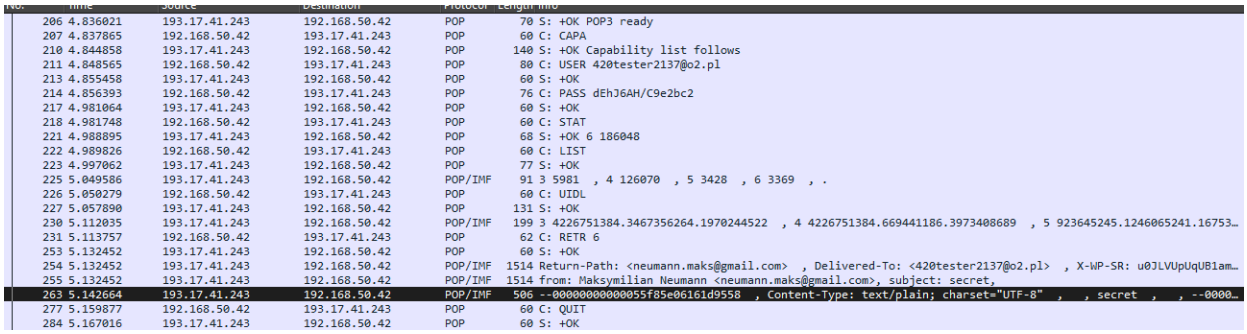
BK Lista 3

PART 1

WSZYSTKO MAMY



No.	Time	Source	Destination	Protocol	Length	Info
206	4.836021	193.17.41.243	192.168.50.42	POP	70	S: +OK POP3 ready
207	4.837865	192.168.50.42	193.17.41.243	POP	60	C: CAPA
210	4.844858	193.17.41.243	192.168.50.42	POP	140	S: +OK Capability list follows
211	4.848565	192.168.50.42	193.17.41.243	POP	80	C: USER 420tester2137@o2.pl
213	4.855458	193.17.41.243	192.168.50.42	POP	60	S: +OK
214	4.856393	192.168.50.42	193.17.41.243	POP	76	C: PASS dEhJ6AH/C9e2bc2
217	4.981064	193.17.41.243	192.168.50.42	POP	60	S: +OK
218	4.981748	192.168.50.42	193.17.41.243	POP	60	C: STAT
221	4.988895	193.17.41.243	192.168.50.42	POP	68	S: +OK 6 186048
222	4.989826	192.168.50.42	193.17.41.243	POP	60	C: LIST
223	4.997062	193.17.41.243	192.168.50.42	POP	77	S: +OK
225	5.049586	193.17.41.243	192.168.50.42	POP/IMF	91	3 5981 , 4 126070 , 5 3428 , 6 3369 , .
226	5.050279	192.168.50.42	193.17.41.243	POP	60	C: UIDL
227	5.057890	193.17.41.243	192.168.50.42	POP	131	S: +OK
230	5.112035	193.17.41.243	192.168.50.42	POP/IMF	199	3 4226751384.3467356264.1970244522 , 4 4226751384.669441186.3973408689 , 5 923645245.1246065241.16753…
231	5.113757	192.168.50.42	193.17.41.243	POP	62	C: RETR 6
253	5.132452	193.17.41.243	192.168.50.42	POP	60	S: +OK
254	5.132452	193.17.41.243	192.168.50.42	POP/IMF	1514	Return-Path: <neumann.maks@gmail.com> , Delivered-To: <420tester2137@o2.pl> , X-WP-SR: u0JLVUpUqUB1am…
255	5.132452	193.17.41.243	192.168.50.42	POP/IMF	1514	from: Maksymilian Neumann <neumann.maks@gmail.com>, subject: secret,
263	5.142664	193.17.41.243	192.168.50.42	POP/IMF	506	--000000000000055f85e06161d9558 , Content-Type: text/plain; charset="UTF-8" , , secret , , --0000…
277	5.159877	192.168.50.42	193.17.41.243	POP	60	C: QUIT
284	5.167016	193.17.41.243	192.168.50.42	POP	60	S: +OK

Tak, protokół SMTP (Simple Mail Transfer Protocol) przewiduje szyfrowanie wiadomości przesyłanych między serwerami poprzez wykorzystanie mechanizmu TLS (Transport Layer Security) lub jego wcześniejszej wersji, SSL (Secure Sockets Layer). Szyfrowanie jest istotne dla zachowania prywatności i bezpieczeństwa danych w transmisji e-maili, szczególnie gdy przesyłane są poufne informacje. Gdy serwery SMTP nawiązują połączenie z innym serwerem, mogą negocjować użycie protokołu TLS/SSL, co umożliwia zabezpieczenie komunikacji poprzez szyfrowanie.

Korzystając z SSL/TLS w programie pocztowym, twoje wiadomości są bezpieczne podczas transmisji przez sieć. Jednak administratorzy serwerów poczty i dostawcy usług mogą mieć dostęp do treści wiadomości. Aby zapewnić pełną prywatność, warto używać także end-to-end encryption.

Aby uzyskać poufność treści przesyłanych maili, możemy zastosować kilka metod, w tym:

1. **Szyfrowanie end-to-end: Ta metoda zapewnia, że treść wiadomości jest zaszyfrowana na urządzeniu nadawcy i odszyfrowywana tylko przez odbiorcę. Żadna inna osoba ani nawet dostawca usług pocztowych nie ma dostępu do niezaszyfrowanej treści.**

2. **Używanie protokołów szyfrowania: Wykorzystywanie protokołów szyfrowania, takich jak S/MIME (Secure/Multipurpose Internet Mail Extensions) lub PGP/MIME**

(Pretty Good Privacy/Multipurpose Internet Mail Extensions), umożliwia szyfrowanie i podpisywanie cyfrowe wiadomości e-mail.

