

Laboratorium 3.4.3: Usługi i protokoły e-mail

Topologia sieci

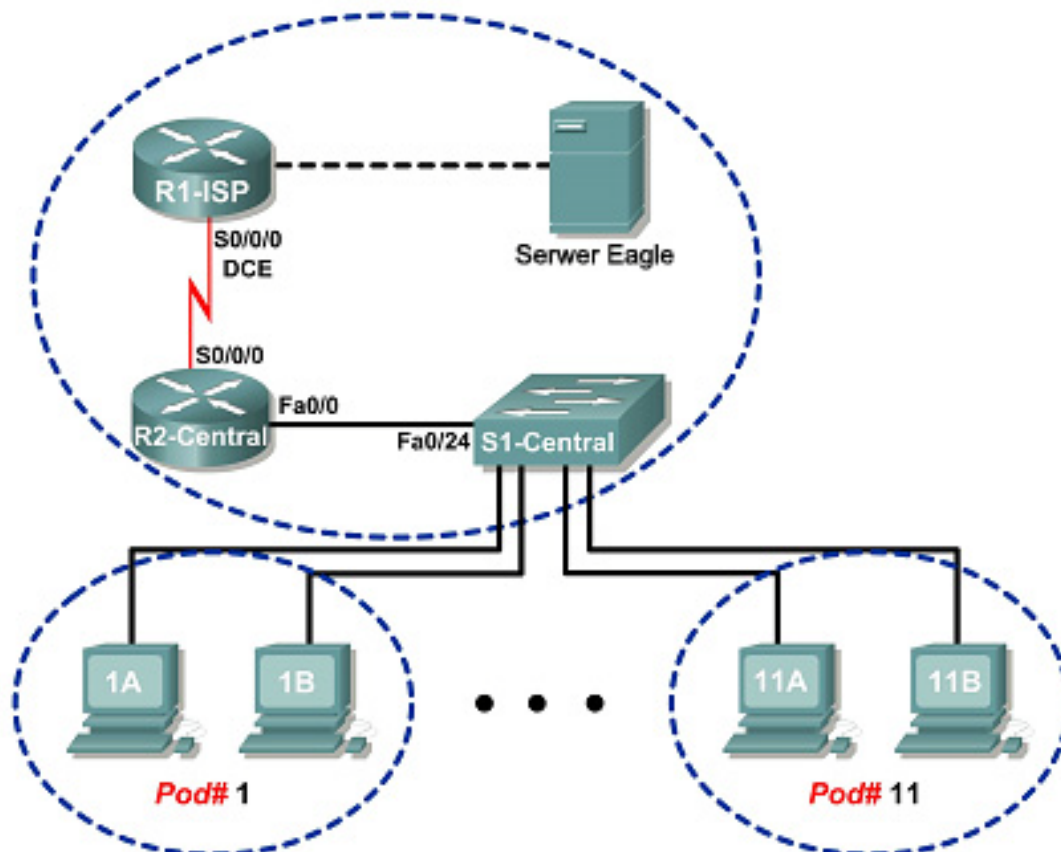


Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Domyślna brama
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	Nie dotyczy
	Fa0/0	192.168.254.253	255.255.255.0	Nie dotyczy
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	10.10.10.6
	Fa0/0	172.16.255.254	255.255.0.0	Nie dotyczy
Serwer Eagle	Nie dotyczy	192.168.254.254	255.255.255.0	192.168.254.253
	Nie dotyczy	172.31.24.254	255.255.255.0	Nie dotyczy
hostPod#A	Nie dotyczy	172.16. Pod#.1	255.255.0.0	172.16.255.254
hostPod#B	Nie dotyczy	172.16. Pod#.2	255.255.0.0	172.16.255.254
S1-Central	Nie dotyczy	172.16.254.1	255.255.0.0	172.16.255.254

Cele nauczania

Po zakończeniu tego ćwiczenia będziesz potrafił:

- skonfigurować komputer PC do obsługi poczty elektronicznej,
- przechwytywać i analizować komunikaty dotyczące poczty elektronicznej pomiędzy komputerem PC i serwerem e-mail.

