

# (In)sicurezza WEP dalla community

Simulazione di una community di sviluppo

Roberto Metere

25 ottobre 2014

**GULCh**

*Gruppo Utenti Linux Cagliari h...?*





## Le community

- Il concetto di community

- La community e la libertà digitale

## Simulazione di una community

- Forum - la nascita

- Divisione dei compiti

- Creazione del repository

- Condivisione del repository

- Lavoro di gruppo

- Test del codice e bugfix

- Mantenimento

## Crackare una WEP (semplice)

- Su cosa si basa la cifratura WEP

- Esempio facilitato

- Trovare la chiave WEP segreta

## Demo dell'applicazione





## Le community

Il concetto di community

La community e la libertà digitale

## Simulazione di una community

Forum - la nascita

Divisione dei compiti

Creazione del repository

Condivisione del repository

Lavoro di gruppo

Test del codice e bugfix

Mantenimento

## Crackare una WEP (semplice)

Su cosa si basa la cifratura WEP

Esempio facilitato

Trovare la chiave WEP segreta

## Demo dell'applicazione





## Il concetto di community

---

### Community e community virtuale

- ▶ In termini generali, la *community* può essere definita un'unità sociale, come aggregazione di due o più persone che condividono valori comuni.
- ▶ La community virtuale in particolare è caratterizzata dall'interazione mediante specifici *media sociali*, tra gli individui che la costituiscono.





## Il concetto di community

---

### Community e community virtuale

- ▶ In termini generali, la *community* può essere definita un'unità sociale, come aggregazione di due o più persone che condividono valori comuni.
- ▶ La community virtuale in particolare è caratterizzata dall'interazione mediante specifici *media sociali*, tra gli individui che la costituiscono.

### Community online

Una community online è una community virtuale che opera attraverso servizi di reti sociali, tra i quali le tecnologie più comuni sono IRC (Internet **R**elay **C**hat), forum sul web o social network come Twitter e Facebook.





## La community e la libertà digitale

*rispetto della libertà digitale*

### Diritti digitali e libertà digitale

Se il non essere esclusi dall'utilizzo delle tecnologie della rete rappresenta una buona definizione per quello che si intende per **diritti digitali**, la possibilità di usare le stesse in modo libero secondo svariati aspetti è il principio di **libertà digitale**

La community online è un esempio di uso libero e produttivo delle tecnologie informatiche per lo sviluppo e la produzione di beni per la libera condivisione delle idee, della cultura, del sapere, ...





## La community e la libertà digitale

*rispetto della libertà digitale*

### Diritti digitali e libertà digitale

Se il non essere esclusi dall'utilizzo delle tecnologie della rete rappresenta una buona definizione per quello che si intende per **diritti digitali**, la possibilità di usare le stesse in modo libero secondo svariati aspetti è il principio di **libertà digitale**

La community online è un esempio di uso libero e produttivo delle tecnologie informatiche per lo sviluppo e la produzione di beni per la libera condivisione delle idee, della cultura, del sapere, ...

### Obiettivo della presentazione

Simulazione di una community online che svilupperà un programmino per Linux, che guida l'utente a crackare una rete WiFi con cifratura WEP (**W**ired **E**quivalent **P**rivacy).





## Le community

Il concetto di community

La community e la libertà digitale

## Simulazione di una community

Forum - la nascita

Divisione dei compiti

Creazione del repository

Condivisione del repository

Lavoro di gruppo

Test del codice e bugfix

Mantenimento

## Crackare una WEP (semplice)

Su cosa si basa la cifratura WEP

Esempio facilitato

Trovare la chiave WEP segreta

## Demo dell'applicazione







## Forum - la nascita

» salta questa sezione

In questa sezione vedremo come può nascere una community, ovvero da uno scambio di messaggi in un forum dal quale scaturisce un **interesse comune** a più persone.




[Visualizza il forum su browser](#)



## Forum - la nascita

schermata 1/6

**Aircrack-ng**
 simple machines forum




Hello **CodeRed**
July 16, 2012, 12:49:01 pm


[HOME](#)
[HELP](#)
[SEARCH](#)
[PROFILE](#)
[MY MESSAGES](#)
[MEMBERS](#)
[LOGOUT](#)

**Aircrack-ng** > **General Category** > **Newbies** > **Testare una WEP da finestra su Linux**

Pages: [1] Go Down « previous next »

Author
 Topic: Testare una WEP da finestra su Linux (Read 8259 times)
 [REPLY](#)
[NOTIFY](#)
[MARK UNREAD](#)
[SEND THIS TOPIC](#)
[PRINT](#)



**Melissa**  
 Newbie  
  
☐ Offline  
 Posts: 4  






**Testare una WEP da finestra su Linux**  
 « on: January 26, 2012, 07:46:39 am »
 [Quote](#)


A casa ho una WEP e vorrei testare la sicurezza, ho letto un po' la guida [simple wep crack](#) ma non capisco bene cosa fare o mi sembra troppo lungo o difficile.

Non si trova qualche programma magari a finestre che faccia al caso mio?


« Last Edit: January 26, 2012, 07:49:14 am by Melissa »

[Report to moderator](#)  Logged


**Nimda**  
 Experienced Newbie  
  
☐ Offline  
 Posts: 53  



**Re: Testare una WEP da finestra su Linux**  
 « Reply #1 on: January 26, 2012, 08:17:04 am »
 [Quote](#)

Usa WPA2/AES e stai tranquilla... )

[Report to moderator](#)  Logged



## Forum - la nascita

*schermata 2/6*


**Melissa**  
Newbie  
Offline  
Posts: 4


**Testare una WEP da finestra su Linux**  
« on: January 26, 2012, 07:46:39 am »

[Quote](#)

A casa ho una WEP e vorrei testare la sicurezza, ho letto un po' la guida [simple wep crack](#) ma non capisco bene cosa fare o mi sembra troppo lungo o difficile.

Non si trova qualche programma magari a finestre che faccia al caso mio?

« Last Edit: January 26, 2012, 07:49:14 am by Melissa »

[Report to moderator](#) [Logged](#)

---


**Nimda**  
Experienced Newbie  
☆☆☆☆☆  
Offline  
Posts: 53


**Re: Testare una WEP da finestra su Linux**  
« Reply #1 on: January 26, 2012, 08:17:04 am »

[Quote](#)

Usa WPA2/AES e stai tranquilla... :)

[Report to moderator](#) [Logged](#)

---


**Melissa**  
Newbie  
Offline  
Posts: 4


**Re: Testare una WEP da finestra su Linux**  
« Reply #2 on: January 26, 2012, 08:20:19 am »

[Quote](#)

Non posso :( perché ho delle apparecchiature WiFi un po' datate di cui non posso fare a meno che si collegano o senza cifratura, o solo WEP.

