مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره تست نفوذ شبکه

Network Penetration Testing

مروری بر دوره

عملیات تهاجمی یکی از شاخه‌های امنیت سایبری می‌باشد. عملیات تهاجمی به چندین زیرمجموعه از جمله تست نفوذ و عملیات تیم قرمز، توسعه بدافزار و ... تقسیم می‌شود. تست نفوذ شبکه نیز یکی از زیرمجموعه‌های شاخه تست نفوذ می‌باشد که هدف اصلی آن تست امنیتی و کشف آسیب‌پذیری‌ها در لایه‌های مختلف شبکه است. در این دوره شما با تست نفوذ انواع سیستم عامل‌های ویندوز سرور و لینوکس، سرویس‌هایی مانند اکتیو دایرکتوری (DNS، Active Directory)، و ...، پروتکل‌هایی مانند DHCP، ARP، و ... آشنا می‌شوید.

سرفصل ها

۱. Introduction to Penetration Testing
    ۱. Penetration Testing Lifecycle
    ۲. Penetration Testing vs. Vulnerability Assessment
    ۳. Penetration Testing Standards
        ۱. OSSTMM
        ۲. PTES
۲. Implementing Infrastructure Penetration Testing
    ۱. MAC Spoofing
    ۲. CAM Overflow
    ۳. IP Spoofing
    ۴. ARP Poisoning

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۵. DHCP Spoofing
۶. DHCP Starvation
۷. DNS Spoofing
۸. VLAN Hopping
    ۱. Switch Spoofing
    ۲. Double Tagging
۹. Python Scapy Module
۱۰. Hardening Cisco Devices
    ۱. Port Security
    ۲. IP Source Guard
    ۳. Dynamic ARP Inspection (DAI)
    ۴. DHCP Snooping
۳. Internal Scanning
    ۱. Host Discovery
    ۲. Port Scanning
    ۳. Service and Version Scanning
    ۴. OS Scanning
    ۵. Vulnerability Scanning
۴. Gaining Initial Access
    ۱. Exploiting Remote Code Execution (RCE) Vulnerabilities
    ۲. Exploiting Misconfiguration Vulnerabilities
    ۳. Password Attacks
        ۱. Password Brute Force
        ۲. Password Spraying
    ۴. Social Engineering
        ۱. Phishing

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۵. Persistence
   ۱. Registry Run Keys and Startup Folder
   ۲. Windows Service
   ۳. Scheduled Task
   ۴. BITS Jobs
۶. Privilege Escalation
   ۱. Bypass User Account Control (UAC)
   ۲. Exploitation for Privilege Escalation
۷. Discovery
   ۱. System Information Discovery
   ۲. System Network Configuration Discovery
   ۳. System Network Connections Discovery
   ۴. Local Accounts
   ۵. Local Groups
   ۶. Browser Information Discovery
   ۷. File and Directory Discovery
   ۸. Network Sniffing
   ۹. Query Registry
۸. Lateral Movement
   ۱. Exploitation of Remote Services
   ۲. Windows Remote Management
   ۳. Pass the Hash
۹. Active Directory Penetration Testing Scenario
   ۱. Domain Enumeration
   ۲. Privilege Escalation
      ۱. Local Privilege Escalation

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۲. Domain Privilege Escalation
۳. Lateral Movement
۴. Defense Evasion
۵. Domain Credential Dumping
۶. Domain Persistence

پیش نیاز ها

۱. CompTIA Network Plus
۲. Cisco CCNA 200-301