Assessors Panel

CREST Certified Tester - Infrastructure (CCT-INF) Syllabus

Issued by	CREST Assessors Panel
Document Reference	
Version Number	
Status	
Issue Date	

Table of Contents

Table of Contents 2
1 Introduction 3
2 Certification Examination Structure 4
3 Syllabus Structure 5
Appendix A - Soft Skills and Assessment Management (PT001) 6
Appendix B - Core Technical Skills (PT002) 11
Appendix C - Internet Information Gathering and Reconnaissance (PT003) 14
Appendix D - Networks (PT004) 16
Appendix E - Network Services (PT005) 22
Appendix F - Microsoft Windows Security Assessment (PT006) 30
Appendix G - Linux / UNIX Security Assessment (PT007) 34
Appendix H - Web Technologies (PT008) 37
Appendix I - Databases (PT009) 45
Appendix J - Virtualisation (PT010) 48
Appendix K - Containerisation (PT011) 49
Appendix L - Cloud Security (PT012) 52
Appendix M - Physical Security (PT014) 53
Appendix N - Secure Development Operations (PT015) 55

1 Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the CREST Certified Tester - Infrastructure exam (CCT INF).

CREST Certified Tester - Infrastructure (CCT INF)

The CCT INF examination tests candidates' knowledge and expertise in assessing operating systems, common network services and general network infrastructure security.

The Certification Examinations also covers a common set of core skills and knowledge; success will confer CREST Certified Tester - Infrastructure status to the individual.

2 Certification Examination Structure

CREST Certified Tester - Infrastructure (CCT INF)

The Certification Examination has three components: multiple choice theory paper, a written scenario paper and a practical assualt course. The multiple choice paper tests a candidates knowledge of the subject and the scenario paper assesses a cadidates ability to write reports. The practical assualt course tests candidates' hands-on penetration testing methodology and skills against reference networks, hosts and applications.

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

3 Syllabus Structure

The syllabus is divided into topics, each of which is subdivided into specific skill areas.

For each skill area, CREST has indicated where and how the area will be assessed: multiple choice theory, written scenario, or practical assualt course.

Appendix A - Soft Skills and Assessment Management (PT001)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
A1	PT001.01	Engagement Lifecycle	Understanding of the penetration testing life-cycle, from the initial client contact, to the delivery of the final report and subsequent consultancy work. Understands the structure of a penetration test, including all relevant processes and procedures. Understands penetration testing methodologies and follows these when required. These include methodologies defined by the tester's employer, together with recognised standards, such as OWASP. Understands the concepts of different types of penetration test, such as infrastructure and application, white and black-box, intelligence led and red team. Can explain the benefits a penetration test will bring to a client. Can accurately convey the results of the penetration testing in a verbal debrief and written report.		√	√
A2	PT001.02	Law and Compliance	Awareness of local legislation pertaining to penetration testing. 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.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
A3	PT001.03	Law and Compliance (UK)	Knowledge of pertinent UK legislation: • Police and Criminal Evidence Act 1984 • Computer Misuse Act 1990 and amendments • Human Rights Act 1998 • Data Protection Act 1998 • Police and Justice Act 2006 • Investigatory Powers Act 2016 • Data Protection Act 2018 Understanding the impact of this legislation on penetration testing activities. Awareness of NCSC Cyber Assessment Framework guidance, specifically NIS B4.d. (Vulnerability Management). Can provide examples of compliance and non-compliance.		√	√
A4	PT001.04	Scoping	Understands client requirements and can produce an accurate and adequately resourced penetration testing scope. Understands technical, logistical, financial and other constraints, and is able to take these into account without compromising the effectiveness of the penetration test.		√	√
A5	PT001.05	Managing Risk	Understands the risks associated with a penetration test, the usual outcomes of such risks materialising and how to mitigate the risks. Understands the importance of availability and how the risk of a denial of service can be reduced. Understands the ethical issues and associated risks related to penetration testing.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
A6	PT001.07	Client Communications	Defining daily checkpoints, escalation paths and emergency contacts as appropriate. Defining regular updates for stakeholders. Understanding of secure email communications such as S/MIME and PGP. Understanding of secure out-of-band communication channels.		√	√
A7	PT001.08	Record Keeping	Understands the record keeping requirements mandated by internal and external standards. Understands the importance of accurate and structured record keeping during the engagement, including the output of tools. Understands the security requirements associated with record keeping, both during the penetration test and following the delivery of the final report. Can create records such that a report can be written based on the data recorded.		√	√
A8	PT001.10	Reporting (Basic)	Understands the reporting requirements mandated by the client, internal and external standards. Ability to classify findings using distinct risk levels (e.g. HIGH, MEDIUM, LOW, etc.) Understands risk in relation to the confidentiality, integrity, and availability of a system and its data. Can interpret and understand versions 2 and 3.x of the Common Vulnerability Scoring System (CVSS)		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
A9	PT001.11	Reporting	Ability to report attack chains made up of multiple vulnerabilities. Ability to convey both a verbal and written summary of a penetration test to technical and non-technical audiences. For any given issue or group of issues, ability to convey: • A risk classification • A list of affected components • A detailed description of the problem • A description of the risk posed in terms of Confidentiality, Integrity and Availability of the system and its data. • The potential impact to the customer's information systems and data preferably in terms of confidentiality, integrity and availability. • The cause of the issue (e.g. misconfiguration, human error, software vulnerability) • Which type of attacker would most likely exploit the issue (e.g. authorised internal user, external Internet connected anonymous user, attacker with physical access etc.) • The difficulty and likelihood of a successful exploit • Possible sources of further information • Detailed recommendations for remediation, with product specific knowledge where possible and providing suitable general recommendations where not.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
A10	PT001.14	Platform Preparation	Ability to prepare the required hardware and software for a penetration test. Ensures all necessary hardware is available, including laptops, switches, media-converters, wireless devices and cabling. Ensures all operating system and testing tools are relevant and up-to-date. Takes steps to avoid data cross-contamination, e.g. by sanitising a hard disk prior to deployment or taking an image from a master build. Ensures all commercial software is suitably licensed. Ensures sufficient Anti-Virus software is installed and is sufficiently up-to-date.		√	√

