Setting Up BackTrack

And automating various tasks with bash scripts

by

Lee Baird

Lee Baird

- Graduate of Marshall University
- Bachelor's degree in accounting
- Offensive Security Certified Professional
- Roadie for 10 years
- Former United States Marine

Lee Baird

- Enterprise security assessments for Fortune 500
- Vulnerability assessments
- 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

Setting up a VM

- Latest version is BackTrack 5 R2
- Choose your environment and download
- 32-bit Gnome ~ 2 GB in size
- OS X – VMware Fusion
- Windows – VMware Workstation
- 1 to 4 GB of RAM

Setting up a VM

- Select the first menu option
- Login: root – toor
- Change the root password: passwd
- Fix the splash screen: fix-splash
- Reboot and login with new creds
- Start the GUI: startx

Install VMware Tools

- Open a Terminal: prepare-kernel-sources
- On the VMware, click 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
- Cut, copy and paste between host and VM

Terminal

- Where you will spend most of your time
- Terminal > Edit > Profile Preferences
- General > Monospace 13
- Color > Text color > white
- Background > Background image (solid black)
- Scrolling > Unlimited *

gedit

- Text based editor
- Edit > Preferences
- Display line numbers
- Highlight current line
- Editor > Tab width 5
- 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
- ./setup
- Create SSH keys
- Setup aliases
- Install Filezilla and xdotool

svn and github

- Some applications under continuous development
- Pull these from repos
- dnsrecon
- theHarvester
- 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
- Fast-Track
- GISKismet
- Metasploit
- Nikto
- Nmap
- scripts
- SET
- sqlmap
- w3af

Open Source Intel Gathering

- Black box engagement
- Social engineering
- What kind of intel do I need?
- Where can I find it?

- 2 scripts to automate the process

Company - Intel

- Open multiple tabs in Firefox and download info from DeepMagic, IntoDNS and Robotex.
- /root/recon/

    dns-health.html

    dns.html

    ptr-records.txt

Company - Intel

- ARIN
- Netcraft
- SHODAN
- Google hacking
- EDGAR
- Google Finance

Google Hacking

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

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

Google Hacking

- filetype:xls OR filetype:xlsx site:marshall.edu
- Excel 636 files
- PowerPoint 1,240
- Word 7,410
- PDF 17,000
- txt 762

Personal - Intel

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

scrape.sh

- Combines 21 different tools
- Names
- Emails
- WhoIs
- DNS
- Route

```
Names and emails
     goog-mail              (1/14)
     goohost                (2/14)
     theHarvester-mod
        123people           (3/14)
        Ask                 (4/14)
        Bing                (5/14)
        Google              (6/14)
        LinkedIn            (7/14)
        Yahoo               (8/14)
        All                 (9/14)
     Metasploit             (10/14)

Whois
     Domain                 (11/14)
     IP                     (12/14)

DNS
     dnsenum-mod            (13/14)  # Note: this could take up to 7 min.

Route
     traceroute             (14/14)
```

Nmap

- 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)
- ~ 380 scripts and growing

Metasploit

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

Automation

- Why do we need automation?

  Do not want to miss a step

  Repeatable process

- What can be automated?

- DEMO

Thanks!

- Welcome all feedback
- Google Code
- backtrack-scripts
- Lee Baird
- leebaird@gmail.com