.
|
|_   Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
3389/tcp open  ms-wbt-server xrdp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_rdp-vuln-ms12-020: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
4000/tcp open  http        Node.js Express framework
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|    State: LIKELY VULNERABLE
|    IDs:  CVE:CVE-2007-6750
|    Slowloris tries to keep many connections to the target web
```

```
server open and hold
|     them open as long as possible.  It accomplishes this by opening
connections to
|     the target web server and sending a partial request. By doing
so, it starves
|     the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_    http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.0 (91%), Linux 2.6.32 (87%), Linux
2.6.32 or 3.10 (87%), Linux 4.4 (86%), Linux 2.6.32 - 2.6.35 (85%),
Linux 2.6.32 - 2.6.39 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust207.18-1.cable.virginm.net (82.46.91.208)
Host is up (0.0031s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux;
protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4.0
cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 4.0 (91%), Linux 2.6.32 (87%), Linux
2.6.32 or 3.10 (87%), Linux 4.4 (87%), Linux 2.6.32 - 2.6.35 (85%),
Linux 2.6.32 - 2.6.39 (85%)
```

```
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for
cpc87219-aztw31-2-0-cust253.18-1.cable.virginm.net (82.46.91.254)
Host is up (0.0010s latency).
All 1000 scanned ports on
cpc87219-aztw31-2-0-cust253.18-1.cable.virginm.net (82.46.91.254) are
filtered
