11.2.5 Firewall Penetration Testing Facts

Firewalls are often the first line of defense against external security breaches. Firewalls can also be configured to prevent internal access to external, restricted, or malicious websites. Firewall penetration testing evaluates the firewall's traffic filtering capabilities. Today, most firewalls use a strict rule set that is secure.

This lesson covers the following topics:

- Firewall penetration testing
- Firewall penetration testing techniques

Firewall Penetration Tests

At the organizational level, firewall penetration testing should ensure that the firewall security configuration aligns with the organization's security practices and policies. Firewalls, whether hardware or software, are only as effective as their configuration. Testing is required to ensure the appropriate rules have been implemented and that those rules operate as intended.

The penetration tester begins by evaluating the organization's security policies, creating threat models, and conducting a risk assessment to further define the systems and resources that should be tested. Then the penetration tester chooses the methods used for the firewall penetration test. Having a strong understanding of the exploits used by attackers and the techniques attackers use to avoid detection is one of the best penetration test practices.

Firewall Penetration Testing Techniques

The following table describes several techniques for firewall penetration testing.

Technique	Description
Footprinting	The first technique the penetration tester will use is to footprint the firewall. Footprinting is done by running a port scan on the system and accessing banners. This allows the penetration tester to determine the type of firewall used. During footprinting, the penetration tester learns as much as possible about the firewall configuration. Firewall configuration information allows the penetration tester to select the penetration tests most appropriate based on the organization's needs and the network configuration.
Firewalking	Firewalking is an active reconnaissance technique that attempts to determine which Layer 4 protocols a specific firewall will allow through. Key points to remember about firewalking are: ▪ Firewalking uses the traceroute command and TTL values to analyze IP packet responses. ▪ A penetration tester analyzes packet responses to discover the IP Layer 4 protocols that are permitted through a network device with a firewall. ▪ TCP and UDP packets are sent using the specified protocol and port number. ▪ The TTL (time to live) value is set one hop farther than the device in question. For instance, if a firewall is three hops away, the TTL of the packets would be set to 4. ▪ Firewalking allows the penetration tester to determine a gateway's Access Control List (ACL) filters and map the network.
TCP packet filtering	Modifying the TCP packet, the penetration tester can: ▪ Spoof the IP address to gain unauthorized access. ▪ Use fragmentation attacks to force the TCP header information into the next fragment. This allows the penetration tester to bypass the firewall. ▪ Use proxy servers that block the actual IP address and display another. This allows access to a blocked website or target device. ▪ Use ICMP tunneling to tunnel a backdoor application in the data portion of ICMP Echo packets. ▪ Perform ACK tunneling using tools such as AckCmd to tunnel a backdoor application using TCP packets with the ACK bit set.