[Report to moderator](#) [Logged](#)

---


**CodeRed**





**Re: Testare una WEP da finestra su Linux**  
« Reply #3 on: January 26, 2012, 03:26:13 pm »



[Quote](#)



## Forum - la nascita

*schermata 3/6*



**Melissa**  
 Newbie  
 ☆  
☐ Offline  
 Posts: 4  
 





**Testare una WEP da finestra su Linux**  
 « on: January 26, 2012, 07:46:39 am »
  Quote



A casa ho una WEP e vorrei testare la sicurezza, ho letto un po' la guida [simple wep crack](#) ma non capisco bene cosa fare o mi sembra troppo lungo o difficile.

Non si trova qualche programma magari a finestre che faccia al caso mio?


« Last Edit: January 26, 2012, 07:49:14 am by Melissa »




[Report to moderator](#)  Logged




**Nimda**  
 Experienced  
 Newbie  
 ☆☆☆☆☆☆☆  
☐ Offline  
 Posts: 53  
 


**Re: Testare una WEP da finestra su Linux**  
 « Reply #1 on: January 26, 2012, 08:17:04 am »
  Quote


Usa WPA2/AES e stai tranquilla... :)



[Report to moderator](#)  Logged


**Melissa**  
 Newbie  
 ☆  
☐ Offline  
 Posts: 4  
 


**Re: Testare una WEP da finestra su Linux**  
 « Reply #2 on: January 26, 2012, 08:20:19 am »
  Quote

Non posso :( perché ho delle apparecchiature WiFi un po' datate di cui non posso fare a meno che si collegano o senza cifratura, o solo WEP.






[Report to moderator](#)  Logged


**CodeRed**  
 « Reply #3 on: January 26, 2012, 03:26:13 pm »
  Quote



## Forum - la nascita





*schermata 4/6*


**Melissa**  
 Newbie  
  
 Posts: 4  




Re: Testare una WEP da finestra su Linux  
 « Reply #2 on: January 26, 2012, 08:20:19 am »

Non posso :( perché ho delle apparecchiature WiFi un po' datate di cui non posso fare a meno che si collegano o senza cifratura, o solo WEP.






[Report to moderator](#)
[Logged](#)


**CodeRed**  
 Jr. Member  
  
 Posts: 64  



Re: Testare una WEP da finestra su Linux  
 « Reply #3 on: January 26, 2012, 03:26:13 pm »

Anche io vorrei un programma facile a finestra che mi aiuti a crackare le WEP, perché sono in affitto senza Internet e vorrei scroccare la connessione... :D

[Report to moderator](#)
[Logged](#)


**Melissa**  
 Newbie  
  
 Posts: 4  




Re: Testare una WEP da finestra su Linux  
 « Reply #4 on: January 26, 2012, 07:25:12 pm »

Servirebbe qualcuno che sa programmare, alla fine aircrack c'è, manca solo un'interfaccia a finestra per linux.

P.S.: attento, CodeRed, è illegale crackare le reti degli altri

« Last Edit: January 26, 2012, 07:55:31 pm by Melissa »

[Report to moderator](#)
[Logged](#)



## Forum - la nascita

schermata 5/6

un'interfaccia a finestre per linux.

P.S.: attento, CodeRed, è illegale crackare le reti degli altri

« Last Edit: January 26, 2012, 07:55:31 pm by Melissa »

Report to moderator

**CodeRed**

Jr. Member  
  
 Posts: 64

Re: Testare una WEP da finestra su Linux  
 « Reply #5 on: January 26, 2012, 11:13:29 pm »

Quote

Io so programmare, ma di linux non so nulla, se qualcuno mi aiuta, possiamo organizzare qualcosa ... volontari?

Report to moderator

**Nimda**

Experienced  
 Newbie  
  
 Posts: 53

Re: Testare una WEP da finestra su Linux  
 « Reply #6 on: January 28, 2012, 05:39:44 am »

Quote

Io di linux sono un esperto, se siete interessati, ci sentiamo su **#swepc** su Freenode, così parliamo più facilmente. Per chi non lo conoscesse, è una rete IRC:

- lista server : [https://freenode.net/irc\\_servers.shtml](https://freenode.net/irc_servers.shtml)
- canale : **#swepc**

Potete usare xchat per linux, ma ce ne sono molti altri...



« Last Edit: January 28, 2012, 09:00:51 am by Nimda »

Report to moderator



## Forum - la nascita

*schermata 6/6*


**Nimda**  
 Experienced  
 Newbie  
 ★★★★★  
☐ Offline  
 Posts: 53  


Re: Testare una WEP da finestra su Linux  
 • Reply #6 on: January 26, 2012, 05:39:44 am •


Quote

Io di linux sono un esperto, se siete interessati, ci sentiamo su **#swepc** su Freenode, così parliamo più facilmente. Per chi non lo conoscesse, è una rete IRC:

- lista server : [https://freenode.net/irc\\_servers.shtml](https://freenode.net/irc_servers.shtml)
- canale : **#swepc**

Potete usare xchat per linux, ma ce ne sono molti altri...

« Last Edit: January 26, 2012, 09:00:51 am by Nimda »

Report to moderator  Logged


**Melissa**  
 Newbie  
 ★  
☐ Offline  
 Posts: 4  


Re: Testare una WEP da finestra su Linux  
 • Reply #7 on: January 26, 2012, 04:32:39 pm •

Quote

Report to moderator  Logged



► [vai alla divisione dei compiti](#)

## Le dinamiche della community di sviluppo

In questa sezione vedremo le dinamiche di una community in una community.

