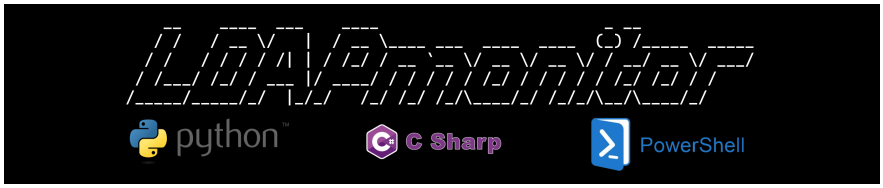
.github
csharp
powershell
python
.gitignore
LICENCE
README.md

README GPL-3.0 license



Monitor creation, deletion and changes to LDAP objects live during your pentest or system administration!

About

Monitor creation, deletion and changes to LDAP objects live during your pentest or system administration!

podalirius.net/

python ldap monitor csharp tool powershell active-directory pentest

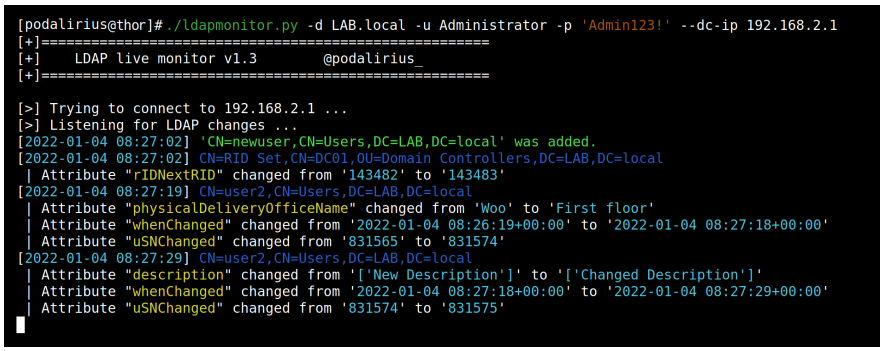
Releases 4

1.4 Latest
on Jan 12, 2023

+ 3 releases

Sponsor this project

With this tool you can quickly see if your attack worked and if it changed LDAP attributes of the target object.



Features

Feature	Python (.py)	CSharp (.exe)	Powershell (.ps1)
LDAPS support	✔	✔	✔
Random delay in seconds between queries	✔	✔	✔
Custom delay in seconds between queries	✔	✔	✔
Save output to logfile	✔	✔	✔
Colored or not colored output with `--no-colors`	✔	✘	✘
Custom page size for paged queries	✔	✔	✔
Authenticate with user and password	✔	✔	✔

Contributors 5

Languages

C# 41.3% Python 33.5% PowerShell 25.2%

Authenticate as current shell user	✗	✓	✓
Authenticate with LM:NT hashes	✓	✗	✗
Authenticate with kerberos tickets	✓	✗	✗
Option to ignore user logon events	✓	✓	✓
Custom search base	✓	✓	✓
Iterate over all naming contexts	✓	✓	✓

Typical use cases

Here is a few use cases where this tool can be useful:

- Detect account lockout in real time

```
[2021-10-17 10:56:58] CN=user1,CN=Users,DC=LAB,DC=local
 | Attribute "whenChanged" changed from '2021-10-16 19:48:25+00:00' to '2021-10-17 10:56:58+00:00'
 | Attribute "uSNChanged" changed from '700476' to '704557'
 | Attribute "badPwdCount" changed from '4' to '5'
 | Attribute "badPasswordTime" changed from '2021-10-17 10:56:56.038124+00:00' to '2021-10-17 10:56:58.066355+00:00'
 | Attribute "lockoutTime" = '2021-10-17 10:56:58.066355+00:00' was created.
```

- Check if your privilege escalation worked (with ntlmrelay's `--escalate-user` option)

- Detect when users are login in to know when to start a network poisoning.

```
[2021-10-17 12:49:58] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute "lastLogon" changed from '2021-10-17 12:48:32.709038+00:00' to '2021-10-17 12:49:57.943645+00:00'
 | Attribute "logonCount" changed from '3' to '4'
```

Cross platform !