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (12 hosts up) scanned in 462.29 seconds
```

A summary of the above information is provided below:

IP:	**Open Ports:**	**OS Guess:**	**Found scan vulnerabilities:**
82.46.91.10	**22/tcp:** ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0) **53/tcp:** domain ISC BIND 9.16.1 (Ubuntu Linux)	Ubuntu, Linux 3.2 - 4.9	
82.46.91.100	All ports filtered	Unknown	
82.46.91.199	All ports filtered	Unknown	
82.46.91.200	**22/tcp:** ssh OpenSSH 8.2p1 **53/tcp:** domain ISC BIND 9.16.1	Ubuntu, Linux 3.2 - 4.9, 2.6.32 - 3.10	
82.46.91.201	**22/tcp:** ssh OpenSSH 8.2p1 **53/tcp:** domain ISC BIND 9.16.1	Linux 2.6.X|3.X|4.X (92%), Synology DiskStation Manager 5.X (85%)	Slowloris DOS attack: State: LIKELY VULNERABLE

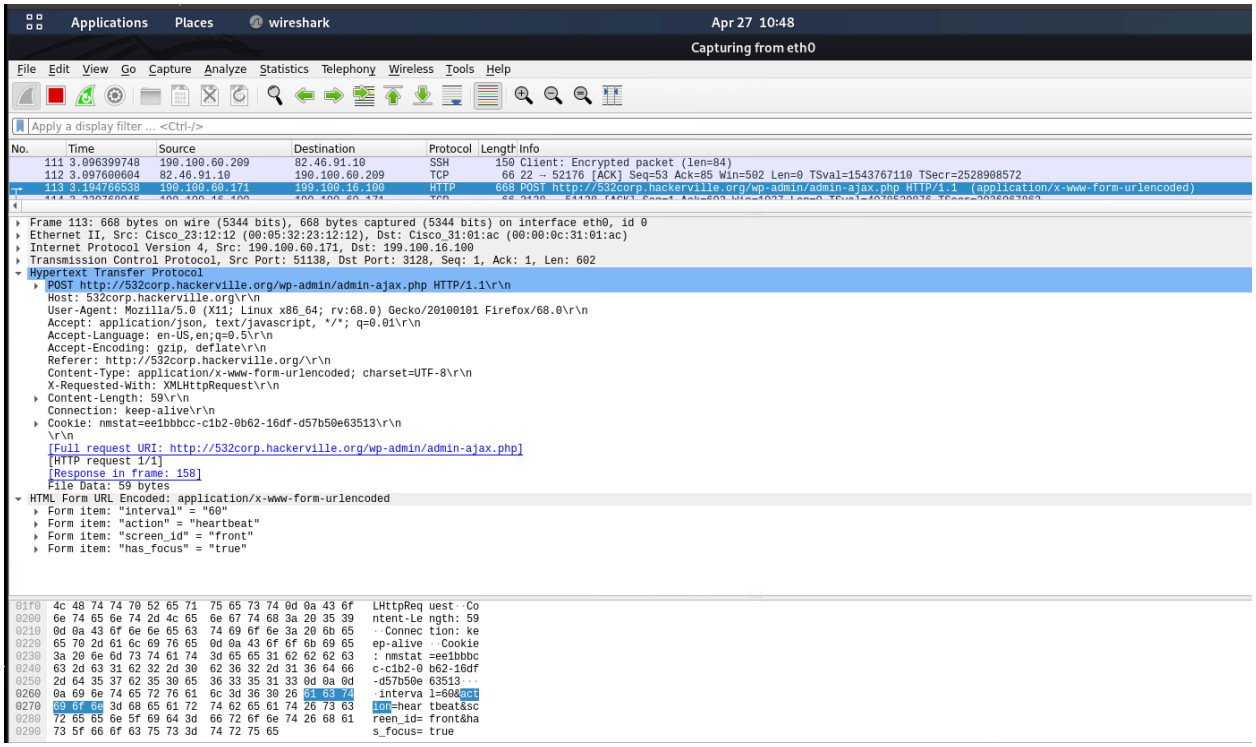
	80/tcp: http Apache httpd 2.4.41 ((Ubuntu)) **3389/tcp:** ms-wbt-server xrdp		CVE:CVE-2007-67 50
82.46.91.203	**22/tcp:** ssh OpenSSH 8.2p1	Linux 4.X	
82.46.91.204	**22/tcp:** ssh OpenSSH 8.2p1 **53/tcp:** domain ISC BIND 9.16.1	Linux 4.0 (90%), Linux 2.6.32 or 3.10 (87%)	
82.46.91.205	**22/tcp:** ssh OpenSSH 8.2p1 **23/tcp:** telnet? **53/tcp:** domain ISC BIND 9.16.1 **80/tcp:** http Apache httpd 2.4.41 **389/tcp:** ldap OpenLDAP 2.2.X - 2.3.X	Linux 4.X|2.6.X|3.X Service Info: Host: 192.168.1.205;	Possible sql injections, telnet is vulnerable.
82.46.91.206	**22/tcp:** ssh OpenSSH 8.2p1 **53/tcp:** domain ISC BIND 9.16.1 **80/tcp:** http Apache httpd 2.4.41	Linux 4.X|2.6.X|3.X	| http-enum: |_ /login.php: Possible admin folder
