BackTrack Overview

An Attack Example

(a cura di **Giuliano Goffi**)

INDICE DELLA PRESENTAZIONE :

BackTrack

Si tratta della più popolare distribuzione linux mirata al penetration testing.

BackTrack 2 nasce dal merge di due precedenti distro dedicate al penetration testing: **Whax** di origine istraeliana e **Auditor Security Collection** su Knoppix, oggi è basata sulla distribuzione Slackware linux.

Ogni pacchetto, il kernel e gli script sono stati ottimizzati per essere usati da **Security Penetration Testers.**

BackTrack

Chi può utilizzarla?

Cosa contiene?

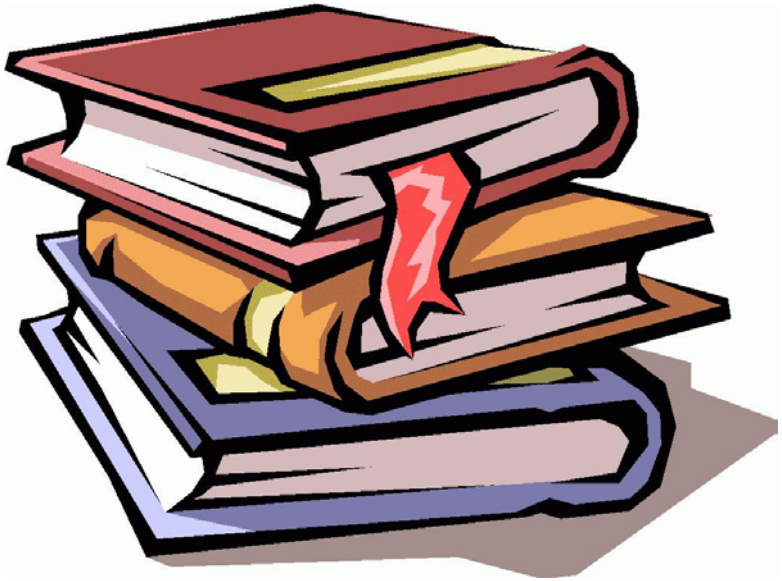
Quali sono i punti di forza?

Dove è consigliato testala?

Cosa contiene?

- Enumeration
- Exploit
- Scanner
- Password
- Fuzzers
- Spoofing
- Sniffers

- Tunneling
- Wireless Tools
- BlueTooth
- Cisco Tools
- Database
- Forensic
- BT Services

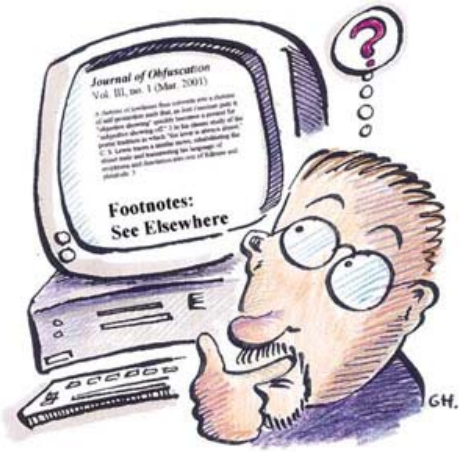


Punti di forza

- E' possibile scaricarla gratuitamente
- Lavora su live CD o su chiavetta USB
- Continuamente aggiornata
- Tools validi e funzionanti

Chi può utilizzarla?

