



Security Testing Methodology, Tools and Resources

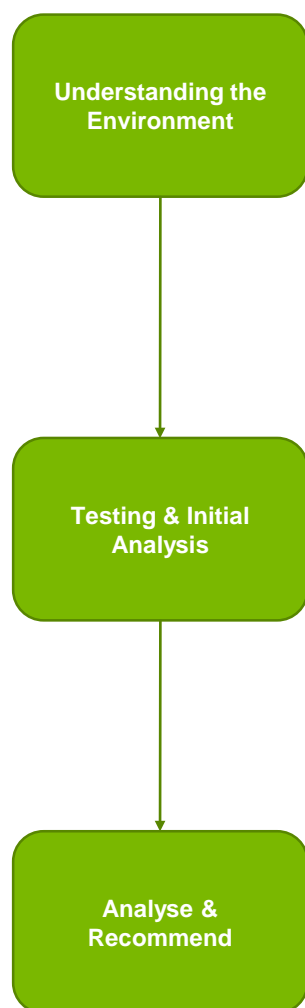
2021

Contents

	Page
Security Testing Process	2
Infrastructure Penetration Testing	5
Application Security Testing	11
Mobile Application Assessment	24
PCI Compliance Readiness	26
Wireless Security Assessment	28
Security Awareness Training	30
The KPMG Firewall Review	33
KPMG Host Reviews	36
Incident Response and Malware Analysis	39
Source Code Audit	46

Security Testing Process

Security Testing Process: Engagement Management



Our security testing engagements consist of three stages:

Understanding the Environment

We evaluate the operating environment and business-specific risks which enables us to focus our efforts on the areas that may represent most significant risk to the organisation. We base our understanding of the environment on information supplied by the client and perform our risk analysis by means of:

- interviews or workshops with risk owners or their representatives
- review of existing risk analysis documentation

In this stage, we also agree with the client the risk rating and risk domains. Typically, these are:

- Technical risk
- Business risk
- Regulatory risk

Testing & Initial Analysis.

Actual security testing is performed to identify risk and issues using the relevant methodologies. Efforts are focused on potential risk areas identified in earlier stages and appropriate tools and techniques are utilised accordingly. We also report identified issues along with their initial technical risk evaluation on issues that may require clients' immediate attention using our Rapid Reporting approach.

Analyse & Recommend.

In this stage we perform the business impact analysis of identified issues using the rating and domains agreed in the first stage. Each issue is triaged according to its urgency, and actionable based on its short, medium or long term recommendations. A root cause analysis is performed to identify the root cause of each issue in an attempt to discern if it was a single failure of the organisation's processes and procedures or if it is a more systemic issue that requires process improvements.

Typically, the deliverable of a security test is a formal report which describes in detail the work performed, results and recommendations. All KPMG reports are written for multiple audiences:

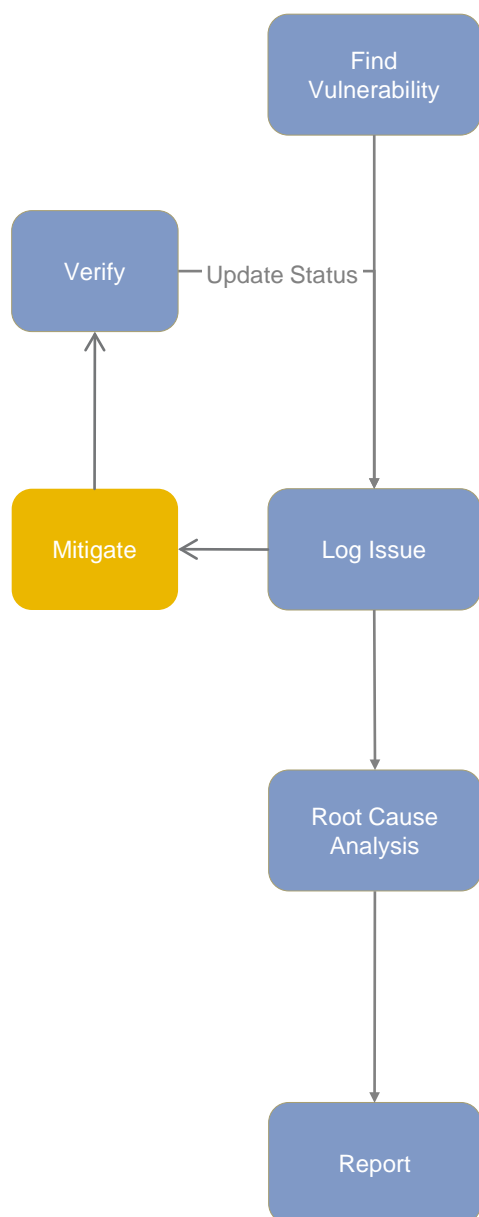
- **Senior management** is provided with a concise and to-the-point summary in easy to understand business English language along with strategic recommendations if applicable.
- **Middle management and line management** are provided with aggregate diagrams and figures, such as heat maps, enabling them to quickly prioritise remediation actions. Strategic and tactical advice for security improvement is also provided.
- **Staff responsible for actual remediation** is provided with detailed and technical description of issues as well as specific recommendations on how to address identified risks.

Quality & Risk Management

Any KPMG advisory engagement is subject to quality and risk management, which ensures that key risk management and quality issues are addressed. Key areas are:

- Resourcing – qualified and motivated staff being available when required
- Ethics and independence – universal ethics and independence rules to ensure that we are not conflicted in any way prior to and during the engagement
- Quality – processes and procedures that ensure that any work we deliver is of professional quality and has had appropriate amount of professional oversight by managers, directors and partners
- Data protection – confidentiality of all client information and reports containing client data are adequately protected against current threats.

Security Testing Process: Reporting and Communication



Rapid Reporting Cycle

The overall objective of the rapid reporting cycle is to reduce the time from the instant a security issue is identified to when it is mitigated. This is in contrast to traditional reporting, when the consultant delivers the report only at the end of engagement, here each issue along with its initial technical risk assessment is reported to the client shortly after its discovery, enabling the client to act on it immediately. This is achieved by the use of our collaboration tool that facilitates this kind of work flow. An outline of the process is described below:

Find vulnerability and log issue

Vulnerability is discovered and logged in the collaboration environment by KPMG along with initial assessment of technical risk, short-term recommendations and supporting evidence. The existence of high risk findings will be additionally notified by an e-mail alert, phone or other agreed communication channels.

Mitigate

The client has the opportunity to react to it immediately and to begin the remediation process. This step is executed by the client with clarifications and support from KPMG if required.

Verify

When the client has mitigated the vulnerability, KPMG verifies that it is mitigated and that it has not introduced undesirable side effects. If the vulnerability is remedied, its status in the collaboration tool is updated accordingly.

Root cause analysis

Root cause analysis of identified issue is performed.

Reporting

The final report is issued with identified issues and root causes.

Communication

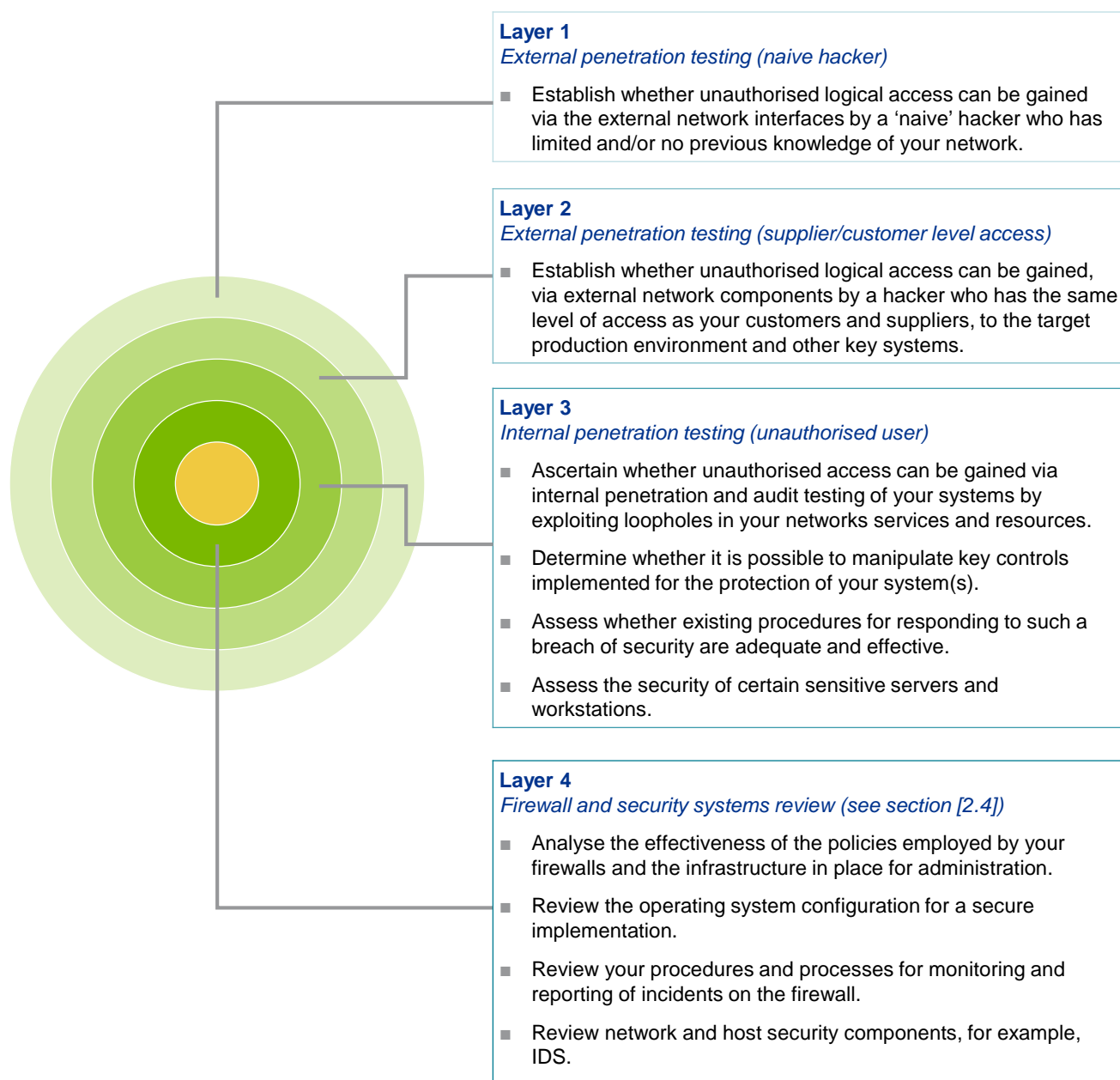
- To facilitate a high quality and effective process, we will use an online collaboration environment. Representatives of the client team will join this collaboration environment and be able to monitor progress as well as provide key input where necessary.
- For real-time communication we will be able to use the collaboration environment's built in chat function, phone and phone conferencing. All e-mail conversations that are of a general nature to the project (not sensitive) will be recorded by CC'ing a special, dedicated e-mail address. This record will be available to collaboration team members.
- If a more interactive online conferencing is necessary, we will organise it using WebEx online meeting services or meet the client in person.

