Capstone Engagement

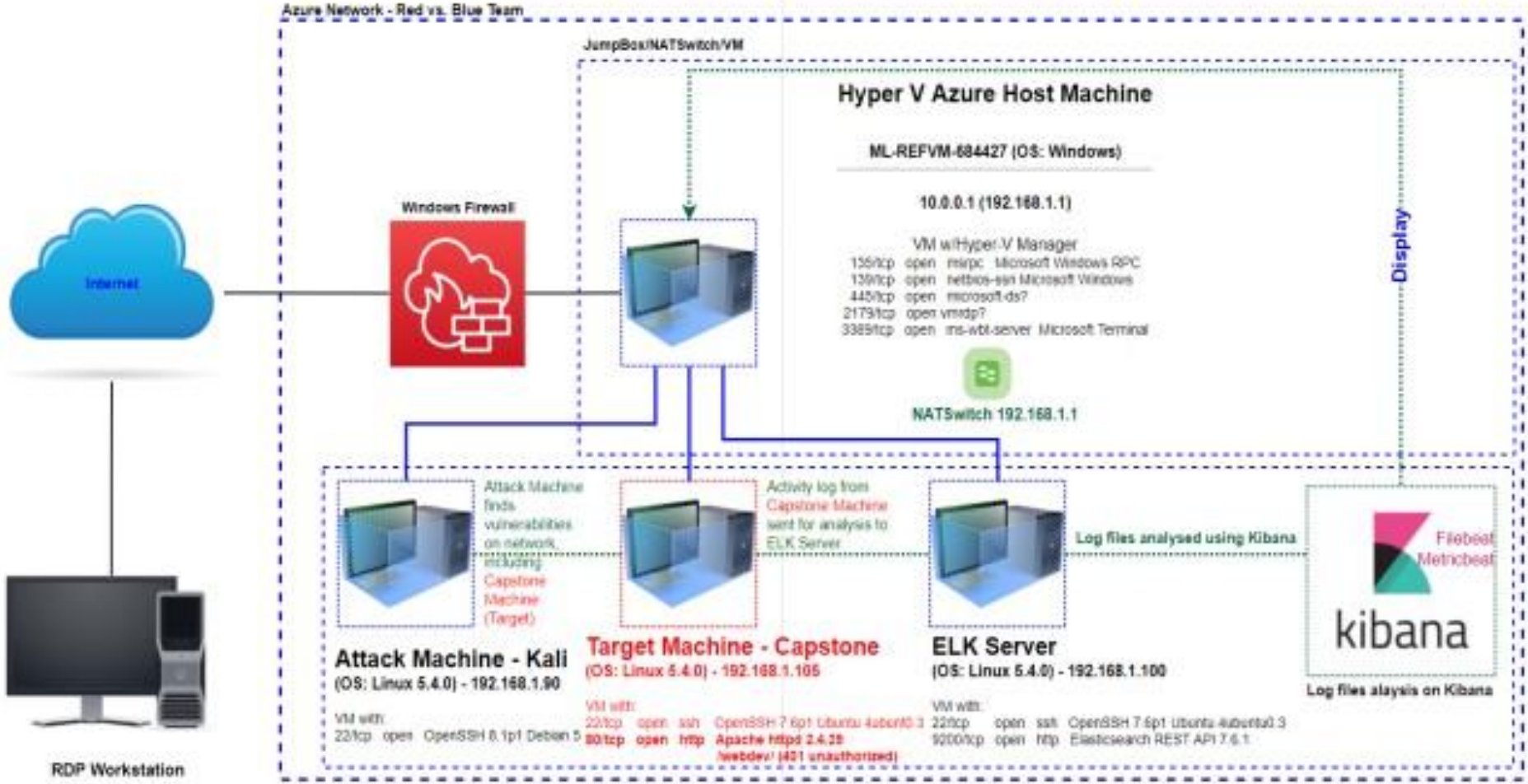
Assessment, Analysis, and Hardening of a Vulnerable System

By Greg Moss

Table of Contents

This document contains the following sections:

Network Topology


Azure Network - Red vs. Blue Team
JumpBox/NATSwitch/VM
Hyper V Azure Host Machine
ML-REFVM-684427 (OS: Windows)
10.0.0.1 (192.168.1.1)
VM w/Hyper-V Manager
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows
445/tcp open microsoft-ds?
2179/tcp open vmrdp?
3389/tcp open ms-wbt-server Microsoft Terminal
NATSwitch 192.168.1.1
Display
Windows Firewall
Internet
RDP Workstation
Attack Machine finds vulnerabilities on network, including Capstone Machine (Target)
Activity log from Capstone Machine sent for analysis to ELK Server
Log files analysed using Kibana
Filebeat
Metricbeat
kibana
Log files alaysis on Kibana
Attack Machine - Kali
(OS: Linux 5.4.0) - 192.168.1.90
VM with:
22/tcp open OpenSSH 8.1p1 Debian 5
Target Machine - Capstone
(OS: Linux 5.4.0) - 192.168.1.105
VM with:
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
80/tcp open http Apache httpd 2.4.29
/webdev/ (401 unauthorized)
ELK Server
(OS: Linux 5.4.0) - 192.168.1.100
VM with:
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
9200/tcp open http Elasticsearch REST API 7.6.1