Appendix B - Core Technical Skills (PT002)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
B1	PT002.01	Using Tools and Interpreting Output	Can use a variety of tools during a penetration test, selecting the most appropriate tool to meet a particular requirement. Can interpret and understand the output of tools, including those used for port scanning, vulnerability scanning, enumeration, exploitation and traffic capture.	√	√	√
B2	PT002.02	Pivoting	Understand the concept of pivoting through compromised devices. Can demonstrate pivoting through a number of devices in order to gain access to targets on a distant subnet.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
B3	PT002.03	Cryptography	Understands cryptography and its use in a networked environment. Understands common encrypted protocols and software applications, such as SSH, SSL, IPsec and PGP. Understands wireless protocols that support cryptographic functions, including: WEP; WPA; WPA2; TKIP; EAP; LEAP; PEAP Understands their associated security attributes and how they can be attacked. Understands the differences between symmetric and asymmetric cryptography and can give examples of each. Understands common cryptographic algorithms, such as DES, 3DES, RSA, RC4 and AES, including their security attributes and how they can be attacked. Understands common hash functions, such as MD5, SHA1 and SHA256 including their security attributes and how they can be attacked. Understands different authentication methods such as passwords and certificates. Understands the generation and role of HMACs. Understands PKI and the concepts of Certificate Authorities and trusted third parties. Understands the difference between encoding and encrypting.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
B4	PT002.04	Hardware Security	Understands the concepts behind common microprocessor vulnerabilities such as Spectre and Meltdown Understands the concepts behind side-channel attacks such as timing analysis and power analysis Understands how side-channel attacks can aid cryptanalysis and otherwise expose sensitive data Understands common risks associated with Bluetooth, including: • Bluesnarfing • Bluejacking • Bluebugging	√	√	√
B5	PT002.05	OS Fingerprinting	Understands active and passive operating system fingerprinting techniques and can demonstrate their use during a penetration test.	√	√	√

Appendix C - Internet Information Gathering and Reconnaissance (PT003)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
C1	PT003.01	Domain Registration	Understands the format of a WHOIS record and can obtain such a record to derive information about an IP address and/or domain.		√	√
C2	PT003.02	DNS	Understands the Domain Name Service (DNS) including queries and responses, zone transfers, and the structure and purpose of records, including: • SOA • NS • MX • A • AAAA • CNAME • PTR • TXT (including use in DMARC policies) • HINFO • SVR Can demonstrate how a DNS server can be queried to obtain the information detailed in these records. Can demonstrate how a DNS server can be queried to reveal other information that might reveal target systems or indicate the presence of security vulnerabilities. Can identify the presence of dangling DNS entries and understands the associated security vulnerabilities (e.g. susceptibility to subdomain takeover). Passive DNS monitoring.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
C3	PT003.03	Web Site Analysis	Can interrogate a website to obtain information about a target network, such as the name and contact details of the network administrator. Can analyse information from a target web site, both from displayed content and from within the HTML source.		√	√
C4	PT003.04	Search Engines	Effective use of search engines and other public data sources to gain information about a target. Knowledge and experience using specialist 'service' search engines (e.g. Shodan).		√	√
C5	PT003.05	News Groups and Mailing Lists	Can use news groups, mailing lists and other services to obtain information about a target network, such as the name and contact details of the network administrator. Can analyse email headers to identify system information.		√	√
C6	PT003.06	Information Leakage	Can obtain information about a target network, such as an internal network IP addresses, from information leaked in email headers, HTML meta tags and other locations.		√	√
C7	PT003.07	Social Media	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.		√	√
C8	PT003.08	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.)		√	√

