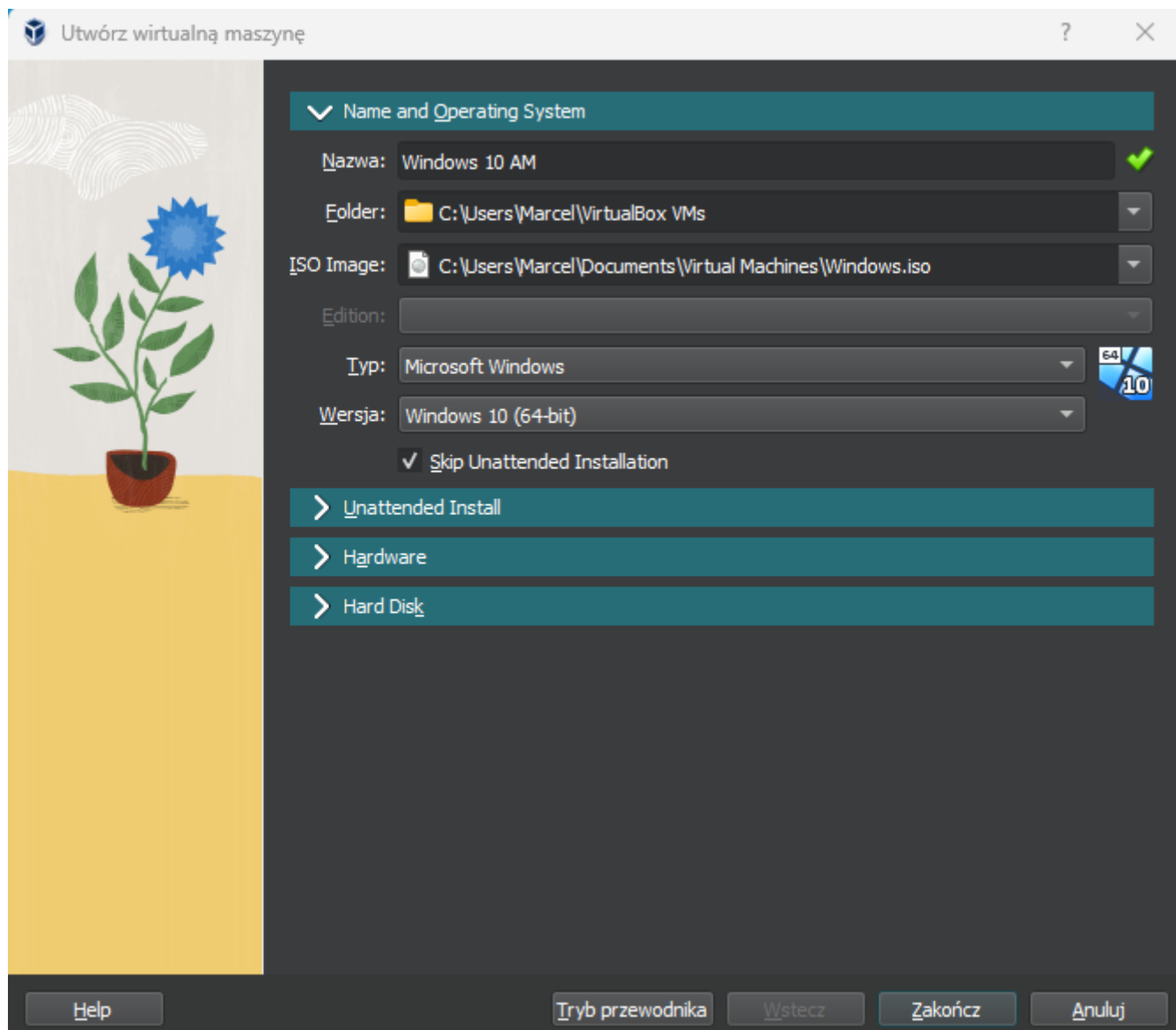


# Przygotowanie środowiska do Analizy Malware

## Instalacja Systemu Windows 10

