WPROWADZENIE DO INFORMATYKI

SPRAWOZDANIE

z realizacji zadania

Podstawowe czynności administracyjne (Zadanie 1)

Autor: Maks_Paluskiewicz_247754

Część obligatoryjna 1

Pamiętaj, aby pracować w zmaksymalizowanym oknie powłoki. Dzięki temu uzyskane listingi będą bardziej czytelne.

1. Polecenia wewnętrzne i zewnętrzne – Windows

Korzystając z polecenia Get-Command sprawdź, jakiego typu są polecenia: echo, Write-Output oraz powershell.

```
mpaluskiewicz(A)@WDI 22.10.2022 00:29 C:\Windows\system32> Get-Command echo, Write-
Output, powershell.exe | Select-Object -Property CommandType, Name

CommandType Name
----------- ----
      Alias echo
     Cmdlet Write-Output
Application powershell.exe
```

Pobierz i wypakuj archiwum z programem Dependencies. Użyj polecenia Get-Command podając za pierwszym razem frazę *dependencies*, zaś za drugim - ścieżkę pliku *Dependencies.exe* pochodzącego z archiwum. Czy możliwe jest uruchomienie programu, jeśli plik wykonywalny znajduje się w katalogu nie objętym przez PATH?

```
mpaluskiewicz(U)@WDI 22.10.2022 01:02 C:\Users\mpaluskiewicz> Get-Command
dependencies
Get-Command : The term 'dependencies' is not recognized as the name of a cmdlet,
function, script file, or operable pro
gram. Check the spelling of the name, or if a path was included, verify that the path
is correct and try again.
At line:1 char:1
+ Get-Command dependencies
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (dependencies:String) [Get-Command],
CommandNotFoundException
    + FullyQualifiedErrorId :
CommandNotFoundException,Microsoft.PowerShell.Commands.GetCommandCommand

mpaluskiewicz(U)@WDI 22.10.2022 01:02 C:\Users\mpaluskiewicz> Get-Command
C:\Users\mpaluskiewicz\Downloads\Dependencies_x64_Release\dependencies.exe

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Application     dependencies.exe                                   1.7.0.0
C:\Users\mpaluskiewicz\Downloads\Depen...
```

Wypisz zawartość zmiennej systemowej PATH ($env:PATH). Dodaj do tej zmiennej ścieżkę bezwzględną katalogu, w którym znajduje się plik Dependencies.exe ($env:PATH += ";<katalog>\"). Ponownie spróbuj żyj polecenia Get-Command podając frazę *dependencies*, a także wydaj polecenie *dependencies*. Otwórz nowe okno PowerShell i wydaj w nim polecenie *dependencies* oraz sprawdź zawartość PATH. Dlaczego wydanie polecenia tym razem zakończyło się błędem?

```
mpaluskiewicz(U)@WDI 22.10.2022 01:00 C:\Users\mpaluskiewicz> $env:Path
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPo
werShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\mpaluskiewicz\AppData\Local\Micr
osoft\WindowsApps;
mpaluskiewicz(U)@WDI 22.10.2022 01:00 C:\Users\mpaluskiewicz> $env:Path +=
"c:\Users\mpaluskiewicz\Downloads\Dependencies_x64_Release\"
mpaluskiewicz(U)@WDI 22.10.2022 01:00 C:\Users\mpaluskiewicz>  Get-Command
dependencies | dependencies
Dependencies.exe : command line tool for dumping dependencies and various utilities.

Usage : Dependencies.exe [OPTIONS] FILE

Options :
  -h -help : display this help
```

```
  -json : activate json output.
  -apisets : dump the system's ApiSet schema (api set dll -> host dll)
  -knowndll : dump all the system's known dlls (x86 and x64)
  -manifest : dump FILE embedded manifest, if it exists.
  -sxsentries : dump all of FILE's sxs dependencies.
  -imports : dump FILE imports
  -exports : dump  FILE exports
  -modules : dump FILE resolved modules
  -chain : dump FILE whole dependency chain
```

2. Programy i biblioteki – Windows

Pobierz i wypakuj archiwum zawierające program testowy. Spróbuj uruchomić oba pliki wykonywalne. Zauważ, że wyniki prób nie są identyczne (dla jednego z plików próba uruchomienia nie przynosi żadnego komunikatu).

```
mpaluskiewicz(U)@WDI 22.10.2022 11:40
C:\Users\mpaluskiewicz\Downloads\scryptwin\scryptwin> .\scrypt.exe
mpaluskiewicz(U)@WDI 22.10.2022 11:40
C:\Users\mpaluskiewicz\Downloads\scryptwin\scryptwin> .\scrypts.exe
Clear: Welcome to WDI
Salsa208sha256 hash:
$7$86..../....2JZwIKT/RJqgG851Em.SrbM//xAhYe.E7rweDDko6e.$7PJljCY3107Y/BW4J7.jjXR1za6
4Gvz7rc1lF7aYTM3
```

