Jacek WOŁOSZYN
Uniwersytet Technologiczno-Humanistyczny w Radomiu, Polska

Wykorzystanie mitm i dnsspoof do przechwycenia sesji komunikacyjnej

Wstęp

Sieć bezprzewodowa wykorzystująca protokół 802.11 jest obecnie często wykorzystywanym medium transmisyjnym. Na jej popularność składa się kilka czynników. Najważniejszy z nich to ten, że do jej funkcjonowania nie trzeba budować kosztownej infrastruktury. Drugim czynnikiem jest szybkość instalacji. Można wpiąć wtyczkę po WANowskiej stronie routera i właściwie już system działa, wykorzystując domyślne ustawienia. W praktyce trzeba poświęcić jednak parę minut na konfigurację wymaganych parametrów sieci i odpowiednich zabezpieczeń w większości opartych na WPA2. Ze względu jednak na naturę medium, czyli fale elektromagnetyczne, które są dostępne dla każdego, zarówno uprawnionego, jak i przypadkowego użytkownika, bezpieczeństwo takiej struktury jest poważnie zagrożone.

1. Nieautoryzowany punkt dostępowy – opis problemu

Utworzenie nieautoryzowanego punktu dostępowego stwarza możliwość aktywnego ataku typu mitm [Fry, Nystrom 2010; Kennedy, O'Gorman 2013] /man-in-the-middle/. W takim przypadku nie działają wyrafinowane reguły firewalla, ponieważ cały ruch sieciowy przechodzi przez NAP. Szczególnie niebezpieczne jest rozwiązanie, gdy nazwa essid jest tożsama z nazwą autoryzowanego punktu dostępowego. Można bowiem tak ustawić parametry, żeby posiadały tę samą nazwę rozgłoszeniową essid, jak i ten sam MAC adres bssid. Używając zaawansowanych narzędzi, wykrycie fałszywego punktu dostępowego nie jest łatwe. Można także wymusić rozłączenie klienta podłączonego do autoryzowanego AP, a jeśli ten ma ustawioną konfigurację wymuszającą ponowne nawiązanie połączenia (a tak jest w większości przypadków), to połączenie następuje, ale już z nieautoryzowanym punktem dostępowym. Dzieje się tak dlatego, że karta sieciowa klienta łączy się z sygnałem o wyższym poziomie. Można wyłączyć w kliencie sieciowym automatycznie łączenie z siecią, wówczas będzie widoczna informacja o próbie nawiązania nowego połączenia.

2. Procedura utworzenia programowego punktu dostępowego

Utworzenie programowego punktu dostępowego jest niezbyt skomplikowane. W pierwszej kolejności należy sprawdzić dostępne interfejsy w komputerze. W tym przypadku można zauważyć dwa interfejsy sieciowe wlan2 oraz wlan0. Aby uzyskać rezultat przedstawiony na rys. 1, należy wydać polecenie iwconfig. Oczywiście wszelkie uzyskane różnice będą spowodowane różnicami konfiguracyjnymi maszyny. Dobrym rozwiązaniem jest nadanie nazwy essid tworzonemu punktowi, która będzie tożsama z nazwą już istniejącego punktu.

```
 iwconfig
wlan2     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0
dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
lo        no wireless extensions.
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20
dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
eth0      no wireless extensions.
```

Rys. 1. Rezultat działania polecenia iwconfig

Aby zaobserwować pracujące AP, jak i stacje robocze podłączone do wybranych routerów, jak też stacji niezalogowanych, należy utworzyć interfejs pracujący w trybie monitora (rys. 2). Tryb monitora RFMON jest to specjalny tryb „RF monitoring mode”, występujący jedynie w kartach bezprzewodowych, w którym interfejs potrafi odbierać wszystkie ramki 802.11 będące w powietrzu, także ramki kontrolne i sterujące. Nie wszystkie drivery potrafią obsłużyć opisywany tryb. W czasie pracy w trybie RFMON interfejs nie jest podłączony do żadnej sieci bezprzewodowej. W przypadku trybu zwykłego i promiscous kanał może być ustawiany automatycznie, zgodnie z informacjami rozgłaszanymi przez punkt dostępowy lub klientów już należących do określonej sieci ad-hoc. Wystarczy podać tylko identyfikator sieci (SSID). W przypadku pracy w trybie monitora, konieczne jest odpowiednie (ręczne) ustawienie kanału pracy karty, gdyż nie jesteśmy podłączeni do żadnej sieci.

