KPMG

Security Testing

Cyber Defense Services

kpmg.ch/cyber

Who are the threat actors

Hacktivism

Hacking inspired by ideology

Motivation: shifting allegiances – dynamic, unpredictable
Impact to business: public distribution, reputation loss

Organised crime

global, difficult to trace and prosecute

Motivation: financial advantage
Impact to business: theft of information

The insider

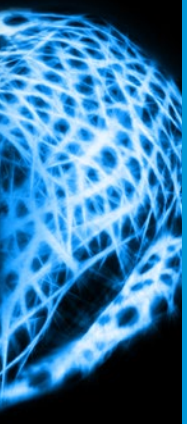
Intentional or unintentional?

Motivation: grudge, financial gain
Impact to business: distribution or destruction, theft of information, reputation loss

State-sponsored

Espionage and sabotage

Motivation: political advantage, economic advantage, military advantage
Impact to business: disruption or destruction, theft of information, reputational loss



Who is being targeted

- Automotive
- Aerospace
- Energy providers
- Retail banks
- Professional & legal services
- Defense
- Physical infrastructure
- Renewable energy
- Investment banks
- Wider financial services
- Retailers
- Pharmaceuticals & biotechnology
- Mining & natural resources
- Communications
- Academia

Our Security Testing Approach

Engagement Management

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 and 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.

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 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.

Security Testing Services

Reporting and Communication

Network and systems testing approach

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. First we test the 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.

Layer 1

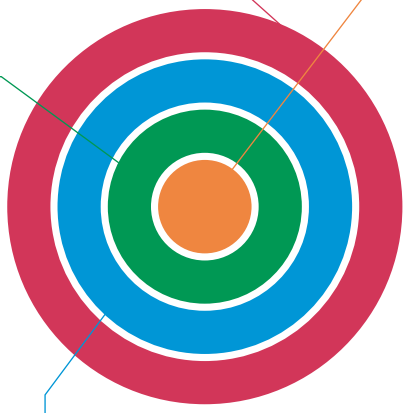
External penetration testing (naive hacker)

- Establish whether unauthorised logical access can be gained via the external network interfaces by a "naive" hacker who has limited and/or no previous knowledge of your network.

Layer 3

Internal penetration testing (unauthorised user)

- Ascertain whether unauthorised access can be gained via internal penetration and audit testing of your systems by exploiting loopholes in your networks services and resources.
- Determine whether it is possible to manipulate key controls implemented for the protection of your system(s).
- Assess whether existing procedures for responding to such a breach of security are adequate and effective.
- Assess the security of certain sensitive servers and workstations.



Layer 4

Firewall and security systems review

Analyse the effectiveness of the policies employed by your firewalls and the infrastructure in place for administration.

- Review the operating system configuration for a secure implementation.
- Review your procedures and processes for monitoring and reporting of incidents on the firewall.
- Review network and host security components, for example, IDS.

Layer 2

External penetration testing (supplier/customer level access)

- Establish whether unauthorised logical access can be gained via external network components by a hacker who has the same level of access as your customers and suppliers, to the target production environment and other key systems.

Web Application Security Testing

The User

- Password management
- Social engineering
- Phishing
- Update management
- Waterhole attacks
- Data governance
- Administrative access

The Application

- Cross-site scripting
- Weak input validation
- Brute force attacks
- Zero-day exploits
- Weak session management
- Vulnerable libraries
- Privileges escalation

The Browser

- Phishing
- Framing
- Click jacking
- Man-in-the-Browser
- Buffer Overflow
- Data Caching

