SANS Forensics Packسرفصل دوره آموزش

SANS SEC504:

- 1: Incident Response and Computer Crime Investigations
    - Incident Response
    - Common incident response mistakes
    - Incident goals and milestones
    - Post-incident activities
    - Digital Investigations
    - Asking and answering the right questions
    - Pivoting during an investigation
    - Taking notes and writing reports
    - Artifact and event-based timelines
    - Live Examination
    - How to start, even with minimal information
    - Examining a live environment
    - Identifying abnormal activity
    - Digital Evidence
    - Understanding what digital evidence is and how to collect it
    - The role and elements of a chain of custody
    - How to collect digital evidence
    - Network Investigations
    - Analyzing packet captures using tcpdump
    - Web proxy logs
    - Memory Investigations
    - How to investigate memory images using the Volatility framework
    - Malware Investigations
    - Basic approaches for investigating malware
    - Best practices for working with malware
    - Monitoring the environment using snapshot and continuous recording tools

- 2: Recon, Scanning, and Enumeration Attacks
    - Introducing the MITRE ATT&CK Framework
    - Attacker evolution and the network for tool, technique, and practice (TTP) mapping
    - Using the MITRE ATT&CK Framework for smarter adversary assessment
    - How we integrate SEC504 with the MITRE ATT&CK Framework
    - Reconnaissance
    - What does your network reveal?
    - Are you leaking too much information?
    - Using certificate transparency for pre-production server identification
    - Domain Name System harvesting
    - Data gathering from job postings, websites, and government databases
    - Identifying publicly compromised accounts
    - FOCA for metadata analysis

  - Aggregate OSINT data collection with SpiderFoot
  - Mastering SHODAN searches for target discovery
  - Scanning
  - Learn the techniques attackers use to enumerate your networks
  - Locating and attacking personal and enterprise Wi-Fi
  - Identifying and exploiting proprietary wireless systems
  - Port scanning: small and large-scale enumeration tasks
  - Quick and effective intel collection from web servers
  - Characterizing network targets by OS, service, patch level
  - Vulnerability scanning and finding prioritization
  - Enumerating Windows Active Directory Targets
  - Windows Active Directory domain enumeration with BloodHound, SharpView
  - Windows Command and Control with PowerShell Empire
  - Operating system bridging from Linux to Windows targets
  - Defending against SMB attacks with sophisticated Windows networking features
  - Understanding SMB security features through Windows Server 2019
  - Defense Spotlight: DeepBlueCLI
  - Using PowerShell to enumerate Windows systems
  - Fast and effective Windows event log analysis
  - Leveraging PowerShell output modifiers for reporting, analysis
  - Characterizing common Windows scans and attacks against Windows servers

- 3: Password and Access Attacks
  - Password Attacks
  - How attackers bypass account lockout policies
  - Choosing a target protocol for password guessing attacks
  - Techniques for choosing password lists
  - How attackers reuse compromise password lists against your organization
  - Techniques for password cracking
  - Recommendations for password cracking in your organization
  - Defense Spotlight: Log Analysis with Elastic Stack (formerly ELK)
  - Establishing a lightweight log analysis system with Elasticsearch, Logstack, Beats, and Kibana
  - Understanding Linux and UNIX authentication logging data
  - Configuring Filebeat for simple log ingestion
  - Using Kibana to identify password attack events
  - Customizing Kibana visualization for effective threat hunting
  - Understanding Password Hashes
  - Hashing algorithms, processes, and problems
  - Understanding Windows hashing function through Windows Server 2019
  - Password hash function strength and quality metrics
  - Extracting Windows domain password hashes using built-in tools
  - Getting password hashes from Windows 10 systems
  - Decoding UNIX and Linux password hashes
  - Mitigating GPU-based cracking: PBKDF2, bcrypt, and scrypt
  - Password Cracking Attacks

  - John the Ripper: single, wordlist, incremental, and external cracking modes
  - Cracking hashes with Hashcat: straight and combinator attacks
  - Effective hash computation using mask attacks
  - Breaking user password selection weaknesses with Hashcat rules
  - Three simple strategies for defeating password cracking
  - Defense Spotlight: Domain Password Auditing
  - Enumerating Windows domain settings with simple PowerShell one-line scripts
  - Characterizing systemic behavior in user password selection
  - Identifying bad password offenders in your organization
  - Mitigating password sharing in Windows domains
  - Netcat: The Attacker's Best Friend
  - Transferring files, creating backdoors, and shoveling shells
  - Netcat relays to obscure the source of an attack
  - Replay attacks with Netcat