Wprowadzenie

Poczta elektroniczna (e-mail) jest najbardziej popularną usługą, która używa modelu klient-serwer. Klient poczty elektronicznej jest konfigurowany na komputerze użytkownika, a celem konfiguracji jest możliwość nawiązywania połączenia z serwerem. Większość dostawców usług internetowych zapewnia instrukcje krok po kroku wspomagające uruchomienie usług poczty. W konsekwencji, typowy użytkownik może być nieświadomy złożoności używanych protokołów.

W środowiskach sieciowych, gdzie klient MUA musi połączyć się z serwerem zlokalizowanym w innej sieci, używane są następujące dwa protokoły:

- Protokół SMTP (ang. Simple Mail Transfer Protocol) został zdefiniowany w sierpniu 1982 r. w RFC 821. Od tego czasu uległ on wielu modyfikacjom i rozszerzeniom. W kwietniu 2001 r. pojawiła się ujednolicona i uaktualniona wersja - RFC 2821. Serwer SMTP nasłuchuje na dobrze znanym porcie TCP 25. SMTP jest używany do wysyłania wiadomości e-mail z zewnętrznego klienta do serwera e-mail, dostarczania wiadomości na lokalne konta i przekazywania poczty pomiędzy serwerami SMTP.
- Protokół POP3 (ang. Post Office Protocol version 3) jest używany w momencie, gdy zewnętrzny klient chce odebrać wiadomość z serwera. Serwery POPv3 nasłuchują na dobrze znanym porcie 110 TCP.
- **Internet Message Access Protocol (IMAP)**—Protokół internetowy, który pozwala centralnemu serwerowi dostarczać zdalnego dostępu do wiadomości e-mail. Serwery IMAP nasłuchują na dobrze znanym porcie 143 TCP.

Podczas tego ćwiczenia, wykorzystasz IMAP zamiast POP do dostarczenia wiadomości e-maila do klienta.

Wcześniejsze wersje obu protokołów nie powinny być używane. Istnieją również bezpieczne wersje obu protokołów, które wykorzystują mechanizmy bezpieczeństwa warstwy transportowej (SSL/TSL) podczas komunikacji.

Poczta elektroniczna jest podatna na ataki. Rozsyłanie bezużytecznego i niechcianego spamu zużywa przepustowość łącza i zasoby sieciowe. Serwery e-mail poddawane były licznym atakom, które narażały komputery na utratę danych.

Scenariusz

Podczas tego ćwiczenia skonfigurujesz i użyjesz aplikację klienta poczty elektronicznej do połączenia z serwerem Eagle. Będziesz monitorować komunikację oraz analizować przechwycone pakiety za pomocą programu Wireshark.

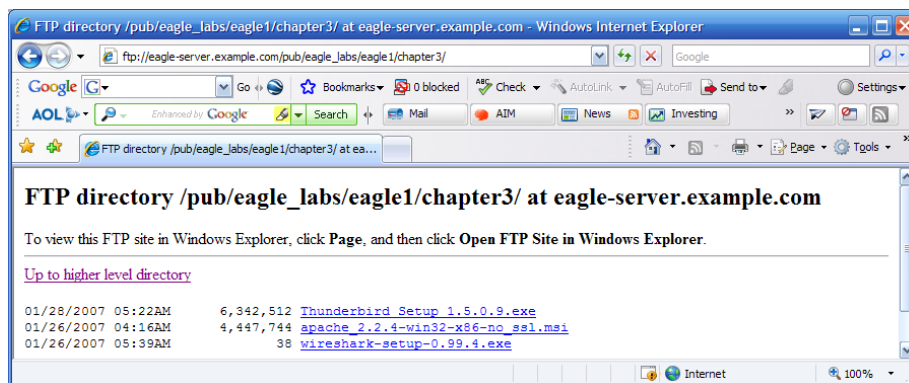
Do połączenia z usługą serwera Eagle zostanie użyty klient e-mail taki jak np. Outlook Express czy Mozilla Thunderbird. Serwer Eagle ma wstępnie skonfigurowaną usługę SMTP z kontami użytkowników, które są przystosowane do wysyłania i odbierania zewnętrznych wiadomości e-mail.

