# Monitorowanie sieci z zastosowaniem NetFlow i Wazuh w celu wykrycia ataków na usługę Active Directory.

Analiza Ruchu Sieciowego

Paweł Zapiór

Wydział Informatyki i Telekomunikacji
Politechnika Krakowska

10.03.2024

**Streszczenie**

Celem projektu jest zastosowanie technologii NetFlow i Wazuh do monitorowania sieci w celu skutecznej identyfikacji ataków na usługę Active Directory. Poprzez analizę ruchu sieciowego za pomocą NetFlow oraz wykorzystanie funkcji detekcji zagrożeń oferowanych przez Wazuh, projekt ma umożliwić szybkie wykrywanie nieprawidłowości i podejrzanych aktywności związanych z usługą Active Directory. Integracja tych narzędzi umożliwi skuteczne śledzenie i reagowanie na potencjalne zagrożenia, zwiększając w ten sposób poziom bezpieczeństwa infrastruktury sieciowej opartej na Active Directory.

# Spis treści

**A Konfiguracja local_rules.xml [][7]** **34**

# Rozdział 1

# Wstęp

## 1.1 Dlaczego stosujemy systemy monitorowania sieci?

## 1.2 Cel i zakres pracy

## 1.3 Plan prac

1. Przygotowanie schematu infrastruktury
2. Przygotowanie obrazów wirtualnych maszyn i środowiska w GNS3
3. Konfiguracja danych adresowych na urządzeniach
4. Konfiguracja routingu z użyciem protokołu OSPF
5. Konfiguracja DHCP na routerach
6. Utworzenie VLANów i przypisanie portów do VLANów
7. Konfiguracja protokołu STP pomiędzy switchami S1, S2, S3
8. Konfiguracja wirtualnej bramy domyślnej i systemu równoważenia obciążenia dla podsieci IT
9. Konfiguracja systemu Windows Server 2016 PD, utworzenie kontrolera domeny
10. Konfiguracja usług sieciowych na Serwer1
11. Konfiguracja i wdrożenie Wazuh
12. Wdrożenie i konfiguracja kolektora NetFlow
13. Wykonanie ataków

14. Analiza ruchu sieciowego równolegle do przeprowadzanych ataków
15. Uzupełnienie dokumentacji i wniosków z pracy

# Rozdział 2

# Wprowadzenie teoretyczne

## 2.1 Analiza ruchu sieciowego

Analiza ruchu sieciowego jest istotna dla monitorowania i utrzymania prawidłowego działania oraz wydajności sieci komputerowych. Pozwala identyfikować potencjalne problemy, błędy w transmisji danych oraz incydenty cyberbezpieczeństwa. Dzięki analizie można więc także optymalizować wydajność sieci i identyfikować trendy, co przekłada się na lepsze zarządzanie infrastrukturą. Niniejsza praca podejmuje jednak temat wykorzystania analizy ruchu sieciowego w identyfikowaniu zagrożeń. Istnieją różne metody analizy ruchu sieciowego i wykrywania zagrożeń. Są to między innymi:

- IDS(Intrusion Detection System) analizują ruch sieciowy w poszukiwaniu nietypowych wzorców, sygnatur lub anomalii w celu wykrycia potencjalnych ataków. IPS (Intrusion Prevention System) działa podobnie do IDS, ale może również podjąć akcje prewencyjne, blokując lub ograniczając dostęp do zasobów w odpowiedzi na wykryte zagrożenie.

- XDR (Extended Detection and Response) rozwija koncepcję detekcji i reakcji integrując dane z różnych źródeł (endpointów, chmury, logów), aby zapewnić bardziej kompleksową analizę. XDR pozwala na szybkie i kompleksowe zrozumienie i reagowanie na zaawansowane ataki poprzez zbieranie i analizę danych.

- SIEM (Security Information and Event Management) gromadzi, analizuje i koreluje logi z różnych systemów w celu identyfikacji potencjalnych zagrożeń. Systemy SIEM umożliwiają monitorowanie zdarzeń w czasie rzeczywistym, a także retrospektywne analizowanie danych, co pomaga w identyfikowaniu nieprawidłowości i reagowaniu na nie.

- Funkcjonalności typu Port Mirroring, do których należą SPAN czy też RSPAN, umożliwia kierowanie kopii ruchu z jednego portu przełącz-

nika do innego w celu monitorowania. Ruch sieciowy jest zbierany i analizowany przez **kolektor**.

## 2.2 Protokół NetFlow

Protokół NetFlow jest technologią opracowaną przez firmę Cisco, używaną do monitorowania ruchu sieciowego. Pozwala na zbieranie informacji o przepływie danych, takich jak adresy źródłowe i docelowe, porty, ilość przesłanych danych itp. Te dane są następnie analizowane w celu optymalizacji wydajności sieci, diagnozowania problemów i planowania zasobów. NetFlow umożliwia administratorom uzyskanie wglądu w użycie sieci oraz identyfikowanie potencjalnych zagrożeń i ataków.

# Rozdział 3

# Metodyka i zastosowane technologie

## 3.1 Wybór narzędzi

### 3.1.1 GNS3

GNS3, (Graphical Network Simulator-3), to narzędzie do emulator sieci komputerowych. Pozwala na łączenie wirtualnych maszyn z różnych źródeł, takich jak obrazy systemów operacyjnych, routery czy przełączniki, bezpośrednio w jednym środowisku. GNS3 obsługuje różne platformy, co pozwala na integrację urządzeń różnych dostawców, co jest przydatne do testowania i eksperymentowania z różnymi konfiguracjami sieci. Dzięki temu użytkownicy mogą realistycznie emulować skomplikowane topologie sieciowe i przeprowadzać testy przed implementacją w rzeczywistych środowiskach.

### 3.1.2 Windows Server 2016 oraz Windows 10 Enterprise

Produkty firmy Microsoft są rozwiązaniami najczęściej stosowanymi w organizacjach. Zazwyczaj serwery i komputery pracowników powiązane są wspólną domeną *Active Directory*. Przez długi czas tylko i wyłącznie systemy z rodziny Windows pozwalały na wdrożenie usługi. Obecnie istnieje możliwość wdrożenia *Active Directory* w systemie Linux na bazie usługi Samba4, jednakże przy istotnie ograniczonej funkcjonalności (na poziomie funkcjonalności charakterystycznych dla usługi *Active Directory* znanej z systemu Windows Server 2008 R2). Między innymi z tego powodu jest to rozwiązanie stosunkowo rzadko spotykane w organizacjach. Wybrano wersję Windows Server 2016. Nie jest to najnowsza wersja systemu Windows Server, ale cały czas posiada wsparcie techniczne i aktualizacje bezpieczeństwa. Jest natomiast znacznie częściej spotykana w organizacjach niż najnowsza wersja Windows Server 2022, ponieważ aktualizacja systemu serwerowego do najnowszej wersji jest procesem złożonym i często nie znajduje z per-

spektywy firm uzasadnienia finansowego. Użycie starszej wersji jaką jest Windows Server 2016 samo w sobie nie może być również rozpatrywane jako podatność, ze względu na ciągłość wsparcia technicznego i aktualizacji bezpieczeństwa dostarczanych przez Microsoft. System Windows 10 w wersji Enterprise jest naturalnym uzupełnieniem systemu Windows Server 2016. Systemy z rodziny Windows są według raportu dostarczonego przez StackOverflow najczęściej wykorzystywane przez deweloperów w pracy profesjonalnej — stanowią aż 45,3% wszystkich urządzeń [1]. Jak natomiast wynika z raportu dostarczonego przez firmę AdDuplex system Windows 10 jest najczęściej używaną wersją spośród klienckich dystrybucji systemu Windows (na podstawie danych z czerwca 2022 roku) [2]. Podobnie jak w przypadku dystrybucji serwerowej, wersję *Trial* można pobrać za darmo na okres 90 dni ze strony: `https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise` oraz `https://info.microsoft.com/ww-landing-windows-server-2016.html`. Studenci mają także możliwość pobrania pełnej wersji systemu Windows Server 2016 oraz Windows 10 w wersji Education wraz z kluczami produktu ze strony `https://azureforeducation.microsoft.com/devtools` w ramach programu Microsoft Azure Dev Tools for Teaching. Wersja Education bazuje na wersji Enterprise i nie istnieją między nimi różnice, które wpływałyby na rezultaty otrzymane w niniejszej pracy.

### 3.1.3 Cisco 7200

Cisco 7200 to popularny model routera. W projekcie został zwirtualizowany przy pomocy orginalnego obrazu systemowego.

### 3.1.4 Kali Linux

Kali Linux system operacyjny oparty na dystrybucji Debian używany powszechnie do prowadzenia testów penetracyjnych. Zawiera wbudowanych wiele narzędzi przydatnych do przeprowadzania ataków, dzięki czemu nie trzeba instalować ich ręcznie. Tester bezpieczeństwa korzysta zazwyczaj z bardzo dużej ilości programów, skryptów, list i innych narzędzi więc użycie systemu Kali Linux pozwala zaoszczędzić bardzo dużo czasu na konfiguracji systemu i oprogramowania. System Kali Linux można pobrać za darmo ze strony `https://www.kali.org/get-kali/`.

