- **What is kerberos authentication?**

1. User logs in to his computer and sends a request for a TGT to the AS. The request includes User's user ID, the ID of the requested service TGT, the IP address of his computer, and the lifetime of TGT.
2. The AS checks if User exists in the KDC database. If he does, it generates a session key to be used between User and TGS. The AS sends two messages back to User: one encrypted with TGS secret key and one encrypted with User's secret key (a hash of his username & password).
3. User decrypts the messages and logs in, caching TGT locally. When he wants to access a network resource (in this case, the SQL server), Nick sends a request to TGS with the resource name he wants to access, his user ID & timestamp, and the cached TGT.
4. The TGS decrypts User's information and provides a service ticket and a service session key for accessing the SQL server. The TGS encrypts the ticket with the SQL server's secret key and sends it back to User.
5. User sends a request to the SQL server, encrypted with the service ticket and the session key.
6. The SQL server decrypts the request and, if it's valid, provides User with access to the SQL server.

- **What is NTLM authentication?**

1. User enters his username and password on any client machine connected to Domain Controller (DC).
2. User's client creates a hash of his password.
3. User's client sends a logon request to the domain controller (DC) with his username.
4. The DC sends a random number (logon challenge) to User's client.
5. User's client encrypts the logon challenge using the hash of his password and sends it back as a response.
6. The DC uses the hash of User's password to encrypt the logon challenge and compares it with User's client's response.
7. User is authenticated and granted access if the encrypted logon challenge and the response match.

- **How to enumerate AD users?**

1. AD-Module
2. Bloodhound
3. Powerview

- **How to get credentials to go into AD?**

1. LLMNR Poisoning attack [Responder]
2. PasswordSpray using Kerbrute tool [linkedin employees name]
3. SMB-Relay attack [NTLMRelayx]

- **What is DCSync attack?**
  The DCSync permission implies having these permissions over the domain itself: DS-Replication-Get-Changes, Replicating Directory Changes All and Replicating Directory Changes In Filtered Set.

Important Notes about DCSync:

- The DCSync attack simulates the behavior of a Domain Controller and asks other Domain Controllers to replicate information using the Directory Replication Service Remote Protocol (MS-DRSR). Because MS-DRSR is a valid and necessary function of Active Directory, it cannot be turned off or disabled.
- By default only Domain Admins, Enterprise Admins, Administrators, and Domain Controllers groups have the required privileges.
- If any account passwords are stored with reversible encryption, an option is available in Mimikatz to return the password in clear text
- **What is LLMNR-Poisoning attack?**
  In LLMNR poisoning, a rogue device sends it’s own IP as a response to a query tricking the computer who sent the query to connect to the rogue device instead of the actual target it was trying to reach (assuming the device name was actually real). When the computer tries to login to the device (this can either happen automatically if signed into a domain or the user will be prompted to enter credentials if on a home network) the device will claim that the credentials were faulty but in the background it will store them to be used for other attacks. automated tool method. Responder
- **What is AS-REP-Roasting attack?**
  AS-REP Roasting is the technique that enables the attacker to retrieve password hashes for AD users whose account options have been set to "Do not require Kerberos pre-authentication". This option relies on the old Kerberos authentication

protocol, which allows authentication without a password. Once we obtain the hashes, we can try to crack it offline, and finally, if it is crackable, we got a password!

- **What is kerberosting attack?**
  Kerberoasting is a common AD attack to obtain AD tickets that helps with persistence. In order for this attack to work, an adversary must have access to SPN (Service Principal Name) accounts such as IIS User, MSSQL, etc. The Kerberoasting attack involves requesting a Ticket Granting Ticket (TGT) and Ticket Granting Service (TGS). This attack's end goal is to enable privilege escalation and lateral network movement
  -find an SPN account(s), and then we can send a request to get a TGS ticket.
  -Once we find the SPN user, we can send a single request to get a TGS ticket for the srv-user user using the -request-user argument.
  All standard domain users can request a copy of all service accounts along with their correlating password hashes, so we can ask a TGS for any SPN that is bound to a "user"
  account, extract the encrypted blob that was encrypted using the user's password and bruteforce it offline.
- **What is permission delegation attack?**
  Permission Delegation exploits are often referred to as ACL-based attacks. AD allows administrators to configure Access Control Entries (ACEs) that populates Discretionary Access Control Lists (DACLs), hence the name ACL-based attacks. Almost any AD object can be secured with ACEs, which then describe the allowed and denied permissions that any other AD object has against the target object. However, if these ACEs are misconfigured, it may be possible for an attacker to exploit them. Let's look at our example again. If the IT Support team were granted the ForceChangePassword ACE over the Domain Users group, this would be considered insecure. Sure they would be able to reset the passwords of employees that forgot their passwords, but this misconfiguration would allow them to also reset the passwords of privileged accounts, such as the accounts that are members of the Domain Admins group essentially allowing for privilege escalation
- **What is kerberos delegation attack & its types?**
  Types:

1. UnConstrained [unlimited delegate to services] : If we have Administrative access on a machine that has Unconstrained Delegation enabled, we can wait for a high value target or DA to connect to it, steal his TGT then ptt and impersonate him! , When set for a particular service account, unconstrained delegation allows delegation to any service to any resource on the domain as a user [TrustedForDelegation].

2. Constrained [limited delegate to services] : If you have compromised a user account or a computer (machine account) that has kerberos constrained delegation enabled, it's possible to impersonate any domain user (including administrator) and authenticate to a service that the user account is trusted to delegate to[TrustedToAuth -prop msds-allowedtodelegateto].
3. Resource-Based
   In unconstrained and constrained Kerberos delegation, a computer/user is told what resources it can delegate authentications to. In resource based Kerberos delegation, computers (resources) specify who they trust and who can delegate authentications to them, use account have Generic All or Generic Write or Write Property permission on the machine has delegation to configure msDS-AllowedToActOnBehalfOfOtherIdentity. Control over an object which has SPN configured and use the object account to create new fake machine and put password, get SID for the fake machine, add new property to the fake machine msds-allowedtoactonbehalfofotheridentity and fill it with SID, using rubeus to hash password and get TGS ticket for DA to impersonate.

- **What is automated-relays attack?**
  In AD, these machine accounts are used quite a bit in different services. Different domain controllers use their machine accounts to synchronise AD updates and changes. When you request a certificate on behalf of the host you are working on, the machine account of that host is used for authentication to the AD Certificate Service. There is an exceptional case in AD, where one machine has admin rights over another machine. Essentially in the AD configuration, administrative permissions over a host have been granted to another host. Again, this is expected functionality such as domain controllers or SQL clusters that must be synchronised. However, these instances provide a very interesting attack vector for coercing authentication
  in this attack must include: the Print Spooler service is running, do not have SMB signing enforced.
- **How to exploit AD-users?**
  • Credential Management - How users store their credentials. In AD, this is quite important since users may have multiple sets of credentials and remembering all of them can be a hassle.
  • Keylogging - Often, during exploitation, we need to understand how normal users interact with a system. Together with screengrabs, Keylogging can be a useful tool to gain this understanding from an attacker's perspective.
  Meterpreter has a built-in keylogger. This will be useful for extracting the user's

keystrokes. However, we can't just start this keylogger and hope for the best since our shell is currently running in the SYSTEM context. SYSTEM won't be typing any keystrokes, so this won't help us. To capture the correct user's credentials, we will need to ensure that our shell is running in the context of that user. you will find active session for user, dump captured keystrokes

`meterpreter\>keyscan_dump`

- **How to exploit GPOS?**
  through the GUI

1. We now want to add the Group Policy Management snap-in
2. We can right-click on the GPO and select Edit. This will open the new Group Policy Management Editor window
3. In order to add our account to the local groups
4. Add both the Administrators and Remote Desktop Users groups.

- **How to exploit certificates** #right_permissions **?**

1. find vulnerable templates , `C:\>certutil -Template -v > templates.txt`
2. Add the Certificates snap-in and make sure to select Computer Account and Local computer on the prompts
3. Request a personal certificate, Change the Alternative name Type option to User principal name. Supply the UPN of the user you want to impersonate. The best would be a DA account such as Administrator@domain and click Add.
4. Export our certificate with the private key.
5. Can finally impersonate a user. To perform this, two steps are required: Use the certificate to request a Kerberos ticket-granting ticket (TGT) , Load the Kerberos TGT into your hacking platform of choice

- **What are persistence techniques?**

1. DC Sync
2. Golden & Silver Tickets
3. Certificates
4. SID History #right_permissions
5. Group Membership
6. ACLs
7. GPOs

- **What is domain-trust?**
  A trust in Active Directory is a secure authentication communication between Domain and Forest. Trust enables you to grant access to the resource to users, groups, and computers across the different domains.
- **What are domain-trust types?**
  Some trust types:

1. Parent-child
2. Cross-link
3. Tree-root (intra-forest)
4. Forest
5. External (inter-forest)
   Enumeration about trust relationship with PS AD-Module:
   `Get-DomainTrust -API`

- **How to exploit Parent-child trust?**
  -Required to forge trust tickets is, obviously, the trust key. Look for [In] trust key from child to parent. Invoke-Mimikatz -Command '"lsadump::trust /patch"' -ComputerName dcorp-dc or Invoke-Mimikatz -Command '"lsadump::dcsync /user:dcorp\mcorp$"'
  -An inter-realm TGT can be forged
  -Get a TGS for a service (CIFS below) in the target domain by using the forged trust ticket.
  -Tickets for other services (like HOST and RPCSS for WMI, HOST and HTTP for PowerShell Remoting and WinRM) can be created as well.
  -Use the TGS to access the targeted service (may need to use it twice).
  -Using DA access to dollarcorp.moneycorp.local, escalate privileges to Enterprise Admin or DA to the parent domain, moneycorp.local using the domain trust key.
  -We will abuse SID history once again Invoke-Mimikatz -Command '"lsadump::lsa /patch"' Invoke-Mimikatz -Command '"kerberos::golden /user:Administrator /domain:dollarcorp.moneycorp.local /sid:S-1-5-21-1874506631-3219952063-538504511 /sids:S-1- 5-21-280534878-1496970234-700767426-519 /krbtgt:ff46a9d8bd66c6efd77603da26796f35 /ticket:C:\AD\Tools\krbtgt_tkt.kirbi"' • In the above command, the mimkatz option "/sids" is forcefully setting the SID History for the Enterprise Admin group for dollarcorp.moneycorp.local that is the Forest Enterprise Admin Group.
- **How to exploit Cross-Forest trust?**

-Require the trust key for the inter-forest trust. Invoke-Mimikatz -Command '"lsadump::trust /patch"'

-An inter-forest TGT can be forged

-Get a TGS for a service (CIFS below) in the target domain by using the forged trust ticket.

-Tickets for other services (like HOST and RPCSS for WMI, HOST and HTTP for PowerShell Remoting and WinRM) can be created as well.

-Use the TGS to access the targeted service.

- **How to Abuse ACLs?**

  -Resides in the System container of a domain and used to control the permissions - using an ACL - for certain built-in privileged groups (called Protected Groups) for AdminSDHolder.

  -It is possible to modify Security Descriptors (security information like Owner, primary group, DACL and SACL) of multiple remote access methods (securable objects) to allow access to non-admin users. Administrative privileges are required for this.

- **How to exploit MSSQL Servers trust?**

  Get a reverse shell on a SQL server in eurocorp forest by abusing database links from dcorp-mssql.

  -Discovery (SPN Scanning) Get-SQLInstanceDomain.

  -Check Accessibility Get-SQLConnectionTestThreaded.

  -Gather Information Get-SQLInstanceDomain | Get-SQLServerInfo -Verbose.

  -A database link allows a SQL Server to access external data sources like other SQL Servers and OLE DB data sources.

  -In case of database links between SQL servers, that is, linked SQL servers it is possible to execute stored procedures.

  -Look for links to remote servers Get-SQLServerLink -Instance dcorp-mssql -Verbose

  -Enumerating Database Links - Manually • Openquery() function can be used to run queries on a linked database select *from openquery("dcorp-sql1",'select* from master..sysservers')

  -Executing Commands • On the target server, either xp_cmdshell should be already enabled; or • If rpcout is enabled (disabled by default), xp_cmdshell can be enabled using: EXECUTE('sp_configure "xp_cmdshell",1;reconfigure;') AT "eu-sql"

  -From the initial SQL server, OS commands can be executed using nested link queries: select *from openquery("dcorp-sql1",'select* from openquery("dcorp□mgmt","select * from openquery("eu-sql",""select @@version as version;exec master..xp_cmdshell "powershell whoami)"")")')

