ENGAGEMENT, LIFESTYLE & RISK KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

ENGAGEMENT LIFECYCLE

- Understand the penetration testing lifecycle, from initial client contact, to the delivery of the final report and subsequent consultancy work
- Understand the structure of a penetration test, including all relevant processes and procedures
- Understand penetration testing methodologies and follows these when required. These include methodologies defined by the testers' employer, together with recognised standards, such as CHECK
- Can articulate the benefits a penetration test will bring to a client
- Can accurately convey the results of the penetration testing in a verbal de-brief and written report

SCOPING

- Understanding of the different types of testing (blackbox, whitebox, etc) and their relative advantages and disadvantages
- Understand client requirements and can produce an accurate and adequately resourced penetration testing proposal
- Understand scoping in Cloud environments, and the impact of IaaS vs PaaS vs SaaS
- Understand technical, logistical, financial and other constraints and is able to take these into account without compromising the effectiveness of the penetration test

LEGAL MATTERS

- Understand the legislation pertaining to penetration testing and can give examples of compliance/non-compliance. This legislation includes: Computer Misuse Act 1990 and its amendments; Data Protection Act 2018; Human Rights Act 1998; Police and Justice Act 2006; Police and Criminal Evidence Act 1984; Investigatory Powers Act 2016
- Awareness of sector-specific regulatory issues, including NIS B4.d (Vulnerability management)

UNDERSTANDING & MITIGATING RISK

- Understand the risks associated with a penetration test (e.g. account lockout, denial of service) and how these can be mitigated
- Understand the importance of availability and how the risk of denial of service can be reduced
- Understand the importance of client confidentiality
- Understand the role/function of customer emergency contacts
- Understand the impact legislation has on the penetration testing process
- Understand the ethical issues associated with penetration testing
- Understand non-disclosure agreements and complies with their requirements

ISSUE IDENTIFICATION & PROOF

- Identify false positives and false negatives and operate within the constraints of the scope of testing whilst keeping risk of disruption to an acceptable level
- Produce proof-of-concept scripts to demonstrate issues
- Can chain together separate vulnerabilities to form more complex attack chains
- Can demonstrate techniques for proving issues, which may fall outside of the constraints and scope in place during the engagement

RECORD KEEPING

- Understand the reporting requirements mandated by internal and external standards
- Understand the importance of keeping accurate and structured records during a penetration test, including the output of tools
- Keep accurate records of changes made to the systems during an assessment
- Understand the security requirements associated with record keeping, both during the penetration test and following the delivery of the final report
- Can write a report from the information gathered during a penetration test
- Understand how to categorise vulnerabilities with respect to recognised methodologies e.g. CVE, BID, CVSS

PLATFORM PREPARATION

- Ability to prepare the required hardware and software for a penetration test
- Take steps to avoid data cross-contamination e.g. by sanitising a hard disk prior to deployment or taking an image from a master build
- Ensure all operating system and testing tools are relevant and up-to-date
- Ensure all commercial software is suitably licensed
- Ensure sufficient Anti-Virus software is installed and is sufficiently up-to-date
- Ensure all necessary hardware is available, including laptops, switches, media-converters, wireless devices and cabling

RESULTS ANALYSIS & PRESENTATION

- For any given issue or group of issues, ability to convey: 1. a detailed description of the problem 2. A list of affected components 3. Possible sources of further information 4. A description of the risk posed in terms of confidentiality, integrity and availability of the system and its data 5. The cause of the issue 6. Which type of attacker would most likely exploit the issue 7. the difficulty and likelihood of a successful exploit 8. The potential impact to the customer's information systems and data preferably in terms of CIA 9. Detailed recommendations for remediation, drawing upon extensive product specific knowledge where possible and providing suitable general recommendations where not (senior or principle responsibility)
- Ability to convey both verbal and written summary of a security test to technical and non-technical audiences.
- Ability to classify/rank findings using numerical and/or distinct risk levels (High, Medium, Low etc) in line with how the client interprets risk within its business

CORE TECHNICAL KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

IP PROTOCOLS

- Understands IPv4 and IPv6 and their associated security attributes
- Understands common IP/Ethernet protocols and their associated security attributes, including:
  • TCP • UDP • ICMP • ARP • DHCP • DNS • CDR HSRP • VRRP • VTP • STP • TACACS+
- Understands the security implications of using clear-text protocols, such as Telnet and FTP

