CREST Assessors Panel

CREST Certified Red Team Specialist (CCRTS) Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	SYL_CCRTS
Version Number	2.1
Status	Public
Issue Date	25/11/2024

Contents

1. Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Simulated Attack Specialist Certification.

Candidates taking the CREST Certified Red Team Specialist (CCRTS) examination may benefit from having passed the CREST Certified Tester (Infrastructure) examination but this is not a pre-requisite. Alternative exam preparation may also be appropriate

2. Syllabus Structure

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

For each skill area, CREST has indicated in which component (Written Multiple Choice, Scenario or Practical) the candidate will be assessed.

Within the tables, the following acronyms apply:

SC Written Scenario Question

MC Written Multiple Choice

P Practical

Appendix A: Soft Skills and Assessment Management

ID	Skill	Details	Multiple Choice	Scenario	Practical
A1	Law & Compliance	Awareness of local legislation pertaining to simulated attacks. Awareness of the legal complexities of dealing with multinational organisations. Awareness of requirements for interaction with law enforcement where appropriate. Knowledge of written authority required to comply with local laws. Understanding of the importance of client confidentiality and non-disclosure agreements. Interaction/notification with law enforcement where appropriate (e.g. out-of-hours physical security assessments or reconnaissance). Knowledge of the written authority required to comply with local laws (e.g. 'Letter of Authority').	MC	SC	
A2	Law & Compliance (Regional)	Knowledge of relevant legislation affecting penetration testing across region(s). Legislation concerning computer misuse • In the UK this includes Computer Misuse Act 1990 and amendments Legislation concerning individual's personal data • In the UK this includes the Data Protection Act 2018 Knowledge of legislation affecting simulated attacks with or on behalf of a specific sector. • For UK financial sector this would include CBEST. Can provide examples of compliance and non-compliance.	MC	SC	
A3	Scoping	Understands client requirements and can produce an accurate and adequately resourced penetration testing scope. Understands legal, technical, logistical, financial and other constraints, and is able to take these into account without compromising the effectiveness of the penetration test.	MC	SC	

		Able to simulate testing to enable attack path testing to continue.			
A4	Risk	Understands the additional risks associated with simulated attacks, can explain and manage risks to customers. Can measure the risks of different attack paths or techniques, the outcomes of such risks materialising and knows how to mitigate these risks. Effective planning for potential DoS conditions.	MC	SC	
A5	Record Keeping & Reporting	Understands reporting requirements and the importance of accurate and structured record keeping during the engagement. Can accurately report vulnerabilities, scenarios, attack paths and organisational failings/weaknesses encountered during the engagement, in addition to root cause analysis and wider organisational themes. Ability to maintain a comprehensive evidence and audit log detailing simulated attack actions in detail. Able to assist customers or other agencies as required.	MC	SC	P
A6	Threat Intelligence	Ability to accurately interpret Threat Intelligence to form realistic simulated attack scenarios. Ability to assess the value and quality of different Threat Intelligence sources. Ability to deliver payloads that simulate threat actors, based on TI.	MC	SC	P
A7	Client Communications	Can plan and implement a customer communication strategy, with regular checkpoints and defined escalation paths. Will provide regular updates of progress to necessary stakeholders. Knowledge and practical use of secure communication channels, and out-of-band channels.	MC	SC	
A8	Operational Security	Identification of risks introduced by a simulated attack operation, including threats and vulnerabilities, and application of appropriate countermeasures. Protection of sensitive information obtained during an engagement from common OpSec risks (e.g.	MC	SC	

		secure communications, eavesdropping, social media etc.).			
A9	Social Engineering	Knowledge of various types of social engineering attacks. Ability to formulate realistic attack scenarios, including necessary 'cover stories', production of fake badges/ID and email or phone-based phishing attacks.	MC	SC	
A10	Physical Security	Awareness and identification of physical security weaknesses and possible entry points into an organisation.	MC	SC	
A11	Threat Modelling	Knowledge regarding phases of the cyber kill chain methodology, attacker TTPs and mappings to the MITRE ATT&CK® framework. Ability to map simulated attack scenarios to threat models.	MC	SC	

Appendix B: Core Technical Skills

ID	Skill	Details	Multiple Choice	Scenario	Practical
B1	Networking	Knowledge of typical network types that could be encountered during a simulated attack, including TCP/IP and common application layer protocols. Security implications of network topologies and media, including WiFi, VLANs, Common security architectures and network topologies including business - multi-site on-premise, cloud or hybrid networks and client, site-to-site or cloud VPNs and user - client VPNs, remote working, cloud portals.	MC	SC	P
B2	Discovery & Mapping	Ability to use tools and intelligence gathering activities to map and discover customer assets. Can attribute accounts, services and assets to a customer, prioritising a target list and verifying scope. OS and Application fingerprinting, banner grabbing and service enumeration. Review and interpret documentation, configuration and intelligence to map networks and route attack paths around access controls.	MC	SC	P
B3	Cryptography	Understands symmetric and asymmetric cryptography, common protocols and their security attributes	MC	SC	P

