Cybersecurity with Python – Defensive Tools

فصل ۱: دفاع در عمق(Defense in Depth)

- اصول طراحی سیستم‌های ایمن
- مدلZero Trust
- آشنایی باIDS/IPS

فصل ۲: مانیتورینگ و لاگینگ

- پردازش لاگ‌های سیستم و وب‌سرور باPython
- شناسایی الگوهای حمله در لاگ‌ها(Brute Force, SQLi)
- ساخت داشبورد ساده گزارش امنیتی

فصل ۳: تشخیص نفوذ(Intrusion Detection)

- تحلیل ترافیک شبکه باScapy
- شناسایی حملات DoS ساده
- پیاده‌سازی سیستم IDS سبک باPython

فصل ۴: رمزنگاری و امنیت داده‌ها

- استفاده از کتابخانهcryptography
- رمزنگاری متقارن و نامتقارن
- امضای دیجیتال و تأیید صحت پیام

فصل ۵: خودکارسازی دفاع

- **نوشتن اسکریپت بلاک‌کردنIP های مشکوک**
- **ایجاد آلارم در زمان تشخیص فعالیت غیرعادی**
- **ادغام ابزارهای دفاعی با SIEM ساده**