Capstone Engagement

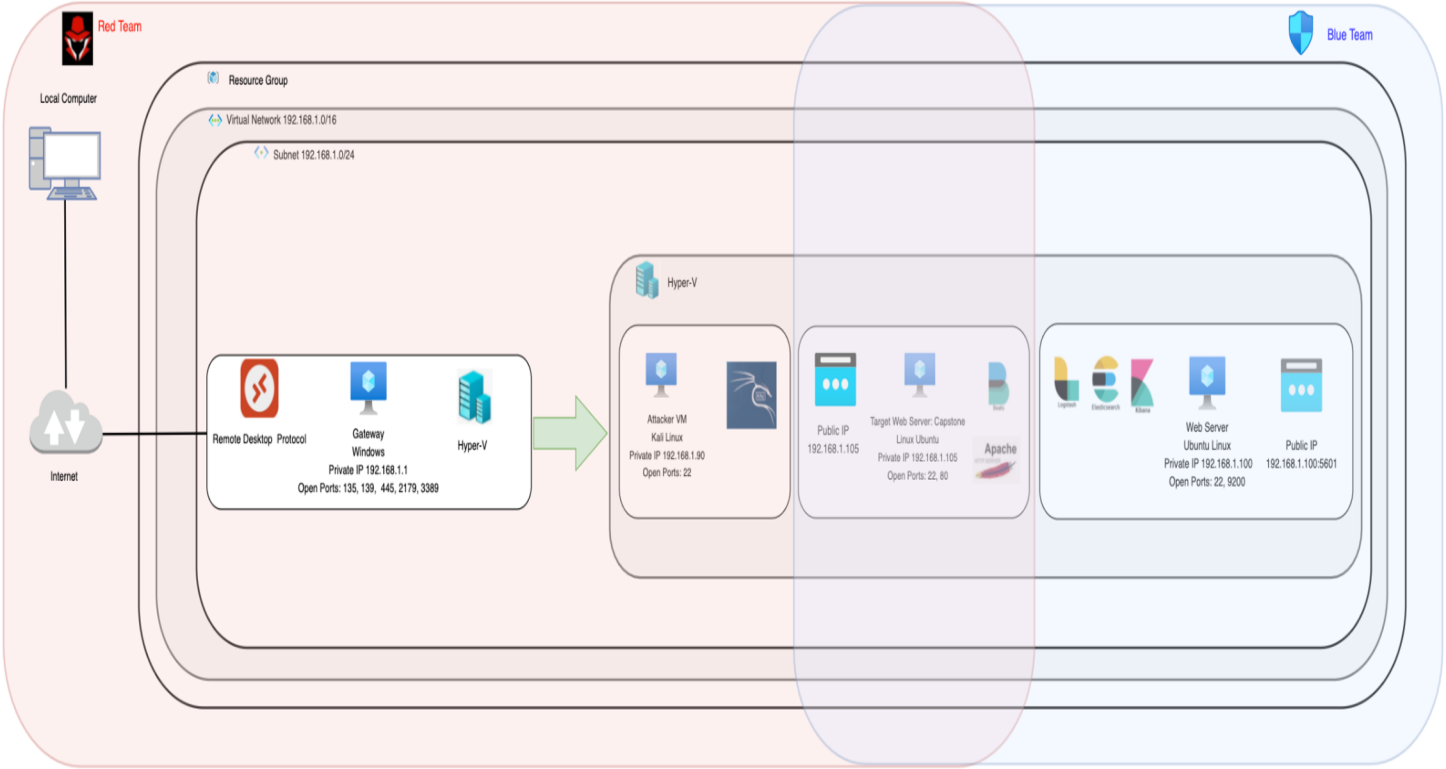
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.1
OS: Windows
Hostname: ML-REFVM-684427

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

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	Host Machine / Gateway
Kali	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Target Web Server
ELK	192.168.1.100	Logging, Monitoring, Reporting

