Cybersecurity Daily Dairy

Day 3: Phishing Attack using CamPhish & Hack Camera

Date: June 20, 2025

Topics Covered:

- Camera-based phishing attack using **Hack-Camera**
- Using GitHub to download hacking tools
- Assigning script execution permissions in Linux
- Launching phishing attacks through the terminal
- Real-world example: capturing webcam images using phishing
- Awareness about **social engineering risks**

What I Did:

Today I learned how phishing attacks can be executed using **webcam-based lures**. I downloaded and executed a tool named **Hack-Camera**, which simulates a fake page asking for camera permission and secretly captures images when users accept.

Steps Performed:

1. Downloaded the **Hack-Camera** tool from GitHub.
2. Opened the tool folder and listed its contents.
3. Switched to root user for administrative access.
4. Gave necessary permission to run the script file.
5. Executed the phishing script.
6. Chose the YouTube video phishing option from the menu.
7. Provided a YouTube video ID when prompted.
8. Received a phishing link and opened it in a browser.
9. When the browser asked for camera access and permission was granted:
    - A YouTube video was played to distract the victim
    - The tool secretly captured webcam images
    - Images were sent to the attacker's terminal
    - Images were stored in the Hack-Camera folder

Real-World Implications:

This attack highlights how attackers exploit **trust and curiosity**:

- Users often allow webcam access without thinking
- Phishing pages can be disguised as something innocent like a video
- Images are captured without user knowledge

Key Learnings:

- GitHub is a resourceful platform to access hacking tools
- Linux permission commands are crucial for running scripts
- Shell scripts can automate complex attacks
- **Social engineering** is one of the most powerful tools in a hacker's arsenal

---

Tools Used:

- **Hack-Camera** GitHub tool
- **Linux Terminal (Kali)**
- **Browser** for phishing simulation