ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

“Hacking dalle origini alla figura professionale dell'Ethical Hacker, accenni alle metodologie internazionali, regole di ingaggio e normativa nazionale.”

Massimiliano Graziani CEH CHFI CFE CIFI CFIP CDFP OPSA ACE TCNU

Roma 14/01/2022

Presentazione relatore

Massimiliano Graziani *attualmente CEO Cybera Srl e CISO Adora ICT Srl*

Fondatore, insieme ad altri nel 2005 del capitolo italiano dell'OWASP.

Socio fondatore del capitolo italiano dell' International Information Systems Forensics Association (IISFA), e dell'Osservatorio Nazionale Informatica Forense (ONIF), è in possesso delle seguenti certificazioni internazionali:

- CEH (v11 Certified Ethical Hacking rilasciata da Ec-Council)
- CHFI (Computer Hacking Forensic Investigator rilasciata da Ec-Council)
- CIFI (Certified Information Forensics Investigator rilasciata da IISFA)
- CFE (Certified Fraud Examiner rilasciata da ACFE)
- ACE (AccessData Certified Examiner rilasciata da AccessData)
- OPSA (OSSTMM Professional Security Analyst rilasciata da ISECOM)
- CIFIP (Certified Forensic Investigation Professional rilasciata da IICFIP)
- CDFP (Certified Digital Forensics Professional rilasciata da IICFIP).

CYBERA

Docente in materia di Digital Forensics Pratica presso Scuola di Polizia Tributaria della Guardia di Finanza (Corso Operativo di Computer Forensics con Logicube Dossier e Falcon), Università La Sapienza Roma (Corso Informatica Giuridica con Aterno), Università LUMSA Roma (Corso Diritto Penale dell'Informatica con Zanotti), Università di Salerno (Convegno La Tecnologia al servizio dell'Indagine Scientifica con De Santis, Cattaneo, Palmieri), Università del Molise (Master Information Security Management – Modulo Computer Forensics con Perrone), Università degli studi Link Campus University di Roma (modulo forensics di vari master, ultimo con Saccone). Docente volontario presso IISFA, OLAF, FF.OO., Consiglio Superiore Magistratura Milano, Ministero Economia e Finanze UCAMP, ISACA Roma e ACFE Italia e Centro Interforze di Formazione Intelligence/GE, Board of Directors ACFE Central.

Maggiori info sul mio background: www.cobrasoft.it

Ospiti di oggi

Alessio L.R. Pennasilico aka -=mayhem=-

Membro del Comitato Scientifico Clusit

Partner, Practice Leader Information & Cyber Security Advisory Team @ P4I

Security Evangelist & Ethical Hacker

Membro del Direttivo dell'Associazione Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano osservatori.net digital innovation

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

"Hacking dalle origini alla figura professionale dell'Ethical Hacker, accenni alle metodologie internazionali, regole di ingaggio e normativa nazionale.".

Ospiti di oggi

Avv.to Stefano Aterno

Partner di E-Lex dal 2020, ha collaborato in precedenza, a lungo, con lo studio in qualità di Of Counsel; è professore e avvocato con una esperienza ultraventennale in materia di delitti informatici e di cybercrime. Dal 2012 è certificato L.A. ISO 27001 ed è esperto di diritto e legislazione della cybersecurity

Avvocato, professore a contratto presso le Università di Foggia, Roma TRE e LUISS – Facoltà di Giurisprudenza.

Svolge la professione di avvocato e consulente prevalentemente nell'ambito del diritto penale e del diritto delle nuove tecnologie.

Certificato Lead auditor ISO 27001 (certificazione internazionale sulla sicurezza dei dati e delle informazioni) e certificato CIFI (Certified Information Forensics Investigator).

Ha pubblicato alcuni libri e numerosi articoli scientifici in tema di criminalità informatica, indagini informatiche e privacy; svolge attività di consulente in materia di privacy per importanti enti e organismi pubblici e per aziende private e multinazionali.

Ospiti di oggi

Alessia Valentini

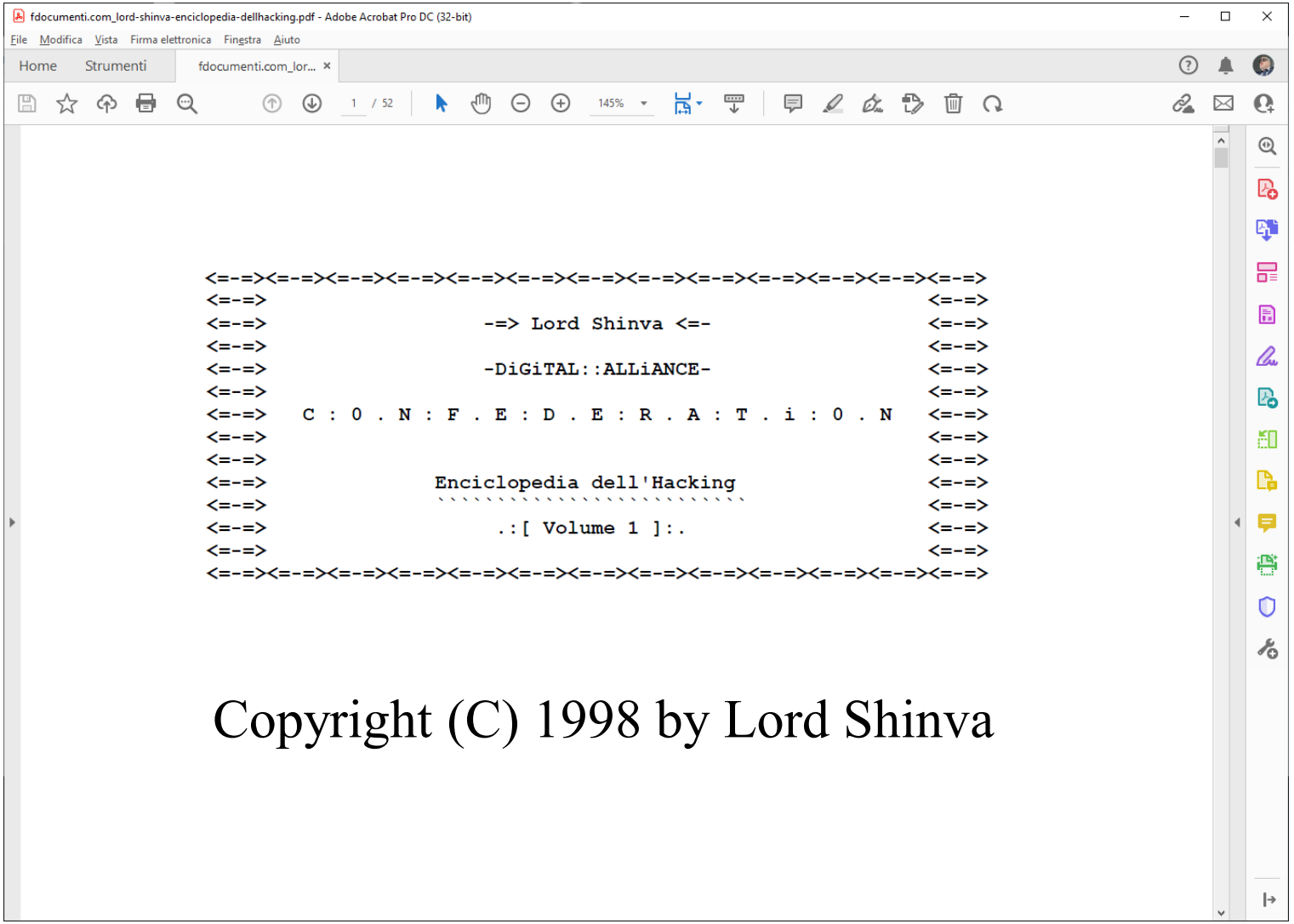
Alessia Valentini – Cybersecurity Liaison Officer, Consulente di Cybersecurity, Advisor e Giornalista in S3K spa.
E' un Cybersecurity Liason Officer con attività legate all'advisory, allo sviluppo del Business, e alla consulenza e strategia di Cybersecurity. Fa parte delle "Women for Security" la community di Cyberladies del Clusit.
È Giornalista (ODG del Lazio dal 2013) e scrive per StartUpItalia!, Cybersecurity 360/digital 360 e InfosecNEWS sui temi della Cybersecurity.
Per il Capitolo di ROMA dell'ISACA cura gli editoriali della newsletter mensile e partecipa ai lavori del workgroup sul FAIR CAM.
Certificata CISA/ISACA nel 2017. Consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016, ha partecipato ai lavori dell'Osservatorio Sicurezza Nazionale presso il CASD fino al 2013.

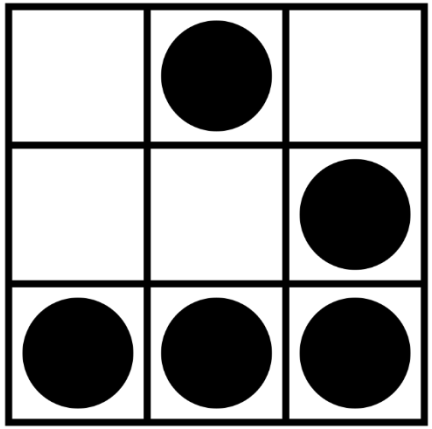
Infonde e diffonde la Cybersecurity sempre e comunque!

Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

Definire il termine **hacker**: la spiegazione in realtà è ben più complessa di quanto si possa immaginare: il significato attribuito a questo termine ha subito molti cambiamenti ed evoluzioni, determinate dal contesto storico, sociale, politico e normativo…





Il **Glider**, rappresentazione della navicella aliante nella teoria degli automi cellulari, proposto come emblema degli hacker.

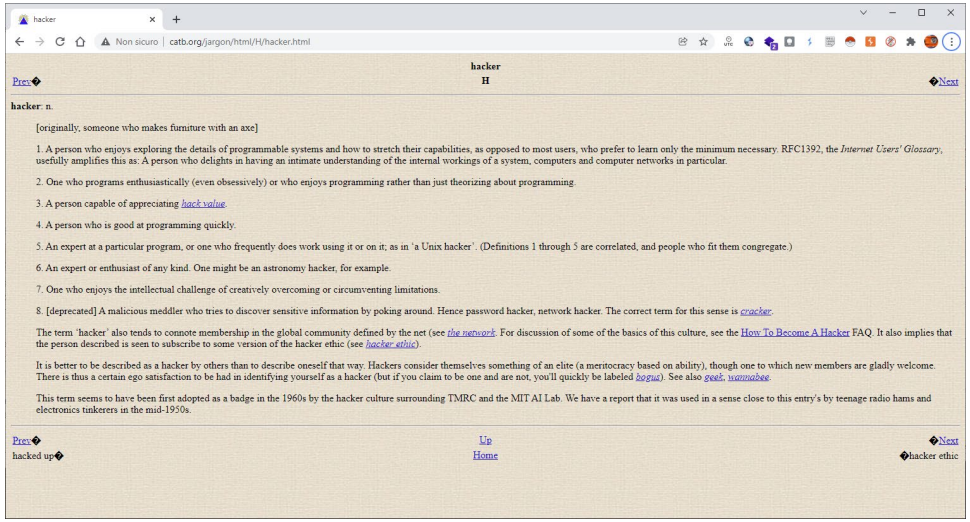
Proposto nel 2003 da Eric Steven Raymond ha riscosso un buon successo tra gli hacker e sostenitori. Il suo scopo principale è quello di colmare una lacuna ben precisa: avere un simbolo che identifichi tutti i sostenitori della comunità hacker indipendentemente dal linguaggio di programmazione preferito e/o sistema operativo più usato. Utilizzarlo non significa definirsi un hacker, anche perché è buona regola non autoproclamarsi tale: significa piuttosto esprimere rispetto verso gli ideali, la cultura e lo stile di vita hacker, riconoscendosi gli uni con gli altri.

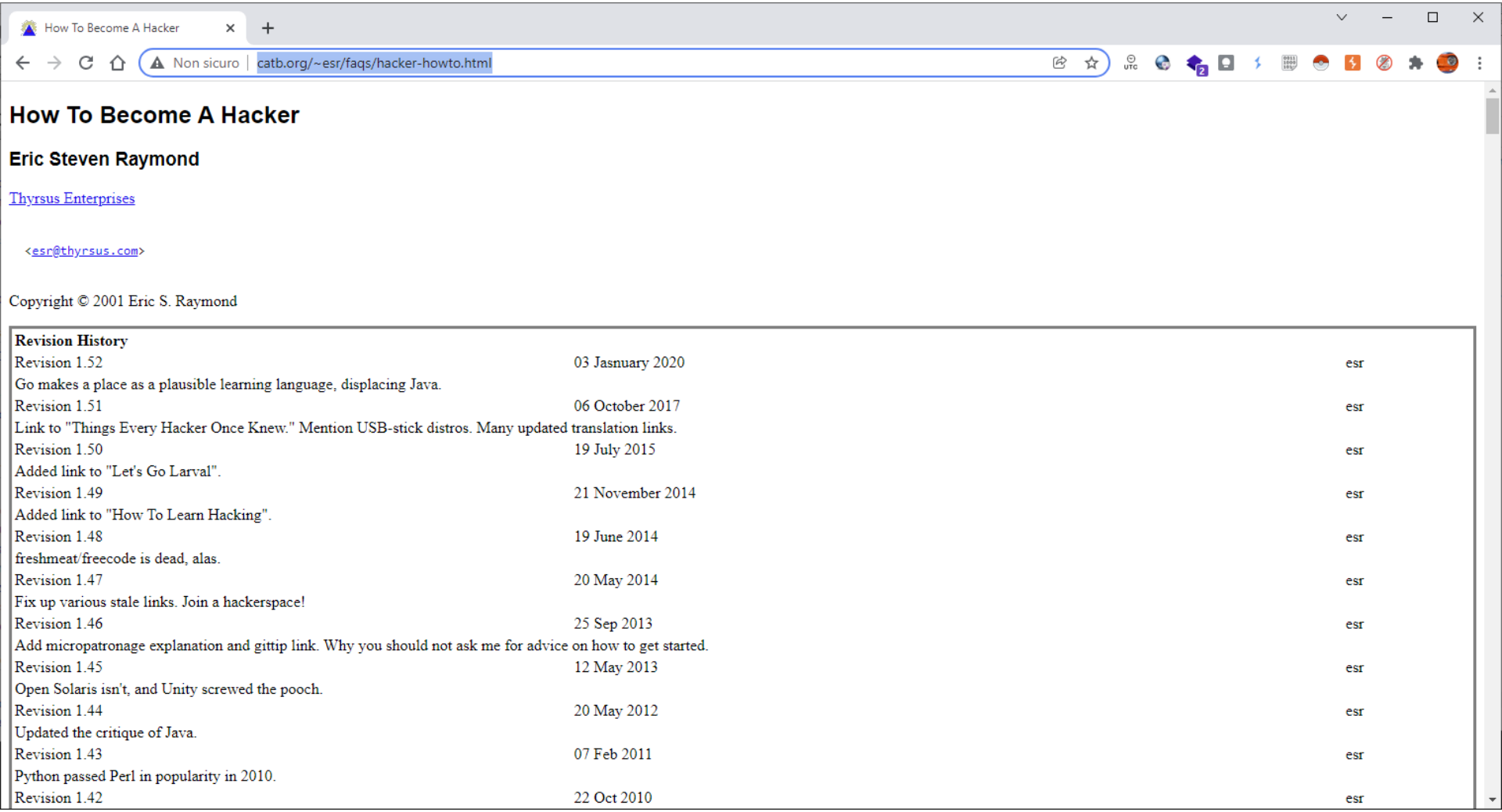
fonte: it.wikipedia.org

Da dove viene il termine hacker?

Hacker è un termine della lingua inglese che designa una persona che utilizza le proprie competenze informatiche per esplorare i dettagli dei sistemi programmabili e sperimenta come estenderne l'utilizzo

Jargon File, su *http://www.catb.org/*. URL consultato il 14 maggio 2019.





How To Become A Hacker

Non sicuro | catb.org/~esr/faqs/hacker-howto.html

How To Become A Hacker

Eric Steven Raymond

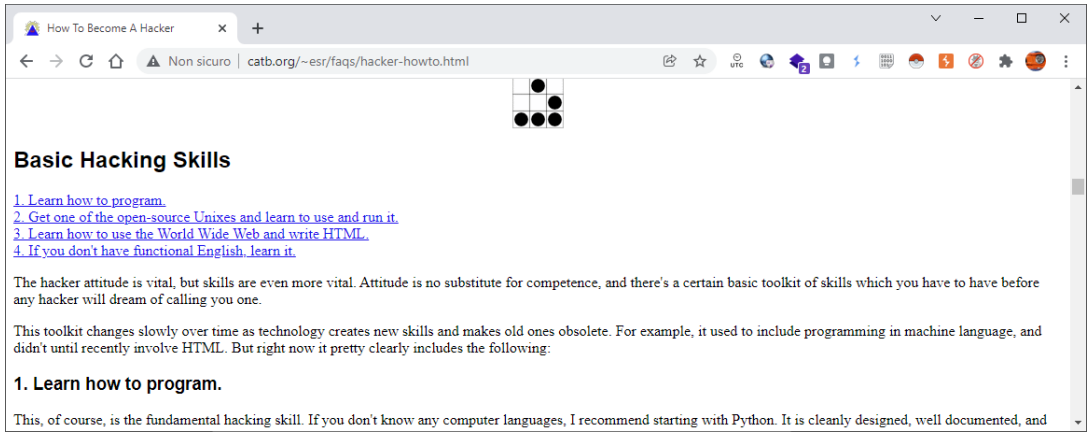
Thyrsus Enterprises

<esr@thyrsus.com>

Revision History		
Revision 1.52	03 Jasnuary 2020	esr
Go makes a place as a plausible learning language, displacing Java.		
Revision 1.51	06 October 2017	esr
Link to "Things Every Hacker Once Knew." Mention USB-stick distros. Many updated translation links.		
Revision 1.50	19 July 2015	esr
Added link to "Let's Go Larval".		
Revision 1.49	21 November 2014	esr
Added link to "How To Learn Hacking".		
Revision 1.48	19 June 2014	esr
freshmeat/freecode is dead, alas.		
Revision 1.47	20 May 2014	esr
Fix up various stale links. Join a hackerspace!		
Revision 1.46	25 Sep 2013	esr
Add micropatronage explanation and gittip link. Why you should not ask me for advice on how to get started.		
Revision 1.45	12 May 2013	esr
Open Solaris isn't, and Unity screwed the pooch.		
Revision 1.44	20 May 2012	esr
Updated the critique of Java.		
Revision 1.43	07 Feb 2011	esr
Python passed Perl in popularity in 2010.		
Revision 1.42	22 Oct 2010	esr

fonte: catb.org

fonte: catb.org



Basic Hacking Skills

1. Learn how to program.
2. Get one of the open-source Unixes and learn to use and run it.
3. Learn how to use the World Wide Web and write HTML.
4. If you don't have functional English, learn it.

The hacker attitude is vital, but skills are even more vital. Attitude is no substitute for competence, and there's a certain basic toolkit of skills which you have to have before any hacker will dream of calling you one.

