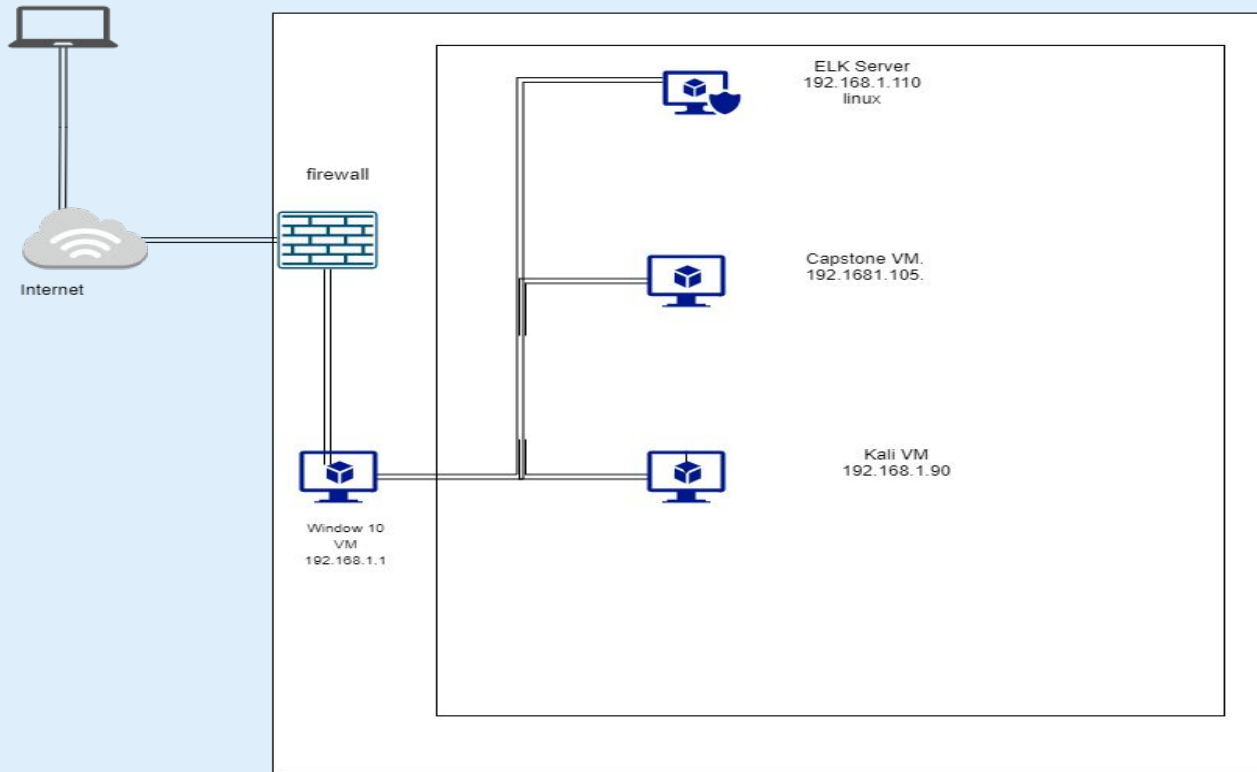


# Network Topology

my computer



## Network

Address Range: 1-255  
Netmask:255.255.255.0  
Gateway:192.168.1.1

## Machines

IPv4:192.168.1.100  
OS: Linux  
Hostname:ELK

IPv4:192.168.1.105  
OS:linux  
Hostname:capstone

IPv4:192.168.1.90  
OS:Linux  
Hostname:Kali

IPv4:192.168.1.1  
OS:Windows 10  
Hostname:ML-RefVm-68  
4427

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	Windows Remote VM with hypervisor
kali	192.168.1.90	Attacker machine
capstone	192.168.10105	Vulnerable Target machine
Elk	192.168.1.100	SIEM VM for lab Environment