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-548: Exposure of Information Through Directory Listing	Web server directories are open to the public and navigable in a browser.	Attackers can gather sensitive information from open directories and use this information and access to launch attacks and upload malicious content. These directories may also be vulnerable to path traversal in which users can navigate across to sensitive regions of the system.
CWE-312: Cleartext Storage of Sensitive Information	Documents with usernames in plain text are available to the public in the webserver	Attackers can use this information in bruteforce attacks. Even just one name can lead to a system breach.
Direct reference to hidden directory	Documents in the webserver give direct reference to a hidden directory with sensitive data.	Attackers can focus attacks to access the contents of the directory.
CWE-434: Unrestricted Upload of File with Dangerous Type	Webdav is enabled and allows uploading of malicious script.	It is easy to upload a payload in the target system e.g. use a reverse shell to open a meterpreter session

Vulnerability Assessment (Contd.)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-311: Missing Encryption of Sensitive Data	Missing encryption of sensitive data.	Attackers can easily read sensitive information
Usernames are employee first names	Usernames are too obvious and most likely discoverable through Google Dorking. These are all senior employees of the company which are vulnerable and easy to find in the company structure in publicly available material.	Attackers can easily create a wordlist of usernames of employees for bruteforcing.
CWE-256: Unprotected Storage of Credentials	Ryan's password hash was printed into a document, publicly available on the web server.	A password hash a key target for an attacker that is trying to gain entry. In this case attacker can easily navigate to it in a browser through minimal effort.
CWE-759: Use of a One-Way Hash without a Salt. CWE-916: Use of Password Hash With Insufficient Computational Effort	Ryan's password is only hashed, but not salted. A password hash can be run through apps to crack the password, however a salted hash will be almost impossible to crack.	A simple hash can be cracked with tools in linux or through websites. In this case it took seconds to crack Ryan's hash.

Vulnerability Assessment (Contd.)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80 with Public Access	Open and unsecured access to anyone attempting entry using Port 80.	Attackers with network access to the web server on port 80 can use it for executing attacks and gaining access into the system such as brute force attack by using hydra.
Weak Passwords	Passwords are too short, lack complexity and include commonly used words.	Passwords can be easily cracked. https://www.security.org/how-secure-is-my-password/ shows that 'leopoldo' can be cracked in 5 seconds.
Unrestricted Access / Root Accessibility	All users have authorization to read/write/delete and access any folders and files without any restrictions.	Attackers can try social engineering attack on any and as many employees as they want and easily get root access. This increases attack surface and does not add any more obstacles for root access once a user credential is compromised.
Open port 22 with Public Access	Open and unsecured access to anyone attempting entry using Port 22.	Attackers with network access to the web server on port 22 can use it for executing attacks, bypass security restrictions and gaining unauthorized access.

Exploitation: Directory Traversal

01

Tools & Processes

Navigated web server directories in a browser.

02

Achievements

Documents available in meet_our_team folder provided sensitive information:

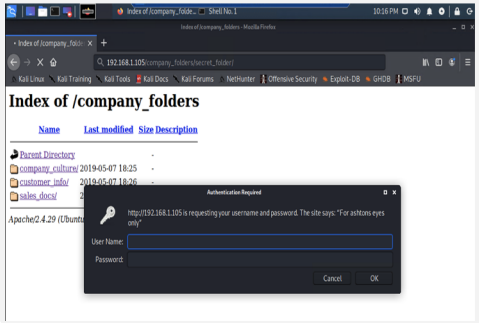
Path to a secret folder is company_folders/secret_folder and Ashton is its owner.

Company employees are not tech savvy.

Reyan is newly appointed CEO.

Hannah is newly appointed VP of IT.

03



Exploitation: Brute Force

01

Tools & Processes

Used Hydra with rockyou.txt wordlist and ‘ashton’ username to bruteforce.

02

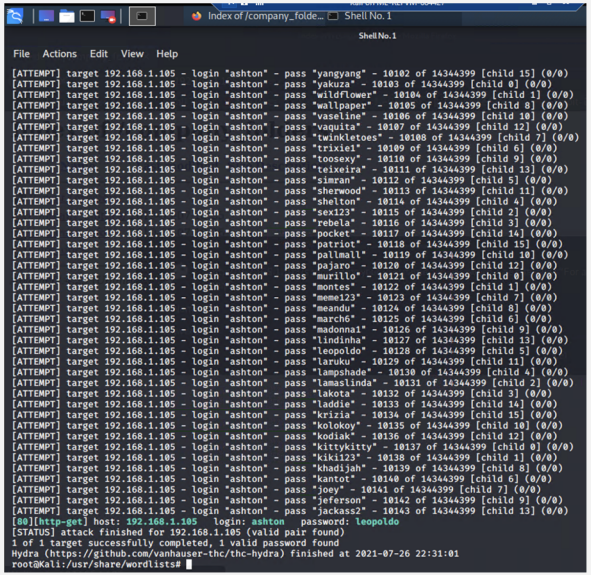
Achievements

Successfully bruteforced Ashton’s password and gained access to the secret folder.

