🧺 AD Information Gathering

Intro

To know what we are going to do in an AD environment The first thing that we should ask ourselves is, What are we interested in doing in an active directory environment? If we have access to a domain, with a user or in the internal network without use, the goal is to **get the credentials of a Domain Admin User**. If we get credentials of a Domain Admin User we *can do everything in the domain*: *Delete or create new users*, *delete or create shares*… We will have compromised the entire domain.

To get those credentials we can enumerate different types of information that will give us clues and also will let us know if we can use *some hacking techniques* or note.

🧺 Information gathering

What kind of information will we gather? Information like:

- **Local Users and Local Accounts** 👦
- **Local Groups** 👫
- **Domain Users and Domain Accounts** 🤵
- **Doman equipment** 🖥️🖨️💻
- **Domain Groups** 👪
- **Organizational Unions (OUs)** 👥
- **Group Policy Objects (GPOs)** 👮
- **Access Control Lists (ACLs)** 📝
- **Trust relationships between forest and domain** 🌳 ✊
- **Attributes of domain objects** 🧱
- **…**

When we talk about *Information Gathering* on windows environment or AD we have to differentiate two types of *Information Gathering* : **Local And Remote**

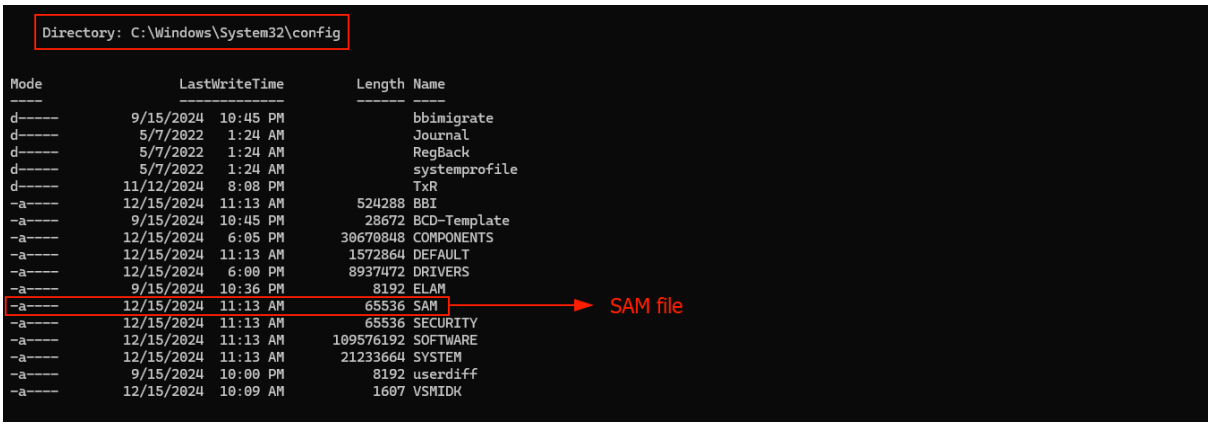
🚮 Local Information Gathering

This form of information collection will correspond to the collection of information about the machine itself, whether it has been given to us for audit or we have compromised it, the fist step that we must do is gather the information on that machine. Information like **Local Users and Local Accounts** 👦**, Local Groups , etc.**

To do that we are going to resort to a database that exists in every Windows OS called **SAM (Security Account Manager)**. SAM contains whole information about users, groups, and passwords… of the *Local System*.

This is important to know, because in an AD environment, when we create a user on the domain will authenticate, the user and password will be in the file **ntds.dit** . But, in local authentication these information will be in the file **SAM.**

SAM file is located on the route **C:\Windows\System32\config\SAM** and can be enumerated in **local** form as **remote,** which means we can enumerate the **SAM** *of a remote computer.*



To enumerate **SAM** on a local machine we going to need

Note: Starting with Windows 10 and Windows Server 2016, only the ***system administrator*** *user can enumerate the SAM*. In the previous version, *any* ***domain user*** *could enumerate the* ***SAM*** file.

🔭 Remote Information Gathering

This is the other way to gather information, and we will be more interested, because *we won't need high administrator privileges,* as we saw in Local information gathering.

🔭 **Remote Information Gathering** is about gather or enumerate information of **NTDS.dit** file. That file stores all the domain information, **users, passwords, groups, OUs, …** all.

If we can enumerate that file it will give us many clues about which user has ***Administrator Privileges***, What ***group a*** user belongs to, what privileges does that user have in that group… etc.

We can interact with that **ntds.dit** file through **LDAP protocol**, but who can interact with that database and what information can be obtained? That's the magic of Remote information Gathering in an AD environment.

Using **LDAP protocol (Lightweight Directory Access Protocol)**

LDAP (Lightweight Directory Access Protocol) is an application protocol that allows a user to interact with directory services (as AD) to store, read or modify information.

Through this protocol any domain user, *regardless of his privileges*, can **consult** that **NTDS.dit** database. Of course, not everyone will have the same access. A domain administrator user can modify that database, but a random user cannot. But we can consult a lot of information about the domain **user, groups, user attributes, etc.**

So, what we are going to be interested in is through **LDAP protocol,** make requests to the domain controller, where NTDS.dit database is stored to enumerate information that could be useful to ***the vulnerable analysis phase*** and ***exploitation phase.***

Note: is ***impossible*** to configure LDAP Protocol so that common domain users cannot enumerate and make requests to this **NTDS.dit** database.

Note II: To do all enumeration techniques using **Kali** 🐉we must have to do the **AD Initial Configuration.**