Capstone Engagement

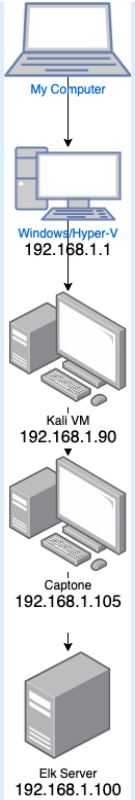
Assessment, Analysis,

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address
Range:192.168.1.0/24
Netmask:
Gateway:

Machines
IPv4:192.168.1.1
OS:Windows 10
Hostname: Hyper-V

IPv4:192.168.1.90
OS: Linux
Hostname:Kali

IPv4:192.168.1.105
OS: Linux
Hostname:Capstone

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
Azure Lab Windows	192.168.1.1	To connect to all VMs
Kali Linux	192.168.1.90	Attacking and exploiting Capstone Server
Capstone	192.168.1.105	To host a Web Server running Webdav
Elk	192.168.1.100	Capture and Monitor systems logs for Capstone Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-521	User having weak password	*Easy to guess passwords*
CWE-307	Improper Restriction of excessive authentication attempts	*an attacker can use a system of trial and error (brute force)in an attempt to guess valid user credentials.*
CWE-200	Exposure of sensitive information to an unauthorized actor	Human error can cause a hacker to get private information.
CWE-98	Improper Control of Filename for Include/Require Statement in PHP Program	Attacker has the ability to download malicious files

Exploitation: Brute Force Vulnerability

01

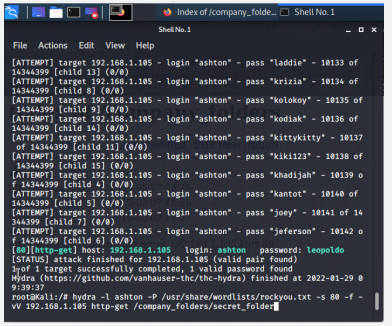
Tools & Processes
Hydra
CrackStation

02

Achievements
Hydra brute force website to get Ashton username and password.

CrackStation was used to crack Ryan hash password

03



Exploitation: Human Error

01

Tools & Processes

Msfconsole
Weak password
Nmap

02

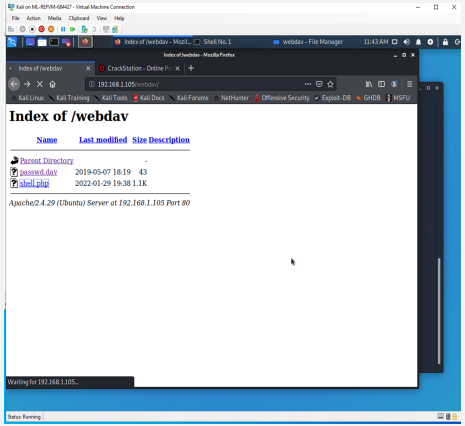
Achievements

Msfconsole achieved for me to be able to make and upload a malicious file to the webdav.

Having weak passwords was easy for me to infiltrate the website.

Port 80 was open for any one.

03



Exploitation: Remote Code Execution

01

Tools & Processes

Msfconsole

Msfvenom

02

Achievements

Msfvenom set up a reverse shell on port 4444

Msfconsole was used to intercept and connect to the reverse shell.