Professionisti del settore



Appassionati di sicurezza

Studenti

Ricercatori

Comunità Hackers

Dove Utilizzarla

A casa

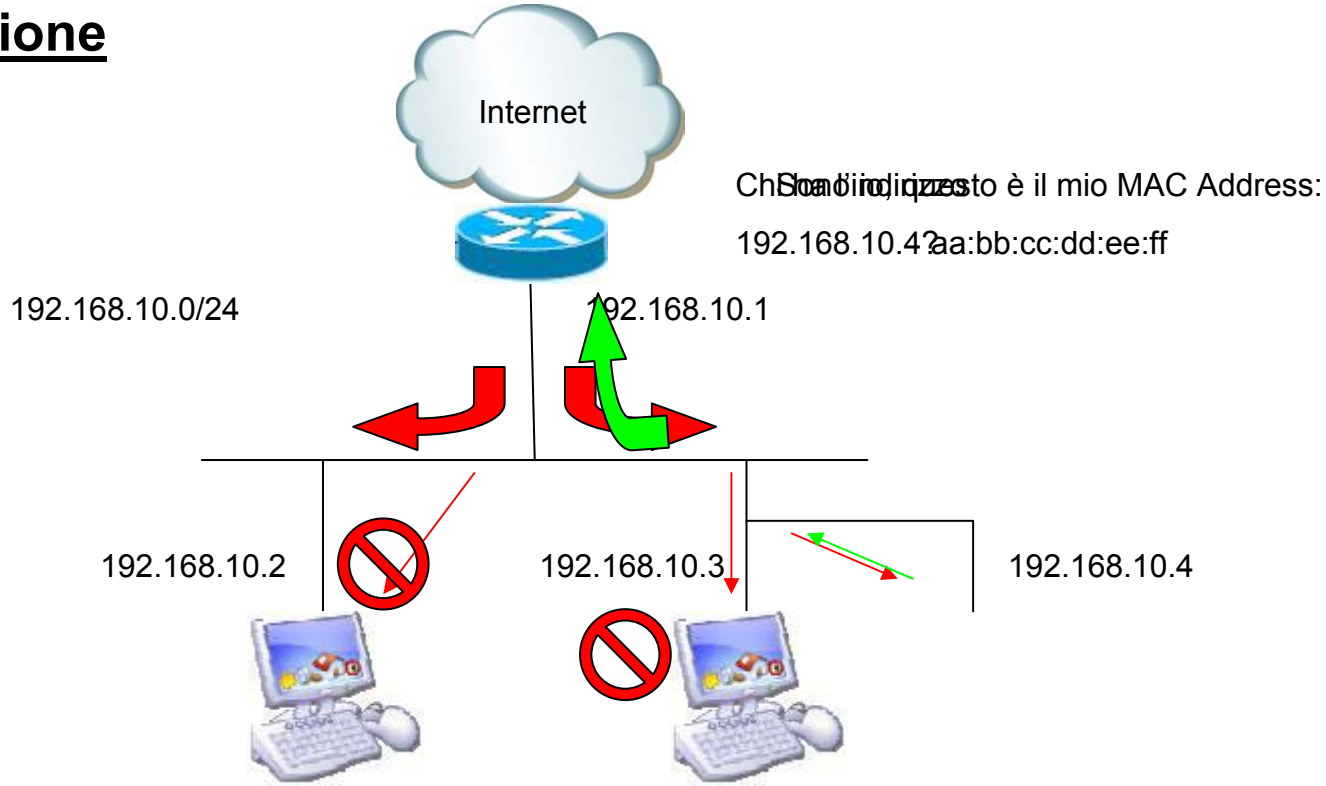
