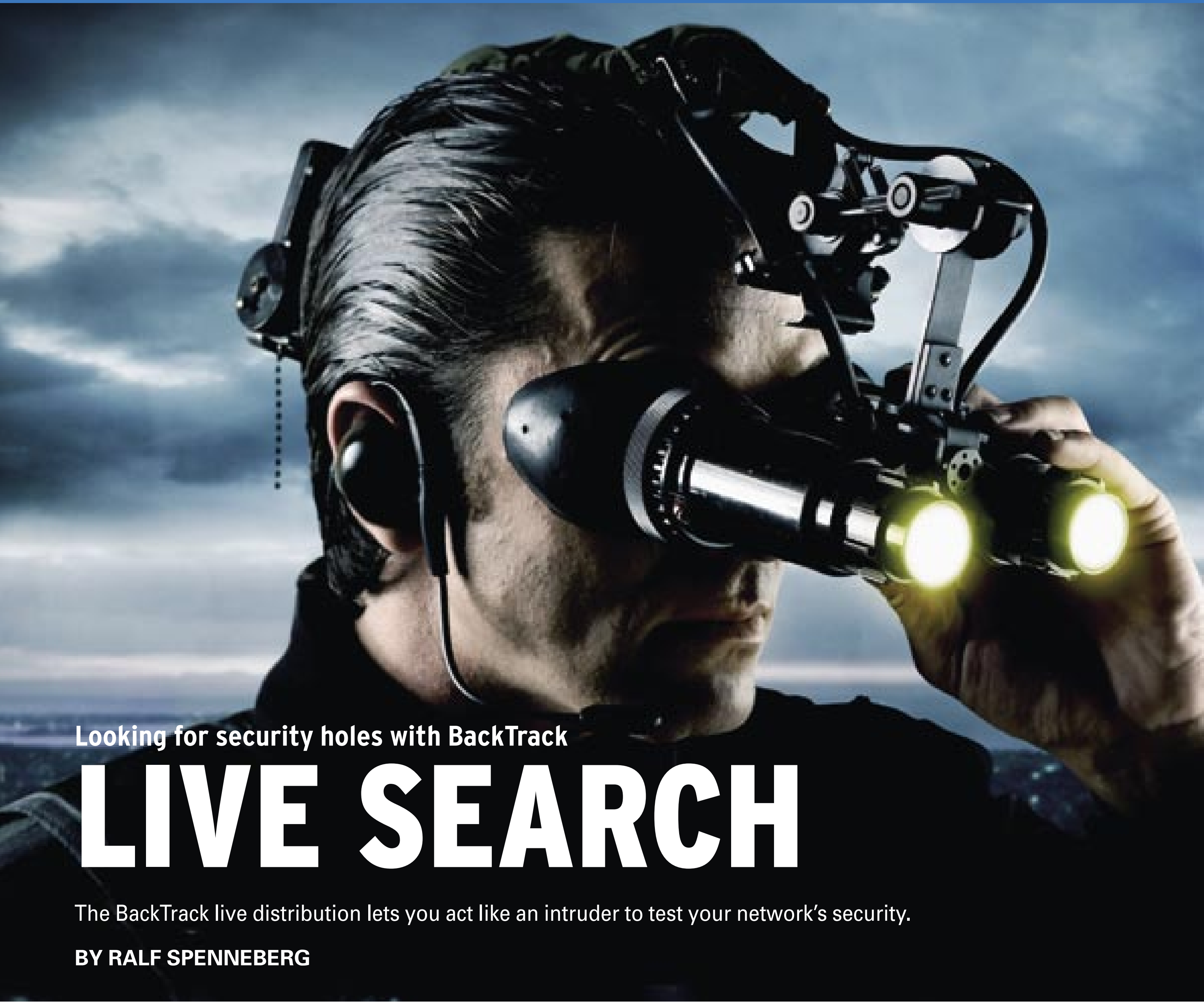


Looking for security holes with BackTrack

LIVE SEARCH

The BackTrack live distribution lets you act like an intruder to test your network's security.

