ManageEngine
ADAudit Plus

Disrupting the cybersecurity kill chain:

Detecting domain reconnaissance

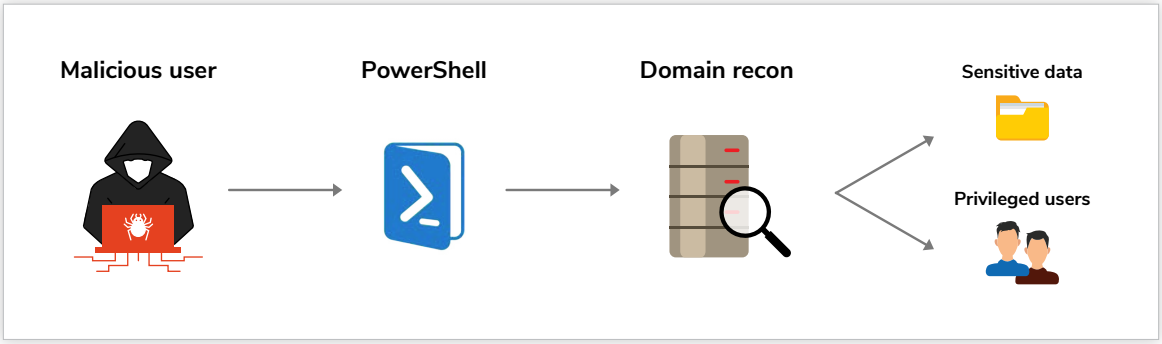
What is Lightweight Directory Access Protocol (LDAP) reconnaissance?

When an attacker manages to break into an on-premises domain environment or a domain user turns rogue, their first step is to perform reconnaissance and gather as much information as possible. With critical information such as members of administrator groups, a list of accounts with service principal names (SPNs), etc., you can start to see why LDAP queries are a potential gold mine for malicious actors to perform targeted attacks.

Why LDAP?

- LDAP is better suited to perform enumerations that return more data.
- Most client systems come with Remote Server Administration Tools (RSAT) installed; using the **saved queries** option within the Active Directory Users and Computers (ADUC) tool can help construct complex LDAP queries with ease.
- LDAP is heavily used by system services and apps for many important operations like querying for user groups and getting user information.

The LDAP recon cycle



To simulate an LDAP recon attack, all we need is a standard user account and a shell. Let's look at a few examples to see why they can be dangerous.

Note: These commands are being run as a standard user—**one with no special rights or privileges.**

Example 1: Enumerating administrators in the domain.

```
PS C:\Users\James> Get-ADUser -LDAPFilter '(objectClass=user)(objectCategory=Person)(adminCount=1)'
```

This LDAP query would search and display all administrators in domain admins and enterprise admins groups. Let's pair the usernames with a classic password spray attack.

```
[*] Password spraying has begun with  1  passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Password@123 against 53 users. Current time is 5:57 PM
[*] Writing successes to
[*] SUCCESS! User:Jery Password:Password@123
[*] SUCCESS! User:George Password:Password@123
[*] SUCCESS! User:Gabriel Password:Password@123
[*] SUCCESS! User:Pete Password:Password@123
[*] SUCCESS! User:Emergencyadmin Password:Password@123
[*] SUCCESS! User:backdoor1 Password:Password@123
[*] Password spraying is complete
PS C:\Users\Administrator\desktop>
```

It's that simple!

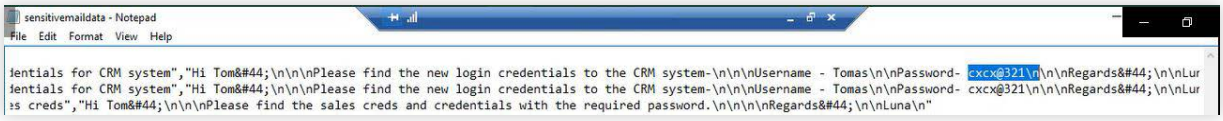
Example 2: Finding Exchange servers in the domain.