### 3.1.5 SolarWinds

Jako kolektor NetFlow wybrano rozwiązanie NetFlow Traffic Analyzer form Solarwinds [4]. T narzędzie, które oferuje kompleksową analizę ruchu sieciowego, umożliwiając dokładne monitorowanie i zrozumienie, jakie aplikacje i urządzenia generują ruch w sieci. Dzięki zaawansowanym funkcjom raportowania i wizualizacji, administratorzy zyskują klarowny wgląd w użycie

pasma, co ułatwia optymalizację wydajności sieci. Do konfiguracji aplikacji użyto bazy danych Microsoft MySQL 2019.

### 3.1.6 Wazuh

Wazuh to otwarte narzędzie do monitorowania bezpieczeństwa i detekcji zagrożeń (Security Information and Event Management - SIEM) zaprojektowane do identyfikowania i reagowania na incydenty bezpieczeństwa w czasie rzeczywistym. Jest to platforma bezpieczeństwa IT, która integruje funkcje analizy logów, detekcji intruzów oraz zbierania i przetwarzania informacji z różnych źródeł. Wazuh oferuje również narzędzia do zarządzania zdarzeniami bezpieczeństwa, korzystając z zaawansowanych mechanizmów korelacji i analizy anomalii. Projekt Wazuh jest rozwijany jako otwarte oprogramowanie, co oznacza, że kod jest dostępny publicznie, co umożliwia społeczności przeglądanie, dostosowywanie i udoskonalanie narzędzia. Wazuh jest często stosowany do wzmocnienia bezpieczeństwa w środowiskach IT, wspomagając administratorów w identyfikowaniu i odpowiadaniu na potencjalne zagrożenia.

## 3.2 Metodyka badań symulacyjnych

Scenariusz zakłada, że jest to urządzenie w sieci, które udało mu się przejąć np. przy pomocy skutecznego ataku phishingowego. Tym komputerem jest maszyna o nazwie "Kali Linux". Następnie przy pomocy technologii do monitorowania sieci podjęta zostanie próba wykrycia i przerwania wykonywanych z tej stacji roboczych ataków.

# Rozdział 4

# Wdrożenie środowiska badawczego

## 4.1 Przygotowanie infrastruktury

Infrastruktura oparta jest o emulator sieci GNS3. Do wdrożenia infrastruktury wykorzystano hiperwizory typu II, oprogramowanie Oracle VM VirtualBox oraz VMWare Workstation 17. Utworzono 5 wirtualnych maszyn. Zezwolono GNS3 na zarządzanie konfiguracją sieciową wirtualnych maszyn.

Utworzone urządzenia to kolejno:

1. Trzy routery Cisco model 7200 połączone ze sobą każdy z każdym w celu uzyskania nadmiarowości. Router **Central** jest połączony z siecią publiczną Internet. Jest on jedynym w tej topologii pojedynczy punkt awarii (dalej w dokumentacji: SPF - Single point of failure). Routing odbywa się na bazie protokołu OSPF. Routery L (Left) oraz R (Right) stanowią bramy domyślne dla urządzeń w sieciach lokalnych.

2. Pięć przełączników Cisco warstwy drugiej.

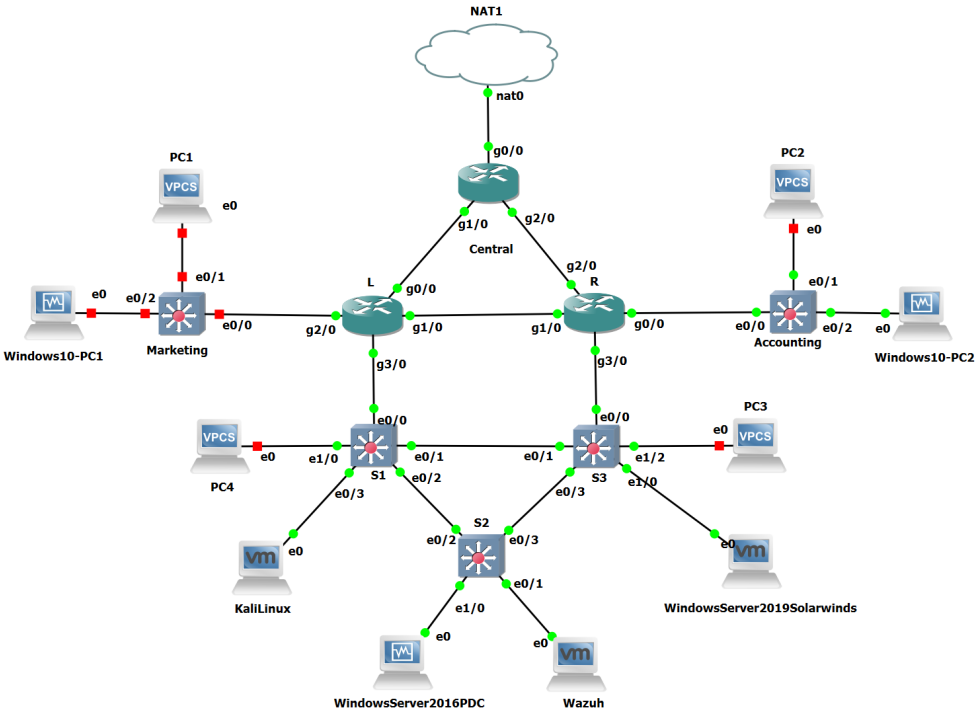
   - Przełącznik w dziale Marketingu
   - Przełącznik w dziale Księgowości
   - Trzy przełączniki S1, S2 i S3 połączone każdy z każdym w celu eliminacji SPF, zapewnienia równoważenia obciążenia oraz zwiększenia wydajności sieci. Podsieć posiada połączenie do dwóch routerów, zarówno do routera L jak i P. W praktyce bramą domyślną jest router wirtualny. Celem jest zapewnienie wysokiej dostępności.

3. Windows Server 2016 „PDC" (*Primary Domain Controler*) - podstawowy kontroler domeny. Pełni również funkcję:

- Preferowanego serwera DNS dla urządzeń w domenie company.sec.
- Serwera plików dla działu IT - udostępniony został katalog sieciowy.

4. Wazuh — system SIEM
5. Windows 10 „PC1" — komputer pracownika firmy z działu Marketingu,
6. Windows 10 „PC2" — komputer pracownika firmy z działu Księgowości. Ze względu na jego potrzeby zawodowe na tym komputerze konieczne było uruchomienie serwera stron Internetowych IIS.
7. Kali Linux „AttackBox" - komputer atakującego. Scenariusz zakłada, że jest to urządzenie w sieci, które udało mu się przejąć np. przy pomocy skutecznego ataku Phishingowego.
8. Windows Server 2019 „SolarWinds" — pełni funkcję kolektora danych i platformy analizy ruchu sieciowego.
9. 4 komputery VPCS standardowo dostępne w GNS3. Ich celem jest dostarczenie większej ilości logów.

Poniżej przedstawiony został schemat wdrożonej infrastruktury:




Rysunek 4.1: Schemat wdrożonej infrastruktury. Źródło: opracowanie własne.

### 4.1.1 Wdrożenie usługi domenowej *Active Directory*

Na wirtualnej maszynie „PDC" z systemem Windows Server 2016 zainstalowane zostały role *„Active Directory Domain Services"* (domenowe usługi *Active Directory*). Kontroler domeny został dodany do nowego lasu. Wybrano nazwę domeny „company.sec". Zainstalowano też rolę *„File and Storage Services"* dzięki czemu system mógł pełnić funkcję serwera plików.

### 4.1.2 Konfiguracja wdrożonego systemu informatycznego

Konfigurację środowiska rozpoczynamy od utworzenia dużej liczby użytkowników, tak aby zasymulować warunki panujące w firmie. Aby to zrealizować użyto skryptu napisanego w języku *PowerShell*. Został on załączony do pracy. Skrypt ten przyjmuje jako argument wejściowy plik *.csv*, pobiera z niego dane o użytkownikach i na ich podstawie tworzy konta domenowe. Wykorzystany plik *.csv* stanowi załącznik do niniejszej pracy.

Pracowników przydzielamy do grup, które stosowane są w systemie *Active Directory* do reglamentacji uprawnień. Odpowiednio utworzone zostają więc grupy o nazwach odpowiadających działowi firmy:

- *IT*,
- *Graphics*,
- *Administration*,
- *Security*.

Pracownicy działu IT firmy *„Company"* potrzebują także współdzielonego folderu do przechowywania danych. Utworzony zostaje więc folder *IT* i udostępniony jako zasób sieciowy. Zezwolono na dostęp do niego tylko pracownikom działu *IT* (grupa bezpieczeństwa *IT*). Dla testu utworzony został w udostępnionym folderze plik tekstowy *„Sensitive data.txt"* i wpisano do niego losowy ciąg znaków w celu weryfikowania, czy odpowiedni użytkownicy rzeczywiście mają do niego dostęp.

Komputery Windows 10 „PC1" i Windows 10 „PC2" zostały dodane do domeny „company.sec". Ponadto na komputerze Windows 10 „PC2" zainstalowany został serwer stron internetowych IIS, ponieważ urządzenie „PC2" należy do programisty stron Internetowych w firmie *„Company"* i lokalny serwer www jest mu niezbędny w codziennej pracy.

Na podstawie raportów **Microsoft Digital Defense Report** [8] [9] wytypowano również często występujące w organizacjach modyfikacje domyślnej konfiguracji powodujące podatności. Wdrożono więc następujące poprawki do domyślnej konfiguracji *Active Directory*, które pozwolą na przeprowadzenie ataków przedstawionych w kolejnych rozdziałach.

