Pentesting Methodology

# **Website or Internal/External Network Pentest**

* **Ping domain for ip address**
* **Scan ip address for all open ports**
  + using nmap sudo nmap -p- -T4 -vv -O --min-rate 20000 -Pn ip.ip.ip.ip  
    -p- scans all 6535 ports  
    -T4 sets the timing template to 4 (0-5). Speeds up scan but possibly less accurete  
    -vv increases verbosity of output  
    -O enables OS detection  
    --min-rate 20000 sends a min of 20,000 packets/sec speeding up the scan but can overwhelm the target. OPTIONAL  
    -Pn Treats all hosts as offline. skips the discovery phase- nmap will attempt to scan every port on the target without doind a pre-lim check to see if it is up  
    ip.ip.ip.ip is the ipaddress target
  + using pentest tools
* **identify services and versions running on those ports from previous scan**
  + using nmap nmap -p 3306 -sV -sC -Pn ip.ip.ip.ip  
    -p 3306 Scan only port 3306  
    -sV Version detection. nmap tries to determine the version of the service running on the port.  
    -sC: Run default script scan. This uses the built-in scripts in nmap to perform various checks and additional information gathering on the target.  
    -Pn: Treat all hosts as online. This skips the discovery phase, so nmap doesn't check first to see if the target is online; it just starts scanning.  
    10.129.156.28 : The target IP address that you're scanning.
  + using pentest tools
* **Identify out of date, unpatched, vulnerable services and versions running on those ports**
  + searching with metasploit
  + Scanning with ConnectSecure