82.46.91.207	**22/tcp:** ssh OpenSSH 8.2p1 **53/tcp:** domain ISC BIND 9.16.1 **3000/tcp:** http Node.js (Express middleware) **3389/tcp:** ms-wbt-server xrdp **4000/tcp:** http Node.js Express framework	Linux 4.X|2.6.X|3.X	VULNERABLE:Slo wloris DOS attack State: LIKELY VULNERABLE CVE:CVE-2007-67 50

82.46.91.208	**22/tcp:** ssh OpenSSH 8.2p1 **53/tcp:** domain ISC BIND 9.16.1	Linux 4.0	
82.46.91.254	All ports filtered	Unknown	

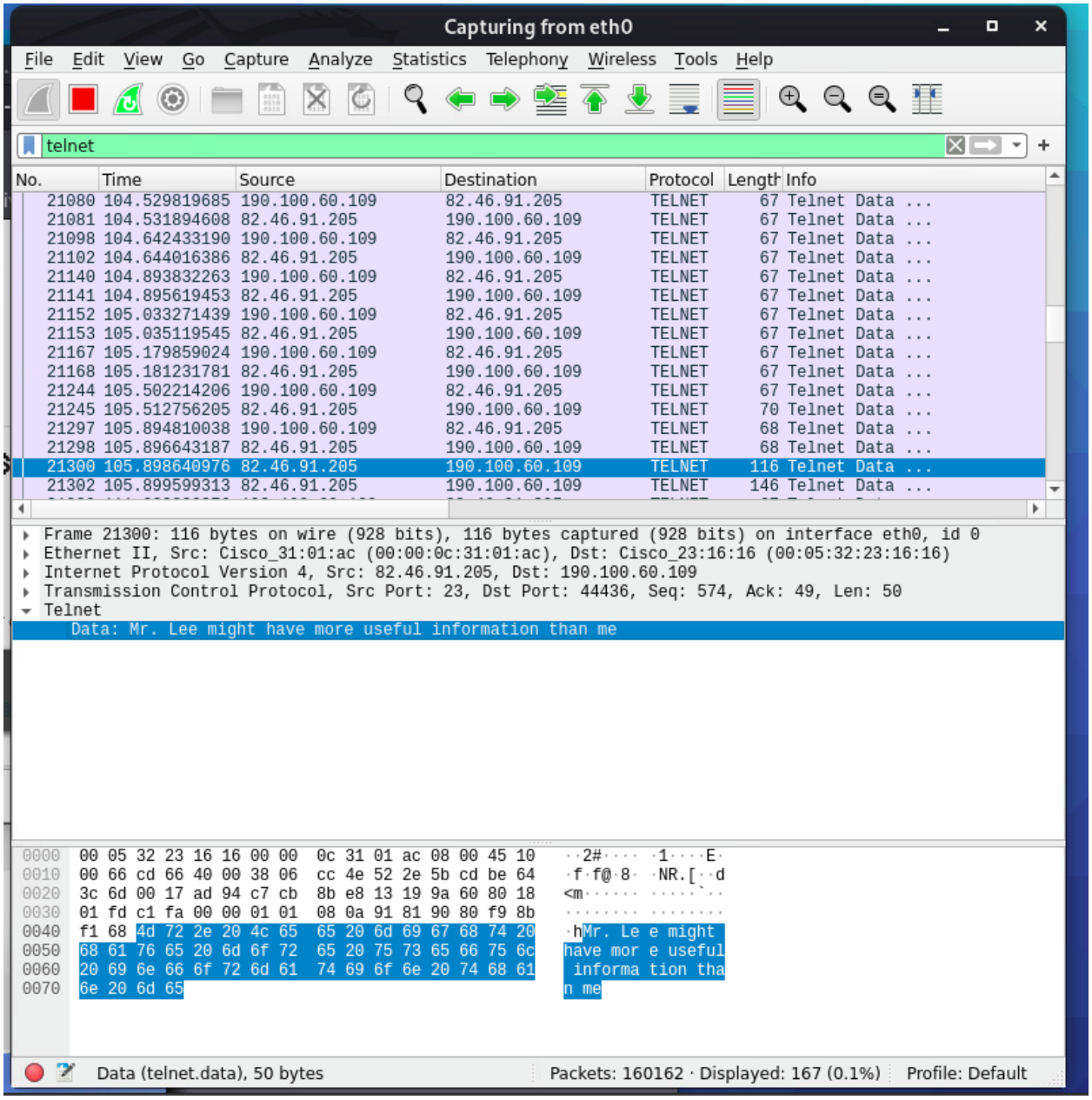
Based on the results of the scan there are quite a few issues to be aware of.

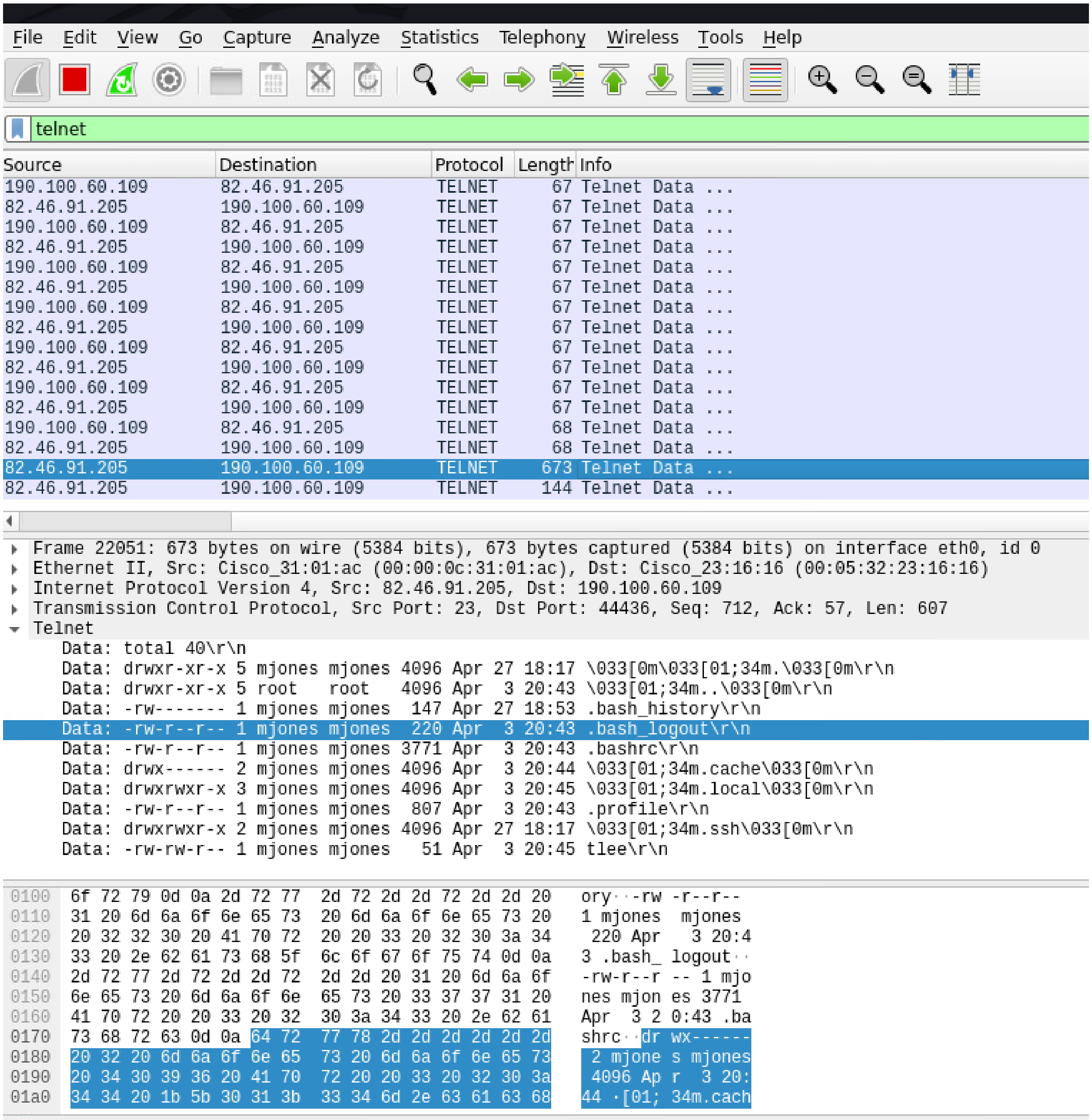
a. For IPs 82.46.91.10, 82.46.91.200, 82.46.91.201, 82.46.91.204, 82.46.91.205, 82.46.91.206, 82.46.91.207, 82.46.91.208 port 22 ssh is open for user remote connections. It was found that I could brute force the SSH logins using metasploit module auxiliary(scanner/ssh/ssh_login). While an attack like this one would take a large amount of time, users with easy to guess passwords can easily be compromised this way. **Strategic Recommendation:** You can configure SSH to timeout repeat login attempts making it extremely difficult to perform this kind of attack.
b. For IPs 82.46.91.10, 82.46.91.200, 82.46.91.201, 82.46.91.204, 82.46.91.205, 82.46.91.206, 82.46.91.207, 82.46.91.208 port 53 was found using ISC BIND 9.16.1. After some quick research we can see that ISC Bind 9.16.1 is outdated and vulnerable to multiple attacks including DNS cache spoofing. I then Attempted to attack the DNS cache spoof attack with metasploit but was unsuccessful. **Strategic Recommendation:** Make sure BIND is updated to its latest version to avoid these vulnerabilities. If DNS is not required, then simply disable the service altogether.
