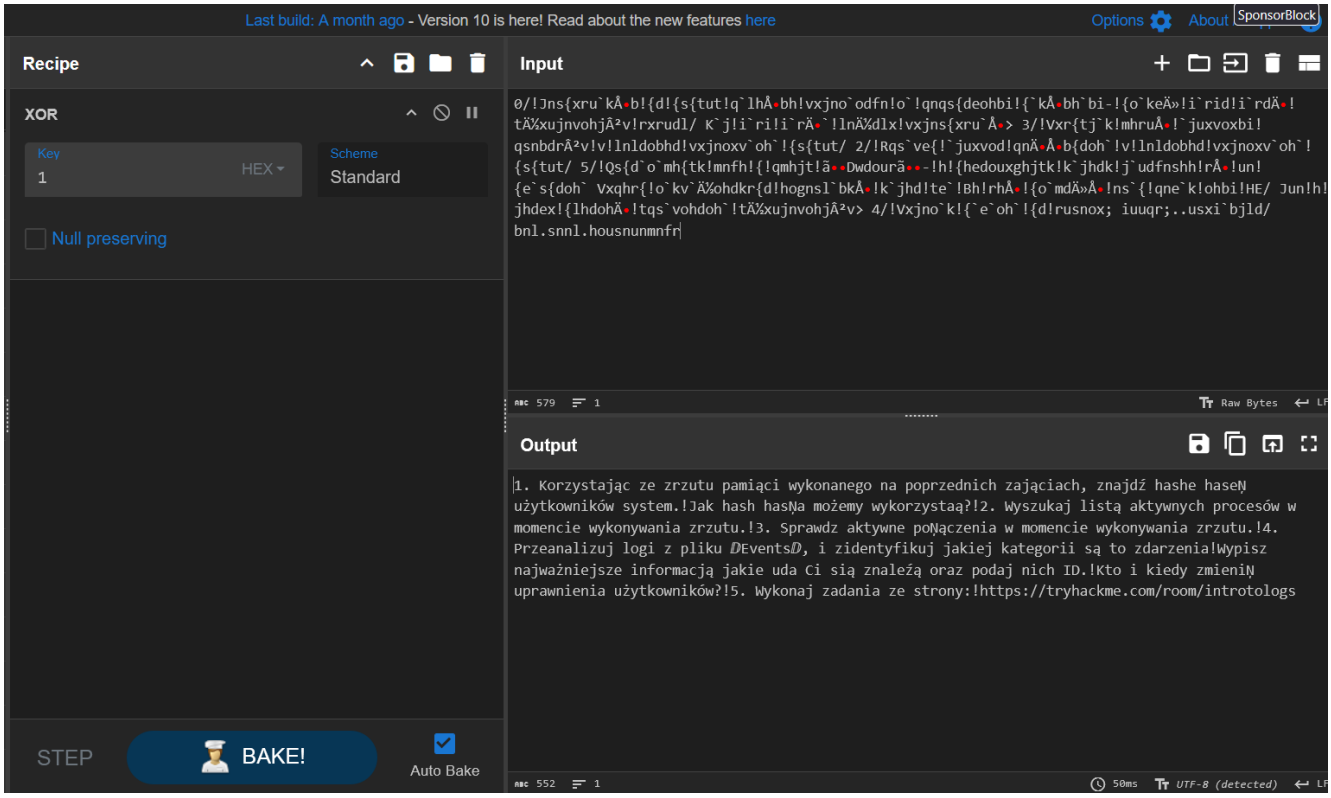
POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 5	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 31.03.2025	
Data oddania sprawozdania: 06.04.2025	

1. Cel ćwiczenia

Analiza zrzutu pamięci i logów systemowych .

