

Herramientas anti-malware y anti-rootkit



Para LINUX

Chkrootkit

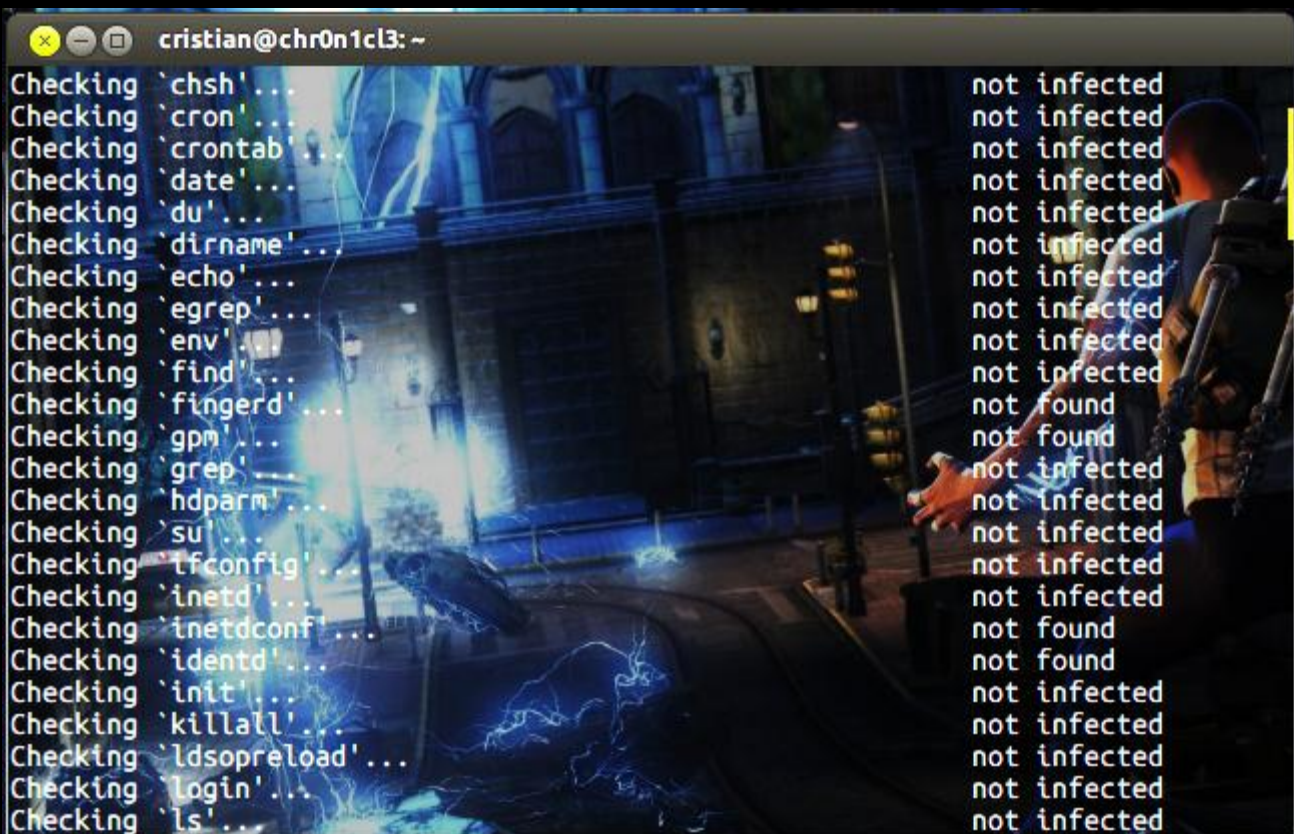
Chkrootkit o Check Rootkit es un programa famoso de código abierto, es una herramienta que se utiliza para la digitalización de rootkits, botnets, malwares, etc en tu servidor o sistema Unix/Linux. Está probado en: Linux 2.0.x, 2.2.x, 2.4.x, 2.6.x, y 3.xx, FreeBSD 2.2.x, 3.x, 4.x, 5.xy 7.x, OpenBSD 2.x, 3.xy 4.x, 1.6.x NetBSD, Solaris 2.5.1, 2.6, 8.0 y 9.0, HP-UX 11, Tru64, BSDI y Mac OS X. Esta herramienta está preinstalada en BackTrack 5 en la parte de Herramientas forenses y anti-Virus.

