

**Wyższa Szkoła Przedsiębiorczości i Administracji w Lublinie**

**Wydział Nauk Technicznych**

Kierunek: **Informatyka**

**Analiza zabezpieczeń w sieciach rozległych**

(Security analysis implementing in wide area networks)

Autor: **Damian Rymarz**Nr albumu: **19337**  
Promotor: **dr Rafał Stegierski**

**Lublin 2022**

**Oświadczenie kierującego pracą.**

Oświadczam, iż niniejsza praca została przygotowana pod moim kierunkiem i stwierdzam, że spełnia ona warunki do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

(data) (podpis)

**Oświadczenie autora pracy.**

Świadomy odpowiedzialności prawnej oświadczam, iż niniejsza praca dyplomowa została napisana przeze mnie samodzielnie nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. Nr 24, poz 83 z poźn. zm.) oraz dóbr osobistych chronionych prawem cywilnym dodatkowo nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej podmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Ponadto oświadczam, iż niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

(data) (podpis)

Spis treści

[**1.** **Bezpieczeństwo Systemów Informatycznych** 4](#_Toc102599155)

[**1.1.** **Definicje związane z bezpieczeństwem** 4](#_Toc102599156)

[**1.2.** **Rodzaje niebezpieczeństw** 5](#_Toc102599157)

[**1.3.** **Główne zalecenia bezpieczeństwa** 7](#_Toc102599158)

[**1.4.** **Polityki bezpieczeństwa** 8](#_Toc102599159)

[**2.** **Zabezpieczenie urządzeń sieciowych warstwy drugiej - Switch** 10](#_Toc102599160)

[**2.1.** **Podstawowe zabezpieczenie urządzenia Switch** 10](#_Toc102599161)

[**2.1.1.** **Tworzenie lokalnego użytkownika i zabezpieczenie linii** 13](#_Toc102599162)

[**2.1.2.** **Tworzenie listy dostępu oraz uwierzytelnianie za pomocą protokołu Radius** 15](#_Toc102599163)

[**2.1.3.** **Implementowanie audytowania oraz zbierania informacji na urządzeniu.** 21](#_Toc102599164)

[**2.2.** **Zabezpieczenie vlan** 21](#_Toc102599165)

# **Bezpieczeństwo Systemów Informatycznych**

W powyższym rozdzielę przedstawię podstawowe definicję związane z bezpieczeństwem systemów informatycznych oraz jego cykl życia. Postaram się również zdefiniować potencjalne zagrożenia czyhające na system, jego użytkowników oraz jak można ochronić jej infrastrukturę sieciową. Na sam koniec omówię politykę bezpieczeństwa.

## **Definicje związane z bezpieczeństwem**

Zagadnienie związane z bezpieczeństwem systemów informatycznych jest pojęciem, które możemy szeroko zdefiniować. Według Polskiej normy PN-EN ISO/IEC 27001 samo Bezpieczeństwo Informacji możemy definiować, że „informacja jest chroniona przed różnymi zagrożeniami w taki sposób aby:

* Zapewnić ciągłość prowadzenia działalności;
* Zminimalizować straty;
* Maksymalizować zwrot nakładów na inwestycję i działania o charakterze biznesowym”[[1]](#footnote-1)

Przytaczając powyższą definicję, bezpieczeństwo systemu informatycznego możemy definiować jako zespół przedsięwzięć podejmowanych do prawidłowej i ciągłej pracy stacji roboczych oraz grupie urządzeń sieciowych działających w danym systemie.

Najważniejszymi atrybutami bezpieczeństwa są:

* Dostępność – właściwość określająca, że zasób systemu informatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym teleinformatyczny;
* Integralność – należy przez to rozumieć właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
* Poufność – należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym; [[2]](#footnote-2)

Należy pamiętać, że nigdy nie będziemy mieć systemy wolnego od jakichkolwiek zagrożeń czy to zewnętrznych czy wewnętrznych. W związku z powyższym wprowadzono cykl życia systemu, który dzieli się na takie etapy jak:

* Planowanie;
* Projektowanie;
* Wdrażanie;
* Eksploatacja;
* Wycofanie.[[3]](#footnote-3)

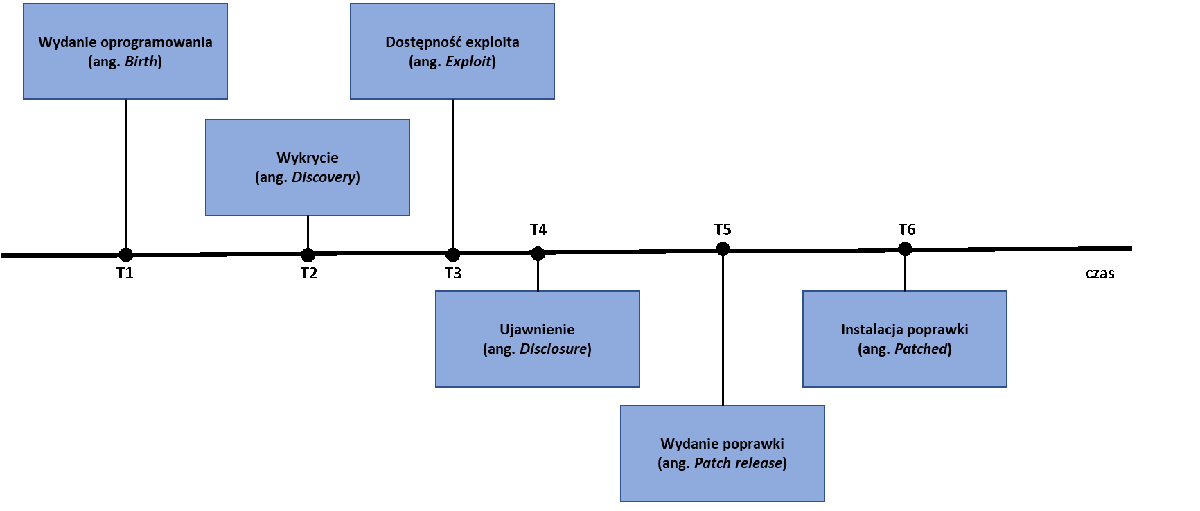
## **Rodzaje niebezpieczeństw**

Następujący postęp informatyczny powoduję ciągły pościg pomiędzy ulepszaniem nowych rozwiązań bezpieczeństwa oraz zagrożeń związanych z próbami ingerencji w bezpieczeństwo. W związku z powyższym tak jak przytaczałem w poprzednim podrozdziale, zagrożenia możemy scharakteryzować jako:

* Wewnętrzne (internal threat) – gdzie pochodzenie zagrożenie możemy zlokalizować w sieci organizacji;
* Zewnętrzne (external threat) – czyli są to zagrożenia, gdzie atakującym jest ktoś spoza sieci.

Analizując te zagrożenia możemy dojść do wniosku, że samo projektowanie odpowiedniego systemu informatycznego pod względem bezpieczeństwa jest problematyczne. Następujący ciągły wzrost nowych technologii oraz usprawnień sprzyja generowaniem podatnościom, które tworzą miejsca wrażliwe na ataki. Taka zależność czasowa od stworzenia oprogramowania do instalacji poprawki została przedstawiona na poniższym rysunku:

Rysunek 1 Cykl życia podatności



źródło: https://csirt-mon.wp.mil.pl/pl/articles6-aktualnosci/2-proces-zycia-podatnosci/, stan na dzień 31.03.2022 r.

Jak można zauważyć na rysunku, od momentu wykrycia podatności do instalacji poprawki istnieje sporo czasu, który może wykorzystać osoba niepowołana. Twórcy oprogramowania czasami są świadomi podatności swojego wyrobu, uważając, że takie albo inne miejsca są błahostkami. Może być też tak, że presja czasu, otoczenia (działania konkurencji), powodują, brak odpowiedniego czasu i środków na odpowiednią weryfikację i testowanie końcowego produktu. Dochodzimy tutaj do drugiego wniosku – ludzie mogą być omylni. W każdym miejscu najbardziej newralgicznym punktem jest człowiek.

Należy pamiętać, że człowiek, może celowo chcieć ingerować w nasze bezpieczeństwo. Agresor tj. osoba lub grupa osób, które swoim zachowaniem i ingerencja podejmuję czynności zmierzające do ataku czy to na system informatyczny czy pojedyncze stanowisko jakiegoś urządzenia. Jego działania możemy podzielić na kilka faz:

* Rekonesans – zbieranie potrzebnych informacji do przyszłego atak. Może być to poprzez oprogramowanie np. Wireshark; zbieranie informacji z legalnych źródeł – często my sami umieszczamy potrzebne informację na stronach internetowych.
* Skanowanie - wyszukiwaniu otwartych portów w systemie;
* Przeprowadzenie ataku – jest to wykorzystanie słabości znalezionych przez agresora. Istnieją różne rodzaje ataków które może przeprowadzić np. Password attack, Man-in-the-middle attack, Buffer overflow, Trust exploitation attack, Smurf attack;
* Ukrywanie – faza ta obejmuję modyfikowanie działań agresora – modyfikowanie dzienników zdarzeń. Może to także być połączone z pozostawieniem otwartych drzwi na przyszłe ataki np. pozostawieniem niechcianych programów, stworzenie użytkownika oraz modyfikowaniem jego uprawnień do działania.

W związku z powyższym należy przeanalizować słabe strony naszego systemu i reagować zawczasu. W symulowanych atakach mając dwie drużyny – broniących (Blue Team) oraz atakujących (Red Team), to zawsze ta pierwsza będzie na gorszej pozycji. Atakującym wystarczy pojedyncza luka, aby zrealizować swój plan. My, jako broniący, musimy zabezpieczyć się przed każdą ewentualnością i nawet myśleć przyszłościowo.

## **Główne zalecenia bezpieczeństwa**

W poprzednim podrozdziale, omówiłem pokrótce rodzaje niebezpieczeństw związanych z cyberbezpieczeństwem. Celem tej pracy magisterskiej jest implementacja oraz uzmysłowienie dlaczego należy stosować zalecenia, które zostaną ukazane na późniejszym etapie tej publikacji. Należy jednak uzmysłowić sobie, że największa podatnością w każdym miejscu będzie człowiek. Administrator, który przez brak doświadczenia, swoje niedopatrzenie, a nawet lenistwo, może doprowadzić do niewłaściwego zabezpieczenia swojego miejsca pracy. W związku z powyższym należy pamiętać o kilku zasadach:

* Używaj trudnych do złamania, ale łatwych do zapamiętania haseł. Możesz użyć na przykład hasła $mCmniMimn0$. Zauważ, że jest dosyć trudne do złamania, zawiera bowiem znaki specjalne oraz cyfrę i wielkie litery, a ponadto nie jest słownikowe. Ale czy łatwo je zapamiętać? Oczywiście, że dla mnie tak. Dlaczego? Ponieważ ułożyłem zdanie $ moja Córka ma na imię Marta i ma niebieskie 0czy $. Hasło tworzą pierwsze litery składających się na to zdanie wyrazów, a dodatkowo w słowie oczy użyłem cyfry 0. Już widzisz, na czym polega prosta umiejętność tworzenia dobrych haseł?
* Zawsze aktualizuj najnowsze łatki systemowe i programowe.
* Rób kopie bezpieczeństwa danych, szczególnie przed ważnymi aktualizacjami.
* Wyłącz wszystkie niepotrzebne usługi i nieużywane porty.
* Chroń fizyczny dostęp do urządzeń. Zamykaj na klucz szafy teleinformatyczne. Pamiętaj o zabezpieczeniu komputerów stacjonarnych kłódką, aby utrudnić użytkownikowi dostęp do zworek na płycie głównej.
* Jeśli możesz, szyfruj ważne informacje.
* Pamiętaj, że dobry pracownik to przeszkolony pracownik.
* Opracuj i stosuj politykę bezpieczeństwa firmy. Dokonuj regularnego sprawdzania pracowników pod względem bezpieczeństwa, organizując planowane ataki lub niespodziewane sytuacje z tym związane. Możesz zadzwonić do wybranego pracownika swojej firmy i poprosić go o podanie loginu i hasła, by sprawdzić w ten sposób, jak zareaguje.[[4]](#footnote-4)

Firma CISCO, odnośnie zabezpieczenia infrastruktury sieciowej, stworzyła taką politykę jak Network Foundation Protection. Głównym jej założeniem jest podzielenie sieci na mniejsze części, dzięki którym łatwiej będzie można zarządząć, a co najważniejsze monitorować wszelkie zdarzenia. Pierwsza z tych sekcji to „Managment Plane”. To w niej są sformułowane protokoły oraz przepływ danych niezbędnych dla administratora do konfiguracji urządzeń sieciowych. To tutaj zostanie ustalone jak będziemy zarządzać naszymi urządzeniami – jeśli dysponujemy małą ilością sprzętu możemy robić to lokalnie. Jednak gdy, będziemy mieli takich urządzeń rozlokowanych więcej, a nawet w różnych lokalizacjach należałoby pomyśleć o zdalnych metodach zarządzania poprzez różne protokoły.

Następnym poziomem jest Control Plane. To tutaj następuje wymiana pakietów przez poszczególne urządzenia tj. informacje ARP czy różne uaktualnienia w protokołach routingu.

Ostatnim natomiast z tej grupy jest Data Plane. To tutaj jest ustalany sposób przesyłania pakietów danych od jednego urządzenia do drugiego.

## **Polityki bezpieczeństwa**

Polityki bezpieczeństwa definiują w danej organizacji obszar bezpieczeństwa – jakie zasoby maja być chronione, jak powinny być przechowywane oraz to kto ma mieć do nich dostęp. Jest to bardzo dobra praktyka, wyjaśniająca pracownikom co mogą robić oraz w jakiej skali. Każde naruszenie wyznaczonych standardów może skutkować szeregiem konsekwencji – ogólnie zależy to od tego jak zostało to wyznaczone w danej organizacji.

Tworząc polityki bezpieczeństwa dla systemów informatycznych nadrzędnym celem jest zabezpieczeniem trzech nadrzędnych atrybutów tj. dostępowość, integralność oraz poufność. Naszym głównym celem jest zminimalizowanie ilości incydentów bezpieczeństwa. Oczywiście najlepiej byłoby, aby zminimalizować je do zera, ale jest to jednak utopijne myślenie. Po pierwsze nie możemy przewidzieć co może wykonać inna osoba – poprzez swoją niewiedzę może wykonać szereg niepowołanych czynności. Po drugie jeśli nie mielibyśmy informacji o zdarzeniach niepożądanych to czy nie warto by się zastanowić czy jednak nie mamy mylnego wrażenia o swoim bezpieczeństwie, a tak naprawdę posiadamy dużo newralgicznych punktów.

Podstawowymi narzędziami jakie powinny być zaimplementowane, jeśli chcemy mówić o bezpieczeństwie to:

* Definiowanie polityk bezpieczeństwa (GPO);
* Przydzielanie odpowiednich uprawnień;
* Definiowanie audytowych polityk bezpieczeństwa;
* Podgląd zdarzeń;
* Wykorzystanie Firewalli;
* Aktualizowanie na bieżąco antywirusów.

Tworząc infrastrukturę sieci komputerowej musimy mieć na uwadze kilka czynników:

* Nadawanie minimalnych uprawnień – stosując tę zasadę mamy na uwadze, aby przydzielać tylko takie uprawnienia jakie są wymagane dla użytkowników.
* Stosowanie wielu poziomów zabezpieczeń – w celu zapewnienia redundancji jeśli jakieś zabezpieczenie uległo awarii to następne urządzenie mogło by zablokować, albo zniwelować zagrożenie.
* Nie nadawanie uprawnień dla jednego użytkownika – w celach administracyjnych nie powinno się nadawać ważnych uprawnień dla jednej osoby. Jeśli będzie ona niedostępna wtedy nie będzie możliwości szybkiego reagowania na zdarzenie.
* Audytowanie zdarzeń – zbieranie zapisów zdarzeń z urządzeń w celu weryfikacji i rodzaju działania.

# **Zabezpieczenie urządzeń sieciowych warstwy drugiej - Switch**

Dla właściwej komunikacji w sieciach komputerowych istotne jest współdziałanie zestawu protokołów. Implementacja ta służy do prostszego ich zdefiniowania oraz zrozumienia. W sieciach komputerowcy możemy wyróżnić dwa takie modele. Model TCP/IP jest definiowany jako model sieci Internet. Powstał on w latach ’70 XX wieku. Podzielony jest on na cztery warstwy: **warstwy aplikacji, warstwy transportowej, internet, oraz ostatniej warstwy dostępu do sieci**. Drugi ze zdefiniowanych modeli to model ISO/OSI. Model sieciowy zdefiniowany przez międzynarodową organizację ISO służy do wzajemnej komunikacji w różnych sieciach. Składa się on z 7 warstw: **warstwa aplikacji, warstwa prezentacji, warstwa sesji, warstwa transportowa, warstwa sieci, warstwa łącza danych, warstwa fizyczna.**

