Wyższa Szkoła Technologii Informatycznych w Katowicach

REFERAT PRACY DYPLOMOWEJ

Temat pracy: Projekt i implementacja systemu wykrywania incydentów bezpieczeństwa na podstawie zdarzeń audytowych

Autor: Patryk Prauze

Promotor: dr Katarzyna Trynda

Kategorie: bezpieczeństwo systemów informatycznych

Słowa kluczowe: bezpieczeństwo IT, zdarzenia audytowe, SIEM, Qradar

1. Cel i podstawowe założenia

Celem pracy jest zaprojektowanie i implementacja systemu klasy SIEM, który na podstawie analizy zdarzeń audytowych zarejestrowanych na podłączonych systemach, będzie wykrywać incydenty bezpieczeństwa. Praca będzie bazować na dostępnym na rynku rozwiązaniu IBM Qradar Community Edition. W ramach pracy zostanie omówiona architektura oraz poszczególne komponenty. W części praktycznej zrealizowane zostanie wdrożenie systemu oraz zdefiniowanie różnych reguł, z których każda będzie miała za zadanie wykrywać różny typ podejrzanej aktywności.

2. Realizacja projektu

Celem projektu było zaprojektowanie i wdrożenie systemu klasy SIEM, który na podstawie zbieranych danych audytowych z podłączonych do niego systemów

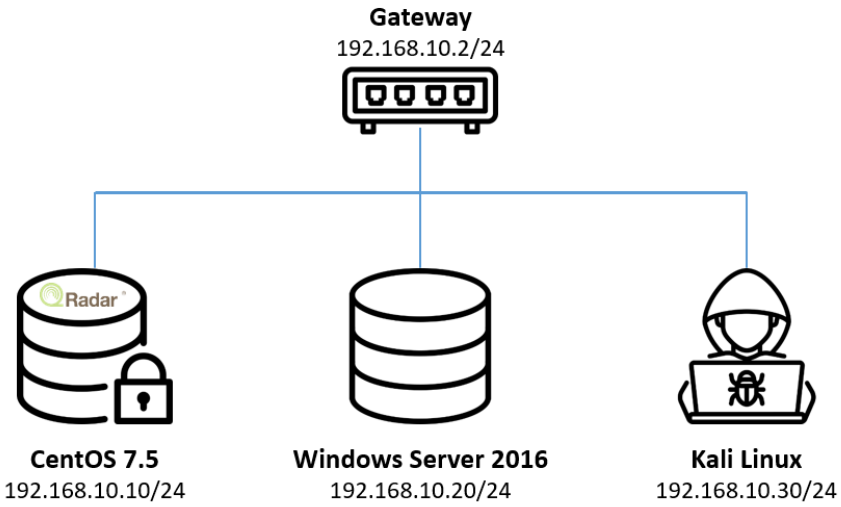
miał wykrywać podejrzane aktywności, które mogą wskazywać na incydent bezpieczeństwa. Na początku projektu został dokonany przegląd rozwiązań klasy SIEM oferowanych przez popularnych producentów. Spośród przeanalizowanych produktów został wybrany system IBM Qradar, ponieważ tylko ten system udostępnia wersję *Community Edition*, która jest darmowa i na potrzeby realizacji pracy dyplomowej w zupełności wystarczy.

W ramach projektu zostały przedstawione różne możliwości wdrożenia systemu w zależności od wielkości firmy i stopnia rozproszenia infrastruktury IT. Na potrzeby pracy zaprojektowane zostało małe środowisko testowe, dzięki któremu możliwe było opracowanie i wdrożenie reguł wykrywania podejrzanych aktywności.

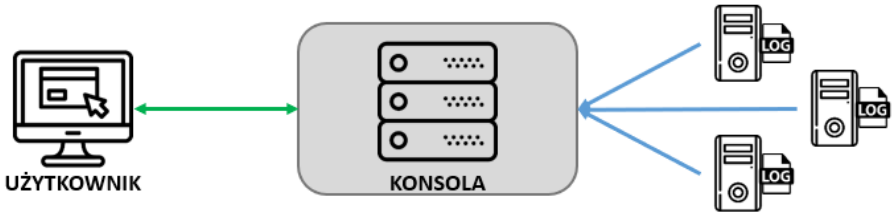
W trakcie tworzenia pracy zostały zdefiniowane różne aktywności, które administratorzy lub dział bezpieczeństwa mogą chcieć monitorować. Następnie na podstawie zdefiniowanych aktywności dokonano konfiguracji audyt monitorowanego systemu tak, aby system ten rejestrował zdarzenia na podstawie, których można będzie te aktywności wykrywać. Wszystkie zarejestrowane zdarzenia przesyłane są następnie do systemu SIEM, w którym przygotowane reguły sprawdzają warunki i dokonują korelacji. W przypadku wystąpienia na monitorowanym systemie zdarzeń, które mogą wskazywać na potencjalnych incydent bezpieczeństwa zostaje stworzony w systemie SIEM incydent, który następnie administrator lub dział bezpieczeństwa może zweryfikować.