Sprawdź, jakie funkcje z jakich bibliotek są wykorzystywane przez oba pliki wykonywalne (dependencies.exe -imports). Porównaj wyniki i znajdź moduł (bibliotekę dynamiczną .dll) który jest wymagany tylko przez jeden z plików. **Ponownie przeprowadź tę próbę na pliku, który wymaga dodatkowego modułu, tak aby w wyniku pokazana została wyłącznie nazwa tego modułu (Select-String).**

```
mpaluskiewicz(U)@WDI 22.10.2022 00:56 C:\Users\mpaluskiewicz> dependencies -imports
'C:\Users\mpaluskiewicz\Downloads\scryptwin\scryptwin\scrypt.exe' |Select-String
libsodium-23.dll

Import from module libsodium-23.dll :
```

Pobierz brakujący plik biblioteki i umieść go w tym samym katalogu, gdzie położone są badane programy. Wykonanie potwierdź wypisując zawartość tego katalogu (dir). Zwróć uwagę na różnicę w rozmiarach badanych plików wykonywalnych. **Ponownie uruchom plik wykonywalny, który wymaga tej biblioteki. Sprawdź, jakie funkcje z jakich bibliotek są wykorzystywane przez nowo dodaną bibliotekę tak, aby w wyniku pokazana została wyłącznie nazwa innej biblioteki znajdującej się w tym samym katalogu.**

```
mpaluskiewicz(U)@WDI 26.10.2022 11:16 z:\scryptwin> ls


    Directory: z:\scryptwin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        22.10.2022     00:18          76288 libgcc_s_seh-1.dll
-a----        26.10.2022     11:08         710417 libsodium-23.dll
-a----        22.10.2022     00:18          52224 libwinpthread-1.dll
-a----        22.10.2022     00:18          15360 scrypt.exe
-a----        22.10.2022     00:18         247808 scrypts.exe
```

```
mpaluskiewicz(A)@WDI 26.10.2022 11:39
C:\Users\mpaluskiewicz\Desktop\scryptwin> .\scrypt.exe
Clear: Welcome to WDI
Salsa208sha256 hash:
$7$86..../....pKxDMMBFWK8Z3whSliJr89X1DZYcjqZdT33OjUW5JbC$B/kDP76KDoZGTnJuprRuAnujiKn
2V2yJQZ0VyWQoRE/
mpaluskiewicz(A)@WDI 26.10.2022 11:39
C:\Users\mpaluskiewicz\Desktop\scryptwin> .\scrypts.exe
Clear: Welcome to WDI
Salsa208sha256 hash:
$7$86..../....FabOlL6ClWJlSSxTrDfVCi1/PIMuscW8qqD5lRtQV08$.FARJ1Kdo8272hpP2pyURpm7pff
Ptmc/8q3rBwWse12
```

3. Przeglądanie dziennika zdarzeń – Windows

Wypisz pierwsze 10 pozycji listy dzienników zdarzeń (Get-WinEvent)(Select-Object).

```
mpaluskiewicz(A)@WDI 22.10.2022 11:50 C:\Windows\system32> Get-WinEvent | Select-
Object -first 10


   ProviderName: Microsoft-Windows-Kernel-Cache

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
22.10.2022 11:50:03             101 Informacje       Zainicjowano VolumeCacheMap dla
unikatowego identyfikatora glob...


   ProviderName: Microsoft-Windows-Security-SPP

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
22.10.2022 11:49:41          16384 Informacje       Zaplanowano restart usługi
ochrony oprogramowania o 2023-02-12T...


   ProviderName: Microsoft-Windows-StorPort

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
22.10.2022 11:49:27             549 Błędy            This is the first instance of
the error seen during this time p...
22.10.2022 11:49:26             548 Ostrzeżenia      The miniport logged a health
event.
22.10.2022 11:49:26             548 Ostrzeżenia      The miniport logged a health
event.
22.10.2022 11:49:26             534 Błędy            The miniport logged an event.
22.10.2022 11:49:26             548 Ostrzeżenia      The miniport logged a health
event.
22.10.2022 11:49:26             548 Ostrzeżenia      The miniport logged a health
event.
22.10.2022 11:49:26             548 Ostrzeżenia      The miniport logged a health
event.
22.10.2022 11:49:26             548 Ostrzeżenia      The miniport logged a health
event.
```

Wypisz po 3 najnowsze zdarzenia z dzienników: System oraz Security

```
mpaluskiewicz(A)@WDI 22.10.2022 12:24 C:\Windows\system32> Get-EventLog -LogName
System -Newest 3
```

```
   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    2829 paź 22 12:20  Information Service Control M...   1073748864 Typ uruchamiania
usługi Usługa inteligentnego t...
    2828 paź 22 12:17  Information Service Control M...   1073748864 Typ uruchamiania
usługi Usługa inteligentnego t...
    2827 paź 22 12:17  Information Microsoft-Windows...          112 Podjęto próbę
zarezerwowania adresu URL http://...


mpaluskiewicz(A)@WDI 22.10.2022 12:24 C:\Windows\system32> Get-EventLog -LogName
Security -Newest 3

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
   10369 paź 22 12:17  SuccessA... Microsoft-Windows...         4672 Przypisano
specjalne uprawnienia do nowego logo...
   10368 paź 22 12:17  SuccessA... Microsoft-Windows...         4624 Logowanie do
konta zakończyło się pomyślnie....
   10367 paź 22 12:17  SuccessA... Microsoft-Windows...         4799 Członkostwo
grupy lokalnej z włączonymi zabezpi...
```

Wypisz najnowsze 3 zdarzenia dziennika System o poziomie ważności (level) 2 lub 3.

