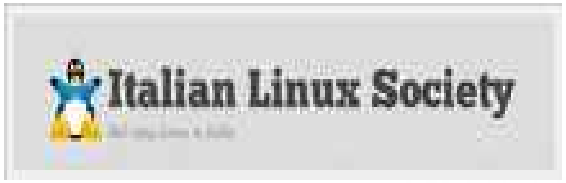
Le basi dell'Hacking

Paolo Giardini

Magione, giugno 2017

paolo ‘aspy’ giardini



Hacker

hacker: [originalmente, uno che faceva attrezzi con un'ascia]

Persona che si diverte esplorando dettagli di sistemi programmabili e di come ampliare le loro caratteristiche, contrariamente a molti utenti, che preferiscono imparare il minimo necessario.
RFC1392, Glossario di utenti Internet, utilmente allarga la definizione così: Persona che è deliziata dalla conoscenza profonda del funzionamento interno del sistema, in particolare di computer e reti di computer.

Da distingure da ***Cracker***Il termine cracker (o Black Hat Hacker), persona che si ingegna per eludere blocchi imposti da qualsiasi sistema informatico al fine di trarne profitto o creare danni.
Jargon file: https://it.wikipedia.org/wiki/Jargon_File

Ditemi cosa vedete

pexels.com
Cat Images · Pexels · Free Stock Photos
5360 × 3560 - 1907 kB - jpeg

rd.com
Cat Behavior: 17 Things Your **Cat** Wants to Tell You | Reader's Digest
2400 × 1600 - 206 kB - jpg

royalcanin.com
Find the Best Food for Your Adult **Cat's** Needs | Royal Canin
470 × 350 - 40 kB - ashx

rd.com
How to Train a **Cat** to Do 5 Life-Changing Things | Reader's Digest
2400 × 1599 - 218 kB - jpg

pixabay.com
Cat - Free images on Pixabay
858 × 720 - 167 kB - jpg

petdrugsonline.co.uk
Cat Products - Pet Drugs Online
400 × 320 - 73 kB

pinterest.com
1000+ ideas about **Cats** on Pinterest | Kitty, Kitty **cats** and Kittens
600 × 900 - 51 kB - jpg

businessinsider.com
The man behind Hamilton the hipster **cat** on Instagram - Business ...
4608 × 3456 - 19587 kB - jpg

bharatint.com
Bharat International - **Cats**-Grooming
525 × 348 - 58 kB - png

royalcanin.ca
The Adult **Cat** Life Stage | Royal Canin Canada
470 × 350 - 81 kB - ashx

youtube.com
Cats scared of Cucumbers Compilation - **Cats** Vs Cucumbers - Funny ...
1280 × 720 - 139 kB - jpg

battersea.org.uk
Cat rehoming gallery | Battersea Dogs & **Cats** Home
400 × 400 - 41 kB

Adesso cosa vedete?

amazon.com
Amazon.com: **Dogs**: Pet Supplies: Apparel & Accessories, Collars ...
593 × 305 - 56 kB - jpg

animalplanet.com
Dogs | Animal Planet
720 × 720 - 70 kB - jpg

pixabay.com
Dog - Free images on Pixabay
960 × 720 - 134 kB - jpg

pexels.com
Dog images · Pexels · Free Stock Photos
5472 × 3648 - 11227 kB - jpg

what-dog.net
What is your **dog**?
600 × 600 - 75 kB - jpg

dogtime.com
Entlebucher Mountain **Dog** Breed Information, Pictures ...
460 × 290 - 15 kB - jpg

royalcanin.com
Dog Food for Medium Breed **Dogs** and Puppies | Royal Canin
309 × 350 - 23 kB - ashx

cesarsway.com
Dog Behavior | Cesar's Way
845 × 450 - 48 kB - jpg

petsmart.com
Dog Treats & Rawhide | PetSmart
550 × 330 - 123 kB

pinterest.com
17 Best ideas about **Dogs** on Pinterest | **Dogs** and puppies, Cute ...

petsmart.com
Dog Toys: Games & Toys for **Dogs** | PetSmart
550 × 330 - 103 kB

cdc.gov
Preventing **Dog** Bites | Features | CDC
456 × 294 - 28 kB - jpg

Pensiamo

Bene.
Ora ditemi perché!

Pensare da Hacker

“think out of the box”

Siete in una stanza illuminata da una lampadina appesa al soffitto. Sul muro c’è un interruttore.

Trovate 10 modi per “fare buio” in quella stanza.

Trovare servizi

Nmap

Nmap è un software libero distribuito con licenza GNU GPL da Insecure.org creato per effettuare **port scanning**, cioè mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP, in modo da determinare quali servizi di rete siano disponibili.

```
bratchc2ddsktop bratch # nmap -T5 -sV -O localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-12 19:07 GMT
Interesting ports on localhost (127.0.0.1):
Not shown: 1709 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.7 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
10000/tcp open  http     Webmin httpd
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.21
Uptime: 0.136 days (since Wed Mar 12 15:52:05 2008)
Network Distance: 0 hops
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 13.241 seconds
bratchc2ddsktop bratch #
```

Web vulnerabile

Sito web: come funziona.

