**Zadanie 2.**

Pobierz obraz wirtualnej maszyny MITM oraz zaimportuj ją do Virtualbox

Będziemy potrzebować trzech urządzeń dlatego sklonuj istniejącą maszynę dwa razy (prawy klik -> clone)

Maszyny odzwierciedlają serwer, uzytkownika oraz intrudera.



Następnie dla każdej maszyny wygeneruj nowy MAC Address (Settings->Network->Advanced->Generate a new random MAC address)

Uruchom maszyny oraz sprawdź czy posiada swój własny adres IP (komenda ifconfig) oraz czy jest możliwa komunikacja między nimi (np poprzez ping).

Jeżeli tak to środowisko jest gotowe i poprawnie skonfigurowane.

Na serwerze uruchom terminal i przejdź do katalogu /app znajdującego się w folderze domowym

Uruchom aplikację poleceniem: flask run --host=0.0.0.0

Na komputerze klienta możesz teraz odwidzić strone wpisując w pasku wyszukiwarki [http://X.X.X.X:5000](http://x.x.x.x:5000/) gdzie X.X.X.X jest adresem serwera.

Utwórz nowe konto, zaloguj się oraz dodaj jakiś post. Nie wylogowywuj się.

Czas na przeprowadzenieataku MITM. Na komputerze intrudera uruchom program ettercap. Możesz to zrobić wpisując w terminalu: sudo ettercap -G (flaga "-G" otwiera program w trybie graficznym chociaż możliwe jest również korzystanie z trybu konsolowego)

Aby znaleźć hosty w naszej sieci wchodzimy w rozwijany panel po prawej stronie Hosts->Hosts list, a następnie Hosts->Scan for hosts



Zaznaczamy adres naszego serwera i dodajemy jako Target 1, analogicznie dodajemy uzytkownika jako Target 2.

Następnie w rozwijanym pasku "MITM menu" wybieramy "ARP poisoning" i odzaznaczamy opcję "Sniff remote connections". Po zatwierdzeniu tablica ARP naszego servera zostanie zatruta i ruch kierowany jest przez nasz komputer.

Przechodzimy do nowego terminala, aby uruchomić program wireshark (sudo wireshark).

Teraz należy wygenerować ruch w sieci np na maszynie uzytkownika dodajemy post lub przechodzimy między podstronami. Na maszynie intrudera w programie wireshark powinniśmy zaobserwować przychodzące pakiety. Wybieramy jeden w którym możemy spodziewać się ciasteczka zawierającego aktywną sesję np HTTP POST. Prawy klik -> Follow->TCP Stream, aby przejrzeć zawartość. Wyszukujemy ciasteczka sesji która będzie miała postać: session=value.

Po skopiowaniu klucza przechodzimy do wyszukiwarki, i przechodzimy pod adres serwera. W narzędziu developerskim (f12) w zakładce storage możemy dodac nowe ciasteczko do strony. Ustawiamy Name jako "session" oraz znalezione value. Należy pamiętać, aby Path było ustawione na całą stonę czyli "/".

Po odświerzeniu strony powinniśmy być zalogowani na koncie uzytkownika.

Wykonaj zrzut ekranu na którym będzie widać znaleziony w wireshark klucz sesji.