



## **Assessors Panel**

# **CREST Certified Tester - Infrastructure (CCT-INF) Syllabus**

Version Number	v3
----------------	----

This document and any information therein are confidential property of CREST and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of CREST, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. CREST retain the right to alter the document at any time unless a written statement to the contrary has been appended.

## 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)	13
Appendix D - Networks (PT004)	15
Appendix E - Network Services (PT005)	21
Appendix F - Microsoft Windows Security Assessment (PT006)	28
Appendix G - Linux / UNIX Security Assessment (PT007)	32
Appendix H - Web Technologies (PT008)	35
Appendix I - Databases (PT009)	42
Appendix J - Virtualisation (PT010)	46
Appendix K - Containerisation (PT011)	47
Appendix L - Cloud Security (PT012)	50
Appendix M - Physical Security (PT014)	53
Appendix N - Secure Development Operations (PT015)	55
Appendix O - Windows Desktop Lockdown (PT018)	57
Appendix P - Social Engineering (PT019)	59
Appendix Q - macOS Security Assessment (PT020)	60



# 1 Introduction

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

The CCT INF examination tests candidates' knowledge and expertise in assessing operating systems, common network services and general network infrastructure security as well as Linux, cloud, databases and other web technologies. It also covers a common set of core skills and knowledge.

The successful completion of this examination will confer CREST Certified Tester - Infrastructure status to the individual.



## 2 Certification Examination Structure

CREST Certified Tester - Infrastructure (CCT INF)

The Certification Examination is made of two exams as follows:

- A written exam which is made of two components: a multiple choice test and a written scenario
- A practical exam

The multiple choice component tests a candidates' knowledge of the subject and the scenario assesses a candidates ability to write reports. The practical component 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 which are subdivided into specific skill areas.

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

Candidates preparing for the written exam should then concentrated on the skill areas of the syllabus that are ticked against multiple choice and scenario whilst candidates preparing for the practical exam should focus on the topics marked against this specific exam.

## Appendix A - Soft Skills and Assessment Management (PT001)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
A1	PT001.01	Engagement Lifecycle	<p>Understanding of the penetration testing life-cycle, from the initial client contact, to the delivery of the final report and subsequent consultancy work.</p> <p>Understands the structure of a penetration test, including all relevant processes and procedures.</p> <p>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.</p> <p>Understands the concepts of different types of penetration test, such as infrastructure and application, white and black-box, intelligence led and red team.</p> <p>Can explain the benefits a penetration test will bring to a client.</p> <p>Can accurately convey the results of the penetration testing in a verbal debrief and written report.</p>	√		√
A2	PT001.02	Law and Compliance	<p>Awareness of the legal complexities of dealing with multinational organisations.</p> <p>Awareness of requirements for interaction with law enforcement where appropriate.</p> <p>Understanding of the importance of client confidentiality and non-disclosure agreements.</p>	√		√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
A3	PT001.03	Law and Compliance (Regional)	<p>Knowledge of relevant legislation affecting penetration testing in the candidate's operating jurisdiction(s). Such legislation might include:</p> <ul style="list-style-type: none"> <li>• Legislation concerning computer misuse</li> <li>• Legislation concerning individual's personal data</li> <li>• Legislation affecting penetration testing with or on behalf of a specific sector</li> </ul> <p>Can provide examples of compliance and non-compliance.</p> <p>Knowledge of written authority required to comply with local laws.</p>	√		
A4	PT001.04	Scoping	<p>Understands client requirements and can produce an accurate and adequately resourced penetration testing scope.</p> <p>Understands technical, logistical, financial and other constraints, and is able to take these into account without compromising the effectiveness of the penetration test.</p>	√		√
A5	PT001.05	Managing Risk	<p>Understands the risks associated with a penetration test, the usual outcomes of such risks materialising and how to mitigate the risks.</p> <p>Understands the importance of availability and how the risk of a denial of service can be reduced.</p> <p>Understands the ethical issues and associated risks related to penetration testing.</p>	√		√

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



ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
A9	PT001.11	Reporting	<p>Ability to report attack chains made up of multiple vulnerabilities.</p> <p>Ability to convey both a summary of a penetration test to technical and non-technical audiences.</p> <p>For any given issue or group of issues, ability to convey:</p> <ul style="list-style-type: none"> <li>• A risk classification</li> <li>• A list of affected components</li> <li>• A detailed description of the problem</li> <li>• A description of the risk posed in terms of Confidentiality, Integrity and Availability of the system and its data.</li> <li>• The potential impact to the customer's information systems and data preferably in terms of confidentiality, integrity and availability.</li> <li>• The cause of the issue (e.g. misconfiguration, human error, software vulnerability)</li> <li>• 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.)</li> <li>• The difficulty and likelihood of a successful exploit</li> <li>• Possible sources of further information</li> <li>• Detailed recommendations for remediation</li> </ul>	√		√
A10	PT001.11A	Report QA	<p>Understands security reporting QA and review, able to understand and comment on reporting written by others</p> <p>Can utilise prior work to influence and continue testing and test plans</p>	√		√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
A11	PT001.14	Platform Preparation	<p>Ability to prepare the required hardware and software for a penetration test.</p> <p>Ensures all necessary hardware is available, including laptops, switches, media-converters, wireless devices and cabling.</p> <p>Ensures all operating system and testing tools are relevant and up-to-date.</p> <p>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.</p> <p>Ensures all commercial software is suitably licensed.</p> <p>Ensures sufficient Anti-Virus software is installed and is sufficiently up-to-date.</p>			√

