

Product Solutions Resources Open Source Enterprise Pricing

Q

Sign in

Sign up

dsnezhkov / TruffleSnout Public

Notifications

Fork 19

Star 85

<> Code

Issues 1

Pull requests

Actions

Security

Insights

Files

master

Go to file

TruffleSnout

Actions

Controllers

Docs

USAGE.md

Properties

Utils

App.config

FodyWeavers.xml

FodyWeavers.xsd

Options.cs

Program.cs

TruffleSnout.csproj

TruffleSnout.csproj.user

packages.config

.gitignore

README.md

TruffleSnout.sln

TruffleSnout / TruffleSnout / Docs / USAGE.md

user1 USAGE 7c2f22e · 4 years ago History

Preview

Code

Blame

457 lines (370 loc) · 17.6 KB

Raw

Intro

TruffleSnout is designed to help operators in a targeted discovery of immediate and adjacent AD infrastructure, query AD objects. It is designed to work in iterative fashion and provides granular control of the types of queries the operator can issue. This helps preserving a degree of operational security where the operator can limit and vary queries to match the perceived defenses and avoid triggering alerts or generate excessive logging.

The tool follows the natural discovery workflow many operators execute on the internal networks and helps answer precise questions like:

- Which forest am I in
- What domains exist in this forest
- What properties and components does a domain have
- What types of trusts do forest and domains have
- What is the first and primary domain in the forest
- Where are the Global catalogs
- What are sites and links
- Can I connect and ask the same of the remote domain
- Can I be flexible with method connection.
- Can I query objects via AD LDAP.
- Can I query a specific attribute or a list of the object
- Can I search for patterns in the returned result.

A few initial utilities to analyze the returned information are provided. By being flexible on the LDAP queries operators are not restricted in their exploration of AD objects to commonly used sets like groups, users, computers. Operators can query DNS, Certificates and other types of resources stored in the hierarchy.

Examples

Forest level

```
.\TruffleSnout.exe forest -n top.int
[*] Discovering forest top.int
Forest Name: top.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int

.\TruffleSnout.exe forest -n top.int -d
[*] Discovering forest top.int
Forest Name: top.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
Forest Root Domain: top.int
```

Page 1 of 7

```
Domains in Forest:
* top.int
- twin.local

.\TruffleSnout.exe forest -n top.int -s
[*] Discovering forest top.int
Forest Name: top.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
Forest Sites:
AD Site: Default-First-Site-Name
Site Link: DEFAULTIPSITELINK

.\TruffleSnout.exe forest -n top.int -g
[*] Discovering forest top.int
Forest Name: top.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
Forest GCs (Discoverable):
GlobalCatalog: win-3gk559644av.twin.local 10.0.2.100, wi
GlobalCatalog: win-inemggj3oef.top.int 10.0.2.200, win-i
Forest GCs (All):
GlobalCatalog: WIN-INEMGGJ30EF.top.int 10.0.2.200, WIN-I
GlobalCatalog: WIN-3GK559644AV.twin.local 10.0.2.100, WI

.\TruffleSnout.exe forest -n top.int -t
[*] Discovering forest top.int
Forest Name: top.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
Forest Trust:
Source: top.int, Target: other.int, Direction: Bidirecti

.\TruffleSnout.exe forest -n top.int -a
[*] Discovering forest top.int
Forest Name: top.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
Forest GCs (Discoverable):
GlobalCatalog: win-3gk559644av.twin.local 10.0.2.100, wi
GlobalCatalog: win-inemggj3oef.top.int 10.0.2.200, win-i
Forest GCs (All):
GlobalCatalog: WIN-INEMGGJ30EF.top.int 10.0.2.200, WIN-I
GlobalCatalog: WIN-3GK559644AV.twin.local 10.0.2.100, WI
Forest Sites:
AD Site: Default-First-Site-Name
Site Link: DEFAULTIPSITELINK
Forest Trust:
Source: top.int, Target: other.int, Direction: Bidirecti
Forest Root Domain: top.int
Domains in Forest:
* top.int
- twin.local

.\TruffleSnout.exe forest -n other.int -a -U user1 -P interactive
Enter <masked> credentials for `user1` : *****

[*] Discovering forest other.int
Forest Name: other.int
Forest Mode: unknown
Forest FSMO Master DC: WIN-VC752UMUPSS.other.int
Forest GCs (Discoverable):
GlobalCatalog: win-vc752umupss.other.int 10.0.2.250, win
Forest GCs (All):
GlobalCatalog: WIN-VC752UMUPSS.other.int 10.0.2.250, WIN
Forest Sites:
AD Site: Default-First-Site-Name
Site Link: DEFAULTIPSITELINK
Forest Trust:
Source: other.int, Target: top.int, Direction: Bidirecti
Forest Root Domain: other.int
Domains in Forest:
* other.int
```

```
.\TruffleSnout.exe forest -n other.int -a -U user1 -P *****
```

