Introduzione alla cyber security, ethical hacking e CTF

Leonardo Taccari
<s1069964@studenti.univpm.it>

Sommario

Concetti fondamentali
- Cyber Security
- CIA: Confidentiality, Integrity, Availability
- Ethical Hacking
- Software Libero

Capture The Flag (CTF)

Un po' di pratica!

Conclusioni

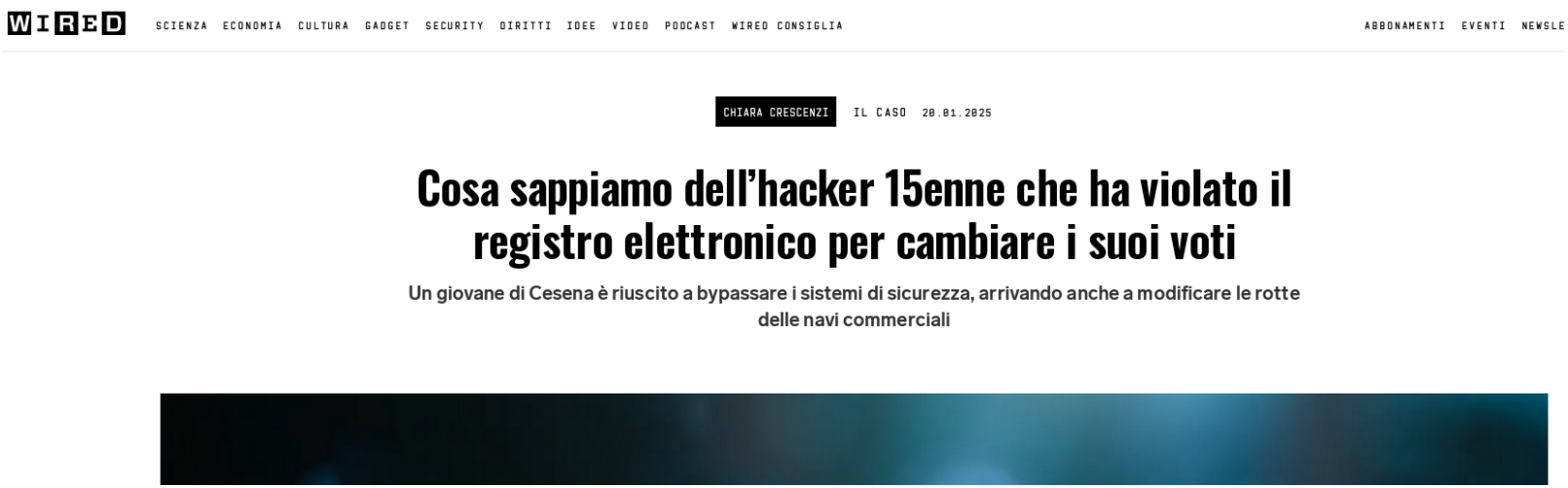
Riferimenti

Un'occhiata a notizie recenti riguardante la cyber security

- Perché la cyber security è importante?
- Proviamo a "sfogliare" i giornali delle ultime settimane
- Come questi incidenti possono coinvolgerci?