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-REFVM-684427 (Hyper-V Azure machine)	162.168.1.1(Preferred)	NATSwitch (Host Machine Cloud based-Hosting the 3 VMs below)
Kali Linux 	192.168.1.90	Attacking Machine used for penetration testing
ELK	192.168.1.100	Network Monitoring Machine running Kibana - Logs data from capstone Machine (192.168.1.105)
Capstone (server1)	192.168.1.105	Target Machine Replicating a vulnerable server - attempting to pop- hosting an Apache and ssh server.

Vulnerability Assessment By Greg Moss

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access	*PORT 80 is most commonly used for web communication and if left open and unsecure, it can allow public access.*	*This vulnerability allows access into the web servers. Files and folders are accessible. Sensitive and secret files can be found.*
Apache Directory Listing	Allowed attackers to reveal the ip address and the secret folder	Allowed attackers to reveal the ip address and the secret folder
Brute-force Attack	An attack that consists of systematically checking all possible username and password combinations until the correct one is found	With the use of brute force and common password list (rockyou.txt), the password can be easily found.
Reverse Shell Backdoor	Allows to send a reverse shell payload on web server while the firewalls do not detect the payload	Attackers gained the remote backdoor access to the capstone web server

Exploitation: Open Web Port (80)

01

Tools & Processes

I used nmap for open ports on the target machine. Heres the commands used:

~# netdiscover -r 192.168.1.255/16

~# nmap -sV 192.168.1.0/24

~# nmap -sS -A 192.168.1.105

Webserver 192.168.1.105/meet_our_team/ashton.txt

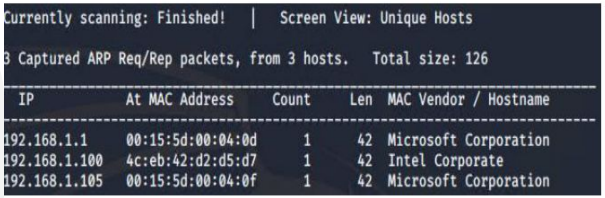
02

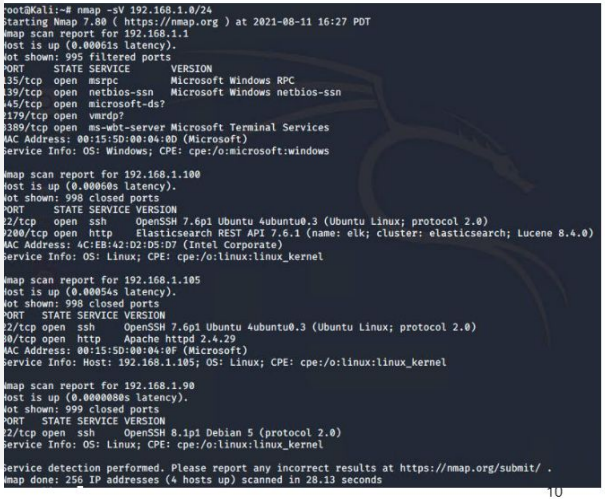
Nmap scanned 256 ip addresses: i found 4 hosts up: Port22 and 80 are open and was of interest to me

The discovered files on Meet_our_team/ashton.txt

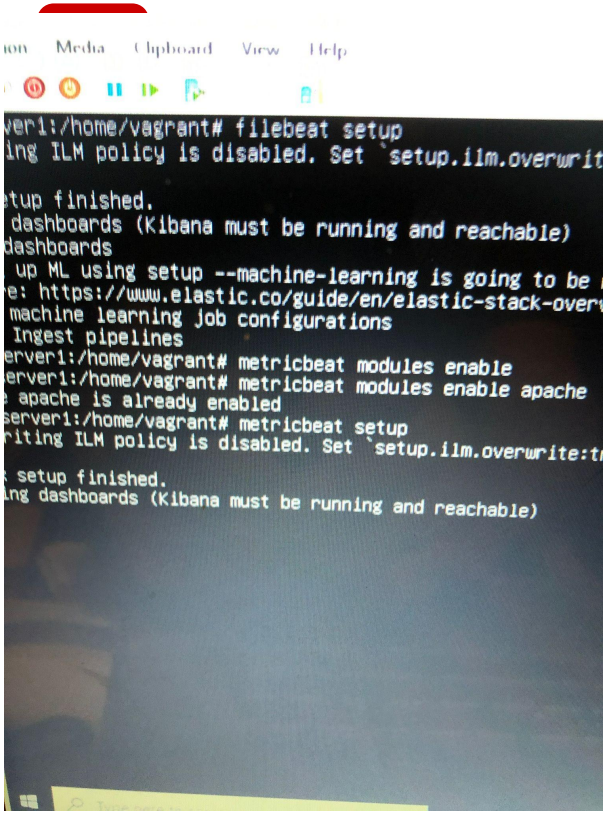
The ashton.txt allowed discovery of the secret folder at /company_folders/secret_folder.

