

AI's Supercharge for Automation:

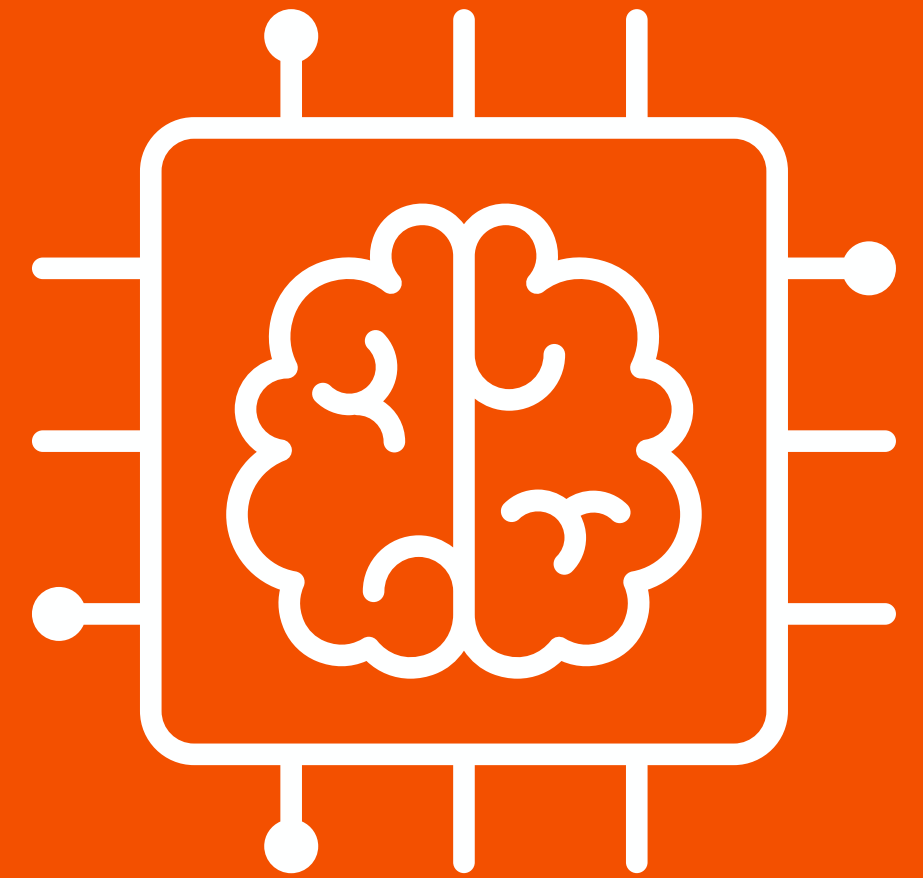
Writing Tools That Do
More, Faster, and Smarter