2. Odkodowanie instrukcji laboratoryjnej



Rysunek 1: Odkodowanie instrukcji za pomocą CyberChef – XOR z kluczem „1”

```
1/ Korzystając ze zrzutu pamięci wykonanego na poprzednich zajęciach, znajdź hashe haseł
użytkowników system.
Jak hash hasła możemy wykorzystać?

2/ Wyszukaj listę aktywnych procesów w momencie wykonywania zrzutu.

3/ Sprawdz aktywne połączenia w momencie wykonywania zrzutu.

4/ Przeanalizuj logi z pliku "Events", i zidentyfikuj jakiej kategorii są to zdarzenia

Wypisz najważniejsze informację jakie uda Ci się znaleźć oraz podaj nich ID.

Kto i kiedy zmienił uprawnienia użytkowników?

5/ Wykonaj zadania ze strony:
https://tryhackme.com/room/introtologs
```

Rysunek 2: Odszyfrowana treść instrukcji

3. Realizacja zadań instrukcji

Zadanie 1. *Korzystając ze zrzutu pamięci wykonanego na poprzednich zajęciach, znajdź hashe haseł użytkowników system.*

```
┌──(venv)─(kali㉿kali)-[~/Desktop/volatility3]
└─$ vol -f memdump.mem windows.registry.hashdump.Hashdump

Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        6597d9fe8469e21d840e2cbff8d43c8b
Gość    501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
vboxuser        1000    aad3b435b51404eeaad3b435b51404ee        6597d9fe8469e21d840e2cbff8d43c8b

┌──(venv)─(kali㉿kali)-[~/Desktop/volatility3]
└─$
```

Rysunek 3: pozyskanie hashy haseł zapisanych w pliku memdump.mem

Jak hash hasła możemy wykorzystać?

Hashe haseł mogą być zaatakowane metodą słownikową lub siłową, w celu odkrycia hasła.