3. Produkt końcowy

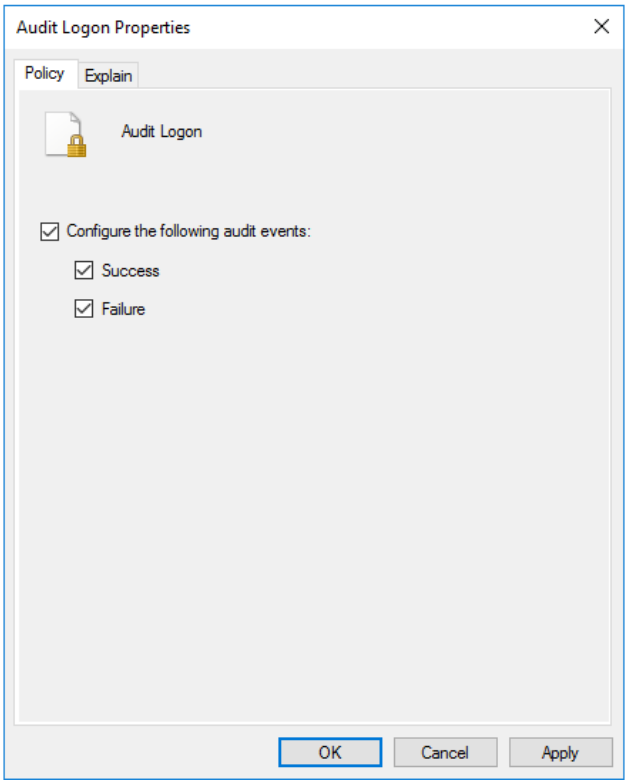
W ramach realizacji pracy system IBM Qradar Community Edition został wdrożony i skonfigurowany tak, aby wykrywać podejrzane aktywności, które mogą wskazywać na wystąpienie incydentu bezpieczeństwa. Na potrzeby pracy zostało zdefiniowane środowisko testowe w ramach, którego odbywała się realizacja pracy (Rysunek 1).

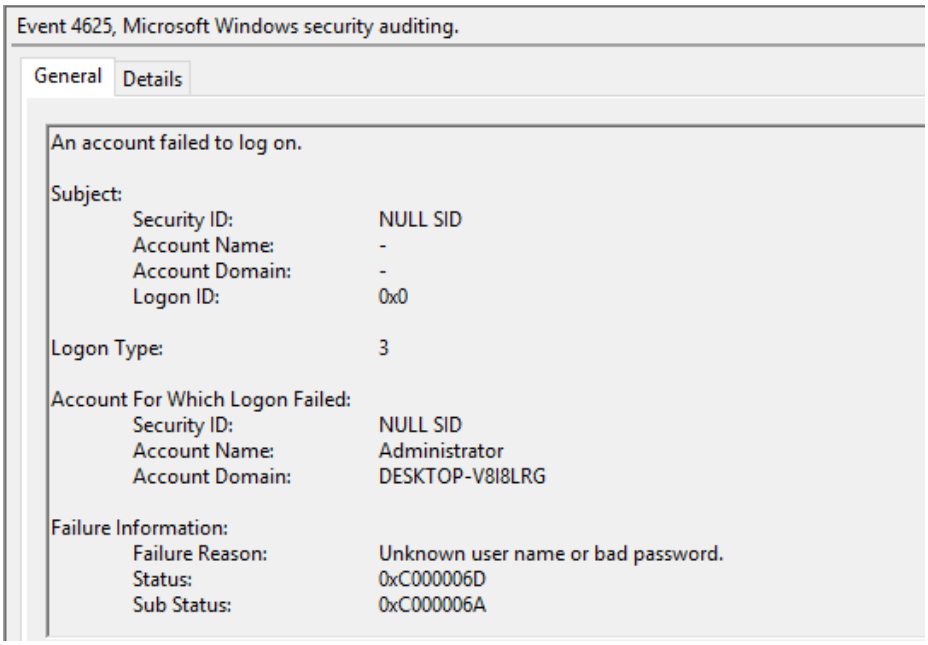


Architektura środowiska testowego nie była rozproszona, dlatego system SIEM został wdrożony w sposób „all-in-one”, co oznacza że cały system wraz ze swoimi wszystkimi komponentami został zainstalowany na jednym serwerze (Rysunek 2).



