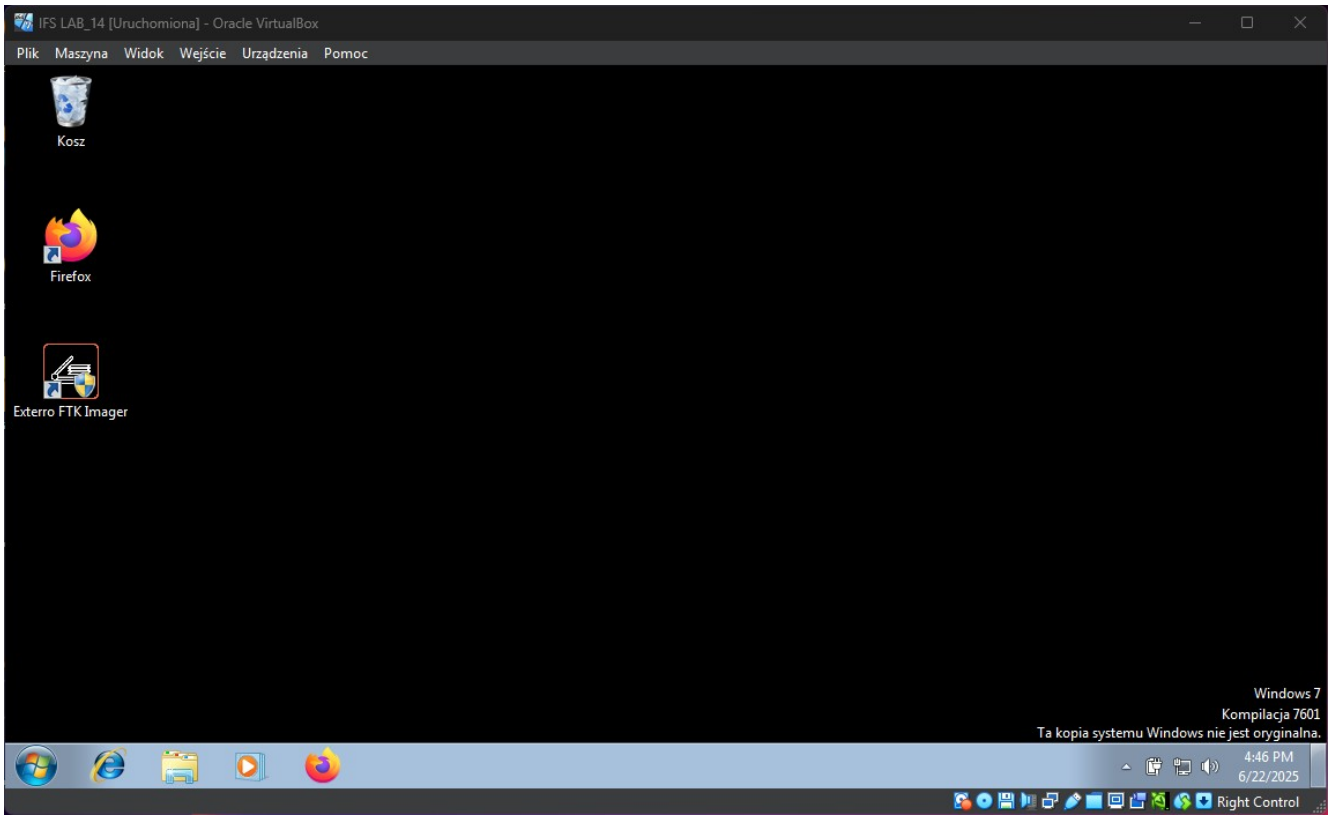
POLITECHNIKA WROCŁAWSKA Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 14	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 16.06.2025	
Data oddania sprawozdania: 22.06.2025	