FILE SYSTEM PERMISSIONS & SYSTEM PROCESSES

- Understands and can demonstrate the manipulation of file system permission on UNIX-like and Windows operating systems
- Can find "interesting' files on an operating system, e.g. those with insecure or "unusual" permissions, or containing user account passwords
- Can identify running processes on UNIX-like and Windows operating systems and exploit vulnerabilities to escalate privileges
- Understands technical, logistical, financial and other constraints and is able to take these into account without compromising the effectiveness of the penetration test
- Understands and can demonstrate the detection and manipulation of weak registry ACLs

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 IKE Certificate Authorities and trusted third parties
- Understands the difference between encoding and encrypting
- Understand the dangers of implementing custom cryptography
- Understand the differences between encryption modes (EBC, CBC, GCM, etc)
- Understand best practices around key management
- Identify and exploit weaknesses in custom cryptography

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
- Network Pivoting Techniques e.g. • Windows netsh Port Forwarding • SSH o SOCKS Proxy o Local Port Forwarding o Remote Port Forwarding • Proxychains • Graphtcp • Web SOCKS • reGeorg • Metasploit • sshuttle • chisel o SharpChisel • gost • Rpivot • RevSocks • plink • ngrok • Basic Pivoting Types o Listen • Listen o Listen • Connect o Connect • Connect

USING TOOLS & INTERPRETING OUTPUT

- Can use a variety of tools during a penetration test, selecting the most appropriate tool to meet a particular requirement
- Understand the limitations of automated testing
- Interpret and understand the output of tools, including those used for port scanning, vulnerability scanning, enumeration, exploitation and traffic capture
- Can identify when tool output can and can not be trusted. Can demonstrate an approach to verifying too output
- Can effectively use command line during assurance testing
- Demonstrate ability to carry out testing when tools are not available or functional

PACKET GENERATION

- Understands the different types of packets that are likely to be encountered during a penetration test
- Understands packet fragmentation
- Can generate arbitrary packets, including TCP, UDP, ICMP and ARP, modifying packet parameters as required, e.g. source and destination IP addresses, source and destination ports, and TTL.
- Understands ARP spoofing and can demonstrate this technique in a safe and reliable way.

PORT SCANNING

- Understands different TCP connection states
- Understands and can demonstrate active techniques for discovery of nodes on a network, such as: • SYN and TCP-Connect scanning • FIN/NULL and XMAS scanning • UDP port scanning • TCP ping scanning • ICMP scanning

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
- Understands advanced analysis techniques for unknown services and protocols.

FINGERPRINTING

- Understands active and passive operating system fingerprinting techniques and can demonstrate their use during a penetration test

TRAFFIC FILTERING & ACCESS CONTROL

- 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
- Understands network access control systems, such as 802.1x and MAC address filtering, and can demonstrate how these technologies can be bypassed

PATCH LEVELS

- Understands Microsoft patch management strategies and tools, including:
  • Microsoft Systems Management Server (SMS)
  • Microsoft Software Update Service (SUS)
  • Microsoft Windows Server Update Services (WSUS)
  • Microsoft Baseline Security Analyser (MBSA)
- Understands network access control systems, such as 802.1x and MAC address filtering, and can demonstrate how these technologies can be bypassed

BUILD REVIEW

- Demonstrate the ability to perform a security build review of common operating systems
- Understands and can test against common build standards such as CIS benchmarks
- Can map technical controls to a customer's business requirements and intents, justifying the need to tighten or relax them where necessary to meet business needs

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

INFORMATION GATHERING KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

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.
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)
WEBSITE 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
SEARCH ENGINES, NEWS GROUPS & MAILING LISTS	Can use search engines, 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 e-mail headers to identify system information
INFORMATION LEAKAGE	Can obtain information about a target network from information leaked in email headers, HTML meta tags and other locations, such as an internal network IP addresses
BANNER GRABBING	Can enumerate services, their software types and versions, using banner grabbing techniques
SNMP	Can retrieve information from SNMP services and understands the MIB structure pertaining to the identification of security vulnerabilities
PHISHING	Understands common phishing techniques and how these can lead to compromise
	Recognises when vulnerabilities discovered elsewhere can be leveraged as part of a phishing campaign

NETWORKING KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

NETWORK ARCHITECTURE

- Can interpret logical network diagrams
- Understands the various networks types that could be encountered during a penetration test:
  • CAT 5 / Fibre • 10/100/1000baseT • Wireless (802.11)
- Understand the difference beween LAN and WAN
- Understand internal (RFC 1918) IP ranges
- Understand basic subnetting
- Understand basics of IPv6 addressing
- Understand the security implications of copper cables vs fibre
- Understands the security benefits of tiered architectures, DMZs and air gaps
- Understands the security implications of shared media and can exploit its vulnerabilities during a penetration test
- 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

