Microsoft Active Directory Audit Techniques

Clay Risenhoover
ISACA North Texas
April 14, 2016
http://tinyurl.com/ISACAClay

RCI

Goals

Lots of hands-on
Common audit tasks
Expand your imagination
No PowerShell

RCI

Assumptions

The ideal student:

- Audits Windows systems
- Secures Windows systems
- Is not a PowerShell programmer
- Needs to automate tests

WMI / WMIC

- Windows management instrumentation (console)
- Allows management and querying of Windows features
- Can be run against local or remote machines
- Seems it will never die

WMIC – Data Sources (1)

Can list information about:

- Baseboard (motherboard)
- BIOS
- CPU
- DCOM applications
- Disk drives

WMIC – Data Sources (2)

Can list information about:

- Disk quotas
- Local groups
- Scheduled jobs
- Logical disks
- Memory chips

WMIC – Data Sources (3)

Can list information about:

- Network client
- Network cards
- Operating system
- Pagefile / virtual memory
- Printers

WMIC – Data Sources (4)

Can list information about:

- Processes
- Installed software
- Installed patches
- Remote desktop
- Shares

WMIC – Try This First

Wmic [alias] list brief

Example:

```
wmic process list brief
```

WMIC – Output Format

Uses XSL to format output data

Can use built-in or create custom

WMIC – Built-In Output Formats

- RawXML
- XML: formatted in HTML
- Hform: one long vertical HTML table
- Htable: HTML table (row per instance)
- CSV: comma separated with hostname at beginning of line
- Table: text table

Dsquery

- Part of Windows administrative tool pack
- Command-line tool to query active directory
- Series of tools: dsquery, dsget, dsadd, dsmod, dsmove, dsrm

Dsquery - LDAP

- Lightweight directory access protocol
- Basis of Windows Active Directory

LDAP – Prefix Notation

Logical operators are given
BEFORE the operands

Example: objects of category
"person" and class "user":

```
(&(objectcategory=person)
  (objectclass=user))
```

LDAP Query Combinations

objectCategory	objectClass	Result
person	User	user objects
person		user and contact objects
person	contact	contact objects
	user	user and computer objects
computer		computer objects
user		user and contact objects
	contact	contact objects
	computer	computer objects

LDAP - Bitwise Operations

Not everything has a pretty filter

UserAccountControl has bits for various attributes

LDAP – UserAccountControl (1)

Some commonly used values:

- 2: disabled
- 16: locked out
- 32: no password required
- 64: cannot change password
- 512: normal account
- 65536: no password expiration

LDAP – UserAccountControl (2)

Disabled accounts:

```
dsquery * -filter
  "(&(objectCategory=person)
  (objectClass=user)
  (userAccountControl:1.2.840.
    113556.1.4.803:=2))"
```

SomarSoft DumpSec

- Free utility to dump Windows security information
- Related to SomarSoft Hyena commercial tool used by some administrators
- Available from SytemTools.com

DumpSec Features

DumpSec can report on:

- Services
- Security policies
- User rights
- Users and groups
- File / registry / share permissions

Conclusion

Hands-on techniques

Barely scratched the surface

Get the tools and play with them:

- WITH PERMISSION
- On test systems

Questions

http://tinyurl.com/ISACAClay