IT Professional Training Center

ارزیابی امنیتی شبکه های بی سیم

مدت دوره: ۶ ساعت

سرفصل دوره:

۱- مقدمه

۲- نیازمندی های ایجاد یک آزمایشگاه تست نفوذ شبکه های بی سیم

۳- آشنایی با استاندارد 802.11 و اصلاحیه های این استاندارد

۴- آشنایی با سازمان های مرتبط با استاندارد شبکه های بی سیم

۵- آشنایی با فرکانس های رادیویی بی سیم

۶- آشنایی با انواع مد های شبکه های بی سیم(infrastructure and Ad-hoc)

۷- آشنایی با اصطلاحات رایج در شبکه های بی سیم

۸- آشنایی با دستورات لازم در Kali Linux جهت تست نفوذ شبکه های بی سیم

۹- آشنایی با ابزارهای تست نفوذ شبکه های بی سیم در kali Linux

۱۰- آشنایی با انواع تهدیدهای شبکه های بی سیم

- حملات از نوع DOS
- شنود اطلاعات شبکه های بی سیم
- Password Cracking

۱۱- آشنایی با تجهیزات کنترلی بی سیم شبکه های بزرگ

۱۲- آشنایی با انواع روش های رمزنگاری شبکه های بی سیم

- WEP
- WPA
- WPA2
- WPS
- EAP
- 802.1x

۱۳- آشنایی با روش های محدودسازی دسترسی در شبکه های بی سیم

- مخفی سازی SSID
- اعمال MAC فیلترینگ
- تنظیم و کاهش پهنای باند شبکه های بی سیم

۱۴- آشنایی با ابزارهای Aircrack suite

- Aircrack-Ng
- Aireplay-Ng
- Airmon-ng
- Airodump-ng
- Airebase-ng

۱۵- آشنایی با ابزارهای password cracking در kali linux

- Wifite
- fern-wifi-cracker
- Reaver
- Pixiewps
- cowpatty

۱۶- آشنایی با ابزارهای مانیتورینگ و آنالیز ترافیک شبکه های بی سیم

- Kismet
- Wireshark
- Acrylic_WiFi
- Dumper
- Wirelessmon
- Vistumbler
- inSSIDer

۱۷- آشنایی با Rogue Access point

۱۸- آشنایی با حملات phishing در شبکه های بی سیم با استفاده از ابزار wifiphisher

۱۹- آشنایی با ابزارFuzzing شبکه های بی سیم