- divisione dei compiti
- creazione di un repository
- condivisione di un repository
- test del codice e bugfix
- mantenimento del codice

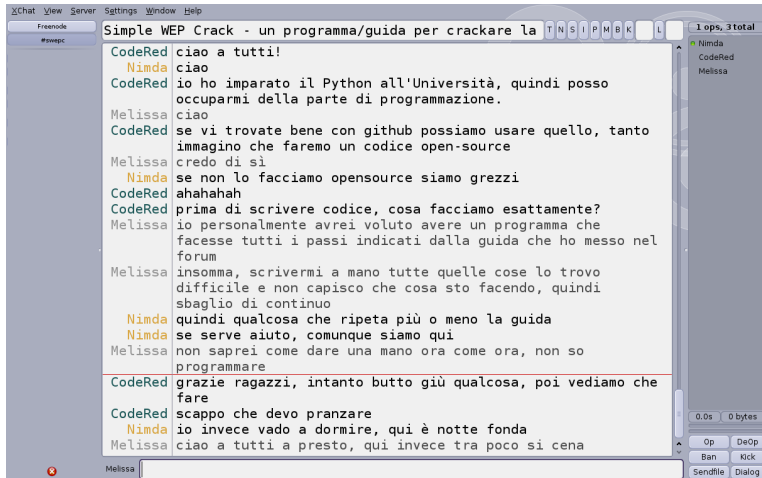


**Apri la chat IRC**





## Divisione dei compiti








## Divisione dei compiti

---

### Divisione dei compiti

I compiti per ogni persona attiva della community si definiscono quindi come:

- ▶  CodeRed - Programmatore
- ▶  Nimda - Esperto del sistema
- ▶  Melissa - Designer





## Creazione del repository

---

*registrazione a GitHub 1/4*

### Lavorare in gruppo

Alcuni aspetti sono fondamentali o spesso utili per lavorare bene in un *team* di sviluppo:

- ▶ una chiara e corretta **divisione dei compiti**
- ▶ **comunicazioni efficaci ed efficienti** tra i membri del gruppo
- ▶ uso di **repository comuni**



## registrazione a GitHub 2/4



## Creazione del repository

*registrazione a GitHub 3/4*

**Create your personal account**

**Username**  
CodeRed ✓  
This will be your username — you can enter your organization's username next.

**Email Address**  
codered@virus.com ✓  
You will occasionally receive account related emails. We promise not to share your email with anyone.

**Password**  
\*\*\*\*\* ✓  
Use at least one lowercase letter, one numeral, and seven characters.

**Confirm your password**  
\*\*\*\*\*

By clicking on "Create an account" below, you are agreeing to the [Terms of Service](#) and the [Privacy Policy](#).

**Create an account**

**You'll love GitHub**

- Unlimited collaborators
- Unlimited public repositories
- ✓ Great communication
- ✓ Friction-less development
- ✓ Open source community

cosa offre GitHub





## Creazione del repository

*registrazione a GitHub 4/4*

The screenshot shows the GitHub 'Create your personal account' form. The form fields are: Username (CodeRed), Email Address (codered@virus.com), Password (masked), and Confirm Password (masked). All fields have green checkmarks indicating they are valid. To the right, a box titled 'You'll love GitHub' lists benefits: Unlimited collaborators, Unlimited public repositories, Great communication, Friction-less development, and Open source community. At the bottom, there is a green 'Create an account' button. Annotations include a blue arrow pointing from the 'Create an account' button to the 'come in tutte le registrazioni...' text, and another blue arrow pointing from the 'You'll love GitHub' box to the 'cosa offre GitHub' text.

**Create your personal account**

**Username**  
CodeRed ✓  
This will be your username — you can enter a organization's username next.

**Email Address**  
codered@virus.com ✓  
You will occasionally receive account related emails. We promise not to share your email with anyone.

**Password**  
\*\*\*\*\* ✓  
Use at least one lowercase letter, one numeral, and seven characters.

**Confirm Password**  
\*\*\*\*\* ✓

By clicking on "Create an account" below, you are agreeing to the [Terms of Service](#) and the [Privacy Policy](#).

**Create an account**

**You'll love GitHub**

**Unlimited** collaborators  
**Unlimited** public repositories

- ✓ Great communication
- ✓ Friction-less development
- ✓ Open source community

**come in tutte le registrazioni...**

**cosa offre GitHub**





## Creazione del repository

*creazione 1/6*

### Repository comune

Creare un repository è più o meno come avere una directory condivisa in rete tra più utenti scelti, gestito in genere da un **sistema di controllo versione e gestione del codice sorgente**.

In repository di questo tipo, ogni collaboratore può, secondo i suoi permessi:



- ▶ aggiungere, modificare o eliminare file e directory;
- ▶ rivedere e scaricare versioni relative a modifiche precedenti.
- ▶ altro...








## Creazione del repository

creazione 2/6

  [explore](#) [gist](#) [blog](#) [help](#)  [CodeRed](#) [+](#) [-](#) [x](#) [y](#) [z](#)

 **Owner**


 **Repository name**

 **CodeRed** ▼


 /

Great repository names are short and memorable. Need inspiration? How about **flaming-wallhack**.

**Description** (optional)

 **Public**

Anyone can see this repository. You choose who can commit.


 **Private**


You choose who can see and commit to this repository.

☒ **Initialize this repository with a README**

This will allow you to `git clone` the repository immediately. Skip this step if you have already run `git init` locally.

ⓘ



**Licenses** 


**None**

Apache License 2.0

GNU GPL v2.0

© 2014 GitHub, Inc. [Terms](#) [Privacy](#) [Security](#) [Contact](#)

[Status](#) [API](#) [Training](#) [Shop](#) [Blog](#) [About](#)







## Creazione del repository

creazione 3/6

Owner: CodeRed / Repository name: simple-wepcrack

Great repository names are short and memorable. Need inspiration? How about **flaming-wallhack**.

Description (optional): Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WIFI

Public: Anyone can see this repository. You choose who can commit.

Private: You choose who can see and commit to this repository.

☒ Initialize this repository with a README  
This will allow you to `git clone` the repository immediately. Skip this step if you have already run `git init` locally.

Add .gitignore: None Add a license: None

Create repository

Licenses: None, Apache License 2.0, GNU GPL v2.0

© 2014 GitHub, Inc. Terms Privacy Security Contact Status API Training Shop Blog About



## Creazione del repository

creazione 4/6

Owner: CodeRed / Repository name: simple-wepcrack

Great repository names are short and memorable. Need inspiration? How about **flaming-wallhack**.

Description (optional): Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WIFI

Public: Anyone can see this repository. You choose who can commit.

Private: You choose who can see and commit to this repository.

☒ Initialize this repository with a README  
This will allow you to `git clone` the repository immediately. Skip this step if you have already run `git init` locally.

