TECIS60442

Plan penetration tests

Overview

This standard is about planning penetration tests.

Penetration testers discover security weaknesses within organisational infrastructure and web applications by performing authorised security tests to identify new vulnerabilities and report findings. They carry out tests using a combination of industry standard tools, in-house developed tools and manual reviews. The objective of a penetration test is to uncover any form of vulnerability - from small implementation bugs to major design flaws resulting from coding errors, system configuration faults, design flaws or deployment weaknesses.

Planning penetration tests involves establishing the scope and requirements of penetration testing assessments, identifying targets and mapping attack vectors to discover exploitable vulnerabilities. It includes engaging with the client prior to testing to confirm logistics arrangements, and agree test goals. It also includes establishing an incident and escalation management process to handle any issues that may arise during the penetration testing process.

This standard is for those who need to plan penetration tests as part of their duties.

Performance criteria

You must be able to:

1. Agree the scope and requirements for penetration testing with the client to plan testing activities
2. Agree the type of penetration testing to be undertaken and the methodologies to be used to deliver client requirements
3. Identify manual, automated or hybrid penetration testing tools and techniques to meet the assignment requirements
4. Identify and request information from the client that are needed to inform penetration testing activities
5. Select resources to deliver penetration testing assignments in line with organisational requirements
6. Produce an accurate, penetration testing resource plan
7. Identify penetration testing reporting requirements with the client in line with organisational procedures
8. Perform a risk assessment to identify and mitigate risks arising from proposed penetration testing assignment activities
9. Plan for potential incidents arising during penetration testing to identify escalation procedures and resolutions
10. Plan clean-up activities to be undertaken following penetration testing in line with organisational procedures
11. Document and communicate penetration testing plans with the client in line with organisational procedures

Knowledge and understanding

You need to know and understand:

1. The benefits and utility of penetration testing to the client
2. How to interpret client requirements for penetration testing
3. How to scope penetration tests and attack exercises
4. The principles of penetration testing
5. The main types of penetration test including infrastructure and web application penetration testing
6. The methodologies associated with infrastructure and web application penetration testing
7. The major steps applied in penetration testing including foot-printing, scanning, enumeration and exploitation
8. How to develop penetration testing plans
9. The steps involved in selecting resources to deliver penetration testing services
10. The difference between a vulnerability assessment and a penetration test
11. the differences between red team, blue team and purple team simulated attack exercises
12. The main concepts of infrastructure and web application penetration testing
13. The steps involved in penetration testing, including the relevant processes and procedures
14. Industry standard and organisation specific manual, automated or hybrid penetration testing tools and techniques
15. Technical, logistical, and financial constraints for penetration testing
16. The risks associated with penetration testing and how to mitigate them
17. The ethical issues related to penetration testing
18. How to define checkpoints, escalation paths and emergency contacts for penetration issues
19. Record keeping requirements mandated by organisational and external standards
20. The importance of accurate and structured record keeping during the engagement
21. The information required from clients prior to conducting penetration tests
22. The reporting requirements and formats required for penetration testing results and recommendations

23. UK legislation related to human rights, data protection, and computer misuse
24. Impact of legislation on penetration testing planning activities
25. Organisational and sector-specific standards and regulatory issues
26. The steps involved in resolving security events and how to apply them
27. The steps involved in performing clean-up activities after conducting penetration testing
28. The importance of accurate and structured documentation for penetration testing planning

Plan penetration tests

Developed by	e-skills
Version Number	1
Date Approved	30 Mar 2023
Indicative Review Date	30 Mar 2026
Validity	Current
Status	Original
Originating Organisation	ODAG Consultants Ltd.
Original URN	TECIS60442
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Penetration testing, security testing, ethical hacking