This LDAP query flushes out information on every Exchange server in the domain.

```
PS C:\Users\James> Get-ADComputer -LDAPFilter '(objectCategory=computer)(servicePrincipalName=exchangeMDB*)(operatingSys
tem=Windows Server*)'


DistinguishedName : CN=ADSolutions,OU=Domain Controllers,DC=test,DC=com
DNSHostName       : ADSolutions.test.com
Enabled           : True
Name              : ADSolutions
ObjectClass       : computer
ObjectGUID        : 5f318c43-a5e1-4d19-bb8d-1a49c4033659
SamAccountName    : ADSolutions
SID               : S-1-5-21-180837044-459910765-454564048-1001
```

Why Exchange? Let's use PowerShell and attack the Outlook Web Access (OWA) portal of the Exchange server, and gain an in-depth view of the emails being sent within the organization.



Credentials for a CRM system? Looks like we're off to a good start!

Example 3: Not just PowerShell; the command line can also be used to perform reconnaissance.

Let's run a simple query to obtain the Distinguished Names (DNs) of all the domain controllers in the forest.

```
C:\Users\James>dsquery server
"CN=ADSolutions,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com"
```

Now, let's leverage the obtained information to identify accounts with stale user passwords.

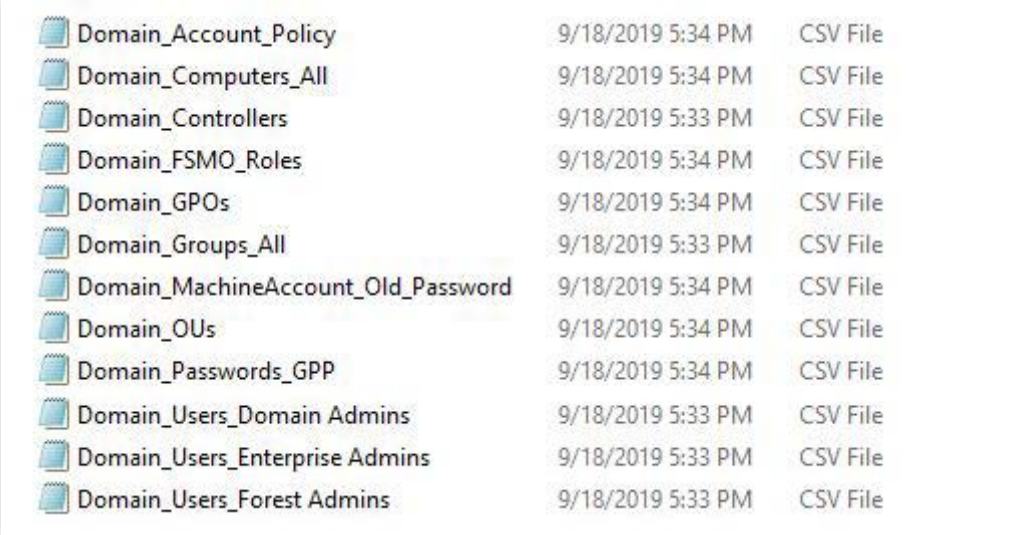
```
C:\Users\James>dsquery user "dc=Child,dc=test,DC=com" -stalepwd 60
"CN=admin,OU=server_OU,DC=child,DC=test,DC=com"
"CN=Administrator,CN=Users,DC=child,DC=test,DC=com"
"CN=Guest,CN=Users,DC=child,DC=test,DC=com"
```

Or, you can run a **set-spn** command.

```
C:\Users\James>setspn -L ADSolutions
Registered ServicePrincipalNames for CN=ADSolutions,OU=Domain Controllers,DC=child,DC=test,DC=com
:       MSSQLSvc/ADSolutions.child.test.com:57017
        MSSQLSvc/ADSolutions.child.test.com:VEEAMSQL2012
```

With the set-spn command, we can now discover accounts with Service Principal Names (SPNs), which is the first step for attacks like Kerberoasting that cater to exploiting service accounts.

