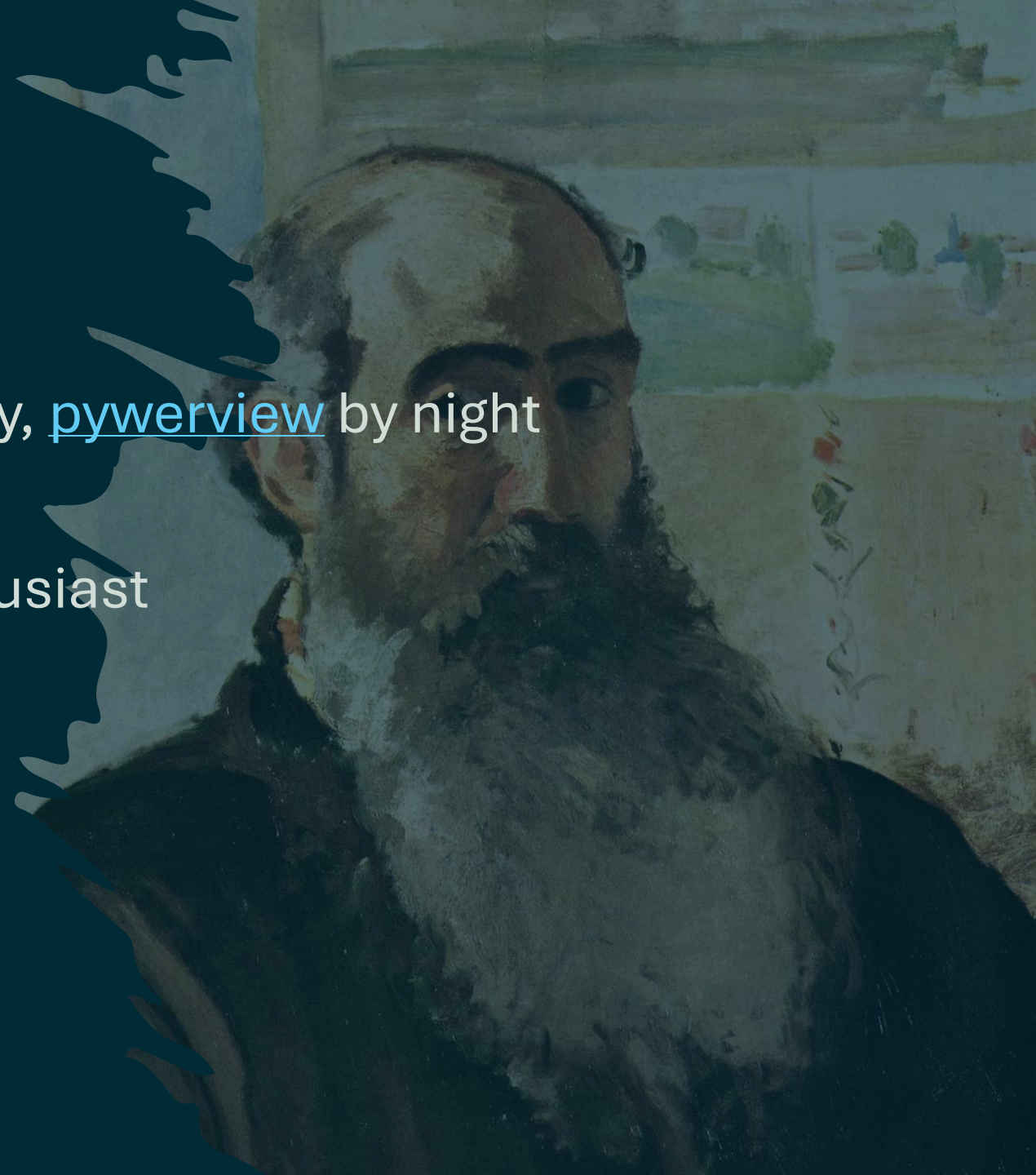
pywerview

A (partial) Python rewriting of PowerSploit's PowerView

DEFCON Paris – June 2024

WHO AM I

- Simon (a.k.a @lowercase_drm)
- Pentester @AlmondOffsec by day, pywerview by night
- Casual hacker
- Open-source security tools enthusiast
- ldap3 hardcore fan



Opinions are my own and not the views of my employer

NICE PREZ BRO, BUT…

- *I can do that with BloodHound/PingCastle/nxc/ldapsearch/…*
- *Python is so 2015, why not using go/rust/zig/pure aarch64 assembly/…?*

- I know
- There are as many pentests as there are pentesters
- Submit your own talk! (Defcon Paris DM are now open)

HISTORY

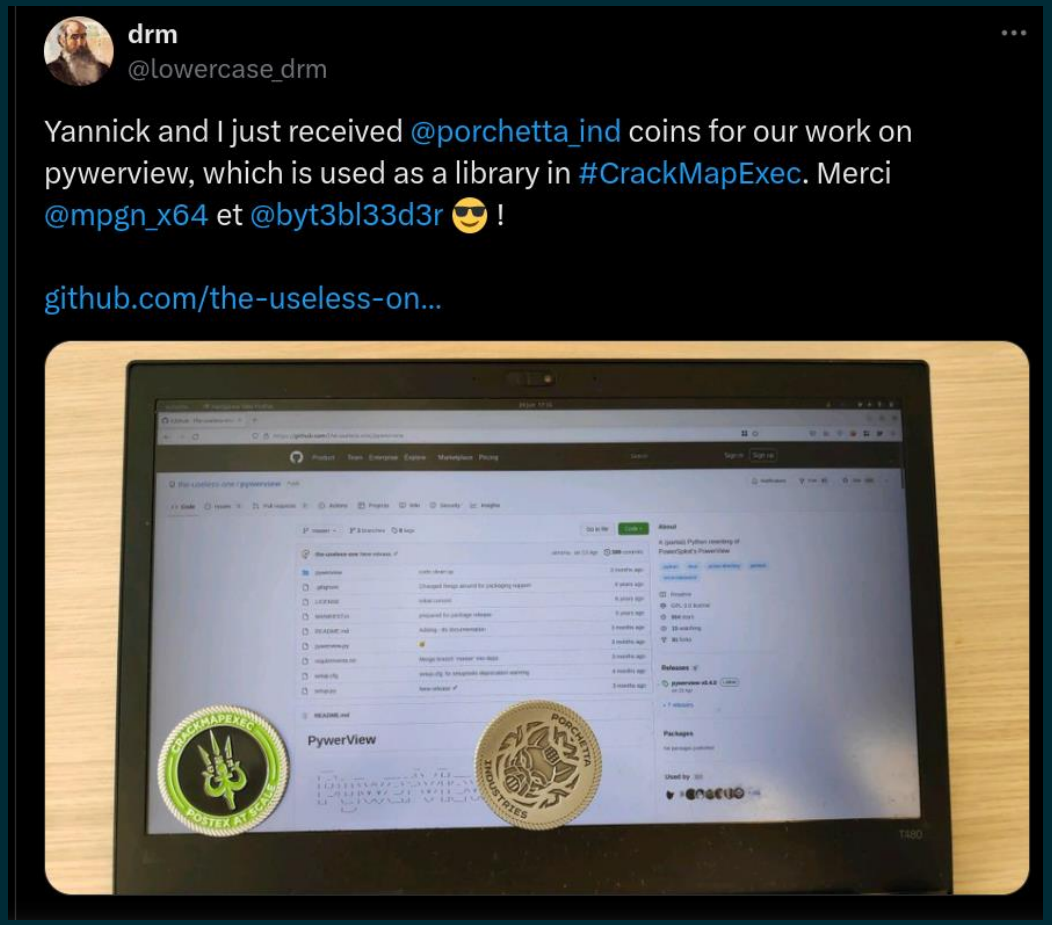
- July 2016
- Powerview is at its prime
- Yannick is a pentester but also (mainly ?) a Linux guy