03





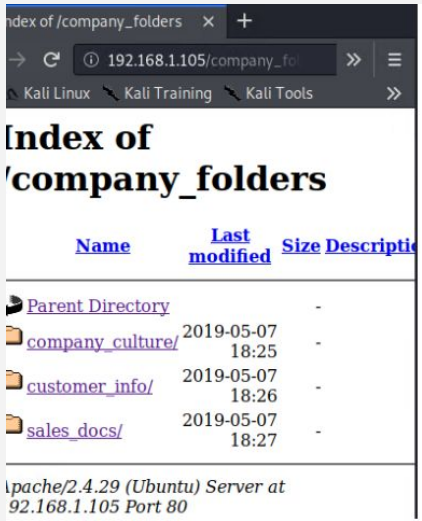
Exploitation: Open port 80



02

After getting in we will ustilize Brute force attacks.

03



Exploitation: Brute-force Attack

01

Used Hydra which is already preinstalled in to linux. I also required a password list in this case i used rockyou.txt

Command used
Hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secre_folder

A hash to ryans password was found

02

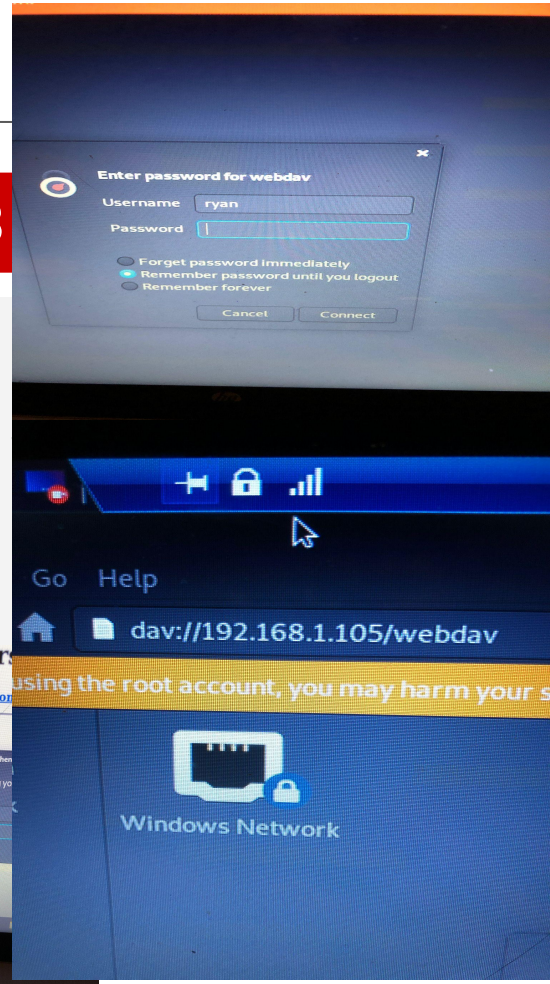
Password for Ashton was tested against the common password dictionary "rockyou"