NETWORK ROUTING

- Understand default gateways and static routes
- Demonstrate ability to configure static IPs and routes
- Understands network routing and its associated protocols, including:
  • RIP• OSPF • EIGRP • BGP • IGMP
- Understands the security attributes of these protocols

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 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
- Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices
- Understand and exploit PXE

MANAGEMENT PROTOCOLS

- Understands and can demonstrate the use of protocols often used for the remote management of devices, including:
  • Telnet • SSH 16 • HTTP/HTTPS
  • SNMP • Cisco Reverse Telnet
  • TFTP • NTP • RDP •VNC
- Can analyse e-mail headers to identify system information
- Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices
- Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices

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

CONFIGURATION ANALYSIS

- Understands configuration files of Cisco routers and switches and can advise on how their security can be approved (most common features, such as access-lists and enabled services)
- Can interpret the configuration files of other network devices, including those produced by a variety of vendors (most common features, such as access-lists and enabled services)

ROUTERS & SWITCHERS

- Understands and can demonstrate the exploitation of vulnerabilities in routers and switches, including the use of the following protocols:
  • Telnet • SSH • HTTP/HTTPS • TFTP • SNMP

VOIP

- Understands VoIP services, such as SIP, and can identify and fingerprint devices offering these services

MICROSOFT WINDOWS KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

RECONNAISSANCE

- Can identify Windows hosts on a target network
- Can identify forests, domains, domain controllers, domain members and work groups
- Can enumerate accessible Windows shares
- Can identify and analyse internal browse lists
- Can identify and analyse Service Principle Names
- Understands and can identify the different types of domain trusts, including:
  • One-way and two-way trusts • Explicit and transitive trusts

ENUMERATION

- Can perform user and group enumeration on target systems and domains, using protocols including:
  • NetBIOS • LDAP • SNMP
- Can obtain other information, such as password policies
- Can perform analysis of an AD (Global catalogue, Master Browser and FSMO)
- Can perform SID enumeration and RID cycling

ACTIVE DIRECTORY

- Understands Active Directory structure
- Understands the reliance of Active Directory on DNS and LDAP
- Understand difference between local and domain users
- Understand the security weaknesses of shared local administrative accounts
- Understands Group Policy
- Understands Local Security 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
- Can demonstrate the recovery of password hashes when given physical access to a Windows host
- Understands and can demonstrate off-line password cracking using dictionary and brute-force attacks, including the use of rainbow tables
- Identify inappropriate accounts or group memberships
- Perform basic SPN/kerberoasting
- Exploit shared local administrative accounts by passing-the-hash
- Obtain passwords from Group Policy Preferences
- Perform more advanced Kerberos attacks (golden/silver tickets/etc)
- Identify inappropriate or dangerous Group Policies or permissions
- Understands Active Directory roles (Global Catalogue, Master Browser, FSMO)

PASSWORDS

- Understands password policies, including complexity requirements and lock-out
- Understands how to avoid causing a denial of service by locking-out accounts
- Understands the security attributes of the above protocols and technologies
- Understands Windows 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, including the use of rainbow tables
- Can demonstrate the recovery of password hashes when given physical access to a Windows host

REMOTE VULNERABILITIES

- Understands the use of tools and techniques to identify new OS and software vulnerabilities
- Understands and can demonstrate the remote exploitation of Windows operating system and third-party software application vulnerabilities
- Understands the techniques used to develop exploit code for existing and new vulnerabilities

LOCAL VULNERABILITIES

- Understands and can demonstrate the remote exploitation of Windows operating system and third-party software application vulnerabilities
- 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
- Understands and can demonstrate local privilege escalation techniques, e.g. through the manipulation of insecure file system or service permissions
- Understand the difference between "Local Service", "Network Service and "Local System"
- Demonstrate the ability to extract service credentials from LSA secrets

POST EXPLOITATION

- Understands and can perform common post exploitation activities, including:
  • obtaining password hashes, both from the local SAM and cached credentials
  • 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

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

PATCH MANAGEMENT

- Understands OS lifecycle management
- Understands patching in air-gapped environments
- Understands common windows patch management strategies, including:
  • SMS • SUS • WSUS

EXCHANGE

- Can identify and analyse Microsoft Exchange servers
- Understands and can perform common attack vectors for Microsoft Exchange Server

COMMON WINDOWS APPLICATIONS

- Can identify and leverage significant vulnerabilities in common windows applications for which there is public exploit code available