Domain level

```
.\TruffleSnout.exe domain -n twin.local
[*] Discovering domain twin.local
Domain Name: twin.local
Domain Forest: top.int
Domain Mode: Unknown
Domain Parent: None
Domain PDC: WIN-3GK559644AV.twin.local
Domain RID Master: WIN-3GK559644AV.twin.local
All DCs:
    DomainController : WIN-3GK559644AV.twin.local, Windows Server 20
All Discoverable DCs:
    DomainController :
        Name: win-3gk559644av.twin.local
        Domain: twin.local
        Forest: top.int
        Time: 3/16/2020 7:20:27 PM
        IP Address: 10.0.2.100
        OS Version: Windows Server 2016 Standard
        Site Name: Default-First-Site-Name
        Is GC?: True
Inbound Replication: CN=1ee4f7a7-e917-43a7-937a-35b9cf010e35 WIN-INEMGGJ
Outbound Replication: CN=88f32859-af2e-4cc0-b114-e3e293d7eda9 WIN-3GK559
Domain Children: None
Domain Trusts:
    Source: twin.local, Target: top.int, Direction: Bidirect
```

```
.\TruffleSnout.exe domain -n twin.local -U user1 -P ***
```

Directory level

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&(
[*] Directory LDAP://other.int/DC=other,DC=int
Auth type: Secure
[*] Query: (&(objectClass=user))

LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
admincount:Int: 1
samaccountname:String: Administrator
cn:String: Administrator
pwdlastset:Int: 132280093628558583
whencreated:DateTime: 3/6/2020 11:14:29 PM
badpwdcount:Int: 0
lastlogon:Int: 132286144697837082
samaccounttype:Int: 805306368
countrycode:Int: 0
objectguid:Bytes : 225 20 177 89 145 45 176 72 185 152 192 115 1
lastlogontimestamp:Int: 132280106153805870
usnchanged:Int: 12769
whenchanged:DateTime: 3/6/2020 11:33:13 PM
name:String: Administrator
objectsid:Bytes : 1 5 0 0 0 0 0 5 21 0 0 0 1 94 67 225 228 177 5
logoncount:Int: 13
badpasswordtime:Int: 0
accountexpires:Int: 0
primarygroupid:Int: 513
objectcategory:String: CN=Person,CN=Schema,CN=Configuration,DC=o
useraccountcontrol:Int: 512
description:String: Built-in account for administering the compu
dscorepropagationdata:DateTime: 3/6/2020 11:33:13 PM
dscorepropagationdata:DateTime: 3/6/2020 11:33:13 PM
dscorepropagationdata:DateTime: 3/6/2020 11:18:03 PM
dscorepropagationdata:DateTime: 1/1/1601 6:12:16 PM
distinguishedname:String: CN=Administrator,CN=Users,DC=other,DC=
iscriticalsystemobject:System.Boolean: True
objectclass:String: top
```