Appendix D - Networks (PT004)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
D1	PT004.01	Network Connections	Can use common network connections that could be required during a penetration test: • Ethernet (copper and fibre) • Wifi (IEEE 802.11.a,b,g,n,ac,ax) • Ethernet VLANs	√	√	√
D2	PT004.02	Ethernet Protocol	Basic understanding of how the Ethernet Protocol works. Can spoof MAC addresses to bypass security restrictions and facilitate man in the middle attacks.	√	√	√
D3	PT004.03	Common Ethernet Protocols	Understands security issues relating to the following ethernet protocols: • CDP • LLDP • VTP • STP	√	√	√
D4	PT004.04	VLAN Tagging	Understands VLAN tagging (IEEE 802.1Q). Understands the security implications of VLAN tagging. Can connect a specific VLAN given the VLAN ID from both Linux and Windows systems. Can identify and analyse VLAN tagged traffic on a network.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
D5	PT004.05	IPv4	Basic understanding of how the IPv4 protocol works. Ability to configure interfaces with IP addresses both statically and using DHCP. Can perform host discovery using ARP and ICMP. Ability to understand and configure IP routing. Ability to perform standard penetration testing activities including network mapping, port scanning, and service exploitation. Awareness of common protocols that use IPv4 e.g. ICMP, IGMP, TCP, UDP. Awareness of IPsec.	√	√	√
D6	PT004.06	IPv6	Basic understanding of how the IPv6 protocol works. Ability to configure interfaces with IP addresses both statically, with DHCPv6 and with SLAAC. Ability to perform host discovery using the Neighbor Discovery Protocol and well known multicast addresses. Ability to understand and configure IP routing manually or with Router Advertisements. Ability to perform standard penetration testing activities including network mapping, port scanning, and service exploitation. Awareness of common protocols that use IPv6 e.g. ICMPv6, TCP, UDP. Awareness of IPsec.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
D7	PT004.07	IPv4 and IPv6 Packet Manipulation	Understands components of IP packets. Can arbitrarily modify IP packet parameters, including source and destination IP addresses and TTL values, to bypass security controls and perform man in the middle attacks. Can parameters of various packet types, including TCP, UDP, ICMP and ARP. Understands and can perform ARP spoofing safely and reliably to bypass security controls and facilitate man in the middle attacks. Understands packet fragmentation.	√	√	√
D8	PT004.08	Network Routing Protocols	Understands common network routing protocols including: • RIP • OSPF • EIGRP • BGP • IGMP Understands the security attributes of these protocols and how they can be used by attackers. Ability to manipulate these protocols to perform traffic capture and man in the middle attacks.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
D9	PT004.09	Network Architecture	Can interpret logical network diagrams. Understands the security benefits of tiered architectures, DMZs and air gaps. Understands the security implications of shared media. Understands the security implications of switched networks. Understands the security implications of VLANS. Understands the core principles and concepts of a Software Defined Network (SDN), including: • Disassociation of data plane and control plane • The role of controllers in the control plane and commonly associated weaknesses • The role and common security risks of the application plane, the northbound API and common SDN applications	√	√	√
D10	PT004.10	Network Mapping	Can demonstrate the mapping of a network using a range of tools, such as traceroute, traceroute and ping, and by querying active searches, such as DNS and SNMP servers. Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices. Can accurately identify all hosts on a target network that meet a defined set of criteria, e.g. to identify all FTP servers or Cisco routers.	√	√	√
D11	PT004.12	Network Devices	Analysing the configuration of the following types of network equipment: • Routers • Switches • Firewalls	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
D12	PT004.13	Network Filtering	Understands network traffic filtering and where this may occur in a network. Understands the devices and technology that implement traffic filtering, such as firewalls, and can advise on their configuration. Can demonstrate methods by which traffic filters can be bypassed.	√	√	√
D13	PT004.14	Traffic Analysis	Can intercept and monitor network traffic, capturing it to disk in a format required by analysis tools (e.g. PCAP). Understands and can demonstrate how network traffic can be analysed to recover user account credentials and detect vulnerabilities that may lead to the compromise of a target device. Can analyse network traffic stored in PCAP files.	√	√	√
D14	PT004.16	TCP	Understands how TCP works and its relationship with IP protocols and higher level protocols. Understands different TCP connection states. Understands and can demonstrate active techniques for discovery of TCP services on a network, such as: • SYN and Connect scanning • FIN/NULL and XMAS scanning	√	√	√
D15	PT004.17	UDP	Understands how UDP works and its relationship with IP protocols and higher level protocols. Understands different UDP connection states. Understands and can demonstrate active techniques for discovery of UDP services on a network.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
D16	PT004.20	Network Access Controls	Understands network access control systems, such as 802.1x and MAC address filtering, and can demonstrate how these technologies can be bypassed.	√	√	√
D17	PT004.21	Wifi	Enumeration and fingerprinting of devices running Wireless (802.11) services. Knowledge of various options for encryption and authentication, and the relative methods of each. • WEP • TKIP • WPA/WPA2 • EAP/LEAP/PEAP Understands how wifi networks can be attacked.		√	√
D18	PT004.22	Service Identification	Can identify the network services offered by a host by banner inspection. Can state the purpose of an identified network service and determine its type and version. Understands the methods associated with unknown service identification, enumeration and validation. Evaluation of unknown services and protocols.	√	√	√
D19	PT004.23	Host Discovery	Can identify targets on common networks using active and passive fingerprinting techniques and can demonstrate their use.	√	√	√

