



# From z3r0 70 r007 in 2 hours

Lezione sul campo di Cyber Security

# Presentazione



**Antonio Cavuoto**

Cyber Security Analyst

Studente di Informatica - Laurea Magistrale  
all'Università degli Studi di Torino

Backend development

Email:

[antonio.cavuoto@edu.unito.it](mailto:antonio.cavuoto@edu.unito.it)

Github:

<https://github.com/doc-dev>

Lavoro in vari settori dell'informatica, ma i miei campi d'azione principali sono lo sviluppo di software e l'Ethical Hacking. Lavoro anche allo sviluppo di architetture e protocolli distribuiti e decentralizzati.

Section 1

Siamo davvero al sicuro ?



# Quanti di voi usano questi prodotti/servizi ?



# Apple

<https://stallman.org/apple.html>

## Location-Based Services

To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.

Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

Sa sempre dove ti trovi

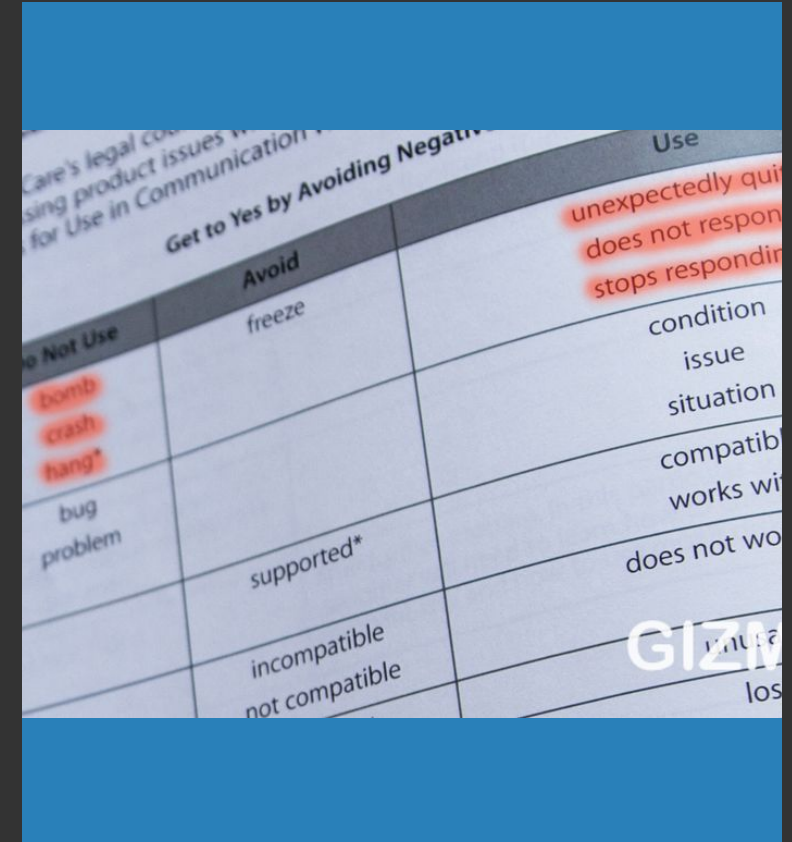
## Safari & Privacy

Done

### Fraudulent Website Warning

When Fraudulent Website Warning is enabled, Safari will display a warning if the website you are visiting is a suspected phishing website. Phishing is a fraudulent attempt to steal your personal information, such as usernames, passwords and other account information. A fraudulent website masquerades as a legitimate one, such as a bank, financial institution or email service provider. Before visiting a website, Safari may send information calculated from the website address to Google Safe Browsing and Tencent Safe Browsing to check if the website is fraudulent. These safe browsing providers may also log your IP

Sa quali siti visiti e quando lo fai



Insegna ai venditori come farti il lavaggio del cervello

# Facebook

<https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them>

- Memorizza ogni tuo accesso al sistema e sa cosa ti piace (glielo dici tu con ogni like)
- Conserva ogni tuo messaggio audio per farlo elaborare alla sua intelligenza artificiale
- Ha il pieno controllo di WhatsApp, per cui potenzialmente sa anche con chi comunichi.
- Vende i tuoi dati ad aziende di terze parti, vedi scandalo Cambridge Analitica