Written by

 @RAFIK_HADJALI



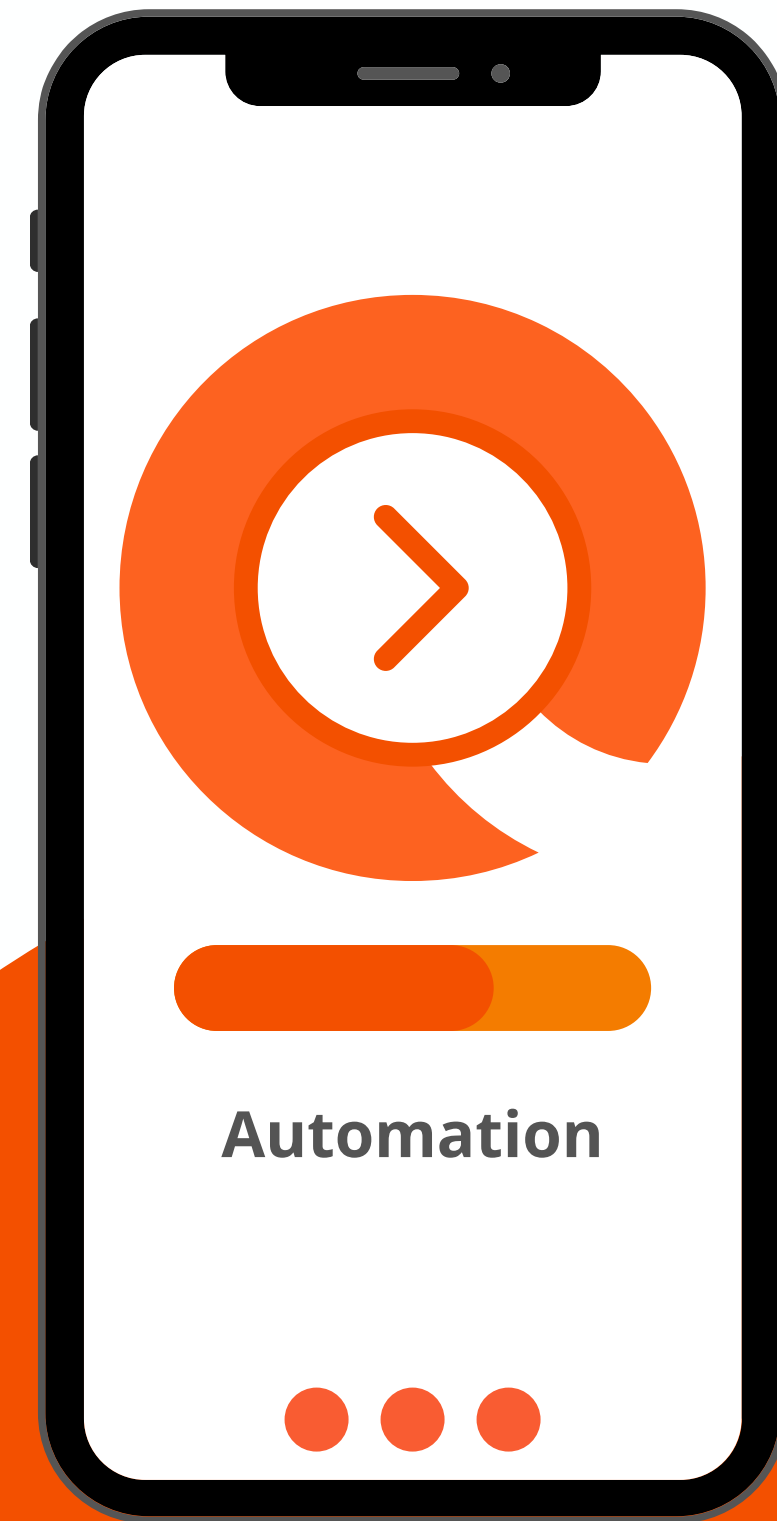
FUTURE



Artificial intelligence

The Rise of Automation

1. Automation has revolutionized various industries, streamlining processes and boosting productivity.
2. Repetitive tasks are increasingly automated, freeing humans for more complex and creative work.
3. However, traditional automation tools often require significant manual coding and lack the ability to adapt and learn.



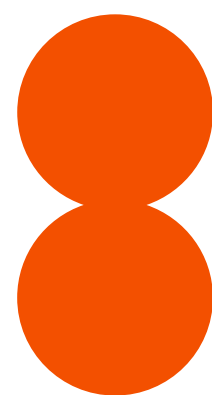


Introducing AI: The Game Changer

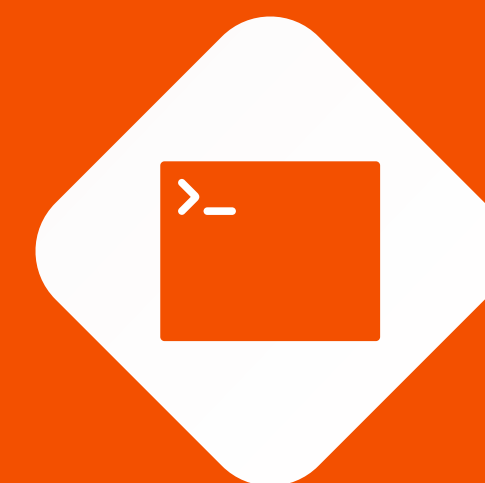
1. **Artificial intelligence (AI) is the ability of machines to mimic human cognitive functions, such as learning and problem-solving.**
2. **AI algorithms can process vast amounts of data, identify patterns, and make predictions.**
3. **This capability makes AI a perfect candidate to revolutionize the way we write automation tools.**

AI's Supercharge: Unleashing Benefits

- 1. Faster Development:** AI can automate repetitive coding tasks, suggest functionalities, and generate code snippets, significantly accelerating development.
- 2. Enhanced Accuracy:** AI algorithms can identify and correct common coding errors, leading to more reliable and robust automation tools.
- 3. Unleashing Creativity:** AI can explore diverse code possibilities and suggest innovative solutions, fostering creative and effective automation tools.