Access to the /secret_folder

Access to /webdav system

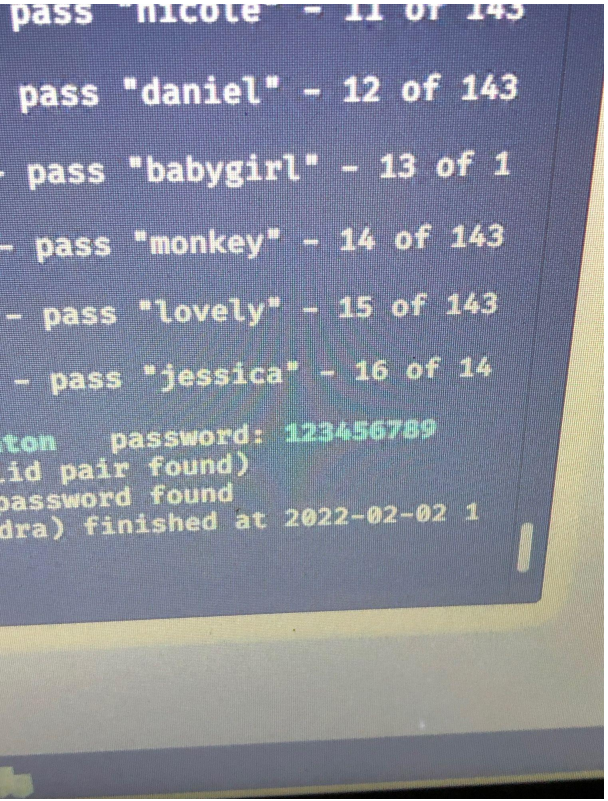
Ryans password.dav was found: linux4u

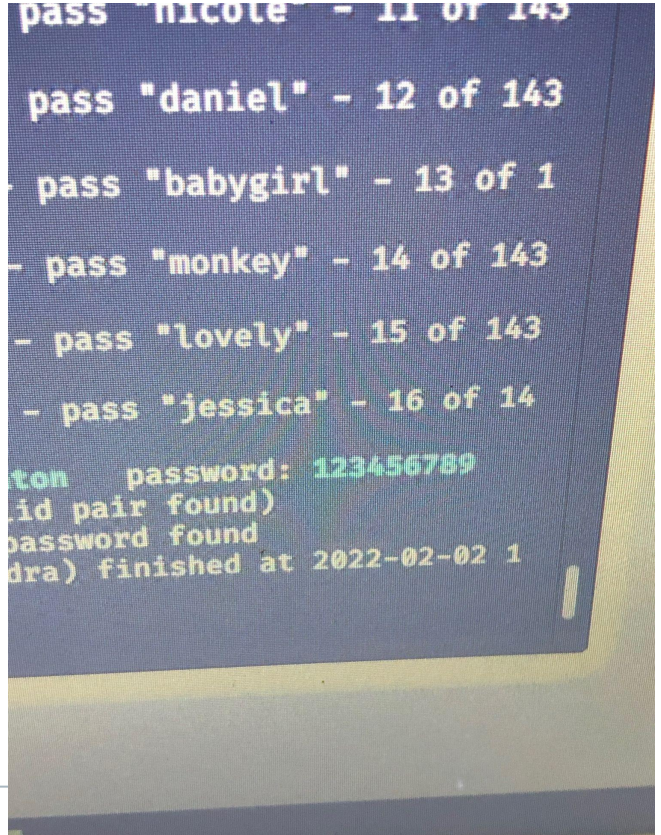
03



Brute force

Using Brute force to scan for user and passwords

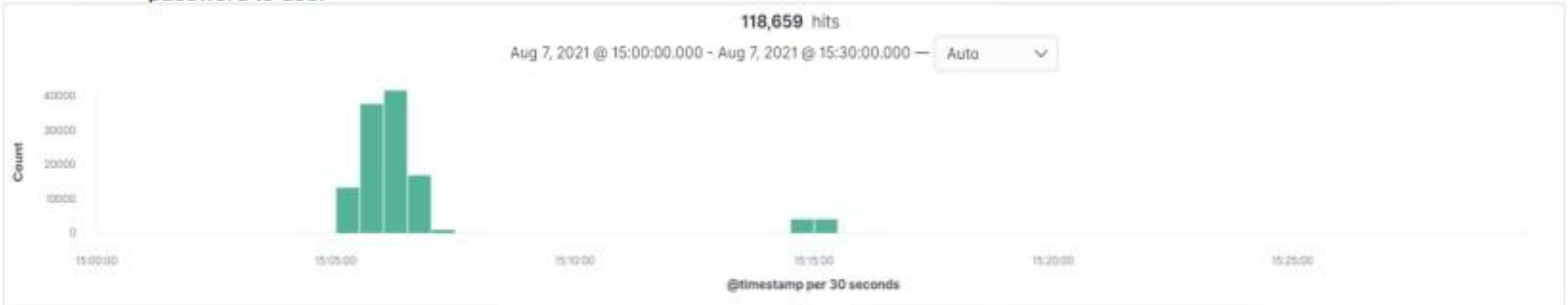


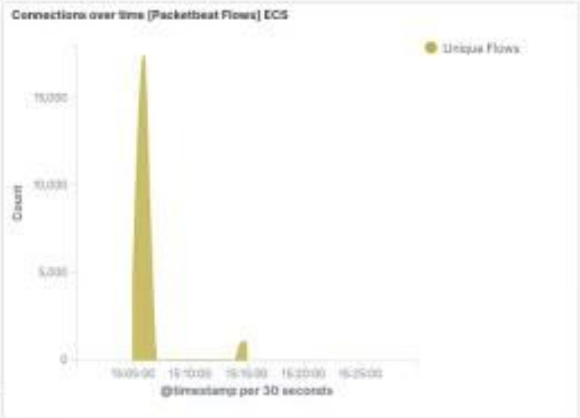


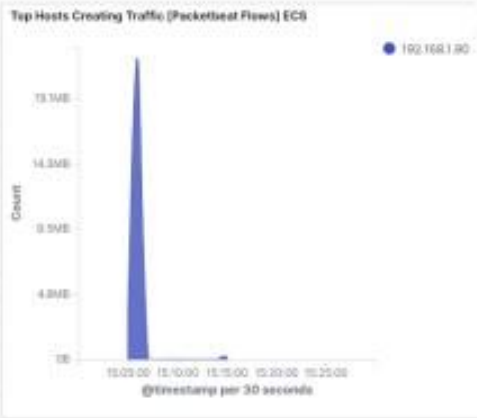
Blue Team
Log Analysis and Attack Characterization

