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

1. Time: 1-4
2. Lecture: Continued from morning
   1. Enumeration
      1. Port Scanning
         1. Differentiating open/closed/filtered ports
            1. Importance of three-way handshake, RST flag
         2. Type of information gained from a port-scan
            1. Identifying OS based on port scan results
   2. Network Attacks
      1. MOTS/MITM
      2. DoS/DDoS
   3. Transition from network attacks to physical attacks
      1. Frame Rubber Ducky as a way to get a foothold in a network
3. Activities
   1. Relating to Lecture
      1. 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
      2. Activity: Turn on Windows Firewall and repeat
         1. Observe that nothing is returned on Windows host
      3. Activity: Use nmap to ping sweep a network
      4. Activity: Use nmap to port scan new hosts in a network
   2. Relating to Rubber Ducky
      1. Activity: Generating a standalone malicious executable with msfvenom and distributing it with a webserver
      2. Activity: Setting up a rubber ducky to open a command prompt and launch calc
      3. Activity: Setting up a rubber ducky to use powershell to download and run an executable
      4. Activity: Post exploitation; hashdump
      5. 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
   1. Rubber Ducky script
      1. <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---Windows-10-:-Download-and-execute-file-with-Powershell>
      2. <https://ducktoolkit.com/encoder/>