Name: Shoaib Akhter
Enrollment No= 02-131212-009
Reg No= 79290

Q No: 1

To address OTP bypass, attackers exploit social Engineering; malware, SIM swapping & a reverse proxy phishing kits: common tools include,

1) Social Engineering:

Attackers trick users into sharing OTPs via phishing or impersonation.

2) SIM Swapping:

Gaining control of the victim's mobile number by tricking telecom providers.

3) Malware:

Injecting keyloggers or remote access tools (RATs) to capture OTPs.

4) Main-in-the-Middle (MitM) Attacks.

Using proxy tools like Modlishka to intercepts OTPs in real-time.

5) Credential Stuffing.

Exploiting reused credentials with brute force to trigger OTPs & bypass them.

6) Tools & Frameworks Employed.

1) Phishing Kits.
2) Advanced Reverse Proxies
   2.1) Modlishka
   2.2) Evilginx2
3) SIM Swapping Tools.
4) RATs and Malware
5) Automated Bots.

7) Mitigation Strategies

1) Adopt Token-Based Authentication.
   Replace SMS-based OTPs with hardware tokens (e.g., Yubikey).

3) Enhanced User Education.
Train users to recognize phishing attempts and SIM swap alerts.

3) Multi-layered Security.
Implement adaptive authentication mechanisms using biometric or behavioral analytics

4) Anti-Malware and Endpoint Protection.
Deploy advanced malware detection systems

5) Encrypted Communications.
Enforce end-to-end encryption for OTP delivery.

6) AI-Driven Fraud Detection.
Use machine learning algorithms to detect anomalies and block suspicious activities of their 2FA system against OTP bypass threats.