

- Filename: eccouncil-ceh31250-v10-3-1-1-host_discovery.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Host Discovery
- Description: In this episode, Daniel and Zach examine the importance and techniques for performing host discovery. Here you'll be presented with the general concepts surrounding host discovery and be shown how to use both common system tools like ping and scripting towards that end. They will also cover using tools like nmap and hping3 to perform host discovery.

=====

Host Discovery

- What is host discovery?
 - Programmatically finding live devices on a target network
 - Workstations
 - Servers
 - Printers
 - VoIP phones
 - Mobile devices
 - Any other network connected device
- Will we need some elite hacker tool for finding these hosts?
 - Not necessarily
 - `ping`
 - Show the tediousness of manually pinging each possible target
 - Scripting `ping`
 - Linux
 - Powershell
- That's great, but I'm guessing there are some tools we can just download and use?
 - Plenty of them
 - GUI Tools
 - CLI Tools
 - `nmap -sn 10.0.0.0/24`
 - `hping3 -l 10.0.0.x --rand-dest -I eth0`