SYNACKTIV

ntdissector, a swiss-army knife for your NTDS files

SSTIC 2024

07/06/2024

who are we

SYNACKTIV

Mehdi Elyassa

Pentester/Redteamer

Julien Legras

Pentest team leader

Agenda

SYNACKTIV

- Introduction
- A few definitions
- Existing tools & libraries
- Features & examples
- Conclusion

Introduction

Introduction

SYNACKTIV

- **Back in December 2022….**
  - Password audit for a customer
    - Extract hashes from NTDS and start cracking!
  - Statistics reporting
    - Group users by a custom user type from **extensionAttribute** field

  → Tool to **extract**, **decrypt** and **format** everything (text + JSON)

A few definitions

NTDS.dit

SYNACKTIV

- **Active Directory database**
  - ESE database
    - Used in Exchange, File Replication Service, KMS, NTUSER.DAT, etc.
  - Important tables
    - **datatable** AD objects (users, groups, computers)
    - **link_table** Relations between the objects (groups, parent, child)
    - **sd_table** Security Descriptors (access control)
  - Secrets stored in **datatable**
    - Encrypted with **password encryptions keys** (PEK)
      - Encrypted with a **bootKey**, from the **SYSTEM** hive

- **Structure**
  - Single file
    - Pages arranged in balanced B-Tree structure
    - 8KB page size limit
  - Standard architecture
    - Database → tables → columns / records
  - Long value
    - Special column type to store large text or binary objects (max 2 GB)
    - Stored in a separate B-Tree

Existing tools & libraries

Existing tools & libraries

SYNACKTIV

- **secretsdump.py / gosecretsdump**
  - Only usernames, LM/NT hashes, account status and pwdLastSet
- **Airbus BTA (python + mongodb)**
  - Audit AD changes & perms, but Python 2 + wrappers on top of libesedb
- **go-ese (Go) / libesedb (C) / dissect.esedb (python)**
  - go-ese — very fast dump **but** does not handle Long Values (can contain interesting secrets)
  - libesedb — C with basic Python bindings (no documentation)
  - dissect.esedb — pure Python with everything we needed, thanks Fox-IT!

Features & examples

Features & examples

SYNACKTIV

- **Features**
  - Extract / format all AD objects with LDAP naming
  - Output JSON files for each object type (similar to ldeep)
  - Retrieved secrets
    - User hashes
    - DPAPI backup keys
    - Supplemental credentials: WDigest, Kerberos-Newer-Keys
    - LAPS and LAPSv2: local administrator passwords

Features & examples

SYNACKTIV

- **DPAPI Domain backup keys**

```
>>> jq '{cn, currentValue}' out/bcf5b328255cc214f14a2cf396ce0a76/secret.json
{
  "cn": "BCKUPKEY_P Secret",
  "currentValue": "10d2694f-8f34-42f8-9e23-49790b79f4c5"
}
{
  "cn": "BCKUPKEY_10d2694f-8f34-42f8-9e23-49790b79f4c5 Secret",
  "currentValue": {
    "legacyKey": "f93981ac52c63b6ac90ab4bc077647e60c869dd4380cb02c7c0460e8c07a5bda49e1eab9bca385df3237736731ba0acdf
2f580c013793814abf6dec7d575c29497d2d94c040425669ceba47f2e8e740734a35777549013f2c6c75f73bdda8c56a8c8554a0c37e97eb8e1
90de82e335e91b118bd85e639553a9a425ca9f1f66e849c8dd114b4301b3df1ddb1ebcd2c7c65be3524742423c11a46630ed4f2050a7fc48376
  }
}
{
  "cn": "BCKUPKEY_PREFERRED Secret",
  "currentValue": "8b530143-76b1-4fda-bf86-e1c12df321cb"
}
{
  "cn": "BCKUPKEY_8b530143-76b1-4fda-bf86-e1c12df321cb Secret",
  "currentValue": {
    "pvk": "HvG1sAAAAAABAAAAAAAAAAAAAACUBAAABwIAAACkAABSU0EyAAgAAAEAAQBFQ1OjYjst02Bg6yglytVfnVVfHKzdvtlhwIU0lIFCiHI
ZzVdtnNkMYV+eoJyQxmiT1vzx5iLXpVZJe+WmG96hXa9nmABY7zfTOXFwJ4TJ2bMOOE8LwU9jS76WrtkDIU4UcQt6nauZIYsjVCu01Uwc649Ub3H3Xi
8tvZ9303TwczfNdmFZB2h/hQLyGEmWrxeoBe/5ldS8h/unbqWsc60Gg/o5TBBmIdtFvRvdR7nUPO63i6rUV0GezovQ0yANQ5UcNvdXntVJB5DH8fJ5m
UbjAyhs9/Qtpg+6hvm1M0nFUVX/iDuS9eO93CAsRnHnB7Wa3govf/A1XqQF9ZXCPI61vjrP1eBPbeZPZXtIy6ZxZagUQLdU2HUbAJQ55ukfnvzJFS6B
D/N2iPmfvlsin4XCuVZAWAPD9hR84c3LIIRsbJSSURjGngk+LqlNEZbhFJCqC4tBkbwPR8Uynaq89CK2WpU9bvYAUFV0C8ZGqugTY0ZtDnhij5Y0CvR
TxiRPTRUyc5UJ0p3JgBwenZUpg+EtOxW8yi7EeOCl3mUXbJYh1OwdXxXgBM6VDGgSLI+2qfV/M2Qc91IIUwnnibIQkG5eq1lHOEcU5d3GVocjI5J33Q
APuQ9l/jCaFGtP4nIoR7cgTWwbgLvpGMr3zpFBdg8WFzT5h9f3mrBqL9Bd9wMhsnS2S6b70305CXVlgU+J8KAfUabggwwfPR4F5H6aoQIHICDlyiZ6n
PNBTcic1naCxLHxbsdXgoKVdLl2atCGthJvYxaq45Bj0vYqjpoNrI5VR99FtMa05++ULt0XDJcwVz22+kIT+k9ncHrRYSV47ely6S/7rT/Fk175ArWo
IqJ6YvQUMi+CrqKFs32IS/ttg2YG9+FklpAtpmWAYRMvMKLsOJ4RSNV4GnO2mLWsFIHu/10/pXi/i+OmTQoZ7dcchni0QHSElC5PhtP1voS94eKFUc0
```

Features & examples

SYNACKTIV

- **DPAPI Domain backup keys**

```
>>> jq -r '.currentValue.pvk? | select(. != null) ' out/bcf5b328255cc214f14a2cf396ce0a76/secret.json | base64 -d > /tmp/demo.pvk
>>> openssl rsa -inform PVK -in /tmp/demo.pvk -text -noout
Private-Key: (2048 bit, 2 primes)
modulus:
    00:ac:a5:6e:a7:fb:87:bc:d4:95:f9:ef:05:a8:17:
    af:96:49:18:f2:02:85:7f:68:07:59:61:76:cd:37:
    73:f0:74:d3:77:9f:bd:2d:0f:3e:93:dc:d6:20:18:
    33:32:43:43:96:b1:26:ae:53:f3:9f:c8:3a:37:fd:
    03:69:11:e8:9f:ea:fe:d3:b1:29:8a:fb:c8:06:09:
    72:f5:33:28:04:9a:79:7a:38:e7:de:1d:b3:e2:75:
    1f:f7:46:f5:b8:ce:c1:54:4d:bb:42:35:b2:18:92:
    b9:da:a9:b7:10:47:e1:14:32:90:ed:6a:e9:bb:34:
    f6:14:bc:f0:84:e3:30:9b:9d:4c:78:02:17:97:33:
    7d:f3:8e:05:80:79:f6:da:15:ea:bd:61:5a:be:97:
    64:55:7a:2d:62:1e:cf:6f:3d:89:66:0c:c9:09:ea:
    f9:15:c6:90:cd:d9:76:d5:9c:15:d5:60:4f:81:2e:
    88:e2:e4:b4:e9:90:a6:05:f5:29:23:30:35:3d:a8:
    7c:62:35:93:01:98:e3:e6:cb:1a:29:4a:94:f3:bf:
    20:0f:db:6c:d0:94:ab:49:b5:d5:d4:b1:5a:2e:72:
    88:42:81:94:34:85:c0:61:d9:be:dd:ac:1c:5f:55:
    9d:5f:d5:ca:25:28:eb:60:60:d3:2d:3b:62:a3:53:
    43:45
publicExponent: 65537 (0x10001)
```