E' utilizzabile ovunque

In azienda

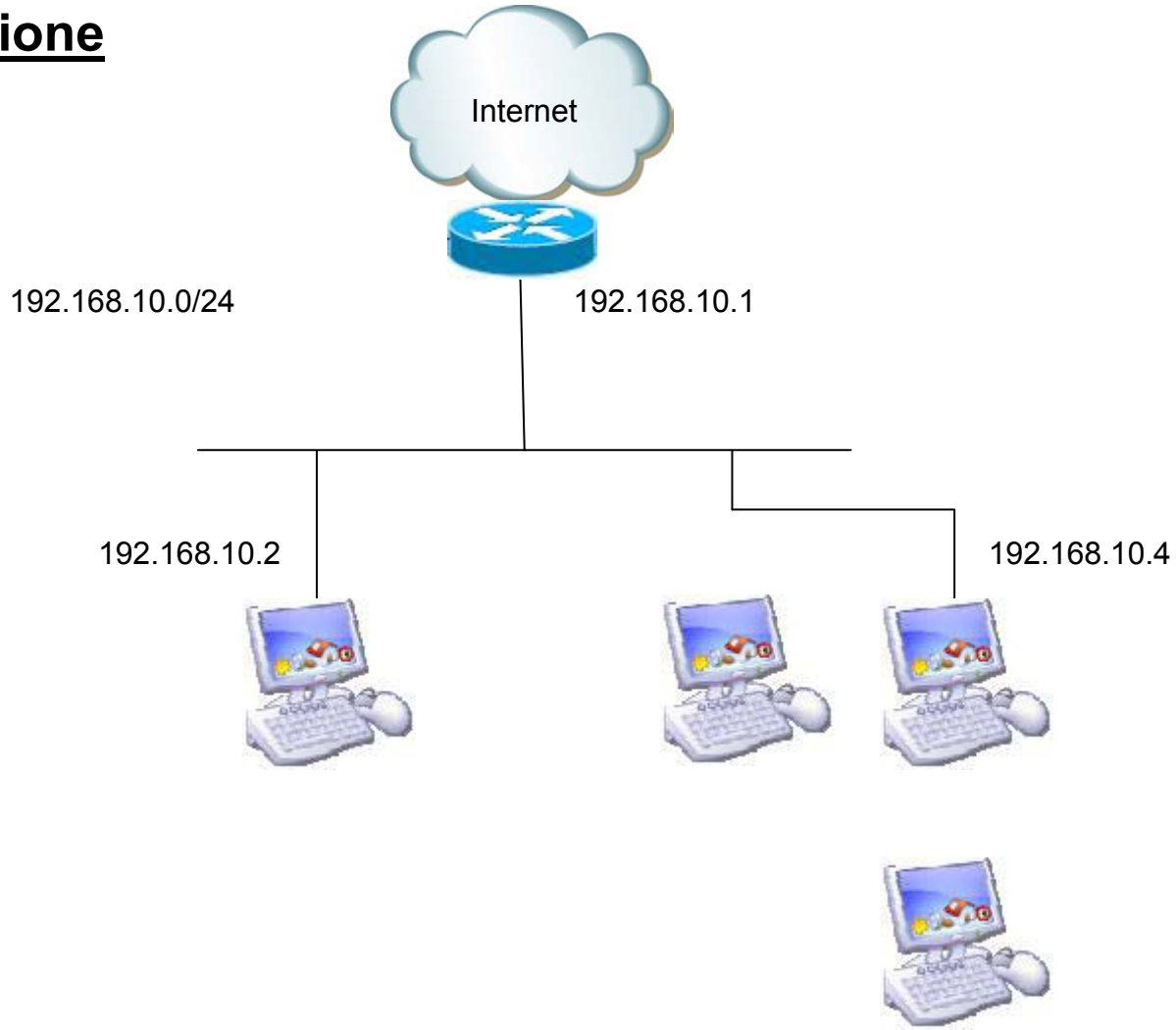
All'interno di piattaforme virtuali

INDICE DELLA PRESENTAZIONE :

