Capstone Engagement

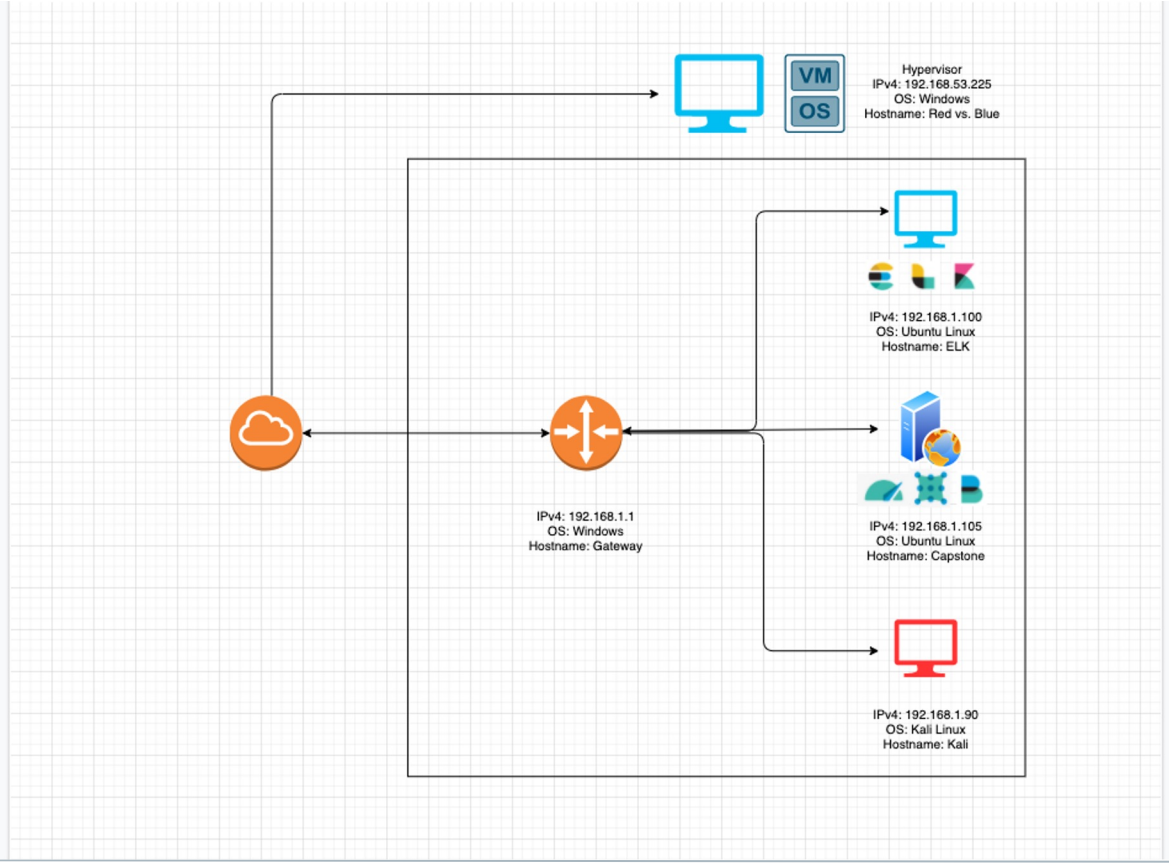
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.100
OS: Ubuntu Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.1
OS: Windows
Hostname: Gateway

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK Machine	192.168.1.100	ELK Server
Capstone Server	192.168.1.105	Apache HTTP WebDav Server
Kali Linux	192.168.1.90	Red Team PenTest Machine
Windows Gateway	192.168.1.1	Default Gateway Router

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure CWE-200	Information included in the public facing code, text, and documents that reveals personal Identifiable information like a name or employment information.	This allows attackers to narrow their field of focus through enumeration to further define/refine their attack surface.
Brute Force Vulnerability CVE-2020-14494	A BFV consists of an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response.	This allows attackers to run values, such as passwords, through software that will guess predetermined strings until a favorable response returns.
PHP Remote File Inclusion CVE-2006-2849	This allows attackers to execute malicious code remotely	This allows attackers to gain backdoor access via a reverse TCP connection

1) GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, http://www.gao.gov/new.items/d08536.pdf.
2) https://owasp.org/www-community/attacks/Brute_force_attack

Exploitation: Sensitive Data Exposure

01

Tools & Processes

Utilize nmap to scan the local network to enumerate which server is the target machine.

