Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

Designed by
دوره طراحی شده
ویژه کاریار ارقام
Carrier Digit

دوره تکمیلی مرکز عملیات امنیت SANS (FOR 572)

Advanced Network Forensics and Analysis

مدت(ساعت): ۴۰ | **پیش نیاز:** SANS SEC 503 | **اعتبار دهنده:** SANS

معرفی دوره :

در این دوره تمام مهارت‌های لازم جهت بررسی و پیگیری موثر و بهینه حوادث امنیتی بعد از وقوع آن‌ها در سازمان، ارائه خواهد شد.

تمرکز این دوره روی دانش و روش‌های تحلیل مورد نیاز جهت تحلیل دقیق شبکه و بررسی جزئیات حوادث امنیتی است به گونه‌ای که علاوه بر شناسایی عوامل حادثه، بتوان از وقوع آن‌ها در آینده نیز پیشگیری کرد.

دانشجویان در این دوره با مهارت‌های لازم جهت شناسایی مراحل وقوع یک حادثه شامل شناخت، نفوذ، عملیات، دستور و کنترل و استخراج داده آشنا خواهند شد.

اهداف دوره :

- آشنایی با روش‌ها و متدولوژی‌های فارنزیک شبکه
- آشنایی با تحلیل Netflow و شیوه‌های مصورسازی داده
- آشنایی با روش‌های ثبت و ذخیره‌سازی بسته‌های شبکه‌ای
- آشنایی با پروتکل‌های پرکاربرد شبکه و شیوه فارنزیک آن‌ها
- معرفی پروتکل‌های تولید و مدیریت Log
- معرفی روش‌های مهندسی معکوس پروتکل‌ها
- معرفی الگوریتم‌های رمزنگاری

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

مخاطبان دوره :

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

Accredited by CARRIER DIGIT Computer Software LLC

EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس: ۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره :

SEC 572

Off the Disk and onto the Wire
- Goals of Forensic Investigation
- Network Forensics Investigative Methodology
- Foundational Network Forensics Tools: tcpdump and Wireshark
- Network Evidence Sources and Types
- Web Proxy Server Examination
- Network Architectural Challenges and Opportunities
- Packet Capture Applications and Data

NetFlow Analysis, Commerical Tools, and Visualization
- NetFlow Analysis and Collection
- Open-Source Flow Tools
- Commercial Network Forensics
- Visualization Techniques and Tools
- Dynamic Host Conϐiguration Protocol (DHCP) and Domain Name Service (DNS)

Network Protocols and Wireless Investigations
- Hypertext Transfer Protocol (HTTP)
- Network Time Protocol (NTP)
- File Transfer Protocol (FTP)
- Wireless Network Forensics
- Simple Mail Transfer Protocol (SMTP)
- Microsoft Protocols

Logging
- Syslog
- Microsoft Eventing
- HTTP Server Logs
- Firewall and Intrusion Detection Systems
- Log Data Collection, Aggregation, and Analysis

Encryption and Protocol Reversing
- Introduction to Encryption
- Man-in-the-Middle
- Traffic Flow Analysis
- Network Protocol Reverse Engineering

Network Forensics Challenge
- Network Forensic Case
- Analysis using only network-based evid
- Reporting

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس :۸۸۰۶۵۲۲۲