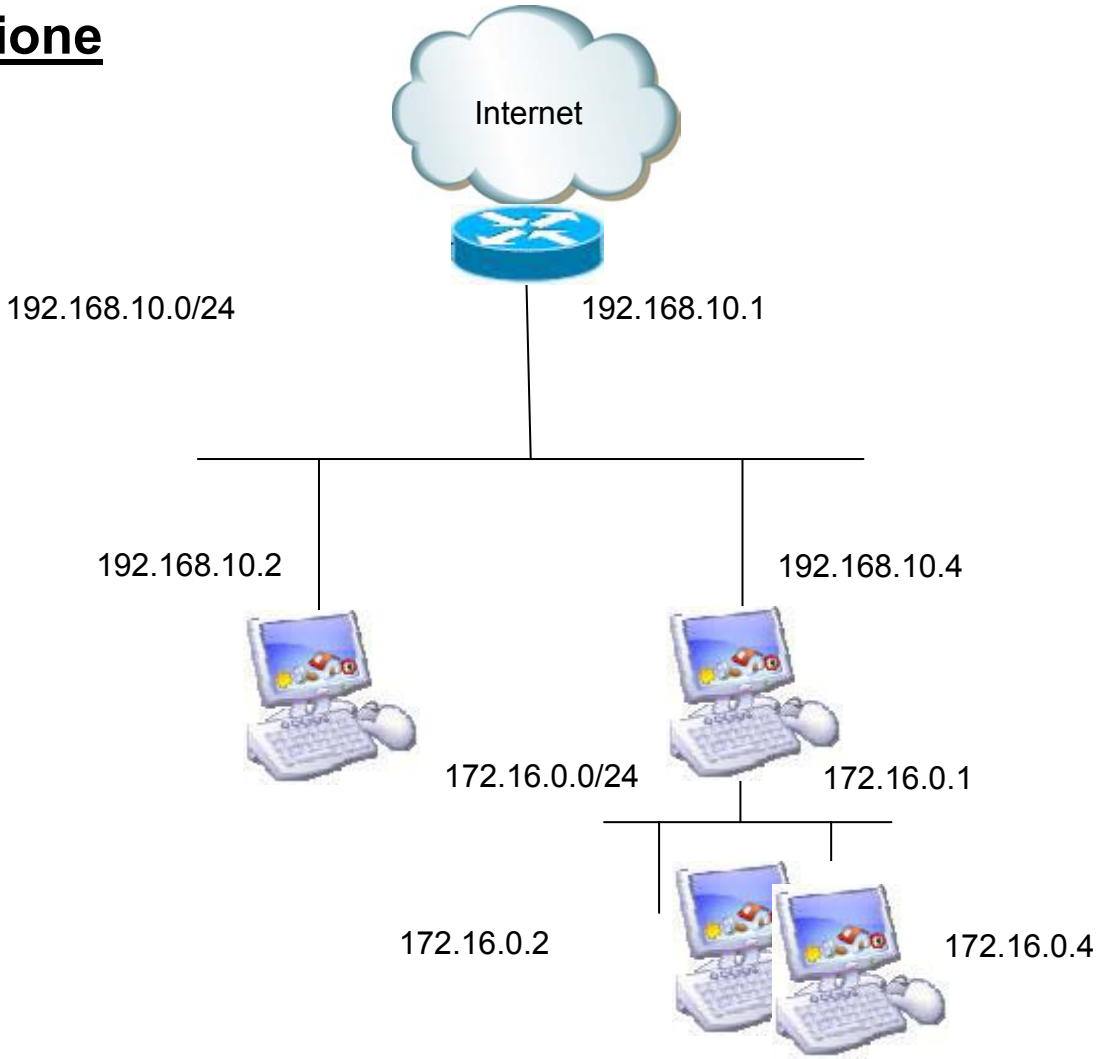
Virtualizzazione



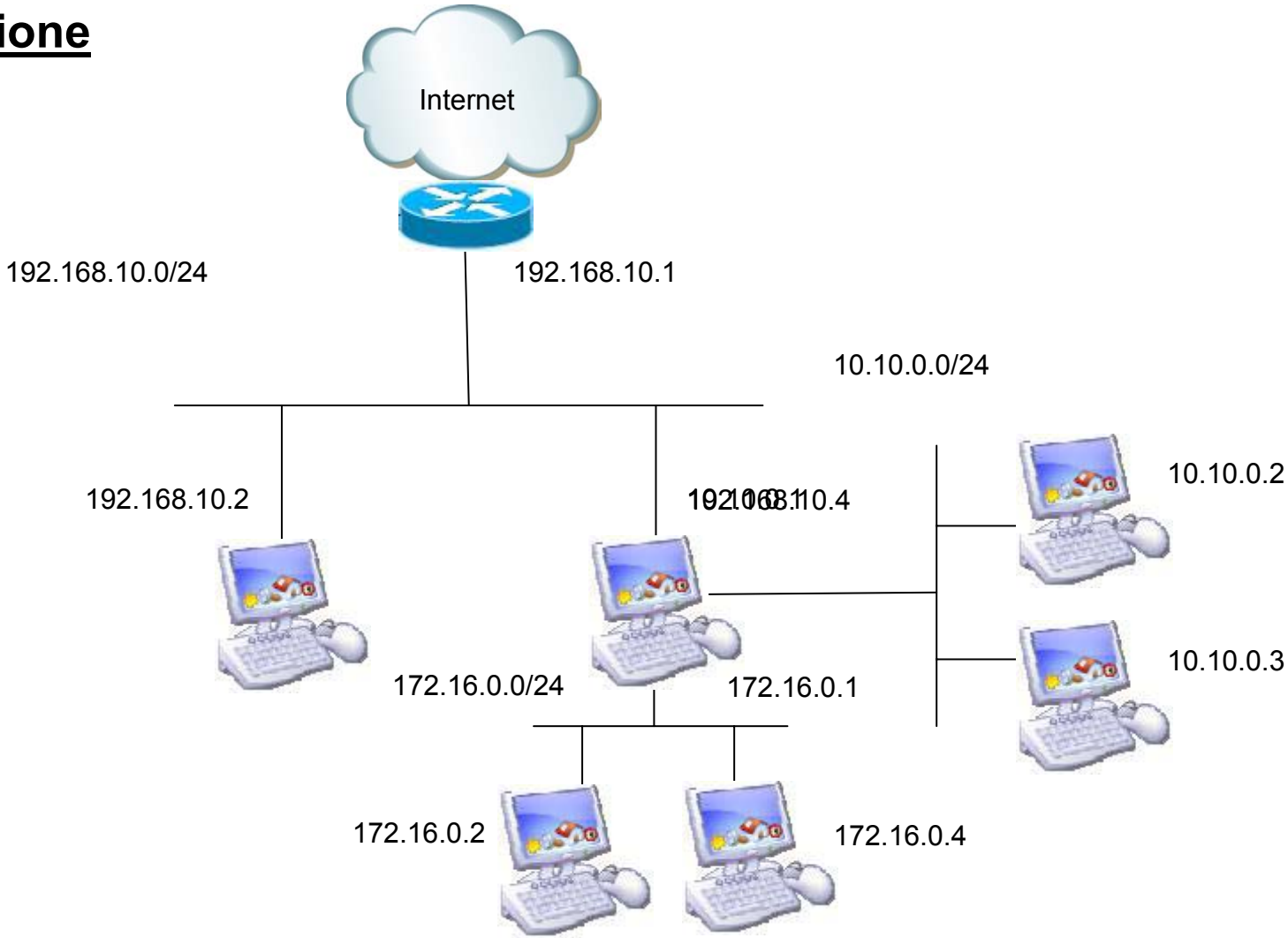