Connect_to_corp_server file in this folder provided information on how to connect to webdav and Ryan’s password hash.

03

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



Exploitation: Crack Hashed Password

01

Tools & Processes

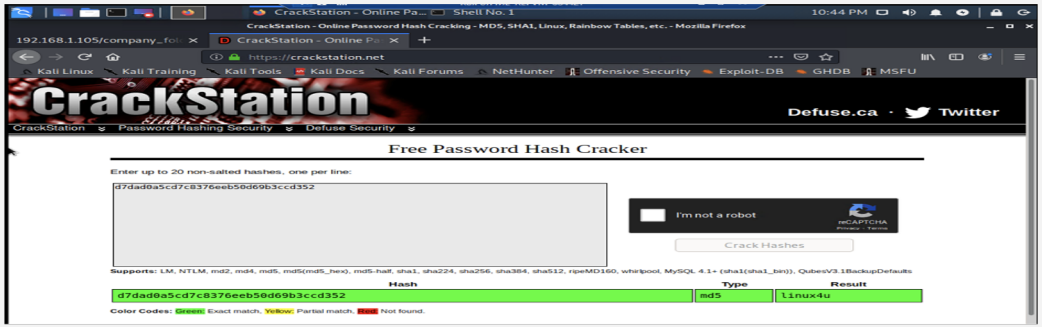
Used website crackstation.net to crack Ryan's hashed password

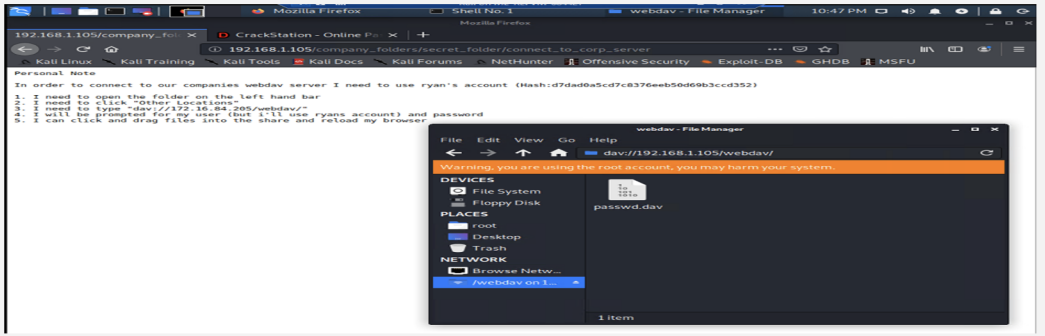
02

Achievements

Successfully cracked hash to find Ryan's password: linux4u, and gained access to webdav folder.

03





Exploitation: PHP Reverse Shell

01

Tools & Processes

Used msfvenom to create a PHP Reverse Shell payload.

Uploaded PHP Reverse Shell payload to webdav.

Refreshed the browser at 192.168.105/webdav/payload.php

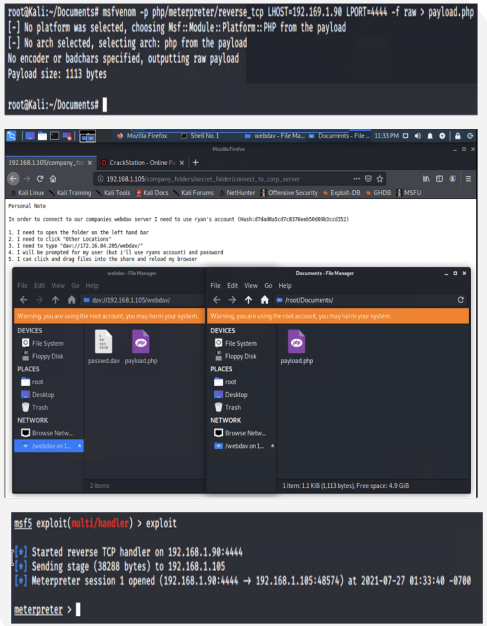
Used metasploit's multi/handler exploit to start a listener to establish a meterpreter session.