- 4: Public-Facing and Drive-By Attacks
  - Metasploit Attack and Analysis
  - Software Update Browser Exploitation
  - System Resource Utilization Database Analysis
  - Command Injection Attack
  - Cross Site Scripting Attack
  - SQL Injection Attack
  - SQL Injection Log Analysis
  - Topics
  - Using Metasploit for System Compromise
  - Using the Metasploit framework for specific attack goals
  - Matching exploits with reconnaissance data
  - Deploying Metasploit Meterpreter Command & Control
  - Identifying Metasploit exploit artifacts on the system and network
  - Drive-By and Watering Hole Attacks
  - Examining the browser attack surface
  - Identifying browser vulnerabilities with JavaScript
  - Code-executing Microsoft Office attacks
  - Backdooring legitimate code with attacker payloads
  - Defense Spotlight: System Resource Usage Monitor (SRUM)
  - Assessing attacker activity with Windows 10 app history
  - Extracting useful data from the protected SRUM database
  - Converting raw SRUM data to useful post-exploit analysis
  - Web Application Attacks
  - Account harvesting for user enumeration
  - Command injection attacks for web server remote command injection
  - SQL Injection: Manipulating back-end databases
  - Session Cloning: Grabbing other users' web sessions
  - Cross-Site Scripting: Manipulating victim browser sessions
  - Defense Spotlight: Effective Web Server Log Analysis
  - Using Elastic Stack (ELK) tools for post-attack log analysis

  - Configuring Filebeat for web server log consumption
  - Using the Kibana Query Language (KQL) to identify custom web attacks
  - Hunting for common SQL Injection attack signatures
  - Decoding obfuscated attack signatures with CyberChef

- 5: Evasion and Post-Exploitation Attacks
  - Advanced network pivoting with Metasploit
  - Insider network attack event analysis
  - Hijacking Windows: Responder attacks
  - Post-exploitation command history analysis
  - Hiding (and finding) valuable data on Windows servers
  - Selectively editing Windows event logs
  - Network threat hunting with RITA
  - Topics
  - Endpoint Security Bypass
  - Evading EDR analysis with executable manipulation: ghostwriting
  - Manipulating Windows Defender for attack signature disclosure
  - Using LOLBAS to evade application whitelisting
  - Adapting Metasploit payloads on protected platforms
  - Pivoting and Lateral Movement
  - Pivoting from initial compromise to internal networks
  - Effective port forwarding with Meterpreter payloads
  - Leveraging compromised hosts for internal network scanning, exploitation
  - Windows netsh and attacker internal network access
  - Privileged Insider Network Attacks
  - Leveraging initial access for network attacks
  - Deploying packet sniffers, MITM attack tools
  - Native packet capture on compromised Windows hosts
  - Abusing weak protocols: DNS, HTTP
  - Network service impersonation attacks with Flamingo
  - Abusing Windows name resolution for password disclosure
  - Covering Tracks
  - Maintaining access by manipulating compromised hosts
  - Editing log files on Linux and Windows systems
  - Hiding data in Windows ADS
  - Network persistence through hidden Command & Control
  - Defense Spotlight: Real Intelligence Threat Analytics (RITA)
  - Characterizing advanced Command & Control activity over the network
  - Capturing and processing network data with Zeek
  - Network threat hunting: beacons, long connections, strobes, and DNS analysis
  - Post-Exploitation Data Collection
  - Harvesting passwords from compromised Linux hosts
  - Password dumping with Mimikatz and EDR bypass
  - Defeating Windows and macOS password managers
  - Windows keystroke logging attacks
  - Data exfiltration over blended network protocols

    - Where To Go From Here
    - Techniques for solving the problem of needing time for study
    - Understanding the Forgetting Curve dilemma
    - Techniques for developing long-term retention from what you have learned
    - Building study strategies for certification, applying your knowledge

SANS FOR500:

- 1: Digital Forensics and Advanced Data Triage
    - Windows Operating System Components
    - Key Differences in Modern Windows Operating Systems
    - Core Forensic Principles
    - Analysis Focus
    - Determining Your Scope
    - Creating and Investigative Plan
    - Live Response and Triage-Based Acquisition Techniques
    - RAM Acquisition and Following the Order of Volatility
    - Triage-Based Forensics and Fast Forensic Acquisition
    - Encryption Detection
    - Registry and Locked File Extraction
    - Leveraging the Volume Shadow Service
    - KAPE Triage Collection
    - Windows Image Mounting and Examination
    - NTFS File System Overview
    - Document and File Metadata
    - File and Stream Carving
    - Principles of Data Carving
    - Recovering File System Metadata
    - File and Stream Carving Tools
    - Custom Carving Signatures
    - Memory, Pagefile, and Unallocated Space Analysis
    - Artifact Recovery and Examination
    - Chat Application Analysis
    - Internet Explorer, Edge, Firefox, Chrome, and InPrivate Browser Recovery
    - Email and Webmail, including Yahoo, Outlook.com, and Gmail