Infrastructure Penetration Testing

Infrastructure Penetration Testing

To facilitate the provision of this service to our clients, we have designed an approach that identifies the most serious risks and security flaws first and then focuses on less obvious areas as the project proceeds. This can be illustrated by the onion skin model.

Our model illustrates how we first test the client network for vulnerabilities from the outside. Initially, we will conduct this test assuming the point of view of an uninformed attacker. We then gradually move on until we assume the role of a trusted user of the network trying to access an unauthorised resource or service. The following list gives some more detail as to the specifics of each level.



The consistent deployment of this approach is ensured by the use of cutting edge technology, and our policy to only use highly specialised staff that work in this area with the use of comprehensive work-programmes to enhance our quality control procedures.

Infrastructure Penetration Testing (cont.)

Focus of our testing

- Our testing is focused on providing clients with a level of confidence that their Internet and LAN infrastructure is secure. However, our methodology is flexible enough, and our team are experienced enough to test the whole range of possible unauthorised access points of an organisation. These would include:
 - War-dialling and PABX hacking
 - Attacking corporate remote access servers
 - Attempting access via wireless access points
 - Attacks via partner organisation network links

Additional services

Open data source reconnaissance

- This is often used as a precursor to technical hacking, this would include extensive research into the background of target systems or organisational units, system users. A target profile is compiled that lists key associated systems, target employees for social engineering, etc.

Social engineering

- Social engineering attacks focus on manipulating users into performing actions imposed by the attacker, for example, opening a malicious document through e-mail or revealing confidential information or passwords over phone. KPMG can perform social engineering exercises to test organisation's defences against this threat.

Physical security

- Many organisations rely on the physical security of their building to a greater extent than their firewalls, yet do not test the physical security controls in place. KPMG can assist an organisation by reviewing these physical controls.

Resilience testing

- If you have a requirement to operate 24x7, you may have invested in resilient hardware and software. You may not however have tested how well this configuration works. We can provide a structured test plan to ensure the system meets its uptime requirements.

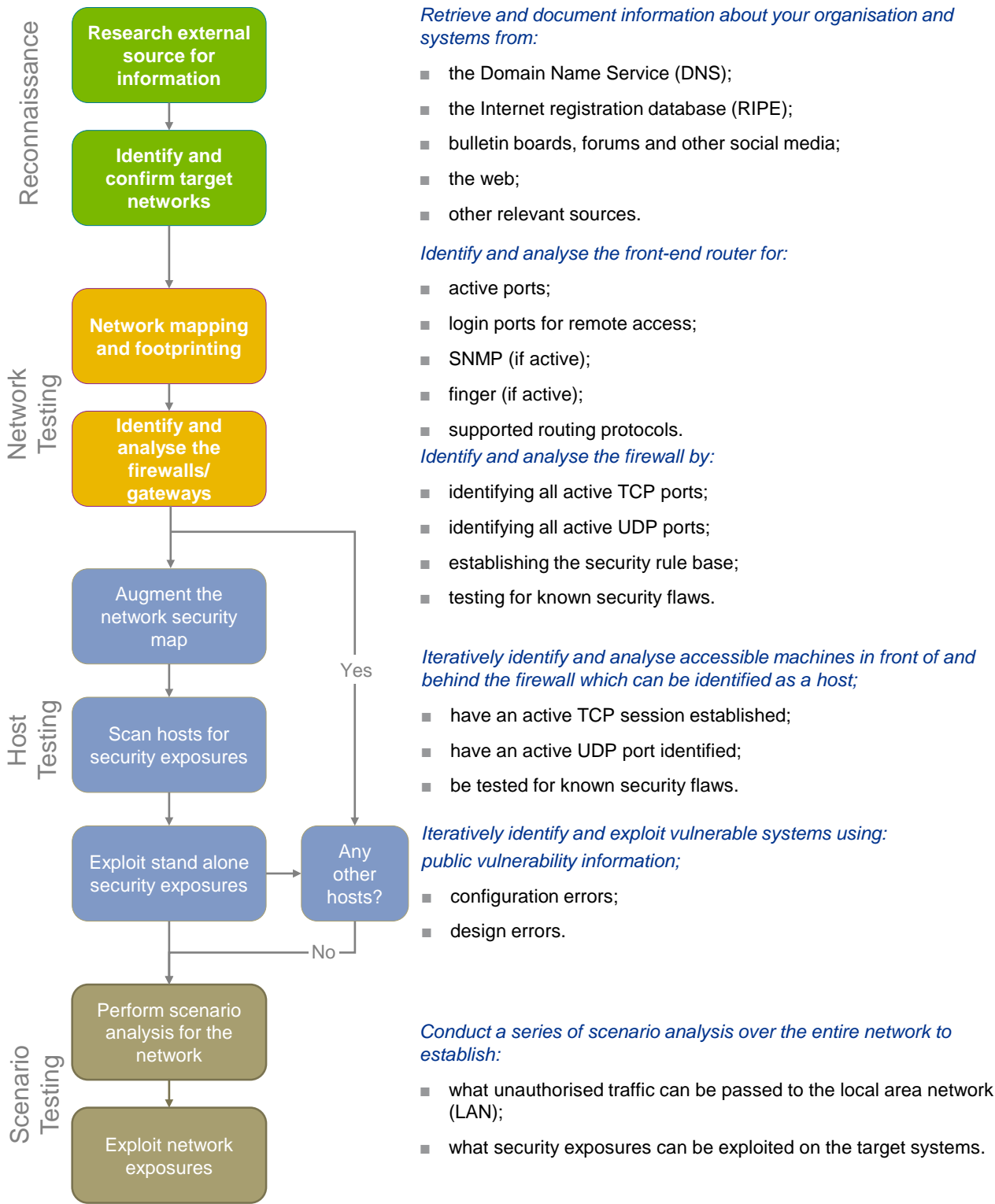
Performance testing

- In conjunction with our testing group, we can provide a performance profile for your hardware to establish if it meets your requirements. We can also perform application stress testing to ensure it can handle the anticipated load.

Infrastructure Penetration Testing: Testing Process

Testing Process

The figure below defines our structured approach to attacking a network.



Infrastructure Penetration Testing: Testing Tools

A number of tools are used during a penetration test, many of these will be specialised network diagnosis tools originating from the UNIX environment. Additional tools will be used to analyse available services on the network. These will include port analysers and network scanners.

Detailed below is a sample of the software tools used during penetration testing at KPMG:

Passive testing

Open source information gathering tools:

- dig, nslookup for DNS exploration
- Maltego
- whois
- FOCA
- GHDB, web search engines and archives
- Goolag Scanner

Passive network analysis tools:

- p0f
- tcpdump
- wireshark

Network testing

Custom scripts for exhaustive network testing of

- TCP services
- UDP services
- Other IP protocols (GRE, IPSEC etc.)
- NFS and SMB services
- Remote management software

Router and network management tools:

- SNMP tools
- RIP query

Network Mapping/tracing/packet dumping tools:

- Network Instruments' Observer
- unicornscan
- ping, sping, spray, probe
- NMAP
- traceroute
- tcpdump, etherfind
- DSNIFF
- snoop, Esniff
- Hping3
- Scapy

Vulnerability assessment

Service scanning tools:

- Nessus
- Metasploit Framework 3
- Nexpose
- nikto
- netcat

Fuzzers - new vulnerability discovery tools:

- Sully
- peach
- Taof
- Scapy

Infrastructure penetration testing:

Testing tools (cont.)

Scenario testing

Password cracking

- John the Ripper
- Cain and Abel
- rainbow tables, Ophcrack
- CeWL – tool for intelligent dictionary generation

Web

- Firefox with security testing extensions
- Internet Explorer for ActiveX and Silverlight testing
- Burp Suite Pro
- Accunetix

SSL

- SSLStrip, THCSSLCheck
- SslDump
- Nessus SSL plugins

Network subversion tools:

- IP spoofing tools
- TCP packet sequence attack tools
- Source routing/traffic redirection
- DNS spoofing tools
- ICMP bomb tools
- SYN flooding tools
- Bailiwicked – DNS cache poisoning
- Metasploit Framework
- Immunity CANVAS
- Iodide
- Scapy

In-house developed tools

- CHILLI – tool to detect rogue network egress points
- SABA – custom host audit scripts for Windows, Linux and UNIX
- iFramework – Injection framework (for SQL injection and XPath)
- WebEx – Web Exploration Tool
- Custom password cracking cluster CrackCloud
- Internet presence –a set of interlinked scripts to automatically gather information based on the client's registrations regarding Internet presence of client's worldwide.
- Iodide – A Cisco Interactive debugger and exploit framework

System, firewall and network equipment configuration review tools

- Nipper
- Winprobe
- SABA
- Custom review scripts for HP-UX, Solaris, Linux

Application Security Testing

Application Security Testing

The process of application security testing does not lend itself to automation and consequently no automated tools exist that can perform an adequate security assessment of a bespoke application.

External hackers that can compromise the security of a remote application are frequently in a position to launch a further attack from the trusted side of a firewall, potentially with access to internal databases and systems. All too often these attacks are carried out with little more than a web browser and will go un-noticed by many current intrusion detection systems.

Traditional systems-based penetration tests and security reviews do not generally identify application vulnerabilities where bespoke software and interfaces are involved.

Our approach is based on the latest version of the leading web security industry standard “OWASP Testing guide” complimented by KPMG’s proprietary security testing process.

How does gray or black box testing differ from white box testing?

During the black and grey box testing approaches, the security tester attempts to circumvent web application security using similar tools and methods as would a malicious attacker. Black box testing assumes no knowledge of internal workings of the system, while during grey box testing, the security tester has knowledge of some internal workings. Black and grey box testing methods are cost-effective means of assessing web application security and are most suitable when organisation assesses customised off-the-shelf applications or bespoke applications that are created by external teams.