## Appendix B - Core Technical Skills (PT002)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
B1	PT002.01	Using Tools and Interpreting Output	<p>Can use a variety of tools during a penetration test, selecting the most appropriate tool to meet a particular requirement.</p> <p>Can interpret and understand the output of tools, including those used for port scanning, vulnerability scanning, enumeration, exploitation and traffic capture.</p>	√	√	√
B2	PT002.02	Pivoting	<p>Understand the concept of pivoting through compromised systems and applications.</p> <p>Can demonstrate pivoting through multiple hops to gain access to targets on different networks</p>	√	√	√
B3	PT002.03	Cryptography	<p>Understands symmetric and asymmetric cryptography, common protocols and their security attributes</p> <p>Understands encryption implementations within software applications, such as SSH, TLS and PGP and in networks such as IPSec and WiFi.</p> <p>Understands common cryptographic algorithms, hash functions, signing and message authentication.</p> <p>Understands PKI and the concepts of certificates, certificate authorities and trusted third parties.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
B4	PT002.04	Hardware Security	<p>Understands the concepts behind common microprocessor vulnerabilities such as Spectre and Meltdown</p> <p>Understands the concepts behind side-channel attacks such as timing analysis and power analysis</p> <p>Understands how side-channel attacks can aid cryptanalysis and otherwise expose sensitive data</p> <p>Understands common risks associated with Bluetooth, including:</p> <ul style="list-style-type: none"> <li>• Bluesnarfing</li> <li>• Bluejacking</li> <li>• Bluebugging</li> </ul>			√
B5	PT002.05	OS Fingerprinting	<p>Understands active and passive operating system fingerprinting techniques and can demonstrate their use during a penetration test.</p>	√	√	√

## Appendix C - Internet Information Gathering and Reconnaissance (PT003)

ID	Skill ID	Skill	Details	Scenario	Practical	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. Can query DNS servers or use passive DNS data to gather information on target systems.  Can identify and exploit misconfigured DNS entries and associated vulnerabilities.	√	√	√
C3	PT003.03	Web Site Analysis	Can analyse information from a target web site, from all sources such as displayed content, HTML, JavaScript, headers and connection metadata.			√
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 such as internet scanners and webcrawlers.			√
C5	PT003.05	News Groups and Mailing Lists	Can use news groups, mailing lists and other services to obtain information about a target network  Can analyse email headers to identify system information.			√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
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	<p>Knowledge of information that can be retrieved from social media sites.</p> <p>Knowledge and experience of information harvesting techniques, and an understanding of the legal implications of scraping social media sites.</p>			√
C8	PT003.08	Document Metadata	<p>Extraction of potentially sensitive data (e.g. usernames, computer names, operating system, software products) from various document formats, including:</p> <ul style="list-style-type: none"> <li>• PDF</li> <li>• Microsoft Office documents</li> <li>• Common picture formats (e.g. JPEG, PNG, GIF etc.)</li> </ul>	√		√

## Appendix D - Networks (PT004)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
D1	PT004.01	Network Connections	<p>Can use common network connections that could be required during a penetration test:</p> <ul style="list-style-type: none"> <li>• Ethernet</li> <li>• Wi-Fi</li> <li>• Ethernet VLANs</li> </ul>	√	√	√
D2	PT004.02	Ethernet Protocol	<p>Basic understanding of how the Ethernet Protocol works.</p> <p>Can spoof MAC addresses to bypass security restrictions and facilitate man in the middle attacks.</p>	√	√	√
D3	PT004.03	Common Ethernet Protocols	<p>Understands security issues relating to the following ethernet protocols:</p> <ul style="list-style-type: none"> <li>• CDP</li> <li>• LLDP</li> <li>• VTP</li> <li>• STP</li> </ul>	√	√	√
D4	PT004.04	VLAN Tagging	<p>Understands VLAN tagging (IEEE 802.1Q).</p> <p>Understands the security implications of VLAN tagging.</p> <p>Can connect a specific VLAN given the VLAN ID from both Linux and Windows systems.</p> <p>Can identify and analyse VLAN tagged traffic on a network.</p>	√	√	√

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



ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
D7	PT004.07	IPv4 and IPv6 Packet Manipulation	<p>Understands components of IP packets.</p> <p>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.</p> <p>Can identify parameters of various packet types, including TCP, UDP, ICMP and ARP.</p> <p>Understands and can perform ARP spoofing safely and reliably to bypass security controls and facilitate man in the middle attacks.</p> <p>Understands packet fragmentation.</p>	√	√	√
D8	PT004.08	Network Routing Protocols	<p>Understands common network routing protocols including:</p> <ul style="list-style-type: none"> <li>• RIP</li> <li>• OSPF</li> <li>• EIGRP</li> <li>• BGP</li> <li>• IGMP</li> </ul> <p>Understands the security attributes of these protocols and how they can be used by attackers.</p> <p>Ability to manipulate these protocols to perform traffic capture and man in the middle attacks.</p>	√		√
D9	PT004.09	Network Architecture	<p>Can interpret logical network diagrams. Understands the security benefits of tiered architectures, DMZs and air gaps.</p> <p>Understands the security implications of shared media, switched networks and VLANs.</p> <p>Understands the core principles, concepts and security of a Software Defined Network (SDN).</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
D10	PT004.10	Network Mapping	<p>Can demonstrate the mapping of a network using a range of tools and by querying active services.</p> <p>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.</p>	√	√	√
D11	PT004.12	Network Devices	<p>Analysing the configuration of the following types of network equipment:</p> <ul style="list-style-type: none"> <li>• Routers</li> <li>• Switches</li> <li>• Firewalls</li> </ul>	√	√	√
D12	PT004.13	Network Filtering	<p>Understands network traffic filtering and where this may occur in a network.</p> <p>Understands the devices and technology that implement traffic filtering, such as firewalls, proxies and next-generation firewalls (NGFW), and can advise on their configuration.</p> <p>Can demonstrate methods by which traffic filters can be bypassed.</p>	√	√	√
D13	PT004.14	Traffic Analysis	<p>Can intercept and monitor network traffic, capturing it to disk in a format required by analysis tools.</p> <p>Understands and can demonstrate network traffic analysis to recover information on targets such as credentials and vulnerabilities present.</p>	√	√	√
D14	PT004.16	TCP	<p>Understands how TCP works and its relationship with IP protocols and higher level protocols.</p> <p>Understands different TCP connection states.</p> <p>Understands and can demonstrate active techniques for discovery of TCP services on a network.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
D15	PT004.17	UDP	<p>Understands how UDP works and its relationship with IP protocols and higher level protocols.</p> <p>Understands different UDP connection states.</p> <p>Understands and can demonstrate active techniques for discovery of UDP services on a network.</p>	√	√	√
D16	PT004.20	Network Access Controls	<p>Understands network access control systems, such as 802.1x and MAC address filtering, and can demonstrate how these technologies can be bypassed.</p>	√	√	√
D17	PT004.21	Wifi	<p>Enumeration and fingerprinting of devices running Wireless (802.11) services.</p> <p>Knowledge of encryption and authentication options, and the relative methods of each.</p> <p>Understands how wifi networks can be attacked.</p>	√		√
D18	PT004.22	Service Identification	<p>Can identify the network services offered by a host by banner inspection.</p> <p>Can state the purpose of an identified network service and determine its type and version.</p> <p>Understands the methods associated with unknown service identification, enumeration and validation.</p> <p>Evaluation of unknown services and protocols.</p>	√	√	√
D19	PT004.23	Host Discovery	<p>Can identify targets on common networks using active and passive fingerprinting techniques and can demonstrate their use.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
D20	PT004.24	Network Intrusion Protection	<p>Understands concepts and the role of network intrusion protections including:</p> <ul style="list-style-type: none"> <li>• IDS/IPS</li> <li>• Honeypots</li> <li>• Data Loss Prevention</li> </ul> <p>Awareness of how network intrusion protections systems may impact security testing</p> <p>Awareness of evasion techniques</p>	√		√
D21	PT004.25	SCTP	Awareness of the Stream Control Transmission Protocol (SCTP)			√