1. Cel ćwiczenia

Analiza powłamaniowa – pozyskanie i zabezpieczenie dowodów cyfrowych

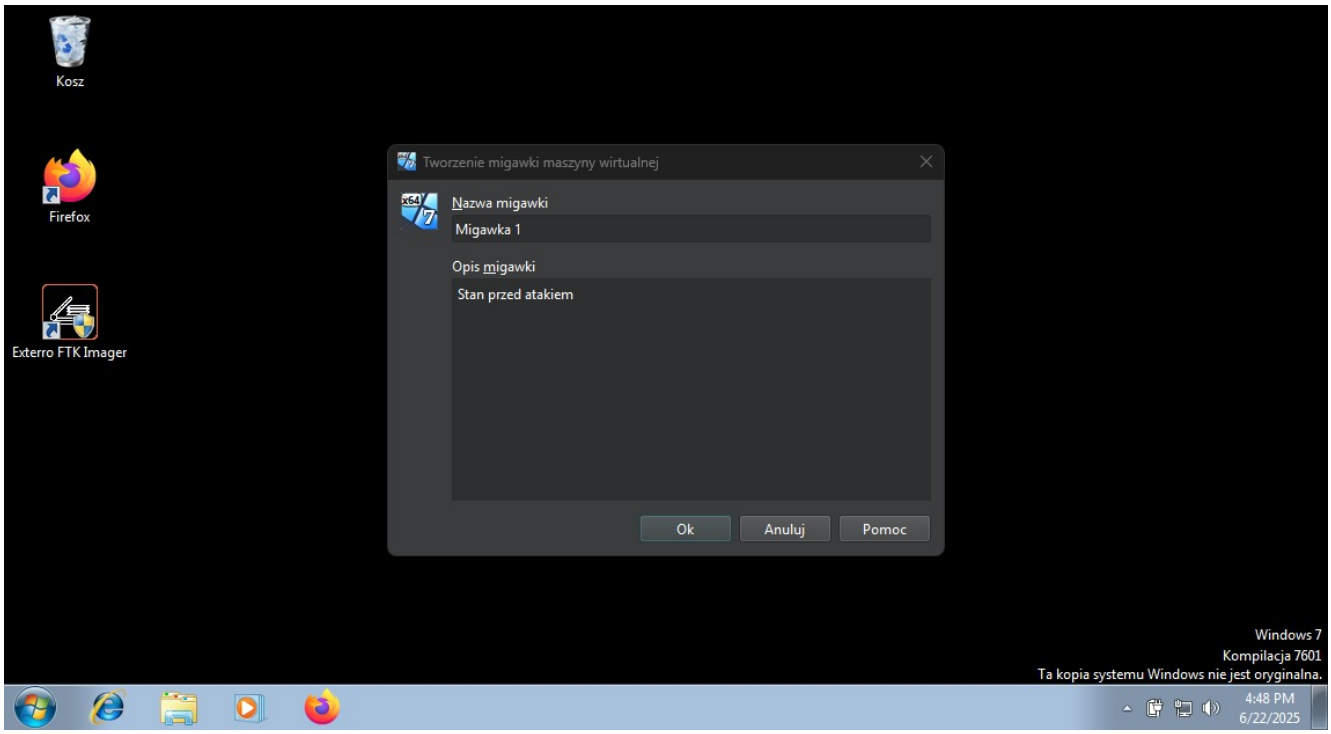
2. Realizacja zadań laboratoryjnych

Zadanie 1. Upewnij się, że ćwiczenie wykonujesz w środowisku testowym (np. maszynie wirtualnej).



Rysunek 1: windows 7 na maszynie wirtualnej

Zadanie 2. Wykonaj snapshot maszyny wirtulanej.

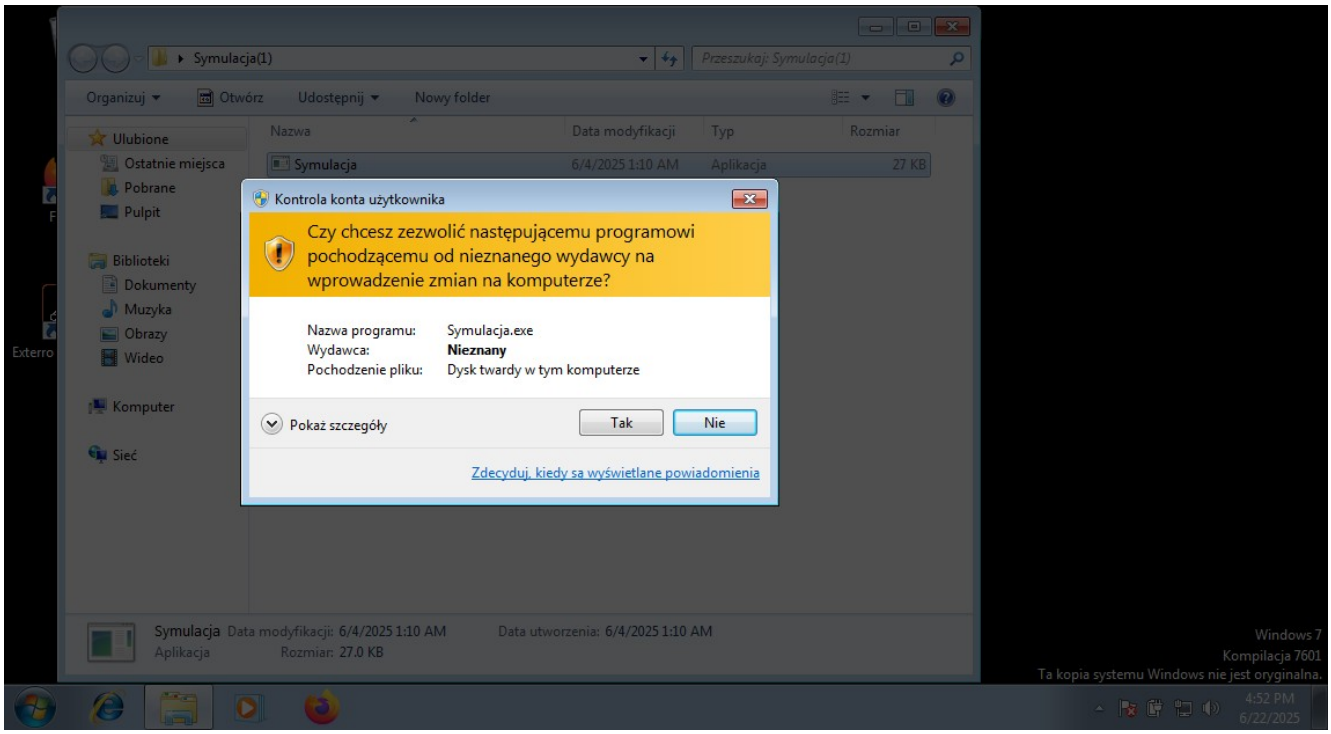


Rysunek 2: tworzenie migawki

Zadanie 3a. Uruchom skrypt Symulacja.exe jako administrator:

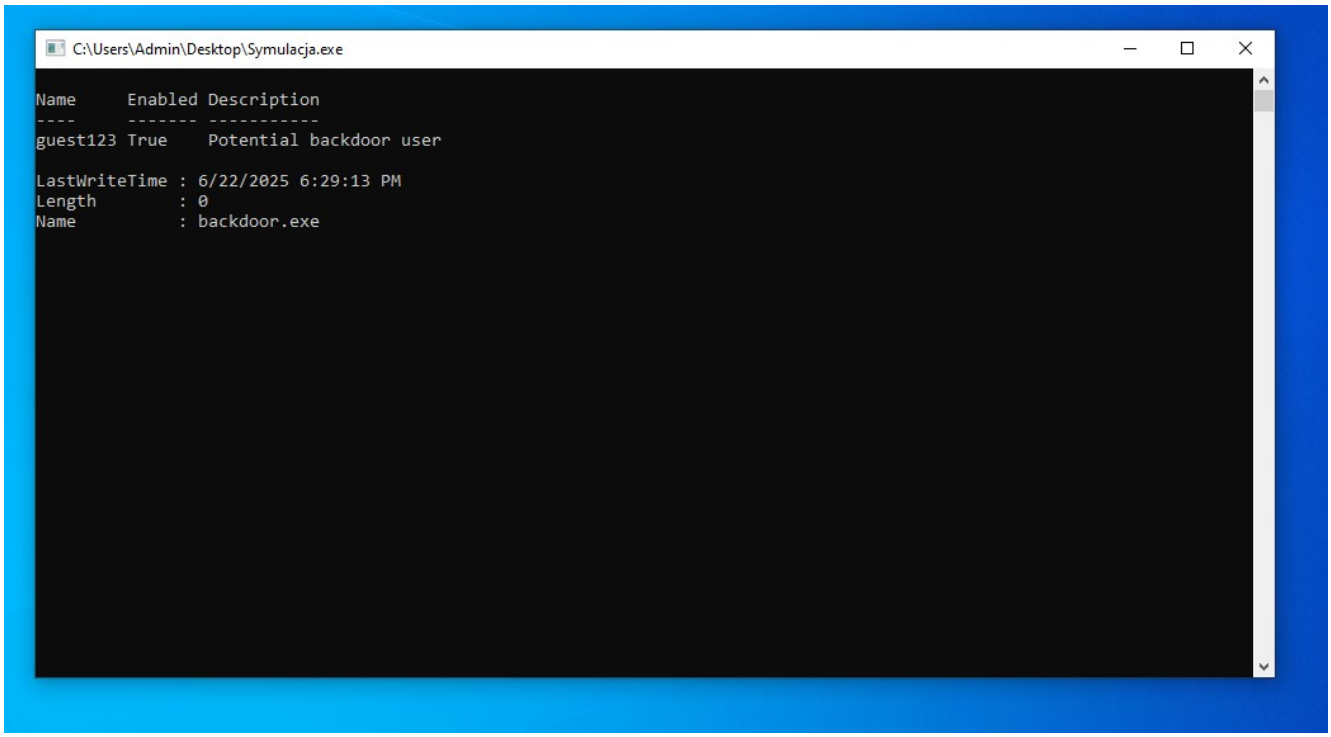
Zidentyfikuj wszystkie ślady aktywności skryptu, m.in.:

- konta użytkowników,
- wpisy w rejestrze,
- nowe pliki,
- wpisy w harmonogramie zadań,
- logi połączeń sieciowych.



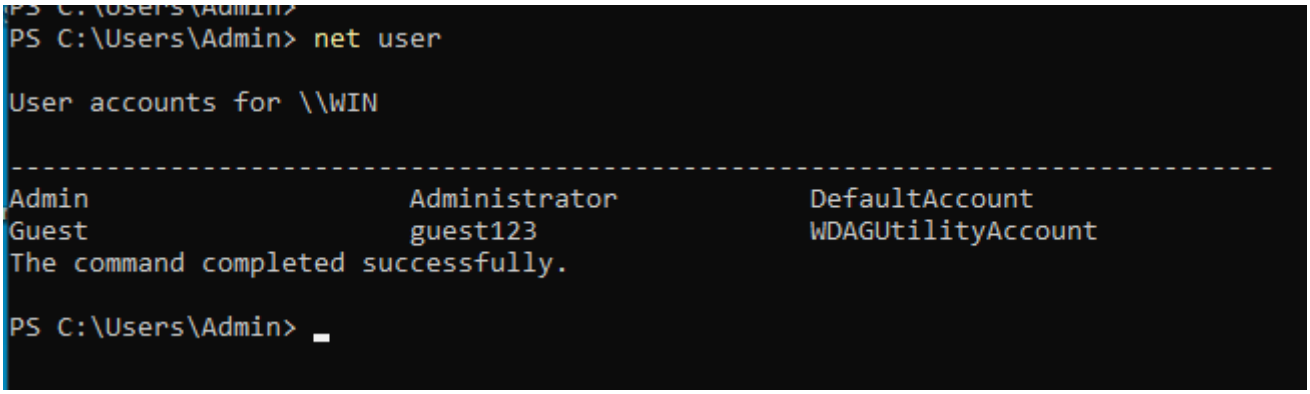
Rysunek 3: uruchomienie programu

Komentarz: nie byłem w stanie poprawnie uruchomić programu na windows 7, stąd zmiana na win 10. Wszystkie poprzednie kroki zostały ponownie wykonane.