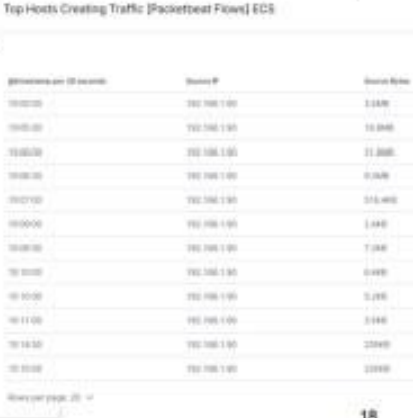
Analysis: Identifying the Port Scan

- The port (192.168.1.90) scan occurred on August 7, 2021 @ 15:05 UTC or 11:05 EST
- There were total of 118,659 hits and 4 requests were made for the secret folder and files contained in the secret folder.
- The file to connect_to_corp_server was requested and returned.
- This file contained instructions for the connections to the WebDAV server, as well as the username: ryan, and the hash password to use.









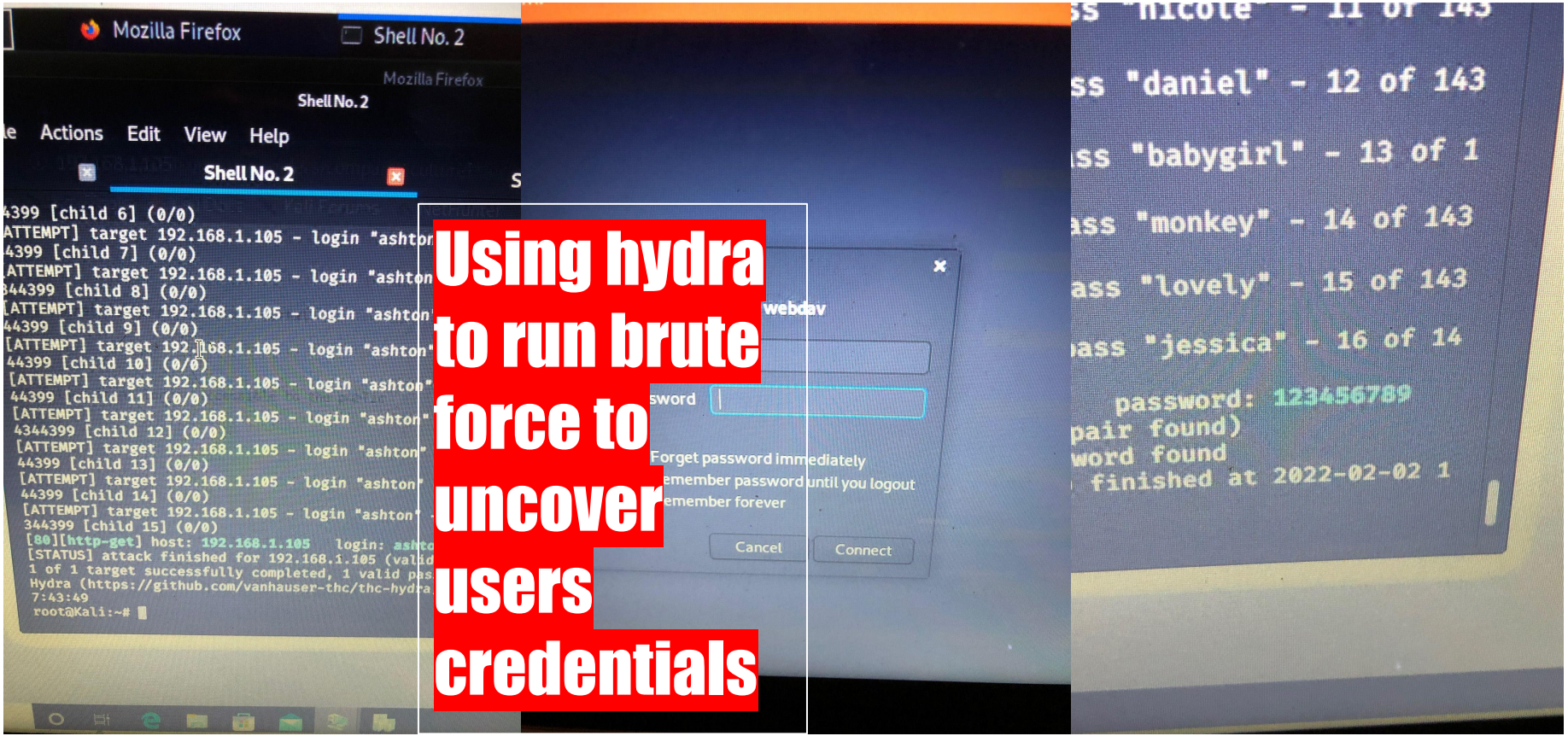
Analysis: Finding the Request for the Hidden Directory

- The attack started around 15:00 UTC (11:00 am EDT) with 16,178 requests were made for the “secret_folder”. The IP address the requests were coming from 192.168.1.90.