Appendix E - Network Services (PT005)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E1	PT005.01	Unknown Services	Understands advanced analysis techniques for unknown services and protocols. Can create simple bespoke scripts for exploiting unknown services that use techniques including: • Username enumeration • Credential brute forcing • Variations on existing publically available exploits	√	√	√
E2	PT005.02	Unencrypted Services	Understands how unencrypted services can be exploited. Can identify unencrypted services on the network and capture sensitive data. Is aware of common unencrypted services including: • Telnet • FTP • SNMP • HTTP	√	√	√
E3	PT005.03	TLS / SSL	Understands the use of TLS and SSL in protecting data in transit. Is aware of SSL and TLS protocols and their common weaknesses. Understands the components of cipher suites and their roles. Understands the role of certificates in SSL and TLS. Can identify insecure configurations.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E4	PT005.04	Network Configuration Protocols	Understands and can demonstrate the use of the following network configuration protocols: • DHCP • DHCPv6 • SLAAC Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	√	√	√
E5	PT005.05	Network Redundancy Protocols	Understands and can demonstrate the use of the following redundancy protocols: • HSRP • VRRP Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E6	PT005.06	Name Resolution Services	Understands and can demonstrate the use of the following name resolution services: • DNS • NetBIOS / WINS • WINS • LLMNR • mDNS Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network. Understands the Domain Name Service (DNS) including queries and responses, zone transfers, and the structure and purpose of records, including: • SOA • NS • MX • A • AAAA • CNAME • PTR • TXT (including use in DMARC policies) • HINFO • SVR	√	√	√
E7	PT005.07	Network Authentication	Understands and can demonstrate the use of the following network authentication protocols: • TACACS+ • RADIUS • LDAP • Kerberos Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E8	PT005.08	Management Services	Understands and can demonstrate the use of the following network management services: • Telnet • Cisco Reverse Telnet • SSH • HTTP • Remote Powershell • WMI • WinRM • RDP • VNC • X Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	√	√	√
E9	PT005.09	Desktop Access	Is aware of common protocols used to provide remote access to desktop services including: • RDP • VNC • XDMCP • X Understands the security attributes of the above protocols and technologies. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.	√	√	√
E10	PT005.10	IPsec	Enumeration and fingerprinting of devices running IPsec services.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E11	PT005.11	FTP	Understands FTP and can demonstrate how a poorly configured FTP server can be exploited, e.g. the downloading of arbitrary files, the uploading and over-writing of files, and the modification of file system permissions. Understands the security implications of anonymous FTP access Understands FTP access control.	√	√	√
E12	PT005.12	TFTP	Understands TFTP and can demonstrate how a poorly configured TFTP server can be exploited, e.g. the downloading of arbitrary files. the uploading over-writing of files. Understands and can exploit TFTP within a Cisco environment.	√	√	√
E13	PT005.13	SNMP	Understands the difference between versions 1, 2c, and 3. Can enumerate information from targets including: • users • processes • network configuration Understands the MIB structure pertaining to the identification of security vulnerabilities. Understands the security attributes of SNMP. Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network. Understands how to extract and replace configuration files of Cisco devices.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E14	PT005.14	SSH	Understands SSH and its associated security attributes, including the different versions of the protocol, version fingerprinting and how the service can be used to provide a number of remote access services. Can demonstrate how trust relationships can lead to the compromise of a server, allow a user to escalate privileges and/or gain further access to a host, e.g. through the use, creation or modification of --/.ssh/authorized_keys files. Understands authentication mechanisms used by SSH.	√	√	√
E15	PT005.15	NFS	Understands NFS and its associated security attributes and can demonstrate how exports can be identified. Can demonstrate how a poorly configured NFS service can lead to the compromise of a server, allow a user to escalate privileges and/or gain further access to a host, e.g. through the creation of SUID-root files, the modification of files and file system permissions, and UID/GID manipulation. Understands the concepts of root squashing, nosuid and noexec options Understands how NFS exports can be restricted at both a host and file level	√	√	√
E16	PT005.16	SMB	Is aware of common SMB implementations including: • Windows File Shares • Samba Can identify and analyse accessible SMB shares.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E17	PT005.17	LDAP	Is aware of common LDAP implementations including: • Windows Active Directory • OpenLDAP Can enumerate LDAP directories and extract arbitrary data including: • usernames and groups • target system names	√	√	√
E18	PT005.18	Berkeley R* Services	Understands the Berkeley r-services and their associated security attributes and can demonstrate how trust relationships can: • lead to the compromise of a server • allow a user to escalate privileges and/or gain further access to a host, e.g. through the use, creation or modification of .rhosts and/or /etc/hosts.equiv files. Can perform user enumeration using the rwho and rusers services.	√	√	√
E19	PT005.19	X	Understands X and its associated security attributes, and can demonstrate how insecure sessions can be exploited, e.g.. by obtaining screen shots, capturing keystrokes and injecting commands into open terminals. Understands X authentication mechanisms. Understands the difference between host based and user based access control.	√	√	√
E20	PT005.20	Finger	Understands how finger daemon derives the information that it returns, and hence how it can be abused. Enumeration of usernames.	√	√	√
E21	PT005.21	RPC Services	Can perform RPC service enumeration. Is aware of common RPC services. Is aware of and can exploit recent or commonly-found RPC service vulnerabilities.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
E22	PT005.22	NTP	Understands the function of NTP and the importance of it for logging and authentication. Can extract information about the target network from NTP services.	√	√	√
E23	PT005.23	IPMI	Understands and can demonstrate use of IPMI for the remote management of devices, such as HP ILO and Dell DRAC. Understands the security attributes of IPMI. Can exploit common vulnerabilities to gain access to a device.	√	√	√
E24	PT005.24	VoIP	Enumeration and fingerprinting of devices running VoIP services. Knowledge of the SIP protocol.	√	√	√
E25	PT005.25	SMTP and Mail Servers	Understands and can demonstrate valid username discovery via EXPN and VRFY. Awareness of recent vulnerabilities in mail server applications (e.g. Postfix and Exchange) and the ability to exploit them if possible Understands mail relaying.	√	√	√
E26	PT005.26	Vulnerable Services	Can identify and remotely exploit services with recent or well known public vulnerabilities.			

