



Motivation and Study Techniques to help you learn, remember, and pass your technical exam!

- [www.mindcert.com](http://www.mindcert.com)
- [Subscribe via RSS](#)

### Information Gathering Methodology

- 1 - Research initial information
  - 2 - Locate the network range
  - 3 - Discover active machines
  - 4 - Discover open ports / access points
  - 5 - Discover operating systems
  - 6 - Discover services on ports
  - 7 - Map the network
- After gathering information, next step is to find the network range of the target
- Information can be obtained from DNS, Whois, IPinfo, etc.
- Trace the route between your network and the target
- Establish the IP TTL
- Search with packets table
- Send out consecutive UDP packets with different TTLs
- Device sends back an ICMP TTL Exceeded message
- Some devices will also reply with DNS information

### Detecting Live Systems on Target Network

- Types of Tools
- Ping utility
  - Traceroute
  - Nmap
  - Metasploit
  - Nessus
  - OpenVAS
  - Snmap
  - Sslstrip
  - Sslstrip2
  - Sslstrip3
  - Sslstrip4
  - Sslstrip5
  - Sslstrip6
  - Sslstrip7
  - Sslstrip8
  - Sslstrip9
  - Sslstrip10
  - Sslstrip11
  - Sslstrip12
  - Sslstrip13
  - Sslstrip14
  - Sslstrip15
  - Sslstrip16
  - Sslstrip17
  - Sslstrip18
  - Sslstrip19
  - Sslstrip20
  - Sslstrip21
  - Sslstrip22
  - Sslstrip23
  - Sslstrip24
  - Sslstrip25
  - Sslstrip26
  - Sslstrip27
  - Sslstrip28
  - Sslstrip29
  - Sslstrip30
  - Sslstrip31
  - Sslstrip32
  - Sslstrip33
  - Sslstrip34
  - Sslstrip35
  - Sslstrip36
  - Sslstrip37
  - Sslstrip38
  - Sslstrip39
  - Sslstrip40
  - Sslstrip41
  - Sslstrip42
  - Sslstrip43
  - Sslstrip44
  - Sslstrip45
  - Sslstrip46
  - Sslstrip47
  - Sslstrip48
  - Sslstrip49
  - Sslstrip50