## Appendix E - Network Services (PT005)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E1	PT005.01	Unknown Services	<p>Understands advanced analysis techniques for unknown services and protocols.</p> <p>Can create simple bespoke scripts for exploiting unknown services that use techniques including:</p> <ul style="list-style-type: none"> <li>• Username enumeration</li> <li>• Credential brute forcing</li> <li>• Variations on existing publically available exploits</li> </ul>	√	√	√
E2	PT005.02	Unencrypted Services	<p>Understands how unencrypted services can be exploited.</p> <p>Can identify unencrypted services on the network and capture sensitive data.</p> <p>Is aware of common unencrypted services including:</p> <ul style="list-style-type: none"> <li>• Telnet</li> <li>• FTP</li> <li>• SNMP</li> <li>• HTTP</li> </ul>	√	√	√
E3	PT005.03	TLS / SSL	<p>Understands the use of TLS and SSL in protecting data in transit.</p> <p>Is aware of SSL and TLS protocols and their common weaknesses.</p> <p>Understands the components of cipher suites and their roles.</p> <p>Understands the role of certificates in SSL and TLS.</p> <p>Can identify insecure configurations.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E4	PT005.04	Network Configuration Protocols	<p>Understands and can demonstrate the use of the following network configuration protocols:</p> <ul style="list-style-type: none"> <li>• DHCP</li> <li>• DHCPv6</li> <li>• SLAAC</li> </ul> <p>Understands the security attributes of the above protocols and technologies.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p>	√	√	√
E5	PT005.05	Network Redundancy Protocols	<p>Understands and can demonstrate the use of the following redundancy protocols:</p> <ul style="list-style-type: none"> <li>• HSRP</li> <li>• VRRP</li> </ul> <p>Understands the security attributes of the above protocols and technologies.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p>			√
E6	PT005.06	Name Resolution Services	<p>Understands and can demonstrate the use of the following name resolution services:</p> <ul style="list-style-type: none"> <li>• DNS</li> <li>• DNS over HTTPS (DoH)</li> <li>• Domain Name System Security Extensions (DNSSEC)</li> <li>• NetBIOS / WINS</li> <li>• WINS</li> <li>• LLMNR</li> <li>• mDNS</li> </ul> <p>Understands the security attributes of the above protocols and technologies.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p> <p>Understands the Domain Name Service (DNS) including queries and responses, zone transfers, and the structure and purpose of DNS records.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E7	PT005.07	Network Authentication	<p>Understands and can demonstrate the use of the following network authentication protocols:</p> <ul style="list-style-type: none"> <li>• TACACS+</li> <li>• RADIUS</li> <li>• LDAP</li> <li>• Kerberos</li> </ul> <p>Understands the security attributes of the above protocols and technologies.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p>	√	√	√
E8	PT005.08	Management Services	<p>Understands and can demonstrate the use of the following network management services:</p> <ul style="list-style-type: none"> <li>• Telnet</li> <li>• SSH</li> <li>• HTTP</li> <li>• Remote Powershell</li> <li>• WMI</li> <li>• WinRM</li> <li>• RDP</li> <li>• VNC</li> </ul> <p>Understands the security attributes of the above protocols and technologies.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p>	√	√	√
E9	PT005.09	Desktop Access	<p>Is aware of common protocols used to provide remote access to desktop services including:</p> <ul style="list-style-type: none"> <li>• RDP</li> <li>• VNC</li> <li>• XDMCP</li> <li>• X</li> </ul> <p>Understands the security attributes of the above protocols and technologies.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E10	PT005.10	IPsec	Enumeration and fingerprinting of devices running IPsec services.		√	√
E11	PT005.11	FTP	<p>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.</p> <p>Understands the security implications of anonymous FTP access</p> <p>Understands FTP access control.</p>	√	√	√
E12	PT005.12	TFTP	Understands TFTP and can demonstrate how a poorly configured TFTP server can be exploited, including Cisco devices.	√	√	√
E13	PT005.13	SNMP	<p>Understands the difference between versions 1, 2c, and 3.</p> <p>Can enumerate information from targets including:</p> <ul style="list-style-type: none"> <li>• users</li> <li>• processes</li> <li>• network configuration</li> </ul> <p>Understands the MIB structure pertaining to the identification of security vulnerabilities.</p> <p>Understands the security attributes of SNMP.</p> <p>Can demonstrate how these services can be exploited to gain access to a device or derive further information about the target network.</p> <p>Understands how to extract and replace configuration files of Cisco devices.</p>	√	√	√



ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E14	PT005.14	SSH	<p>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.</p> <p>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 <code>--/.ssh/authorized_keys</code> files.</p> <p>Understands authentication mechanisms used by SSH.</p>	√	√	√
E15	PT005.15	NFS	<p>Understands NFS and its associated security attributes and can demonstrate how exports can be identified.</p> <p>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.</p> <p>Understands the concepts of root squashing, nosuid and noexec options</p> <p>Understands how NFS exports can be restricted at both a host and file level</p>	√	√	√
E16	PT005.16	SMB	<p>Is aware of common SMB implementations including:</p> <ul style="list-style-type: none"> <li>• Windows File Shares</li> <li>• Samba</li> </ul> <p>Can identify and analyse accessible SMB shares.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E17	PT005.17	LDAP	<p>Is aware of common LDAP implementations including:</p> <ul style="list-style-type: none"> <li>• Windows Active Directory</li> <li>• OpenLDAP</li> </ul> <p>Can enumerate LDAP directories and extract arbitrary data including:</p> <ul style="list-style-type: none"> <li>• usernames and groups</li> <li>• target system names</li> </ul>	√	√	√
E18	PT005.18	Berkeley R* Services	<p>Understands the Berkeley r-services and their associated security attributes and can demonstrate how trust relationships can:</p> <ul style="list-style-type: none"> <li>• lead to the compromise of a server</li> <li>• 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.</li> </ul> <p>Can perform user enumeration using the rwho and rusers services.</p>			√
E19	PT005.19	X	<p>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.</p> <p>Understands X authentication mechanisms.</p> <p>Understands the difference between host based and user based access control.</p>	√	√	√
E20	PT005.20	Finger	<p>Understands how finger daemon derives the information that it returns, and hence how it can be abused.</p> <p>Enumeration of usernames.</p>			√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
E21	PT005.21	RPC Services	<p>Can perform RPC service enumeration.</p> <p>Is aware of common RPC services.</p> <p>Is aware of and can exploit recent or commonly-found RPC service vulnerabilities.</p>	√	√	√
E22	PT005.22	NTP	<p>Understands the function of NTP and the importance of it for logging and authentication.</p> <p>Can extract information about the target network from NTP services.</p>	√	√	√
E23	PT005.23	IPMI	<p>Understands and can demonstrate use of IPMI for the remote management of devices, such as HP ILO and Dell DRAC.</p> <p>Understands the security attributes of IPMI.</p> <p>Can exploit common vulnerabilities to gain access to a device.</p>	√	√	√
E24	PT005.24	VoIP	<p>Enumeration and fingerprinting of devices running VoIP services.</p> <p>Knowledge of the SIP protocol.</p>	√	√	√
E25	PT005.25	SMTP and Mail Servers	<p>Understands and can demonstrate valid username discovery via EXPN and VRFY.</p> <p>Awareness of recent vulnerabilities in mail server applications (e.g. Postfix and Exchange) and the ability to exploit them if possible</p> <p>Understands mail relaying.</p>	√	√	√
E26	PT005.26	Vulnerable Services	<p>Can identify and remotely exploit services with recent or well known public vulnerabilities.</p>	√	√	√

## Appendix F - Microsoft Windows Security Assessment (PT006)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
F1	PT006.01	Windows Reconnaissance	<p>Can identify Windows hosts on a target network.</p> <p>Can identify forests, domains, domain controllers, domain members and workgroups.</p> <p>Can enumerate accessible Windows shares.</p> <p>Can identify and analyse internal browse lists.</p>	√	√	√
F2	PT006.02	Windows Network Enumeration	<p>Can perform user and group enumeration on target systems and domains, using various protocols and methods including:</p> <ul style="list-style-type: none"> <li>• NetBIOS</li> <li>• LDAP</li> <li>• SNMP</li> <li>• RID Cycling</li> </ul> <p>Can obtain other information, such as password policies.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
F3	PT006.03	Active Directory	<p>Understands Active Directory structure</p> <p>Understands Active Directory roles (Global Catalogue, Master Browser, FSMO)</p> <p>Understands Group Policy.</p> <p>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.</p> <p>Understands the reliance of Active Directory on DNS and LDAP.</p> <p>Understands the role of Kerberos within Active Directory.</p> <p>Understands and can identify the different types of domain trusts, including:</p> <ul style="list-style-type: none"> <li>• One-way and two-way trusts</li> <li>• Explicit and transitive trusts</li> </ul>	√	√	√
F4	PT006.04	Active Directory Enumeration	<p>Can enumerate information from Active Directory including:</p> <ul style="list-style-type: none"> <li>• Users</li> <li>• Groups</li> <li>• Computers</li> <li>• Trusts</li> <li>• Service Principle Names</li> </ul>	√	√	√
F5	PT006.05	Windows Passwords	<p>Understands password policies, including complexity requirements and lock-out.</p> <p>Understands how to avoid causing a denial of service by locking-out accounts.</p> <p>Understands Windows password hashing algorithms, the merits of each algorithm, and their associated security attributes.</p> <p>Understands how passwords are stored and protected and can demonstrate how they can be recovered.</p> <p>Understands and can demonstrate off-line password cracking using dictionary and brute-force attacks, including the use of rainbow tables.</p>	√	√	√

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

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
F12	PT006.12	Advanced Local Exploitation	<p>Understands the use of tools and techniques to identify new OS and software vulnerabilities.</p> <p>Understands the techniques used to develop exploit code for existing and new vulnerabilities.</p>	√	√	√
F13	PT006.13	Windows Post Exploitation	<p>Understands and can perform common post exploitation activities, including:</p> <ul style="list-style-type: none"> <li>• obtaining password hashes, both from the local SAM and cached credentials or obtaining locally stored clear-text passwords</li> <li>• cracking password hashes</li> <li>• obtaining patch levels</li> <li>• deriving a list of missing security patches</li> <li>• reverting to a previous state</li> <li>• lateral and horizontal movement</li> </ul>	√	√	√
F14	PT006.14	Windows Patch Management	<p>Understands common windows patch management strategies, including:</p> <ul style="list-style-type: none"> <li>• SMS</li> <li>• SUS</li> <li>• WSUS</li> </ul>	√	√	√
F15	PT006.16	Active Directory Attack Paths	<p>Can analyse a Windows Active Directory environment and identify attack paths that can be used to escalate privileges or compromise a specific target.</p>	√	√	√
F16	PT006.17	Common Windows Applications	<p>Knowledge of significant vulnerabilities in common windows applications for which there is public exploit code available.</p>	√	√	√

## Appendix G - Linux / UNIX Security Assessment (PT007)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
G1	PT007.01	Linux / UNIX Host Discovery and Reconnaissance	Can identify Linux / UNIX hosts on a network.	√	√	√
G2	PT007.02	Linux / UNIX Network Enumeration	<p>Can demonstrate and explain the enumeration of data from a variety of common network services on various platforms including:</p> <ul style="list-style-type: none"> <li>• Filesystems or resources shared remotely, such as NFS and SMB</li> <li>• SMTP</li> <li>• SSH</li> <li>• Telnet</li> <li>• SNMP</li> </ul> <p>Is aware of legacy user enumeration techniques such as rusers, rwho and finger.</p> <p>Can enumerate RPC services and identify those with known security vulnerabilities.</p>	√	√	√



ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
G3	PT007.03	Linux / UNIX Passwords	<p>Understands users, groups and password policies, including complexity requirements and lock out.</p> <p>Understands how to avoid causing a denial of service by locking out accounts.</p> <p>Understands the format of the passwd, shadow, group and gshadow files.</p> <p>Understands UNIX password hashing algorithms and their associated security attributes.</p> <p>Understands how passwords are stored and protected and can demonstrate how they can be recovered.</p> <p>Understands and can demonstrate off-line password cracking using dictionary and brute force attacks.</p> <p>Can demonstrate the recovery of password hashes when given physical access to a Linux / UNIX host.</p>	√	√	√
G4	PT007.04	Linux / UNIX File Permissions	<p>Understands and can demonstrate the manipulation of file system permission on Linux and UNIX operating systems.</p> <p>Understands how insecure file system permissions can be exploited to escalate privileges and/or gain further access to a host.</p> <p>Can find 'interesting' files on an operating system, e.g. those with insecure permissions, assigned setuid / setgid permissions, assigned sensitive capabilities or containing user account passwords.</p>	√	√	√
G5	PT007.05	Linux / UNIX Processes	<p>Can identify running processes on Linux / UNIX hosts and exploit vulnerabilities to escalate privileges.</p> <p>Understands and can exploit shared library loading mechanisms to escalate privileges.</p>	√	√	√
G6	PT007.06	Linux Remote Exploitation	<p>Understands and can demonstrate the remote exploitation of Linux systems</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
G7	PT007.07	Linux Local Exploitation	<p>Understands and can demonstrate the local exploitation of Linux operating system vulnerabilities.</p> <p>Understands and can demonstrate Local privilege escalation techniques, e.g. through the manipulation of insecure file system permissions.</p>	√	√	√
G8	PT007.08	Linux / UNIX Post Exploitation	<p>Understands and can demonstrate common post-exploitation activities, including:</p> <ul style="list-style-type: none"> <li>• obtaining locally stored clear-text passwords</li> <li>• password recovery (exfiltration and cracking)</li> <li>• lateral movement</li> <li>• checking OS and third party software application patch levels</li> <li>• deriving a list of missing security patches</li> <li>• reversion of OS and software components to previous state</li> </ul>	√	√	√
G9	PT007.10	Unix Exploitation	Understands weaknesses, common misconfigurations and exploits that may affect Unix systems.	√	√	√

## Appendix H - Web Technologies (PT008)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H1	PT008.01	Web Servers	<p>Can identify web servers on a target network and can remotely determine their type and version.</p> <p>Understands the various mechanisms web servers use for hosting applications, including:</p> <ul style="list-style-type: none"> <li>• virtual hosts</li> <li>• multiple ports</li> <li>• application specific URLs</li> </ul> <p>Understands and can demonstrate the remote exploitation of web servers.</p> <p>Understands the concepts of web proxies including reverse proxies.</p> <p>Understands the purpose, operation, limitation and security attributes of web proxy servers.</p>		√	√
H2	PT008.02	Web Application Frameworks	<p>Can identify common web application frameworks and technologies.</p> <p>Is aware of and can exploit vulnerabilities in common web application frameworks and technologies.</p>		√	√
H3	PT008.03	Common Web Applications	<p>Can identify common web applications and exploit well known vulnerabilities.</p>		√	√
H4	PT008.04	Web Protocols	<p>Understands and can demonstrate the use of web protocols, including:</p> <ul style="list-style-type: none"> <li>• HTTP / HTTPS</li> <li>• WebSockets</li> </ul> <p>Understands all HTTP methods and response codes.</p> <p>Understands HTTP header fields relating to security features.</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H5	PT008.05	Mark Up Languages	<p>Understands common web mark up languages, including:</p> <ul style="list-style-type: none"> <li>• HTML</li> <li>• XHTML</li> <li>• XML</li> </ul>		√	√
H6	PT008.06	Web Languages	<p>Understands common web client and server programming languages.</p> <p>Understands and can demonstrate how the insecure implementation of software developed using these languages can be exploited.</p>		√	√
H7	PT008.07	Web APIs	<p>Understands and can demonstrate the use of web based APIs to remotely access remote services.</p> <p>Understands the concepts behind SOAP, REST and GraphQL APIs, payload formats and API definitions and documentation.</p> <p>Understands common authentication techniques used in web APIs.</p> <p>Understands and can demonstrate how the insecure implementation of web-based APIs can be exploited.</p>		√	√
H8	PT008.08	Web Clients	<p>Understands thick client software and its use of web or API endpoints.</p> <p>Can analyse client side code to facilitate server side testing.</p>		√	√
H9	PT008.09	Web Application Reconnaissance	<p>Understands content discovery techniques and can demonstrate web-site enumeration and reconnaissance through spidering, code analysis, forced browsing or other relevant process to map linked or unlinked content.</p> <p>Can interpret website data and meta-data to refine reconnaissance methods.</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H10	PT008.10	Web Threat Modelling and Attack Vectors	<p>Simple threat modelling based on customer perception of risk.</p> <p>Relate functionality offered by the application to potential attack vectors.</p>		√	√
H11	PT008.11	Information Gathering	<p>Can gather information from a web site and application mark up or application code, including:</p> <ul style="list-style-type: none"> <li>• hidden form fields</li> <li>• database connection strings</li> <li>• user account credentials</li> <li>• developer comments</li> <li>• external and/or authenticated-only URLs.</li> </ul> <p>Can gather information about a web site and application from the error messages it generates.</p>		√	√
H12	PT008.12	Web Authentication	<p>Understands common authentication mechanisms and their security issues, including external authentication providers and single sign-on.</p> <p>Understands and can demonstrate authentication vulnerabilities in web application authentication processes.</p>		√	√
H13	PT008.13	Web Authorisation	<p>Understands common pitfalls associated with the design and implementation of application authorisation mechanisms.</p>		√	√
H14	PT008.14	Input Validation	<p>The importance of input validation as part of a defensive coding strategy.</p> <p>How input validation can be implemented and the differences between allow list, deny list and data sanitisation.</p> <p>Understands the need for server side validation and the flaws associated with client-side validation.</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H15	PT008.15	Web Application Fuzzing	<p>Understands fuzzing and its use in web application testing.</p> <p>Understands the generation of fuzzing strings and their potential effects, including the dangers they may introduce.</p>		√	√
H16	PT008.16	Cross Site Scripting	<p>Understands cross site scripting (XSS) and can demonstrate the launching of a successful XSS attack.</p> <p>Understands the difference between persistent, reflected and DOM based XSS.</p>		√	√
H17	PT008.17	SQL Injection	<p>Determine the existence of SQL injection conditions in web applications.</p> <p>Can exploit SQL injection to execute arbitrary SQL commands in a database.</p>		√	√
H18	PT008.18	ORM Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of ORM injection in a web application.</p>		√	√
H19	PT008.19	XML Related Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of the different types of XML related injections within web applications.</p>		√	√
H20	PT008.20	LDAP Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of LDAP injection in a web application.</p> <p>Can exploit LDAP injection to extract arbitrary data from an LDAP directory.</p>		√	√
H21	PT008.21	Server-Side Includes (SSI) Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of SSI injection in a web application.</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H22	PT008.22	Mail Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of the following types of mail related injection in a web application:</p> <ul style="list-style-type: none"> <li>• SMTP injection</li> <li>• IMAP injection</li> </ul>		√	√
H23	PT008.23	Code Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of code injection in a web application built with common web scripting languages.</p>		√	√
H24	PT008.24	OS Command Injection	<p>Can demonstrate the ability to identify, explain and prove the existence of OS command injection in a web application.</p>		√	√
H25	PT008.25	Sessions & Tokens	<p>Understands the use of session or token authentication mechanisms used within web applications and APIs.</p> <p>Understands the security implications of sessions, exploiting weaknesses including hijacking, fixation, session puzzling and specific vulnerabilities in common session implementations.</p> <p>Understands the security implications of tokens, exploiting weaknesses including token manipulation, re-use and specific vulnerabilities in common token implementations.</p>		√	√
H26	PT008.26	Cookies	<p>Understands how cookies work in a web application.</p> <p>Understands cookie attributes and how they can affect the security of a web application.</p>		√	√
H27	PT008.29	Request Forgery	<p>Understands and can exploit cross-site and server-side request forgery vulnerabilities.</p> <p>Understands the role of sessions in CSRF attacks.</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H28	PT008.31	Mass Assignment	Understands and can identify and exploit mass assignment vulnerabilities.		√	√
H29	PT008.32	Web Cryptography	<p>Understands how cryptography can be used to protect data in transit and data at rest, both on the server and client side.</p> <p>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).</p> <p>Understanding how hashing can be used appropriately within web applications.</p> <p>Exploitation of weak cryptography or poorly configured encryption within web applications, including padding oracle and man-in-the-middle.</p> <p>Understands and can perform relevant attacks against web applications or web APIs where the connections are insecure.</p>		√	√
H30	PT008.35	Parameter Manipulation	Understands parameter manipulation techniques, particularly the use of client-side proxies.		√	√
H31	PT008.36	Directory Traversal	Understands and can identify directory traversal vulnerabilities within applications.		√	√
H32	PT008.37	File Uploads	<p>Understands and can identify common vulnerabilities with file upload capabilities within applications.</p> <p>Understands the role of MIME types in relation to file upload features.</p> <p>Can generate malicious payloads in a variety of common file formats.</p>		√	√
H33	PT008.38	CRLF Attacks	<p>Understands and can demonstrate CRLF attacks, including:</p> <ul style="list-style-type: none"> <li>• HTTP Splitting</li> <li>• HTTP Smuggling</li> </ul>		√	√



ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
H34	PT008.39	Web Application Logic Flaws	Can assess and exploit vulnerabilities within the functional logic, function access control and business logic of an application.		√	√
H35	PT008.40	Client Side Vulnerabilities	<p>Understands and can demonstrate client side vulnerabilities within web applications, including:</p> <ul style="list-style-type: none"> <li>• DOM based XSS</li> <li>• HTML injection</li> <li>• URL redirect</li> <li>• CSS injection</li> <li>• Resource manipulation</li> <li>• Cross origin resource sharing</li> <li>• Clickjacking</li> <li>• Web messaging ( cross document messaging)</li> <li>• Browser storage</li> <li>• Cross site script inclusion</li> </ul>		√	√

## Appendix I - Databases (PT009)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
I1	PT009.01	SQL Relational Databases	<p>Can use SQL to interact with relational databases and extract information, e.g. SQLite, PostgreSQL.</p> <p>Understands common connection and authentication methods to connect to SQL databases.</p> <p>Can recognise common database connection string formats, e.g. JDBC, ODBC.</p> <p>Understands and can demonstrate the remote exploitation of common SQL databases.</p> <p>Understands and can demonstrate how access can be gained to a database through the use of default accounts credentials and insecure passwords.</p> <p>Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
12	PT009.02	Microsoft SQL Server	<p>Understands and can demonstrate the remote exploitation of Microsoft SQL Server.</p> <p>Understands and can demonstrate how access can be gained to a Microsoft SQL server through the use of default accounts credentials and insecure passwords.</p> <p>Can identify and exploit linked server configurations.</p> <p>Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).</p> <p>Can leverage database features to enumerate domain information.</p> <p>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.</p>	√	√	√
13	PT009.03	Oracle RDBMS	<p>Understands and can demonstrate the remote exploitation of an Oracle RDBMS instance.</p> <p>Understands the security attributes of the Oracle TNS Listener service.</p> <p>Understands and can demonstrate how access can be gained to an Oracle RDBMS through the use of default accounts credentials and insecure passwords.</p> <p>Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).</p> <p>Can demonstrate how the software version and patch status can be obtained from an Oracle database.</p> <p>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.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
14	PT009.04	MySQL	<p>Understands and can demonstrate the remote exploitation of an MySQL database.</p> <p>Understands and can demonstrate how access can be gained to an MySQL database through the use of default accounts credentials and insecure passwords.</p> <p>Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).</p> <p>Can demonstrate how the software version and patch status can be obtained from an MySQL database.</p> <p>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.</p>	√	√	√
15	PT009.05	PostgreSQL	<p>Understands and can demonstrate the remote exploitation of an PostgreSQL database.</p> <p>Understands and can demonstrate how access can be gained to an PostgreSQL database through the use of default accounts credentials and insecure passwords.</p> <p>Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).</p> <p>Can demonstrate how the software version and patch status can be obtained from an PostgreSQL database.</p> <p>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.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
16	PT009.06	NoSQL	<p>Understands and can demonstrate the remote exploitation of common NoSQL databases including key-value, document, graph and column types.</p> <p>Understands and can demonstrate how access can be gained to such a database through the use of default accounts credentials and insecure passwords.</p> <p>Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible).</p>	√	√	√

