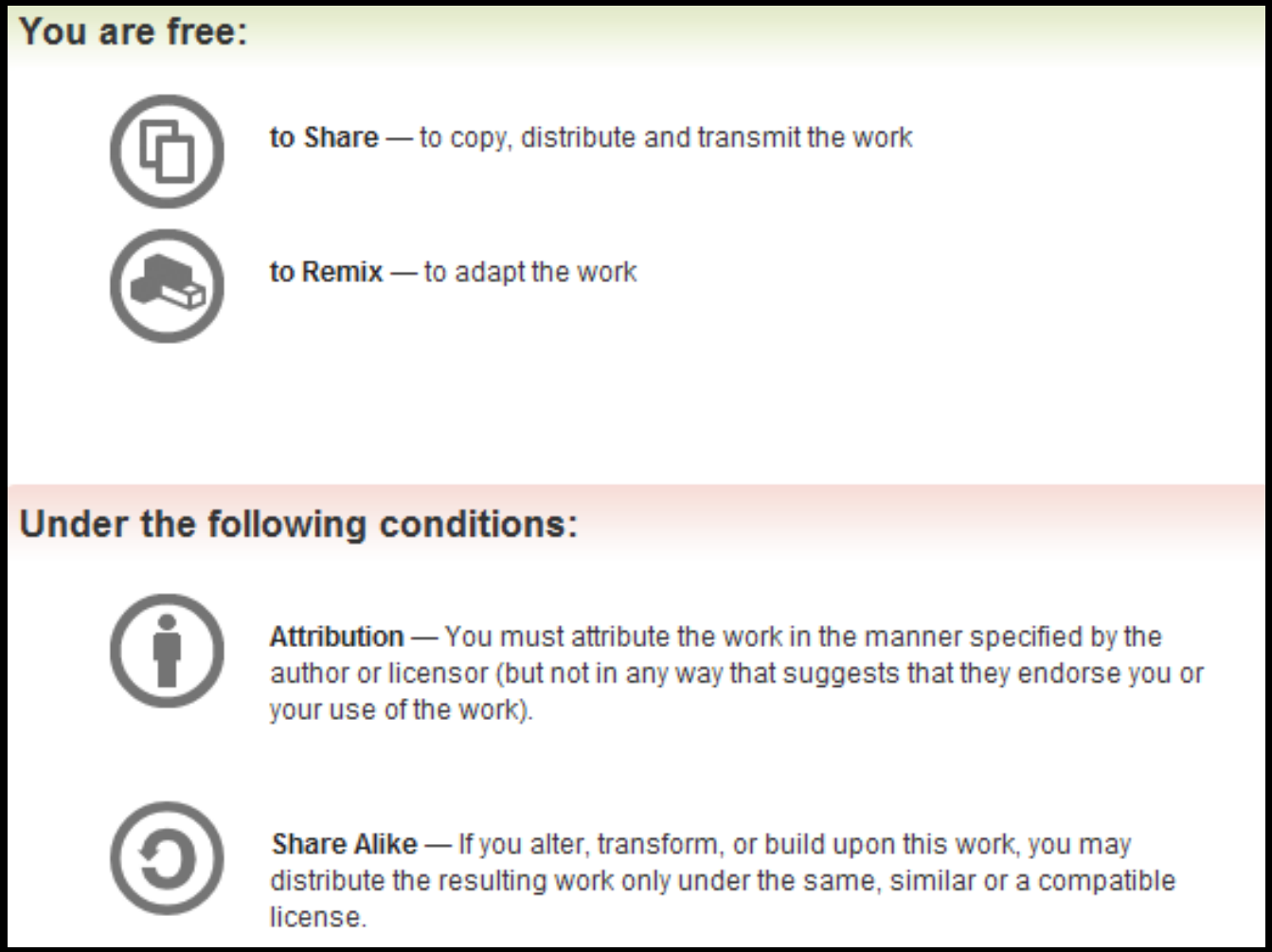
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

<< backtrack

the quieter you become, the more you're able to hear !!!