Add .gitignore: None | Add a license: None

Licenses: None, Apache License 2.0, GNU GPL v2.0

© 2014 GitHub, Inc. | Terms | Privacy | Security | Contact

tutti leggono  
ma si sceglie  
chi lo scrive





## Creazione del repository

creazione 5/6

The screenshot shows the GitHub 'Create repository' form. The 'Owner' is set to 'CodeRed' and the 'Repository name' is 'simple-wepcrack'. The 'Description' is 'Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WIFI'. The 'Visibility' is set to 'Public'. The 'Initialize this repository with a README' checkbox is checked. A license selection dropdown is open, showing 'None', 'Apache License 2.0', and 'GNU GPL v2.0'. A blue arrow points from the text 'tutti leggono ma si sceglie chi lo scrive' to the 'Public' visibility option. Another blue arrow points from the text 'non dimentichiamo la giusta licenza' to the license dropdown menu.

Owner: CodeRed / Repository name: simple-wepcrack

Great repository names are short and memorable. Need inspiration? How about **flaming-wallhack**.

Description (optional): Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WIFI

☒ Public: Anyone can see this repository. You choose who can commit.

☐ Private: You choose who can see and commit to this repository.

☒ Initialize this repository with a README: This will allow you to git clone the repository immediately. Skip this step if you have already run git init locally.

Add .gitignore: None

Add a license: None

Licenses: Filter licenses... None, Apache License 2.0, GNU GPL v2.0

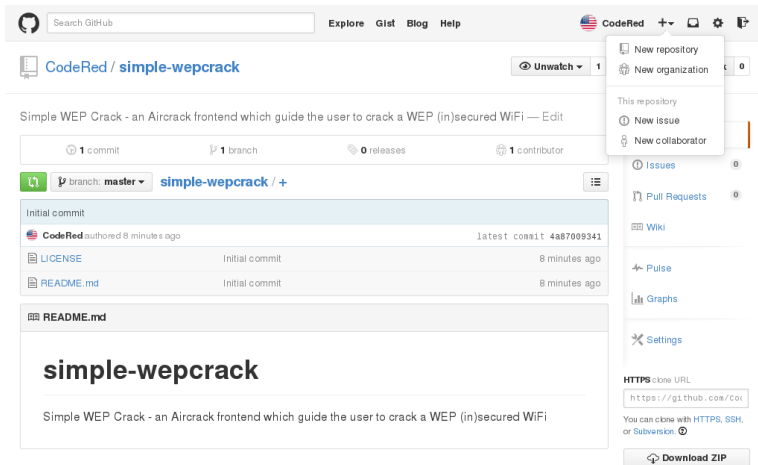
tutti leggono ma si sceglie chi lo scrive

non dimentichiamo la giusta licenza



## Creazione del repository

creazione 6/6



The screenshot shows a GitHub repository page for 'simple-wepcrack' by user 'CodeRed'. The repository description is 'Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi'. It shows 1 commit, 1 branch (master), 0 releases, and 1 contributor. The 'Initial commit' section lists files: LICENSE, README.md, and a commit message 'Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi'. The right sidebar contains links to Issues, Pull Requests, Wiki, Pulse, Graphs, and Settings. At the bottom right, there is a 'Download ZIP' button and a small cartoon character.

Search GitHub

Explore Gist Blog Help

CodeRed +

CodeRed / simple-wepcrack

Unwatch 1

Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi — Edit

1 commit 1 branch 0 releases 1 contributor

branch: master simple-wepcrack / +

Initial commit

CodeRed authored 8 minutes ago latest commit 4a8709341

File	Commit	Time
LICENSE	Initial commit	8 minutes ago
README.md	Initial commit	8 minutes ago

README.md

### simple-wepcrack

Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi

Issues 0

Pull Requests 0

Wiki

Pulse

Graphs

Settings

HTTPS clone URL

`https://github.com/CodeRed/simple-wepcrack`

You can clone with [HTTPS](#), [SSH](#), or [Subversion](#).

Download ZIP



► [vai alla condivisione del repository](#)

## Condividere il repository

Più tipologie di sviluppatori possono usufruire dello stesso spazio di lavoro.

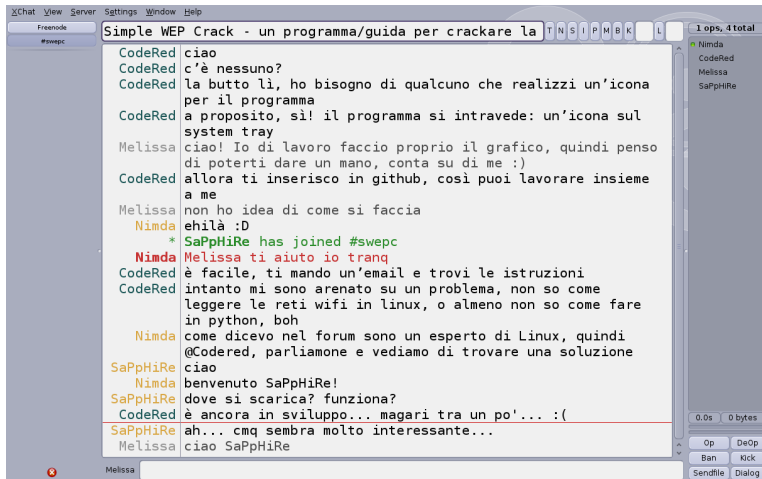
- programmatori
- grafici e designer
- sistemisti
- linguisti
- maintainer
- esperti in marketing
- ...

... vediamo i collaboratori su #swepc ...



**Apri la chat IRC**





The screenshot shows a chat application window with a title bar containing 'Simple WEP Crack - un programma/guida per crackare la'. The chat area displays a conversation between several users: CodeRed, Melissa, Nimda, and SaPpHiRe. The messages discuss the development of a program to crack WEP, with CodeRed providing instructions and Melissa asking for help. A system message indicates that SaPpHiRe has joined the channel. The chat interface includes a menu bar (Chat, View, Server, Settings, Window, Help), a status bar (1 ops, 4 total), and a list of users on the right. A small cartoon character is visible in the bottom right corner.

```
Chat View Server Settings Window Help
Simple WEP Crack - un programma/guida per crackare la TNSIPMBK L 1 ops, 4 total
#swepc
CodeRed ciao
CodeRed c'è nessuno?
CodeRed la butto lì, ho bisogno di qualcuno che realizzi un'icona
per il programma
CodeRed a proposito, sì! il programma si intravede: un'icona sul
system tray
Melissa ciao! Io di lavoro faccio proprio il grafico, quindi penso
di poterti dare un mano, conta su di me :)
CodeRed allora ti inserisco in github, così puoi lavorare insieme
a me
Melissa non ho idea di come si faccia
Nimda ehilà :D
* SaPpHiRe has joined #swepc
Nimda Melissa ti aiuto io tranq
CodeRed è facile, ti mando un'email e trovi le istruzioni
CodeRed intanto mi sono arenato su un problema, non so come
leggere le reti wifi in linux, o almeno non so come fare
in python, boh
Nimda come dicevo nel forum sono un esperto di Linux, quindi
@Codedred, parliamone e vediamo di trovare una soluzione
SaPpHiRe ciao
Nimda benvenuto SaPpHiRe!
SaPpHiRe dove si scarica? funziona?
CodeRed è ancora in sviluppo... magari tra un po'... :(
SaPpHiRe ah... cmq sembra molto interessante...
Melissa ciao SaPpHiRe
```

