دوره‌های آموزشی
زمستان ۱۳۹۶

دانشگاه فردوسی مشهد
آزمایشگاه تخصصی آپا

معرفی دوره آموزشی تخصصی

آزمون نفوذپذیری شبکه‌های رایانه‌ای

کد دوره : APA 134

۳۲ ساعت

http://cert.um.ac.ir
cert@um.ac.ir
@fum_apa

مخاطبان دوره: هدف آزمایشگاه تخصصی امنیتی آپا دانشگاه فردوسی مشهد از برگزاری این دوره آموزشی که ویژه کارشناسان و مدیران شبکه‌های رایانه‌ای تعریف شده است، انتقال تجربه و پرورش نیروی متخصص به عنوان تحلیل‌گر امنیتی است که با بهره‌گیری از متدها و تکنیک‌های ارزیابی امنیتی و آزمون نفوذپذیری یک شبکه جهت تشخیص موثر و کاهش ریسک، توانایی برقراری امنیت در زیرساخت شبکه‌ها را فراهم سازد. این دوره آموزشی بر روی تکنیک‌ها و فناوری‌های نفوذ از دیدگاه حمله‌کننده تکیه دارد و به دنبال روش‌های ممکن و موثر برای ایجاد امنیت در شبکه‌ها می‌باشد. این دوره به صورت تئوری و عملی برگزار می‌گردد.

پیش‌نیازهای دوره: آشنایی با مدیریت شبکه‌های رایانه‌ای متوسط و بزرگ – آشنایی با محیط فرمان سیستم‌عامل لینوکس

*: به‌همراه آوردن لپ‌تاپ در این دوره موجب کارآیی بیشتر و یادگیری بهتر شرکت‌کنندگان خواهد شد.

روش ثبت‌نام: به‌صورت الکترونیکی و از طریق وب‌گاه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد به نشانی http://cert.um.ac.ir انجام می‌گیرد.

سرفصل دوره:

1. Penetration Testing
   - Penetration Testing Methodologies
     - Open Source
     - Proprietary
   - Penetration Testing Road Map And Procedure
   - OS Penetration Testing
   - Preparing Laboratory Penetration Testing
2. TCP/ IP Packet Analysis
3. Advanced Sniffing Techniques
   - Passive Sniffing
   - Active Sniffing
   - Tools
4. Information Gathering / Enumeration
   - Footprint
   - Network Scanning
     - TCP Communication Flag
       - SYN/ACK/PSH/RST/FIN/URG

    - Scanning Technique
        - TCP Connect / Full open scan
        - Stealth scan(Half-open scan)
        - Xmas scan
        - FIN Scan
        - Null scan
        - UDP Scanning
    - Port scanning
- OS Fingerprinting, Banner Grabbing
    - BOGUS probe, TCP ISN sampling, TCP initial window size, RTO delay, ...
- Service Identification
- Evading IDS, Firewall and Honeypots
- Port Knocking technique

5. Penetration Testing of Switches / Layer 2 Attack
    - Basic Layer 2 Security Feature
    - CAM Overflow Attack / MAC Flooding
    - VLAN Security
        - VLAN Hopping
        - VTP Attack
    - STP Attack
    - ARP Attack & Security
        - ARP Poisoning / Spoofing
    - MITM Attacks
    - Spoofing Attacks
    - Access Port Security
        - Port base Authentication 802.1x
        - Port Security
    - CDP Attack
    - Port-Level Traffic Controls
    - Layer 2 Attack Tools
6. Cryptography
    - History of Cryptography
    - Hashing
    - Coding
    - Encryption
        - Symmetric Key
        - Asymmetric Key
    - PKI
    - Digital signature
7. Denial of Service (DOS) / Distributed Denial of Service (DDoS) Attack

- Attack Type and Executing
  - UDP Flood, ICMP Flood, SYN Flood, Teardrop, Ping of Death, Reflected…

8. Password Cracking / Penetration Testing
   - Brute Force Attack
   - Dictionary Attack
   - Windows Password
     - LM hash
     - NTLM v1,2
     - Kerberos
   - Unix Password Attack
     - Salting
   - Replay Attack
   - Cracking tools
9. Service Penetration Testing
   - DHCP
     - DHCP starvation
     - DHCP Spoofing
   - DNS
     - DNS Spoofing
     - DNS Cache Poisoning
     - Zone Transfer
     - DNS Sec
   - Active Directory / LDAP
   - NTP
   - SNMP
   - Telnet /SSH
   - FTP
   - Remote Desktop Services
   - Important Other Services ...
10. Exploitation And Tools
    - Metasploit, Armitage, Fast Track
    - Client-Side Exploitation
    - Post- Exploitation
    - Local privilege escalation
11. Log Analysis & Management Penetration Testing
12. VoIP Penetration Testing
    - Assess VoIP vulnerabilities
    - Perform VoIP penetration testing