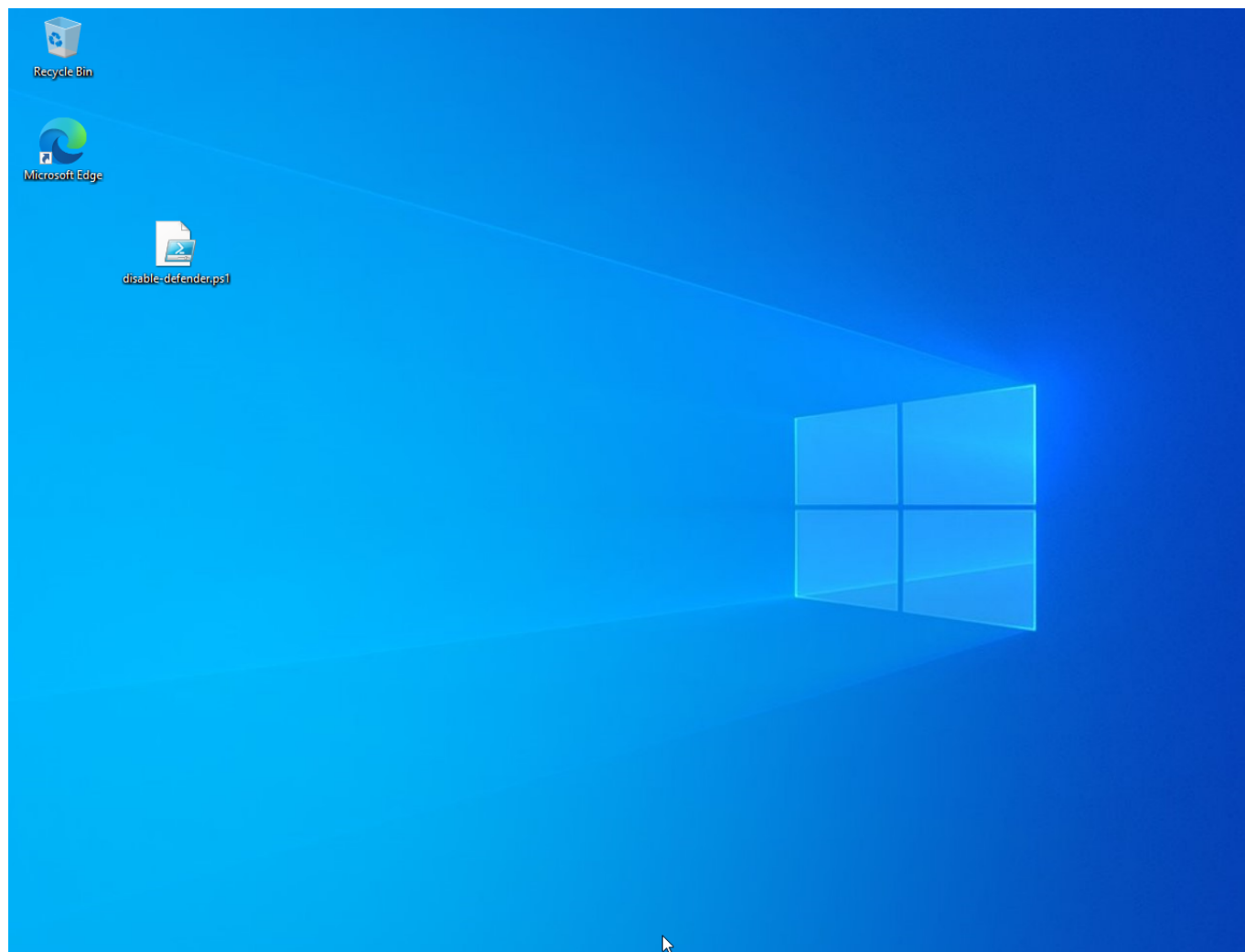


Dla systemu windows należy przeznaczyć conajmniej 60 GB miejsca na dysku  
Ja przeznaczyłem:

- 80 GB miejsca na dysku
- 8 GB pamięci RAM
- 6 wątków procesora

Następnie należy przejść przez proces instalacji

Po udanej instalacji mamy gotowy system Windows 10



## Instalacja Flare VM

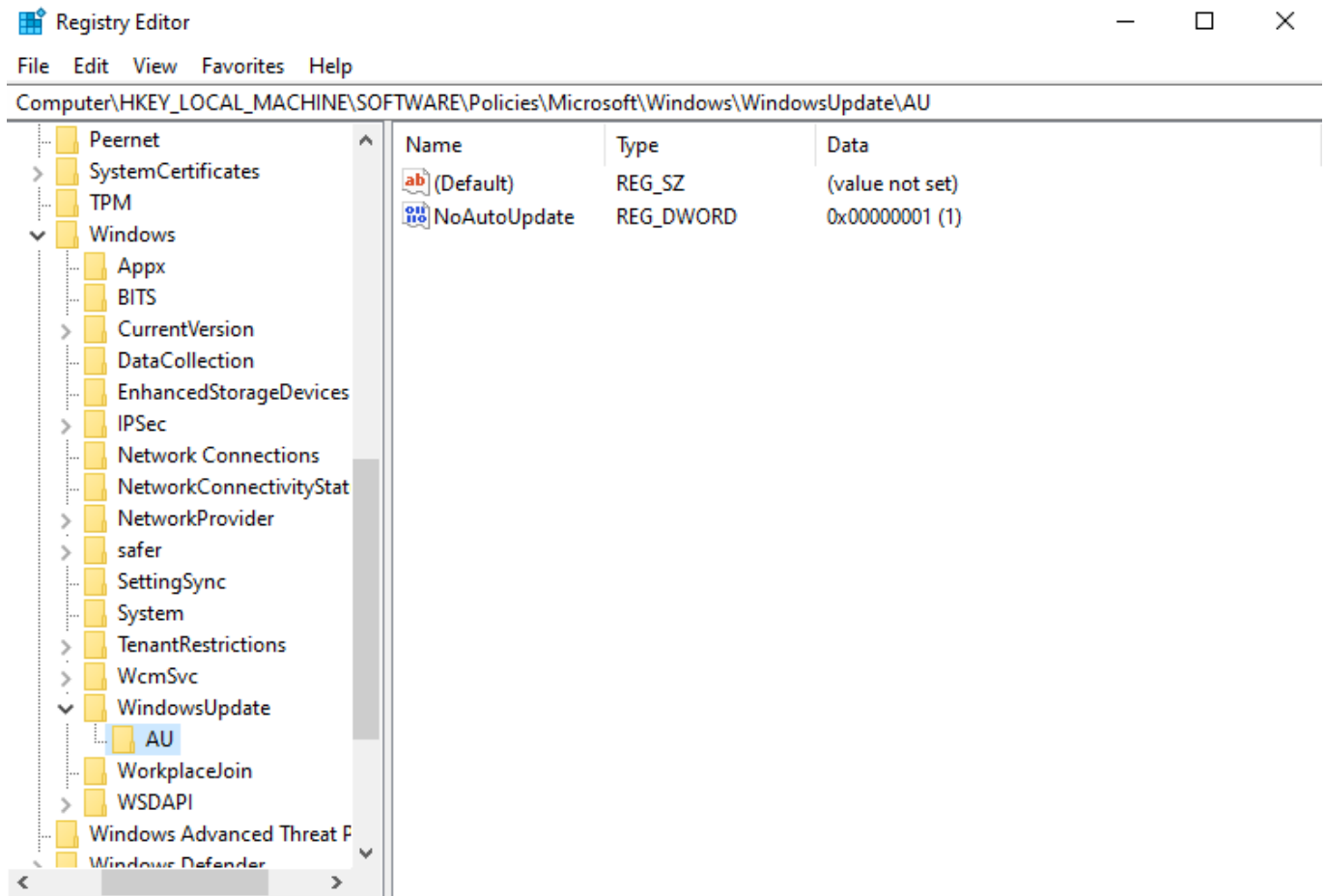
Zanim zainstaluje się środowisko Flare VM, należy przejść przez kilka kroków

### Wyłączenie Windows Update

Windows Update można wyłączyć na 2 sposoby

- Group Policy Edit (Wymagany Windows Pro)
- Windows Registry

Ja miałem problem z użyciem GPE, dlatego dodałem klucz do rejestru za pomocą [poradnika](#)



## Wyłączenie Tamper Protection

Prevents others from tampering with important security features.

This change requires you to restart your device.

Real-time protection is off, leaving your device vulnerable.