c. For IPs 82.46.91.201, 82.46.91.205,82.46.91.206 Apache httpd 2.4.41 is being used on port 80. This seems to be an old version of Apache vulnerable to a few attacks. One major attack it is susceptible to is a slowloris DoS attack. This was found by the nmap vulnerability scanner script. **Strategic Recommendation:** Using an updated version of Apache and utilizing modules for apache like Mod_limitipconn, Mod_qos, Mod_evasive, Mod security, Mod_noloris, Mod_antiloris to prevent slowloris attacks.
d. I attempted an SSH bruteforce using my custom wordlist based off of the https://532corp.hackerville.org/ and found 532rockyou wordlist that seems to be left behind by Sarah. But no match was found with the given usernames list.
e. Scrolling through some wireshark data I found a suspicious connection to the company's website. There were 2 things that stood out to me mainly. First, after doing some research and visiting http://532corp.hackerville.org/wp-admin.admin-ajax.php I found that this led to a page with a in it. Researching further I found this link can be susceptible to a wordpress arbitrary file upload attack. Secondly, I found that this packet presents

a cookie in plaintext. It may be possible for this cookie to be used for some sort of session hijacking. I was unsuccessful in my attempt to execute it though. **Strategic Recommendations**:I found that this sort of issue is because of a wordpress misconfiguration and can be solved with a proper configuration implementation. Otherwise, ditching wordpress may be a better choice.