02

Achievements

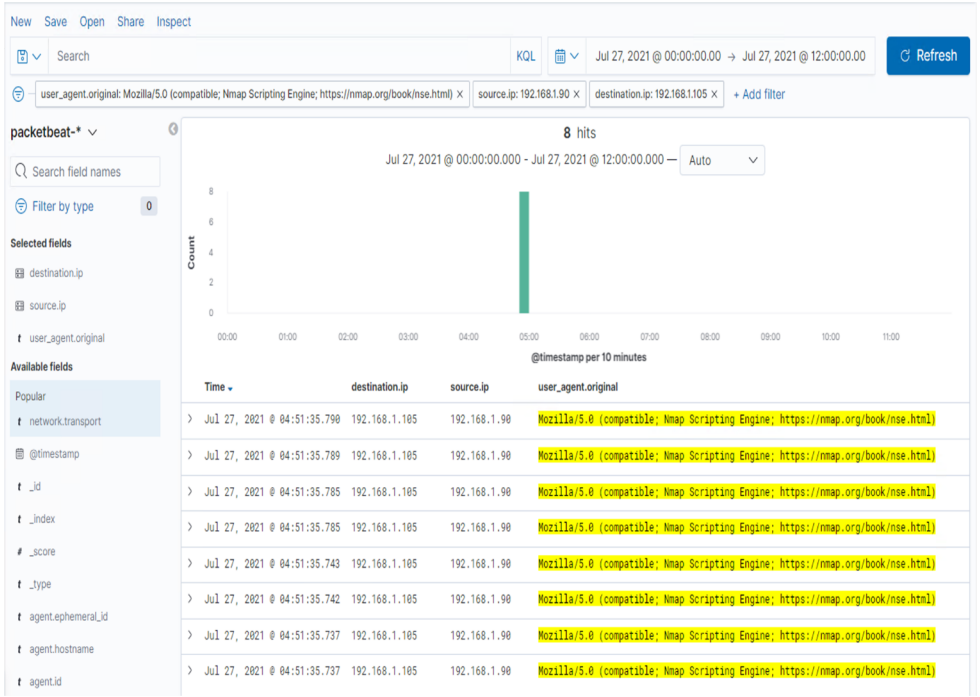
Gained access to web server by starting a meterpreter session from Kali Machine