BY RALF SPENNEBERG

Penetration testing is the art of breaking into your own network. Security consultants and system administrators use penetration testing todiscover holes before an intruder can find them. Unfortunately, intruders use a vast collection of powerful tools for sniffing, snooping, cracking, and hiding out on a target network.

If you want to simulate an attack, you could always download this large collection of applications and temporarily install them on whatever system you plan to use for the attack. However, searching for the right tools and then installing them on your system can take up hours or even days of your time.

A number of Linux distributions are designed to support penetration testing. Two of the most popular security testing distributions (Auditor and Whax) merged early this year to create the BackTrack distribution.

BackTrack [1] is based on the Slackware Live CD, Slax [2].

In addition to the many intrusion tools, BackTrack also includes a large selection of applications for investigating and uncovering signs of clandestine entry.

You can obtain BackTrack from the project website [1]. Or, if you have a copy of last month's Linux Magazine (March 2007), you'll find BackTrack on the Best of Live Distros DVD. This article will show you how to

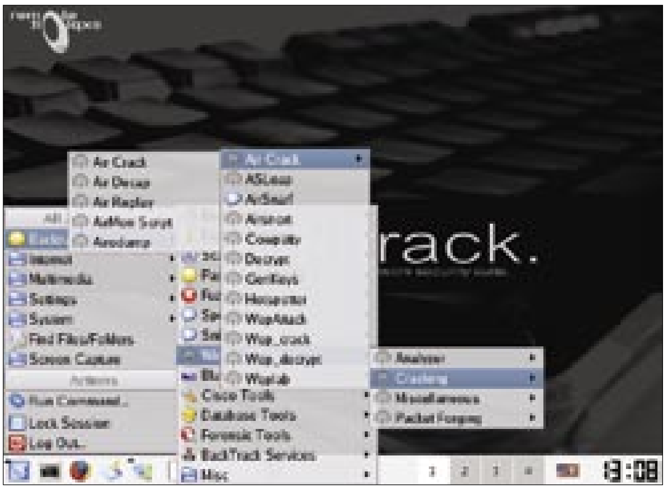
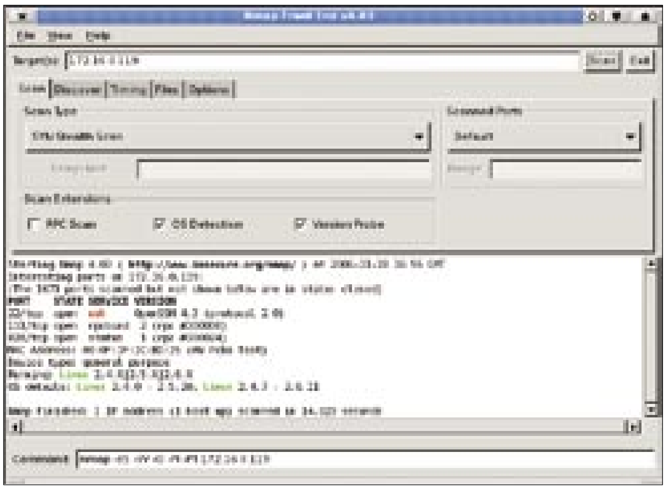


Figure 1: The KDE desktop lets admins easily navigate BackTrack's huge collection of programs.

get started with BackTrack, and it also provides a glimpse of the many tools that are included on the BackTrack CD.

