Scenario:

Climbology, a climbing equipment manufacturer, never dedicated too much effort or resources to their accounting department. Unlike other accountants, who don't understand much about computers, you cannot ignore the potential bugs and security threats you see daily. During mandatory security tests on the company's networks, you asked to volunteer with the penetration testing team and focus on vulnerabilities in the accounting web application. To prove the importance of security, you decided to set a goal of obtaining the password and access to the application's server, which also hosts sensitive company information.

Objectives:

- Identify a vulnerability in the web application that can cause credentials to be sent across the network.
- Trigger the identified vulnerability and intercept the credentials sent over the network.
- Crack the hash of the intercepted credentials and obtain the password of the server's Administrator user.

Used tools:

Responder-Windows
Browser DevTools
John.exe

Fist of all checking the powershell machine ip using 'ipconfig' command:

Figure 1 - checking the IP of the machine

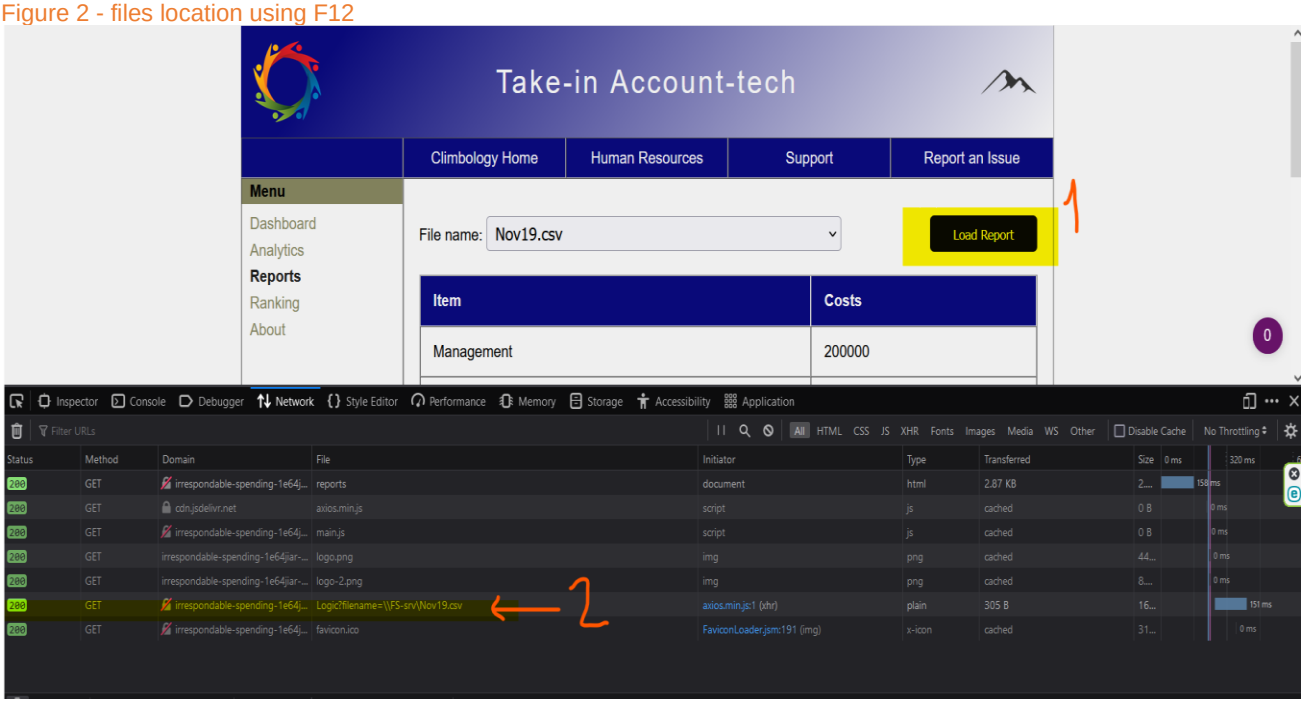
```
Windows IP Configuration


Ethernet adapter vEthernet (Ethernet) 3:

   Connection-specific DNS Suffix  . : ec2.internal
   Link-local IPv6 Address . . . . . : fe80::2d13:4b56:71:5545%34
   IPv4 Address. . . . . . . . . . . : 172.17.68.167
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.17.64.1
```

then starting Responder at : /tools/Responder-windows/binaries/Responder/responder.exe
the command syntax is : ./Responder.exe -i [ip]
the responder is a multi-protocol fake service provider written in python, it can respond to queries by LLMNR, NBT-NS, WPAD and other authintication protocols.
And the command above will generate NTLM-v2 HASH when LLMNR protocol is triggered, this happens when a user misstypes a location and the DNS service fails to locate the 'wrong location' of what the user was intending to visit.

Now we need to trigger a wrong location on the server.
Browsing the server looking for files locations.
In Report section we can see that there is File name with several file options and load file button.

This means that the server had files and the user choose a file to display from a specific location on the server. In order to locate the file's location, using dev.tools (F12), in the Network section we can have the requests method which will contain the file's location.

Figure 2 - files location using F12



* Notice the location – Logic?filename=//FS-srv/Nov19.csv
Navigating to that location will not trigger LLMNR because the location exists, but if we prove the filename input a wrong location the DNS service will fail to locate and LLMNR will be triggered and NTLM-v2 of the service owner will be displayed.

Figure 3 - triggering LLMNR.

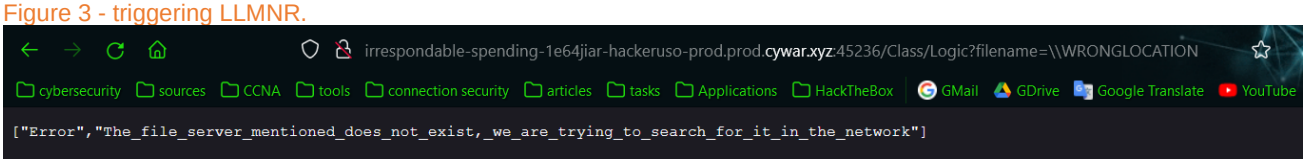


Figure 4 - displaying NTLM-V2 hash using Responder.exe

The hash will be saved in the Responder's log files, which are located in /logs directory.

Our next step will be to brute-force the given hash using john.exe using the command: John.exe –format=netntlmv2 –wordlist=[“path-to-rockyou.exe”] [path-to-log-file]

Figure 5 - brute-forcing using john.exe

```
PS C:\Users\Jackie\tools\john\run> .\john.exe --format=netntlmv2 --wordlist="..\..\rockyou.txt" C:\Users\Jackie\tools\Responder-Windows\binaries\Responder\logs\SMBv2-NTLMv2-SSP-172.17.67.190.txt
>>
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
MrCash           (iis-admin)
1g 0:00:00:00 DONE (2021-12-19 19:20) 6.896g/s 600275p/s 600275c/s 600275C/s bunny10..100777
Warning: passwords printed above might not be all those cracked
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
PS C:\Users\Jackie\tools\john\run>
```

After having the password (MrCash) , the challenge asks to generate the password to MD5 hash which will be the flag’s value:

Figure 6 - generating the password to MD5

MrCash

Generate →

Your String	MrCash
MD5 Hash	c9d43a699089e19dbf47bbf8b53df3f2 Copy

CHALLENGE PWNED!

Please feel free to contact me on: **Monhalsarbouch@gmail.com**