What is a Service Principal Name?

A Service Principal Name (SPN) is a unique identifier in Active Directory that maps a running service, such as a SQL database or web service, to the account that runs it. Kerberos needs the SPN to issue a service ticket (TGS) encrypted with that account's password hash. The catch is that any authenticated user can request a service ticket for any SPN, so any account with an SPN can be Kerberoasted: the attacker pulls the ticket and cracks the service account's password offline. SPNs are necessary for Kerberos to work, which is why the defence is strong service-account passwords, not removing SPNs.

HOW IT WORKS

01 Why attackers target SPNs

Requesting a service ticket is an ordinary, allowed action, so any single authenticated user can ask for a ticket for any SPN. Part of that ticket is encrypted with the service account's hash, often with weak RC4.

That is Kerberoasting: the attacker collects tickets for SPN accounts and cracks the passwords offline, with no failed logons and no privileges required. Service accounts with old, human-chosen passwords, especially ones that also sit in privileged groups, fall quickly and hand the attacker real access.

There is also targeted Kerberoasting: an attacker with GenericWrite over an account writes a fake SPN onto it, then Kerberoasts the account they just made roastable.

02 How the attack runs

Listing and roasting SPN accounts is well-documented:

- Find SPN accounts and request tickets: `GetUserSPNs.py corp.local/user -request` (Impacket)
- Or from a domain-joined host: `Rubeus.exe kerberoast`
- Crack the captured ticket offline: `hashcat -m 13100 hashes.txt wordlist.txt`

HOW TO DEFEND

- Use Group Managed Service Accounts (gMSAs) so Windows sets a long, random, auto-rotating password no attacker can crack.
- Give remaining service accounts a 25-plus character passphrase.
- Keep service accounts out of privileged groups so a cracked one is not also an admin.
- Disable RC4 for Kerberos where possible to force the stronger AES.
- Restrict GenericWrite on accounts to block targeted Kerberoasting.
- Monitor for one account requesting many service tickets quickly.

SOURCES

[1] Microsoft: Kerberos Authentication Overview

[2] MITRE ATT&CK Enterprise Matrix

[3] NIST SP 800-115 Technical Guide to Security Testing

If the service-account password is guessable, it falls, and a privileged service account hands the attacker its access. These are published techniques included so defenders know what to watch for.

> DEFENDER QUICK WIN
>
> *List every account that has an SPN and check its password age and group membership. A kerberoastable account that sits in a privileged group with an old password is a direct escalation path. Move it to a Group Managed Service Account.*

Test your Active Directory before an attacker does.
securelayer7.net/learn/active-directory/what-is-an-spn

Open online