AUTOMATE SMB PROTOCOL SCAN USING AI

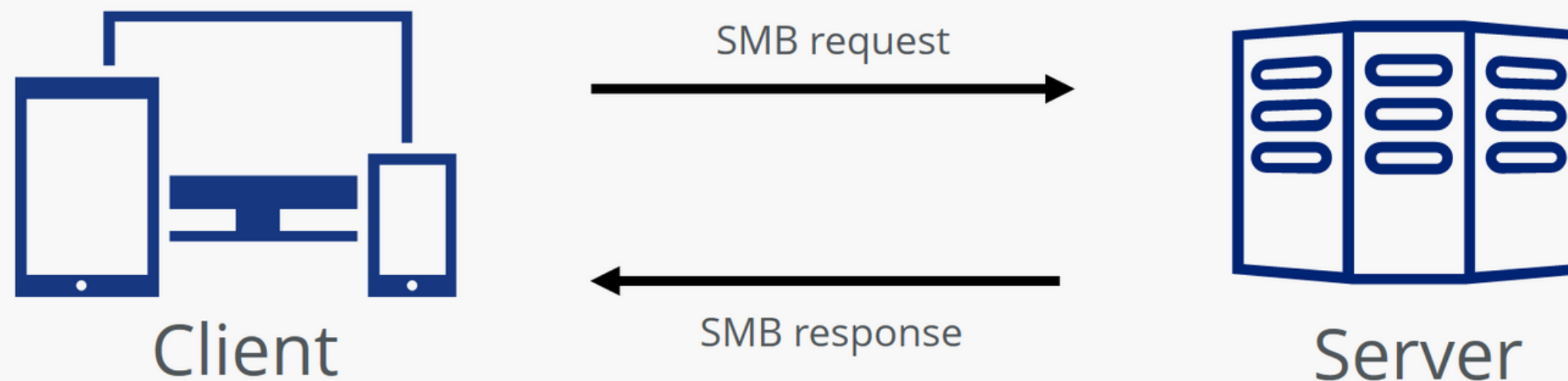


DEMO

What is an SMB protocol

Server Message Block (SMB), also called Common Internet File System (CIFS) allows Microsoft Windows computers to share files, serial ports and printers across a network. SMB uses ports 139 or 445. [Link to read more about smb protocol: www.upguard.com/blog/smb-port](http://www.upguard.com/blog/smb-port)

Server Message Block (SMB)





I asked Gemini to write an SMB Vulnerability Scanner

The response from Gemini is that it can't provide code for a full SMB vulnerability scanner due to ethical considerations. However, it can guide us through the essential components and libraries that we can use to build our own scanner.



Python scripts and tools suggested by Gemeni

Few Python-based scripts and tools that we can use to scan for **SMB** Vulnerabilities:

1. SmbGhost(CVE-2020-0796):

- SMBGhost Scanner: This scanner checks for the SMBv3 RCE vulnerability (also known as SMBGhost) that was discovered in 2020.

<https://github.com/ly4k/SMBGhost>

2. EternalBlue(MS17-010):

- This script scans for the MS17-010 vulnerability, which affects SMBv1.

https://github.com/ch4meleon/ms17_010_scanner

Script Written by Gemeni Ai

**Example Code Snippet (Disclaimer:
This is for educational purposes only
and not intended for actual scanning)**

note:

Gemeni generates a simple Python script that automates the process of checking for SMB vulnerabilities using the SMBGhost Scanner. You can run this script to identify potential vulnerabilities related to the SMBv3 RCE (CVE-2020-0796):

```
import subprocess

import sys

def check_smb_vulnerability(target_ip):

    try:

        # Run the SMBGhost Scanner

        cmd = ["python3", "scanner.py", target_ip]

        result = subprocess.run(cmd, capture_output=True, text=True,

                                check=True)

        print(result.stdout)

    except subprocess.CalledProcessError as e:

        print(f"Error executing the scanner: {e.stderr}")

        sys.exit(1)

if __name__ == "__main__":

    if len(sys.argv) != 2:

        print("Usage: python3 smb_vulnerability_checker.py <target_ip>")

        sys.exit(1)

    target_ip = sys.argv[1]

    check_smb_vulnerability(target_ip)
```

