- Filename: eccouncil-ceh31250-v11-3-10-1-nmap-idle-ipid-scan.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: Nmap: IDLE/IPID Scan
  ==========

Nmap: IDLE/IPID Scan

Objectives:

- Describe the process of an IDLE/IPID scan
- Use nmap to perform an IDLE/IPID scan to enumerate ports states and service detail
- Explain the pros and cons when utilizing this type of scan

- Kathy (spooky episode. There be zombies!)
  - Zombie scan
  - Takes advantage of incremental IPID values
    - Used to combat fragmentation
      - We want Global rather than per-host IPID increments
- How does the process work?
  - Step 1
    - Attacker >--SYN/ACK--> Zombie
    - Attacker <----RST----< Zombie
      - IPID is 2000
  - Step 2
    - Attacker >----SYN----> Target
      - *Source IP is spoofed to that of Zombie*
        - Target >----RST----> Zombie
          - *OPEN port increments IPID value of Zombie to 2001*
          - *CLOSED port doesn't increment Zombie IPID Value*
          - *FILTERED and CLOSED output are the same*
            - RST is sent back by CLOSED ports, which are ignored by Zombie
            - Nothing is sent back by FILTERED, which doesn't affect Zombie IPID
  - Step 3
    - Repeat Step 1
      - *nmap reports port status by inspecting IPID Value*
        - *If IPID = 2002, then port is OPEN*
        - *If IPID = 2001, then port is CLOSED|FILTERED*
- (Kathy): Well that sounds really...
  - (me): COOL!?...
  - (Kathy): Complicated. Enough of the talk, show us how this is done.
- Zombie Scan Demo

- `nmap -Pn -sI 10.0.10.50 <targetIP>`
    - *10.0.10.50 is the IP of the Edutainer Printer*

https://nmap.org/book/idlescan.html