Aby utworzyć taki interfejs, należy wydać polecenie airmon-ng, wskazując jako parametr nazwę interfejsu bezprzewodowego.

```
root@bt:~# airmon-ng start wlan2
Process with PID 2590 (dhclient3) is running on interface wlan0
Interface    Chipset             Driver
wlan2        Ralink RT2870/3070  rt2800usb - [phy1]
                                 (monitor mode enabled on mon0)
wlan0        Atheros AR9285      ath9k - [phy0]
```

Rys. 2. Rezultat działania polecenia airmon-ng

W wyniku działania polecenia utworzony został nowy interfejs o nazwie mon0 pracujący w trybie monitor mode. Można teraz użyć airodump z parametrem mon0, aby nasłuchiwać na wszystkich kanałach przychodzący i wychodzący ruch sieciowy. W wyniku tego można uzyskać listę wszystkich pracujących AP znajdujących się w zasięgu działania interfejsu, jak też klientów podłączonych do AP oraz niezalogowanych. Stosując dodatkowo parametr – w /file, można zapisać ruch do pliku. Podając nazwę essid lub bssid i parametr – c ch, można dokonać selekcji wybranego kanału. Zebrane w ten sposób informacje można wykorzystać do znalezienia klucza szyfrującego. W przypadku WEP wystarczy zebrać odpowiednią ilość ramek, a w przypadku WPA ramki procesu uwierzytelnienia niezbędne do przeprowadzenia ataku słownikowego.

Aby utworzyć programowy punkt dostępowy, należy wydać polecenie airbase-ng (rys. 3) z parametrami wskazującymi nazwę rozgłaszania essid, jak i wskazującą częstotliwość pracy karty. W przypadku tworzenia punktu dostępowego typu /tvin evil/ należy jeszcze zadbać o odpowiedni MAC adres karty.

```
root@bt:~# airbase-ng --essid brigde -c 11 mon0
09:50:01  Access Point with BSSID 00:C0:CA:59:AC:75 started.
```

Rys. 3. Utworzenie punktu dostępowego

Aby nowo powstały AP funkcjonował prawidłowo, należy utworzyć most sieciowy pomiędzy AP dostępnym dla klienta a stroną systemu. W tym celu należy wydać polecenia, jak pokazano na rys. 4.

```
root@bt:~# brctl addbr my-bridge
root@bt:~# brctl addbr my-bridge eth0
root@bt:~# brctl addif my-bridge eth0
root@bt:~# brctl addif my-bridge at0
root@bt:~# ifconfig eth0 0.0.0.0 up
root@bt:~# ifconfig at0 0.0.0.0 up
root@bt:~# ifconfig my-bridge 192.168.1.150 up
```

Rys. 4. Proces tworzenia mostu sieciowego

Kolejnym krokiem jest włączenie w jądrze systemu opcji przekazywania pakietów IP /IP – forwarding/ w celu ich dalszego routingu.

```
root@bt:~# echo > 1 /proc/sys/net/ipv4/ip_forward
```

Rys. 5. Włączenie przkazywania pakietów IP

Aby przyznać nowo powstałym numery IP, należy uruchomić serwer DHCP, który takie numery nada z puli adresów.

```
root@bt:~# dhclient3
There is already a pid file /var/run/dhclient.pid with pid 5645
killed old client process, removed PID file
```

Rys. 6. Uruchomienie serwera DHCP

Po uruchomieniu serwera DHCP [Tandenbaum, Wetheral 2010] nic już nie stoi na przeszkodzie, aby podłączyć klienta do systemu. Należy zauważyć, że cały ruch sieciowy przechodzi przez interfejs at0 mostu sieciowego. W przypadku uruchomienia w systemie narzędzia do sniffingu typu Wireshark™ [Sanders 2013; Sanders, Smith 2014; Chappel 2012] czy tcpdump [Allen 2014; Bejtlich 2014] istnieje możliwość zapisu i analizy całego ruchu sieciowego generownego przez klienta, jak i do niego i późniejsza jego analiza. W przypadku transmisji nieszyfrowanej można przechwycić wrażliwe informacje w postaci loginów haseł czy innych istotnych wiadomości. Wykorzystanie przechwyconych informacji zależy już tylko od wyobraźni intruza, ale zapewne każdy wolałby uniknąć takich sytuacji.

3. Dnsspoof

Ostatnim już krokiem w omawianym temacie jest zamiana numerów IP DNS w taki sposób, aby niczego nieświadomy klient, łącząc się z wybranym serwisem, został przekierowany pod wybrany przez nas numer IP, na którym może działać np. serwer Apache, gdzie funkcjonuje fałszywa strona emulująca stronę, do której logował się klient. Klient podaje login, hasło, w tle działa program przechwytujący i zapisujący pakiety. W rezultacie intruz pozyskuje wiedzę, której zapewne klient nie chciałby ujawnić. Aby takie przekierowanie DNS wykonać, należy użyć polecenia dnsspoofing [Allen 2014; Wilhelm 2010].

Zatruwanie DNS jest techniką phishingu polegającą na wysłaniu przez atakującego do serwera DNS fałszywej informacji kojarzącej nazwę domeny z adresem IP. Serwer DNS zapamiętuje ją na pewien czas i zwraca klientom zapamiętany adres IP, czego skutkiem jest przeniesienie na fałszywą stronę.