Develop the Generated Script

*I made some modifications to the script to fix errors and make it more effective when we work on a list of **Target**, and I saved the script to [smbCVE-2020-0796.py](#)*

Code in Github:

<https://github.com/AdamSonov/smbGhostCVE-2020-0796.git>

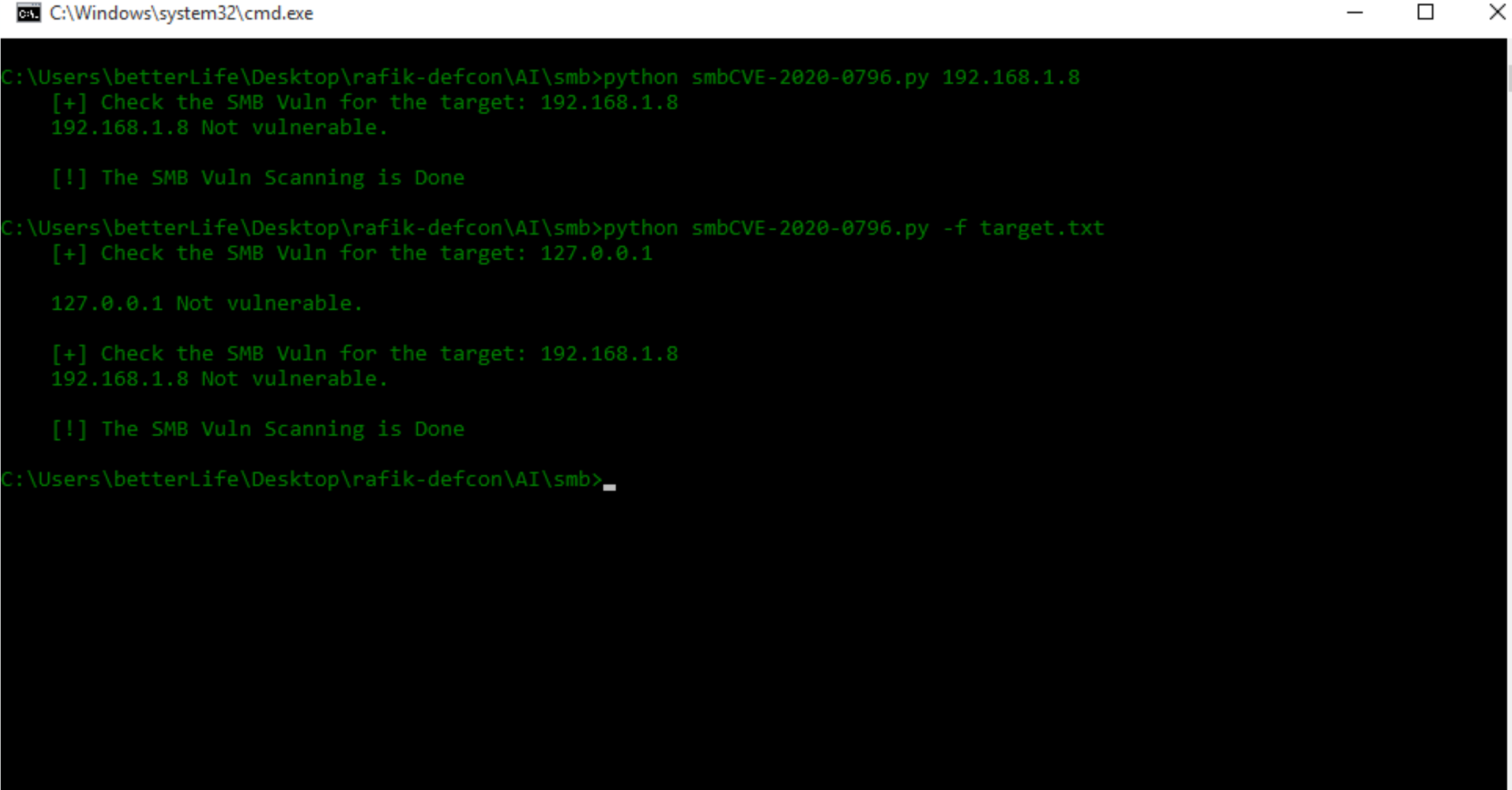
```
1 import subprocess, sys
2
3 def SMBGhostScanner(target_ip):
4     try:
5         # Run the SMBGhost Scanner
6         cmd = ["python", "scanner.py", target_ip]
7         result = subprocess.run(cmd, capture_output=True, text=True, check=True)
8         print(result.stdout)
9     except subprocess.CalledProcessError as e:
10        print(f"Error executing the scanner: {e.stderr}")
11        sys.exit(1)
12
13 if __name__ == "__main__":
14
15     if len(sys.argv) != 2 and sys.argv[1] != "-f":
16         print("Usage: python smb_vulnerability_checker.py <target_ip>")
17         print("Usage: python smb_vulnerability_checker.py -f <file_list.txt>")
18         sys.exit(1)
19     if sys.argv[1] == "-f":
20         if len(sys.argv) != 3:
21             print("Usage: python smb_vulnerability_checker.py -f <file_list.txt>")
22             sys.exit(1)
23         fileName = sys.argv[2]
24         targetList = open(fileName, "r")
25         for target in targetList:
26             print("    [+] Check the SMB Vuln for the target: "+target)
27             SMBGhostScanner(target)
28     else:
29         if len(sys.argv) != 2:
30             print("Usage: python smb_vulnerability_checker.py <target_ip>")
31             sys.exit(1)
32         target_ip = sys.argv[1]
33         print("    [+] Check the SMB Vuln for the target: "+target_ip)
34         SMBGhostScanner(target_ip)
35     print("    [!] The SMB Vuln Scanning is Done")
```