UNIX SECURITY KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

RECONNAISSANCE

- Can identify Unix hosts on a target 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 and RID cycling
- Is aware of legacy user enumeration techniques such as rusers and rwho
- Can enumerate RPC services and identify those with known security vulnerabilities

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 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 UNIX host
- Understands the format of the passwd, shadow, group and gshadow files

REMOTE VULNERABILITIES

- Understands and can demonstrate the remote exploitation of Solaris and Linux operating system vulnerabilities

LOCAL VULNERABILITIES

- Understands and can demonstrate Local privilege escalation techniques, e.g. through the manipulation of insecure file system permissions
- Understands and can demonstrate the local exploitation of Solaris and Linux operating system vulnerabilities

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

FTP/TFTP

- 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 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

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

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

SSH

- Understand that SSH can be used for port forwarding and file transfer
- 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
- Demonstrate ability to use forward and reverse port forwarding

X COMMAND

- 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
- Can describe the differences between X and %SYSRC and the typical use cases within a test

SENDRAIL/ SMTP

- Understands and can demonstrate valid username discovery via EXPN and VRFY
- Awareness of recent sendmail vulnerabilities and ability to exploit them if possible
- Understands mail relaying

PATCHING

- Understands backported patches, and the effect they have on scanning tools
- Understands OS lifecycle management
- Understands enterprise patching strategies for Linux
- Understands patching in air-gapped environments
- Understands security implications of installing software outside of OS package manager

SUDO

- Understands purpose of using sudo rather than logging in as root
- Understands difference between sudo and su
- Demonstrates ability to exploit weak sudo configuration

DATABASES KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

RECONNAISSANCE

- 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 use stored procedures to execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host

ORACLE

- Understands and can demonstrate the remote exploitation of an Oracle database
- Understands the security attributes of the Oracle TNS Listener service
- Can demonstrate how the software version and patch status can be obtained from an Oracle database
- Understands and can demonstrate how access can be gained to an Oracle database 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 an Oracle database server, can use stored procedures to execute system commands, escalate privileges, read/write from/to the file system, and/or gain further access to a host

OTHER DATABASES

- Understands and can demonstrate the remote exploitation of other common SQL database servers, such as MySQL and PostgreSQL
- Understands and can demonstrate the remote exploitation of common no-SQL database servers, such as MongoDB
- Understands and can demonstrate how access can be gained to such a database 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)

DATABASE CONNECTIVITY

- Understands common connection and authentication methods used by web applications to connect to database servers
- Can recognise common database connection string formats, e.g. JDBC

SQL SERVER

- Can identify running databases using from the SQL browser service
- Understands the difference between local SQL Server accounts and integrated auth, an the security implications of both
- Demonstrate ability to execute operating system commands without xp_cmdshell

WEB TECHNOLOGIES KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

WEB SERVERS

- Can identify web servers on a target network and can remotely determine their type and version
- Has knowledge of vulnerabilities in the following common application frameworks, servers and technologies:
  - .NET • J2EE • Coldfusion • Ruby on Rails • NodeJS
- Understands the purpose, operation, limitation and security attributes of web proxy servers
- Understands and can demonstrate the remote exploitation of web servers
- Understands the concepts of virtual hosting and web proxies

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

PROTOCOLS AND METHODS

- Understands all HTTP methods and response codes
- Understands HTTP Header Fields relating to security features
- Understands and can demonstrate the use of web protocols, including:
  - HTTP • HTTPS • Web Sockets
- Understands and can demonstrate HTTP Request Smuggling

LANGUAGES

- Understands common web mark-up and programming languages, including:
  - .NET • ASP Classic • Perl • PHP • JSP • Python • JavaScript
- Understands and can demonstrate how the insecure implementation of software developed using these languages can be exploited (candidate may select two languages)

API'S

- Understands and can demonstrate the use of web-based APIs to remotely access remote services
- Understands the use of tools and techniques to identify new OS and software vulnerabilities
- Understands common authentication techniques used in web APIs, e.g. API keys
- Can demonstrate the use of relevant tools to test APIs, e.g. SoapUI and Postman
- 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

INFORMATION GATHERING

- Can gather information from a web site and application mark-up or programming language, 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

AUTHENTICATION

- Understands common authentication vulnerabilities, including:
  - Transport of credentials over an unencrypted channel
  - Testing for username enumeration • Brute-force testing • Authentication bypass
  - Session hijacking • Insecure password reset features • Insufficient logout timeout/functionality
  - Vulnerable CAPTCHA controls • Race Conditions • Lack of MFA