Zadanie 1: Skonfiguruj usługę e-mail na komputerze

Urządzenia powinny być skonfigurowane zgodnie ze schematem topologii i tabelą adresacji. Jeśli tak nie jest, poproś instruktora o pomoc.

Krok 1: Pobierz i zainstaluj aplikację Mozilla Thunderbird

Jeśli Thunderbird nie jest zainstalowany na Twoim komputerze, możesz go pobrać z eagle-server.example.com. Spójrz na Rysunek 1. Adres URL: ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter3/.



Rysunek 1. Miejsce, z którego można pobrać Mozilla Thunderbird

1. Kliknij dwa razy na nazwę pliku Thunderbird, następnie wybierz Zapisz, aby zapisać plik na komputerze.

Szybkość pobierania zależy od szybkości połączenia pomiędzy dwoma routerami oraz liczby studentów pobierających plik.

2. Kiedy plik zostanie pobrany, zainstaluj program z domyślnymi ustawieniami, akceptując wcześniej licencję oprogramowania.
3. Kiedy instalacja zostanie zakończona, uruchom program Thunderbird.

Krok 2: Skonfiguruj program Thunderbird, aby mógł otrzymywać i wysyłać wiadomości e-mail

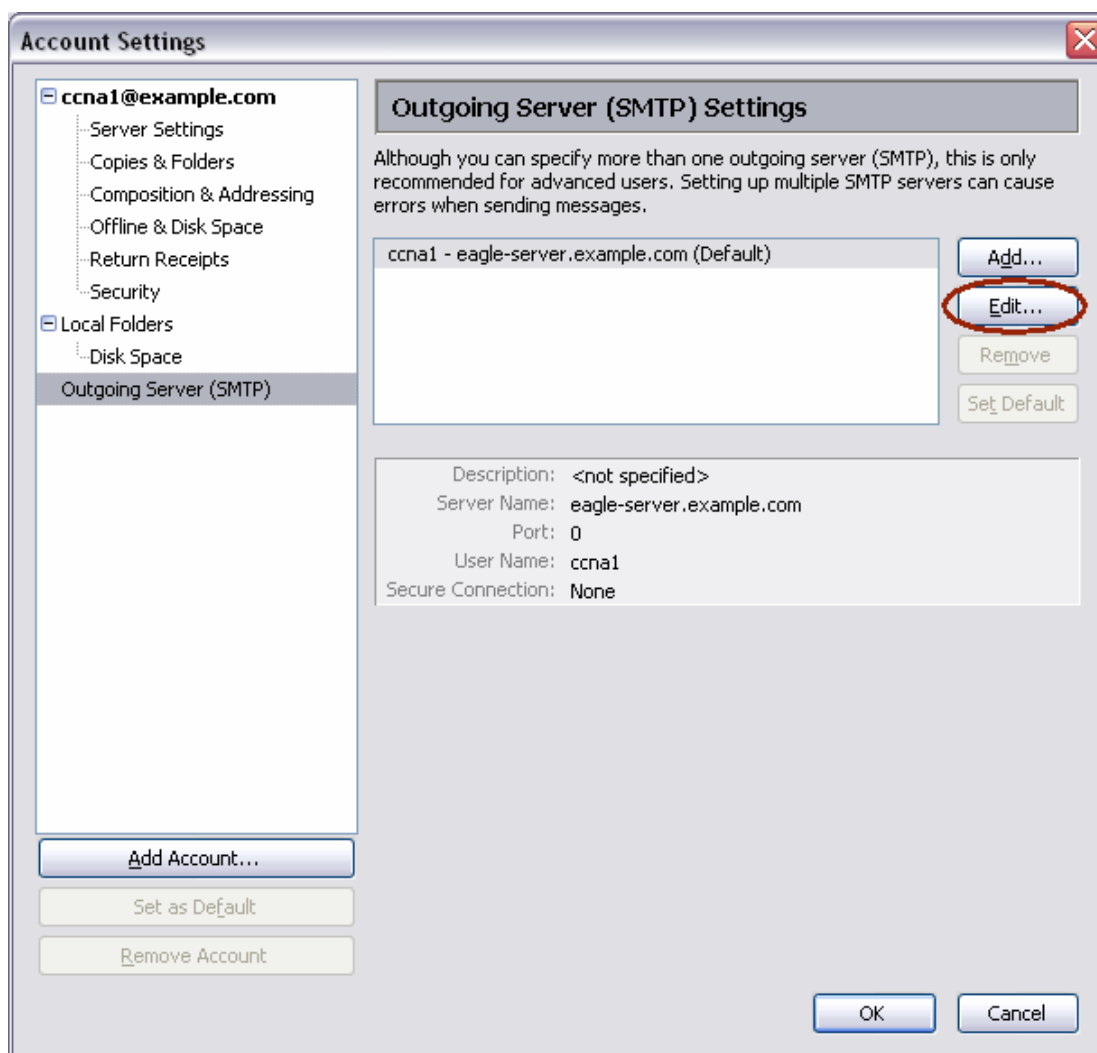
1. Jeżeli zostaniesz zapytany o opcje importu, wybierz "Don't import anything", a następnie kliknij Next.
2. Aby Thunderbird działał poprawnie, należy skonfigurować ustawienia konta poczty elektronicznej. W New Account Setup, wybierz "Email account" następnie wybierz **Next**.
3. Wypełnij informacje dotyczące konta zgodnie z poniższymi wskazówkami:

Pole	Wartość
Account Name (Nazwa konta)	Nazwa konta oparta jest na nazwie hosta. Na serwerze Eagle zostały skonfigurowane 22 konta o nazwach ccna1, ccna2, ... , ccna22. Nazwy kont powinny być wybierane w następujący sposób: HostA w Pod1 - nazwa konta: ccna1; HostB w Pod3 - nazwa konta: ccna6, itp.
Your Name (Twoja nazwa)	Użyj tej samej nazwy co powyżej.
E-mail address (Adres e-mail)	Twoja_nazwa@example.com
Type of incoming server you are using (Rodzaj używanego serwera poczty przychodzącej)	IMAP
Incoming Server (IMAP)	Eagle-server.example.com

Outgoing Server (SMTP) (Serwer poczty wychodzącej)	Eagle-server.example.com
Incoming User Name	Użyj tej samej nazwy co powyżej.
Account Name (Nazwa konta)	Twoja_nazwa@eagle-server.example.com

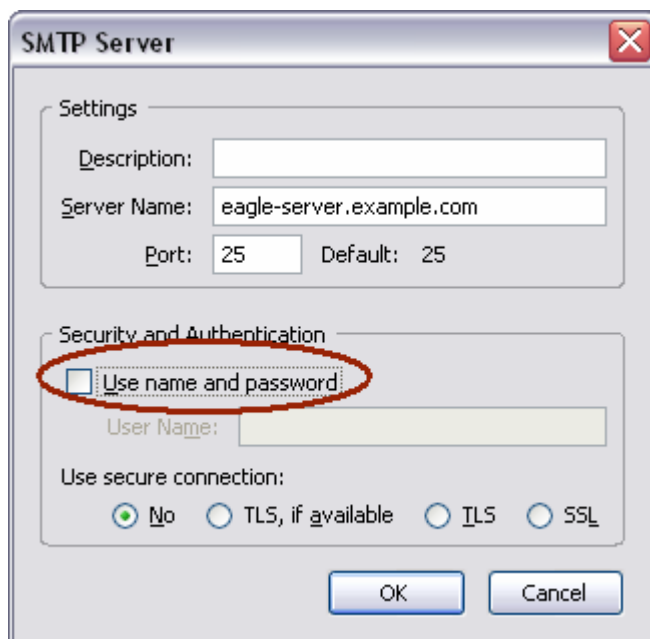
4. Kiedy uruchomi się program Thunderbird, zostaniesz zapytany o hasło do twojego konta poczty. Wybierz **"Cancel"**

Klient Thunderbird wymaga wyłączonej opcji logowania do serwera SMTP. Aby to zrobić, wybierz **Tools > Account Settings>Outgoing Server (SMTP)**. Następnie z ekranu Outgoing server, wybierz **Edit**. Spójrz na Rysunek 2.