“However, running PowerView on a computer which is not connected to the domain is a pain: I always find myself using mimikatz's sekurlsa::pth to run a Powershell prompt with stolen domain credentials, and that's not easy to script. [...] That's why I decided to rewrite some of PowerView's functionalities in Python, using the wonderful impacket library.”

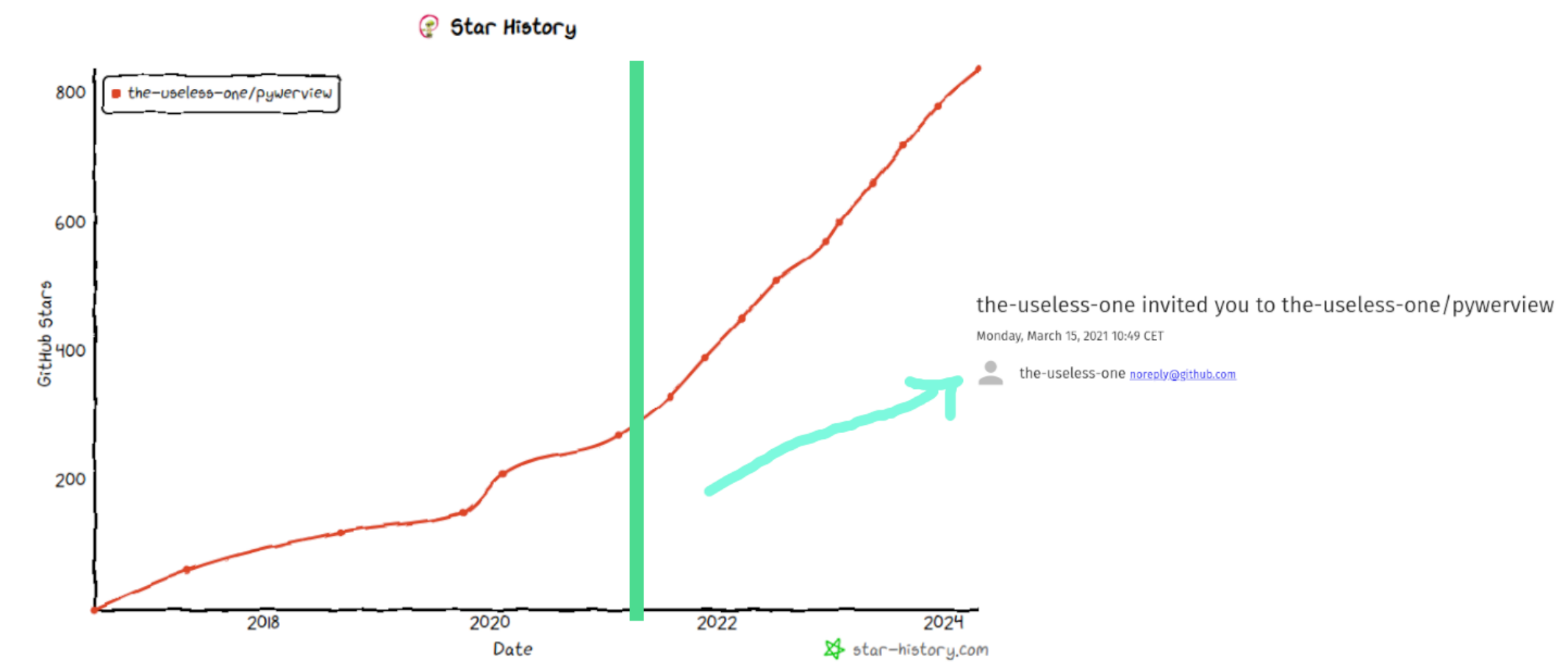
- pywerview is born!

HISTORY

- ~~Developed and tested in prod~~
- python2 then python3 (migration kick started by … mpgn!)
- `impacket.ldap` then `ldap3`
- Early adopter but I became officially co-maintainer in 2021
  - ok JiaTan75…
- 800+ stars