Tabela 1 Porównanie modeli sieciowych – opracowanie własne

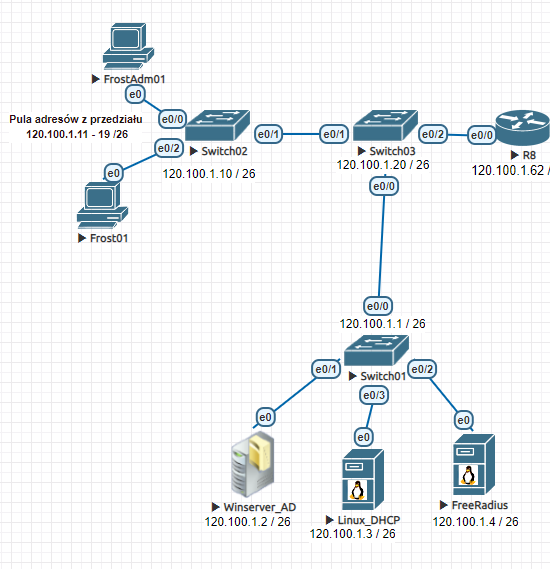
|  |  |
| --- | --- |
| Model OSI | Model TCP/IP |
| Warstwa aplikacji | Warstwa aplikacji |
| Warstwa prezentacji |
| Warstwa sesji |
| Warstwa transportowa | Warstwa transportowa |
| Warstwa sieci | Internet |
| Warstwa łącza danych | Warstwa dostępu do sieci |
| Warstwa fizyczna |

W tym rozdziale omówię zabezpieczenie warstwy drugiej urządzeń sieciowych – warstwie łącza danych. Na potrzeby tej pracy magisterskiej cała topologia sieciowa wykorzystana w tym oraz późniejszych rozdziałach będzie stworzona w Emulated Virtual Environment Next Generation (EVE – NG). Jest to maszyna systemu Linux. Oprogramowaniem do wirtualizacji jakie użyłem na potrzeby publikacji to VMware Workstation.

## **Podstawowe zabezpieczenie urządzenia Switch**

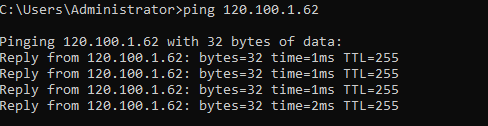
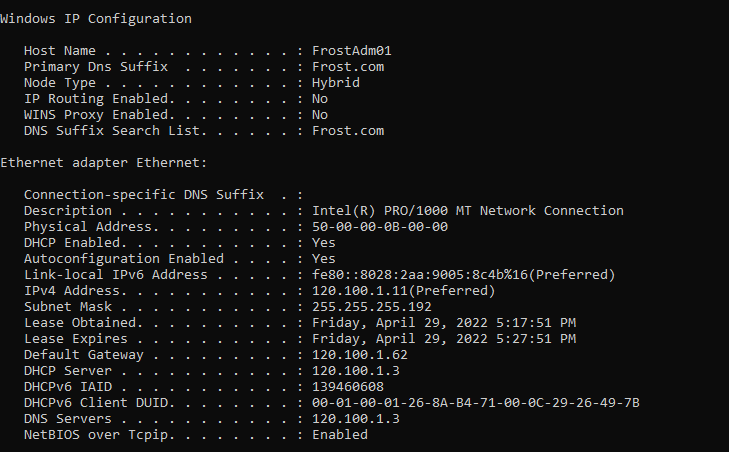
Zabezpieczenia które zostaną użyte w tym podrozdziale nie będą dotyczyły tylko Przełącznika (Switcha). Te podstawowe zalecenia powinny być wdrażane we wszystkich urządzeniach sieciowych. Dlatego też w późniejszych podrozdziałach dotyczących innych urządzeń nie będą one już ponownie opisywane.

Na potrzeby tej publikacji będę również korzystał z anglojęzycznych nazw urządzeń, funkcji itp.

Na potrzeby tej pracy magisterskiej poniżej umieściłem początkową topologię wewnętrznej sieci. Zawiera ona trzy switche, router, dwie stacje końcowe z oprogramowaniem systemowym Windows 10 Enterprise oraz Windows 7, oraz trzy serwery: Windows 2016 który pełni role kontrolera domeny oraz dwa Linux jeden jako serwer DHCP, a drugi pomocniczy do uwierzytelnienia protokołem Radius. Topologia bazuję na strukturze klient – serwer. W następnych rozdziałach będzie ona rozbudowywana o następne elementy.

Rysunek 2 Początkowa topologia sieci - wykonanie własne

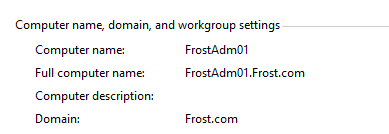
Docelowo po wstępnej adresacji sieciowej przedstawionej na załączonej topologii urządzenia końcowe są w stanie ze sobą komunikować. Poniżej przedstawiłem komunikat protokołu ICMP Echo Request ze stacji końcowej 120.100.1.3, a także konfiguracja sieciowa tej stacji.

Rysunek 3 ICMP Echo Request oraz konfiguracja sieciowa stacji 120.100.1.3

Niestety taka implementacja nie jest zabezpieczona w pełni i nasza sieć w tym przypadku jest podatna na wszelkie ataki zewnętrzne. Prawdopodobnie też tak wygląda większość sieci domowych – bo tak naprawdę zwykły użytkownik dostaje urządzenie od dostawcy internetowego i myśli, że jest bezpieczny. Dlatego też celem tej publikacji jest uzmysłowienie, że może warto też przynajmniej zainteresować się swoim bezpieczeństwem.

Każde urządzenie powinno być obligatoryjnie chronione przed dostępem osób niepowołanych, ale też od innymi czynnikami. Stacje końcowe są dołączone do fikcyjnej domeny Frost.com, która definiuje globalne polityki bezpieczeństwa.



W rozdziale tym natomiast pokaże podstawowe zabezpieczenie przełączników oraz niektóre ataki z wykorzystaniem stacji Kali Linux. Początkowe zabezpieczenie przełącznika obejmuje utworzenie lokalnego użytkownika, wyłączenie nieużywanych interfejsów oraz usług, ograniczeniu zdalnego dostępu urządzenia oraz separacja sieci.