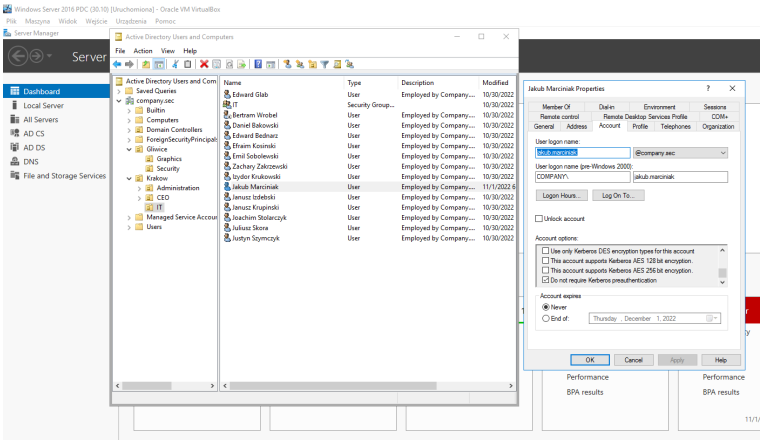
**Scenariusz konfiguracji: włączenie konta lokalnego Administratora na komputerach.**

Przyczyną, dla której pracownicy działów IT często włączają konto standardowego Administratora lokalnego jest konieczność utrzymania na stacji roboczej przynajmniej jednego konta użytkownika o uprawnieniach administracyjnych. Nie biorą jednak pod uwagę, że zamiast tego mogą oni pozostawić konto użytkownika z uprawnieniami Administracyjnymi uzyskiwanymi na bazie mechanizmu UAC (*User Access Control*). Aby uprościć zarządzanie infrastrukturą w dużych organizacjach zdarza się też, że Administrator ustawia to samo hasło do konta lokalnego Administratora na każdym komputerze w organizacji. Dodatkowy problem stanowi też współdzielenie tego hasła przez pracowników działu IT. Jednym z celów pracy będzie zrealizowanie i wykrycie ataku wynikającego z takiej metodyki zarządzania infrastrukturą w organizacji może nieść ze sobą niebezpieczeństwo.

**Scenariusz konfiguracji: Wyłączenie na wybranym koncie użytkownika wymogu preautentykacji**

Firma Company rozwija się ponadprzeciętnie szybko i liczba kont użytkowników w *Active Directory* dla pracowników przekroczyła kilkaset tysięcy.

W celu sprawnego zarządzania dostępami przy zachowaniu zasady „najmniejszego uprzywilejowania" Administratorzy utworzyli też bardzo dużą ilość grup bezpieczeństwa. W rezultacie każdy użytkownik należy do kilkuset grup. Okazało się, że bilet przyznawania biletów protokołu Kerberos jest tak duży, że usługa odpowiedzialna za uwierzytelnianie jest silnie przeciążona i nie w stanie realizować swoich zadań ze względu na ograniczone zasoby mocy obliczeniowej. Administrator zauważył, że problem znika, jeśli odznaczy opcję ***Do not require Kerberos preauthentication***. W rezultacie tego



Rysunek 4.2: Aktywowanie opcji ***Do not require Kerberos preauthentication*** dla jednego z użytkowników domenowych

działania proces uwierzytelniania oparty na protokole Kerberos znów odbywa się sprawnie, a procesor serwera na którym zainstalowany jest kontroler domeny nie jest przeciążony. W analizowanym środowisku wprowadzona zostaje więc następująca konfiguracja: na wybranych kontach użytkowników opcja ***Do not require Kerberos preauthentication*** zostaje aktywowana, tak jak na zamieszczonym wcześniej zrzucie ekranowym. Należy jednak nadmienić, że dysponując symulowanym środowiskiem opartym o wirtualizację typu II wdrożoną na komputerze osobistym nie istnieje możliwość odpowiedniego zasymulowania warunków, które przedstawione zostały w scenariuszu i które doprowadzą do wywołania omawianego problemu wydajnościowego. Do wdrażanej konfiguracji nie zostaje więc dodana ani tak duża ilość użytkowników, ani tak duża ilość grup bezpieczeństwa. Aktywowano jedynie wspomnianą opcję na koncie użytkowników domenowych *pawel.zapior* oraz *jakub.marciniak*, co często jest wykorzystywane jako rozwiązanie opisanego problemu. Na etapie testów penetracyjnych wdrożonej infrastruktury przeanalizujemy konsekwencje związane z aktywowaniem tej opcji.

**Scenariusz konfiguracji: przypisanie usługi IIS do konta Administrator**

Zgodnie z przedstawioną w części teoretycznej zasadą działania usług w *Active Directory*, utworzony został *Service Principal Name* dla usługi IIS z kontem *Administrator*. Akcja ta została wykonana z poziomu konta **Administratora Domeny**. Zostało użyte następujące polecenie w celu przypisania usługi do konta:

```
1 setspn -a http/PC2.company.sec company.sec\Administrator
```

### 4.1.3 Konfiguracja danych adresowych

Przydzielone zostały następujące dane adresowe:

| Urządzenie | Interfejs | Adres IP | Maska podsieci | VLAN |
|---|---|---|---|---|
| Central | g0/0 | DHCP | DHCP (/24) | - |
| | g1/0 | 10.0.0.1 | 255.255.255.252 | - |
| | g2/0 | 10.0.0.5 | 255.255.255.252 | - |
| L | g0/0 | 10.0.0.2 | 255.255.255.252 | - |
| | g1/0 | 10.0.0.10 | 255.255.255.252 | - |
| | g2/0 | 10.2.0.1 | 255.255.255.0 | VLAN30 Marketing |
| | g3/0.10 | 10.1.0.1 | 255.255.255.0 | VLAN10 Management |
| | g3/0.20 | 10.2.0.1 | 255.255.255.0 | VLAN20 Admin |
| R | g0/0 | 10.4.0.1 | 255.255.255.0 | VLAN40 Accounting |
| | g1/0 | 10.0.0.9 | 255.255.255.252 | - |
| | g2/0 | 10.0.0.6 | 255.255.255.252 | - |
| | g3/0.10 | 10.1.0.2 | 255.255.255.0 | VLAN10 Management |
| | g3/0.20 | 10.2.0.2 | 255.255.255.0 | VLAN20 Admin |
| HSRP | Virtual Gateway | 10.1.0.10 | | VLAN10 Management |
| HSRP | Virtual Gateway | 10.2.0.10 | | VLAN20 Admin |

Sieci lokalne i urządzenia końcowe:

| Urządzenie | Interfejs | Adres IP | Maska podsieci | Brama domyślna | VLAN |
|---|---|---|---|---|---|
| Marketing | VLAN30 | 10.3.0.2 | 255.255.255.0 | 10.3.0.1 | 30 |
| WS10 PC1 | VLAN30 | DHCP | 255.255.255.0 | 10.3.0.1 | 30 |
| PC1 | VLAN30 | DHCP | 255.255.255.0 | 10.3.0.1 | 30 |
| Accounting | VLAN40 | 10.3.0.2 | 255.255.255.0 | 10.4.0.1 | 40 |
| WS10 PC2 | VLAN40 | 10.4.0.20 | 255.255.255.0 | 10.4.0.1 | 40 |
| PC2 | VLAN40 | DHCP | 255.255.255.0 | 10.4.0.1 | 40 |
| S1 | VLAN10 | 10.1.0.11 | 255.255.255.0 | 10.1.0.10 | 10 |
| | VLAN20 | 10.2.0.11 | 255.255.255.0 | 10.2.0.10 | 20 |
| S2 | VLAN10 | 10.1.0.12 | 255.255.255.0 | 10.1.0.10 | 10 |
| | VLAN20 | 10.2.0.12 | 255.255.255.0 | 10.2.0.10 | 20 |
| S3 | VLAN10 | 10.1.0.13 | 255.255.255.0 | 10.1.0.10 | 10 |
| | VLAN20 | 10.2.0.13 | 255.255.255.0 | 10.2.0.10 | 20 |
| KaliLinux * | VLAN10 | DHCP | 255.255.255.0 | 10.1.0.10 | 10 |
| | VLAN20 | DHCP | 255.255.255.0 | 10.2.0.10 | 20 |
| PC4 | VLAN20 | DHCP | 255.255.255.0 | 10.2.0.10 | 20 |
| WS2016 PDC | VLAN10 | 10.1.0.100 | 255.255.255.0 | 10.1.0.10 | 10 |
| WS2019 SolarWinds | VLAN10 | 10.1.0.200 | 255.255.255.0 | 10.1.0.10 | 10 |
| Wazuh | VLAN10 | 10.1.0.201 | 255.255.255.0 | 10.1.0.10 | 10 |
| PC3 | VLAN20 | DHCP | 255.255.255.0 | 10.2.0.10 | 20 |

W celu realizacji różnych scenariuszy ataku system Kali Linux może być przenoszony pomiędzy VLANem 20 a 10. Domyślnym serwerem DNS dla wszystkich urządzeń jest Windows Server 2016 PDC (10.1.0.100).