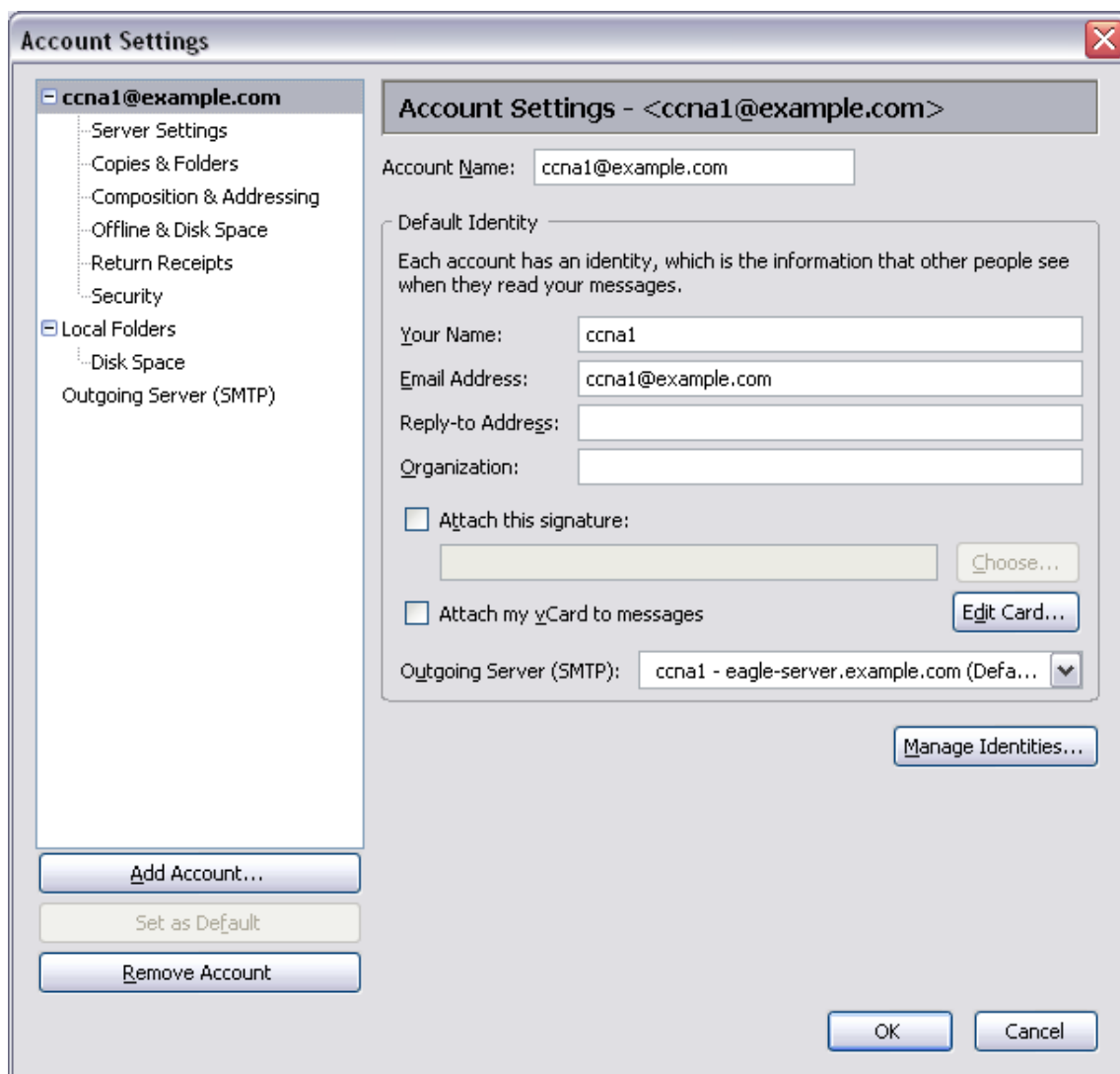
Rysunek 2. Thunderbird SMTP server settings

W okienku SMTP Server odznacz pole **"Use name and password"** i wybierz **OK** . Spójrz na Rysunek 3.