L'etica hacker si basava infatti su cinque principi fondamentali:

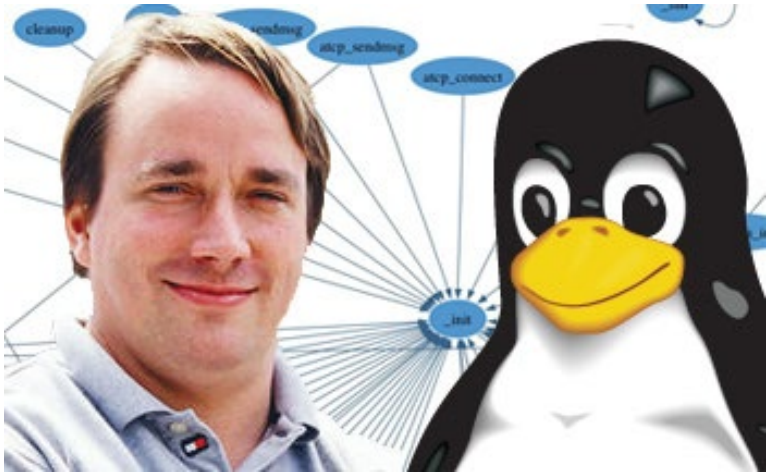
1. L'informazione vuole essere libera

2. Diffida dell'autorità (nel senso di «viola le regole»)

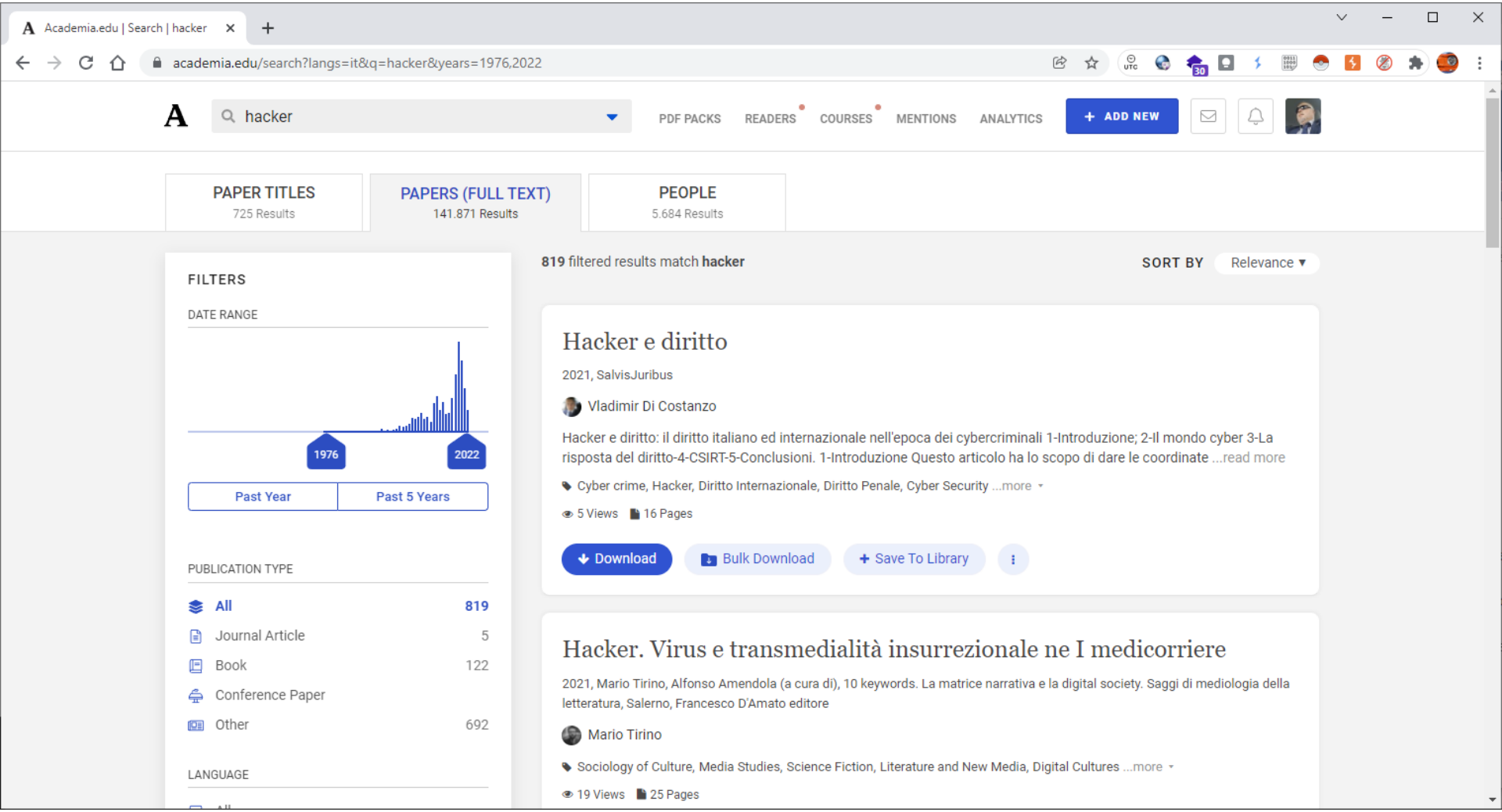
3. Gli hacker devono essere giudicati in base alle loro azioni, e non su pregiudizi o gerarchie sociali

4. Attraverso il computer puoi creare arte e bellezza

5. Il computer può cambiarti la vita in meglio



Linus Torvarlds, il giovane finlandese che ha progettato il sistema operativo Linux, che in forma open source, è stato perfezionato con l'aiuto di hacker in tutto il mondo, che lo hanno sviluppato, migliorato, studiando le potenzialità, e le carenze.
In questo modo, gratuitamente e con l'aiuto di molti hacker nel mondo, è stato possibile “hackerarlo”, per poterlo rendere uno dei migliori sistemi operativi al mondo.


Academia.edu | Search | hacker
academia.edu/search?langs=it&q=hacker&years=1976,2022
hacker
PDF PACKS
READERS
COURSES
MENTIONS
ANALYTICS
+ ADD NEW
PAPER TITLES
725 Results
PAPERS (FULL TEXT)
141.871 Results
PEOPLE
5.684 Results
FILTERS
DATE RANGE
1976
2022
Past Year
Past 5 Years
PUBLICATION TYPE
All 819
Journal Article 5
Book 122
Conference Paper
Other 692
LANGUAGE
819 filtered results match hacker
SORT BY
Relevance
Hacker e diritto
2021, SalvisJuribus
Vladimir Di Costanzo
Hacker e diritto: il diritto italiano ed internazionale nell'epoca dei cybercriminali 1-Introduzione; 2-Il mondo cyber 3-La risposta del diritto-4-CSIRT-5-Conclusioni. 1-Introduzione Questo articolo ha lo scopo di dare le coordinate ...read more
Cyber crime, Hacker, Diritto Internazionale, Diritto Penale, Cyber Security ...more
5 Views 16 Pages
Download
Bulk Download
+ Save To Library
Hacker. Virus e transmedialità insurrezionale ne I medicorriere
2021, Mario Tirino, Alfonso Amendola (a cura di), 10 keywords. La matrice narrativa e la digital society. Saggi di mediologia della letteratura, Salerno, Francesco D'Amato editore
Mario Tirino
Sociology of Culture, Media Studies, Science Fiction, Literature and New Media, Digital Cultures ...more
19 Views 25 Pages

Per comprendere l'hacking: storia

Non sicuro | adir.unifi.it/rivista/2003/tavassi/cap1.htm

Centro di ricerca interuniversitario su carcere, devianza, marginalità e governo delle migrazioni

ADIR - L'altro diritto

Il centro | I Quaderni | La Rivista | Laboratorio sullo sfruttamento lavorativo | Convenzioni | RUEBES | La ODV

LA RIVISTA / HACKING E CRIMINALITÀ INFORMATICA /

ISSN 1827-0565

← Precedente Successivo →

Capitolo I
Per comprendere l'hacking: storia e valori di una cultura attuale

Federico Tavassi La Greca, 2003

Sommario: 1. *Hacking*: storia di un fenomeno sociale. - 2. L'esperienza italiana: dai videogiochi all'assalto della Rete. - 2.1 I primi significativi interventi delle forze dell'ordine: le operazioni *Hardware 1*, *Peacelink* e ICE-TRAP. - 3. Chi sono gli *hackers* - Premessa. - 3.1. *Hackers*: una prima lettura. - 3.2. Essere *hacker*. - 3.3. La sfida attuale. - 3.4. *Hackers*: per una filosofia di vita.

1. *Hacking*: storia di un fenomeno sociale

La storia degli *hackers*, ufficialmente (o meno) (1), ha inizio nell'inverno 1958-59, al Massachussets Institute of Technology (Mit) di Cambridge, il quartiere universitario di Boston. L'istituto ospitava al suo interno una serie di gruppi, piccoli club che univano studenti dagli interessi comuni fuori dalle ore di studio. Uno di questi gruppi era il *Tech model railroad club* (Tmrc), la cui stanza era quasi interamente occupata da un enorme plastico ferroviario molto dettagliato e perfettamente funzionante grazie ad un immenso intreccio di cavi, relè ed interruttori situati sotto il modello. Il club assegnava ai suoi soci una chiave d'accesso ai locali, ma prima che questo privilegio potesse essere concesso, lo studente doveva dedicare almeno quaranta ore di lavoro al plastico.

Il Tmrc era strutturato in due sottogruppi: alcuni soci realizzavano i modellini dei treni e curavano la parte scenografica della riproduzione. Altri, quelli che facevano parte della "Signal&Power Subcommittee" (S&P - sottocommissione per lo studio dei segnali e dell'energia), si occupavano di tutto ciò che accadeva sotto il modellino ferroviario.

La compagnia dei telefoni Western Electric, sponsor dell'istituto, procurava allo stesso i ricambi e i materiali necessari al corretto funzionamento del sistema telefonico universitario. Non di rado però qualche pezzo "sfuggiva" al controllo dei responsabili e finiva per essere riadattato ai nuovi scopi del club.

Con grande impegno e sincera passione, l'elaborato sistema che faceva muovere i trenini e funzionare i singoli scambi, era continuamente testato, smontato, riassemblato, riparato e perfezionato.

Steven Levy racconta che un progetto intrapreso o un prodotto costruito non soltanto per adempiere ad uno scopo specifico, ma che portasse con sé il piacere scatenato della pura partecipazione, era detto "hack". Il termine proveniva dal vecchio gergo del Mit: era stato a lungo usato per indicare gli scherzi elaborati che gli studenti si inventavano regolarmente (come rivestire di alluminio la cupola che dominava l'università). Ma il senso in cui era inteso da quelli del Tmrc denotava rispetto. Se un intelligente collegamento di relè si poteva definire un "hack semplice", si sarebbe inteso che, per qualificarsi come un "vero hack", l'impresa avrebbe dovuto dimostrare innovazione, stile, virtuosismo tecnico. "Perfino se uno avesse detto, autocommiserandosi, di aver 'fatto a pezzi il sistema', il talento con cui 'faceva a pezzi' gli poteva essere riconosciuto come notevole" (2). I più produttivi tra quelli che lavoravano al Signal and Power si definivano, con grande orgoglio, "*hackers*".

I trenini elettrici e gli Hackers | by

medium.com/@danielebottonibomber/i-trenini-elettrici...

Daniele Bottoni Bomber 48 Followers About Follow Sign in Get started

I trenini elettrici e gli Hackers

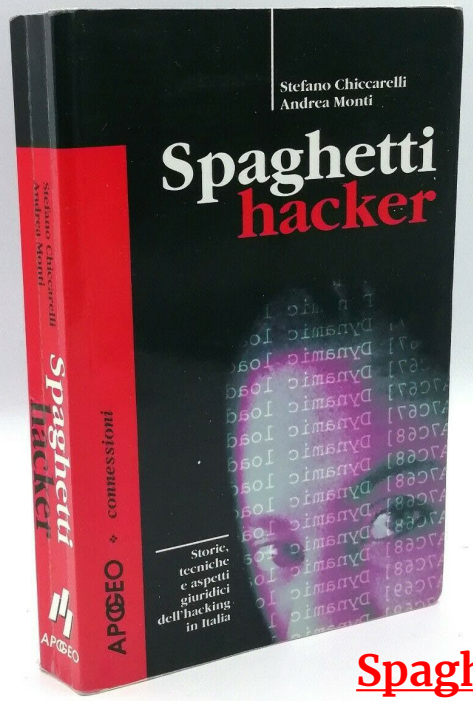
Daniele Bottoni Bomber Jan 12, 2017 · 8 min read

Risultati immagini per mit boston Tmrc 1959

Immagine del The Tech Model Railroad Club (TMRC) al M.I.T. di Boston

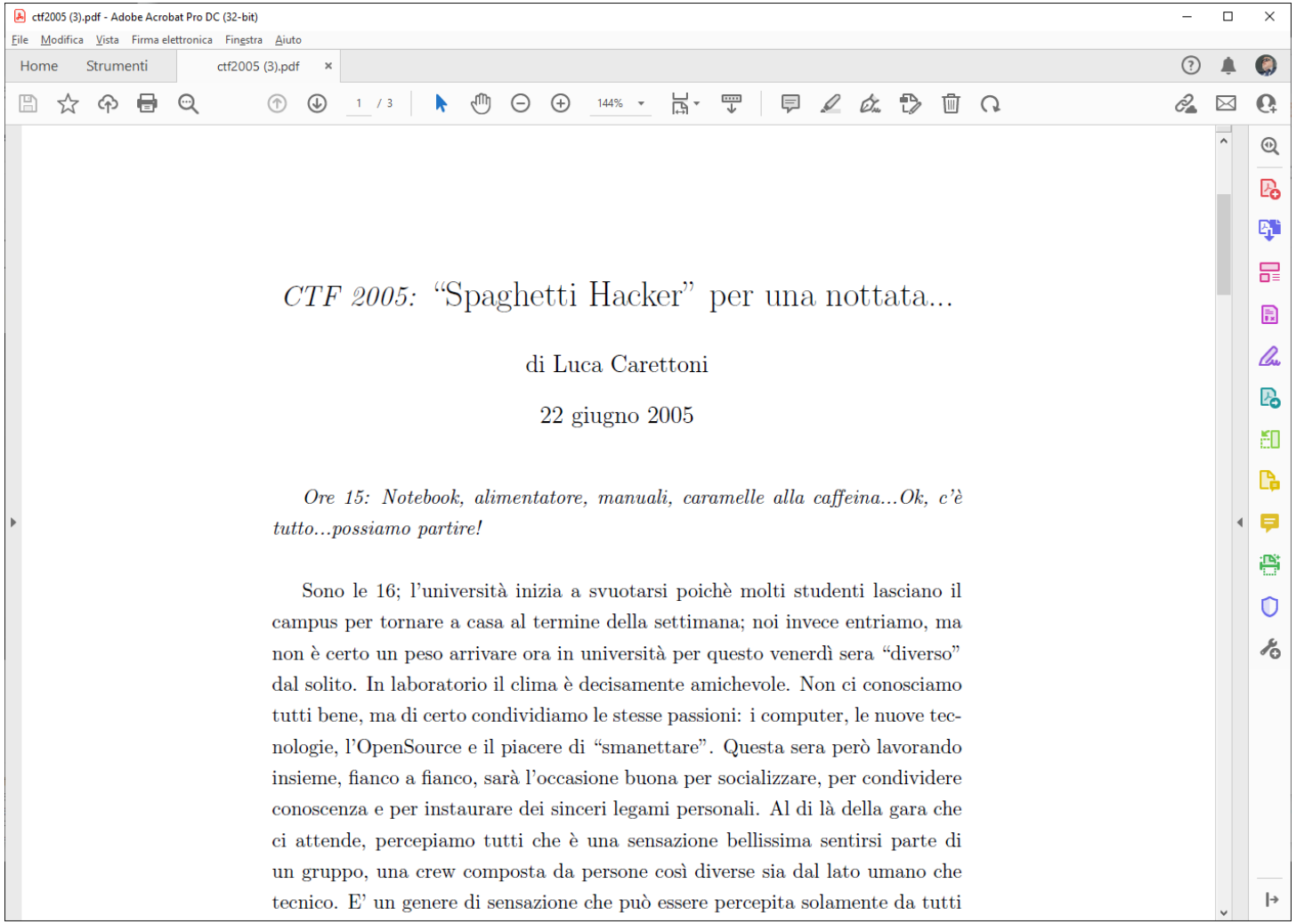
Come tutte le storie che fanno sorgere dei miti, la nascita dell’haking è difficile da ricostruire con certezza, provo a riportarvi qui quella che mi sembra più attendibile.

E non stupitevi, perché per parlarvi della nascita dell’Haking dovrò



SPAGHETTI HACKER Storie tecniche e aspetti giuridici dell'hacking in Italia 1997 di Stefano Chiccarelli e Andrea Monti

Spaghetti Hacker è un libro che racconta la storia degli hacker italiani e della “via” italiana allo hacking e che, ancora oggi, è l’unica “osservazione partecipante, l’unica indagine sul campo, su quello che si chiamava “underground telematico”.



CTF 2005: “Spaghetti Hacker” per una nottata...

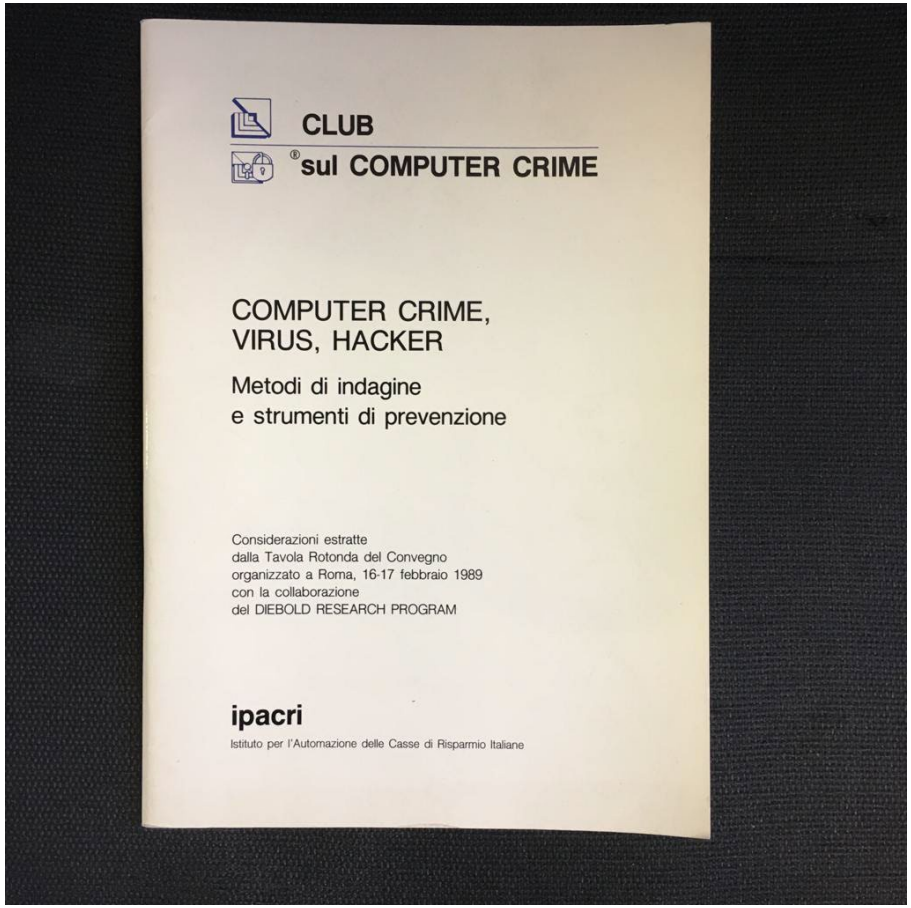
di Luca Carettoni

22 giugno 2005

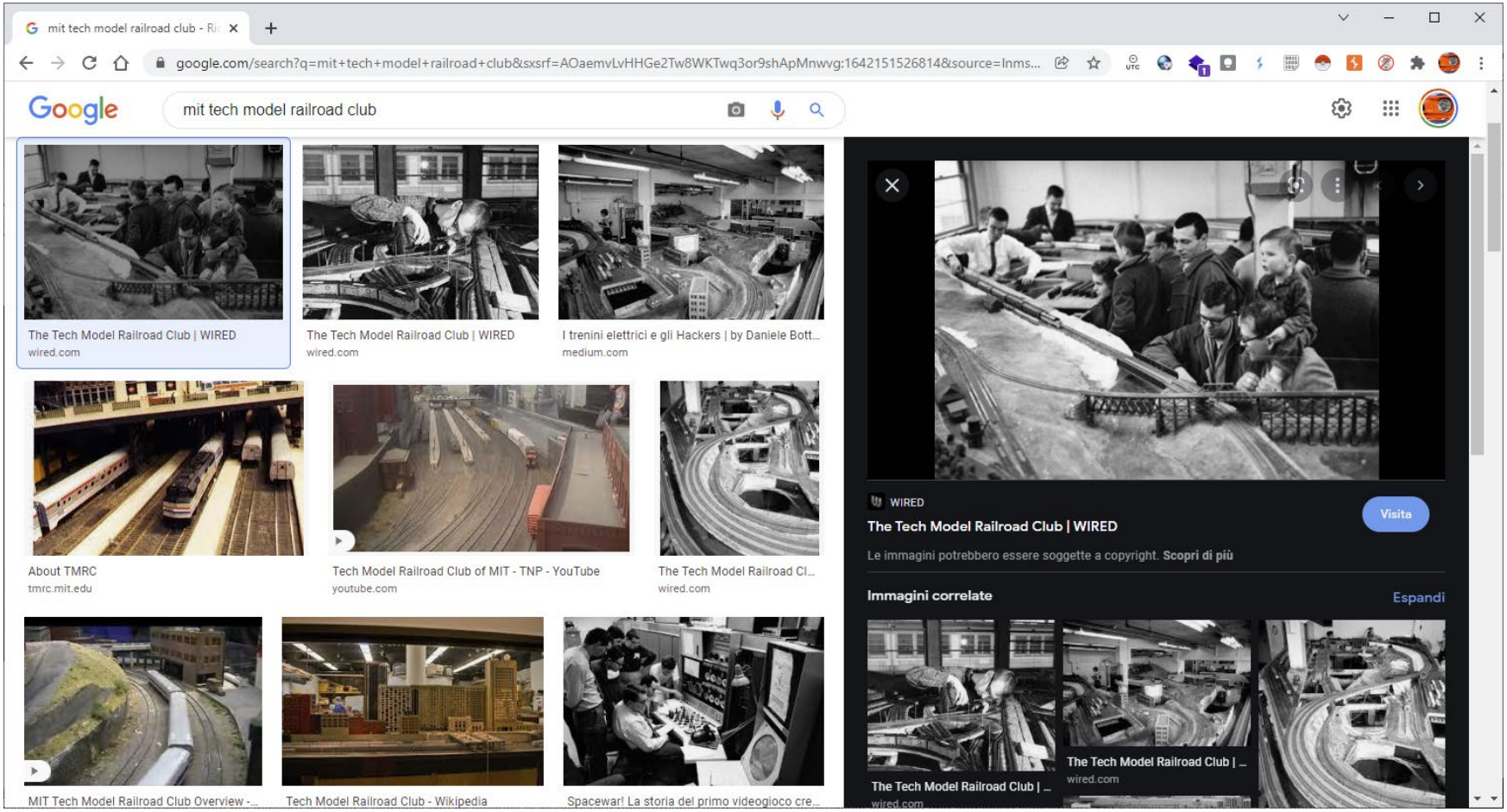
Ore 15: Notebook, alimentatore, manuali, caramelle alla caffeina...Ok, c'è tutto...possiamo partire!

