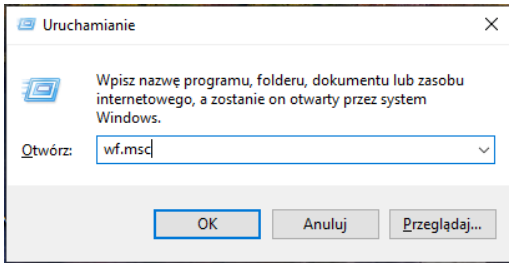
Zadanie 1 - Opracować 5 metod hardeningu systemów Windows.

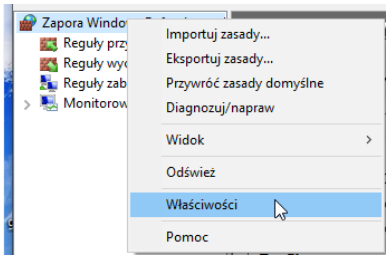
Metoda 1

Skonfiguruj Windows Firewall z regułami „deny-by-default” dla przychodzących; dodaj tylko niezbędne wyjątki.

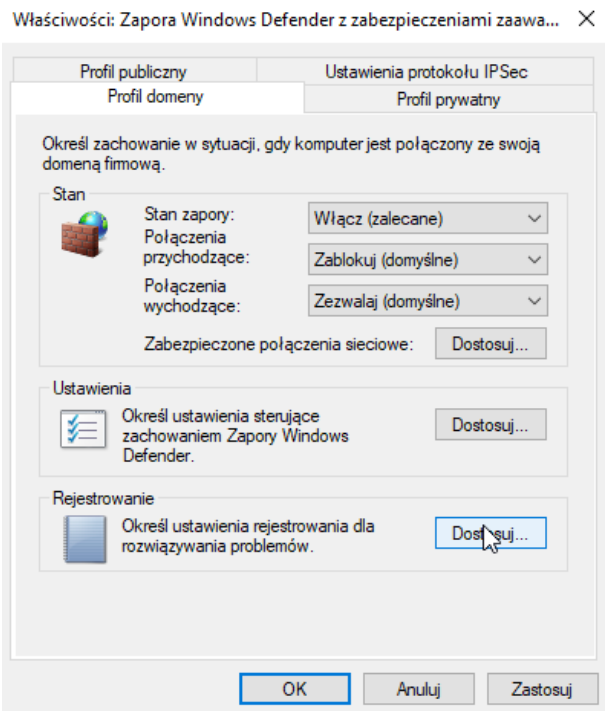
- Ustaw “blokuj wszystkie przychodzące” (dla wszystkich profili)
  1. Naciśnij Win + R → wpisz wf.msc → Enter.



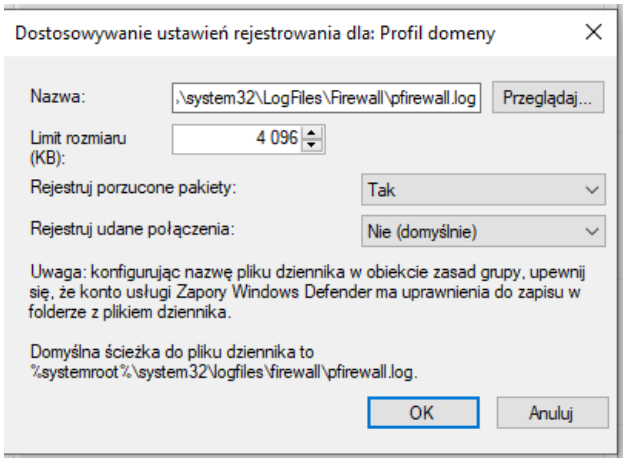
  2. U góry kliknij Zapora systemu Windows z zabezpieczeniami zaawansowanymi (prawy przycisk) → Właściwości.



  3. Zakładka Profil domeny:
     a) Stan zapory: Włączone
     b) Połączenia przychodzące: Zablokuj
     c) Połączenia wychodzące: Zezwalaj

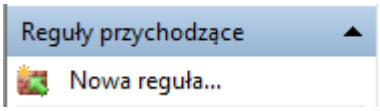


4. Kliknij Dostosuj… przy Rejestrowaniu → Rejestruj połączenia porzucone: Tak, ścieżka zostaje domyślna → OK.

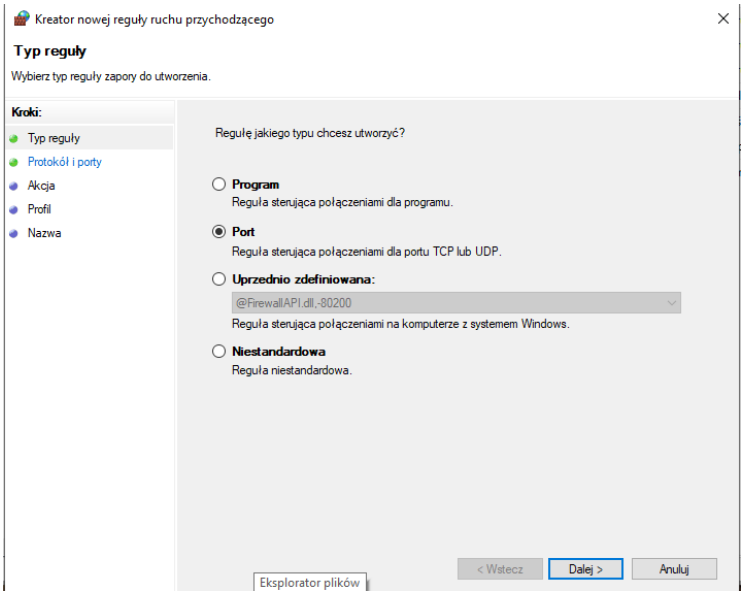


5. Powtórz punkt 1.3 dla Profil prywatny i Profil publiczny → OK.

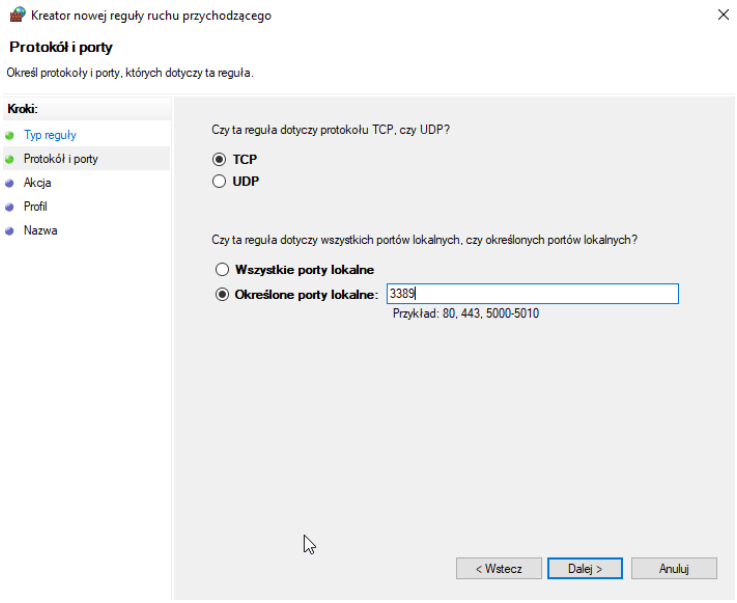
- Dodaj tylko niezbętne wyjątki
  1. RDP (port 3389) tylko z Twojej sieci admina (np. 10.0.0.0/24)
     a) W lewej kolumnie: Reguły przychodzące → Nowa reguła…



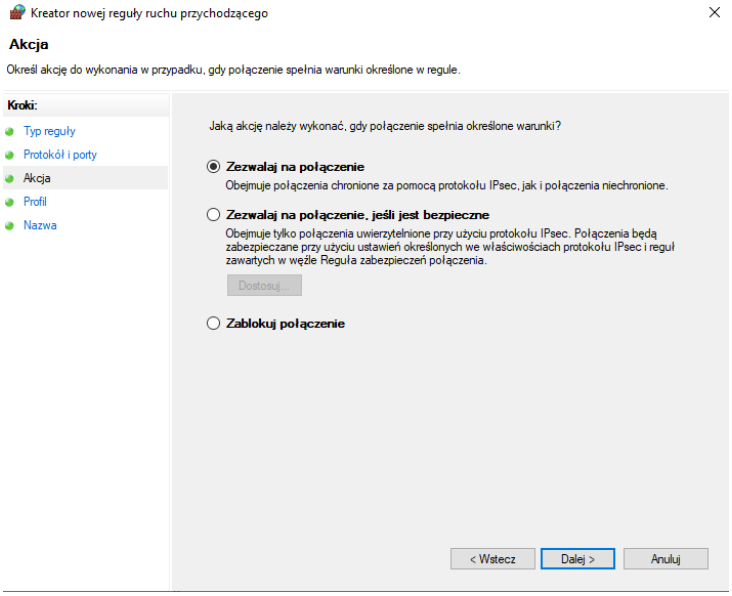
     b) Port → Dalej.



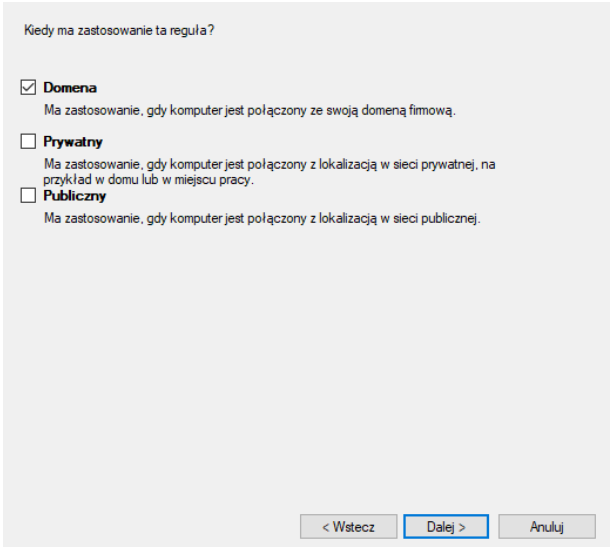
     c) TCP, Określone porty lokalne: wpisz 3389 → Dalej.



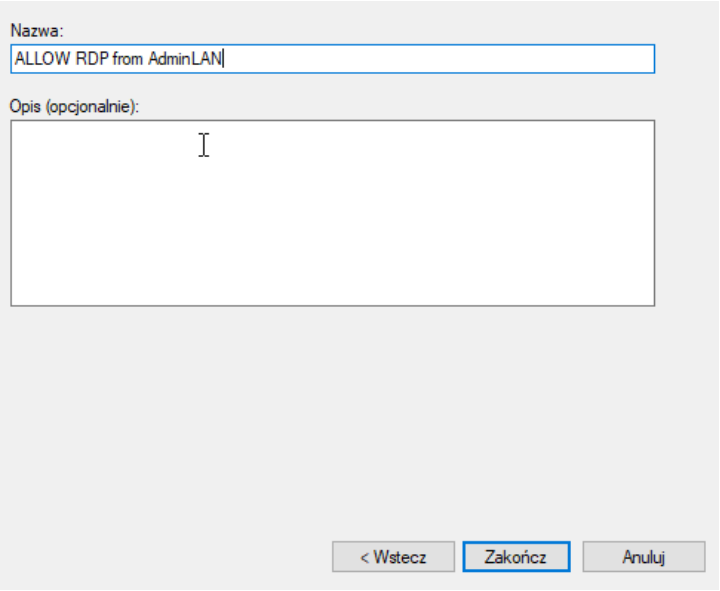
d) Zezwalaj na połączenie → Dalej.



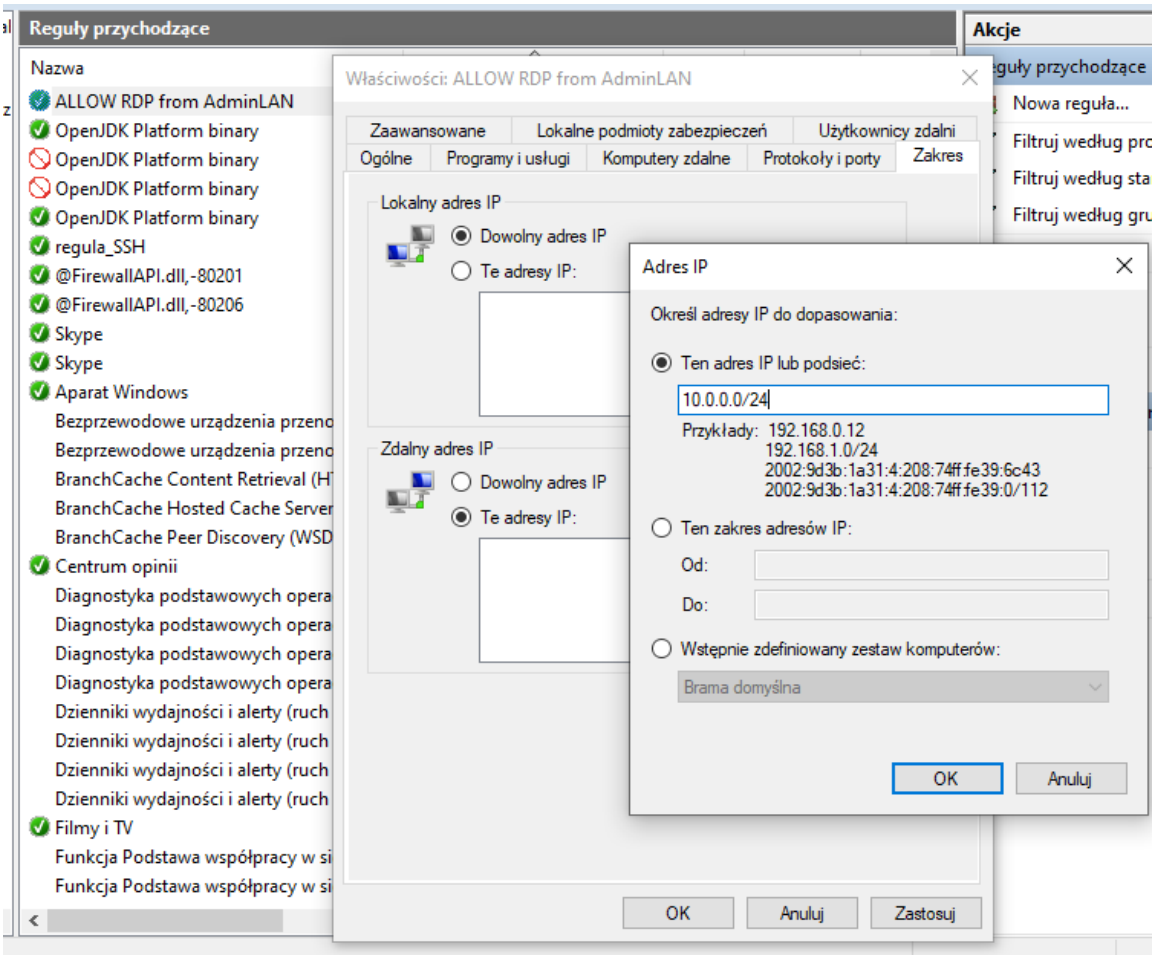
e) Zaznacz tylko profil Domena (jeśli serwer w domenie) → Dalej.



f) Nazwa: ALLOW RDP from AdminLAN → Zakończ.