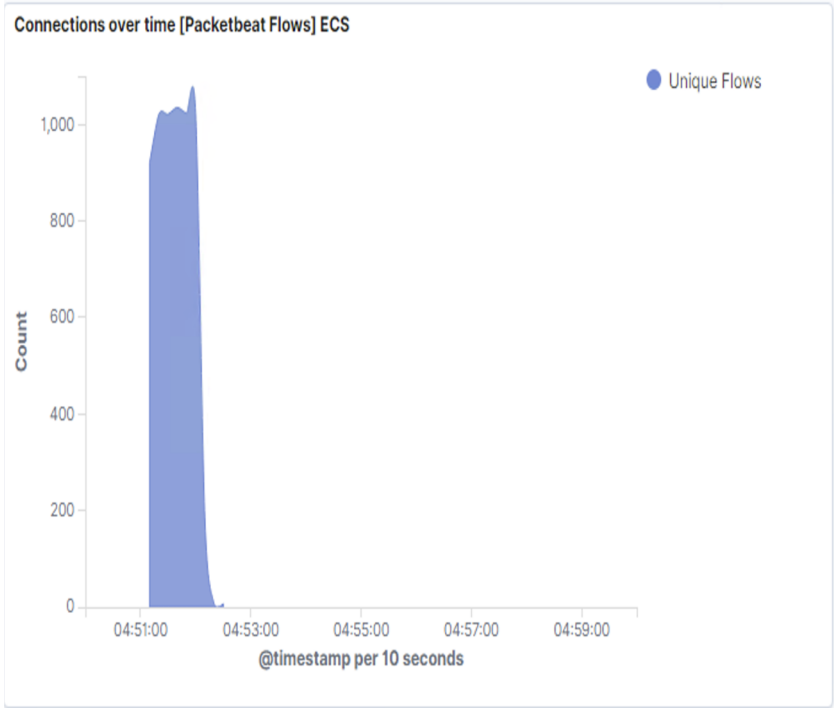
03



Blue Team
Log Analysis and Attack Characterization

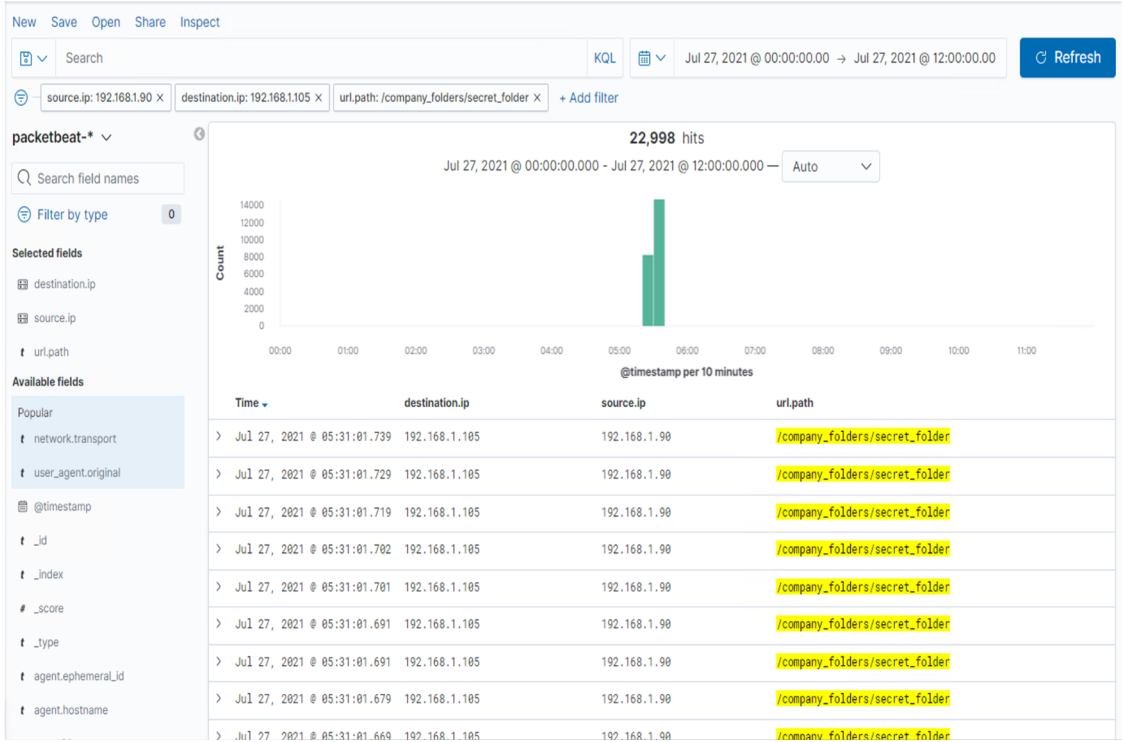
Analysis: Identifying the Port Scan





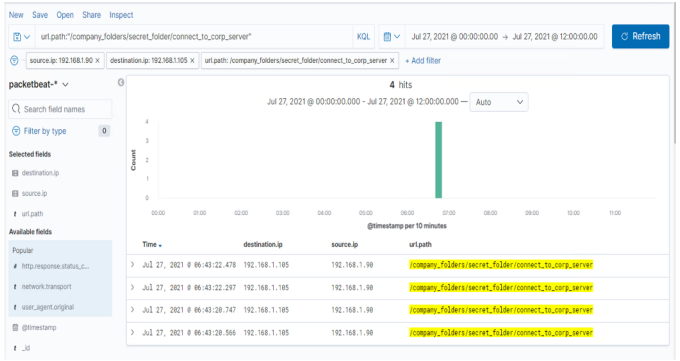
- Port Scan occurred on July 27, 2021 at 04:51 AM.
- 8 packets were sent from 192.168.1.90 within a span of 53 Milliseconds.
- User_agent.original field shows that these packets were sent from NMAP and there was spike in connections at the same time indicating a port scan.