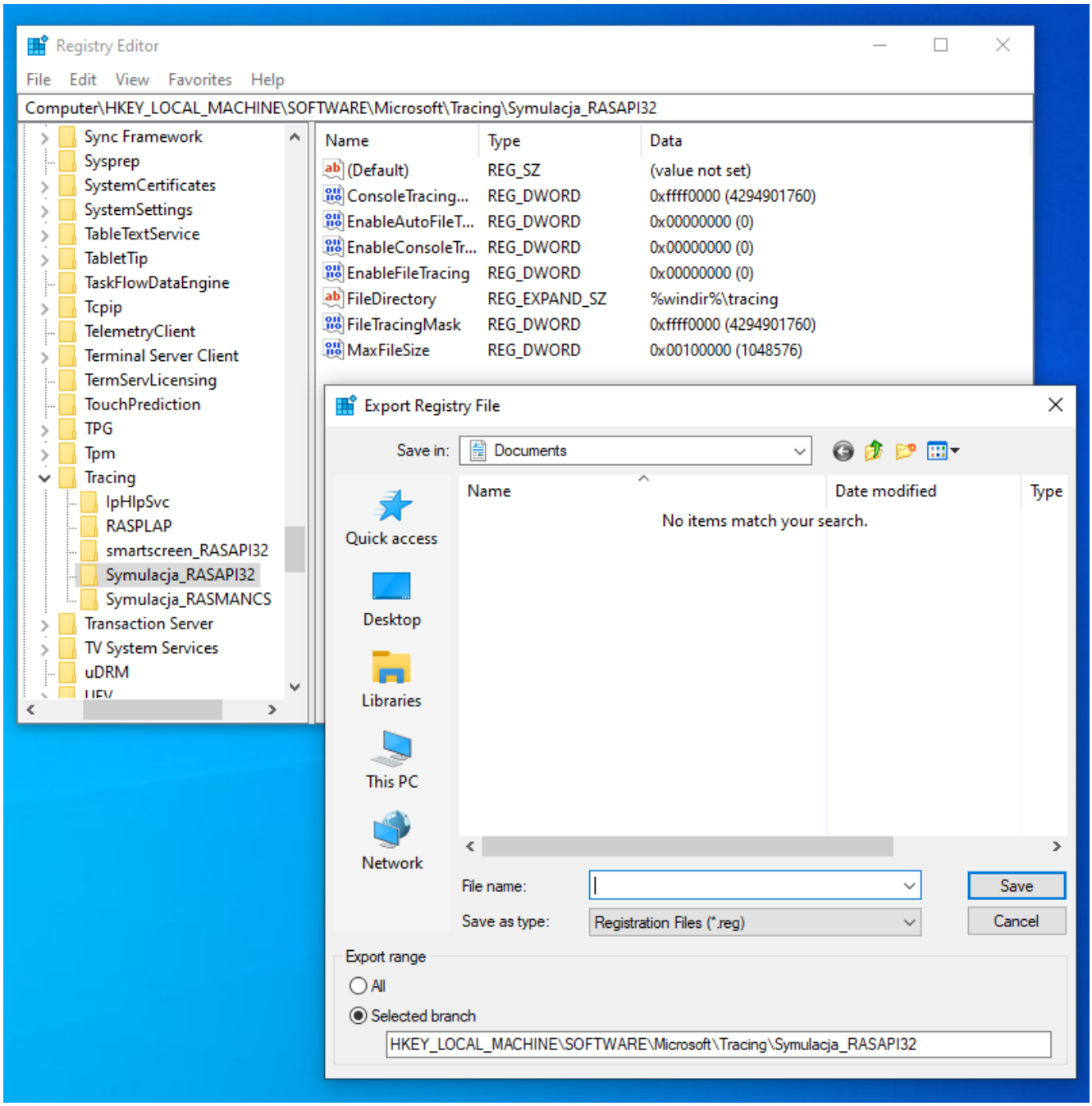
Rysunek 4: uruchomienie programu

- konta użytkowników

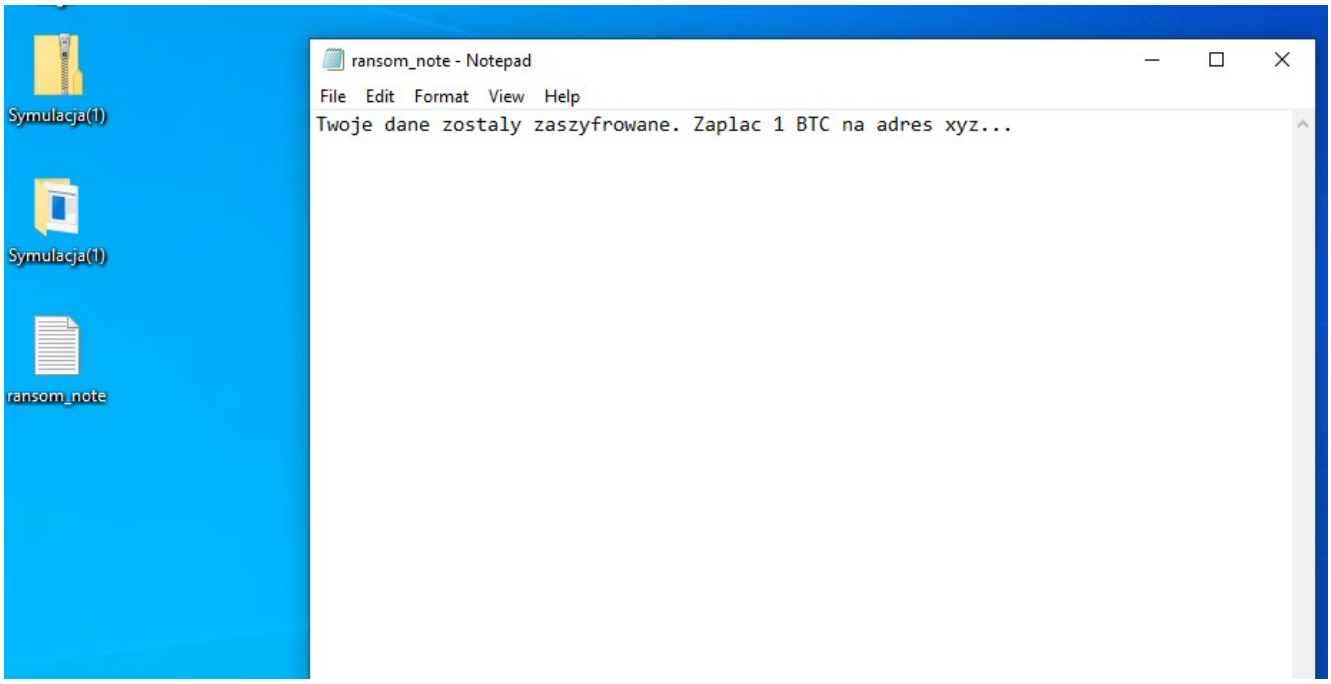