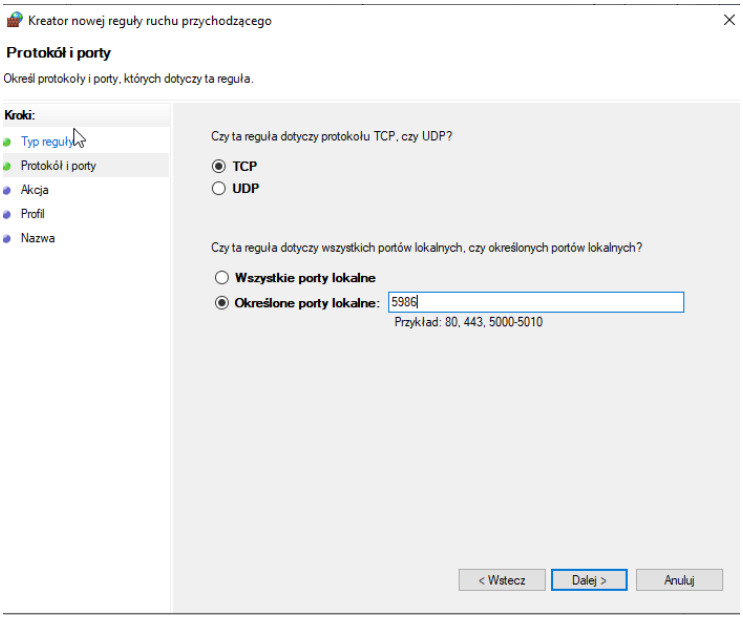
g) Odszukaj tę regułę na liście → Dwuklik → zakładka Zakres →
   - Zdalne adresy IP: Dodaj → wpisz 10.0.0.0/24 → OK → OK.
     (teraz RDP działa tylko z tej podsieci)



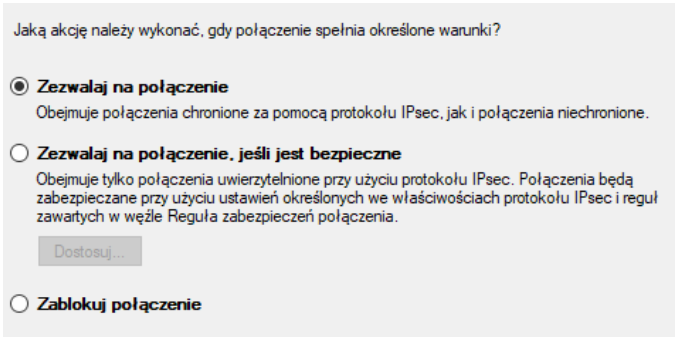
2. WinRM po HTTPS (port 5986) tylko z bastionu (np. IP 10.0.10.5)

a) Reguły przychodzące → Nowa reguła…

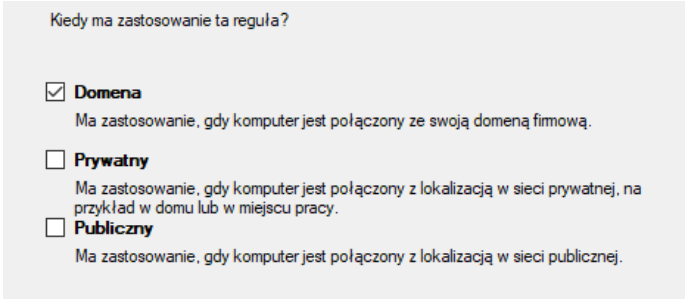
b) Port → TCP → 5986 → Dalej.



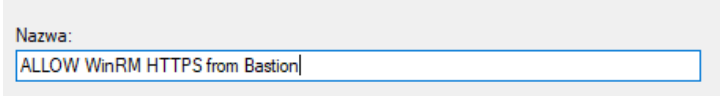
c) Zezwalaj na połączenie → Dalej.



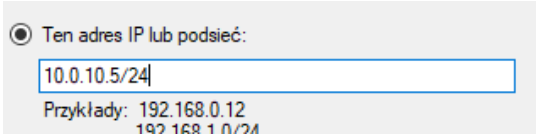
d) Profil: Domena → Dalej.



e) Nazwa: ALLOW WinRM HTTPS from Bastion → Zakończ.



f) Dwuklik reguły → Zakres → Zdalne adresy IP → Dodaj → 10.0.10.5 → OK.



3. (Tylko jeśli to ten serwer) DNS – port 53
   a) Zrób dwie reguły jak wyżej: jedną UDP 53, drugą TCP 53.

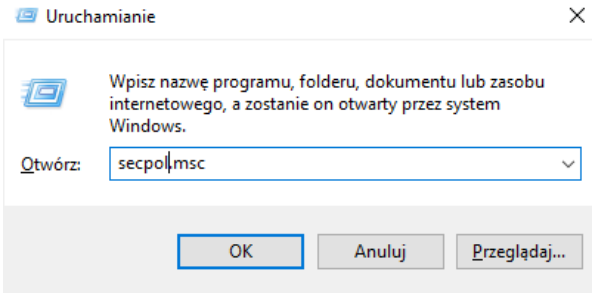
b) Profil zwykle Domena.
c) Jeśli możesz, ogranicz Zakres do podsieci klientów.

- Wyłącz szerokie stare reguły
  1. W Regułach przychodzących poszukaj reguł typu „Zezwalaj RDP z dowolnego adresu”.
  2. Kliknij na nie prawym → Wyłącz regułę.
- Szybka weryfikacja
  1. W oknie głównym (Właściwości zapory) upewnij się, że Połączenia przychodzące = Zablokuj dla wszystkich profili.
  2. Z komputera w dozwolonej sieci połącz się RDP — powinno działać.
  3. Z komputera poza dozwoloną siecią spróbuj RDP — powinno blokować.

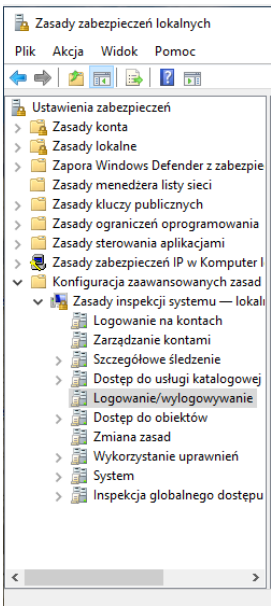
Metoda 2

Włącz i ustandaryzuj rejestrowanie: Advanced Audit Policy, PowerShell (Module, ScriptBlock, Transcription), Object Access.

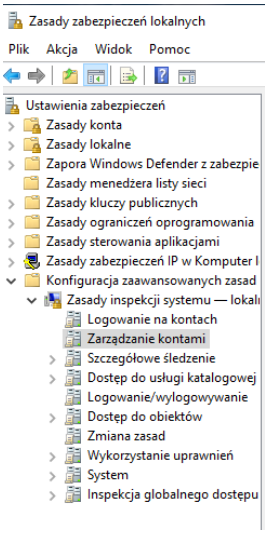
- Otwórz lokalne zasady zabezpieczeń (secpol.msc)
  1. Naciśnij Win + R
  2. Wpisz: secpol.msc → Enter



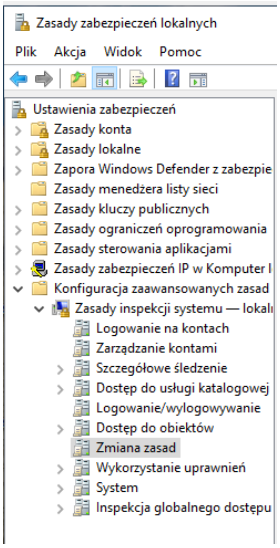
  3. Otworzy się okno Zasady zabezpieczeń lokalnych
  4. Przejdź do:
     Zasady zaawansowanego inspekcjonowania (Advanced Audit Policy Configuration) → Konfiguracja komputera → Ustawienia systemu Windows → Ustawienia zabezpieczeń → Zaawansowana konfiguracja inspekcji
- Włącz kluczowe kategorie audytu
  1. W lewej kolumnie znajdź i po kolei wybierz poniższe kategorie:
     a) Logon/Logoff



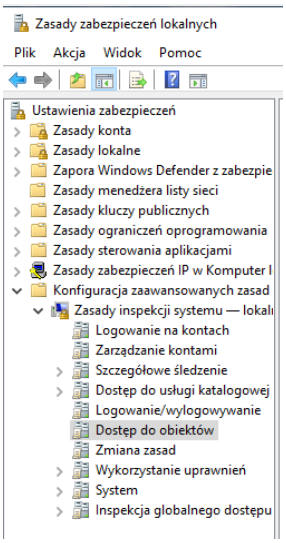
b) Account Management



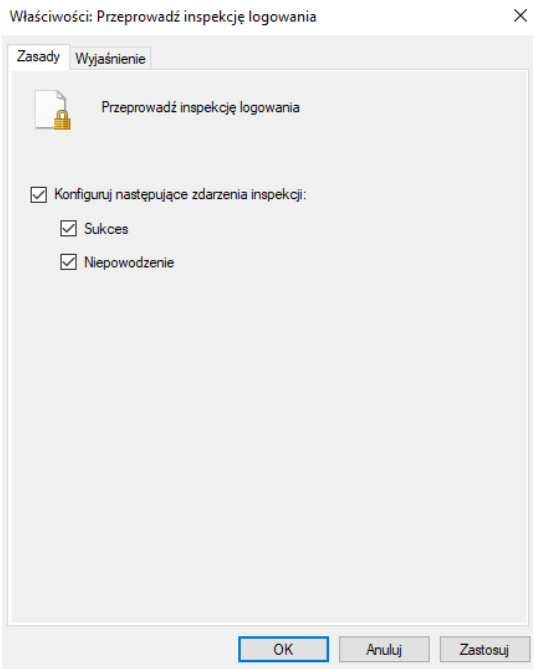
c) Policy Change



d) Object Access

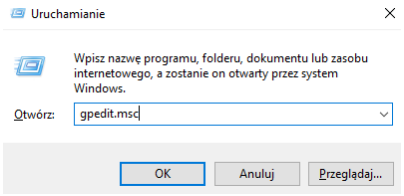


2. W każdej z nich kliknij np. Audit Logon (lub „Inspekcja logowania”)
3. Zaznacz:
   a) Skonfigurowano tę kategorię zasad
   b) Sukces i Niepowodzenie

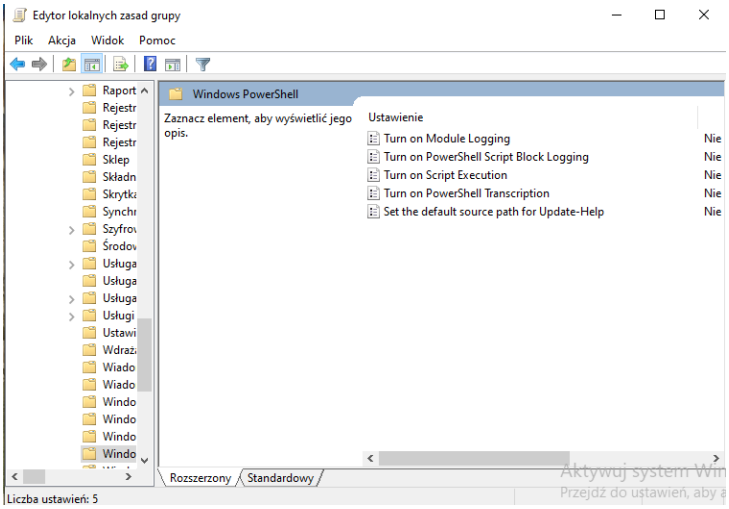


4. Kliknij OK
5. Powtórz to samo dla:
   a) Audit Account Management
   b) Audit Policy Change
   c) Audit Object Access

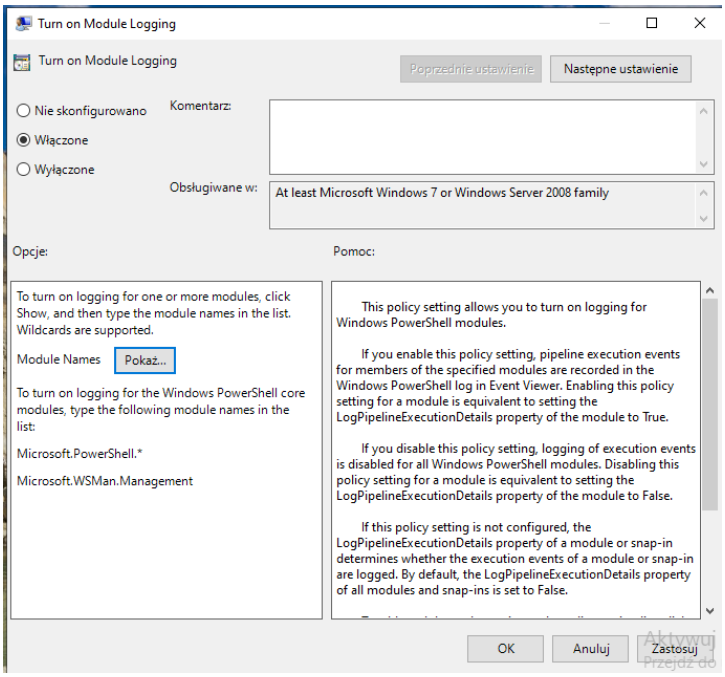
- Włącz rejestrowanie PowerShella
  1. Naciśnij Win + R, wpisz gpedit.msc → Enter