		Understands encryption implementations within software applications, such as SSH, TLS and PGP and in networks such as IPSec and WiFi. Understands common cryptographic algorithms, hash functions, signing and message authentication. Understands PKI and the concepts of certificates, certificate authorities and trusted third parties.			
B4	File System Permissions	File permission attributes within Unix and Windows file systems and their security implications. Analysing registry ACLs.	MC	SC	P
B5	Audit Techniques	Ability to audit live hosts and services or saved settings. Includes, by example, listing processes, network sockets, file handles, and assessing patch levels, system configuration or installed software. Ability to use audit data to assist attack paths.	MC	SC	P
B6	Automation and Scripting	Awareness and practical experience of scripting languages that may be required in automating and enabling the process of real word testing on common Windows and Unix based platforms. Candidates should have specific experience of the capabilities of Windows Batch Files, PowerShell, Bash scripting, Python and other script types	MC	SC	P

Appendix C: Reconnaissance

ID	Skill	Details	Multiple Choice	Scenario	Practical
C1	Registration Records	Information contained within IP and domain registries (WHOIS).	MC	SC	
C2	DNS	Understands the Domain Name Service (DNS) including queries and responses, zone transfers, and the structure and purpose of records. Can query DNS servers or use passive or historical DNS data to gather information on target systems. Can identify and exploit misconfigured DNS entries and associated vulnerabilities.	MC	SC	P
C3	Internet Reconnaissance	Analysis of information from a target web site, search engines and other public data sources to gain information about a target, including social media. Knowledge and experience of information harvesting techniques, and an understanding of the legal implications of scraping social media sites and use of stolen databases or leaks. Exploitation of technical data sources such as service scanning search engines, code repositories and recovering intelligence from metadata leaked or obtained from the target. Extraction of potentially sensitive data (e.g. usernames, computer names, operating system, software products) from various file formats Understands how key internet technologies such as web and email work in detail to assist in intelligence gathering and targeting.	MC	SC	
C4	Third Parties	Ability to perform cloud reconnaissance, identifying SaaS products or Cloud service providers in use by a target, and how they are utilised. Understand limitations of scope and legalities with third party providers, simulating attack paths if necessary.	MC	SC	

Appendix D: Implants

ID	Skill	Details	Multiple Choice	Scenario	Practical
D1	Implant Design	Implant design, evaluation, configuration and customisation, considering (for example): Engagement scope and target assets Appropriate implant types Built-in operating system functionality vs. custom code Available exfiltration techniques, data security and viability of exfiltration routes Evasion techniques required for anti-virus, anti-malware and OS defences. Pivoting and proliferation requirements Threat Intelligence & simulation requirements	MC	SC	
D2	Implant Assessment	Able to select and use publicly available implant frameworks to meet requirements and provide appropriate threat emulation.			P
D3	Exploitation of common file formats	Ability to create trojanised versions of common documents, including Microsoft Office. Ability to mask the origin of documents and smuggle content within other filetypes. Can utilise embedded scripting or programming interfaces, such as VBA, understanding their capabilities and limitations as well as defensive capabilities and bypass techniques.	MC		P
D4	Persistence	Ability to ensure an implant can persist reboot or logout events, using multiple methods. Able to persist in userland by ensuring implant code is loaded following user action, including with common business applications.	MC		P
D5	Physical Implants	Knowledge of physical implants that can be used to intercept keystrokes, video and mouse actions. Can utilise network bridges (e.g. 3G/4G, WiFi) to enable remote access, or can simulate based on a risk assessment.	MC	SC	

Appendix E: Initial Access

ID	Skill	Details	Multiple Choice	Scenario	Practical
E1	Email Delivery	Ability to create and spoof emails by direct SMTP protocol interaction with a mail server. Knowledge of spear phishing techniques and ability to manage and deliver phishing campaigns, limiting user interaction. Knowledge of email authentication and anti-spoofing technologies such as SPF, DKIM and DMARC.	MC	SC	P
E2	Application Delivery	Use of other applications to deliver implants, such as business communication & management or cloud apps. Knowledge of website seeding techniques that can be used to deliver malicious code to victims.	MC	SC	P
E3	Supply Chain Attacks	Knowledge of supply chain attacks, can identify risks within a customer environment and simulate a supply chain attack.	MC	SC	P
E4	Perimeter Attacks	Ability to perform application and infrastructure attacks against a customer's internet facing assets or cloud hosted services, using vulnerabilities as an initial access vector.	MC	SC	P
E5	Access Broker / Insider Threat	Awareness and simulation of an insider threat or a malicious third party providing access to a customer network.	MC	SC	P
E6	Remote Credential Theft	Ability to create spoofing portals and man-in-the-middle reverse proxies to perform credential or MFA capture, obtain access tokens or coerce users into granting access to rogue devices or malicious applications.	MC	SC	P