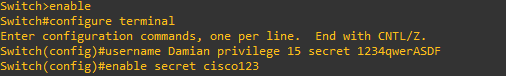
## **Tworzenie lokalnego użytkownika i zabezpieczenie linii**

Docelowo każde urządzenie posiada login i hasło. Zazwyczaj jest to Admin – hasło Admin. Dlatego też dobrą praktyką jest utworzenie swojego użytkownika. Początkowo, po włączeniu urządzenia jesteśmy w trybie podstawowym (po nazwie urządzenia wyświetla się znak „>”). Następny tryb pracy to tryb uprzywilejowany (oznaczenie „#”) – dostajemy się do niego poprzez wydanie komendy **enable**



Rysunek 4 tryb uprzywilejowany

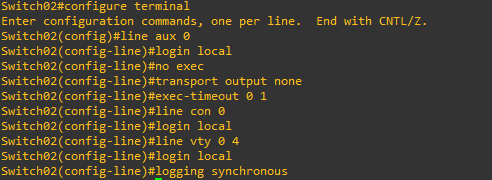
W trybie tym możemy już modyfikować ustawienia naszego urządzenia, dlatego też w trakcie tworzenia lokalnego użytkownika zabezpieczymy ten tryb.

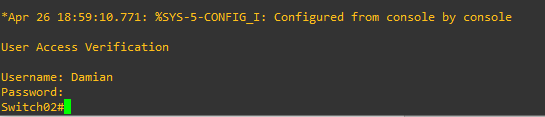


Rysunek 5 Zabezpieczenie trybu uprzywilejowanego

Po zdefiniowaniu nazwy użytkownika oraz nadaniu uprawnień zdefiniowaliśmy metodę szyfrowania hasła. Możemy też wyróżnić komendę **„password”** jednak nie jest ona zalecana. Będzie ona widoczna jako czysty tekst bez żadnego szyfrowania. Komenda **„secret”** natomiast szyfruję hasło algorytmem kryptograficznym ciągiem znaków o dowolnej długości. Dla najlepszego zabezpieczenia należy go dopełnić komendą **„service password-encryption”**. Sama powyższa komenda powoduje słabe szyfrowanie podczas wyświetlenia pliku konfiguracyjnego.

Następnym punktem jest zabezpieczenie wszystkich linii komunikacyjnych z urządzeniem. Dostęp do przełącznika możemy uzyskać poprzez port auxilary (obecnie rzadko stosowany – łącze telekomunikacyjne), port konsolowy, oraz wirtualne linie. Na potrzeby tej pracy wyłączymy możliwość korzystania z portu aux oraz zmodyfikujemy 2 pozostałe.





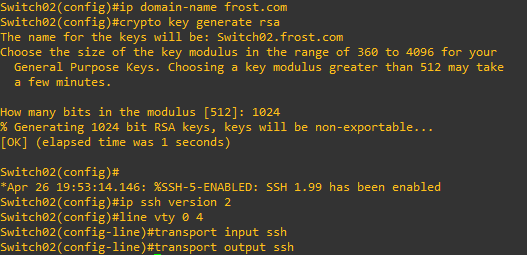
Rysunek 6 Podstawowe zabezpieczenie linii komunikacyjnych

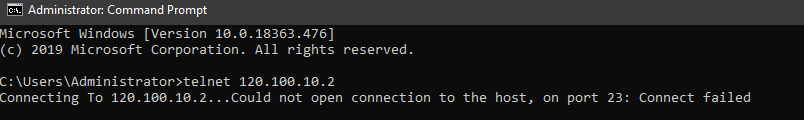
Powyższa konfiguracja jest podstawową implementacją. Dla zdalnego dostępu do urządzenia sieciowego potrzebny też jest adres sieciowy urządzenia. Obecnie na urządzeniu mamy zdefiniowany adres bramy – komenda **„ip default-gateway + adres ip”**. Dla urządzenia Switch02 jest to adres ip interfejsu E0/0 Routera01.

W podstawowej konfiguracji wszystkie interfejsy na przełączniku należą do Vlanu 1. Vlan czyli Virtual Local Area Network jest wydzieloną logicznie siecią w obszarze większej sieci fizycznej. W powyższej topologii wszystkie urządzenia przynależą do nowo stworzonego Vlanu 30. Poprzez zdefiniowanie adresu IP oraz maski dla Interfejsu Vlan 30 będzie możliwe zdalnie konfigurowanie tych urządzeń. Dla urządzenia Switch01 nadany zostanie adres ip 120.100.1.1 z 26 bitową maską, dla Switch02 – 120.100.1.10 / 26, natomiast Switch03 – 120.100.1.20 /26.





Dla powyższej zdalnej komunikacji z urządzeniami sieciowymi został użyty protokół Telnet. Nie jest on jednak wskazany – nie jest on zabezpieczony, dane podczas komunikacji przesyłane są w postaci tekstu. Brak też w nim jakiegokolwiek szyfrowania. Przeciwieństwem tego protokołu jest protokół SSH (Secure Shell). Używa on wygenerowanego przez urządzenie klucza publicznego oraz prywatnego. Sama komunikacja jest szyfrowana i niewidoczny dla użytkownika. Aby skonfigurować ten proces komunikacji ustalić nazwę urządzenia (hosta). Następnie ustalamy nazwę domenową niezbędną do uzyskania klucza publicznego. Ostatnim krokiem jest ustalenie klucza prywatnego poprzez jego wygenerowanie na urządzeniu. Po wykonaniu tych punktów zabezpieczymy linię wirtualną urządzenia poprzez ustalenia docelowego protokołu SSH do komunikacji z urządzeniem. Dzięki temu nie będzie możliwe zdalna komunikacja poprzez protokół Telnet.