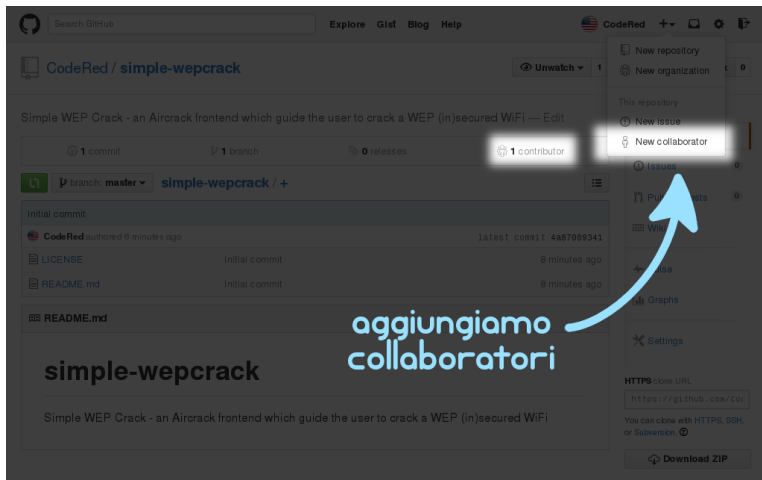
## Condivisione del repository

creazione 1/6

The screenshot shows a GitHub repository page for 'CodeRed / simple-wepcrack'. The repository is described as 'Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi'. It has 1 commit, 1 branch, 0 releases, and 1 contributor. The 'master' branch is selected. The commit history shows an initial commit by 'CodeRed' 8 minutes ago. The repository includes a 'LICENSE' file and a 'README.md' file. The README content is visible, showing the title 'simple-wepcrack' and the description 'Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi'. On the right side, there is a sidebar with links to 'Issues', 'Pull Requests', 'Wiki', 'Pulse', 'Graphs', and 'Settings'. At the bottom right, there is a 'Download ZIP' button and a small cartoon character.

## Condivisione del repository

creazione 2/6



CodeRed / simple-wepcrack

Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi — Edit

1 commit 1 branch 0 releases 1 contributor

branch: master simple-wepcrack / +

Initial commit

File	Commit	Time
LICENSE	Initial commit	8 minutes ago
README.md	Initial commit	8 minutes ago

aggiungiamo collaboratori

simple-wepcrack

Simple WEP Crack - an Aircrack frontend which guide the user to crack a WEP (in)secured WiFi

New repository  
New organization  
This repository  
New issue  
New collaborator  
Issues  
Pull requests  
Wiki  
Discussions  
Graphs  
Settings

HTTPS clone URL  
https://github.com/CodeRed/simple-wepcrack

You can clone with HTTPS, SSH, or Subversion.


Download ZIP











## Condivisione del repository





creazione 3/6



[Explore](#) [Gist](#) [Blog](#) [Help](#)

 **CodeRed**    

 **CodeRed** / [simple-wepcrack](#)

 **Unwatch**  **1**  **Star** **0**  **Fork** **0**



[Options](#)



**Collaborators**

[Webhooks & Services](#)








[Deploy keys](#)

**Collaborators** Full access to the repository

 **Melissa** 

 **Nimda** 

**Add collaborator**





## Condivisione del repository

creazione 4/6

Search GitHub

Explore Gist Blog Help

CodeRed + - ⚙️

CodeRed / simple-wepcrack

Unwatch 1 Star 0 Fork 0

Options


**Collaborators**

Webhooks & Services

Deploy keys

**Collaborators**

Full access to the repository

	Melisa	×
	Nimda	×

Type a username

Add collaborator

aggiunti (devono avere un account)

© 2014 GitHub, Inc. Terms Privacy Security Contact

Status API Training Shop Blog About





## Condivisione del repository

creazione 5/6

The screenshot shows a user profile for 'Melissa' on a GitHub-like platform. The header includes a search bar, navigation links (Explore, Gist, Blog, Help), and user avatars. The profile section shows the user's name 'Melissa' with a dropdown arrow, a 'News Feed' tab, and links to 'Pull Requests' and 'Issues'. A recent activity log entry states 'CodeRed added Melissa to CodeRed/simple-weprack 2 minutes ago'. Below this is a 'Welcome to GitHub! What's next?' message with links to 'Create a repository', 'Tell us about yourself', 'Browse interesting repositories', and 'Follow @github on Twitter'. On the right, the 'Your repositories' section shows a '+ New repository' button and a search bar. Below the search bar are tabs for 'All', 'Public', 'Private', 'Sources', and 'Forks'. The 'All' tab is selected, showing a repository named 'CodeRed/simple-weprack'. Below the repository list is a 'Subscribe to your news feed' button. The footer contains copyright information '© 2014 GitHub, Inc.', links for 'Terms', 'Privacy', 'Security', and 'Contact', a GitHub logo, and links for 'Status', 'API', 'Training', 'Shop', 'Blog', and 'About'.

Search GitHub

Explore Gist Blog Help

Melissa

News Feed Pull Requests Issues

CodeRed added Melissa to CodeRed/simple-weprack 2 minutes ago

Welcome to GitHub! What's next? (39 minutes ago)

Create a repository

Tell us about yourself

Browse interesting repositories

Follow @github on Twitter

Your repositories 1 + New repository

Find a repository...

All Public Private Sources Forks

CodeRed/simple-weprack

Subscribe to your news feed

© 2014 GitHub, Inc. Terms Privacy Security Contact

Status API Training Shop Blog About





## Condivisione del repository

creazione 6/6

The screenshot shows a GitHub profile for user 'Melissa'. Annotations include:

- A blue arrow pointing to the user's name 'Melissa' in the top navigation bar, with the text **utente Melissa** written next to it.
- A blue arrow pointing to the repository **CodeRed/simple-weprack** in the 'Your repositories' section, with the text **adesso ha un repository condiviso da CodeRed** written below it.

Other visible elements on the page include the search bar, user avatars, a welcome message, and various navigation links.





