TRAINING DAY 24 REPORT

Understand Phishing

Today, I learn some important concepts

Introduction to Phishing

Phishing is a type of cyberattack where attackers trick individuals into providing sensitive information (like passwords, credit card numbers, or personal data) by pretending to be trustworthy entities—usually via email, fake websites, or messages.

Phishing Part – 1

This typically covers the **basics of phishing attacks**, including:

- How phishing works
- Types of phishing (email phishing, spear phishing, smishing, etc.)
- How attackers craft deceptive messages or websites

Phishing Part – 2

Usually involves **hands-on or technical aspects**, such as:

- Creating fake login pages (for social media, banking, etc.)
- Hosting phishing pages locally
- Understanding how credentials are captured

Phishing Part – 3

Covers **advanced techniques** like:

- Deploying phishing pages online
- Avoiding detection
- Bypassing browser security warnings
- Using tunneling services like Ngrok for real-world deployment

Installation of Ngrok

Ngrok is a tunneling tool that allows users to expose local servers (like a phishing page hosted on localhost) to the internet. It's often used in phishing demonstrations to share fake login pages online using a public URL.

Phishing Tools – Blackeye, Shellphish, Setoolkit

These are **automated phishing frameworks**:

- **Blackeye**: A tool that generates phishing pages for popular websites and captures login credentials.
- **Shellphish**: A tool similar to Blackeye, often used in penetration testing to create fake login pages quickly.
- **Setoolkit (Social-Engineer Toolkit)**: A more advanced tool used for social engineering attacks, including phishing, credential harvesting, and more.