<https://stallman.org/facebook.html>

# Google

- Google sa tutto quello che fai online

Attraverso Gmail sa cosa compri, qual'è la tua carta di credito e di fatto tutto ciò che passa per la tua mail

- Google play ti traccia

È autorizzato a mandare agli sviluppatori i tuoi dati personali

- Google Home è sempre attivo e conserva tutto l'audio intorno a lui

Non importa che qualcuno stia effettivamente parlando o no

- Memorizza svariati Gigabyte per ogni utente

<https://www.youtube.com/watch?v=hLjht9uJWgw>

<https://stallman.org/google.html#surveillance>



# Facciamo un esperimento





Section 2

Ma i problemi non finiscono qui

# Ogni giorno in rete accadono cose del genere

HOME INTERNET WEB

## Il virus Wannacry è ancora in giro e 1,7 milioni di computer sono a rischio

A due anni dall'exploit del malware, che ha colpito in 150 paesi, ci sono 1,7 milioni di terminali che potrebbero essere infettati da un download del virus perché sprovvisti di una patch



COLPITI ANCHE I SITI DI CONFINDUSTRIA

## Anonymous contro il governo, attacco hacker il 5 novembre



(© Ralf-Udo Thiele/imageBROKER)

2' di lettura

Anonymous Italia, il gruppo di attivisti hacker legato alla rete **Anonymous**, ha dato il via lo scorso 29 ottobre a una «settimana nera» di attacchi a portali istituzionali, dalle università alle associazioni degli industriali.

TECH FINANCE POLITICS STRATEGY LIFE BUSINESS INTELLIGENCE ALL

## The man accused of hacking into celebrity iCloud accounts and stealing naked photos has agreed to plead guilty

Steve Gorman, Reuters 14/11/2016, 10:36 AM



An Illinois man accused of breaking into the Apple iCloud and Gmail accounts of celebrities to obtain their private photos and videos has agreed to plead guilty to a felony computer hacking charge, prosecutors said on Friday.

---

## ECONOMIA & Finanza

Home Finanza con Bloomberg Lavoro Calcolatori Finanza Personale **AFFARI & FINANZA** Osservatorio

## Unicredit, attacchi hacker su 400mila clienti. "Nessun conto a rischio"

Ricostruite due violazioni dei dati personali, tra l'autunno del 2016 e pochi giorni fa. "Non è stato acquisito nessun dato, quali le password, che possa consentire l'accesso ai conti dei clienti o che permetta transazioni non autorizzate". Procura in azione

Section 3

Adesso entriamo in gioco noi

# Che cos'è un Security Analyst



Gli analisti della sicurezza informatica valutano, pianificano e attuano misure di sicurezza per aiutare a proteggere un'organizzazione da violazioni della sicurezza e attacchi alle sue reti e sistemi informatici. Questo lavoro prevede la simulazione di attacchi per identificare le vulnerabilità, testare nuovi software per proteggere i dati dell'azienda e aiutare gli utenti ad aderire a nuovi regolamenti e processi per garantire che la rete rimanga sicura. Gli analisti della sicurezza informatica di solito lavorano come parte di un dipartimento IT per varie organizzazioni e in genere lavorano a tempo pieno. Questo lavoro è più adatto a persone con ottima conoscenza ed esperienza nell'uso di computer e software di sicurezza a cui piace pensare in modo critico per trovare nuovi modi per risolvere i problemi.



Domande ?

Section 4

Passiamo ad una  
dimostrazione pratica

# Proviamo a fare un hacking in diretta

Ecco quello che mi servirà

## Macchina Virtuale

Un programma dove eseguire un sistema operativo diverso dal mio.

## Kali linux

Un sistema operativo usato spesso dagli Hacker per svolgere le loro operazioni

## Rete virtuale

Così non verrò arrestato mentre svolgo varie operazioni illegali

## Strumenti del mestiere

- Nmap
- Netdiscover
- Metasploit (e tanti altri ancora)

Scommessa: cerchiamo di completare l'hacking prima che finisca la lezione

# Grazie per l'attenzione !

E ricordate sempre:

