Advanced Port scanning - Scanning and Enumeration

EC-Coincil's (ECC) scanning methodology

- Check for live systems
- check for open ports
- discover services
- discover the operating systems (banner grabbing)
- scan for vulnerabilities
- map the network
- create proxies

Port scanning Ethics

- Never scan without written permission or out of the scope of that permission.

Port scanning is like checking to see if doors and windows on a house are locked. It's looking through the window to see what valuables are there. It may not be illegal, but you are going to make somebody uncomfortable and they might call the cops.

Scanning Defined

Scanning is the process of determining what ports are open and what services are running on those ports.

ECC - 5 network security Zones

EEC divides networks into zones in order to manage systems with proper security controls. This is important when trying to map a network.

1. Internet

- The wile west and uncontrollable

2. Internet DMZ

- Security buffer between network and the internet

3. Production network zone

- Restricted zone that controls access from uncontrolled zones

4. Intranet Zone

- Controlled zone with few restrictions
- "appropiate span of control in in the place to assure that network traffic does not compromise the operation of ciritical business functions."

5. Management Network Zone

- "Tightly controlled and available to only a small number of authorized users"