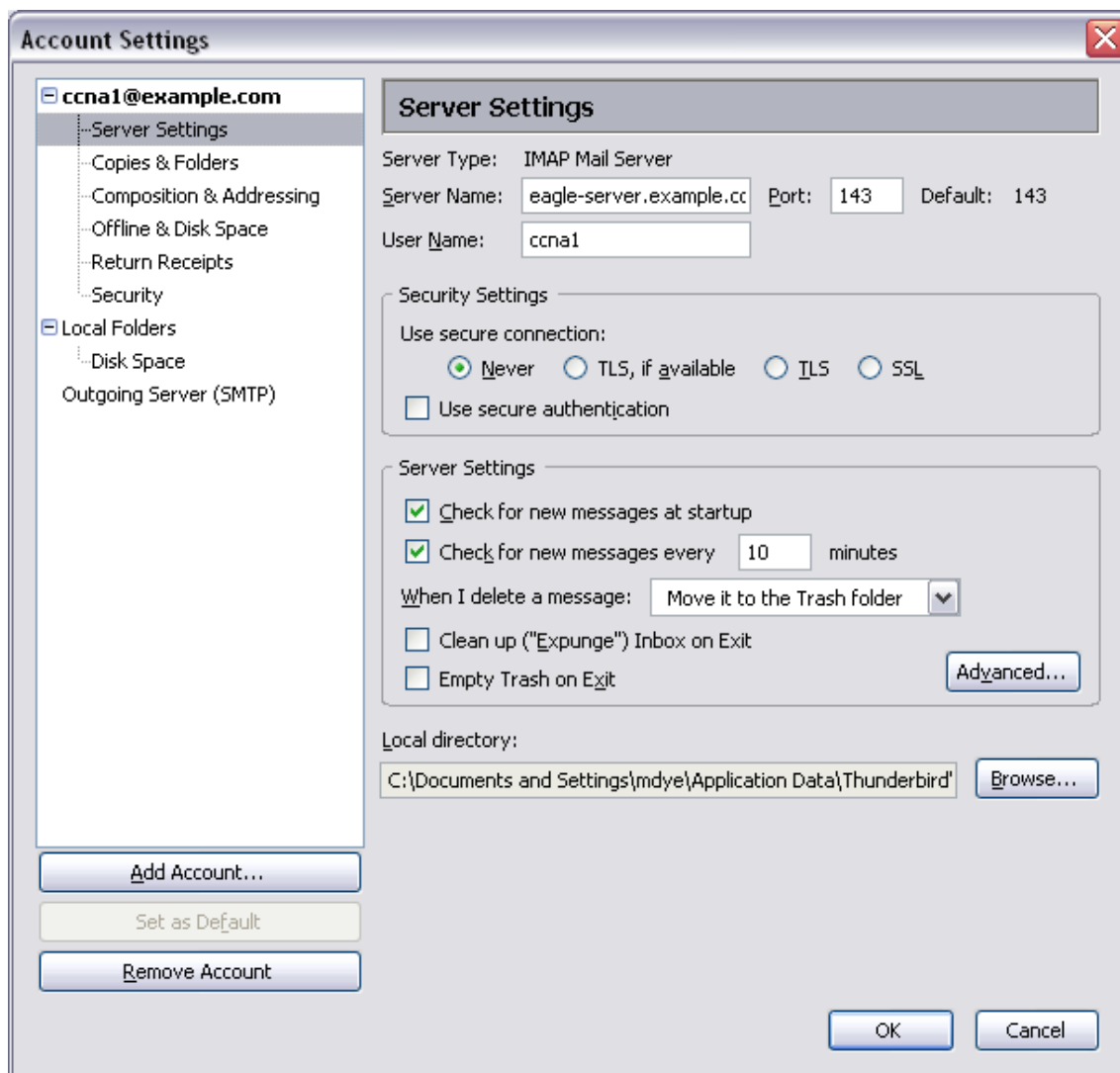
Rysunek 3. Edycja ustawień serwera SMTP

5. Aby zweryfikować ustawienia konta wybierz **Tools > Account Settings**. Spójrz na Rysunek 4.



Rysunek 4. Ustawienia konta Thunderbird

6. W lewym panelu kliknij **Server Settings**. Zostanie wyświetlony ekran podobny do ekranu z Rysunku 5.



Rysunek 5. Ustawienia serwera Thunderbird

Do czego służy protokół SMTP? Jakiego portu TCP używa?