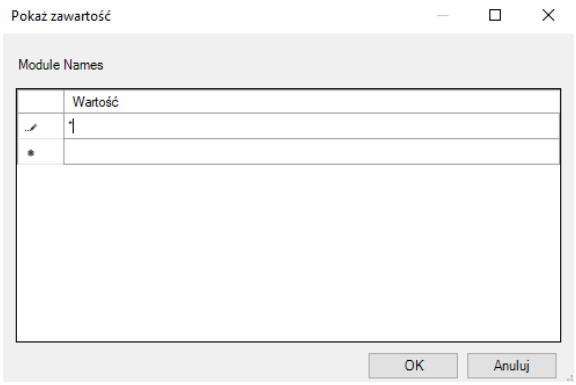
2. Przejdź do:
   Konfiguracja komputera → Szablony administracyjne → Windows Components → Windows PowerShell



3. Teraz włącz trzy funkcje:
   a) Module Logging
      - Otwórz Turn on Module Logging
      - Ustaw na Enabled

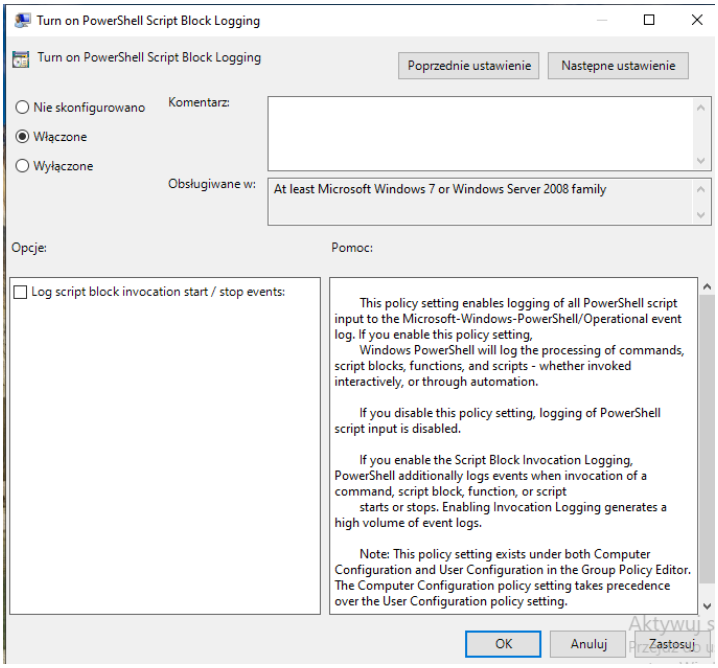


      - W polu Module Names wpisz: *
        (oznacza logowanie wszystkich modułów)

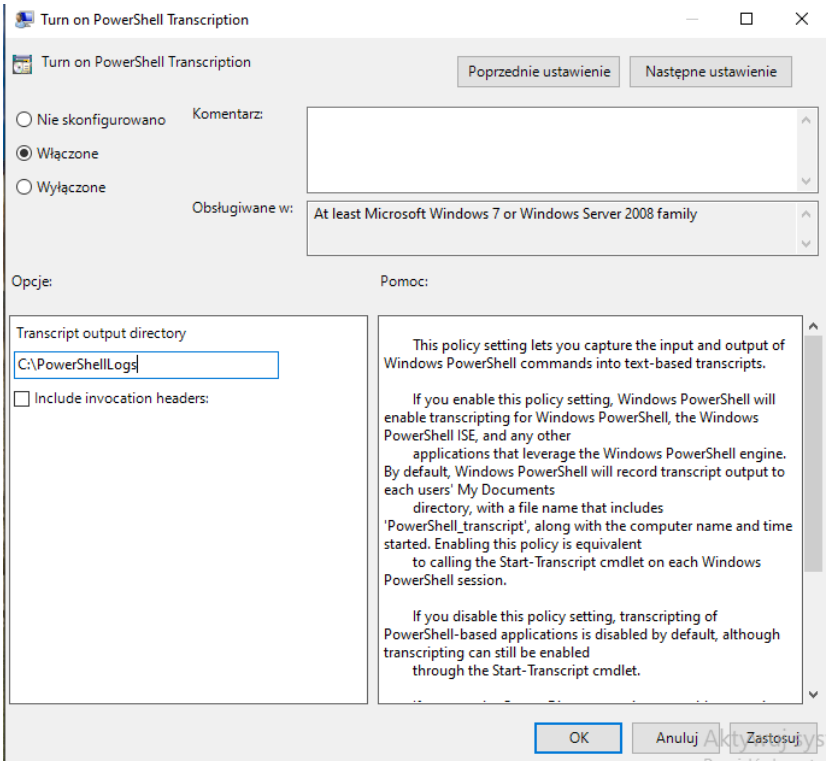


- Kliknij OK

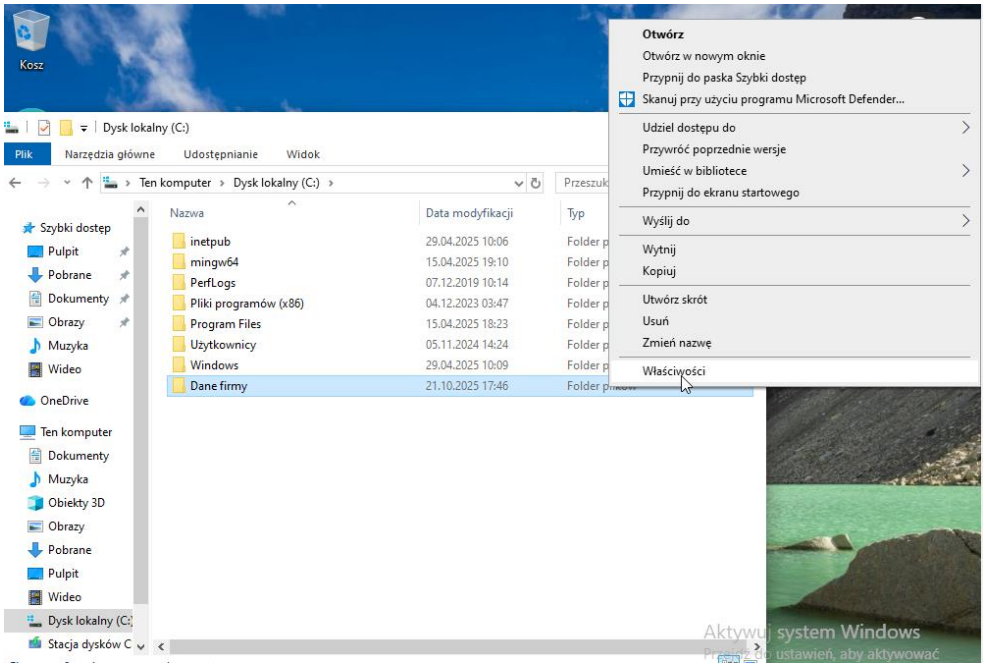
b) Script Block Logging
   - Otwórz Turn on PowerShell Script Block Logging
   - Ustaw na Enabled → OK



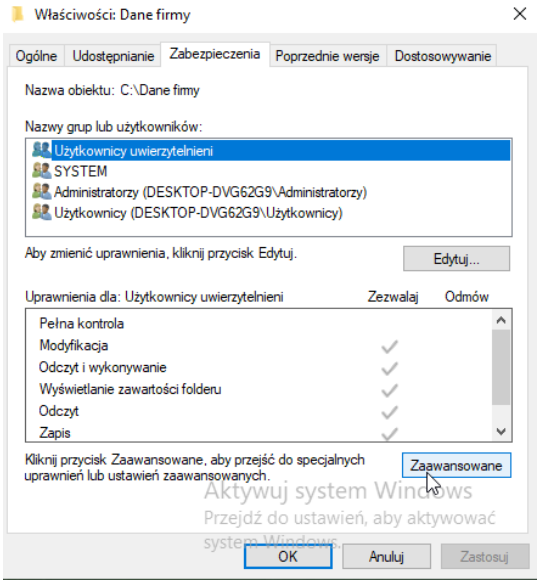
c) Transcription (pełna transkrypcja sesji)
   - Otwórz Turn on PowerShell Transcription
   - Ustaw na Enabled
   - W polu Output Directory wpisz: C:\PowerShellLogs
   - Kliknij OK



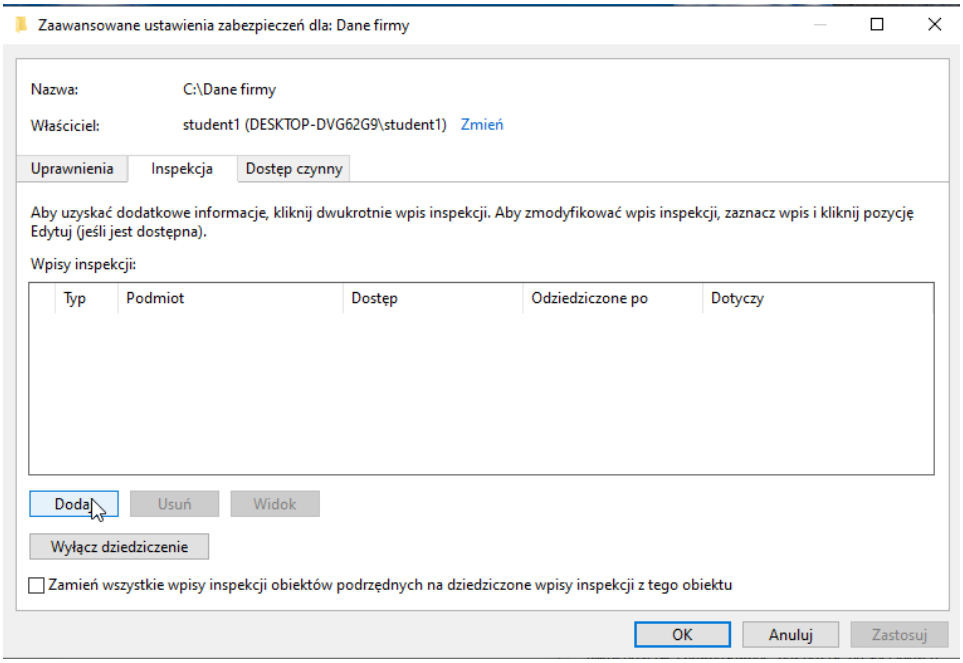
- Włącz rejestrowanie dostępu do plików (Object Access)
  1. Kliknij prawym przyciskiem myszy na folder, który chcesz monitorować (np. C:\DaneFirmy)



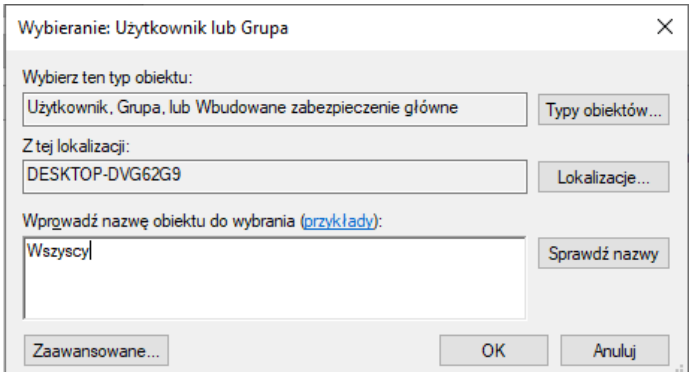
  2. Wybierz Właściwości → Zabezpieczenia → Zaawansowane



3. Kliknij zakładkę Inspekcja (Auditing) → Dodaj



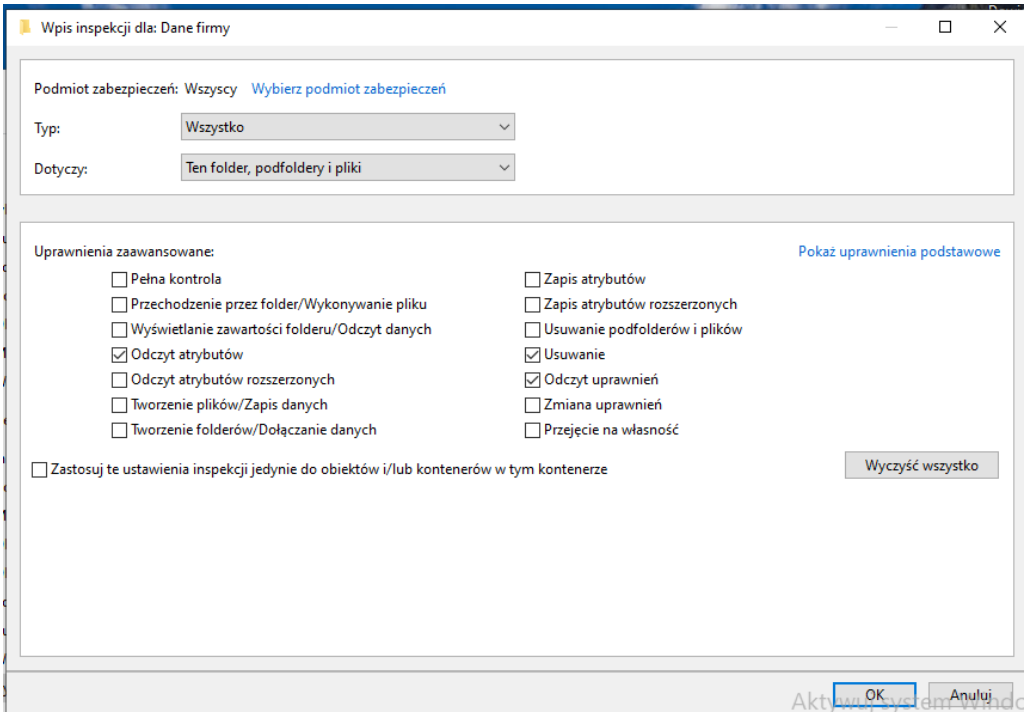
4. Kliknij Wybierz podmiot → wpisz Everyone → OK



