Cybersecurity Daily Dairy

Day 4: Phishing Attacks using Zphisher & ErisPhisher

Date: June 21, 2025

Topics Covered:

- Phishing attack automation with *Zphisher* and *ErisPhisher*
- Cloning phishing tool repositories from GitHub
- Setting up fake login pages for social media platforms
- Simulating credential theft and capturing results
- Port forwarding using Cloudflared
- DNS theory and DNS Flood attack using Xerxes
- Threat analysis tools and platforms
- Introduction to certifications: *CEH* and *OSCP*

What I Did:

On Day 4, I explored how to carry out realistic phishing simulations using *Zphisher* and *ErisPhisher*. I also studied DNS concepts and executed a DNS flooding attack using the tool *Xerxes*. Additionally, I explored various platforms used to detect and investigate phishing websites. Finally, I researched some popular cybersecurity certifications.

Tools Used to Create Fake Login Pages:

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

Steps Followed

1. Cloning the Repositories

I downloaded both Zphisher and ErisPhisher from GitHub by using the git clone command to copy the code to my local machine.

2. Navigating to Tool Directories

I changed the working directory in the terminal to either zphisher or ErisPhisher, depending on which tool I wanted to use.

3. Gaining Root Access (Optional)

I switched to the root user to get administrative privileges, which some scripts may require to execute properly.

4. Giving Execution Permission and Running the Script

I modified the permissions of the main script file to make it executable and then ran the script to launch the phishing tool interface.

5. Selecting Target Platform

When the tool started, it showed a list of platforms (like Facebook, Instagram, Google, etc.) that I could use to simulate a phishing page.
I selected Facebook for this simulation.

6. Selecting Login Page Style

The tool provided several styles of fake login pages, such as:

- Traditional login page
- Advanced voting poll login page
- Fake security login page
- Messenger login page

I chose the traditional login page for the test.

7. Choosing Port Forwarding Method

The tool offered options for making the phishing page accessible over the internet. I selected **Cloudflared**, a port forwarding method that creates a public URL for my local server.

8. Responding to Additional Prompts

The tool asked whether I wanted to use a custom port or mask the URL. I declined both options for simplicity.

9. Final Output

The tool generated a phishing URL.
When opened in a browser, the fake login page loaded.
Any credentials entered into the fake form appeared in my terminal and were saved locally in the tool's folder.

Disclaimer:

This documentation is for educational purposes only as part of cybersecurity training. Launching phishing attacks without permission is illegal and unethical.

What is DNS?

DNS (Domain Name System) is a system that translates human-readable domain names (like example.com) into IP addresses (like 93.184.216.34) that computers use to identify each other on the internet.

- It maps domain names to IP addresses

- Eliminates the need to remember numerical IPs
- Uses a hierarchical structure with root, top-level domains (.com, .org), and subdomains

---

DNS Attack using Xerxes:

Tool used :

XERXES

I simulated a **DNS Flood attack** using a tool called *Xerxes*. This type of attack sends excessive requests to the target server, exhausting its resources and making it unresponsive.

Steps Performed:

1. I downloaded the Xerxes tool from GitHub using Git.
2. I entered the Xerxes folder and accessed root user mode.
3. I compiled the attack script and executed it with a domain name and port number.

This launched a DNS Flood attack aimed at overwhelming the target's server with traffic, simulating a Denial of Service condition.

Threat Analysis & Phishing Detection Platforms:

Tool	Description
VirusTotal	Scans URLs and files using over 70 antivirus engines
urlscan.io	Displays how a website behaves, including redirects and embedded scripts
webcheck	Analyzes URLs and gives basic risk scores
HaveIBeenPwned	Checks if an email or data has been leaked in past breaches
Censys.io	Search engine for internet-connected systems and assets
Whois Lookup	Provides domain registration and ownership details
Metasploitable	A purposely vulnerable Linux VM used for practice in penetration testing
Tenable Nessus	A widely used vulnerability scanner
Bug Bounty Platforms	Platforms like HackerOne and Bugcrowd for reporting security vulnerabilities

---

Cybersecurity Certifications:

CEH (Certified Ethical Hacker)

- Provided by EC-Council

- Covers ethical hacking tools and techniques
- Good for beginners looking to enter ethical hacking

OSCP (Offensive Security Certified Professional)

- Offered by Offensive Security
- Hands-on, practical penetration testing exam
- Highly respected in the cybersecurity industry
- Requires strong technical and practical skills

Key Learnings:

- Tools like Zphisher and ErisPhisher can automate phishing simulation setups
- DNS Flood attacks can disable web services by overwhelming servers
- Several online tools can detect and analyze phishing threats
- CEH and OSCP are valuable certifications for a career in ethical hacking

---

Tools Used:

- Zphisher and ErisPhisher for phishing simulations
- Xerxes for DNS attack testing
- VirusTotal, urlscan.io, Censys, Whois, HaveIBeenPwned for threat analysis
- Kali Linux Terminal and web browsers for testing environments
- Tenable Nessus and Metasploitable for vulnerability analysis