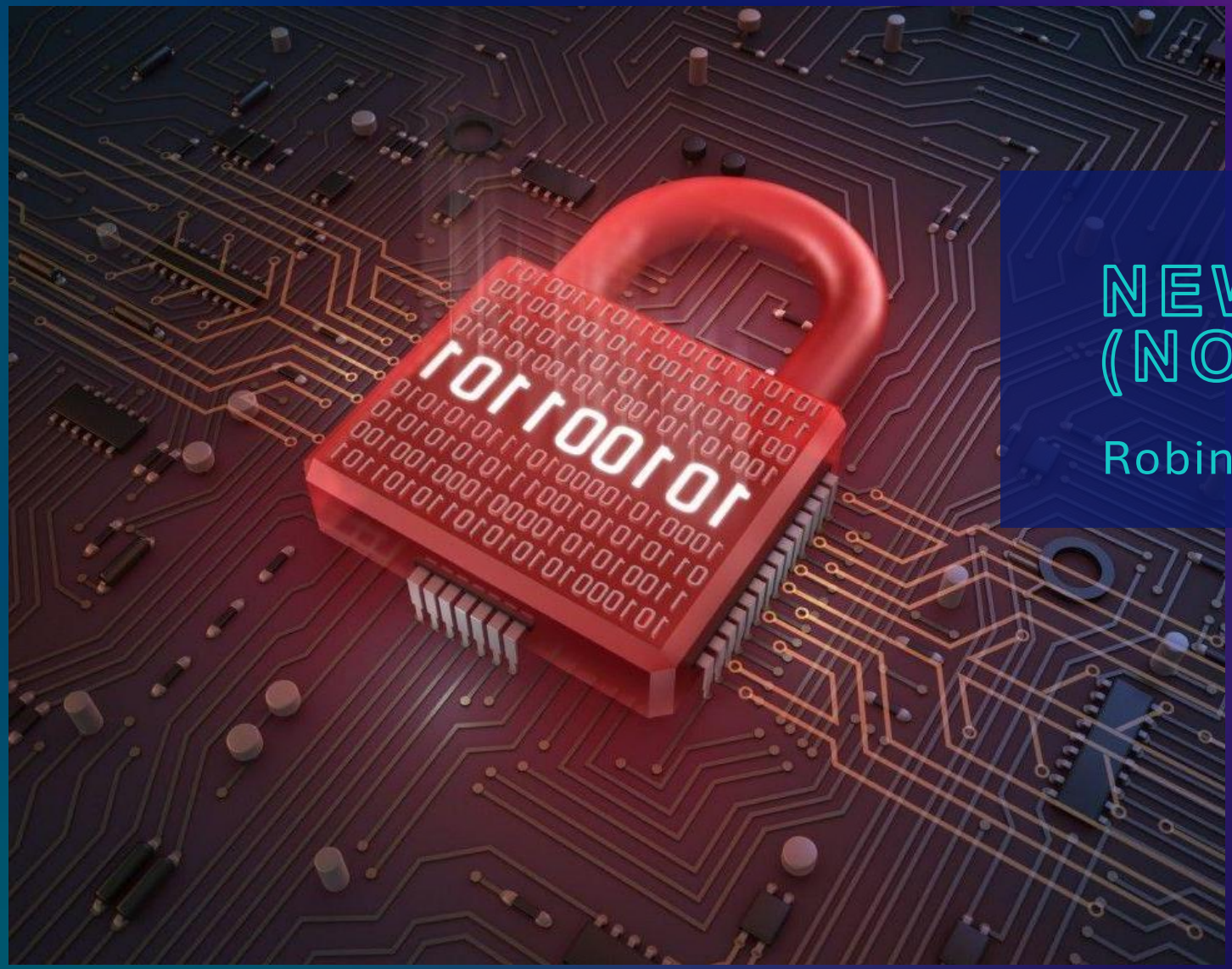


NEW PENTEST TOOLS (NOVEMBER 2022)

Robin

D4TA-HUNTER

https://github.com/micro-joan/D4TA-HUNTER

PYCRYPT - PYTHON BASED CRYPTER THAT CAN BYPASS ANY KINDS OF ANTIVIRUS PRODUCTS

https://github.com/machine1337/pycrypt

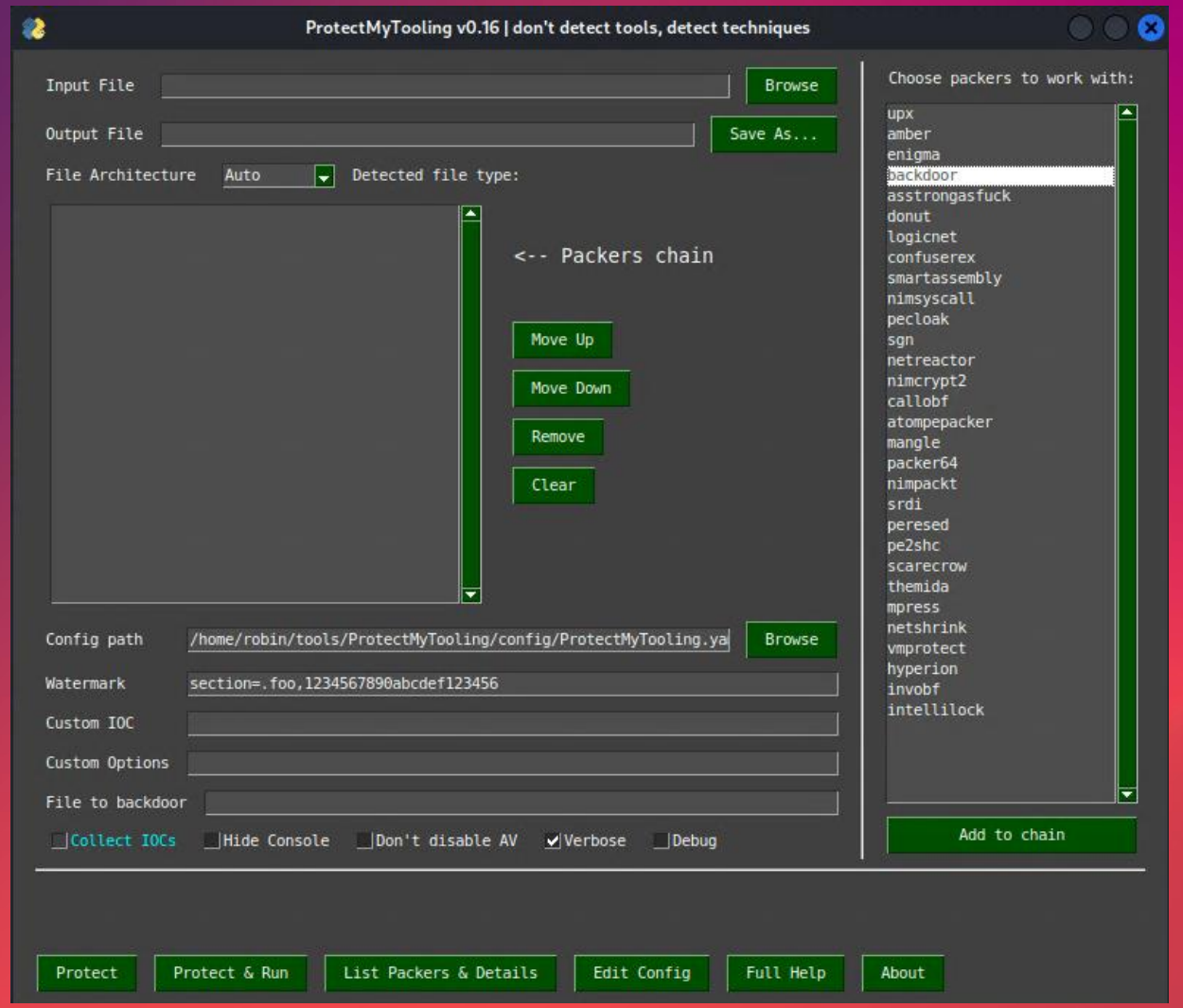
PROTECTMYTOOLING - MULTI-PACKER WRAPPER

```
:::::::::::::::..      ...  ::::::::::::,::::::  .,-:::::::::::::::
 `;;;```.;;;;;;;``;;;;  .;;;;;;;;;;;;;;;;;;;;;;;;;;;'''''`;;;;;;;;
  `]]nnn]]' [[[,/[[[' ,[[     \[[,  [[     [[cccc [[[           [[
   $$$""    $$$$$$c   $$$,     $$$  $$     $$""""" $$$          $$
   888o     888b "88bo"888,_ _,88P  88,    888oo,_`88bo,__,o,   88,
.  YMMMb :.-:.MM   ::-. "YMMMMMP"   MMM    """"YUMMM"YUMMMMMP"  MMM
;;,.    ;;;';;.   ;;;;'
[[[[, ,[[[[, '[[,[[['
$$$$$$$$"$$$   c$$"
888 Y88" 888o,8P"`
::::::::::::mM...        ...     :::    :::::.    :::. .,-:::::/
;;;;;;;;.;;;;;;;.  .;;;;;;;;.  ;;;    ;;`;;;;,  `;;,;;;-'````'
     [[   ,[[     \[[,[[     \[[,[[[    [[[ [[[[[. '[[[[   [[[[[[/
     $$   $$$,     $$$$$,     $$$$$'    $$$ $$$ "Y$c$"$$c.    "$$
     88,  "888,_ _,88"888,_ _,88o88oo,._888 888    Y88`Y8bo,,,o88o
     MMM    "YMMMMMP"  "YMMMMMP"""""YUMMMMM MMM     YM  `'YMUP"YMM

Red Team implants protection swiss knife.

Multi-Packer wrapping around multitude of packers, protectors, shellcode loaders, encoders.
```

https://github.com/mgeeky/ProtectMyTooling



EVILTREE - A REMAKE OF THE CLASSIC "TREE"