## Appendix J - Virtualisation (PT010)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
J1	PT010.01	Virtualisation Platforms	<p>Can identify use of popular virtualisation technologies, including:</p> <ul style="list-style-type: none"> <li>• VMware</li> <li>• Microsoft HyperV</li> <li>• Citrix</li> <li>• Oracle VirtualBox</li> <li>• Linux KVM</li> </ul> <p>Understands common vulnerabilities found in hypervisors, including:</p> <ul style="list-style-type: none"> <li>• Exposure of management interface</li> <li>• Use of default or insecure credentials</li> <li>• Common high profile CVEs</li> </ul> <p>Understands the inherent risks in shared virtualised environments, e.g. shared memory space</p>	√	√	√
J2	PT010.02	Virtual Machine Escape	<p>Understands and can demonstrate common techniques for escaping a virtualised environment, including:</p> <ul style="list-style-type: none"> <li>• Directory traversal in shared folders</li> <li>• Virtual device communication breakout</li> <li>• Public CVEs relating to memory corruption</li> </ul>	√	√	√
J3	PT010.03	Snapshots	<p>Can demonstrate how to take snapshots and techniques for recovering key sensitive information</p> <p>Understands the security implications of reverting a VM to a previous state</p> <p>Understands the sensitive nature of snapshot files and the need to restrict access</p>	√	√	√

## Appendix K - Containerisation (PT011)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
K1	PT011.01	Containers	<p>Understands the key differences between virtualisation and containerisation</p> <p>Understands how containers are isolated from the host system</p> <p>Can identify and interrogate running containers on a host</p> <p>Can identify common vulnerabilities and weaknesses present in containers, including:</p> <ul style="list-style-type: none"> <li>• Missing security patches</li> <li>• Weak file permissions</li> <li>• Insufficient or lack of resource quotas</li> <li>• Presence of sensitive information in environment variables, running processes or filesystem</li> </ul>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
K2	PT011.02	Docker	<p>Understands how Docker containers are implemented on Linux and Windows.</p> <p>Understands the concepts of layered filesystems and how to extract and analyse specific layers within an image</p> <p>Understands and can analyse Dockerfile files to uncover weaknesses in static images, including:</p> <ul style="list-style-type: none"> <li>• Use of unencrypted connections for performing downloads</li> <li>• Use of overly generous permissions, e.g. running as the root user</li> <li>• Inclusion of sensitive information, e.g. passwords or private keys o Unnecessary exposure of ports</li> </ul> <p>Understands Docker networking and how containers interact with each other and the host networks.</p> <p>Understands and can exploit misconfigurations in containers that can lead to privilege elevation and escaping the container.</p> <p>Understands and can exploit misconfigurations in the environment that could allow malicious containers to be deployed.</p>	√	√	√
K3	PT011.03	Kubernetes	<p>Understands how Kubernetes containers are implemented.</p> <p>Understands Kubernetes networking and how containers interact with each other and the host networks.</p> <p>Understands how Kubernetes containers are managed and deployed.</p> <p>Understands and can exploit misconfigurations in containers that can lead to privilege elevation and escaping the container.</p> <p>Understands and can exploit misconfigurations in the environment that could allow malicious containers to be deployed.</p>	√	√	√



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

## Appendix L - Cloud Security (PT012)

ID	Skill ID	Skill	Details	Scenario	Practical	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	<p>Understands the concepts of a VPC and the implications on performing security assessments.</p> <p>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).</p>		√	√
L3	PT012.03	Logging and Monitoring	<p>Can analyse logging configuration within a cloud environment and advise on improvements.</p> <p>Can analyse the configuration of resource monitoring and alarm generation and advise on improvements.</p>		√	√
L4	PT012.04	Identity and Access Management	<p>Understands the identity and access management models of popular cloud providers.</p> <p>Can assess roles and policies to identify weaknesses relating to insecure permissions.</p>		√	√
L5	PT012.05	Denial of Service and Resource Exhaustion	<p>Understands how (Distributed) Denial of Service attacks are performed and the protective measures available in cloud environments.</p> <p>Understands the financial implications of excessive resource consumption.</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
L6	PT012.06	General Cloud Reconnaissance	<p>Can identify services and configurations associated with popular cloud providers</p> <p>Can enumerate the services that are deployed and used within a cloud account</p> <p>Can interpret cloud policies and permissions</p> <p>Can identify common cloud misconfigurations</p>		√	√
L7	PT012.07	General Host to Cloud Transition	<p>Understands and can demonstrate how compromise of systems can be used to gain access to cloud services</p> <p>Understands and can demonstrate the ability to recover credentials that could be used to access cloud services</p>		√	√
L8	PT012.08	General Cloud Secrets Management	<p>Understands the concepts of cloud secrets management such as Azure Key Vaults and AWS Secrets Manager</p> <p>Can demonstrate the ability to query secrets from AWS Secrets Manager using CLI tools</p> <p>Can interpret AWS policies to identify principals with access to secrets in AWS Secrets Manager</p>	√	√	√
L9	PT012.09	AWS Cloud Reconnaissance	<p>Can enumerate the services that are deployed within an account</p> <p>Can interpret AWS policies</p> <p>Can identify common cloud misconfigurations</p>	√	√	√
L10	PT012.10	AWS Host to Cloud Transition	<p>Understands and can demonstrate how compromise of systems can be used to gain access to cloud services</p> <p>Understands and can demonstrate the ability to recover credentials that could be used to access cloud services</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
L11	PT012.11	AWS Workspaces	<p>Understands Workspace storage restrictions</p> <p>Can demonstrate recovery of sensitive information from accessible services using compromised credentials</p>	√	√	√