Zadanie 2. *Wyszukaj listę aktywnych procesów w momencie wykonywania zrzutu.*

```
┌──(venv)─(kali㉿kali)-[~/Desktop/volatility3]
└─$ vol -f memdump.mem  windows.pslist.PsList

Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa8002402890  92      479     N/A     False   2025-03-25 10:31:31.000000 UTC  N/A     Disabled
280     4       smss.exe        0xfa800364db30  2       31      N/A     False   2025-03-25 10:31:31.000000 UTC  N/A     Disabled
364     348     csrss.exe       0xfa8004030b30  10      334     0       False   2025-03-25 10:31:35.000000 UTC  N/A     Disabled
416     348     wininit.exe     0xfa80040e1800  3       80      0       False   2025-03-25 10:31:36.000000 UTC  N/A     Disabled
424     408     csrss.exe       0xfa80040df060  11      201     1       False   2025-03-25 10:31:36.000000 UTC  N/A     Disabled
472     416     services.exe    0xfa8003916b30  7       192     0       False   2025-03-25 10:31:36.000000 UTC  N/A     Disabled
500     408     winlogon.exe    0xfa800414e060  3       113     1       False   2025-03-25 10:31:36.000000 UTC  N/A     Disabled
508     416     lsass.exe       0xfa8003014b30  6       562     0       False   2025-03-25 10:31:36.000000 UTC  N/A     Disabled
516     416     lsm.exe 0xfa80040da620  10      142     0       False   2025-03-25 10:31:36.000000 UTC  N/A     Disabled
640     472     svchost.exe     0xfa80041bd060  9       352     0       False   2025-03-25 10:31:37.000000 UTC  N/A     Disabled
708     472     VBoxService.ex  0xfa80041e33e0  13      130     0       False   2025-03-25 10:31:37.000000 UTC  N/A     Disabled
776     472     svchost.exe     0xfa80041f83d0  7       245     0       False   2025-03-25 10:31:37.000000 UTC  N/A     Disabled
860     472     svchost.exe     0xfa80042269e0  20      470     0       False   2025-03-25 10:31:37.000000 UTC  N/A     Disabled
908     472     svchost.exe     0xfa8004252320  11      301     0       False   2025-03-25 10:31:37.000000 UTC  N/A     Disabled
948     472     svchost.exe     0xfa800427fb30  32      934     0       False   2025-03-25 10:31:37.000000 UTC  N/A     Disabled
376     472     svchost.exe     0xfa8004289b30  12      306     0       False   2025-03-25 10:31:38.000000 UTC  N/A     Disabled
512     472     svchost.exe     0xfa8004287b30  15      363     0       False   2025-03-25 10:31:38.000000 UTC  N/A     Disabled
1088    472     spoolsv.exe     0xfa800435d910  12      274     0       False   2025-03-25 10:31:38.000000 UTC  N/A     Disabled
1120    472     svchost.exe     0xfa8004373560  17      300     0       False   2025-03-25 10:31:38.000000 UTC  N/A     Disabled
1504    472     taskhost.exe    0xfa8004499b30  8       155     1       False   2025-03-25 10:31:39.000000 UTC  N/A     Disabled
1580    908     dwm.exe 0xfa80044c2b30  3       136     1       False   2025-03-25 10:31:39.000000 UTC  N/A     Disabled
1640    1564    explorer.exe    0xfa80044f0060  26      731     1       False   2025-03-25 10:31:39.000000 UTC  N/A     Disabled
2000    1640    VBoxTray.exe    0xfa800361a630  13      144     1       False   2025-03-25 10:31:42.000000 UTC  N/A     Disabled
1708    472     SearchIndexer.  0xfa80045c5060  11      523     0       False   2025-03-25 10:31:50.000000 UTC  N/A     Disabled
632     472     svchost.exe     0xfa80041bc060  11      147     0       False   2025-03-25 10:33:45.000000 UTC  N/A     Disabled
1136    472     sppsvc.exe      0xfa80041c5060  4       150     0       False   2025-03-25 10:33:45.000000 UTC  N/A     Disabled
1452    472     svchost.exe     0xfa800465f060  13      322     0       False   2025-03-25 10:33:46.000000 UTC  N/A     Disabled
932     1780    firefox.exe     0xfa80027d3a70  0       -       1       False   2025-03-25 10:41:52.000000 UTC  2025-03-25 10:42:04.000000 UTC  Disabled
2320    860     audiodg.exe     0xfa8002811060  5       128     0       False   2025-03-25 11:32:10.000000 UTC  N/A     Disabled
2492    1640    FTK Imager.exe  0xfa8002833480  9       293     1       False   2025-03-25 11:32:13.000000 UTC  N/A     Disabled
```

