CREST Practitioner Intrusion Analyst (CPIA) Syllabus (V8.1 - Sep 23)

The (CPIA) examination tests a candidates' knowledge across all 3 subject areas at a basic level below that of the CREST Registered examination.

1. Introduction

This syllabus identifies the technical skills and knowledge that CREST expects candidates to achieve success in the CREST Practitioner Intrusion Analyst certification. The Exam is entirely multiple choice with 120 Questions in 120 Mins.

2. Syllabus Structure

The syllabus is divided into six knowledge groups (Appendices A to F below), each of which is subdivided into specific skill areas.

Appendix A - Soft Skills and Incident Handling

ID	Skill	Details	CPIA
A 1	Engagement Lifecycle Management	Benefits and utility of incident response to the client. Awareness of steps that can be taken to prepare for potential incidents. Structure of incident response engagements, including the relevant processes and procedures. Knowledge of appropriate actions that should be taken when investigating an incident. Understanding that some actions should be avoided due to risk of evidence corruption. Know how to safely handle malware and potentially malicious files encountered during an engagement. Understanding limitations of system logs.	MC
A 2	Incident Chronology	Use of timelines to analyse event data Time zone issues System interpretation of timestamps with images	MC
A 3	Law & Compliance	Digital Millennium Copyright Act and consequences for reverse engineering. Knowledge of evidential integrity and chain of custody. Awareness of sector-specific regulatory issues (e.g. FSA, PCI). Understanding of situations that require notification of third parties. Understanding of when and how to engage law enforcement Knowledge of CERTS and their role and jurisdiction Good Practice Guide for Computer-Based Electronic Evidence	MC
A 4	Record Keeping, Interim Reporting & Results	Understanding reporting requirements. Understanding the importance of accurate and structured record keeping during the engagement.	MC
A 5	Threat Assessment	Understanding how a threat translates to the client and the business context of a given incident. High level methodologies surrounding threat assessment. Attribution of attacks. Knowledge of attacker motivation. Identifying key individuals likely to be selected for targeted attack. MITRE ATT&CK® Framework Cyber Kill-Chain	MC

Appendix B - Core Technical Skills

ID	Skill	Details	CPIA
B1	IP Protocols	IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. Detailed knowledge of application layer protocols commonly used by Trojan malware, namely TCP, UDP, HTTP[S], SMTP, and DNS. In-depth understanding of how the Internet (web browser/server architecture) and email systems function. Fundamental knowledge of at least the following protocols; IRC, DHCP, FTP, SMB, SNMP, ICMP.	MC
B2	Network Architectures	Varying network types that could be encountered during analysis: CAT 5/6/7/8 Basic understanding of common fibre technologies Windows Domain architectures Network Address Translation 10/100/1000baseT Wireless (802.11) Security implications of shared media switched media and VLANs. IP Subnets IP Routing Autonomous System Number (ASN)	MC
B3	Common Classes of Tools	Knowledge of common classes of tools used to perform intrusion analysis and reverse engineering. Basic understanding of the capabilities of common tools.	MC
B4	OS Fingerprinting	Passive operating system fingerprinting techniques.	MC
B5	Application Fingerprinting	Determining server types and network application versions from evidential data. Identification of client software versions from meta-data contained within common document types. Identification of client/server software versions from service banners, user-agent strings, email headers etc.	MC
B6	Network Access Control Analysis	Reviewing firewall rule bases and network access control lists.	MC
B7	Cryptography	Differences between encryption and encoding. Symmetric / asymmetric encryption Encryption algorithms: DES, 3DES, AES, RSA, RC4. Hashes: SHA family and MD5 Message Integrity codes: HMAC	MC
B8	Applications of Cryptography	SSL, IPsec, SSH, PGP Common wireless (802.11) encryption protocols: WEP, WPA, WPA2,,TKIP	MC
B9	File System Permissions	File permission attributes within Windows file systems and their security implications. Analysing registry ACLs.	MC
B10	Host Analysis Techniques	Listing processes and their associated network sockets (if any). Assessing patch levels on a Windows host using the command prompt. Finding interesting files on a Windows host. Web Servers	MC
B11	Understanding Common Data Formats	Candidates are expected to be able to interpret email headers, commenting on the reliability of the information contained within. Understanding of the information contained within a PKI certificate Understanding of various encoding employed for transmission of data (e.g. web and email)	MC