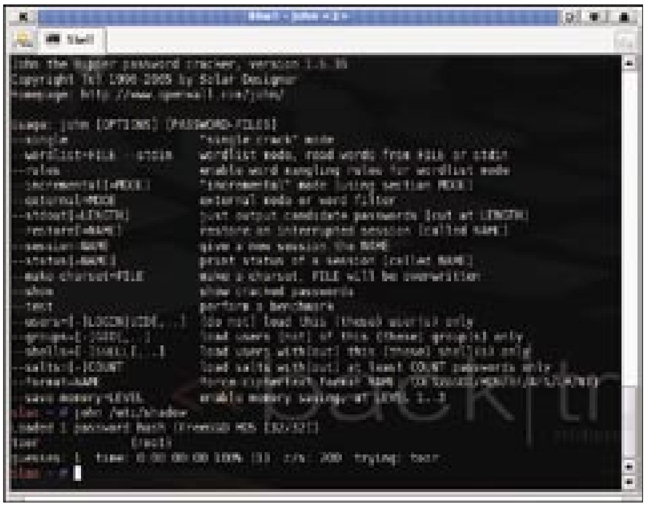


```
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-11-20 16:56 CET
Interesting ports on 172.16.0.119:
(The 1673 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh      OpenSSH 4.2 (protocol 2.0)
111/tcp open  rpcbind  2 (rpc #100000)
826/tcp open  status   1 (rpc #100024)
MAC Address: 00:0F:1F:1C:8D:75 (WW Pcba Tech)
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.7 - 2.6.11

Nmap finished: 1 IP address (1 host up) scanned in 16.123 seconds
```

Command: nmap -sS -sV -O -PI -PT 172.16.0.119

Figure 2: NMapFE supports easy scanning; the tool is based on the popular NMap program.



```
John the Ripper password cracker, version 1.6.38
Copyright (c) 1996-2005 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test                    perform a benchmark
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]COUNT          load salts with[out] at least COUNT passwords only
--format=NAME             force ciphertext format NAME (DES/BSDI/MD5/BF/AFS/LM/NT)
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
slax ~ # john /etc/shadow
Loaded 1 password hash (FreeBSD MD5 [32/32])
toor             (root)
guesses: 1  time: 0:00:00:00 100% (1)  c/s: 200  trying: toor
slax ~ #
```

Figure 3: john lets admins test the strength of passwords. toor was cracked in a single round of guessing.

Getting Started

BackTrack comes as a live CD, so to run it, you simply need to insert it in the CD drive and then boot the system. At the prompt, log on as root and then enter the root password *toor* before going on to set up the GUI with *xconf*.

After you have completed the setup, simply type *startx* to launch the GUI.

If an error occurs, try *gui* as a workaround for launching the graphical interface.

If you need to, you can type *dhcpcd* to ask the DHCP server for an IP address. BackTrack does not do this automatically.

BackTrack's KDE-based menu system provides access to dozens of security tools and other forensic-analysis applications (see Figure 1).

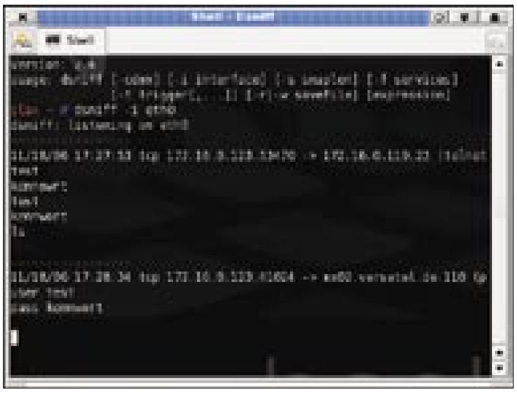
Browsing the BackTrack menu is a little like browsing the many menus and submenus of a games distribution; only, instead of a bunch of games, the GUI is stocked with sniffers, spoofers, scanners, and other utilities to assist you with security testing.

The tools are organized by group:

- Enumeration
- Exploit Archives
- Scanner
- Password Attacks
- Fuzzer
- Spoofing
- Sniffers
- Wireless Tools
- Bluetooth
- Cisco Tools
- Database Tools
- Forensic Tools

BackTrack's security tools will give system administrators everything they need in order to hunt down their security holes.

