TECIS60443

Carry out infrastructure penetration testing

Overview

This standard is about carrying out infrastructure 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 other operational deployment weaknesses.

Carrying out infrastructure penetration testing involves testing internal computer system networks, associated devices, and cloud infrastructure to detect vulnerabilities and security flaws that could be exploited. Infrastructure penetration testing is also performed to assess an organisation's compliance with information security policies and its response to cyber security threats. The infrastructure penetration testing approach includes foot-printing and reconnaissance, scanning networks, enumeration and exploitation to demonstrate where vulnerabilities exist so that these can be reported on and mitigated.

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

Performance criteria

You must be able to:

1. Identify penetration testing requirements to support infrastructure penetration testing activity planning
2. Select the infrastructure penetration testing tools and techniques necessary to deliver client requirements
3. Prepare hardware and software tools ready for an infrastructure penetration testing in line with organisational requirements
4. Perform network mapping to identify IP addresses and open ports on the network
5. Perform foot-printing analysis to gather information about a target network infrastructure, systems and users
6. Undertake port scanning to scan for open ports on the target network and devices
7. Use port lookup tools to determine which network service runs on each port
8. Perform username enumeration on target infrastructure network services using industry standard protocols and methods to identify valid user accounts
9. Demonstrate where infrastructure vulnerabilities could be exploited to gain access to devices or obtain information about the network
10. Manipulate network routing protocols and bypass security controls to perform traffic capture and demonstrate possible man in the middle attacks between two legitimate hosts
11. Demonstrate pivoting through devices used to gain access to targets on an infrastructure subnet
12. Interpret the output of tools, including those used for port scanning, enumeration, exploitation and traffic capture
13. Validate the presence of identified vulnerabilities, suspicious files and assess patch levels accurately
14. Perform clean-up activities after conducting penetration testing in line with organisational procedures

15. Document vulnerabilities detected during infrastructure penetration testing in line with organisational procedures
16.
Update knowledge base to record new knowledge on infrastructure penetration testing techniques and discoveries
17.
Provide the client with a report for each infrastructure penetration testing service completed and provide recommendations to mitigate vulnerabilities and risks
18. Present infrastructure penetration testing findings and recommendations to clients and colleagues

Knowledge and understanding

You need to know and understand:

1. The fundamental principles and concepts relevant to the penetration testing of digital system infrastructure
2. The main components of an infrastructure penetration test and the high-level processes involved
3. The infrastructure penetration testing life-cycle, from the initial client contact, to the delivery of the final report and subsequent mitigation work
4. How to interpret client requirements for infrastructure penetration testing
5. The structure of an infrastructure penetration test, including all relevant processes and procedures
6. Industry standard infrastructure penetration testing methodologies and how to apply them
7. How to select and apply industry standard tools and techniques to identify and exploit vulnerabilities in digital system infrastructure
8. Industry standard and bespoke organisational tools and techniques to conduct infrastructure penetration testing and how to apply them
9. The types of foot-printing analysis including passive and active foot-printing
10. The tools and techniques used for foot-printing and how to apply them
11. Industry standard operating systems
12. the stages, tools, techniques, attack vectors, and surfaces to identify weak links
13. How to interpret the outputs of infrastructure penetration testing tools
14. The concept of pivoting through compromised devices
15. Understand the concept of pivoting through compromised devices.
16. The types of enumeration used to identify hosts and usernames on a network and how to apply them
17. Industry standard networking protocols including IPv4, IPv6, TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol)
18. Industry standard network devices including TCP/IP, DNS, switches and firewalls
19. Industry standard networks types that could be encountered during a penetration test:
20. Security implications of shared media, switched media and VLANs (Virtual

Local Area Network)
21. The importance of egress and ingress filtering, including the risks associated with outbound connections
22. Remote operating system fingerprinting active and passive techniques
23. File permission attributes within operating system file systems and their security implications
24. How finger daemon derives the information that it returns, and hence how it can be abused
25. UK legislation related to human rights, data protection, and computer misuse and the impact of these on infrastructure penetration testing
26. The concepts behind common microprocessor vulnerabilities such as Spectre and Meltdown
27. Common risks associated with Bluetooth
28. Active and passive operating system fingerprinting techniques and can demonstrate their use during a penetration test
29. how the Ethernet Protocol works
30. how the IPv4 and Ipv6 protocols works
31. Common network routing protocols and their security attributes
32. The configuration of routers, switches and Firewalls
33. Network traffic filtering and where this may occur in a network
34. The steps involved in performing clean-up activities after conducting infrastructure penetration testing
35. How to analyse and interpret the results of infrastructure penetration testing
36. How to mitigate vulnerabilities and prevent the associated exploits
37. How to document the results of infrastructure penetration testing

TECIS60443

Carry out infrastructure penetration testing

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	TECIS60443
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT(Cyber Security)
Keywords	Penetration testing, security testing, ethical hacking