

Nepenthes Unofficial Italian FAQ

KlaatuProject

FRANCESCO MATARAZZO

ti@siinfor.it

v0.3

13 giugno 2009

Sommario

Breve raccolta di FAQ (Frequently Asked Questions) su [Nepenthes](#).

Quest'opera è stata rilasciata sotto la licenza Creative Commons Attribuzione-Non commerciale-Condividi allo stesso modo 2.5 Italia. Per leggere una copia della licenza visita il sito web <http://creativecommons.org/licenses/by-nc-sa/2.5/it/> o spedisci una lettera a Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

Indice

1	Cos'è Nepenthes?	2
2	Nepenthes è un honeypot a bassa interazione?	2
3	Nepenthes è gratuito?	2
4	Come posso installare Nepenthes?	2
5	Ho problemi nel compilare Nepenthes con g++ 4.3?	3
6	Nepenthes ha una gui?	3
7	Come posso far inviare i dati a NepenthesFE?	3
8	Con NepenthesFE non funziona rrd?	4
9	A quali sandbox faccio inviare i binari?	4
10	Funziona l'invio a NormanSandbox?	4
11	È possibile usare Nepenthes come un sottosistema di Honeyd?	4

12 Cos' è e a cosa serve module-portwatch?	4
13 Nepenthes riesce a gestire exploit 0day?	5
14 Nepenthes riceve soprattutto attacchi che sfruttano la dcom, come mai?	5
15 Non sono presenti binari in /var/binaries/, come posso verificare che tutto stia funzionando?	5
16 È utile posizionare Nepenthes in una LAN? Perché?	5
17 Quali porte apre Nepenthes?	5
18 Posso partecipare attivamente con la mia installazione di Nepenthes a Mwcollect?	6
19 Esistono dei software simili a Nepenthes?	6

1 Cos'è Nepenthes?

Nepenthes è un honeypot per sistemi Unix, progettato per la cattura di malware. Esso ha un'architettura fortemente modulare, scritto in C++ si presenta come un demone classico. L'ultima versione è la 0.2.2.

2 Nepenthes è un honeypot a bassa interazione?

No, non proprio. Esso è più propriamente un honeypot a media interazione. Gli honeypot a media interazione combinano i vantaggi degli honeypot a bassa e alta interazione. La sostanziale differenza rispetto ad un honeypot a bassa interazione è che vengono simulate delle parti di sistema operativo, tramite un livello di virtualizzazione. Ad esempio, può essere eseguito uno shellcode ed emulato un file system con alcune utility (ftp, cp, etc). Tutto questo per diminuire la sinteticità tipica degli honeypot a bassa interazione.

3 Nepenthes è gratuito?

Si, è free software. È rilasciato sotto GPL v2.

4 Come posso installare Nepenthes?

Nepenthes può essere installato tramite pacchetti precompilati in caso si stia usando una distribuzione che dispone di questi ultimi. In caso contrario è necessario ricompilare nepenthes dai sorgenti. Per Ubuntu e Debian basta lanciare il comando

```
apt-get install nepenthes
```

per avere l'honeykot installato nel proprio sistema. Si noti che nepenthes ha delle dipendenze da soddisfare. Nel caso di installazione tramite apt-get, esse vengono soddisfatte automaticamente; se invece si vuole ricompilare manualmente il pacchetto e si sta usando un sistema Ubuntu, le dipendenze possono essere soddisfatte con il seguente comando:

```
apt-get install automake1.9 libtool flex bison libcurl3-dev libmagic-dev \
libpcre3-dev libadns1-dev libpcap0.8-dev
iptables-dev make g++
```

Per compilare Nepenthes dai sorgenti eseguire i seguenti comandi:

```
svn checkout https://svn.nepenthes.carnivore.it /nepenthes/trunk/ nepenthes
cd nepenthes
autoreconf -v -i
./configure
make
make install
```

Per conoscere le opzioni di compilazione di Nepenthes, lanciare:

```
./configure --help
```

5 Ho problemi nel compilare Nepenthes con g++ 4.3?

SI, è noto che esistono dei problemi di compilazione con gcc 4.3. Esiste una patch per compilare Nepenthes, con gcc 4.4: <http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=505383>.

6 Nepenthes ha una gui?

Il progetto ufficiale non fornisce nessun tipo di interfaccia grafica/web. Tuttavia esistono dei progetti non legati a Mwcollect, il progetto ufficiale, che rendono disponibili delle interfacce web.

Uno è NepenthesFE (<http://www.emre.de/wiki/NepenthesFE>) e un altro è SURFids (<http://ids.surfnet.nl/wiki/doku.php>). Un'interfaccia grafica è necessaria per monitorare con facilità i dati raccolti. L'invio dei dati a NepenthesFE viene fatta tramite il modulo submit-http mentre per SURFids tramite l'apposito modulo log-surfnet.