## **Tworzenie listy dostępu oraz uwierzytelnianie za pomocą protokołu Radius**

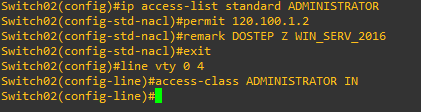
Listy Kontroli Dostępu (ang. Access Control Lists) są jednym z podstawowych zabezpieczeń sieci komputerowych. Poprzez filtrację pakietów wchodzących i wychodzących mogą definiować podstawowe reguły. Prawidłowe skonstruowanie ACL zapewni wyrzucenie niepożądanych pakietów, ustanowi poziom zabezpieczeń w wyniku zdefiniowania określonych reguł oraz zniweluje dostęp do urządzeń dla niepowołanych osób.

Możemy wyróżnić dwa typy ACL:

1. **Standardowa** – weryfikują one pakiety IP w oparciu o adres źródłowy;
2. **Rozszerzona** – ta sama funkcjonalność w oparciu o adres źródłowy, dodatkowo także o adres docelowy oraz szersza filtracja pakietów poprzez weryfikacje typów oraz numerów portu.

Na chwilę obecną w naszej topologii znajdują się dwie stacje końcowe z oprogramowaniem systemu Windows 10 oraz serwer Windows 2016. Stworzymy listę kontroli dostępu na urządzeniach sieciowych, tak aby tylko z serwera Windows 2016 o adresie IP 120.100.1.2 można będzie się do nich dostawać. W konfiguracji globalnej poprzez wydanie komendy **ip access-list standard** plus nasza nazwa wejdziemy do szczegółowej konfiguracji ACL. Następnie wskazujemy adres IP urządzenia z którego chcemy mieć dostęp. Dodatkowo także dla naszej informacji nazywamy ta zdefiniowaną ACL.

Następnie tą zdefiniowaną ACL umieszczamy czy to na interfejsach do urządzenia czy też na liniach komunikacyjnych. Na poniższym rysunku zdefiniowaliśmy dostęp do urządzenia Switch02. Widoczny jest jeden warunek – pozwól wejść ze stacji o numerze IP 120.100.100.2. Jednakże zawsze trzeba pamiętać o drugim warunku jakim jest zabronienie dostępu z innych stacji. Jest to bardzo ważne przy późniejszym filtrowaniu ruchu przez Firewall.

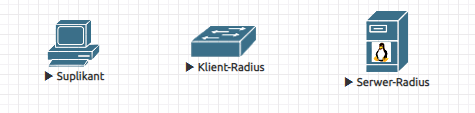


Rysunek 7 Standardowa ACL

Oczywiście takie rozwiązanie nie będzie dawało nam bezpieczeństwa. Poprzez zmianę adresu IP stacji roboczej można będzie się bez problemu dostawać do pożądanego urządzenia.

Innym rozwiązaniem, które warto wdrożyć do zabezpieczenia naszego dostępu są protokoły RADIUS oraz TACACS. Protokoły te powstały w latach ’90 XX wieku. Służą one do weryfikacji użytkowników oraz urządzeń sieciowych. Poprzez komunikacje Klient – Serwer weryfikowane są poświadczenia oraz uprawnienia dostępowe. Weryfikacji mogą podlegać dane użytkownika, certyfikat urządzeń czy też adresy fizyczne.

Działanie tych protokołów polega na tym, że użytkownik przesyła swoje poświadczenia do klienta-Radius, a ten przesyła ja celem weryfikacji do serwera-Radius. Komunikacja Klient-Serwer następuję po porównaniu wspólnego hasła. Następnie Serwer wysyła do Klienta, że dany użytkownik (Suplikant) jest uprawniony do logowania się do stacji.



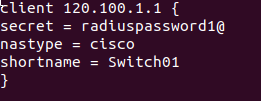
Rysunek 8 Uwierzytelnienie za pomocą protokołu Radius

W prezentowanej pracy pokaże dwa sposoby uwierzytelniana się za pomocą protokołu Radius wykorzystując obecną topologię sieci. W pierwszym ze sposobów serwerem Radius będzie Server Linux Ubuntu. Poprzez wprowadzenie komendy **sudo apt install freeradius** rozpoczniemy instalację odpowiedniego pakietu.Następnie modyfikujemy plik znajdujący **users.conf** znajdujący się w ścieżce **/etc/freeradius/3.0/.**

Na samym początku utworzyliśmy dostęp do urządzeń sieciowych dla użytkownika **Damian** z hasłem **123qwerASDF.** Na serwerze tym stworzymy innego użytkownika z loginem **Patryk** z hasłem **Dostep89@**.

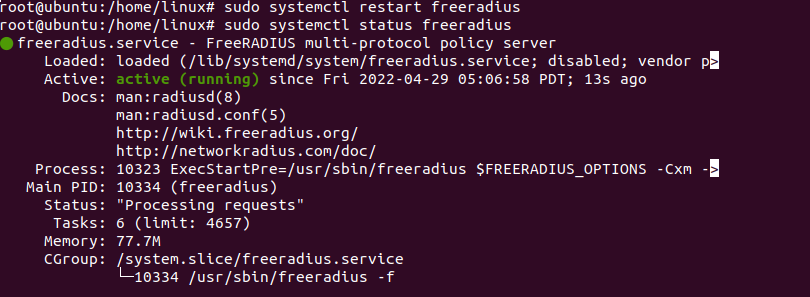
Kolejnym krokiem jest zdefiniowanie jakie urządzenia muszą brać udział w wymianie jako Klienci. Ustalamy to poprzez modyfikowanie pliku **clients.conf**, który również jest w ścieżce powyżej. W pliku tym musimy zdefiniować adres sieciowy urządzenia, wspólne hasło oraz nazwa urządzenia.

