Bezpieczeństwo Sieci Komputerowych - laboratorium

Ćwiczenie 5: **Bezpieczeństwo infrastruktury sieciowej**

Podstawy teoretyczne

1. Bezpieczeństwo na przełącznikach (blokowanie portów)

Przełączniki narażone są na ataki typu ARP Flooding (przepełnianie tablic ARP) oraz ARP Poissoning (Zatruwanie tablic ARP – umieszczanie fałszywych wpisów). Prostym mechanizmem ograniczającym możliwość takich ataków jest określenie dla każdego portu przełącznika:

- listy źródłowych adresów (MAC) które są do tego portu dołączone (oraz blokowanie na tym porcie adresów nieuprawnionych)
- liczby różnych adresów źródłowych (MAC), które mogą korzystać z portu.

Dzięki takim prostym rozwiązaniom atak ARP Flooding staje się niemożliwy (np. przełącznik nie przyjmuje więcej niż 3 adresów MAC z jednego portu) a ARP Poissoning znacznie utrudniony (fałszywe adresy nie znajdują się na liście, więc ramki są odrzucane przez przełącznik).

Oczywiście powyższych mechanizmów nie możemy zastosować na portach (łączach) pomiędzy przełącznikami (tzw. trunk), gdyż z definicji pojawiają się tam ramki z różnymi źródłowymi adresami MAC.

Dobrą praktyką jest również wyłączanie nieużywanych portów przełączników.

Konfiguracja na przełącznikach Cisco:

Przejście do trybu konfiguracji interfejsu:

```
S1(config)#interface fastethernet 0/5
```

Konfiguracja portu jako dostępowego (na portach trunk lub działających w trybie automatycznego wyboru nie możemy konfigurować mechanizmów bezpieczeństwa):

```
S1(config-if)#switchport mode access
```

Aktywacja mechanizmów bezpieczeństwa na porcie - uaktywnia konfigurację domyślną, czyli (patrz dalej) maximum=1, violation=shutdown:

```
S1(config-if)#switchport port-security
```

Wyświetlenie dostępnych opcji:

```
S1(config-if)#switchport port-security ?
```

Określenie maksymalnego rozmiaru listy uprawnionych adresy MAC dla portu (w przykładzie 3 różne adresy):

```
S1(config-if)#switchport port-security maximum 3
```

Dopisanie adresu do listy:

```
S1(config-if)#switchport port-security mac-address 0050.56C0.0008
```

Jeżeli lista nie zostanie wypełniona 'ręcznie', to będzie wypełniana w trybie dynamicznym, czyli pierwsze N adresów jakie pojawią się na porcie zostanie zapisanych. Lista ulegnie wyczyszczeniu po restarcie przełącznika.

Konfiguracja 'lepka', czyli pierwsze N adresów jakie pojawią się na porcie zostanie zapisanych i zapamiętanych. Lista nie ulegnie wyczyszczeniu po restarcie przełącznika:

```
S1(config-if)#switchport port-security mac-address sticky
```

Określenie sposobu reakcji na przekroczenie limitu, czyli co zrobić gdy lista jest pełna a ramki z nowymi adresami MAC pojawiają się na porcie (protect – port odrzuca ramki od nadmiarowych adresów, restrict – port odrzuca ramki od nieuprawnionych adresów i odnotowuje w logach i licznikach fakt pojawienia się takich ramek, shutdown – port jest wyłączany i pojawiają się wpisy w logach):

```
S1(config-if)#switchport port-security violation [ protect | restrict |
shutdown ]
```

Wyświetlenie tablic z dozwolonymi adresami MAC:

```
S1#show port-security address
```

Wyświetlenie konfiguracji bezpieczeństwa portu fa0/1:

```
S1#show port-security interface fa0/1
```

Wyłączenie portu:

```
S1(config-if)#shutdown
```

2. Bezpieczeństwo urządzeń sieciowych

Routery dostępowe, jako urządzenia dostępne z sieci publicznych są szczególnie narażone na próby ataków i uzyskania nielegalnego dostępu. Jeżeli atakującemu uda się uzyskać dostęp do routera, może ingerować w konfiguracje krytycznych usług sieciowych, jak NAT, DHCP, przekierowywanie portów, listy kontroli dostępu, routing. Zabezpieczenie urządzeń sieciowych polega głównie na:

- zablokowaniu niebezpiecznych kanałów dostępu

- stosowanie bezpiecznych haseł
- monitorowaniu i wykrywaniu prób ataku

W domyślnej konfiguracji na routerze uruchomionych jest kilkanaście usług sieciowych. Nieużywane usługi należy wyłączyć. Można to zrobić indywidualnie dla każdej z usług lub za pomocą komendy *auto secure*, wyłączającej wszystkie zbędne usługi:

```
R1#auto secure
```

Listę otwartych portów można wyświetlić za pomocą komendy:

```
R1#show control-plane host open-ports
```

Bezpieczeństwo haseł

Utworzenie konta użytkownika i hasła:

```
R1(config)# username Kazio password kazio123
```

W konfiguracji domyślnej hasła są przechowywane w startup-config i running-config w postaci jawnej. Dostępne są dwa mechanizmy zabezpieczania haseł, pierwszy z nich to prosty i niezbyt bezpieczny algorytm szyfrujący (określany jako Type 7), uruchamiany komendą:

```
R1(config)# service password-encryption
```

Po uruchomieniu wszystkie hasła utworzone komendą password (np. enable password) będą przechowywane w postaci zaszyfrowanej.

Drugi z mechanizmów to przechowywanie skrótów haseł (MD5). Zamiast *password* należy używać komendy *secret* (np. *enable secret*).

Minimalną długość haseł można zdefiniować komendą:

```
R1(config)#security passwords min-length
```

Konfiguracja dostępu do urządzenia

Możliwy jest dostęp lokalny (port konsoli routera czy przełącznika) lub zdalny (usługa sieciowa, np. telnet, ssh, http – linia VTY, dostęp modemowy – linia AUX).

Zalecane jest wyłączenie dostępu przez nie używane linie (wydając komendy login i no password), np.:

```
R1(config)#line aux 0
R1(config-line)#no password
R1(config-line)#login
```

Konfiguracja protokołów akceptowanych przez linie VTY:

```
R1(config)#line vty 0 4
```

```
R1(config-line)#no transport input          //zablokowane wszystkie protokoły
R1(config-line)#transport input telnet      // umożliwiony dostęp przez telnet
R1(config-line)#secret sU73%er34            // bezpieczne hasło (MD5)
R1(config-line)#login    // konieczność wprowadzenia hasła przed uzyskaniem dostępu
```

Konfiguracja dostępu przez ssh:

```
Router(config)#hostname R1                  // konfiguracja nazwy (konieczna)
R1(config)#ip domain-name pwr.local         // konfiguracja domeny (konieczna)
R1(config)#crypto key generate rsa  // generacja kluczy RSA (należy podać długość)
R1(config)# username Kazio secret sU73%er34      / utworzenie konta użytkownika
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config)#ip ssh authentication-retries 3       // dopuszczalne 3 próby logowania,
                                                 // (potem blokada konta)
```

3. Bezpieczeństwo routingu

Głównymi zagrożeniami związanymi z protokołami routingu są:

a) przechwytywanie pakietów routingu w celu analizy danych umożliwiającej rozpoznanie topologii sieci, tras, routerów,

b) wprowadzanie do sieci fałszywych informacji o trasach, co umożliwia skierowanie ruchu sieciowego przez węzeł/komputer atakującego a następnie ataki man-in-the-middle oraz ataki DoS (skierowanie pakietów na nie istniejące trasy, tworzenie pętli, itp.)

Konfiguracja routingu (RIP) na urządzeniach Cisco:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0 255.255.255.0   // rip będzie rozgłaszał w
```

komunikatach trasę do tej sieci – na ogół należy wydać taką komendę dla wszystkich podłączonych sieci

Komunikaty RIP nie powinny być wysyłane ani przyjmowane do/z sieci końcowych (czyli tam, gdzie nie ma innych routerów a tylko komputery, drukarki, itp.) – zagrożenia a). Osiągnąć to można wydając komendę dla interfejsu:

```
R1(config--router)#passive-interface fastethernet 0/0
```

Zabezpieczeniem przed zagrożeniem b) jest z kolei podpisywanie pakietów routingu. Realizowane jest to za pomocą tajnego hasła oraz funkcji skrótu MD5: skrót generowany z wiadomości oraz tajnego hasła jest przesyłany z pakietem i weryfikowany przez router odbierający.

Konfiguracja na routerach Cisco:

Utworzenie klucza do podpisu:

```
R1(config)#key chain KLUCZ_RIP
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string tajne_haslo
```

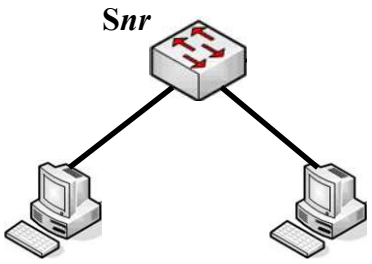
Konfiguracja podpisywania komunikatów RIP:

```
R1(config)#interface fastethernet 0/1
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain KLUCZ_RIP
```

Ćwiczenia do wykonania

- Cain (zad 5) należy zainstalować (na systemie macierzystym lub wirtualnym).
- Wykonując zadania proszę wszędzie gdzie to możliwe umieszczać **dane członków grupy** (nazwiska i numery indeksów) – w nazwach tworzonych plików, katalogów, kont użytkowników, treści plików, komunikatach, itp. Ich obecność na zrzutach ekranu w sprawozdaniu jest potwierdzeniem wykonania ćwiczeń.
- [ZE] oznacza konieczność umieszczenia odpowiedniego zrzutu ekranu w sprawozdaniu.

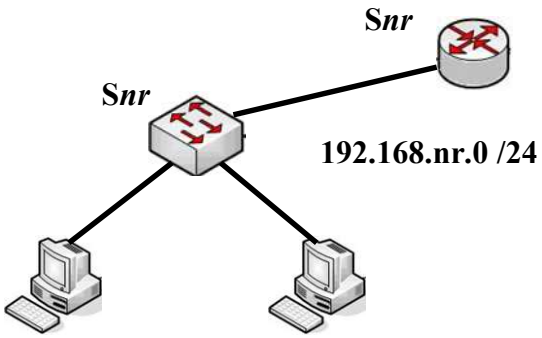
1. Bezpieczeństwo przełączników
   - Skonfigurować mechanizm bezpieczeństwa na jednym z portów przełącznika: jeden dozwolony adres MAC, konfiguracja ‘lepka’, tryb shutdown.
   - Podłączyć jeden z komputerów do tak skonfigurowanego portu
   - Zapisać (do sprawozdania) konfigurację portu
   - Odłączyć komputer i podłączyć do portu drugi komputer. Jaka jest reakcja przełącznika [ZE] ?
   - Zapisać (do sprawozdania) konfigurację portu



Rys. 1. Topologia do zadania 1 (*nr* oznacza numer grupy)

2. Dostęp do routera

- Skonfigurować router (2 konta użytkowników z hasłem niezabezpieczonym, interfejsy sieciowe, dostęp przez telnet).
- Wyświetlić hasła za pomocą show run [ZE]. Włączyć proste szyfrowanie haseł. Wyświetlić hasła za pomocą show run [ZE].
- Przechwytując transmisję (Wireshark) zalogować się poprawnym hasłem i uruchomić show run. Odczytać z pakietów login i hasło użytkownika oraz rezultat komendy [ZE].
- Skonfigurować na routerze dostęp wyłącznie przez ssh. Utworzyć nowe konto z hasłem zabezpieczonym przez MD5. Wyświetlić hasło za pomocą show run [ZE].