Appendix F: Lateral Movement & Privilege Escalation

ID	Skill	Details	Multiple Choice	Scenario	Practical
F1	Active Directory	Knowledge, use and abuse of Active Directory Directory Services, including Domain, Federation & Certificate Services. Enumeration of AD configuration, objects, users, ACLs and trusts, including LDAP enumeration. Exploitation of misconfiguration and misplaced trusts to further attack paths against a target. Exploitation of authentication controls, including Kerberos and certificate attacks, SSO & federation, tickets and replay attacks. Extraction of AD configuration and secrets from files and backups.	MC	SC	P
F2	Cloud Directory Services	Knowledge, use and abuse of Cloud Directory Services or and Identity and Access Management (IAM) solutions.	MC		
F3	Enumeration of hosts	Ability to query internal name services and directories to identify targets on a network, both internally and within cloud or third party. Internal fingerprinting of hosts and services. The ability to find embedded devices (e.g. telephony or door access systems) on a network and subsequently exploit to gain unauthorised access to the device or information pertinent to the attack path.	MC		P
F4	Enumeration of users	Identification and exploitation of common internal and external interfaces that may facilitate username enumeration. Can use valid information to establish further users and username patterns.	MC		P
F5	Operating System Vulnerabilities	Knowledge of local and remote Windows, Linux & macOS vulnerabilities, particularly those for which robust exploit code exists in the public domain. Knowledge of privilege escalation vulnerabilities and techniques.	MC		P

		Knowledge of common post exploitation activities, including: - password hashes, cracking & clear-text passwords - spoofing/poisoning services for authentication capture or relay - patch levels & missing security patch identification Knowledge of common OS services & remote management, able to leverage these to facilitate a chosen attack path.			
F6	Software enumeration	Ability to fully list all installed applications on Windows or macOS and identify potentially vulnerable installations that could be exploited. Ability (both from a local and remote perspective) to list missing patches/updates and associated security vulnerabilities against Operating Systems, common business applications and other third-party software.	MC		P
F7	Enumeration of sensitive files	Ability to conduct complex searches for sensitive files on local or networked storage. Can identify and mount remote locations.	MC		P
F8	Browser Exploitation	Exploitation of browser data, including credential theft, ticket stealing, accessing cookies and browser history. Able to use stolen data to facilitate wider attack paths. Perform man-in-the-browser attacks, capturing or manipulating a user's browser session.	MC		P
F9	Application Exploitation	Exploit high value applications, business services and team collaboration software, including cloud services and web applications. Extract sensitive data, poison documents and otherwise leverage access for further attacks paths. Identify, exploit and decrypt data from registry and application files.	MC		P
F10	User Interaction	The ability to intercept keystrokes and take screenshots without the victim's knowledge.	MC		P

		Use peripherals such as microphones and webcams to obtain audio and video capture without the victim's knowledge.			

Appendix G: Evasion

ID	Skill	Details	Multiple Choice	Scenario	Practical
G1	Host AV/EDR	Evasion of common host defensive capabilities, including low-level logging such as ETW, fileless malware defences such as AMSI and Anti-Virus and EDR solutions. Evasion of allow-listing controls, including applications, filetypes or devices, using solutions inbuilt to the operating system or third party. Able to defeat security controls implemented in userland. Can modify open-source tools to evade signature-based detection. Knowledge of capabilities of monitoring solutions and ability to simulate a threat actor's footprint.	MC	SC	P
G2	Network IDS/IPS	Awareness of IDS/IPS solutions, and implications upon simulated attacks. Ability to throttle network traffic and understand how to limit unnecessary connections or log entries, prioritising likely attack paths. Knowledge of capabilities of monitoring solutions and ability to simulate a threat actor's footprint.	MC	SC	P
G3	Perimeter Controls	Enumeration and evasion of SMTP and HTTP proxy perimeter filtering, antivirus defences and TLS inspection.	MC		P
G4	Stealth	Understand the impact of tools and techniques used within a target environment. Can both limit opportunities for detection by EDR and also provide detection opportunities in line with a simulation's threat intelligence or emulated threat actor's methodology.	MC	SC	P

Appendix H: Egress / Command and Control

ID	Skill	Details	Multiple Choice	Scenario	Practical
H1	Reverse Communications	Demonstrate the ability to establish an outbound command and control channel from a compromised workstation through a well configured perimeter firewall, enumerating traffic types and network ports permissible. Awareness of IDS/IPS capabilities, egress filtering, and ability to hide traffic within common protocols.	MC	SC	P
H2	Tunnelling	Knowledge of various protocols that can be used for tunnelling arbitrary traffic out of a network, and typical limitations. Tunnelling through applications or cloud services, masking C2 traffic within business application data. Tunnelling C2 traffic through internal hosts, bypassing firewall rules and controlling implants on non-internet connected hosts.	MC	SC	P
H3	Attack Source Obfuscation	Knowledge of various techniques that can be used to obfuscate the source of an attack. For example, the use of residential proxies, relays or anonymising networks to impede attribution.	MC	SC	
H4	Secure Egress	Knowledge of risks associated with egress/C2 channels, and demonstration of security considerations to protect channels from attack. Practical use of authentication and encryption to ensure the confidentiality of exfiltrated data and integrity of the control channel.	MC	SC	P

Telephone: +44 (0)20 3058 3122

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

Press / Public Relations: media@crest-approved.org