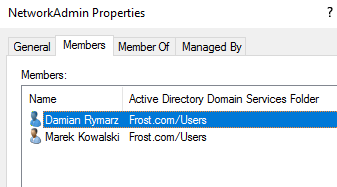


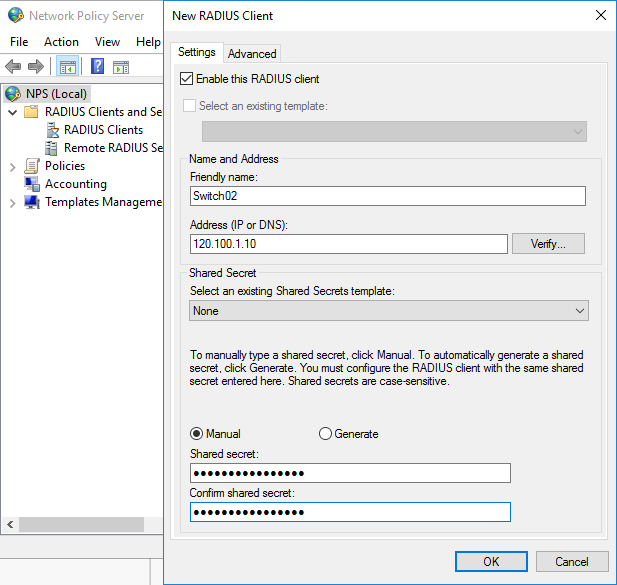


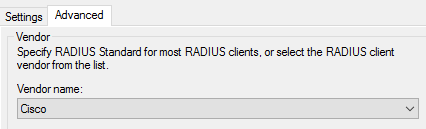
Rysunek 9 Przykładowy wpis na serwerze uwierzytelniającym

Po zapisaniu zmian w tych plikach restartujemy usługę FreeRadius. Celem weryfikacji możemy sprawdzić działanie czy działa poprawnie.



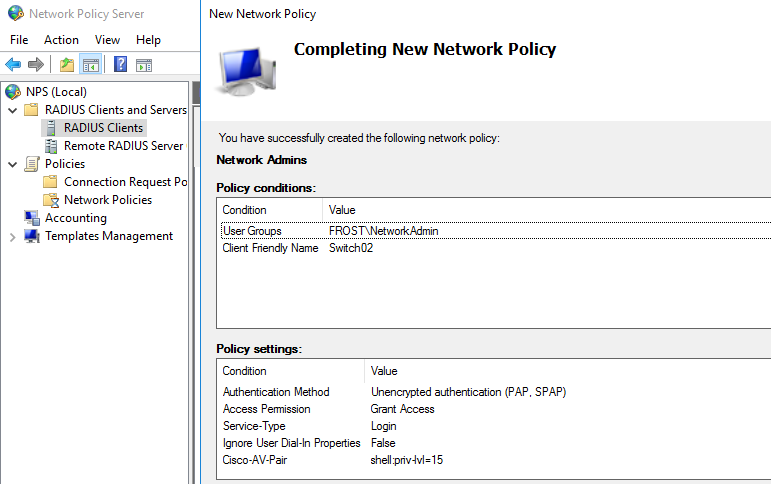
Drugi sposób konfiguracji uwierzytelnienia za pomocą protokołu Radius przedstawię za pomocą Serwera Windows 2016, poprzez zainstalowanie dodatkowej roli. W tym celu musimy wybrać opcję ***Network Policy Server* (Serwer Zasad Sieciowych). Tworzymy także grupę w Active Directory (NetworkAdmin) z użytkownikami, którzy będą mieli uprawnienia do zarządzaniem urządzeń.**

 Wybierając role NPS rozwijamy folder Radius Client – new Radius Client. W pierwszej zakładce ustalamy nazwę własną urządzenia, jego adres IP oraz wspólne hasło (ustalone wcześniej radiuspassword1@). W tym wypadku jednak będziemy konfigurować Switch02. W zakładce zaawansowane musimy wybrać Cisco.



Kolejnym krokiem jest zdefiniowanie polityk dostępowych. Wybieramy Network Policies. Poniższy rysunek obrazuję ustawienia, które należy wprowadzić:

1. Zdefiniowanie grupy z AD oraz nazwy maszyny;
2. Do czego mają mieć uprawnienia oraz jak wysokie uprawnienia;



Powyżej ukazałem dwie możliwości konfiguracji serwerów Radius. Ostatnią konfigurację musimy już wprowadzić na docelowych urządzeniach.

Urządzenia sieciowe posiadają lokalnych użytkowników i hasła. Jest to wskazane w razie jakichkolwiek problemów z serwerem. – oczywiście możemy zabezpieczyć linię konsolową, jakbyśmy chcieli fizycznie konfigurować urządzenie. Ale nie jest to wskazane, ponieważ obniży to nasze bezpieczeństwo. Po rozpoczęciu konfiguracji poświadczeniami lokalnymi nie dostaniemy się w trakcie prawidłowo skonfigurowanego protokołu Radius.

W konfiguracji globalnej rozpoczynamy poprzez wprowadzenie polecenia

*aaa new-model.*

Następnie nazywamy utworzoną grupę, wskazujemy adres IP serwera wraz z portami oraz definiujemy wspólne hasło.

*aaa group server radius*

*radius-server host (adres ip serwera) auth-port 1812 acct-port 1813 key radiuspassword1@*

Włączamy na urządzeniu możliwość uwierzytelnienia, autoryzacji oraz raportowaniu poprzez wydanie komend:

*aaa authentication login default group radius local*

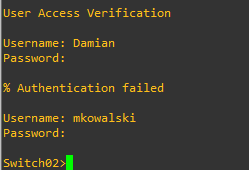
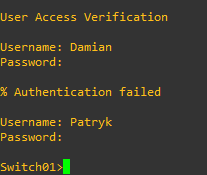
*aaa authorization exec default group radius local*

*aaa accounting exec default start-stop group radius*

*aaa accounting system default start-stop group radius*

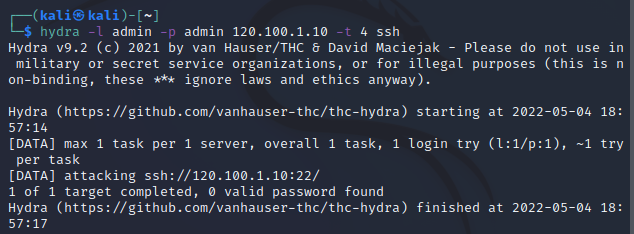
Ostatni wyraz „*local*” zabezpiecza możliwość uwierzytelniania się lokalnymi poświadczeniami w wypadku problemów z protokołem Radius.

