Bezpieczna komunikacja w sieci | materiał pomocniczy

Instrukcja dla grup: Działanie sieci

✂

Za chwilę będziecie odgrywać działanie sieci zgodnie z 3 różnymi scenariuszami. Zanim jednak zaczniecie, przygotujcie się do gry. Wykonajcie następujące zadania:

1. Wyznaczcie jedną osobę, która podczas trwania ćwiczenia będzie czytać instrukcję.
2. Wytnijcie kartki — etykiety z materiału pomocniczego dla grup „Sieć".
3. Rozdzielcie między sobą następujące role:
   - użytkowniczka,
   - oszust,
   - dostawca łącza internetowego użytkowniczki,
   - administrator systemu,
   - policja w kraju użytkowniczki,
   - dostawca łącza internetowego serwera strony internetowej,
   - administrator strony,
   - policja w kraju dostawcy strony.

Jeśli jest Was więcej niż 8 osób, przydzielcie 2 osoby do jednej roli.

4. Połóżcie przed sobą odpowiednie kartki — etykiety.
5. Usiądźcie w kole — w takiej kolejności, jak role wymienione w punkcie 2.
6. Wytnijcie kartki — informacje i połóżcie przed sobą. Każdy powinien mieć przed sobą 4 różne kartki: adres strony WWW, login i hasło, adres IP (lokalizacja) i dane.
7. Teraz pora na stworzenie historii — ustalcie, jak ma na imię użytkowniczka, na jakiej stronie WWW się loguje, jaki ma login i jakie hasło. Wymyślcie, co na danej stronie będzie robić, na jakim komputerze i w jakim miejscu korzysta z Internetu.

Teraz na podstawie scenariuszy odegrajcie kolejno 3 scenki, które ukazują, w jaki sposób przepływają informacje w sieci.

[Cd. Instrukcji na kolejnej stronie]

W trakcie odgrywania uzupełnijcie poniższą tabelę, wpisując w odpowiednich miejscach dane, jakie są widoczne dla poszczególnych osób.

	Sieć niezabezpieczona	HTTPS	TOR
Użytkowniczka			
Oszust			
Dostawca łącza internetowego użytkowniczki			
Administrator systemu i policja w kraju użytkowniczki			
Dostawca łącza internetowego serwera strony internetowej			
Administrator strony i policja w kraju użytkowniczki			

Pierwszy scenariusz — logowanie się w sieci niezabezpieczonej

1. Użytkowniczka loguje się na stronie internetowej. Wszystkie 4 kartki użytkowniczki powinny być odkryte.
2. Oszust ma dostęp do wszystkich danych. Wszystkie 4 kartki oszusta są odkryte.
3. Informacja dociera do dostawcy łącza internetowego użytkowniczki. Dostawca łącza użytkowniczki ma dostęp do wszystkich danych. Wszystkie 4 kartki są odkryte.
4. Administrator systemu i policja w kraju użytkowniczki mają dostęp do tych samych informacji. Wszystkie kartki administratora systemu i policji są odkryte.
5. Informacja dociera do dostawcy łącza internetowego serwera strony internetowej. Wszystkie kartki są odkryte.
6. Informacja dociera do administratora strony. On i policja w kraju dostawcy strony mają dostęp do wszystkich informacji. Wszystkie 4 kartki są odkryte.

Drugi scenariusz — logowanie się sieci z użyciem HTTPS

1. Użytkowniczka loguje się na stronie internetowej. Wszystkie 4 kartki użytkowniczki są odkryte.
2. Oszust ma dostęp do adresu strony WWW i adresu IP użytkowniczki, ale nie ma dostępu do loginu i hasła oraz przesyłanych przez użytkowniczkę danych. Może się dowiedzieć, że użytkowniczka wysyła i odbiera jakieś informacje z sieci, ale nie zna adresata ani treści tych informacji. 2 kartki są odkryte, 2 — odwrócone.
3. Informacja dociera do dostawcy łącza internetowego użytkowniczki, który ma dostęp do adresu strony WWW i adresu IP użytkowniczki, ale tak jak oszust nie ma dostępu do loginu i hasła oraz danych. 2 kartki są odkryte, 2 — odwrócone.
4. Administrator systemu i policja w kraju użytkowniczki mają dostęp do tych samych informacji. 2 kartki są odkryte, 2 — odwrócone.
5. Informacja dociera do dostawcy łącza internetowego serwera, na którym znajduje się strona internetowa. Ma on dostęp do tych samych informacji co oszust i dostawca łącza internetowego użytkowniczki. 2 kartki są odkryte, 2 — odwrócone.
6. Informacja dociera do administratora strony. On i policja w kraju dostawcy strony mają dostęp do wszystkich informacji. Wszystkie 4 kartki są odkryte.

Trzeci scenariusz — komunikacja w sieci TOR

1. Użytkowniczka loguje się na stronie internetowej. Wszystkie 4 kartki użytkowniczki są odkryte.
2. Oszust ma dostęp tylko do adresu IP użytkowniczki. Nie zna adresu strony internetowej, loginu i hasła. Nie widzi też danych, które przesyła lub odbiera użytkowniczka. 1 kartka jest odkryta, 3 kartki — odwrócone.
3. Dostawca łącza internetowego Użytkowniczki ma dostęp do tych samych danych co oszust, czyli tylko do adresu IP. 1 kartka jest odkryta, 3 kartki — zakryte.
4. Administrator systemu i policja w kraju użytkowniczki mają dostęp do tych samych danych. 1 kartka jest odkryta, 3 kartki — zakryte.
5. Dostawca łącza internetowego serwera strony internetowej ma dostęp do: adresu strony WWW, loginu i hasła, danych. Nie zna jednak adresu IP użytkowniczki. 3 kartki są odkryte, 1 kartka — zakryta.
6. Administrator strony i policja w kraju dostawcy strony mają dostęp do tych samych danych co dostawca łącza internetowego serwera strony internetowej. 3 kartki są odkryte, 1 kartka — zakryta (z adresem IP).

Materiał pomocniczy dla grup: Sieć

Kartki — etykiety

✂

użytkowniczka
oszust
dostawca łącza internetowego użytkowniczki
administrator systemu
policja w kraju użytkowniczki
dostawca łącza internetowego serwera strony internetowej
administrator strony
policja w kraju dostawcy strony

Kartki — informacje

✂

adres strony WWW	adres strony WWW
login i hasło	login i hasło
adres IP (lokalizacja)	adres IP (lokalizacja)
dane	dane
adres strony WWW	adres strony WWW
login i hasło	login i hasło
adres IP (lokalizacja)	adres IP (lokalizacja)
dane	dane

adres strony WWW	adres strony WWW
login i hasło	login i hasło
adres IP (lokalizacja)	adres IP (lokalizacja)
dane	dane
adres strony WWW	adres strony WWW
login i hasło	login i hasło
adres IP (lokalizacja)	adres IP (lokalizacja)