Para instalar chkrootkit en una distro basada en Ubuntu o Debian, puede teclear:

```
~$ sudo apt-get install chkrootkit
```

Para comenzar a comprobar las posibles rootkits y puertas traseras en el sistema, escriba el comando:

```
~$ sudo chkrootkit
```



```
cristian@chr0n1cl3: ~
Checking chsh' ... not infected
Checking cron' ... not infected
Checking crontab' ... not infected
Checking date' ... not infected
Checking du' ... not infected
Checking dirname' ... not infected
Checking echo' ... not infected
Checking egrep' ... not infected
Checking env' ... not infected
Checking find' ... not infected
Checking fingerd' ... not found
Checking gpm' ... not found
Checking grep' ... not infected
Checking hdpam' ... not infected
Checking su' ... not infected
Checking tfconfig' ... not infected
Checking inetd' ... not infected
Checking inetdconf' ... not found
Checking identd' ... not found
Checking init' ... not infected
Checking killall' ... not infected
Checking ldsopreload' ... not infected
Checking login' ... not infected
Checking ls' ... not infected
```

Rootkit Hunter

Rootkit Hunter o rkhunter es un código abierto Licencia Pública General (GPL) Rootkit escáner similar a chkrootkit que está también pre-instalado en BackTrack 5 en Herramientas Forenses y Anti-Virus. Esta herramienta analiza en busca de rootkits, backdoors y exploits locales mediante la ejecución de pruebas como: MD5 hash de comparar, buscar archivos predeterminados utilizados por rootkits, permisos de archivo incorrectos para archivos binarios, buscar sospechosos cadenas en módulos LKM y KLD, buscar archivos ocultos, y opcionales escanear dentro de archivos de texto y binarios.

Para instalar rkhunter en una distro basada en Ubuntu o Debian, puede teclear:

```
~$ sudo apt-get install rkhunter
```