Appendix F - Microsoft Windows Security Assessment (PT006)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
F1	PT006.01	Windows Reconnaissance	Can identify Windows hosts on a target network. Can identify forests, domains, domain controllers, domain members and workgroups. Can enumerate accessible Windows shares. Can identify and analyse internal browse lists.	√	√	√
F2	PT006.02	Windows Network Enumeration	Can perform user and group enumeration on target systems and domains, using various protocols and methods including: • NetBIOS • LDAP • SNMP • RID Cycling Can obtain other information, such as password policies.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
F3	PT006.03	Active Directory	Understands Active Directory structure Understands Active Directory roles (Global Catalogue, Master Browser, FSMO) Understands Group Policy. Understands user accounts and can manipulate these accounts to gain further access to a target system, e.g. by escalating privileges from a domain user to a domain admin. Understands the reliance of Active Directory on DNS and LDAP. Understands the role of Kerberos within Active Directory. Understands and can identify the different types of domain trusts, including: • One-way and two-way trusts • Explicit and transitive trusts	√	√	√
F4	PT006.04	Active Directory Enumeration	Can enumerate information from Active Directory including: • Users • Groups • Computers • Trusts • Service Principle Names	√	√	√
F5	PT006.05	Windows Passwords	Understands password policies, including complexity requirements and lock-out. Understands how to avoid causing a denial of service by locking-out accounts. Understands Windows password hashing algorithms, the merits of each algorithm, and their associated security attributes. Understands how passwords are stored and protected and can demonstrate how they can be recovered. Understands and can demonstrate off-line password cracking using dictionary and brute- force attacks, including the use of rainbow tables.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
F6	PT006.06	Windows Processes	Can identify running processes and exploit vulnerabilities to escalate privileges. Understands and can exploit DLL loading mechanisms to escalate privileges.	√	√	√
F7	PT006.07	Windows File Permissions	Understands and can demonstrate the manipulation of file system permissions on Windows operating systems. Understands how insecure file system permissions can be exploited to escalate privileges and/or gain further access to a host. Can identify files with insecure or "unusual" permissions that can be exploited.	√	√	√
F8	PT006.08	Registry	Understands and can demonstrate the detection and manipulation of weak registry ACLs. Can extract data from registry keys.	√	√	√
F9	PT006.09	Windows Remote Exploitation	Understands and can demonstrate the remote exploitation of Windows operating system and third-party software application vulnerabilities.	√	√	√
F10	PT006.10	Windows Advanced Remote Exploitation	Understands the use of tools and techniques to identify new OS and software vulnerabilities. Understands the techniques used to develop exploit code for existing and new vulnerabilities.	√	√	√
F11	PT006.11	Windows Local Exploitation	Understands and can demonstrate the local exploitation of Windows operating system and third-party software application vulnerabilities. Understands and can demonstrate local privilege escalation techniques, e.g. through the manipulation of insecure file system or service permissions	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
F12	PT006.12	Advanced Local Exploitation	Understands the use of tools and techniques to identify new OS and software vulnerabilities. Understands the techniques used to develop exploit code for existing and new vulnerabilities.	√	√	√
F13	PT006.13	Windows Post Exploitation	Understands and can perform common post exploitation activities, including: • obtaining password hashes, both from the local SAM and cached credentials or obtaining locally stored clear-text passwords • cracking password hashes • obtaining patch levels • deriving a list of missing security patches • reverting to a previous state • lateral and horizontal movement	√	√	√
F14	PT006.14	Windows Patch Management	Understands common windows patch management strategies, including: • SMS • SUS • WSUS	√	√	√
F15	PT006.15	Windows Desktop Lockdown	Understands and can demonstrate techniques to break out of a locked down Windows desktop or Citrix environment. Can perform privilege escalation techniques from a desktop environment.	√	√	√
F16	PT006.17	Common Windows Applications	Knowledge of significant vulnerabilities in common windows applications for which there is public exploit code available.	√	√	√

Appendix G - Linux / UNIX Security Assessment (PT007)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
G1	PT007.01	Linux / UNIX Reconnaissance	Can identify Linux / UNIX hosts on a network.	√	√	√
G2	PT007.02	Linux / UNIX Network Enumeration	Can demonstrate and explain the enumeration of data from a variety of common network services on various platforms including: • Filesystems or resources shared remotely, such as NFS and SMB • SMTP • SSH • Telnet • SNMP Is aware of legacy user enumeration techniques such as rusers, rwho and finger. Can enumerate RPC services and identify those with known security vulnerabilities.	√	√	√
G3	PT007.03	Linux / UNIX Passwords	Understands users, groups and password policies, including complexity requirements and lock out. Understands how to avoid causing a denial of service by locking out accounts. Understands the format of the passwd, shadow, group and gshadow files. Understands UNIX password hashing algorithms and their associated security attributes. Understands how passwords are stored and protected and can demonstrate how they can be recovered. Understands and can demonstrate off-line password cracking using dictionary and brute force attacks. Can demonstrate the recovery of password hashes when given physical access to a Linux / UNIX host.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
G4	PT007.04	Linux / UNIX File Permissions	Understands and can demonstrate the manipulation of file system permission on Linux and UNIX operating systems. Understands how insecure file system permissions can be exploited to escalate privileges and/or gain further access to a host. Can find "interesting' files on an operating system, e.g. those with insecure or "unusual" permissions, or containing user account passwords.	√	√	√
G5	PT007.05	Linux / UNIX Processes	Can identify running processes on Linux / UNIX hosts and exploit vulnerabilities to escalate privileges. Understands and can exploit shared library loading mechanisms to escalate privileges.		√	
G6	PT007.06	Linux / UNIX Remote Exploitation	Understands and can demonstrate the remote exploitation of Linux and UNIX systems including: • Solaris • Linux • FreeBSD • OpenBSD		√	
G7	PT007.07	Linux / UNIX Local Exploitation	Understands and can demonstrate the local exploitation of Solaris, Linux and *BSD operating system vulnerabilities. Understands and can demonstrate Local privilege escalation techniques, e.g. through the manipulation of insecure file system permissions.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
G8	PT007.08	Linux / UNIX Post Exploitation	Understands and can demonstrate common post-exploitation activities, including: • obtaining locally stored clear-text passwords • password recovery (exfiltration and cracking) • lateral movement • checking OS and third party software application patch levels • deriving a list of missing security patches • reversion of OS and software components to previous state	√	√	√

Appendix H - Web Technologies (PT008)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H1	PT008.01	Web Servers	Can identify web servers on a target network and can remotely determine their type and version. Understands the various mechanisms web servers use for hosting applications, including: • virtual hosts • multiple ports • application specific URLs Understands and can demonstrate the remote exploitation of web servers. Understands the concepts of web proxies. Understands the purpose, operation, limitation and security attributes of web proxy servers.		√	
H2	PT008.02	Web Application Frameworks	Can identify common application frameworks and technologies, including: • .NET • J2EE • Coldfusion • Ruby on Rails • NodeJS • Django • Flask Is aware of and can exploit vulnerabilities in common application frameworks and technologies.		√	√
H3	PT008.03	Common Web Applications	Can identify common web applications and exploit well known vulnerbilities.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H4	PT008.04	Web Protocols	Understands and can demonstrate the use of web protocols, including: • HTTP / HTTPS • WebSockets Understands all HTTP methods and response codes. Understands HTTP header fields relating to security features.		√	√
H5	PT008.05	Mark Up Languages	Understands common web mark up languages, including: • HTML • XHTML • XML		√	√
H6	PT008.06	Web Languages	Understands common web programming languages, including: • ASP .NET • ASP Classic • Perl • PHP • Java / JSP • Python • JavaScript Understands and can demonstrate how the insecure implementation of software developed using these languages can be exploited.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H7	PT008.07	Web APIs	Understands and can demonstrate the use of web based APIs to remotely access remote services. Understands the concepts behind SOAP, REST and GraphQL APIs. Can demonstrate the use of relevant tools to test APIs, e.g. SoapUI and Postman. Understands common authentication techniques used in web APIs, e.g. API keys. Understands and can demonstrate how the insecure implementation of web-based APIs can be exploited. Understands different common payload formats such as XML and JSON. Understands how to interpret definition files, e.g. WSDL and Swagger.		√	√
H8	PT008.08	Web Sub Components	Understands Web architecture sub-components including: • Active X • Flash • .NET Silverlight • Java Applets Can decompile and analyse the client side code.		√	√
H9	PT008.09	Web Application Reconnaissance	Can use spidering tools and understands their relevance in a web application test for discovering linked content. Understands and can demonstrate forced browsing techniques to discover default or unlinked content. Can identify functionality within client-side code.		√	√
H10	PT008.10	Web Threat Modelling and Attack Vectors	Simple threat modelling based on customer perception of risk. Relate functionality offered by the application to potential attack vectors.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H11	PT008.11	Information Gathering	Can gather information from a web site and application mark up or application code, including: • hidden form fields • database connection strings • user account credentials • developer comments • external and/or authenticated-only URLs. Can gather information about a web site and application from the error messages it generates.		√	√
H12	PT008.12	Web Authentication	Understands common authentication mechanisms and their security issues, including: • HTML Form Fields • kerberos • NTLM • OpenID Connect • SAML Understands common authentication vulnerabilities, including: • Transport of credentials over an unencrypted channel • Username enumeration • Brute force password attacks • Authentication bypass • Insecure password reset features • Insufficient logout timeout/functionality • Vulnerable CAPTCHA controls • Race Conditions • Lack of MFA		√	√
H13	PT008.13	Web Authorisation	Understands common pitfalls associated with the design and implementation of application authorisation mechanisms.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H14	PT008.14	Input Validation	The importance of input validation as part of a defensive coding strategy. How input validation can be implemented and the differences between allow list, deny list and data sanitisation. Understands the need for server side validation and the flaws associated with client-side validation.		√	√
H15	PT008.15	Web Application Fuzzing	Understands fuzzing and its use in web application testing. Understands the generation of fuzzing strings and their potential effects, including the dangers they may introduce.		√	√
H16	PT008.16	Cross Site Scripting	Understands cross site scripting (XSS) and can demonstrate the launching of a successful XSS attack. Understands the difference between persistent, reflected and DOM based XSS. Can use XSS to perform arbitrary JavaScript execution to obtain sensitive information from other users.		√	√
H17	PT008.17	SQL Injection	Determine the existence of an SQL injection condition in a web application. Determine the existence of a blind SQL injection condition in a web application. Can exploit SQL injection to execute arbitrary SQL commands in a database.		√	√
H18	PT008.18	ORM Injection	Can demonstrate the ability to identify, explain and prove the existence of ORM injection in a web application.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H19	PT008.19	XML Related Injection	Can demonstrate the ability to identify, explain and prove the existence of the following types of XML related injection in a web application: • XML Injection • XXE Injection • XPath Injection		√	√
H20	PT008.20	LDAP Injection	Can demonstrate the ability to identify, explain and prove the existence of LDAP injection in a web application. Can exploit LDAP injection to extract arbitrary data from an LDAP directory.		√	√
H21	PT008.21	SSI Injection	Can demonstrate the ability to identify, explain and prove the existence of SSI injection in a web application.		√	√
H22	PT008.22	Mail Injection	Can demonstrate the ability to identify, explain and prove the existence of the following types of mail related injection in a web application: • SMTP injection • IMAP injection		√	√
H23	PT008.23	Code Injection	Can demonstrate the ability to identify, explain and prove the existence of script code injection in a web application built with common web scripting languages.		√	√
H24	PT008.24	OS Command Injection	Can demonstrate the ability to identify, explain and prove the existence of OS command injection in a web application.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H25	PT008.25	Sessions	Can identify the session control mechanism used within a web application. Can identify the session ID in a web application. Understands the security implications of session IDs exposed in URLs. Can harvest and analyse a number of session identifiers for weaknesses.		√	√
H26	PT008.26	Cookies	Understands how cookies work in a web application. Understands cookie attributes and how they can affect the security of a web application.		√	√
H27	PT008.27	Session Fixation	Understands and can exploit session fixation vulnerabilities.		√	√
H28	PT008.28	Session Hijacking	Understands and can exploit session hijacking vulnerabilities.		√	√
H29	PT008.29	Cross Site Request Forgery	Understands and can exploit CSRF vulnerabilities. Understands the role of sessions in CSRF attacks.		√	√
H30	PT008.30	Session Puzzling	Understands and can identify and exploit session puzzling (aka variable overloading) vulnerabilities.		√	√
H31	PT008.31	Mass Assignment	Understands and can identify and exploit mass assignment vulnerabilities.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H32	PT008.32	Web Cryptography	Understands how cryptography can be used to protect data in transit and data at rest, both on the server and client side. Understands the concepts of TLS and can determine whether a TLS-enabled web server has been configured in compliance with best practice (i.e. it supports recommended ciphers and key lengths). Identification and exploitation of Encoded values (e.g. Base64). Identification and exploitation of Cryptographic values (e.g. MD5 hashes).		√	√
H33	PT008.33	Web Cryptography Vulnerabilities	Can identify and exploit common cryptography vulnerabilties, such as padding oracle.		√	√
H34	PT008.34	Web Application Man in the Middle	Understands and can perform man in the middle attacks against web applications or web APIs where the connections are unencrypted or TLS encrypted.		√	√
H35	PT008.35	Parameter Manipulation	Understands parameter manipulation techniques, particularly the use of client-side proxies.		√	√
H36	PT008.36	Directory Traversal	Understands and can identify directory traversal vulnerabilities within applications.		√	√
H37	PT008.37	File Uploads	Understands and can identify common vulnerabilities with file upload capabilities within applications. Understands the role of MIME types in relation to file upload features. Can generate malicious payloads in a variety of common file formats.		√	√
H38	PT008.38	CRLF Attacks	Understands and can demonstrate CRLF attacks, including: • HTTP Splitting • HTTP Smuggling		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
H39	PT008.39	Web Application Logic Flaws	Can assess and exploit vulnerabilities within the functional logic, function access control and business logic of an application.		√	√
H40	PT008.40	Client Side Vulnerabilities	Understands and can demonstrate client side vulnerabilities within web applications, including: • DOM based XSS • HTML injection • URL redirect • CSS injection • Resource manipulation • Cross origin resource sharing • Clickjacking • Web messaging (cross document messaging) • Browser storage • Cross site script inclusion		√	√

