CYBERSECURITY DAILY DAIRY

Day 4: Phishing Attacks using Zphisher & ErisPhisher (June 21, 2025)

Topics Covered:

- Phishing automation with *Zphisher* and *ErisPhisher*.
- Cloning GitHub repositories.
- Setting up fake login pages.
- Simulating credential theft.
- Port forwarding with Cloudflared.
- DNS theory and DNS Flood attack with Xerxes.
- Threat analysis tools.
- Certifications: *CEH* and *OSCP*.

What I Did:

I did phishing simulations with *Zphisher* and *ErisPhisher*. I also learned about DNS and did a DNS flooding attack with *Xerxes*. I looked at tools for detecting phishing and researched cybersecurity certifications.

Tools Used to Create Fake Login Pages:

- **Zphisher**
- **ErisPhisher**

Steps Followed:

1. **Cloning Repositories:** Downloaded Zphisher and ErisPhisher from GitHub.
2. **Navigating Directories:** Changed terminal directory to the tool.
3. **Gaining Root Access (Optional):** Switched to root user.
4. **Giving Execution Permission and Running Script:** Made the script executable and ran it.
5. **Selecting Target Platform:** Chose a platform (e.g., Facebook).
6. **Selecting Login Page Style:** Chose a fake login page style.
7. **Choosing Port Forwarding Method:** Selected **Cloudflared** for a public URL.
8. **Responding to Additional Prompts:** Declined custom port/URL masking.
9. **Final Output:** Generated a phishing URL. Credentials entered on the fake page appeared in my terminal and were saved.

Disclaimer:

This is for educational purposes only. Phishing without permission is illegal.

What is DNS?

DNS translates domain names (like example.com) into IP addresses (like 93.184.216.34) for computers.