Analysis: Finding the Requests for the Hidden Directory



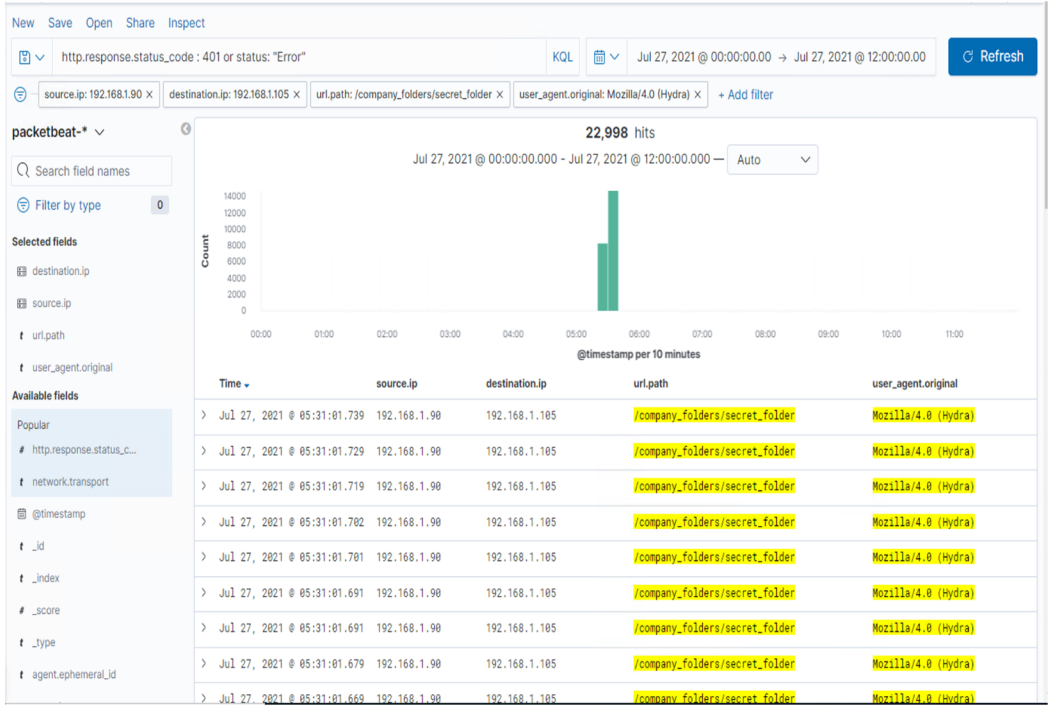
Top 10 HTTP requests [Packetbeat] ECS

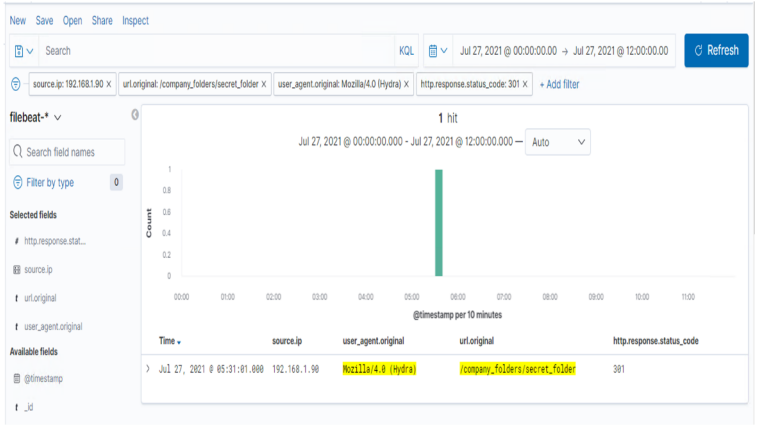
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	22,998
http://192.168.1.105/webdav	405
http://192.168.1.105/webdav/payload.php	133
http://192.168.1.105/webdav/passwd.dav	41
http://192.168.1.105/	10



- 22,998 requests were made to secret folder on July 27, 2021 between 05:28 AM and 05:31 AM.
- There is only one file in this folder: connect_to_corp_server. It was accessed 4 times from the suspicious source IP: 192.168.1.90. It has CEO Ryan's hashed password and information on how to connect to webdav.

