

Introduction

When you pass the Wireless LAN Security exam, you earn credit towards the CWSP certifications.

This exam measures your ability to understand the weaknesses inherent in wireless LANs, the solutions available to address those weaknesses, and the steps necessary to implement a secure and manageable wireless LAN in an enterprise environment.

The skills and knowledge measured by this examination are derived from a survey of wireless networking experts and professionals from around the world. The results of this survey were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following chart provides the breakdown of the exam as to the weight of each section of the exam.

Wireless LAN Security Subject Area	% Of Exam
Wireless LAN Intrusion	20%
Wireless LAN Security Policy	30%
Wireless LAN Security Solutions	50%
Total	100%

Wireless LAN Intrusion – 20%

- 1.1. Explain how intruders obtain network access through analysis, spoofing, and information theft including the following methods:
 - 1.1.1. Monitoring & obtaining data sent in clear text or with weak encryption
 - 1.1.2. Use of wireless LAN protocol analysis and site survey tools
 - 1.1.3. WEP Decryption
 - 1.1.4. MAC address spoofing and circumventing filters
 - 1.1.5. Active intrusion techniques (connecting, probing, and configuring the network)
- 1.2. Explain how the following types of Denial of Service (DoS) attacks can occur in a wireless LAN and identify the tools that can be used to perform these attacks.
 - 1.2.1. RF jamming
 - 1.2.2. Data flooding
 - 1.2.3. Client hijacking
 - 1.2.4. Infrastructure misconfiguration
- 1.3. Demonstrate vulnerability auditing in a wireless LAN to determine weaknesses
 - 1.3.1. Locate & identify wireless LANs within and around a facility
 - War Driving
 - War Chalking
 - War Flying
 - 1.3.2. Explain common points of attack
 - Default configurations
 - Clear text data transmissions
 - Rogue hardware
- 1.4. Describe common non-secure configuration issues that can be the focus of an attack
- 1.5. Describe weaknesses in existing security solutions
- 1.6. Explain security vulnerabilities associated with public access wireless networks
- 1.7. Explain how malicious code or file insertion occurs in a wireless LAN through the use of:
 - 1.7.1. Viral attacks
 - 1.7.2. Placement of illegal content
- 1.8. Describe how intruders use profiling to select a target or gather information
 - 1.8.1. Searching publicly available resources
 - 1.8.2. Social engineering
 - 1.8.3. Wireless peer attacks to obtain corporate information

- 1.9. Explain peer-to-peer hacking and how it can be prevented
 - 1.9.1. Recognize wireless client exposure
 - 1.9.2. Identify detection and prevention mechanisms including IDS and personal firewall software
 - 1.9.3. Understand how corporate policy can be used to prevent use of corporate hardware on public networks

- 1.10. Describe weaknesses in and identify and configure the appropriate security-related controls for each of the following:
 - 1.10.1. SSIDs
 - 1.10.2. SNMP security (alarms, strong strings, disabling)
 - 1.10.3. Output power settings
 - 1.10.4. MAC filters
 - 1.10.5. Manufacturer's default settings
 - 1.10.6. Strong passwords
 - 1.10.7. Secure access to wireless infrastructure devices

- 1.11. Given the following wireless LAN hacking hardware & software, explain how an intruder could gain access to a network
 - 1.11.1. Password gathering software
 - 1.11.2. Protocol analysis software
 - 1.11.3. Session reconstruction software
 - 1.11.4. Enumerating software
 - 1.11.5. Rogue hardware
 - 1.11.6. Directional & Omni antennas

- 1.12. Summarize the following legal issues that apply to wireless LANs, and how they apply to computers and intellectual property:
 - 1.12.1. U.S. Federal laws regarding information security and illegal intrusion
 - 1.12.2. U.S. State laws regarding information security and illegal intrusion

Wireless LAN Security Policy – 30%

- 2.1. Explain the purpose and goals of the following wireless LAN security policies
 - 2.1.1. Password policy
 - 2.1.2. User training
 - 2.1.3. On-going review (auditing)
 - 2.1.4. Acceptable use & abuse policy
 - 2.1.5. Consistent implementation procedure
 - 2.1.6. Centralized implementation and management guidelines and procedures