KEY PERFORMANCE INDICATORS



THE TOOL

- Command line and library
- Mostly Active Directory (LDAP) enumeration tool
  - *sprinkled with a little bit of SMB and RPC*
- 30+ functions
  - `get-netuser`
  - `get-adobject`
  - `get-netpso`
  - `get-netgroupmember`
  - …

```
Rewriting of some PowerView's functionalities in Python

options:
  -h, --help            show this help message and exit

Subcommands:
  Available subcommands

  {get-adobject,get-objectowner,get-netgmsa,get-netsmsa,get-objectacl,get-netuser,get-netgroup,get-netcomputer,get-netdomaincontroller,get-netfileserver,get-dfsshare,get-netou,get-netsite,get-netsubnet,get-netdomaintrust,get-netgpo,get-netpso,get-domainpolicy,get-gpttmpl,get-netgpogroup,find-gpocomputeradmin,find-gpolocation,get-netgroupmember,get-netsession,get-localdisks,get-netdomain,get-netshare,get-netloggedon,get-netlocalgroup,invoke-checklocaladminaccess,get-netprocess,get-userevent,invoke-userhunter,invoke-processhunter,invoke-eventhunter}
    get-adobject        Takes a domain SID, samAccountName or name, and return the associated object
    get-objectowner     Takes a domain SID, samAccountName or name, and return the associated object owner
    get-netgmsa         Returns a list of all the gMSA of the specified domain. To retrieve passwords, you need a privileged account and a TLS connection to the LDAP server (use the --tls switch).
    get-netsmsa         Returns a list of all the sMSA of the specified domain.
    get-objectacl       Takes a domain SID, samAccountName or name, and return the ACL of the associated object
    get-netuser         Queries information about a domain user
    get-netgroup        Get a list of all current domain groups, or a list of groups a domain user is member of
    get-netcomputer     Queries informations about domain computers
    get-netdomaincontroller
                        Get a list of domain controllers for the given domain
    get-netfileserver   Return a list of file servers, extracted from the domain users' homeDirectory, scriptPath, and profilePath fields
    get-dfsshare        Return a list of all fault tolerant distributed file systems for a given domain
    get-netou           Get a list of all current OUs in the domain
    get-netsite         Get a list of all current sites in the domain
    get-netsubnet       Get a list of all current subnets in the domain
    get-netdomaintrust  Returns a list of all the trusts of the specified domain
    get-netgpo          Get a list of all current GPOs in the domain
    get-netpso          Get a list of all current PSOs in the domain
    get-domainpolicy    Returns the default domain or DC policy for the queried domain or DC
    get-gpttmpl         Helper to parse a GptTmpl.inf policy file path into a custom object
    get-netgpogroup     Parses all GPOs in the domain that set "Restricted Group" or "Groups.xml"
    find-gpocomputeradmin
                        Takes a computer (or OU) and determine who has administrative access to it via GPO
    find-gpolocation    Takes a username or a group name and determine the computers it has administrative access to via GPO
    get-netgroupmember  Return a list of members of a domain group
    get-netsession      Queries a host to return a list of active sessions on the host (you can use local credentials instead of domain credentials)
    get-localdisks      Queries a host to return a list of active disks on the host (you can use local credentials instead of domain credentials)
    get-netdomain       Queries a host for available domains
    get-netshare        Queries a host to return a list of available shares on the host (you can use local credentials instead of domain credentials)
    get-netloggedon     This function will execute the NetWkstaUserEnum RPC call to query a given host for actively logged on users
    get-netlocalgroup   Gets a list of members of a local group on a machine, or returns every local group. You can use local credentials instead of domain credentials, however, domain credentials are needed
                        to resolve domain SIDs.
    invoke-checklocaladminaccess
                        Checks if the given user has local admin access on the given host
    get-netprocess      This function will execute the 'Select * from Win32_Process' WMI query to a given host for a list of executed process
    get-userevent       This function will execute the 'SELECT * from Win32_NTLogEvent' WMI query to a given host for a list of executed process
    invoke-userhunter   Finds which machines domain users are logged into
    invoke-processhunter
                        Searches machines for processes with specific name, or ran by specific users
    invoke-eventhunter  Searches machines for events with specific name, or ran by specific users
```

```
(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netuser -u eddard.stark -p "FightP3aceAndHonor!"  -w "north" -t 192.168.56.11 --username eddard.stark
objectclass:            top, person, organizationalPerson, user
cn:                     eddard.stark
sn:                     Stark
l:                      King's Landing
description:            Eddard Stark
givenname:              Eddard
distinguishedname:      CN=eddard.stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
instancetype:           4
whencreated:            2024-04-03 10:17:35+00:00
whenchanged:            2024-05-29 12:27:25+00:00
usncreated:             13228
memberof:               CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
                        CN=Domain Admins,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
                        CN=Administrators,CN=Builtin,DC=north,DC=sevenkingdoms,DC=local
usnchanged:             157693
name:                   eddard.stark
objectguid:             {da36d51f-f959-4c0d-927a-ff0981ca75f0}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
badpwdcount:            0
codepage:               0
countrycode:            0
badpasswordtime:        1601-01-01 00:00:00+00:00
lastlogoff:             1601-01-01 00:00:00+00:00
lastlogon:              2024-06-08 08:47:25.304464+00:00
pwdlastset:             2024-04-03 10:17:35.746481+00:00
primarygroupid:         513
objectsid:              S-1-5-21-1946681813-1497360990-87279489-1111
admincount:             1
accountexpires:         9999-12-31 23:59:59.999999+00:00
logoncount:             11497
samaccountname:         eddard.stark
samaccounttype:         USER_OBJECT
managedobjects:         CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
objectcategory:         CN=Person,CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local
dscorepropagationdata: 2024-04-03 10:25:51+00:00, 2024-04-03 10:25:48+00:00, 2024-04-03 10:19:27+00:00,
                        1601-01-01 00:00:00+00:00
lastlogontimestamp:     2024-05-29 12:27:25.223522+00:00
```

```
(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netuser -u eddard.stark -p "FightP3aceAndHonor!"  -w "north" -t 192.168.56.11 --attributes samaccountn
ame memberof
samaccountname: sql_svc
memberof:

memberof:       CN=Mormont,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
                CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: jeor.mormont

memberof:       CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: samwell.tarly

memberof:       CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
                CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: jon.snow

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: hodor

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: rickon.stark

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: brandon.stark

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local
samaccountname: sansa.stark

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
                CN=Administrators,CN=Builtin,DC=north,DC=sevenkingdoms,DC=local
samaccountname: robb.stark

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
                CN=Administrators,CN=Builtin,DC=north,DC=sevenkingdoms,DC=local
samaccountname: catelyn.stark

memberof:       CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local,
```

```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py get-netuser -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --custom-filter '(!(UserAccountControl:1.2.840.113556.1.4.803:=2))' --attribute samaccountname
samaccountname: hboproducer

samaccountname: maester.pycelle

samaccountname: lord.varys

samaccountname: petyer.baelish

samaccountname: stannis.baratheon

samaccountname: renly.baratheon

samaccountname: joffrey.baratheon

samaccountname: robert.baratheon

samaccountname: tyron.lannister

samaccountname: cersei.lannister

samaccountname: jaime.lannister