Rysunek 5: konta użytkowników

- wpisy w rejestrze

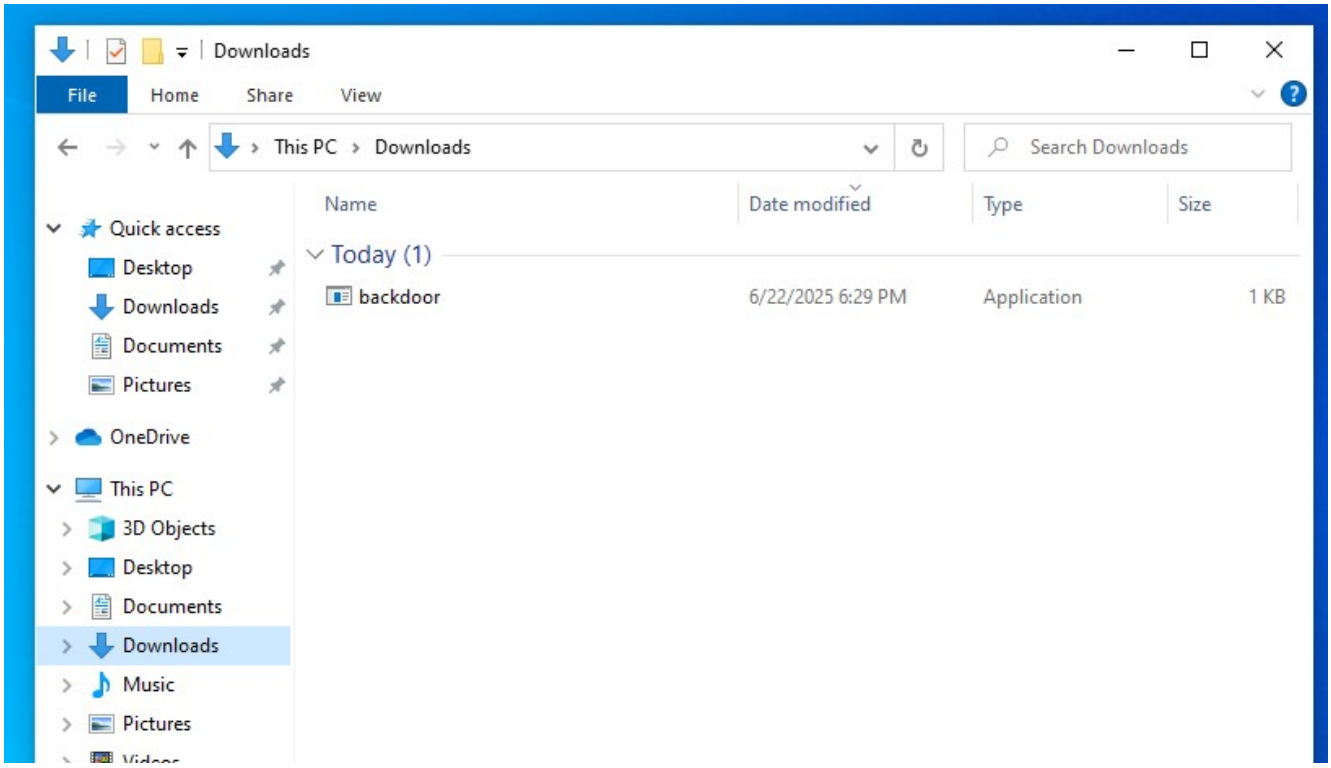


Rysunek 6: zidentyfikowane