In Python (.py)

```
[podalirius@thor]# ./ldapmonitor.py -d LAB.local -u Administrator -p 'Admin123!' --dc-ip 192.168.2.1
[+]=====================================================
[+]    LDAP live monitor v1.3        @podalirius_
[+]=====================================================

[>] Trying to connect to 192.168.2.1 ...
[>] Listening for LDAP changes ...
[2022-01-04 08:27:02] 'CN=newuser,CN=Users,DC=LAB,DC=local' was added.
[2022-01-04 08:27:02] CN=RID Set,CN=DC01,OU=Domain Controllers,DC=LAB,DC=local
 | Attribute "rIDNextRID" changed from '143482' to '143483'
[2022-01-04 08:27:19] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute "physicalDeliveryOfficeName" changed from 'Woo' to 'First floor'
 | Attribute "whenChanged" changed from '2022-01-04 08:26:19+00:00' to '2022-01-04 08:27:18+00:00'
 | Attribute "uSNChanged" changed from '831565' to '831574'
[2022-01-04 08:27:29] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute "description" changed from '['New Description']' to '['Changed Description']'
 | Attribute "whenChanged" changed from '2022-01-04 08:27:18+00:00' to '2022-01-04 08:27:29+00:00'
 | Attribute "uSNChanged" changed from '831574' to '831575'
```

In CSharp (.exe)

```
Microsoft Windows [Version 10.0.19043.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dev>ldapmonitor.exe /dcip:192.168.2.1 /user:LAB\user1 /pass:October2021!
[+]=====================================================
[+]  Sharp LDAP live monitor v1.3        @podalirius_
[+]=====================================================

[+] Using the following credentials:
  | Target: LDAP://192.168.2.1:389
  | User: 'LAB\user1'
  | Pass: 'October2021!'

[>] Listening for LDAP changes ...
[2021/10/16 07:58:18] 'CN=newuser,CN=Users,DC=LAB,DC=local' was added.
[2021/10/16 07:58:18] CN=RID Set,CN=DC01,OU=Domain Controllers,DC=LAB,DC=local
 | Attribute ridnextrid changed from '143453' to '143454'
[2021/10/16 07:58:41] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute usnchanged changed from '696374' to '700486'
 | Attribute whenchanged changed from '10/16/2021 5:33:57 PM' to '10/16/2021 7:58:40 PM'
 | Attribute physicaldeliveryofficename changed from 'Woo' to 'First floor'
[2021/10/16 07:58:50] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute usnchanged changed from '700486' to '700487'
 | Attribute whenchanged changed from '10/16/2021 7:58:40 PM' to '10/16/2021 7:58:50 PM'
 | Attribute description changed from 'New Description' to 'Changed Description'
```

In Powershell (.ps1)

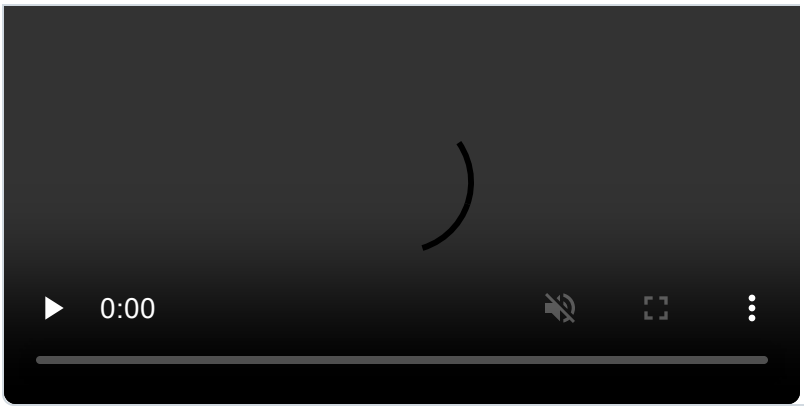
```
PS C:\Users\dev> .\ldapmonitor.ps1 -dcip 192.168.2.1 -Username "LAB\user1" -Password "October2021!"
[+]=====================================================
[+] Powershell LDAP live monitor v1.3    @podalirius_
[+]=====================================================

[>] Listening for LDAP changes ...

[2021/10/16 09:58:18] 'CN=newuser,CN=Users,DC=LAB,DC=local' was created.
[2021/10/16 09:58:18] CN=RID Set,CN=DC01,OU=Domain Controllers,DC=LAB,DC=local
 | Attribute ridnextrid changed from '143453' to '143454'
[2021/10/16 09:58:40] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute usnchanged changed from '696374' to '700486'
 | Attribute whenchanged changed from '10/16/2021 5:33:57 PM' to '10/16/2021 7:58:40 PM'
 | Attribute physicaldeliveryofficename changed from 'Woo' to 'First floor'
[2021/10/16 09:58:50] CN=user2,CN=Users,DC=LAB,DC=local
 | Attribute description changed from 'New Description' to 'Changed Description'
 | Attribute usnchanged changed from '700486' to '700487'
 | Attribute whenchanged changed from '10/16/2021 7:58:40 PM' to '10/16/2021 7:58:50 PM'
```

Demonstration

ldapmonitor_demo.mp4



Limitations

LDAP paged queries returns **pageSize** results per page, and it takes approximately 1 second to query a page. Therefore your monitoring refresh rate is **(number of LDAP objects // pageSize)** seconds. On most domain controllers **pageSize = 5000**.