Applications
Places
System
Fri Aug 17, 2:19 PM
Accessories
BackTrack
Graphics
Internet
Office
Other
Sound & Video
System Tools
Wine
Information Gathering
Vulnerability Assessment
Exploitation Tools
Privilege Escalation
Maintaining Access
Reverse Engineering
RFID Tools
Stress Testing
Forensics
Reporting Tools
Services
Miscellaneous
Network Exploitation Tools
Web Exploitation Tools
Database Exploitation Tools
Wireless Exploitation Tools
Social Engineering Tools
Physical Exploitation
Open Source Exploitation
Cisco Attacks
Fast-Track
Metasploit Framework
SAP Exploitation
isr-evilgrade
armitage
msfcli
msfconsole
msfupdate
start msfpro
<< back | track 5
the quieter you become, the more you are able to hear
[root@bt: ~]
[localhost / localhost | ...

Backtrack 5 R3

- About BackTrack
- Installing BackTrack 5 R3
- I Know Your Password!
- Starting X
- Configuring Network (DHCP|Static)
- Configuring Basic Network Services
- Exploring the Pentest Directory
- Keeping Your Arsenal up2date
- Knowing Your Toolbox
- Backtrack 5 R3 Toolbox
- Other Useful CLI's

About BackTrack

- First release was 2007.
- The evolution of BackTrack spans many years of development, penetration tests, and unprecedented help from the security community.
- BackTrack originally started with earlier versions of live Linux distributions called Whoppix, WHAX, and Auditor.
- When BackTrack was developed, it was designed to be an all in one live cd used on security audits and was specifically crafted to not leave any remnants of itself on the laptop.
- It has since expanded to being the most widely adopted penetration testing framework in existence and is used by the security community all over the world.

Installing BackTrack

- BackTrack can be installed in different ways, I recommend you installing it using Virtualbox (Open Source).
- By using Virtualbox, its easy to copy, replicate and clone the whole system in case something wrong happens.
- No need to dedicate a machine for the system, use resources already available (only if you want to pay the price of getting a new machine).

I Know Your Password!!!

- Change your Password, before some1 does!
- Imagine getting into war and your own machinery store is played with by someone behind your lines, "*the enemy!*"
- Before doing any security tests for people, you must protect yourself. Start that by changing the BackTrack's default password (root/toor):

passwd

Starting X

- You prefer to work in a GUI environment with windows and a mouse? All you need is to start the X Window System:

```
# startx
```

Configuring Network (DHCP|Static)

- Dynamic Configuration (DHCP):

  # dhclient

  OR

  # /etc/init.d/networking restart

- Manual Configuration (Static)

  # ifconfig eth0 up

  # ifconfig eth0 [youripaddress] netmask [your netmask]

  # route add default gw [your gateway] eth0

  # echo nameserver [yourDNS]> /etc/resolv.conf

Configuring Basic Network Services

- Sometimes you need to test stuff locally, or import data to a database, or even copy files. That's why Backtrack comes with a different set of services we can use for such scenarios:
- SSH (OpenSSH)
- FTP (vsftpd)
- Web (Apache)
- Database (MySQL, Postgress)
- TFTP

Exploring the Pentest Directory

- Going to battles without knowing what arsenal you're carrying can lead to failure !
- Lets take a walk through the BackTrack penetration testing tools directory.

```
# cd /pentest
```

Keeping Your Arsenal up2date

- It is very important to keep your tools up to date,
- New features and enhancement are added,
- Bugs are fixed,
- New tools maybe added!

```
# apt-get update
# apt-get upgrade
OR
# apt-get dist-upgrade
```

Knowing Your Toolbox

- You want to know nearly all your toolbox?

dpkg --list

- You want to know if a specific tool is installed?

dpkg --list | grep <tool-name>

Backtrack 5 R3 Toolbox

Backtrack's main toolbox categories:

- Information Gathering Analysis
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress Testing
- Forensics
- Reporting Tools

Other Useful CLI's

- Getting Help
  - man <command-name>
  - info <command-name>
  - <command-name> --help
  - GNOME Help
- Searching
  - find
  - locate <filename>
  - GNOME Search
- Creating and Editing Files
  - GNOME gedit
  - vim
  - nano
- Fetching File From Internet
  - wget -c <URL>
- Installing new software/packages
  - apt-cache <software-name>
  - apt-get install <exact-software-name>

