Nmap

Networking Tools:

Ping, Whois, traceroute, dig

Nmap:

NULL Scans: the TCP request is sent with no flags set.

FIN Scans: a request is sent with the FIN flag to close an active connection

Xmas Scans: send malformed TCP packet and expects a RT response for closed ports

ICMP Network Scanning:

First objective: obtain a "map" of network structure, or see which IP addresses contain active host and which don't.

One way to do this: ping sweep--Nmap sends ICMP packet to each possible IP address for specified network. Response=marks IP address as being alive.

Nmap Scripting Engine (NSE)

NSE Scripts used for: scanning for vulnerabilities, atuomating explits for them.

NSE Script library, helpful categories:

safe:- Won't affect the target

intrusive:- Not safe: likely to affect the target

vuln:- Scan for vulnerabilities

exploit:- Attempt to exploit a vulnerability

auth:- Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)

brute:- Attempt to bruteforce credentials for running services

discovery:- Attempt to query running services for further information about the network (e.g. query an SNMP server).

Firewall Evasion:

Typical Winodows host blocks all ICMP packets

Switches for firewall evasion:

-f:- Used to fragment the packets (i.e. split them into smaller pieces) making it less likely that the packets will be detected by a firewall or IDS.

An alternative to -f, but providing more control over the size of the packets: --mtu <number>, accepts a maximum transmission unit size to use for the packets sent. This must be a multiple of 8.

--scan-delay <time>ms:- used to add a delay between packets sent. This is very useful if the network is unstable, but also for evading any time-based firewall/IDS triggers which may be in place.

--badsum:- this is used to generate in invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond automatically, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence of a firewall/IDS.