## 4.2 Konfiguracja

### 4.2.1 Routery

W ramach konfiguracji urządzeń sieciowych nadano adresy na odpowiednich interfejsach zgodnie z powyższą adresacją. Routing między Central, L i P skonfigurowano z użyciem protokołu OSPFv2. Nadano *process_ID* numer **10**. Routerom nadano następujące identyfikatory:

- Central: 1.1.1.1
- R: 2.2.2.2
- L: 3.3.3.3

Dodano baner o treści "Authorized Users Only!". Następnie na L i P skonfigurowano routing między VLANami 10 i 20 poprzez technikę tzw. "routera na patyku" oraz protokół FHRP, który pozwala na utworzenie wirtualnej

bramy domyślnej i równoważenia obciążenia między dwa fizyczne urządzenia. Na koniec skonfigurowano dostęp do sieci Internet poprzez trasę domyślną na routerze Central skierowaną na interfejs g0/0.

```
Central(config)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         192.168.60.130  YES DHCP   up                    up
GigabitEthernet1/0         10.0.0.1        YES NVRAM  up                    up
GigabitEthernet2/0         10.0.0.5        YES NVRAM  up                    up
GigabitEthernet3/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0         unassigned      YES NVRAM  administratively down down
Central(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.60.2 to network 0.0.0.0

C    192.168.60.0/24 is directly connected, GigabitEthernet0/0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       10.0.0.8/30 [110/2] via 10.0.0.6, 00:11:29, GigabitEthernet2/0
                    [110/2] via 10.0.0.2, 00:11:29, GigabitEthernet1/0
O       10.2.0.0/24 [110/2] via 10.0.0.6, 00:04:03, GigabitEthernet2/0
                    [110/2] via 10.0.0.2, 00:11:29, GigabitEthernet1/0
O       10.3.0.0/24 [110/2] via 10.0.0.2, 00:11:29, GigabitEthernet1/0
C       10.0.0.0/30 is directly connected, GigabitEthernet1/0
O       10.1.0.0/24 [110/2] via 10.0.0.6, 00:03:53, GigabitEthernet2/0
                    [110/2] via 10.0.0.2, 00:11:29, GigabitEthernet1/0
O       10.4.0.0/24 [110/2] via 10.0.0.6, 00:11:29, GigabitEthernet2/0
C       10.0.0.4/30 is directly connected, GigabitEthernet2/0
S*   0.0.0.0/0 [1/0] via 192.168.60.2
Central(config)#do sh ip ospf ne

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:31    10.0.0.6        GigabitEthernet2/0
3.3.3.3           1   FULL/DR         00:00:30    10.0.0.2        GigabitEthernet1/0
Central(config)#
```

Rysunek 4.3: Konfiguracja routera Central. Źródło: opracowanie własne.

### 4.2.2 Przełączniki

Konfigurację przełączników rozpoczęto od zdefiniowania połączeń trunkowych. W przypadku powyższego schematu są to połączenia pomiędzy przełącznikami S1, S2 i S3. Następnie skonfigurowano protokół STP, który zapobiega powstawaniu pętli w przy połączeniach z redundancją i pozwala na utworzenie topologii mesh z przełączników. Na przełącznikach skonfigurowano vlany. Na routerze L skonfigurowano serwer DHCP dla podsieci 10.2.0.0/24.

## 4.3 Wdrożenie systemu monitorowania sieci

Jako system pełniący w sieci funkcję kolektora NetFlow i jest platformą do analizy logów kolektora wybrano Windows Server 2019 „SolarWinds". W systemie zainstalowano NetFlow Traffic Analyzer form SolarWinds. [4].

```
S1#show vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/1, Et1/2, Et1/3, Et2/0
                                                 Et2/1, Et2/2, Et2/3, Et3/0
                                                 Et3/1, Et3/2, Et3/3
10   VLAN0010                          active
20   VLAN0020                          active    Et0/3, Et1/0
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.1.0.11       YES NVRAM  up                    up
Vlan20                 10.2.0.11       YES NVRAM  up                    up
S1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     aabb.cc00.0200
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     aabb.cc00.0200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
Et2/0               Desg FWD 100       128.9    Shr
Et2/1               Desg FWD 100       128.10   Shr
Et2/2               Desg FWD 100       128.11   Shr
 --More--
```

Rysunek 4.4: Konfiguracja przełącznika S1. Źródło: opracowanie własne.

# Rozdział 5

# Badania symulacyjne

## 5.1 Password spraying

### 5.1.1 Wstęp teoretyczny

Atak ***Password Spraying*** zgodnie z klasyfikacją *MITRE ATT&CK* [12] zaliczany jest do ataków siłowych (ang. *Brute Force*). Zakłada on wykorzystanie jednego lub kilku haseł w celu uzyskania popranych danych uwierzytelniających konta domenowego w sposób opisany poprzednim podrozdziale. Atak ten jest powszechnie wykorzystywany przez wiele grup przestępczych, ponieważ minimalizuje on prawdopodobieństwo zablokowania pojedynczego konta domenowego, co mogłoby nastąpić przy wielokrotnych próbach logowania się na jedno konto wieloma hasłami. Rozpylane hasło które wybierają grupy hakerskie często jest związane z nazwą firmy i geolokalizacją. Praktyka pokazuje, że z użyciem właśnie takich słów kluczowych pracownicy najczęściej tworzą swoje hasła.

### 5.1.2 Scenariusz ataku

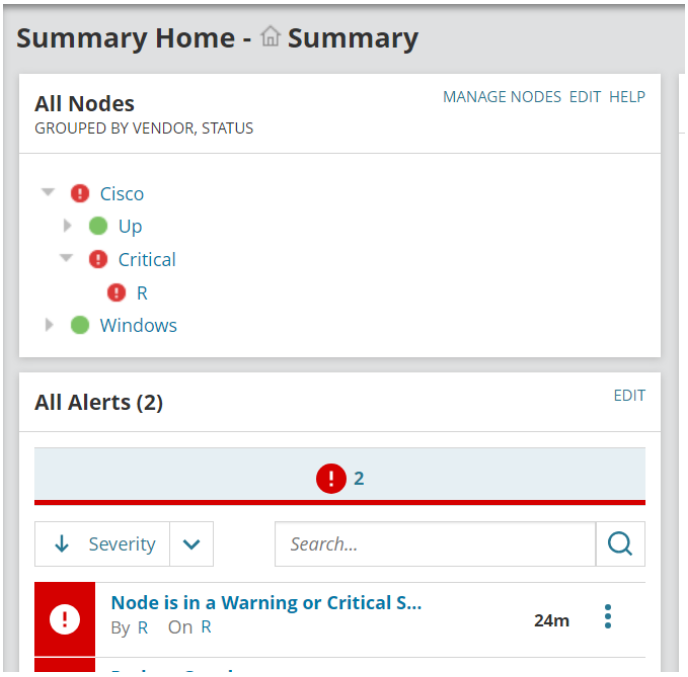
Użyte zostało narzędzie *crackmapexec*. Dokonano próby logowania na każdego użytkownika w domenie używając protokołu SMB na kontroler domeny „PDC" z hasłami *'Company1', 'Companysec1', 'CompanySec1'*.


Rysunek 5.1: Atak passowrd spraying. Źródło: opracowanie własne.

Atakujący odniósł sukces: okazuje się, że użytkownik jakub.marciniak używał hasła 'CompanySec1'. Wygenerował jednak dużą ilość ruchu sieciowego.