Server. Programmi. Linguaggi.

Vulnerabilità: difetto di progettazione, codifica, installazione o configurazione di un software o di un sistema che possono permettere ad un attaccante di acquisire il controllo di un sistema, rubare dati od eseguire attività normalmente non consentite.

Hacking di database

Linguaggio SQL

Esempio di autenticazione con username e password

```
Select nome, password from utenti where
nome='$nome' and password='$password';
```

SQL injection:

```
Select nome, password from utenti where
nome='' or '1=1' and password='' or
'1=1';
```

Prova pratica

Esempi di attacco sfruttando le vulnerabilità presenti sul nostro server target

- Sql injection login bypass
- malware upload
- mySql server credential steal
- User credential steal
- Passwd dump
- Ssh login attack
- Shell access

esercizi online:
http://sqlidemo.altervista.org/index.php

Craccare password

John the Ripper

Modalità:
- File dizionari
- Brute force

1) creare zip con password (zip e)
2) estrarre hash (zip2john)
3) lanciare john con opzione dizionario (john --wordlist=)
4) mostrare risultato (john –show)

Craccare login ssh

hydra

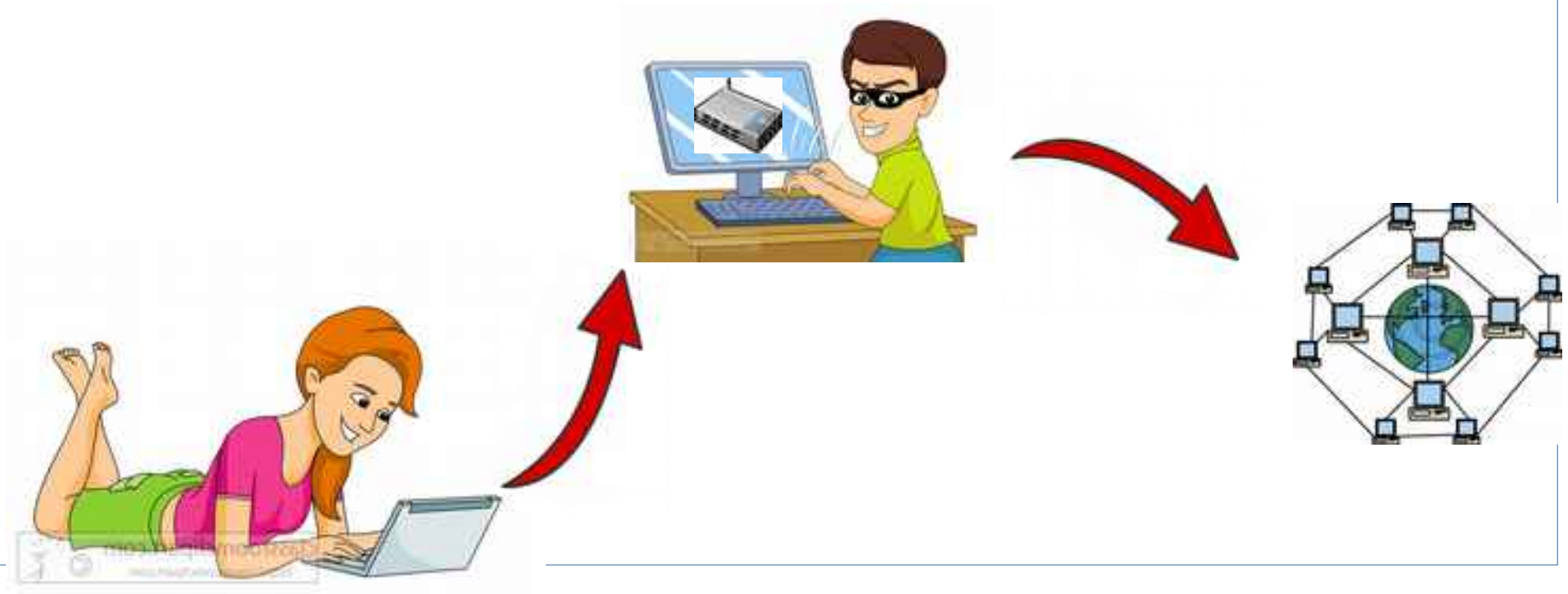
Rischi del WiFi

- E’ possibile trovare Access Point **aperti: pericolo!**
- Protetti con cifratura **WEP** (wireless equivalent privacy): **inutile!**
- Protetti con cifratura **WPA** o **WPA2** (WiFi protected access).
  - Difficile ma non impossibile da bucare, soprattutto se si usano password deboli (attacco dizionario o brute force)
- Problema: tutto il traffico è via radio, quindi **intercettabile!**
- **Client Isolation**: configurazione dell’access point *legittimo* che isola le comunicazioni di ciascun utente impedendo di fatto lo sniffing. **Indispensabile!**