Appendix C - Background Information Gathering & Open Source

ID	Skill	Details	CPIA

C1	Registration Records	Information contained within IP and domain registries (WHOIS).	MC
C2	Domain Name Server (DNS)	DNS queries and responses DNS zone transfers Structure, interpretation, and analysis of DNS records: • SOA • MX • TXT • A • NS • PTR • HINFO • CNAME Awareness of dynamic DNS providers, how they function and security implications. Understand the concept of fast-flux DNS.	MC
C3	Open-Source Investigation and Web Enumeration	Effective use of search engines and other open-source intelligence sources to gain information about a target. Knowledge of information that can be retrieved from common social networking sites Network and host fingerprinting tools and techniques	MC
C4	Extraction of Document Meta Data	Be able to extract meta-data such as author, application versions, machine names, print and operating system information from common document formats.	MC
C5	Community Knowledge	Ability to interpret common anti-virus threat reports Ability to interpret open-source research when investigating incidents, eliminating false positives. Knowledge of popular open-source security resources (web sites, forums, etc.).	MC

Appendix D - Network Intrusion Analysis

ID	Skill	Details	CPIA
D1	Network Traffic Capture	Methods of data collection and types of data to be collected. Designing a collection system to ensure sufficient data is collected without overwhelming capture devices. Impact assessment of any changes to network. Knowledge of SPAN ports, traditional network TAPs and aggregating TAPs. Ability to estimate capture requirements during scoping. Consideration of appropriate capture device deployment location. Constraints and limitations of capture and analysis toolsets. Knowledge of different capture options (e.g. NetFlow, limited capture, full packet capture etc.) The ability to assure integrity and security of network after introduction of a capture device Provide arguments and evidence that supports the integrity of any data captured.	MC
D2	Data Sources and Network Log Sources	Types of data to be collected and existing data sources which should be considered to provide a complete picture of activity. Candidates should be familiar with the type of information provided in at least the following: • Proxy logs • syslog • Email logs • Firewall logs	MC

		• DHCP logs • VPN logs • Web server logs • Antivirus logs • DNS logs • Domain logs • Windows event logs • Internet history • Database logs • O365 Unified Logs Correlation of information contained within any number of different log formats.	
D3	Network configuration security issues	Observation/detection of common network misconfiguration issues such as: • IP Routing issues • DNS information leakage • Unexpected traffic routes • Email routing issues • Firewalls/rules not working Detection of deliberate attempts to bypass firewall/proxy rules.	MC
D4	Unusual Protocol Behaviour	Observation/detection of common protocols exhibiting non-standard behaviour. Verification of various protocols regardless of TCP/UDP port in use. Identification of illegal protocol usage for purposes of vulnerability exploitation or cache poisoning etc.	MC
D5	Beaconing	Ability to recognise and detect both covert and open malware beacons from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	
D6	Encryption	Understanding of channel fingerprinting. Analysis of traffic flows (volume, directions, QoS, timing, custom or standard encryption). Identification of weak obfuscation using XOR, ROL or codebooks and approaches to de-obfuscation.	MC
D7	Command and Control Channels	Ability to recognise and detect both covert and open C&C from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC
D8	Exfiltration of Data	Ability to recognise and detect both covert and open exfiltration of data from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC
D9	Incoming attacks	Detect successful incoming attacks against public facing services, including email, from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC
D10	Reconnaissance	Detect internal and external reconnaissance activities from statistical analysis, signatures, and manual review of traffic and logs. Traffic may include a variety of IP protocols.	MC
D11	Internal spread and privilege escalation	Detect the spread of malware within a network and indicators of privilege escalation from statistical analysis and manual review of traffic that may include a variety of different IP protocols and logs. Understanding of offensive tool capabilities	MC
D12	Web based attacks	Ability to identify potentially malicious elements within HTML and other common web file types Ability to decode obfuscated JavaScript code and determine whether the code is malicious in nature.	
D13	False Positive Acknowledgement	Determine whether a given IDS alert is a true hit or false positive.	MC

		Suggest improvements to common IDS signatures to reduce false positive rates.	