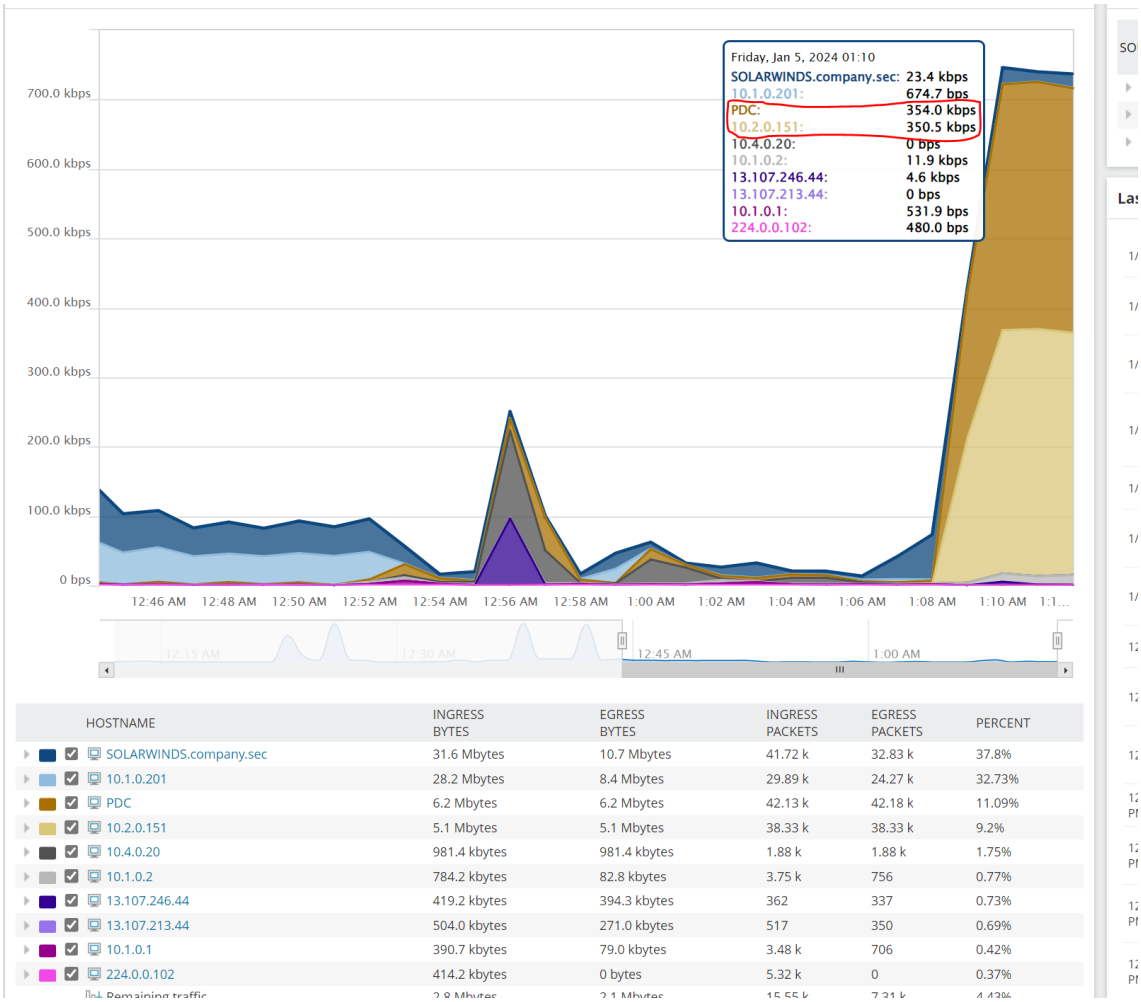
### 5.1.3 Wykrycie i mityzacja

Analityk bezpieczeństwa otrzymuje powiadomienie z systemu Solarwinds.




Rysunek 5.2: Alert z kolektora NetFlow. Źródło: opracowanie własne.

Okazuje się, że jest to ruch do kontrolera domeny PDC wysyłany z urządzenia o adresie 10.2.0.151. To adres, który w sieci korporacyjnej jest przydzielany przez serwer DHCP w VLANie 2 dla użytkowników końcowych.



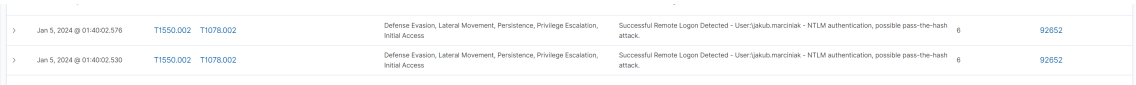

| HOSTNAME | INGRESS BYTES | EGRESS BYTES | INGRESS PACKETS | EGRESS PACKETS | PERCENT |
|---|---|---|---|---|---|
| SOLARWINDS.company.sec | 31.6 Mbytes | 10.7 Mbytes | 41.72 k | 32.83 k | 37.8% |
| 10.1.0.201 | 28.2 Mbytes | 8.4 Mbytes | 29.89 k | 24.27 k | 32.73% |
| PDC | 6.2 Mbytes | 6.2 Mbytes | 42.13 k | 42.18 k | 11.09% |
| 10.2.0.151 | 5.1 Mbytes | 5.1 Mbytes | 38.33 k | 38.33 k | 9.2% |
| 10.4.0.20 | 981.4 kbytes | 981.4 kbytes | 1.88 k | 1.88 k | 1.75% |
| 10.1.0.2 | 784.2 kbytes | 82.8 kbytes | 3.75 k | 756 | 0.77% |
| 13.107.246.44 | 419.2 kbytes | 394.3 kbytes | 362 | 337 | 0.73% |
| 13.107.213.44 | 504.0 kbytes | 271.0 kbytes | 517 | 350 | 0.69% |
| 10.1.0.1 | 390.7 kbytes | 79.0 kbytes | 3.48 k | 706 | 0.42% |
| 224.0.0.102 | 414.2 kbytes | 0 bytes | 5.32 k | 0 | 0.37% |

Rysunek 5.3: Analiza ruchu z NetFlow. Źródło: opracowanie własne.

Analityk przechodzi na system Wazuh. Okazuje się, że jest duża ilość niepoprawnych prób logowania na urządzeniu PDC.


Rysunek 5.4: Analiza eventów dla klienta PDC w Wazuh. Źródło: opracowanie własne.

Wśród logów dla tego urządzenia końcowego, analityk odnajmuje ostrzeżenie o skutecznym logowaniu na konto jakub.marciniak z hosta podejrzanego o przeprowadzenie ataku.



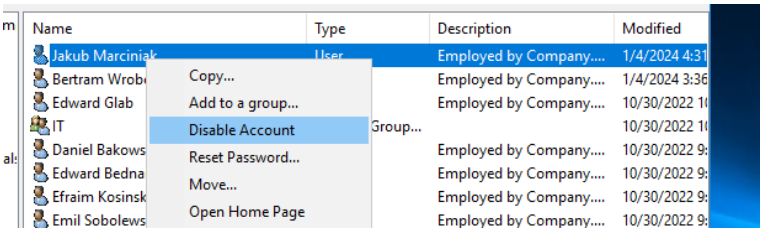
Rysunek 5.5: Analiza logów w systemie Wazuh. Źródło: opracowanie własne.

Table JSON Rule

| | |
|---|---|
| @timestamp | 2024-01-05T01:40:02.530Z |
| _id | d7hH14wB2Z7qb4VGA7VW |
| agent.id | 001 |
| agent.ip | 10.1.0.100 |
| agent.name | PDC |
| data.aws.accountId | |
| data.aws.region | |
| data.win.eventdata.authenticationPackageName | NTLM |
| data.win.eventdata.elevatedToken | %%1842 |
| data.win.eventdata.impersonationLevel | %%1833 |
| data.win.eventdata.ipAddress | 10.2.0.151 |
| data.win.eventdata.ipPort | 58280 |
| data.win.eventdata.keyLength | 128 |
| data.win.eventdata.lmPackageName | NTLM V2 |
| data.win.eventdata.logonGuid | {00000000-0000-0000-0000-000000000000} |
| data.win.eventdata.logonProcessName | NtLmSsp |
| data.win.eventdata.logonType | 3 |
| data.win.eventdata.processId | 0x0 |
| data.win.eventdata.subjectLogonId | 0x0 |
| data.win.eventdata.subjectUserSid | S-1-0-0 |
| data.win.eventdata.targetDomainName | COMPANY |
| data.win.eventdata.targetLinkedLogonId | 0x0 |
| data.win.eventdata.targetLogonId | 0x862d3 |
| data.win.eventdata.targetUserName | jakub.marciniak |

Rysunek 5.6: Analiza logów w systemie Wazuh. Źródło: opracowanie własne.

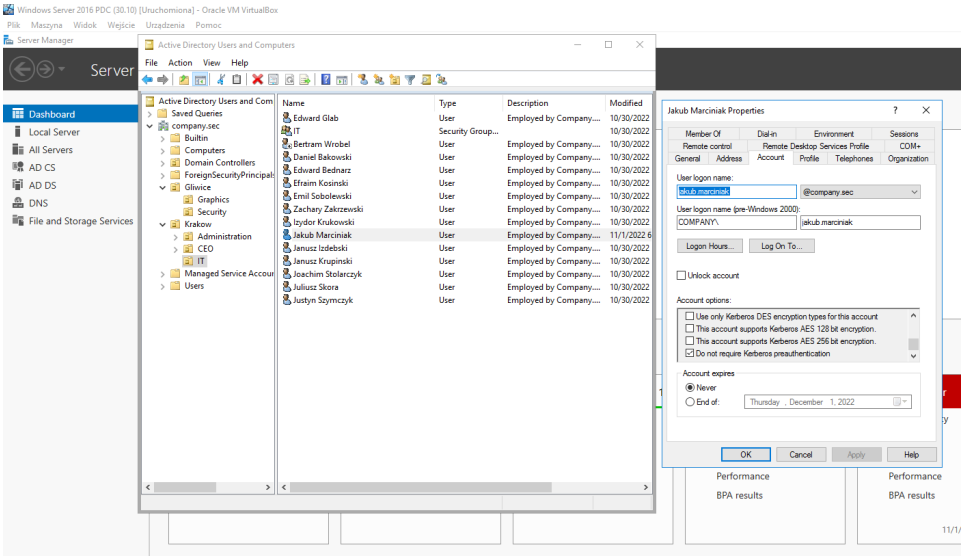
Analityk podejmuje decyzje o natychmiastowym zablokowaniu konta Pana Jakuba Marciniaka po stronie Active Directory. Konto nie może być już wykorzystane do eskalacji uprawnień przez atakującego.




Rysunek 5.7: Zablokowanie konta Pana Jakuba Marciniaka. Źródło: opracowanie własne.

## 5.2 AS-REP Roasting

Atak o nazwie *AS-REP Roasting* zakłada zastosowanie niebezpiecznej konfiguracji konta użytkownika polegającej na włączeniu opcji ***Do not require Kerberos preauthentication*** (Nie wymagaj preuwierzytelniania protokołu Kerberos). Poniżej przedstawiony został zrzut ekranowy, pokazujący gdzie można wprowadzić omawiane ustawienie.