Virtualizzazione



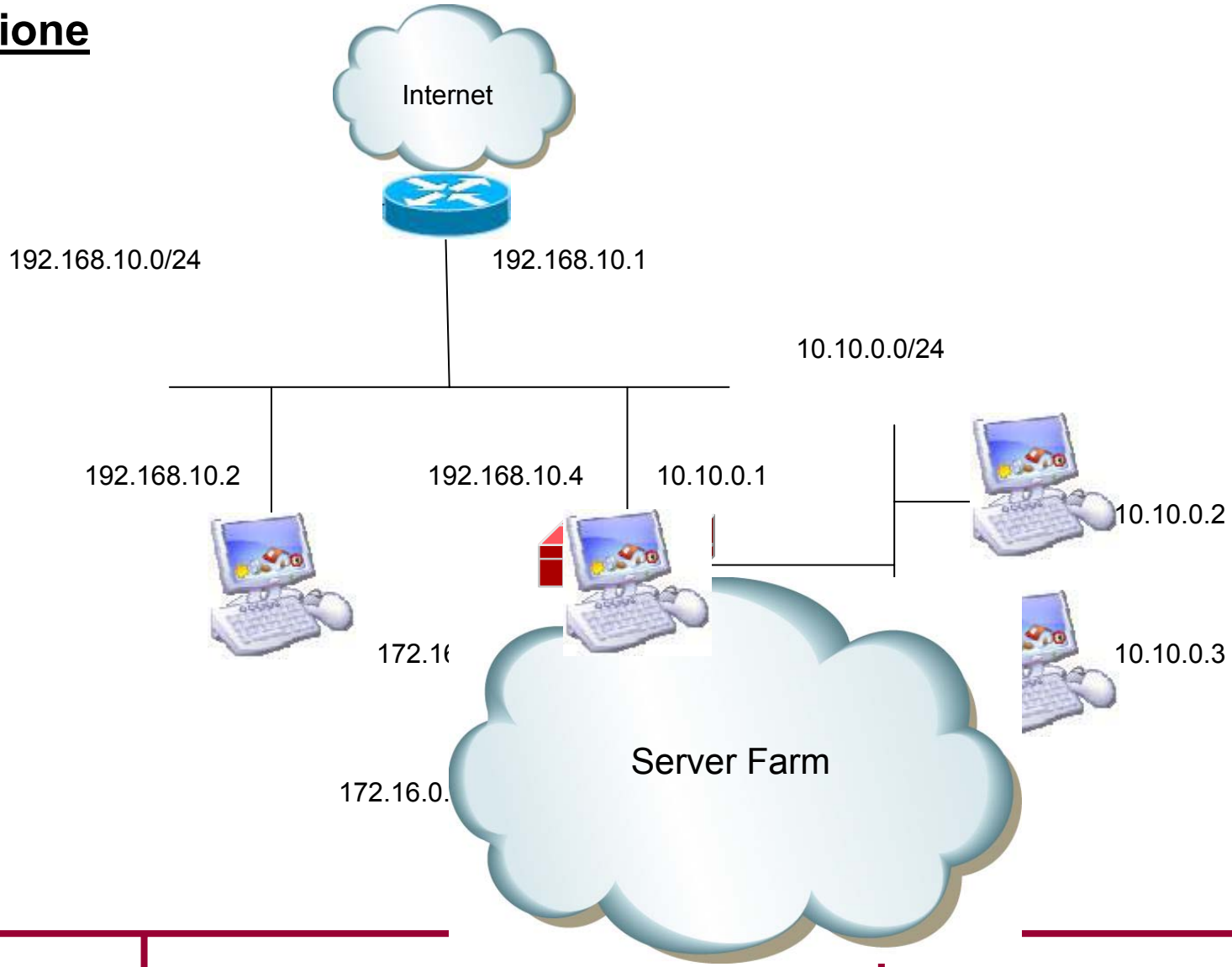
Virtualizzazione



Virtualizzazione