Access the vulnerable server through the IP address listed.

Scan the Webdav pages for Sensitive Data Exposure.

02

Achievements

This exploit allowed us to find the Webdav server.

Find three important pieces of information:

- secret_folder
- Ryan M. C.E.O
- Ashton is the manager of direct communication
- Ashton manages the secret folder
- Ryan manages the webdav folder

03

```
Ashton is 22 years young, with a masters
degreee in aquatic jousting. "Moving
over to managing everyone's credit card
and security information has been
terrifying. I can't believe that they
have me managing the
company_folders/secret_folder! I really
shouldn't be here" We look forward to
working more with Ashton in the future!
```

```
In order to connect to our companies
webdav server I need to use ryan's
account
(Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left
hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205
/webdav/"
4. I will be prompted for my user (but
i'll use ryans account) and password
5. I can click and drag files into the
share and reload my browser
```

Exploitation: Brute Force Vulnerability

01

Tools & Processes

Utilize the hydra and the enumerated web pages to crack the passwords.

Command:

Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder

02

Achievements

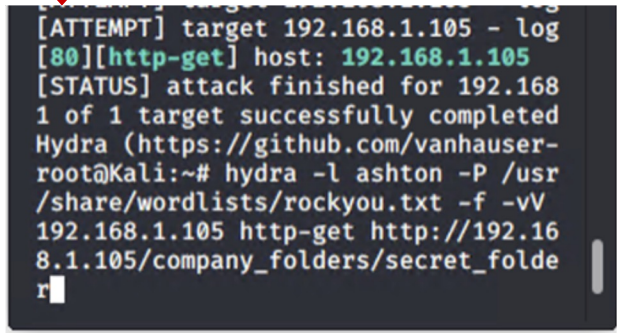
After running the command, we found ashton's login credentials:

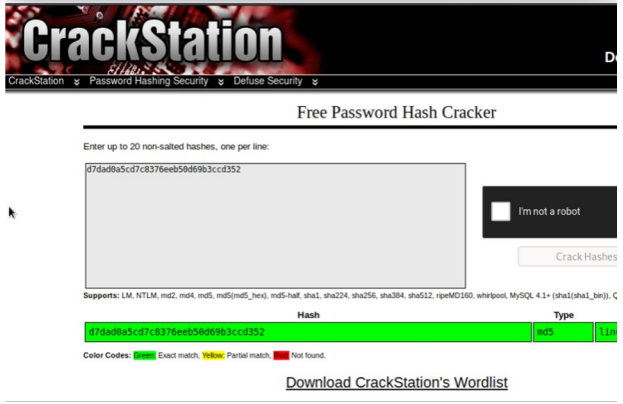
Username: ashton
Password: leopoldo

We then used the hash provided in the secret folder to crack ryan's password using crackstation:

username : ryan
Password: linux4u

03





Exploitation: Local File Inclusion/Unauthorized File Upload

01

Tools & Processes

After cracking the password hash for ryan's account, we then could add the WebDav file share to our Network Files manger.

This will allow us to upload the malicious PHP script that we later execute for a reverse tcp connection.

02

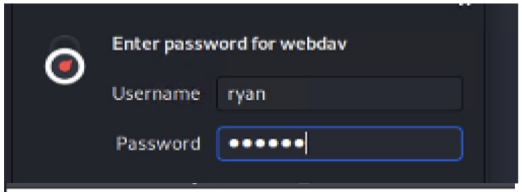
Achievements

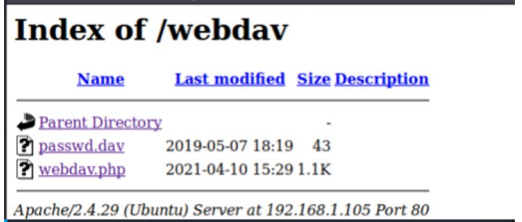
This allowed us to upload the malicious PHP script to initiate a reverse tcp connection.