White box security testing assumes full access to the application’s documentation, source code and operating environment and methods such as architecture reviews, code reviews and interviews with developers. This approach is more resource intensive, but offers greater assurance, detection of corner cases, complex business logic flaws and serves as useful training for developers involved. This method is therefore best suited when an application is developed by internal teams.

The KPMG approach to Application security testing

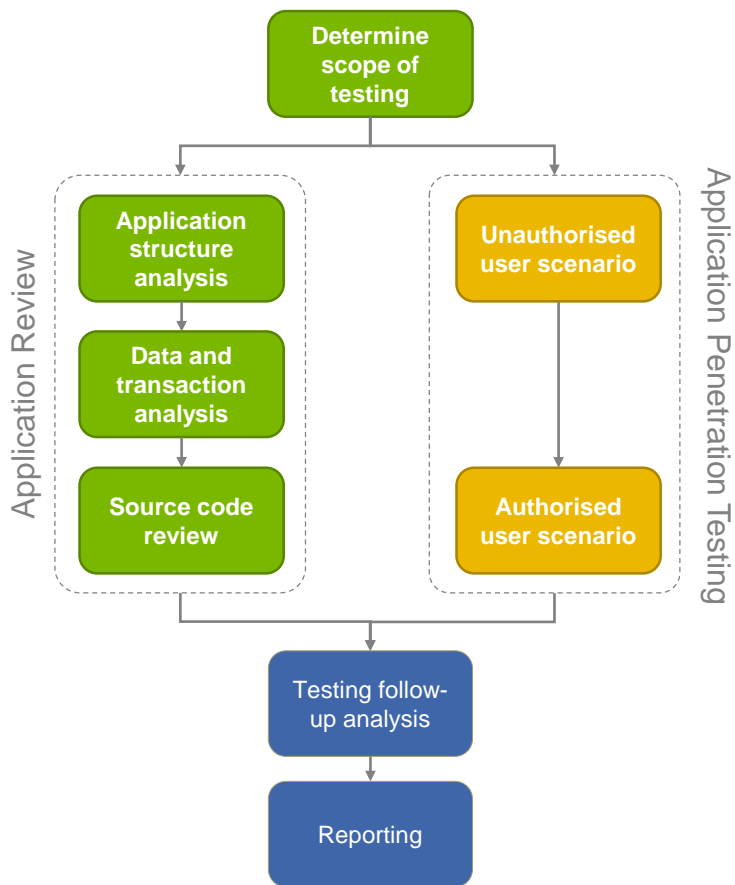
Each application and environment is unique, however, KPMG has developed a unified methodology that addresses the requirements of application security testing. The KPMG methodology for application security testing includes a dual approach:

White box testing

This is a detailed examination of the application architecture and software source code. Data and transaction processing within the architecture is examined as is application documentation and associated procedures.

Black/Grey box testing

This is a remote attack on the application from the perspective of both an authorised and unauthorised external user. This test simulates the type of action an external attacker would use to subvert security controls.



Application Security Control Areas

Below are detailed web application security control areas and their OWASP identifiers that KPMG checks as part of complete web application security testing, unless otherwise agreed with the client:

Information gathering

Web applications may inadvertently disclose information that is useful to the attacker by means of verbose response headers, error messages etc. or by using common conventions, such as an admin interface being located in "/admin". Furthermore, some of these error messages may be cached by search engines long after the message has been remedied in the application. The first phase in security assessment is focused on collecting as much information as possible about a target application.

OWASP control areas:

- OWASP-IG-001 Spiders, Robots and Crawlers -
- OWASP-IG-002 Search Engine
- OWASP-IG-003 Identify application entry points
- OWASP-IG-004 Testing for Web Application
- OWASP-IG-005 Application Discovery
- OWASP-IG-006 Analysis of Error Codes

Configuration management testing

Secure web application must be deployed on secure infrastructure. In this control area, the immediately supporting infrastructure is analysed for various misconfigurations that can be of an advantage to the attacker, for example, if application is deployed on top of a web server, does it use file extensions (.php, .aspx, .jsp, .pl) to handle dynamic programming? If so, then possibly by uploading a file with such extensions could allow attackers to take over the web server and circumvent the application security.

OWASP control areas:

- OWASP-CM-001 SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)
- OWASP-CM-002 DB Listener Testing
- OWASP-CM-003 Infrastructure Configuration
- OWASP-CM-004 Application Configuration
- OWASP-CM-005 Testing for File Extensions Handling
- OWASP-CM-006 Old, backup and unreferenced files
- OWASP-CM-007 Infrastructure and Application Admin Interfaces
- OWASP-CM-008 Testing for HTTP Methods and XST

Authentication testing

Almost every web application requires some form of user authentication (establishing identity of the user) to provide additional functionality, for example, to alter content in a content management system, administrators must authenticate themselves. Authentication mechanism are inspected in detail to examine the possibility of altering or intercepting authentication data to gain additional access to the system. For example, common usernames and passwords are checked, such as admin/admin.

OWASP control areas:

- OWASP-AT-001 Credentials transport over an encrypted channel
- OWASP-AT-002 Testing for user enumeration
- OWASP-AT-003 Testing for Guessable (Dictionary)
- OWASP-AT-004 Brute Force Testing
- OWASP-AT-005 Testing for bypassing authentication schema
- OWASP-AT-006 Testing for vulnerable remember password and password reset
- OWASP-AT-007 Testing for Logout and Browser Cache Management
- OWASP-AT-008 Testing for CAPTCHA
- OWASP-AT-009 Testing Multiple Factors Authentication
- OWASP-AT-010 Testing for Race Conditions

Application Security Control Areas (cont.)

Session management

HTTP is a stateless protocol and does not have a concept of a user's session built-in. In order to avoid continuous authentication for each page of a website or service, web applications implement various mechanisms to store and validate credentials for a pre-determined timespan. These session mechanisms are subject to common risks and flaws that may lead to unauthorised access to additional functionality or can be abused to force users to unwillingly and unknowingly execute an action in the system using social engineering tricks. For example, a common error is to rely on usernames stored in a browser cookie in a way that can be easily manipulated by the attacker.

OWASP control areas:

- OWASP-SM-001 Testing for Session Management schema
- OWASP-SM-002 Testing for Cookies attributes
- OWASP-SM-003 Testing for Session Fixation
- OWASP-SM-004 Testing for Exposed Session Variables
- OWASP-SM-005 Testing for CSRF

Business logic testing

Each purpose-built web application will have a specific set of requirements and restrictions specific to the business environment it operates, for example, a junior employee may not authorise transactions over a specific sum or may not authorise transactions where he/she is the initiating party to preserve segregation of duties. To conduct business logic testing, the analyst first builds an understanding of what specific business rules and restrictions must be in place and then attempts to bypass these restrictions using a variety of tests, such as form field tampering, forced browsing etc.

OWASP control areas:

- OWASP-BL-001 Testing for business logic

Data validation testing

Web applications must accept only valid data, e.g. only valid dates, no spaces in e-mail, only plain text in comments areas. If such checks are not enforced, attackers may hijack the execution flow of the program, for example by inserting a portion of a SQL statement in a lookup query that uses user-supplied input, e.g. instead of specifying first name like "John", attackers may input "John' OR 1=1;--" and possibly obtain output of all users in a directory that may be otherwise unavailable, or use this to extract data from other tables or gain a foothold in the underlying operating system. In this control area, we check if correct user input syntax is enforced and if not, what can be gained from abusing weak data validation functionality.

OWASP control areas:

- | | |
|---|---|
| ■ OWASP-DV-001 Testing for Reflected Cross Site Scripting | ■ OWASP-DV-010 XPath Injection |
| ■ OWASP-DV-002 Testing for Stored Cross Site Scripting | ■ OWASP-DV-011 IMAP/SMTP Injection |
| ■ OWASP-DV-003 Testing for DOM based Cross Site Scripting | ■ OWASP-DV-012 Code Injection |
| ■ OWASP-DV-004 Testing for Cross Site Flashing | ■ OWASP-DV-013 OS Commanding |
| ■ OWASP-DV-005 SQL Injection | ■ OWASP-DV-014 Buffer overflow |
| ■ OWASP-DV-006 LDAP Injection | ■ OWASP-DV-015 Incubated vulnerability |
| ■ OWASP-DV-007 ORM Injection | ■ OWASP-DV-016 Testing for HTTP Splitting/Smuggling |
| ■ OWASP-DV-008 XML Injection | |
| ■ OWASP-DV-009 SSI Injection | |

Application Security Control Areas (cont.)

Denial of service testing

A denial of service is a condition when an application cannot answer valid user requests within acceptable time frames. This may be caused by overload in infrastructure resources, for example, caused by excessive queries to the database. This type of attack is common when the attacker's goal is to extract "protection money" or as a political "hacktivism" when opponent's information resources are overloaded to prevent dissemination of information. Common errors include improper syntax validation in search fields, allowing wildcard characters, such as "%" in SQL queries to be included which may cause the database server to retrieve all rows from a table. If the table is large, then effectively, all other users might not be able to use its functionality as it will be busy serving the computationally-expensive request issued by the attacker.

OWASP control areas:

- OWASP-DS-001 Testing for SQL Wildcard Attacks
- OWASP-DS-002 Locking Customer Accounts
- OWASP-DS-003 Testing for DoS Buffer Overflows
- OWASP-DS-004 User Specified Object Allocation
- OWASP-DS-005 User Input as a Loop Counter
- OWASP-DS-006 Writing User Provided Data to Disk
- OWASP-DS-007 Failure to Release Resources
- OWASP-DS-008 Storing too Much Data in Session

Web services testing and AJAX testing

Web services are an essential component of Web 2.0 architecture. Private or restricted web services typically use SOAP – an XML-based communication protocol over HTTP, while public services, especially those geared for mashups or widgets, increasingly use JSON – a JavaScript serialisation based protocol instead of custom XML or SOAP. The latter is often referred to as AJAX. Common errors in this area include insecurely implemented XML parsers and unsecured SOAP endpoints where anybody can execute available functions.

OWASP control areas:

- OWASP-WS-001 WS Information Gathering
- OWASP-WS-002 Testing WSDL
- OWASP-WS-003 XML Structural Testing
- OWASP-WS-004 XML content-level Testing
- OWASP-WS-005 HTTP GET parameters/REST
- OWASP-WS-006 Naughty SOAP attachments
- OWASP-WS-007 Replay Testing
- OWASP-AJ-001 AJAX Vulnerabilities
- OWASP-AJ-002 AJAX Testing



**Application
Security
Testing:**

**White Box
Testing**

White Box Testing

White box testing

This component of application security testing involves a detailed examination of the application security design and implementation. The final result of an application review will be a report detailing all security related issues identified, classified in order of priority. Potential impact, if any, will be detailed for all security exposures identified and also full recommendations for reducing any risks identified.