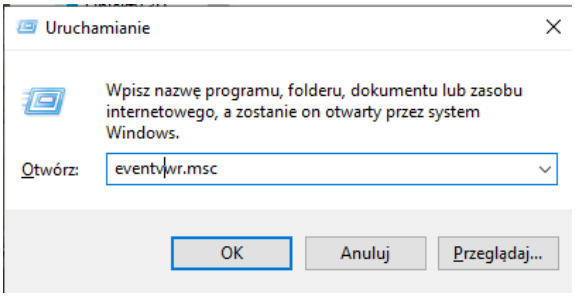
5. Typ: Sukces i Niepowodzenie
6. Zaznacz pola np.:
   a) „Odczyt atrybutów pliku”

b) „Odczyt uprawnień”
c) „Usunięcie”

7. Zatwierdź wszystkie okna OK



- Sprawdź, czy logowanie działa
  1. Otwórz Podgląd zdarzeń (Event Viewer) → Win + R → eventvwr.msc

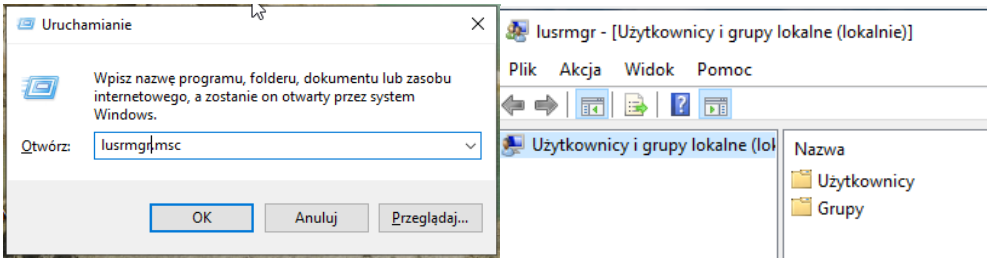


  2. Sprawdź następujące sekcje:
     a) Security
     b) Windows PowerShell → Operational
     c) C:\PowerShellLogs

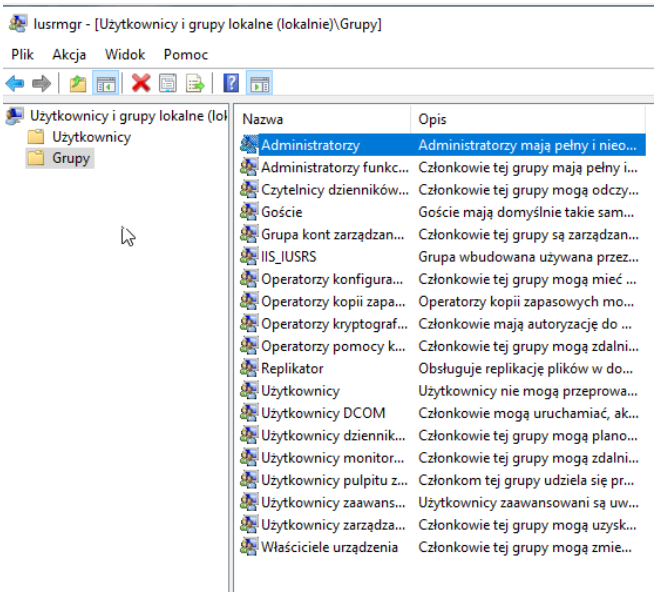
Metoda 3

Ogranicz prawa lokalne: usuń użytkowników z „Administrators/Power Users”; zastosuj „Deny log on locally/through RDP” tam, gdzie potrzebne.

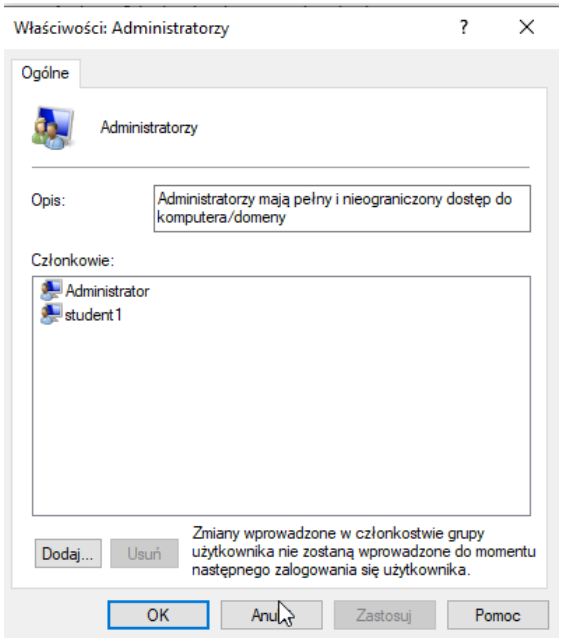
- Sprawdź kto jest w grupie Administratorzy
  1. Naciśnij Win + R → wpisz lusrmgr.msc → Enter.
     (Otworzy się „Zarządzanie komputerem lokalnym” → „Użytkownicy i grupy lokalne”).



2. Po lewej kliknij Grupy.
3. Po prawej dwukrotnie kliknij Administratorzy (Administrators).

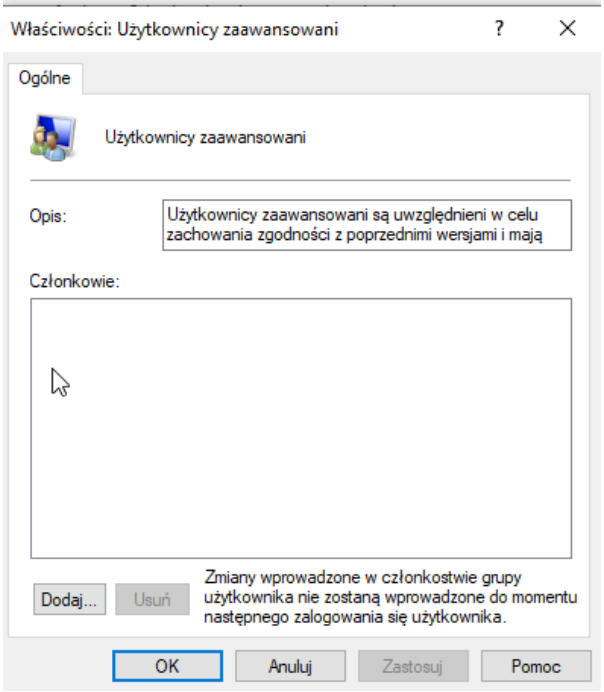


4. Sprawdź, kto tam jest. Domyślnie powinno być:
   a) Administrator
   b) ewentualnie Administrator domeny (jeśli komputer w domenie)

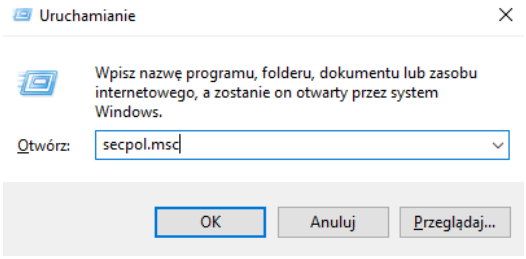


5. Jeśli zobaczysz inne konta (np. użytkowników lub „Everyone”), usuń ich z listy:
   a) Zaznacz użytkownika → Usuń → OK.

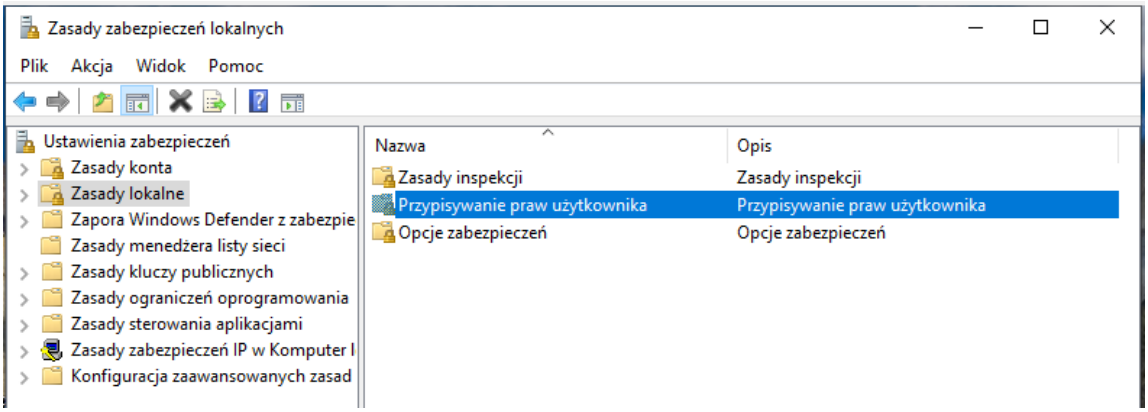
- Sprawdź grupę Power Users
    1. W tym samym miejscu kliknij Power Users.
    2. Jeśli widzisz tam jakichkolwiek użytkowników, usuń ich – ta grupa nie jest już potrzebna w nowoczesnych wersjach Windows.
    3. Kliknij OK.



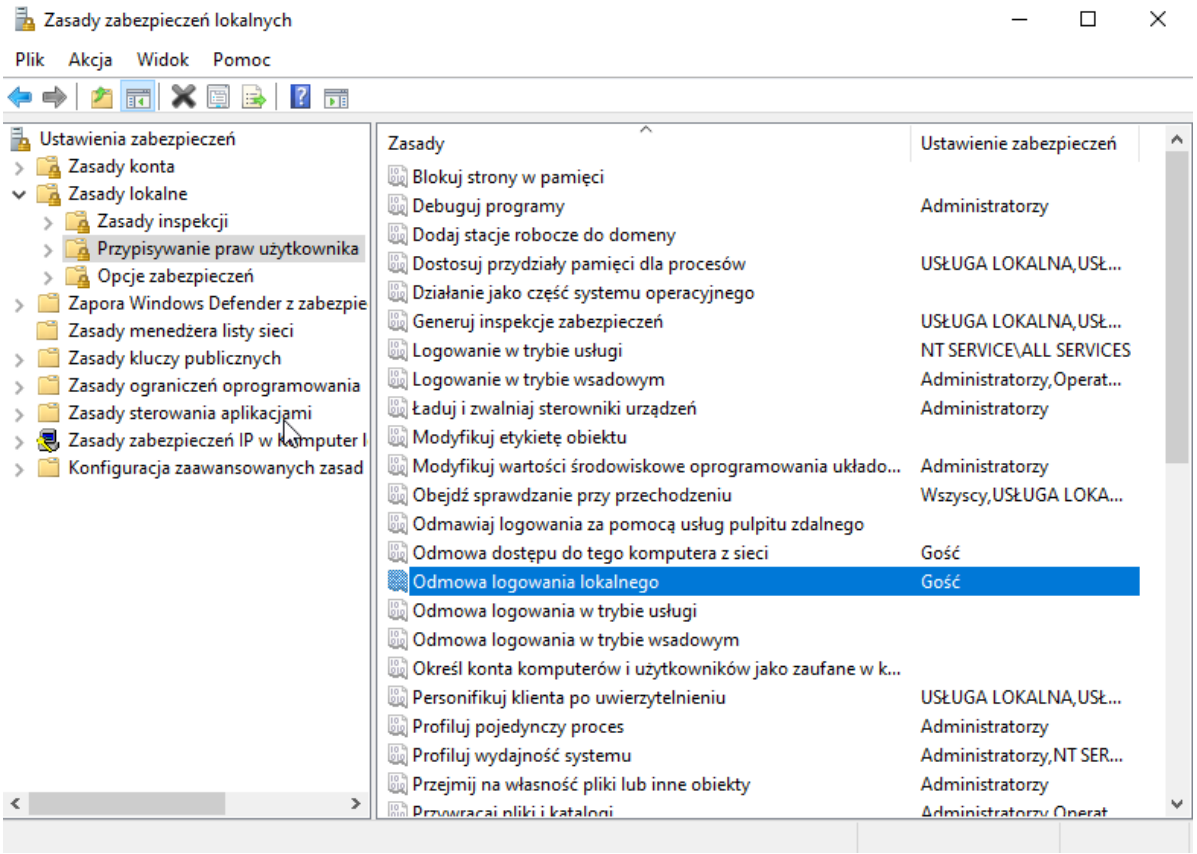
- Zastosuj zasady „Deny log on locally” (zabroń logowania lokalnego)
    1. Naciśnij Win + R → wpisz secpol.msc → Enter.