Zadanie 2: Przechwycić i przeanalizuj komunikację e-mail pomiędzy komputerem i serwerem e-mail

Krok 1: Wyślij wiadomość e-mail

1. Zapytaj innego studenta w pracowni o jego adres e-mail.
2. Aby utworzyć i wysłać wiadomość e-mail, wybierz ikonę "Write". Każdy powinien stworzyć i wysłać wiadomość e-mail do pozostałych studentów.
3. Kiedy wiadomość zostanie wysłana sprawdź swoje konto e-mail. Aby sprawdzić swoje konto e-mail, musisz być zalogowany. Jeżeli nie zalogowałeś się wcześniej, wprowadź **cisco** jako hasło. Zwróć uwagę na to, że jest to domyślne hasło wbudowane w serwer Eagle.

Krok 2: Uruchom program Wireshark

Po upewnieniu się, że wysyłanie i odbieranie poczty elektronicznej przebiega prawidłowo, uruchom przechwytywanie pakietów. Wireshark wyświetli przechwytywane pakiety w oparciu o ich typ.

Krok 3: Dokonaj analizy przechwyconej sesji SMTP

1. Za pomocą klienta e-mail ponownie wyślij oraz odbierz wiadomość do/od studenta. W tym czasie wszystkie transakcje będą przechwytywane.
2. Po wysłaniu i odebraniu jednej wiadomości przerwij proces przechwytywania pakietów w programie Wireshark. Na Rysunku 6 przedstawiono przechwycone pakiety zawierające część komunikatów przesyłanych w trakcie wysyłania poczty przy użyciu protokołu SMTP.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
2	0.741371	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
3	1.492443	172.16.1.1	172.16.255.255	NBNS	Name query NB WORKGROUP<1b>
4	3.306445	172.16.1.1	192.168.254.254	TCP	1250 > smtp [SYN] Seq=0 Len=0 MSS=1460
5	3.306968	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
6	3.307012	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=1 Ack=1 Win=64240 Len=0
7	3.313519	192.168.254.254	172.16.1.1	SMTP	Response: 220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13
8	3.353004	172.16.1.1	192.168.254.254	SMTP	Command: EHLO [172.16.1.1]
9	3.353436	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=90 Ack=20 Win=5840 Len=0
10	3.353657	192.168.254.254	172.16.1.1	SMTP	Response: 250-localhost.localdomain Hello host-1.example.com [172.16.1.1]
11	3.356823	172.16.1.1	192.168.254.254	SMTP	Command: MAIL FROM:<ccna1@example.com> SIZE=398
12	3.359743	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.0 <ccna1@example.com>... Sender ok
13	3.363127	172.16.1.1	192.168.254.254	SMTP	Command: RCPT TO:<ccna2@example.com>
14	3.365007	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.1.5 <ccna2@example.com>... Recipient ok
15	3.367680	172.16.1.1	192.168.254.254	SMTP	Command: DATA
16	3.368230	192.168.254.254	172.16.1.1	SMTP	Response: 354 Enter mail, end with "." on a line by itself
17	3.376881	172.16.1.1	192.168.254.254	SMTP	Message Body
18	3.387830	192.168.254.254	172.16.1.1	SMTP	Response: 250 2.0.0 l0S8dIOY005299 Message accepted for delivery
19	3.395347	172.16.1.1	192.168.254.254	SMTP	Message Body
20	3.395855	192.168.254.254	172.16.1.1	SMTP	Response: 221 2.0.0 localhost.localdomain closing connection
21	3.395897	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [FIN, ACK] Seq=564 Ack=502 Win=6432 Len=0
22	3.395929	172.16.1.1	192.168.254.254	TCP	1250 > smtp [ACK] Seq=502 Ack=565 Win=63677 Len=0
23	3.405772	172.16.1.1	192.168.254.254	TCP	1250 > smtp [FIN, ACK] Seq=502 Ack=565 Win=63677 Len=0
24	3.406204	192.168.254.254	172.16.1.1	TCP	smtp > 1250 [ACK] Seq=565 Ack=503 Win=6432 Len=0

Rysunek 6. Przechwytywanie komunikatów SMTP

3. W oknie programu Wireshark podświetl pierwszy wiersz od góry, który informuje o przechwyceniu sesji SMTP. Na Rysunku 6 jest to linia 7.
4. W drugim oknie rozszerz rekord opisujący SMTP.