https://github.com/t3l3machus/eviltree

```
C:\Users\pxart\Desktop>python3 eviltree.py -r C:\Users\kostas -k passw,admin,account,login,user -L 3 -v

 ▄▄▄ ▄ ▄ ▄ ▄ ▄▄▄ ▄▄▄ ▄▄▄ ▄▄▄
 ▀▀▀ ▀▄▀ ▀ ▀ ▀▀▀ ▀▀▀ ▀▀▀ ▀▀▀
                by t3l3machus

C:\Users\kostas\
├── NTUSER.DAT
├── NTUSER.DAT{fd93a27f-14fb-11ec-bebb-544f503b0403}.TM.blf
├── NTUSER.DAT{fd93a27f-14fb-11ec-bebb-544f503b0403}.TMContainer00000000000000000001.regtrans-ms
├── NTUSER.DAT{fd93a27f-14fb-11ec-bebb-544f503b0403}.TMContainer00000000000000000002.regtrans-ms
├── ntuser.dat.LOG1
├── ntuser.dat.LOG2
├── ntuser.ini
├── 3D Objects
│   └── desktop.ini
├── AppData
│   ├── Local
│   │   ├── IconCache.db
│   │   ├── Application Data [error accessing dir]
│   │   ├── Avast Software
│   │   ├── CEF
│   │   ├── Comms
│   │   ├── ConnectedDevicesPlatform
│   │   ├── D3DSCache
│   │   ├── Google
│   │   ├── History [error accessing dir]
│   │   ├── Microsoft
│   │   ├── NVIDIA
│   │   ├── NVIDIA Corporation
│   │   ├── Packages
│   │   ├── PeerDistRepub
│   │   ├── PlaceholderTileLogoFolder
│   │   ├── Publishers
│   │   ├── Temp
│   │   ├── Temporary Internet Files [error accessing dir]
│   │   └── VirtualStore
│   └── LocalLow
│       └── Microsoft
├── Application Data [error accessing dir]
├── Contacts
│   └── desktop.ini
├── Cookies [error accessing dir]
├── Desktop
│   ├── Google Chrome.lnk
│   ├── Microsoft Edge.lnk
│   └── desktop.ini
├── Documents
│   ├── desktop.ini
│   ├── My Music [error accessing dir]
│   ├── My Pictures [error accessing dir]
│   ├── My Videos [error accessing dir]
│   └── mystuff
│       └── creds.csv [passw, admin, account]
├── Downloads
│   └── desktop.ini
├── Favorites
│   ├── Bing.url
│   ├── desktop.ini
│   └── Links
│       └── desktop.ini
```

WODAT - WINDOWS ORACLE DATABASE ATTACK TOOLKIT

```
WODAT - Windows Oracle Testing Toolkit
@initroot
################################################
[!] -- Socket connection established to target
[!] -- Checking if 192.168.10.207:1521 is a working TNS listener...
TNS Connection string mode enabled and SID used for connection string
Oracle connection string: user id=ERTUICS;password=PASSWD;data source=(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=192.168.10.207)(PORT=1521)
[!] -- SUCCESS Working TNS listener. Continue...
[?] -- Please provide location to file for testing:
> D:\TestCreds.txt
[?] -- Please select which type of file has been provided:
 A - Username:Password
 B - Usernames
 C - Passwords
 D - Username as Pass
> a
[!] -- Now attempting to connect using [7] unique credential combos...
        Testing: admin:admin    State: ORA-01017: invalid username/password; logon denied
        Testing: user:pass      State: ORA-01017: invalid username/password; logon denied
        Testing: CE:CE          State: ORA-01017: invalid username/password; logon denied
        Testing: SYS:1234       State: Potential SYSDBA or SYSOPER account found, manually confirm..
[!] -- DB Connection Success!
        Testing: system:1234    State: Success!
        Testing: CLARK:CLOTH    State: ORA-01017: invalid username/password; logon denied
```

https://github.com/InitRoot/wodat

LIST OF THE BEST SQL INJECTION TOOLS

SQLMap - Automatic SQL Injection And Database Takeover Tool
jSQL Injection - Java Tool For Automatic SQL Database Injection
BBQSQL - A Blind SQL Injection Exploitation Tool
NoSQLMap - Automated NoSQL Database Pwnage
Whitewidow - SQL Vulnerability Scanner
DSSS - Damn Small SQLi Scanner
explo - Human And Machine Readable Web Vulnerability Testing Format
Blind-Sql-Bitshifting - Blind SQL Injection via Bitshifting
Leviathan - Wide Range Mass Audit Toolkit
Blisqy - Exploit Time-based blind-SQL injection in HTTP-Headers (MySQL/MariaDB)

ARSENAL

https://github.com/Orange-Cyberdefense/arsenal

SOURCES

D4TA-HUNTER : https://github.com/micro-joan/D4TA-HUNTER

PROTECTMYTOOLING : https://github.com/machine1337/pycrypt

EVILTREE : https://github.com/t3l3machus/eviltree

WODAT : https://github.com/InitRoot/wodat

ARSENAL : https://github.com/Orange-Cyberdefense/arsenal

A avoir absolument dans vos favoris ! ↓↓↓↓↓↓↓

https://www.kitploit.com/

MERCI POUR VOTRE ATTENTION!