Virtualizzazione



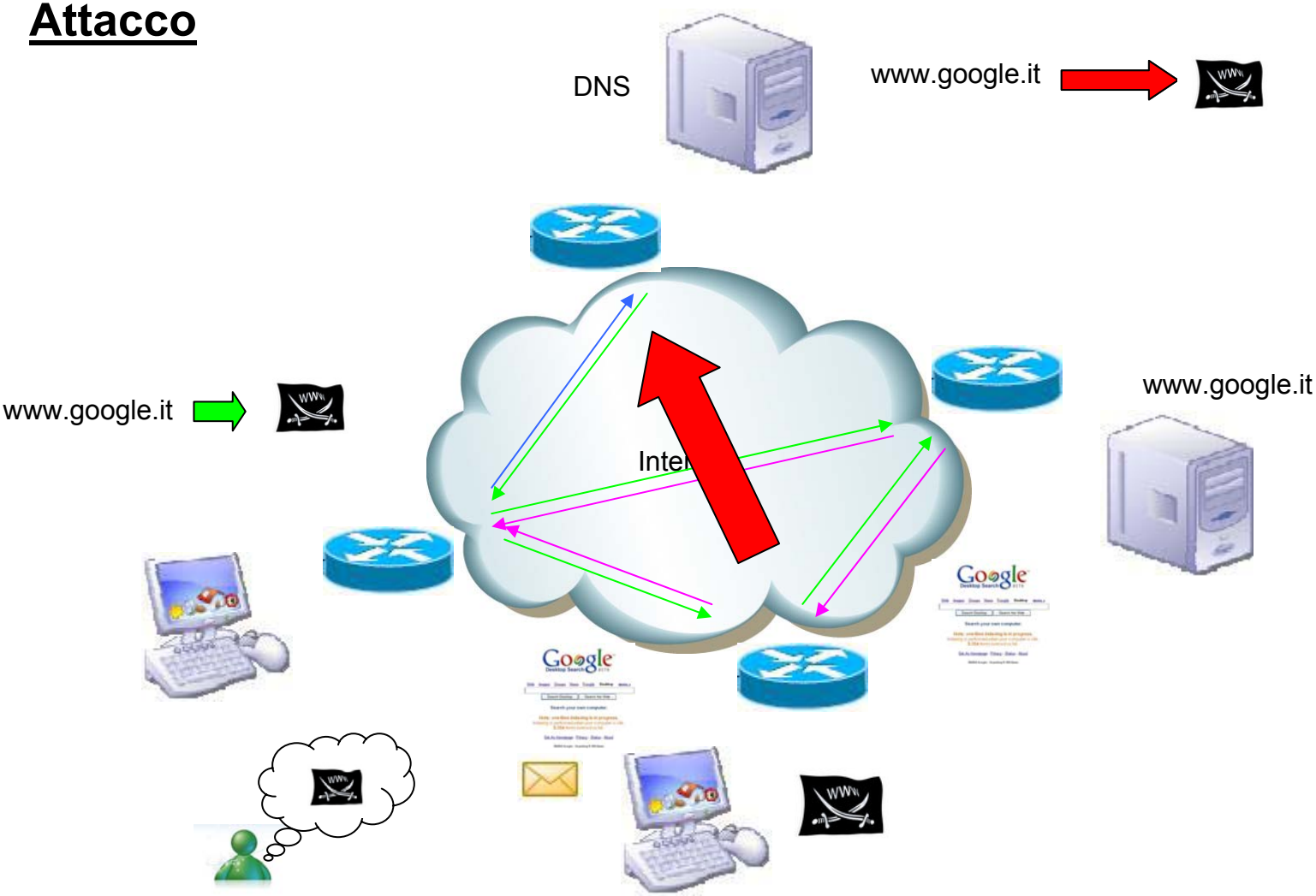
INDICE DELLA PRESENTAZIONE :

Che cos'è un EXPLOIT?