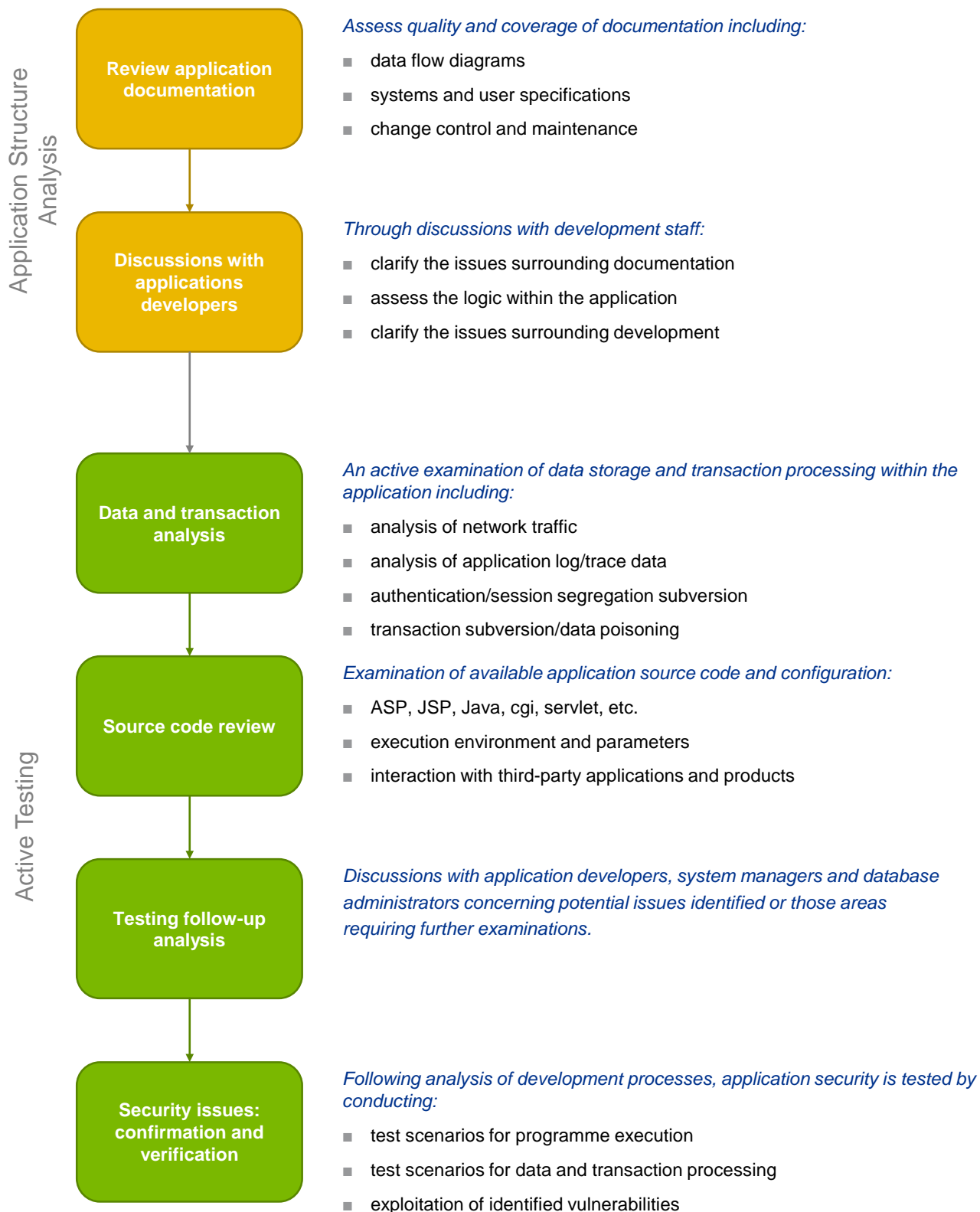
An application review is conducted primarily on-site and will require access to/information on:

- Application programming environments
- Application execution (test, non-production and production) environments
- User authentication
- User session segregation
- Transaction processing
- Data access
- Data integrity
- Application availability

Areas of scrutiny include:

- Application and host systems (including valid application user accounts)
- Application source code
- Systems and development personnel
- Application and systems documentation
- Network infrastructure

White Box Testing (cont.)



White Box Testing (cont.)

Review application documentation

To understand the application, the system and user specification documentation is examined along with data flow charts and any other related material. At this stage change control and backup/recovery documentation may also be examined.

Discussions with application developers

To derive a complete understanding of the application structure and data flow it may be necessary to discuss the implementation with developers responsible for the application. Any particular issues or concerns that the developers may have with the application design or implementation will be identified and explored at this stage.

Data and transaction analysis

Known test data will be input and processed through the system and the resultant debug/tracking logs will be analysed at each stage of the data processing path. In addition to log analysis network capture will be used at all relevant network points to verify the transmission of the data in the expected manner (i.e. encrypted using 128-bit SSL). Following the known data tests will be a series of tests with spurious, engineered and out-of-bounds data with the log and network analysis stages repeated to identify potential issues.

Source code review

All available source code will be examined for potential security risks. Such risks generally arise from not following secure programming guidelines and are often found in scripts parsing user input, e.g. failing to strip escape characters from a user input field on an HTML form within an ASP or PHP script. The execution environment for code and scripts will also be examined to ensure process isolation, and process access restrictions are securely coded. Where source code is not available, for instance in a third-party product then the interaction between the application and the product will be examined.

Testing follow-up analysis

All potential issues identified up to this stage are discussed with the relevant application or system personnel where necessary to determine the seriousness of each issue. Where insufficient information has been deduced from previous testing stages it may be necessary to request additional guidance from client personnel at this time regarding certain issues.

Security issues – confirmation and verification

Where necessary, potential security issues will be verified by testing and this may require exploitation of a particular vulnerability. Scenario tests may be performed at this stage, these will involve various 'what-if' tests on both program execution and data handling/transaction processing to determine if potential security issues may exist, for example if two separate users authenticate at the same time is session segregation maintained?

Reporting

All identified security risks and issues will be classified and documented with likely impact and recommendations for mitigating the risks. The report may also contain information detailing the test procedure.



**Application
Security
Testing:**

**Black/Grey
Box Testing**

Black/Grey Box Testing

Black/Grey Box Testing

This component of application security testing involves a simulated external attack on the application, generally from the perspective of both an authorised and unauthorised user. The final result of an application review will be a report detailing all security-related issues identified, classified in order of priority. Potential impact if any will be detailed for all issues as will full recommendations for reducing any risks identified.

The test is performed first as an unauthorised user without a valid account on the system. After completion of the first scenario the relevant tests are repeated using a valid user account that generally provides greater application visibility.

Areas of scrutiny include:

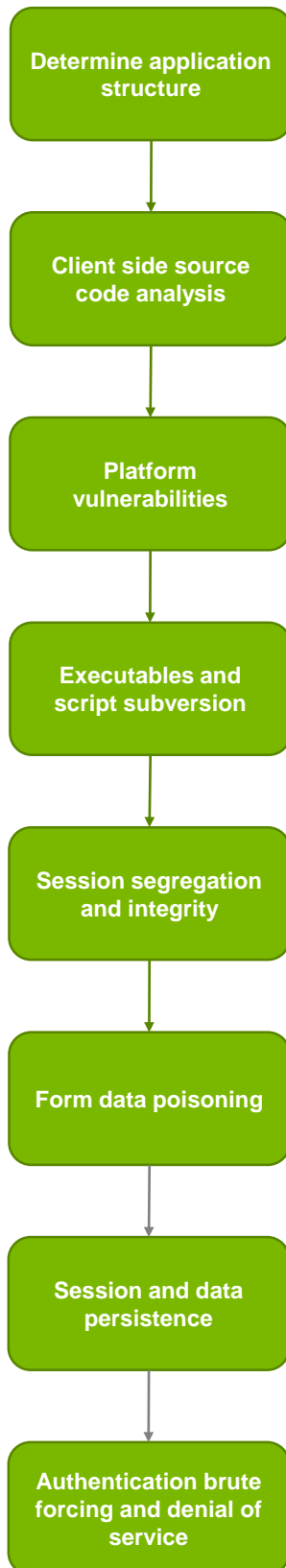
- Platform security vulnerabilities
- User input validation
- Available source code
- User authentication
- Executable/script parameters
- Folder and File accessibility
- Data access
- Data integrity
- Application availability

An application penetration test can be conducted remotely and will require access to:

- Application and host systems
- Valid application user accounts

Black/Grey Box Testing (cont.)

Active Testing



By looking at the supporting infrastructure, identify:

- the hosts, platforms and products that serve the application
- all content, scripts and other accessible files
- a mapping of the web site

Analyse the source code to identify:

- developer comments
- client side validation
- applet and class de-compilation

Once the supporting infrastructure has been identified:

- exploit known OS and application vulnerabilities
- attempt to use default insecure configurations

Using client software, attempt to circumvent application normal processing by:

- parameter poisoning
- directory traversal
- source code retrieval

By looking into the client processing of information attempt to:

- hijack and spoof of user sessions
- disruption of user sessions
- data theft and modification of user sessions
- authentication mechanism subversions

By looking at the web based elements of the application attempt:

- HTML form modification, field lengths, names, etc.
- SQL command insertion
- unauthorised database access
- database corruption

Looking at session related information, perform:

- cookie examination
- sensitive cached information
- session re-use

Finally, if required, highly intrusive account testing is performed including:

- brute force user account and password attacks
- platform denial-of-service
- application denial-of-service
- data denial-of-service

Black/Grey Box Testing(cont.)

Determine application structure

The addresses of all systems deducible from the application will be identified, as will the server software and third-party application software where possible. All available content will be identified and copied to the testing system for analysis. Additionally site-spidering and exploration scripts will be used in an attempt to discover hidden resources within the applications and the servers.

Source code analysis

All static and dynamically generated content will be examined for relevant information contained in the source code. Of particular interest will be developer comments, change control comments and directory/path names. Client-side validation scripts may also be examined and any relevant java applets may be downloaded and decompiled for analysis. Where executable script is obtained in source form it too will be examined.