3. **Bezpieczne połączenia SSL/TLS: Korzystanie z bezpiecznych połączeń SSL/TLS między programem pocztowym a serwerem poczty elektronicznej zapewnia szyfrowanie danych w transmisji.**

4. **Używanie bezpiecznych sieci WiFi: Podczas korzystania z publicznych sieci WiFi należy upewnić się, że są one bezpieczne, aby uniknąć potencjalnego podsłuchu.**

5. **Unikanie załączników o dużej poufności: Jeśli dane są bardzo poufne, lepiej unikać wysyłania ich jako załączników w wiadomości e-mail, a zamiast tego skorzystać z dedykowanych narzędzi do udostępniania plików z szyfrowaniem, takich jak usługi do udostępniania w chmurze z opcją szyfrowania.**

6. **Zarządzanie kluczami kryptograficznymi: Ważne jest odpowiednie zarządzanie kluczami prywatnymi i publicznymi podczas korzystania z szyfrowania end-to-end lub protokołów szyfrowania, aby zapewnić bezpieczeństwo i integralność komunikacji.**

PART 2

1.
```
xtb.pl.          3600    IN      MX      1 aspmx.l.google.com.
xtb.pl.          3600    IN      MX      10 aspmx2.googlemail.com.
xtb.pl.          3600    IN      MX      10 aspmx3.googlemail.com.
xtb.pl.          3600    IN      MX      5 alt1.aspmx.l.google.com.
xtb.pl.          3600    IN      MX      5 alt2.aspmx.l.google.com.
```
2. DKIM: 'PASS' z domeną xtb.pl
3. DMARC: 'PASS'
4. “v=DMARC1; p=reject; pct=100”
   - 4.1. p=none: Oznacza to, że domena nie wdrożyła jeszcze żadnych działań zgodnie z polityką DMARC. Żadne wiadomości nie zostaną odrzucone ani uznane za spam na podstawie polityki DMARC. Jednak nadawca może otrzymywać raporty DMARC dotyczące wiadomości, które nie przeszły autentykacji.
   - 4.2. p=quarantine: Wiadomości, które nie przeszły autentykacji DMARC, mogą zostać oznaczone jako podejrzane i dostarczone do folderu spamu lub oznaczone jako podejrzane przez klientów poczty.
   - 4.3. p=reject: Wiadomości, które nie przeszły autentykacji DMARC, zostaną odrzucone przez serwery pocztowe nadawcy lub oznaczone jako spam.

5. Tak, istnieje możliwość, że mimo zwrócenia statusu "pass" przez mechanizmy SPF, DKIM oraz DMARC, wiadomość może zostać uznana za spam przez serwer pocztowy odbiorcy. Istnieje kilka powodów, dla których taka sytuacja może się zdarzyć:

5.1. Inne czynniki filtra spamu: Serwery pocztowe mogą uwzględniać dodatkowe czynniki przy ocenie, czy wiadomość jest spamem czy nie. Mogą to być na przykład treści wiadomości, zachowanie nadawcy, obecność załączników, itp.

5.2. Reputacja nadawcy: Chociaż mechanizmy SPF, DKIM i DMARC pomagają w uwierzytelnianiu nadawcy, reputacja samej domeny nadawcy może również mieć wpływ na to, czy wiadomość trafi do skrzynki odbiorczej, czy do folderu spamu. Domeny, które często wysyłają spam lub mają historię naruszania zasad wysyłania, mogą zostać uznane za podejrzane przez filtry spamu.

5.3. Konfiguracja serwera pocztowego odbiorcy: Niektóre serwery pocztowe mogą mieć bardziej restrykcyjne ustawienia filtrowania spamu niż inne. Nawet jeśli wiadomość przeszła pomyślnie autentykację SPF, DKIM i DMARC, serwer odbiorczy może zastosować dodatkowe kryteria, które mogą wpłynąć na klasyfikację wiadomości.

5.4. Częste błędy w konfiguracji: Choć stosowanie SPF, DKIM i DMARC zwiększa bezpieczeństwo wiadomości e-mail, błędy w ich konfiguracji mogą prowadzić do nieprzewidywalnych rezultatów. Niewłaściwa konfiguracja może spowodować, że serwery pocztowe niepoprawnie oceniają wiadomość.

6. TAK, mogą istnieć sytuacje, w których wiadomość e-mail uzyska status "pass" we wszystkich mechanizmach uwierzytelniania (SPF, DKIM i DMARC), ale nadal zawierać złośliwy link lub załącznik. Mechanizmy SPF, DKIM i DMARC pomagają w uwierzytelnianiu nadawcy i zapewnieniu integralności wiadomości e-mail, ale nie analizują samej treści wiadomości ani załączników. Dlatego nadal istnieje ryzyko, że złośliwe treści mogą zostać dostarczone do skrzynki odbiorczej, nawet jeśli wiadomość ma status "pass" w tych mechanizmach. W celu skutecznego zapobiegania złośliwym treściom w wiadomościach e-mail, konieczne jest stosowanie dodatkowych mechanizmów zabezpieczeń, takich jak filtry antyspamowe, skanery antywirusowe i świadomość użytkowników.