03

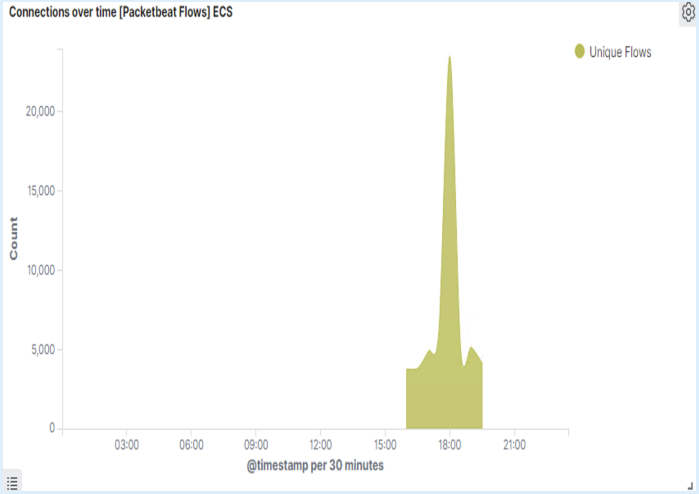
Blue Team

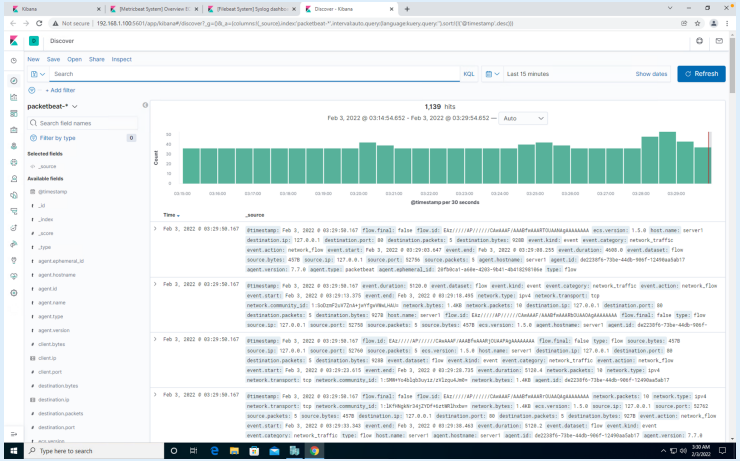
Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space al
Otherwise, add the answers to speaker n

- Port Scan occur around 16:00-18:00
- 15,746 packets by 192.168.1.90
- By the amount of communication both VMS were having

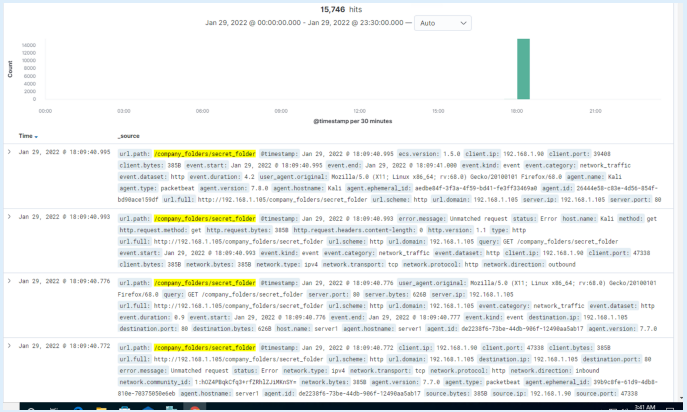




Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space al
Otherwise, add the answers to speaker n

- 15,746 request occur by 18:00-18:30
- File “secret folder” was being request that many times



Analysis: Uncovering the Brute Force Attack

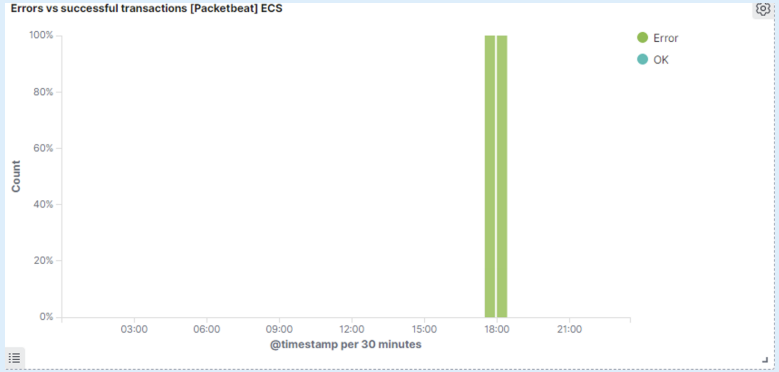
Answer the following questions in bullet points under the screenshot if space al
Otherwise, add the answers to speaker n