samaccountname: tywin.lannister
```

```
(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netgmsa -u daenerys.targaryen -p "BurnThemAll!"  -w essos.local -t 192.168.56.12
distinguishedname:       CN=gmsaDragon,CN=Managed Service Accounts,DC=essos,DC=local
objectsid:               S-1-5-21-2011510485-1632559128-417639-1119
samaccountname:          gmsaDragon$
msds-groupmsamembership: S-1-5-21-2011510485-1632559128-417639-1104
description:
enabled:                 True

(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netgmsa -u daenerys.targaryen -p "BurnThemAll!"  -w essos.local -t 192.168.56.12 --resolve-sid
distinguishedname:       CN=gmsaDragon,CN=Managed Service Accounts,DC=essos,DC=local
objectsid:               S-1-5-21-2011510485-1632559128-417639-1119
samaccountname:          gmsaDragon$
msds-groupmsamembership: CN=BRAAVOS,OU=Laps,DC=essos,DC=local
description:
enabled:                 True

(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netgmsa -u 'BRAAVOS$' --hashes adeafd093cf82c4cba33974a789354e1  -w essos.local -t 192.168.56.12 --res
olve-sid --tls
distinguishedname:       CN=gmsaDragon,CN=Managed Service Accounts,DC=essos,DC=local
objectsid:               S-1-5-21-2011510485-1632559128-417639-1119
samaccountname:          gmsaDragon$
msds-managedpassword:    4e1ade85df9f6ee64aa3260f9aded33b
msds-groupmsamembership: CN=BRAAVOS,OU=Laps,DC=essos,DC=local
description:
enabled:                 True
```

```
(venv) user@goad-linux:~/tools/pywerview$ pywerview invoke-userhunter -u eddard.stark -w north.sevenkingdoms.local -p 'FightP3aceAndHonor!' --threads 10 -t 192.168.56.11 --username robb.stark
computername: castelblack.north.sevenkingdoms.local
localadmin:
sessionfrom:
userdomain:   NORTH
username:     robb.stark

computername: winterfell.north.sevenkingdoms.local
localadmin:
sessionfrom:
userdomain:   NORTH
username:     robb.stark

computername: winterfell.north.sevenkingdoms.local
localadmin:
sessionfrom:
userdomain:   NORTH
username:     robb.stark

computername: winterfell.north.sevenkingdoms.local
localadmin:
sessionfrom:
userdomain:   NORTH
username:     robb.stark
(venv) user@goad-linux:~/tools/pywerview$ pywerview invoke-processhunter -u eddard.stark -w north.sevenkingdoms.local -p 'FightP3aceAndHonor!' --threads 10 -t 192.168.56.11 --processname notepad.exe
computername: winterfell.north.sevenkingdoms.local
domain:       NORTH
processid:    5012
processname:  notepad.exe
user:         robb.stark
```

```
(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netgpogroup -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.loc
al --resolve-sids
gpodisplayname: Add_Local_admin
gponame:        {1D846DF3-865C-4C4F-B734-205F9F12829C}
gpopath:        \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}\MACHINE\Preferences\Groups\Groups.xml
members:        CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
memberof:       CN=Administrators,CN=Builtin,DC=sevenkingdoms,DC=local

gpodisplayname: Add_Local_admin
gponame:        {1D846DF3-865C-4C4F-B734-205F9F12829C}
gpopath:        \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.
inf
members:        CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local
memberof:       CN=Administrators,CN=Builtin,DC=sevenkingdoms,DC=local


(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netgpo -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --
gponame {1D846DF3-865C-4C4F-B734-205F9F12829C}
objectclass:              top, container, groupPolicyContainer
cn:                       {1D846DF3-865C-4C4F-B734-205F9F12829C}
distinguishedname:        CN={1D846DF3-865C-4C4F-B734-205F9F12829C},CN=Policies,CN=System,DC=sevenkingdoms,DC=local
instancetype:             4
whencreated:              2024-05-23 12:54:43+00:00
whenchanged:              2024-05-23 13:30:11+00:00
displayname:              Add_Local_admin
usncreated:               485495
usnchanged:               485758
showinadvancedviewonly:   True
name:                     {1D846DF3-865C-4C4F-B734-205F9F12829C}
objectguid:               {8da651f0-3cdc-47e0-954d-f1c24f74702a}
flags:                    0
versionnumber:            7
objectcategory:           CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local
gpcfunctionalityversion:  2
gpcfilesyspath:           \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}
gpcmachineextensionnames: [{00000000-0000-0000-0000-000000000000}{79F92669-4224-476C-9C5C-6EFB4D87DF4A}][{17D89FEC-5C44-4972-B12D-241CAEF74509}{79F92669-4224-
476C-9C5C-6EFB4D87DF4A}][{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
dscorepropagationdata:    1601-01-01 00:00:00+00:00
```

```
(venv) user@goad-linux:~/tools/pywerview$ pywerview get-netou -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --g
uid 1D846DF3-865C-4C4F-B734-205F9F12829C --full-data
objectclass:            top, organizationalUnit
ou:                     BackendServer
distinguishedname:      OU=BackendServer,DC=sevenkingdoms,DC=local
instancetype:           4
whencreated:            2024-05-23 13:02:09+00:00
whenchanged:            2024-05-23 13:02:51+00:00
usncreated:             485576
usnchanged:             485587
name:                   BackendServer
objectguid:             {3f478a60-9614-4449-a51d-342d590f69e3}
objectcategory:         CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local
gplink:                 [LDAP://cn={1D846DF3-865C-4C4F-B734-205F9F12829C},cn=policies,cn=system,DC=sevenkingdoms,DC=local;0]
dscorepropagationdata: 2024-05-23 13:02:10+00:00, 1601-01-01 00:00:00+00:00
```

```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py find-gpocomputeradmin -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --ouname 'OU=BackendServer,DC=seven
nkingdoms,DC=local'
sevenkingdoms.local
computername:
ou:             OU=BackendServer,DC=sevenkingdoms,DC=local
gpodisplayname: Add_Local_admin
gpopath:        \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}\MACHINE\Preferences\Groups\Groups.xml
objectname:     HBO Producer
objectdn:       CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
objectsid:      S-1-5-21-67569864-3602506533-194968141-1125
isgroup:        False

computername:
ou:             OU=BackendServer,DC=sevenkingdoms,DC=local
gpodisplayname: Add_Local_admin
gpopath:        \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
objectname:     LocalAdmins
objectdn:       CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local
objectsid:      S-1-5-21-67569864-3602506533-194968141-1126
isgroup:        True
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py find-gpocomputeradmin -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --computername 'HBOSERVER.sevenkin
gdoms.local'
computername:   HBOSERVER.sevenkingdoms.local
ou:             OU=BackendServer,DC=sevenkingdoms,DC=local
gpodisplayname: Add_Local_admin
gpopath:        \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}\MACHINE\Preferences\Groups\Groups.xml
objectname:     HBO Producer
objectdn:       CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
objectsid:      S-1-5-21-67569864-3602506533-194968141-1125
isgroup:        False

computername:   HBOSERVER.sevenkingdoms.local
ou:             OU=BackendServer,DC=sevenkingdoms,DC=local
gpodisplayname: Add_Local_admin
gpopath:        \\sevenkingdoms.local\SysVol\sevenkingdoms.local\Policies\{1D846DF3-865C-4C4F-B734-205F9F12829C}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
objectname:     LocalAdmins
objectdn:       CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local
objectsid:      S-1-5-21-67569864-3602506533-194968141-1126
isgroup:        True
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py find-gpolocation -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --username hboproducer
objectname:     CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
gponame:        Add_Local_admin
gpoguid:        {1D846DF3-865C-4C4F-B734-205F9F12829C}
containername: OU=BackendServer,DC=sevenkingdoms,DC=local
computers:      hboserver.sevenkingdoms.local

objectname:     CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
gponame:        Add_Local_admin
gpoguid:        {1D846DF3-865C-4C4F-B734-205F9F12829C}
containername: OU=BackendServer,DC=sevenkingdoms,DC=local
computers:      hboserver.sevenkingdoms.local
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py find-gpolocation -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --groupname LocalAdmins
objectname:     CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local
gponame:        Add_Local_admin
gpoguid:        {1D846DF3-865C-4C4F-B734-205F9F12829C}
containername: OU=BackendServer,DC=sevenkingdoms,DC=local
computers:      hboserver.sevenkingdoms.local
(venv) user@goad-linux:~/tools/pywerview$
```

