Technical Committee and Assessors Panel

CREST Simulated Attack Technical Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	SYL_CCSAS/M
Version Number	1.0
Status	Public Release
Issue Date	23 May 2014

Table of Contents

Version History

Version	Date	Authors	Status
0.1	26 March 2014	Technical Committee and Assessors Panel	Internal Release
0.6	04 April 2014	Technical Committee and Assessors Panel	Internal Release
1.0	23 May 2014	Technical Committee and Assessors Panel	Public Release

Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board

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 Certification Certifications. There are two examinations available, as detailed below. Both examinations cover a common set of core skills and knowledge as well as more specific role related areas

Success at the CREST Certified Simulated Attack Manager (CCSAM) examination will confer CREST Certified status to the individual.

The CREST Certified Simulated Attack Specialist (CCSAS) examination is only open to candidates who have already passed the CREST Certified Tester (Infrastructure) examination and will confer the additional status of Certified Simulated Attack Specialist to the individual.

1.1 CREST Certified Simulated Attack Manager (CCSAM)

The (CCSAM) examination tests candidates' knowledge and expertise in leading a team that specialises in Simulated Attacks. The candidate is expected to have a good breadth of knowledge in all areas of Simulated Attack and proven experience in managing incidents, penetration tests and simulated attack exercises. The exam will assess the candidate's ability to conduct Simulated Attacks in a realistic, legal and safe manner, ensuring appropriate evidence is collated to provide the customer with actionable intelligence of organisational risks and failings while minimising the risks to the customer's staff, data and systems.

1.2 CREST Certified Simulated Attack Specialist (CCSAS)

The (CCSAS) examination tests candidates' knowledge and expertise delivering technical components of a Simulated Attack, specifically exploitation of client vulnerabilities through Trojanised files, phishing campaigns, implant development, evasion skills and lateral movement within a compromised network. This exam is considered an specialism to the existing CREST CCT Infrastructure certification, which is a mandatory prerequisite for all candidates wishing to complete this examination. While it is acknowledged that there is significant overlap with the existing INF exam syllabus this examination is set at a significantly higher level of detail in a number of areas.

2 Certification Examination Structure

2.1 Crest Certified Simulated Attack Manager (CCSAM)

The CCSAM Examination is a purely written exam consisting of three sections: a set of multiple choice questions, a selection of long form questions that will require written answers and finally a section that details two in-depth scenario questions. The scenario questions are designed to assess the candidates' real world experience in leading large complex simulated attacks in a safe, controlled and realistic manner.

2.2 Crest Certified Simulated Attack Specialist (CCSAS)

The CCSAS Examination has two components: a written paper and a practical assessment. The written paper consists of two sections: a set of multiple choice questions and a selection of long form questions that will require written answers. The practical assessment tests candidates' hands-on simulated attack skills against reference networks, hosts and applications.

The *Notes for Candidates (NFC)* document provides further information regarding the Certification Examinations in general and the specific skill areas that will be assessed within the practical components.

3 Syllabus Structure

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

For each skill area, CREST has indicated where and how the area will be assessed: in which Certification Examination (SAM or SAS) and in which component (Written Multiple Choice, Written Long Form, Scenario or Practical).

Within the tables, the following acronyms apply:

CCSAM	Simulated Attack Manager Examination
CCSAS	Simulated Attack Specialist Examination
SC	Written Scenario Question
MC	Written Multiple Choice
LF	Written Long Form
P	Practical