Platform vulnerabilities

All server software and third-party applications that are reachable are examined for known security vulnerabilities and security configuration issues. This stage may involve the use of automated software such as whisker or other in-house scripts. Discovered platform vulnerabilities may also be used to assist in the subversion of the application unless requested otherwise.

Executables and script subversion

All scripts and executables that were identified during the first stages will be examined in an attempt to cause them to perform unauthorised functions, ABEND (crash) or otherwise not execute as intended. Such examination will involve modification of parameters passed and may be used to attempt to read files from the target server file-system or pass parameters to a system executable. Attempts will be made to recover the source code of scripts and binary images of executables where possible.

Session segregation and integrity

User sessions will be examined to determine their nature, e.g. cookie based or IP-address based. Attempts will be made to spoof, hijack and disrupt existing user sessions. Multiple concurrent sessions will be established in an attempt to read or write data to another session. The authentication mechanism will be examined in detail during this stage.

Form and data poisoning

All forms and means of data entry identified in earlier stages of the exercise will be subject to a series of tests where parameters such as hidden form fields and field lengths are modified. Additionally form fields will be subject to escape character, meta-character and SQL insertion tests in order to execute commands, access or modify data held within the database.

Session and data persistence

Cookies and cached data will be identified to determine whether sensitive information remains accessible within the application, platform or client PC after the user session has ended.

Authentication brute forcing and denial of service

Account username and passwords will be subject to a brute force/dictionary attack in an attempt to gain unauthorised access to the target application/system. Account lockout is examined at this stage. Additionally platform and application denial of service attacks may be attempted at this stage if previously agreed.

Testing follow-up analysis

All potential issues identified up to this stage are discussed with the relevant applications or systems personnel to determine the seriousness of each issue. Where insufficient information has been deduced from previous testing stages it may be necessary to request additional guidance from client personnel at this time regarding certain issues.

Reporting

All identified security risks and issues will be classified and documented with likely impact and recommendations for mitigating the risks. The report may also contain information detailing the test procedure.

Mobile Application Assessment

Mobile Application Assessment

The Mobile Application security assessment approach is based on our application security assessment. The key difference is the security model around the client-side security – traditionally, an end-user is in control of his device and is responsible for securing his computer against attackers and malware with the service provider only offering hints or free software. Furthermore, the most common client-side application - a web browser lives in a dynamic security ecosystem in which many security researchers raise awareness of various security issues and major vendors quickly respond with a fix.

In mobile application environments, end-users may not always be aware of the threats they are facing and may not be in complete control of the device. Additionally most mobile web applications are bespoke and for single purpose and typically do not benefit from the “many eyes” advantage a popular software product receives. To address these issues, KPMG mobile application assessment methodology incorporates in addition to application security assessment, an end-user application security review process.

Server-side security

The server-side security testing is carried out using one of the approaches described in the application security assessment methodology: black box, grey box or white box approach.

Client-side security

The client application is tested either using a platform emulator typically provided together with SDK and/or actual hardware device.

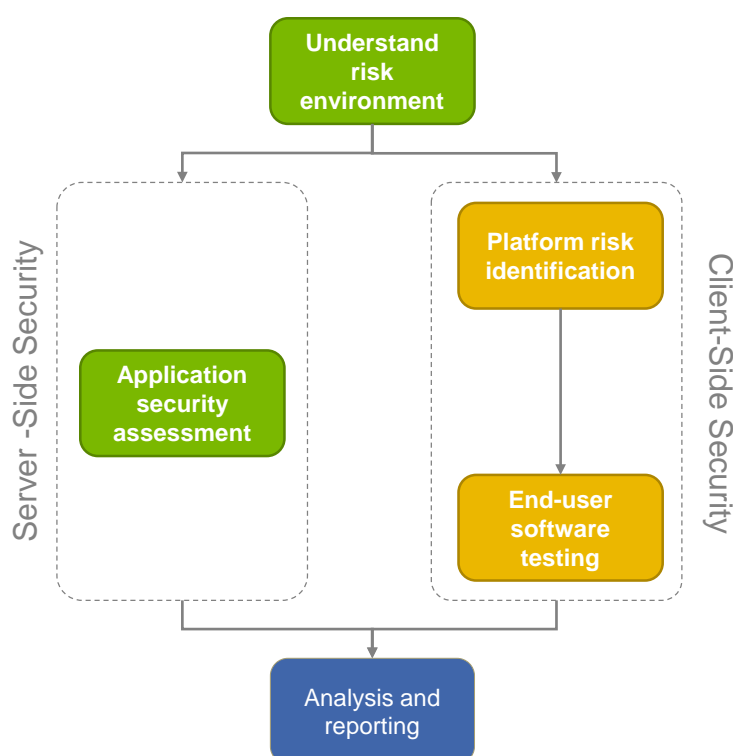
Platform risk identification

Functionality of the client application is thoroughly analysed to identify assumptions about platforms of executions that may not be always true, for example:

- an application relies on GPS data being accurate, then such data may be spoofed if the application is executed on an emulator;
- storage and exchange of cryptographic keys or shared secrets between application and a security device such as SIM card cannot be intercepted by other applications;

End-user software testing

The data exchange between client-side application and server-side application is intercepted using various tools and the client-side application is being supplied with invalid responses to trigger erroneous behaviour. Fuzzing tools are used where possible to cover the maximum attack surface followed by manual investigation of suspicious behaviour.



PCI Compliance Readiness

PCI Compliance Readiness

KPMG is not a Qualified Security Assessor (QSA) or an Approved Scanning Vendor (ASV); therefore KPMG offers its clients a PCI Readiness assessment that prepares them to pass a compliance audit by a QSA or ASV.

During this assessment, KPMG performs all activities as would a QSA and ASV, with the added benefit of providing recommendations on mitigations required in order to pass the compliance audit. KPMG has contractual relationships with QSA and ASV companies and can offer a bundled service.

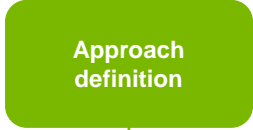
PCI Readiness



Review of card processing environment
All card payment information flows and processes are identified. Processing systems are enumerated.



Gap analysis & scanning
A gap analysis is performed against current and applicable PCI DSS. Scanning using the same tools as ASV.

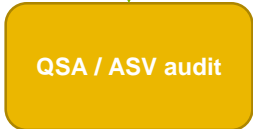


Approach definition
Together with the client, gap closure approach is agreed. Common PCI compliance approaches include:

- tokenisation
- end to end encryption
- card processing environment reduction
- risk transference



Remediation
Based on the previously selected approach, remediation activities are carried out. KPMG helps the client by providing mitigation advice and assisting with project management



QSA / ASV audit
A third-party QSA or ASV performs the audit. KPMG assists the client by helping the client prepare necessary documentation for the third-party auditor as well as supporting the client in discussions with the auditor.

Wireless Security Assessments

Wireless Security Assessments

KPMG's wireless security assessment methodology has three main assessment targets:

- WiFi 802.11a/b/g/n infrastructure
- Organisation devices connecting to wireless infrastructure, e.g. laptops, PDA
- Non-WiFi systems, such as RFID access and payment systems, Bluetooth devices

WiFi 802.11a/b/g/n infrastructure

- Perform reconnaissance to identify Infrastructure-mode access points and Ad-Hoc connections available.
- Obtain Wireless Network Information such as:
 - Wireless mode (802.11a, b, g, n/900mhz/etc)
 - Service set identifier (SSID)
 - Key management method (Shared, challenge-response)
 - Capture device pairing exchanges; and
 - Encryption method
- Identify weakly protected Access Points using WEP, WPA-PSK or no encryption.
- Use Wireless packet capture tools to capture WEP/WPA-PSK cipher text to prepare for cracking
- Perform cracking using rented cloud computing or KPMG's CLOUDCRACK cluster
- Using the cracked or supplied access key gain access to the target network and perform infrastructure penetration testing on select in-scope targets, such as WiFi hotspot management platforms, captive portals, AAA servers etc.
- A last, optional step - KPMG host reviews can be performed on the networking equipment

Wireless client assessment

- Perform reconnaissance of wireless clients onsite and identify the connections they are using or attempt to use (listen for broadcasts)
- Setup fake access points and force clients to connect to these APs
- Perform man-in-the-middle attacks and infrastructure testing on these clients

Non-WiFi system testing

Non-WiFi system testing mostly focuses around cloning or data alterations, eavesdropping, replay attacks and unauthorised connections. Specific tests performed are dependent on the security model and technology chosen. Before each test, security model analysis of the specific technology application case is performed and relevant attacks are chosen. These attacks may include:

- Device cloning
- Cryptanalysis of communication protocol
- Eavesdropping and session key recovery, for example, for authenticated Bluetooth devices
- Data alteration on device, for example, available balance modification for e-wallets

Security Awareness Training

Security Awareness Training

KPMG’s security awareness training approach focuses on altering the behaviour of an organisation’s information system users.

Improvement of Security Awareness



Define the desired vision

To achieve successful transformation of an organisation’s security awareness culture, a target vision must be defined. This is achieved by:

- considering current threat environment
- interviews with key stakeholders
- vision definition workshops

The output of this stage is a security culture vision document, that at a high-level describes desirable traits of the security culture within organisation.

Measure current status

The current status of the security culture is measured by selecting a sample of employees and interviewing them through asking simple, long-lasting questions that encourage honest answers. Based on this measurement, gaps between new vision and current status are identified.

