Service Principal Name (SPN) Discovery

Why are SPNs Important

Services that support Kerberos authentication require a Service Principal Name associated to point users to the appropriate resources for connection. SPNs are discovered via LDAP queries and assists in the identification of hosts that run high value services like SQL databases, Exchange servers, etc.

SPN discovery is the first step in carrying out a kerberoast attack. 1

SPN Discovery Tools

SetSPN

SetSPN is a native windows binary which can be used to retrieve the mapping between user accounts and services. This utility can add, delete or view SPN registrations.

Services that bind to a domain user account, not a local account, are more likely to be configured with a weak password because the user set the password instead of the administrator. So, services that have their **Canonical-Name** assigned to **Users** are potential targets for kerberoasting. 1

Ex. `setspn -T pentestlab -Q */*`

GetUserSPNs.py

GetUserSPNs.py is a tool in the Impacket collection which directly queries a domain controller for SPNs running under a domain user account. Requires user credentials.

Ex. `sudo GetUserSPNs.py LIFELINE.local/mmeow:Password1 -dc-ip 10.0.2.7 -request > GetUserSPNs.out`

How SPNs Enable Kerberoasting

The main security issue surrounding the use of Service Principle Name (SPN) accounts is the fact that any valid user on the domain can abuse the Kerberos authentication protocol to begin the authentication process and receive a hash of any SPN accounts in use. This action can be performed by any user on the domain and does not require any elevated privileges. Most often, the accounts set up with a Service Principle Name (SPN) are service accounts or other accounts with elevated privileges on the domain.

Once an SPN account's user hash has been captured, it can be taken offline and potentially cracked by the attacker. If the password cracking process is a success, then the attacker has the ability to log in as that SPN account and will have all privileges of that user. 2

To successfully perform this attack, the attacker would only need the following:

- Any user account on the domain. This can be achieved through social engineering, network poisoning attacks, or various exploits.

- A tool capable of querying the SPN user accounts and their hash. There are many tools that can be downloaded to perform this type of attack. Some of the more popular are Rubeus, Impacket Toolkit, and the Invoke-Kerberoast PowerShell module. Each of these tools is freely available online and has many guides written about performing this particular attack.
- The last requirement is for the attacker to have the ability to crack the SPN's password hash. The success of this step will depend on the strength of the password in use and the capabilities of the attacker.

Resources

1. https://pentestlab.blog/2018/06/04/spn-discovery/
2. https://sbscyber.com/blog/kerberoasting-the-potential-dangers-of-spn-accounts