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Use the CVE number if it exists. Otherwise, use the common name.</i>	<i>Describe the vulnerability.</i>	<i>Describe what this vulnerability allows the attacker to do.</i>
NMAP port scanning enabled	I was able to see all the open ports without restriction, when i run the Nmap.	The attacker is able to gain access to the target machine due to knowing type of servers and information about the target machine.
Hydra Brute force	I was able to run Hydra nonstop to get as much information as I could	No alerts or security measures means I can endlessly force entry into the target resources
Easily cracked hashes and weak passwords	Readily available wordlists can crack the weak hashes used by personnel	It only takes one weak password to gain access and allow time to sniff out administrative control

# Exploitation: NMAP Scanning]

01

## Tools & Processes

Detailed NMAP scan of the capstone VM showed ports 22 port and 80 open and other ports as well

Port 80 was chosen as the most interesting to place start

02

## Achievements

The exploit achieved information about the target machine, such as type of server and model of the OS. and this is the best way to gain access to the target machine.

03

```
ShellNo.1
File Actions Edit View Help

3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp  open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.33 seconds
root@kali:~#
```

# Exploitation: [Hydra Brute Force]

01

## Tools & Processes

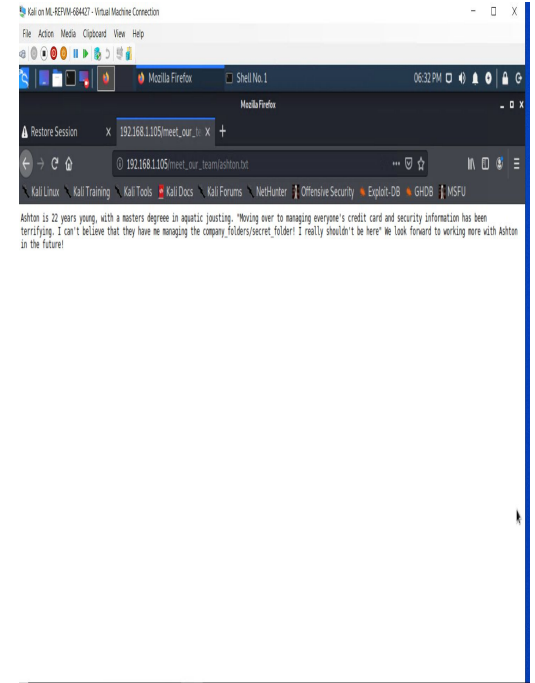
Hydra was used to access brute force account by using admin credentials.

02

## Achievements

I was able to access to webserve secret folder . that secret folder provider information that i can use to gain additional resources.

03



# Exploitation: [weak passwords and hashes]

01

## Tools & Processes

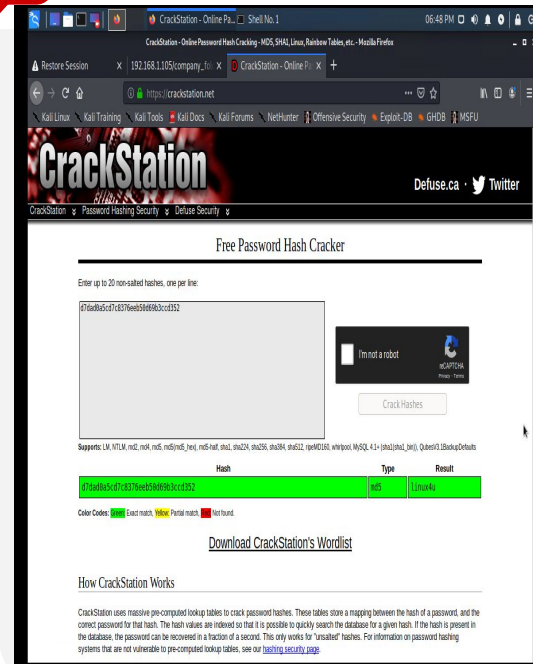
John the Ripper can easily and easily crack simple hashes.