Wskazówka: użyj filtrowania typu FilterHashtable.

```
mpaluskiewicz(A)@WDI 22.10.2022 12:33 C:\Windows\system32> Get-WinEvent -
FilterHashtable @{
>>    LogName='*'
>>    level=2, 3
>> } |Select-Object -First 3


   ProviderName: Microsoft-Windows-PowerShell

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
22.10.2022 12:33:33           4100 Ostrzeżenia      Error Message = You must specify
at least one Log, Provider or ...
22.10.2022 12:30:46           4100 Ostrzeżenia      Error Message = You must specify
at least one Log, Provider or ...
22.10.2022 12:30:42           4100 Ostrzeżenia      Error Message = You must specify
at least one Log, Provider or ...
```

Wypisz maksymalnie po 3 udane oraz nieudane próby zalogowania z ostatnich 24 godzin. UWAGA: Jeżeli brak jest takich zdarzeń, najpierw doprowadź do ich zaistnienia.

Wskazówka: dziennik zdarzeń Security, identyfikatory zdarzeń odpowiednio 4624 oraz 4625.

Wskazówka: StartTime=(Get-Date).AddHours()

```
mpaluskiewicz(A)@WDI 22.10.2022 12:52 C:\Windows\system32> Get-WinEvent -LogName
Security | Where-Object id -eq 4624 |Where-Object TimeCreated -gt (Get-
Date).AddDays(-1)|Select-Object -first 3


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
```

```
22.10.2022 12:39:10           4624 Informacje       Logowanie do konta zakończyło
się pomyślnie....
22.10.2022 12:39:06           4624 Informacje       Logowanie do konta zakończyło
się pomyślnie....
22.10.2022 12:17:55           4624 Informacje       Logowanie do konta zakończyło
się pomyślnie....


mpaluskiewicz(A)@WDI 22.10.2022 12:54 C:\Windows\system32> Get-WinEvent -LogName
Security | Where-Object id -eq 4625 |Where-Object TimeCreated -gt (Get-
Date).AddDays(-1)|Select-Object -first 3
```

4. Uruchamianie powłoki z tożsamością użytkownika – Windows

Dla użytkownika bolek wypisz w jednym wierszu datę ostatniego logowania oraz datę ostatniej zmiany hasła (Get-Localuser)(Select-Object).

```
mpaluskiewicz(A)@WDI 22.10.2022 13:33 C:\Windows\system32> Get-LocalUser -name bolek
| Select-Object 'PasswordLastChange*', 'LastLogon'

PasswordLastChange LastLogon
------------------- ---------
21.10.2022 21:35:52    22.10.2022 12:59:14
```

Uruchom powłokę PowerShell z identyfikacją użytkownika bolek (runas). W otwartym oknie powłoki zaprezentuj nazwę użytkownika (whoami). *Pozostaw nowe okno powłoki otwarte i wróć do poprzedniego okna powłoki*. **Ponownie wypisz w jednym wierszu datę ostatniego logowania oraz datę ostatniej zmiany hasła użytkownika bolek. Sprawdź też, czy został utworzony profil użytkownika (dir). Wypisz wszystkie aktualnie otwarte sesje użytkowników (query user). Wypisz wszystkie procesy powershell uwzględniając identyfikację użytkownika dla każdego procesu (Get-Process).**

```
Bolek(U)@WDI 22.10.2022 15:36 C:\Windows\system32> whoami
wdi\bolek

Bolek(U)@WDI 22.10.2022 15:42 C:\Windows\system32> Get-LocalUser -name bolek |
Select-Object 'PasswordLast*', 'LastLogon'

PasswordLastSet LastLogon
------------------- ---------
21.10.2022 21:35:52    22.10.2022 15:36:26

Bolek(U)@WDI 22.10.2022 15:50 C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        22.10.2022     13:00                Bolek
d-----        22.10.2022     14:05                mpaluskiewicz
d-r---        15.10.2022     10:59                Public
d-----        22.10.2022     15:51                Tola

Bolek(U)@WDI 22.10.2022 15:43 C:\Windows\system32> query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
>mpaluskiewicz         console             1  Active      none   22.10.2022 15:34

mpaluskiewicz(A)@WDI 26.10.2022 10:57 C:\Windows\system32> get-process -
IncludeUserName | Where-Object processName -match "powershell"
```

```
Handles      WS(K)   CPU(s)     Id UserName               ProcessName
-------      -----   ------     -- --------               -----------
    599      72536     0,72   2228 WDI\Bolek             powershell
   1100     115004     6,17   2904 WDI\mpaluskiewicz     powershell
    689     151040     3,34   5684 WDI\mpaluskiewicz     powershell
```

5. Ustawianie hasła i blokowanie konta użytkownika – Windows

Dla użytkownika lolek wypisz w jednym wierszu datę ostatniego logowania oraz datę ostatniej zmiany hasła (Get-Localuser)(Select-Object).

```
mpaluskiewicz(U)@WDI 22.10.2022 21:52 C:\Users\mpaluskiewicz> Get-LocalUser -name
lolek | Select-Object 'passwordlast*', 'lastlogon*'

PasswordLastSet     LastLogon
---------------     ---------
21.10.2022 21:35:43
```