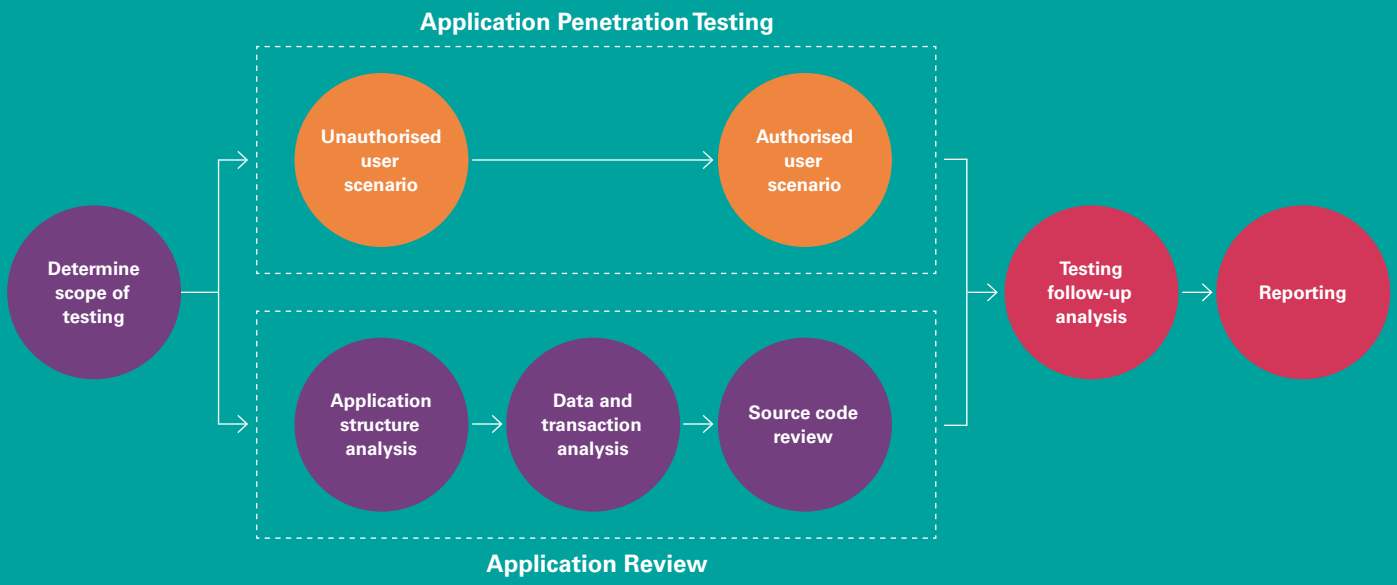
The Backend

Web Server

- Platform vulnerabilities
- Server misconfiguration
- Cross-site scripting
- Cross-site request forgery
- Weak input validation
- Brute force attacks

Database

- SQL injection
- Privileges escalation
- Data dumping
- OS command execution



The process of Web 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 unnoticed 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 Web Application Security Testing

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

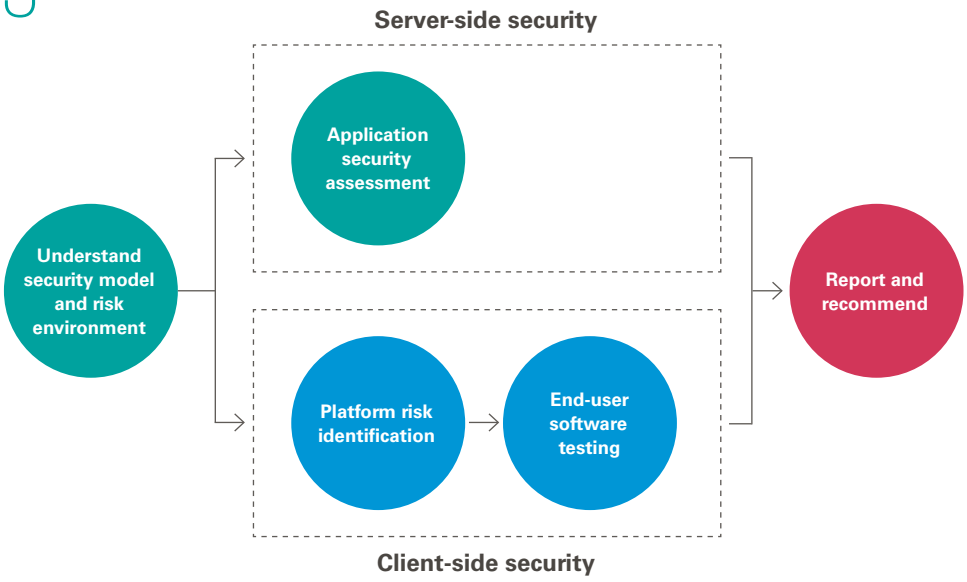
White box testing

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.

Mobile Application Testing



Mobile application testing approach

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 guidance 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 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, the KPMG mobile application assessment methodology incorporates in addition to application security assessment, an end-user application security review process.

Client-side security

The client application is tested either using a platform emulator typically provided together with software development kit (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.

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.

