NooraNet®
CyberSecurity Leadership

موسسه نورانت

نام دوره : FOR526	مدت دوره : ۳۰ ساعت	اعتبار دهنده:SANS

❖ توضیح دوره :

دوره FOR526یا همان دوره Memory Forensicبه افراد فارنزیک بر روی حافظه موقت (Ram)را آموزش می دهد. در دوره FOR526که توسط شرکت SANSارائه داده می شود افراد با جمع آوری شواهد و مدارک از RAMمی توانند به اطلاعاتی دسترسی پیدا کنند که در هیچ کجای سیستم یافت نمیشود.

دسترسی به اطلاعات از قبیل پردازش های مخفی ، نام کاربری ، گذرواژه ، کلیدهای خصوصی ، دستوراتی که کاربر تایپ کرده و بسیاری از موارد از مطالبی می باشد که در این دوره آموزش داده می شود.

❖ پیش نیاز دوره

- آشنایی با ساختار و عملکرد حافظه های موقت
- آشنایی با مباحث عمومی فارنزیک
- دوره CHFI
- دوره FOR500 (ترجیحا)

❖ 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

- کارشناسان تجزیه و تحلیل بدافزار
- کارشناسان فارنزیک بدافزار
- کارشناسان مرکز عملیات امنیت (SOC)
- کارشناسان واحد پاسخگویی به حوادث (IR)

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 FOR526

FOR526.1: Foundations in Memory Analysis and Acquisition
Why Memory Forensics?
Investigative Methodologies
The Ubuntu SIFT and Windows 10 Workstations
The Volatility Framework
System Architectures
Triage vs. Full Memory Acquisition
Physical Memory Acquisition

FOR526.2: Unstructured Analysis and Process Exploration
Unstructured Memory Analysis
Page File Analysis
Exploring Process Structures
List Walking and Scanning
Exploring Process Relationships
Exploring Dynamic Link Libraries
Pool Memory
Kernel Objects

FOR526.3: Investigating the User via Memory Artifacts
Network Connections
Virtual Address Descriptors
Detecting Injected Code
Analyzing the Registry via Memory Analysis
User Artifacts in Memory

FOR526.4: Internal Memory Structures
Interrupt Descriptor Tables
Drivers
Direct Kernel Object Manipulation
Module Extraction
Hibernation Files
Crash Dump Files

FOR526.5: Memory Analysis on Platforms Other than Windows
Linux Memory Acquisition and Analysis
Mac Memory Acquisition and Analysis

FOR526.6: Memory Analysis Challenges
Malware and Rootkit Behavior Detection
Persistence Mechanism Identification
Code Injection Analysis
User Activity Reconstruction
Linux Memory Image Parsing
Mac OSX Memory Image Parsing
Windows Hibernation File Conversion and Analysis
Windows Crash Dump Analysis

www.noorasec.com
Info@noorasec.com

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