[Some of your files have been affected by ransomware.](#)

☐ Off

## Wyłączenie Windows Defender

Ostatnim krokiem przed instalacją Flare VM jest wyłączenie Windows Defendera

Posłużyłem się do tego [skryptem](#), który automatycznie go wyłącza

```
Administrator: Windows PowerShell
[+] Disable Windows Defender (as desktop-dvmrcp1\marcel)
[i] PsExec not found, will continue as Administrator
[+] Add exclusions
[+] Disable scanning engines (Set-MpPreference)
[+] Set default actions to Allow (Set-MpPreference)
[+] Disable services
[i] Disable service WdNisSvc (next reboot)
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\Users\Marcel\Desktop\disable-defender.ps1:114 char:13
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Se ...
+ CategoryInfo          : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[i] Disable service WinDefend (next reboot)
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\Users\Marcel\Desktop\disable-defender.ps1:114 char:13
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Se ...
+ CategoryInfo          : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[i] Disable service Sense (next reboot)
[+] Disable drivers
[i] Disable driver WdNisDrv (next reboot)
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\Users\Marcel\Desktop\disable-defender.ps1:135 char:13
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Se ...
+ CategoryInfo          : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[i] Disable driver Wdfilter (next reboot)
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\Users\Marcel\Desktop\disable-defender.ps1:135 char:13
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Se ...
+ CategoryInfo          : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[i] Disable driver Wdboot (next reboot)
Set-ItemProperty : Attempted to perform an unauthorized operation.
At C:\Users\Marcel\Desktop\disable-defender.ps1:135 char:13
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Se ...
+ CategoryInfo          : PermissionDenied: (Start:String) [Set-ItemProperty], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.SetItemPropertyCommand

[+] WinDefend Service still running (reboot required)
[+] This script will be started again after reboot.
Press any key to continue: _
```

Skrypt potrzebuje 5 cykli restartowania, aby wyłączyć Windows Defender całkowicie

```
[+] Disable Windows Defender (as desktop-dvmrcp1\marcel)
[i] PsExec not found, will continue as Administrator
[+] Add exclusions
[+] Disable scanning engines (Set-MpPreference)
[+] Set default actions to Allow (Set-MpPreference)
[+] Disable services
[i] Disable service WdNisSvc (next reboot)
[i] Disable service WinDefend (next reboot)
[i] Service Sense already disabled
[+] Disable drivers
[i] Disable driver WdNisDrv (next reboot)
[i] Disable driver Wdfilter (next reboot)
[i] Disable driver Wdboot (next reboot)
[+] WinDefend Service still running (reboot required)
[+] This script will be started again after reboot.
Press any key to continue: _
```

Skrypt powinien bez problemów wyłączyć Windows Defender

Flare VM

Aby zainstalować Flare VM, sklonowałem repo, wykonałem polecenia z instrukcji instalacji, a następnie włączyłem skrypt

```
Mode                LastWriteTime         Length Name
-----
d-----          3/9/2023   7:25 PM                flare-vm-4

PS C:\Users\Marcel\Desktop\flare-vm-4> cd .\flare-vm-4\
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> ls

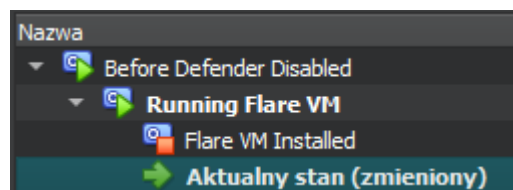
Directory: C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4

Mode                LastWriteTime         Length Name
-----
-a-----          3/9/2023   7:25 PM           550 .gitattributes
-a-----          3/9/2023   7:25 PM           469 .gitignore
-a-----          3/9/2023   7:25 PM        1851 config.xml
-a-----          3/9/2023   7:25 PM       13129 flarevm.png
-a-----          3/9/2023   7:25 PM       45869 install.ps1
-a-----          3/9/2023   7:25 PM      162897 installer_gui.png
-a-----          3/9/2023   7:25 PM         9192 LICENSE.txt
-a-----          3/9/2023   7:25 PM       12466 README.md

PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> Unblock-File .\install.ps1
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): a
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> .\install.ps1 -password 1234
[+] Checking if script is running as administrator...
[+] Running as administrator
[+] Checking if execution policy is unrestricted...
[+] Execution policy is unrestricted
[+] Checking if Windows Defender Tamper Protection is disabled...
[+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
[+] Defender is disabled
[+] Checking to make sure Operating System is compatible...
[!] Windows version 19045 has not been tested. Tested versions: 17763, 19042
[+] You are welcome to continue, but may experience errors downloading or installing packages
[-] Do you still wish to proceed? (Y/N): y
[+] Checking if host has enough disk space...
[+] Disk is larger than 60 GB
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N):
```