The Device

Browser
- Phishing
- Framing
- Click jacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching

Application
- Sensitive data storage
- No / Weak encryption
- Improper SSL validation
- Configuration manipulation
- Runtime injection
- Privileges escalation
- Device access

Phone / SMS
- Baseband attacks
- SMS phishing

The System

Operating System
- Password management
- Jail breaking / rooting
- OS data caching
- Data access
- Carrier-loaded software
- Zero-day exploit

The Network

Communication Channels
- No / weak Wi-Fi encryption
- Rogue access point
- Packet sniffing
- Man-in-the-middle
- Session hijacking
- DNS poisoning
- Fake SSL certificate

The Backend

Web Server
- Platform vulnerabilities
- Server misconfiguration
- Cross-site scripting
- Cross-site request forgery
- Weak input validation
- Brute force attacks

Database
- SQL injection
- Privileges escalation
- Data dumping
- OS command execution

Network & Systems Testing

Retrieve and document information about your organisation and systems from:

- The Domain Name Service (DNS)
- The Internet registration database (RIPE)
- Bulletin boards, forums and other social media
- The web
- other relevant sources

Identify and analyse the front-end router for:

- Active ports
- Login ports for remote access
- SNMP (if active)
- Finger (if active)
- Supported routing protocols

Identify and analyse the firewall by:

- Identifying all active TCP ports
- Identifying all active UDP ports
- Establishing the security rule base
- Testing for known security flaws

Iteratively identify and analyse accessible machines in front of and behind the firewall, which can be identified as a host using the following tests:

- Has an active TCP session established
- Has an active UDP port identified
- Test for known security flaws

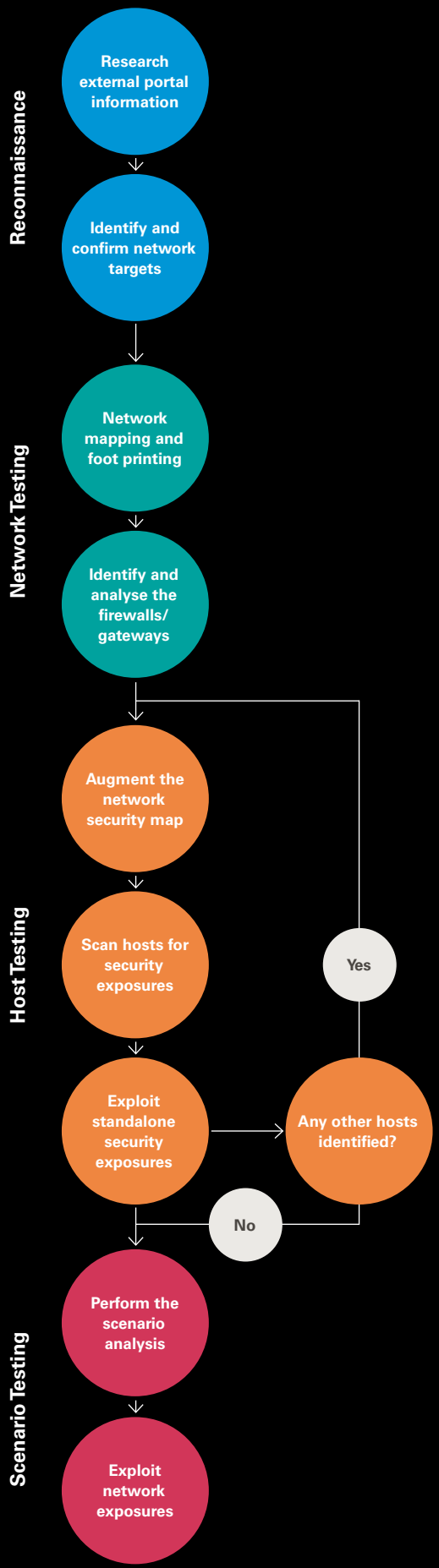
Iteratively identify and exploit vulnerable systems using:

- Public vulnerability information
- Configuration errors
- Design errors

Conduct a series of scenario analysis over the entire network to establish:

- What unauthorised traffic can be passed to the local area network (LAN)
- What security exposures can be exploited on the target systems

The Testing Process



Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch/cyber

Matthias Bossardt
Partner, Head of
Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Thomas Rhyner
Senior Manager,
Cyber Security

+41 58 249 48 93
trhyner@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

©2017 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity. All rights reserved.