THE TOOL

- LDAPS
- Debug output (`-l DEBUG`)
- JSON output (`--json`)
  - Ain’t no time to learn Cypher query language!
  - …
  - Have you heard about our Lord and Savior `jq`?

```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py get-netdomaintrust -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --json | jq
{
  "cmd": {
    "submodule": "get-netdomaintrust",
    "args": {
      "domain": "sevenkingdoms.local",
      "user": "cersei.lannister",
      "password": "il0vejaime",
      "do_kerberos": false,
      "domain_controller": "kingslanding.sevenkingdoms.local",
      "do_tls": false,
      "user_cert": null,
      "user_key": null,
      "queried_domain": null,
      "full_data": false,
      "lmhash": "",
      "nthash": ""
    },
    "starting_time": "2024-04-26 12:41:03.146460",
    "ending_time": "2024-04-26 12:41:03.218760"
  },
  "results": [
    {
      "whencreated": "2024-04-03 10:13:56+00:00",
      "whenchanged": "2024-04-03 10:42:16+00:00",
      "trustdirection": "bidirectional",
      "trustpartner": "essos.local",
      "trusttype": "windows_active_directory",
      "trustattributes": [
        "TRUST_ATTRIBUTE_FOREST_TRANSITIVE",
        "TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL"
      ]
    },
    {
      "whencreated": "2024-04-03 10:03:53+00:00",
      "whenchanged": "2024-04-03 10:03:53+00:00",
      "trustdirection": "bidirectional",
      "trustpartner": "north.sevenkingdoms.local",
      "trusttype": "windows_active_directory",
      "trustattributes": [
        "TRUST_ATTRIBUTE_WITHIN_FOREST"
      ]
    }
  ]
}
```

```
[redacted]/tmp $ jq '.results|.[] | select(.operatingsystem) | select(.operatingsystem | contains("7")
or contains("2008") or contains("XP") or contains("2003") or contains("2000") or contains("2012")) | sele
ct(.operatingsystem | contains("NetApp") | not) | select(.lastlogontimestamp | contains("2024-")) | "* \(
.dnshostname) (\(.operatingsystem)) (dernière connexion le \(.lastlogontimestamp|split(" ")|.[0]))"' -r g
et-netcomputer_redacted.json
* [redacted].redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-03)
* [redacted]5.redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-06)
* [redacted].redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-03)
* [redacted]4.redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-07)
* [redacted]1.redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-07)
* [redacted]dacted.local (Windows XP Professional) (dernière connexion le 2024-04-06)
* [redacted]1.redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-03-31)
* [redacted]1.redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-01)
* [redacted].redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-04)
* [redacted].redacted.local (Windows XP Professional) (dernière connexion le 2024-03-30)
* [redacted]C.redacted.local (Windows 7 Professionnel N) (dernière connexion le 2024-03-30)
* [redacted]A-L.redacted.local (Windows 7 Professionnel) (dernière connexion le 2024-03-30)
* [redacted]001.redacted.local (Windows 7 Professionnel) (dernière connexion le 2024-04-01)
* [redacted]2.redacted.local (Windows Server 2012 R2 Standard) (dernière connexion le 2024-04-06)
* [redacted]002.redacted.local (Windows 7 Professionnel) (dernière connexion le 2024-03-29)
* [redacted]3.redacted.local (Windows 7 Professionnel) (dernière connexion le 2024-04-01)
* [redacted]4.redacted.local (Windows Server 2008 R2 Standard) (dernière connexion le 2024-03-30)
* [redacted]3.redacted.local (Windows Server 2008 R2 Standard) (dernière connexion le 2024-04-06)
```

```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py get-netgroup -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingd
oms.local --full-data --json | jq '.results | .[] | {rid: (.objectsid | split("-") | .[-1]), dn: .distinguishedname, objectsid: .objectsid, name: .name} | sel
ect((.rid | tonumber)>1000)'
{
  "rid": "1126",
  "dn": "CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local",
  "objectsid": "S-1-5-21-67569864-3602506533-194968141-1126",
  "name": "LocalAdmins"
}
{
  "rid": "1112",
  "dn": "CN=AcrossTheNarrowSea,CN=Users,DC=sevenkingdoms,DC=local",
  "objectsid": "S-1-5-21-67569864-3602506533-194968141-1112",
  "name": "AcrossTheNarrowSea"
}
{
  "rid": "1111",
  "dn": "CN=DragonRider,OU=Crownlands,DC=sevenkingdoms,DC=local",
  "objectsid": "S-1-5-21-67569864-3602506533-194968141-1111",
  "name": "DragonRider"
}
{
  "rid": "1110",
  "dn": "CN=KingsGuard,OU=Crownlands,DC=sevenkingdoms,DC=local",
  "objectsid": "S-1-5-21-67569864-3602506533-194968141-1110",
  "name": "KingsGuard"
}
{
  "rid": "1109",
  "dn": "CN=DragonStone,OU=Crownlands,DC=sevenkingdoms,DC=local",
  "objectsid": "S-1-5-21-67569864-3602506533-194968141-1109",
  "name": "DragonStone"
}
{
  "rid": "1108",
  "dn": "CN=Small Council,OU=Crownlands,DC=sevenkingdoms,DC=local",
```

THE TOOL

- Supported authentications
  - NTLM (cleartext password or hashes)
  - Kerberos (with SPN patching if needed, based on impacket #1256)
  - SChannel
- Supported hardening
  - Channel Binding
  - LDAP Signing
- … but can also falls back
  - SIMPLE

YouTube FR

la comédie musicale de Yannick VOSTFR FANSUB

10:43 / 21:59 • Extrait 2 - Colombe

🔞 TOP 5 des meilleures authentifications LDAP 🔥🔥 La troisième est vraiment A.B.U.S.É.E 😱😱 (spoiler c'est GSS-SPNEGO....)