Sono le 16; l'università inizia a svuotarsi poichè molti studenti lasciano il campus per tornare a casa al termine della settimana; noi invece entriamo, ma non è certo un peso arrivare ora in università per questo venerdì sera “diverso” dal solito. In laboratorio il clima è decisamente amichevole. Non ci conosciamo tutti bene, ma di certo condividiamo le stesse passioni: i computer, le nuove tecnologie, l'OpenSource e il piacere di “smanettare”. Questa sera però lavorando insieme, fianco a fianco, sarà l'occasione buona per socializzare, per condividere conoscenza e per instaurare dei sinceri legami personali. Al di là della gara che ci attende, percepiamo tutti che è una sensazione bellissima sentirsi parte di un gruppo, una crew composta da persone così diverse sia dal lato umano che tecnico. E' un genere di sensazione che può essere percepita solamente da tutti

Conoscevate il Club sul Computer Crime?



Inizia tutto da un plastico di treni modellini in scala: cercate «mit tech model railroad club" e flaggate Immagini



fonte: google immagini

Cenni Storici

La storia degli *hackers*, ufficialmente (o meno), ha inizio nell'inverno 1958-59, al Massachussets Institute of Technology (Mit) di Cambridge, il quartiere universitario di Boston. L'istituto ospitava al suo interno una serie di gruppi, piccoli club che univano studenti dagli interessi comuni fuori dalle ore di studio. Uno di questi gruppi era il *Tech model railroad club* (Tmrc), la cui stanza era quasi interamente occupata da un enorme plastico ferroviario molto dettagliato e perfettamente funzionante grazie ad un immenso intreccio di cavi, relè ed interruttori situati sotto il modello. Il club assegnava ai suoi soci una chiave d'accesso ai locali, ma prima che questo privilegio potesse essere concesso, lo studente doveva dedicare almeno quaranta ore di lavoro al plastico.
Il Tmrc era strutturato in due sottogruppi: alcuni soci realizzavano i modellini dei treni e curavano la parte scenografica della riproduzione. Altri, quelli che facevano parte della "Signal&Power Subcommittee" (S&P - sottocommissione per lo studio dei segnali e dell'energia), si occupavano di tutto ciò che accadeva sotto il modellino ferroviario.
La compagnia dei telefoni Western Electric, sponsor dell'istituto, procurava allo stesso i ricambi e i materiali necessari al corretto funzionamento del sistema telefonico universitario. Non di rado però qualche pezzo "sfuggiva" al controllo dei responsabili e finiva per essere riadattato ai nuovi scopi del club.
Con grande impegno e sincera passione, l'elaborato sistema che faceva muovere i trenini e funzionare i singoli scambi, era continuamente testato, smontato, riassemblato, riparato e perfezionato.
Steven Levy racconta che un progetto intrapreso o un prodotto costruito non soltanto per adempiere ad uno scopo specifico, ma che portasse con sé il piacere scatenato della pura partecipazione, era detto "hack". Il termine proveniva dal vecchio gergo del Mit: era stato a lungo usato per indicare gli scherzi elaborati che gli studenti si inventavano regolarmente (come rivestire di alluminio la cupola che dominava l'università). Ma il senso in cui era inteso da quelli del Tmrc denotava rispetto. Se un intelligente collegamento di relè si poteva definire un "hack semplice", si sarebbe inteso che, per qualificarsi come un "vero hack", l'impresa avrebbe dovuto dimostrare innovazione, stile, virtuosismo tecnico.
"Perfino se uno avesse detto, autocommiserandosi, di aver 'fatto a pezzi il sistema', il talento con cui 'faceva a pezzi' gli poteva essere riconosciuto come notevole". I più produttivi tra quelli che lavoravano al Signal and Power si definivano, con grande orgoglio, "*hackers*".
"La tecnologia era il loro parco giochi. I membri anziani stavano al club per ore, migliorando costantemente il sistema, discutendo sul da farsi, sviluppando un gergo esclusivo, incomprensibile per gli estranei che si fossero imbattuti in questi ragazzi fanatici, con le loro camice a maniche corte a quadretti, matita nel taschino, pantaloni chino color cachi e perenne bottiglia di coca-cola al fianco".

fonte: www.adir.unifi.it

Cenni Storici

1960 -70

Fino agli ultimi anni sessanta la comunità hacker del Mit, impegnata ad hakkare le macchine di cui disponeva, studiandone cioè il sistema, progettando assemblatori, debuggers, programmi migliori, al fine di renderle sempre più efficienti, ebbe modo di crescere indisturbata. Spesso partendo da un progetto impostato anche da professori del Mit, gli hackers si impegnavano con una tale abnegazione, passione nel realizzarlo, da portarli a delle prolungate veglie. Nel frattempo l'hakkaggio stava coinvolgendo sempre più individui, grazie anche allo svilupparsi, dal 1965, nella terza generazione di computers, contrassegnata dall'utilizzo di circuiti integrati a media e larga scala, dispositivi di memoria di massa con capacità di memorizzazione assai elevata e periferiche più sofisticate ed efficienti. Questo permise l'utilizzo di mini e microcalcolatori negli uffici, nelle aziende ed i calcolatori personali vennero introdotti sul mercato dei beni di largo consumo. Gli hackers non si erano posti il problema del possibile conflitto che, avrebbe generato nelle persone comuni, questo relazionarsi nella vita con il computer. Nelle molte manifestazioni pacifiste che si tennero in America, nel periodo della guerra del Vietnam, ci furono accuse generalizzate, rivolte ai detentori di un sapere scientifico legato ai computers ed accuse specifiche rivolte a quelli del Tech Square e quindi dell' Ia lab, il laboratorio di intelligenza artificiale. L'Ia lab era finanziato dall'Arpa, del Ministero della Difesa e la conseguenza logica, per il movimento dei pacifisti, era che quello che veniva creato nei suoi laboratori avesse un impiego militare. Il ministero della difesa pur non pretendendo, si aspettava delle possibili applicazioni militari dai risultati del lab. La risposta degli hackers fu diversa; ci furono alcuni che negarono l'evidenza ed altri che misero la questione in termini di scelte ossia meglio il ministero della difesa con le sue chiare richieste che il ministero del commercio o dell'educazione, con la egemonizzazione della ricerca. Gli anni settanta videro l'applicazione dell'etica hacker su scala maggiore. Un leggendario di questo periodo è John T.Draper, alias Captain Crunch, che adottò questo pseudonimo da una marca di cornflakes che dava in omaggio un fischietto; Draper scoprì che emetteva una frequenza di 2600 hertz la quale, quando una linea telefonica diretta, in particolare interurbana, è inattiva, viene inviata all'altro estremo. Entrambi gli estremi inviano questa frequenza l'un l'altro. Con questo segnale era perciò possibile effettuare telefonate in qualsiasi parte del mondo gratis. Questa possibilità era già conosciuta da un gruppo di ragazzini ciechi, Dennie, Jimmie ed altri che J.Draper conobbe in quel periodo. Dal fischietto giocattolo si passò alle blue, black e red boxes, le quali avevano le stesse funzioni di questo; producevano i segnali necessari ad eludere il sistema telefonico americano. Era l'inizio del phone-phreaking.

fonte www.autistici.org

Cenni Storici

fonte: www.accademiacivicadigitale.org

Cenni Storici

il Phreaking: crackare le reti telefoniche

Il termine **phreaking** fa parte delle espressioni gergali inglesi e nasce dalla fusione delle parole ***phone*** **(telefono) e** ***freak*** **(fanatico)**. Negli anni Cinquanta e Sessanta, con la diffusione della rete telefonica pubblica negli Stati Uniti, sono state molte le persone a dimostrare un forte interesse nel voler capire il suo funzionamento e nel voler scoprire i segreti celati dietro a questa novità. Questa terminologia è stata coniata esattamente in seguito a questo fenomeno. Si è infatti voluto attribuire un'identità all'insieme delle attività di coloro che studiavano, sperimentavano ed esploravano i **sistemi di telecomunicazione** per curiosità o divertimento.

fonte: www.accademiacivicadigitale.org

Phreaking

John Draper AKA Capitan Crunch

Cenni Storici

Steve Jobs And Steve Wozniak

LO SAPEVATE?

fonte www.autistici.org

Cenni Storici

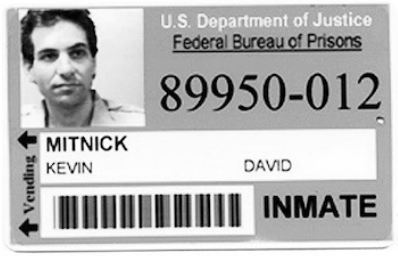
1980-90

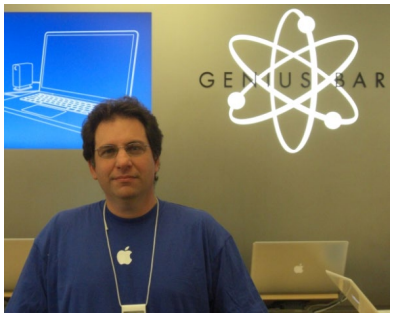
Alla fine degli anni settanta si sviluppò la quarta generazione di computer, con l'avvento dei circuiti integrati a larga scala di integrazione. All'inizio degli anni ottanta, il panorama informatico, era in pieno fermento non solo in America. Ai più della "massa europea" fino a questo periodo, il termine computer era sconosciuto; furono però in parte scossi da un produttore inglese, Sir Clive Sinclair, ideatore dello ZX Spectrum. Un prodotto che non era certamente tra i migliori, ma immesso sul mercato nel momento giusto. Questi sono gli anni in cui la febbre del computer, iniziata in piccoli negozi di software esplode nei grandi magazzini e nei punti vendita specializzati, proponendo prodotti sia professionali che familiari. I media si pongono domande sulla mania dei computer diffusasi come un virus e su come considerare i giovanissimi che rimangono incollati alla tastiera per ore; disadattati o anticipatori di un modo di vivere del 2000? E gli hacker? Loro avevano contribuito a questa espansione ed alla creazione di nuove società di hardware e software. Per esempio, Steve Wornak, era un hacker puro la cui creazione, l'Apple II, fu lanciata sul mercato da Steve Jobs, non propriamente un hacker, che portò l'Apple ad essere una delle industrie più dinamiche del settore, con sorpassi e rimonte clamorosi con l'IBM e nel 1980, ad essere quotata in borsa. Da alcuni anni, molti hacker vengono assunti da grosse aziende per controllare il loro software e la sicurezza delle loro reti, perchè particolarmente abili nell'intrufolarsi nel sistema informatico. Questo ventennio ha visto inoltre il crescere e svilupparsi di una nuova "attitudine", il Cyberpunk. Non facile da definire, è uno stile di vita ed un genere letterario. Il primo uso della parola "cyberpunk" per descrivere un genere letterario viene fatto risalire ai primi anni '80 ed è accreditato a Gardner Dozois, l'editore dell'Isaac Asimov's Science Fiction Magazine; prelevò la parola breve storia di Bruce Bethke "Cyberpunk" . All'interno del Cyberpunk è possibile far confluire essenzialmente: Hacker craker: il loro obiettivo principale sono i sistemi operativi e Preaker: conoscono il sistema telefonico ed il modo di raggirarlo.

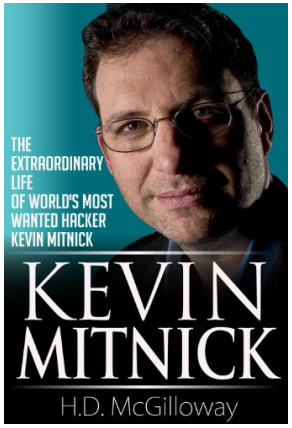
The Condor

1990-2000

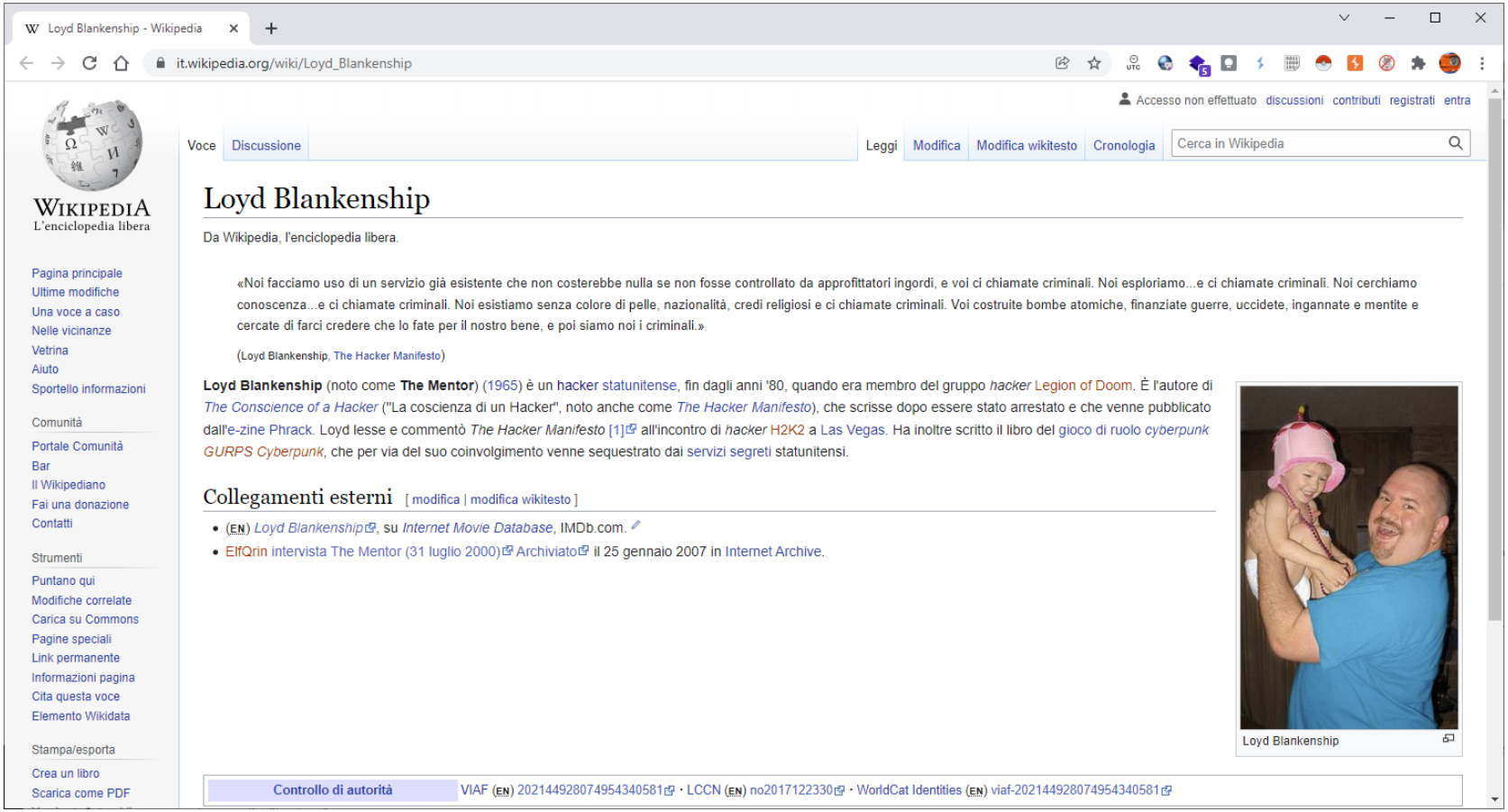
I teenager che negli anni 80/90 si poterono permettere uno dei primi home computer misero le basi della prima generazione moderna di hacker. Questi sono stati precursori delle prime reti telematiche come itapac, BBS, circuiti email fidonet, ecc.
Qui si inizia a notare la differenza tra chi difende il diritto d’autore, molti hacker sono anche autori di software e chi invece lavora per diffondere copie pirata dei software protetti, quindi possiamo dire che in questa epoca si iniziano ad identificare hacker buoni e hacker cattivi, sono gli anni dove sulla scena criminale dell’hacking spicca il nome di Kevin David Mitnick AKA Condor, è un programmatore, phreaker, cracker, ed ingegnere sociale statunitense, che si è distinto per avere inventato la tecnica dell'IP spoofing e per le sue notevoli capacità di ingegnere sociale, avendo eseguito alcune tra le più ardite incursioni nei computer del governo degli Stati Uniti. Catturato, fu condannato a svariati anni di carcere. Attualmente è un famoso consulente per la sicurezza.







"Il mio crimine è la curiosità" (The Mentor).



«Noi facciamo uso di un servizio già esistente che non costerebbe nulla se non fosse controllato da approfittatori ingordi, e voi ci chiamate criminali. Noi esploriamo...e ci chiamate criminali. Noi cerchiamo conoscenza...e ci chiamate criminali. Noi esistiamo senza colore di pelle, nazionalità, credi religiosi e ci chiamate criminali. Voi costruite bombe atomiche, finanziate guerre, uccidete, ingannate e mentite e cercate di farci credere che lo fate per il nostro bene, e poi siamo noi i criminali.»

The Hacker Manifesto

Loyd Blankenship (noto come The Mentor) (1965) è un hacker statunitense, fin dagli anni '80, quando era membro del gruppo hacker Legion of Doom. È l'autore di The Conscience of a Hacker ("La coscienza di un Hacker", noto anche come The Hacker Manifesto), che scrisse dopo essere stato arrestato e che venne pubblicato dall'e-zine Phrack. Loyd lesse e commentò The Hacker Manifesto [1] all'incontro di hacker H2K2 a Las Vegas. Ha inoltre scritto il libro del gioco di ruolo cyberpunk GURPS Cyberpunk, che per via del suo coinvolgimento venne sequestrato dai servizi segreti statunitensi.

fonte: it.wikipedia.org

Cenni Storici - Italia

1990-2000

In Italia nello stesso periodo, per una intrusione nella rete della Banca d’Italia viene arrestato Raoul Chiesa AKA Nobody e Matteo Del Mistro AKA neXus nell’operazione ICE-TRAP. Avevano lasciato un messaggio con scritto “questa rete non è sicura. Firmato Falange Armata. ” L’operazione trappola di ghiaccio - perché partita dalla divisione surgelati della Unilever, dove era stata scoperta un'incursione nella rete in cui erano custoditi i progetti per un nuovo gelato: puntava a un'organizzazione internazionale di spionaggio industriale. E invece ha scoperto solo un gruppo di ragazzi appassionati di computer, sbattuti in prima pagina per una bravata di troppo.