Appendix A: Soft Skills and Assessment Management

ID	Skill	Details	CCSAM	CCSAS
A1	Law & Compliance	Knowledge of pertinent UK legal issues: • Computer Misuse Act 1990 • Human Rights Act 1998 • Data Protection Act 1998 • Police and Justice Act 2006 Impact of this legislation on penetration testing and simulated attack activities. Awareness of sector-specific regulatory issues. Awareness of the legal complexities of dealing with multinational organisations 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 LF SC	MC LF
A2	Scoping	Understanding client requirements. Scoping project to fulfil client requirements. Accurate timescale scoping. Resource planning. Rules of engagement/limitations/constraints.	MC LF SC	MC LF
A3	Understanding Explaining and Managing Risk	Knowledge of additional risks that penetration testing (and simulated attacks) can present. Levels of risk relating to penetration testing and simulated attacks, the usual outcomes of such risks materialising and how to mitigate the risks. Effective planning for potential DoS conditions.	MC LF SC	MC LF
A4	Record Keeping, Interim Reporting & Final Results	Understanding reporting requirements. Understanding the importance of accurate and structured record keeping during the engagement. Accurate reporting of vulnerabilities and organisational failings/weaknesses encountered during the engagement. Full audit log of all commands/activities conducted on a 'compromised' host.	MC LF SC	MC LF P

A5	Threat Intelligence	Ability to accurately interpret Threat Intelligence to form realistic simulated attack scenarios. Ability to generate Threat Intelligence reports in a completely objective, factual manner. Ability to assess the value and quality of different Threat Intelligence sources.	MC LF SC	MC LF
A6	Client Communications	Knowledge sharing, daily checkpoints and defining escalation paths for encountered problems. Knowledge and practical use of secure out-of-band communication channels. Regular updates of progress to necessary stakeholders. Email encryption options available (e.g. SMIME, PGP).	MC LF SC	MC LF
A7	Operations Security (OpSec)	Identification of risks associated with 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. secure communications, eavesdropping, social media etc.).	MC LF SC	MC LF
A8	Social Engineering Attacks	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/phone based phishing attacks.	MC LF SC	MC LF
A9	Physical Security	Awareness and identification of physical security weaknesses and possible entry points into an organisation.	MC LF SC	MC LF
A10	Kill Chain	Knowledge regarding phases of the cyber 'kill chain' methodology.	MC LF	MC LF

Appendix B: Core Technical Skills

ID	Skill	Details	CCSAM	CCSAS
B1	IP Protocols	IP protocols: IPv4 and IPv6, TCP, UDP and ICMP. VPN Protocols (e.g. PPTP). Awareness that other IP protocols exist.	MC	MC P
B2	Network Architectures / Topologies	Varying networks types that could be encountered during a penetration test: • CAT 5 / 6 / Fibre • 10/100/1000/10000baseT • Wireless (802.11) Security implications of shared media, switched media and VLANs. Common security architectures and network topologies (e.g. CESG Walled Garden)	MC	MC P
B3	Network Mapping & Target Identification	Analysis of output from tools used to map the route between the engagement point and a number of targets. Network sweeping techniques to prioritise a target list and the potential for false negatives.	MC LF SC	MC LF P
B4	Interpreting Tool Output	Interpreting output from port scanners, network sniffers and other network enumeration tools.	MC	MC P
B5	Filtering Avoidance Techniques	The importance of egress and ingress filtering, including the risks associated with outbound connections.	MC LF SC	MC LF P
B6	Packet Crafting	Packet crafting to meet a particular requirement: • Modifying source ports • Spoofing IP addresses • Manipulating TTL's • Fragmentation • Generating ICMP packets	MC	MC
B7	OS Fingerprinting	Remote operating system fingerprinting; active and passive techniques.	MC	MC P
B8	Application Fingerprinting and Evaluating Unknown Services	Determining server types and network application versions from application banners. Evaluation of responsive but unknown network applications.	MC	MC P

B9	Network Access Control Analysis	Reviewing firewall rule bases and network access control lists. Ability to bypass basic NAC protection (e.g. MAC address lockdown).	MC	MC P
B10	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	MC
B11	Applications of Cryptography	SSL/TLS, IPSEC, SSH, PGP Common wireless (802.11) encryption protocols: WEP, WPA2, TKIP	MC	MC
B12	File System Permissions	File permission attributes within Unix and Windows file systems and their security implications. Analysing registry ACLs.	MC	MC
B13	Audit Techniques	Listing processes and their associated network sockets (if any). Assessing patch levels. Finding interesting files.	MC	MC P
B14	Windows Vulnerabilities	Knowledge of remote windows vulnerabilities, particularly those for which robust exploit code exists in the public domain. Knowledge of local windows privilege escalation vulnerabilities and techniques. Knowledge of common post exploitation activities: • obtain password hashes, both from the local SAM and cached credentials • obtaining locally-stored clear-text passwords • crack password hashes • check patch levels • derive list of missing security patches • reversion to previous state	MC	MC LF P

B15	Unix/Linux Vulnerabilities	Recent or commonly-found Solaris vulnerabilities, and in particular those for which there is exploit code in the public domain. Recent or commonly-found Linux vulnerabilities, and in particular those for which there is exploit code in the public domain. Use of remote exploit code and local exploit code to gain root access to target host Common post-exploitation activities: • exfiltrate password hashes • crack password hashes • check patch levels • derive list of missing security patches • reversion to previous state	MC	MC LF P
B16	Wireless Networks	Ability to detect and exploit vulnerable wireless networks to gain unauthorised access (e.g. WEP protected networks, WPA2 protected networks with weak PSKs, common WPA Enterprise misconfiguration issues)	MC LF	MC LF P
B17	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 scripts, Unix Shell (e.g. Bash) scripting, Python and Perl.	MC	MC P
B18	Directory Services	Awareness and practical experience of DNS configurations that may be found in real word testing on common Windows and Unix based platforms for both public and private networks. Candidates should have specific experience of the capabilities of common implementations such as Microsoft DNS Server and BIND.	MC	MC LF P
B19	VPN Technologies	Awareness and practical experience of VPN configurations that may be found in real word testing on common Windows and Unix based platforms. Candidates should have specific experience of the capabilities of common clients for a variety of VPN protocols including (but not limited to) PPTP, IPSEC, L2TP, OpenVPN and SSL/TLS VPNs.	MC	MC LF P

Appendix C: Background Information Gathering & Open Source

ID	Skill	Details	CCSAM	CCSAS
C1	Registration Records	Information contained within IP and domain registries (WHOIS).	MC LF SC	MC LF
C2	Domain Name Server (DNS)	DNS queries and responses DNS zone transfers DNS hostname enumeration/guessing Structure, interpretation and analysis of DNS records: • SOA • MX • TXT • A • AAAA • NS • PTR • HINFO • CNAME • SPF • SRV Passive DNS monitoring	MC LF SC	MC LF P
C3	Customer Web Site Analysis	Analysis of information from a target web site, both from displayed content and from within the HTML source.	MC LF SC	MC LF P
C4	Web Enumeration and Social Media	Effective use of search engines and other public data sources to gain information about a target. Knowledge of information that can retrieved from social media sites, for example Facebook, Twitter, LinkedIn and PasteBin. Knowledge and experience of information harvesting techniques, and an understanding of the legal implications of scraping social media sites. Knowledge and experience using specialist 'service' search engines (e.g. Shodan).	MC LF SC	MC LF
C5	NNTP Newsgroups, Mailing Lists and Forums	Searching newsgroups, forums and/or mailing lists for useful information about a target.	MC LF SC	MC LF

C6	Information Leakage from Mail & News Headers	Analysing news group and e-mail headers to identify internal system information.	MC LF SC	MC LF P
C7	Document Metadata	Extraction of potentially sensitive data (e.g. usernames, computer names, operating system, software products) from various document formats, including: • PDF • Microsoft Office documents • Common picture formats (e.g. JPEG, PNG, GIF etc.)	MC LF SC	MC LF P