## Lavoro di gruppo




---

I vari collaboratori della community quindi contribuiscono attivamente sul repository, ovvero ognuno, simultaneamente, lavora allo stesso progetto.

È compito del sistema di versionamento e gestione del codice sorgente unire correttamente le versioni di sviluppo aggiunte via via.

### Un'occhiata da vicino

Vediamo brevemente, ma da vicino, in cosa consiste il lavoro dei tre membri della community. Ricordiamo

- ▶  CodeRed - Programmatore
- ▶  Nimda - Esperto del sistema
- ▶  Melissa - Designer





## Lavoro di gruppo

*CodeRed - Programmatore*





CodeRed è il programmatore del gruppo. Lavora in python.  
È open source: bene! Spiamo il suo lavoro...



## Lavoro di gruppo

CodeRed - Programmatore

 CodeRed è il programmatore del gruppo. Lavora in python.  
È open source: bene! Spiamo il suo lavoro...

 **CodeRed** 2 days ago First upload

1 contributor

Executable File | 18 lines (16 slocc) | 570 byte
 

Raw
 Blame
 History

```

1 import sys
2 from PyQt4 import QtCore, QtGui
3 class SimpleWEPCrack(QtGui.QApplication):
4     def __init__(self, arguments):
5         super(SimpleWEPCrack, self).__init__(arguments)
6         self.systemTrayIcon = QtGui.QSystemTrayIcon()
7         self.systemTrayIcon.setIcon(QtGui.QPixmap('res/swepec_gray.png'))
8         self.trayMenu = QtGui.QMenu()
9         self.trayMenu.addAction("Exit", self.quit)
10        self.systemTrayIcon.setContextMenu(self.trayMenu)
11        self.systemTrayIcon.show()
12
13    def main():
14        app = SimpleWEPCrack( sys.argv )
15        sys.exit(app.exec_())
16
17    if __name__ == '__main__':
18        main()
    
```





## Lavoro di gruppo

*estratto di codice sorgente*

```
1 import sys
2 from PyQt4 import QtCore, QtGui
3 class SimpleWEPCrack (QtGui.QApplication):
4     def __init__(self, arguments):
5         super(SimpleWEPCrack, self).__init__(arguments)
6         self.systemTrayIcon = QtGui.QSystemTrayIcon()
7         self.systemTrayIcon.setIcon(QtGui.QPixmap('res/swepc_gray.png'))
8         self.trayMenu = QtGui.QMenu()
9         self.trayMenu.addAction("Exit", self.quit)
10        self.systemTrayIcon.setContextMenu(self.trayMenu)
11        self.systemTrayIcon.show()
12
13    def main():
14        app = SimpleWEPCrack( sys.argv )
15        sys.exit(app.exec_())
16
17    if __name__ == '__main__':
18        main()
```







## Lavoro di gruppo

---

*Nimda - Esperto linux*

- ☒ Nimda è l'esperto Linux del gruppo.





## Lavoro di gruppo

*Nimda - Esperto linux*

- Nimda è l'esperto Linux del gruppo.

## Cosa fa per la community

- ▶ Tiene il server IRC online
- ▶ Ospita il sito web dell'applicazione
- ▶ Aiuta il programmatore per le parti più riguardanti Linux



## Lavoro di gruppo

*shell e script*

Spiano il suo lavoro...

The screenshot shows a Linux desktop environment with three windows:

- Terminal:** Displays the user's commands and the system's output.
 

```
nimda@fedora:~$ write iw1.sh &
[1] 459
nimda@fedora:~$ write iw1.awk &
[2] 460
nimda@fedora:~$ cat /proc/net/
anycast6      icmp      ip_tables_targets  psc
arp           icmp6     ipv6_route         pty
bnep          if_inet6  l2cap              raw
dev           igmp      mcfilter           raw
dev_mcast     igmp6     mcfilter6          rfc
dev_snmp5     ip6_flowlabel  netfilter/         rou
fib_trie      ip_mr_cache netlink            rpc
fib_tristat   ip_mr_vif  netstat            rt6
hci           ip_tables_matches packet             rt_
hidp          ip_tables_names protocols          rt_c
```
- iw1.sh - KWrite:** Shows the content of the shell script.
 

```
#!/bin/sh
# Copyright (C) Nimda. All rights reserved.
AWKSCRIPT="iw1.awk"
```
- iw1.awk - KWrite:** Shows the content of the AWK script.
 

```
# AWK Script
# Copyright (C) Nimda. All rights reserved.
/BSS / {
    MAC = $2
}
/SSID/ {
    wifi[MAC]["SSID"] = $2
}
/primary channel/ {
    wifi[MAC]["channel"] = $NF
}
# Insert new block here
END {
    printf "%s\t%s\n", "SSID", "channel"
    for (w in wifi) {
        printf "%s\t%s\n", wifi[w]["SSID"], wifi[w]["channel"]
    }
}
```





## Lavoro di gruppo

---

*Melissa - Grafica e design*


 Melissa è la professionista di grafica e design.





## Lavoro di gruppo

*Melissa - Grafica e design*

 Melissa è la professionista di grafica e design.

### Come contribuisce

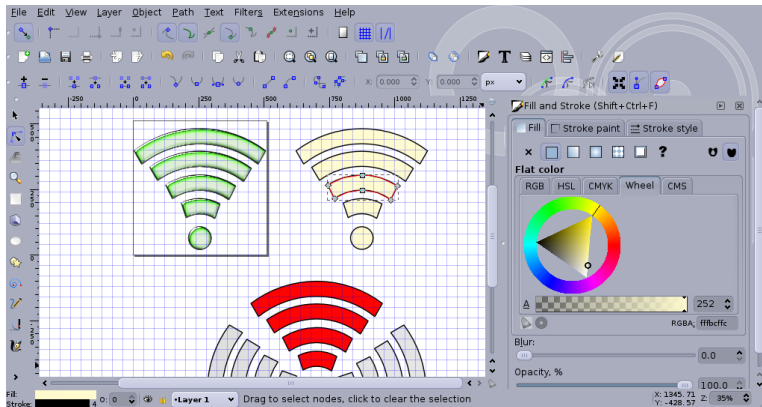
- ▶ Genera le icone per il programma, in formato vettoriale.
- ▶ Disegna e crea il sito web dell'applicazione



## Lavoro di gruppo

*grafica vettoriale*

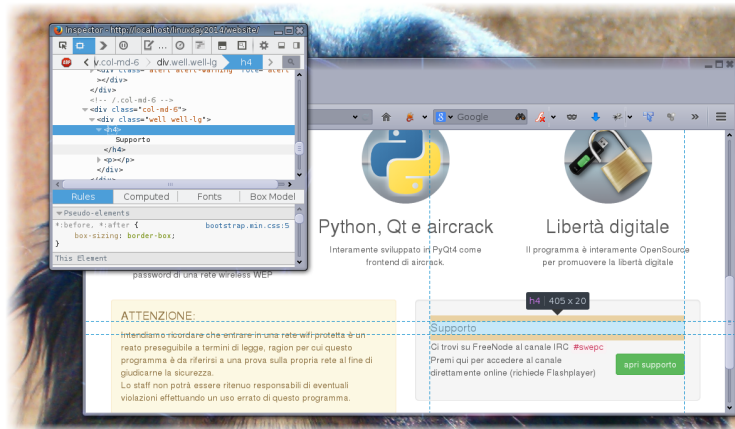
Icone in formato vettoriale con **Inkscape**...