z nazwą skryptu wpisy w rejestrze



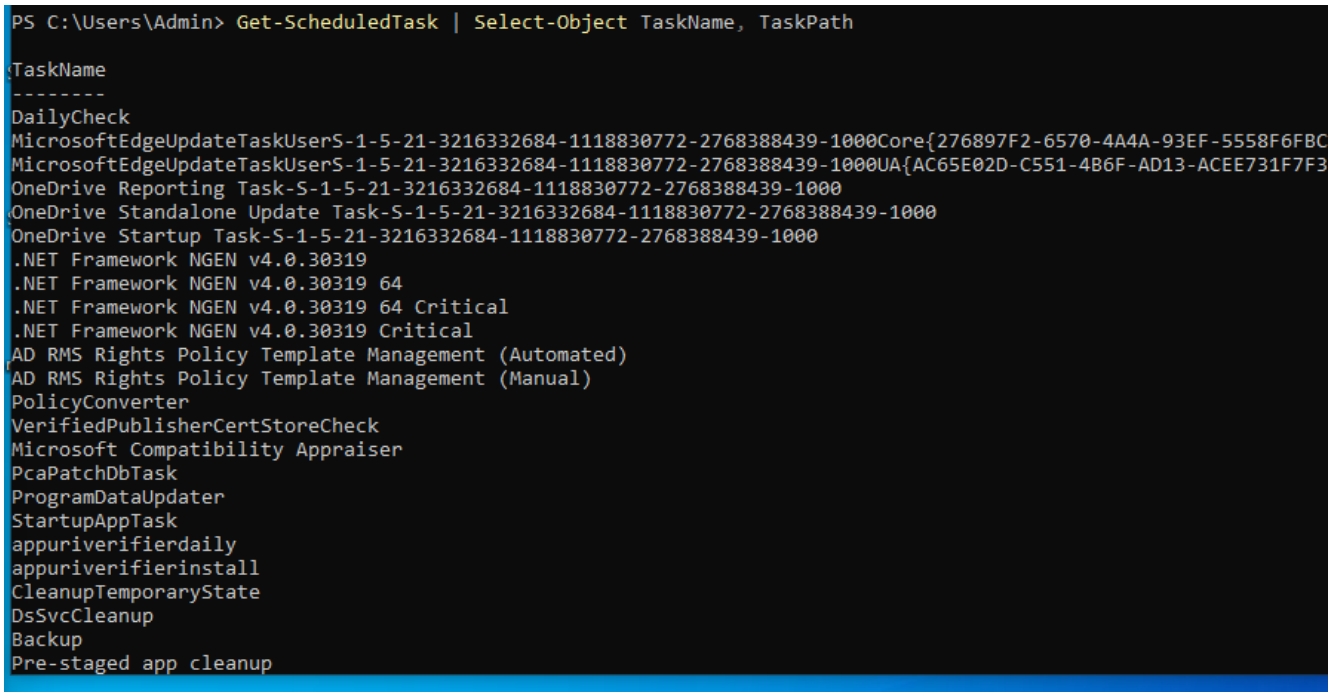
Rysunek 7: plik tekstowy powstały na pulpicie