Rysunek 4: lista wszystkich aktywnych, podczas wykonywania zrzutu, procesów

Zadanie 3. *Sprawdź aktywne połączenia w momencie wykonywania zrzutu.*

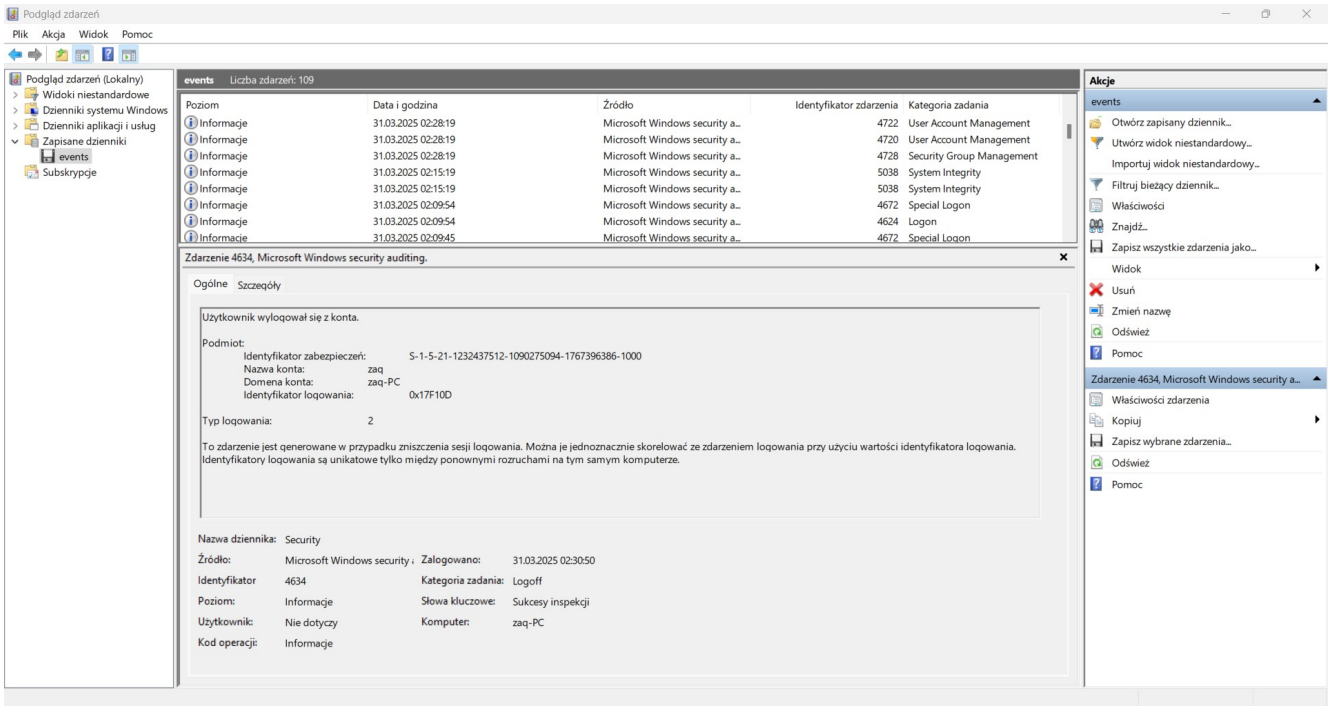
```
┌──(venv)─(kali㉿kali)-[~/Desktop/volatility3]
└─$ vol -f memdump.mem  windows.netscan.NetScan
Volatility 3 Framework 2.25.0
Progress:  100.00               PDB scanning finished
Offset  Proto    LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0×bbe2dd10      UDPv4   10.0.2.15       1900    *       0               632     svchost.exe     2025-03-25 10:33:46.000000 UTC
0×bbe2e320      TCPv6   -       0       38fb:2704:80fa:ffff:38fb:2704:80fa:ffff 0       CLOSED  512     svchost.exe     N/A
0×bc06bc20      UDPv4   0.0.0.0 5355    *       0               512     svchost.exe     2025-03-25 10:31:42.000000 UTC
0×bc078370      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       508     lsass.exe       -
0×bc106010      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0×bc106010      TCPv6   ::      445     ::      0       LISTENING       4       System  -
0×bc11f950      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       472     services.exe    -
0×bc11f950      TCPv6   ::      49155   ::      0       LISTENING       472     services.exe    -
0×bc11fef0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       472     services.exe    -
0×bc200360      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       776     svchost.exe     -
0×bc201ef0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       776     svchost.exe     -
0×bc201ef0      TCPv6   ::      135     ::      0       LISTENING       776     svchost.exe     -
0×bc2187c0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       416     wininit.exe     -
0×bc24f5e0      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       860     svchost.exe     -
0×bc24f5e0      TCPv6   ::      49153   ::      0       LISTENING       860     svchost.exe     -
0×bc251420      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       860     svchost.exe     -
0×bc2e7440      UDPv4   10.0.2.15       138     *       0               4       System  2025-03-25 10:31:38.000000 UTC
0×bc2eb930      TCPv4   10.0.2.15       139     0.0.0.0 0       LISTENING       4       System  -
0×bc2ebec0      UDPv4   10.0.2.15       137     *       0               4       System  2025-03-25 10:31:38.000000 UTC
