THE CSTL-INF

(CYBER SCHEME TEAM LEADER - INFRASTRUCTURE).

SETTING THE STANDARD IN TECHNICAL EXAMINATIONS FOR SECURITY TESTERS.

ABOUT THE EXAM

The Cyber Scheme Team Leader (CSTL) infrastructure exam tests candidates' knowledge and expertise of common network services and weaknesses along with an understanding of operating systems and networking.

Candidates are expected to be able to demonstrate a high level of understanding of different protocols & services, Operating System's and network devices to demonstrate they are able to identify, assess and exploit common misconfigurations or vulnerabilities to move laterally through a network identifying the key areas of weakness within the environment.

A pass in this highly regarded technical qualification is a mandatory requirement for the Principal and Chartered Level Professional Title with the UK Cyber Security Council (security testing).

CSTL-INF assessment components

Phase 1 – Scoping

Candidates will share a common scoping briefing. Following the common scoping briefing, individually candidates will have up to 10 minutes to ask questions concerning the scope of the penetration test. During the individual scoping session, the Assessor will play the role of the commissioning client. The candidate's performance during the individual scoping session will form part of the assessment.

Phase 2 – Practical Penetration Test

The candidate's laptop will be connected to the assessment infrastructure, from which they will perform the practical penetration test, as defined in the scoping session. Connectivity will end after 4.5 hours. During the final 30 minutes the candidate will be advised to prepare for the interview which follow.

Phase 3 – Interview

During the interview the candidate will be required to produce a network diagram on a white board or flip chart. The network diagram must logically detail the infrastructures architecture at the network/IP layer (OSI layer 3), clearly showing all hosts, interfaces, subnets, subnet masks, firewalls and routes. The interview is an assessed component of the examination.

A candidate will also be expected to inform the commissioning client (Assessor) of the significant aspects/findings during the practical penetration test they conducted.

KNOWLEDGE DOMAINS

- Engagement Lifecycle and Risk
- Core Technical Knowledge
- Information Gathering
- Networking
- Microsoft Windows Security
- UNIX Security
- Databases
- Web Technologies
- Physical Access and Security
- Virtualisation and Containerisation
- Cloud Security
- Secure Development Operations

Please note the knowledge domains and topics outlined in this document are for guidance only and subject to change.

ENGAGEMENT, LIFESTYLE AND RISK .1

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)

ENGAGEMENT, LIFESTYLE AND RISK .2

Understanding and 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 and 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

ENGAGEMENT, LIFESTYLE AND RISK .3

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 and Presentation

For any given issue or group of issues, ability to convey:
I . 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 .1

Hardware Security

Understands common risks associated with Bluetooth, including: • Bluesnarfing • Bluejacking • Bluebugging

Understands how side-channel attacks can aid cryptanalysis and otherwise expose sensitive data

Understands the concepts behind side-channel attacks such as timing analysis and power analysis

Understands the concepts behind common microprocessor vulnerabilities such as Spectre and Meltdown

Build Review

Understands and can test against common build standards such as CIS benchmarks

Demonstrate the ability to perform a security build review of common operating systems

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

Patch Levels

Can obtain operating system patch levels on UNIX-like and Windows operating systems

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)

Traffic Filtering and Access Control

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

Can demonstrate methods by which traffic filters can be bypassed

Understands the devices and technology that implement traffic filtering, such as firewalls, and can advise on their configuration

Understands network traffic filtering and where this may occur in a network

Fingerprinting

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

CORE TECHNICAL KNOWLEDGE .2

Service Identification

Understands advanced analysis techniques for unknown services and protocols

Understands the methods associated with unknown service identification, enumeration and validation

Can state the purpose of an identified network service and determine its type and version

Can identify the network services offered by a host by banner inspection

Port Scanning

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

Understands different TCP connection states

Packet Generation

Understands packet fragmentation

Understands the different types of packets that are likely to be encountered during a penetration test

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

Using tools and interpreting output

Can effectively use command line during assurance testing

Can identify when tool output can and cannot be trusted. Can demonstrate an approach to verifying tool output

Interpret and understand the output of tools, including those used for port scanning, vulnerability scanning, enumeration, exploitation and traffic capture

Understand the limitations of automated testing

Can use a variety of tools during a penetration test, selecting the most appropriate tool to meet a particular requirement

Demonstrate ability to carry out testing when tools are not available or functional

CORE TECHNICAL KNOWLEDGE .3

Pivoting

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

Can demonstrate pivoting through a number of devices in order to gain access to targets on a distant subnet

Understand the concept of pivoting through compromised devices

Cryptography

Identify and exploit weaknesses in custom cryptography

Understand best practices around key management

Understand the differences between encryption modes (EBC, CBC, GCM, etc)