Skrypt upewnia się, że zrobiliśmy migawkę (snapshota) przed instalacją



Skrypt instaluje teraz Boxstartera oraz Chocolatey

```

Administrator: Windows PowerShell

Mode                LastWriteTime         Length Name
----                -
Expand-Archive
The archive file 'C:\Users\Marcel\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip' expansion is in progress...
[ooooooooooooooooooooo]

-a----             3/9/2023   7:25 PM           9192 LICENSE.txt
-a----             3/9/2023   7:25 PM          12466 README.md

PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> Unblock-File .\install.ps1
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?linkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): a
PS C:\Users\Marcel\Desktop\flare-vm-4\flare-vm-4> .\install.ps1 -password 1234
[+] Checking if script is running as administrator...
    [+] Running as administrator
[+] Checking if execution policy is unrestricted...
    [+] Execution policy is unrestricted
[+] Checking if Windows Defender Tamper Protection is disabled...
    [+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
    [+] Defender is disabled
[+] Checking to make sure Operating System is compatible...
    [!] Windows version 19045 has not been tested. Tested versions: 17763, 19042
    [+] You are welcome to continue, but may experience errors downloading or installing packages
[-] Do you still wish to proceed? (Y/N): y
[+] Checking if host has enough disk space...
    [+] Disk is larger than 60 GB
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): y
[+] Installing Boxstarter...
Welcome to the Boxstarter Module installer!
Chocolatey is going to be downloaded and installed on your machine. If you do not have the .NET Framework Version 4 or g
reater, that will also be downloaded and installed.
Forcing web requests to allow TLS v1.2 (Required for requests to Chocolatey.org)
Getting latest version of the Chocolatey package for download.
Not using proxy.
Getting Chocolatey from https://community.chocolatey.org/api/v2/package/chocolatey/1.3.0.
Downloading https://community.chocolatey.org/api/v2/package/chocolatey/1.3.0 to C:\Users\Marcel\AppData\Local\Temp\choco
latey\chocoInstall\chocolatey.zip
Not using proxy.
Extracting C:\Users\Marcel\AppData\Local\Temp\chocolatey\chocoInstall\chocolatey.zip to C:\Users\Marcel\AppData\Local\Te
mp\chocolatey\chocoInstall

```

Okienko z wyborem narzędzi do zainstalowania

FLARE VM Install Customization

Welcome to FLARE VM's custom installer. Please select your options below.  
Default values will be used if you make no modifications.

Environment Variable Customization

%VM\_COMMON\_DIR%

%ProgramData%\\_VM

Select Folder

Shared module and metadata for VM (e.g., config, logs, etc...)

%TOOL\_LIST\_DIR%

%ProgramData%\Microsoft\Windows\Start Menu\Programs\Tools

Select Folder

Folder to store tool categories and shortcuts

%TOOL\_LIST\_SHORTCUT%

%UserProfile%\Desktop\Tools.lnk

Select Folder

Shortcut to %TOOL\_LIST\_DIR%

%RAW\_TOOLS\_DIR%

%SystemDrive%\Tools

Select Folder

Folder to store downloaded tools

Note:

Metapackages may install in a different location (package author's decision)