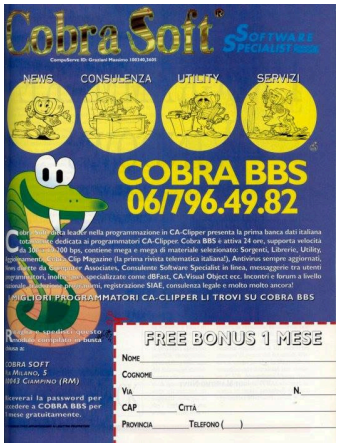
*Stefano Chiccarelli AKA NeURo esperto di telematica e autore, con il giurista Andrea Monti, di Spaghetti hacker (ed. Apogeo). da un corretto significato della parola HACKER: "La traduzione più vicina al concetto originario non è pirata o scassinatore, ma è smanettone, cioè un appassionato di informatica che ama capire le macchine nel loro profondo", **Non esistono hacker buoni e hacker cattivi**, secondo lui, ma esistono gli hacker e quelli che non lo sono e si spacciano per tali (spregiativamente, in gergo, lamer). Poi ci sono i delinquenti, ma quelli stanno ovunque, non solo in Rete.*
Gli hacker "bucano" i sistemi informatici come stile di vita, da quando questi hanno incominciato ad esistere. E nel farlo, si sentono eroici. Il loro "gioco" è dimostrare la loro bravura, mettendo a nudo l'inaffidabilità della Rete allo stato attuale.
*Così, di fatto, contribuiscono a migliorarla di giorno in giorno. **Infatti sono gli stessi hacker che trovano i cosiddetti "bachi"**, e a scoprire poi anche i rimedi. Le aziende lo sanno, tanto è vero che i sistemi di sicurezza aziendali migliori sono affidati a ex-hacker che sono riusciti a mettersi in luce per la loro bravura e a farsi assumere, passando dall'altra parte della barricata.*

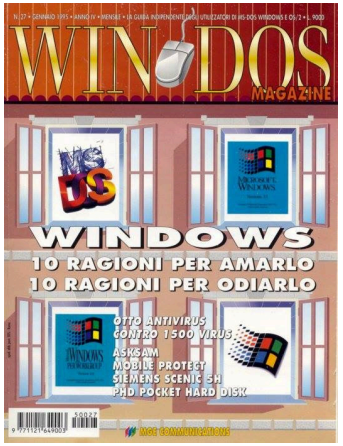
Cenni Storici

1990-2000

Ormai, con la diffusione di Internet, gli hacker hanno fatto proseliti. Sono centinaia. Per sfatare il mito di pirati fuori legge, sono usciti allo scoperto, organizzando incontri, e addirittura corsi aperti al pubblico, sulle nuove tecnologie. In Germania il "Caos Computer Club", considerato tra i migliori gruppi di hacker al mondo, organizza corsi di aggiornamenti tecnici riconosciuti dal governo, in Olanda e in America ci sono molti party e convention facilmente accessibili. In Italia dove è avvenuto l'incontro-scontro "L'hacker e il magistrato", organizzato a Pescara da Metro Olografics, "Per la prima volta in Italia gli organizzatori hanno avuto il coraggio di dichiarare la natura hacker dell'evento“.

Poi c’eravamo noi che ci ingegnavamo in sistemi di protezione antihacker, dovevamo pensare come loro e prevenirne le mosse in anticipo!





Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

OGGI ESISTONO NORMATIVE NAZIONALI E STANDARD DI MERCATO

CHE REGOLANO I LIMITI DI PRATICABILITA' DELL'HACKING.

L'EXPLOITATION DI UN SISTEMA SENZA AUTORIZZAZIONE

E' CONSIDERATO UN ACCESSO ABUSIVO!

L'ILLECITO INFORMATICO, DALLA FRODE TELEMATICA AI FURTI DI INFORMAZIONI OGGI E' UN BUSINESS DI ORGANIZZAZIONI CRIMINALI, CHE HANNO COMPRESO CHE ESISTE UN MERCATO SU CUI INVESTIRE... QUESTI ILLECITI FRUTTANO DI PIÙ E CON MENO RISCHI DEL MERCATO DI DROGA

L'HACKER ETICO È:

QUELLO CHE SVOLGE LA SUA ATTIVITÀ CON LE "DOVUTE AUTORIZZAZIONI".

ANTICIPA LE MOSSE DEI CRIMINALI, SCOPRENDO LE VULNERABILITÀ,

CON LO SCOPO DI FAR APPLICARE LE DOVUTE CONTROMISURE !

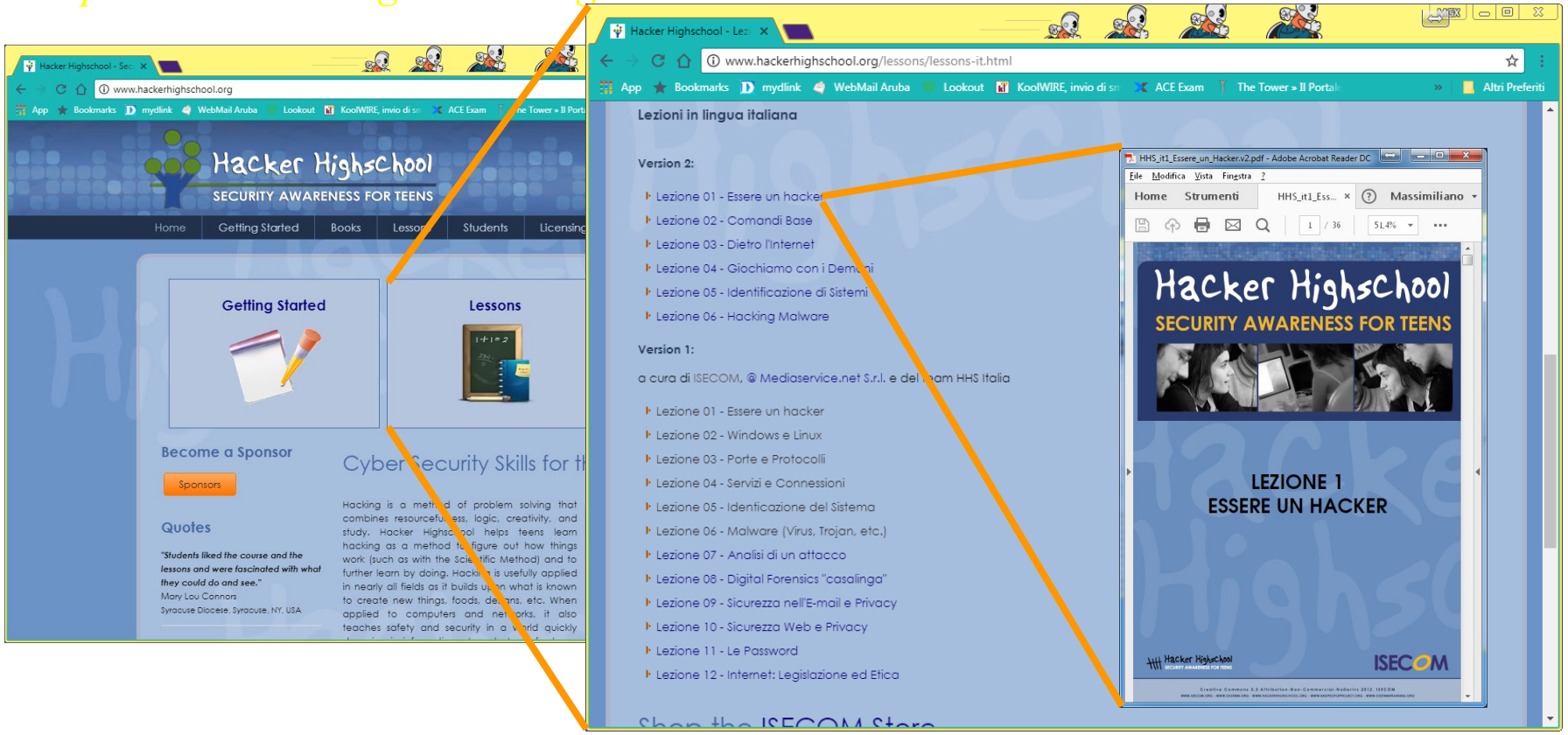
CYBERCOP e HACKER ETICI
lavorano insieme ormai da 30 anni

OGGI OGNI CORPO DI POLIZIA HA IL SUO REPARTO SPECIALIZZATO in CYBER INTELLIGENCE e DIGITAL FORENSICS

Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

http://www.hackerhighschool.org/lessons/lessons-it.html



Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

CHIAREZZA SULLA TERMINOLOGIA :

- ***Hacker:*** *esperto informatico che apporta innovazione e sicurezza ai sistemi informatici testando i loro limiti, di regola un hacker dovrebbe essere un programmatore, quindi conoscere almeno un linguaggio di programmazione.*

- ***Cracker:*** *Hacker che adotta la propria conoscenza per eliminare la protezione dei software e altri sistemi. In gergo venivano chiamati Pirati Informatici, la loro attività, a meno che non sia autorizzata, come test di debug, è illegale.*

• ***Phreaker****: persona che dimostra un forte interesse nel voler capire il funzionamento della Rete Telefonica o altri sistemi di gestione e nel voler scoprire i segreti celati dietro a questa tecnologie.*

• ***Cybercriminale:*** *Hacker che usa la sua conoscenza per mettere in atto reati informatici, come attacchi non autorizzati a scopo estorsivo e ricattatorio, attacchi di negazione dei servizi mirati a rendere i sistemi informatici di un determinato sito/ sistema inutilizzabili, furto di informazioni, come credenziali, carte di credito, dati sensibili, ecc.*

• ***Virus Writer:*** *Hacker che scrive software Malware, in alcuni casi questa attività è autorizzata se sviluppata per enti governativi (vedi captatore o spyware di Stato), diversamente, se non a scopo di ricerca è considerate reato.*

Molti reati informatici, in alcuni Paesi extraeuropei sono considerati alla stregua di reati di Terrorismo.

CHIAREZZA SULLA TERMINOLOGIA :

- ***Vulnerability Scan:*** *scansione automatica delle vulnerabilità conosciute.*

- ***Vulnerability Assessment:*** *una verifica automatizzata e umana delle vulnerabilità tecnologiche e infrastrutturali di una rete. Oltre al vulnerability scan, l'analista configura ad hoc la scansione e verifica a mano la corretezza dei risultati.*

- ***Risk Assessment****: metodologie di analisi del rischio si possono applicare anche all'infrastruttura informativa. Servono per quantificare il rischio e dimostrare l'importanza dell'investimento nella sicurezza.*

- ***Penetration test:*** *è un test di quello che potrebbe fare un Hacker sui nostri sistemi, per questioni di tempo non può essere esaustivo, ha valore solo se il team è competente e ha esperienza.*

- ***Security audit:*** *il security auditing è un processo aziendale, è riferito ad uno standard come l'ISO 27.001, l'audit mira a verificare l'aderenza ai controlli e le politiche dell'ISMS così come definito dallo standard.*

- ***Security assessment:*** *Un test omnicomprensivo della della sicurezza, logica, infrastrutturale, fisica, sociale. (es. OSSTMM)*

Terminologia pubblicata la prima volta in Italia dal Prof. Stefano Zanero

CHE COSA PUO' FARE UN HACKER SUI SISTEMI CHE DEVO PROTEGGERE?

Lo schema classico di un attacco prevede in genere le seguenti fasi:

1. *RICOGNIZIONE*
   - *Attiva (interagisce con il target)*
   - *Passiva (cerca informazioni su l sistema target altrove)*

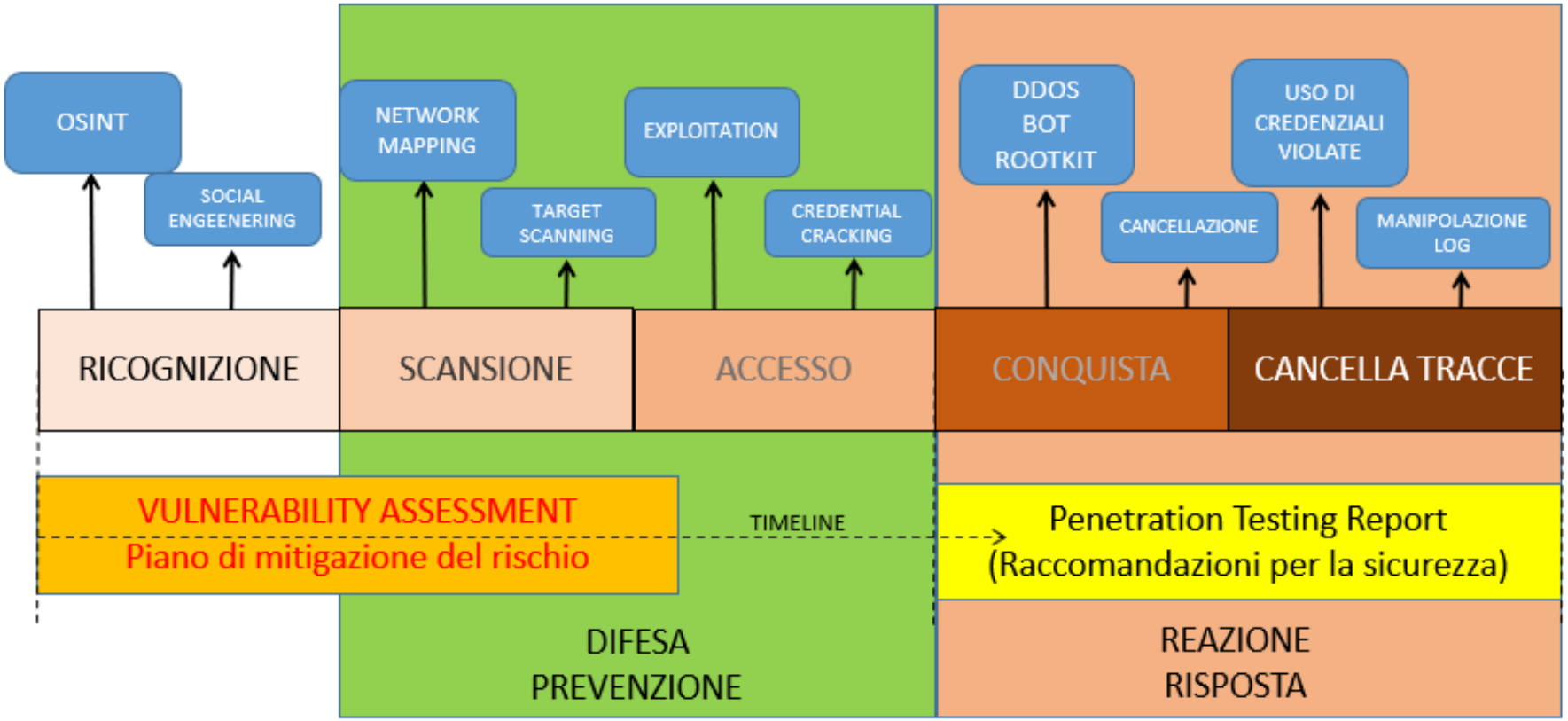
2. *SCANSIONE*
   - *Rilevazione servizi, Sistemi di sicurezza, Vulnerabilità*

3. *ACCESSO*
   - *Entra nel sistema e lo esplora*

4. *CONQUISTA*
   - *Configura il sistema, lo protegge da altri hacker, lo amministra da remoto*

5. *CANCELLA LE TRACCE*
   - *Cancella i log, elimina le tracce della fase di attacco*

MAPPATURA ATTIVITA' HACKING



Due le definizioni di incidente IT, in funzione delle modalità con cui gli stessi sono gestiti. La prima definizione si applicherà a tutti quelli gli eventi che pur rappresentando potenziali minacce saranno annullati dalle protezioni messe in atto, mentre la seconda si applicherà a tutti quegli eventi in cui l'attaccante riuscirà a violare sistemi, norme o regolamenti. Più precisamente definiamo il primo tipo di incidente ***tentativo di attacco*** *ed il secondo* ***incidente.***

Attacco non riuscito!

Attacco riuscito!

Tentativo di attacco di Sicurezza IT

Qualsiasi evento che minacci di compromettere il corretto funzionamento dei sistemi e/o delle infrastrutture aziendali o l’integrità e/o la riservatezza delle informazioni in essi memorizzate o in transito o che violi le politiche di sicurezza definite dall’Azienda o le leggi in vigore.

Incidente di Sicurezza IT

Qualsiasi evento che necessiti di un intervento di contenimento o reazione, al fine di evitare o limitare la compromissione del corretto funzionamento dei sistemi e/o delle infrastrutture aziendali o l’integrità e/o la riservatezza delle informazioni in essi memorizzate o in transito o che violi le politiche di sicurezza definite dall’Azienda o le leggi in vigore.