## Lavoro di gruppo

*web design*

Melissa lavora al design della pagina web dell'applicazione...





## Lavoro di gruppo

[▶ vai al test del codice](#)

### Il software cresce e diventa testabile

Sebbene un primo *test rozzo* viene fatto dal programmatore stesso, il test vero e proprio è considerato un'attività che deve essere da lui staccata.

Il **test del codice** può essere:

- ▶ automatico (aiutato da qualche framework magari)
- ▶ manuale
- ▶ ... tutte le sfumature tra automatico e manuale

... vediamo come pensano di fare test su #swepc ...

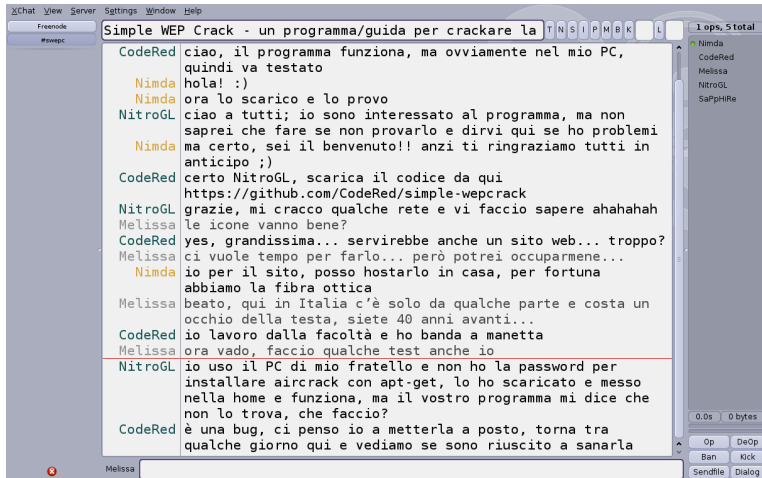


Apri la chat IRC





## Lavoro di gruppo



The screenshot shows a chat window with a title bar containing 'XChat View Server Settings Window Help'. The window title is 'Simple WEP Crack - un programma/guida per crackare la'. The chat area shows a conversation between several users: CodeRed, Nimda, NitroGL, and Melissa. The messages are as follows:

- CodeRed**: ciao, il programma funziona, ma ovviamente nel mio PC, quindi va testato
- Nimda**: hola! :)
- Nimda**: ora lo scarico e lo provo
- NitroGL**: ciao a tutti; io sono interessato al programma, ma non saprei che fare se non provarlo e dirvi qui se ho problemi
- Nimda**: ma certo, sei il benvenuto!! anzi ti ringraziamo tutti in anticipo ;)
- CodeRed**: certo NitroGL, scarica il codice da qui <https://github.com/CodeRed/simple-wepcrack>
- NitroGL**: grazie, mi cracco qualche rete e vi faccio sapere ahahahah
- Melissa**: le icone vanno bene?
- CodeRed**: yes, grandissima... servirebbe anche un sito web... troppo?
- Melissa**: ci vuole tempo per farlo... però potrei occuparmene...
- Nimda**: io per il sito, posso hostarlo in casa, per fortuna abbiamo la fibra ottica
- Melissa**: beato, qui in Italia c'è solo da qualche parte e costa un occhio della testa, siete 40 anni avanti...
- CodeRed**: io lavoro dalla facoltà e ho banda a manetta
- Melissa**: ora vado, faccio qualche test anche io
- NitroGL**: io uso il PC di mio fratello e non ho la password per installare aircrack con apt-get, lo ho scaricato e messo nella home e funziona, ma il vostro programma mi dice che non lo trova, che faccio?
- CodeRed**: è una bug, ci penso io a metterla a posto, torna tra qualche giorno qui e vediamo se sono riuscito a sanarla

On the right side of the chat window, there is a list of users: Nimda, CodeRed, Melissa, NitroGL, and SaPpHiRe. Below this list, there are buttons for 'Op', 'DeOp', 'Ban', 'Kick', 'Sendfile', and 'Dialog'. At the bottom right, there is a small cartoon character of a pirate.



## Test del codice e bugfix

---

In questa simulazione di community si fanno solo dei test manuali, ovvero si prova l'applicazione per intero e si inviano i problemi alla community.

### Segnalazione degli errori

Sebbene GitHub abbia un **sistema interno di segnalazione degli errori** (cosa comune offerta dai *provider* di repository), nel nostro esempio è stato segnalato un bug nel canale IRC #swepec di supporto.



## Test del codice e bugfix

---

In questa simulazione di community si fanno solo dei test manuali, ovvero si prova l'applicazione per intero e si inviano i problemi alla community.

### Segnalazione degli errori

Sebbene GitHub abbia un **sistema interno di segnalazione degli errori** (cosa comune offerta dai *provider* di repository), nel nostro esempio è stato segnalato un bug nel canale IRC #swepec di supporto.

**Tutti i test dovrebbero essere portati a termine e con esito positivo prima di rilasciare una versione del software**

Ma spesso non succede, non è infrequente la tendenza a rilasciare software non testato, offrendo frequenti aggiornamenti.





## Mantenimento

► vai all'attacco della WEP!

### Mantenimento del prodotto

Durante la vita della community di sviluppo, possono cambiare molte cose

- membri (si aggiunge un programmatore)
- risorse online (non si usa più GitHub, ma un altro provider)
- risorse fisiche (si acquista un server)
- ...

Mentre altre tendono a rimanere pressoché uguali, eccetto qualche precisazione o modifica **filosofia**, **mission**, ...