Appendix E - Analysing Host Intrusions

ID	Skill	Details	CPIA
E1	Host-based Data Acquisition	Fundamental acquisition concepts, techniques, and methodologies, including static and dynamic evidence gathering and image formats. Local and remote acquisition scenarios Forensic Artefact collection (Kape, CyLr, Brimor Labs etc)	MC
E3	Windows File System Essentials	Disk partitioning FAT – File Allocation Table, directory entries NTFS – $MFT, $Bitmap ACLs & SIDs Unallocated space File carving EFS & BitLocker	MC
E4	Windows File Structures	Prefetch Volume Shadow Copy System Restore Points User profiles Temporary files Network configuration (hosts file) Pagefile & hibernation file Shimcache Registry hives Recycle bin Event logs (Binary XML e.g. evtx) NTDS (Active Directory) WMI (OBJECTS.DATA)	MC
E5	Application File Structures	Archive formats (Zip, RAR, etc) Browser artefacts PE files Office documents (OLE and Office Open XML), including knowledge of DDE and Macro exploits PDF Email file structures (Exchange, PST) AV artefacts (quarantines and logs) SQLite databases Log files	MC
E6	Windows Registry Essentials	Registry structures (hive format) USB/removable storage artefacts Autorun/startup locations ACLs Protected storage Shimcache User accounts	MC
E7	Identifying Suspect Files	Use of hash tables to find common malware Strings File permissions Packed executables Fuzzy hashing Signature analysis	MC
E8	Storage Media	Hard Disks – Interface types (PATA/SATA, SCSI, SAS), HPA, DCO, Password protection Solid State Devices – Hard Disks, Pen Drives, Media Cards, wear levelling issues, how this media type varies from magnetic Full Disk Encryption RAID – levels of RAID type and error correction NAS	MC
E9	Memory Analysis	Analysis – running processes, parent/child process identification, DLLs, sockets Process acquisition	MC

		Clipboard contents Correlating memory artefacts with on-disk applications Network connections Command prompt history Browser history Process Injection Use of common memory analysis frameworks (e.g. Volatility)	
E10	Infection Vectors	Infected Executables/DLL, Documents (Macros, DDE), JavaScript Drive-by downloads USB/external media/shared drive vectors Passive exploitation Email-based attacks	MC
E11	Malware Behaviours and Anti-Forensics	Encryption Steganography Password Protection Obfuscation Covert storage techniques Covert communication techniques (command and control, recon, and exfiltration) Data Erasure Applications Filing System – NTFS ADS	MC
E12	Rootkit Identification	How to identify rootkits Hooking techniques	MC
E13	Live Malware Analysis	Identification of open files/registry keys/network sockets Process monitoring tools	MC
E14	Linux OS File Structures	Analysis techniques Common forensic artefacts	MC

Appendix F – Malware Analysis/Reverse Engineering

ID	Skill	Details	CPIA
F2	Functionality Identification	Identifying common cryptographic algorithms in binaries through, for example, use of standard constants and common instructions. Identifying network send/receive loops Infection vectors and persistence mechanisms	MC
F6	Cryptographic Techniques	Encryption Key material identification and extraction Identifying implementation weaknesses	MC
F8	Windows Executable File Formats	Standard windows executable formats (e.g. PE, EXE, COM) Extracting valuable information in executable files	MC
F9	Hiding Techniques	Common techniques for process injection Rootkit techniques for hiding files and other system resources including: • SSDT patching • Filter drivers • Process list manipulation	MC
F12	Behavioural Analysis	Use of common tools to identify patterns of behaviour Aspects of command and control Infection vectors and persistence mechanisms	MC