CYBERSECURITY DAILY DAIRY

Day 15: Session Hijacking & Network Scanning (July 4, 2025)

Topics Covered:

- Session hijacking basics.
- Vulnerability scanning with Nmap.
- Introduction to NetVision Nmap GUI Tool.
- File encryption with FileCrypti.

What is Session Hijacking?

Attackers gain unauthorized access to an active session, often by capturing session tokens or cookies.

- **Active hijacking:** Attacker takes over.
- **Passive hijacking:** Attacker monitors silently.
  Tools like Wireshark, Burp Suite, or custom scripts can be used.

Nmap: Vulnerability & Port Scanner

Nmap is an open-source tool for network scanning and security auditing.

- Host discovery
- Port scanning
- Service/version detection
- OS fingerprinting
  Helps find open ports and services for reconnaissance.

NetVision: GUI-based Nmap Scanner

NetVision is a graphical interface for Nmap, making scanning easier.

- User-friendly.
- Target-based scanning.
- Real-time results.
- Custom scan profiles.

FileCrypti: File Encryption Utility

FileCrypti is a command-line tool for encrypting/decrypting files.

- Strong encryption.
- Protects sensitive files.
- Easy to use.
- Useful for data protection.

Key Learnings:

- Session hijacking is a big risk; use proper session management and encryption.
- Nmap is a fundamental scanning tool.
- NetVision simplifies Nmap for beginners.