- Przechwytując transmisję zalogować się przez ssh i uruchomić show run. Odczytać z pakietów login i hasło użytkownika oraz rezultat komendy [ZE].



Rys. 2. Topologia z adresacją do zadania 2

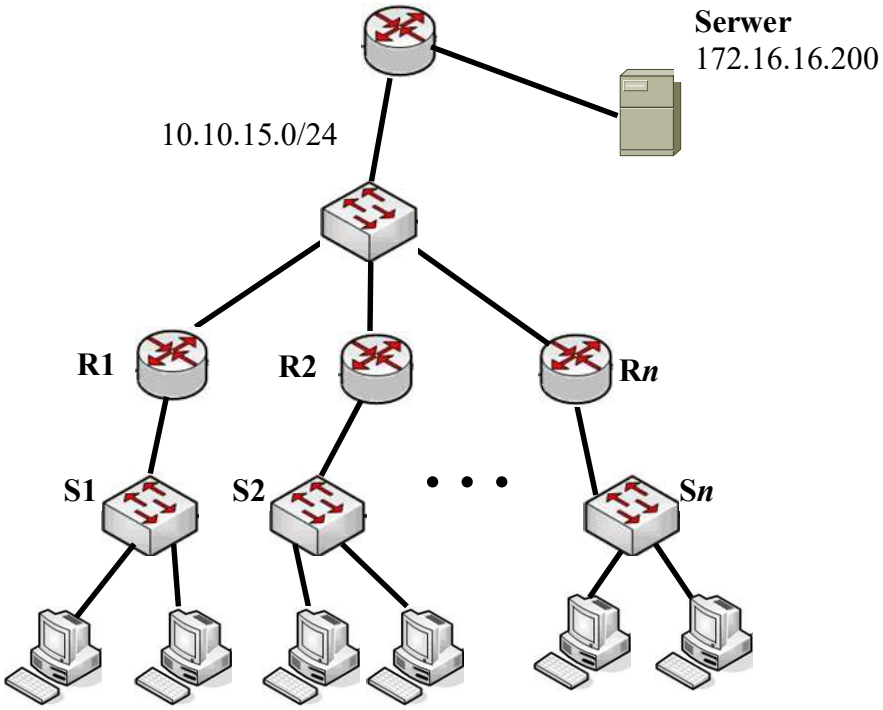
3. Bezpieczeństwo routingu

- Podłączyć sieć do wspólnej sieci laboratoryjnej (rys. 3), drugiemu interfejsowi routera nadać adres 10.10.15.*nr*.
- Uruchomić RIP na routerze, dodać obie sieci. Czy router otrzymuje informacje o trasie do sieci 172.16.16, oraz o trasach do innych podsieci 192.168 ? Czy możliwa jest komunikacja komputerów z serwerem?
- Podsłuchać pakiety routingu na stacji roboczej [ZE].
- Skonfigurować passive-interface (od strony ‘swojej’ sieci). Czy pakiety z trasami routingu nadal są wysyłane do komputerów?
- Router ‘internetowy’ do sieci 172.16. jest skonfigurowany z bezpiecznym RIP’em. Skonfigurować tak samo swój router (hasło: *bsk_lab5*). Czy router otrzymuje informacje o trasie do sieci 172.16.16, oraz o trasach do innych podsieci 192.168 [ZE]? Czy możliwa jest komunikacja komputerów z serwerem [ZE]?

4. Wyłączanie nieużywanych usług

Wyświetlić listę otwartych portów swojego routera. Wykonać komendę *auto secure* na routerze i ponownie wyświetlić listę otwartych portów [ZE]. Porównać obie listy.

5. Atak na słabe hasła
   Na routerze 'internetowym' zalogowany jest użytkownik, o którym wiadomo, że używa słabych haseł (na ogół hasła takiego samego jak login). Konta innych użytkowników na routerze zabezpieczone są słabym algorytmem kryptograficznym. Odkryć login niefrasobliwego użytkownika (usługa *finger*), włamać się na jego konto na routerze i złamać hasła do pozostałych kont (*show run* i Cain) [ZE]. Zalogować się na routerze jako jeden z pozostałych użytkowników i zgłosić ten fakt prowadzącemu. Proszę nie modyfikować konfiguracji routera (m.in. nie zmieniać haseł).



Rys. 3. Topologia z adresacją do zadania 3

Sprawozdanie

Zamieścić i skomentować zrzuty ekranu oraz fragmenty plików konfiguracyjnych. Odpowiedzieć na zadane pytania. Zamieścić i przeanalizować przechwycone pakiety.

Sprawozdanie

Zamieścić zrzuty ekranu, analizę przechwyconych pakietów, analizę otwartych portów, tablic routingu, itp. Analizy i komentarze mają bardzo duży wpływ na ocenę ćwiczenia!

Ocena

Wyznaczona na podstawie przygotowania do zajęć, zrealizowanych ćwiczeń, sprawozdania.