Improve awareness

An awareness improvement program is created to address using the 3C model (see next page) issues previously identified. A holistic approach is used that alters a variety of organisation’s culture aspects:

- | | |
|------------------|--------------------|
| ■ new knowledge | ■ new roles |
| ■ new attitudes | ■ new environments |
| ■ new behaviours | ■ new systems |

After the improvement material is created, an internal marketing campaign is carried out using a rich set of communication tools most suited to the organisation, including:

- | | |
|------------------|-------------------------------|
| ■ posters | ■ awareness training sessions |
| ■ e-mail alerts | ■ games |
| ■ video content, | ■ social media |

Apply sticky factors

To counteract the fall-back of culture to old habits, various tools and means to be applied continuously are developed to preserve the positive improvement:

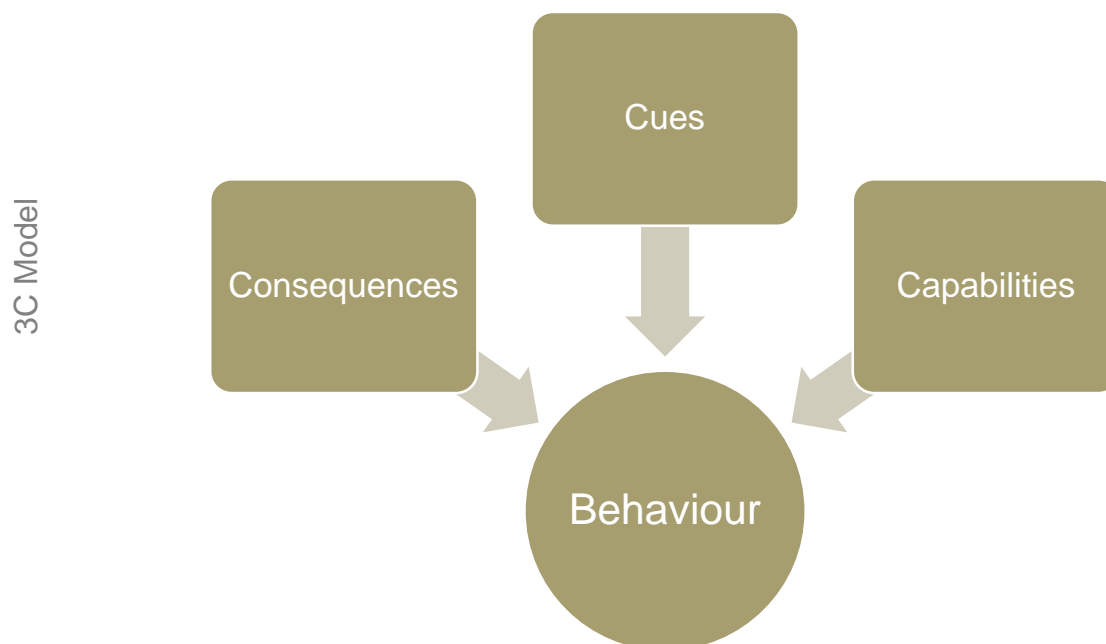
- quizzes
- new examples
- affirmation by tone at the top

Measure new status

A new sample of users is selected and the same questions posed initially are asked. These answers are used to measure the success of the security awareness programme. Lessons learned are used for future awareness programmes.

Security Awareness Training: 3C model

Security awareness programmes are developed, considering the 3C model. In order to successfully perform long-lasting alterations to organisation's culture, all three aspects must be considered.



Consequences

A Security Awareness programme must be backed by a “carrot and a stick” model – rewards and punishments. A balanced model must be developed to encourage people adopt the new, desired behaviour. How the consequences are perceived is just as important as how they are executed.

Cues

Cues are behaviour shaping instructions. They may consist of:

- instructions
- rules
- hints
- prompts & warnings
- orders
- policies
- tips

In addition to such instructions, environment – both physical and cyber and how other people behave signal important cues.

Capabilities

For an organisation's employee to be able to adopt the new culture, he must have the necessary tools and means to carry out the desired behaviour. This is developed through education, personal development and close attention to controls, resources, facilities & design.

The KPMG Firewall Review

The KPMG Firewall Review



Figure 6: The KPMG Firewall Review process.

The KPMG Firewall Review (cont.)

The firewall review (Level 4) is an on-site review which establishes the effectiveness of a client's firewall policy and whether the machine is secure.

From previous analysis of the firewall during the attacking phases we would have ascertained many details about the types of rules that are contained within the firewall's policy. This review will cover in more depth the appropriateness of these rules and whether there are any potential flaws in their logic. We will also analyse the configuration of network nodes attached to insecure networks.

We have experience in most commercial application firewalls including:

- Check Point FireWall-1
- SunScreen EFS
- Gauntlet
- CyberGuard
- Symantec Raptor
- Cisco PIX and ASA
- Juniper
- Border Manager
- 3 Com

We have configured firewalls and designed firewall access lists for leading banks, insurance companies and retail organisations. We specialise in the financial and Government sectors— if you use an Internet bank in the UK, chances are it has been reviewed, tested, configured or audited by KPMG.

The KPMG Host Review

The KPMG Host Review

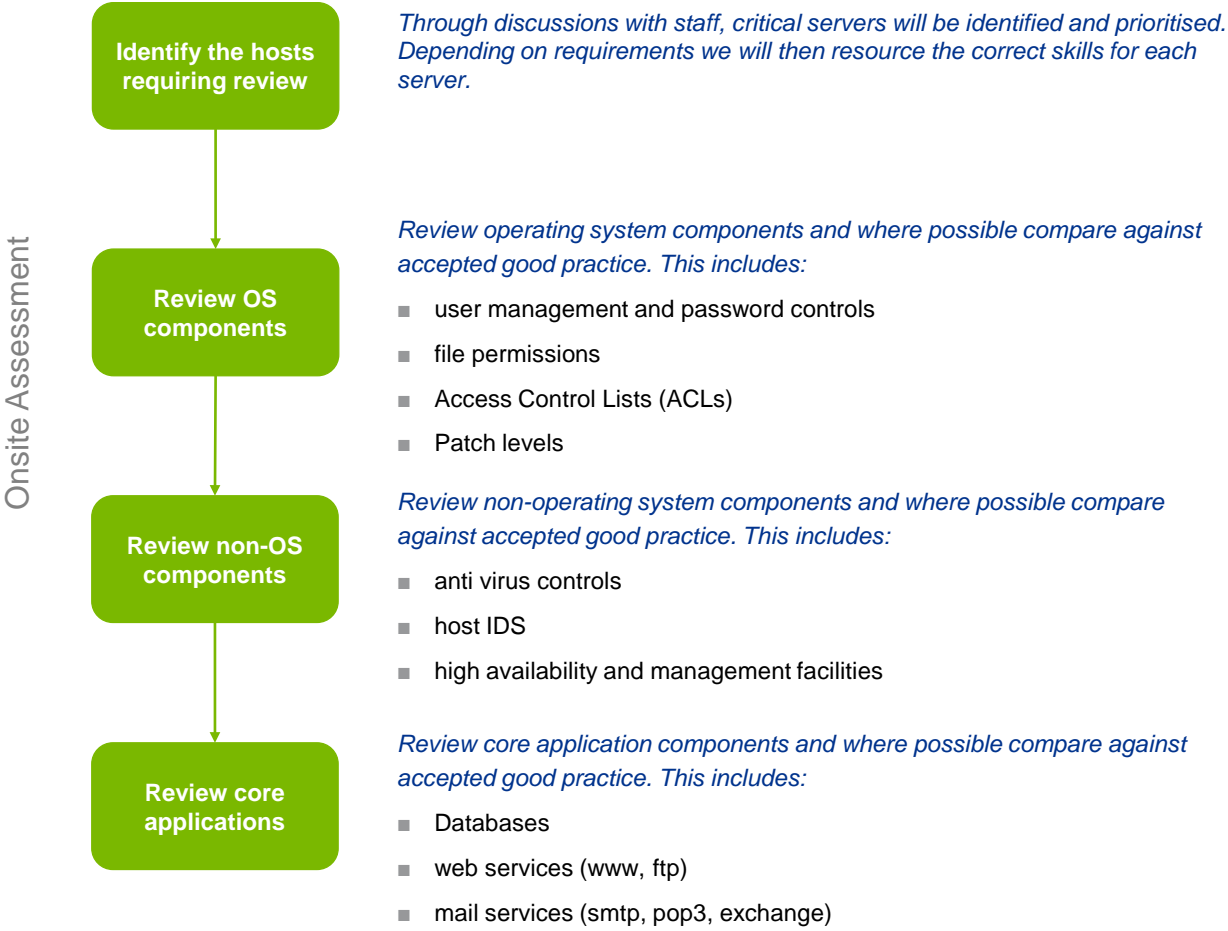


Figure 7: The KPMG Host Review Process

KPMG’s host review service provides our clients with an independent assessment of their critical server configurations. By directly examining the settings configured on the servers, KPMG can compare your current configurations against your own baselines or industry recognised good practice. KPMG perform assessment reviews on all operating systems including, but not limited to:

- Windows
- Unix and derivatives, such as (Solaris, AIX, RS6000, Linux)
- Novell; and
- AS/400

The KPMG Host Review (cont.)

In addition to looking at specific operating system components and configurations, we will also examine non-operating system controls and server-based applications that provide the business with key resources. Applications included within the server reviews include:

- Web and web application servers, such as Internet Information Server (IIS), Apache, JBoss
- Key databases, such as SQL Server, Oracle, MySQL, PostgreSQL, Informix, DB2
- Communications platforms, such as Microsoft Exchange Suite, Lotus Notes

Our host reviews can be performed at two levels, depending on the type of assessment required; Organisation Host Security or Internet Server Security.

Organisation Host Security

The KPMG Organisation Host Security assessment incorporates a combination of skilled security professionals and structured work programs to cover a number of areas including:

- User Account Management (built-in accounts and administrator access)
- File permissions and shares (around sensitive areas including system files)
- Registry permissions and use of Access Control Lists
- Password management and control
- Installation of appropriate hot fixes and service packs
- Use of anti-virus and management processes
- Active directory design
- Security monitoring


Internet Server Security

The KPMG Internet Server Security assessment examines your Internet facing servers. These normally reside in a DMZ or other segregated network segment and require a tighter level of security than internal servers due to their susceptibility to external attack. KPMG has analysed various baseline sources and has an understanding of how these servers can be protected against attack using a variety of controls and tools including:

- Operating system configuration
- Third party security applications
- Non-host based controls

Host review tools

- Nipper
- Winprobe
- SABA
- Custom review scripts for HP-UX, Solaris, Linux
- John the Ripper, Cain and Abel for password security
- Pyro – KPMG tool for graphing firewall rules