- nowe pliki



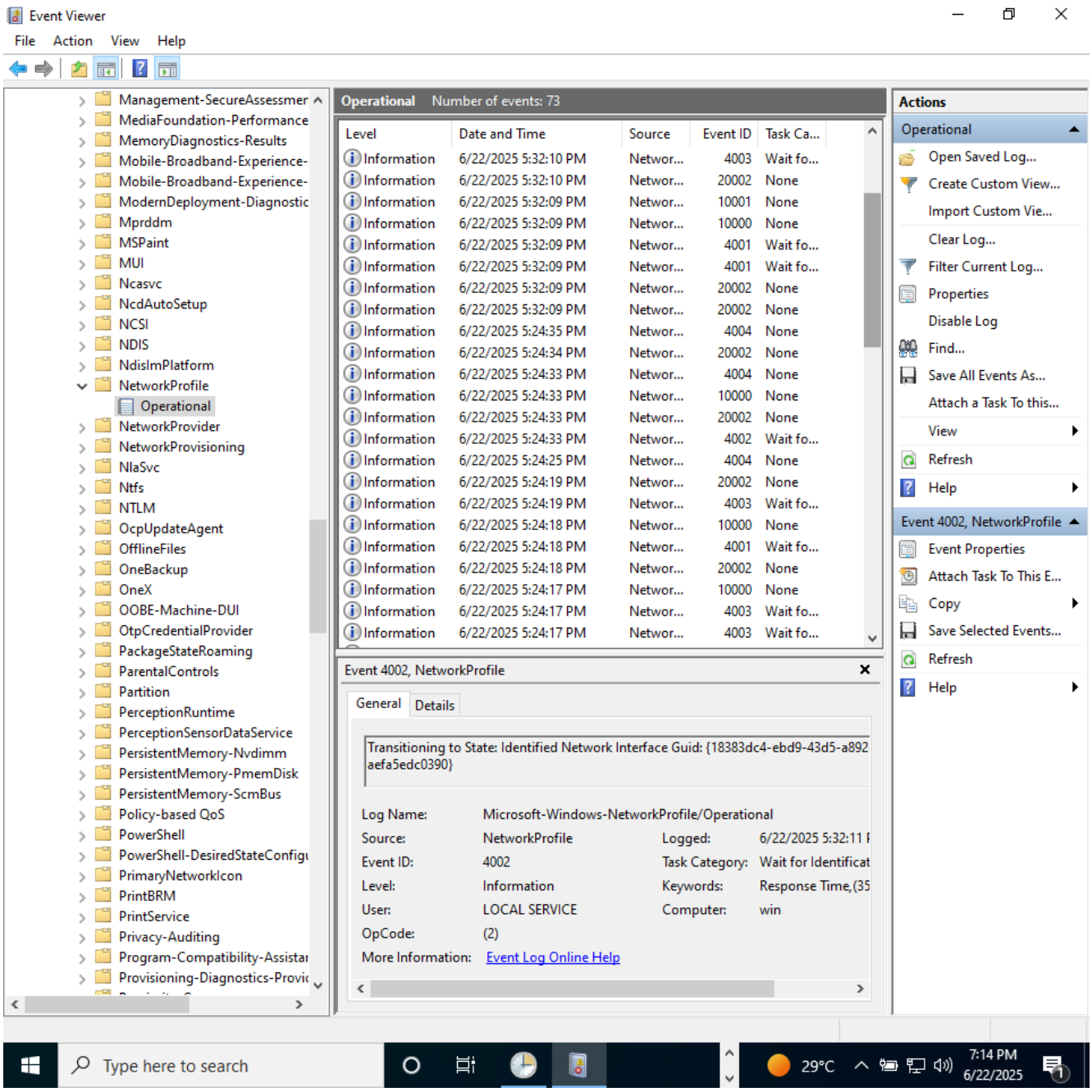
Rysunek 8: plik wykonywalny odnaleziony w folderze Downloads

- wpisy w harmonogramie zadań



Rysunek 9: lista wszystkich zaplanowanych zadań

- logi połączeń sieciowych

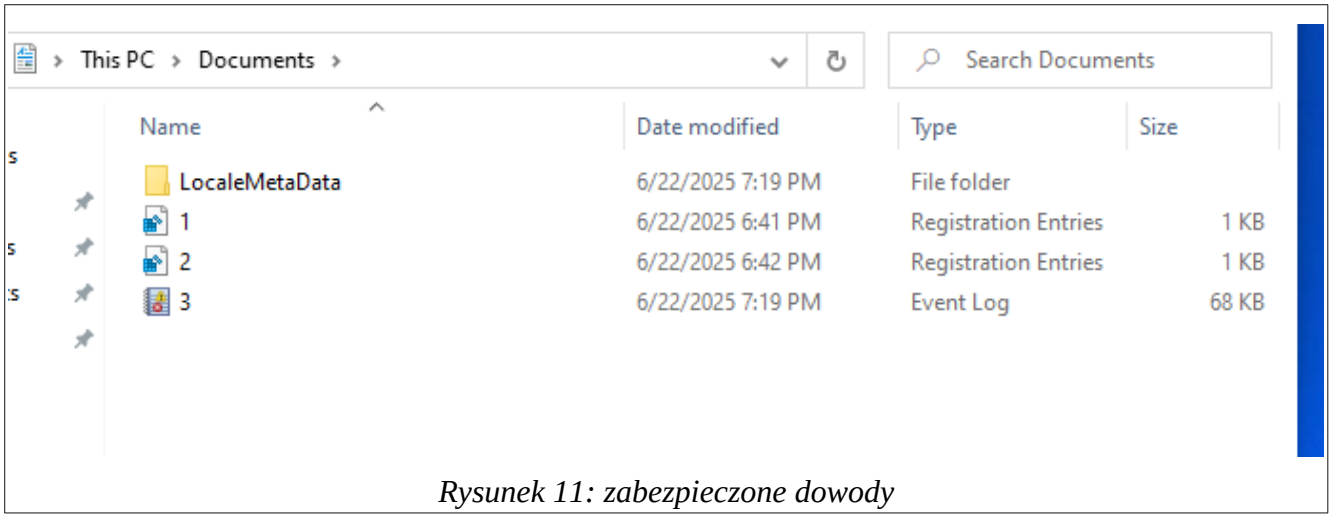


Rysunek 10: przegląd logów sieciowych

Zadanie 3b. Zabezpiecz wybrane dowody cyfrowe, np.:

- eksport rejestru,

- zrzut logów z Event Viewera.