Features & examples

SYNACKTIV

- **LAPSv2**

```
>>> jq '{cn, "msLAPS-PasswordExpirationTime", "msLAPS-EncryptedPassword", "msLAPS-EncryptedPasswordHistory"}' \
        out/bcf5b328255cc214f14a2cf396ce0a76/computer.json
{
  "cn": "EX",
  "msLAPS-PasswordExpirationTime": "2023-10-15T16:11:51.477503+00:00",
  "msLAPS-EncryptedPassword": "efe7d901f3194656dc040000000000003082044606092a864886f70d010703a082043730820433020
00001b0000000700000006884f60fbfa66c085c232b42fcecb5550803000014000000140000004448504200010000087a8e61db4b6663cffbb
1b2aa3016c3d91134096faa3bf4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d
902d52526735488a0ef13c6d9a51bfa4ab3ad8347796524d8ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f79715060
54330c198af126116d2276e11715f693877fad7ef09cadb094ae91e1a15973fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f
7e8c6f62901228f8c28cbb18a55ae31341000a650196f931c77a57f2ddf463e5e9ec144b777de62aaab8a8628ac376d282d6ed3864e67982
c80d052b985d182ea0adb2a3b7313d3fe14c8484b1e052588b9b7d2bbd2df016199ecd06e1557cd0915b3353bbb64e0ec377fd028370df92
2327cfef98c582664b4c0f6cc4165911bcd3587471342887e9329ac75ef5120b138715090da3e5e805559c186e7f81b27be375c4f33b6840
42765bfacf1dc7ceb5b6f29fd15f41cff4cd10fed3922a44381c1b4df010e5f950cd12c056825f14ee0e6c7b1d42e7a53ee17ac12b33d670
b11e759702047e448b1a5eb66d6cad7da991c70ed9ab66afb79c5d7f04af236e2b44d30c02a9b8b9e6170c217c0391a4d45e93db75219553
400450056002e004c004f00430041004c0000004400450056002e004c004f00430041004c00000030530609 2b0601040182374a013046060
343833393934363 92d323735363032343939332d333638353635313031352d353132300b0609608648016503040 12d0428c32f1a47e808f7
b06092a864886f70d010701301e0609608648016503040 12e3011040c7b27634b43eca0c32a2eadda020110b30be95ca7cd75c1e0071819b
277de47e353ba79a36c0fb3d4b788da21696b499af257548373b0e3769e1ca0f214754b276a39a33bc9679bf53d73baf20361228c8c4002a
a31acb4b47af604c8",
  "msLAPS-EncryptedPasswordHistory": [
    "4ae6d901f5d3d9bcdc040000000000003082044606092a864886f70d010703a0820437308204330201023182 3ffa28203fb0201043
0fbfa66c085c232b42fcecb5550803000014000000140000004448504200010000087a8e61db4b6663cffbbd19c651959998ceef608660dd0
4296d830e9a7c209e0c6497517abd5a8a9d306bcf67ed91f9e6725b4758c022e0b1ef4275bf7b6c5bfc11d45f9088b941f54eb1e59bb8bc3
51bfa4ab3ad8347796524d8ef6a167b5a41825d967e144e5140564251ccacb83e6b486f6b3ca3f7971506026c0b857f689962856ded4010a
15f693877fad7ef09cadb094ae91e1a15973fb32c9b73134d0b2e77506660edbd484ca7b18f21ef205407f4793a1a0ba12510dbc15077be4
```

Features & examples

SYNACKTIV

- **LAPSv2**

```
>>> jq '{cn, "msLAPS-PasswordExpirationTime", "msLAPS-EncryptedPassword_", "msLAPS-EncryptedPasswordHistory_"}' \
>       out/bcf5b328255cc214f14a2cf396ce0a76/computer.json
{
  "cn": "EX",
  "msLAPS-PasswordExpirationTime": "2023-10-15T16:11:51.477503+00:00",
  "msLAPS-EncryptedPassword_": {
    "n": "Administrator",
    "t": "2023-09-15T16:11:51.477503+00:00",
    "p": "6tuf2mz$.ZAOp3"
  },
  "msLAPS-EncryptedPasswordHistory_": [
    {
      "n": "Administrator",
      "t": "2023-09-13T14:01:05.450085+00:00",
      "p": "0e08}XAQx{yFXj"
    },
    {
      "n": "Administrator",
      "t": "2023-09-13T14:01:07.915447+00:00",
      "p": "7QVFYpBbRY@P2A"
    },
    {
      "n": "Administrator",
      "t": "2023-09-15T16:02:05.566803+00:00",
      "p": "3$fGs-95+Pb&(Q"
    }
  ]
```