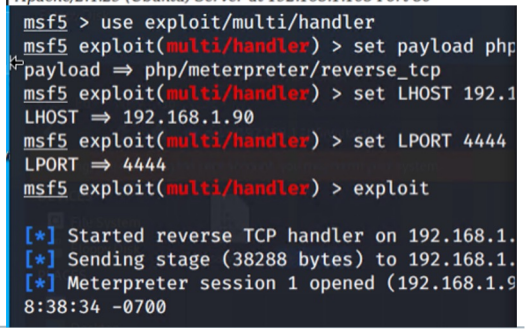
Msfvenom was used to build the script.

Msfconsole was used to open the meterpreter session that ultimately allowed us a remote connection to find the flag.

03

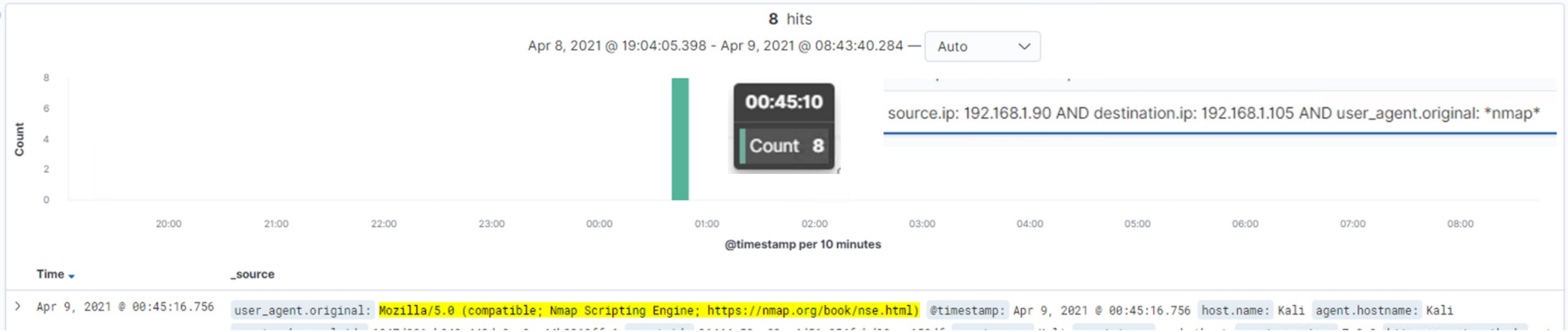




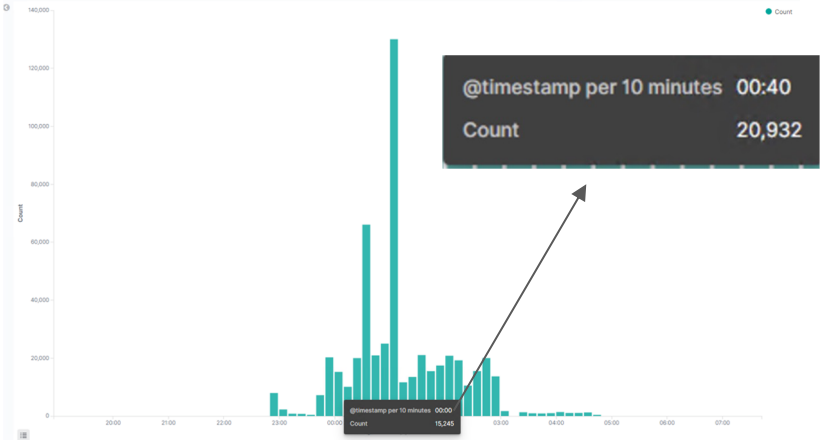


Blue Team
Log Analysis and Attack Characterization

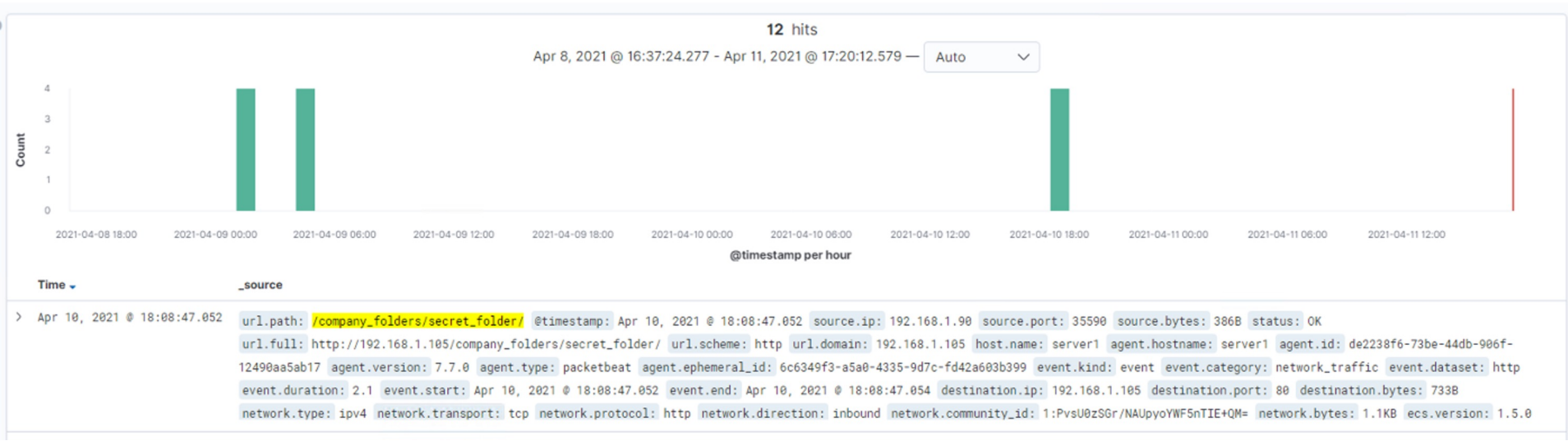
Analysis: Identifying the Port Scan



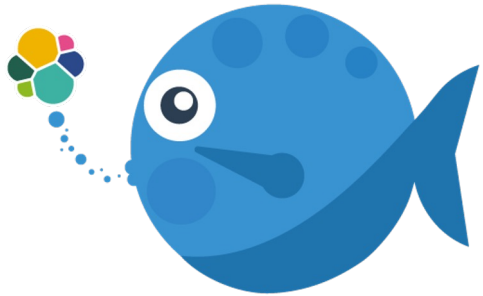
- We know the port scan occurred at 0:45 on 04-09-2021 from 192.168.1.90
- After analyzing the network flow, we can approximate that 20,932 packets were sent during the scan.
- The user_agent was used to indicate that a port scan occurred by utilizing nmap (top).
- The network_flow indicated the amount of packets sent (right).