- 15,746 request were made
- 15,746

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,746
http://127.0.0.1/server-status?auto=	1,192
http://snnmnkxdhflwgthqismb.com/post.php	187
http://www.gstatic.com/generate_204	98
http://192.168.1.105/compay_folder/secret_folder	64

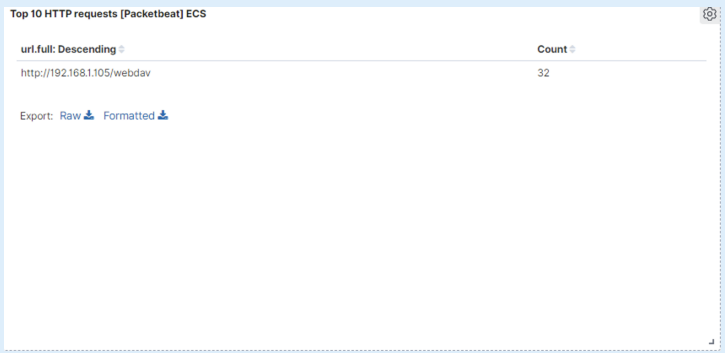
Export: Raw Formatted

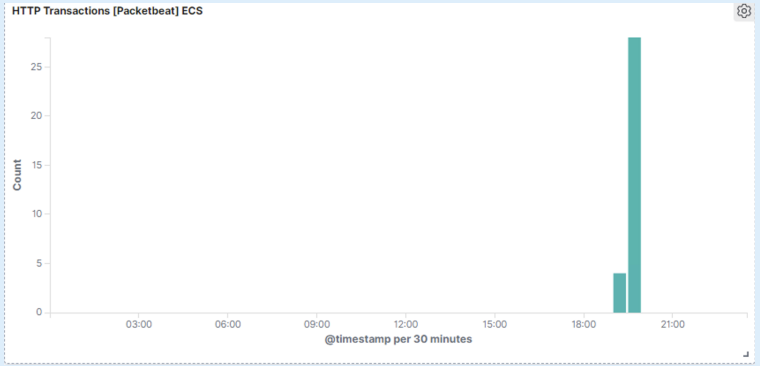


Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space al
Otherwise, add the answers to speaker n

- 32 request were made to this directory.
- Shell.php and passwd.dav





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?
Having a limit to how many request are made within 30 mins.

What threshold would you set to activate this alarm?
No more than 150 request are made within 30 mins

System Hardening

What configurations can be set on the host to mitigate port scans?
To have a strong firewall set up.

Ensure the firewall detects and cuts off the scan attempt in real time

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Have a alarm when a unauthorized ip logins in and finds the request of the hidden directory

What threshold would you set to activate this alarm?

A maximum 5 attempts per hour that would trigger an alert to be sent.

System Hardening

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

Not allow outside ips

Highly confidential folders should not be shared for public access

Encrypt data contained within confidential folders

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? Limit to how many failed logins.

What threshold would you set to activate this alarm?
No more than 10 failed logins per 10 mins

System Hardening

What configuration can be set on the host to block brute force attacks?
2 way factor authentication or multifactor authentication.

Employes will have login in and use they're phone.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
I would set an alarm that activates on any IP address trying to access the webDAV directory outside of those trusted IP addresses.

What threshold would you set to activate this alarm?
I would set to activate this alarm would be when any HTTP PUT request is made

System Hardening

What configuration can be set on the host to control access?
Creating a whitelist of trusted IP addresses and ensure my firewall security policy prevents all other access

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
An alert be set for any traffic attempting to access port 4444

An alert for any files being uploaded into the /webDAV folder

What threshold would you set to activate this alarm?
Threshold for the alert to be sent is when one or more attempt is made.

System Hardening

What configuration can be set on the host to block file uploads?
Block any other ips other than trust Ips

Ensure only necessary ports are open

Set access to the /webDAV folder to read only to prevent payloads from being uploaded


The End