Certified Ethical Hacker
Module 2 – Footprinting

Footprinting is the Reconnaissance phase of the 5 step attack wheel.

What is Footprinting?

1. Unearth Initial Information
2. Locate the network range
3. Ascertain active machines
4. Discover open ports / access points
5. Detect operating systems
6. Uncover services on ports
7. Map the network

Certifi
ced Ethical Hacker

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

Visit us www.mindcert.com

What is Footprinting?

- Domain Name Lookups
- Telephone
- E-mail
- Contacts
- Search Engines and Websites
- Open Source
- Domain and IP information
- Information about Registered Domains
- Whois
- Hacking Tools
- Tools
- SmartWhois
- Nslookup
- Provides DNS information
- Provides Whois and DNS Dig functionality
- Unearths Initial Information
- Information Gathering Methodology
- Locate the Network Range
- Unearths Initial Information
- After gathering information, next step is to find the network range of the target
- Traceroute
- Exploits the IP TTL
- Reveals path IP packets take
- Sends out consecutive UDP packets with ever increasing TTLs
- Device sends back an ICMP TTL Exceeded message
- Some devices will also reply with DNS information

Information can be obtained from IANA Providers
- ARIN
- APNIC
- RIPE

Information Gathering Methodology
- 1 - Unearth Initial Information
- 2 - Locate the network range
- 3 - Ascertain active machines
- 4 - Discover open ports / access points
- 5 - Detect operating systems
- 6 - Uncover services on ports
- 7 - Map the network

Certified Ethical Hacker
Module 2 – Footprinting

More coming soon...