NooraNet®
CyberSecurity Leadership

موسسه نورانت

نام دوره : FOR500	مدت دوره : ۳۰ ساعت	اعتبار دهنده:SANS

❖ توضیح دوره :

دوره FOR500یا همـان دوره Windows Forensic به افراد فارنزیک بر روی سیسـتم عامل ویندوز را آموزش می دهد. در دوره FOR500که توسط شـرکت SANS ارائه داده می شود افراد با جمع آوری شـواهد و مدارک از بخشـهای مختلف سیسـتم عامل ویندوز آشنا می شوند. تجزیه و تحلیل ریجستری ویندوز، Jump، Shell bag List USIBاز مطالب اصـلی این دوره می باشد. در این دوره، افراد با فارنزیک مرورگرهای مختلف به صـورت کامل آشـنا می شـوند. نام مدرک بین المللی این دوره GCFAمی باشد.

❖ پیش نیاز دوره

- آشنایی با تهدیدات مختلف پیرامون سیستم عامل ها
- کاربری حرفه ای سیستم عامل
- دوره CEH
- دوره CHFI

❖ مجوزها و اعتبارات

دارای مجوز رسمی از :

- شورای عالی انفورماتیک
- اداره کل نظام مدیریت امنیت اطلاعات
- سازمان نظام صنفی رایانه ای
- گواهی ISO9001

❖ امتیازات دوره :

- اساتید با تجربه (بالای ۱۲ سال سابقه)
- لابراتوارهای مجهز
- اعطای مدارک فارسی و انگلیسی با قابلت ترجمه و تایید قوه قضاییه
- مشاوره رایگان قبل و بعد از دوره
- دسترسی به پرتال اختصاصی noorasec

❖ مخاطبین دوره

- مدیران فناوری اطلاعات
- مدیران امنیت اطلاعات
- کارشناسان امنیت
- کارشناسان واحد پاسخگویی به حوادث
- کارشناسان واحد مرکز عملیات امنیت

آدرس: تهران-خیابان مطهری-خیابان کوه نور- کوچه دوم پلاک ۹ -طبقه اول
تلفن : ۸۸۱۷۵۵۶۰ - فکس : ۸۸۱۷۵۵۳۴

www.noorasec.com
Info@noorasec.com

NooraNet®
CyberSecurity Leadership

موسسه نورانت

سرفصل دوره FOR500

FOR500.1: Windows Digital Forensics And Advanced Data Triage

Windows Operating System Components
Core Forensic Principles
Live Response and Triage-Based Acquisition Techniques
Acquisition Review with Write Blo
Windows Image Mounting and Examination
NTFS File System Overview
Document and Fcker
Advanced Acquisition Challengesile Metadata
File Carving
Memory, Pagefile, and Unallocated Space Analysis

FOR500.2: Core Windows Forensics Part I: Windows Registry Forensics, Analysis

Registry Core
Profile Users and Groups
Core System Information
User Forensic Data
Tools Used

FOR500.3: Core Windows Forensics Part II: Usb Devices And Shell Items

Shell Item Forensics
USB and Bring Your Own Device (BYOD) Forensic Examinations

FOR500.4: Core Windows Forensics Part III: E-Mail, Key Additional Artifacts, And Event Logs

E-mail Forensics
Microsoft Outlook
Web-Based Mail
Microsoft Exchange and Office 365
Lotus Notes
Connected Networks, Duration, and Bandwidth Usage
Applications Run and Bytes Sent/Received Per Application
Appllication Push Notifications
Energy Usage
Track Account Usage including RDP, Brute Force Password Attacks
Audit and Analyze File and Folder Access
Prove System Time Manipulation
Track Bring Your Own Device (BYOD) and External Devices
Geo-locate a Device via Event Logs

FOR500.5: Core Windows Forensics Part IV: Web Browser Chrome Forensics — Firefox, Internet Explorer,

Browser Forensics
Firefox
Chrome
Examination of Browser Artifacts
Tools Used

FOR500.6: Windows Forensic Challenge

Digital Forensic Case
Presentation

www.noorasec.com
Info@noorasec.com

آدرس: تهران-خیابان مطهری-خیابان کوه نور- کوچه دوم پلاک ۹ -طبقه اول
تلفن : ۸۸۱۷۵۵۶۰ - فکس : ۸۸۱۷۵۵۳۴