- 2: Registry Analysis, Application Execution, and Cloud Storage Forensics
    - Registry Forensics In-Depth
    - Registry Core
    - Hives, Keys, and Values
    - Registry Last Write Time
    - MRU Lists
    - Deleted Registry Key Recovery
    - Identify Dirty Registry Hives and Recover Missing Data

  - Rapidly Search and Timeline Multiple Hives
  - Profile Users and Groups
  - Discover Usernames and Relevant Security Identifiers
  - Last Login
  - Last Failed Login
  - Login Count
  - Password Policy
  - Core System Information
  - Identify the Current Control Set
  - System Name and Version
  - Document the System Timezone
  - Wireless, Wired, VPN, and Broadband Network Auditing
  - Perform Device Geolocation via Network Profiling
  - Identify System Updates and Last Shutdown Time
  - Registry-Based Malware Persistence Mechanisms
  - User Forensic Data
  - Evidence of File Downloads
  - Office and Microsoft 365 File History Analysis
  - Windows 7, Windows 8/8.1, Windows 10 Search History
  - Typed Paths and Directories
  - Recent Documents (RecentDocs)
  - Open Save/Run Dialog Boxes Evidence
  - Application Execution History via UserAssist, Prefetch, Windows 10 Timeline, System Resource Usage Monitor (SRUM), and BAM/DAM
  - Cloud Storage Forensics
  - Microsoft OneDrive
  - OneDrive Files on Demand
  - Microsoft OneDrive for Business
  - OneDrive Unified Audit Logs
  - Google Drive
  - Google Workspace (G Suite) File Stream
  - Google Workspace (G Suite) Logging
  - Dropbox
  - Dropbox Decryption
  - Dropbox Logging
  - Box Drive
  - Box Backup and Sync
  - Synchronization and Timestamps
  - Forensic Acquisition Challenges
  - User Activity Enumeration

- 3: Shell Items and Removable Device Profiling
  - Shell Item Forensics
  - Shortcut Files (.lnk) - Evidence of File Opening
  - Windows 7-10 Jumplists - Evidence of File Opening and Program Execution
  - Shellbag Analysis - Evidence of Folder Access

  - USB and BYOD Forensic Examinations
  - Vendor/Make/Version
  - Unique Serial Number
  - Last Drive Letter
  - MountPoints2 Last Drive Mapping Per User (Including Mapped Shares)
  - Volume Name and Serial Number
  - Username that Used the USB Device
  - Time of First USB Device Connection
  - Time of Last USB Device Connection
  - Time of Last USB Device Removal
  - Auditing BYOD Devices at Scale

- 4: Email Analysis, Windows Timeline, SRUM, and Event Logs
  - Email Forensics
  - Evidence of User Communication
  - How Email Works
  - Email Header Examination
  - Email Authenticity
  - Determining a Sender's Geographic Location
  - Extended MAPI Headers
  - Host-Based Email Forensics
  - Exchange Recoverable Items
  - Exchange Evidence Acquisition and Mail Export
  - Exchange Compliance Search and eDiscovery
  - Unified Audit Logs in Office 365
  - Google Workspace (G Suite) Logging
  - Recovering Data from the Google Workspace (G Suite)
  - Web and Cloud-Based Email
  - Webmail Acquisition
  - Email Searching and Examination
  - Mobile Email Remnants
  - Business Email Compromise
  - Forensicating Additional Windows OS Artifacts
  - Windows Search Index Forensics
  - Extensible Storage Engine (ESE) Database Recovery and Repair
  - db and Thumbcache Files
  - Windows Recycle Bin Analysis (XP, Windows 7-10)
  - Windows 10 Timeline Activities Database
  - System Resource Usage Monitor (SRUM)
  - Connected Networks, Duration, and Bandwidth Usage
  - Applications Run and Bytes Sent/Received Per Application
  - Application Push Notifications
  - Energy Usage
  - Windows Event Log Analysis
  - Event Logs that Matter to a Digital Forensic Investigator
  - EVTX and EVT Log Files

