

WDI Zadanie 1

Obszar tematyczny 1: Sesje użytkowników, zmiana tożsamości poprzez sudo, su, runas; blokady i inne ograniczenia.

Windows:

!!! PO PIERWSZE TRZEBA PAMIĘTAĆ ŻEBY ODPALIĆ POWERSHELLA JAKO ADMINISTRATOR !!!

1. Czy zablokowanie konta tola (bez zmiany terminu ważności konta i hasła dla tola) uniemożliwi kontynuację pracy w otwartej wcześniej powłoce sudo, su i runas przez tołą?

1. Najpierw trzeba zrobić użytkownika tola:

New-LocalUser tola

Po tym podajemy hasło użytkownika i dostajemy takie coś

```
dgradowski(A)@251524-WDI 15.11.2023 20:11 C:\Windows\system32> New-LocalUser tola

cmdlet New-LocalUser at command pipeline position 1
Supply values for the following parameters:
Password: ***

Name Enabled Description
----
tola True

dgradowski(A)@251524-WDI 15.11.2023 20:12 C:\Windows\system32> _
```

2. Jako użytkownik trzeba uruchomić nową powłokę, której nie wyłączamy aż do momentu jak nie skończymy odpowiadać z pierwszego obszaru tematycznego
runas /user:tolal powershell

```
Administrator: Windows PowerShell

dgradowski(A)@251524-WDI 15.11.2023 20:20 C:\Windows\system32> runas /user:tolal powershell
Wpisz hasło dla tola:
Attempting to start powershell as user "251524-WDI\tolal" ...

powershell (running as 251524-WDI\tolal)

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

tolal(U)@251524-WDI 15.11.2023 20:20 C:\Windows\system32>
```

3. Trzeba teraz zablokować konto użytkownika, aby to zrobić należy w terminalu administratora wpisać komendę:
Disable-LocalUser tola

(w razie czego komendą odwrotną jest Enable-LocalUser tola)

warto użyć komendy `Get-LocalUser tola` by wyświetlić stan konta użytkownika tola

```
Administrator: Windows PowerShell
dgradowski(A)@251524-WDI 15.11.2023 20:20 C:\Windows\system32> runas /user:tolu powershell
Wpisz hasło dla tola:
Attempting to start powershell as user "251524-WDI\tolu" ...
dgradowski(A)@251524-WDI 15.11.2023 20:20 C:\Windows\system32> Disable-LocalUser tola
dgradowski(A)@251524-WDI 15.11.2023 20:21 C:\Windows\system32>
dgradowski(A)@251524-WDI 15.11.2023 20:22 C:\Windows\system32>
dgradowski(A)@251524-WDI 15.11.2023 20:22 C:\Windows\system32> Get-LocalUser tola

Name Enabled Description
----
tolu False
```

4. Kiedy konto jest zablokowane w wcześniej otwartej jako tola powłoce wpisać dowolną komendę. Ja użyłem takiej.
whoami

```
powershell (running as 251524-WDI\tolu)
tolu(U)@251524-WDI 15.11.2023 20:27 C:\Windows\system32> whoami
251524-wdi\tolu
tolu(U)@251524-WDI 15.11.2023 20:27 C:\Windows\system32> _
```

Zapyta czy zablokowanie konta uniemożliwi prace w już otwartej powłoce.

-> Zablokowanie konta nie uniemożliwia pracy w już otwartej powłoce

2. Należy wykazać wszystkie istniejące sesje użytkowników w systemie operacyjnym i trzy ostatnie poprawne próby uwierzytelnienia użytkowników w systemie.

1. Aby wyświetlić istniejące sesje należy wpisać komendę
query user lub query session

```
dgradowski(A)@251524-WDI 20.11.2023 19:49 C:\Windows\system32> query user
USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME
>dgradowski console 1 Active none 20.11.2023 19:44
dgradowski(A)@251524-WDI 20.11.2023 19:49 C:\Windows\system32> query session
SESSIONNAME USERNAME ID STATE TYPE DEVICE
services 0 Disc
>console dgradowski 1 Active
```