02

## Achievements

John the Ripper gave access to network share for web server where malicious payload was delivered and gave me a shell on the box

03





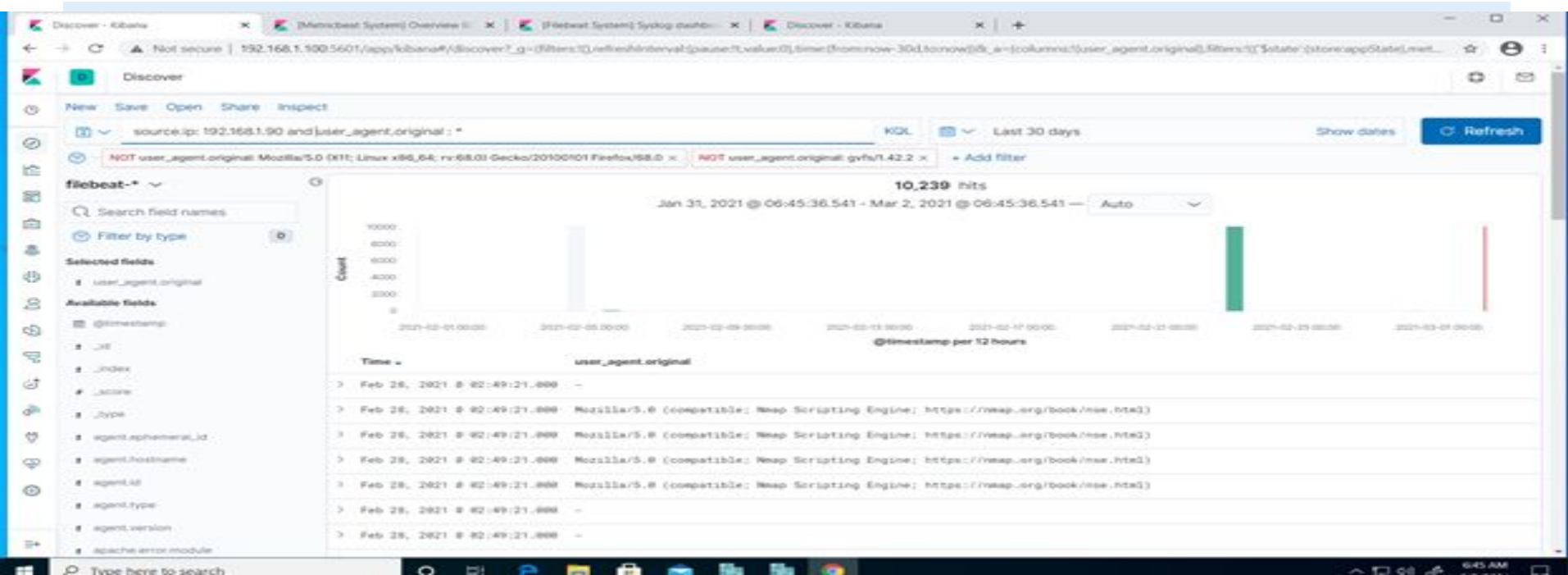
# **Blue Team**

## Log Analysis and Attack Characterization



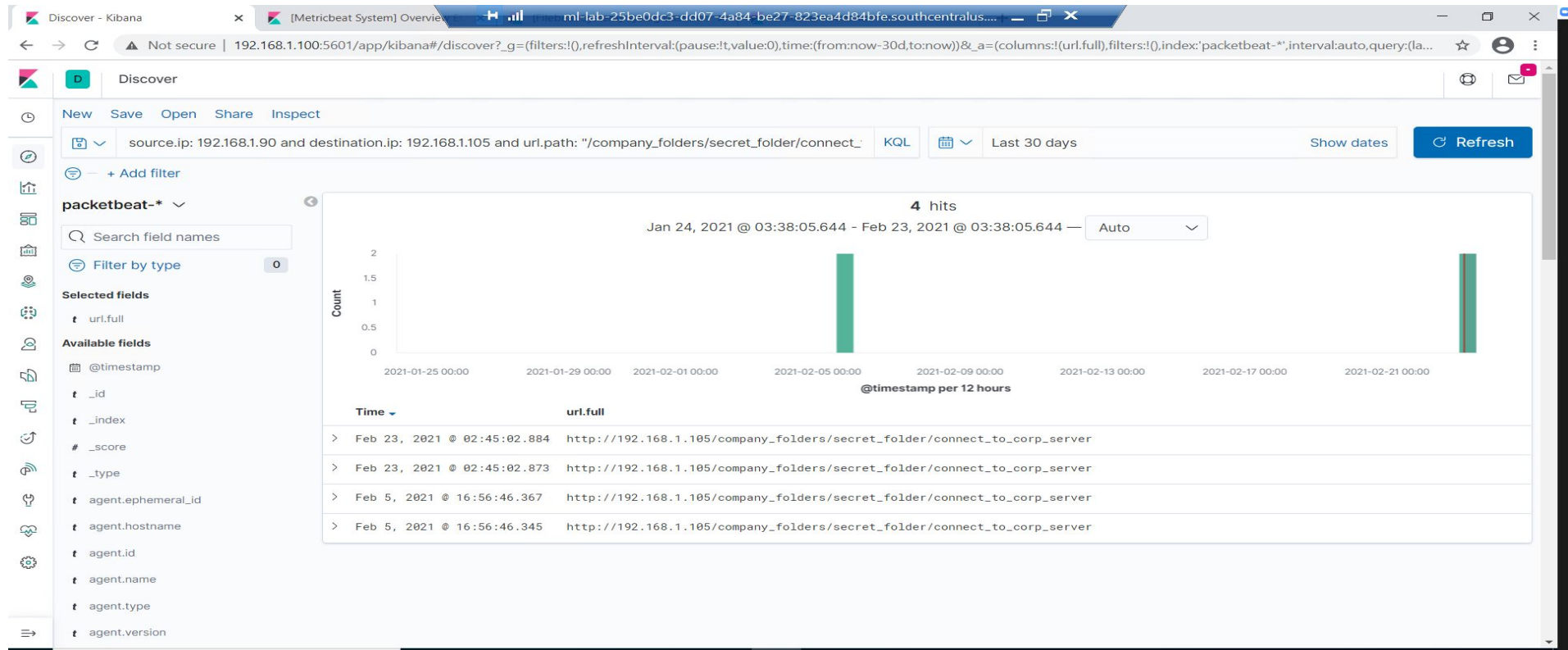
# Analysis: Identifying the Port Scan

- What time did the port scan occur? 02/28/21 @ 2:49
- How many packets were sent, and from which IP? 10,239
- What indicates that this was a port scan? User\_Agent NMAP scripting engine used