Metapackages are wrappers around tools that install via dependencies

Package Installation Customization

Available to Install

asreproast.vm

bloodhound.vm

bytecodeviewer.vm

cutter.vm

dependencywalker.vm

exeinfope.vm

exiftool.vm

fiddlerclassic.vm

file.vm

gobuster.vm

hollowshunter.vm

hxd.vm

libraries.python2.vm

networkminer.vm

nmap.vm

npcap.vm

ollydbg.scyllahide.vm

ollydbg2.scyllahide.vm

pebear.vm

pestudio.vm

sctdbg.vm

setdllcharacteristics.vm

sqlrecon.vm

ybddec.vm

Total: 26

To Install

010editor.vm

7zip-15-05.vm

apimonitor.vm

apktool.vm

capa.vm

cmder.vm

cyberchef.vm

cygwin.vm

die.vm

dnspyex.vm

explorersuite.vm

fakenet-ng.vm

floss.vm

ghidra.vm

hashmyfiles.vm

idafree.vm

libraries.python3.vm

map.vm

notepadplusplus.vm

notepadpp.plugin.compare.vm

ollydbg.ollydumpex.vm

ollydbg.vm

ollydbg2.ollydumpex.vm

ollydbg2.vm

Total: 35

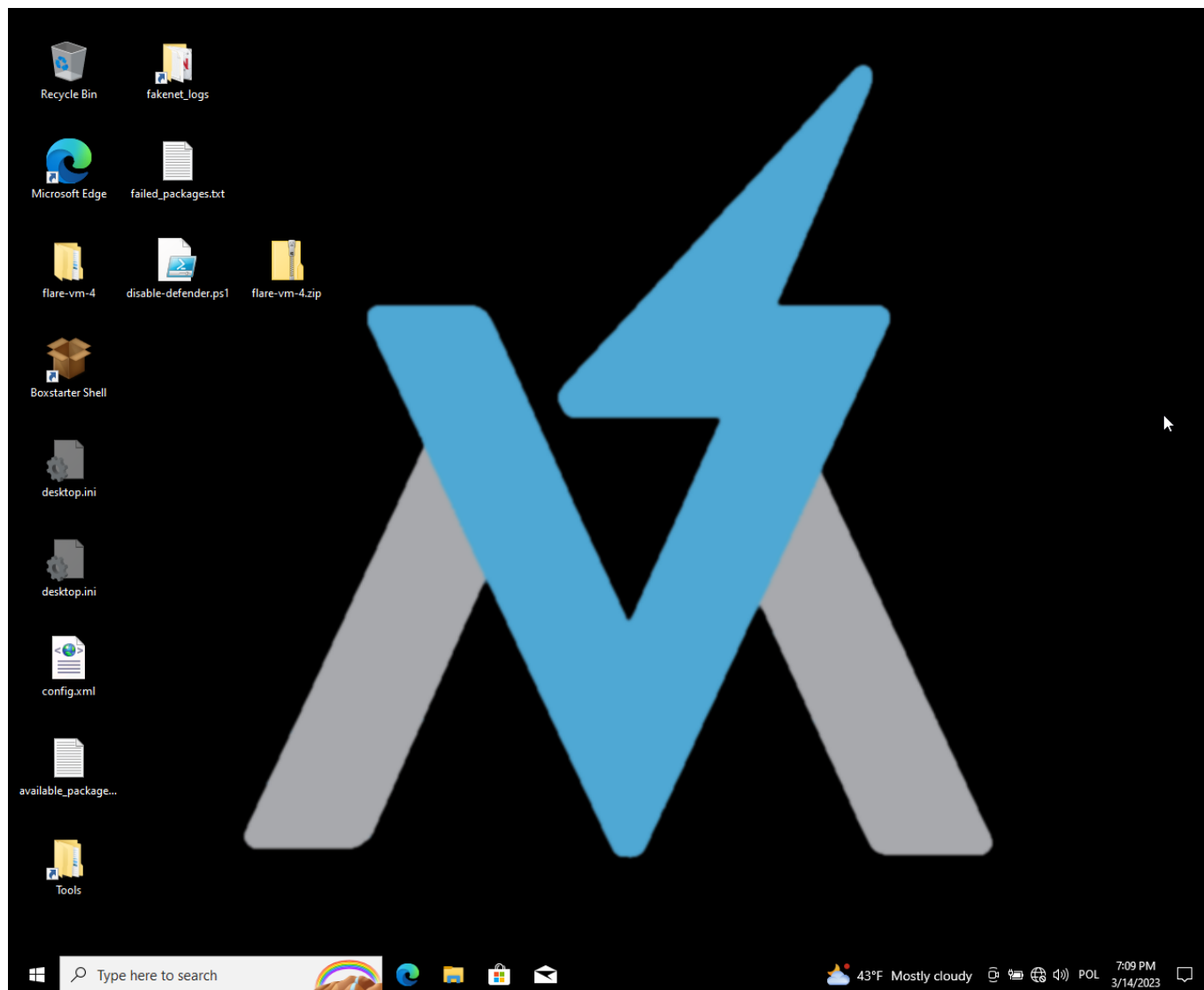
Reset

OK

Cancel

Po wyborze narzędzi została przeprowadzona instalacja narzędzi, która potrwała kilkadziesiąt minut