f. Open remote desktop port on 3389 for multiple machines. I was able to successfully connect to the port using rdesktop. This is susceptible to a brute force attack using Hydra. **Strategic Recommendations:** Take the process off of it's common network ports to make it harder to find. Make sure you have updated xrdp. Also, if not necessary remove the remote desktop.
g. On the 82.46.91.205 machine there is a possible SQL injection for multiple queries based on the nmap report. **Strategic Recommendations:**Minimize the number of user inputs allowed if possible. With user inputs you must have, make sure that the input is validated before accepting it.
h. Telnet is rather outdated. It does not provide encryption to the data that is being sent through it. My attempt to exploit this vulnerability led to me using Wireshark to listen to the telnet traffic for 82.46.91.205. I found the following information that could be employees sharing secrets:


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
No. Time Source Destination Protocol Length Info
21080 104.529819685 190.100.60.109 82.46.91.205 TELNET 67 Telnet Data ...
21081 104.531894608 82.46.91.205 190.100.60.109 TELNET 67 Telnet Data ...
21098 104.642433190 190.100.60.109 82.46.91.205 TELNET 67 Telnet Data ...
21102 104.644016386 82.46.91.205 190.100.60.109 TELNET 67 Telnet Data ...
21140 104.893832263 190.100.60.109 82.46.91.205 TELNET 67 Telnet Data ...
21141 104.895619453 82.46.91.205 190.100.60.109 TELNET 67 Telnet Data ...
21152 105.033271439 190.100.60.109 82.46.91.205 TELNET 67 Telnet Data ...
21153 105.035119545 82.46.91.205 190.100.60.109 TELNET 67 Telnet Data ...
21167 105.179859024 190.100.60.109 82.46.91.205 TELNET 67 Telnet Data ...
21168 105.181231781 82.46.91.205 190.100.60.109 TELNET 67 Telnet Data ...
21244 105.502214206 190.100.60.109 82.46.91.205 TELNET 67 Telnet Data ...
21245 105.512756205 82.46.91.205 190.100.60.109 TELNET 70 Telnet Data ...
21297 105.894810038 190.100.60.109 82.46.91.205 TELNET 68 Telnet Data ...
21298 105.896643187 82.46.91.205 190.100.60.109 TELNET 68 Telnet Data ...
21300 105.898640976 82.46.91.205 190.100.60.109 TELNET 116 Telnet Data ...
21302 105.899599313 82.46.91.205 190.100.60.109 TELNET 146 Telnet Data ...
Frame 21300: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_31:01:ac (00:00:0c:31:01:ac), Dst: Cisco_23:16:16 (00:05:32:23:16:16)
Internet Protocol Version 4, Src: 82.46.91.205, Dst: 190.100.60.109
Transmission Control Protocol, Src Port: 23, Dst Port: 44436, Seq: 574, Ack: 49, Len: 50
Telnet
Data: Mr. Lee might have more useful information than me
0000 00 05 32 23 16 16 00 00 0c 31 01 ac 08 00 45 10
0010 00 66 cd 66 40 00 38 06 cc 4e 52 2e 5b cd be 64
0020 3c 6d 00 17 ad 94 c7 cb 8b e8 13 19 9a 60 80 18
0030 01 fd c1 fa 00 00 01 01 08 0a 91 81 90 80 f9 8b
0040 f1 68 4d 72 2e 20 4c 65 65 20 6d 69 67 68 74 20
0050 68 61 76 65 20 6d 6f 72 65 20 75 73 65 66 75 6c
0060 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 74 68 61
0070 6e 20 6d 65
Data (telnet.data), 50 bytes
Packets: 160162 · Displayed: 167 (0.1%)
Profile: Default



I tried using the telnet ldap login using some of the words from these findings but was not successful. I was not able to probe this any further with the lack of information and context given. **Strategic Recommendations**: Make the switch from telnet to SSH for encryption and avoid eavesdropping as I did above.