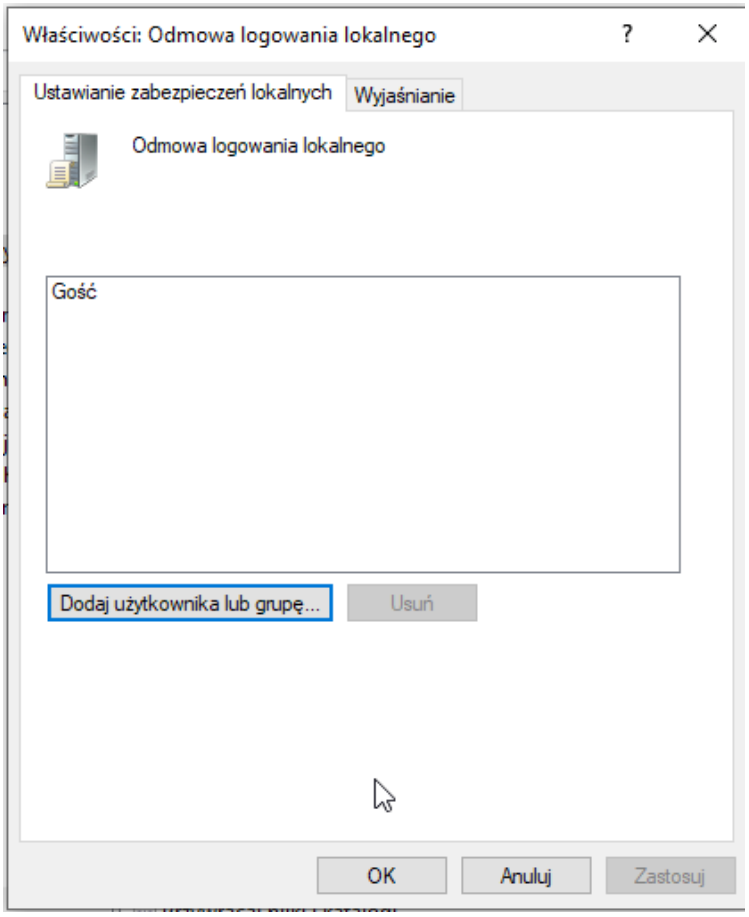
    2. Przejdź do: Zasady lokalne → Przypisywanie praw użytkownika.



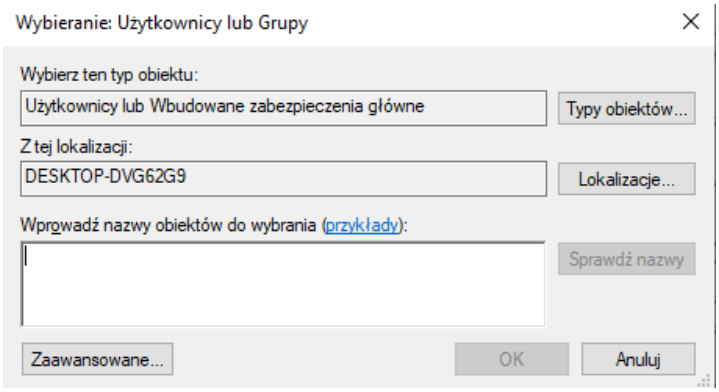
    3. Znajdź pozycję: Odmowa logowania lokalnego (Deny log on locally).



4. Dwuklik, potem Dodaj użytkownika lub grupę….

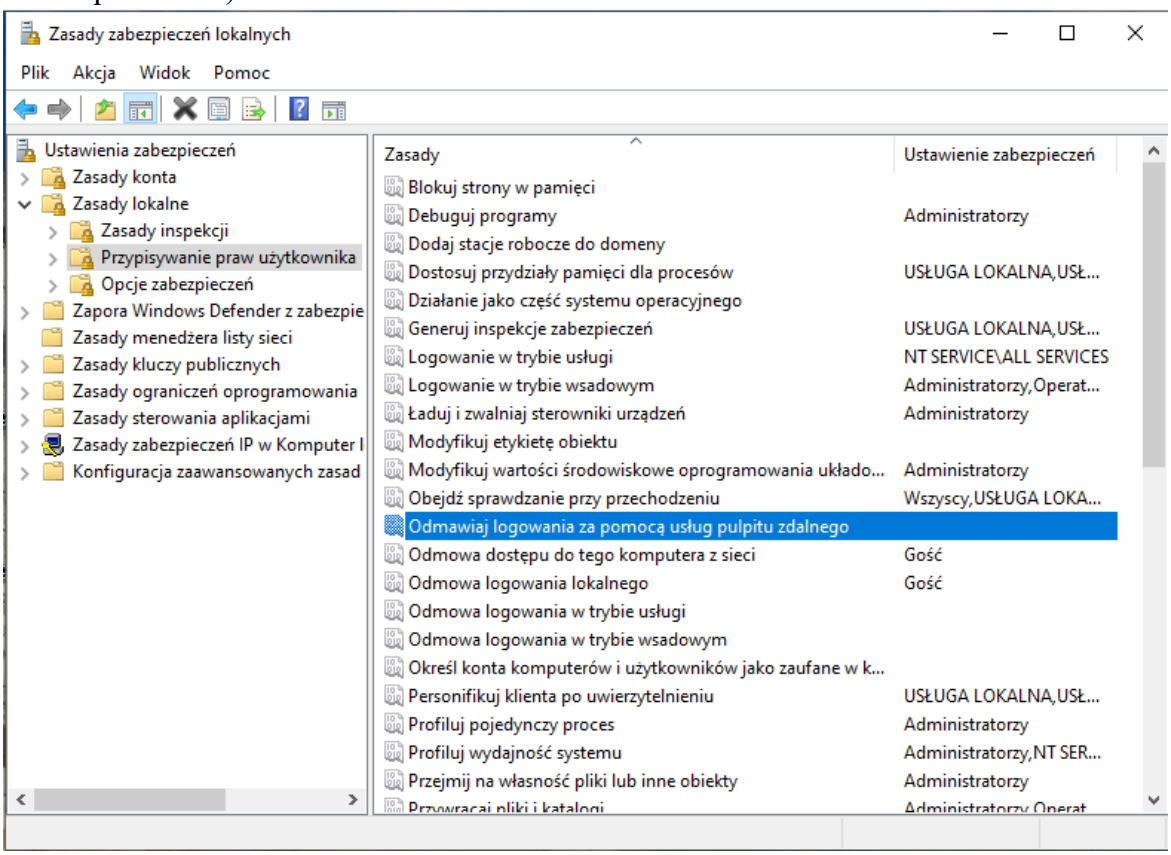


5. Wpisz nazwę konta lub grupy, które chcesz zablokować (np. Użytkownicy, Wszyscy lub konkretne konto, np. student).

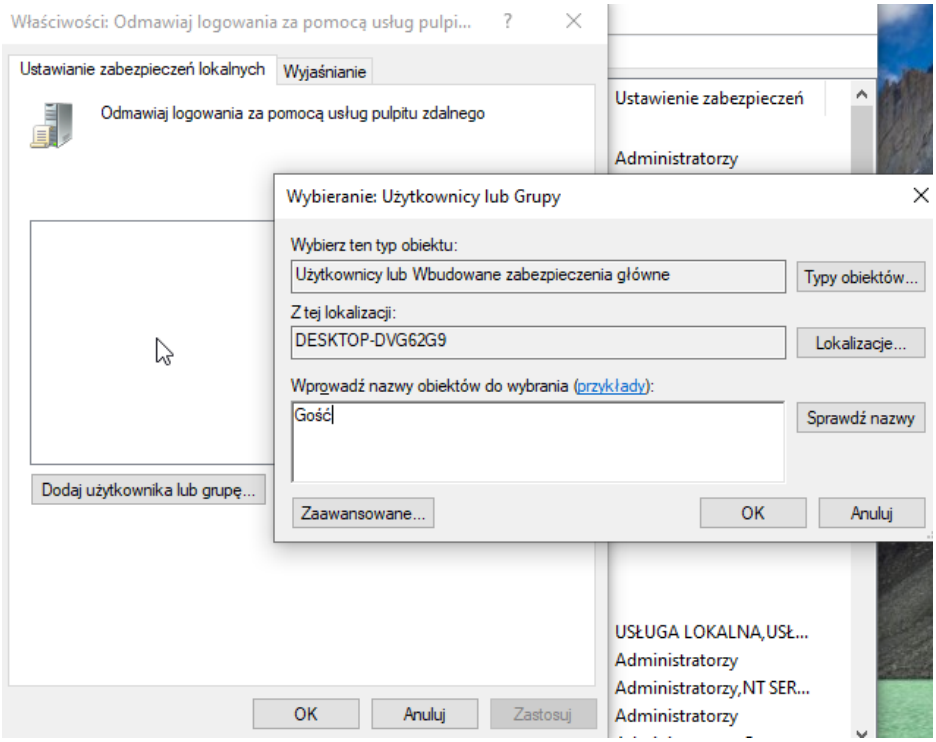


6. Kliknij OK → Zastosuj → OK.

- Zastosuj zasady „Deny log on through Remote Desktop Services”
  1. Nadal w secpol.msc → Zasady lokalne → Przypisywanie praw użytkownika,
  2. Znajdź: Odmowa logowania za pomocą usług pulpitu zdalnego (Deny log on through Remote Desktop Services).

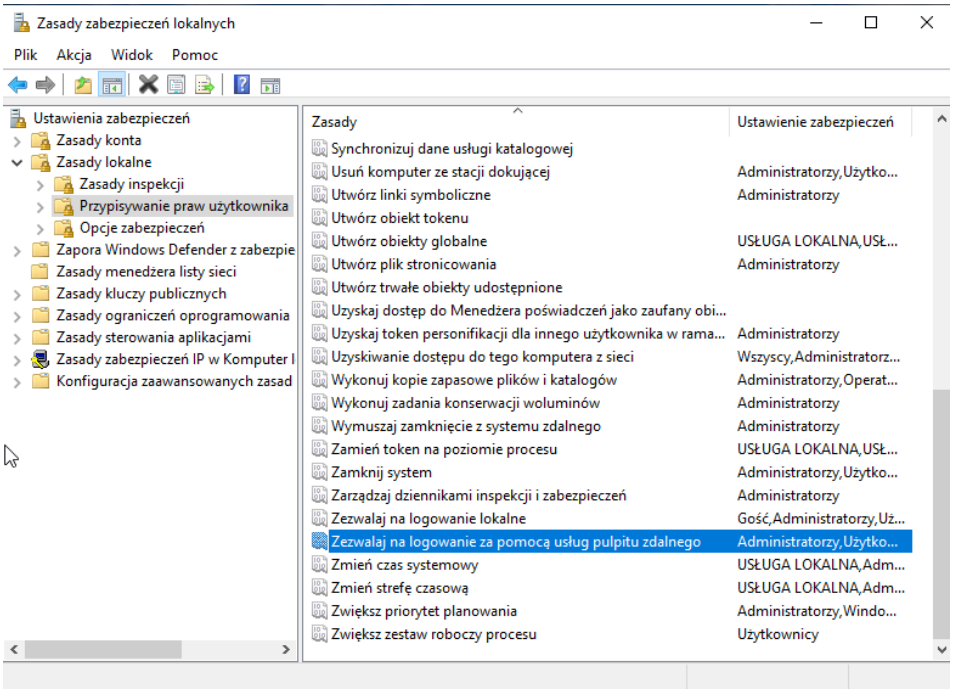


  3. Dwuklik → Dodaj użytkownika lub grupę….
  4. Wpisz:
     a) Użytkownicy
     b) lub konkretnych użytkowników, którzy nie powinni mieć RDP (np. JanNowak, Guest)

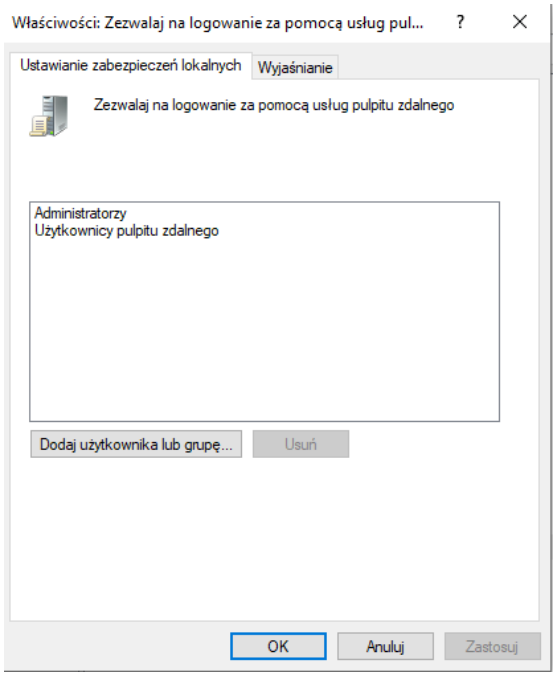


5. Kliknij OK → Zastosuj → OK.

- Sprawdź, kto ma prawo do logowania przez RDP
  1. Nadal w secpol.msc → ta sama sekcja (Przypisywanie praw użytkownika),
  2. Znajdź: Zezwalaj na logowanie przez usługi pulpitu zdalnego (Allow log on through Remote Desktop Services).



3. Powinny tam być tylko:
   a) Administratorzy
   b) lub Remote Desktop Users (jeśli istnieje taka grupa i jest kontrolowana).
4. Jeśli widzisz inne grupy (np. „Użytkownicy”), usuń je.

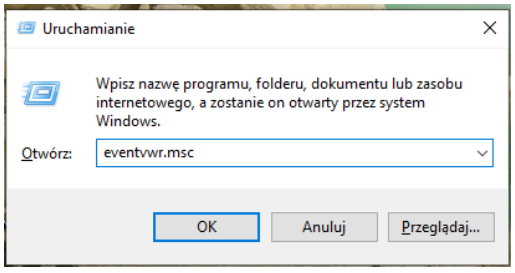


- Test
    1. Spróbuj zalogować się z konta, któremu zabroniłaś dostępu — powinien pojawić się komunikat o odmowie logowania.
    2. Sprawdź w Event Viewer → Security (ID 4625) – znajdziesz tam nieudane logowanie

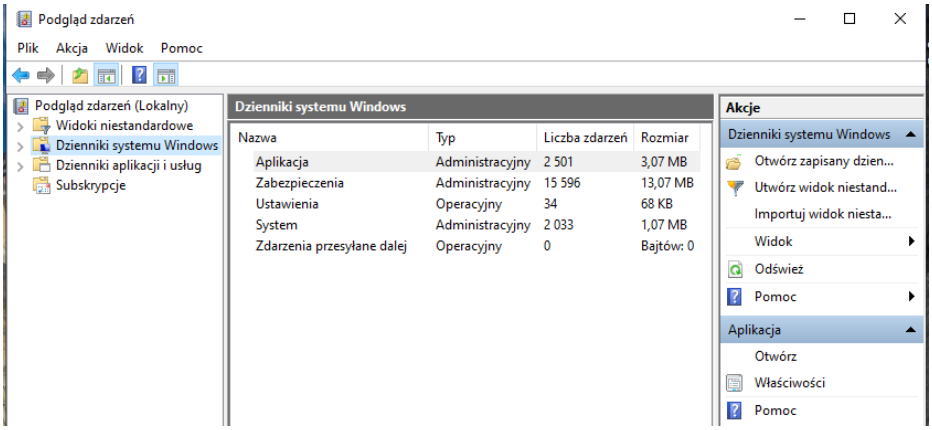
Metoda 4

Zmień domyślne kanały logów na „retention/do not overwrite” i zwiększ ich rozmiar; uzasadnij wartości.