- The “secret_folder” contained a hash password for the employee’s credentials (Ryan), which can be used for uploading a payload, thus exploiting other vulnerabilities

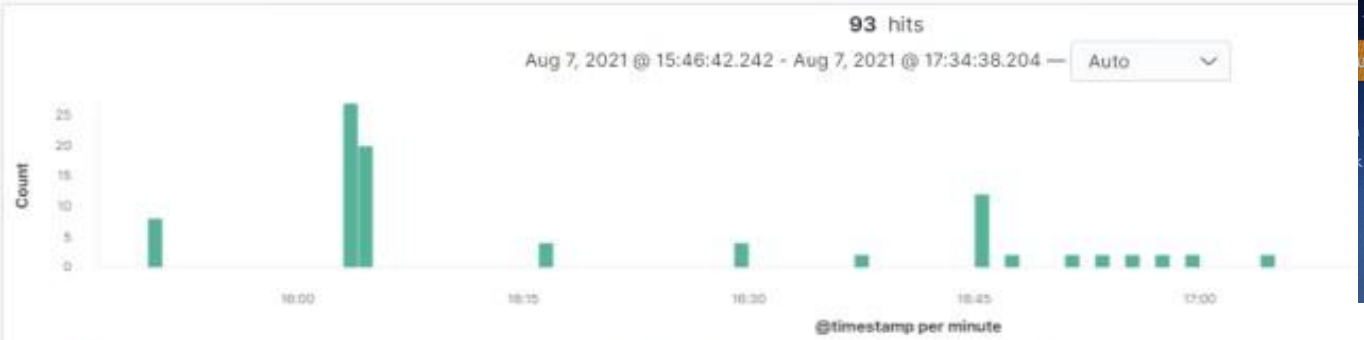
It contained a folder called “connect_to_corp_server” which was accessed 4 times.

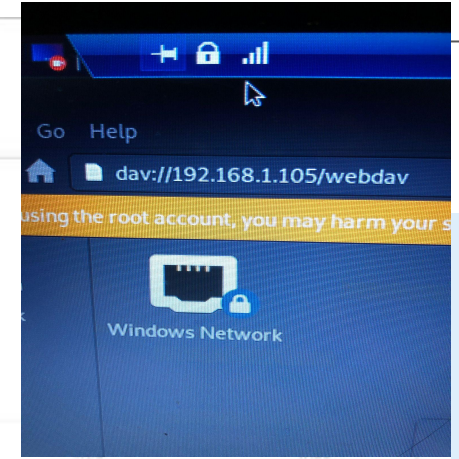
Analysis: Uncovering the Brute Force Attack



Analysis: Finding the WebDAV Connection

- 93 total requests were made for the WebDAV directory (192.168.1.105/webdav)
- The files passwd.dav and shell.php were requested.
- Request methods include the following: GET, PUT, PROPFIND and OPTIONS





Time	source.ip	destination.ip	method	url.path
Aug 7, 2021 @ 17:29:4	192.168.1.90	192.168.1.105	get	/webdav/
			get	/webdav/
			get	/webdav/shell.php
			get	/webdav/shell.php

