Cybersecurity with Python – Offensive Tools

فصل ۱: مبانی تست نفوذ(Penetration Testing)

- فرآیند تست نفوذ(Reconnaissance, Scanning, Exploitation, Reporting)
- قوانین اخلاقی و چارچوب‌های استاندارد(OWASP, PTES)

فصل ۲: جمع‌آوری اطلاعات(Information Gathering)

- اسکن شبکه با nmap وPython Wrapper
- نوشتن اسکریپت برایDNS Enumeration
- وب‌اسکرپینگ برای جمع‌آوری اطلاعات

فصل ۳: آسیب‌پذیری‌ها و اکسپلویت‌ها

- شناسایی سرویس‌های آسیب‌پذیر
- نوشتن اسکریپت Brute Force ساده باPython
- ایجاد PoC Exploit برای آسیب‌پذیری‌های شناخته‌شده

فصل ۴: مهندسی اجتماعی(Social Engineering)

- تولید ایمیل‌های فیشینگ تستی باPython
- شبیه‌سازی حملات Keylogger ساده
- اسکریپت‌های جعلی برای تست کاربر

فصل ۵: پست-اکسپلویتیشن(Post-Exploitation)

- مدیریت نشست‌ها(Sessions)
- اجرای دستورات از راه دور
- استخراج و ارسال داده‌ها