BACKDOOR

SOC Analyst Level: 2

Course Schedule

Step	Topic	Length(Hours)	Format
Step 1	Meet your mentor	1	Community Chat
Step 2	Soc Analyst 2 Assessment	0.5	Assessment
Step 3	ComTIA CySA+	12	Course
Step 4	ComTIA CySA+	22	Lab
Step 5	ComTIA CySA+	3	Practice Test
Step 6	NMAP	6.5	Course
Step 7	Perform a Network Vulnerability Assessment Using Nmap	1	Lab
Step 8	Identify Non-secure Network Traffic	1	Lab
Step 9	Parse Files out of Network Traffic	1	Lab
Step 10	Participate in Attack Analysis Using Trusted Tool Set	1	Lab
Step 11	Network Miner	1	Lab
Step 12	Advanced Cyber Threat Intelligence	2	Course
Step 13	Incident Response Steps	0.5	Course
Step 14	Incident Response Planning	1	Course
Step 15	Implementing an Incident Response Plan	1	Course
Step 16	Incident Response Recovery	1	Course
Step 17	Post-Incident Service Restoration	1	Lab
Step 18	Performing Incident Response in a Windows Environment	1	Lab
Step 19	Incident Response and Advanced Forensics	7.5	Course
Step 20	Computer and Hacking Forensics	7	Course
Step 21	Monitoring Network Traffic	1	Lab

Step 22	Monitoring Network Traffic for potential IOA/IOC	1	Lab
Step 23	Windows Event Log Manipulation via Windows Event Viewer	1	Lab
Step 24	Introduction to Splunk	2	Course
Step 25	Centralized Monitoring (Splunk)	1	Lab
Step 26	Creating SIEM Reports with Splunk	1	Lab
Step 27	Splunk	1	Assessment
Step 28	Identify and Remove Trojan Using Various Tools	1	Lab
Step 29	Identify Rootkit and DLL Injection Activity	1	Lab
Step 30	Identify Whether High-Risk Systems were Affected	1	Lab
Step 31	Identifying Intrusion and Mitigating Attacks with RHEL Server	1	Lab
Step 32	Identify Attack Types	1	Lab
Step 33	Identify Malicious Network Connections	1	Lab
Step 34	Resume and Job Prep Session	3.5	Course
Step 35	Review	1	One to One