Understand the dangers of implementing custom cryptography

Understands the difference between encoding and encrypting

Understands PKI and the concepts of IKE Certificate Authorities and trusted third parties

Understands the generation and role of HMACs

Understands different authentication methods such as passwords and certificates

Understands common hash functions, such as MD5, SHA1 and SHA256 including their security attributes and how they can be attacked

Understands common cryptographic algorithms, such as DES, 3DES, RSA, RC4 and AES, including their security attributes and how they can be attacked

Understands the differences between symmetric and asymmetric cryptography and can give examples of each

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 common encrypted protocols and software applications, such as SSH, SSL, IPSEC and PGP

Understands cryptography and its use in a networked environment

Identify and exploit weaknesses in custom cryptography

CORE TECHNICAL KNOWLEDGE .4

File System Permissions and System Processes

Can identify running processes on UNIX-like and Windows operating systems and exploit vulnerabilities to escalate privileges

Can find “interesting’ files on an operating system, e.g. those with insecure or “unusual” permissions, or containing user account passwords

Understands and can demonstrate the manipulation of file system permission on UNIX-like and Windows operating systems

IP Protocols

Understands the security implications of using clear-text protocols,such as Telnet and FTP

Understands common IP/Ethernet protocols and their associated security attributes, including: • TCP • UDP • ICMP • ARP • DHCP • DNS • CDR HSRP • VRRP • VTP • STP • TACACS+

Understands IPv4 and IPv6 and their associated security attributes

INFORMATION GATHERING .1

Phishing

Recognises when vulnerabilities discovered elsewhere can be leveraged as part of a phishing campaign

Understands common phishing techniques and how these can lead to compromise

SNMP

Can retrieve information from SNMP services and understands the MIB structure pertaining to the identification of security vulnerabilities

Banner Grabbing

Can enumerate services, their software types and versions, using banner grabbing techniques

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

Search Engines, News Groups and Mailing Lists

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

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

Website Analysis

Can analyse information from a target web site, both from displayed content and from within the HTML source

Can interrogate a website to obtain information about a target network, such as the name and contact details of the network administrator

INFORMATION GATHERING .2

DNS

Can identify the presence of dangling DNS entries and understands the associated security vulnerabilities (e.g. susceptibility to subdomain takeover)

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 demonstrate how a DNS server can be queried to obtain the information detailed in these records

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

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

NETWORKING .1

VOIP

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

Routers and Switches

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

Configuration Analysis

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)

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)

Traffic Analysis

Understands network access control systems, such as 802.1x and MAC address filtering, and can Understands and can demonstrate how network traffic can be analysed to recover user account credentials and detect vulnerabilities that may lead to the compromise of a target device

Can intercept and monitor network traffic, capturing it to disk in a format required by analysis tools (e.g. PCAP)

Management Protocols

Can analyse e-mail headers to identify system information

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

NETWORKING .2

Network Mapping

Can demonstrate the mapping of a network using a range of tools, such as traceroute, traceroute and ping, and by querying active searches, such as DNS and SNMP servers

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

Can accurately identify all hosts on a target network that meet a defined set of criteria, e.g.. to identify all FTP servers or CISCO routers

Understand and exploit PXE

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 • EIG RP • BGP • IG MP

Understands the security attributes of these protocols

Network Architecture

Understands the security implications of shared media and can exploit its vulnerabilities during a penetration test

Understands the security implications of VLANS

Understands the security implications of switched networks

Understands the security benefits of tiered architectures, DMZs and air gaps

Understand the security implications of copper cables vs fibre

Understand basics of IPv6 addressing

Understand basic subnetting

Understand internal (RFC 1918) IP ranges

Understand the difference between LAN and WAN

Understands the various networks types that could be encountered during a penetration test: • CAT 5 / Fibre • 10/100/1000baseT • Wireless (802.11)

Can interpret logical network diagrams

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

MICROSOFT WINDOWS SECURITY .1

Reconnaissance

Understands and can identify the different types of domain trusts, including: • One-way and two-way trusts • Explicit and transitive trusts

Can identify and analyse Service Principal Names

Can identify and analyse internal browse lists

Can enumerate accessible Windows shares

Can identify forests, domains, domain controllers, domain members and work groups

Can identify Windows hosts on a target network

Common Windows Applications

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

Exchange

Understands and can perform common attack vectors for Microsoft Exchange Server

Can identify and analyse Microsoft Exchange servers

Patch Management

Understands OS lifecycle management

Understands patching in air-gapped environments

Understands common windows patch management strategies, including: • SMS • SUS • WSUS

Desktop Lockdown

Can perform privilege escalation techniques from a desktop environment

Understands and can demonstrate techniques to break out of a locked down Windows desktop or Citrix environment