AUTHORISATION

- Understands common pitfalls associated with the design and implementation of application authorisation mechanisms

INPUT VALIDATION

- Understands the importance of input validation and how it can be implemented, e.g. allow-lists, deny-lists and regular expressions
- Understands the need for server-side validation and the flaws associated with client-side validation

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

CROSS SITE SCRIPTING (XSS)

- Understands cross-site-scripting (XSS) and can demonstrate the launching of a successful XSS attack
- Understands the difference between persistent (stored) and reflected XSS

INJECTION

- Can demonstrate the ability to identify, explain and prove the existence of the following types of network infrastructure vulnerabilities and exposures:
  - XXE • XML Injection • LDAP Injection • ORM injection • SSI injection
  - XPath injection • IMAP/SMTP injection • Code injection • OS Commanding

SQL INJECTION

- Identifying SQL injection
- Exploiting UNION based injection
- Exploiting auth bypass (' or 'a'='a)
- Exploiting SQL injection to execute operating system commands or read files

BLIND SQL INJECTION

- Can determine the existence of a blind SQL injection condition in a web application
- Can exploit a blind SQL injection vulnerability

SESSIONS

- Identifying JWTs
- Exploiting "none" signature or lack of signature checking in JWTs
- Understanding the difference between HMAC and public key JWTs
- Can identify the session control mechanism used within a web application
- Understands and can exploit session fixation vulnerabilities
- Understands the security implications of session IDs exposed in URLs
- Understands the role of sessions in CSRF attacks
- Identifying low entropy in sessions
- Brute-forcing weak HMAC keys in JWTs

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)

PARAMETER MANIPULATION

- Understands parameter manipulation techniques, particularly the use of client-side proxies

DIRECTORY TRAVERSAL

- Understands and can identify directory traversal vulnerabilities within applications

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

CRLF ATTACKS

- Can generate malicious payloads in a variety of common file formats

APPLICATION LOGIC FLAWS

- Can assess and exploit vulnerabilities within the functional logic, function access control and business logic of an application

PHYSICAL ACCESS & SECURITY KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

LOCKS	Understands how locks can be used to restrict access to computer hardware
TAMPER SEALS	Understands how tamper seals can be used to deter access to computer hardware
PLATFORM INTEGRITY	Understands platform integrity technologies, e.g. TPM.
BOOT SEQUENCE	Understands and can demonstrate the remote exploitation of common no-SQL database servers, such as MongoDB
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 vulnerabiliites into an operating system
RECOVERY FUNCTIONALITY	Understands the security attributes of operating system recovery functionality, e.g. Windows Recovery Console and Safe Mode
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

VIRTUALISATION & CONTAINERISATION

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

VIRTUALISATION PLATFORMS

Can identify use of popular virtualisation technologies, including:
• VMware • Microsoft HyperV • Citrix • Oracle VirtualBox

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

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

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

CONTAINERISATION

Understands the key differences between virtualisation and containerisation

Can identify and interrogate running containers on a host

Understands the concepts of layered filesystems and
how to extract and analyse specific layers within an image

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

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 30
• Inclusion of sensitive information, e.g. passwords or private keys
• Unnecessary exposure of ports

Understand the security implications
of using third-party containers

Understand how to manage containers
throughout their lifecycle

Understand the functionality
offered by Kubernetes

Understand the security implications
of using Kubernetes

Understand the different deployment models
(OpenShift, EKS/AKS,
Docker on a single server, etc)

CLOUD SECURITY KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

AUTHORISATION	Understands the importance of obtaining authorisation from cloud hosting providers and the potential effects on permitted types of testing during engagements
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)
LOGGING & 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
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
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
CLOUD ARCHITECTURE	Understand the differences between cloud and on-prem architecture. Understand how to link between the two
	Understand the different security responsibility boundaries between IaaS, PaaS and SaaS
AZURE	Identify and understand the key administrative roles in Azure
	Identify the Azure metadata service
	Understand and review conditional access policies
	Understand the difference between AD, Azure AD DS and Azure AD
AWS	Identify and understand the key administrative roles in AWS
	Understand the difference between roles and policies
	Identify the AWS metadata service
MOBILE DEVICE MANAGEMENT	Understand the purpose MDM solutions and the functionality they offer
	Review MDM configuration policies

SECURE DEVELOPMENT OPERATIONS KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

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

SECURITY AS CODE

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

INFRASTRUCTURE AS CODE

Understands the role of tools to automate the building, configuration and deployment of infrastructure, including:
- Terraform
- Puppet
- Ansible
- Chef

Can identify and advise on common security misconfigurations of these tools

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