Appendix D: Enumeration/Reconnaissance

ID	Skill	Details	CCSAM	CCSAS
D1	Enumeration of hosts	Candidates must be able to query both DNS and LDAP via legitimate methods to identify potentially interesting targets on a network. Candidates must be able to enumerate relevant information from an Active Directory.	MC	MC P
D2	Enumeration of users	Identification and exploitation of internally and externally facing interfaces that may facilitate username enumeration, for example: • SMTP • SNMP • Custom and COTS web applications (e.g. Intranet, phone directories etc.) • SIP • LDAP • Active Directory	MC LF SC	MC LF P
D3	Enumeration of operating systems	Identification of exact operating system versions via advertised user-agent strings and other browser idiosyncrasies.	MC	MC P
D3	Enumeration of software packages	Ability to fully list all installed applications on a Microsoft Windows workstation, and identify potentially vulnerable installations that could be exploited.	MC	MC LF P
D4	Enumeration of missing security updates	Ability (both from a local and remote perspective) to list missing patches/updates and associated security vulnerabilities against: • Microsoft Windows operating systems • Microsoft Office installations • Third party software installations	MC LF	MC LF P
D5	Enumeration of sensitive files	Ability to conduct complex searches for sensitive files on a Microsoft Windows workstation, using both command line tools and Explorer search utilities.	MC	MC P
D6	Enumeration of registry and configuration settings	Ability to identify and modify registry and configuration settings on a Microsoft Windows workstation, using both command line tools and Registry utilities.	MC	MC P

Appendix E: Trojan Delivery

ID	Skill	Details	CCSAM	CCSAS
E1	Email Spoofing	Ability to create spoofed emails by direct SMTP protocol interaction with a mail server. Knowledge of spear phishing techniques and ability to manage and deliver phishing campaigns.	MC LF SC	MC LF P
E2	Anti-Spoofing Countermeasures	Knowledge of anti-spoofing technologies, including Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).	MC LF	MC LF
E3	Web Site Seeding	Knowledge of website seeding techniques that can be used to deliver malicious code to victims. Practical knowledge and experience of common OWASP vulnerabilities that may facilitate delivery of 'drive-by' download attacks.	MC SC	MC LF P
E4	Trojanised Legitimate Binaries	Ability to take a legitimate functional binary and add extra malicious functionality via recompiling or packing, without compromising the original functionality of the binary.	MC	MC P

Appendix F: Client-Side Exploitation Skills

ID	Skill	Details	CCSAM	CCSAS
F1	Exploitation of common document formats	Ability to create trojanised versions of the following document formats: • Adobe Acrobat • Microsoft Office family (2003 – 2013) Techniques should include arbitrary code execution via exploitation of unpatched software installations and also code execution of fully patched software installations through social engineering attacks (e.g. embedded files/JavaScript/macros).	MC LF SC	MC LF P
F2	Exploitation of client web browsers	Ability to download and execute an arbitrary Win32 executable with no user interaction via exploitation of a client web browser. Knowledge of common vulnerabilities in unpatched versions of: • Google Chrome • Mozilla Firefox • Safari • Internet Explorer	MC LF SC	MC LF P
F3	Exploitation of rich content	Exploitation of rich content supported by many client browsers, for example: • Adobe Flash • Java installations • Microsoft Silverlight Ability to create a staging website to deliver malicious code to exploit these software installations. Ability to download and execute an arbitrary Win32 executable with minimal or zero user interaction.	MC LF SC	MC LF P
F4	Exploitation of underlying operating system vulnerabilities	Exploitation of Microsoft Windows vulnerabilities that require an element of social engineering to succeed. For example, exploitation of core Microsoft Windows components that can be instantiated by visiting a malicious web site. The candidate should be capable of hosting a staging site to deliver an exploit and subsequent payload to the victim.	MC LF SC	MC LF P
F5	Exploitation of Cross-site scripting Vulnerabilities	Exploitation of cross-site scripting vulnerabilities to intercept keystrokes, mouse clicks, cookies from a victim.	MC LF SC	MC LF P

Appendix G: Embedded and Peripheral Devices

ID	Skill	Details	CCSAM	CCSAS
G1	Identification and exploitation of embedded devices	The ability to find potentially interesting embedded devices (e.g. video conferencing equipment, VoIP telephones, door access systems) on a network and subsequently exploit to gain unauthorised access to the device. Expected techniques include eavesdropping, password guessing attacks, exploitation of the embedded operating system and exploitation of any other exposed services (e.g. databases etc.)	MC LF SC	MC LF P
G2	Identification and remote control of peripheral devices	The ability to detect the presence of microphones and webcams and remotely control the device to obtain audio and video capture without the victim's knowledge.	MC LF SC	MC LF P
G3	Key Logging	The ability to intercept both keystrokes and mouse clicks without the victim's knowledge.	MC LF SC	MC LF P