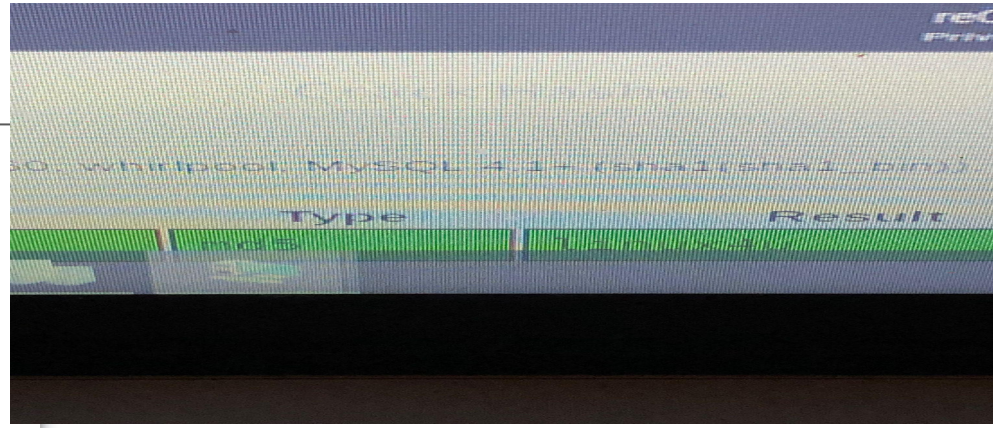
Top 10 HTTP requests [Packetbeat] ECS

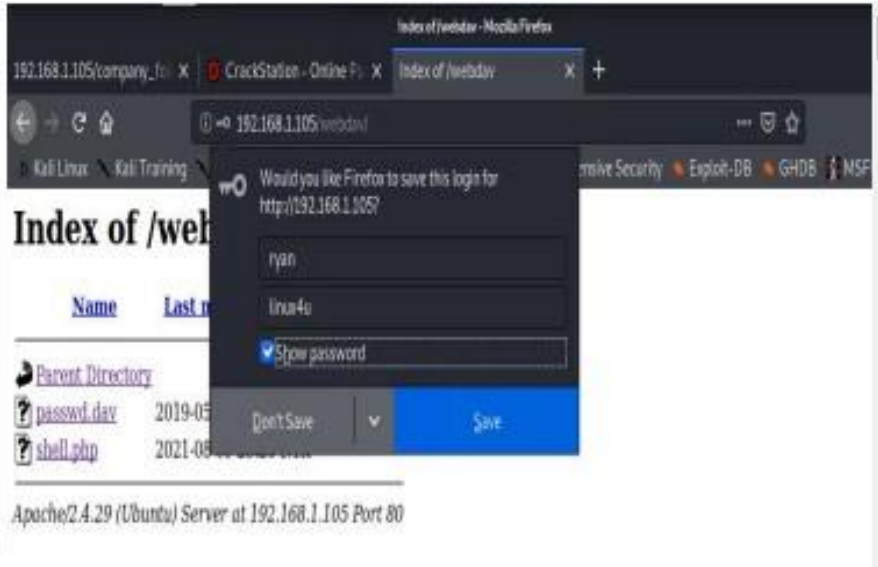
url.full: Descending	Count
http://192.168.1.105/webdav/passwd.dav	63
http://192.168.1.105/webdav/	16
http://192.168.1.105/webdav/shell.php	14

Using CrackStation

Alarm

Crack station is used to break hashes, hashes are used to protect a users credentials





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?

An alert could be set to trigger when a large amount of traffic occurs in a short time from a single source ip that targets multiple ports.

What threshold would you set to activate this alarm?

A possible threshold for this alert could be if any single ip address request more than 10 request per second and more than 10 seconds or 100 consecutive pings (ICMP) request

System Hardening

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

Enable only traffic needed to access internal hosts. Deny everything else. Including the standard ports. Such as TCP 80 for HTTP and ICMP for ping request.

Configure the firewall to look for potentially malicious behavior over time and have rules in place to cut off attacks if a certain threshold is reached.

Describe the solution. If possible, provide required command lines.

Create and set up iptables for the firewall port blocking and scanning an ids like kibana or splunk allows for an immediate alerting of port scans activity

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? **An alarm should be configured to trigger if any request is made for the hidden directories from outside the company internal network. The hidden directories are for the company use only and should not be accessible from outside the premises.**
Additionally an alarm should trigger if sequential requests for the directories are made from a single ip address.

What threshold would you set to activate this alarm? **An appropriate threshold for sequential request from a single ip address should be set for greater than 0 request made.**

System Hardening

What configuration can be set on the host to block unwanted access?
-Stronger usernames and passwords
-Encrypt the contents of the hidden directories, and its content.
-disable directories listing in the apache

Describe the solution. If possible, provide required command lines.
-create a whitelist for authorized IP addreses
-make the folder private by changing permissions

Mitigation: Preventing Brute Force Attacks

Alarm

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

An alarm should be set or triggered if z predefined number of request are issued to the server from a single IP address.

What threshold would you set to activate this alarm?

An appropriate threshold should be set for greater than 50 request from a single IP address in the span of 30 minutes.

System Hardening

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

-Use unique user names, and stronger passwords
-restricting access to authentication URLs.
-setting up a lockout after 3 tries.
-two factor authentications for all users in the company.

Describe the solution. If possible, provide the required command line(s).

-strong passwords are unique, long harder to guess
-A requirement for brute force attacks is to send credentials so changing the login page url canusually be enough to stop most automated tools.
-CAPTCHAS prevents access by bots and auto tools.

Mitigation: Detecting the WebDAV Connection

Alarm

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

-An alarm should be set to trigger if any access to the WEBDAV directory is made from outside the company's internal network

What threshold would you set to activate this alarm?

Any single instance would trigger an alarm, if the WebDav directory is accessed, or possible of uploading of any files to the directory.

System Hardening

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

-The host should be configured to deny webdav uploads by default, and only allow uploads from a specific ip address this can be accomplished using apaches configuration.

-make sure software patches are up to date

Describe the solution. If possible, provide the required command line(s).

-install Filebeat on host machine for monitoring

-iptables -A INPUT -s (trusted ip address) -p tcp -m multiport -dports 80,443 -j ACCEPT

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

-alert if invalid file types are uploaded to the web server
-alert if any port is open.
-alert on traffic that does not belong there.

What threshold would you set to activate this alarm?