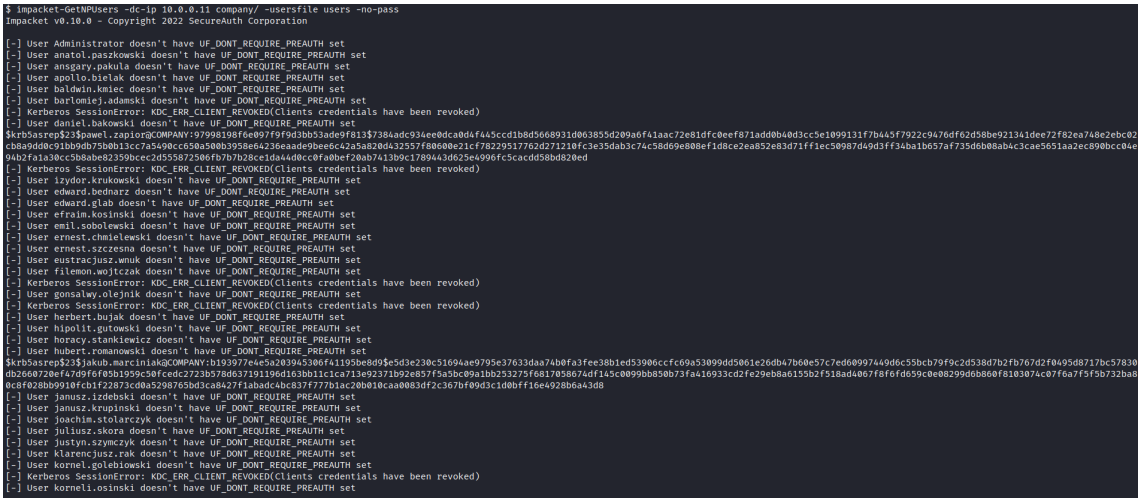



Rysunek 5.8: Zrzut ekranowy przedstawia aktywowanie opcji **Do not require Kerberos preauthentication** dla użytkownika jakub.marciniak. Źródło: opracowanie własne.

### Scenariusz ataku

Załóżmy, że analitykowi bezpieczeństwa nie udało się wykryć pierwszego ataku. Atakujący przejął zatem już konto użytkownika domenowego w ramach pierwszego ataku przedstawionego w ramach testów bezpieczeństwa infrastruktury (Nazwa użytkownika: jakub.marciniak, Hasło: CompanySec1) i ma on możliwość wykonania zrzutu całej struktury bazy LDAP co pozwoli mu odkryć wszystkich użytkowników w domenie. Następnie korzystając ze skryptu z narzędzia *Impacket* o nazwie *GetNPUsers* atakujący może sprawdzić czy, którykolwiek z użytkowników w domenie posiada aktywowaną opcję ***Do not require Kerberos preauthentication*** i uzyskać skrót jego hasła **Kerberos 5, etype 23, AS-REP**.

Jak widać na powyższym zrzucie ekranowym, konta dwóch użytkowników zostały skonfigurowane w ten sposób. Atak spowodował przejęcie skrótów ich haseł. Łamiąc je atakujący jest wstanie przejąć ich konta i wy-

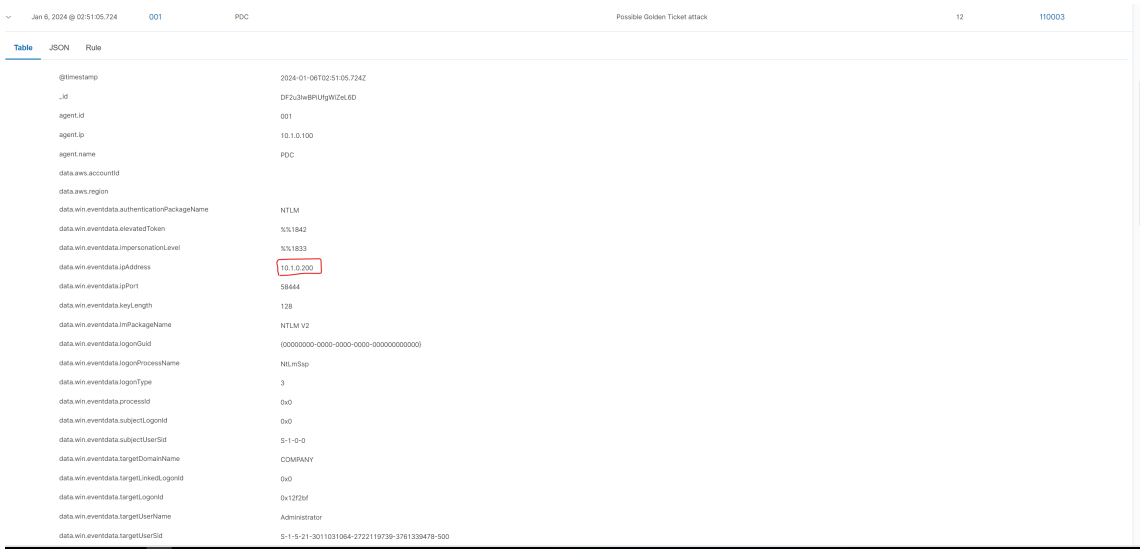



Rysunek 5.9: Przy pomocy pakietu *Impacket* atakujący sprawdza, czy istnieją użytkownicy domenowi, od których preuwierzytelnianie protokołu Kerberos nie jest wymagane. Źródło: opracowanie własne.

konywać wszystkie działania w domenie w ich imieniu. W tym przypadku użytkownik pawel.zapior posiada uprawnienia Administratora Domeny więc przejęcie jego konta daje atakującemu uprawnienia do zarządzania domeną.

### Wykrywanie

Ilość ruchu sieciowego nie była duża. Jej charakter nie był też na tyle podejrzany, aby wygenerować alert w Solarwinds. Wazuh wygenerował natomiast alert o możliwym ataku na złoty bilet Kerberos. Okazuje się jednak, że alert ten nie dotyczy maszyny wirtualnej atakującego.



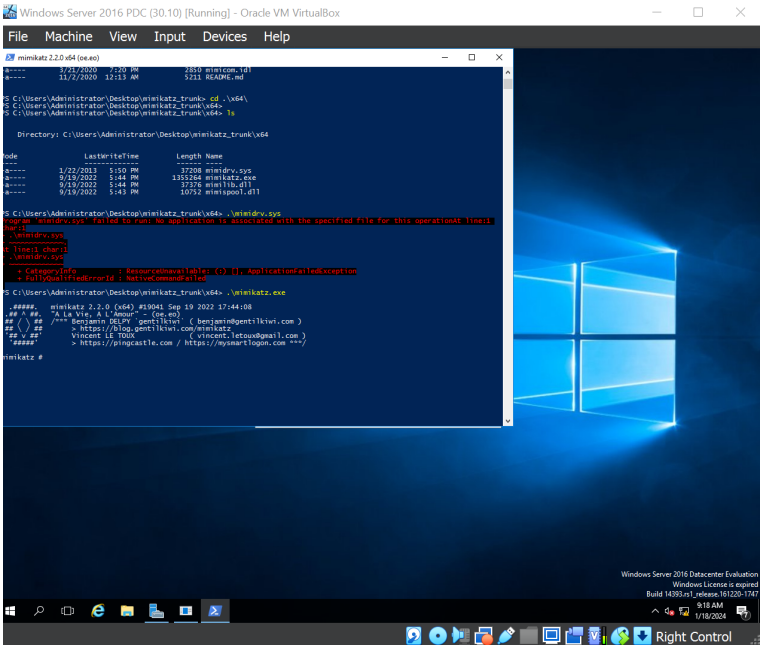

Rysunek 5.10: Weryfikacja alertu o możliwym ataku na Golden Ticket. Źródło: opracowanie własne.

Ataku nie udało się więc wykryć pomimo zastosowania dodatkowych reguł dedykowanych przez twórców Wazuh. To pokazuje trudnym do wykrycia jest atak AS-REP Roasting. Co za tym idzie, jak poważnym błędem konfiguracyjnym jest wyłączenie preautentykacji. Atak ten jest w swojej charakterystyce bardzo cichy i wygenerowany ruch sieciowy nie jest podejrzany z punktu widzenia charakterystyki usługi domeny Active Directory.