Po instalacji tak powinno wyglądać gotowe środowisko

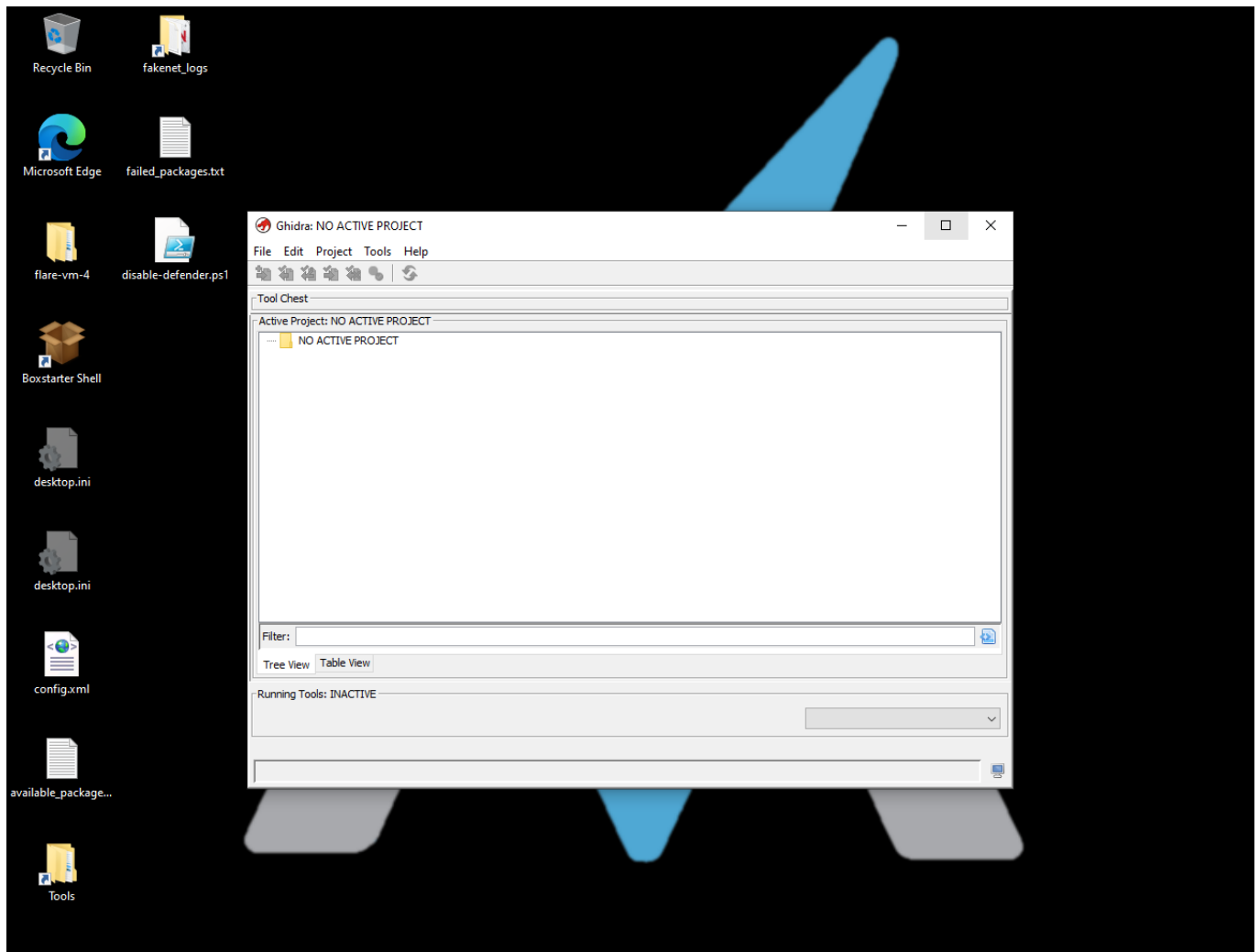


## Pozostałe kroki

### Ghidra

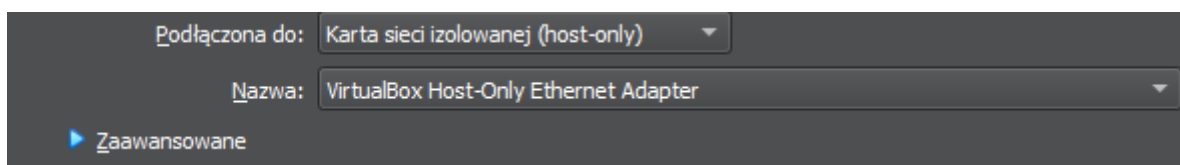
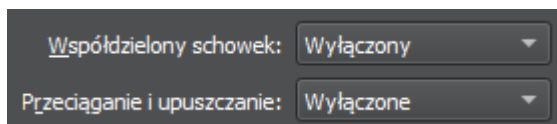
Programu Ghidra nie trzeba pobierać, ponieważ został już zainstalowany wraz z Flare VM





## Izolacja Maszyny

Aby malware nie miał dostępu do Hosta należy go od niego jak najbardziej odseparować