Przeprowadź próbę uruchomienia powłoki PowerShell z identyfikacją użytkownika lolek (runas). Ustaw hasło użytkownika lolek (net user) i ponów próbę uruchomienia powłoki. *Pozostaw nowe okno powłoki otwarte i wróć do poprzedniego okna powłoki*. **Ponownie wypisz w jednym wierszu datę ostatniego logowania oraz datę ostatniej zmiany hasła użytkownika lolek. Wypisz wszystkie procesy powershell uwzględniając identyfikację użytkownika dla każdego procesu (Get-Process).**

```
mpaluskiewicz(U)@WDI 22.10.2022 21:52 C:\Users\mpaluskiewicz> runas /user:lolek
powershell
Wpisz hasło dla lolek:
Attempting to start powershell as user "WDI\lolek" ...
RUNAS ERROR: Unable to run - powershell



1327: Ograniczenia konta uniemożliwiają temu użytkownikowi zalogowanie się. Mogą to
być na przykład: niedozwolone puste hasła, ograniczone godziny logowania lub
wymuszanie ograniczenia zasad.

mpaluskiewicz(A)@WDI 22.10.2022 21:55 C:\Windows\system32> net user lolek 123
Polecenie zostało wykonane pomyślnie.

mpaluskiewicz(A)@WDI 22.10.2022 21:55 C:\Windows\system32> Get-LocalUser -name lolek
| Select-Object 'passwordlast*','last*'

PasswordLastSet     LastLogon
---------------     ---------
22.10.2022 21:55:11 22.10.2022 21:55:40

mpaluskiewicz(A)@WDI 26.10.2022 11:02 C:\Windows\system32> get-process -
IncludeUserName | Where-Object processName -match "powershell"

Handles      WS(K)   CPU(s)     Id UserName               ProcessName
-------      -----   ------     -- --------               -----------
    615      72204     0,53   1000 WDI\Lolek             powershell
    599      68808     0,77   2228 WDI\Bolek             powershell
   1226     115168     6,38   2904 WDI\mpaluskiewicz     powershell
    689     147584     3,38   5684 WDI\mpaluskiewicz     powershell
```

Zablokuj konto użytkownika lolek (Disable-LocalUser) i wypisz jego właściwości w widoku domyślnym (Get-Localuser). Przejdź do zachowanego okna powłoki użytkownika lolek, wydaj puste polecenie aby odświeżyć znak zachęty i **wydaj polecenie whoami.** Czy zablokowanie konta miało wpływ na możliwość pracy w już uruchomionej powłoce? Zamknij tę powłokę (exit) i wróć do poprzedniego okna powłoki. **Podejmij próbę ponownego uruchomienia powłoki PowerShell z identyfikacją użytkownika lolek (runas).**

```
mpaluskiewicz(A)@WDI 22.10.2022 21:58 C:\Windows\system32> Get-LocalUser lolek

Name  Enabled Description
----  ------- -----------
Lolek False

Lolek(U)@WDI 22.10.2022 21:58 C:\Windows\system32> whoami
wdi\lolek

mpaluskiewicz(A)@WDI 22.10.2022 21:58 C:\Windows\system32> runas /user:lolek
powershell
Wpisz hasło dla lolek:
Attempting to start powershell as user "WDI\lolek" ...
RUNAS ERROR: Unable to run - powershell
1327: Ograniczenia konta uniemożliwiają temu użytkownikowi zalogowanie się. Mogą to
być na przykład: niedozwolone puste hasła, ograniczone godziny logowania lub
wymuszanie ograniczenia zasad.
```

Odblokuj konto użytkownika lolek (Enable-LocalUser) oraz ustaw ustaw datę wygaśnięcia tego konta na dowolną datę z przeszłości. Ponownie podejmij próbę ponownego uruchomienia powłoki PowerShell z identyfikacją użytkownika lolek (runas).

```
mpaluskiewicz(A)@WDI 22.10.2022 22:00 C:\Windows\system32> net user lolek
/expires:21.11.2022
Polecenie zostało wykonane pomyślnie.

mpaluskiewicz(A)@WDI 22.10.2022 22:01 C:\Windows\system32> runas /user:lolek
powershell
Wpisz hasło dla lolek:
Attempting to start powershell as user "WDI\lolek" ...
```

Część obligatoryjna 2

Pamiętaj, aby pracować w zmaksymalizowanym oknie powłoki. Dzięki temu uzyskane listingi będą bardziej czytelne.