Un'occhiata a notizie recenti riguardante la cyber security

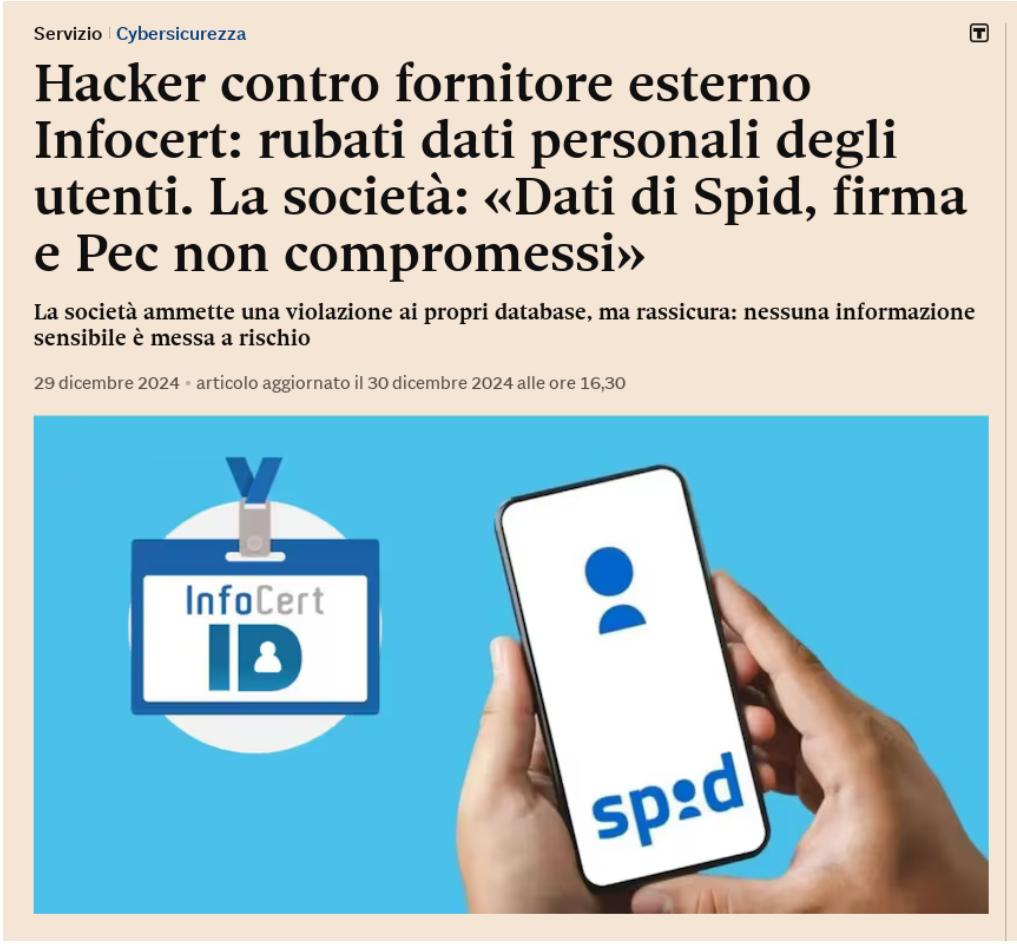
Ragazzo viola registro elettronico per cambiare i suoi voti



Cosa sappiamo dell'hacker 15enne che ha violato il registro elettronico per cambiare i suoi voti, Chiara Crescenzi, Wired, 20/01/2025 (link)

Un'occhiata a notizie recenti riguardante la cyber security

Rubati dati personali di più di 5.5 milioni di utenti InfoCert



Servizio | Cybersicurezza

Hacker contro fornitore esterno Infocert: rubati dati personali degli utenti. La società: «Dati di Spid, firma e Pec non compromessi»

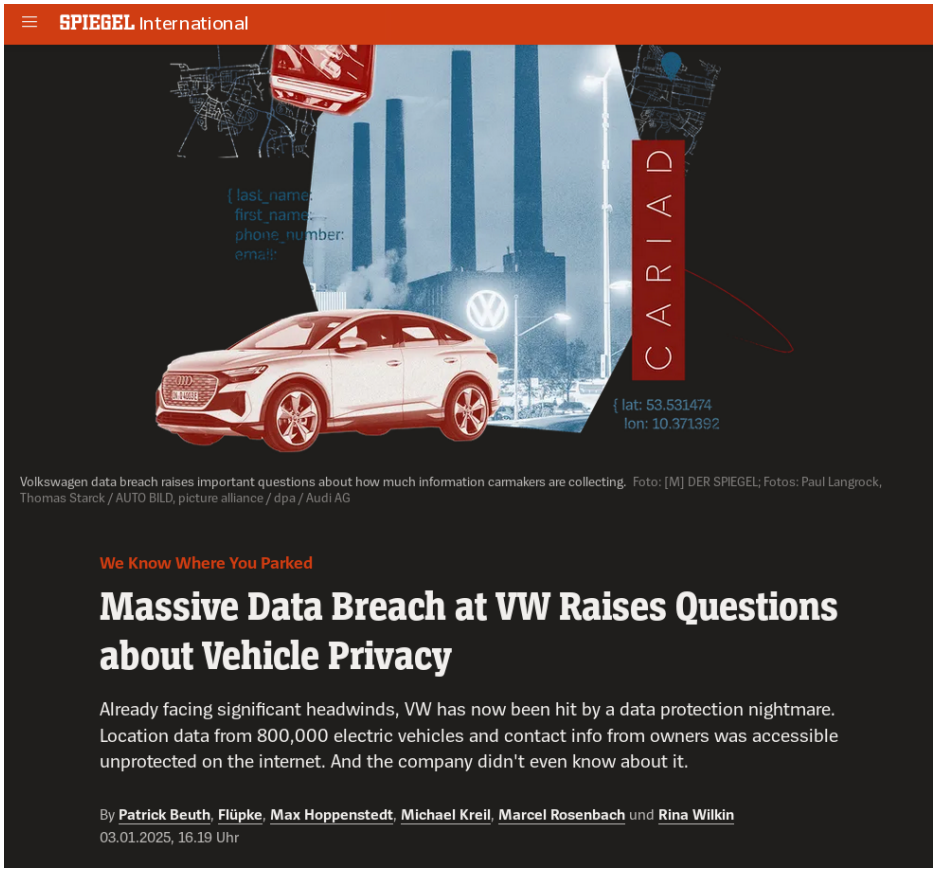
La società ammette una violazione ai propri database, ma rassicura: nessuna informazione sensibile è messa a rischio