Una basica classificazione degli Incidenti

1. ***Denial of Service***
   - *Flooding*
   - *Shut down*
   - *Sabotaggio*
2. ***Hacking***
   - *Account Compromise*
   - *Root compromise*
   - *Consolidamento*
   - *Covering Trace And Creating Back Door*
3. ***Accesso e Compromissione dei dati***
   - *Intercettazione*
   - *Application compromise*
4. ***Violazione di policy***
5. ***Violazione di leggi***
6. ***Frode informatica***
7. ***Malware***
   - *Virus*
   - *Worm*
   - *Trojan*
   - *Hoax*
   - *Spyware*
   - *Backdoor*
   - *Dialer*
   - *Rootkit*
   - *Bot*
   - *ecc.*
8. ***Perdita accidentale di dati riservati causa fattore umano***
   - *Furto*
   - *Smarrimento*
   - *Errori umani*
9. ***Perdita accidentale di dati riservati cause naturali***
   - *Incendio*
   - *Allagamento*
   - *Terremoto*
   - *Interruzioni di energia elettrica*
   - *Esplosioni*

Qualche esempio di attività di ethical hacking:

1) *Attacco al palazzo gi Giustizia Milano - IISFA 2009*
2) *Spear Phishing sui dipendenti con Questionario a premi - Cliente NDA*
3) *Social Engineering ad effetto FEAR - Simulazione*

Attacco al palazzo di Milano - IISFA 2009

http://milano.repubblica.it/dettaglio/un-pm-hacker-viola-il-tribunale-ecco-come-far-sparire-dati-delicati/1584048

International Information System

Forensics Association

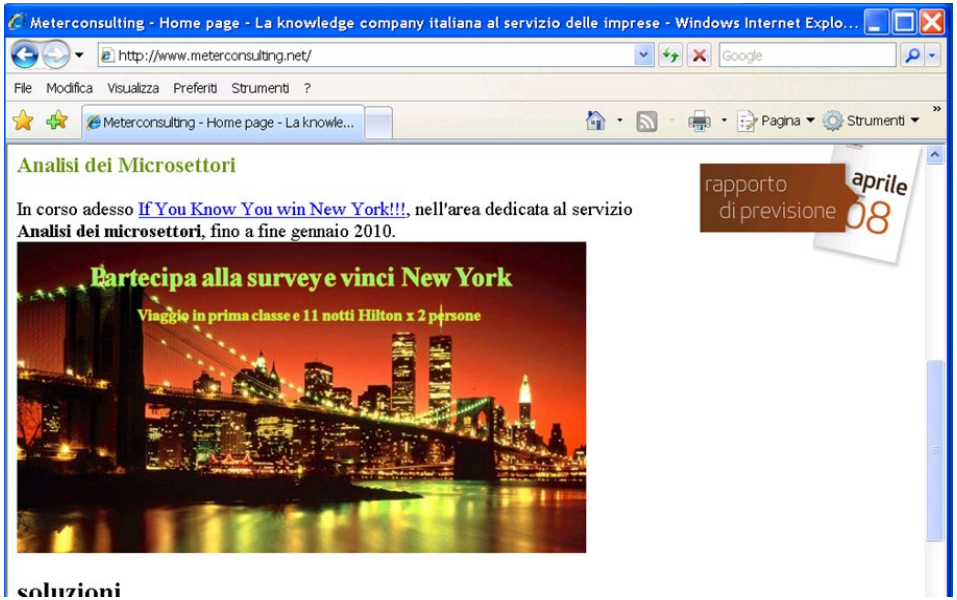
Italy Chapter

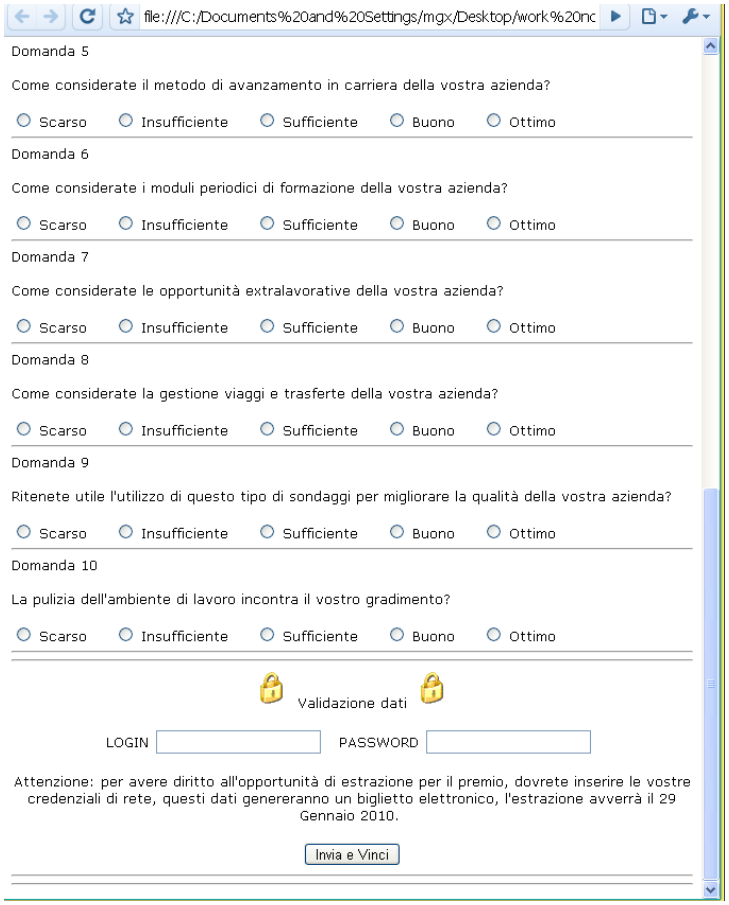
Attacco al Palazzo di Giustizia

Fase 1) Piano di Azione

www.iisfa.it

Spear Phishing sui dipendenti questionario a premi - Cliente NDA 2010

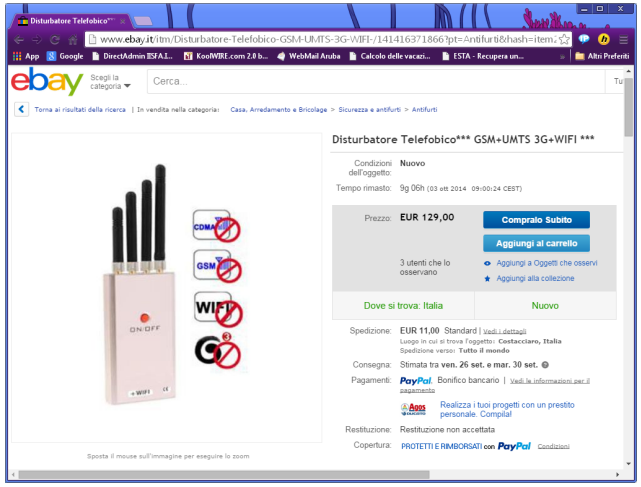




Social Engineering ad effetto FEAR – Simulazione 2014

Come poter prendere i dati vitali di una azienda usando:

1 jammer portatile
1 server per invio di SMS spoofati da internet



Numero cellulari dell’AD e della segretaria ottenuti con tecniche di social engineering

Social Engineering ad effetto FEAR - Cliente NDA 2014

Piano di azione:

1) *Ottenere i cellulari dell'AD e della sua segretaria*
2) *Seguire gli spostamenti dell'AD a ora di pranzo per un periodo sufficiente*
3) *Azione: Seguire l'AD mentre va a pranzo con il jammer acceso. Inviare alla segretaria un SMS dal numero dell'AD: "URGENTE sta per arrivare la GdF, ho mandato un tecnico mio amico per cancellare i dati dal portatile, si chiama Marco, devi consegnargli il mio portatile, lui sa già cosa deve fare, lo restituirà a me stasera! Mi raccomando è URGENTE non posso rientrare adesso!"*

Un fantomatico Marco (un bisognoso chiunque, per un centinaio di euro, andrebbe a ritirare il portatile dicendo che si chiama Marco) va a prendere il portatile mentre un altro segue l'AD con il jammer acceso (a circa 10 metri di distanza)….. cosa farà la segretaria non riuscendo a chiamare l'AD al telefono?

Questa tecnica di social engineering fa leva sulla paura che hanno le aziende delle ispezioni di polizia tributaria!

Quale tra questi hacker dobbiamo temere di più?

*Conoscete **Kristina Svechinskaya**? E' considerata la più sexy del mondo hacker, una splendida ragazza russa che è salita alla ribalta delle cronache perché accusata di far parte di una banda di truffatori informatici che avrebbero sottratto più di 220 milioni dollari con frodi bancarie e l'utilizzo di passaporti falsi.*

FISSIAMO ADESSO ALCUNE REGOLE DI BASE

1. *VAPT può essere svolto sempre solo dietro autorizzazione*
2. *L'autorizzazione può essere esplicita ed implicita*
   a) *esplicita dietro contratto e manleva*
   b) *implicita in caso di Bug Hunting e Responsible Disclosure*

Il **BUG Hunting** è una sorta di concorso on line che molte aziende lanciano per migliorare il proprio livello di sicurezza, chi lo esegue deve iscriversi ed accettare le regole del concorso, quasi sempre, per ogni vulnerabilità individuata, il Cliente paga premi in denaro.

La **Responsible Disclosure** definisce una modalità per segnalare vulnerabilità dei sistemi informatici, lasciando al Cliente Target il tempo necessario per poter individuare ed applicare le opportune contromisure, prima di renderle pubbliche.

Queste attività se svolte senza regole o disposizioni che le autorizzano, possono essere considerate illecito penale, come ad esempio accesso abusivo.

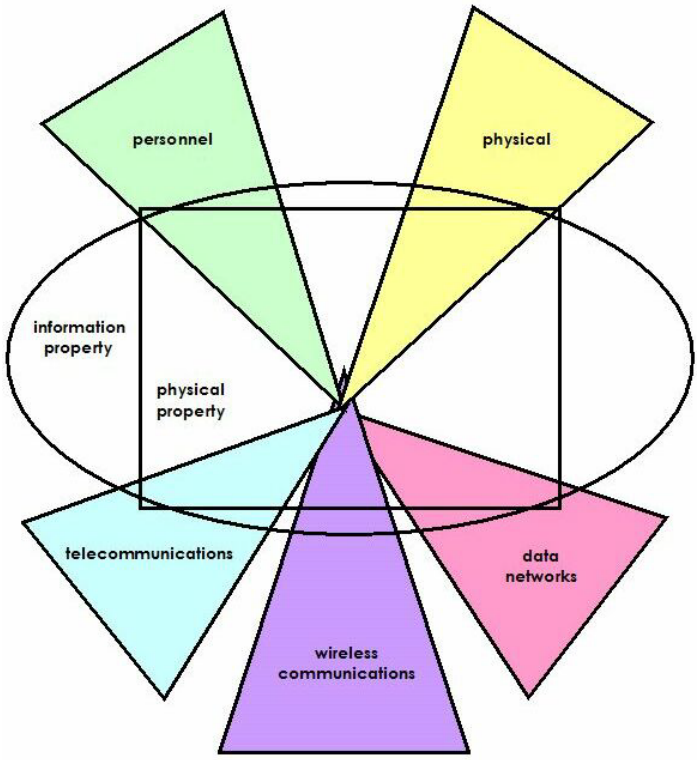
Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

L’Open Source Security Testing Methodology Manual, è uno standard internazionale di riferimento per l’esecuzione di verifiche di sicurezza, sviluppato da ISECOM tramite il modello peer review.
ISECOM (Institute for Security and Open Methodologies) è un’organizzazione internazionale di ricerca senza scopo di lucro, fondata nel 2001 al fine di sviluppare e condividere metodologie aperte nel campo della sicurezza delle informazioni.
ISECOM è inoltre un’autorità di certificazione sostenuta da partner istituzionali.
OSSTMM è una metodologia scientifica che definisce esattamente quali elementi devono essere verificati, che cosa occorre fare prima, durante e dopo i test di sicurezza e come misurare i risultati ottenuti. Consente pertanto di valutare sul campo in modo consistente e ripetibile la superficie di attacco relativa al contesto oggetto di analisi. La metodologia OSSTMM ha introdotto numerosi nuovi concetti nella disciplina della Sicurezza Proattiva, quali: OPSEC e controlli, Competitive Intelligence (CI), metriche per misurare la superficie di attacco (RAV), reportistica certificata (STAR).

Una verifica di sicurezza conforme allo standard OSSTMM assicura:

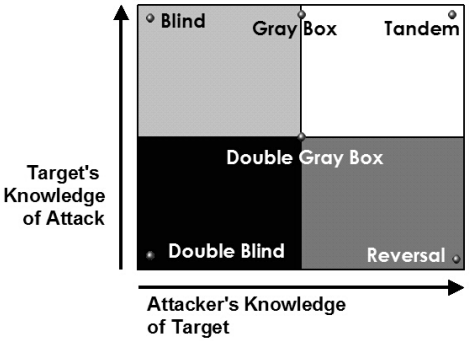
1. *Esaustività e profondità dei test, con riduzione sostanziale dei falsi positivi e negativi.*
2. *Conclusioni oggettivamente derivate dai risultati dei test stessi, tramite applicazione del metodo scientifico.*
3. *Rispetto di politiche, normative e leggi vigenti applicabili al contesto oggetto di analisi.*
4. *Risultati consistenti e ripetibili.*
5. *Risultati misurabili e quantificabili secondo precise regole.*
6. *La reportistica certificata costituisce la prova di un test basato sui fatti e rende gli analisti responsabili dell'audit.*



Tramite il calcolo del RAV e l'emissione di reportistica STAR certificata, OSSTMM consente alla azienda di ottenere le risposte alle seguenti domande fondamentali:

1. *Quanto dobbiamo investire nella sicurezza?*
2. *Su quali aspetti dobbiamo concentrarci in modo prioritario?*
3. *Di quali soluzioni di sicurezza abbiamo bisogno?*
4. *Quanto migliora il livello di sicurezza a seguito dell'adozione di specifiche contromisure?*
5. *Come possiamo misurare i risultati dei piani correttivi?*
6. *Come possiamo sapere se stiamo riducendo l'esposizione alle minacce?*
7. *Quanto è resistente un determinato componente?*
8. *Come possiamo ottenere conformità e sicurezza?*

L'obiettivo finale di una verifica conforme allo standard OSSTMM, pertanto, è fornire un processo concreto per essere funzionalmente sicuri.



Tipologia di penetration Test:

BLIND: *quando l'attaccante non conosce minimamente il sistema da analizzare. E' conosciuto solamente il target (IP-URL)*
DOUBLE BLIND: *simile a quello precedente con la differenza che alcune persone del committente sono al corrente del test. Viene tipicamente usato per verificare se il personale interno dedicato alla sicurezza è "vigile" e svolge con diligenza il proprio lavoro.*
GRAY BOX: *sia l'attaccante che l'attacco sono pienamente a conoscenza sia del sistema informatico da analizzare che delle modalità di attacco. Viene utilizzato quando si analizza il proprio sistema interno.*
DOUBLE GRAY BOX: *è un gray box che prevede la conoscenza delle credenziali di accesso. Viene usato per testare l'accesso ad informazioni più riservate rispetto al suo livello da parte di un utente.*
TANDEM: *analisi del codice. Chi verifica e chi crea il codice collaborano*
REVERSAL: *test a uso interno. Il tester ha una grande quantità di informazione il committente non sa i tempi e le metodologie con cui verrà attaccato.*

OSSTMM prevede regole di ingaggio, di lavorazione e reportistica ben definite, dopo averle rispettate nella trattativa con il cliente prevede 4 fasi fondamentali ben precise che permettono di svolgere al meglio l'analisi di sicurezza e sono applicabili a qualsiasi tipologia di test di sicurezza. Ogni singola fase ha una diversa profondità sull'analisi ma tutte hanno la stessa importanza in termini di sicurezza.

1. *Induction Phase*
2. *Interaction Phase*
3. *Inquest Phase*
4. *Intervention Phase*

Induction Phase

E' il primo step dell'analisi. Durante questa fase l'analista inizia con la raccolta dei requisiti di audit, definendo la portata e le limitazioni del test. In questa fase viene coinvolto il committente e quindi definita la tipologia di test da svolgere. La fase di induzione di suddivide a sua volta in tre momenti:

1. *Posture Review: identificare le normative, regole, norme e politiche associate al target da analizzare. Ad esempio, nel caso di una multinazionale, le normative in termini di privacy possono essere diverse a seconda dello stato in cui risiede il sistema da analizzare.*
2. *Logistics: analizzare i possibili errori e limitazioni quali distanza, velocità, fallibilità. Tutto questo per ridurre al minimo la possibile fallibilità del test.*
3. *Active Detection Verification: identificare i possibili limiti dei test interattivi verso il target.*

Interactive Phase

Per svolgere un test di sicurezza bisogna definire lo scope associato al target da analizzare. Questa fase è suddivisa in quattro moduli:

1. *Visibility audit: determinare gli obiettivi da testare. E' considerata "visibility" la presenza e non solamente la visibilità. Se un sistema non risponde non vuol dire che questo non esiste.*
2. *Access Verification: definire i punti di interattività e misurare la robustezza ed efficacia delle richieste di autenticazione.*
3. *Trust Verification: verificare l'affidabilità e sicurezza delle relazioni tra e verso i target da analizzare. Vi è una relazione di trust ogni qualvolta il target accetta interazione.*
4. *Control Verification: vengono fatti i controlli definiti di classe B:*
   - *non ripudio (tracciabilità delle informazioni)*
   - *confidenzialità (informazioni scambiate in sicurezza)*
   - *privacy (le informazioni sono scambiate in riservatezza)*
   - *integrity (controllo integrità delle informazioni scambiate)*

Inquest Phase

Molti dei test di sicurezza svolti vengono fatti secondo le informazioni reperite dall'analista. I test infatti vengono creati
"su misura" a seconda delle caratteristiche del sistema da analizzare. Questa fase è suddivisa in 6 moduli.

1. *Process Verification: identificare e comprendere i processi informatici del committente*
2. *Configuration Verification / Training Verification: identificare il normale stato di funzionamento dei sistemi per rilevarne eventuali problemi di fondo quando questi sono soggetti a stress test di sicurezza.*
3. *Property Validation: verificare lo stato dei diritti di proprietà (licenze, software abusivi, ecc)*
4. *Segregation Review: verificare se il sistema informatico rispetta le leggi vigenti nello stato in cui risiede il sistema, ad esempio la legge sulla privacy.*
5. *Exposure Verification: rilevare se esistono informazioni dichiarate riservate che invece risultano visibili*
6. *Competitive Intelligence Scouting: ricercare informazioni liberamente disponibili e pubbliche che potrebbero danneggiare o compromettere il sistema.*

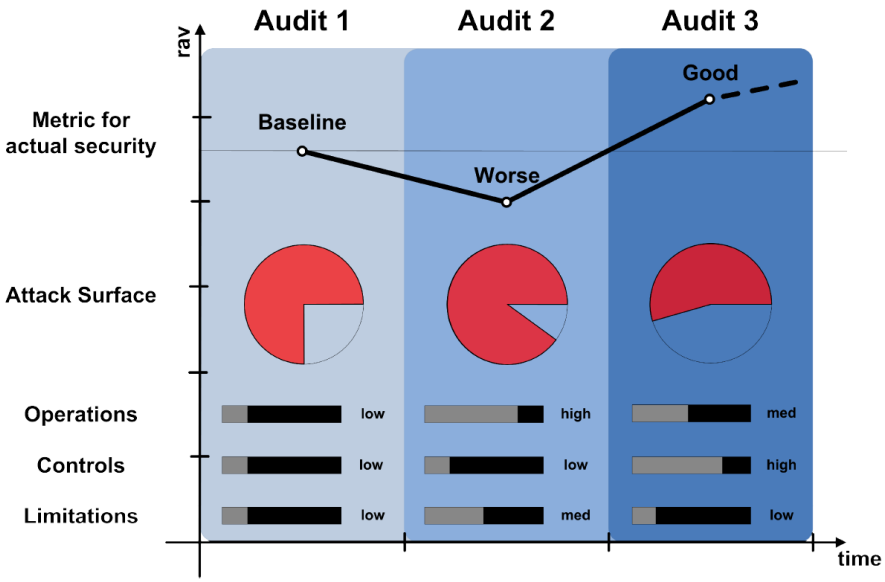
Intervention Phase

E' la fase finale che prevede 4 step:

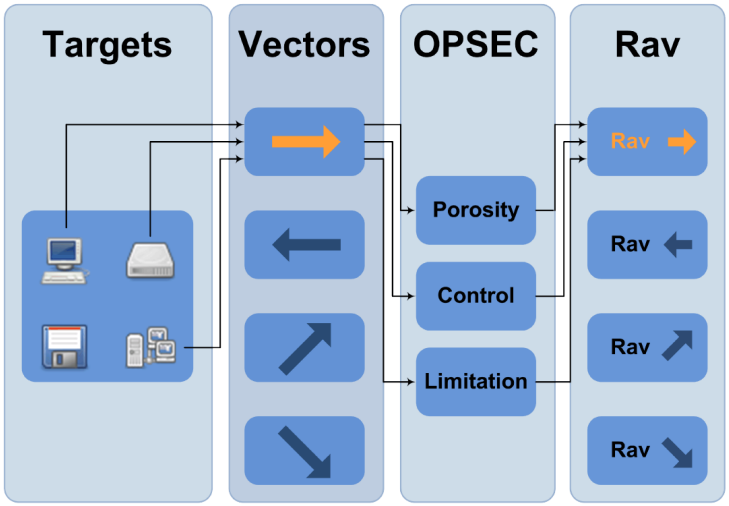
1. *Quarantine Verification: verificare come il sistema di "quarantena" funzioni adeguatamente (virus, black list, ecc)*
2. *Privileges Audit: controllo della robustezza delle credenziali di accesso, politiche applicate o non autorizzate "privilege escalation".*
3. *Survivability Validation / Service Continuity: misurare la resistenza del sistema in caso di sovraccarico (DOS). Il controllo viene fatto solo su esplicita richiesta e autorizzazione scritta.*
4. *Alert and Log Review / End Survey: verificare come e se il sistema ha tracciato e identificato l'attacco informatico.*

Il Manuale comprende anche:

- *Metodologia TRIFECTA*
- *Classificazione Falsi Positivi*
- *Classificazione degli Errori*
- *Security Test Audit Report (STAR)*
- *Metriche da applicare alla comparazione*



OSSTMM offre una soluzione per verificare se il budget speso per la Security è adeguato o meno.