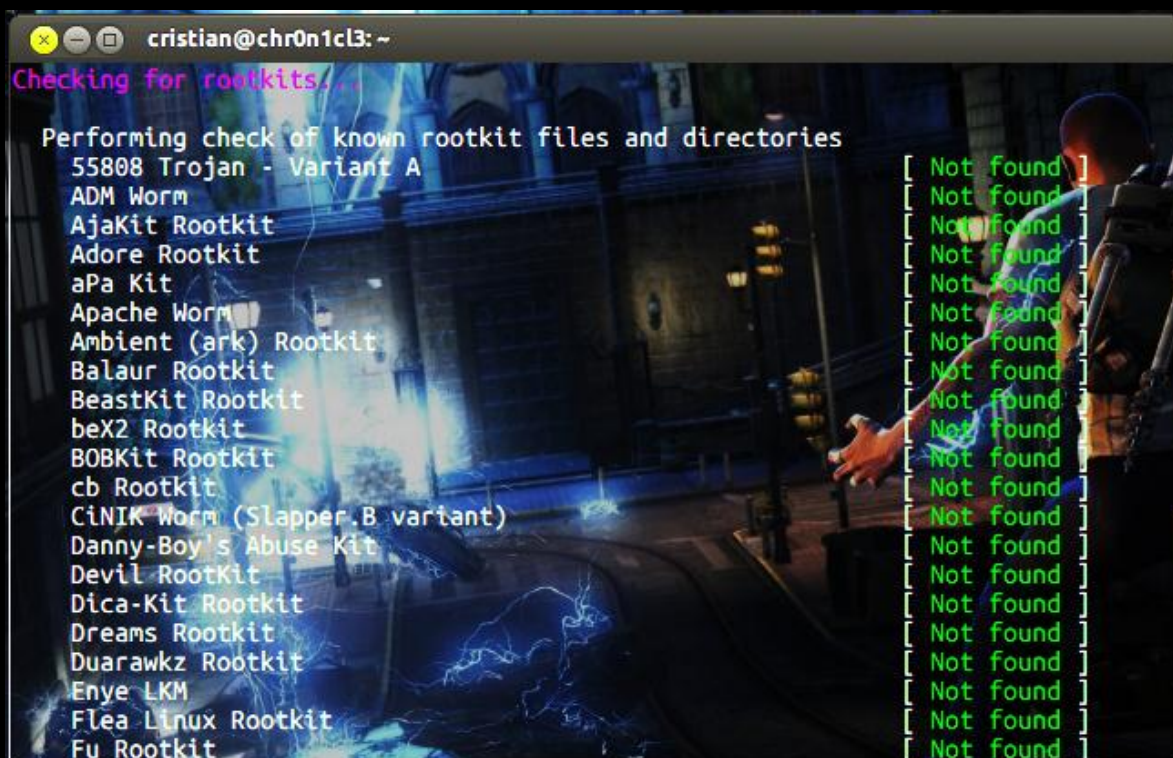
Para iniciar el análisis del sistema de archivos, escriba el comando:

```
~$ sudo rkhunter -check
```

Y si quieres comprobar si hay actualizaciones, ejecute el comando:

```
~$ sudo rkhunter -update
```

Después que rkhunter ha terminado de escanear su sistema de archivos, todos los resultados se registran en (/var/log/rkhunter.log)



```
cristian@chr0n1cl3: ~
Checking for rootkits...
Performing check of known rootkit files and directories
55808 Trojan - Variant A [ Not found ]
ADM Worm [ Not found ]
AjaKit Rootkit [ Not found ]
Adore Rootkit [ Not found ]
aPa Kit [ Not found ]
Apache Worm [ Not found ]
Ambient (ark) Rootkit [ Not found ]
Balaur Rootkit [ Not found ]
BeastKit Rootkit [ Not found ]
bex2 Rootkit [ Not found ]
BOBKit Rootkit [ Not found ]
cb Rootkit [ Not found ]
CiNIK Worm (Slapper.B variant) [ Not found ]
Danny-Boy's Abuse Kit [ Not found ]
Devil RootKit [ Not found ]
Dica-Kit Rootkit [ Not found ]
Dreams Rootkit [ Not found ]
Duarawkz Rootkit [ Not found ]
Enye LKM [ Not found ]
Flea Linux Rootkit [ Not found ]
Fu Rootkit [ Not found ]
```

ClamAV

ClamAV es un conocido software anti-virus en Linux. Es el más famoso antivirus de Linux que tiene una versión de interfaz gráfica de usuario diseñada para una detección más fácil de trojanos, virus, malware y otras amenazas maliciosas. ClamAV también se puede instalar en Windows, BSD, Solaris e incluso en MacOSX. El becario investigador de seguridad Dejan de Lucas tiene un [tutorial](#) detallado en la página del Instituto de Recursos de InfoSec sobre cómo instalar ClamAV y cómo trabajar con su interfaz en la línea de comandos.

BotHunter

BotHunter es un sistema basado en el diagnóstico de red botnet que sigue el camino de dos flujos de comunicación entre el ordenador personal e Internet. Es desarrollado y mantenido por el Computer Science Laboratory, SRI International, y está disponible para Linux y Unix, pero ahora han lanzado una versión de prueba privada y un pre-lanzamiento para Windows.