- Track Account Usage, including RDP, Brute Force Password Attacks, and Rogue Local Account Usage
    - Audit and Analyze File and Folder Access
    - Prove System Time Manipulation
    - Track BYOD and External Devices
    - Microsoft Office Alert Logging
    - Geo-locate a Device via Event Logs

- 5: Web Browser Forensics
    - Browser Forensics
    - History
    - Cache
    - Searches
    - Downloads
    - Understanding Browser Timestamps
    - Chrome
    - Chrome File Locations
    - Correlating URLs and Visits Tables for Historical Context
    - History and Page Transition Types
    - Chrome Preferences File
    - Web Data, Shortcuts, and Network Action Predictor Databases
    - Chrome Timestamps
    - Cache Examinations
    - Download History
    - Web Storage, IndexDB, and the HTML5 File System
    - Chrome Session Recovery
    - Chrome Profiles Feature
    - Identifying Cross-Device Chrome Synchronization
    - Edge
    - Chromium Edge vs. Google Chrome
    - History, Cache, Cookies, Download History, and Session Recovery
    - Microsoft Edge Collections
    - Edge Internet Explorer Mode
    - Chrome and Edge Extensions
    - Edge Artifact Synchronization and Tracking Multiple Profiles
    - Edge HTML and the Spartan.edb Database
    - Reading List, WebNotes, Top Sites, and SweptTabs
    - Internet Explorer
    - IE Forensic File Locations
    - History Files: Index.dat and WebCache.dat
    - Cache Recovery and Timestamps
    - Microsoft Universal Application Artifacts
    - IE Download History
    - Gaining Access to Credentials Stored in the Windows Vault
    - Internet Explorer Tab Recovery Analysis
    - Cross-Device Synchronization, Including Tabs, History, Favorites, and Passwords

  - Firefox
  - Firefox Artifact Locations
  - SQLite Files and Firefox Quantum Updates
  - Download History
  - Firefox Cache2 Examinations
  - Detailed Visit Type Data
  - Form History
  - Session Recovery
  - Firefox Extensions
  - Firefox Cross-Device Synchronization
  - Private Browsing and Browser Artifact Recovery
  - IE and EdgeHTML InPrivate Browsing
  - Chrome, Edge, and Firefox Private Browsing
  - Investigating the Tor Browser
  - Identifying Selective Database Deletion
  - SQLite and ESE Database Carving and Examination of Additional Browser Artifacts
  - DOM and Web Storage Objects
  - Rebuilding Cached Web Pages
  - Browser Ancestry

- 6: Windows Forensics Challenge
  - Digital Forensics Capstone
  - Start at the Beginning with a New Set of Evidence
  - Find Critical Evidence Following the Evidence Analysis Methods Discussed Throughout the Week
  - Examine Memory, Registry, Chat, Browser, Recovered Files, Synchronized Artifacts, Installed Malware, and More
  - Build an Investigative Timeline
  - Answer Critical Investigative Questions with Factual Evidence
  - Practice Executive Summary and Report Generation

SANS FOR572:

- 1: Off the Disk and Onto the Wire
  - Web Proxy Server Examination
  - Role of a web proxy
  - Proxy solutions - commercial and open source
  - Squid proxy server
  - Configuration
  - Logging
  - Automated analysis
  - Cache extraction
  - Foundational Network Forensics Tools: tcpdump and Wireshark
  - tcpdump re-introduction
  - pcap file format

  - Berkeley Packet Filter (BPF)
  - Data reduction
  - Useful command-line parameters
  - Wireshark re-introduction
  - User interface
  - Display filters
  - Useful features for network forensic analysis
  - Network Evidence Acquisition
  - Three core types: full-packet capture, Logs, NetFlow
  - Capture devices: switches, taps, Layer 7 sources, NetFlow
  - Planning to capture: strategies; commercial and home-built platforms
  - Network Architectural Challenges and Opportunities
  - Challenges provided by a network environment
  - Future trends that will affect network forensics

