Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK Machine	192.168.1.100	ELK Server
Capstone Server	192.168.1.105	Apache HTTP WebDav Server
Kali Linux	192.168.1.90	Red Team PenTest Machine
Windows Gateway	192.168.1.1	Default Gateway Router

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure CWE-200	Information included in the public facing code, text, and documents that reveals personal Identifiable information like a name or employment information.	This allows attackers to narrow their field of focus through enumeration to further define/refine their attack surface.
Brute Force Vulnerability CVE-2020-14494	A BFV consists of an attacker configuring predetermined values, making requests to a server using those values, and then analyzing the response.	This allows attackers to run values, such as passwords, through software that will guess predetermined strings until a favorable response returns.
PHP Remote File Inclusion CVE-2006-2849	This allows attackers to execute malicious code remotely	This allows attackers to gain backdoor access via a reverse TCP connection

1) GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, http://www.gao.gov/new.items/d08536.pdf.
2) https://owasp.org/www-community/attacks/Brute_force_attack

Exploitation: Sensitive Data Exposure

01

Tools & Processes

Utilize nmap to scan the local network to enumerate which server is the target machine.

Access the vulnerable server through the IP address listed.

Scan the Webdav pages for Sensitive Data Exposure.

02

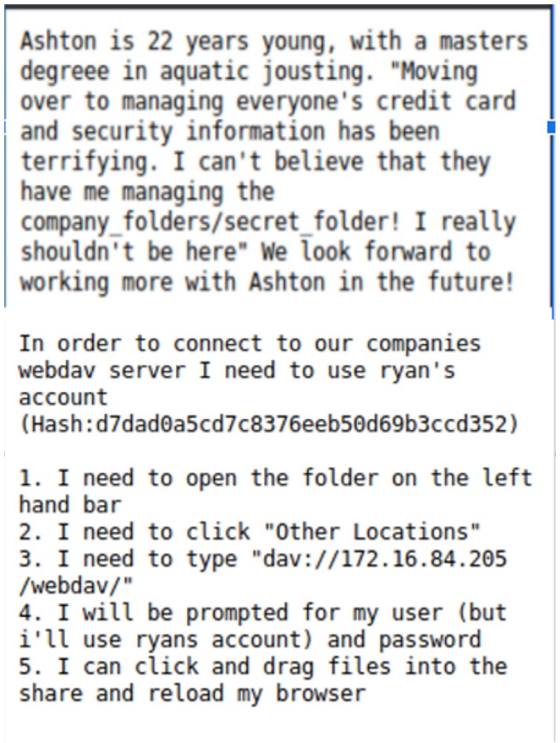
Achievements

This exploit allowed us to find the Webdav server.

Find three important pieces of information:

- secret_folder
- Ryan M. C.E.O
- Ashton is the manager of direct communication
- Ashton manages the secret folder
- Ryan manages the webdav folder

03



Exploitation: Brute Force Vulnerability

01

Tools & Processes

Utilize the hydra and the enumerated web pages to crack the passwords.

Command:

Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder

02

Achievements

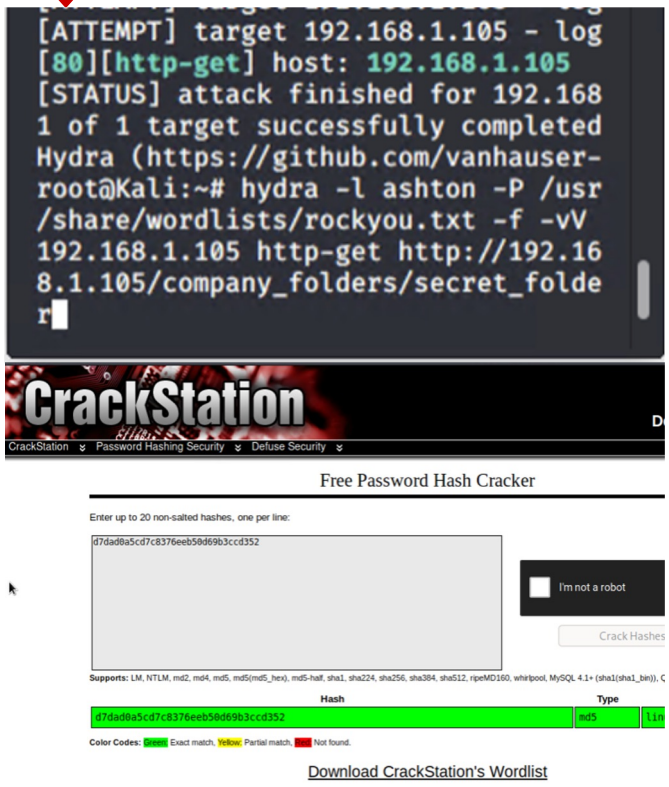
After running the command, we found ashton's login credentials:

Username: ashton
Password: leopoldo

We then used the hash provided in the secret folder to crack ryan's password using crackstation:

username : ryan
Password: linux4u

03



Exploitation: Local File Inclusion/Unauthorized File Upload

01

Tools & Processes
After cracking the password hash for ryan's account, we then could add the WebDav file share to our Network Files manger.

This will allow us to upload the malicious PHP script that we later execute for a reverse tcp connection.

02

Achievements
This allowed us to upload the malicious PHP script to initiate a reverse tcp connection.

Msfvenom was used to build the script.

Msfconsole was used to open the meterpreter session that ultimately allowed us a remote connection to find the flag.

03