ACTIVE DIRECTORY CHEAT SHEET

It's Not Just for Auditors

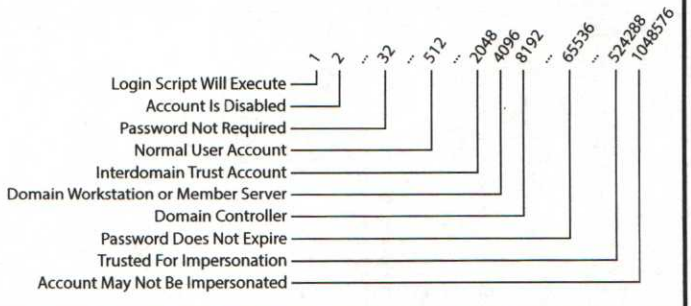
If you think this sheet looks useful, you need to experience the SANS Advanced Auditing and Monitoring course that it comes from. During this six-day hands-on course, we dive deep into security process and settings while using a risk-based approach to connect to the things that matter most for your business and to your management team. Not only will you learn to apply technical security controls in an enterprise context but you will also learn how to automate these important systems to create continuous monitoring systems that matter!

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`')

UserAccount Control bit Values



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

Convert Windows LDAP Timestamps in Excel

Content:

```
=IF(C2>0,C2/(8.64*10^11) - 109205,"")
```

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
```