1. Polecenia wewnętrzne i zewnętrzne – Linux, bash

Zaprezentuj dostępne warianty polecenia echo (type -a) (*uwaga: informacja o wariancie zewnętrznym jest zdublowana, ponieważ /bin jest dowiązaniem do /usr/bin, obie ścieżki są równoważne*). **Uruchom oba warianty tak, aby wypisać napisy WEWNETRZNY / ZEWNETRZNY adekwatnie do wybranego wariantu.**

```
[mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 18:34:47 ~]$ type -a echo
echo jest wewnętrznym poleceniem powłoki
echo jest /usr/bin/echo
echo jest /bin/echo

[mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 18:36:00 ~]$ echo wewnetrzene &
/bin/echo zewnetrzne
[1] 1161
wewnetrzene
zewnetrzne
```

Jako użytkownik uprzywilejowany: uruchom polecenie ldconfig, wypisz wartość zwróconą przez proces (wynik wykonania), wypisz zawartość zmiennej PATH oraz wyszukaj ścieżkę pliku wykonywalnego dla tego polecenia (which). Porównaj znalezioną ścieżkę z zawartością zmiennej PATH.

```
[mpaluskiewicz@247754-WDI ttyid:0 nie paź 23 00:04:53 ~]$ echo $PATH
bash: /usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamese

[mpaluskiewicz@247754-WDI ttyid:0 nie paź 30 16:27:40 ~]$ which -a ldconfig
```

Jako użytkownik nieuprzywilejowany: uruchom polecenie ldconfig, wypisz zawartość zmiennej PATH oraz wyszukaj ścieżkę pliku wykonywalnego dla tego polecenia (which). Porównaj zawartość zmiennej PATH do analogicznej zawartości uzyskanej jako użytkownik uprzywilejowany. Dlaczego uruchomienie polecenia nie powiodło się? **Uruchom program ldconfig korzystając z poznanej uprzednio ścieżki, wypisz wartość zwróconą przez proces (wynik wykonania).** Czy możliwe jest uruchomienie programu, jeśli plik wykonywalny znajduje się w katalogu nie objętym przez PATH?

```
mpaluskiewicz@247754-WDI ttyid:0 nie paź 30 16:26:45 ~]$ ldconfig
bash: ldconfig: nie znaleziono polecenia


[mpaluskiewicz@247754-WDI ttyid:0 nie paź 23 00:04:53 ~]$ echo $PATH
bash: /usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/gamese


[mpaluskiewicz@247754-WDI ttyid:0 nie paź 30 16:27:40 ~]$ which -a ldconfig

[mpaluskiewicz@247754-WDI ttyid:0 nie paź 30 16:27:47 ~]$ /sbin/ldconfig
/sbin/ldconfig: Nie można utworzyć tymczasowego pliku pamięci podręcznej
/etc/ld.so.cache~: Brak dostępu
```

2. Programy i biblioteki – Linux

Pobierz i wypakuj archiwum zawierające testowy program w wariancie dla systemu Linux. Dla obu plików znajdujących się w archiwum (scrypt, scrypts) zbadaj typ pliku (file) oraz wymagane biblioteki (ldd). Porównaj wielkości obu plików. **Uruchom oba pliki** (jeżeli to potrzebne, uczyń je wcześniej wykonywalnymi: chmod a+x <plik>).

```
[root@247754-WDI ttyid:0 czw paź 27 18:56:35 Desktop]# ldd ./scrypt
      linux-vdso.so.1 (0x00007ffd83d4f000)
      libsodium.so.23 => /lib/x86_64-linux-gnu/libsodium.so.23 (0x00007f8f2ba5c000)
```

```
      libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f8f2b887000)
      libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f8f2b865000)
      /lib64/ld-linux-x86-64.so.2 (0x00007f8f2bad2000)
[root@247754-WDI ttyid:0 czw paź 27 18:56:45 Desktop]# ldd ./scrypts
      nie jest dynamicznym programem wykonywalnym

[root@247754-WDI ttyid:0 czw paź 27 18:57:56 Desktop]# ./scrypts
Clear: Welcome to WDI
Salsa208sha256 hash:
$7$86..../....c5cK1LoyIGM5lWA6EsQk966aSP2AgOSgEIVI5LYnrE0$n2qjBVxAVj59KidGfbckxsGnjK6
1Nt0YyQOqu2jh.d5
[root@247754-WDI ttyid:0 czw paź 27 18:58:01 Desktop]# ./scrypt
Clear: Welcome to WDI
Salsa208sha256 hash:
$7$86..../....abRaiiyZKcG7w/4GOrS1eAoTdhzOWAVx9AMaZo/SYsC$GpXpmliwVqGN0M4.GriCKYzbMi8
NWyNgRBXvWM36n3/
```

Wykaż, że biblioteka libsodium jest dostępna dla systemowego konsolidatora bibliotek, tzw. linkera, tak aby w wyniku wypisana była tylko ta jedna biblioteka (ldconfig -p, grep). Usuń wskazany plik biblioteki (rm) i ponownie spróbuj uruchomić oba programy. Co jest przyczyną niepowodzenia w jednym przypadku i dlaczego w drugim przypadku uruchomienie zakończyło się powodzeniem?

```
[root@247754-WDI ttyid:0 czw paź 27 18:59:07 Desktop]# ldconfig -p | grep libsodium
      libsodium.so.23 (libc6,x86-64) => /lib/x86_64-linux-gnu/libsodium.so.23

[root@247754-WDI ttyid:0 czw paź 27 19:00:16 Desktop]# ./scrypt
./scrypt: error while loading shared libraries: libsodium.so.23: cannot open shared
object file: No such file or directory
[root@247754-WDI ttyid:0 czw paź 27 19:00:20 Desktop]# ./scrypts
Clear: Welcome to WDI
Salsa208sha256 hash:
$7$86..../....k66cEY0k/0.JBfZqm9V.MppGloeAwoUeIQkVIM5yFm.$.Q8YJOI6L2t5qXg2j2HmGtbPNmV
w9WlR3AmSUgGmjC9
```