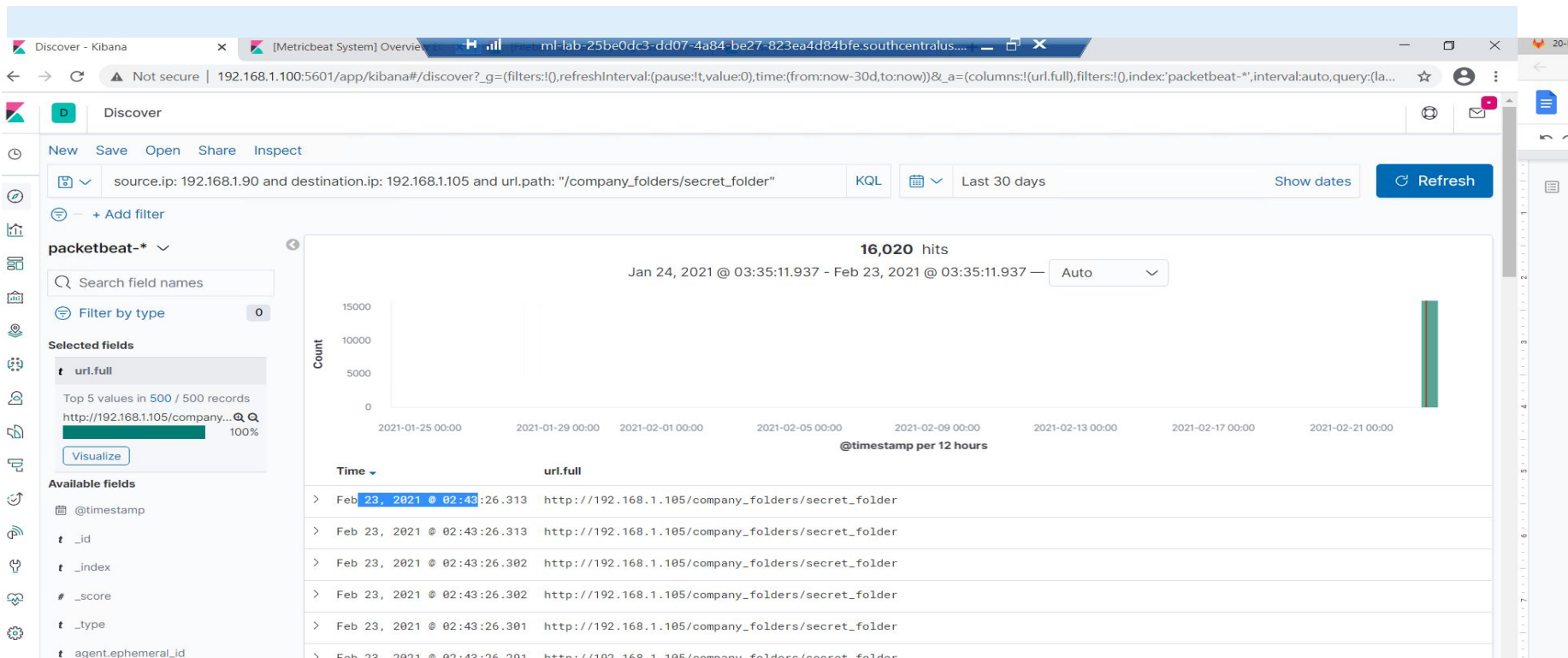
# Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? 02/23/21 @ 2:45. How many requests were made? 4
- Which files were