OPSEC		
Visibility	1	
Access	3	
Trust	0	
Total (Porosity)	4	

CONTROLS		
Class A		Missing
Authentication	7	0
Indemnification	0	4
Resilience	0	4
Subjugation	0	4
Continuity	0	4
Total Class A	7	16
Class B		Missing
Non-Repudiation	0	4
Confidentiality	0	4
Privacy	1	3
Integrity	0	4
Alarm	9	0
Total Class B	10	15
		True Missing
All Controls Total	17	31
Whole Coverage	42.50%	77.50%

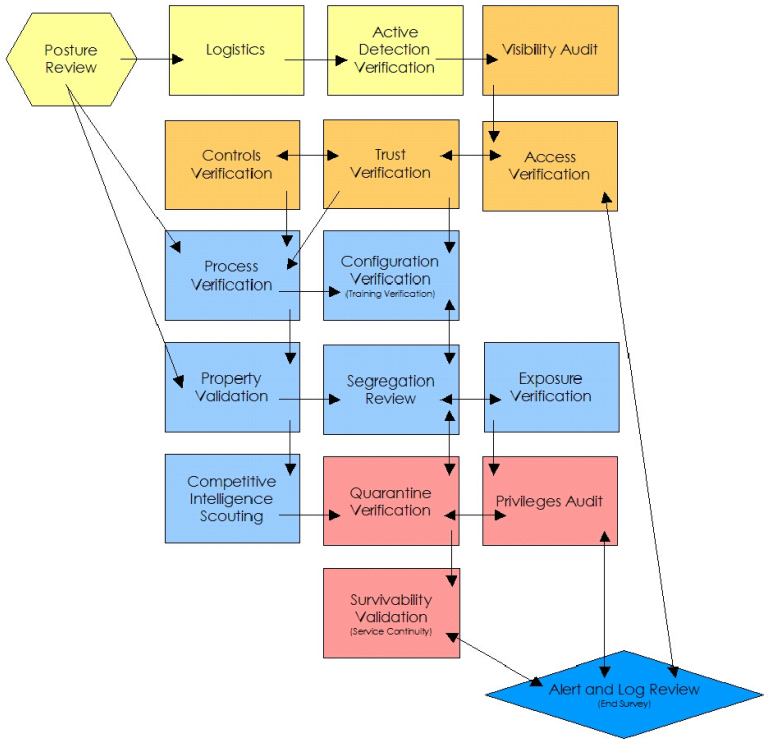
LIMITATIONS		Item Value	Total Value
Vulnerabilities	4	8.750000	35.000000
Weaknesses	5	5.000000	25.000000
Concerns	8	4.750000	38.000000
Exposures	0	5.025000	0.000000
Anomalies	0	4.250000	0.000000
Total # Limitations	17		98.0000

OPSEC	6.776361
True Controls	3.837843
Full Controls	4.986272
True Coverage A	20.00%
True Coverage B	25.00%
Total True Coverage	22.50%
Limitations	15.930239
Security Δ	-17.72
True Protection	81.13

Actual Security: 82.23

Il manuale OSSTMM contempla schede dei controlli necessari alle 4 fasi di test, i processi di test sono codificati, descritti e spiegati. OSSTMM è applicabile come unica metodologia ripetibile.
In Italia la metodologia usata è molto light, nel materiale è
Inclusa anche una versione light della metodologia OSSTMM.

Il manuale OSTMM attualmente pubblico è la 3.0



2.4 Rules Of Engagement

These rules define the operational guidelines of acceptable practices in marketing and selling testing, performing testing work, and handling the results of testing engagements.

A. Sales and Marketing

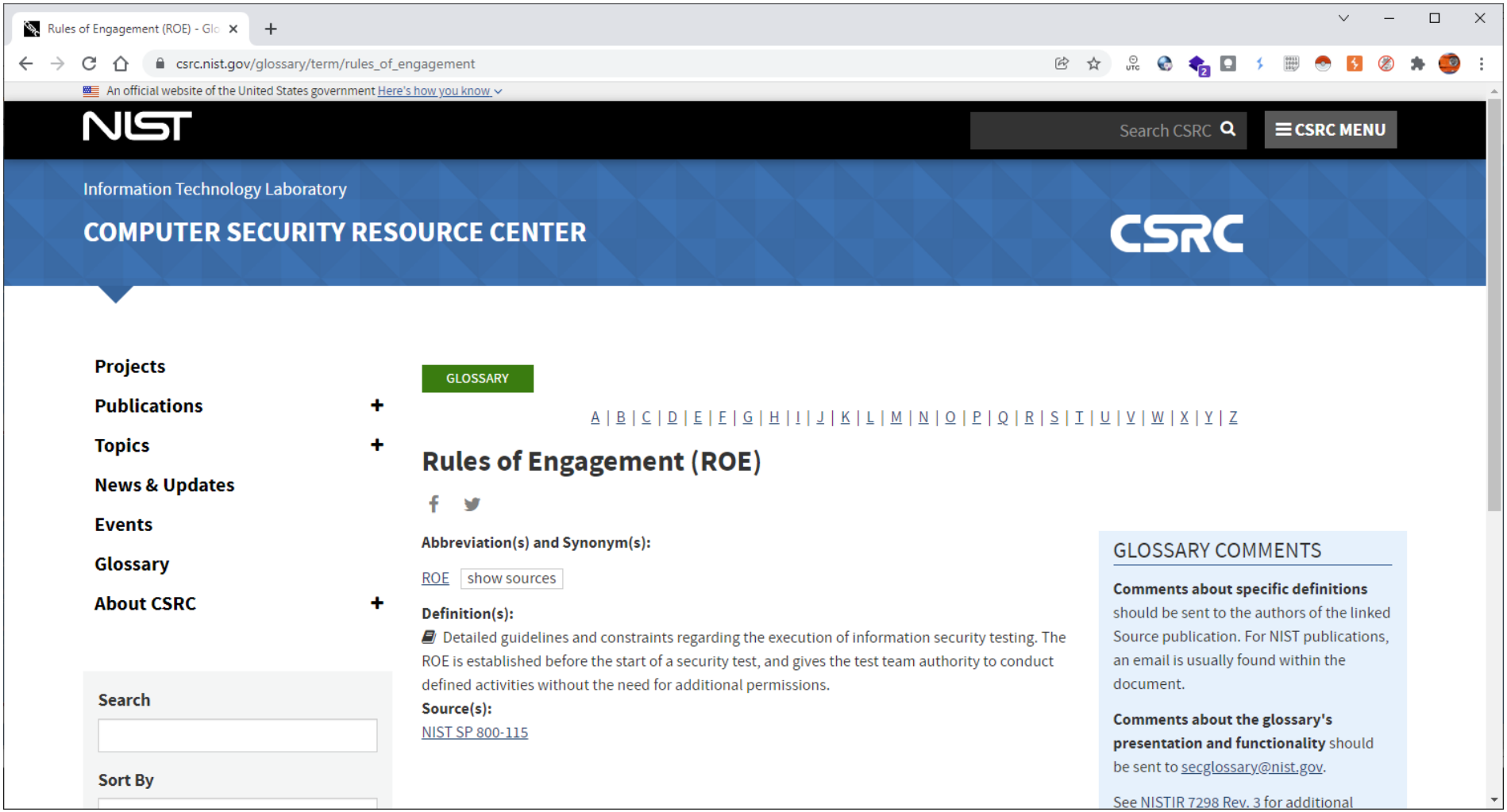
1. The use of fear, uncertainty, doubt, and deception may not be used in the sales or marketing presentations, websites, supporting materials, reports, or discussion of security testing for the purpose of selling or providing security tests. This includes but is not limited to highlighting crimes, facts, glorified criminal or hacker profiles, and statistics to motivate sales.
2. The offering of free services for failure to penetrate the target is forbidden.
3. Public cracking, hacking, and trespass contests to promote security assurance for sales or marketing of security testing or security products are forbidden.
4. To name past or present clients in the marketing or sales for potential customers is only allowed if the work for the client was specifically the same as being marketed or sold and the named client has provided written permission to do so.
5. It is required that clients are advised truthfully and factually in regards to their security and security measures. Ignorance is not an excuse for dishonest consultancy.

B. Assessment / Estimate Delivery

6. Performing security tests against any scope without explicit written permission from the target owner or appropriate authority is strictly forbidden.
7. The security testing of obviously highly insecure and unstable systems, locations, and processes is forbidden until the proper security infrastructure has been put in place.

C. Contracts and Negotiations

8. With or without a Non-Disclosure Agreement contract, the security Analyst is required to provide confidentiality and non-disclosure of customer information and test results.
9. Contracts should limit liability to the cost of the job, unless malicious activity has been proven.
10. Contracts must clearly explain the limits and dangers of the security test as part of the statement of work.
11. In the case of remote testing, the contract must include the origin of the Analysts by address, telephone number or IP address.
12. The client must provide a signed statement which provides testing permission exempting the

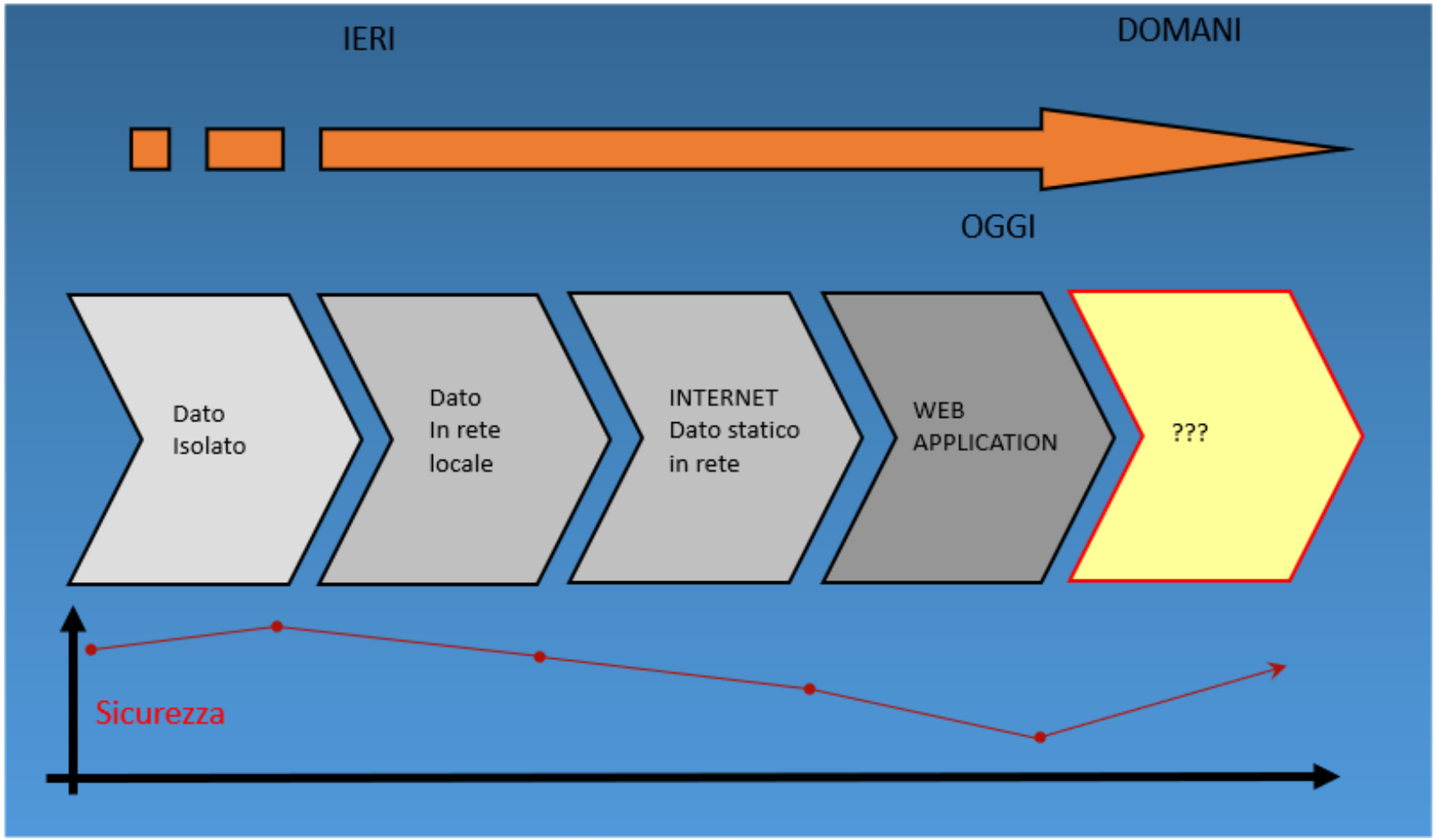

Rules of Engagement (ROE) - Glo
csrc.nist.gov/glossary/term/rules_of_engagement
An official website of the United States government Here's how you know
NIST
Search CSRC
CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
CSRC
Projects
Publications
Topics
News & Updates
Events
Glossary
About CSRC
Search
Sort By
GLOSSARY
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z
Rules of Engagement (ROE)
Abbreviation(s) and Synonym(s):
ROE show sources
Definition(s):
Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions.
Source(s):
NIST SP 800-115
GLOSSARY COMMENTS
Comments about specific definitions should be sent to the authors of the linked Source publication. For NIST publications, an email is usually found within the document.
Comments about the glossary's presentation and functionality should be sent to secglossary@nist.gov.
See NISTIR 7298 Rev. 3 for additional

- *Definisce uno standard per la sicurezza delle applicazioni WEB*
- *OWASP mantiene una Testing Guide aggiornata*
- *OWASP mantiene una lista delle 10 vulnerabilità più critiche aggiornate*
- *OWASP mantiene una Guida allo Sviluppo del codice Sicuro*
- *Sempre più accettata come standard:*
  - *Federal Trade Commission (US Gov)*
  - *Oracle*
  - *Foundstone Inc.*
  - *@ Stake*
  - *VISA, MasterCard, American Express*
  - *PCI-DSS*

Quando la verifica comprende applicazioni pubblicate via WEB si adotta la metodologia OWASP per svolgere le attività di analisi. Questo è lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza applicative, sviluppato da OWASP tramite il modello peer review.

OWASP (Open Web Application Security Project) è una comunità internazionale di ricerca senza scopo di lucro, fondata nel 2001 (in Italia nasce nel 2005) al fine di aumentare la sicurezza del software applicativo, promuovendo lo sviluppo ed il mantenimento di applicazioni web sicure. Nonostante numerose aziende del settore abbiano aderito ad OWASP, la comunità non supporta o raccomanda prodotti o servizi commerciali, ma rimane vendor-independent al fine di assicurare la massima imparzialità. Tutto il materiale documentale ed il software prodotto nell'ambito dei progetti promossi da OWASP è distribuito gratuitamente sotto licenza aperta. La OWASP Testing Guide è un framework di verifica che descrive nel dettaglio come rilevare le problematiche di sicurezza associate al software applicativo. In particolare, essa fornisce gli strumenti metodologici per comprendere quando ed in che modo analizzare le applicazioni web.
Una verifica di sicurezza conforme alle linee guida OWASP consente di rilevare periodicamente la Top Ten delle vulnerabilità più diffuse!

Introduzione (dalla cassaforte a internet)

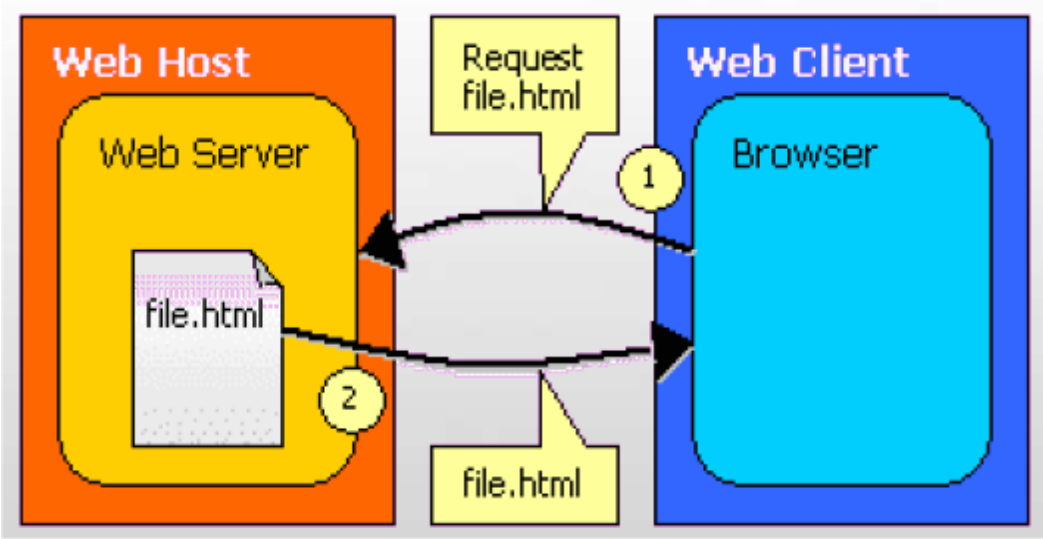


HTTP

L'inizio di tutto...
il protocollo HTTP
nasce come canale di
comunicazione per
scambiarsi le informazioni
tra i centri di ricerca.
Semplici file di testo interpretabili
da un software detto 'Browser'.

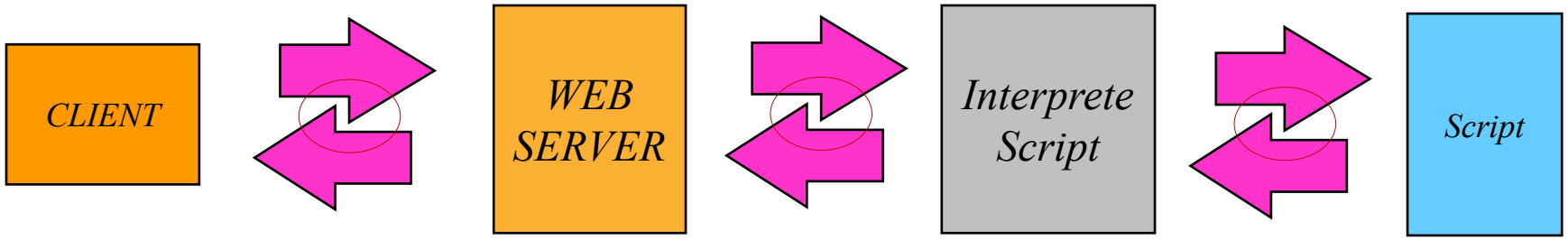
HTTP statico

Il sistema era basato sullo scambio di dati
contenenti informazioni statiche
Interazione minima = Sicurezza Semplice



1 sola interfaccia = 1 solo ingresso
1 catena formata da 1 solo anello
1 solo SPoF

CGI, Script, La rivoluzione delle pagine dinamiche



*Tre interfacce, quattro **punti di attacco***

*Quattro target potenzialmente **vulnerabili***

Java, CGI, Script, La rivoluzione delle pagine dinamiche

Il sistema non funziona:

1. *Non attrae i fruitori come si sperava….*
2. *Costi di acesso ad internet elevati*
3. *Richiede manutenzione complicata*
4. *I costi di accesso ai servizi on line sono troppo alti*
5. *Il time to market diventa una necessità impellente!*

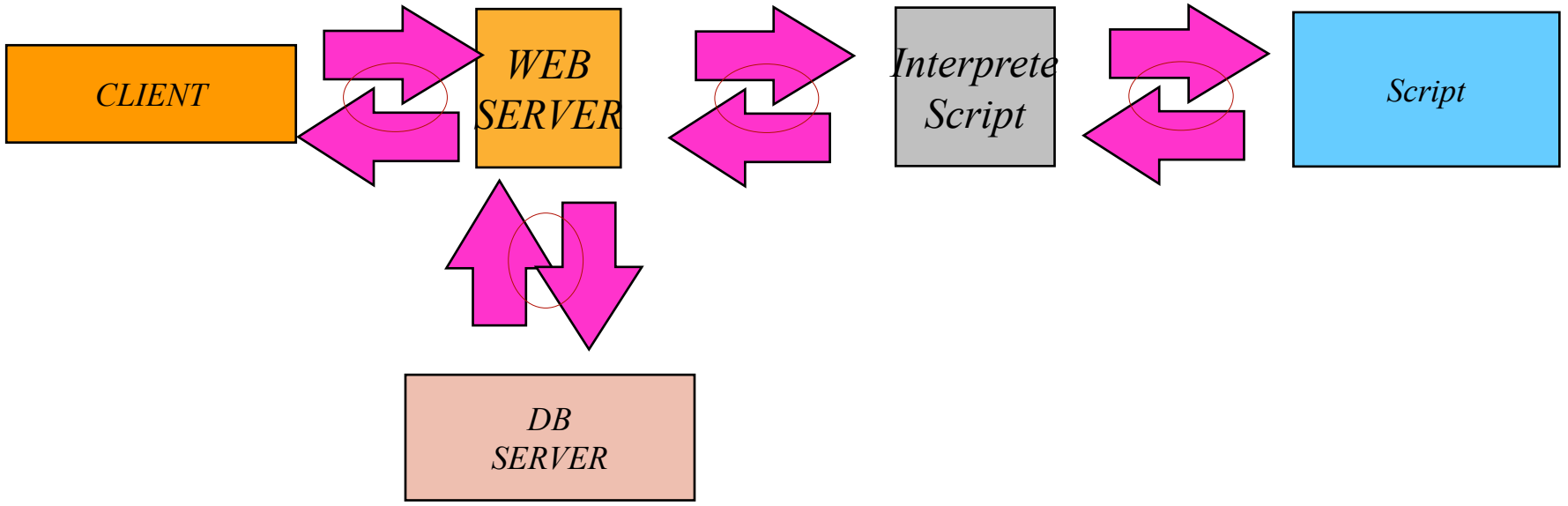
Il web diventa interattivo

Ecco le soluzioni vincenti:

1. *Applicazioni web fruibili (motori di ricerca, B2C, B2B, Tol..)*
2. *Semplificazione della gestione e dell'interazione*
3. *Costi accessibili a tutti*
4. *Aumento delle opportunità di business*
5. *Nascono i Portali ed i CMS*
6. *L'utente fa tutto con un semplice CLICK !*
7. *Tutti voglio cliccare, chattare, creare home page*
8. *Tutti cliccano dappertutto, nascono le comunità virtuali…*
9. *Proliferano le interfacce di comunicazione WAP, MMS…*

…ma in informatica semplificare le cose da un punto di vista, spesso, vuol dire complicarle da un altro…

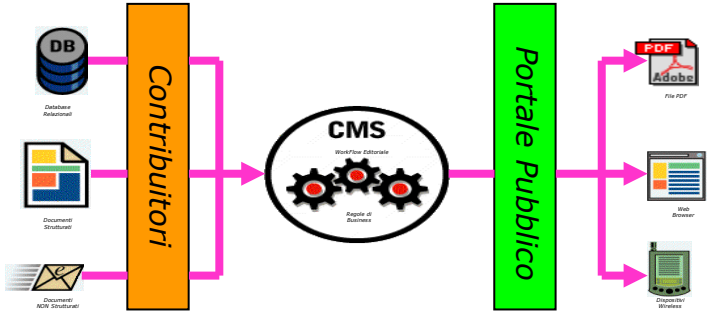
Il web diventa interattivo ma.....



