Hacking Techniques & Intrusion Detection

Winter Semester 2012/2013

Dr. Ali Al-Shemery
aka: B!n@ry
the quieter you become, the more you’re able to hear !!!
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
```

Just as simple as that !!!
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
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

Doesn’t end here !!!

Dr. Ali Al-Shemery (aka: B!n@ry)
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>`
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!
- Others (added later)
SUMMARY

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

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