drm on secruity
1337K subscribers

Subscribe

2.1K

Share

Save

THE TOOL

- Supported authentications
  - NTLM (cleartext password or hashes)
  - Kerberos (with SPN patching if needed, based on impacket #1256)
  - SChannel
- Supported hardening
  - Channel Binding
  - LDAP Signing
- … but can also falls back
  - SIMPLE

- More info: https://offsec.almond.consulting/ldap-authentication-in-active-directory-environments.html

```
(venv) user@goad-linux:~/tools/impacket$ getST.py -spn cifs/kingslanding.sevenkingdoms.local sevenkingdoms.local/cersei.lannister:'il0vejaime'
Impacket v0.12.0.dev1+20240418.131633.ea96b63a - Copyright 2023 Fortra

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Getting ST for user
[*] Saving ticket in cersei.lannister@cifs_kingslanding.sevenkingdoms.local@SEVENKINGDOMS.LOCAL.ccache
```

```
(venv) user@goad-linux:~/tools/pywerview$ KRB5CCNAME=../impacket/cersei.lannister@cifs_kingslanding.sevenkingdoms.local@SEVENKINGDOMS.LOCAL.ccache python pywerview.py get-netuser -u cersei.lannister -k -t kingsl
anding.sevenkingdoms.local --username cersei.lannister -l debug
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : LDAP sign and seal are not supported
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : TLS channel binding is not supported
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_kerberos_auth : LDAP authentication with Kerberos: ldap_scheme = ldap / seal_and_sign = False
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_kerberos_auth : TGS not found in KRB5CCNAME, looking for TGS with alternative SPN
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_kerberos_auth : Alternative TGS found, patching SPN
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _patch_spn : Patching principal to ldap/kingslanding.sevenkingdoms.local@SEVENKINGDOMS.LOCAL
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_kerberos_auth : LDAP binding parameters: server = kingslanding.sevenkingdoms.local / user = cersei.lannister@SEVENKINGDOMS.LOCAL / Kerberos auth
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_kerberos_auth : Successfully connected to the LDAP as u:SEVENKINGDOMS\cersei.lannister
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _ldap_search : search_base = dc=SEVENKINGDOMS,dc=LOCAL / search_filter = (&(samAccountType=805306368)(samAccountName=cersei.lannister)) / attributes = *
objectclass:            top, person, organizationalPerson, user
cn:                     cersei.lannister
sn:                     Lanister
l:                      King's Landing
description:            Cersei Lanister
givenname:              Cersei
distinguishedname:      CN=cersei.lannister,OU=Crownlands,DC=sevenkingdoms,DC=local
instancetype:           4
whencreated:            2024-04-03 10:17:37+00:00
whenchanged:            2024-04-23 11:32:47+00:00
usncreated:             16664
memberof:               CN=Small Council,OU=Crownlands,DC=sevenkingdoms,DC=local,
                        CN=Baratheon,OU=Stormlands,DC=sevenkingdoms,DC=local,
                        CN=Lannister,OU=Westerlands,DC=sevenkingdoms,DC=local,
```

```
(venv) user@goad-linux:~/tools/Certipy$ certipy req -u cersei.lannister@sevenkingdoms.local -p il0vejaime -ca 'SEVENKINGDOMS-CA'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 4
[*] Got certificate with UPN 'cersei.lannister@sevenkingdoms.local'
[*] Certificate object SID is 'S-1-5-21-67569864-3602506533-194968141-1115'
[*] Saved certificate and private key to 'cersei.lannister.pfx'



(venv) user@goad-linux:~/tools/Certipy$ certipy cert -pfx cersei.lannister.pfx -nocert -out cersei.lannister.key
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing private key to 'cersei.lannister.key'
(venv) user@goad-linux:~/tools/Certipy$ certipy cert -pfx cersei.lannister.pfx -nokey -out cersei.lannister.crt
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing certificate and  to 'cersei.lannister.crt'
(venv) user@goad-linux:~/tools/Certipy$
```

```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py get-netuser --cert ../Certipy/cersei.lannister.crt --key ../Certipy/cersei.lannister.key -w seve
nkingdoms.local -t kingslanding.sevenkingdoms.local -l DEBUG
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : LDAP sign and seal are not supported
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : TLS channel binding is not supported
[WARNING] pywerview_main_logger.LDAPRPCRequester - _create_ldap_connection : Cross domain query with certificate is not yet supported, so domain=queried domai
n
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : LDAP authentication with SChannel: ldap_scheme = ldap
[WARNING] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : Using certificate authentication but --tls not provided, setting up TLS with StartTLS
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : LDAP binding parameters: server = kingslanding.sevenkingdoms.local / cert = ../Certipy/ce
rsei.lannister.crt / key = ../Certipy/cersei.lannister.key / Explicit TLS / SChannel auth
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : Sending StartTLS command
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : StartTLS succeeded
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : Successfully connected to the LDAP as u:SEVENKINGDOMS\cersei.lannister
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _ldap_search : search_base = dc=sevenkingdoms,dc=local / search_filter = (&(samAccountType=805306368)) / attr
ibutes = *
objectclass:            top, person, organizationalPerson, user
cn:                     HBO Producer
sn:                     Producer
givenname:              HBO
distinguishedname:      CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
instancetype:           4
whencreated:            2024-05-23 12:56:46+00:00
whenchanged:            2024-05-23 13:04:32+00:00
displayname:            HBO Producer
usncreated:             485515
memberof:               CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local
usnchanged:             485603
name:                   HBO Producer
objectguid:             {d345bd2e-2813-4b5b-9e16-68c01df10810}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
badpwdcount:            0
codepage:               0
countrycode:            0
badpasswordtime:        1601-01-01 00:00:00+00:00
```

```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py get-netuser --cert ../Certipy/cersei.lannister.crt --key ../Certipy/cersei.lannister.key -w seve
nkingdoms.local -t kingslanding.sevenkingdoms.local -l DEBUG --tls
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : LDAP sign and seal are not supported
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : TLS channel binding is not supported
[WARNING] pywerview_main_logger.LDAPRPCRequester - _create_ldap_connection : Cross domain query with certificate is not yet supported, so domain=queried domai
n
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _create_ldap_connection : LDAPS connection forced
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : LDAP authentication with SChannel: ldap_scheme = ldaps
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : LDAP binding parameters: server = kingslanding.sevenkingdoms.local / cert = ../Certipy/ce
rsei.lannister.crt / key = ../Certipy/cersei.lannister.key / Implicit TLS / SChannel auth
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_schannel_auth : Successfully connected to the LDAP as u:SEVENKINGDOMS\cersei.lannister
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _ldap_search : search_base = dc=sevenkingdoms,dc=local / search_filter = (&(samAccountType=805306368)) / attr
ibutes = *
objectclass:            top, person, organizationalPerson, user
cn:                     HBO Producer
sn:                     Producer
givenname:              HBO
distinguishedname:      CN=HBO Producer,CN=Users,DC=sevenkingdoms,DC=local
instancetype:           4
whencreated:            2024-05-23 12:56:46+00:00
whenchanged:            2024-05-23 13:04:32+00:00
displayname:            HBO Producer
usncreated:             485515
memberof:               CN=LocalAdmins,CN=Users,DC=sevenkingdoms,DC=local
```