Taken from:
Linux Arab Community,
http://linuxac.org

Cli commands

FILE COMMANDS

- ls - directory listing
- ls -al - formatted listing with hidden files
- cd dir - change directory to dir
- cd - change to home
- pwd - show current directory
- mkdir dir - create a directory dir
- rm file - delete file
- rm -r dir - delete directory dir
- rm -f file - force remove file
- rm -rf dir - force remove directory dir *
- cp file1 file2 - copy file1 to file2
- cp -r dir1 dir2 - copy dir1 to dir2; create dir2 if it doesn't exist
- mv file1 file2 - rename or move file1 to file2 if file2 is an existing directory, moves file1 into directory file2
- ln -s file link - create symbolic link link to file
- touch file - create or update file
- cat > file - places standard input into file
- more file - output the contents of file
- head file - output the first 10 lines of file
- tail file - output the last 10 lines of file
- tail -f file - output the contents of file as it grows, starting with the last 10 lines

SEARCHING

- grep pattern files - search for pattern in files
- grep -r pattern dir - search recursively for pattern in dir
- command | grep pattern - search for pattern in the output of command
- locate file - find all instances of file

PROCESS MANAGEMENT

- ps - display your currently active processes
- top - display all running processes
- kill pid - kill process id pid
- killall proc - kill all processes named proc (use with extreme caution)
- bg - lists stopped or background jobs; resume a stopped job in the background
- fg - brings the most recent job to foreground
- fg n - brings job n to the foreground

SHORTCUTS

- Ctrl+C - halts the current command
- Ctrl+Z - stops the current command, resume with fg in the foreground or bg in the background
- Ctrl+D - log out of current session, similar to exit
- Ctrl+W - erases one word in the current line
- Ctrl+U - erases the whole line
- Ctrl+R - type to bring up a recent command
- !! - repeats the last command
- exit - log out of current session

SYSTEM INFO

- date - show the current date and time
- cal - show this month's calendar
- uptime - show current uptime
- w - display who is online
- whoami - who you are logged in as
- finger user - display information about user
- uname -a - show kernel information
- cat /proc/cpuinfo - cpu information
- cat /proc/meminfo - memory information
- man command - show the manual for command
- df - show disk usage
- du - show directory space usage
- free - show memory and swap usage
- whereis app - show possible locations of app
- which app - show which app will be run by default

COMPRESSION

- tar cf file.tar files - create a tar named file.tar containing files
- tar xf file.tar - extract the files from file.tar
- tar czf file.tar.gz files - create a tar with Gzip compression
- tar xzf file.tar.gz - extract a tar using Gzip
- tar cjf file.tar.bz2 - create a tar with Bzip2 compression
- tar xjf file.tar.bz2 - extract a tar using Bzip2
- gzip file - compresses file and renames it to file.gz
- gzip -d file.gz - decompresses file.gz back to file

NETWORK

- ping host - ping host and output results
- whois domain - get whois information for domain
- dig domain - get DNS information for domain
- dig -x host - reverse lookup host
- wget file - download file
- wget -c file - continue a stopped download

INSTALLATION

- Install from source:
  ./configure
  make
  make install

- dpkg -i pkg.deb - install a package (Debian)
- rpm -Uvh pkg.rpm - install a package (RPM)

FILE PERMISSIONS

- chmod octal file - change the permissions of file to octal, which can be found separately for user,

  group, and world by adding:
  - 4 - read (r)
  - 2 - write (w)
  - 1 - execute (x)

  Examples:

  chmod 777 - read, write, execute for all
  chmod 755 - rwx for owner, rx for group and world
  For more options, see man chmod.

Appendix – The Lab

What is Needed?

- Virtualbox
- BackTrack 5 R3
- OWASP Broken Web Applications Project *(1 NIC's needed)*
- Slackware VM for Software Exploitation *(1 NIC's needed)*
- Windows XP/2003 *(2 NIC's needed)*
- Exploit KB, grab vulnerable software
- Use a Host-only Network!

SUMMARY

- What is Backtrack and howto prepare it for pentesting,
- Available Backtrack Toolbox,
- Backtrack basic usage,
- Creating a simple lab for security testing.

References

[-] Backtrack Linux Distro., http://www.backtrack-linux.org/

[-] Slackware Exploitation VM, http://opensecuritytraining.info/slack12.zip

[-] OWASP Broken Web Applications VM, http://downloads.sourceforge.net/project/owaspbwa/1.0/OWASP_Broken_Web_Apps_VM_1.0.7z