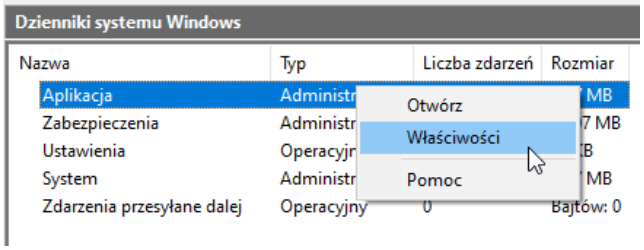
- Otwórz Podgląd zdarzeń (Event Viewer)
    1. Naciśnij Win + R → wpisz eventvwr.msc → Enter.



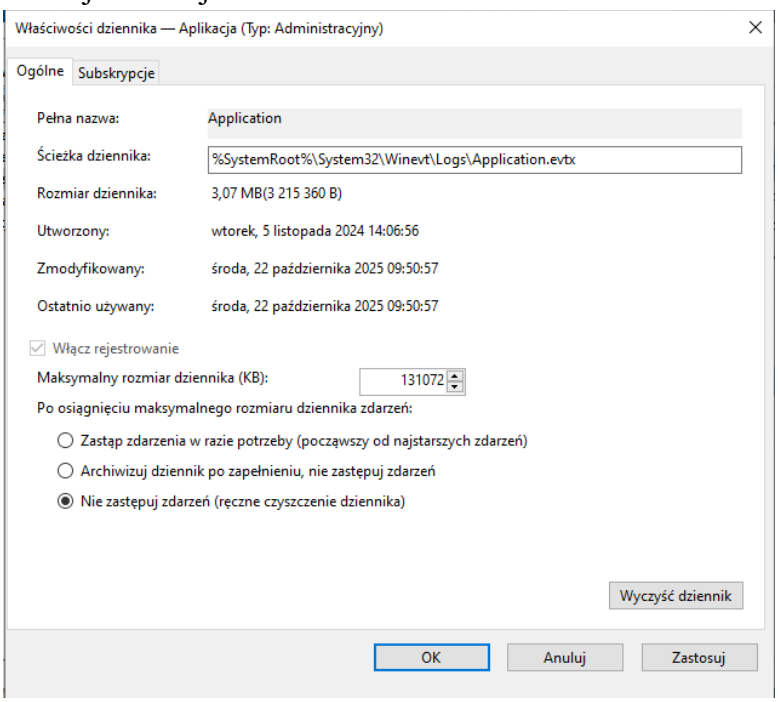
    2. Po lewej rozwiń: Dzienniki systemu Windows (Windows Logs)
       i zobaczysz 5 głównych kanałów:
        a) Aplikacja (Application)
        b) Zabezpieczenia (Security)
        c) Ustawienia (Setup)
        d) System (System)
        e) Zdarzenia przesyłane dalej (Forwarded Events)



- Zmień ustawienia każdego logu (zrobisz to osobno dla każdego z tych dzienników)
  1. Kliknij prawym przyciskiem np. na Aplikacja (Application) → Właściwości.



  2. □W oknie, które się otworzy:
     a) Maksymalny rozmiar dziennika:
        Zmień z domyślnych na np. 128 MB lub 256 MB
        (zależnie od ilości miejsca na dysku — uzasadnienie poniżej)
     b) Gdy osiągnięto maksymalny rozmiar dziennika:
        Zaznacz Nie zastępuj zdarzeń (Zachowaj dziennik)
        (czyli retention mode)
     c) Kliknij Zastosuj → OK



  3. Powtórz to samo dla wszystkich 5 głównych kanałów:

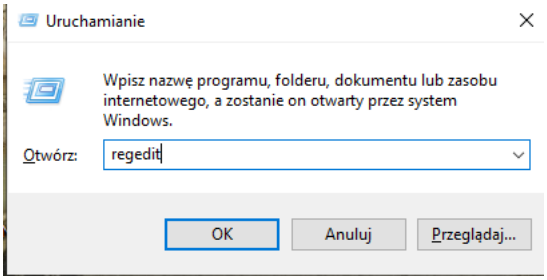
a) Application
b) Security
c) Setup
d) System
e) Forwarded Events

- Uzasadnij wybrane wartości
  1. Tryb „Nie zastępuj zdarzeń (retention)”
     a) Chroni logi przed przypadkowym nadpisaniem.
     b) Administrator musi ręcznie wyczyścić dziennik, co zapobiega utracie dowodów w razie incydentu.
     c) Zgodne z zaleceniami CIS Benchmark i Microsoft Security Guidance.
  2. Rozmiar logu (np. 128 MB / 256 MB)
     a) Domyślne wartości (20–30 MB) są zbyt małe – przy aktywnym systemie nadpisują się w kilka dni.
     b) 128 MB wystarcza dla stacji roboczej (ok. 2–4 tygodnie historii).
     c) 256 MB lub więcej warto ustawić na serwerach lub kontrolerach domeny (dużo zdarzeń bezpieczeństwa).
     d) Większy rozmiar = dłuższa historia, łatwiejsza analiza incydentów.
     e) Jeśli masz mało miejsca na dysku, możesz dobrać np. 64 MB — ale zawsze lepiej zwiększyć niż zostawić domyślnie.
- Sprawdź konfigurację PowerShellem
  1. Otwórz PowerShell jako administrator.
  2. Wpisz np.: Get-WinEvent -ListLog Security | Select-Object LogName, MaximumSizeInBytes, LogMode
  3. Wartości powinny wyglądać mniej więcej tak:
     a) MaximumSizeInBytes : 134217728 (czyli 128 MB)
     b) LogMode : Retain (czyli „Nie nadpisuj”)

Metoda 5

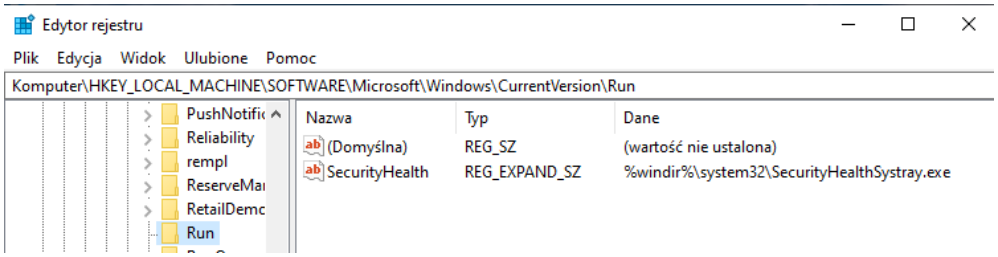
Zidentyfikuj i usuń „persistence mechanisms” atakującego (Run keys, Scheduled Tasks, WMI, Services); udokumentuj proces.

- Sprawdź klucze autostartu (Run keys)
  1. Naciśnij Win + R → wpisz: regedit

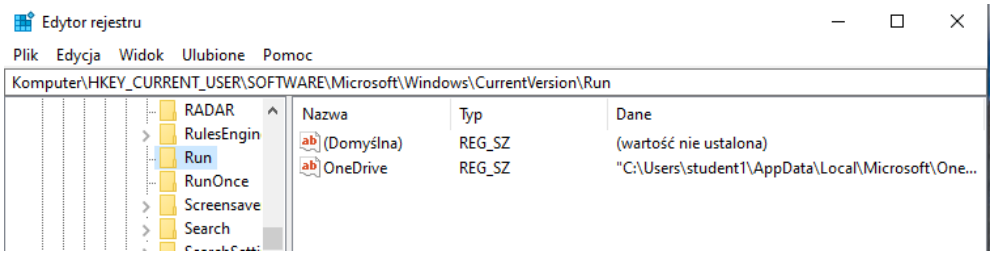


  2. Enter (otworzy się Edytor rejestru).

3. Przejdź do lokalizacji:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

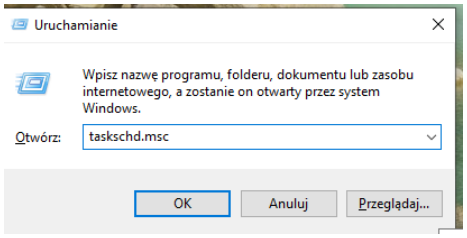


HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

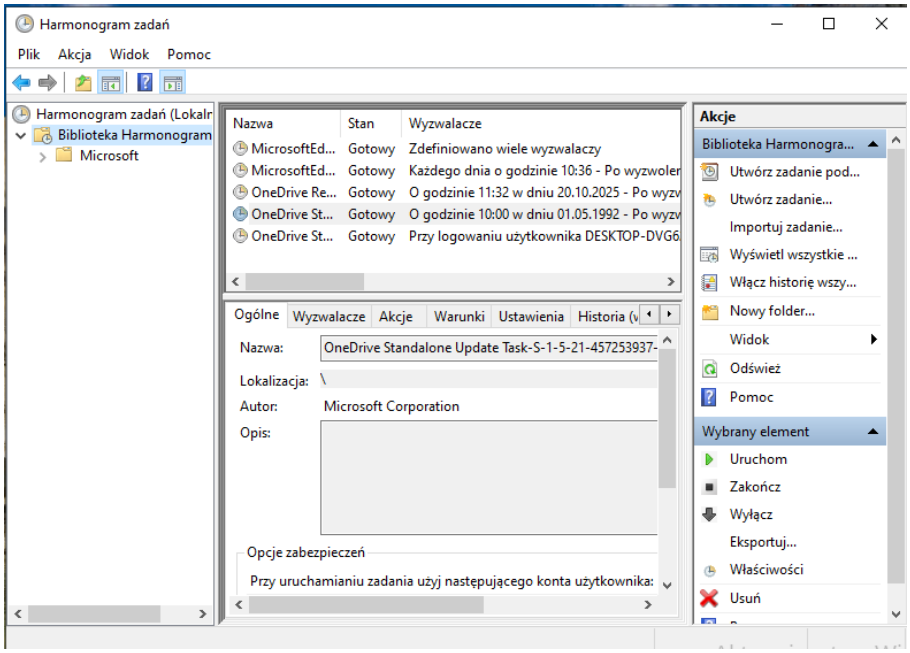


4. Sprawdź wpisy w prawej części okna.
   a) Zwróć uwagę na podejrzane nazwy (np. update.exe, svchost123, AdobeUpdate itp.)
   b) Kliknij prawym → Usuń, jeśli masz pewność, że to nie jest legalny program.

- Sprawdź zaplanowane zadania (Scheduled Tasks)
  1. Naciśnij Win + R → wpisz: taskschd.msc → Enter.



  2. Po lewej rozwiń: Harmonogram zadań → Biblioteka Harmonogramu zadań

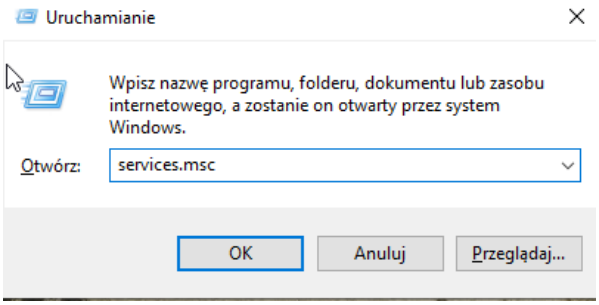


  3. Sprawdź listę zadań po prawej stronie. Zwróć uwagę na:
     a) dziwne lub losowe nazwy (np. abc123, WindowsUpdateChecker),

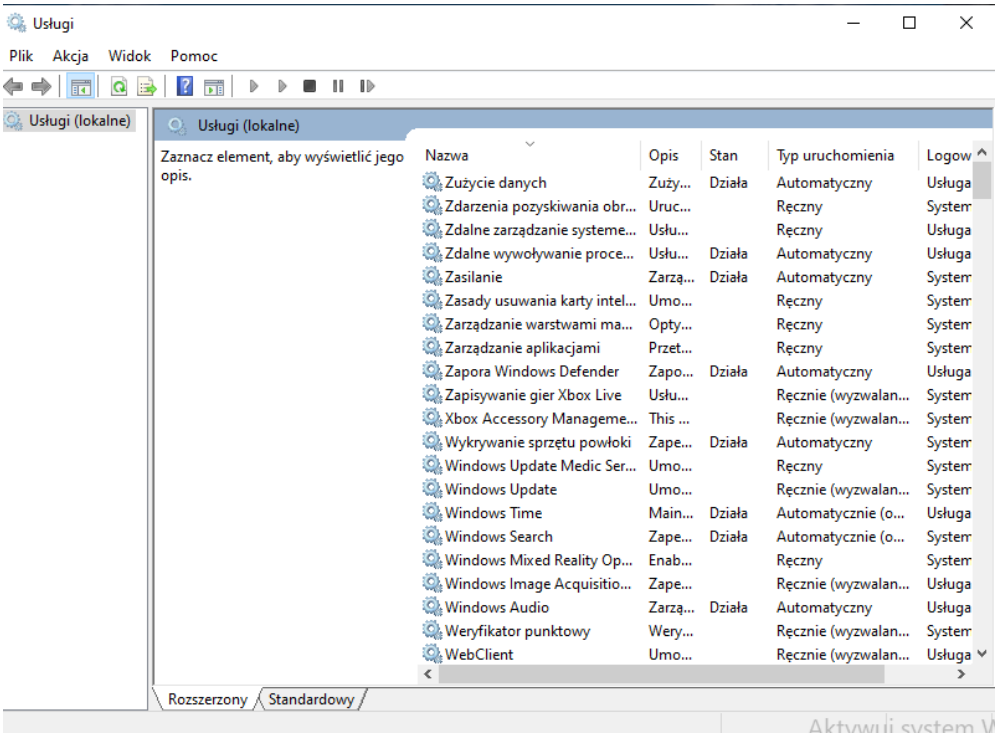
b) ścieżki prowadzące do nietypowych folderów (np. C:\Users\Public, %TEMP%),
c) zadania, które uruchamiają cmd.exe, powershell.exe lub wscript.exe.

