Name: Chaudhary Tuba Sharif

Roll No: 231410

Practical No: 9

Date Of Performance: 15/09/2025

Aim: To implement and demonstrate keylogger attacks

Lab Outcome: A comprehensive theoretical understanding of what keyloggers are, how they are deployed, the mechanisms they use to capture data, and the best practices for detecting, removing, and preventing them.

Theory:

What is a Keylogger?

A keylogger, or keystroke logger, is a form of surveillance technology used to monitor and record every keystroke typed on a specific computer's keyboard. While there are legitimate uses for keyloggers (e.g., parental control, corporate monitoring), they are most commonly associated with malicious activities. Cybercriminals deploy keyloggers to surreptitiously steal sensitive information such as usernames, passwords, credit card numbers, private messages, and other confidential data.

Types of Keyloggers

As detailed in the research material, keyloggers can be broadly categorized based on their method of operation:

- Software-Based Keyloggers: These are the most common type. They are programs installed on a victim's device that run silently in the background, capturing keystrokes and often sending the logged data to a remote attacker.
- Hardware-Based Keyloggers: These are physical devices, such as a small USB
- dongle that connects between the keyboard and the computer, which intercept and store keystrokes locally. They require physical access to the machine for both installation and retrieval of data.
- Kernel-Level Keyloggers: These are highly sophisticated and operate at the core (kernel) of the operating system. Their deep integration makes them extremely difficult for standard antivirus programs to detect.
- Remote Access Trojan (RAT) Keyloggers: This type is a component of a larger malware package (a trojan). The keylogging functionality is one of many malicious capabilities, which can also include taking screenshots, accessing the webcam, and stealing files.

Common Installation Vectors

Keyloggers are installed on a system without the user's consent through various deceptive methods:

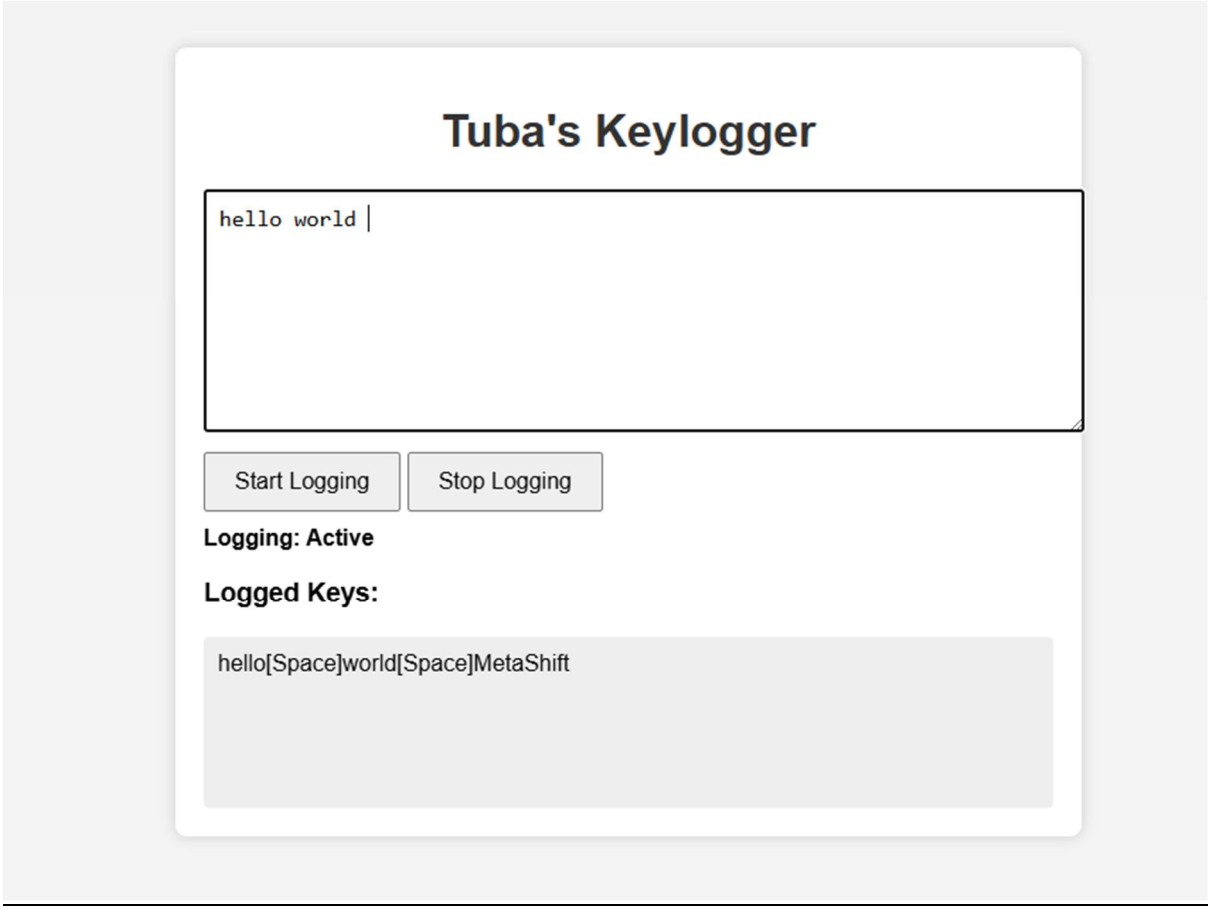
- Phishing & Malicious Attachments: Victims are tricked into opening an infected email attachment that silently installs the keylogger.
- Drive-By Downloads: Visiting a compromised website can trigger an automatic download and installation by exploiting browser vulnerabilities.
- Cracked or Fake Software: Illegitimate copies of software or "free" utilities are often bundled with malware, including keyloggers.
- Social Engineering: Attackers convince a user to voluntarily install a program that has a hidden keylogging component.