The following sections will describe just a sampling of some of the tools that are available on the BackTrack CD.



```
Version: 2.4
Usage: dsniff [-cdmn] [-i interface] [-s snaplen] [-f services]
              [-t trigger[,...]] [-r|-w savefile] [expression]
slax ~ # dsniff -i eth0
dsniff: listening on eth0
-----------------
11/18/06 17:27:53 tcp 172.16.0.110.33470 -> 172.16.0.119.23 (telnet)
test
Kennwort
test
Kennwort
ls

-----------------
11/18/06 17:28:34 tcp 172.16.0.110.41024 -> xx60.versatel.de.110 (pop)
USER test
PASS Kennwort
```

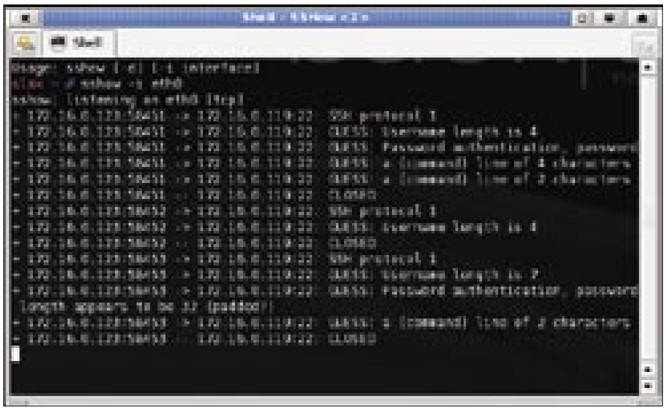
Figure 4: DSniff identifies user passwords transmitted by clear-text protocols.

Enumeration

Security analysis normally starts with an inventory of the computers, operating systems, and network services.

The *Enumeration* menu provides some popular port scanners, such as NMap and the NMapFE, in addition to SNMP analysis tools and tools for accessing LDAP servers and Windows SMB shares.

Submenus contain scanners for special protocols. For example, Nikto scans and analyzes web servers, while IKE Scan and IKEProbe help administrators analyze their virtual private networks (VPNs). After ascertaining the operating systems and services on the network, you can move on and search for matching exploits in three major vulnerability and exploit archives: Milw0rm [3], Metasploit [4], and Securityfocus [5].



```
Usage: sshow [-d] [-i interface]
slax ~ # sshow -i eth0
sshow: listening on eth0 [tcp]
+ 172.16.0.123:58451 -> 172.16.0.119:22  SSH protocol 1
+ 172.16.0.123:58451 -> 172.16.0.119:22  GUESS: Username length is 4
+ 172.16.0.123:58451 -> 172.16.0.119:22  GUESS: Password authentication, password
+ 172.16.0.123:58451 -> 172.16.0.119:22  GUESS: a (command) line of 4 characters
+ 172.16.0.123:58451 -> 172.16.0.119:22  GUESS: a (command) line of 2 characters
+ 172.16.0.123:58451 -- 172.16.0.119:22  CLOSED
+ 172.16.0.123:58452 -> 172.16.0.119:22  SSH protocol 1
+ 172.16.0.123:58452 -> 172.16.0.119:22  GUESS: Username length is 4
+ 172.16.0.123:58452 -- 172.16.0.119:22  CLOSED
+ 172.16.0.123:58453 -> 172.16.0.119:22  SSH protocol 1
+ 172.16.0.123:58453 -> 172.16.0.119:22  GUESS: Username length is 7
+ 172.16.0.123:58453 -> 172.16.0.119:22  GUESS: Password authentication, password
 length appears to be 32 (padded)
+ 172.16.0.123:58453 -> 172.16.0.119:22  GUESS: a (command) line of 2 characters
+ 172.16.0.123:58453 -- 172.16.0.119:22  CLOSED
```

Figure 5: sshow exploits weaknesses in the SSH protocol and calculates the length of the username, the password, and the commands entered in the session.

