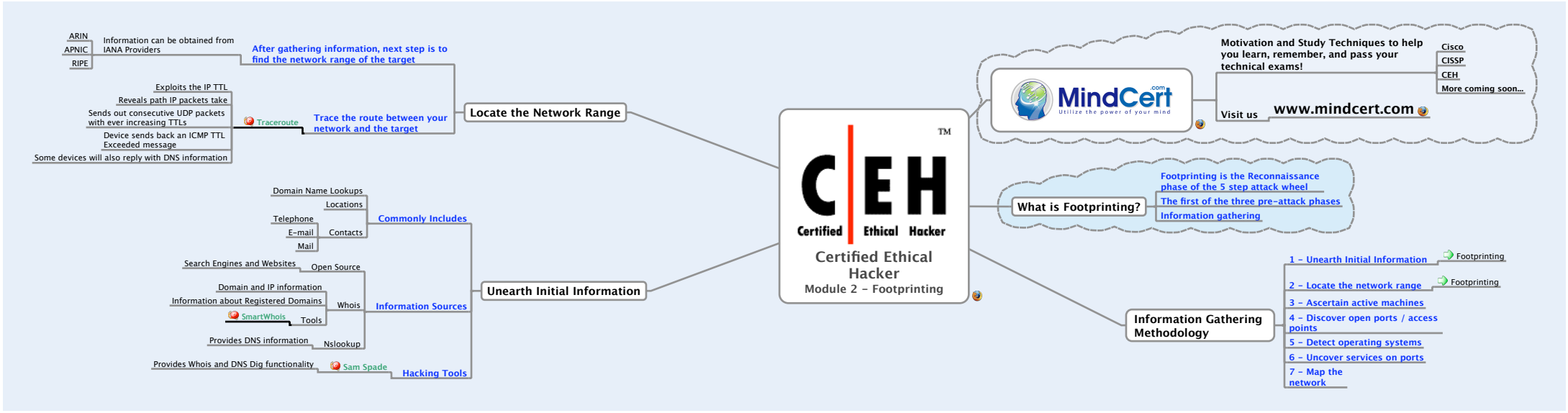
Certified Ethical Hacker
Module 2 - Footprinting
Locate the Network Range
After gathering information, next step is to find the network range of the target
ARIN
APNIC
RIPE
Information can be obtained from IANA Providers
Trace the route between your network and the target
Traceroute
Exploits the IP TTL
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
Unearth Initial Information
Commonly Includes
Domain Name Lookups
Locations
Telephone
E-mail
Contacts
Mail
Information Sources
Open Source
Search Engines and Websites
Whois
Domain and IP information
Information about Registered Domains
Tools
SmartWhois
Nslookup
Provides DNS information
Hacking Tools
Sam Spade
Provides Whois and DNS Dig functionality
MindCert
Utilize the power of your mind
Motivation and Study Techniques to help you learn, remember, and pass your technical exams!
Visit us
www.mindcert.com
Cisco
CISSP
CEH
More coming soon...
What is Footprinting?
Footprinting is the Reconnaissance phase of the 5 step attack wheel
The first of the three pre-attack phases
Information gathering
Information Gathering Methodology
1 - Unearth Initial Information
Footprinting
2 - Locate the network range
Footprinting
3 - Ascertain active machines
4 - Discover open ports / access points
5 - Detect operating systems
6 - Uncover services on ports
7 - Map the network