11.2.4 Evade Firewalls Facts

Firewall evasion is one of the most common skills attackers seek to master. As an ethical hacker and penetration tester, it is important for you to familiarize yourself with firewall evasion techniques and how to implement countermeasures.

This lesson covers the following topics:

- Evasion techniques
- Evasion tools
- Evasion countermeasures

Evasion Techniques

After an attacker detects a firewall, the next step is to evade the firewall and compromise a trusted host. The following table describes techniques attacker use to evade firewalls.

Technique	Description
Spoofing	Spoofing is one of the most effective evasion techniques. In this technique, attacker modifies the addressing information in the IP packet header and source address field, allowing the attacker to masquerade as a trusted host and bypass network access controls. An attacker can also use spoofing to make the source of an attack appear to come from a trusted source.
Source routing	In source routing, the sender of the packet designates the route that a packet should take through the network. The purpose is to specify a route that bypasses the firewall. Using this technique, the attacker attempts evade the firewall restrictions. For example, the attacker will not send a packet directly to destination F, but rather to B, C, D, E, and then F, evading the firewall.
IP addressing	The use of an IP address instead of a URL may be effective for evading or bypassing a firewall. This method involves typing the IP address directly into the browser's address bar instead of typing the blocked website's domain name. The attacker must have the IP address in order to use this method. The IP address can be obtained using traceroute or other tools.
Fragmentation	Using IP fragmentation, an attacker creates tiny fragments of outgoing packets, forcing some of the TCP packet's header information into the next fragment. The firewall filter rules will not identify the tiny fragmented packets as a threat. The attack will succeed if the firewall examines only the first fragment and allows all the other fragments to pass through. This attack is used to avoid user-defined filtering rules. It works when the firewall checks only for the TCP header information.
HTTP tunneling	HTTP tunneling can bypass firewalls and may be one of the easiest tunneling methods to use because the protocol is already allowed through many firewalls as part of normal operations. This method can be implemented if the target network has a public web server with port 80 unfiltered on its firewall. Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate traffic.
ICMP tunneling	In ICMP tunneling, the hacker tunnels a backdoor application in the data portion of an ICMP echo packet. RFC 792, the ICMP specification, does not define contents in the data portion. Therefore, any data can be inserted in the payload portion of the ICMP packet. Some administrators keep ICMP open on their firewall because it is useful for tools like **ping** and **traceroute**. Assuming that ICMP is allowed through a firewall, attackers can use an ICMP tunneling tool to execute commands by tunneling them inside the payload of ICMP echo packets.
ACK tunneling	Attackers can bypass a firewall using ACK tunneling. Some firewalls do not check packets with the ACK bit set because ACK bits are used to support response to legitimate traffic. This allows an attacker to tunnel a backdoor application in TCP packets with the ACK bit set.
Anonymous web surfing sites	Attackers that can potentially bypass blocked sites using anonymous web surfing sites. Many websites around the internet enable surfing the internet anonymously. Some websites even provide options to encrypt the website's URLs.
Proxy server	Firewalls can be evaded by using a proxy server. An attacker would need to find an appropriate proxy server for the type of firewall being evaded.
DNS server poisoning	An attacker can perform DNS server poisoning. This technique typically uses a a man-in-the-middle attack to bypass the firewall.

Evasion Tools

There are many evasions tools available. Be familiar with the most well-known evasion tools and how to effectively use them for ethical hacking, penetration testing, and countermeasure defenses. These tools include:

- nmap
- tcp-over-dns
- Colasoft Packet Builder
- HTTPTunnel
- MGEN
- Snare Agent
- AckCmd
- Freenet

Evasion Countermeasures

The first line of evasion defense is having knowledge of the network architecture. With knowledge of the network architecture, you can implement the following evasion countermeasures.

Countermeasure	Description
Configuration	The firewall should be configured to filter the IP address of an intruder. Use firewall ruleset to deny all traffic and enable only the services required. Whenever possible, create a unique user ID to run the firewall services. Always avoid using the default, administrator, or root IDs on any device. Additionally, a best practice is to document all configuration changes when vulnerabilities are discovered and countermeasures implemented. Remember to configure remote syslog servers using these countermeasures.
Defense in depth	Practice defense in depth techniques and adjust security policies to adapt to the evolving threats. Conduct countermeasures using the same evasion tools that malicious attackers use. These include: - Port scanning to know the available ports that uniquely identify the firewalls. - Banner grabbing to detect the services run by the firewall. When possible, disable or change the banner. - Firewalking to expose TTL vulnerabilities.
Probe packets	Determine how information is retrieved from the firewall when probe packets are sent. Perform fragmentation attacks with an IDS fragmentation reassembly timeout set. Then implement evasion defense security measures.
Firewall monitoring	Have a consistent and disciplined policy to monitor firewall logs at regular intervals. Investigate all suspicious log entries when found. An example of a dedicated evasion defense tool is Traffic IQ Professional, which enables security professionals to audit and validate the behavior of security devices. This tool can be used to assess, audit, and test the behavioral characteristics of any non-proxy packet filtering device, including application-layer firewalls, intrusion detection and prevention system, routers, and switches.