ENUMERATION

Active Directory

Prerequisites

- **Low privileged** access/foothold to a domain workstation.
- Interactive shell as a domain user

User and Service Enumeration

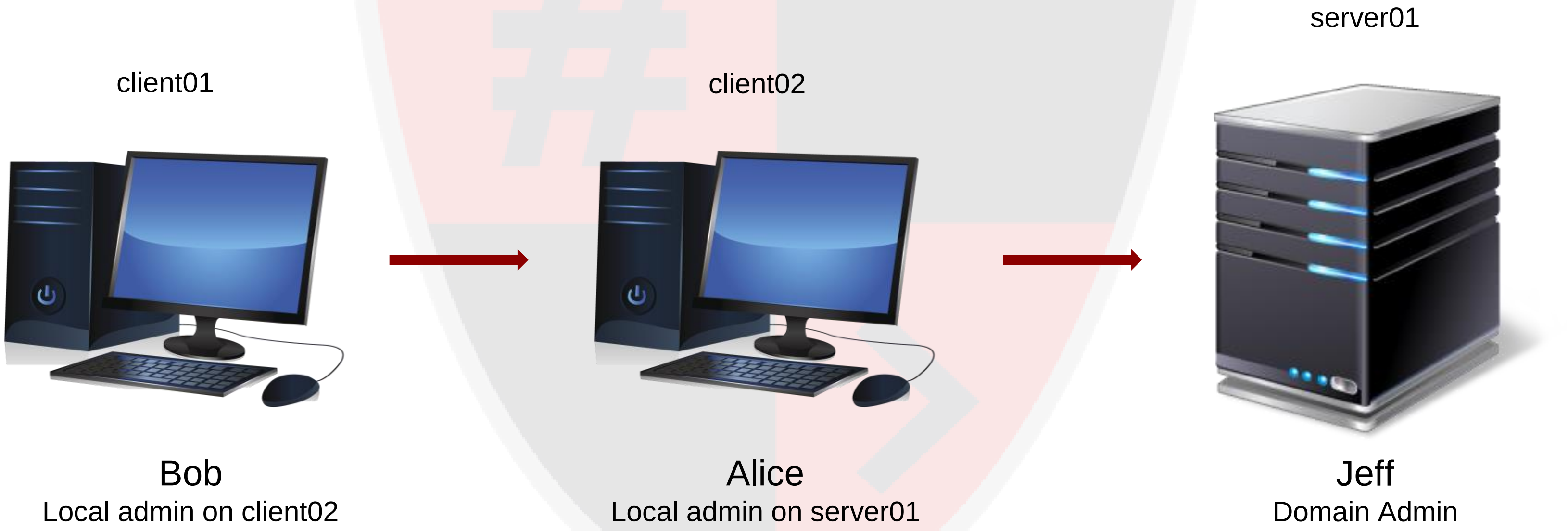
Service Enumeration

- Each service is ran when an application is executed in context of an operating system user, services launched by the system run under Service Accounts.
- Complex applications are run under an active domain user account
- Service Principal Name (SPN) is a unique service instance identifier that is used to associate a service to a service account in the AD.
- We can query all domain accounts and know which account has a valid SPN which can be a potential target for service attacks.
- Example services: SQL, Exchange, IIS

User Enumeration

- Target is to generate an enumeration map on the target
- We find the domain users first and move on to find currently logged in users on the compromised machine
- These users can be enumerated further to obtain info like high value domain groups, SPNs, ACLs, etc.
- Compromising these users can allow us to move laterally and compromise more domain machines

User Enumeration



client01

Bob
Local admin on client02

client02

Alice
Local admin on server01

server01

Jeff
Domain Admin

User and Service Enumeration

- Tools Used
  - Powershell (PowerView)
  - Bloodhound
  - Command Prompt