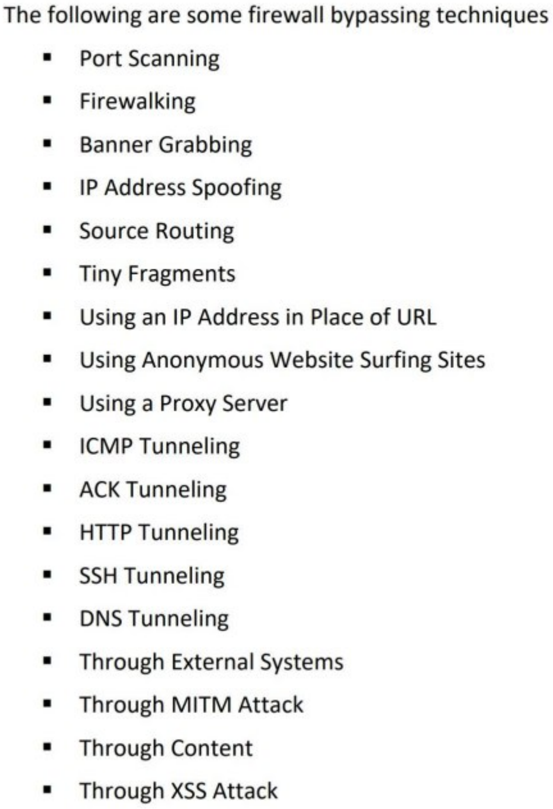
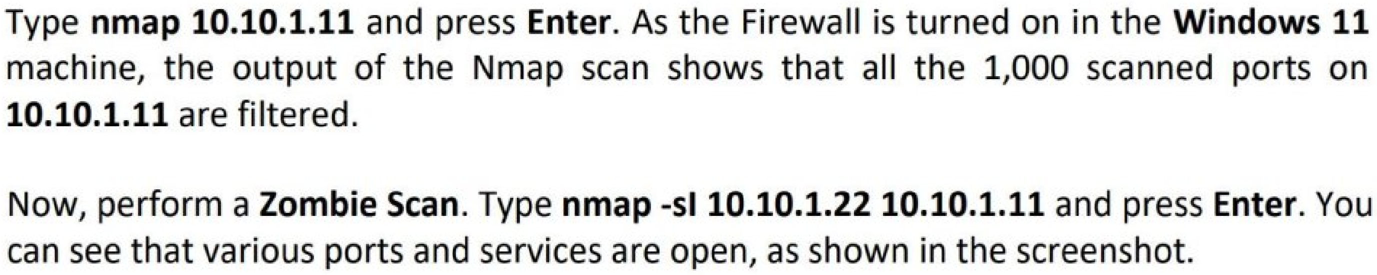
Bypassing Firewalls using Nmap

Bypassing Firewalls using Nmap



The following are some firewall bypassing techniques

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack



Type **nmap 10.10.1.11** and press **Enter**. As the Firewall is turned on in the **Windows 11** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.1.11** are filtered.

Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.1.22 10.10.1.11** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.