

- Filename: eccouncil-ceh31250-v11-4-1-1-enumeration-basics.md
- Show Name: CEHV11 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: Enumeration Basics

=====

## Enumeration Basics

### Objectives:

- Define Enumeration
- List assets targeted during Enumeration process
- List and describe Enumeration techniques
- Recognize common ports and services targeted during Enumeration

- 
- Kathy - I've heard you using the term 'Enumeration' in many of our episodes already. Can you formally define that for us?

- Discovering and listing target information

- Network hosts
- Network services
- Network shares
- User accounts
- Email addresses
- Groups

- How is this done?

- Brute-force
- Guessing
- Defaults
- Banners
- Email
- SNMP
- Zone Transfers
- Network sniffing

- What are a few common ports and services targeted for enumeration?

- Could be any port/service that is discovered
- Here are a few common

- NetBIOS
- SNMP:161 (UDP)
- LDAP:389 (TCP/UDP)
- HTTP(s):80,443 (TCP)
- NTP:123 (UDP)
- NFS:2049 (TCP)
- SMTP:25 (TCP)
- DNS:53 (TCP/UDP)