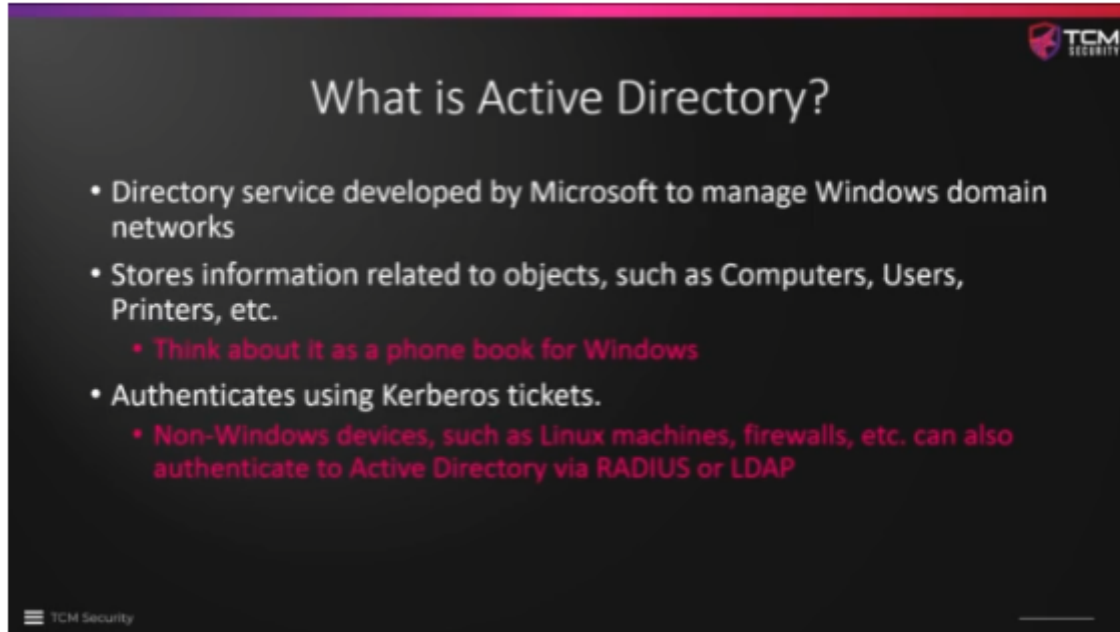


# Active Directory - Overview

---

Active Directory is most likely to be involve in internal penetration test assessments. It is like a phone book for windows.



**What is Active Directory?**

- Directory service developed by Microsoft to manage Windows domain networks
- Stores information related to objects, such as Computers, Users, Printers, etc.
  - Think about it as a phone book for Windows
- Authenticates using Kerberos tickets.
  - Non-Windows devices, such as Linux machines, firewalls, etc. can also authenticate to Active Directory via RADIUS or LDAP

TCM Security

It is a tool that is used to manage a network of computers that belongs and are connected to the Active Directory Domain. Although is a windows feature, Linux machines, firewalls, and other devices can also authenticate to AD via RADIUS or LDAP.



**Why Active Directory?**

- Active Directory is the **most commonly used** identity management service in the world
  - 95% of Fortune 1000 companies implement the service in their networks (<https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Success-with-Enterprise-Mobility-Identity/bap/248613>)
- Can be exploited **without ever attacking** patchable exploits.
  - Instead, we abuse features, trusts, components, and more.

TCM Security