0×bc30b7d0      UDPv4   0.0.0.0 0       *       0               512     svchost.exe     2025-03-25 10:31:38.000000 UTC
0×bc30b7d0      UDPv6   ::      0       *       0               512     svchost.exe     2025-03-25 10:31:38.000000 UTC
0×bc5bc8e0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       416     wininit.exe     -
0×bc5bc8e0      TCPv6   ::      49152   ::      0       LISTENING       416     wininit.exe     -
0×bc7d2b60      UDPv6   ::1     51046   *       0               632     svchost.exe     2025-03-25 10:33:46.000000 UTC
0×bcd5f5a0      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       948     svchost.exe     -
0×bcd5f5a0      TCPv6   ::      49154   ::      0       LISTENING       948     svchost.exe     -
0×bce16300      UDPv6   fe80::11e0:5816:3f74:1f66       1900    *       0               632     svchost.exe     2025-03-25 10:33:46.000000 UTC
0×bce2e670      UDPv4   127.0.0.1       51047   *       0               632     svchost.exe     2025-03-25 10:33:46.000000 UTC
0×bcf56b60      UDPv6   ::1     1900    *       0               632     svchost.exe     2025-03-25 10:33:46.000000 UTC
0×bcf921a0      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       948     svchost.exe     -
0×bcf92cf0      TCPv6   -       49172   ::1     445     CLOSED  4       System  -
0×bd15f090      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       508     lsass.exe       -
0×bd15f090      TCPv6   ::      49156   ::      0       LISTENING       508     lsass.exe       -
0×bd18dec0      UDPv4   0.0.0.0 5355    *       0               512     svchost.exe     2025-03-25 10:31:42.000000 UTC
0×bd18dec0      UDPv6   ::      5355    *       0               512     svchost.exe     2025-03-25 10:31:42.000000 UTC
0×bd1cb2f0      UDPv4   127.0.0.1       1900    *       0               632     svchost.exe     2025-03-25 10:33:46.000000 UTC
0×bdc4d610      TCPv6   -       445     ::1     49172   CLOSED  4       System  -
0×bdc5b010      TCPv4   -       49165   10.0.2.3        443     CLOSED  932     firefox.exe     -
0×bdc74010      TCPv4   -       49168   104.81.99.218   80      CLOSED  932     firefox.exe     -
0×bdc79450      TCPv4   -       49167   192.228.79.201  443     CLOSED  932     firefox.exe     N/A
0×bdff62a0      TCPv6   -       49170   2600:1901:0:92a9::      443     CLOSED  932     firefox.exe     N/A
```

