- Filename: eccouncil-ceh31250-v10-3-2-2-scanning_with_nmap_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Scanning with Nmap Pt.2
- Description: In this episode, Daniel and Zach demonstrate using the very popular scanning tool Nmap for engaging in a variety of host scanning techniques. Specifically here you'll see how to target specific ports for enumeration, scan UDP and TCP separately or together, perform OS enumeration and service versioning, and utilizing the Nmap Scripting Engine which will allow you to even perform vulnerability scanning and exploitation.

==========

Scanning with Nmap Pt.2

- So we see the list of open ports and services that Nmap discovers; is there any way to control it to look for specific ports?
- Port selection (`-p`)
    - Simple port selections
        - Single Port
        - Port range (`1-1024, -1024, 50000-`)
            - All ports (`-p-`)
        - Specific ports (eg `21,23,80,443`,etc)
    - TCP and/or UDP port scanning
        - `-sU` scans UDP ports
            - Then you specify the port number like normal
        - You can scan for both TCP and UDP ports at the same time
            - `nmap -sU -sS -p U:53,64,T:21,23,80 10.0.0.165`
- Is this the extent of the information that Nmap can discover, or are there other things it can extract?
- OS and Services Enumeration
    - OS
        - `nmap -O -T5 -F -n 10.0.0.165-168`
    - SSH, HTTP, FTP, Telnet (God forbid!), other...
    - Looking for version info
    - Service identification (-sV)
        - Get version info: `nmap -sV -n -p 21,22,80 10.0.0.165`
        - `--version-intensity`
            - Scale of 0 - 9
                - `--version-light` == `--version-intensity 2`
- Are there any other things about Nmap that we should be familiar with?
- Disabling ping (-Pn)
    - Skip host discovery
        - Will attempt to scan host without pinging to determine if up first
    - `--send-ip` and `--disable-arp-ping`
        - Used in local network environments

- Target input file (-iL)
- NSE Scripts
    - `nmap -Pn --script vuln 10.0.0.165`
    - `nmap -Pn --script exploit`
    - `nmap -Pn --script dos`
    - `nmap -sV -vv`
    - `nmap -A -T4 -n -Pn -p- 10.0.0.165`
        - OR change ip for ip range
            - `nmap -A -T4 -n -Pn -sU -p 1-65535 10.0.0.165`
    - `-sC` == `--script=default`
    - `-A` = Aggressive Scan
        - `-O`, `-sV`, `-sC`, `--traceroute`
- Output parameters
    - -oA (Dump ALL formats)
    - -oN (Dump to .nmap file)
    - -oG (Dump to grepable file)
    - -oX (Dump to XML file)
        - Use `xsltproc` to render XML in HTML document
            - `xsltproc nmap_output.xml -o nmap_output.html`
- Packet crafting
    - Nmap
    - hping3
    - Scapy
    - Modifying TCP packets in order to test firewall rules
        - `nmap -sX -n 10.0.0.165`
        - `nmap --scanflags URGACKPSHRSTSYNFIN`
        - `hping3 -V -S -c 5 -p 80 10.0.0.165 -s 8888`
        - ```
          $ scapy
          >>> packet = IP(dst="10.0.0.200")/TCP(dport=139, flags="S")
          >>> unans, ans = sr(packet)
          >>> unans.summary()
          >>> ans.summary()
          ```
          ```