سرفصل دوره آموزشSANS Forensics Pack Level 2

**FOR610.1: Malware Analysis Fundamentals**

Assembling a toolkit for effective malware analysis

Examining static properties of suspicious programs

Performing behavioral analysis of malicious Windows executables; Performing dynamic code analysis of malicious Windows executables

Exploring network interactions of malware in a lab for additional characteristics

**FOR610.2: Reversing Malicious Code**

Understanding core x86 assembly concepts for malicious code analysis

Identifying key assembly constructs with a disassembler

Following program control flow to understand decision points

Recognizing common malware characteristics at the Windows API level

Extending assembly knowledge to include x64 code analysis

**FOR610.3: Analyzing Malicious Documents**

Malicious PDF file analysis, including the analysis of suspicious websites; VBA macros in Microsoft Office documents

Examining malicious RTF files, including the analysis of shellcode

Making sense of XLM macros

**FOR610.4: In-Depth Malware Analysis**

Deobfuscating malicious JavaScript

Recognizing packed Windows malware

Getting started with unpacking

Using debuggers for dumping packed malware from memory; Analyzing multi-technology and "fileless" malware

Code injection and API hooking

**FOR610.5: Examining Self-Defending Malware**

How malware detects debuggers and protects embedded data

Unpacking malicious software that employs process hollowing

Bypassing the attempts by malware to detect and evade analysis tools

Handling code misdirection techniques, including SEH and TLS callbacks

Unpacking malicious executables by anticipating the packer's actions