Rysunek 5: lista wszystkich połączeń sieciowych

Komentarz: powyższa lista to lista *wszystkich* połączeń, niektóre nie są aktywne: „CLOSED”, ale nadal są widoczne w zrzucie pamięci.

Zadanie 4. *Przeanalizuj logi z pliku "Events", i zidentyfikuj jakiej kategorii są to zdarzenia*

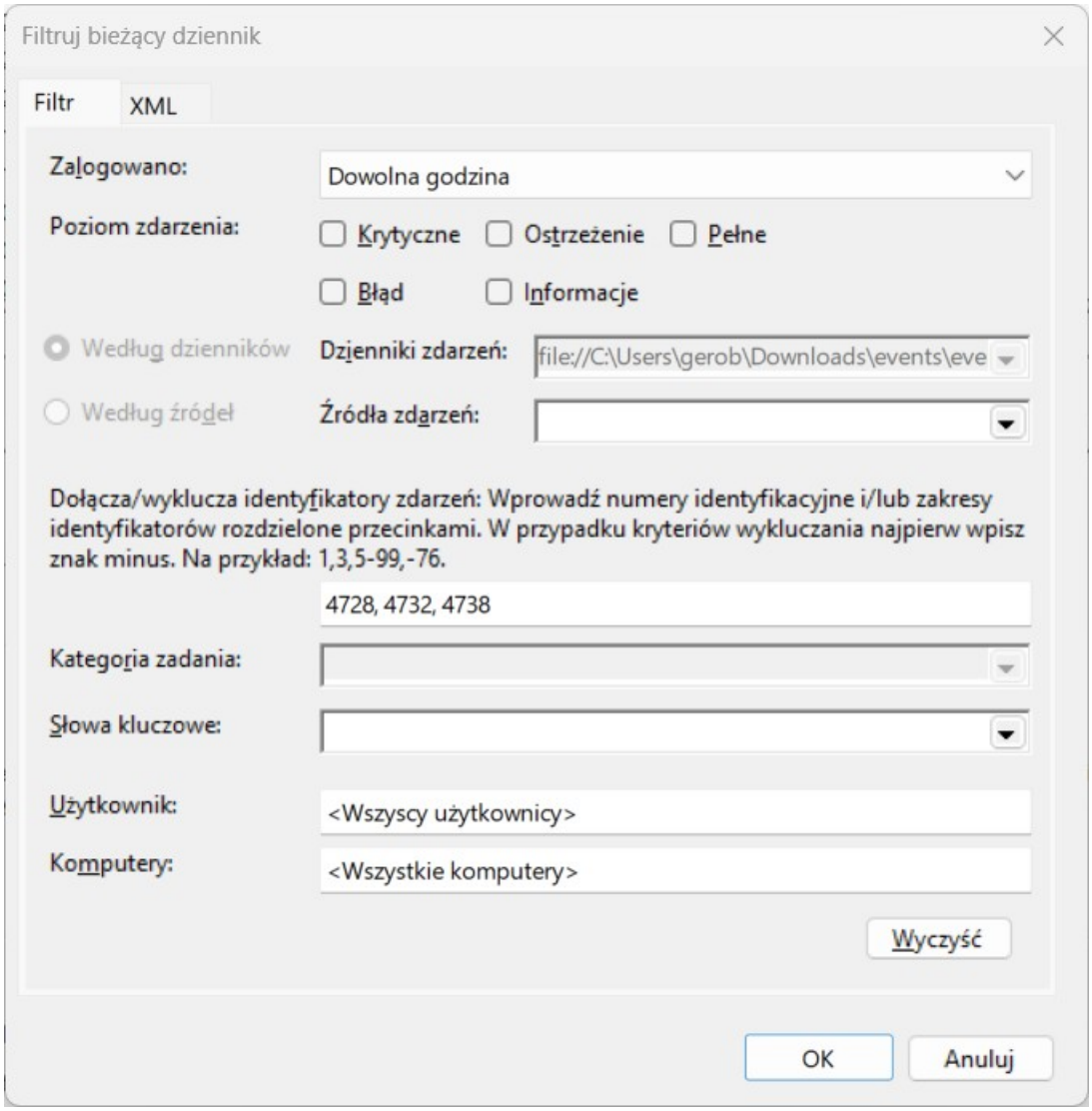


Rysunek 6: Analiza logów za pomocą aplikacji „podgląd zdarzeń”.

Zdarzenia są różnych kategorii ale głównie związane z logowaniem do systemu, np.

- 4624 - Użytkownik pomyślnie zalogował się na koncie.
- 4634 - Użytkownik wylogował się z konta.
- 4672 - Przypisano specjalne uprawnienia do nowego logowania.

Wypisz najważniejsze informację jakie uda Ci się znaleźć oraz podaj nich ID.



Rysunek 7: Filtrowanie najważniejszych informacji

Poziom	Data i godzina	Źródło	Identyfikator zdarzenia	Kategoria zadania
Informacje	31.03.2025 02:28:19	Microsoft Windows security a...	4738	User Account Management
Informacje	31.03.2025 02:28:19	Microsoft Windows security a...	4738	User Account Management
Informacje	31.03.2025 02:28:19	Microsoft Windows security a...	4738	User Account Management
Informacje	31.03.2025 02:28:35	Microsoft Windows security a...	4732	Security Group Management
Informacje	31.03.2025 02:28:19	Microsoft Windows security a...	4732	Security Group Management
Informacje	31.03.2025 02:28:19	Microsoft Windows security a...	4728	Security Group Management