Much of the tedious work in cybercrime hacking is being automated, making it much easier to accomplish.There are free tools that can run multiple LDAP queries and instantly export the results into a CSV file, with just a single command.This can help enhance the reconnaissance and discovery process. Here's an example:



These CSV files can be uploaded into open-source applications that can be used to find identify different attack paths within Active Directory (AD), which can help attackers draw and plan their moves laterally in a domain.

Detecting LDAP recon attempts in Active Directory

Advanced audit policies must be configured to enable LDAP auditing and to retrieve LDAP queries.

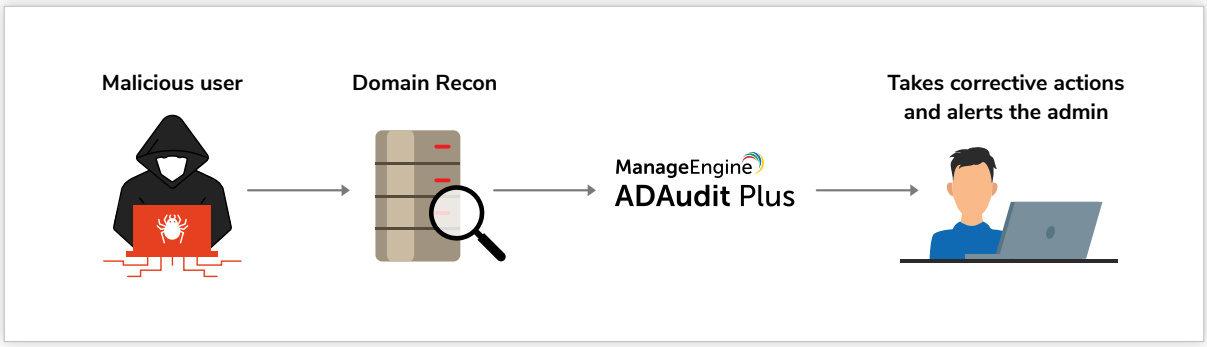
Enabling LDAP auditing:

- To check if the advanced audit policies are already enabled, use the command prompt to execute **auditpol/get/category:*** with admin privileges on the LDAP server. This will list all the available audit policy settings.
    - Within the **Advanced Audit Policies** Group Policy Object (GPO), ensure that **Directory Service access** and **Directory Service Changes** are set to **Success.**
    - Setting audit policies will not immediately trigger the LDAP audit logs; there must be changes made within the registry, too. The **Field Engineering** and **LDAP Interface Events** keys in the registry **(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics)** must be set to value 5.

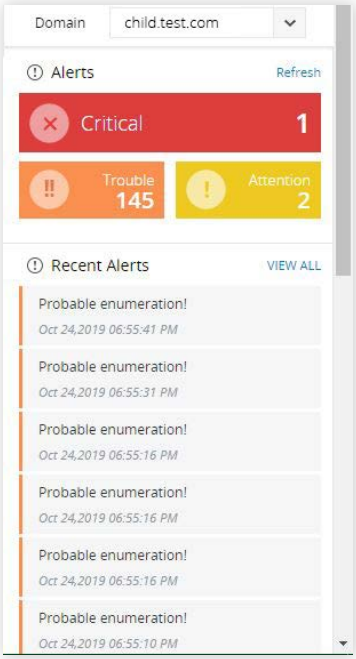
Detecting malicious LDAP queries with native tools:

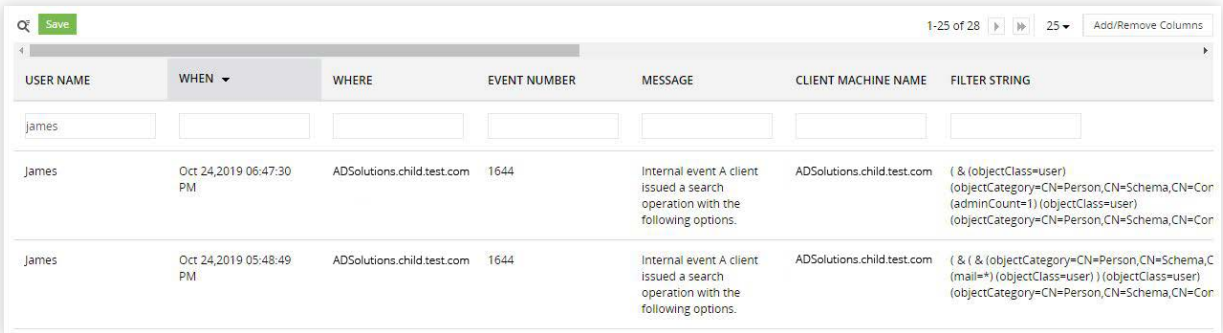
Native methods	Difficulties
The generated logs can be checked within the event viewer, in the **Applications and Services Logs > Directory Service.**	These are diagnostic logs and are disabled by default. Setting a value as high as 5 on the registry key will generate a large volume of logs, increasing the load on the server.
Event ID 1644 in the Directory Service Logs can be checked for malicious LDAP enumeration attempts.	Users may run LDAP queries for legitimate enumeration reasons, applications may query LDAP for listing usernames, and combing through every diagnostic event is cumbersome. There's no way to segregate malicious LDAP attempts from regular ones.

Detecting LDAP recon attempts with ADAudit Plus:



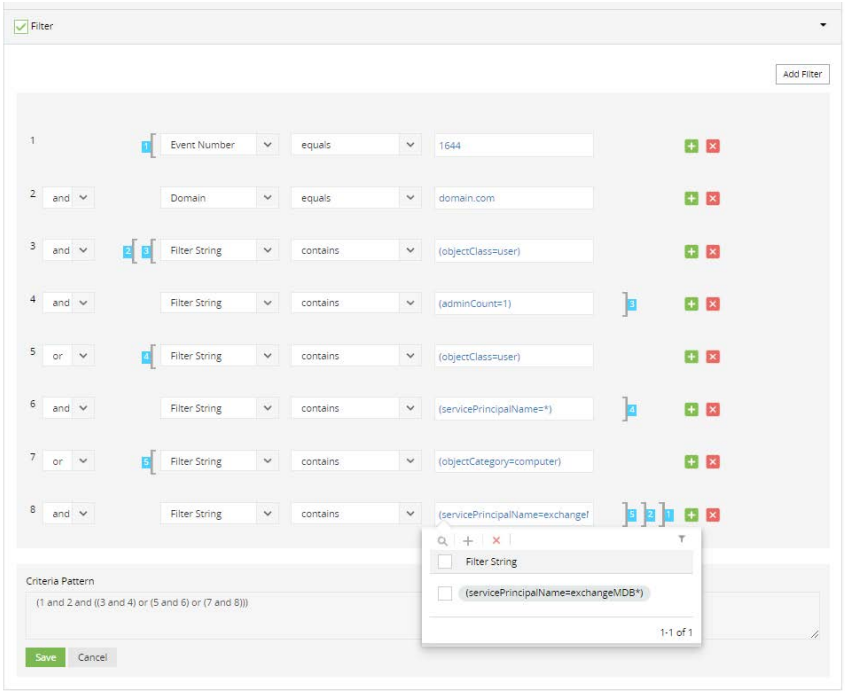
With advanced auditing enabled, ADAudit Plus can check both PowerShell and the command line to provide a summary of activities that generated the threat in real time, and instantly alert the administrator during a potential recon attempt.





ADAudit Plus can provide evidence of the exact query that was executed, the user executing the query, the attributes involved, and the number of entries returned.

Custom keyword-based filters can be configured to target specific enumeration activities, and instant remedial measures can be set up in the unfortunate event of a recon attempt.



The screenshot above shows the rules that need to be configured in ADAudit Plus to detect the 3 ways of LDAP recon by enumerating administrators, finding Exchange servers, and discovering accounts with Service Principal Names.

To configure these rules, Log in to ADAudit Plus > Navigate to **Alerts > New Alert Profile** > Enter a suitable **Name, Description, Severity,** and Alert message > Click + under **Category** and choose **LDAP Auditing** > Tap the **Filter** tick box > **Add Filter** > Enter the rules as shown in the above screenshot > Click **Save.**