## Appendix M - Physical Security (PT014)

ID	Skill ID	Skill	Details	Scenario	Practical	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.		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
M6	PT014.06	Recovery Functionality	Understands the security attributes of operating system recovery functionality, e.g. Windows Recovery Console and Safe Mode.		√	√
M7	PT014.07	Authentication	<p>Understands multi-factor authentication systems, such as tokens and SMS.</p> <p>Understands types of biometrics and how they can be applied.</p> <p>Understands the concept of one-time pads.</p> <p>Understands the use of digital certificates as an authentication mechanism.</p> <p>Understands the concept of contactless RFID smart cards.</p>		√	√

## Appendix N - Secure Development Operations (PT015)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
N1	PT015.01	Secure Coding Practices	<p>Understands common insecure programming practices, including:</p> <ul style="list-style-type: none"> <li>• Use of dangerous functions</li> <li>• Insufficient sanitisation of user-supplied data</li> <li>• Use of outdated third party components</li> <li>• Logic errors</li> </ul>		√	√
N2	PT015.02	Security in the Development Lifecycle	<p>Understands the role of automated security testing tools as part of the development process, including:</p> <ul style="list-style-type: none"> <li>• Static analysis tools (SAST)</li> <li>• Dependency checking tools</li> <li>• Dynamic analysis tools (DAST)</li> </ul> <p>Understands how automated tooling can safely and effectively be incorporated into the development pipeline.</p> <p>Can identify and advise on common security misconfigurations of these tools.</p>		√	√
N3	PT015.03	Infrastructure as Code	<p>Understands the role of tools to automate the building, configuration and deployment of infrastructure, including:</p> <ul style="list-style-type: none"> <li>• Terraform</li> <li>• AWS Cloud Formation</li> <li>• Azure Resource Manager</li> <li>• Puppet</li> <li>• Ansible</li> <li>• Chef</li> </ul> <p>Can identify and advise on common security misconfigurations of these tools.</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
N4	PT015.04	Code Repository Security	<p>Can identify and advise on issues relating to weakly protected code repositories, for example:</p> <ul style="list-style-type: none"> <li>• Openly exposed repositories containing closed source code</li> <li>• Weak or insufficiently protected credentials</li> </ul> <p>Understands the security implications of storing sensitive information in source code repositories, e.g. passwords, private cryptographic keys or API keys.</p>	✓	✓	✓



## Appendix O - Windows Desktop Lockdown (PT018)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
O1	PT018.01	Lockdown Solutions	<p>Is familiar with common methods of implementing application restrictions including:</p> <ul style="list-style-type: none"> <li>• Software Restriction Policies (SRP)</li> <li>• AppLocker</li> <li>• Virtualisation-based restrictions</li> <li>• Citrix</li> </ul>	√	√	√
O2	PT018.02	Breakout Techniques	<p>Understands and can demonstrates enumeration of lockdown policies</p> <p>Understands and can demonstrate techniques to break out of a locked down Windows desktop or Citrix environment</p> <p>Can perform privilege escalation techniques from a desktop environment</p> <p>Awareness of how native Microsoft Windows tools and features can be used to execute code and bypass restrictions</p>	√	√	√
O3	PT018.03	Local Filesystem Protections	<p>Understands techniques used to restrict read / write access to the local filesystem</p> <p>Understands common techniques to bypass filesystems</p>	√	√	√
O4	PT018.04	PowerShell Restrictions	<p>Understands the restrictions enforced via constrained language mode</p> <p>Can demonstrate bypass of constrained language mode</p>	√	√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
O5	PT018.05	User Account Control (UAC)	<p>Understands the limitations of UAC</p> <p>Can enumerate and interpret UAC policies</p> <p>Understands the concepts of integrity levels and the consequences of executing code in different levels</p> <p>Can demonstrate UAC bypass</p>	√	√	√

## Appendix P - Social Engineering (PT019)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
P1	PT019.01	Phishing	<p>Understands the concept of Phishing, spear Phishing and Whaling</p> <p>Understands how common document formats can be used to execute code</p> <p>Understands common methods used to connect to Command and Control (C2) Infrastructure</p>		√	√
P2	PT019.02	Vishing	<p>Understands the concept of Vishing</p> <p>Understands the concepts of caller ID spoofing</p>		√	√

## Appendix Q - macOS Security Assessment (PT020)

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
Q1	PT020.01	macOS Reconnaissance	Can identify macOS systems hosts on a network		√	√
Q2	PT020.02	macOS Network Enumeration	<p>Can demonstrate and explain the enumeration of data from a variety of common network services</p> <p>Familiarity with the native macOS firewall, its default configuration and policy configurations</p>		√	√
Q3	PT020.03	macOS Passwords	<p>Familiarity with the macOS privilege model including the default permissions of the Administrator, Standard and Sharing Only groups and the default configuration of the 'root' account</p> <p>Understands password and account lockout policy configurations including complexity requirements and user lock out</p> <p>Understands how passwords are stored and protected and can demonstrate how they can be recovered</p> <p>Understands and can demonstrate off-line password cracking using dictionary and brute force attacks</p> <p>Knowledge of password storage mechanisms such as the local Keychain and iCloud Keychain and the key differences</p>		√	√

ID	Skill ID	Skill	Details	Scenario	Practical	Multiple choice
Q4	PT020.04	macOS File Permissions	<p>Understands and can demonstrate the manipulation of file system permission on macOS operating systems.</p> <p>Understands how insecure file system permissions can be exploited to escalate privileges and/or gain further access to a host.</p> <p>Can find "interesting" files on an operating system, e.g. those with insecure or "unusual" permissions, or containing user account passwords</p>		√	√
Q5	PT020.05	macOS Remote Exploitation	Understands and can demonstrate the remote exploitation of macOS systems		√	√
Q6	PT020.06	macOS Local Exploitation	<p>Understands and can demonstrate Local privilege escalation techniques, e.g. through the manipulation of insecure file system permissions</p> <p>Knowledge of system and binary restriction implementations such as those configured through Jamf and Microsoft Intune</p>		√	√
Q7	PT020.07	macOS Post Exploitation	<p>Understands and can demonstrate common post-exploitation activities, including:</p> <ul style="list-style-type: none"> <li>• obtaining locally stored clear-text passwords</li> <li>• password recovery (exfiltration and cracking)</li> <li>• checking OS and third party software application patch levels</li> <li>• deriving a list of missing security patches</li> </ul>		√	√