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

MICROSOFT WINDOWS SECURITY .2

Local Vulnerabilities

Demonstrate the ability to extract service credentials from LSA secrets

Understand the difference between "Local Service", "Network Service and "Local System"

Understands and can demonstrate local privilege escalation techniques, e.g. through the manipulation of insecure file system or service permissions

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

Remote 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

Passwords

Understands how passwords are stored and protected and can demonstrate how they can be recovered

Understands how to avoid causing a denial of service by locking-out accounts

Can demonstrate the recovery of password hashes when given physical access to a Windows host

Understands Windows password hashing algorithms and their associated security attributes

Understands the security attributes of the above protocols and technologies

Understands password policies, including complexity requirements and lock-out

Understands and can demonstrate off-line password cracking using dictionary and brute-force attacks, including the use of rainbow tables

MICROSOFT WINDOWS SECURITY .3

Active Directory

Can demonstrate the recovery of password hashes when given physical access to a Windows host
Obtain passwords from Group Policy Preferences
Exploit shared local administrative accounts by passing-the-hash
Perform basic SPN/kerberoasting
Identify inappropriate accounts or group memberships
Understands and can demonstrate off-line password cracking using dictionary and brute-force attacks, including the use of rainbow tables
Understands user accounts and can manipulate these accounts to gain further access to a target system, e.g. by escalating privileges from a domain user to a domain admin
Understands Local Security Policy
Understands Group Policy
Understand the security weaknesses of shared local administrative accounts
Understand difference between local and domain users
Understands the reliance of Active Directory on DNS and LDAP
Understands Active Directory structure
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)

UNIX SECURITY .1

Sudo

Demonstrate ability to exploit weak sudo configuration

Understand difference between sudo and su

Understand purpose of using sudo rather than logging in as root

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

Reconnaissance

Can identify Unix hosts on a target network

Sendmail/SMPT

Understands mail relaying

Awareness of recent sendmail vulnerabilities and ability to exploit them if possible

SSH

Can demonstrate how trust relationships can lead to the compromise of a server, allow a user to escalate privileges and/or gain further access to a host, e.g. through the use, creation or modification of –/.ssh/ authorized_keys files

Understands 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

Understand that SSH can be used for port forwarding and file transfer

Demonstrate ability to use forward and reverse port forwarding

UNIX SECURITY .2

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

NFS

Understands how NFS exports can be restricted at both a host and file level

Understands the concepts of root squashing, nosuid and noexec options

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 NFS and its associated security attributes and can demonstrate how exports can be identified

FTP/TFTP

Understands and can exploit TFTP within a Cisco environment

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 the security implications of anonymous FTP access

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

Understand that SSH can be used for port forwarding and file transfer

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

UNIX SECURITY .3

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

Remote Vulnerabilities

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

Passwords

Can demonstrate the recovery of password hashes when given physical access to a UNIX host

Understands and can demonstrate off-line password cracking using dictionary and brute-force attacks

Understands UNIX password hashing algorithms and their associated security attributes

Understands users, groups and password policies, including complexity requirements and lock-out

Understands how passwords are stored and protected and can demonstrate how they can be recovered

Understands how to avoid causing a denial of service by locking-out accounts

Understands the format of the passwd, shadow, group and gshadow files

Enumeration

Can enumerate RPC services and identify those with known security vulnerabilities

Is aware of legacy user enumeration techniques such as rusers and rwho

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

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

DATABASES .1

SQL Server

Understands the difference between local SQL Server accounts and integrated auth, an the security implications of both

Can identify running databases using from the SQL browser service

Demonstrate ability to execute operating system commands without xp_cmdshell

Database Connectivity

Can recognise common database connection string formats, e.g. JDBC

Understands common connection and authentication methods used by web applications to connect to database servers

Other Databases

Understands and can demonstrate how access can be gained to such a database server through the use of default accounts credentials and insecure passwords

Understands and can demonstrate the remote exploitation of common no-SQL database servers, such as MongoDB

Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible)

Oracle

Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible)

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

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

DATABASES .2

Reconnaissance

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

Can identify and extract useful information stored within a database (e.g. user account names and passwords, recovering passwords where possible)

Understands and can demonstrate how access can be gained to a Microsoft SQL server through the use of default accounts credentials and insecure passwords

Understands and can demonstrate the remote exploitation of Microsoft SQL Server

WEB TECHNOLOGIES .1

Application Logic Flaws

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

CRLF Attacks

Can generate malicious payloads in a variety of common file formats

File Uploads

Can generate malicious payloads in a variety of common file formats

Understands the role of MIME types in relation to file upload features

Understands and can identify common vulnerabilities with file upload capabilities within applications

Directory Traversal

Understands and can identify directory traversal vulnerabilities within applications

Parameter Manipulation

stands parameter manipulation techniques L particularly the use of client-side proxies