- **How to detect AD attacks?**
  -Never run a service with a DA
  -Check out Temporary Group Membership! (Requires Privileged Access Management Feature to be enabled which can't be turned off later)
  -Check Events (account/admin login) / creation or change
- **How to defend against AD attacks?**
  -Running lsass.exe as a protected process is really handy as it forces an attacker to load a kernel mode driver
  -Service Account Passwords should be hard to guess
  -Limit DA/Admin logins to specific servers
  -Use Managed Service Accounts (Automatic change of password periodically and delegated SPN Management)
  -Set "Account is sensitive and cannot be delegated" for privileged accounts.
  -AD ACL Scanner - Create and compare create reports of ACLs.
  -SID Filtering
  -In an inter-forest trust, if Selective Authentication is configured, users between the trusts will not be automatically authenticated. Individual access to domains and servers in the trusting domain/forest should be given
  -Microsoft ATA (Advanced Threat Analytics).
  -Credential Guard Now called, Windows Defender Credential Guard, it "uses virtualization□based security to isolate secrets so that only privileges system software can access them".
  -Effective in stopping PTH and Over-PTH attacks by restricting access to NTLM hashes and TGTs. As of Windows 10 1709, it is not possible to write Kerberos tickets to memory even if we have credentials
  -Protected Users Group
- **How to Abuse GPO without GUI?**
  -Once you have permission, overwrite GPO Permissions.
- **What is your strategy in Lateral movement and pivoting?**
  -If we could leak any hashes,keys and tickets we can do PTH,PTT,PTK attacks.
  -Pivoting with socat.
- **What is LAPS?**
  -A Windows OS has a built-in Administrator account which can be accessed using a password. Changing passwords in a large Windows environment with many computers is challenging.
  -find which AD organizational unit (OU) has the "All extended rights" attribute that deals with LAPS. We will be using the "Find-AdmPwdExtendedRights" cmdlet to

provide the right OU. Note that getting the available OUs could be done in the enumeration step, You can use the -Identity * argument to list all available OUs. Find-AdmPwdExtendedRights -Identity THMorg

- **What is AMSI & How to bypass?**
  -That's when Microsoft introduce AMSI with the release of Windows 10. At a high level, think of AMSI like a bridge which connects powershell to the antivirus software, every command or script we run inside powershell is fetched by AMSI and sent to installed antivirus software for inspection.
  -PowerShell Downgrade | powershell -version 2
  -Base64 Encoding
  -obfuscation | "Invo"+"ke-Mimikatz" .. there's no way for the AV to tell if it's malicious.
- **What is dc replication?**
  the process by which the changes that originate on one domain controller are automatically transferred to other domain controllers that store the same data.
- **What can you dump from kerberosting?**
  tickets that lead to pass-the-ticket attack
- **IF you got hash from LLMNR can you use it on PTH attack?**
  No, because its from ticket not pure hash
- **What can you dump form LSSAS memory?**
  users credentials
- **What are restricted groups in GPO?**
  Restricted Groups is **a client configuration means, and can't be used with domain groups**. Restricted Groups is designed specifically to work with local groups. Domain objects must be managed within traditional AD tools.
- **What is the diff between security group and other groups in GPO?**
  Distribution groups are simpler in that they would be used if only one-way notifications are required from the central controller. **Security groups are more complex, and they are applied when you want to enable users to access and modify data**.
- **Which permission will you enumerate on users?**
  -**GenericAll** - full rights to the object (add users to a group or reset user's password)
  -**GenericWrite** - update object's attributes (i.e logon script)
  -**WriteOwner** - change object owner to attacker controlled user take over the object
  -**WriteDACL** - modify object's ACEs and give attacker full control right over the object
  -**AllExtendedRights** - ability to add user to a group or reset password

-**ForceChangePassword** - ability to change user's password
-**Self (Self-Membership)** - ability to add yourself to a group

- **What will u do if u found Generic write permission on user?**
  i'll force SPN on the account to launch kerberoasting attack.
- **What is the difference between OU and group?**
  The difference between an OU and a group is that **OUs can contain different kinds of objects rather than being limited to accounts or groups, whereas groups can only contain accounts and other groups**.
- **What are ACLs & its types & ACE?**
  An ACL is a ordered list of classification rules and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). An ACL must have at least one ACE. Each ACE is made up of filters that determine traffic classifications and associated actions.
  DACL: A list of the users and groups allowed or denied access and the degree of access they have to the securable object. This list is called the discretionary access control list (DACL).
  SACL: A list that contains the types of access attempts that are to be audited. This list is called the system access control list (SACL).
  `Using ACL you can add FullControl rights / add rights for DCSync / Abusing Reset Pass`
- **What are protected groups?**
  it's group that contain high privileged accounts like DA,EA,DC
- **What is GPO filtering & How to do it?**
  Security filtering: an AD functionality that allows you to specify the users or computers to which you want a particular GPO to be applied.
  WMI filtering: allows administrators to target specific computers based on filters that are provided to them, and then apply GPOs to the targeted computers
- **What is GPP?**
  Group Policy Preferences (GPP) allow you to specify computer and user configuration settings. These settings allow granular configuration not available using regular Group Policy.
- **What is the diff between PTH & Over-PTH/Pass-the-Key attack?**
  Over-PTH similar to PTH but applied to Kerberos networks and passes the available key with different type[rc4-aes128-aes256].
- **What is the background details behind PTH attack?**

Microsoft's NTLM security mechanisms ensure that only authorized users may access protected resources while keeping all communications between those users private. To confirm the user's identity without requesting a password, NTLM uses a challenge-response protocol, making it possible for users to log in with just their network name and a challenge answer.