Features & examples

SYNACKTIV

- **Domain trusts (NT hash)**

```
>>> jq '{trustPartner, trustType, trustAttributes, trustAuthIncoming}' \
        out/bcf5b328255cc214f14a2cf396ce0a76/trustedDomain.json
{
  "trustPartner": "corp.local",
  "trustType": 2,
  "trustAttributes": 8,
  "trustAuthIncoming": {
    "count": 2,
    "authInfo": [
      {
        "lastUpdateTime": "2022-10-13T04:19:50.569931+00:00",
        "authType": "TRUST_AUTH_TYPE_CLEAR",
        "authInfo": "1bb3fcff5446bca271e2a1b7067f6ad082e8e38766504b28a454a66e78ee9f123f
4dd8e3a856e385026bf339c9c43dc993c73c3eba46eeb3604a151bcbf6a3258e67ba98e5679fb58d4e13ea5
d99858e411fac53f775d714c000d010b11b9822fe1d32b73af0253b3c11ec8671c95a0b5c88c979a448a71c
        "authInfo_RC4-HMAC": "fbf117cf4c10500638fb0a28e769f8df"
      },
      {
        "lastUpdateTime": "2022-10-13T04:19:50.569931+00:00",
        "authType": "TRUST_AUTH_TYPE_VERSION",
        "authInfo": "2a000000"
      }
    ],
    "previousAuthInfo": [
```

Features & examples

SYNACKTIV

- **Domain trusts (Kerberos keys)**
  - User objects with flag INTERDOMAIN_TRUST_ACCOUNT

```
>>> jq 'select(.cn == "CORP$") | {sAMAccountName, userAccountControl, unicodePwd, supplementalCredentials}' \
        out/bcf5b328255cc214f14a2cf396ce0a76/user.json
{
  "sAMAccountName": "CORP$",
  "userAccountControl": "PASSWD_NOTREQD | INTERDOMAIN_TRUST_ACCOUNT",
  "unicodePwd": "fbf117cf4c10500638fb0a28e769f8df",
  "supplementalCredentials": {
    "Primary:Kerberos-Newer-Keys": [
      "aes256-cts-hmac-sha1-96:7294412a8e76f9af2dba00173de94f685542abf204795ac1ea34d487a905dd48",
      "aes128-cts-hmac-sha1-96:740644f320676c97f776f331b4256750",
      "des-cbc-md5:b3eee8d8657e9dbd"
    ],
    "Primary:Kerberos": [],
    "Packages": [
      "NTLM-Strong-NTOWF",
      "Kerberos-Newer-Keys",
      "Kerberos",
      "WDigest"
    ],
    "Primary:WDigest": [
      "6e6527082f9b583fa3493b5f808ffb66",
```

Features & examples

SYNACKTIV

- **Internal cache system**
  - Dump of security descriptors from **sd_table**
  - Extraction of links and backlinks from **link_table**
  - Formatting of all records in **datatable**
    - Name resolution: **objectClassSchema** and **attributeSchema**
    - Secrets decryption: **Pek-List** for the first layer of encryption
    - **KDSRootKeys** for **MS-GKDI** : used by LAPSv2

Features & examples

SYNACKTIV

- **Unattended feature**
  - ADAM NTDS support: **AD LDS** uses variant of NTDS structure
- **Ad-hoc scripts available**
  - user_to_secretsdump.py
    Parse JSON files to get **secretsdump** formatted hashes
  - convert_to_bloodhound.py (soon)
    Parse JSON files to create Bloodhound formatted JSON files

Conclusion

Conclusion

SYNACKTIV

- **Issues**
  - First version was very slow
    - PR to **dissect.esedb** improved by 10x the processing speed
  - Compression algorithms
    - **XPRESS10** not yet implem (no open-source implem, PR welcomed)
  - Bloodhound
    - Minimal / outdated documentation, custom field naming, etc.
    - It is a rocky road!

Conclusion

SYNACKTIV

- **ntdissector**
  - **Dump records** as flat files with JSON objects
  - **Decent performances** on large databases
  - **Seamless decryption** and formatting of secrets
  - **Versatile** usage for offensive and defensive teams
  - **Simple** usage, easy to integrate in other tools
- **Public release**
  - https://github.com/synacktiv/ntdissector
  - Contributions welcomed

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com