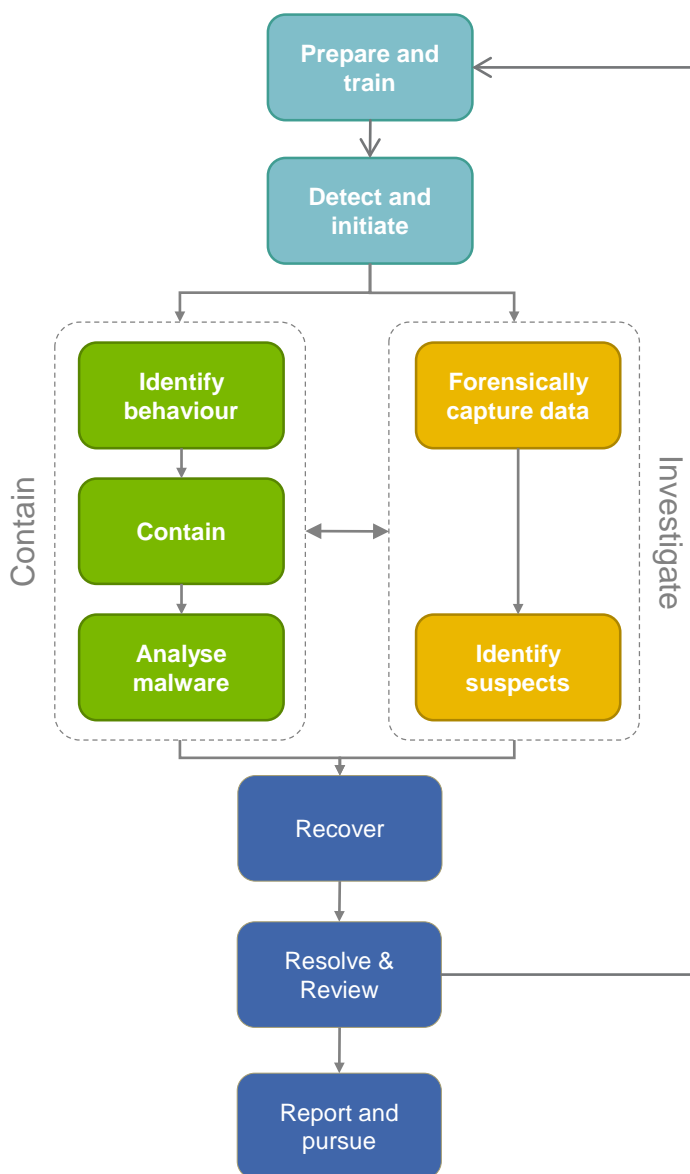
The background is a solid blue color, split diagonally from the bottom-left to the top-right. The upper-right portion of the image is white, creating a sharp contrast with the blue.

Cyber Response and Malware Analysis

Cyber Response and Malware Analysis

KPMG Cyber Response methodology overview

KPMG's Cyber Response methodology scope includes not only actual response to Cyber incidents, but also preparation for a potential incident and post-incident effectiveness review and improvement.



Prepare and train

- Develop incident classification schemes, escalation procedures, communication plans, call trees, response checklists
- Develop rules of engagement in regards to activities, chains of evidence, and attorney/client privilege
- Familiarisation with organisation's technology and environment
- Execute Training exercises

Detect and initiate

- Initial event detection and classification (breach, misuse, fraud, etc)
- Communication to all stakeholders including: KPMG, business owners, legal counsel, public relations, etc
- Initiation of chain of custody if applicable
- Prioritisation of activities in the event of complex events (ie. determine the order of activities in the next phase)

Contain & Investigate

- Deployment of monitoring, forensic and data capture systems and tools
- Technical analysis of live systems, images, and live network data
- Blocking or limiting the connectivity or privileges of suspect systems, applications, or individuals

Recover

- Deployment of system patches or updated configurations
- Rebuilding suspect systems
- Removal of, or changes in user or applications accounts
- Destruction of any "residue" from malicious actions such as rootkits, suspect code, created accounts, etc
- Correction of the access or processes that allowed the malicious activity to occur, whether technical or procedural

Resolve & Review

This phase consists of the final analysis of the "how" of the event under investigation. The purpose is to fully evaluate and document the underlying causes of the episode to allow for improvement in regards to both the technical and governance factors that contributed to its origination.

Report and pursue

This final phase consists of the official reporting of the overall engagement and on-going support activities related to legal or civil pursuits of individuals or groups.

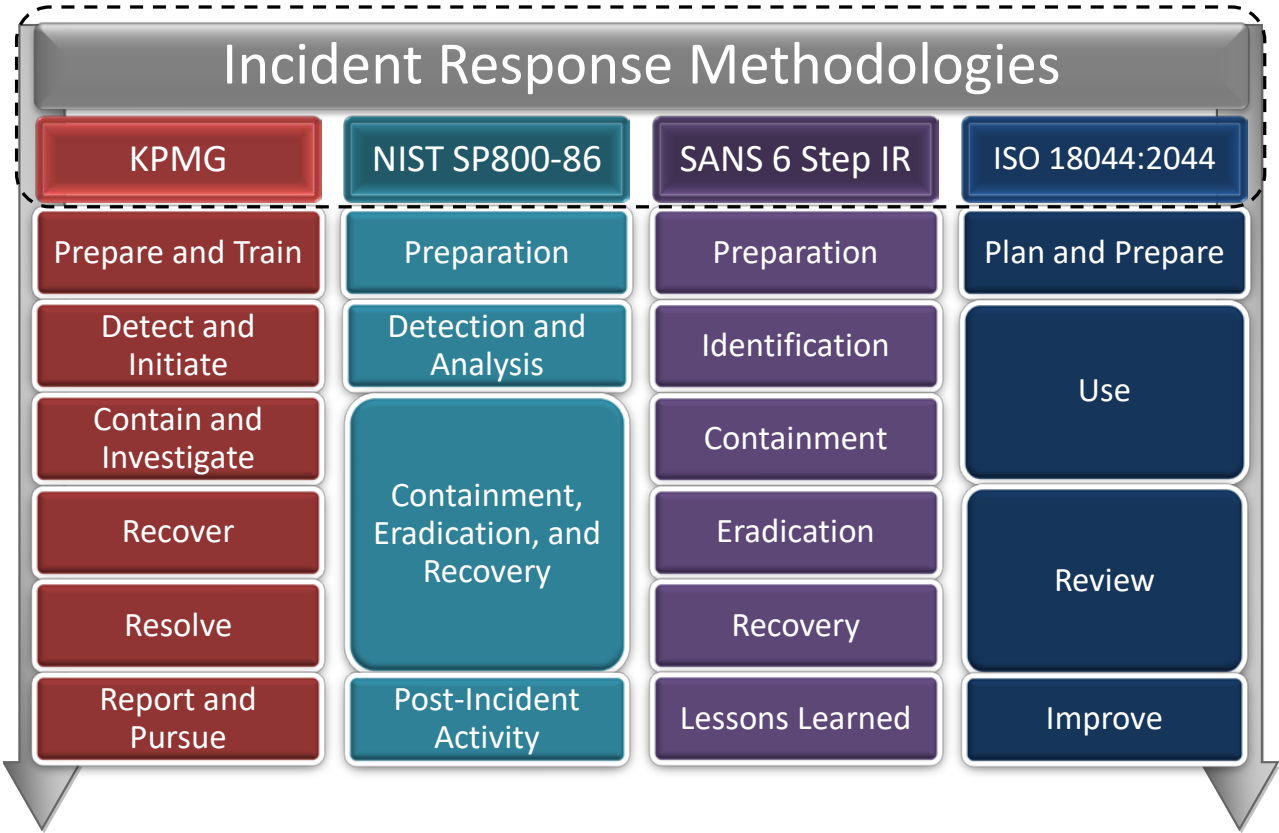
Cyber Response

Comparison with other methodologies

KPMG Cyber Response methodology overview

KPMG's Cyber Response process was created in accordance with several internationally accepted frameworks including the National Institute of Standards and Technology Special Publication 800-86 (NIST SP800-86), the International Organization for Standardization publication 18044:2044 (ISO 18044:2044), and the SANS institute's published Six Step Incident Response Process (SANS 6 Step IR).

While these guides were utilized in order to confirm the completeness of our framework with regards to industry best practices, KPMG's process was further refined through real-world experience and a focus on actionable results, rules of evidence, and deeply technical security testing during the after action phases. KPMG's process is mapped to the other major standards in the diagram below, and each phase is then broken out at high level in order to describe the underlying activities:



Cyber Response (cont.)

Prepare and train

The “prepare and train” phase consists of two tracks – training and helping prepare the client organisation’s Incident Response team and, if applicable, preparing the KPMG Cyber Response team to respond to an incident in the client’s organisation by familiarising with the environment.

- Training and preparation of the client’s Incident Response team includes the following activities.
 - Review of current Incident Response readiness at the client’s organisation and perform gap analysis against chosen industry standard or methodology
 - Help develop incident classification schemes, escalation procedures, communication plans, call trees, response checklists
 - Conduct training workshops for Incident Response staff
 - Conduct training exercises using “red team” approach, whereby KPMG penetration testers will attempt breach of the client’s network while the Incident Response team will be in charge of detecting and responding to the simulated breach.
- If retained for an engagement in future, KPMG works with the client to establish lines of communication, policies, procedures and rules of engagement to set the groundwork for a successful and efficient response if, or when, an incident does occur. The following activities will be performed:
 - Establish rules of engagement with regards to activities, chains of evidence, and attorney/client privilege.
 - KPMG team familiarises with target technology and environment

Detect & Initiate

This phase consists of two tracks executed in parallel:

- Detect & assess the nature and impact of incident; and
- Initiate the response and establish a response team

Detect the incident & assess the current and potential impact

Depending on the type of event, this could involve anything from a technical alert (such as an Intrusion Detection System), to an indication of fraud, or even communication from an outside entity such as law enforcement or an Internet Service Provider. Paramount to successful management of incidents is proper detection and understanding of the nature of incident, and the levels of associated business risk. This includes:

- enumeration of the incident source,
- determination of type of incident (breach, misuse, fraud, etc)
- assessment of the extent of the incident (the scale of affected areas and resources) and the propagation rate and method – i.e. how the effects of an incident might be spreading across networks and the relative speed at which this might occur across interconnected systems.

Initiate the response and establish a response team

The Incident Response team should comprise individuals from the organisation with the authority to make business critical decisions. Additionally, the team should include technical specialists capable of making on-the-fly configuration changes as part of incident containment and management. Depending on the nature of the incident, the team may well require Legal counsel and media liaison officers. Regular contact will be required between these team members in order to maintain a focussed incident response strategy that is strictly adhered to. Key activities in this phase are:

- Communication to all stakeholders including: KPMG, business owners, legal counsel, public relations, etc
- Scope & role of KPMG involvement agreed and contracted
- Initiation of chain of custody if applicable
- Prioritisation of activities in the event of complex events (ie. determine the order of activities in the next phase)

Cyber Response (cont.)

