filename:comptia-secplussy0601-9-1-network_reconnaissance_and_discovery
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Security Assessment Techniques

Given a scenario, use the appropriate tool to assess organizational security.

Description: In this episode, the viewer will identify techniques to assess organizational security through network reconnaisance and discovery using utilities such as tracert, nmap, nslookup and dig, hping, arp, route and more.

- Network reconnaissance and discovery
    - Network Administration
        - **tracert/traceroute**
        - nslookup/dig
        - pathping
        - route
            - ipconfig/ifconfig
            - arp
            - netstat
    - Network discovery, vulnerabilites, enumeration
        - nmap
            - port scanning vulnerabilities
            - hosts, services, operating systems
        - hping
            - Packet analyzer
            - Packer assembler
        - scanless

    - Port scanner
- netcat
    - Remote shell
    - Banner grabbing
    - Transfer files
    - Port scanning
- curl
    - Web page grabing
    - use curl to fetch a file of upload a file
- the harvester (OSINT)
    - Python Script written by Christian Martorella
    - Used to catalog e-mail addresses and subdomains of a target
    - Must keep it up to date
- sn1per
    - Automated scanner for collecting data
    - Pentesting and exploration
    - basic recon, open ports, sub-domain hijacking
    - DNS and subdomain info
- Dnsenum
    - DNS record enumeration
- Nessus
    - Vulnerability scanner
- Cuckoo
    - Sandbox for malware analysis