- Filename: eccouncil-ceh31250-v10-3-2-1-scanning_with_nmap.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Scanning with Nmap
- 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 perform SYN(Stealth) scans, TCP Connect scans, ACK scans, XMAS Scans, NULL scans, and FIN Scans. You'll also be shown how to change the timing of the scan (for performance or stealth) as well as how to deploy other obfuscation tactics like fragmenting the scan, deploying decoys, and spoofing source IP addresses.

==========

Scanning with Nmap

- We've been talking about learning everything we can about a client's systems. What is it that Nmap does to help us in that effort?
    - It scans systems or ip ranges for live hosts
    - Then it queries their ports to discover services
- How does it do that?
- SYN scan (`-sS`) vs. full connect scan (`-sT`)
    - Look at the man page for nmap
    - Wireshark capture both `-sS` and `-sT` scans to see the differences
- ACK scan (`-SA`)
    - Helps you map out firewall rules
    - Sends an ACK packet
        - Meant to see if the port is filtered
            - If port responds with RST then the port is not filtered
            - If port doesn't respond or sends error then port is filtered
- `-sX`
    - XMAS scan
    - URG, PSH, and FIN flags set
    - May slip through non-stateful firewalls
    - `--scanflags=URGACKPSHRSTSYNFIN`
- `-sN`
    - NULL scan
    - No flags raised
    - May slip through non-stateful firewalls
- `-sF`
    - FIN flag set
    - May slip through non-stateful firewalls
- `-f`
    - Fragment packets to avoid IDS and/or packet filtering firewalls
- `-D`
    - Decoys
    - `nmap -Pn -n --send-ip -D 10.0.0.1,10.0.0.165 10.0.0.231`
- Timing
    - Slow the timing of the packets down

        - `-T0,-T1`

- `-S`
    - Spoofed source address
    - `nmap -e eth0 -S 10.0.0.165 10.0.0.231`