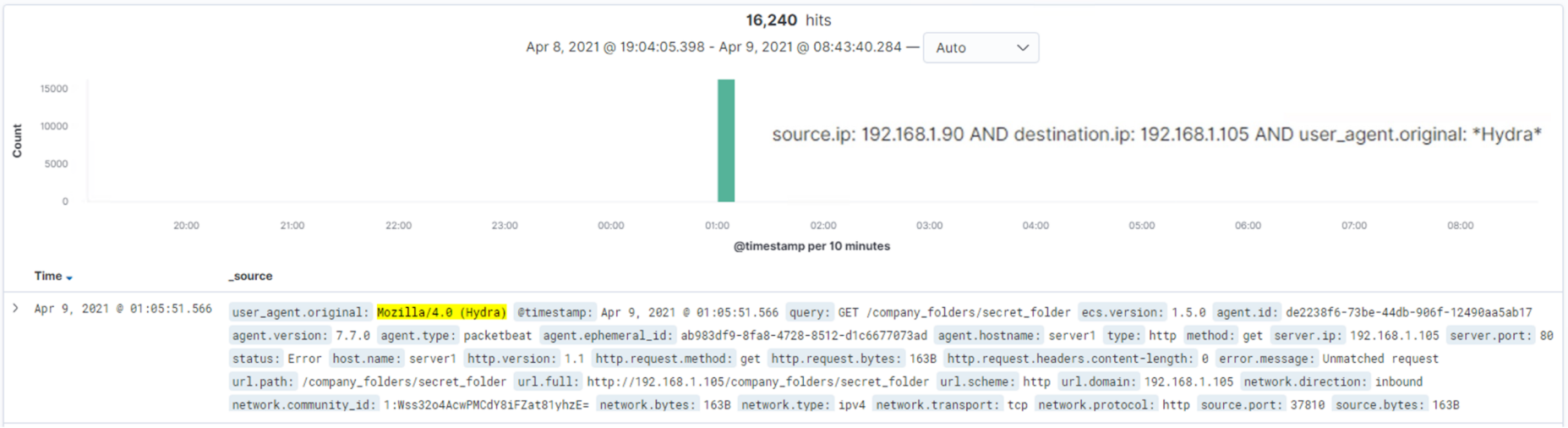
Analysis: Finding the Request for the Hidden Directory



- Requests for the hidden /secret_folder/ directory started at 1:00pm
- 12 Requests total were made from IP address 192.168.1.90
- The Connect_to_corp_server text file was the file that the attackers accessed.

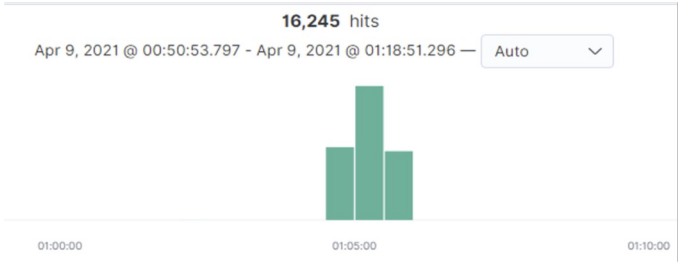


Analysis: Uncovering the Brute Force Attack

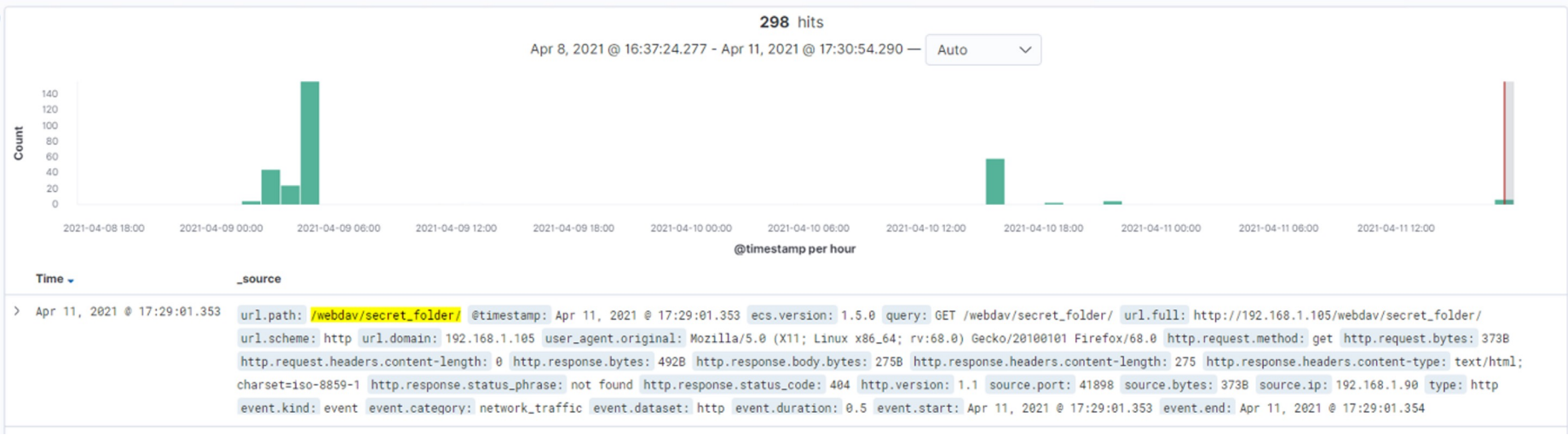


16,245 requests were made during the attack.
16,240 requests were made by the attacker before the correct password was discovered.
A user_agent search was used to determine the attacking software used is Hydra (top)
An http.status_code: 401 search was used to determine the total attempts made (right).

