Admin

- Assignment turn-in review
- Connectivity Issues???
- Pacing?
- Questions?

Passive Information Gathering (did not cover last lesson)

- Google (public)
    - Site:x.com (only domains ending in x.com),
    - -site:x.com (-site means do not include)
    - Filetype, inurl, intitle
- Theharvester (public)
    - -d <domain> -b <searchmethod>
- Whois (public)
- Recon-ng

Active Information Gathering

- DNS (What is DNS? Why is it important?)
    - Host -t <type> <domain>
        - Host -t ns megacorpone.com
        - Forward (looking up by domain name to get IP)
        - Reverse (looking up ip to get domain name)
        - Zone Transfer
            - -l <domain name> <dns server>
    - Nslookup
    - DNSrecon -d <domain> -t axfr
    - Dnsenum <domain>
        - What is zonetransfer.me
    - Test
- Port Scanning (Nmap) https://nmap.org/book/man-briefoptions.html
    - What does nmap <ip> do by default? What ports?
    - Three way handshake
    - -sS, -sT, -Pn, -p-, -A, -O, -Sv, -Oa, -v (shows progress as it goes)
    - Via a proxy
        - You cannot do any kind of ICMP (ping) or UDP scans, no SYN stealth scan, no OS detection etc. This means that the default nmap commands you are using will not work
        - -Pn -sT
    - UDP?
    - Scripts? https://nmap.org/book/nse-usage.html
        - --script , can use wild cards like --script “smb*”--script “safe and default”
- SMB (Server Message Block). What is this? Port 445

        - The Server Message Block Protocol (SMB protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network
        - Nbtscan
        - Enum4linux (most used)
    - SMTP (Simple Mail Transfer Protocol)
    - SNMP (Simple Network Management Protocol) Ports 161/162
        - Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more
        - SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications
        - Public / private community strings
        - Snmpwalk
        - onesixtyone
    - Sparta
        - Does incremental scanning

Chapter 5 Warning

Vulnerability Scanning

- Nessus (is very big! Will take some time to install)
- Overkill in general - do not rely on
    - More specific tools best (same goes for nmap)
    - Data can be inaccurate