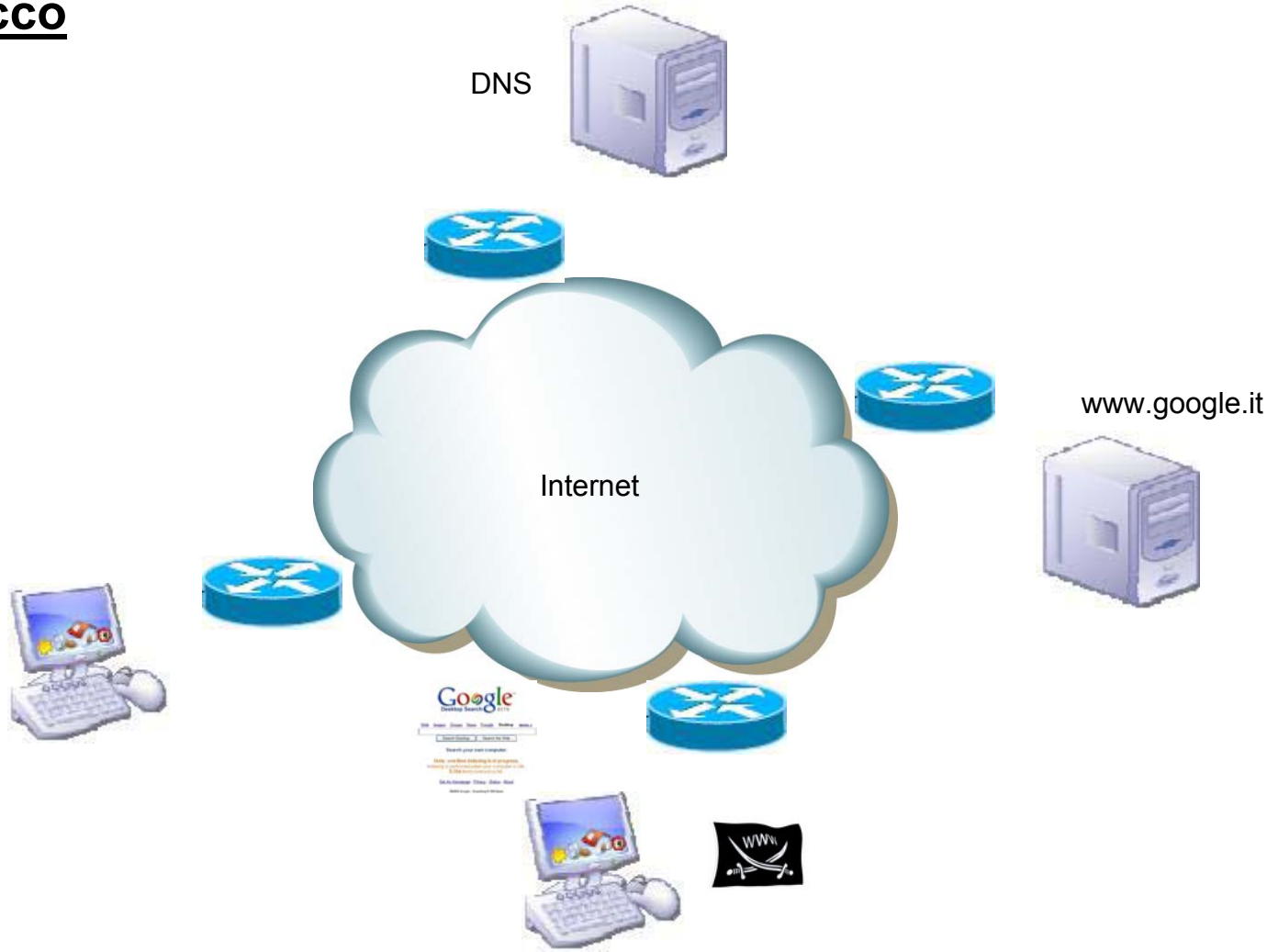
L'exploit è un programma che consente di sfruttare falle in un sistema, le cosi dette vulnerabilità