Dokonaj przeinstalowania pakietu libsodium23 (apt reinstall). **Wykaż poprawne uruchamianie się tego programu, którego uruchomienie nie było możliwe poprzednio. Zbadaj, jakie biblioteki są wymagane dla odzyskanego pliku biblioteki.**

```
Miejsce na wklejenie listingu.
[mpaluskiewicz@247754-WDI ttyid:0 nie paź 30 16:39:12 Desktop]$ ldd /lib/x86_64-
linux-gnu/libsodium.so.23
      linux-vdso.so.1 (0x00007ffdaa39f000)
      libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007fa1afc3a000)
      libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fa1afa65000)
      /lib64/ld-linux-x86-64.so.2 (0x00007fa1afccb000)
```

3. Przeglądanie dziennika zdarzeń – Linux

Wypisz po 3 najnowsze zdarzenia z dziennika systemowego (journalctl), kolejno: bez dodatkowych kryteriów, o priorytecie błędu lub istotniejszym, pochodzących od procesu o identyfikatorze równym 1, pochodzących od procesów użytkownika o identyfikatorze równym 0, pochodzących od usługi cron, pochodzących z jądra systemu. UWAGA: do wybierania zdarzeń używaj tylko opcji polecenia journalctl.

```
[mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:09:57 ~]$ sudo journalctl | head -4
-- Journal begins at Sat 2022-10-15 13:19:29 CEST, ends at Thu 2022-10-27 21:10:17
CEST. --
```

```
paź 15 13:19:29 247754-WDI kernel: Linux version 5.10.0-18-amd64 (debian-
kernel@lists.debian.org) (gcc-10 (Debian 10.2.1-6) 10.2.1 20210110, GNU ld (GNU
Binutils for Debian) 2.35.2) #1 SMP Debian 5.10.140-1 (2022-09-02)
paź 15 13:19:29 247754-WDI kernel: Command line: BOOT_IMAGE=/vmlinuz-5.10.0-18-amd64
root=UUID=00453557-19e2-4240-8d23-29ad3c1ff2c0 ro quiet
paź 15 13:19:29 247754-WDI kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87
floating point registers'

mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:25:15 ~]$ sudo journalctl -p 'err' |
head -4
-- Journal begins at Sat 2022-10-15 13:19:29 CEST, ends at Thu 2022-10-27 21:25:26
CEST. --
paź 15 13:19:29 247754-WDI kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send
host log message.
paź 15 13:19:29 247754-WDI kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send
host log message.
paź 15 13:19:33 247754-WDI connmand[436]: __connman_inet_get_pnp_nameservers: Cannot
read /proc/net/pnp Failed to open file "/proc/net/pnp": No such file or directory

[mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:28:08 ~]$ sudo journalctl -t 1 | head
-4
-- Journal begins at Sat 2022-10-15 13:19:29 CEST, ends at Thu 2022-10-27 21:28:21
CEST. --
-- No entries –

[mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:31:34 ~]$ sudo journalctl --user-unit
-0 | head -4
-- Journal begins at Sat 2022-10-15 13:19:29 CEST, ends at Thu 2022-10-27 21:31:37
CEST. --
-- No entries –

mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:37:30 ~]$ sudo journalctl -u cron |
head -4
-- Journal begins at Sat 2022-10-15 13:19:29 CEST, ends at Thu 2022-10-27 21:37:32
CEST. --
paź 15 13:19:33 247754-WDI systemd[1]: Started Regular background program processing
daemon.
paź 15 13:19:33 247754-WDI cron[434]: (CRON) INFO (pidfile fd = 3)
paź 15 13:19:33 247754-WDI cron[434]: (CRON) INFO (Running @reboot jobs)

mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:37:30 ~]$ sudo journalctl -u cron |
head -4
-- Journal begins at Sat 2022-10-15 13:19:29 CEST, ends at Thu 2022-10-27 21:37:32
CEST. --
paź 15 13:19:33 247754-WDI systemd[1]: Started Regular background program processing
daemon.
paź 15 13:19:33 247754-WDI cron[434]: (CRON) INFO (pidfile fd = 3)
paź 15 13:19:33 247754-WDI cron[434]: (CRON) INFO (Running @reboot jobs)
```

Wypisz udane oraz nieudane próby zalogowania z dnia bieżącego (dzisiejszego)(last, lastb). UWAGA: Jeżeli brak jest takich zdarzeń, najpierw doprowadź do ich zaistnienia.

```
[mpaluskiewicz@247754-WDI ttyid:0 czw paź 27 21:47:52 ~]$ last -s yesterday
mpaluski tty7         :0               Thu Oct 27 20:55   still logged in
reboot   system boot  5.10.0-18-amd64  Thu Oct 27 20:55   still running
mpaluski tty7         :0               Thu Oct 27 18:41 - 19:28  (00:46)
reboot   system boot  5.10.0-18-amd64  Thu Oct 27 18:41 - 19:28  (00:47)
mpaluski tty7         :0               Thu Oct 27 18:34 - crash  (00:06)
reboot   system boot  5.10.0-18-amd64  Thu Oct 27 18:34 - 19:28  (00:54)
```