**Wyłączenie preautentykacji protokołu Kerberos jest błędem krytycznym!**

## 5.3 Użycie Mimikatz w systemie Windows Server

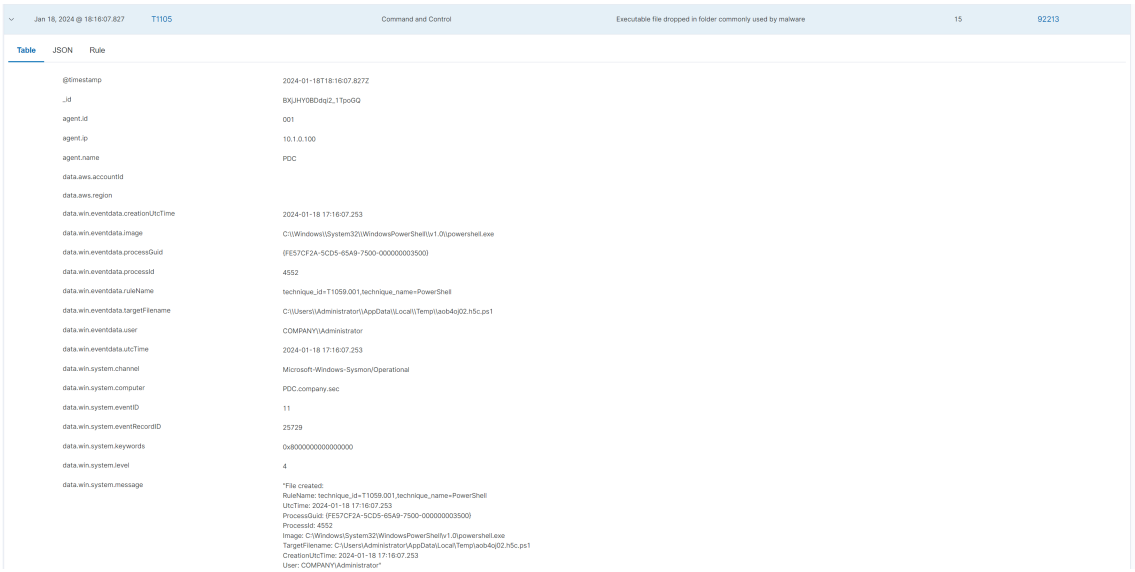
Mimikatz to narzędzie stworzone przez Benjamina Delpy, które jest używane do ekstrakcji i manipulacji danych uwierzytelniających w systemach Windows. Zdolne jest do odzyskiwania haseł w formie tekstowej z pamięci systemowej, złamywania systemów uwierzytelniania jednorazowego (np. Kerberos), oraz uzyskiwania dostępu do haseł przechowywanych w systemie. Mimikatz może również umożliwiać przejęcie tokenów dostępowych, co pozwala na eskalację uprawnień. Narzędzie to jest często wykorzystywane w testach penetracyjnych, ale także może być używane w atakach przez złośliwe oprogramowanie w celu kradzieży danych uwierzytelniających. Warto zauważyć, że choć Mimikatz ma zastosowania w celach badawczych, może być również wykorzystywane w działaniach nielegalnych, stąd istnieje konieczność ścisłego monitorowania i zabezpieczania systemów przed jego potencjalnym użyciem.




Rysunek 5.11: Uruchomienie Mimikatz. Źródło: opracowanie własne.

### 5.3.1 Wykrycie i mitygacja

Jak widać na poniższym zrzucie ekranowym Wazuh wykrył zagrożenie od razu i sklasyfikował je na najwyższym, 15 poziomie.




Rysunek 5.12: Wykrycie próby pobrania mimikatz. Źródło: opracowanie własne.

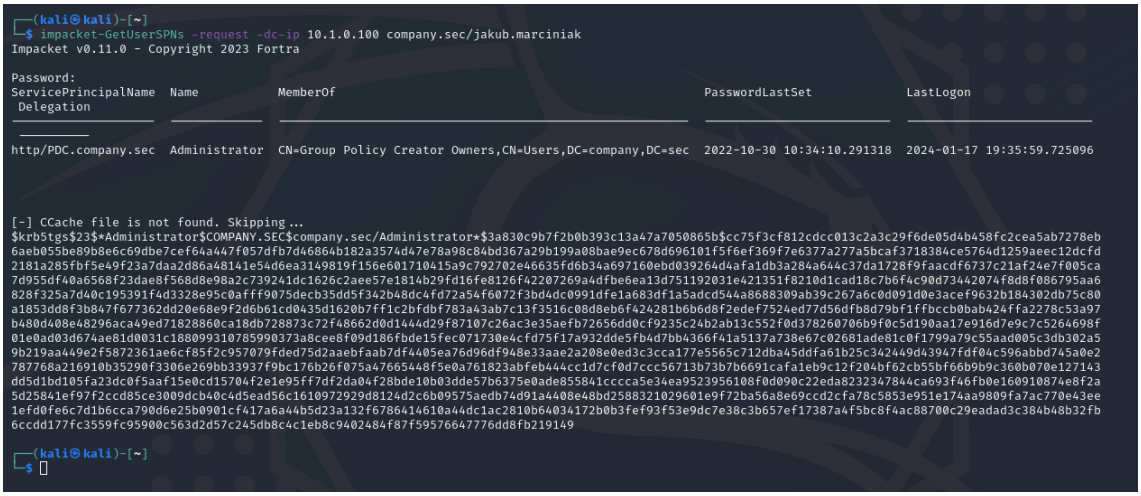
## 5.4 Kerberoasting

Na wstępie warto przypomnieć, że we wdrożonym środowisku przypisane zostało konto użytkownika Administrator do usługi stron Internetowych IIS. Skutkiem takiej konfiguracji każdy użytkownik domenowy jest wstanie zażądać biletu do tej usługi, a w odpowiedzi otrzyma zahashowane hasło konta przypisanego do SPN w formacie **$krb5tgs$23$*** (jeżeli poprosi o szyfrowanie RC4) albo **$krb5tgs$18$*** (jeżeli poprosi o szyfrowanie AES-256).

Do usługi działającej w ramach *Active Directory* można przypisać zarówno konto użytkownika jak i konto maszynowe. Celem ataku Kerberoasting jest przechwycenie biletu TGS dla usługi, która została przypisana do konta użytkownika. Usługi powiązane z kontem komputera są odporne na atak, ponieważ hasła kont maszynowych są niemożliwe do złamania ze względu na długość (120 znaków) i są automatycznie zmieniane co 30 dni w podstawowej konfiguracji. W związku z tym część biletów TGS jest szyfrowana za pomocą kluczy bazujących na hasłach użytkowników. W przypadku powodzenia ataku przechwycone dane uwierzytelniające mogą zostać złamane na lokalnej maszynie atakującego. Z tego powodu do Kerberoasting atakujący potrzebuje tylko konta domenowego standardowego użytkownika, które może zażądać biletu TGS. Nie są wymagane inne specjalne uprawnienia [**?**].

### Scenariusz ataku

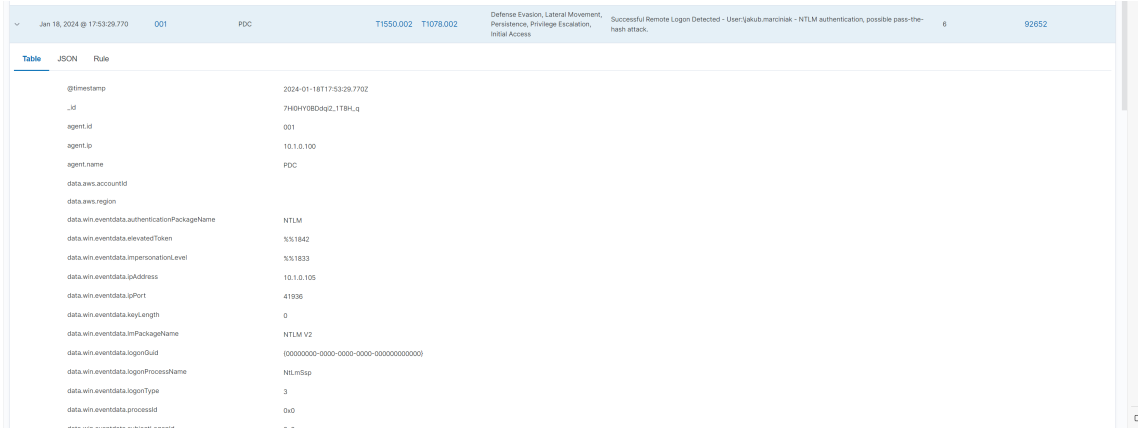
Aby zażądać biletu TGS dla usługi wykorzystano skrypt pakietu Impacket GetUserSPNs podając w zapytaniu dane uwierzytelniające przejętego wcześniej użytkownika domenowego.




Rysunek 5.13: Uzyskanie zahashowanych danych uwierzytelniających poprzez atak *Kerberoasting*. Źródło: opracowanie własne.

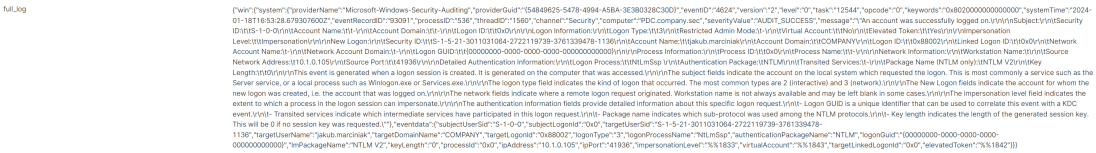
## 5.4.1 Wykrycie i mitygacja

Pojawił się alert o zdalnym logowaniu na konto jakub.marciniak, które zostało wykorzystane do ataku. Tym razem zablokowanie konta nie będzie




Rysunek 5.14: Analiza ataku *Kerberoasting* w Wazuh. Źródło: opracowanie własne.

jednak wystarczające. Z pełnych logów widać, że wykonano zdalne logowa-




Rysunek 5.15: Analiza ataku *Kerberoasting* w Wazuh. Źródło: opracowanie własne.

nie na konto, co może sugerować przeprowadzanie ataku. Nie pojawił się jednak alert sugerujący wprost przeprowadzenie ataku Kerberoasting. Analityk może jednak wyciągnąć taki wniosek z szerszego kontekstu. Wcześniej atakujący musi zdobyć poświadczenia standardowego użytkownika, więc jeśli wykonuje z tego samego adresu IP kolejne połącznie, które jest sklasyfikowane jako potencjalnie niebezpieczne to powinno to stanowić podstawę do analizy podejrzanego hosta.