L'obbiettivo è l'esecuzione di codice dannoso che in condizioni normali non funzionerebbe

Attacco



Attacco

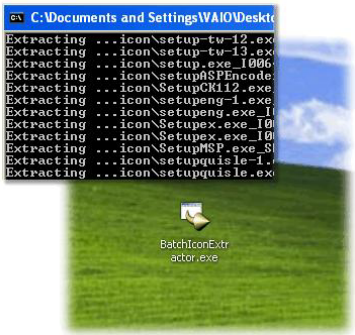



Google


WWW


WWW

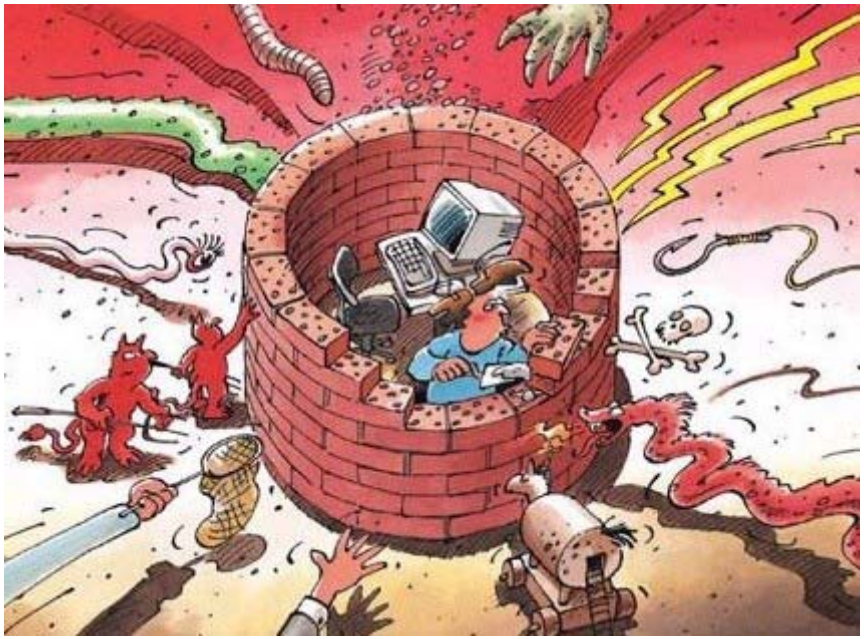

Google


C:\Documents and Settings\VAIO\Deskt
Extracting ...icon\setup-tw-12.ex
Extracting ...icon\setup-tw-13.ex
Extracting ...icon\setup.exe_I006
Extracting ...icon\setupASPEncode
Extracting ...icon\SetupCKi12.exe
Extracting ...icon\setupeng-1.exe
Extracting ...icon\setupeng.exe_I
Extracting ...icon\Setupex.exe_I0
Extracting ...icon\Setupex.exe_I0
Extracting ...icon\SetupMSP.exe_S
Extracting ...icon\setupquisle-1.
Extracting ...icon\setupquisle.ex
BatchIconExtr
actor.exe

INDICE DELLA PRESENTAZIONE :

Come difendersi

Corsi di sensibilizzaziono



Corsi di sensibilizzaziono

Corsi di sensibilizzaziono

Corsi di sensibilizzaziono

Anche l'operazione piu semplice e trasparente potrebbe nascondere un'ipotetica minaccia

INDICE DELLA PRESENTAZIONE :

1. BackTrack
2. Virtualizzazione
3. L'attacco
4. Come difendersi

5. Riferimenti bibliografici e sitografici

Bibliografia e sitografia :

• Scrivere un Exploit con Nessus

di Stefano Maccaglia & Giuliano Goffi

Articolo publicato dalla rivista Hackin9 nel numero 7-8/2007

• www.remote-exploit.org/backtrack_download.html

BackTrack

• www.vmware.com

Sistemi di virtualizzazione

• www.metasploit.com

Metasploit Framework

Altri Riferimenti :

GRAZIE PER L'ATTENZIONE

Giuliano Goffi

gf.giuliano@gmail.com
3299591661