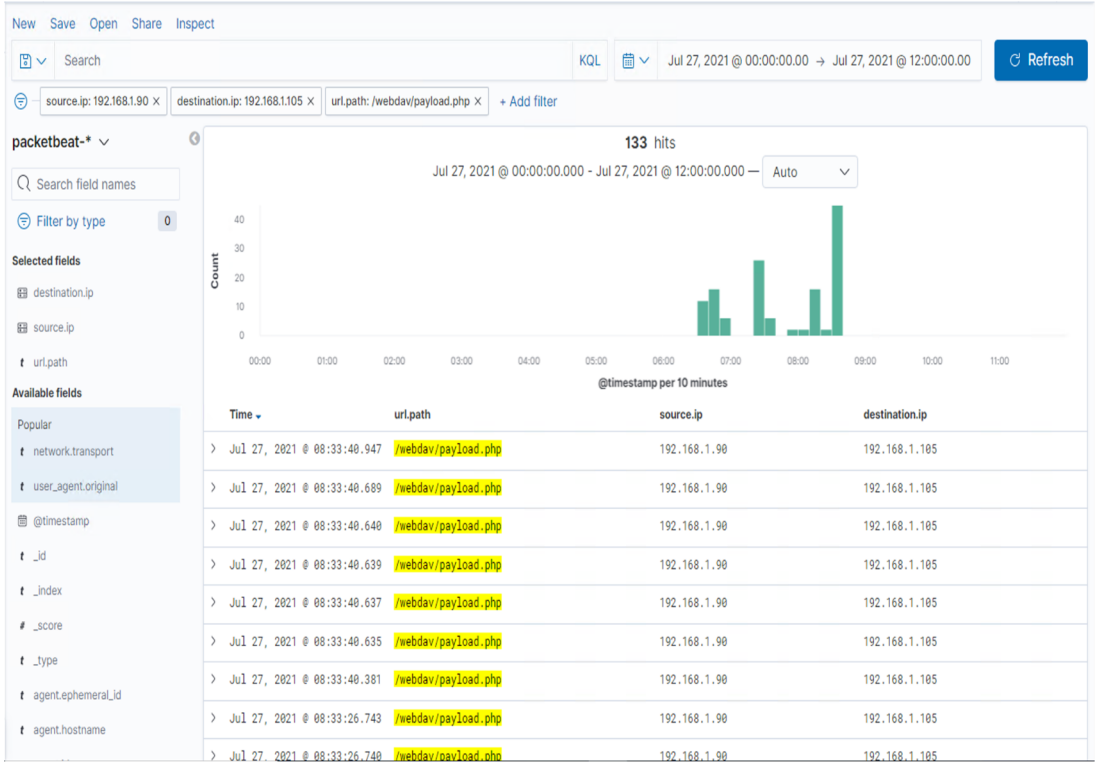
Analysis: Uncovering the Brute Force Attack





- 22,998 requests were made on July 27, 2021 between 05:28 AM and 05:31 AM which failed. User_agent.original field shows these requests were made by Hydra indicating Brute Force Attack.
- One more request was made by Hydra at 5:31 AM which got http response code 301 indicating it was successful.

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	22,998
http://192.168.1.105/webdav	405
http://192.168.1.105/webdav/payload.php	133
http://192.168.1.105/webdav/passwd.dav	41
http://192.168.1.105/	10

- 405 requests were made to the webdav folder.
- Out of these 133 requests were made to this directory through reverse shell using the file payload.php