CODE:

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>Tuba's Keylogger</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f4f4f4;
      padding: 30px;
    }

    h1 {
      text-align: center;
      color: #333;
    }

    .container {
      max-width: 600px;
      margin: 0 auto;
      background: white;
      padding: 20px;
      border-radius: 8px;
      box-shadow: 0 0 10px #ccc;
    }

    textarea {
      width: 100%;
      height: 150px;
      padding: 10px;
      font-size: 16px;
    }

    button {
      margin-top: 10px;
      padding: 10px 20px;
      font-size: 16px;
      cursor: pointer;
    }

    #log {
      margin-top: 20px;
      background: #eee;
      padding: 10px;
      min-height: 100px;
      white-space: pre-wrap;
      border-radius: 4px;
    }

    .status {
      margin-top: 10px;
      font-weight: bold;
    }
  </style>
</head>
<body>

  <div class="container">
    <h1>Tuba's Keylogger</h1>

    <textarea id="inputArea" placeholder="Type something..."></textarea>

    <br>
    <button id="startBtn">Start Logging</button>
    <button id="stopBtn">Stop Logging</button>

    <div class="status" id="status">Logging: Inactive</div>

    <h3>Logged Keys:</h3>
    <div id="log"></div>
  </div>

  <script>
    const inputArea = document.getElementById('inputArea');
    const logDiv = document.getElementById('log');
    const startBtn = document.getElementById('startBtn');
    const stopBtn = document.getElementById('stopBtn');
    const status = document.getElementById('status');

    let isLogging = false;
    let logData = '';

    function logKey(e) {
      if (!isLogging) return;

      let key = e.key;
      if (key === ' ') key = '[Space]';
      else if (key === 'Enter') key = '[Enter]\n';
```

```
        else if (key === 'Backspace') key = '[Backspace]';

        logData += key;
        logDiv.textContent = logData;
    }

    startBtn.onclick = function () {
        isLogging = true;
        status.textContent = 'Logging: Active';
        inputArea.focus();
    };

    stopBtn.onclick = function () {
        isLogging = false;
        status.textContent = 'Logging: Inactive';
    };

    inputArea.addEventListener('keydown', logKey);
  </script>

</body>
</html>
```

OUPTUT:



Performance (7M)	Journal (3M)	Lab Ethics (2M)	Attendance (3M)	Total (15M)	Faculty Signature