An appropriate threshold should be set for each singular file uploaded to the server if a file with the name xxxxxxxxxxxxxx.php comes in the alert should trigger

System Hardening

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

-all files from outside the company internal network shall be blocked.
-stored uploaded files in a location not accessible from the web.
-have all files run threw an antivirus

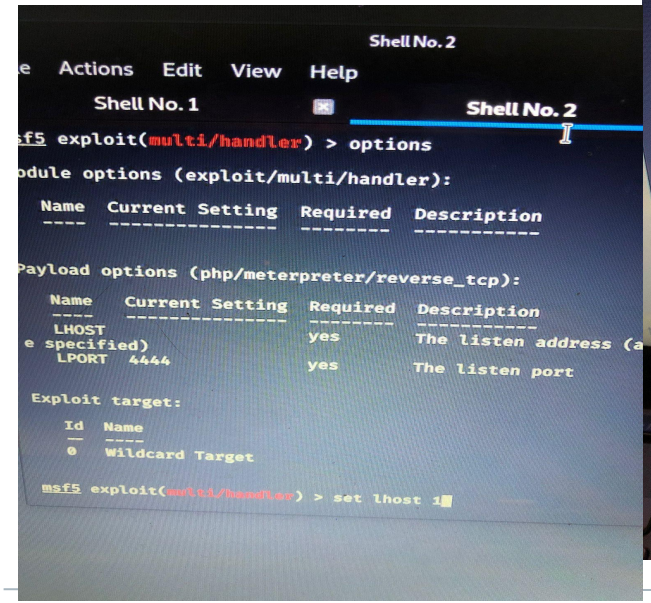
Describe the solution. If possible, provide the required command line.

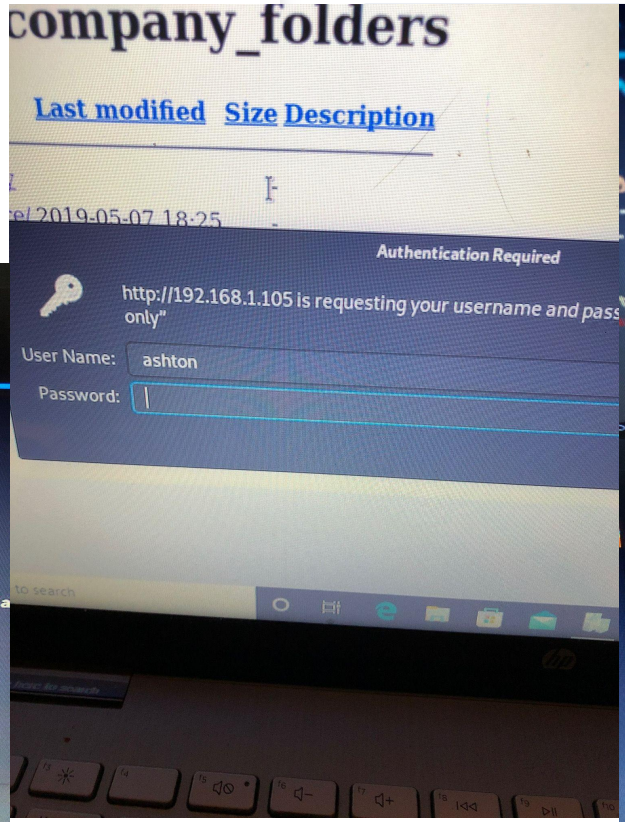
By heaving the file validated it can prevent extension spoofing that is used to hide file type

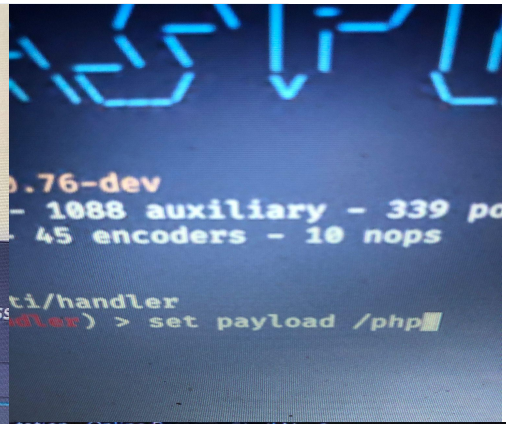
Bonus Info Metasploit

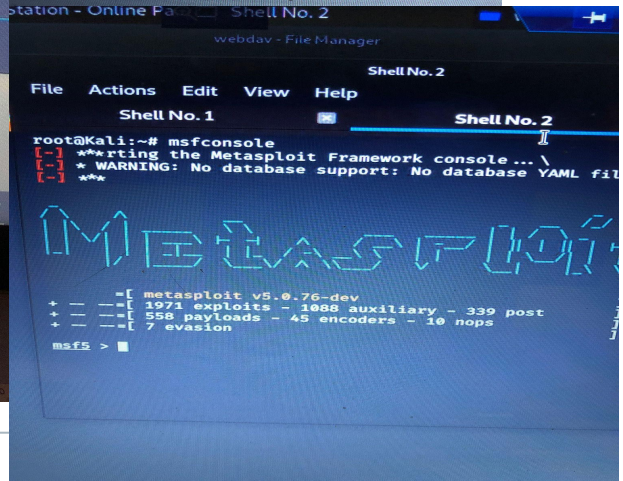
Alarm

Used metasploit to help get all information on ryans password information.










The End