Appendix H: Implant Creation

ID	Skill	Details	CCSAM	CCSAS
H1	Implant Design	Implant design, considering (for example): • Engagement scope and target assets • Appropriate implant types • Available exfiltration techniques, data security and viability of exfiltration routes • Evasion techniques required • Pivoting requirements	MC SC	MC LF
H2	Win32 Implant Creation	Knowledge of implant creation techniques for Microsoft Windows systems, including: • Implant design and functionality • Built-in operating system functionality and custom code creation • AV/Anti-Malware evasion techniques • Pivoting / proliferation requirements • Safe gathering / exfiltration of target data • Operating system defence bypass	MC	MC LF
H3	VBA Macro Creation	Knowledge of malicious VBA macro creation, including: • Inherent capabilities • Limitations of the technique • Defensive capabilities and bypass techniques • Exfiltration options	MC	MC LF
H4	Operating System Bootstrap	Ability to run an arbitrary Win32 executable upon reboot of a Microsoft Windows operating system using common registry 'autorun' locations.	MC LF	MC LF P
H5	USB 'Autorun'	Ability to execute an arbitrary Win32 executable upon insertion of a USB stick into a insecurely configured Microsoft Windows workstation.	MC LF	MC LF P
H6	Physical Implants	Knowledge of physical implants that can be used to intercept keystrokes, video and mouse actions. Egress of information via such devices (e.g. 3G/4G, WiFi etc.)	MC LF	MC LF

Appendix I: Evasion

ID	Skill	Details	CCSAM	CCSAS
I1	Antivirus Detection Evasion	Ability to take a known hacking tool which is flagged as malicious by antivirus and re-engineer the binary to evade detection using a variety of methods: • Packing • Encoding/obfuscation • Recompiling It is expected the candidate should be able to accomplish this task without modification of the original functionality of the tool. Practical examinations will include use of the five most commonly used commercial products.	MC LF	MC LF P
I2	Disable/Re-Enable Antivirus	Be able to disable and subsequently re-enable antivirus using a variety of methods given 'administrator' level access on a Microsoft Windows workstation.	MC	MC LF P
I3	Port Scanning	The ability to enumerate open ports without triggering IDS alerts by throttling network requests to the target and other evasion techniques	MC LF	MC LF P
I4	Operating System Defences	Knowledge of common operating system defensive capabilities, including: • Software Restriction Policies • AppLocker • Lumension Sanctuary • AppArmor • Third-party endpoint protection suites	MC LF	MC LF P
I5	Perimeter Controls	Enumeration and evasion of SMTP and HTTP proxy perimeter filtering and antivirus defences.	MC LF	MC LF P
I6	IDS Evasion	The ability to evade common IDS configurations that may be triggered by simulated attack attempts.	MC LF	MC LF P

Appendix J: Egress/Command and Control

ID	Skill	Details	CCSAM	CCSAS
J1	Outbound Firewall Rules	Enumerate all outbound (egress) perimeter firewall rules and determine protocols that are permitted to traverse the firewall.	MC LF	MC LF P
J2	Reverse Shell	Demonstrate the ability to establish an outbound reverse TCP/UDP shell from a compromised Microsoft Windows workstation through a well configured perimeter firewall.	MC	MC LF P
J3	Tunnelling	Knowledge of various protocols that can be used for tunnelling arbitrary traffic out of a network, and typical limitations. Example protocols include DNS, various messaging protocols (e.g. SMTP, IRC), 6in4/6to4, HTTP(S) traffic via a proxy etc.	MC LF SC	MC LF P
J4	Attack Source Obfuscation	Knowledge of various techniques that can be used to obfuscate or 'spoof' the source of an attack. For example, the use of multiple proxies, TOR and other anonymising networks to impede attribution.	MC LF SC	MC LF
J5	Secure Egress	Knowledge of risks associated with egress/C2C channels, and demonstration of security considerations to protect channels from attack. Practical use of encryption to ensure the confidentiality of exfiltrated data.	MC LF SC	MC LF P