# Rozdział 6

# Podsumowanie

## 6.1 Rezultaty

W przebiegu projektów wykonano 4 ataki charakterystyczne dla domeny Active Directory. Pomimo zastosowania dodatkowych regół i konfiguracji w Wazuh udało się wykryć jedynie 3 z nich.

- Najprostszym do wykrycia atakiem był Password Spraying. Technika ta generuje dużą ilość ruchu sieciowego. Użytkownik, którego konto zostało przejęte został skutecznie wyznaczony, a jego konto mogło zostać zablokowane. Użyteczny był zarówno protokół Netflow jak i Wazuh.
- Zagrożenie związane z użyciem niebezpiecznego oprogramowania zostało poprawnie zidentyfikowane przez Wazuh.
- Najtrudniejszy do wykrycia i zarazem jedyny atak, którego nie udało się wykryć był AS-REP Roasting oraz Kerberoasting. Wynikają one z krytycznych błędów konfiguracyjnych, które pozostawia otwarte drzwi do ataków hakerskich. Przeciwdziałanie powinno polegać przede wszystkim na prewencji i wykryciu błędnej konfiguracji podczas audytu bezpieczeństwa.

## 6.2 Wnioski

Projekt miał na celu zastosowanie technologii NetFlow i narzędzia Wazuh do monitorowania sieci w celu skutecznej identyfikacji ataków na usługę Active Directory. W trakcie realizacji projektu zauważono, że Wazuh, chociaż jest potężnym narzędziem do detekcji zagrożeń, zaraz po instalacji nie był wystarczający. Konieczne było zdefiniowanie dodatkowych reguł, aby dostosować go do konkretnych potrzeb i charakterystyki środowiska. Po instalacji narzędzie Wazuh wymagało dostosowania poprzez zdefiniowanie dodatkowych reguł. To pokazuje, że konfiguracja jest kluczowym elementem, aby

maksymalnie wykorzystać potencjał detekcji zagrożeń oferowany przez Wazuh.

Po zdefiniowaniu i dostosowaniu reguł, Wazuh stał się skuteczniejszym narzędziem do szybkiego wykrywania nieprawidłowości i podejrzanych aktywności związanych z usługą Active Directory. Zagadnienie okazało się jednak trudne do analizy, ponieważ ataki wynikające z błędów konfiguracyjnych nie generują ruchu sieciowego, który

Protokół NetFlow jest przydatny, ale nie jest wystarczający. Pomaga wykrywać ataki, które generują dużą ilość ruchu sieciowego o nietypowej charakterystyce. Do zbudowania pełnowartościowego SOC konieczne jest stosowanie systemu typu SIEM takiego jak Wazuh.

Integracja narzędzi NetFlow i Wazuh są przydatnymi narzędzami do śledzenia i reagowania na potencjalne zagrożenia i przyczyniły się do wzrostu poziomu bezpieczeństwa infrastruktury sieciowej opartej na usłudze Active Directory, ale nie wszystkie ataki były możliwe do wykrycia w ten sposób. To potwierdza, że skomplikowane i wielowarstwowe podejście do monitorowania jest kluczowe w dzisiejszym środowisku cybernetycznym.

# Bibliografia


[1] Developer Survey Results 2019 https://insights.stackoverflow.com/survey/2019#technology-_-developers-primary-operating-systems, 2022.

[2] AdDuplex Report for June 2022, https://reports.adduplex.com/#/r/2022-06.

[3] D. Dwornikowski, NetFlow, Politechnika Poznańska, https://www.cs.put.poznan.pl/ddwornikowski/sieci/pizsk/netflow.html.

[4] NetFlow Traffic Analyzer form Solarwinds, https://try.solarwinds.com/pdp/netflow-traffic-analyzer.

[5] How to Configure Traditional NetFlow v5 on a Cisco Router, https://www.youtube.com/watch?v=ceqkBdOscqc.

[6] How to detect Active Directory attacks with Wazuh, https://wazuh.com/blog/how-to-detect-active-directory-attacks-with-wazuh-part-1-of-2/.

[7] How to detect Active Directory attacks with Wazuh, https://wazuh.com/blog/how-to-detect-active-directory-attacks-with-wazuh-part-2/.

[8] Microsoft Digital Defense Report 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv,

[9] Microsoft Digital Defense Report 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

[10] , Kerberoasting: czyli atakowanie windowsowego Kerberosa – jako bonus narzędzia i garść innych ataków https://sekurak.pl/kerberoasting-czyli-atakowanie-windowsowego-kerberosa-jako-bonus-narzedzia-i-gar

[11] , Mimikatz: czym jest, jakie ma zastosowanie i jak się przed nim bronić? https://nordvpn.com/pl/blog/co-to-jest-mimikatz/.

[12] Opis ataku Password Spraying, Mitre Att&ck, https://attack.mitre.org/techniques/T1110/003/,

# Dodatek A

# Konfiguracja local_rules.xml [][7]

```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from
       1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP
        1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10
        .2.5,</group>
  </rule>

</group>

<group name="security_event, windows,">

  <!-- This rule detects when PsExec is launched remotely to
       perform lateral movement within the domain. The rule
      uses Sysmon events collected from the domain
      controller. -->
  <rule id="110004" level="12">
    <if_sid>61600</if_sid>
```

```
26      <field name="win.system.eventID" type="pcre2">17|18</
            field>
27      <field name="win.eventdata.PipeName" type="pcre2">\\
            PSEXESVC</field>
28      <options>no_full_log</options>
29      <description>PsExec service launched for possible
            lateral movement within the domain</description>
30    </rule>
31
32    <!-- This rule detects NTDS.dit file extraction using a
          sysmon event captured on the domain controller -->
33    <rule id="110006" level="12">
34      <if_group>sysmon_event1</if_group>
35      <field name="win.eventdata.commandLine" type="pcre2">
            NTDSUTIL</field>
36      <description>Possible NTDS.dit file extraction using
            ntdsutil.exe</description>
37    </rule>
38
39    <!-- This rule detects Pass-the-ash (PtH) attacks using
          windows security event 4624 on the compromised
          endpoint -->
40    <rule id="110007" level="12">
41      <if_sid>60103</if_sid>
42      <field name="win.system.eventID">^4624$</field>
43      <field name="win.eventdata.LogonProcessName" type="pcre2
            ">seclogo</field>
44      <field name="win.eventdata.LogonType" type="pcre2">9</
            field>
45      <field name="win.eventdata.AuthenticationPackageName"
            type="pcre2">Negotiate</field>
46      <field name="win.eventdata.LogonGuid" type="pcre2"
            >{00000000-0000-0000-0000-000000000000}</field>
47      <options>no_full_log</options>
48      <description>Possible Pass the hash attack</description>
49    </rule>
50
51    <!-- This rule detects credential dumping when the command
          sekurlsa::logonpasswords is run on mimikatz -->
52    <rule id="110008" level="12">
53      <if_sid>61612</if_sid>
54      <field name="win.eventdata.TargetImage" type="pcre2">(?i
            )\\\\system32\\\\lsass.exe</field>
55      <field name="win.eventdata.GrantedAccess" type="pcre2"
            >(?i)0x1010</field>
56      <description>Possible credential dumping using mimikatz
            </description>
57    </rule>
58
59      <!-- This rule detects DCSync attacks using windows
            security event on the domain controller -->
60    <rule id="110001" level="12">
61      <if_sid>60103</if_sid>
62      <field name="win.system.eventID">^4662$</field>
```

```
63      <field name="win.eventdata.properties" type="pcre2"
            >{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}|{19195a5b-6
            da0-11d0-afd3-00c04fd930c9}</field>
64      <options>no_full_log</options>
65      <description>Directory Service Access. Possible DCSync
            attack</description>
66    </rule>
67
68  <!-- This rule ignores Directory Service Access originating
        from machine accounts containing $ -->
69  <rule id="110009" level="0">
70      <if_sid>60103</if_sid>
71      <field name="win.system.eventID">^4662$</field>
72      <field name="win.eventdata.properties" type="pcre2"
            >{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}|{19195a5b-6
            da0-11d0-afd3-00c04fd930c9}</field>
73      <field name="win.eventdata.SubjectUserName" type="pcre2"
            >\$$</field>
74      <options>no_full_log</options>
75      <description>Ignore all Directory Service Access that is
             originated from a machine account containing $</
            description>
76    </rule>
77
78    <!-- This rule detects Keberoasting attacks using windows
        security event on the domain controller -->
79    <rule id="110002" level="12">
80      <if_sid>60103</if_sid>
81      <field name="win.system.eventID">^4769$</field>
82      <field name="win.eventdata.TicketOptions" type="pcre2">0
            x40810000</field>
83      <field name="win.eventdata.TicketEncryptionType" type="
            pcre2">0x17</field>
84      <options>no_full_log</options>
85      <description>Possible Keberoasting attack</description>
86    </rule>
87
88    <!-- This rule detects Golden Ticket attacks using windows
        security events on the domain controller -->
89    <rule id="110003" level="12">
90      <if_sid>60103</if_sid>
91      <field name="win.system.eventID">^4624$</field>
92      <field name="win.eventdata.LogonGuid" type="pcre2"
            >{00000000-0000-0000-0000-000000000000}</field>
93      <field name="win.eventdata.logonType" type="pcre2">3</
            field>
94      <options>no_full_log</options>
95      <description>Possible Golden Ticket attack</description>
96    </rule>
97
98  </group>
```