

- Filename: eccouncil-ceh31250-v12-4-2-1-snmp-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: SNMP Enumeration

=====

SNMP Enumeration

Objectives:

- Define SNMP Enumeration
- Identify useful information that could be gathered through SNMP Enum
- Utilize common SNMP Enum tools like Snmpcheck to enumerate target info

-
- What is SNMP?
 - A system of communication to relay status info
 - Used for system health monitoring
 - OS independent
 - SNMP basics
 - Managers
 - Agents
 - Trap
 - Informs Agent of events
 - Community String
 - Basically a password
 - Default of 'public'
 - Default of READ access
 - 'private' is another commonly used string
 - Typically set to READ/WRITE
 - Management Information Base (MIB)
 - Database of objects that can be managed with SNMP
 - Object Identifier (OID)
 - Identifies the MIB objects
 - Enumeration Tools
 - onesixtyone
 - snmp-check
 - Nmap
 - `ls /usr/share/nmap/scripts | grep snmp`
 - `sudo nmap -sU -p 161 --script snmp-win32-users.nse <targetIP>`
 - SNMPWalk
 - `snmpwalk -c public -v1 <targetIP> <OID>`