Appendix I - Databases (PT009)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
I1	PT009.01	SQL Relational Databases	Can use SQL to interact with relational databases and extract information, e.g. SQLite, PostgreSQL. Understands common connection and authentication methods to connect to SQL databases. Can recognise common database connection string formats, e.g. JDBC, ODBC. Understands and can demonstrate the remote exploitation of common SQL databases. Understands and can demonstrate how access can be gained to a database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).	√	√	√
I2	PT009.02	Microsoft SQL Server	Understands and can demonstrate the remote exploitation of Microsoft SQL Server. Understands and can demonstrate how access can be gained to a Microsoft SQL server through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Following the compromise of Microsoft SQL server, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
I3	PT009.03	Oracle RDBMS	Understands and can demonstrate the remote exploitation of an Oracle RDBMS instance. Understands the security attributes of the Oracle TNS Listener service. Understands and can demonstrate how access can be gained to an Oracle RDBMS through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Can demonstrate how the software version and patch status can obtained from an Oracle database. Following the compromise of an Oracle database, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	√	√	√
I4	PT009.04	MySQL	Understands and can demonstrate the remote exploitation of an MySQL database. Understands and can demonstrate how access can be gained to an MySQL database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Can demonstrate how the software version and patch status can obtained from an MySQL database. Following the compromise of an MySQL database, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
I5	PT009.05	PostgreSQL	Understands and can demonstrate the remote exploitation of an PostgreSQL database. Understands and can demonstrate how access can be gained to an PostgreSQL database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible). Can demonstrate how the software version and patch status can obtained from an PostgreSQL database. Following the compromise of an PostgreSQL database server, can execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host.	√	√	√
I6	PT009.06	NoSQL / Document Databases	Understands and can demonstrate the remote exploitation of common NoSQL / document databases, such as MongoDB. Understands and can demonstrate how access can be gained to such a database through the use of default accounts credentials and insecure passwords. Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).	√	√	√

Appendix J - Virtualisation (PT010)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
J1	PT010.01	Virtualisation Platforms	Can identify use of popular virtualisation technologies, including: • VMware • Microsoft HyperV • Citrix • Oracle VirtualBox • Linux KVM Understands common vulnerabilities found in hypervisors, including: • Exposure of management interface • Use of default or insecure credentials • Common high profile CVEs Understands the inherent risks in shared virtualised environments, e.g. shared memory space	√	√	√
J2	PT010.02	Virtual Machine Escape	Understands and can demonstrate common techniques for escaping a virtualised environment, including: • Directory traversal in shared folders • Virtual device communication breakout • Public CVEs relating to memory corruption	√	√	√
J3	PT010.03	Snapshots	Can demonstrate how to take snapshots and techniques for recovering key sensitive information Understands the security implications of reverting a VM to a previous state Understands the sensitive nature of snapshot files and the need to restrict access	√	√	√