29 dicembre 2024 • articolo aggiornato il 30 dicembre 2024 alle ore 16,30

Hacker contro fornitore esterno Infocert: rubati dati personali degli utenti. La società: «Dati di Spid, firma e Pec non compromessi», Il Sole 24 Ore, 29/12/2024 (link)

Un'occhiata a notizie recenti riguardante la cyber security

Fuga di dati da Volkswagen: accessibili in chiaro posizioni geografiche e dati personali dei possessori di 800000 automobili



Massive Data Breach at VW Raises Questions about Vehicle Privacy, Patrick Beuth, Flüpke, Max Hoppenstedt, Michael Kreil, Marcel Rosenbach e Rina Wilkin, Der Spiegel, 03/01/2025 (link)

Concetti fondamentali

Cyber Security: definizioni

Alcune definizioni dal NIST [1] Computer Security Resource Center (CSRC) Glossary (via NIST SP 800-30).

[1] National Institute of Standards and Technology

Cyberspace

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cyber Security: definizioni

Cyber Security

Cyber Security

The ability to protect or defend the use of cyberspace from cyber attacks.

CIA: Confidentiality, Integrity, Availability

I pilastri della cyber security sono costituiti dalla "triade" CIA: Confidentiality, Integrity, Availability.

Confidentiality (Confidenzialità, Riservatezza)

La confidentiality (confidenzialità, riservatezza) è la proprietà che garantisce che le risorse sono accessibili solo ai soggetti autorizzati.

Integrity (Integrità)

La integrity (integrità) è la proprietà che garantisce che le risorse non siano alterate o distrutte da soggetti non autorizzati ad accederle.

Availability (Disponibilità)

La availability (disponibilità) è la proprietà che garantisce un accesso affidabile e tempestivo alle risorse da parte dei soggetti autorizzati.

Cyber security e CIA (Confidentiality, Integrity, Availability)

Quando una o più di queste proprietà viene violata si ha un problema di cybersecurity.

Vulnerabilità

Bug, difetto, debolezza o esposizione accidentale di un'applicazione, sistema, dispositivo o servizio che può portare alla violazione di confidentiality, integrity o availability.

CIA: Confidentiality, Integrity, Availability I

Esempio: Registro elettronico

Le proprietà CIA dipendono dal sistema considerato. Cerchiamo di contestualizzarle nel Registro elettronico!

confidentiality uno studente può visualizzare solo i propri voti
(se uno studente potesse vedere i voti di altri studenti si avrebbe una fuga di informazioni (unauthorized disclosure))

integrity uno studente può accedere ai voti solo in lettura, non può modificarli; un docente può assegnare una votazione che va da 1 a 10
(se uno studente potesse modificare i voti o un docente potesse mettere una votazione di 11 si avrebbe una modifica non autorizzata (unauthorized modification) o modifica impropria (improper modification))

CIA: Confidentiality, Integrity, Availability II

Esempio: Registro elettronico

availability uno studente deve poter leggere i voti, un docente deve poter assegnare i voti (se un docente non potesse assegnare delle valutazioni si avrebbe una "ritenuta" non autorizzata (unauthorized withholding))

Ethical Hacking

Da 'The Jargon File (version 4.4.7, 29 Dec 2003)':

Hacker

hacker n. [originally, someone who makes furniture with an axe]
1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. RFC1392, the Internet Users' Glossary, usefully amplifies this as: «A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular».

Da ‘Errore di Sistema’ di Edward Snowden:

> *È da qui che ha origine l’attività dell’hacker: dalla consapevolezza del legame sistematico tra input e output, tra causa ed effetto. L’hacker non esiste soltanto in informatica, ma ovunque ci siano delle regole. Per hackerare un sistema occorre conoscere le sue regole ancor meglio di chi le ha create o di chi quel sistema lo gestisce, e sfruttare al massimo la discrepanza tra il modo in cui il sistema dovrebbe funzionare e il suo effettivo funzionamento. Nel trarre vantaggio da questi usi non intenzionali, gli hacker non infrangono le regole, ma piuttosto le demistificano.*

Da 'The Jargon File (version 4.4.7, 29 Dec 2003)':

{Black,Gray,White} Hacker

black hat

1. [common among security specialists] A cracker, someone bent on breaking into the system you are protecting. Oppose the less common white hat for an ally or friendly security specialist; the term gray hat is in occasional use for people with cracker skills operating within the law, e.g. in doing security evaluations. All three terms derive from the dress code of formulaic Westerns, in which bad guys wore black hats and good guys white ones.

