Practical Cybersecurity with Python

(امنیت با پایتون – ویژه ویندوز)

مخاطب : علاقه‌مندان به امنیت، توسعه‌دهندگان، دانشجویان
پیش‌نیاز : آشنایی با مبانی پایتون، آشنایی با مفاهیم شبکه
محیط تدریس : ویندوز (Windows ۱۰ یا بالاتر)

فصل ۱: مقدمه بر امنیت و نقش پایتون

- تعریف امنیت اطلاعات و امنیت سایبری
- معرفی حوزه‌های امنیت: وب، شبکه، رمزنگاری، بدافزار، تست نفوذ
- چرا پایتون؟ ابزارها و توانایی‌ها
- نصب پایتون، pip، و ابزارهای لازم در ویندوز
- معرفی کتابخانه‌های امنیتی: scapy, cryptography, requests, nmap, shodan, paramiko

🔻تمرین: نصب و تست ابزارهای اولیه در ویندوز (ترجیحا با دسترسی Administrator)

فصل ۲: امنیت شبکه در ویندوز با پایتون

- مروری برTCP/IP ، پورت‌ها، ساکت‌ها
- برنامه‌نویسی سوکت در ویندوز (client-server ساده)
- sniffکردن بسته‌ها در ویندوز با Scapy (نیازمند WinPcap یا npcap)
- تحلیل بسته‌های TCP وHTTP

🔻پروژه Sniffer :ساده برای ذخیره‌ی بسته‌های شبکه در ویندوز

فصل ۳: تست نفوذ ساده در ویندوز با پایتون

- معرفی تست نفوذ (Penetration Testing)
- استفاده از کتابخانه python-nmap برای اسکن شبکه در ویندوز
- اسکن پورت‌های باز، سیستم عامل، سرویس‌ها
- بررسی سیستم هدف در شبکه داخلی (مثلا دستگاه دیگر یا localhost)

🔷پروژه: طراحی اسکنر امنیتی ساده با خروجی فایل در ویندوز

فصل ۴: حملات وب (Web Security)

- بررسی آسیب‌پذیری‌های رایج وب SQL Injection, XSS :
- ارسال درخواست‌های مخرب با requests و http.client
- تست فرم‌های لاگین برای Brute Force
- بررسی Header های پاسخ و آسیب‌پذیری‌های شناسایی‌شده

🔷پروژه: ابزار ارسال درخواست‌های POST/GET به آدرس‌های دلخواه جهت تست

فصل ۵: رمزنگاری در ویندوز با پایتون

- اصول رمزنگاری متقارن و نامتقارن
- رمزنگاری پیام و فایل با cryptography (Fernet, AES)
- هش کردن رمز عبور (SHA۲۵۶, bcrypt)
- ساخت ابزار هش‌ساز برای بررسی integrity فایل‌ها

🔷پروژه: ابزار رمزگذاری/رمزگشایی فایل در محیط ویندوز

فصل ۶: تحلیل امنیت و لاگ‌خوانی در ویندوز

- خواندن فایل‌های log (مثلا لاگ سرور یا سیستم)

- تشخیص فعالیت‌های مشکوک با regex و تحلیل محتوا
- ذخیره گزارش‌ها در فایل CSV یا Excel با pandas یا csv
- تولید گزارش PDF ساده با reportlab

🔻پروژه: ابزار گزارش‌ساز از لاگ‌های متنی با فرمتCSV

فصل ۷: آشنایی با حملات رایج (به صورت شبیه‌سازی آموزشی)

- حمله brute force روی فرم تستی
- ساخت کی‌لاگر ساده آموزشی (تنها برای شبیه‌سازی؛ با هشدار اخلاقی)
- شبیه‌سازی phishing page در localhost با فرم جعلی

●هشدار: تمامی موارد این فصل صرفا جهت شناخت و آگاهی هستند.

فصل ۸: ساخت ابزار امنیتی واقعی با رابط CLI

- طراحی رابط خط فرمان با argparse
- افزودن گزینه‌های مختلف برای عملکردهای مختلف ابزار
- ساخت فایل exe از اسکریپت پایتون با pyinstaller برای ویندوز
- نحوه اجرا و به‌اشتراک‌گذاری ابزار نهایی روی سیستم‌های ویندوزی دیگر

🔻پروژه نهایی: ساخت یک ابزار امنیتی قابل‌اجرا (exe.) با رابط خط فرمان

پروژه پایانی (انتخابی)

دانشجویان می‌توانند یکی از موارد زیر را به عنوان پروژه پایان دوره انتخاب کنند:

- ابزار رمزنگاری فایل‌ها با رابط کاربری خط فرمان
- اسکنر پورت و سرویس با امکان خروجی گرفتن
- ابزار لاگ‌خوان و تولید گزارش امنیتی

نکات خاص آموزش در ویندوز:

- معرفی ابزارهای نصب WinPcap/npcap
- استفاده از PowerShell برای اجرای دستورات امنیتی
- بررسی فایروال و آنتی‌ویروس در اجرای ابزارها
- تنظیم VirtualBox/VMWare برای تست در محیط ایزوله در صورت نیاز