4. Jeśli coś wygląda podejrzanie → kliknij prawym → Usuń.

- Sprawdź usługi (Services)
  1. Naciśnij Win + R → wpisz: services.msc → Enter.



  2. Przejrzyj listę usług — kliknij kolumnę „Nazwa” żeby sortować.



  3. Na co zwrócić uwagę:
     a) Usługi o dziwnych lub nieczytelnych nazwach, np. sysupdater, winfix, MicrosoftUpdateSvc.
     b) Opis pusty lub po angielsku wśród polskich.
     c) Typ uruchomienia: Automatyczny mimo że nie znasz programu.
  4. Jeśli znajdziesz coś podejrzanego:
     a) kliknij prawym → Zatrzymaj,
     b) potem Właściwości → Typ uruchomienia → Wyłączony,
     c) Zastosuj → OK.

- Sprawdź zdarzenia WMI (Windows Management Instrumentation)
  1. Otwórz PowerShell jako administrator.
  2. Wpisz komendę:
     Get-WmiObject -Namespace root\subscription -Class __EventFilter

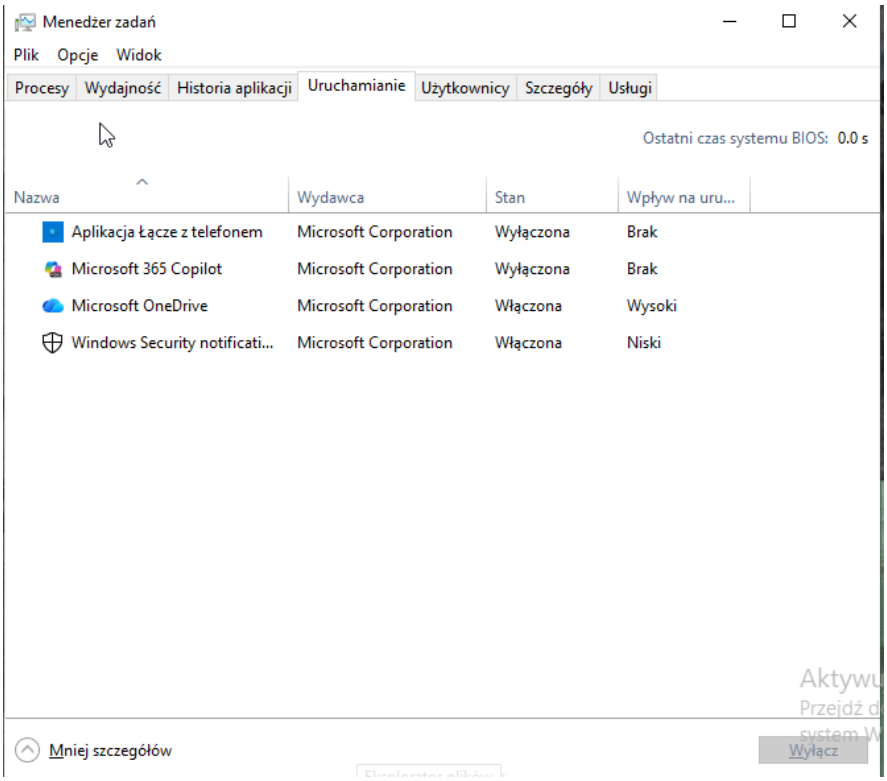
```
PS C:\Windows\system32>  Get-WmiObject -Namespace root\subscription -Class __EventFilter


__GENUS          : 2
__CLASS          : __EventFilter
__SUPERCLASS     : __IndicationRelated
__DYNASTY        : __SystemClass
__RELPATH        : __EventFilter.Name="SCM Event Log Filter"
__PROPERTY_COUNT : 6
__DERIVATION     : {__IndicationRelated, __SystemClass}
__SERVER         : DESKTOP-DVG62G9
__NAMESPACE      : ROOT\subscription
__PATH           : \\DESKTOP-DVG62G9\ROOT\subscription:__EventFilter.Name="SCM Event Log Filter"
CreatorSID       : {1, 2, 0, 0...}
EventAccess      :
EventNamespace   : root\cimv2
Name             : SCM Event Log Filter
Query            : select * from MSFT_SCMEventLogEvent
QueryLanguage    : WQL
PSComputerName   : DESKTOP-DVG62G9


PS C:\Windows\system32>
```

3. Jeśli pojawią się jakieś wpisy — sprawdź ich nazwy i opisy.
   Złośliwe WMI będą wyglądać podejrzanie (np. nazwy bez sensu, odwołania do skryptów .vbs lub .exe w dziwnych folderach).
4. Aby je usunąć:
   Get-WmiObject -Namespace root\subscription -Class __EventFilter | Remove-WmiObject

- Dodatkowo sprawdź autostart systemu
  1. Naciśnij Ctrl + Shift + Esc → otwórz Menedżer zadań.
  2. Przejdź do zakładki Uruchamianie (Startup).
  3. Zobacz listę aplikacji uruchamianych przy starcie systemu.

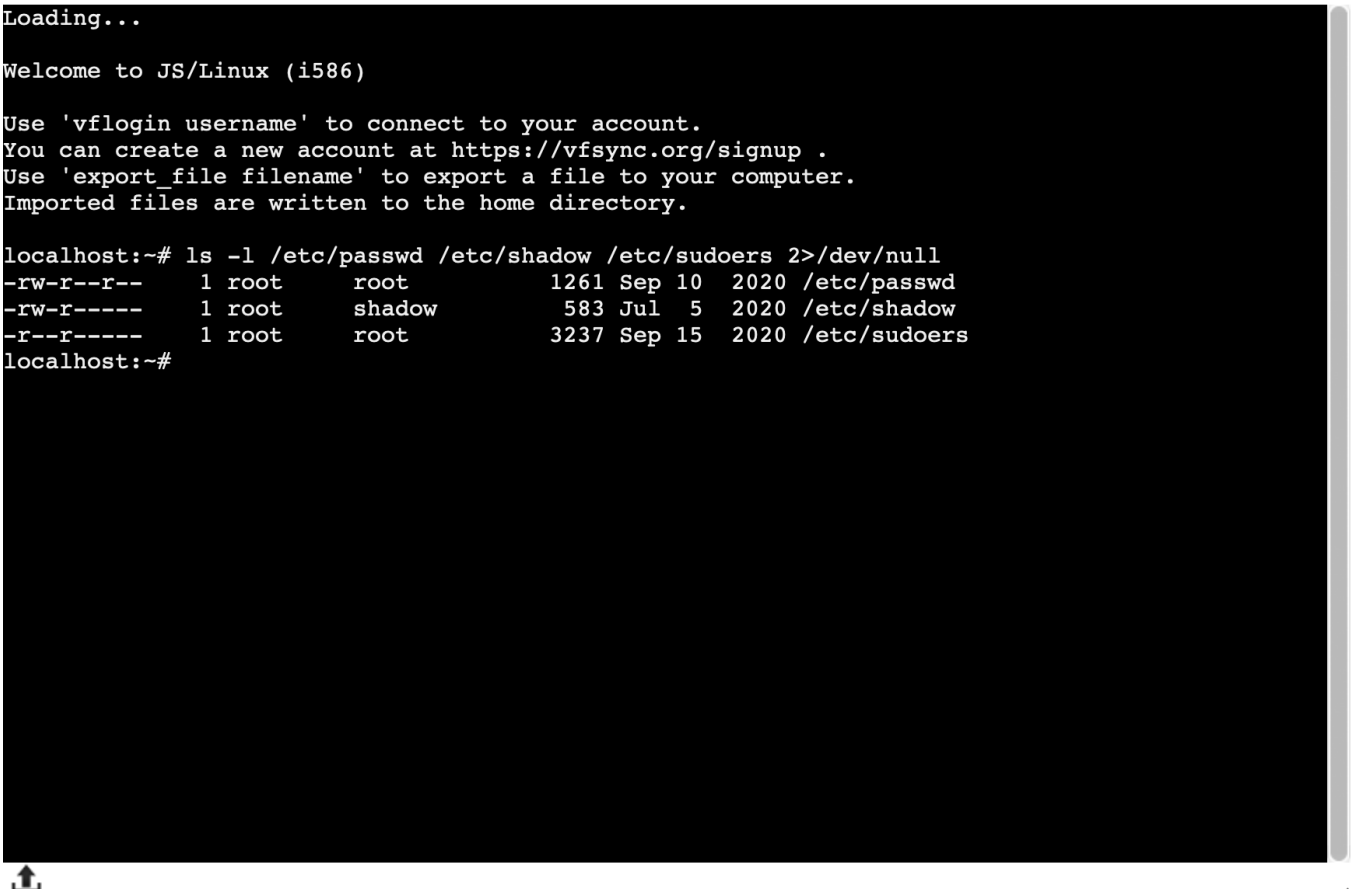


4. Wyłącz wszystko, co, jest nieznane lub niepotrzebne:
   a) Zaznacz aplikację → Wyłącz (Disable).

Zadanie 2 - Opracować 5 metod hardeningu linux.

Metoda 1
Ogranicz uprawnienia wrażliwych plików: /etc/passwd, /etc/shadow, /etc/sudoers, klucze SSH, pliki systemd unit override.

Cel: Zabezpieczenie ważnych plików systemowych przed nieautoryzowanym odczytem lub modyfikacją – szczególnie /etc/passwd, /etc/shadow, /etc/sudoers oraz kluczy SSH.



```
Loading...

Welcome to JS/Linux (i586)

Use 'vflogin username' to connect to your account.
You can create a new account at https://vfsync.org/signup .
Use 'export_file filename' to export a file to your computer.
Imported files are written to the home directory.

localhost:~# ls -l /etc/passwd /etc/shadow /etc/sudoers 2>/dev/null
-rw-r--r--    1 root     root          1261 Sep 10  2020 /etc/passwd
-rw-r-----    1 root     shadow         583 Jul  5  2020 /etc/shadow
-r--r-----    1 root     root          3237 Sep 15  2020 /etc/sudoers
localhost:~# chmod 664 /etc/passwd
localhost:~# chmod 640 /etc/shadow
localhost:~# chown root:root /etc/shadow
localhost:~# chmod 440 /etc/sudoers
localhost:~#
```

```
localhost:~# chmod 664 /etc/passwd
localhost:~# chmod 640 /etc/shadow
localhost:~# chown root:root /etc/shadow
localhost:~# chmod 440 /etc/sudoers
localhost:~# mkdir -p /root/.ssh
localhost:~# chmod 700 /root/.ssh
localhost:~# touch /root/.ssh/authorized_keys
localhost:~# chmod 600 /root/.ssh/authorized_keys
localhost:~#
```

```
localhost:~# ls -l /etc/passwd /etc/shadow /etc/sudoers 2>/dev/null
-rw-r--r--    1 root     root          1261 Sep 10  2020 /etc/passwd
-rw-r-----    1 root     shadow         583 Jul  5  2020 /etc/shadow
-r--r-----    1 root     root          3237 Sep 15  2020 /etc/sudoers
localhost:~# chmod 664 /etc/passwd
localhost:~# chmod 640 /etc/shadow
localhost:~# chown root:root /etc/shadow
localhost:~# chmod 440 /etc/sudoers
localhost:~# mkdir -p /root/.ssh
localhost:~# chmod 700 /root/.ssh
localhost:~# touch /root/.ssh/authorized_keys
localhost:~# chmod 600 /root/.ssh/authorized_keys
localhost:~# ls -l /etc/passwd /etc/shadow /etc/sudoers
-rw-rw-r--    1 root     root          1261 Sep 10  2020 /etc/passwd
-rw-r-----    1 root     root           583 Jul  5  2020 /etc/shadow
-r--r-----    1 root     root          3237 Sep 15  2020 /etc/sudoers
localhost:~# ls -ld /root/.ssh
drwx------    2 root     root            69 Oct 23 21:20 /root/.ssh
localhost:~# ls -l /root/.ssh
total 0
-rw-------    1 root     root             0 Oct 23 21:21 authorized_keys
localhost:~#
```

Co widać na zrzutach ekranu:

- przed i po: ls -l /etc/passwd /etc/shadow /etc/sudoers,
- poprawne uprawnienia 700/600 dla /root/.ssh.

Wniosek: plik shadow nie jest już czytelny dla użytkowników, sudoers nie można przypadkowo edytować, a klucze SSH są chronione.

Metoda 2
Oczyść PATH, wyłącz . w PATH, ustaw bezpieczne umaski (UMASK 027) globalnie.

Cel: ograniczyć domyślne uprawnienia nowych plików i usunąć niebezpieczny . z PATH.

```
localhost:~# umask
0022
localhost:~# echo "$PATH"
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
localhost:~#
```

```
localhost:~# echo "$PATH"
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
localhost:~# umask 027
localhost:~# export PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:usr/bin:/sbin:/bin"
localhost:~# umask
0027
localhost:~# echo "$PATH"
/usr/local/sbin:/usr/local/bin:/usr/sbin:usr/bin:/sbin:/bin
localhost:~#
```

```
localhost:~# echo "$PATH"
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
localhost:~# umask 027
localhost:~# export PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:usr/bin:/sbin:/bin"
localhost:~# umask
0027
localhost:~# echo "$PATH"
/usr/local/sbin:/usr/local/bin:/usr/sbin:usr/bin:/sbin:/bin
localhost:~# rm -f /tmp/testfile && touch /tmp/testfile && ls -l /tmp/testfile
-rw-r-----    1 root     root             0 Oct 23 21:28 /tmp/testfile
localhost:~#
```

Co widać na zrzutach ekranu:

- wynik umask przed i po zmianie,
- nowy plik ma uprawnienia np. rw-r-----,
- PATH bez ..