HTTP 401 Unauthorized



Analysis: Finding the WebDAV Connection



- 298 requests were made to the /WebDav folder during the attack
- The files requested were the passwd.dav file and the webdav.php file
- The webdav.php was the malicious payload that granted remote access to the attacker.

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alarm can be sent when nmap is located in the user.agent_original field to notify the system administrator when a port scan is occurring on the local network.

A threshold of 1 verified nmap user agent is sufficient from a non-whitelisted IP address.

An alarm can also be set when more than 500 connections are made within a 5 minute period.

System Hardening

Configure the network firewall to detect and respond to any port scan attempt in real time.

Conduct regular in-house port scans to ensure vulnerable ports are not open to malicious actors.

Set server firewall to drop packet traffic when connection thresholds are exceeded.

Regularly patch firewalls and software to avoid zero-day attacks.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect unauthorized access requests for hidden folders, I would block all incoming HTTP traffic when the source IP originates outside whitelisted company IP addresses.

A threshold should be set to a maximum of 10 attempts per hour before a triggered alert is sent to the system administrator.

System Hardening

Sensitive files should not be open to the public facing file systems. An alternative to the Web Distributed Authoring and Versioning (WebDAV) service should be explored.

In the meantime, sensitive information/data should be encrypted and the folders should only be accessed by whitelisted IP addresses.

VPN tunneling could also be a solution that will provide infrastructure towards continuing security improvements.

Mitigation: Preventing Brute Force Attacks

Alarm

Send an email alert and lock the account when more than 20 bad login attempts are made.

Create a dashboard item that tracks HTTP 401 Unauthorized client error statuses and the associated IP address.

Send an alert when the user agent indicates usage of Hydra or any other credential stuffing software.

System Hardening

Implementation of more complex passwords that are 8-12 characters in length with at least one number and one symbol included.

Account lockout policy that triggers a 30 minute waiting period after 20 bad login attempts.

A running blacklist and whitelist of IP addresses that trigger the lockout alert. If a lockout effects an employee, a password locker/education may be necessary.

Mitigation: Detecting the WebDAV Connection

Alarm

Block all HTTP traffic originating outside of a whitelisted company IP address to the WebDAV folder.

Email the system administrator when more than 5 HTTP GET requests are made to the folder from a single IP source outside the company whitelist.

Email the system administrator of any HTTP PUT request made to the folder from outside the company whitelist.

System Hardening

Restrict access to sensitive portions of the linux server and website with:

mod_authz_host

```
<RequireAll>
    Require all granted
    Require not ip 10.252.46.165
</RequireAll>
```

Uncomplicated Firewall (UFW)

```
sudo iptables -I INPUT -s xxx.xxx.xxx.xxx -j DROP
```

iptables

```
sudo ufw deny from xxx.xxx.xxx.xxx to any
```

Firewalld

```
sudo firewall-cmd --permanent --add-rich-rule="rule family='ipv4'
        source address='xxx.xxx.xxx.xxx' reject"
```

https://docs.rackspace.com/support/how-to/block-an-ip-address-on-a-Linux-server/

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alert the system administrator when any http PUT request is recorded to sensitive folders from an IP address outside of the company whitelist.

Alert the system administrator when an attempt is made to access port 80, 4444, and 1337 from all network traffic.

The previous alert can be paused if/when remote access is needed by the I.T. dept. for scheduled maintenance purposes.

System Hardening

Block all http PUT requests from IP addresses outside of the company whitelist.

Set access to the WebDAV folder to read only to prevent any unwanted executable files from being uploaded.

Close/Block any ports that are not necessary to continue with business operations.


The End