Przeszukaj pod kątem frazy „install" wszystkie pliki (jednym poleceniem) dziennika historii aplikacji apt, pokaż ostatnie 3 wystąpienia (zgrep)(/var/log/apt/)(tail)

```
Miejsce na wklejenie listingu.
[root@247754-WDI ttyid:0 nie paź 30 16:45:07 Desktop]# zgrep install
/var/log/apt/history.log | tail -3
Commandline: apt-get install stress
Commandline: apt-get reinstall libsodium23
Reinstall: libsodium23:amd64 (1.0.18-1)
```

4. Uruchamianie powłoki z tożsamością użytkownika – Linux

Otwórz dwa okna/karty terminala jako użytkownik nieuprzywilejowany utworzony w trakcie instalacji. W jednym z nich uruchom powłokę z identyfikacją użytkownika bolek poprzez użycie programu su (su bolek), zaś w drugim – poprzez użycie programu sudo (sudo -u bolek bash). W obu przypadkach wypisz bieżący identyfikator oraz przynależność do grup użytkownika (id – bez argumentów). Pozostaw obie powłoki do dalszych działań. Zaobserwuj różnicę w sposobie uwierzytelniania w obu przypadkach.

```
Miejsce na wklejenie listingu.
[mpaluskiewicz@247754-WDI ttyid:1 nie paź 30 16:46:49 ~]$ sudo su bolek
bolek@247754-WDI:/home/mpaluskiewicz$ id
uid=1001(bolek) gid=1001(bolek) grupy=1001(bolek)

[mpaluskiewicz@247754-WDI ttyid:1 nie paź 30 16:46:49 ~]$ su bolek
bolek@247754-WDI:/home/mpaluskiewicz$ id
uid=1001(bolek) gid=1001(bolek) grupy=1001(bolek)
```

Pracując w powłoce z identyfikacją użytkownika uprzywilejowanego wypisz sesje aktualnie zalogowanych użytkowników (who) oraz udane próby zalogowania z dnia bieżącego. Czy uruchomienie powłoki ze zmienioną identyfikacją poprzez su lub sudo jest traktowane jako tożsame z zalogowaniem (otwarciem sesji)?

```
Miejsce na wklejenie listingu.
[mpaluskiewicz@247754-WDI ttyid:2 nie paź 30 16:50:36 ~]$ sudo who
mpaluskiewicz tty7         2022-10-30 16:24 (:0)
[mpaluskiewicz@247754-WDI ttyid:2 nie paź 30 16:50:39 ~]$ last -s today
mpaluski tty7         :0               Sun Oct 30 16:24   still logged in
reboot   system boot  5.10.0-18-amd64  Sun Oct 30 16:22   still running

wtmp zaczyna się Sat Oct 15 16:32:43 2022
```

5. Hasło / konto zablokowane a uruchamianie powłoki z tożsamością użytkownika – Linux

Jako użytkownik nieuprzywilejowany utworzony w trakcie instalacji dokonaj próby uruchomienia powłoki z identyfikacją użytkownika lolek (którego hasło powinno pozostawać nie ustawione) za pomocą su oraz sudo analogicznie jak w poprzednim rozdziale. W każdej udanej próbie do listingu dołącz tylko nowy znak zachęty i zakończ powłokę (exit). Która z prób się powiodła, a która nie? W jaki sposób różnica w sposobie uwierzytelniania w su i sudo wpłynęła na rezultat próby? Zweryfikuj (nie zamieszczając wyniku w sprawozdaniu) czy wynik eksperymentu jest taki sam, kiedy su / sudo wykonywane są przez użytkownika uprzywilejowanego. Czy wobec uzyskanych wyników istnieje potrzeba wykazywania, czy praca w otwartej już powłoce po zablokowaniu konta może być kontynuowana?

```
Miejsce na wklejenie listingu.
Miejsce na wklejenie listingu.
[mpaluskiewicz@247788-WDI ttyid:1 sob paź 29 12:02:16 ~]$ su lolek
Hasło:
[root@247788-WDI ttyid:0 sob paź 29 12:01:05 mpalluskiewicz]# sudo -u lolek bash
lolek@247788-WDI:/home/ismolarczyk$ exit exit
```

Jako użytkownik uprzywilejowany ustaw hasło użytkownika lolek, a także ustaw ustaw datę wygaśnięcia tego konta na dowolną datę z przeszłości (chage). Następnie ponów próby uruchomienia powłoki z identyfikacją użytkownika lolek jak w poprzednim akapicie. Która z prób się powiodła, a która nie? W jaki sposób różnica w sposobie uwierzytelniania w su i sudo wpłynęła na rezultat próby? Zweryfikuj (nie zamieszczając wyniku w sprawozdaniu) czy wynik eksperymentu jest taki sam, kiedy su / sudo wykonywane są przez użytkownika uprzywilejowanego. Czy wobec uzyskanych wyników istnieje potrzeba wykazywania, czy praca w otwartej już powłoce po wygaśnięciu konta może być kontynuowana?

```
Miejsce na wklejenie listingu.
[root@247788-WDI ttyid:1 sob paź 29 12:21:38 mpaluskiewcz]# passwd lolek Nowe hasło:
Proszę ponownie wpisać nowe hasło:
passwd: hasło zostało zmienione


[root@247788-WDI ttyid:1 sob paź 29 12:25:06 mpaluskiewicz]# chage -E 2022-10-27
lolek

[root@247788-WDI ttyid:1 sob paź 29 12:25:55 mpaluskiewicz]# su lolek Konto wygasło;
proszę skontaktować się z administratorem komputera. su: Uwierzytelnienie się nie
powiodło

[root@247788-WDI ttyid:1 sob paź 29 12:26:16 ]# sudo -u mpaluskiewicz lolek bash
lolek@247788-WDI:/home/mpaluskiewicz$
```