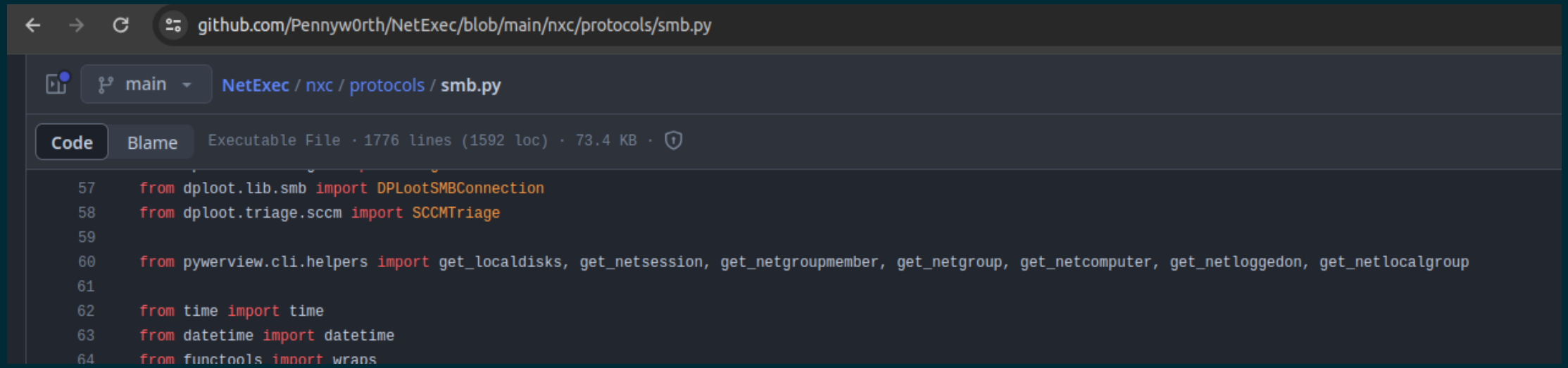
```
(venv) user@goad-linux:~/tools/pywerview$ python pywerview.py get-netcomputer -u cersei.lannister -w sevenkingdoms.local -p il0vejaime -t kingslanding.sevenkingdoms.local --full-data -l debug
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : LDAP sign and seal are not supported
[DEBUG] pywerview_main_logger.LDAPRequester - __init__ : TLS channel binding is not supported
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _get_netfqdn : SMB loging parameters: user = cersei.lannister  / password = il0vejaime / domain = sevenkingdoms.local / LM hash =  / NT hash =
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : LDAP authentication with NTLM: ldap_scheme = ldap / seal_and_sign = False / tls_channel_binding = False
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : LDAP binding parameters: server = kingslanding.sevenkingdoms.local / user = sevenkingdoms.local\cersei.lannister / password = il0vejaime
[WARNING] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : Server returns LDAPStrongerAuthRequiredResult
[WARNING] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : Sealing not available, falling back to LDAPS
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : LDAP authentication with NTLM: ldap_scheme = ldaps / seal_and_sign = False / tls_channel_binding = False
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : LDAP binding parameters: server = kingslanding.sevenkingdoms.local / user = sevenkingdoms.local\cersei.lannister / password = il0vejaime
[WARNING] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : Server returns LDAPInvalidCredentialsResult
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_ntlm_auth : Server requires Channel Binding Token but you are using password authentication, falling back to SIMPLE authentication, hoping LDAPS port is open
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_simple_auth : LDAP authentication with SIMPLE: ldap_scheme = ldaps
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_simple_auth : LDAP binding parameters: server = kingslanding.sevenkingdoms.local / user = cersei.lannister@sevenkingdoms.local / password = il0vejaime
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _do_simple_auth : Successfully connected to the LDAP as u:SEVENKINGDOMS\cersei.lannister
[DEBUG] pywerview_main_logger.LDAPRPCRequester - _ldap_search : search_base = dc=sevenkingdoms,dc=local / search_filter = (&(samAccountType=805306369)) / attributes = *
objectclass:                    top, person, organizationalPerson, user, computer
cn:                             KINGSLANDING
usercertificate:                308206703082055 8a003020102021379000000002b6b555e01285c65d00000000002300d06092a864886f70d01010b050...
distinguishedname:              CN=KINGSLANDING,OU=Domain Controllers,DC=sevenkingdoms,DC=local
instancetype:                   4
whencreated:                    2024-04-03 09:54:10+00:00
whenchanged:                    2024-04-25 10:43:13+00:00
usncreated:                     12293
memberof:                       CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=sevenkingdoms,DC=local,
                                CN=Cert Publishers,CN=Users,DC=sevenkingdoms,DC=local
usnchanged:                     232817
name:                           KINGSLANDING
objectguid:                     {d73f29cb-4f4a-48c5-8f81-9050f1bcde8e}
useraccountcontrol:             SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
badpwdcount:                    0
codepage:                       0
countrycode:                    0
badpasswordtime:                1601-01-01 00:00:00+00:00
lastlogoff:                     1601-01-01 00:00:00+00:00
lastlogon:                      2024-04-26 12:22:49.814198+00:00
localpolicyflags:               0
pwdlastset:                     2024-04-03 09:54:36.296841+00:00
primarygroupid:                 516
objectsid:                      S-1-5-21-67569864-3602506533-194968141-1001
accountexpires:                 9999-12-31 23:59:59.999999+00:00
logoncount:                     198
samaccountname:                 KINGSLANDING$
samaccounttype:                 MACHINE_ACCOUNT
operatingsystem:                Windows Server 2019 Datacenter
operatingsystemversion:         10.0 (17763)
serverreferencebl:
                                CN=KINGSLANDING,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=sevenkingdoms,DC=local
dnshostname:                    kingslanding.sevenkingdoms.local
ridsetreferences:               CN=RID Set,CN=KINGSLANDING,OU=Domain Controllers,DC=sevenkingdoms,DC=local
serviceprincipalname:           Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/kingslanding.sevenkingdoms.local,
                                ldap/kingslanding.sevenkingdoms.local/ForestDnsZones.sevenkingdoms.local,
                                ldap/kingslanding.sevenkingdoms.local/DomainDnsZones.sevenkingdoms.local, TERMSRV/KINGSLANDING,
```

THE LIBRARY

- pywerview is also a library
- create your own audit scripts!

