

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 (۱۰ Windows) یا بالاتر

فصل ۱: مقدمه ای 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
 - مروری بر هک اخلاقی و حدود قانونی
- ❖ تمرین: نصب و تست ابزارهای اولیه در ویندوز (ترجیحا با دسترسی Administrator)
-

فصل ۲: امنیت شبکه در ویندوز با پایتون

۱-۲ : مفاهیم تئوریک شبکه

- مقدمه‌ای بر شبکه و اینترنت (LAN ، WAN، شبکه محلی و اینترنت)
- مدل‌های شبکه : OSI (۷ لایه) و TCP/IP (۴ لایه) و توضیح ساده هر لایه
- : IP Address and Subnet

- **IPv4 and IPv6:** Understanding the differences and formats of IP addresses.
- **Private and Public IP:** Identifying internal (private) versus external (public) addresses.
- **Gateway:** The device that forwards traffic from a local network to other networks.
- **DNS (Domain Name System):** Translating domain names into IP addresses.

- پورت‌ها و پروتکل‌ها : TCP ، UDP ، کاربرد پورت‌ها (۸۰ HTTP, ۴۴۳ HTTPS, ۲۲ SSH)
- ICMP و Ping : بررسی آنلاین بودن میزبان، کاربرد ICMP در شبکه و امنیت
- Firewall و فیلترینگ بسته‌ها : محدودیت‌ها، دلیل پاسخ ندادن بعضی پینگ‌ها
- ساختار بسته‌ها (Packet Structure) : Header و Payload ، بررسی TCP/UDP و HTTP packet

۲-۲ : برنامه‌نویسی عملی با پایتون در ویندوز

• Socket Programming ساده (Client-Server)

- ساخت TCP Server ساده در ویندوز
- ساخت TCP Client برای ارسال و دریافت پیام

• Sniff کردن بسته‌ها با Scapy

- نصب WinPcap/Npcap
- گرفتن و نمایش بسته‌ها در شبکه محلی

• تحلیل بسته‌ها

- خواندن header های IP و TCP
- بررسی پروتکل‌ها و پورت‌ها
- مثال با بسته HTTP ساده

۳-۲ : پروژه عملی فصل

♦ پروژه : ساخت یک Sniffer ساده برای ذخیره بسته‌های TCP

- دریافت بسته‌ها با Scapy
 - نمایش اطلاعات بسته‌ها : IP Source/Dest ، Port ، Protocol
 - ذخیره اطلاعات در فایل CSV
-

فصل ۳: امنیت شبکه در ویندوز با پایتون

- مروری بر TCP/IP ، پورت‌ها، سوکت‌ها
 - برنامه‌نویسی سوکت در ویندوز (client-server ساده)
 - sniff کردن بسته‌ها در ویندوز با Scapy (نیازمند WinPcap یا npcap)
 - تحلیل بسته‌های TCP و HTTP
- ❖ پروژه Sniffer: ساده برای ذخیره‌ی بسته‌های شبکه در ویندوز
-

فصل ۴: 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 ۵: حملات وب (Web Security)

- بررسی آسیب‌پذیری‌های رایج وب XSS, SQL Injection :

- 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 ۶: 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 ۷: 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 فرمت CSV
-

فصل ۸: 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 صرفاً جهت شناخت و آگاهی هستند.
-

فصل ۹: 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 فایل‌وال و آنتی‌ویروس در اجرای ابزارها
- تنظیم VirtualBox/VMWare برای تست در محیط ایزوله در صورت نیاز