Część nieobligatoryjna

Pamiętaj, aby pracować w zmaksymalizowanym oknie powłoki. Dzięki temu uzyskane listingi będą bardziej czytelne.

1. Bieżąca i zachowawcza przynależność do grup – Windows.

Utwórz grupę *proba* (New-LocalGroup). Na przykładzie tej grupy i wybranego użytkownika (bolek, lolek lub tola) wykaż, że dodanie użytkownika do grupy nie wpływa na tożsamość w już otwartej powłoce.

Wskazówka: przeanalizuj rozdział części obligatoryjnej, w którym sprawdzany jest wpływ operacji blokowania konta na już otwartą powłokę.

Uwaga: musisz wykazać, że użytkownik został dodany do grupy w konfiguracji zachowawczej (**Get-LocalGroupMember)** oraz sprawdzić tożsamość bieżącą w powłoce (**whoami** z opcją wyświetlenia informacji o grupach).

Sugestia: przekonaj się, czy zmiana zostanie uwzględniona po otwarciu nowej powłoki.

```
Miejsce na wklejenie listingu.
W przypadku utraty formatowania należy zaznaczyć akapit i zastosować styl akapitowy
„Listing”.
Pamiętaj aby umieszczać wszystkie, a zarazem tylko te informacje, które zostały
określone w treści rozdziału. W szczególności nie możesz zignorować jawnie
zasugerowanych sposobów filtrowania zawartości listingów.
```

2. Bieżąca i zachowawcza przynależność do grup – Linux.

Utwórz grupę *proba* (addgroup). Na przykładzie tej grupy i wybranego użytkownika (bolek, lolek lub tola) wykaż że dodanie użytkownika do grupy nie wpływa na tożsamość w już otwartej powłoce.

Wskazówka: schemat postępowania nie różni się od tego zastosowanego w przypadku systemu Windows.

Uwaga: musisz wykazać, że użytkownik został dodany do grupy w konfiguracji zachowawczej oraz sprawdzić tożsamość bieżącą w powłoce. Przeanalizuj różnicę w działaniu polecenia **id <nazwa>** oraz **id** bez argumentów.

Sugestia: przekonaj się, czy zmiana zostanie uwzględniona po otwarciu nowej powłoki.

```
Miejsce na wklejenie listingu.
W przypadku utraty formatowania należy zaznaczyć akapit i zastosować styl akapitowy
„Listing”.
Pamiętaj aby umieszczać wszystkie, a zarazem tylko te informacje, które zostały
określone w treści rozdziału. W szczególności nie możesz zignorować jawnie
zasugerowanych sposobów filtrowania zawartości listingów.
```

3. Ograniczenia hasła – Windows.

Ustaw minimalną długość hasła (net accounts) na 8 znaków. Sprawdź, czy próba ustawienia hasła (net user) nie spełniającego tego wymagania dla wybranego użytkownika (bolek, lolek lub tola) powiedzie się.

```
Miejsce na wklejenie listingu.
W przypadku utraty formatowania należy zaznaczyć akapit i zastosować styl akapitowy
„Listing”.
Pamiętaj aby umieszczać wszystkie, a zarazem tylko te informacje, które zostały
określone w treści rozdziału. W szczególności nie możesz zignorować jawnie
zasugerowanych sposobów filtrowania zawartości listingów.
```

4. Ograniczenia hasła – Linux.

Ustaw minimalną długość hasła (/etc/pam.d/common-password)(man pam_unix) na 8 znaków. **Jako potwierdzenie wykonania operacji wypisz dokładnie jedną niezbędną linię z tego pliku (grep). Sprawdź, czy próba ustawienia hasła (passwd) nie spełniającego tego wymagania dla wybranego użytkownika (bolek, lolek lub tola) powiedzie się w**

przypadku, kiedy użytkownik uprzywilejowany ustawia hasło wybranego użytkownika oraz w przypadku, gdy użytkownik samodzielnie ustawia własne hasło.

Wskazówka: Przeanalizuj różnicę w działaniu polecenia **passwd <nazwa>** oraz **passwd** bez argumentów.

```
Miejsce na wklejenie listingu.
W przypadku utraty formatowania należy zaznaczyć akapit i zastosować styl akapitowy
„Listing”.
Pamiętaj aby umieszczać wszystkie, a zarazem tylko te informacje, które zostały
określone w treści rozdziału. W szczególności nie możesz zignorować jawnie
zasugerowanych sposobów filtrowania zawartości listingów.
```