Setting Up BackTrack

And automating various tasks with bash scripts

by

Lee Baird

Lee Baird

- Malware analysis
- Enterprise security assessments for Fortune 500
- Computer network exploitation
- Wireless
- Social engineering
- Physical

Overview

- What is BackTrack?
- Setting up your virtual machine
- Information gathering
- Nmap
- Metasploit
- Automation with bash scripts

What is BackTrack?

- Linux-based security distro
- Contains many tools used for security assessments
- 32 and 64-bit
- Gnome and KDE environment
- Bare metal, live DVD, USB thumb drive or VM
- Free!

Where can I find it?

- www.backtrack-linux.org
- Downloads
- How To
- Forums
- Wiki
- Training through Offensive Security

Setting up a VM

- Latest version is BackTrack 5 R3
- Choose your environment and download
- VMware version, 32-bit Gnome ~ 2 GB in size
- OS X – VMware Fusion 4 or 5
- Windows – VMware Workstation 8 or 9
- 1 to 4 GB of RAM

Setting up a VM

- Expand BT5R2-GNOME-VM-32.7z
- File > Open > BT5R2-GNOME-VM-32.vmx > Open
- Play > I copied it
- Login with default account: root - toor
- Change the root password: passwd
- Fix the splash screen: fix-splash

Setting up a VM

- Reboot: reboot
- Login with new password
- Start the GUI: startx
- Take a snapshot

Install VMware Tools

- Open a Terminal: prepare-kernel-sources
- On VMware, Virtual Machine > Install VMware Tools > Install
- mkdir /mnt/cdrom; mount /dev/cdrom /mnt/cdrom
- cp /mnt/cdrom/VMwareTools-<version>.tar.gz /tmp/
- cd /tmp/

Install VMware Tools

- tar zxpf VMwareTools-<version>.tar.gz
- cd vmware-tools-distrib/
- ./vmware-install.pl
- Accept all the defaults.
- reboot
- Enjoy cut, copy and paste between host and VM

Terminal

- Where you will spend most of your time
- Edit > Profile Preferences
- General > Monospace 13
- Color > Text color > white
- Background > Transparent background > Maximum
- Scrolling > Unlimited *

gedit

- Text based editor
- Edit > Preferences
- Display line numbers
- Highlight current line
- Editor > Tab width 5, Insert spaces instead of tabs
- Font & Colors > Monospace 12, Oblivion

Auto Login

- apt-get install rungetty
- nano /etc/init/tty1.conf
- #exec /sbin/getty -8 38400 tty1
- exec /sbin/rungetty tty1 --autologin root
- echo startx > .bash_profile
- reboot

Firefox

- Help > About Firefox > Check for Updates
- Plug-ins: Firebug, Tamper Data, Web Developer
- Metasploit https://localhost:3790
- Nessus https://localhost:8834
- NeXpose https://localhost:3780
- NSEDoc http://nmap.org/nsedoc/

Scripts

- svn co https://backtrack-scripts.googlecode.com/svn/ /opt/scripts
- chmod 755 /opt/scripts/ -R
- cd /opt/scripts/
- ./setup.sh

setup.sh

- Create SSH keys
- Sets up aliases
- Installs Filezilla
- Installs xdotool

svn and github

- dnsrecon
- theHarvester
- jigsaw
- Metasploit
- Nmap
- sqlmap

Aliases – Short Cuts

- c clear
- l ls –l
- cl clear & ls -l
- e exit
- r cd /root/ & clear
- s cd /opt/scripts/ & clear

Aliases - Networking

- i ifconfig && ping –c3 google.com
- n netstat –antup

  Interface

  Mac address

  Internal IP

  External IP

Alias - Misc

- sip correctly sort a list of IP addresses

sort hosts.txt	sip hosts.txt
10.0.0.1	10.0.0.1
10.0.0.10	10.0.0.2
10.0.0.2	10.0.0.10
10.0.0.200	10.0.0.200

Alias - update

- date & time
- BackTrack distro
- aircrack-ng
- dnsrecon
- exploit-db
- GISKismet
- theHarvester
- Jigsaw
- Metasploit
- Nikto
- Nmap
- scripts
- SET
- sqlmap
- w3af

Recon

- Black box engagement
- Social engineering
- What kind of intel do I need?
- Where can I find it?
- script - Open source intelligence gathering
- script - Scrape

Company

- Downloads info from DeepMagic, IntoDNS and Robtex.
- /root/recon/

  dns-health.html

  dns.html

  ptr-records.txt
- Open multiple tabs in Firefox with various URLs

Company

- ARIN
- IPinfoDb
- Netcraft
- SHODAN
- Jigsaw
- Pastebin
- Google hacking
- EDGAR
- Google Finance

Google Hacking

- Search for all URLs of a particular domain
- site:<domain>

- Search for a particular file type
- Excel, PowerPoint, Word, PDF and txt
- filetype:<type>

Person

- 123people.com
- 411.com
- phonenumbers.addresses.com
- cvgadget.com
- search.nndb.com
- spokeo.com
- zabasearch.com

Scrape

- Combines various different tools
- Passive
- Active

Passive

- goofile
- goo-mail
- goohost
- theHarvester
- Metasploit
- Whois

Active

- dnsenum
- dnsrecon
- dnswalk
- traceroute
- lbd – load balance detector

Discover

- Host discovery
- Ping sweep
- Single host or URL
- Local area network
- List of hosts
- CIDR notation

Nmap

- Port scanning
- Service enumeration
- OS identification

- Nmap scripting engine (NSE)
- 432 scripts and growing

Metasploit

- Exploitation framework
- Database integration
- Auxiliary scanners
    - Brute force
    - Enumeration
- Resource files

Automation

- Why do we need automation?

  Repeatable process

  Do not want to miss any steps

- What can be automated?

- DEMO

Lee Baird

- Google Code
- http://code.google.com/p/backtrack-scripts/

- Ping me on GTalk
- leebaird@gmail.com