Windows DSQuery & LDAP

C H E A T S H E E T

DSQuery

Important Options:

`-s`	Specify the target domain controller
`-u`	Specify a domain user ID
`-p`	Specify password
`-limit`	Override default 100 item limit (Use '`-limit 0`' for '`no limit`')

LDAP Query Format

Prefix notation:

(`&(objectClass=User)(objectCategory=Person)`)
is equivalent to (`objectClass=User`)
AND (`objectCategory=Person`)

Bitwise LDAP Rule OIDs:

`Logical AND: 1.2.840.113556.1.4.803`

`Logical OR: 1.2.840.113556.1.4.804`

Using DSQuery –filter:

```
Dsquery * -filter "<your filter here>"
```

Double quotes are mandatory, single quotes fail silently

User Account Control bit Values

1	Logon Script Will Execute
2	Account Is Disabled
32	Password Not Required
512	Normal User Account
2048	Interdomain Trust Account
4096	Domain Workstation or Member Server
8192	Domain Controller
65536	Password Does Not Expire
524288	Trusted For Impersonation
1048576	Account May Not Be Impersonated

Examples:

Find all enabled users whose passwords do not expire:

```
Dsquery * -filter "(&(objectClass=User)(objectCategory=Person)
(userAccountControl:1.2.840.113556.1.4.803:=65536)
(!(userAccountControl:1.2.840.113556.1.4.803:=2)))" –limit 0 –attr sAMAccountName
```

Examine all attributes available on a User object for your domain:

```
Dsquery * -filter "(&(objectClass=User)(objectCategory=Person))" –limit 1 –attr *
```

Find all domain computers:

```
Dsquery * -filter "(objectCategory=Computer)" –limit 0 –attr sAMAccountName
```

Find all Domain Controllers:

```
Dsquery * -filter "(&(objectCategory=computer)
(userAccountControl:1.2.840.113556.1.4.803:=8192))" –limit 0 –attr sAMAccountName
```

Windows DSQuery & LDAP

C H E A T S H E E T

DSQuery

Important Options:

`-s`	Specify the target domain controller
`-u`	Specify a domain user ID
`-p`	Specify password
`-limit`	Override default 100 item limit (Use '`-limit 0`' for '`no limit`')

LDAP Query Format

Prefix notation:

(`&(objectClass=User)(objectCategory=Person)`)
is equivalent to (`objectClass=User`)
AND (`objectCategory=Person`)

Bitwise LDAP Rule OIDs:

`Logical AND: 1.2.840.113556.1.4.803`

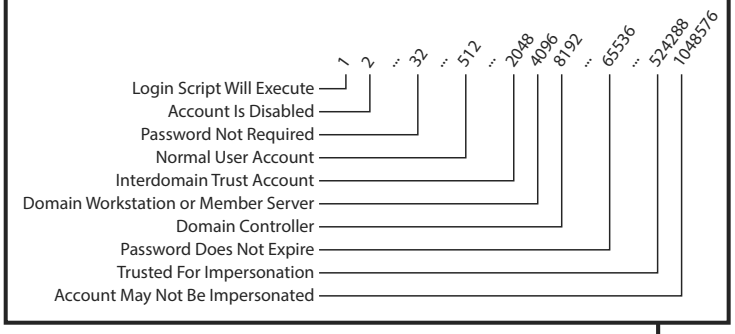
`Logical OR: 1.2.840.113556.1.4.804`

Using DSQuery –filter:

```
Dsquery * -filter "<your filter here>"
```

Double quotes are mandatory, single quotes fail silently

UserAccount Control bit Values



Examples:

Find all enabled users whose passwords do not expire:

```
Dsquery * -filter "(&(objectClass=User)(objectCategory=Person)
(userAccountControl:1.2.840.113556.1.4.803:=65536)
(!(userAccountControl:1.2.840.113556.1.4.803:=2)))" –limit 0 –attr sAMAccountName
```

Examine all attributes available on a User object for your domain:

```
Dsquery * -filter "(&(objectClass=User)(objectCategory=Person))" –limit 1 –attr *
```

Find all domain computers:

```
Dsquery * -filter "(objectCategory=Computer)" –limit 0 –attr sAMAccountName
```

Find all Domain Controllers:

```
Dsquery * -filter "(&(objectCategory=computer)
(userAccountControl:1.2.840.113556.1.4.803:=8192))" –limit 0 –attr sAMAccountName
```