Several flaws in the way NTLM handled password hashing and salting are well-documented. When using NTLM, the password is not "salted," meaning that an additional random string of characters is not added to the hashed password to make it more secure. This means that attackers can authenticate a session with just the password hash, rather than the actual password.

- **What is Diamond ticket?**
  A **diamond ticket** is made by **modifying the fields of a legitimate TGT that was issued by a DC**. This is achieved by **requesting** a **TGT**, **decrypting** it with the domain's krbtgt hash, **modifying** the desired fields of the ticket, then **re-encrypting it**
- **What is the difference between Domain Admin & Enterprise Admin?**
  The enterprise admin has more authority than domain admins.. and has rights across the entire forest. An enterprise admin has full control over the entire forest and can do anything that would affect multiple domains, like linking group policies to a site that can span domain boundaries.
- **What is Zero Logon Attack?**
  This vulnerability allows a hacker to take control of a domain controller (DC), including the root DC. This is done by changing or removing the password for a service account on the controller. The hacker can then simply cause a denial of service or take over and own the entire network.
  Once the attacker successfully authenticates with the all-zero credential, they can make MS-NRPC calls. Specifically, a call can be sent to set the client machine’s password to a new value. Now, this call requires encryption of the new password using the session key once again.
  However, as we have already used this session key to authenticate with all zeroes, we know that we can also send a password parameter of all zeroes. The last byte of the password parameters specifies the password length. As this will be set to zero, the password will be set to a blank value.
  At this point, an attacker can authenticate as this machine normally, using a blank password. With knowledge of the new password, the attacker can now perform any

actions the computer could normally perform in the domain.
The common attack pattern is as follows:

1. Use the ZeroLogon attack to authenticate as a domain controller to a domain controller
2. Set the domain controller's machine password to blank
3. Authenticate properly with the domain controller's account
4. Perform a DCSync attack to extract password hashes from Active Directory
5. (optional) Set the domain controller's machine password back to its original value to prevent obvious issues and cover the attacker's tracks

- **What is Skeleton Key?**
  The Skeleton Key attack is malware that can be injected into the LSASS process on a Domain Controller and creates a master password that will hijack [sic] any authentication request on the domain and allow an attacker to log in as any user on any system on the domain with the same password
- **What is DSRM?**
  DSRM is Directory Services Restore Mode. There is a local administrator on every DC called "Administrator" whose password is the DSRM password. DSRM password (SafeBackUpPassword) is required when a server is promoted to Domain Controller and it is rarely changed. After altering the configuration on the DC, it is possible to pass the NTLM hash of this user to access the DC. Since it is the local administrator of the DC, we can pass the hash to authenticate.
- **What is Custom SSP?**
  A Security Support Provider (SSP) is a DLL which provides ways for an application to obtain an authenticated connection. Some SSP Packages by Microsoft are – NTLM – Kerberos – Wdigest – CredSSP. Mimikatz provides a custom SSP - mimilib.dll. This SSP logs local logons, service account and machine account passwords in clear text on the target server. All local logons on the DC are logged to C:\Windows\system32\kiwissp.log.
- **What is DNSAdmins?**
  It is possible for the members of the DNSAdmins group to load arbitrary DLL with the privileges of dns.exe (SYSTEM). In case the DC also serves as DNS, this will provide us escalation to DA. Need privileges to restart the DNS service. Once we know the members of the DNSAdmins group, we need to compromise a member. We already have hash of srvadmin because of derivative local admin.

- ##### What If you have permissions like GenericAll/GenericWrite?

we can set a SPN on a target account, request a TGS

if current user has already an SPN setted

Get-ADUser -Identity -Properties ServicePrincipalName | select ServicePrincipalName

#Force set the SPN on the account:

Set-ADUser -Identiny -ServicePrincipalNames @{Add='ops/whatever1'}