2. Zeby wyświetlić ostatnie logowania trzeba wpisać taką komendę:

Get-WinEvent -FilterHashtable @{Logname='Security'; ID=4624} -MaxEvents 3

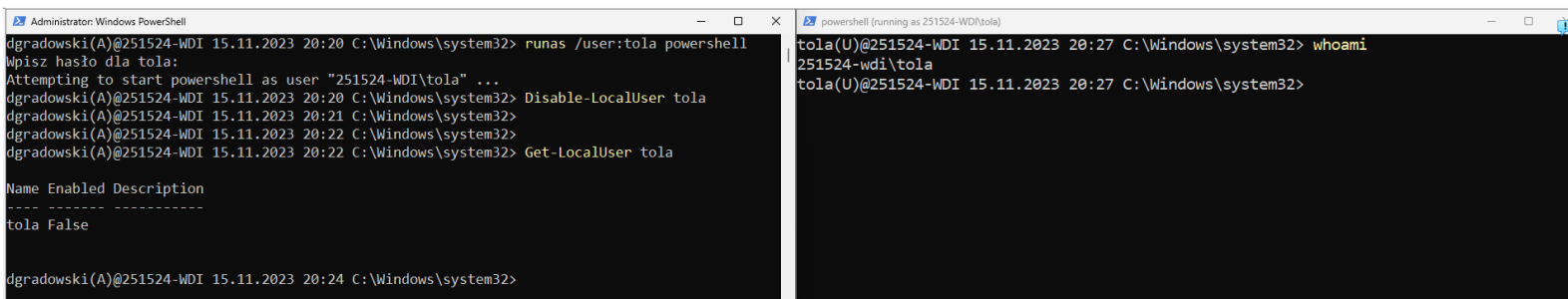
```
dgradowski(A)@251524-WDI 20.11.2023 19:59 C:\Windows\system32> Get-WinEvent -FilterHashtable @{Logname='Security'; ID=4624} -MaxEvents 3

ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated          Id LevelDisplayName Message
-----
20.11.2023 19:59:14 4624 Informacje Logowanie do konta zakończyło się pomyślnie....
20.11.2023 19:58:41 4624 Informacje Logowanie do konta zakończyło się pomyślnie....
20.11.2023 19:58:40 4624 Informacje Logowanie do konta zakończyło się pomyślnie....

dgradowski(A)@251524-WDI 20.11.2023 20:01 C:\Windows\system32>
```

Podczas odpowiedzi musi to wyglądać mniej więcej tak:



```
dgradowski(A)@251524-WDI 15.11.2023 20:20 C:\Windows\system32> runas /user:tola powershell
Wpisz hasło dla tola:
Attempting to start powershell as user "251524-WDI\tola" ...
dgradowski(A)@251524-WDI 15.11.2023 20:20 C:\Windows\system32> Disable-LocalUser tola
dgradowski(A)@251524-WDI 15.11.2023 20:21 C:\Windows\system32>
dgradowski(A)@251524-WDI 15.11.2023 20:22 C:\Windows\system32> Get-LocalUser tola

Name Enabled Description
-----
tola False

dgradowski(A)@251524-WDI 15.11.2023 20:24 C:\Windows\system32>

dgradowski(A)@251524-WDI 20.11.2023 20:01 C:\Windows\system32> query user
USERNAME      SESSIONNAME  ID STATE  IDLE TIME  LOGON TIME
>dgradowski   console      1 Active   8 20.11.2023 19:44
dgradowski(A)@251524-WDI 20.11.2023 20:07 C:\Windows\system32> Get-WinEvent -FilterHashtable @{Logname='Security'; ID=4624} -MaxEvents 3

ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated          Id LevelDisplayName Message
-----
20.11.2023 19:59:14 4624 Informacje Logowanie do konta zakończyło się pomyślnie....
20.11.2023 19:58:41 4624 Informacje Logowanie do konta zakończyło się pomyślnie....
20.11.2023 19:58:40 4624 Informacje Logowanie do konta zakończyło się pomyślnie....

dgradowski(A)@251524-WDI 20.11.2023 20:07 C:\Windows\system32> _
```

Linux

1. Czy zablokowanie konta tola (bez zmiany terminu ważności konta i hasła dla tola) uniemożliwi kontynuację pracy w otwartej wcześniej powłoce sudo, su i runas przez tole?

1. Najpierw trzeba zrobić użytkownika tola:

Sudo su

Useradd -m konto -s /bin/bash

Passwd konto

2. Jako użytkownik trzeba uruchomić nową powłokę, której nie wyłączamy aż do momentu jak nie skończymy odpowiadać z pierwszego obszaru tematycznego. Trzeba odpalić w nich 2 okna terminala i w każdym z nich odpalić po jednej komendzie:

Su konto

Sudo -u konto /bin/bash

3. Trzeba teraz zablokować konto użytkownika, aby to zrobić należy w terminalu administratora wpisać komendę:

Passwd -l konto

4. Kiedy konto jest zablokowane w wcześniej otwartej jako konto powłóce wpisać dowolną komendę. Ja użyłem takiej.

Cd ~

Ls -a

Zapyta czy zablokowanie konta uniemożliwi prace w już otwartej powłóce.

-> Zablokowanie konta nie uniemożliwia pracy w już otwartej powłóce

2. Należy wykazać wszystkie istniejące sesje użytkowników w systemie operacyjnym i trzy ostatnie poprawne próby uwierzytelnienia użytkowników w systemie.