Contain & Investigate

Actions must be defined and followed which seek to minimise and contain further propagation of the incident. This is typically the hardest part of any incident response, requiring quick yet informed critical business decisions in order to minimise damage while simultaneously maintaining business operations. This phase consists of the effort to determine the actual source, method, and impact of the event as well as the effort to limit the ongoing damage resulting from the event as much as possible. The actual detailed steps that occur will often reflect a delicate balancing act between the need to properly investigate the event while limiting the risk of not immediately eradicating the threat. Responses often range anywhere between allowing the malicious actions to continue in order to gather additional evidence for prosecution, to an immediate suppression of the actions in order to limit subsequent damage, or anywhere between the two extremes. This is also the phase in which the vast majority of the investigative efforts occur including the majority of technical and documentary evidence collection.

Gathering of system events and traffic

It is critical to gather data – system events and traffic from an early stage. To achieve this, the following steps are executed:

- Deployment of monitoring, forensic systems and tools, such as:
 - NetWitness Investigator, Eagle or Decoder
 - FireEye malware protection system,
 - Mandiant Intelligent Response and/or
 - custom traffic loggers based on tcpdump or Wireshark,
 - Intrusion Detection Systems, such as SNORT with specific rulesets.
- Deployment of system event “sink” if centralised logging is not present or not considered trusted

Containment & Investigation

Containment & investigation is carried out synchronously – once traffic patterns, methods or other identification means of the intrusion are identified, the intrusion is contained or blocked while an in-depth investigation is performed. Typically, the following steps are carried out:

- Technical analysis of live systems, images, and live network data
- Blocking or limiting the connectivity or privileges of suspect systems, applications, or individuals
- Initial impact is determined
- Initial communications to law enforcement if applicable
- Entrance of data and documents into the chain of custody and execution of the KPMG Digital Evidence Recovery Methodology

Key tools used are:

- EnCase
- NetWitness Investigator, Eagle or Decoder and Spectrum
- Mandiant Intelligent Response
- FireEye malware protection system

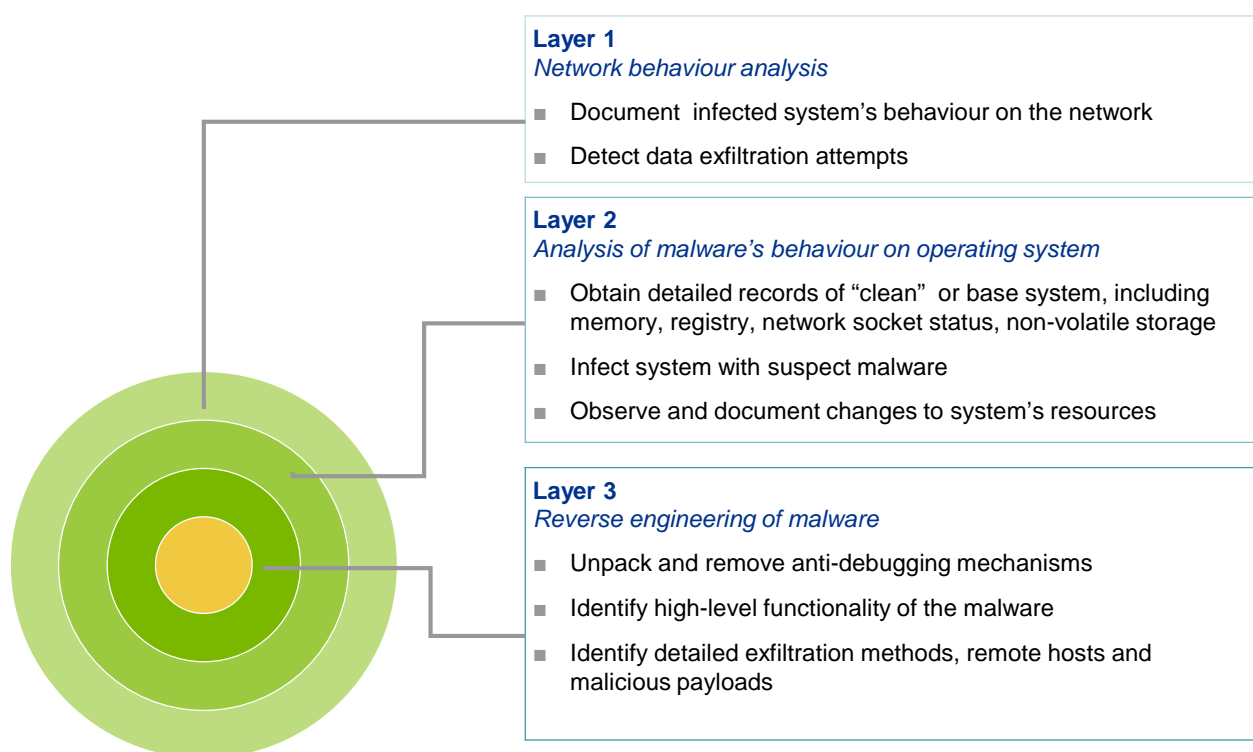
Malware Analysis Process

Role of malware analysis

Malware analysis and reverse engineering is a sub-section of KPMG's Incident Response methodology's section "Contain & Investigate". In this stage, two tracks are executed simultaneously: Containment which includes malware analysis and an investigation track which is executed in accordance with KPMG's Forensic methodologies available on request.

Approach to malware analysis

The KPMG malware analysis process is based on a "peeling layers" approach. This approach is optimised to quickly obtain immediately useful information about suspect binary objects to perform containment or removal of its traces. Each subsequent layer is usually more time and resource consuming to perform.



The consistent deployment of this approach is ensured by the use of cutting edge technology, and our policy to only use highly specialised staff that work in this area and the use of comprehensive work-programmes to enhance our quality control procedures.

Cyber Response (cont.)

Recover

This phase consists of removal efforts that could not occur during the previous phases because of the impact on investigative efforts or prioritisation of other activities. The focus of this stage is to securely return the environment to normal operations. Key activities include:

- Deployment of system patches or updated configurations
- Rebuilding suspect systems
- Removal or changes in user or application accounts
- Destruction of any "residue" from malicious actions such as rootkits, suspect code, created accounts, etc.
- Correction of the access or processes that allowed the malicious activity to occur, whether technical or procedural

Resolve & Review

This phase consists of the final analysis of the "how" and "what next" of the event under investigation. Issues identified during the detection and management phases must be reviewed to identify additional technical and/or procedural controls to be introduced such that the likelihood of a repeat incident is significantly reduced or removed; essentially a root cause analysis is performed. As changes made during containment are typically temporary, additional controls will be required to advance from containment to incident resolution.

A significant work stream during this phase may be information security testing and analysis, commonly referred to as vulnerability assessments or penetration testing. The output of this work stream is used to further understanding of the intrusion.

The effectiveness of incident response capabilities should be reviewed in the form of lessons learned from a post-incident analysis. Any training or development needs in this domain should be identified and followed in order to facilitate any future incidents. This phase of the incident response also includes review of IT or procedural controls changed as part of the mitigation phase – the effectiveness of these new controls should be assessed through focussed security testing and if necessary, simulated repeat incident. Key activities include:

- root cause analysis
- logical and physical network architecture review
- information system governance review

Report and Pursue

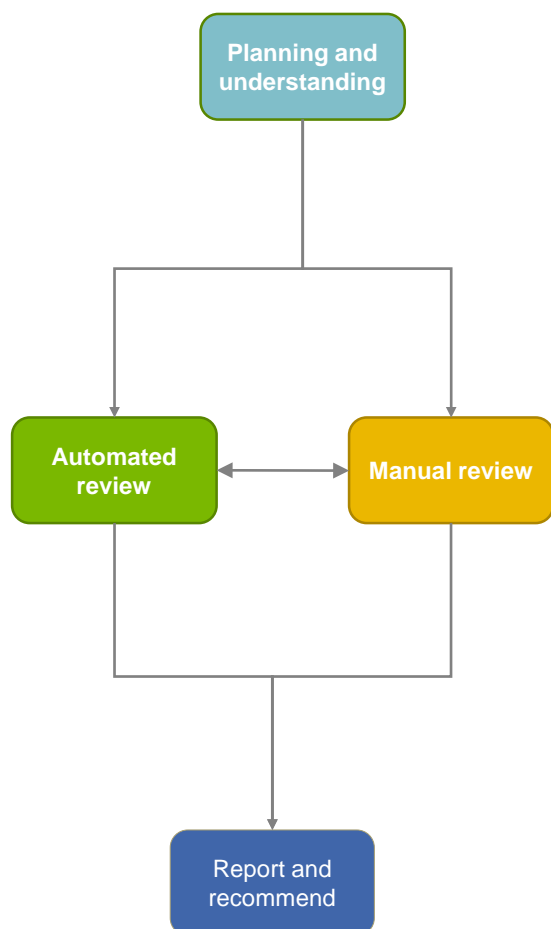
This final phase consists of the official reporting of the overall engagement and ongoing support activities related to legal or civil pursuits of individuals or groups. Key activities include:

- Lessons learned meetings
- Formal executive, board, and legal briefings
- Final reports
- Expert witness testimony
- Coordination with law enforcement
- Remediation steps and recommendations

Source code Audit

Source Code Audit

KPMG's source code audit methodology is a modification of the OWASP Code Review Guide. The control objectives are described in the application security testing section of this document. Manual and automated review approaches can be mixed and matched. For large code bases, the emphasis would be on automated review with manual review of critical code areas. Smaller code bases can be reviewed more thoroughly using a purely manual or semi-automated approach, where the analyst primarily relies on his knowledge while using tools to navigate or find offending software patterns in the code base.



Planning and understanding

- Understand and/or model application risks
- Identify key risk areas, understand technical risks and language specific idioms and inherent flaws
- Set out initial sampling approach – which sections to review within the resource constraints
- Determine approach – automated, manual or mixed
- Understand approaches, software patterns and idioms used

Automated review

- Adjust automated source code review tools with codebase specific information
- Review output and if necessary, adjust and re-run code review tool
- Analyse critical source areas, such as authentication, authorisation and auditing

Manual review

- Sample source files and review
- Analyse critical source areas, such as authentication, authorisation and auditing

Report and recommend

- Identify repeating code flaw patterns, such as poor re-use, lack of input validation, no separation of concern etc.
- Analyse flaw root cause
- Recommend coding process improvements



Our values

We lead by example

We work together

We respect the individual

We seek the facts and provide insight

We are open and honest in our communication

We are committed to our communities

Above all, we act with integrity

© 2021 KPMG Advisory SRL. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name, logo and 'cutting through complexity' are registered trademarks or trademarks of KPMG International Cooperative (KPMG International).