Poprawnie działający serwer powinien zapamiętywać tylko odpowiedzi na pytania faktycznie przez niego wysłane, a nie każdą „odpowiedź”, niezależnie od źródła pochodzenia, jednak nawet w takiej sytuacji ze względu na słabości protokołu DNS [Tandenbaum, Wetheral 2010; Whaley, Hein 2010].

```
root@bt:~# dnsspoof -i my-bridge
dnsspoof: listening on my-bridge [udp dst port 53 and not src
192.168.1.104]
192.168.1.100.49641 > 193.111.144.12.53:  32994+ A?
```

Rys. 7. Rezultat działania dnsspoof

4. Podsumowanie

Sieci bezprzewodowe działające w oparciu o protokół 802.11 należą do bardzo popularnego medium transmisyjnego. Zawdzięczają to upodobaniom użytkownika, który nie musi się wpinać do systemu przewodami. Można przebywać na rynku, pić kawę w kawiarni i trzymając w ręku tablet, smartfon, notebooka czy inne urządzenie posiadające interfejs działający w oparciu o protokół 802.11 korzystać z dostępu do Internetu, logować się do banku, odbierać pocztę, korzystać z serwisu społecznościowego. Jednak droga, którą dostęp ten jest uzyskiwany, nie jest znana zwykłemu użytkownikowi. W przypadku zastosowania rozwiązania typu Tvin Evil praktycznie jest bardzo trudne do wykrycia, a o wyborze sieci decyduje siła sygnału AP. Napastnik może też wymusić rozłączenie z autoryzowanym AP i wówczas zgodnie z teorią wyboru silniejszego sygnału nastąpi przyłączenie do nieautoryzowanego AP. Zwykłe prześledzenie routingu przez użytkownika nie zawsze daje informację o nieprawidłowym połączeniu – przecież wszystko działa. Problem tylko w tym, że pakiety wędrują drogą przez programowy AP i są zapisywane przez intruza, który może potem uzyskać z nich interesujące informacje. Powstaje pytanie, jak uniknąć takich sytuacji. Zwykły użytkownik ma małe szanse ominięcia problemu. Może zauważyć zmniejszenie prędkości działania, ponieważ w przypadku dużego ruchu dużej liczby osób korzystających z nieautoryzowanego systemu może on stanowić wąskie gardło transmisyjne. W przypadku logowania się bezpiecznym protokołem należy zwrócić uwagę, czy taki występuje na stronie, do której się logujemy. Należy jednak pamiętać, że i intruz może sobie zadać tyle trudu, aby i z jego strony takie logowanie było wymagane.

Najwięcej zależy w tym przypadku od administratora sieci. To on musi znać doskonale swoją sieć, całą infrastrukturę, wszystkie punkty dostępowe i inne wrażliwe miejsca, musi stale monitorować ruch w sieci [Collins 2014; Rash 2008] i sprawdzać wszelkie anomalie występujące podczas pracy. W przypadku pojawienia się nowego punktu dostępowego zweryfikować, czy jest on autoryzowany. Uruchomienie zamiany numerów DNS nie jest takie łatwe do zrealizowania jeśli intruz ma utrudniony dostęp do sieci. W przypadku jednak zastosowania nieautoryzowanego AP i utworzenia mostu cały ruch sieciowy przechodzi przez ręce napastnika i może on kierować nim dowolnie.

Literatura

Allen L. (2014), *Advanced Penetration Testing for higly secured environments PACKT 2014*.

Bejtlich R. (2014), *The practice of network security monitoring*, No Starch Press.

Chappel L. (2012), *Wireshark Network Analysis Second Edition*, Protocol Analysis Institute, Inc., dba Chappel University.

Collins M. (2014), *Network security through data analysis*, O'Reilly.

Fry C., Nystrom M. (2010), *Monitoring i bezpieczeństwo sieci*, Gliwice.

Kennedy D., O'Gorman J., Kearns D., Aharoni M. (2013), *Metasploit. Przewodnik po testach penetracyjnych*, Gliwice.

Rash M. (2008), *Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad i fwsnort*, Gliwice.

Sanders C. (2013), *Praktyczna analiza pakietów*, Gliwice.

Sanders C., Smith J. (2014), *Applied network security monitoring, colletion detection and analisys*, Syngress.

Tandenbaum A., Wetheral D. (2010), *Computer Networks Fifth Edition*, Prentice Hall.

Whaley B., Hein T., Snyder G., Nemeth E. (2010), *Unix and Linux system administration handbook*, Prentice Hall.

Wilhelm T. (2010), *Professional Penetration Testing Creating and Operating a Formal Hacking Lab*, Syngress.

Streszczenie

Artykuł opisuje przeprowadzenie ataku mitm /man-in-the-middle/ wraz z przekierowaniem ruchu DNS na wybraną maszynę. Omówiony proces pozwala prześledzić ścieżkę napastnika do uzyskania celu, a jej znajomość pozwoli administratorom sieciowym na wnikliwe spojrzenie na problem i odniesienie się do własnych zasobów sieciowych.

Słowa kluczowe: dnsspoof, mitm, 802.11, sieci bezprzewodowe, bezpieczeństwo.

Monitoring system logs using the Logcheck

Abstract

The article describes an attack mitm /man-in-the-middle/ along with redirecting DNS traffic on the selected machine. Discuss the process allows you to trace the path of the attacker. Network administrators will be able to carefully look at the problem in relation to their own network resources.

Key words: man-in-the-middle, dnsspoof, 802.11, wireless network.