3. Aby wyświetlić istniejące sesje należy wpisać komendę
who

4. Zeby wyświetlić ostatnie logowania trzeba wpisać taką komendę:

last | grep -v reboot -m 3

Podczas odpowiedzi musi to wyglądać mniej więcej tak:

Nie chce mi się screena robić 😊

Obszar tematyczny 2: Konfiguracja bieżąca i zachowawcza na przykładzie usług (realizacja Windows lub Linux)

1. Należy wyszukać usługę systemową odpowiedzialną za obsługę wydruku (wyszukać usługi po frazie "druk" lub "print"). Należy określić czy usługa ta jest włączona czy wyłączona w konfiguracji bieżącej i zachowawczej.

```
Get-Service -DisplayName "*druk*"
```

```
Get-Service -Name "Spooler" | Select-Object DisplayName, ServiceName, Status, StartType
```

Uwaga: Status jest konfiguracją bieżącą a StartType jest konfiguracją zachowawczą.

Automatic oznacza, że zostanie podjęta próba uruchomienia usługi przy uruchamianiu systemu operacyjnego.

2. Dla usługi wydruku należy zmienić status konfiguracji bieżącej i zachowawczej na przeciwny (tzn. jeżeli usługa była włączona to ją wyłączyć, a jeżeli była wyłączona to ją włączyć).

```
Stop-Service -Name "Spooler" // Zatrzymanie usługi w systemie bieżącym
```

```
Start-Service -Name "Spooler" // Uruchomienie usługi w systemie bieżącym
```

```
Set-Service -Name "Spooler" -StartupType Automatic // Ustawienie automatycznego uruchamiania w statusie zachowawczym - podejmuje próbę uruchomienia podczas startu systemu operacyjnego
```

```
Set-Service -Name "Spooler" -StartupType Manual // Ustawienie manualnego uruchamiania w statusie zachowawczym - uruchamia, gdy jest to konieczne i wymaga ręcznego uruchomienia przez użytkownika lub inną usługę Status - system bieżący, StartType
```

Obszar tematyczny 3: analiza dzienników zdarzeń (realizacja Windows i Linux)

1. Należy wyświetlić najnowsze 5 zdarzeń o priorytecie błąd oraz wszystkie istotniejsze niż błąd z systemowego dziennika zdarzeń. Dla najnowszego z wyszukanych zdarzeń należy określić czas i źródło zdarzenia oraz zarejestrowany w dzienniku komunikat.

Windows:

```
Get-Winevent -FilterHashtable @{Logname="System"; Level=1,2} -Maxevents 5 | Format-List
```

```
Get-WinEvent -FilterHashtable @{Logname="System"; Level=1,2} -MaxEvents 1 | Select-Object TimeCreated, ProviderName, Message | Format-Table -Wrap
```

A to linuxa:

```
sudo journalctl -p 3 -n 5
```

```
sudo journalctl -p 3 -n 1
```

```
[dgradowski@251524-WDI ttyid:0 wto lis 21 22:16:05 ~]$ sudo journalctl -p3 -n 5
lis 21 22:39:37 251524-WDI connmand[512]: The name net.connman.vpn was not provided by any .service files
lis 21 22:15:29 251524-WDI lightdm[923]: gkr-pam: unable to locate daemon control file
lis 21 22:15:30 251524-WDI pulseaudio[947]: Usługa ALSA została wybudzona, aby zapisać nowe dane do urządzenia, ale nie było nic do zapisania.
lis 21 22:15:30 251524-WDI pulseaudio[947]: Prawdopodobnie jest to błąd w sterowniku ALSA „snd_intel8x0”. Proszę zgłosić ten problem programistom usługi ALSA.
lis 21 22:15:30 251524-WDI pulseaudio[947]: Wybudzono za pomocą ustawienia POLLOUT – ale jednocześnie wywołanie snd_pcm_avail() zwróciło zero lub inną wartość < min_avail.
[dgradowski@251524-WDI ttyid:0 wto lis 21 22:16:09 ~]$ ^C
[dgradowski@251524-WDI ttyid:0 wto lis 21 22:17:55 ~]$
```

Na screenie są pokazane źródła zdarzenia, są to procesy. To w nawiasach kwadratowych to PID.

Szybkie notatki

Po zablokowaniu użytkownika na linuxie którą komendą i jak można uruchomić powłokę?

Po zablokowaniu usera uruchomić nową powłokę przy pomocy komendy sudo, ale nie przy pomocy su.

Odpalić to można papierosa lub raketę, powłokę się uruchamia – tak samo jak system operacyjny.

System nie jest systemem, a systemem operacyjnym – jest to w chuj ważne.

Zalogowanie użytkownika robi nową sesję, a wylogowanie ją kończy.

Co to znaczy manual i automatic?

Co to konfiguracja bieżąca a zachowawcza?

W 3.1 na Windowsie najnowsze zdarzenie musi mieć pełny komunikat!