- 2.2. Explain necessary items to include in the creation and maintenance of a wireless LAN security checklist

- 2.3. Describe when and how to implement traffic filtering

- 2.4. Describe and recognize the importance of asset management and inventory procedures for wireless LANs

- 2.5. Explain the importance of including wireless LANs in existing change management programs

- 2.6. Risk Assessment
 - 2.6.1. Explain the assets to be protected through securing a wireless LAN
 - 2.6.2. Explain and demonstrate the inherent weaknesses in wireless LAN security
 - 2.6.3. Given a wireless LAN attack scenario, explain and respond to the attack
 - 2.6.4. Given a wireless LAN configuration, explain and implement all the necessary steps to securing the wireless LAN
- 2.7. Perform an impact analysis for a series of wireless LAN attack scenarios which may include the following methods of attack:
 - 2.7.1. Analysis, spoofing, & information theft
 - 2.7.2. Denial of Service
 - 2.7.3. Malicious code or file insertion
 - 2.7.4. Target profiling
 - 2.7.5. Peer-to-peer hacking
 - 2.7.6. Physical security
 - 2.7.7. Social engineering
 - 2.7.8. Wireless LAN hacking hardware & software
- 2.8. Summarize risks to wired networks from wireless networks
- 2.9. Summarize the security policy related to wireless public-access network use
- 2.10. Summarize the security implications of using non-standard security solutions
- 2.11. Given a set of business requirements, design a scalable and secure wireless LAN solution considering the following security tactics:
 - 2.11.1. Wireless LAN segmentation
 - 2.11.2. Wireless DMZ configuration
 - 2.11.3. Use of NAT/PAT
 - 2.11.4. NAT/PAT impact on secure tunneling mechanisms
 - 2.11.5. Redundancy
 - 2.11.6. Wireless LAN equipment staging & deployment
 - 2.11.7. Wireless LAN cell sizing and shaping
 - 2.11.8. Scalability
 - 2.11.9. Appropriate use of different antenna types
 - 2.11.10. Operational verification
- 2.12. Secure equipment configuration and placement
- 2.13. Describe appropriate installation locations for wireless LAN hardware in order to avoid physical theft and tampering, considering the following:
 - 2.13.1. Security implications of remote placement of devices
 - 2.13.2. Physical security for remote infrastructure devices
 - 2.13.3. Secure remote connections to wireless LAN infrastructure devices
- 2.14. Implement physical security measures and describe why they are essential to prevent the following:
 - 2.14.1. Hardware theft
 - 2.14.2. Access to secure consoles

2.15. Security solution interoperability and layering

- 2.15.1. Explain the benefits of interoperable wireless LAN security solutions
- 2.15.2. Design and implement co-existing wireless LAN security solutions

2.16. Security management

- 2.16.1. Explain the necessary criteria for regular wireless LAN security reporting and documentation
- 2.16.2. Implement and conduct timely and consistent reporting procedures
- 2.16.3. Implement & maintain wireless LAN security checklist

2.17. Explain how to identify and prevent social engineering

- 2.17.1. Educate staff and security personnel
- 2.17.2. Implementation and enforcement of corporate policy regarding social engineering
- 2.17.3. Security marketing and propaganda campaigns to heighten awareness

Wireless LAN Security Solutions – 50%

3.1. Static and Dynamic WEP & TKIP

- 3.1.1. Explain the functionality, strengths, and weaknesses of WEP and TKIP
- 3.1.2. Explain appropriate scenarios and applications of static and dynamic WEP and TKIP
- 3.1.3. Install and configure static and dynamic WEP & TKIP
- 3.1.4. Illustrate feasibility of WEP exploitation
- 3.1.5. Manage scalable WEP & TKIP solutions