*Quattro interfacce, cinque **punti di attacco***
*Cinque Software potenzialmente **vulnerabili***

E non solo……

Entra in gioco il fattore umano……



Aumenta il livello di complessità delle architetture, aumenta l’interazione tra diverse figure professionali (Sistemista, DBA, Programmatore , Analista……)

Scende il livello di complessità di utilizzo da parte dell’utente….. basta un CLICK!

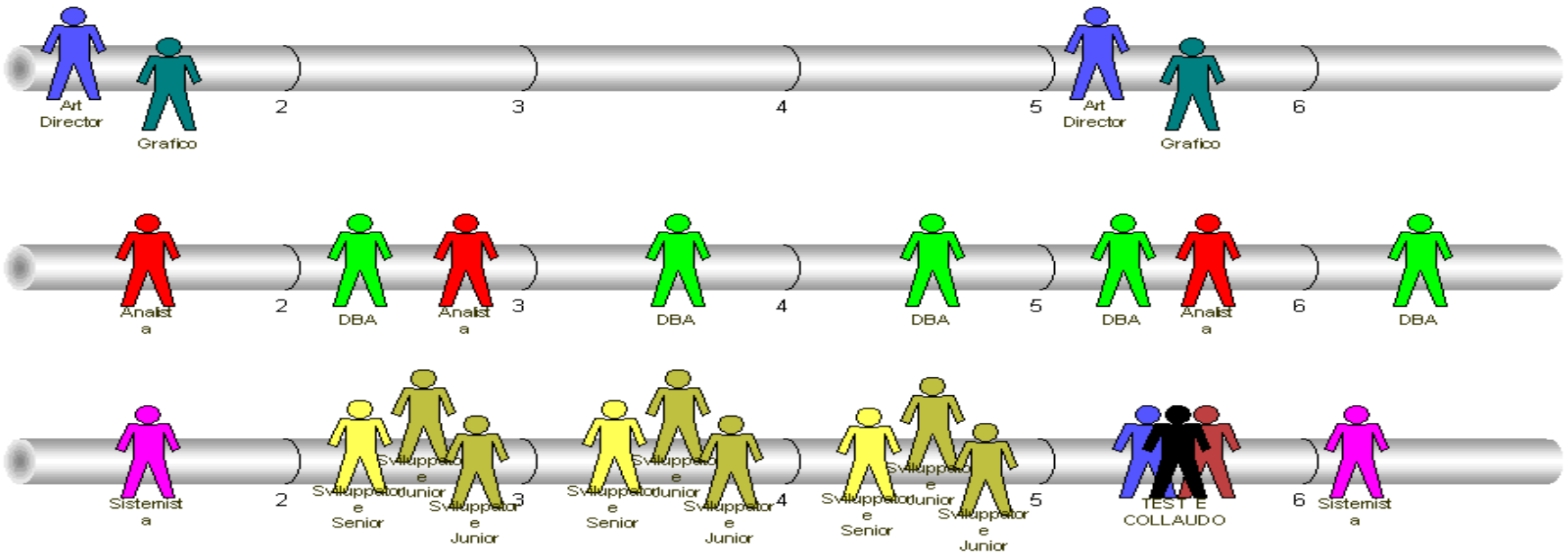


Figure:

1 Art Director
1 Grafico
1 Analista
1 Sistemista
1 Sviluppatore Senior
2 Sviluppatori Junior
1 DBA

Tempi:

Portale di piccole dimensioni	2 Mesi
Portale di medie dimensioni	4 Mesi
Portale di grandi dimensioni	6 Mesi

Stima:

piccolo:	3 sezioni e 1 servizio dinamico
medio:	8 sezioni e 3 servizi dinamici
grande:	12 sezioni e 6 servizi dinamici

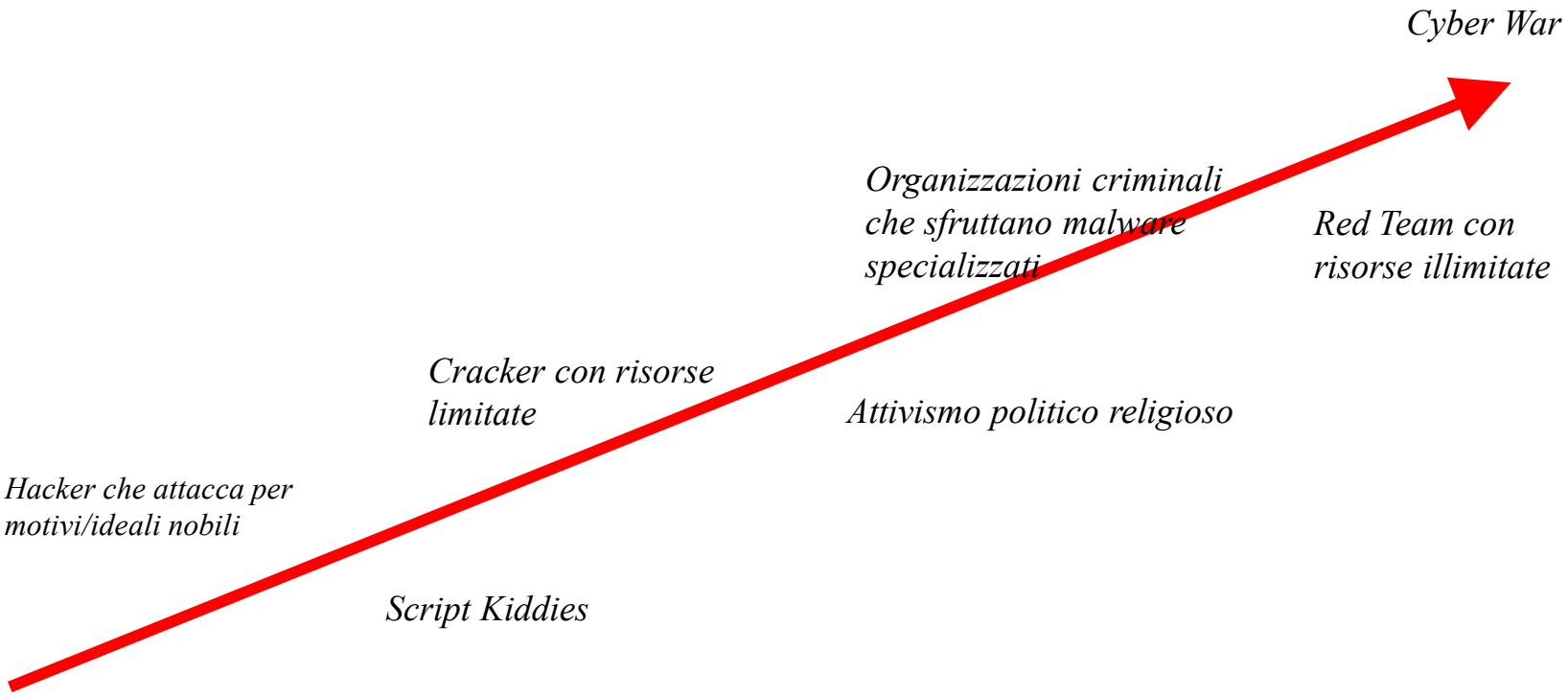
Per ogni sezione in più, calcolare + 5gg
Per ogni servizio in più, calcolare + 10gg

Legenda:

sezione = equivale ad un canale e comunque ad una pagina foglia
servizio = equivale ad una o più pagine dinamiche connesse al DB

E per finire…..

Aumenta la specializzazione del nemico



Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

Rapporto Clusit ottobre 2021

Rispetto al secondo semestre 2020, in termini assoluti nel 1° semestre 2021 la crescita maggiore nel numero di attacchi gravi si osserva verso le categorie "Transportation / Storage" (**+108,7%**), "Professional, Scientific, Technical" (**+85,2%**) e "News & Multimedia" (**+65,2%**), seguite da "Wholesale / Retail" (**+61,3%**) e "Manufacturing" (**+46,9%**). Aumentano anche gli attacchi verso le categorie "Energy / Utilities" (**+46,2%**), "Government" (**+39,2%**), "Arts / Entertainment" (**+36,8%**) ed "Healthcare" (**+18,8%**).

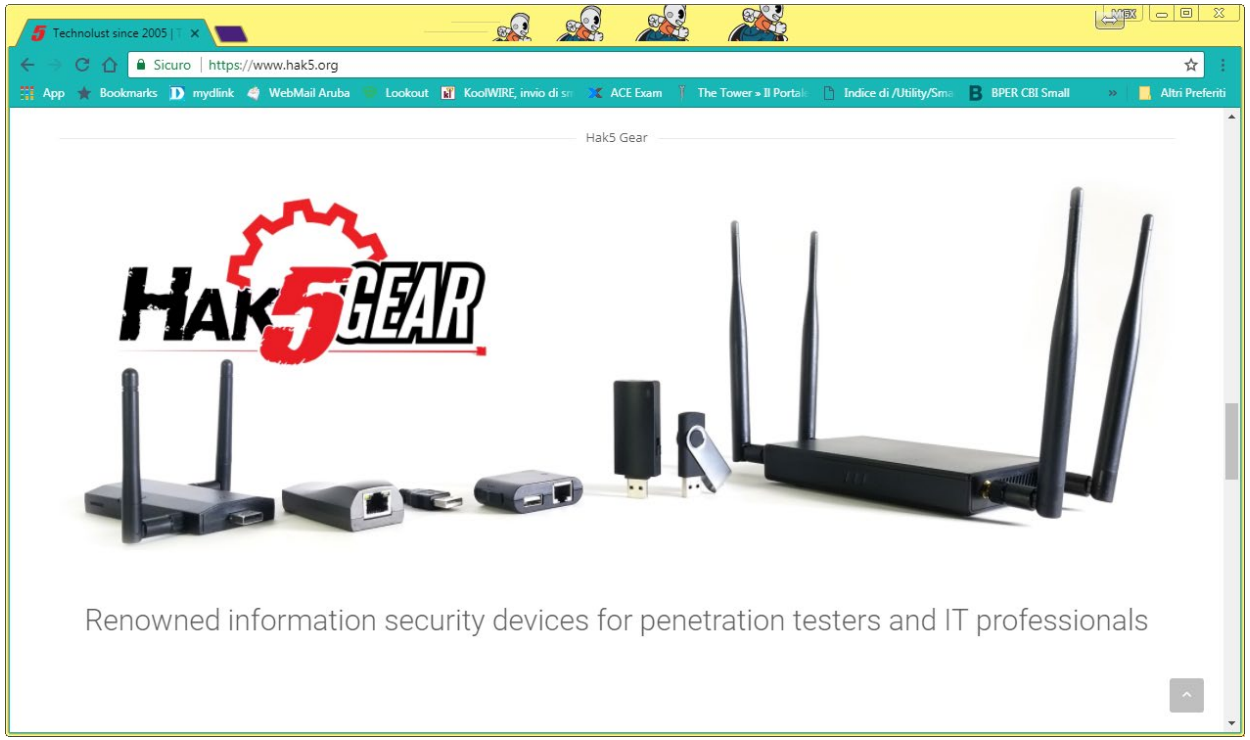
Per quanto riguarda la **severity**: nel 2020 gli attacchi con impatto "Critico" rappresentavano il **13%** del totale, quelli di livello "Alto" il **36%**, quelli di livello "Medio" il **32%** ed infine quelli di livello "Basso" il **19%**. Complessivamente, gli attacchi gravi con effetti molto importanti (High) o devastanti (Critical) nel 2020 erano il **49%** del campione. Nel primo semestre 2021 la situazione è molto diversa, e francamente impressionante: gli attacchi gravi con effetti molto importanti (High) sono il **49%**, quelli devastanti (Critical) rappresentano il **25%**, quelli di impatto significativo (Medium) il **22%**, e quelli con impatto basso solo il **4%**. In questo caso gli attacchi con impatto Critical e High sono il **74%**.

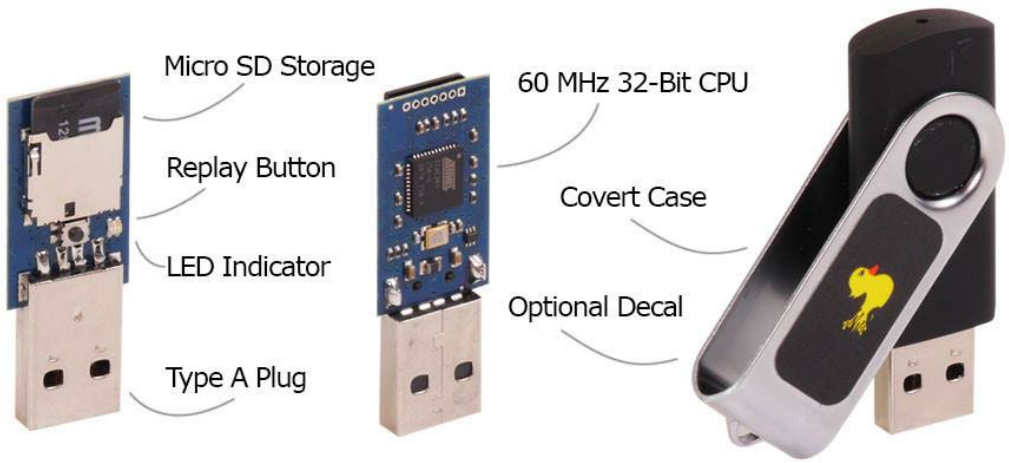
Agenda

- *Una avvincente indagine sulle origini*
- *Chi sono i veri HACKER, chi i Cybercriminali e i Cybercop*
- *ISECOM 12 Dispense in italiano per "diventare" Ethical Hacker*
- *Principi fondamentali di VAPT*
- *Cenni alle metodologie OSSTMM e OWASP*
- *Crimine Organizzato… V2.0*
- *Nuovi hardware, nuove minacce…*

TRUST YOUR TECHNOLUST

High tools at low cost!





