**Wrocław 01.10.2023**

**CyberBezpieczeństwo**

**Lab 8**

1. **Wstęp**

Ataki nie zawsze wiążą się z dostępem do komputera lub danych na serwerze. Rosnące znaczenie Internetu i ilości przesyłanych danych w sieci spowodowało rozwój ataków związanych z komunikacją sieciową, zwłaszcza ataków należących do grupy ataków Man in the Middle.

MitM to grupa ataków, których podstawowym założeniem jest podsłuchiwanie komunikacji między dwoma urządzeniami w sieci. W efekcie atakujący uzyskuje dostęp do danych przesyłanych w trakcie komunikacji, może je odczytać, dowolnie modyfikować (łącznie z całkowitą zmianą przesyłanych treści, np. W celu przesłania fałszywej strony internetowej) oraz zablokować.



Rysunek 1 Man of the Middle attack

**Ataki MitM można podzielić na kilka grup:**

* **Podsłuch Wi-Fi -** prosty rodzaj ataku polegający na tworzeniu hotspotów / punktów dostępowych sieci Wi-Fi podszywających się pod znane i bezpieczne sieci (np. kawiarnie, kina, sieci publiczne). Za pomocą tego ataku haker ma możliwość wysłania dowolnej treści do użytkownika sieci (np. fałszywych wersji znanych usług internetowych).
* **Zatrucie ARP (ARP poisoning)** - atak wykorzystujący brak uwierzytelnienia podczas transmisji z wykorzystaniem protokołu ARP. Wysyłając odpowiednią wiadomość ARP, atakujący zatruwa tablicę routingu ARP, zamieniając adres MAC dowolnego urządzenia w zaatakowanej sieci z własnym adresem IP. W wyniku zmiany tablicy wszystkie pakiety sieciowe ofiary są wysyłane do atakującego, jednocześnie atakujący traktowany jest jako odbiorca wiadomości, a jego odpowiedzi jako poprawne odpowiedzi na każde żądanie.
* **DNS spoofing** - Zatruwanie pamięci podręcznej DNS pozwala napastnikowi zmusić ofiarę do pobrania szkodliwych danych, próbując połączyć się ze znanymi usługami sieciowymi. Atakujący wysyła fałszywą wiadomość zawierającą nazwę domeny i adres IP np. złośliwej witryny. Kiedy ofiara próbuje połączyć się ze stroną internetową, podając nazwę domeny, zostaje przekierowana na stronę atakującego.
* **Przekierowanie ICMP (ICMP redirects)** - Używając pakietów przekierowania ICMP, osoba atakująca może poinstruować router, aby przekazywał pakiety przeznaczone dla ofiary do maszyny atakującego. Atakujący może następnie monitorować lub modyfikować pakiety przed ponownym wysłaniem do miejsca przeznaczenia.
* **Kradzież portów (Port stealing)** - atak przeprowadzony w sieciach lokalnych polegający na zmianie informacji przechowywanych w tablicy przekazywania przełącznika sieciowego. Po wykonaniu tej czynności wszystkie pakiety sieciowe adresowane do oryginalnego portu są przekierowywane do portu, do którego podłączona jest maszyna atakującego.
* **STP mangling** - w sieci każdy router domyślnie przyjmuje siebie jako most główny (bridge). Istnieje jednak możliwość wysłania Bridge Protocol Data Units (BPDU) w celu ustanowienia nowego mostu głównego. W przypadku braku wsparcia dla odpowiedniej ochrony, cały ruch sieciowy z przełącznika ofiary zaczyna być przesyłany przez przełącznik wskazany przez atakującego jako root.

1. **Wymagana konfiguracja środowiska**

* Kali
* Metasploitable2

1. **Wymagana wiedza**

* Routing tables
* DNS
* APR
* DNS/ARP cache
* MAC
* Ettercap
* Arpspoof
* Wireshark

1. **Problemy i pytania**
2. Jaka jest różnica między aktywnymi i pasywnymi atakami MitM?
3. Jak zabezpieczyć swoją sieć przed atakami zatruwania ARP?
4. Dlaczego ważne jest, aby używać rozszerzeń DNSSEC w celu zapobiegania atakom polegającym na fałszowaniu DNS?
5. Co to jest tryb monitorowania i jak można go używać do podsłuchiwania komunikacji sieciowej?
6. **Zadania**

**W niektórych przypadkach mechanizmy bezpieczeństwa routera oraz zapisane dane w pamięci cache mogą przeszkadzać w obserwacji wyniku poprawnego wykonania ataku. W takim przypadku, aby poprawnie wykonać atak może być konieczne:**

* **Podłączenie komputera do hotspota uruchomionego za pomocą smartfona**
* **Zmiana ustawień kart sieciowych maszyn wirtualnych na Bridged Adapter: VirtualBox -> dla każdej maszyny wirtualnej -> Settings -> Network -> Attached to: Bridged Adapter**

**Pamiętaj, aby po wykonaniu zadań przywrócić poprzednie ustawienia karty sieciowej!**

**Tabela ARP dla Twojego komputera zostanie zmodyfikowana w trakcie ćwiczenia. Pamiętaj, aby zakończyć atak MitM po zakończeniu ćwiczeń, aby odwrócić ten proces!!!!**

1. W tym zadaniu maszyną ofiary jest Ubuntu Server VM. Dodatkowo będziemy wykorzystywać Metasplitable 2 VM jako maszynę z serwerem WWW.
2. Otwórz wiersz poleceń i zlokalizuj plik **etter.dns** na Kali VM

**locate etter.dns**

1. Przejdź do tej ścieżki i otwórz plik
2. Edytuj plik, aby sfałszować nazwę domeny (dodaj wpis):

**pwr.edu.pl A {KALI\_VM\_IP\_ADDRESS}**

**pwr.edu.pl A {KALI\_VM\_IP\_ADDRESS}**

**www.pwr.edu.pl PTR {KALI\_VM\_IP\_ADDRESS}**

1. W Kali VM uruchom Apache2

**service apache2 start**

1. Uruchom Ettercap na Kali VM

***sudo ettercap -G***

1. Rozpocznij nasłuch
2. Użyj **Scan for hosts** z menu Hosts a następnie przejdź do **Hosts List** z tego samego menu.
3. Dodaj adres routera/bramy domyślnej do Target 1 i adres atakowanej maszyny (Ubuntu Server VM) do Target 2
4. Rozpocznij ARP Poisoning

**Mitm menu -> ARP Poisoning -> Check Sniff remote connections**

1. Przejdź do menu Wtyczki i aktywuj wtyczkę dns\_spoof

**Plugins -> Manage plugins -> double click on dsn\_spoof**

1. Otwórz w przeglądarce **pwr.edu.pl** na maszynie symulującej ofiarę i obserwuj wyniki
2. Zatrzymaj ostatni atak MitM
3. Wyczyść adresy celów ataku, a następnie dodaj adres ofiary do Target 1 oraz adres Metasploitable VM do Target 2
4. Uruchom ARP Poisoning
5. Otwórz w przeglądarce na maszynie ofiary adres **http://{METASPLOITABLE\_VM\_IP\_ADDRESS}/dvwa i** spróbuj zalogować się przy użyciu dowolnego loginu i hasła. Obserwuj wyniki w ettercap.
6. Otwórz Wireshark na Kali VM, zacznij przechwytywać ruch na interfejsie sieciowym eth i spróbuj wygenerować ruch sieciowy na Metasploitable VM (spróbuj zalogować się ponownie, otwórz inne aplikacje na serwerze WWW, spróbuj połączyć się z ssh). Obserwuj wyniki.