If you need to crack password-protected services or find out how robust your passwords are, BackTrack offers a variety of tools for password attacks.

In addition to the classic *john* cracker, which will have no trouble finding the root password (see Figure 3), you'll find a number of other tools for offline cracking of encrypted passwords or online password guessing.

Sniffing

Sniffers help network administrators scan their networks and test for secure protocols. BackTrack has a number of useful helpers, including the classic Ethereal, Etherape, Driftnet, and DSniff (see Figure 4), along with many other helpful sniffers.

It is even possible to crack SSH connections with BackTrack. *sshow* and *sshmitm* attack the SSH connections that use version 1 of the SSH protocol (see Figure 5).

Administrators can run *sshmitm* to launch a Man-in-the-Middle attack on an SSH connection.

To use sniffers on switched networks or to run *sshmitm* for a Man-in-the-Middle exploit, admins will also need spoofing tools. *arpspoof* or *macof* support sniffing on switched networks.

While *macof* generates much conspicuous network traffic, *arpspoof* is a tool that is very difficult to detect.

arpspoof attacks the ARP cache on the target systems, tricking the system into delivering packets to the sniffer via the switch. This is achieved by poisoning the ARP cache on the victim machines. (For more information on ARP spoofing, see the resources [6] [7].)

Wireless

BackTrack also comes with a number of very useful tools for testing the WLAN and the Bluetooth networks.

Besides Kismet, the collection of tools includes Aircrack, Airsnort, WEPAttack, and WEP_crack.

Of course, the administrative workstation will need a WLAN interface to run these tools.

BackTrack supports common Bluetooth attack scenarios.

Besides legacy exploit tools for Bluetooth networks – for finding vulnerable mobile phones, for example – the distribution also has auditing tools for help with identifying Bluetooth devices in the vicinity.

Web Servers and Databases

Because attacks today increasingly tend to target web applications and the underlying databases, the BackTrack distribution also has a number of programs that can help administrators with analyzing web applications and the database systems.

For example, *curl* supports script-based access to web servers; DMitry and HTTPrint will serve up useful information about web servers and domains (see Figure 6).

If the web server is not configured correctly, *httpput* will support file uploads; *list-urls* extracts all the URLs from a website, and *isr-form.pl* analyzes the HTML forms.

Last but not least, Nikto will analyze a web server to discover the known vulnerabilities.

The Paros penetration proxy gives the system administrator the ability to modify HTTP requests before sending them to the web server. In this way, hidden fields in HTML forms and cookies can be manipulated to work around Javascript plausibility tests for form input.

BackTrack also has automatic blind SQL injection scripts and brute-force password crackers for database analysis. Tools such as Absinthe (see Figure 7) provide automatic mechanisms to simplify the analysis process.

Cisco: A Special Case

The BackTrack developers also provide tools for analyzing Cisco network devices. First and foremost, there are two tools that exploit known vulnerabilities in Cisco devices: Cisco Global Exploiter, and Yersinia.

Yersinia is particularly interesting because it attacks Cisco's proprietary Layer 2 protocols to enable VLAN hopping.

System administrators can use the Yersinia tool to reprogram the port used by the current connection to make the connection part of a different VLAN. However, as VLANs are often used to separate networks for security reasons, this can be very dangerous.