Appendix K - Containerisation (PT011)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
K1	PT011.01	Containers	Understands the key differences between virtualisation and containerisation Understands how containers are isolated from the host system Can identify and interrogate running containers on a host Can identify common vulnerabilities and weaknesses present in containers, including: • Missing security patches • Weak file permissions • Insufficient or lack of resource quotas • Presence of sensitive information in environment variables, running processes or filesystem	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
K2	PT011.02	Docker	Understands how Docker containers are implemented on Linux and Windows. Understands the concepts of layered filesystems and how to extract and analyse specific layers within an image Understands and can analyse Dockerfile files to uncover weaknesses in static images, including: • Use of unencrypted connections for performing downloads • Use of overly generous permissions, e.g. running as the root user • Inclusion of sensitive information, e.g. passwords or private keys o Unnecessary exposure of ports Understands Docker networking and how containers interact with each other and the host networks. Understands and can exploit misconfigurations in containers that can lead to privilege elevation and escaping the container. Understands and can exploit misconfigurations in the environment that could allow malicious containers to be deployed.	√	√	√
K3	PT011.03	Kubernetes	Understands how Kubernetes containers are implemented. Understands Kubernetes networking and how containers interact with each other and the host networks. Understands how Kubernetes containers are managed and deployed. Understands and can exploit misconfigurations in containers that can lead to privilege elevation and escaping the container. Understands and can exploit misconfigurations in the environment that could allow malicious containers to be deployed.	√	√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
K4	PT011.04	LXD	Understands how LXD containers are implemented. Understands LXD networking and how containers interact with each other and the host networks. Understands how LXD containers are managed and deployed. Understands and can exploit misconfigurations in containers that can lead to privilege elevation and escaping the container. Understands and can exploit misconfigurations in the environment that could allow malicious containers to be deployed.	√	√	√

Appendix L - Cloud Security (PT012)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
L1	PT012.01	Penetration Testing Authorisation	Understands the importance of obtaining authorisation from cloud hosting providers and the potential effects on permitted types of testing during engagements.		√	√
L2	PT012.02	Virtual Private Clouds	Understands the concepts of a VPC and the implications on performing security assessments. Can competently assess resources within a private cloud-hosted environment, advising on any necessary temporary changes that may be needed (e.g. creation of bastion hosts, changes to Security Groups / firewalls).	√	√	√
L3	PT012.03	Logging and Monitoring	Can analyse logging configuration within a cloud environment and advise on improvements. Can analyse the configuration of resource monitoring and alarm generation and advise on improvements.	√	√	√
L4	PT012.04	Identity and Access Management	Understands the identity and access management models of popular cloud providers. Can assess roles and policies to identify weaknesses relating to insecure permissions.	√	√	√
L5	PT012.05	Denial of Service and Resource Exhaustion	Understands how (Distributed) Denial of Service attacks are performed and the protective measures available in cloud environments. Understands the financial implications of excessive resource consumption.	√	√	√

Appendix M - Physical Security (PT014)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
M1	PT014.01	Locks	Understands how locks can be used to restrict access to computer hardware.		√	√
M2	PT014.02	Tamper Seals	Understands how tamper seals can be used to deter access to computer hardware.		√	√
M3	PT014.03	Platform Integrity	Understands platform integrity technologies, e.g. TPM.		√	√
M4	PT014.04	Boot Sequence	Understands the BIOS boot sequence and can obtain privileged access to an operating system by exploiting vulnerabilities in a boot sequence configuration, e.g. booting from removable media or enabling PXE boot. Understands how Secure Boot works.		√	√
M5	PT014.05	Disk Encryption	Understands the security implications of unencrypted storage devices, such as hard disks. Can demonstrate how data can be recovered from unencrypted storage devices, and how such data can be manipulated to introduce vulnerabilities into an operating system. Understands the difference between hardware and software disk encryption implementation and the related security implications. Understands the limitations of disk encryption.		√	√
M6	PT014.06	Recovery Functionality	Understands the security attributes of operating system recovery functionality, e.g. Windows Recovery Console and Safe Mode.		√	√

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
M7	PT014.07	Authentication	Understands multi-factor authentication systems, such as tokens and SMS. Understands types of biometrics and how they can be applied. Understands the concept of one-time pads. Understands the use of digital certificates as an authentication mechanism. Understands the concept of contactless RFID smart cards.		√	√

Appendix N - Secure Development Operations (PT015)

ID	Skill ID	Skill	Details	Assault Course	Scenario	Multiple choice
N1	PT015.01	Secure Coding Practices	Understands common insecure programming practices, including: • Use of dangerous functions • Insufficient sanitisation of user-supplied data • Use of outdated third party components • Logic errors		√	√
N2	PT015.02	Security in the Development Lifecycle	Understands the role of automated security testing tools as part of the development process, including: • Static analysis tools (SAST) • Dependency checking tools • Dynamic analysis tools (DAST) Understands how automated tooling can safely and effectively be incorporated into the development pipeline. Can identify and advise on common security misconfigurations of these tools.		√	√
N3	PT015.03	Infrastructure as Code	Understands the role of tools to automate the building, configuration and deployment of infrastructure, including: • Terraform • AWS Cloud Formation • Azure Resource Manager • Puppet • Ansible • Chef Can identify and advise on common security misconfigurations of these tools.	√	√	√
N4	PT015.04	Code Repository Security	Can identify and advise on issues relating to weakly protected code repositories, for example: • Openly exposed repositories containing closed source code • Weak or insufficiently protected credentials Understands the security implications of storing sensitive information in source code repositories, e.g. passwords, private cryptographic keys or API keys.	√	√	√