```
objectclass:String: person
objectclass:String: organizationalPerson
objectclass:String: user
usncreated:Int: 8196
memberof:String: CN=Group Policy Creator Owners,CN=Users,DC=othe
memberof:String: CN=Domain Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Enterprise Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Schema Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Administrators,CN=Builtin,DC=other,DC=int
adspath:String: LDAP://other.int/CN=Administrator,CN=Users,DC=ot
lastlogoff:Int: 0
logonhours:Bytes : 255 255 255 255 255 255 255 255 255 255 2
instancetype:Int: 4
codepage:Int: 0
LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
iscriticalsystemobject:System.Boolean: True
samaccountname:String: Guest
cn:String: Guest
pwdlastset:Int: 0
whencreated:DateTime: 3/6/2020 11:14:29 PM
badpwdcount:Int: 0
lastlogon:Int: 0
samaccounttype:Int: 805306368
countrycode:Int: 0
objectguid:Bytes : 63 61 74 97 39 244 73 66 164 18 41 101 168 20
usnchanged:Int: 8197
whenchanged:DateTime: 3/6/2020 11:14:29 PM
name:String: Guest
objectsid:Bytes : 1 5 0 0 0 0 5 21 0 0 0 1 94 67 225 228 177 5
logoncount:Int: 0
badpasswordtime:Int: 0
accountexpires:Int: 9223372036854775807
primarygroupid:Int: 514
objectcategory:String: CN=Person,CN=Schema,CN=Configuration,DC=o
useraccountcontrol:Int: 66082
description:String: Built-in account for guest access to the com
dscorepropagationdata:DateTime: 3/6/2020 11:18:03 PM
dscorepropagationdata:DateTime: 1/1/1601 12:00:01 AM
distinguishedname:String: CN=Guest,CN=Users,DC=other,DC=int
objectclass:String: top
objectclass:String: person
objectclass:String: organizationalPerson
objectclass:String: user
usncreated:Int: 8197
memberof:String: CN=Guests,CN=Builtin,DC=other,DC=int
adspath:String: LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=i
lastlogoff:Int: 0
instancetype:Int: 4
codepage:Int: 0
```

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&
```

```
[*] Directory LDAP://other.int/DC=other,DC=int
Auth type: Secure
[*] Query: (&(objectClass=user))
```

```
LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
badpwdcount:Int: 0
LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
badpwdcount:Int: 0
```

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&
```

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(& 
```

```
[*] Directory LDAP://other.int/DC=other,DC=int
Auth type: Secure
[*] Query: (&(objectClass=user))
```

```
LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
cn:String: Administrator
badpwdcount:Int: 0
memberof:String: CN=Group Policy Creator Owners,CN=Users,DC=othe
memberof:String: CN=Domain Admins,CN=Users,DC=other,DC=int
```

```
memberof:String: CN=Enterprise Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Schema Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Administrators,CN=Builtin,DC=other,DC=int
LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
cn:String: Guest
badpwdcount:Int: 0
memberof:String: CN=Guests,CN=Builtin,DC=other,DC=int
LDAP://other.int/CN=DefaultAccount,CN=Users,DC=other,DC=int
cn:String: DefaultAccount
badpwdcount:Int: 0
memberof:String: CN=System Managed Accounts Group,CN=Builtin,DC=
LDAP://other.int/CN=WIN-VC752UMUPSS,OU=Domain Controllers,DC=other,DC=in
cn:String: WIN-VC752UMUPSS
badpwdcount:Int: 0
LDAP://other.int/CN=krbtgt,CN=Users,DC=other,DC=int
cn:String: krbtgt
badpwdcount:Int: 0
memberof:String: CN=Denied RODC Password Replication Group,CN=Us
LDAP://other.int/CN=TOP$,CN=Users,DC=other,DC=int
cn:String: TOP$
badpwdcount:Int: 0
```

```
.\TruffleSnout.exe util --expires 9223372036854775807
Expires? True
```

```
.\TruffleSnout.exe util --ticks2date 132280170552471892
3/7/2020 1:10:55 AM
```

```
.\TruffleSnout.exe util -s 1 5 0 0 0 0 5 21 0 0 0 1 94 67 225 228
SID: S-1-5-21-3779288577-439595492-2162805249-1104
```

```
.\TruffleSnout.exe util -g 24 184 226 216 110 108 41 79 149 222 213 1.
GUID: d8e2b818-6c6e-4f29-95de-d58c0674c8ac
```

Usage

Actions

```
> .\TruffleSnout.exe help
```

forest	Forest discovery workflow
domain	Domain discovery workflow
directory	Directory discovery workflow
util	Utilities
help	Display more information on a specific command.
version	Display version information.

