First Principles: Domain Separation, data hiding, simplicity, and least privilege

1. Time: 1-4
2. Lecture: Continued from morning
    a. Enumeration
        i. Port Scanning
            1. Differentiating open/closed/filtered ports
                a. Importance of three-way handshake, RST flag
            2. Type of information gained from a port-scan
                a. Identifying OS based on port scan results
    b. Network Attacks
        i. MOTS/MITM
        ii. DoS/DDoS
    c. Transition from network attacks to physical attacks
        i. Frame Rubber Ducky as a way to get a foothold in a network
3. Activities
    a. Relating to Lecture
        i. Activity: Use netcat to try to connect to ports 139/445 on a Windows and Linux host
            1. Observe the attempts in Wireshark; note that the handshake completes on Windows, RST on Linux
        ii. Activity: Turn on Windows Firewall and repeat
            1. Observe that nothing is returned on Windows host
        iii. Activity: Use nmap to ping sweep a network
        iv. Activity: Use nmap to port scan new hosts in a network
    b. Relating to Rubber Ducky
        i. Activity: Generating a standalone malicious executable with msfvenom and distributing it with a webserver
        ii. Activity: Setting up a rubber ducky to open a command prompt and launch calc
        iii. Activity: Setting up a rubber ducky to use powershell to download and run an executable
        iv. Activity: Post exploitation; hashdump
        v. Activity: Post exploitation; pivoting to the domain controller with stolen credentials
            1. Setting up a port forward on an exploited host to bypass a firewall
4. Reference
    a. Rubber Ducky script
        i. https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---Windows-10-:-Download-and-execute-file-with-Powershell
        ii. https://ducktoolkit.com/encoder/