7 Come posso far inviare i dati a NepenthesFE?

Aggiungere

```
http://IpMacchinaConNepenthesfe:porta/percorsonepenthesfe/submit.php
```

a submit-http. Assicurarsi che le credenziali in submit-http siano corrette.

8 Con NepenthesFE non funziona rrd?

Potrebbero esserci dei problemi con l'autenticazione con lo script cron.php. Assicurarsi che NepenthesFE sia in modalità debug e controllare i log. Se è presente il messaggio

```
[warning] Authentication failed for client 127.0.0.1 with username
```

procedere come segue.

1. assicurarsi che l'IP usato nella linea di cron (/etc/crontab) sia lo stesso inserito in NepenthesFE.
2. eventualmente sostituire wget con curl .

9 A quali sandbox faccio inviare i binari?

Esistono diversi servizi per l'analisi dei malware raccolti. Questi servizi usano delle sandbox per eseguire i binari e tracciarne l'esecuzione. Alcune sandbox sono anche in grado di salvare il traffico generato su rete dai malware analizzati. Seguono gli URL da aggiungere al proprio submit-http per la sottomissione a diverse sandbox:

- Anubis: http://anubis.iseclab.org/nepenthes_action.php.
- CWSandbox:
<http://luigi.informatik.uni-mannheim.de/submit.php?action=verify>.
- Joebox: <http://analysis.joebox.org/submit>.

10 Funziona l'invio a NormanSandbox?

Al momento non più. Se si usa SurfIDS, Alberto Fontanella ha sviluppato un plug-in che permette l'invio dei binari a NormanSandbox e integra i report ricevuti con l'interfaccia di SurfIDS.

11 È possibile usare Nepenthes come un sottosistema di Honeyd?

Dovrebbe, ma al momento non sembra funzionare:

http://nepenthes.carnivore.it/howto:run_nepenthes_as_honeyd_subsystem

12 Cos'è e a cosa serve module-portwatch?

È un modulo il cui compito è solo creare i log delle richieste che arrivano alle varie porte; utili per poi scrivere dei nuovi moduli relativi alle vulnerabilità, in base ai dati raccolti.

13 Nepenthes riesce a gestire exploit 0day?

No, Nepenthes è progettato per gestire solo ciò che conosce. Infatti, riesce a gestire solo gli exploit per cui ha un modulo. Questo non significa che cattura solo i malware che conosce ma solo i malware che lanciano exploit gestibili. Quando arriva uno shellcode non gestibile, sulle porte su cui c'è un modulo in ascolto, Nepenthes crea un log dell'evento e salva l'hexdump della comunicazione. Tramite l'hexdump sarà poi possibile sviluppare un nuovo modulo per emulare la vulnerabilità. Per le porte dove non è in ascolto un modulo, non verrà creato nessun hexdump. Per tracciare l'attività su tali porte si potrà ricorrere all'uso del modulo portwatch.

14 Nepenthes riceve soprattutto attacchi che sfruttano la dcom, come mai?

Sicuramente questo fenomeno è in parte imputabile alla sinteticità di Nepenthes. Molti degli attacchi che arrivano non vengono considerati tali perchè non gestiti correttamente dai moduli delle vulnerabilità o per la completa assenza di un modulo funzionante per quella specifica vulnerabilità.

15 Non sono presenti binari in /var/binaries/, come posso verificare che tutto stia funzionando?

Si verifichi in /etc/nepenthes/submit-file.conf qual'è la directory dove verranno salvati i binari catturati e si verifichi che Nepenthes abbia i permessi per compiere tale operazione. Si può inoltre controllare i log di Nepenthes (/var/log/nepenthes.*) e verificare se sono stati ricevuti attacchi e se è avvenuto il download di binari.

16 È utile posizionare Nepenthes in una LAN? Perché?

Si. Ad esempio, per misurare il livello di infezione degli host in una LAN, capire quali sono quelli infetti e da che cosa. Ovviamente se l'obiettivo è catturare binari, è preferibile il posizionamento in Internet.

17 Quali porte apre Nepenthes?

L'installazione di default su Debian 4 emula vulnerabilità sulle porte: 21, 25, 42, 80, 110, 135, 139, 143, 220, 443, 445, 465, 993, 995, 1023, 1025, 1423, 2103, 2105, 2107, 2745, 3127, 3140, 3372, 5000, 5554, 6129, 10000, 17300, 27347.

18 Posso partecipare attivamente con la mia installazione di Nepenthes a Mwcollect?

Sì, teoricamente. Ci sono dei requisiti da soddisfare (https://alliance.mwcollect.org/public/join_requirements). È noto che Mwcollect sia particolarmente attenta nella scelta delle collaborazioni.

19 Esistono dei software simili a Nepenthes?

Sì. Un software che fa lo stesso mestiere di Nepenthes è **Amun**, un honeypot scritto in Python.