- 2: Core Protocols & Log Aggregation/Analysis
  - Hypertext Transfer Protocol (HTTP) Part 1: Protocol
  - Forensic value
  - Request/response dissection
  - Useful HTTP fields
  - HTTP tracking cookies
  - HTTP/2 artifacts
  - Artifact extraction
  - Hypertext Transfer Protocol (HTTP) Part 2: Logs
  - Log formats
  - Expanded mod_forensic logging
  - Analysis methods
  - Domain Name Service (DNS): Protocol and Logs
  - Architecture and core functionality
  - Tunneling
  - Fast flux and domain name generation algorithms (DGAs)
  - Logging methods
  - Amplification attacks
  - Forensic Network Security Monitoring
  - Network Security Monitoring (NSM) emergence from Intrusion Detection Systems (IDSes)
  - Zeek NSM platform
  - Proactive/live use case
  - Post-incident DFIR use case
  - Logs created and formats used
  - JSON parsing with the "jq" utility
  - Community-ID flow hash value
  - Logging Protocol and Aggregation
  - Syslog
  - Dual role: server and protocol
  - Source and collection platforms

  - Event dissection
  - rsyslog configuration
  - Microsoft Eventing
  - Deployment model and capabilities
  - Windows Event Forwarding
  - Architecture
  - Analysis mode
  - Log Data Collection, Aggregation, and Analysis
  - Benefits of aggregation: scale, scope, independent validation, efficiency
  - Known weaknesses and mitigations
  - Evaluating a comprehensive log aggregation platform
  - Elastic Stack and the SOF-ELK Platform
  - Basics and pros/cons of the Elastic stack
  - SOF-ELK
  - Inputs
  - Log-centric dashboards
  - Use as a data exploration platform

- 3: NetFlow and File Access Protocols
  - NetFlow Collection and Analysis
  - Origins and evolution
  - NetFlow v5 and v9 protocols
  - Architectural components
  - NetFlow artifacts useful for examining encrypted traffic
  - Open-Source Flow Tools
  - Using open-source tool sets to examine NetFlow data
  - nfcapd, nfpcapd, and nfdump
  - SOF-ELK: NetFlow ingestion and dashboards
  - File Transfer Protocol (FTP)
  - History and current use
  - Shortcomings in today's networks
  - Capture and analysis
  - File extraction
  - Microsoft Protocols
  - Architecture and capture positioning
  - Exchange/Outlook
  - SMB v2, and v3

- 4: Commercial Tools, Wireless, and Full-Packet Hunting
  - Simple Mail Transfer Protocol (SMTP)
  - Lifecycle of an email message
  - Artifacts embedded along the delivery pathway
  - Adaptations and extensions
  - Object Extraction with NetworkMiner
  - Value of commercial tools in a DFIR workflow
  - NetworkMiner

  - Capabilities and user interface
  - Use cases for object extraction
  - Limitations and mitigations
  - Wireless Network Forensics
  - Translating analysis of wired networks to the wireless domain
  - Capture methodologies: Hardware and Software
  - Useful protocol fields
  - Typical attack methodologies based on protection mechanisms
  - Automated Tools and Libraries
  - Common tools that can facilitate large-scale analysis and repeatable workflows
  - Libraries that can be linked to custom tools and solutions
  - Chaining tools together effectively
  - Full-Packet Hunting with Moloch
  - Moloch architecture and use cases
  - Methods of ingesting packet data for DFIR workflows
  - Session awareness, filtering, typical forensic use cases
  - Raw packet searching with hunt jobs
  - Enrichment of extracted metadata
  - Custom decoding with CyberChef

- 5: Encryption, Protocol Reversing, OPSEC, and Intel
  - Encoding, Encryption, and SSL/TLS
  - Encoding algorithms
  - Encryption algorithms
  - Symmetric
  - Asymmetric
  - Profiling SSL/TLS connections with useful negotiation fields
  - Analytic mitigation
  - Perfect forward secrecy
  - Meddler-in-the-Middle (MITM)
  - Malicious uses and their artifacts
  - Benevolent uses and associated limitations
  - Common MITM tools
  - Network Protocol Reverse Engineering
  - Using known protocol fields to dissect unknown underlying protocols
  - Pattern recognition for common encoding algorithms
  - Addressing undocumented binary protocols
  - What to do after breaking the protocol
  - Investigation OPSEC and Threat Intel
  - Operational Security
  - Basic analysis can tip off attackers
  - How to mitigate risk without compromising quality
  - Intelligence
  - Plan to share smartly
  - Protect intelligence to mitigate risks

- 6: Network Forensics Capstone Challenge
    - Analysis using only network-based evidence
    - Determine the original source of an advanced attacker's compromise
    - Identify the attacker's actions while in the victim's environment
    - Confirm what data the attacker stole from the victim
    - Present executive-level summaries of your findings at the end of the day-long lab
    - Document and provide low-level technical backup for findings
    - Establish and present a timeline of the attacker's activities

Unpacking