Istnieje wiele typów serwerów SMTP. Wiedza o typie serwera SMTP oraz jego wersji może być niezwykle cenna dla agresorów.

Jaka jest nazwa i wersja serwera SMTP?

Klienci e-mail wysyłają do serwerów e-mail polecenia, a serwery wysyłają odpowiedzi. Podczas pierwszej wymiany SMTP klient wysyła polecenie **EHLO**. Polecenia wysyłane przez różnych klientów nie muszą być takie same. W czasie pierwszej wymiany może być również wysłane np. polecenie **HELO** lub **HELLO**. Serwer musi odpowiedzieć na to polecenie.

Jaka jest odpowiedź serwera na komendę EHLO?

Kolejna wymiana między klientem i serwerem zawiera informacje dotyczące poczty elektronicznej. Używając informacji przechwyconych przez Wireshark wypisz odpowiedzi serwera na polecenia klienta:

Klient e-mail	Serwer e-mail
MAIL FROM: ,ccna1@example.com>	
RCPT TO:<ccna2@example.com>	
DATA	
(wysyłana jest zawartość listu elektronicznego)	

Jaka jest zawartość ostatniego komunikatu pochodzącego od klienta?

Co odpowiedział serwer?

Zadanie 3: Wyzwanie

Usiądź przy komputerze z dostępem do sieci Internet. Znajdź nazwy serwerów SMTP i ich wersje oraz zapoznaj się z ich słabymi punktami i sposobami ich skompromitowania. Czy są dostępne nowsze wersje?

Zadanie 4: Przemyślenia

E-mail jest prawdopodobnie najbardziej powszechną usługą sieciową. Zrozumienie przepływu ruchu SMTP pomoże Ci dowiedzieć się, w jaki sposób protokół zarządza komunikacją klient-serwer. Problemy z pocztą elektroniczną mogą również obejmować zagadnienia związane z konfiguracją. Czy problem wynika z błędnego działania klienta czy serwera e-mail? Jedną z metod przetestowania operacji serwera SMTP jest użycie narzędzia Telnet, które dostępne jest w systemie Windows.

1. Aby przetestować proces SMTP, otwórz okno wiersza poleceń w systemie Windows i rozpocznij sesję Telnet z serwerem SMTP.

```
C:\>telnet eagle-server.example.com 25
220 localhost.localdomain ESMTP Sendmail 8.13.1/8.13.1; Sun, 28 Jan
2007 20:41:0
3 +1000
HELO eagle-server.example.com
250 localhost.localdomain Hello [172.16.1.2], pleased to meet you
MAIL From: ccna2@example.com
250 2.1.0 ccna2@example.com... Sender ok
RCPT To: instructor@example.com
250 2.1.5 instructor@example.com... Recipient ok
DATA
354 Please start mail input.
Test e-mail serwera SMTP...
.
250 Mail queued for delivery.
QUIT
221 Closing connection. Good bye.
Połączenie z hostem przerwane.
C:\>
```

Zadanie 5: Porządkowanie

Jeśli Thunderbird został zainstalowany tylko na potrzeby tego ćwiczenia, instruktor może poprosić o odinstalowanie tej aplikacji. Aby usunąć aplikację, kliknij **Start > Ustawienia > Panel sterowania > Dodaj lub usuń programy**. Przewiń listę i kliknij **Thunderbird**, a następnie - **Usuń**.

Jeśli instruktor nie polecił inaczej, wyłącz komputery. Zabierz wszystkie rzeczy przyniesione do laboratorium. Pozostaw pomieszczenie w stanie gotowym do rozpoczęcia zajęć z następną grupą studentów.