Ethical Hacking I

Ethical hacker

Un ethical hacker è un white hat hacker e opera legalmente ed in modo etico.

Legge 547 del 1993, Art.615-ter. (Accesso abusivo ad un sistema informatico e telematico).

> *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

In altre parole, possiamo esclusivamente - legalmente - attaccare sistemi di cui abbiamo un permesso. Possibili modi per fare ciò:

Bug Bounty programmi in cui organizzazioni permettono a ricercatori di trovare vulnerabilità offrendo loro una ricompensa (esempi: HackerOne, Intigriti, Bugcrowd)

Ethical Hacking II

Ethical hacker

CTF (Capture the Flag) competizioni di cyber security (le vedremo tra poco più in dettaglio!)

Software Libero

Durante il corso utilizzeremo software libero (free software), vediamo alcune definizioni dal Progetto GNU.

Software Libero

Il software libero è software che rispetta la libertà degli utenti e la comunità. In breve, significa che gli utenti hanno la libertà di eseguire, copiare, distribuire, studiare, modificare e migliorare il software.

Software Libero

Quattro libertà essenziali

Libertà 0 Libertà di eseguire il programma come si desidera, per qualsiasi scopo

Libertà 1 Libertà di studiare come funziona il programma e di modificarlo in modo da adattarlo alle proprie necessità

Libertà 2 Libertà di ridistribuire copie in modo da aiutare gli altri

Libertà 3 Libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti da voi apportati (e le vostre versioni modificate in genere), in modo tale che tutta la comunità ne tragga beneficio

Software Libero

GNU/Linux ed altri software liberi

- GNU/Linux è anche il sistema operativo più diffuso nei server
- Gran parte dei software di cyber security - sia offensivi che difensivi - è software libero

Capture The Flag (CTF)

- CTF (Capture The Flag) sono delle competizioni di cyber security
- Ogni anno si svolgono 100ia di CTF a livello internazionale e la maggior parte di esse sono aperte a tutti
- CTFtime.org raccoglie la maggior parte di questi eventi
- Le CTF simulano uno scenario di cyber security. Lo scopo è effettuare un cyber attack. Quando si riesce a fare ciò con successo si ottiene una flag, che dimostra che abbiamo sfruttato la vulnerabilità e risolto la challenge

Capture The Flag (CTF)

Tipologie di CTF

Esistono tre tipologie di CTF:

Jeopardy challenge di diverse categorie (Web, Crypto, Binary). Si ottengono punti ogni volta che si risolve una challenge. Il punteggio può essere statico o dinamico.

Attack-Defence ogni squadra deve far girare dei servizi vulnerabili ed è responsabile di mantenere, aggiustare e difendere i servizi. Allo stesso tempo deve attaccare le squadre avversarie. Il punteggio è calcolato in base a:

Mixed formati vari, ad esempio wargames

- **attacco** flag catturate
- **difesa** flag perse
- **SLA** Service Level Agreement

Capture The Flag (CTF) I

OliCyber

- Durante il corso svolgeremo diverse challenge dal portale di addestramento di OliCyber
- OliCyber sono le Olimpiadi Italiane di Cybersicurezza, un programma di competizioni mirato a favorire e incentivare l'avvicinamento delle studentesse e degli studenti alle problematiche della cybersicurezza
- Sono organizzate dal Cybersecurity National Lab del CINI

Un po' di pratica!

- Svolgiamo la challenge Misc 01 - Sanity Check
- Svolgiamo la challenge Misc 02 - Suggerimenti
- Svolgiamo la challenge Misc 03 - Allegati

Compiti per casa

- Iscriversi a training.olicyber.it!
- (facoltativo/per approfondire) potete vedere nel Materiale didattico di OliCyber le lezioni:
  - Modulo Introduzione, MISC_1.1 - Introduzione
  - Modulo Extra, da CS_1.01 a CS_1.05

Conclusioni

- Abbiamo visto i concetti fondamentali di cyber security, ethical hacking e software libero
- Abbiamo visto che cosa sono le CTF e svolto un paio di CTF introduttive
- Abbiamo visto perché la cyber security è attuale ed importante e come può coinvolgerci

Riferimenti

- Materiale Didattico del Portale di allenamento delle Olimpiadi Italiane di Cybersicurezza
- pwn.college
- NIST CSRC Glossary
- The Jargon File
- CTFtime.org
- Wir wissen wo dein Auto steht, Volksdaten von Volkswagen, 38C3