In (all too) many environments, the people in charge do not pay enough at-

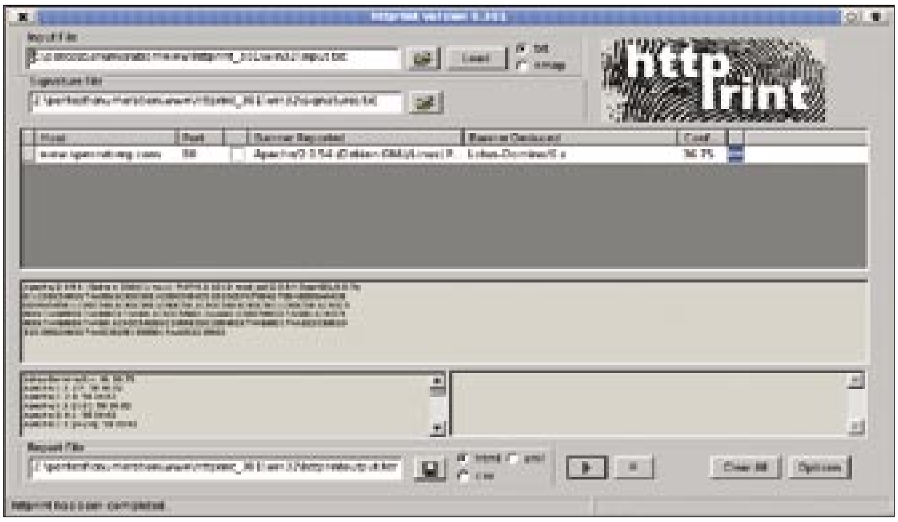


Figure 6: httprint can reveal the web server software for an application server.

tention to their switches; therefore, Yersinia exploits work more often than you might expect them to.

The Cisco vulnerability scanner, Cisco Torch, helps system administrators close the gaps.

BackTrack is also useful for forensic analysis of systems after a suspected compromise. The forensic team includes the tried-and-trusted Sleuthkit and Autopsy tools, versions 2.03 and 2.06, respectively.

The Foremost [8] tool helps analysts identify and restore deleted files purely based on their content. This is what forensics specialists refer to as file carving.

Miscellaneous

In addition to penetration, scanning, and forensics tools, BackTrack has a number of interesting tunneling applications.

SSLTunnel encrypts arbitrary TCP connections, NSTX or OzymanDNS set up tunnels via the DNS protocol using mandatory caching name servers as proxies.

You'll also find a special Hijetter tool for Jetdirect printers. The Hijetter tool gives the user access to variables, the display, and also to the filesystem.

Documentation is another important consideration in any penetration test. The BackTrack distribution includes the revolutionary Leo [9] editor.

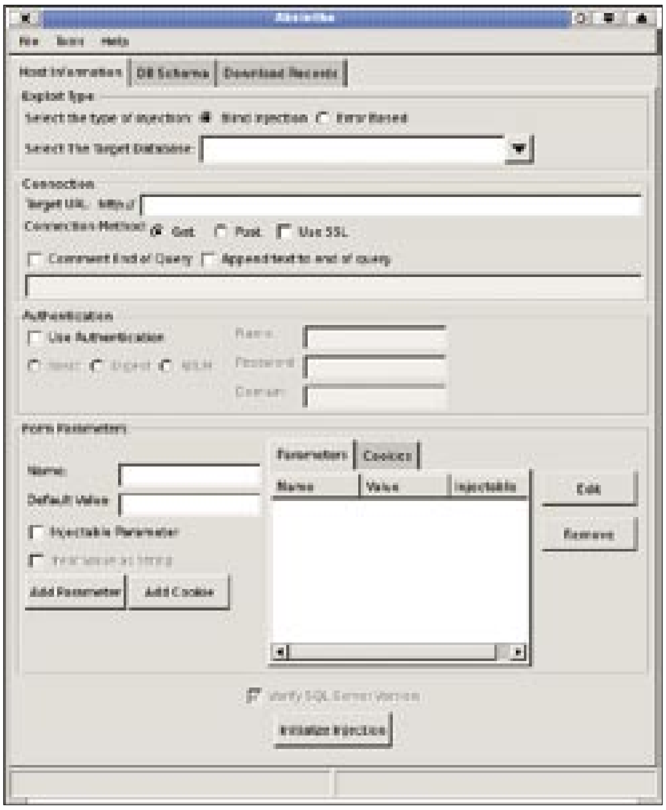


Figure 7: Absinthe makes child's play of SQL injection.