Forest

```
> .\TruffleSnout.exe help forest
```

-n, --name	Required. The name of a forest or `current` Example: -n top.int
-d, --domains	Get forest domains Example: -d
-t, --trusts	Get forest trusts Example: -t

-s, --sites	Get forest sites Example: -s
-g, --gcs	Get Global Catalogs Example -g
-a, --all	Get all forest info. This is a shortcut to -g -s -d Example: -a
-U, --username	(Auth) User Name for connection to the service Example: -U username
-P, --password	(Auth) Password fot the user. Provide: `interactive` to ask for a password. OpSec: Clear text passwords on the command line if u Example: -P <password> -P interactive
--help	Display this help screen.
--version	Display version information.

Domain

> .\TruffleSnout.exe help domain

-n, --name	Required. The name of a domain or `current`
-c, --controller	Get domain controllers
-t, --trusts	Get domain trusts
-a, --all	Get all domain info. This is a shortcut to -c -t Example: -a
-U, --username	(Auth) User Name for connection to the service Example: -U username
-P, --password	(Auth) Password fot the user. Provide: `interactive` to ask for a password. OpSec: Clear text passwords on the command line if Example: -P <password> -P interactive
--help	Display this help screen.
--version	Display version information.


Directory

.\TruffleSnout.exe help directory

-l, --ldap	Required. LDAP Connection Path. Can include startin Example: LDAP://other.int/DC=other,DC=int
-f, --filter	Required. Query Filter, in relation to the starting Syntax: https://docs.microsoft.com/en-us/windows/wi Example: '(&(objectClass=user))'
-a, --attr	Limit query to specific attribute(s). Attributes se `meta` - shows the attribute keys. Example: -a meta -a badpwdcount,cn,memberof
-c, --count	Required. Limit of entries returned in a query Example: -c 10
-n, --nonsecure	Do basic authentication. Do not use Kerberos/NTLM. Opsec: clear text connectivity. Example: -n
-s, --ssl	Connect as LDAP/S (SSL). This assumes certificates Note: to specify port use the format provided in `-

	Example: <code>-s</code>
<code>-U, --username</code>	(Auth) User Name <code>for</code> connection to the service Example: <code>-U username</code>
<code>-P, --password</code>	(Auth) Password fot the user. Provide: <code>`interactive`</code> to ask <code>for</code> a password. OpSec: Clear text passwords on the command line <code>if</code> Example: <code>-P <password> -P interactive</code>
<code>--help</code>	Display this help screen.
<code>--version</code>	Display version information.

Utilities

<code>> .\TruffleSnout.exe help util</code>		
<code>-t, --ticks2date</code>	Convert time ticks to DateTime. Example: <code>-t 132280170552471892</code> . Output: <code>3/7/2020 1</code>	
<code>-e, --expires</code>	Check <code>if</code> a value of record expires Example: <code>-e 9223372036854775807</code> . Output: <code>Expires?`</code>	
<code>-s, --bytes2SID</code>	Convert Bytes to SID. Used <code>in`objectsid`</code> attribut Example: <code>-s 1 5 0 0 0 0 0 5 21 0 0 0 1 94 67 225 2</code> Output: SID: <code>S-1-5-21-3779288577-439595492-2162805</code>	
<code>-g, --bytes2GUID</code>	Convert Bytes to GUID. Used <code>in`objectguid`</code> attrib Example: <code>-g 24 184 226 216 110 108 41 79 149 222 2</code> Output: GUID: <code>d8e2b818-6c6e-4f29-95de-d58c0674c8ac</code>	
<code>--help</code>	Display this help screen.	
<code>--version</code>	Display version information.	