Bezpieczeństwo komputerowe

semestr letni 2023/24

Lista nr 3

(laboratorium)

Terminy oddania: przed 20.04.2024

Zadanie 1. Poufność maili (5 pkt). Wykonaj kolejno polecenia i odpowiedz na pytania:

1. Utwórz testowe konto mailowe na `https://poczta.o2.pl/`, zaloguj się do niego korzystając z przeglądarki www i w opcjach włącz możliwość pobierania poczty przez POP.
2. Zainstaluj klienta pocztowego (np. Thunderbird) i dodaj w nim to konto, ustawiając ręcznie serwer poczty przychodzącej na `poczta.o2.pl`, port 110, połączenie bez szyfrowania a metodę uwierzytelniania na zwykłe hasło.
3. Z dowolnego swojego konta pocztowego wyślij maila na nowo utworzone konto testowe.
4. Uruchom przechwytywanie pakietów w zainstalowanym wcześniej snifferze (wireshark).
5. Odbierz pocztę z konta testowego w programie pocztowym.
6. Sprawdź, jakie informaje o odebranym mailu udało się przechwycić.
7. Czy protokół SMTP przewiduje szyfrowanie wiadomości przesyłanych pomiędzy serwerami?
8. Czy wybierając w programie pocztowym opcję bezpiecznego połączenia (SSL/TLS) mamy gwarancję, że tylko nadawca i odbiorca mają wgląd w treść maili?
9. Jakie metody możemy zastosować, aby uzyskać poufność wiadomości przesyłanych mailem?
10. Przyjrzyj się i omów zabezpieczenia stosowane przez `Proton Mail` (`https://proton.me/mail`).

Zadanie 2. SPF, DKIM, DMARC (10 pkt). Przeanalizuj nagłówki kilku wybranych wiadomości ze swojej skrzynki odbiorczej i kilku z folderu spam pod kątem mechanizmów uwierzytelniania wiadomości.

- Czy serwery pocztowe, z których pochodzą wiadomości, są upoważnione do wysyłania wiadomości w imieniu domeny nadawcy? (Sprawdź nie tylko status, ale użyj narzędzia

`dig`[1] do weryfikacji, czy rzeczywiście serwer pocztowy nadawcy jest na liście dozwolonych serwerów dla danej domeny)

- Czy wiadomości zostały podpisane cyfrowo przez domenę nadawcy, a podpis został poprawnie zweryfikowany przez serwery pocztowe? Jakie elementy zostały podpisane?
- Czy stosowany jest mechanizm DMARC? Jaki zwraca status?
- Sprawdź politykę DMARC dla domeny przy użyciu `dig`. Jakie są konsekwencje ustawienia konkretnej polityki?
- Czy może się zdarzyć, że SPF, DKIM oraz DMARC zwrócą status `pass` a pomimo to wiadomość trafi do spamu?
- Czy może się zdarzyć, że SPF, DKIM oraz DMARC zwrócą status `pass` a pomimo to wiadomość zawiera złośliwy link/załącznik?

[1] Domain Information Groper