Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

# دوره تخصصی امنیت؛ تشخیص نفوذ در عمق SANS (SEC 503)

## Intrusion Detection InDepth
## GCIA

| مدت(ساعت): 40 | پیش نیاز: SANS SEC 504 | اعتبار دهنده: SANS |
|---|---|---|

### معرفی دوره :

در این دوره مهارت‌های لازم جهت شناسایی حملات و محافظت از شبکه سازمان ارائه خواهد شد. در این دوره دانشجویان با مفاهیم و تئوری TCP/IP و پروتکل‌های پرکاربرد لایه Applicatin مانند HTTP آشنا خواهند شد لذا قادر خواهند بود به صورت هوشمندانه ترافیک شبکه را تحلیل کرده و نشانه‌های نفوذ و حمله را شناسایی نمایند. در این دوره کار با ابزارهای متن باز مانند tcpdump، Wireshark، Snort و Bro جهت یادگیری کاربردی مفاهیم ارائه شده، آموزش داده خواهد شد.

### اهداف دوره :

- آشنایی با مفاهیم و اصول آنالیز ترافیک
- معرفی پروتکل‌های لایه Application و شیوه تحلیل ترافیک آن‌ها
- کار با سامانه‌های تشخیص نفوذ متن باز مانند Bro و Snort
- آشنایی با پروتکل‌های پرکاربرد شبکه و شیوه فارنزیک آن‌ها
- تنظیم و بهینه‌سازی تنظیمات IDS
- معرفی چالش‌های استفاده از IDS و ارائه راهکارهای متناسب

### مخاطبان دوره :

- کارشناسان تیم امداد رایانه‌ای
- کارشناسان مرکز عملیات امنیت
- کارشناسان جرائم رایانه‌ای
- مدیران شبکه
- مدیران امنیت سازمان

### امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات ( نما )
  - سازمان مدیریت و برنامه ریزی کشور ( معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- برگزاری لابراتوارهای دوره مبتنی بر Workshop رسمی دوره
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

### محتوای دوره :

- Packet Crafting and nmap OS Identification
- IDS/IPS Evasion Theory
- Real-World Traffic Analysis

**Open-Source IDS: Snort and Bro**

- Operational Lifecycle of Open-Source IDS
- Introduction
- Snort
- Bro
- Comparing Snort and Bro to Analyze Same Traffic

**Network Traffic Forensics and Monitoring**

- Analyst Toolkit
- SiLK
- Network Forensics
- Network Architecture for Monitoring
- Correlation of Indicators

**IDS Hands-on Challenge**

### Course Outline :

**Fundamentals of Traffic Analysis**

- Concepts of TCP/IP
- Introduction to Wireshark
- Network Access/Link Layer: Layer 2
- IP Layer: Layer 3
- Wireshark Display Filters
- Writing tcpdump Filters
- TCP
- UDP
- ICMP

**Application Protocols and Traffic Analysis**

- Advanced Wireshark
- Detection Methods for Application Protocols
- Microsoft Protocols
- HTTP
- SMTP
- DNS





EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک 242 تلفن مستقیم آموزش: 8 ،88062203 فاکس :88065222