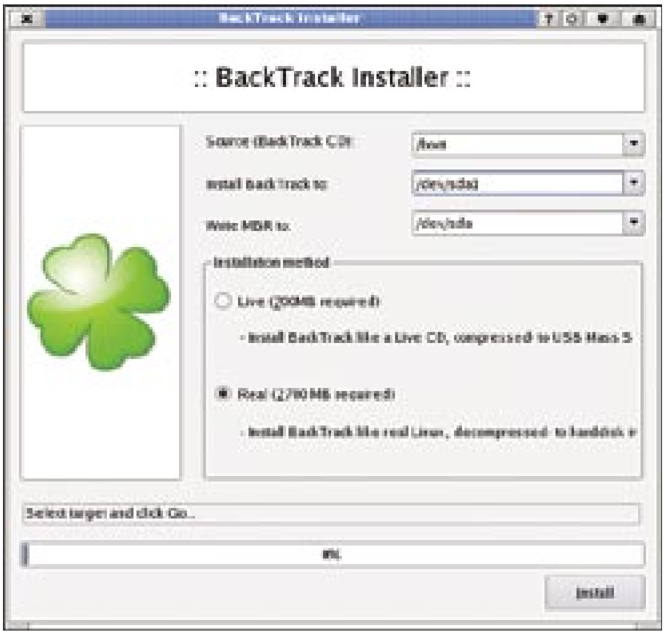
The Leo editor has a very intelligent outline mode, featuring the ability to launch scripts directly within a document. The Leo editor also supports intelligent access to the integrated file browser.

Because Leo is written in Python, system administrators can use the browser to write their own Python scripts or even use it to write very simple plugins.

For Ever and Ever

If you enjoy the experience of working with BackTrack, you might like to have the abilty to save data or update the applications. If this is the case, you can install BackTrack on a hard disk or on a USB stick.

To do so, just select *BackTrack Installer* in the *System* menu (see Figure 8).



Source (BackTrack CD): /boot

Install BackTrack to: /dev/sda1

Write MBR to: /dev/sda

○ Live (700MB required)
- Install BackTrack like a Live CD, compressed to USB Mass S

● Real (2700 MB required)
- Install BackTrack like real Linux, decompressed to harddisk e

Select target and click Go..

0%

Figure 8: Run the installer to install BackTrack on your disk.

After selecting the target medium, you will also need to decide whether to install a live version (700 MB) or else opt for a genuine Linux system (2.7 GB).

Opt for the genuine Linux system option if you really want to update applications and also to store your data.

Conclusions

The BackTrack distribution is something no system administrator's toolbox should be without. The BackTrack distribution provides sysadmins with everything necessary to test the security posture of a network.

The BackTrack distribution developers are currently working on version 2.0, which will include updates to many of the the BackTrack tool collection. Other changes in the new version include aufs with zlib compression instead of UnionFS, dual core support, and new tools like defcon, blackhat, and packetstorm. New features include network boot and cracking cluster support. A beta version of BackTrack 2.0 is on the BackTrack site [1]. ■

INFO

[1] BackTrack: *http://www.remote-exploit.org*

[2] Slax: *http://www.slax.org*

[3] Milw0rm: *http://www.milw0rm.com*

[4] Metasploit: *http://www.metasploit.org*

[5] Securityfocus: *http://www.securityfocus.com*

[6] ARP spoofing: *http://de.wikipedia.org/wiki/ARP-Spoofing*

[7] "Traffic Tricks: ARP Spoofing and Poisoning," by Thomas Demuth and Achim Leitner, Linux Magazine July, 2005; *http://www.linux-magazine.com/issue/56/ARP_Spoofing.pdf*

[8] Foremost: *http://foremost.sourceforge.net*

[9] Leo: *http://webpages.charter.net/edreamleo/*