requested? Connect\_to\_corp\_server. What did they contain? It contain Ryan's hash and directions.



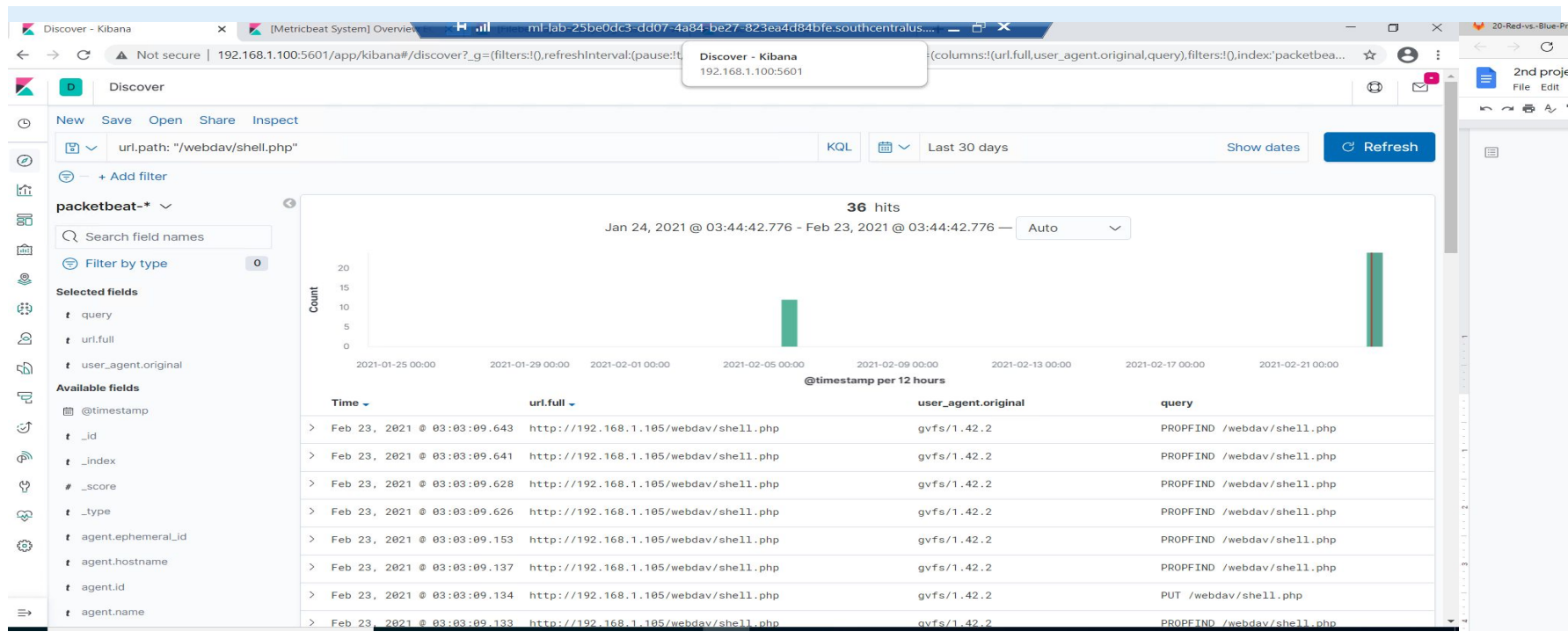
# Analysis: Uncovering the Brute Force Attack


