Cybersecurity Internship Report – Arch Technologies

Intern: Umar Farooq
Position: Cybersecurity Intern
Internship Duration: July 1 – July 27, 2025

Overview

During my remote internship at **Arch Technologies**, I participated in two hands-on cybersecurity projects focused on core concepts of **network traffic analysis** and **keystroke logging**. These experiences provided me with a solid foundation in both theoretical understanding and practical skills. Below is a comprehensive report of my work.

Project 1: Network Sniffer in Python

Objective

To develop a **network sniffer** using Python that captures and analyzes real-time network traffic, enabling better understanding of packet structures and data transmission in a networked environment.

Tools & Technologies

- **Python**
- **Scapy**: For packet sniffing and analysis
- **Logging module**: To log captured packet details with timestamps

Installation:
```
pip install scapy
```

Implementation Details

1. **Packet Capture**
    - Used Scapy's `sniff()` function with a filter to capture only **IP packets** using **TCP or UDP** protocols.
2. **Packet Analysis**
    - Extracted source and destination IP addresses.
    - Retrieved port numbers from TCP/UDP headers.

3. **Logging Output**

```
[IP] 192.168.1.10 -> 142.250.190.14
[TCP] Port: 50345 -> 443
```

This output shows communication between a local device and a remote server over HTTPS.

4. **Execution & Safety**
    - Requires elevated privileges (e.g., sudo).
    - Interrupt safely using Ctrl+C.

Sample Output

```
2025-07-22 14:03:01 - [IP] 10.0.0.5 -> 142.250.191.206
2025-07-22 14:03:01 - [TCP] Port: 53123 -> 443
```

Learning Outcomes

- Gained experience in live traffic monitoring.
- Understood IP, TCP, and UDP packet structure.
- Developed foundational skills for intrusion detection and analysis tools.

Project 2: Keylogger Simulation in Python

Objective

To simulate a basic **keylogger** in a secure, offline setting to understand the behavior and implications of keystroke logging.

Tools & Technologies

- **Python**
- **pynput**: For keyboard input monitoring
- **CSV module**: For structured log storage

Installation:
`pip install pynput`

Implementation Details

1. **Key Monitoring**
    - Utilized `keyboard.Listener` to detect all key presses.
2. **Key Formatting**
    - Regular characters logged directly.
    - Special keys (e.g., Enter, Space) formatted as `[ENTER]`, `[SPACE]`, etc.

3. **Log File Creation**
    - Stored keystrokes in daily `.csv` files with timestamps.
4. **Safe Exit**
    - Pressing the `ESC` key stops the logger.

Sample Log Output

TIMESTAMP	KEY PRESSED
2025-07-26 10:34:12	H
2025-07-26 10:34:13	E
2025-07-26 10:34:14	L
2025-07-26 10:34:15	L
2025-07-26 10:34:16	O
2025-07-26 10:34:17	[SPACE]

Risks Associated with Keylogging

1. **Theft of Sensitive Information**: Keyloggers can capture login credentials, credit card numbers, personal messages, and other private data without user consent.
2. **Identity Theft**: Collected data can be used to impersonate victims, leading to fraudulent transactions, unauthorized access, and reputational damage.
3. **Unauthorized Access**: Attackers can gain access to restricted systems or accounts, potentially compromising entire networks.

Ethical Note

This project was conducted purely for **educational purposes**. Unauthorized use of keyloggers is **illegal** and **unethical**. The simulation helps security professionals understand threats and build defensive strategies.

Learning Outcomes

- Learned to build input monitoring tools.
- Understood attacker techniques and data theft risks.
- Gained insight into ethical boundaries and legal considerations in cybersecurity.

Conclusion

My internship at Arch Technologies was a significant milestone in my cybersecurity learning journey. Through two practical projects, I:

- Learned the fundamentals of **packet sniffing and protocol analysis**.
- Understood the inner workings of **keystroke logging**.
- Strengthened my Python programming and system-level scripting skills.
- Became more aware of **cyber ethics**, legal considerations, and best practices.

These projects have deepened my interest in cybersecurity, particularly in areas such as **network security**, **digital forensics**, and **ethical hacking**. I look forward to continuing my learning and contributing to a safer digital environment.