Poniżej zamieściłem odrzuconą możliwość logowania poświadczeniami lokalnymi na obu przełącznikach oraz zaakceptowane poświadczenia Switch01 z serwera Linux, a Switch02 z serwera Windows 2016.



Rysunek 10 Prawidłowa implementacja protokołu Radius

Oczywiście można zadać pytanie, czy samo zabezpieczenie lokalnym hasłem i użytkownikiem nie wystarczy. W celu weryfikacji tych zabezpieczeń poniżej przeprowadzę tak zwany brute-force attack mający na celu zgadnięcie nazwy użytkownika i hasła. Wiele urządzeń posiada fabryczne loginy i hasła typu admin-admin, root-root, admin-password. W celu przygotowania ataku na urządzeniu Switch02 utworzyłem użytkownika **admin** z hasłem **admin**. Takie ataki polegają na przygotowanych wcześniej słownikach haseł – jedynie dla pokazania działania serwera Radius i ustawień na przełączniku uprościłem to.



Rysunek 11 Próba brute-force attack password

Na urządzeniu Switch02 utworzony został użytkownik o takich parametrach. Jednak atak okazał się niepowodzeniem. Stało się tak ponieważ w pierwszej kolejności przełącznik komunikuje się z serwerem Radius i to od niego pobiera dane do uwierzytelnienia. Dopiero później urządzenie posiłkuje się danymi ze swojego urządzenia. Odnośnie loginów i haseł zalecałbym jednak usunięcie domyślnych danych, przemianowanie ich na trudniejsze do odgadnięcia, stosowanie małych i dużych znaków razem ze znakami specjalnymi oraz numerycznymi.

## **Implementowanie audytowania oraz zbierania informacji na urządzeniu.**

Celem zweryfikowania rozliczalności na urządzeniu powinno się wprowadzić zapis zdarzeń podejmowanych na urządzeniu, które samo nie oferuję automatycznego zapisywanie wszystkich zdarzeń. Wszystkie poprawne logowania oraz te niepoprawne powinny być rejestrowane. Możemy to wprowadzić poprzez wprowadzenie komendy w ustawieniach globalnych:

*login on-success log*

*login on-failure log*

Kolejnym zabezpieczeniem wartym wprowadzenia jest blokownanie możliwości zalogowania się do urządzenia po wprowadzeniu x – prób logowania. Na przełącznikach ustawimy możliwość 2-krotnego błędnego logowania użytkownika, który błędnie poda dane w przeciągu 3 minut oraz oczekiwany czas ponownych prób po upływie 5 minut:

*login block-for 300 attempts 2 within 180*

Wszelkie próby logowania zapisywane są na urządzeniu. Komenda *show login failures* ukaże nam wszystkie próby wraz z datami oraz danymi użytkownika.

## **Zabezpieczenie vlan**

W poprzednich podrozdziałach dla powyższej topologii wszystkie urządzenia pracują w wirtualnej podsieci o numerze 30 (Vlan 30). Domyślnie wszystkie interfejsy pracują w Vlanie 1, jednak bez implementacji innych zabezpieczeń nasza sieć była by podatna na ataki. W związku z powyższym należy odseparować sieciowo nieużywane interfejsy od tych działających.

Dalszym krokiem należy także, oddzielić zarządzanie urządzeniami od innych urządzeń końcowych. W tym celu na każdym z przełączników utworzony zastanie Vlan 99 do zarządzania urządzeniami. W konfiguracji globalnej konfigurujemy Vlan 99, a także interfejs Vlan99 – nadając im adresy kolejno 120.100.99.1 (Switch01), 120.100.99.10 (Switch02) oraz 120.100.99.20 (Switch03). Adresem bramy będzie adres ip 120.100.99.62 – jest to adres subinterfejsu e0/0.99 Routera01.

Należy także pamiętać, że urządzenia końcowe są w Vlanie 30, więc aby móc konfigurować zdalnie urządzenia poprzez protokół SSH, trzeba mieć stację również w tej podsieci (Vlan 99).

Przełączniki mogą obsługiwać ruch do wielu sieci. Urządzenie weryfikuję dokąd dana ramka ma być przesłana poprzez wpis VLAN TAG, który jest zawarty w ramce ethernetowej. Umożliwia to znajdowanie urządzeń gdzie mają być przekazane dane. Podczas komunikacji trunk przesyłane są wiele vlanów w postaci jednego łacza. Vlan natywny zawarty w tym łączu jest nietagowany. Właściwa komunikacja pomiędzy urządzeniami następuje poprzez ustalenie numeru tego Vlanu natywnego po obydwu stronach urządzenia. Domyślnie na urządzeniach jest to Vlan 1. Dla bezpieczeństwa należy go zmienić. W powyższej topologii nadamy mu numer 999. Na interfejsie w kierunku innego przełącznika czy routera należy wprowadzić komendę:

*switchport trunk native vlan 999*

1. Wg. Urząd Dozoru Technicznego; https://www.udt.gov.pl/certyfikacja-systemow-zarzadzania/pn-iso-iec-27001-2007-system-zarzadzania-bezpieczenstwem-informacji; stan na dzień 29.03.2022 r. [↑](#footnote-ref-1)
2. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. (Dz.U. z 2011 r. nr. 159 poz. 948 §2) „w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego”; [↑](#footnote-ref-2)
3. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. (Dz.U. z 2011 r. nr. 159 poz. 948 §18 pkt. 1) „w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego”; [↑](#footnote-ref-3)
4. Security CCNA 210-260 Zostań Administratorem Sieci Komputerowych CISCO, Adam JÓZEFIOK, Helion 2016, str. 24. [↑](#footnote-ref-4)