Si deseas descargar este programa podrás hacerlo desde [aquí](#) . También puede utilizar su addon llamado [BotHunter2Web.pl](#) . Este addon convierte perfiles de infección BotHunter en las páginas web, que se pueden ver a través de tu navegador directamente o a través de un servidor web privado. Los perfiles de infección BotHunter se encuentran normalmente en `~ cta-bh/BotHunter/LIVEPIPE/botHunterResults.txt`.

Ejemplo de uso para BotHunter2Web.pl:

```
~$ perl BotHunter2Web.pl [fecha AAAA-MM-DD]-i sampleresults.txt
```

avast! Linux Home Edition

avast! Linux Home Edition es un motor antivirus ofrecido en forma gratuita, pero sólo para el hogar y no para uso comercial. Incluye un escáner de línea de comandos y en base a la experiencia del autor de la nota original, detecta algunos de los bots de Perl IRC que contiene funciones maliciosas como las funciones udpflood y tcpflood, y permite a su master o controlador del bot para ejecutar comandos arbitrarios con el uso de la función system() para Perl.

Te puedes descargar este software antivirus [aquí](#) .

NeoPI

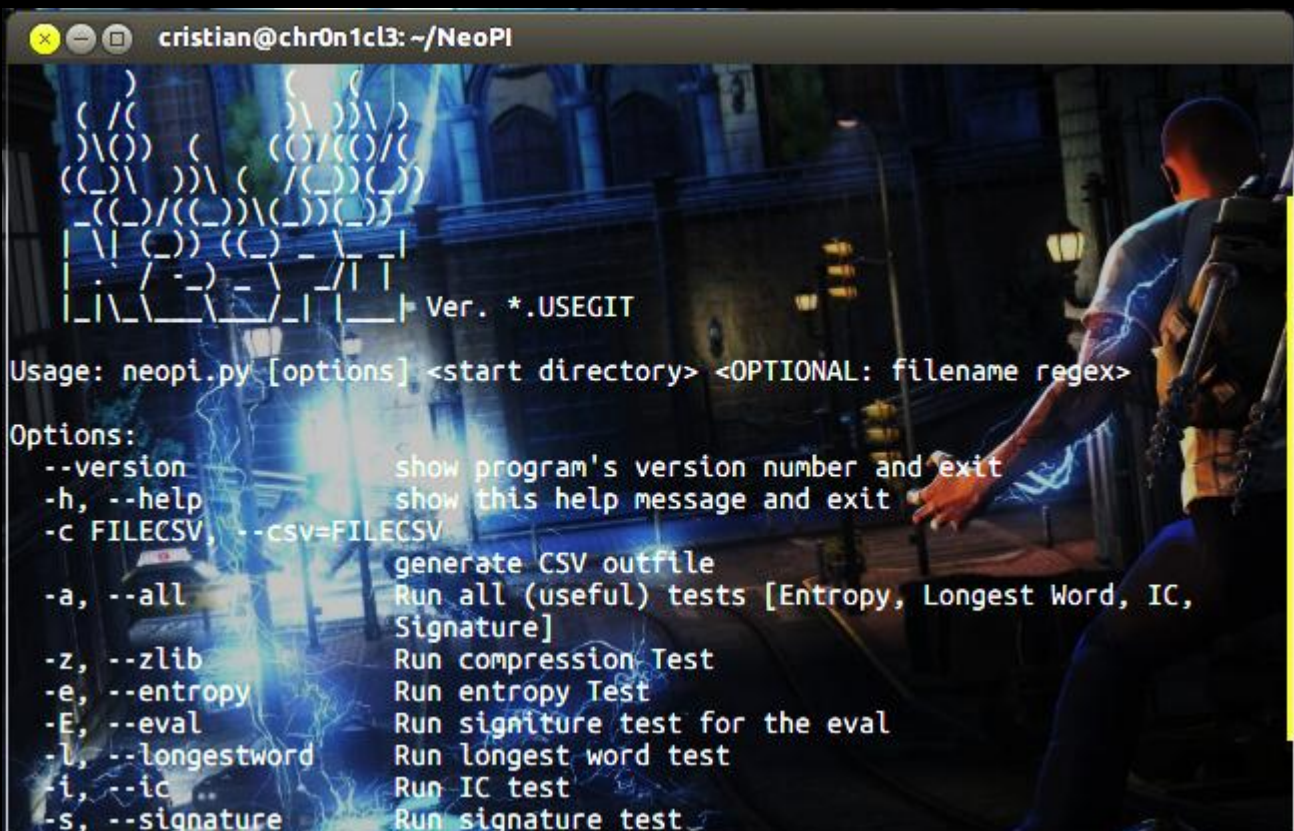
NeoPI es un script en Python útil para la detección de contenido corrupto y cifrado dentro de archivos de texto o scripts. La finalidad de NeoPI es ayudar en la detección de código oculto en shell web. El enfoque de desarrollo de NeoPI fue la creación de una herramienta que puede ser utilizada en combinación con otros métodos de detección comunes basados ??en firmas o palabras claves. Se trata de un script multiplataforma para Windows y Linux. No sólo ayuda a los usuarios a detectar posibles puertas traseras, sino también scripts maliciosos como botnets IRC, shells udpflood, scripts vulnerables, y herramientas maliciosas.