Rysunek 8: Widok najważniejszych wydarzeń

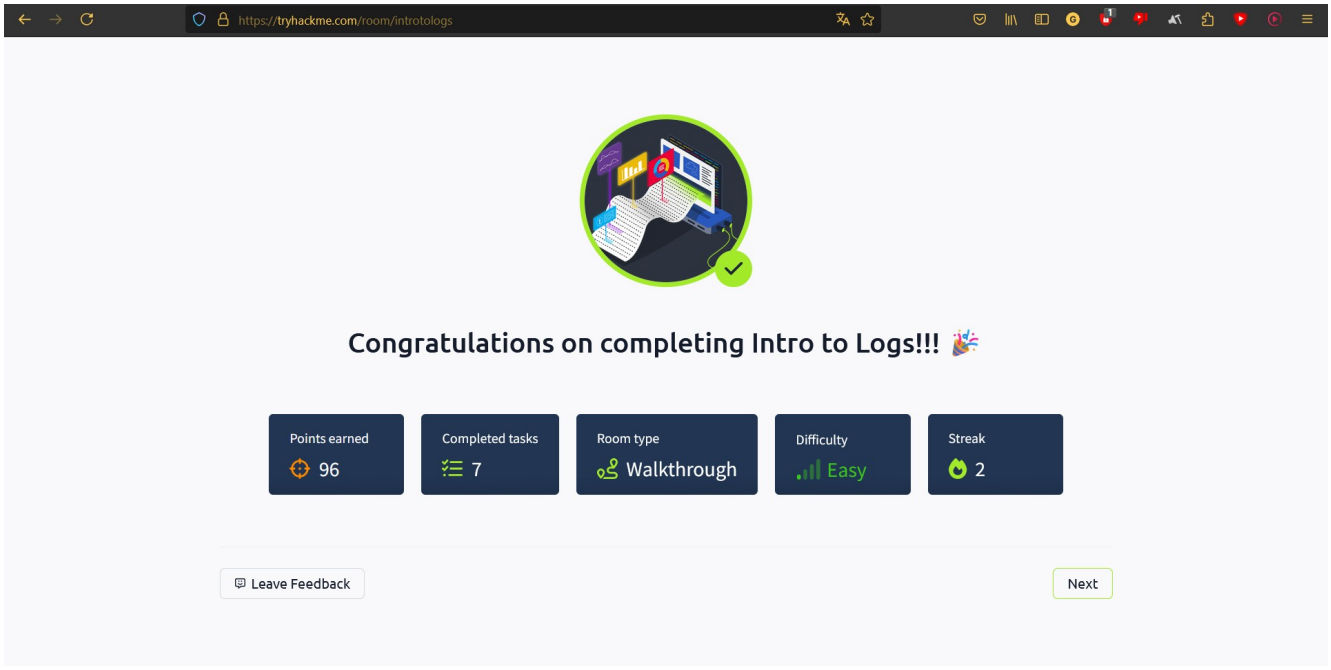
- 4738 - Zmieniono konto użytkownika.
- 4732 - Dodano członka do grupy lokalnej z włączonymi zabezpieczeniami.
- 4728 - Dodano członka do grupy globalnej z włączonymi zabezpieczeniami.

Te wydarzenia są najważniejsze bo ingerują w uprawnienia użytkowników, co może świadczyć o naruszaniu bezpieczeństwa.

Kto i kiedy zmienił uprawnienia użytkowników?

Użytkownik: „zaq”, godzina: 31.03.2025 02:28

Zadanie 5. *Wykonaj zadania ze strony: https://tryhackme.com/room/introtologs*



Rysunek 9: Potwierdzenie wykonania pracy na trychackme.com

4. Wnioski

Zrzuty pamięci jak i logi systemowe zawierają dużo przydatnych informacji, które można wykorzystać do analizy śledczej, celem wykrycia sprawców ataku, zidentyfikowanie podatności konfiguracji systemu, poznaniem metod używanych przez atakujących.