Cryptography

Identification and exploitation of Encoded values (e.g. Base64)

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)

Understands how cryptography can be used to protect data in transit and data at rest, both on the server and client side

WEB TECHNOLOGIES .2

Sessions

Understands the security implications of session IDs exposed in URLs

Understands the role of sessions in CSRF attacks

Understands and can exploit session fixation vulnerabilities

Can identify the session control mechanism used within a web application

Understanding the difference between HMAC and public key JWTs

Exploiting "none" signature or lack of signature checking in JWTs

Identifying JWTs

Identifylng low entropy In sessions

Brute-forcing weak HMAC keys In JWTs

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

Blind SQL Injection

Can exploit a blind SQL injection vulnerability

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

SQL Injection

Exploiting SQL injection to execute operating system commands or read files

Exploiting auth bypass (' or 'a'='a)

Exploiting UNION based injection

Identifying SQL injection

Cross-Site Scripting (XSS)

Understands the difference between persistent (stored) and reflected XSS

Understands cross-site-scripting (XSS) and can demonstrate the launching of a successful XSS attack

WEB TECHNOLOGIES .3

Input Validation

Understands the need for server-side validation and the flaws associated with client-side validation

Understands the importance of input validation and how it can be implemented, e.g. allow-lists, deny-lists and regular expressions

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

Information Gathering

Can gather information about a web site and application from the error messages it generates

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

APIs

Understands how to interpret definition files, e.g. WSDL and Swagger

Understands different common payload formats such as XML and JSON

Understands and can demonstrate how the insecure implementation of web-based APIs can be exploited

Can demonstrate the use of relevant tools to test APIs, e.g. SoapUI and Postman

Understands common authentication techniques used in web APIs, e.g. API keys

Understands and can demonstrate 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

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

WEB TECHNOLOGIES .4

Languages

Understands and can demonstrate how the insecure implementation of software developed using these languages can be exploited (candidate may select two languages)

Understands common web mark-up and programming languages, including: • .NET • ASP Classic • Perl • PHP • JSP • Python • JavaScript

Protocols and Methods

Understands and can demonstrate the use of web protocols, including: • HTTP • HTTPS • Web Sockets

Understands HTTP Header Fields relating to security features

Understands all HTTP methods and response codes

Understands and can demonstrate HTTP Request Smuggling

Web Servers

Understands the concepts of virtual hosting and web proxies

Understands and can demonstrate the remote exploitation of web servers

Understands the purpose, operation, limitation and security attributes of web proxy servers

Can identify web servers on a target network and can remotely determine their type and version

Reconnaissance

Understands and can identify the different types of domain trusts, including: • One-way and two-way trusts • Explicit and transitive trusts

Can identify and analyse Service Principal Names

Can identify and analyse internal browse lists

Can enumerate accessible Windows shares

Can identify forests, domains, domain controllers, domain members and work groups

Can identify Windows hosts on a target network

PHYSICAL ACCESS AND SECURITY

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

Recovery Functionality

Understands the security attributes of operating system recovery functionality, e.g. Windows Recovery Console and Safe Mode

Disk Encryption

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 security implications of unencrypted storage devices, such as hard disks

Boot Sequence

Understands and can demonstrate the remote exploitation of common no-SQL database servers, such as MongoDB

Platform Integrity

Understands platform integrity technologies, e.g. TPM

Tamper Seals

Understands how tamper seals can be used to deter access to computer hardware

Locks

Understands how locks can be used to restrict access to computer hardware

VIRTUALISATION AND CONTAINERISATION .1

Containerisation

Understand the functionality offered by Kubernetes
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)

VIRTUALISATION AND CONTAINERISATION .2

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

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

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

CLOUD SECURITY .1

Mobile Device Management

Review MDM configuration policies

Understand the purpose MDM solutions and the functionality they offer

AWS

Understand the difference between roles and policies

Identify and understand the key administrative roles in AWS

Azure

Understand the difference between AD, Azure AD DS and Azure AD

Understand and review conditional access policies

Identify and understand the key administrative roles in Azure

Understand the difference between AD, Azure AD DS, and Azure AD

Cloud Architecture

Understand the different security responsibility boundaries between IaaS, PaaS and SaaS

Understand the differences between cloud and on-prem architecture. Understand how to link between the two

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

Identity and Access Management

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

Logging and Monitoring

Can analyse logging configuration within a cloud environment and advise on improvements

Can analyse the configuration of resource monitoring and alarm generation and advise on improvements

CLOUD SECURITY .2

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)

Authorisation

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

SECURE DEVELOPMENT OPERATIONS

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

Infrastructure as Code

Can identify and advise on common security misconfigurations of these tools: Puppet • Ansible • Chef

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

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