- Rischi:
  - **Fake Access Point**
  - **Man in the Middle**
  - **Sniffing**

Rogue AP attack

1) l’attaccante crea un falso access point
2) la vittima crede di connettersi ad un Access Point legittimo
3) l’attaccante può intercettare tutto il traffico



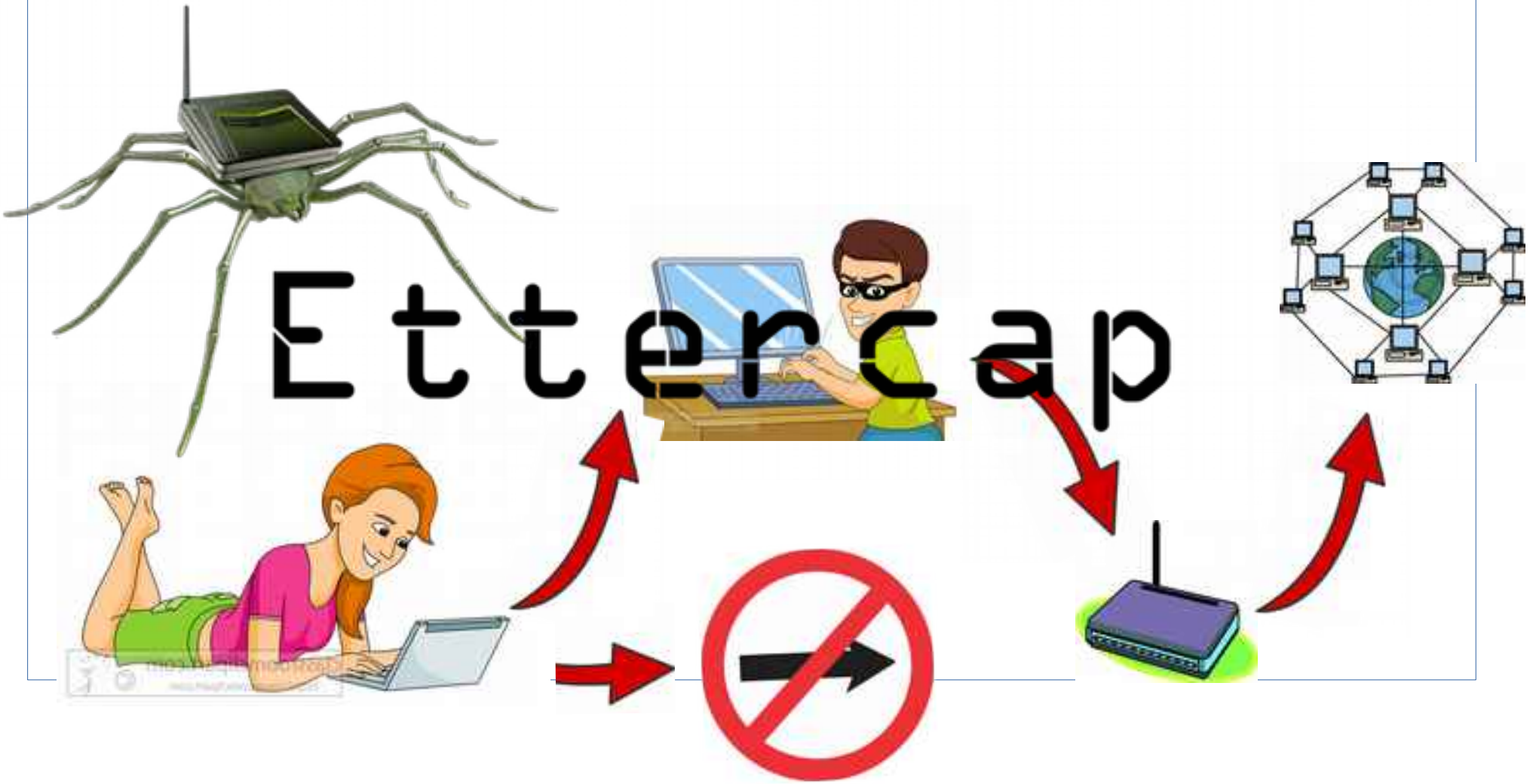
MitM attack

Attacco MITM (Man In The Middle)
Funziona con un Fake Access Point oppure con un access point legittimo ma al quale l'attaccante riesca a connettersi (è aperto o conosce la chiave)

1) l'attaccante individua la vittima ed il gateway
2) sostituisce il suo pc al gateway legittimo (ARP poisoning)
3) la vittima naviga normalmente
4) l'attaccante può intercettare tutto il traffico

MitM attack

Vediamo ora un esempio pratico con ETTERCAP, uno strumento Italiano



Domande?

STUDIO GIARDINI
www.solution.it

paolo.giardini@solution.it

Studio Giardini

SICUREZZA INFORMATICA

Tel.+(39) 337-65.28.76 – 02-006.10.235
Fax +(39) 075 9383 1174
email: studio.giardini@solution.it

http://www.solution.it
http://blog.solution.it