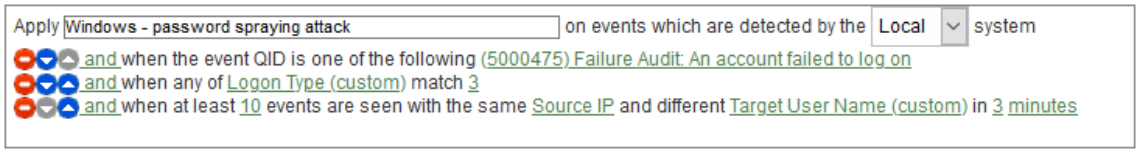
W ramach pracy został wdrożony również system Windows Server 2016, który pełnił rolę systemu dostarczającego dane do systemu SIEM. Na systemie Windows został skonfigurowany audyt systemowy (Rysunek 3, 4), dzięki któremu system rejestrował zdarzenia, które następnie było można wykorzystać przy tworzeniu reguł w systemie SIEM.



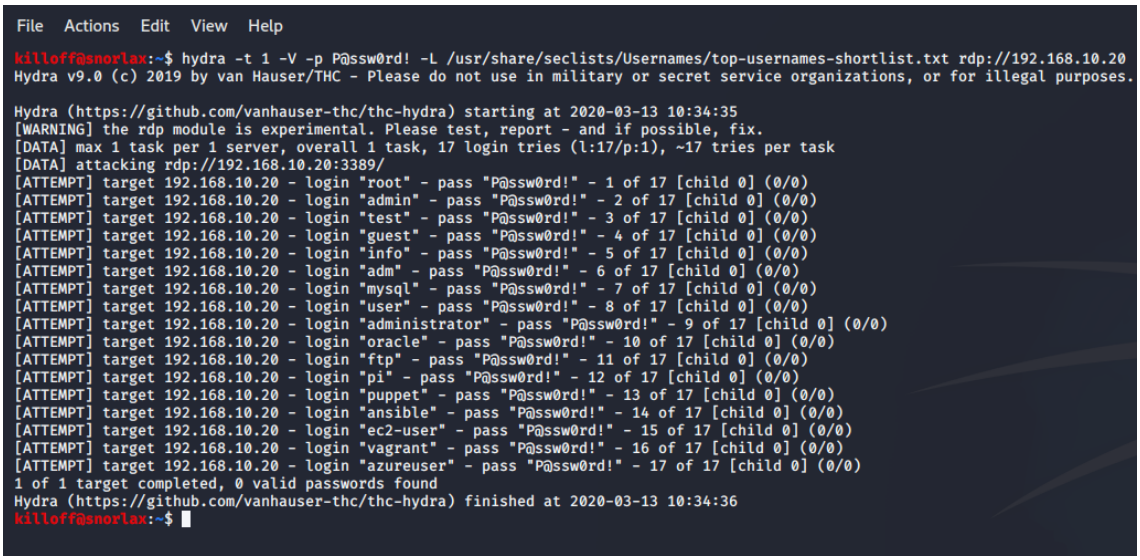


Podczas realizacji pracy zostały zdefiniowane różne aktywności, które administratorzy systemów lub dział bezpieczeństwa mogą chcieć monitorować. Następnie wdrożono na systemie SIEM reguły, dzięki czemu system jest w stanie wykrywać takie aktywności jak:

- Atak typu brute force
- Atak typu password spraying (Rysunek 5)
- Interaktywne logowanie na konto wysoko uprzywilejowane
- Uruchomienie niebezpiecznego załącznika phishingowego
- Uruchomienie niedozwolonego oprogramowania



W celu weryfikacji poprawności działania stworzonych reguł przeprowadzono testy sprawdzające czy reguły działają poprawnie i wykrywają zdefiniowane aktywności. Testy zostały przeprowadzone przy pomocy systemu Kali linux, który pełnił rolę systemu atakującego. Wszystkie przeprowadzone testy (Rysunek 6) potwierdziły poprawność działania przygotowanych reguł. System SIEM po otrzymaniu zdarzeń z systemu Windows dokonał korelacji zdarzeń, a następnie wygenerował incydent (Rysunek 7, 8).



	Event Name	Log Source	EventID (custom)	Username	Event Count	Start Time
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	root	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	guest	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	admin	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	info	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	adm	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	mysql	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	administrator	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	user	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	oracle	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	test	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	ftp	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	puppet	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	ec2-user	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	ansible	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	azureuser	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	vagrant	1	13 mar 2020, 10:35:45
	Failure Audit: An account failed to log on	WindowsAuthServer @ WIN-SRV2016-01	4625	pi	1	13 mar 2020, 10:35:45

4. Informacje o możliwości wykorzystania / wykorzystaniu pracy

Proces wdrażania systemów SIEM w firmie może w zależności od architektury być bardzo skomplikowany. Opracowana w ramach pracy architektura oraz reguły mogą służyć jako punkt referencyjny podczas wdrażania systemu.