Visualizza il sito web su browser

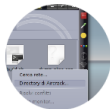


## Mantenimento



Simple WEP Crack è un programma che guida l'utente Linux a recuperare la password della propria WEP o a verificarne la sicurezza

[Scarica sorgente](#)
[Supporto online](#)



Icona semplice



Python. Ota aircrack



Libertà digitale





## Le community

Il concetto di community

La community e la libertà digitale

## Simulazione di una community

Forum - la nascita

Divisione dei compiti

Creazione del repository

Condivisione del repository

Lavoro di gruppo

Test del codice e bugfix

Mantenimento

## Crackare una WEP (semplice)

Su cosa si basa la cifratura WEP

Esempio facilitato

Trovare la chiave WEP segreta

## Demo dell'applicazione





## Su cosa si basa la cifratura WEP

[▶ salta questa sezione](#)

La cifratura WEP si basa su l'operazione *xor*, in simbolo  $\oplus$ , tra numeri binari.

### XOR - è molto semplice

- ▶  $0 \oplus 0 = 1 \oplus 1 = 0$  - se i bit sono uguali fa 0;
- ▶  $0 \oplus 1 = 1 \oplus 0 = 1$  - se sono diversi fa 1.

E vale chiaramente la proprietà:  $A \oplus A = 0$ .





## Su cosa si basa la cifratura WEP

### Debolezza della cifratura

- ▶ Se  $A$  e  $B$  sono due messaggi segreti e  $K$  la chiave di cifratura, il messaggio cifrato risulta essere  $T = A \oplus K$ ,  $U = B \oplus K$ .
- ▶ L'attaccante legge quindi  $T$  e  $U$  e sa che vale la proprietà:  
$$T \oplus U = A \oplus K \oplus B \oplus K = A \oplus B.$$
- ▶ Usare la stessa chiave quindi offre troppe informazioni che aiutano l'attaccante a trovare la chiave e i messaggi originali.

Per evitare il problema si usano dei **numeri casuali in combinazione con la chiave**, detti VI (**V**ettore di **I**nizializzazione)

**Il problema della WEP è che ne usa troppo pochi** e le ripetizioni sono comunque numerose.







## Esempio facilitato

*problema*

Supponiamo che una banda dei Corleone debba inviare alla banda dei Tartaglia l'orario per scambiarsi un ostaggio rapito la sera prima. Ovviamente la polizia vuole sapere quest'orario.

La polizia sa che lo scambio avverrà tra l'1 di notte e le 4 di notte, perché altrimenti c'è troppa gente in giro, ma se i mafiosi vedono un solo poliziotto uccideranno l'ostaggio, per cui le tempistiche sono molto importanti.





## Esempio facilitato

*messaggi*

I Corleone vogliono inviare ai Tartaglia l'orario 3:12 coi messaggi 3 e 12 e hanno precedentemente concordato la chiave binaria di cifratura 1010.

messaggi originali	3	12
in binario	0011	1100
cifratura	$\oplus$	$\oplus$
	1010	1010
	=	=
	1001	0110
messaggi cifrati	9	6

La polizia vede i messaggi  $T = 9$  e  $U = 6$ , quindi l'orario 9:06.





## Esempio facilitato

*violazione della chiave*

La polizia ha avuto una soffiata da un informatore che gli orari che scelgono i Corleone sono, per scaramanzia, sempre con i minuti multipli delle ore.

La polizia, conosce la proprietà  $T \oplus U = A \oplus B$ , quindi  $1001 \oplus 0110 = 1111$ . Quindi sa che i minuti e le ore hanno, in binario, cifre tutte diverse.

	binario	$\oplus$ 1111	orario finale
1	0001	1110	1:14
2	0010	1101	2:13
3	0011	1100	3:12
4	0100	1011	4:11





## Esempio facilitato

*violazione della chiave*

La polizia ha avuto una soffiata da un informatore che gli orari che scelgono i Corleone sono, per scaramanzia, sempre con i minuti multipli delle ore.

La polizia, conosce la proprietà  $T \oplus U = A \oplus B$ , quindi  $1001 \oplus 0110 = 1111$ . Quindi sa che i minuti e le ore hanno, in binario, cifre tutte diverse.

	binario	$\oplus$ 1111	orario finale
<del>1</del>	<del>0001</del>	<del>1110</del>	<del>1:14</del>
<del>2</del>	<del>0010</del>	<del>1101</del>	<del>2:13</del>
3	0011	1100	3:12
<del>4</del>	<del>0100</del>	<del>1011</del>	<del>4:11</del>





## Trovare la chiave WEP segreta

---




### Step by step

I passi principali per violare una rete WEP sono i seguenti:

- ▶ identificare la rete protetta da violare
- ▶ creare una scheda di WiFi virtuale in modalità *Monitor*
- ▶ essere certi di poter iniettare pacchetti sulla rete
- ▶ (opzionale) fare autenticazioni fasulle
- ▶ catturare i pacchetti della rete da violare
- ▶ (opzionale) replicare richieste ARP per generare traffico utile
- ▶ ... crackare la password



Per la presentazione ringrazio molto i partecipanti della community simulata:

- ▶ **Francesca Pirisi**, nel ruolo di  Melissa
- ▶ **Gian Michele Meloni**, nel ruolo di  Nimda
- ▶ **Matteo Pani**, nel ruolo di  CodeRed

che hanno contribuito a renderla meno *noiosa*.





## Simple WEP Crack

- ▶ Il codice mostrato è reale ed è open-source con licenza GPL.
- ▶ È programmato in Python e Qt.
- ▶ Funziona nel PC del programmatore e non vi è stato il tempo per condurre nessun tipo di test, per cui potrebbe funzionare in altri linux, ma non è garantito.
- ▶ È su GitHub e lo si può trovare e scaricare dal seguente link:  
<https://github.com/nitrogl/simple-wepecrack>



## Le community

Il concetto di community

La community e la libertà digitale

## Simulazione di una community

Forum - la nascita

Divisione dei compiti

Creazione del repository

Condivisione del repository

Lavoro di gruppo

Test del codice e bugfix

Mantenimento

## Crackare una WEP (semplice)

Su cosa si basa la cifratura WEP

Esempio facilitato

Trovare la chiave WEP segreta

## Demo dell'applicazione







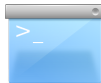
*demo - Simple WEP Crack*



**esegui SimpleWEPCrack  
da utente normale**



**esegui SimpleWEPCrack  
da superutente**



**(se qualcosa va storto c'è sempre il terminale)**





# Fine

**sono tutti OPEN  
con il SOURCE degli altri**