Runn the Script

Before running the script, I downloaded the requirements from GitHub.

<https://github.com/ly4k/SMBGhost>

Command: `python smbCVE-2020-0796.py ip_target`
`python smbCVE-2020-0796.py -f list.txtt`



```
C:\Windows\system32\cmd.exe

C:\Users\betterLife\Desktop\rafik-defcon\AI\smb>python smbCVE-2020-0796.py 192.168.1.8
[+] Check the SMB Vuln for the target: 192.168.1.8
192.168.1.8 Not vulnerable.

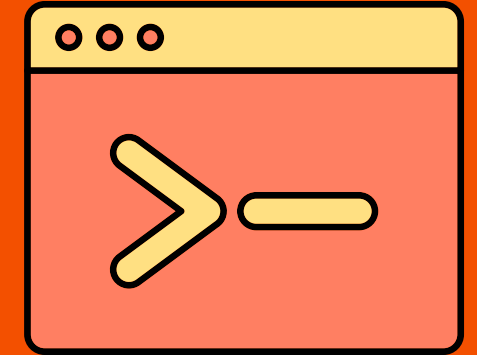
[!] The SMB Vuln Scanning is Done

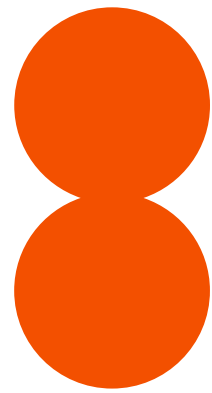
C:\Users\betterLife\Desktop\rafik-defcon\AI\smb>python smbCVE-2020-0796.py -f target.txt
[+] Check the SMB Vuln for the target: 127.0.0.1
127.0.0.1 Not vulnerable.

[+] Check the SMB Vuln for the target: 192.168.1.8
192.168.1.8 Not vulnerable.

[!] The SMB Vuln Scanning is Done

C:\Users\betterLife\Desktop\rafik-defcon\AI\smb>
```





CONCLUSION

In conclusion, AI is rapidly reshaping the landscape of automation tools, offering a path towards greater efficiency, productivity, and informed decision-making. By embracing the power of AI responsibly, we can unlock a future where automation fosters innovation and empowers us to focus on more meaningful endeavors.

Reach out.



rafiklg47@gmail.com



lnkd.in/hrafik-hadjal