3.2. 802.1x and EAP

- 3.2.1. Explain the functionality of 802.1x & EAP
- 3.2.2. Explain dynamic key generation and rotation for solution scalability
- 3.2.3. Explain the strengths, weaknesses, and appropriate applications of 802.1x & EAP
- 3.2.4. Install and configure 802.1x & EAP, including
 - LEAP
 - EAP-TLS
 - EAP-TTLS
 - EAP-MD5
 - PEAP

- 3.2.5. Manage scalable 802.1x and EAP solutions

3.3. VPNs

- 3.3.1. Implement, configure, and manage the following VPN solutions in a wireless LAN environment:
 - PPTP
 - IPSec
 - L2TP
- 3.3.2. Explain the importance and benefits of session persistence in a wireless VPN environment

- 3.3.3. Explain the differences, strengths, and limitations of each of the following as a wireless VPN solution
 - Routers
 - VPN Concentrators
 - Firewalls
- 3.3.4. Describe benefits of mobile VPN solutions
- 3.4. Enterprise Wireless Gateways
 - 3.4.1. Understand the functionality of enterprise wireless gateways
 - 3.4.2. Recognize strengths, weaknesses, and appropriate applications for an enterprise wireless gateway
 - 3.4.3. Describe common security features, tools, and configuration techniques among enterprise wireless gateway products
 - 3.4.4. Install and configure an enterprise wireless gateway, including profiles and VPNs
 - 3.4.5. Manage and recognize scalability limitations of an enterprise wireless gateway
- 3.5. RADIUS and AAA
 - 3.5.1. Explain the wireless authentication and association processes
 - 3.5.2. Explain the purpose, location, and scalability of RADIUS and AAA solutions
 - 3.5.3. Describe the wireless standards supported by RADIUS
 - 3.5.4. Implement scalable RADIUS/AAA user authentication and auditing solutions
- 3.6. Switches and VLANs
 - 3.6.1. Describe the security advantages of switches and VLANs
 - 3.6.2. Describe the security disadvantages of hubs
- 3.7. Firewalls and Routers
 - 3.7.1. Given a wireless LAN topology, explain where firewalls can be added for security
 - 3.7.2. Describe the wireless security benefits of routers
 - 3.7.3. Explain the benefits of implementing access control lists
 - 3.7.4. Given a wireless LAN design, demonstrate how to implement a wireless DMZ
 - 3.7.5. Explain the benefits of network segmentation in a wireless network
 - 3.7.6. Implement segmentation of wireless LAN segments on a network
- 3.8. Software Solutions
 - 3.8.1. Implement software solutions for the following
 - 3.8.2. SSH2 Tunneling
 - 3.8.3. Securing wireless thin clients
 - 3.8.4. Port redirection
 - 3.8.5. Transport Layer Security (TLS)
- 3.9. Mobile IP
 - 3.9.1. Roaming across subnets and networks
 - 3.9.2. Tunneling through firewalls using HTTP

3.10. Differentiate between the following encryption schemes in terms of efficiency and security

- 3.10.1. RC4
- 3.10.2. DES/3DES
- 3.10.3. AES (FIPS 197)

3.11. Explain the following wireless LAN security standards

- 3.11.1. 802.1x
- 3.11.2. 802.11i

3.12. Describe the following types of intrusion detection methods and tools for wireless LANs

- 3.12.1. 24x7 centralized, skilled monitoring
- 3.12.2. Honey pots
- 3.12.3. Professional security audits
- 3.12.4. Accurate, timely reporting
- 3.12.5. Distributed agent software
- 3.12.6. Security spot checking
- 3.12.7. Available wireless LAN intrusion detection software and hardware tools

3.13. Given a list of wireless LAN configuration and security requirements, select and implement the appropriate type of authentication from among the following

- 3.13.1. Kerberos
- 3.13.2. EAP / LEAP / PEAP
- 3.13.3. WEP / TKIP
- 3.13.4. VPN
- 3.13.5. Certificates
- 3.13.6. 2-factor & 3-factor authentication
- 3.13.7. PAP / CHAP / MS-CHAP-v2
- 3.13.8. LDAP / Directory Services
- 3.13.9. RADIUS / AAA