simple ducky payload.txt - Notepad

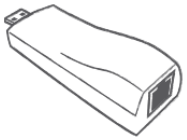
File Edit Format View Help

```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

HAK5
TRUST YOUR TECHNOLUST

Sembra una normale chiavetta USB… ma lavora come una tastiera…

HAK5
TRUST YOUR TECHNOLUST

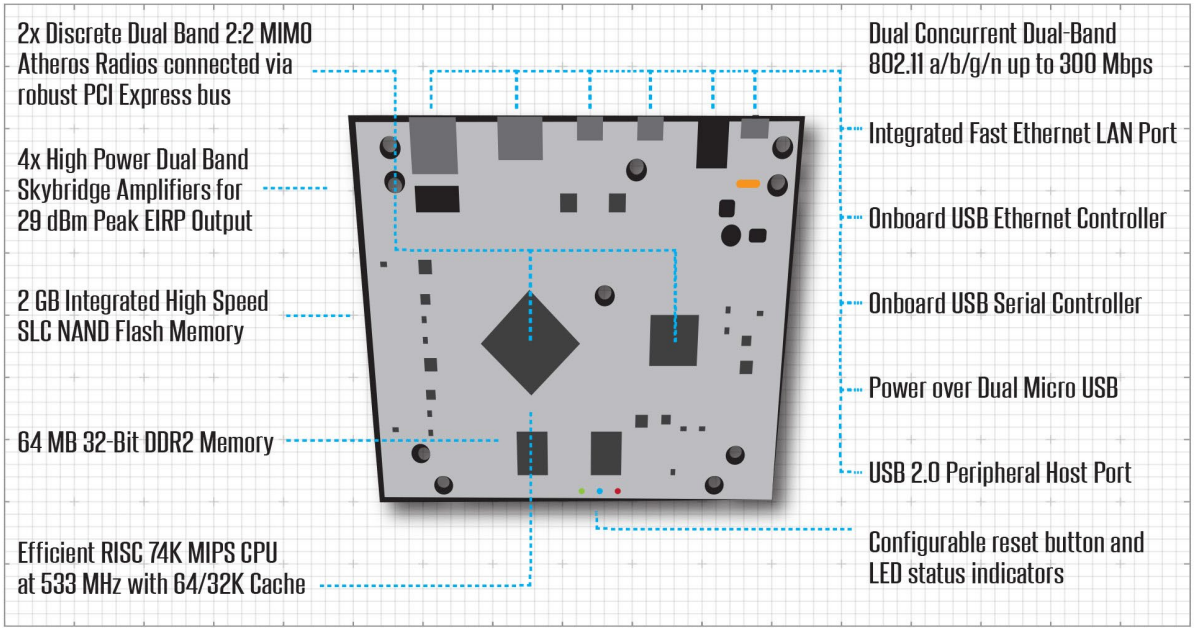


CONFIGURE

DEPLOY

ACCESS

HAK5
TRUST YOUR TECHNOLUST



USBKill | USB Kill devices for pen

usbkill.com

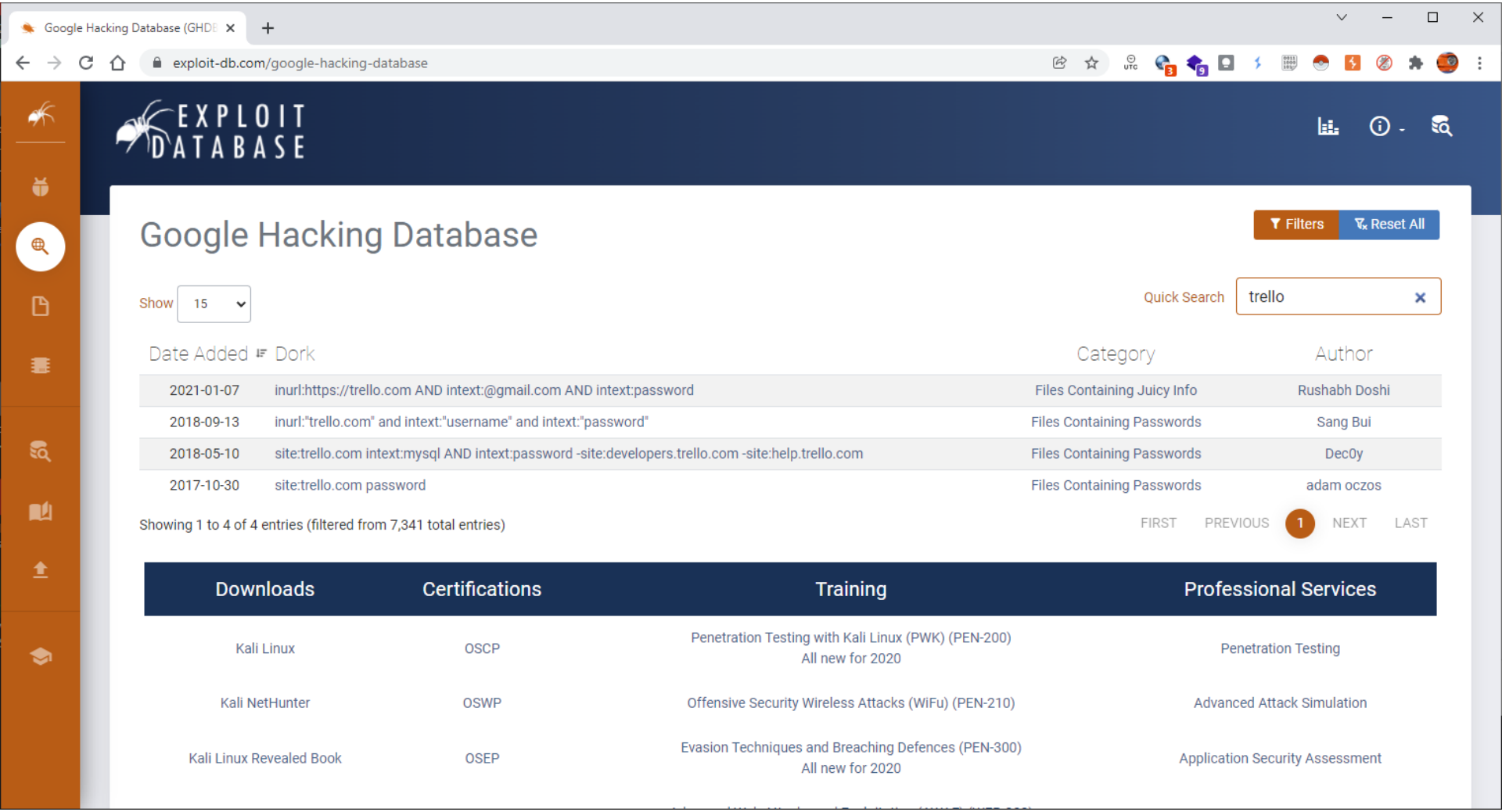
USBKILL

USBKill | USB Kill Kits | Accessories | Test Results | NFCKill | FAQ

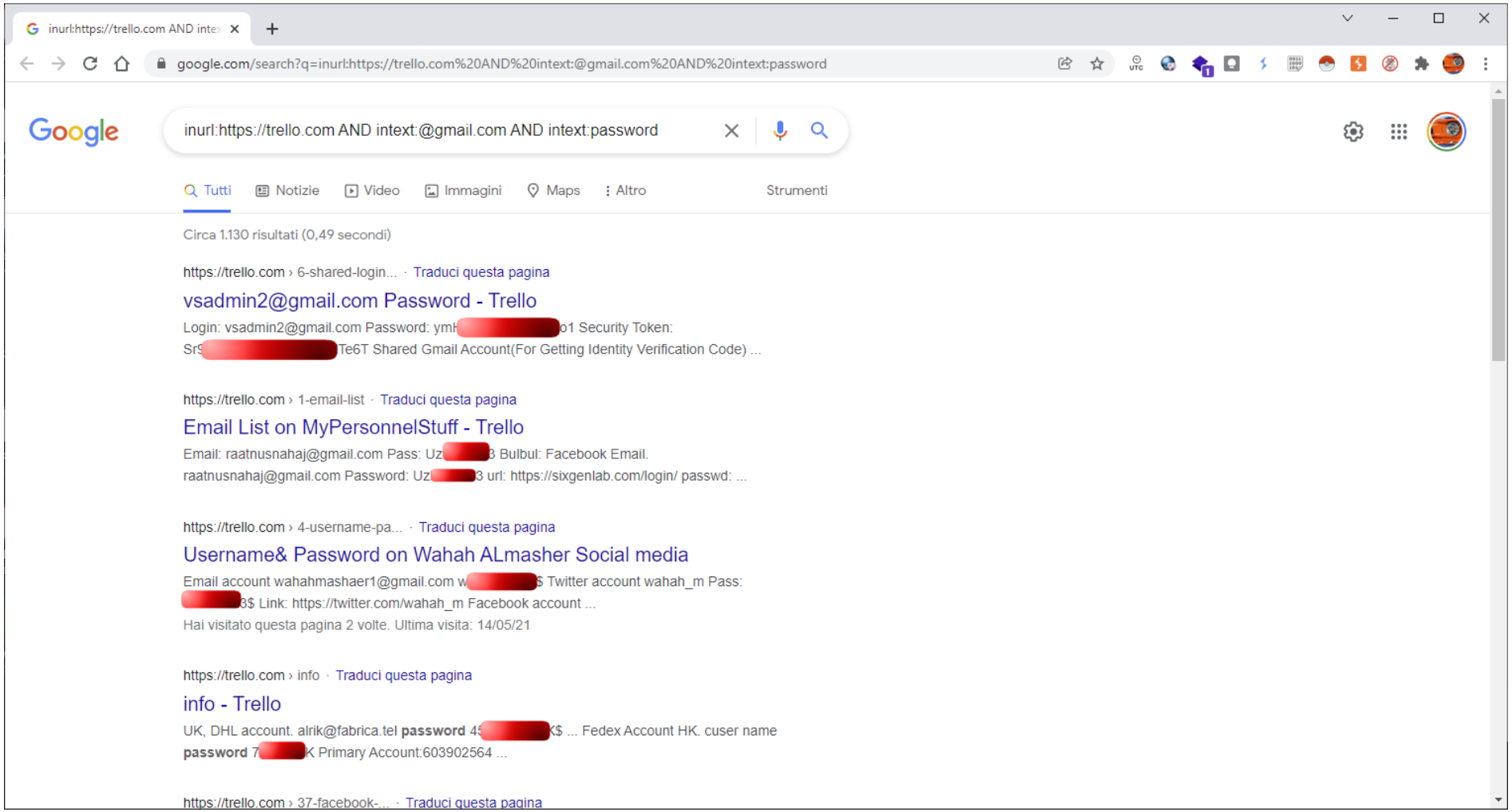
USBKill V4.0

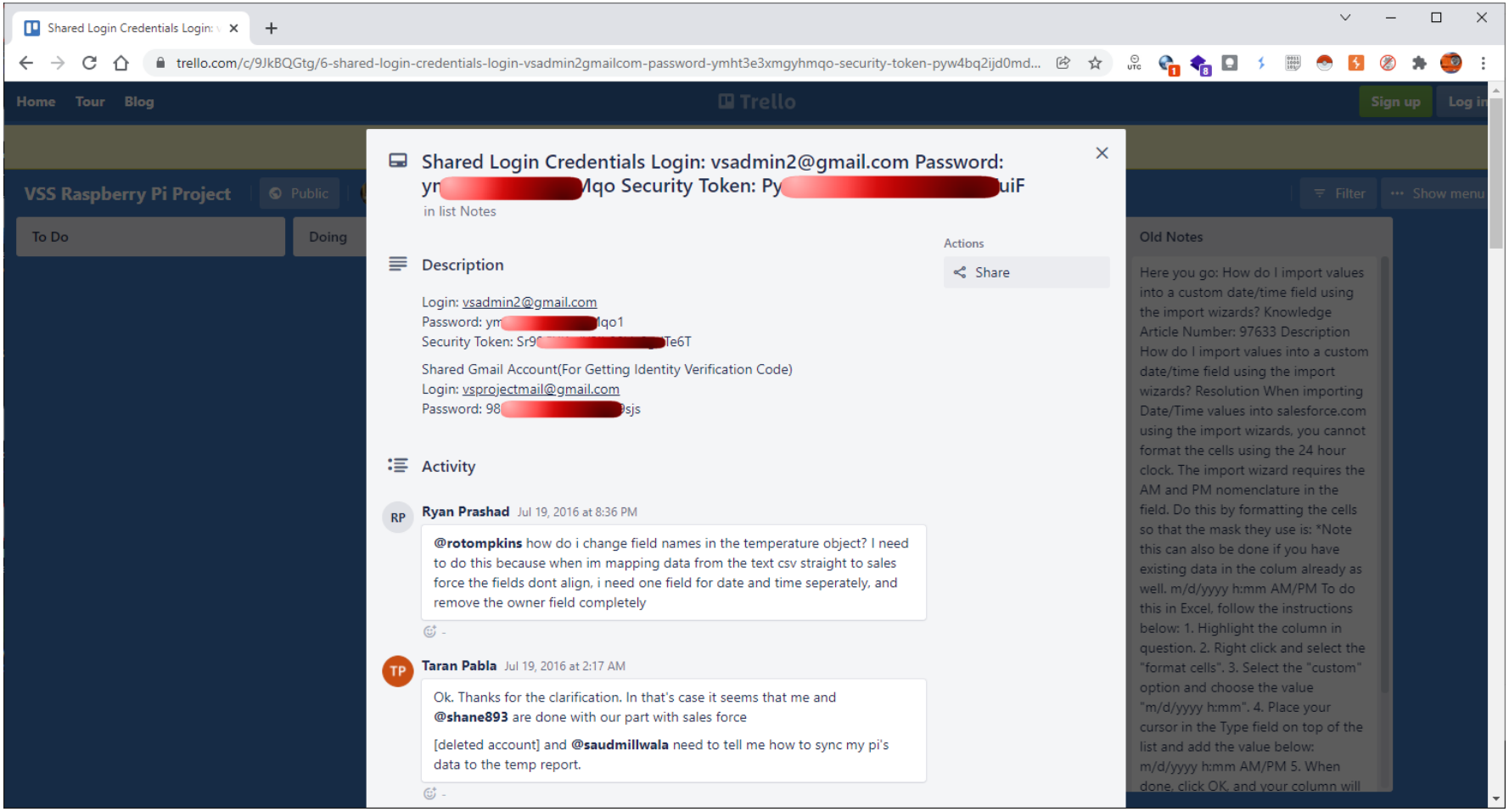
The new USBKill plugs into everything.|

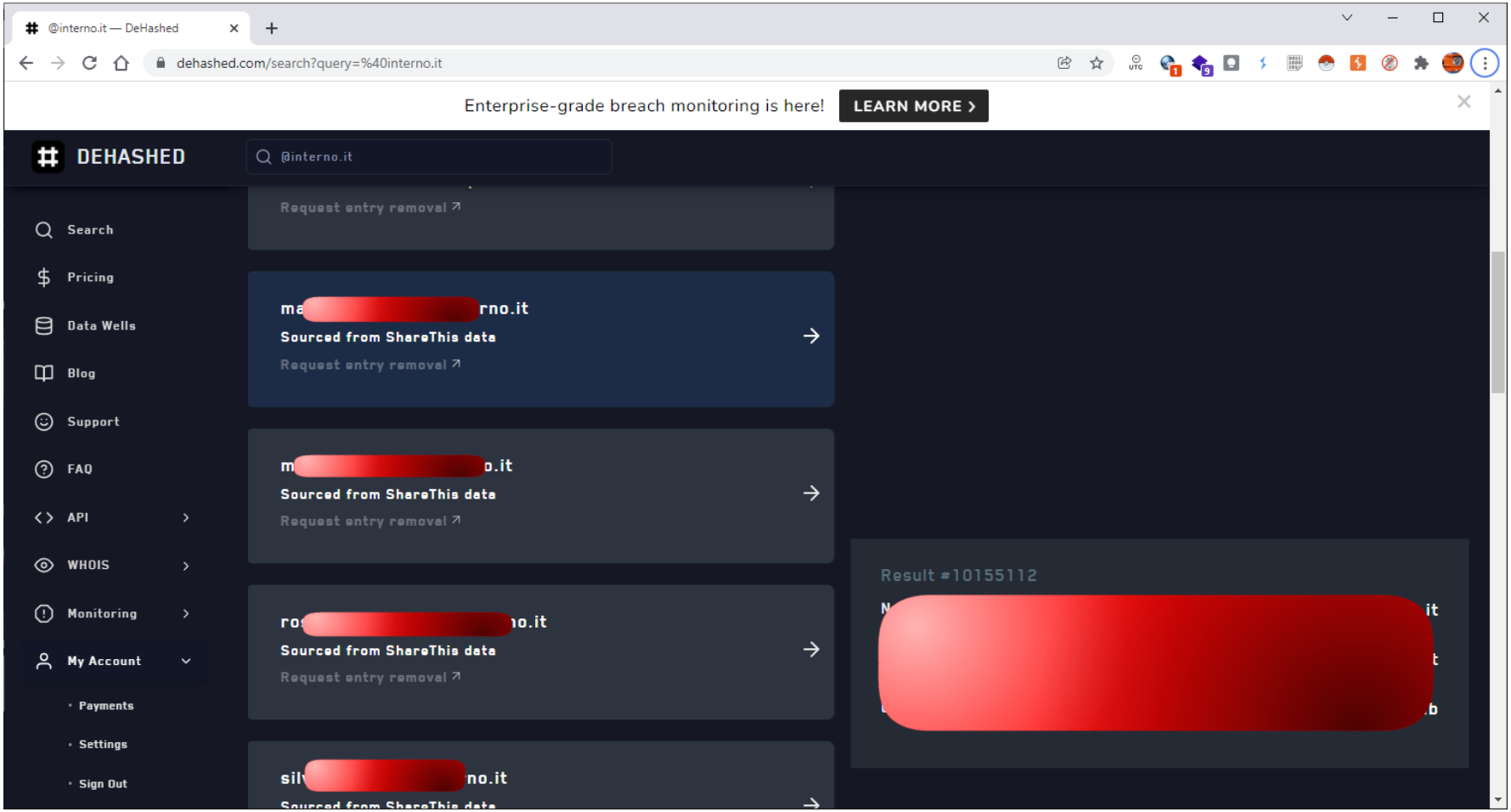
The most powerful USBKill ever. New unstoppable attack modes. Remote controlled. The ultimate pentesting device.


Google Hacking Database (GHDB
exploit-db.com/google-hacking-database
EXPLOIT DATABASE
Google Hacking Database
Filters
Reset All
Show 15
Quick Search
trello
Date Added
Dork
Category
Author
2021-01-07
inurl:https://trello.com AND intext:@gmail.com AND intext:password
Files Containing Juicy Info
Rushabh Doshi
2018-09-13
inurl:"trello.com" and intext:"username" and intext:"password"
Files Containing Passwords
Sang Bui
2018-05-10
site:trello.com intext:mysql AND intext:password -site:developers.trello.com -site:help.trello.com
Files Containing Passwords
Dec0y
2017-10-30
site:trello.com password
Files Containing Passwords
adam oczos
Showing 1 to 4 of 4 entries (filtered from 7,341 total entries)
FIRST
PREVIOUS
1
NEXT
LAST
Downloads
Certifications
Training
Professional Services
Kali Linux
OSCP
Penetration Testing with Kali Linux (PWK) (PEN-200)
All new for 2020
Penetration Testing
Kali NetHunter
OSWP
Offensive Security Wireless Attacks (WiFu) (PEN-210)
Advanced Attack Simulation
Kali Linux Revealed Book
OSEP
Evasion Techniques and Breaching Defences (PEN-300)
All new for 2020
Application Security Assessment

inurl:https://trello.com AND intext:@gmail.com AND intext:password






@interno.it — DeHashed
dehashed.com/search?query=%40interno.it
Enterprise-grade breach monitoring is here!
LEARN MORE >
DEHASHED
@interno.it
Search
Pricing
Data Wells
Blog
Support
FAQ
API
WHOIS
Monitoring
My Account
Payments
Settings
Sign Out
Request entry removal
Sourced from ShareThis data
Request entry removal
Sourced from ShareThis data
Request entry removal
Sourced from ShareThis data
Request entry removal
Result #10155112

Segue intervento dell’Avv.to Stefano Aterno, e successivamente tavola rotonda moderata dalla giornalista Alessia Valentini.

Sitografia in ordine di apparizione 1

https://documen.site/download/enciclopedia-dellhacking-lord-shiva_pdf
https://it.wikipedia.org/wiki/Glider_(hacker)
https://www.autistici.org/ironbishop/glider/hacker_emblem.html
http://www.catb.org/jargon/html/
http://www.catb.org/~esr/ecsl/index.html
https://it.wikipedia.org/wiki/Linus_Torvalds
https://www.academia.edu/search?q=hacker
http://www.adir.unifi.it/rivista/2003/tavassi/
https://medium.com/@danielebottonibomber/i-trenini-elettrici-e-gli-hackers-5639643c5666
https://it.wikipedia.org/wiki/Spaghetti_hacker
https://www.ikkisoft.com/stuff/ctf2005.pdf
https://www.google.com/search?q=mit+tech+model+railroad+club&sxsrf=AOaemvJiBFG35nzAf0a1jBivVn5WhljT3Q:1642884029101&source=lnms&tbm=isch&sa=X&ved=2ahUKEwizxdj3m8b1AhXqS_EDHYJCBGQQ_AUoAXoECAIQAw&biw=1512&bih=730&dpr=1
https://www.accademiacivicadigitale.org/phreaking-definizione/
https://en.wikipedia.org/wiki/John_Draper
https://www.macitynet.it/quella-volta-jobs-wozniak-fecero-uno-scherzo-al-vaticano
https://it.wikipedia.org/wiki/Kevin_Mitnick
https://it.wikipedia.org/wiki/Loyd_Blankenship
https://www.youtube.com/watch?v=4eydT_iB0-U&t=80s
https://ricerca.repubblica.it/repubblica/archivio/repubblica/2003/09/23/ora-sono-un-hacker-etico.html
https://www.cobrasoft.it/
https://www.hackerhighschool.org/lessons.html
http://milano.repubblica.it/dettaglio/un-pm-hacker-viola-il-tribunale-ecco-come-far-sparire-dati-delicati/1584048

Sitografia argo

https://it.wikipedia.org/wiki/Phishing
https://www.redhotcyber.com/post/le-hacker-girl-pi%C3%B9-famose-kristina-svechinskaya
https://it.wikipedia.org/wiki/Penetration_test
https://bughunters.google.com/about/rules/6625378258649088
https://www.gruppotim.it/it/footer/responsible-disclosure.html
https://www.isecom.org/research.html
https://www.isecom.org/OSSTMM.3.pdf
https://www.isecom.org/certification.html
https://csrc.nist.gov/glossary/term/roe
https://doi.org/10.6028/NIST.SP.800-115
https://owasp.org/
https://owasp.org/www-project-top-ten/
https://owasp.org/www-chapter-italy/
https://hak5.org/
https://hak5.org/products/usb-rubber-ducky-deluxe
https://hak5.org/products/wifi-pineapple
https://it.wikipedia.org/wiki/USB_Killer
https://www.youtube.com/watch?v=X1LfPASxDpI
https://www.exploit-db.com/google-hacking-database
https://www.dehashed.com/
https://crackstation.net/
http://fabruggeri.sganawa.org/art_dir.htm

Contatti

massimiliano.graziani@cybera.it

Dubbi, altre domande? Desiderate approfondimenti riguardo gli argomenti trattati? Scrivetemi, rispondo sempre a tutti!

Grazie…

Era il 6 giugno 2018 mentre ero relatore al Security Summit di Roma, non rispondevo al cellulare e non potevo soccorrere mio padre, colto da un infarto, mentre tutti mi chiamavano…

Tra sensi di colpa e rimorso per non essere arrivato in tempo per vederlo ancora vivo, per l'ultima volta…
…per questo dedico a Giuseppe, mio padre, ogni attività di divulgazione e condivisione accademica, perseguendo i valori che mi ha trasmesso: umiltà, generosità e sacrificio.

Grazie di tutto papà.