Para utilizar esta secuencia de comandos de Python, simplemente hay que descargar el código en su sitio oficial github y navegar a través de su directorio:

```
~$ git clone https://github.com/Neohapsis/NeoPI.git
~$ cd NeoPI
```

A continuación, se utiliza el indicador-h para ver las opciones para ejecutar el script:

```
~$ sudo ./neopi.py -h
```



```
cristian@chr0n1c13: ~/NeoPI
(
  )
  (/
  )\() ( (O/O/O/
  ((\ )\ ( /()()
  -(/(/)\()()
  | \() ( - \ - |
  | / - - \ - |
  | \ \ \ \ \ \ \ | | | Ver. *.USEGIT

Usage: neopi.py [options] <start directory> <OPTIONAL: filename regex>

Options:
--version      show program's version number and exit
-h, --help    show this help message and exit
-c FILECSV, --csv=FILECSV
              generate CSV outfile
-a, --all     Run all (useful) tests [Entropy, Longest Word, IC,
              Signature]
-z, --zlib    Run compression Test
-e, --entropy Run entropy Test
-E, --eval    Run signiture test for the eval
-l, --longestword Run longest word test
-i, --ic      Run IC test
-s, --signature Run signature test
```

Ourmon

Ourmon es un programa basado en Unix de código abierto y una herramienta de paquetes de red común sniffendo en FreeBSD, pero también puede ser utilizado para la detección de botnets como explica Ashis Dash en su artículo titulado '[Herramienta de detección de botnets: Ourmon](#)' en la revista Clubhack o Chmag.

Grep

Y el último, pero no menos importante, tenemos el comando grep, que es una poderosa herramienta de línea de comandos en Unix y Linux. Se utiliza para buscar y probar conjuntos de datos de sondeo para las líneas que coinciden con una expresión regular. Haciéndola corta, esta utilidad fue codificada por Ken Thompson el 3 de marzo de 1973 para Unix. Hoy en día, Grep es conocido para la detección y búsqueda de molestas shells de puerta trasera y también scripts maliciosos.

Grep también se puede utilizar para la detección de secuencias de comandos vulnerables (por ejemplo, la función shell_exec de PHP que es una función riesgosa de PHP que permite la ejecución remota de código o comando de ejecución). Podemos usar el comando grep para buscar el shell_exec() como ventaja en nuestro directorio /var/www para comprobar posibles archivos PHP vulnerables a ICE o la inyección de comandos. Aquí está el comando:

```
~$ grep -Rn "shell_exec *( " /var/www
```

Grep es una buena herramienta para detección manual y análisis forense.