THE LIBRARY

- pywerview is also a library
- create your own audit scripts!



```python
from pywerview.functions.net import NetRequester
import pywerview.objects.adobjects as adobj
from pywerview.functions.misc import Misc

dc = "192.168.56.12"
domain = "essos.local"
user = "daenerys.targaryen"
password = "BurnThemAll!"
lmhash = nthash = str()

customfilter = "(ObjectClass=organizationalUnit)"
#customfilter = str()

misc = Misc(dc, domain, user, password, lmhash, nthash)
domain_sid = misc.get_domainsid()

netrequester = NetRequester(dc, domain, user, password, lmhash, nthash)
raw = netrequester.get_objectacl(custom_filter=customfilter, resolve_guids=True)
sid_mapping = adobj.ADObject._well_known_sids.copy()
rid_mapping = adobj.ADObject._well_known_rids.copy()
results = list()

for entry in raw:
    try:
        sid_mapping[entry.securityidentifier]
        continue
    except KeyError:
        rid = entry.securityidentifier.replace(domain_sid+'-', '')
        try:
            rid_mapping[rid]
        except KeyError:
            if entry.acetype == 'ACCESS_ALLOWED_OBJECT_ACE':
                source = netrequester.get_adobject(queried_sid=entry.securityidentifier)[0]
                target = entry.objectdn
                if 'generic_all' in entry.activedirectoryrights:
                    right = ['generic_all']
                else:
                    right = entry.activedirectoryrights
                on = entry.objectacetype
                on_inherited = entry.inheritedobjectacetype
                if 'object_ace_type_present' in entry.objectaceflags and on == "ms-Mcs-AdmPwd":
                    print("{0} have {1} rights on {2} within {3}".format(source.distinguishedname, right, on, target))
                #elif 'inherited_object_ace_type_present' in entry.objectaceflags:
                 #   print("{0} have {1} rights on {2} within {3} (inherited)".format(source.distinguishedname, right, on_inherited, target))
                else:
                    continue
```

```
(venv) user@goad-linux:~/tools/scripts$ python3 get_object_ace.py
CN=Spys,CN=Users,DC=essos,DC=local have ['read_property', 'extended_right'] rights on ms-Mcs-AdmPwd within OU=Laps,DC=essos,DC=local
CN=jorah.mormont,CN=Users,DC=essos,DC=local have ['read_property', 'extended_right'] rights on ms-Mcs-AdmPwd within OU=Laps,DC=essos,DC=local
(venv) user@goad-linux:~/tools/scripts$
```

```
(venv) user@goad-linux:~/tools/scripts$ python kingcastle.py -u cersei.lannister -p il0vejaime -w sevenkingdoms.local -t kingslanding.sevenkingdoms.local --debug --gpo -o /tmp/
  _  ___              ____          _   _
 | |/ (_)_ __   __ _ / ___|__ _ ___| |_| | ___
 | ' /| | '_ \ / _` | |   / _` / __| __| |/ _ \
 | . \| | | | | (_| | |__| (_| \__ \ |_| |  __/
 |_|\_\_|_| |_|\__, |\____\__,_|___/\__|_|\___|
               |___/
                Make my castle ping again

[+] Let's go!
[-] Creating NetRequester
[+] recursive get_netgroupmember
[-] done!
[-] 3 domain admins
[+] get_netuser (only enabled accounts)
[-] done!
[-] 13 domain users
[-] PASSWD_NOTREQD
[]
[-] DONT_REQ_PREAUTH
[]
[-] DONT_EXPIRE_PASSWORD
[{'samaccountname': 'maester.pycelle', 'is_da': False}, {'samaccountname': 'lord.varys', 'is_da': False}, {'samaccountname': 'petyer.baelish', 'is_da': False}, {'samaccountname': 'stannis.baratheon', 'is_da': Fa
lse}, {'samaccountname': 'renly.baratheon', 'is_da': False}, {'samaccountname': 'joffrey.baratheon', 'is_da': False}, {'samaccountname': 'robert.baratheon', 'is_da': True}, {'samaccountname': 'tyron.lannister',
'is_da': False}, {'samaccountname': 'cersei.lannister', 'is_da': True}, {'samaccountname': 'jaime.lannister', 'is_da': False}, {'samaccountname': 'tywin.lannister', 'is_da': False}, {'samaccountname': 'vagrant',
 'is_da': False}, {'samaccountname': 'Administrator', 'is_da': True}]
[-] serviceprincipalname
[]
[+] Writing /tmp//sevenkingdoms.local_users_passwd_notreqd.json....
[+] Writing /tmp//sevenkingdoms.local_users_dont_req_preauth.json....
[+] Writing /tmp//sevenkingdoms.local_users_dont_expire_password.json....
[+] Writing /tmp//sevenkingdoms.local_users_serviceprincipalname.json....
[-] Creating GPORequester
[+] Retrieving information for GPOs
        GPO "Default Domain Controllers Policy" ({6AC1786C-016F-11D2-945F-00C04fB984F9}) applied on:
           OU=Domain Controllers,DC=sevenkingdoms,DC=local
        MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity: Signature not required (1)
        MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature: Signature Enabled (1)
        MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature: Signature Required (1)
        SeMachineAccountPrivilege: Authenticated Users
        SeDebugPrivilege: Administrators
        SeEnableDelegationPrivilege: Administrators
        SeInteractiveLogonRight: Enterprise Domain Controllers, Print Operators, Server Operators, Account Operators, Backup Operators, Administrators

        GPO "Default Domain Policy" ({31B2F340-016D-11D2-945F-00C04FB984F9}) applied on:
           DC=sevenkingdoms,DC=local
        MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash: LM hash disabled (1)

[+] The End!
```

THE END

- Download / debug / contribute
  - https://github.com/the-useless-one/pywerview/
- Hack’n Speak podcast (in French)
  - https://podcasters.spotify.com/pod/show/hacknspeak/episodes/0x12---the-useless-one--lowercase_drm--Retour-sur-la-librairie-Pywerview-e1i3r1d/a-a7sd75d
- Contact
  - https://twitter.com/lowercase_drm
  - https://mastodon.social/@drm
  - https://github.com/ThePirateWhoSmellsOfSunflowers
- s/o Yannick!