Domain ADventuring w/ ADSI: Exploiting Admin tools for Fun and Profit

Grimmie!

([ADSI]“LDAP://CN=Grimmie”).Properties

- Name : {Grimmie}
- Description : {couch potato, wannabe RT/researcher, finding ways to find how to find things to break, committing culinary crimes since ‘14}
- MemberOf : {Security Intern at FortyNorth Security, PNPT}

Agenda

- So what is ADSI and why do we care?
- LDAP Filtering
- Leveraging ADSI as an attacker
- Crash course: ACLs
- (Ab)using ADSI: Act II
- Introducing Coeus

- Based on article I released last year, which can be found here
- Aside: This talk will not be about popping shells w/ ADSI, rather using it to find ways to pop shells. ADSI for persistence is an option, but that's beyond the scope of this talk

So what’s ADSI and why do we care?

- Type Accelerator
- Admin tool
- Part of DirectoryServices
- Ships by default on Win7+
- Bypasses CLM…most of the time (applies only to PS)
    - PowerShell language mode greatly limiting users
    - Doesn’t allow for method invocation (i.e the calling of .NET namespaces)

LDAP Filtering

- General layout
  - “([condition]([propName]=[propValue])...)...”
- Conditionals
  - ! - not, | - or, & - and
- Wildcards
  - You get a *, you get a *, you all get a *
- Examples!
  - “(&(samaccounttype=805306368)(|(cn=admin)(cn=dev))(!(cd=honeypot)))”
- docs

Leveraging ADSI as an attacker (admin + misconfig stuffs)

- DirectoryEntry ([adsi])
  - Points to a specific object
  - Returns the single specified object
  - Allows for property querying and modifying the specified object
- DirectorySearcher ([adsisearcher])
  - Predominantly used to return data on objects based on a filter
  - Can return multiple objects
  - Mainly search capabilities
- Setting up and searching w/ filters
  - Demo time!

Crash course: ACLs

- ACLs? ACEs?
  - ACL - Access Control Lists (DACLs/SACLs), contain ACEs (Access Control Entities)
  - ACE - tell Windows whether to allow or deny access
- DACLs?SACLs?
  - DACLs - Discretionary Access Control List, perms handling.usually what’s referenced when folks say “ACL abuse”
  - SACLs - Secure Access Control List, more for logging purposes
- A Few Rights
  - GenericAll - god mode (full reign to affected object)
  - WriteDACL - modify DACL of affected object

(Ab)using ADSI: Act II

- Properties
  - ActiveDirectoryRights - perm acting on object
  - AccessControlType - Allow/Deny right to object
  - IdentityReference - object right belongs to

- Querying object ACEs w/ ADSI
  - Demo time!

Introducing Coeus

- Named after Greek Titan of knowledge and roughly translates to “query/questioning/intelligence” (ty wikipedia)

- Gains a lay of the land by leveraging ADSI to perform basic administrative enumeration tasks (fetch users, groups, etc.)

- Enumerates common misconfigs found within a domain (roasting, delegation, etc.)

- Demo time!

Mah socials/QnA

Twitter: @Gr1mmie

Blog: https://grimmie.net

Github: https://github.com/Gr1mmie

Discord: Grimmie#0772