Windows

Antivirus

1. `sc query windefend`

   > Query the Service Control Manager for Windows Defender
   >
   > > I couldn't find a list of Anti-Virus service names online :(

2. `nxc smb <ip> -u user -p pass -M enum_av`

Domain SID

1. `nxc ldap DC1.scrm.local -u sqlsvc -p Pegasus60 -k --get-sid`
2. `whoami /user`
3. PowerShell(Requires Active Directory Module)
   1. Direct retrieval: `(Get-ADDomain).DomainSID.Value`
   2. From user object: `(Get-ADUser "Username").SID.AccountDomainSID`

#windows #domain-sid #netexec #antivirus #enumeration