Rysunek 11: zabezpieczone dowody

Zadanie 3c. Sporządź krótki raport zawierający:

- opis znalezionych artefaktów,

- metodę ich pozyskania,

- możliwy wektor ataku i jego cel

Podczas analizy po wykonaniu programu, można stwierdzić:

- Program tworzy nowego użytkownika w systemie
- Program tworzy pliki: tekstowy z żądaniem okupu oraz wykonywalny w kartotece pobrane.
- Program łączy się z domeną http://example.com/
- Zmienia wartość HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run w rejestrze
- Dodaje nowe zadanie harmonogramu.
- Tworzy nowy ukryty folder.

Artefakty/dowody zebrane poprzez przeglądanie logów, katalogów, rejestrów zwracając uwagę na rzeczy nowe/powstałe w chwili uruchomienia programu symulującego atak.

Wektor ataku i jego cel: działania analizowanego programu ze względu na jego testową naturę nie wskazują na poważne zagrożenia bezpieczeństwa, choćby dlatego, że zadania domena do której łączy się program jest testowa. Natomiast przyjmując, że byłby to atak prawdziwy to mamy do czynienia z uzyskaniem backdora do systemu poprzez

stworzenie odpowiedniej furtki oraz stworzenie nowego użytkownika systemu, który ma najwyższe uprawnienia. Ponadto program utworzył zadanie rejestrujące uruchomione procesy, a następnie za pomocą harmonogramu utworzył jego cykliczność, z starającą się nie wzbudzić wątpliwości nazwą – mamy więc do czynienia ze spyware. (Zadanie jest również uruchamiane „potajemnie” z dwuminutowym opóźnieniem.) Łącząc to ze wspomnianymi wcześniej tworzonymi plikami, to program, przyjmując, że byłby programem faktycznym a nie testowym, spełnia znamiona backdora, spyware, ransomware łączącego się z internetem i próbującego ukrywać się przed analizą. Jest więc to niezwykle niebezpieczny program.

Zadanie 4. Przeanalizuj program i wskaż, które jego fragmenty odpowiadają za konkretne działania.

```
Tworzenie konta "podejrzanego" uÅ¼ytkownika
New-LocalUser -Name "guest123" -Password (ConvertTo-SecureString "P@ssw0rd!" -AsPlainText -Force) -FullName "Temporary Guest" -Description "Potential
backdoor user" -UserMayNotChangePassword -AccountNeverExpires
Add-LocalGroupMember -Group "Administrators" -Member "guest123"

# Utworzenie pliku sugerujÄ•cego zÅ•oÅ•liwÄ• aktywnoÅ•Ä•
$path = "$env:USERPROFILE\Downloads\backdoor.exe"
New-Item -ItemType File -Path $path -Force
Set-Content -Path $path -Value "This is a dummy file simulating a backdoor executable."

# Utworzenie notatki sugerujÄ•cej atak ransomware
$note = "$env:USERPROFILE\Desktop\ransom_note.txt"
Set-Content -Path $note -Value "Twoje dane zostaÅ•y zaszyfrowane. ZapÅ•aÄ• 1 BTC na adres xyz..."

# Dodanie nietypowego zadania harmonogramu
$action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument "-Command `"Get-Process > C:\Temp\proc_dump.txt`""
$trigger = New-ScheduledTaskTrigger -Once -At (Get-Date).AddMinutes(2)
Register-ScheduledTask -TaskName "DailyCheck" -Action $action -Trigger $trigger -RunLevel Highest -Force

# Modyfikacja rejestru â•• autorun
New-Item -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Force
New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "Updater" -Value "C:\Windows\Temp\backdoor.exe" -PropertyType String -
Force
```

Rysunek 12: fragment zdekodowanego programu

Komentarze na tyle trafnie opisują działanie programu, że nie ma nic do dodania.

```
# Symulacja aktywnoÅ•ci sieciowej
Invoke-WebRequest -Uri "http://example.com" -OutFile "$env:TEMP\webtest.html"

# Dodanie wpisu do EventLog (Application)
Write-EventLog -LogName Application -Source "Application Error" -EntryType Error -EventId 1001 -Message "Symulowany bÅ•Ä•d aplikacji (moÅ¼liwe zÅ•oÅ•liwe
dziaÅ•anie)."

# Tworzenie ukrytego folderu
New-Item -Path "C:\ProgramData\HiddenLogs" -ItemType Directory -Force
attrib +h "C:\ProgramData\HiddenLogs"
Set-Content -Path "C:\ProgramData\HiddenLogs\keylogs.txt" -Value "user1:password123"

Write-Host "Symulacja wÅ•amania zakoÅ•czona. MoÅ¼esz rozpoczÄ•Ä• analizÄ• Å•edczÄ•." -ForegroundColor Green%%%BSJB%%%%
```

Rysunek 13: dalsza część programu

3. Wnioski

Analiza powłamaniowa jako ważny element informatyki śledczej pozwala na odkrycie celów i sposobu ataku wykonanego wcześniej ataku.