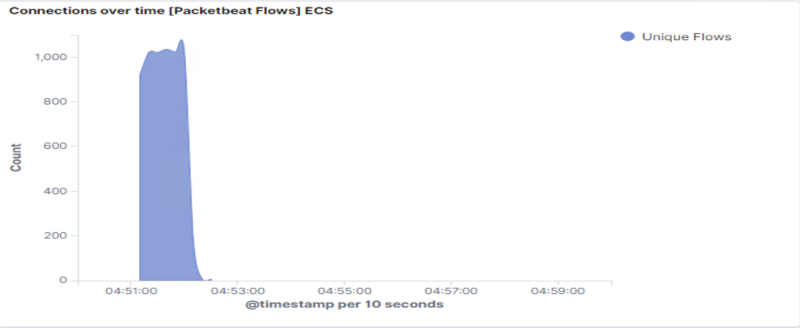
Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Any packets with user_agent.original name containing the word “Nmap” should trigger an alert right away. In this case user_agent.original was “Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)”

Moreover, if connections cross threshold of more than 100 in a minute it should trigger an alarm.



System Hardening

Open ports only on need basis, all other ports should be closed.

Create a whitelist of IPs and have the firewall block unauthorized IPs from scanning.

Set server iptables to drop packet traffic when thresholds are exceeded.

Keep all services running on open ports and firewalls up to date.

Regularly run system port scans to proactively detect and block open ports.

Review IDS regularly to update thresholds.

Ensure IPS and Firewalls are set up to block the scan in real time according to defined thresholds.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Alarm should be triggered for every unauthorized access request for hidden folders and files.

Threshold of more than 3 failed attempts in an hour should trigger an alert.

IPs not on whitelist attempting to access should trigger an alert.

System Hardening

Highly confidential folders should not be shared on public access.

Folders with sensitive information should not have obvious names such as “secret_folder”.

Regularly review IP addresses that cause an alert and block them or add them to whitelist.

Encrypt data contained within confidential folders.

Set lockout time for 30mins or more after 3 password failures. Blacklist the IP address are 10 failed attempts.

Increase password strength requirements for hidden directories. This may include: a larger minimum length and a mixture of upper case, lower case, numbers and special characters.

Require a password reset on regular basis, such as every 3 months.

Use multi-factor authentication and/or captcha.

Limit user access to the hidden directory (read/write/delete) only on need basis.

Remove all reference to the hidden directory on web server.

Mitigation: Preventing Brute Force Attacks

Alarm

For all password portals such web server and SSH set up alert for more than 3 failed attempts (or 401 error).

System Hardening

Create a lockout policy to lock out accounts for 30 mins or more after 3 failed password attempts. Blacklist the IP address are 10 failed attempts.

Create password policy to increase password complexity requirements: this may include: a larger minimum length and a mixture of upper case, lower case, numbers and special characters.

Require a password reset on regular basis, such as every 3 months.

Use multi-factor authentication and/or captcha.

Rate limit traffic to block mass password attempts in real time.

Mitigation: Detecting the WebDAV Connection

Alarm

Any attempt to connect to WebDav from an IP which is not on the white list should trigger an alarm.

System Hardening

Create a white list of IPs and ensure that firewall prevents all other access.

Limit user access to the hidden directory (read/write/delete) only on need basis.

Increase password complexity requirements: this may include: a larger minimum length and a mixture of upper case, lower case, numbers and special characters.

Require a password reset on regular basis, such as every 3 months.

Use multi-factor authentication and/or captcha.

Scan all incoming traffics with anti-virus / anti-malware.

Perform regular updates.

Upgrade to a more secure application.

Only allow internal access to WebDav, block all external connections.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Create an alert for any file being uploaded to WebDav.

Monitor all incoming uploads and set up an alert for anything detected by anti-virus / anti-malware.

Create an alert for any file being uploaded that contains suspicious code/script/file extensions.

System Hardening

Block all IP addresses other the one on the whitelist.

Ensure only necessary ports are open.

Only allow internal access to WebDav, block all external connections.

If external access is required, set access to WebDav to read only to prevent payloads from being uploaded.

If external upload is required limit file types that can be uploaded, including restricting PHP. Uploaded file types should be strictly on need basis only.

Set up anti-virus / anti-malware that scans all incoming filed and updates automatically on daily basis.

Update firewall rules to restrict uploaded file types to those only absolutely needed and only those that are cleared by anti-virus / anti-malware application and contain no suspicious code/script/file extension. Block everything else from being uploaded.


The End.