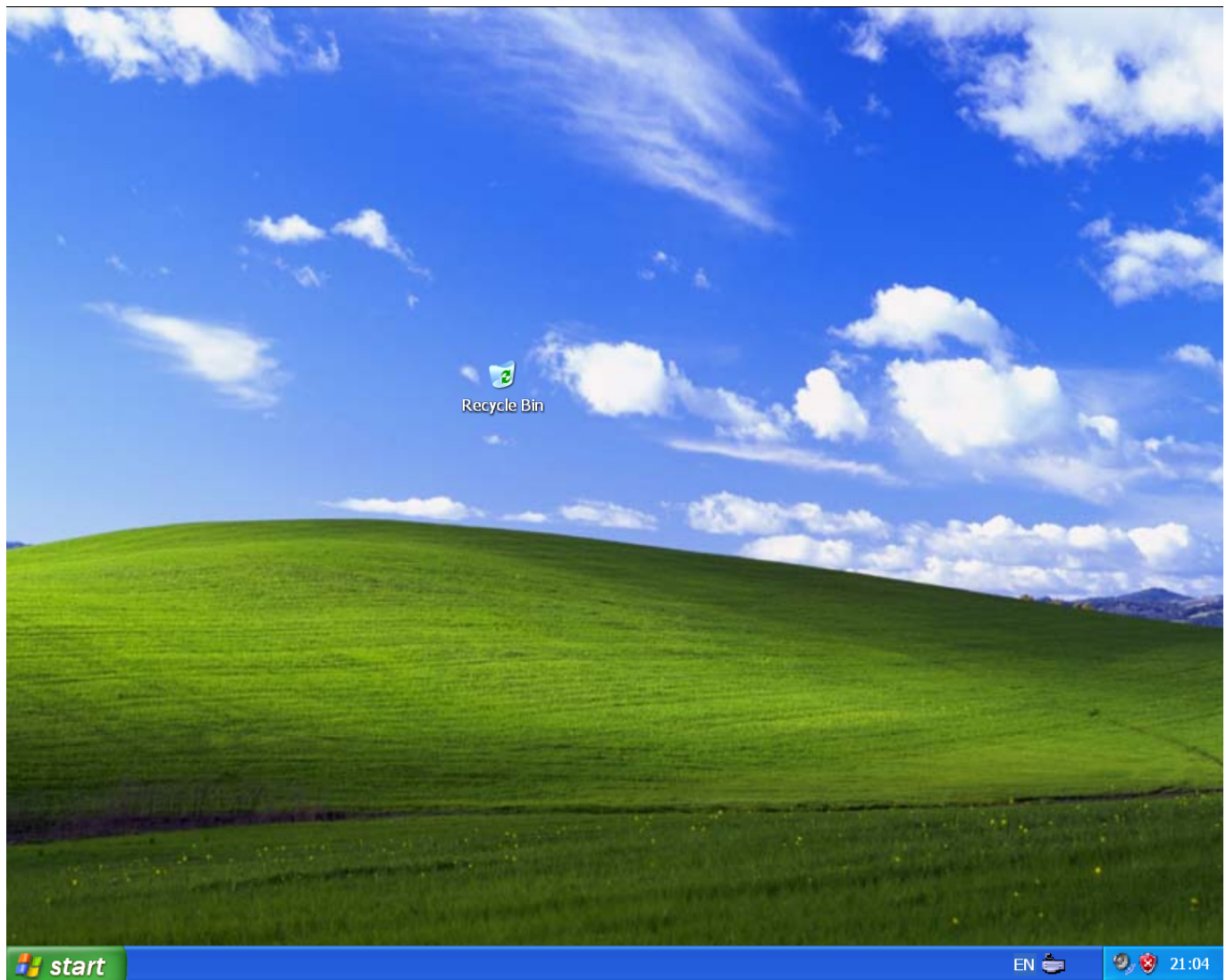
## Windows XP

Na potrzeby labów 3+ zainstalowałem również [Windows XP](#)

Do aktywacji użyłem klucza

B2RBK-7KPT9-4JP6X-QQFWM-PJD6G

*Klucz działa dla każdej instalacji Windowsa XP*



## Podsumowanie

- Windows Defender wyłączony
- Maszyna FlareVM do analizy malware została zainstalowana bez problemów
- Maszyna jest odizolowana od sieci oraz systemu Hosta
- Potrzebne narzędzia zostały zainstalowane
- Windows XP zainstalowany