- How many requests were made in the attack? 16020 hits
- How many requests had been made before the attacker discovered the password? 16019



# Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 36 hits
- Which files were requested? shell.php





# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

---

## Alarm

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

- Trigger an alert when ports other than 80 receive packets of data

What threshold would you set to activate this alarm?

- 5 packets within 1 minute to any port other than 80

## System Hardening

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

- Configure ICMP echo request and reply to block or drop all traffic

Describe the solution. If possible, provide required command lines.

- Syntax depends on specific appliance being configured. Likely cloud based deployment needed

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

What kind of alarm can be set to detect future unauthorized access?

- Alert to trigger when remote access to protected folders is detected.

What threshold would you set to activate this alarm?

- I would set this alarm, any packet that comes should be alert the SOC team.

## System Hardening

What configuration can be set on the host to block unwanted access?

- The system should not allow remote access to any secret folder or protect folders to be accessed other than admin team.

Describe the solution. If possible, provide required command lines.

- Web Server can only be allowed to specific files that are intended for remote access

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

What kind of alarm can be set to detect future brute force attacks?

- Alert trigger packets coming from ip address that is unknown as well as outside local network

What threshold would you set to activate this alarm?

- About 80-90 packets from legitimate ip address within 1 minutes

## System Hardening

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

- Patched or block any ip addresses that is unknown.

Describe the solution. If possible, provide the required command line(s).

- Configure network security group as well as the cloud security and block it any suspect issues.



# Mitigation: Detecting the WebDAV Connection

---

## Alarm

What kind of alarm can be set to detect future access to this directory?

- Alert to trigger if there is numerous resource outside of website data.

What threshold would you set to activate this alarm?

- This alarm should be set to zero.

## System Hardening

What configuration can be set on the host to control access?

- Ryan and Ashton did not do well on their job. Both need to be replaced by someone who is more skillful as well as get the job secure.

Describe the solution. If possible, provide the required command line(s).

- Ryan and Ashton should be searched thoroughly, before they leave the building and security should escort them.

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

What kind of alarm can be set to detect future file uploads?

- All files that end txt. Or pdf

What threshold would you set to activate this alarm?

- The alarm should set to zero.

## System Hardening

What configuration can be set on the host to block file uploads?

- Files should be prioritized to webdav

Describe the solution. If possible, provide the required command line.

- Be able to managed or configured to scan files on-going different networking.

*The  
End*