Wniosek: nowe pliki nie są dostępne dla „others”, a PATH nie zawiera bieżącego katalogu.

Metoda 3
Zablokuj core dumps (limits, fs.suid_dumpable=0) i włącz pełne ASLR (kernel.randomize_va_space=2).

Cel: uniemożliwić zapisywanie pamięci procesów (core dump) oraz włączyć losowanie przestrzeni adresowej pamięci (ASLR), aby utrudnić ataki.

```
localhost:~# cat /proc/sys/kernel/randomize_va_space
1
localhost:~# cat /proc/sys/fs/suid_dumpable
0
localhost:~# ulimit -c
0
localhost:~# ulimit -c 0
localhost:~# echo 0 > /proc/sys/fs/suid_dumpable
localhost:~# echo 2 > /proc/sys/kernel/randomize_va_space
localhost:~#
```

```
1
localhost:~# cat /proc/sys/fs/suid_dumpable
0
localhost:~# ulimit -c
0
localhost:~# ulimit -c 0
localhost:~# echo 0 > /proc/sys/fs/suid_dumpable
localhost:~# echo 2 > /proc/sys/kernel/randomize_va_space
localhost:~# cat /proc/sys/kernel/randomize_va_space
2
localhost:~# cat /proc/sys/fs/suid_dumpable
0
localhost:~# ulimit -c 0
localhost:~# ulimit -c
0
localhost:~# cat /proc/sys/kernel/randomize_va_space
2
localhost:~# cat /proc/sys/fs/suid_dumpable
0
localhost:~# ulimit -c
0
localhost:~#
```

Co widać na zrzutach ekranu:

- przed/po: randomize_va_space, suid_dumpable, ulimit -c.

Wniosek: system nie tworzy plików zrzutu pamięci (core), a przestrzeń adresowa jest losowa (2 – pełne ASLR).

Metoda 4
Wdróż bezpieczne polityki dla użytkowników: separacja ról, minimalne uprawnienia do plików i gniazd, dedykowane grupy per usługa.

Cel: Wprowadzić zasadę najmniejszych uprawnień — konta użytkowników bez powłoki, dedykowane grupy, brak logowania dla kont technicznych.

```
localhost:~# cut -d: -f1,3,6 /etc/passwd
root:0:/root
bin:1:/bin
daemon:2:/sbin
adm:3:/var/adm
lp:4:/var/spool/lpd
sync:5:/sbin
shutdown:6:/sbin
halt:7:/sbin
mail:8:/var/mail
news:9:/usr/lib/news
uucp:10:/var/spool/uucppublic
operator:11:/root
man:13:/usr/man
postmaster:14:/var/mail
cron:16:/var/spool/cron
ftp:21:/var/lib/ftp
sshd:22:/dev/null
at:25:/var/spool/cron/atjobs
squid:31:/var/cache/squid
xfs:33:/etc/X11/fs
```

```
news:9:/usr/lib/news
uucp:10:/var/spool/uucppublic
operator:11:/root
man:13:/usr/man
postmaster:14:/var/mail
cron:16:/var/spool/cron
ftp:21:/var/lib/ftp
sshd:22:/dev/null
at:25:/var/spool/cron/atjobs
squid:31:/var/cache/squid
xfs:33:/etc/X11/fs
games:35:/usr/games
cyrus:85:/usr/cyrus
vpopmail:89:/var/vpopmail
ntp:123:/var/empty
smmsp:209:/var/spool/mqueue
guest:405:/dev/null
nobody:65534:/
dhcp:100:/var/lib/dhcp
svn:101:/var/svn
localhost:~# adduser -D testuser || useradd testuser 2>/dev/null || true
localhost:~# addgroup web-admins 2>/dev/null || true
localhost:~# addgroup testuser web-admins 2>/dev/null || true
localhost:~# passwd -l testuser 2>/dev/null || true
localhost:~# usermod -s /sbin/nologin testuser 2>/dev/null || true
localhost:~# getent passwd testuser
testuser:x:1001:1001:Linux User,,,:/home/testuser:/bin/ash
localhost:~# groups testuser
testuser web-admins
localhost:~#
```

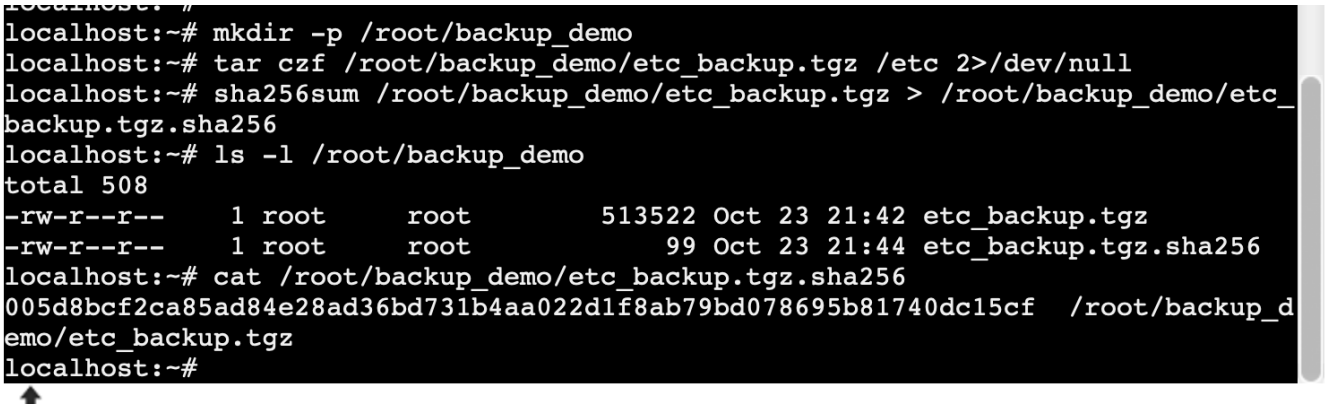
Co widać na zrzutach ekranu:

- testuser w pliku passwd,
- brak możliwości logowania (nologin),
- przypisanie do grupy web-admins.

Wniosek: konto testuser istnieje, ale nie może się zalogować — spełnia zasady „least privilege”.

Metoda 5
Przygotuj plan kopii zapasowych - szyfrowanych, podpisanych, wykonaj próbę odtworzenia i porównaj Checksumy.

Cel: wykonać kopię zapasową konfiguracji systemu, zabezpieczyć ją sumą SHA256 i sprawdzić możliwość odtworzenia.



Co widać na zrzutach ekranu:

- plik .tgz w katalogu backup_demo,
- plik .sha256,
- katalog restore_test/etc z rozpakowaną konfiguracją.

Wniosek: backup istnieje, można go odtworzyć i jego spójność można zweryfikować przez checksum.

W ramach hardeningu systemu Linux wdrożyłyśmy 5 wybranych metod. Każda została opisana, wykonana w środowisku testowym oraz udokumentowana poprzez zrzuty ekranu. Zabezpieczono pliki systemowe, włączono ASLR, zablokowano core dumps, wdrożono politykę kont i wykonano backup konfiguracji. Wszystkie zmiany są odwracalne i zgodne z dobrymi praktykami bezpieczeństwa.

Zadanie 3 - Odpowiedzieć na pytania

- Dlaczego wyłączenie SMBv1 i RDP dla wszystkich jest sensowne w środowisku domyślnym? Kiedy można zrobić wyjątek i jak go bezpiecznie wdrożyć?

Wyłączenie SMBv1 i RDP ma sens, bo to stare i często atakowane usługi. SMBv1 ma znane luki i nie zapewnia szyfrowania, więc łatwo przez niego rozprzestrzenia się ransomware. RDP z kolei, gdy jest otwarte dla wszystkich, ułatwia ataki brute-force i przejęcie systemu. Wyjątek można zrobić tylko wtedy, gdy jakaś starsza maszyna lub aplikacja naprawdę potrzebuje SMBv1 albo gdy administrator musi użyć RDP do zdalnego zarządzania. Wtedy najlepiej ograniczyć dostęp przez VPN, tylko z konkretnych adresów IP i włączyć logowanie oraz uwierzytelnianie NLA/MFA, żeby było bezpiecznie.

- ASR w Defenderze: które 2–3 reguły są najbardziej uciążliwe dla użytkowników i jak minimalizować fałszywe alarmy?
  Najbardziej uciążliwe reguły ASR to te, które blokują typowe działania w biurze. Najczęściej przeszkadza „Block Office apps from creating child processes", bo zatrzymuje np. makra w Excelu uruchamiające PowerShella. Druga to „Block Office apps from creating executable content", która blokuje tworzenie plików .exe z poziomu Worda czy Excela. Czasem kłopotliwa bywa też „Block executable content from email and webmail", bo uniemożliwia pobieranie niektórych załączników. Żeby ograniczyć fałszywe alarmy, najlepiej najpierw uruchomić te reguły w trybie audytu, sprawdzić logi i dodać wyjątki tylko dla zaufanych aplikacji lub lokalizacji (np. podpisanych makr czy folderów firmowych). Dzięki temu bezpieczeństwo zostaje, ale użytkownicy nie tracą komfortu pracy.
- SSH: dlaczego „PasswordAuthentication no" oraz klucze Ed25519 to lepsza praktyka niż długie hasła?
  Wyłączenie logowania hasłem i używanie kluczy Ed25519 to bezpieczniejsza i wygodniejsza metoda niż nawet bardzo długie hasła. Gdy ustawimy PasswordAuthentication no, serwer w ogóle nie przyjmuje haseł, więc ataki typu brute-force lub próby zgadnięcia hasła nie mają sensu. Klucz Ed25519 jest dużo trudniejszy do złamania, działa szybciej niż stare RSA i jest krótszy, co ułatwia jego użycie. Dodatkowo klucz prywatny zostaje tylko na komputerze użytkownika, więc nawet jeśli ktoś przechwyci serwer, nie pozna hasła. To daje zarówno lepsze bezpieczeństwo, jak i wygodę logowania.
- Czym różni się UFW od fail2ban - które ryzyko redukuje każdy z nich?
  UFW i fail2ban pełnią różne role, choć obie zwiększają bezpieczeństwo systemu. UFW (Uncomplicated Firewall) to prosty firewall, który kontroluje, które porty i usługi są dostępne z sieci. Dzięki temu ogranicza powierzchnię ataku – np. można zostawić otwarty tylko SSH i HTTP, a resztę zablokować. Z kolei fail2ban analizuje logi systemowe i po wykryciu wielu nieudanych prób logowania tymczasowo blokuje adres IP atakującego. Chroni więc głównie przed atakami brute-force. Czyli UFW zapobiega dostępowi tam, gdzie nie powinno go być, a fail2ban reaguje, gdy ktoś próbuje się włamać.
- Po co AIDE, skoro mamy backupy? Jakie scenariusze wykryje AIDE, a backup nie? AIDE nie służy do przywracania danych jak backup, tylko do wykrywania zmian w systemie, które mogły być skutkiem włamania lub sabotażu. Backup po prostu kopiuje pliki, często razem z ewentualnym złośliwym kodem, więc nie ostrzeże, że coś zostało podmienione. AIDE tworzy bazę kontrolnych sum plików (hashy) i później porównuje je z aktualnym stanem. Dzięki temu może wykryć np. podmianę plików systemowych, zmianę uprawnień, dodanie tylnego wejścia (backdoora) czy modyfikację w /etc/sudoers. Backup tego nie zauważy, bo uzna zmieniony plik za „nowszą wersję". Czyli AIDE wykrywa atak lub manipulację, a backup tylko odzyskuje dane po fakcie.

- AppArmor/SELinux w trybie enforcing - podaj przykład, jak polityka MAC mogła zablokować eskalację uprawnień.
  Przykładowo, jeśli atakujący przejmie kontrolę nad serwerem WWW (np. Apache) i spróbuje uruchomić z jego procesu /bin/bash albo odczytać plik /etc/shadow, to w systemie z włączonym SELinux lub AppArmor w trybie enforcing taka akcja zostanie zablokowana. Proces Apache działa w swojej odseparowanej domenie bezpieczeństwa (np. httpd_t w SELinux lub profil usr.sbin.apache2 w AppArmor), która nie ma uprawnień do uruchamiania innych programów ani dostępu do plików systemowych użytkowników. Dzięki temu nawet jeśli ktoś wykorzysta lukę w aplikacji webowej, nie będzie mógł eskalować uprawnień ani przejąć całego systemu. Czyli polityka MAC uniemożliwia procesowi z ograniczonym profilem wykonywanie działań, które normalnie wymagają uprawnień administratora.
- Jak skonfigurować centralizację logów (Windows + Linux) w małej organizacji (kilka zdań, narzędzia/open source mile widziane)?
  W małej organizacji najprościej zrobić centralizację logów przy użyciu darmowych narzędzi open source. Na Windowsie można włączyć Windows Event Forwarding (WEF), żeby wszystkie komputery wysyłały logi do jednego serwera-kolektora. Dodatkowo warto zainstalować Sysmon, który daje dokładniejsze dane o procesach i sieci. Na Linuksie logi z rsyslog lub journald można wysyłać po TLS do tego samego serwera (np. z Graylog, Wazuh albo Elastic Stack). Ważne, żeby ustawić wspólny NTP i trzymać logi na osobnej maszynie, żeby nie dało się ich łatwo usunąć po włamaniu.
- Jakie trzy wskaźniki/metryki w logach/audytach monitorować stale, aby szybko wykryć atak?
  Trzy najważniejsze rzeczy, które warto stale obserwować w logach, to:
  - Nieudane logowania – nagły wzrost błędnych prób logowania (np. „Failed password” w Linuxie lub zdarzenia 4625 w Windows) może oznaczać atak brute-force albo próby zgadnięcia haseł.
  - Tworzenie nowych kont lub zmiany uprawnień – pojawienie się nowych użytkowników administracyjnych (np. eventy 4720, 4728 w Windows) często wskazuje na eskalację uprawnień.
  - Nietypowe procesy i połączenia sieciowe – np. PowerShell uruchamiany z Worda, albo proces łączący się z nieznanym adresem IP. Takie anomalie można wychwycić przez logi Sysmon lub auditd.