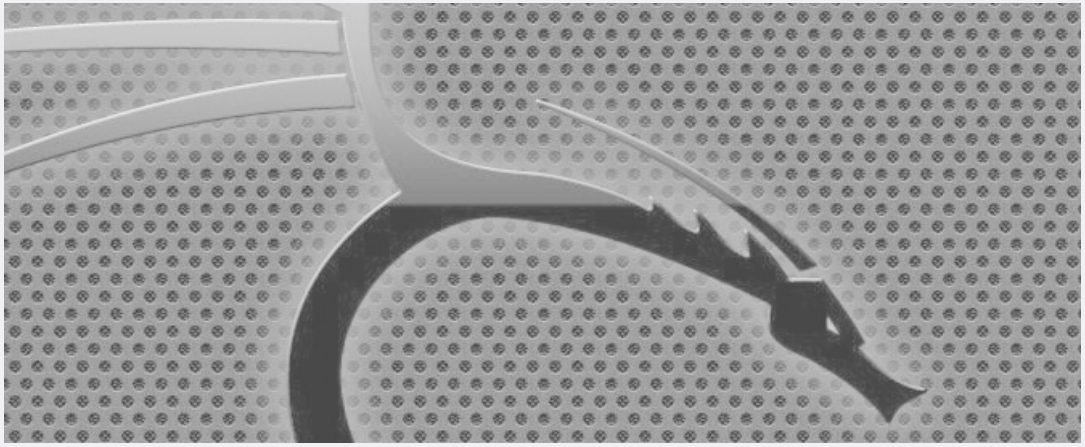


Kali Linux

OpenSourceDay 2013

Università degli studi di Udine

-*Fabio Carletti aka Ryuw*-

“the quieter you became, the more you are able to hear”

Whoami?...FabioCarletti

- *Member:Clusit,DebianItalia,Sikurezza.org,MetroOlografix,Camelug,LinuxFriends,LinuxItalia,OpenBSD group,...ecc*
- *Currently IT Security Specialist presso*

Lejot-OpenSource tecnology

- *I like unix :-)*

Security IT

La sicurezza informatica è un processo, non un prodotto, non vi è nulla che con il semplice acquisto garantisca la sicurezza della nostra infrastruttura.La sicurezza della nostra rete dipende da molti fattori, i software firewall è solo uno di essi!

Secure code

La sicurezza del codice è un processo da inserire nella strategia security IT

Il software scritto senza molte attenzioni nell'ambito della sicurezza sta influendo le fondamenta di infrastrutture informatiche

Il mio sistema Operativo è sicuro..

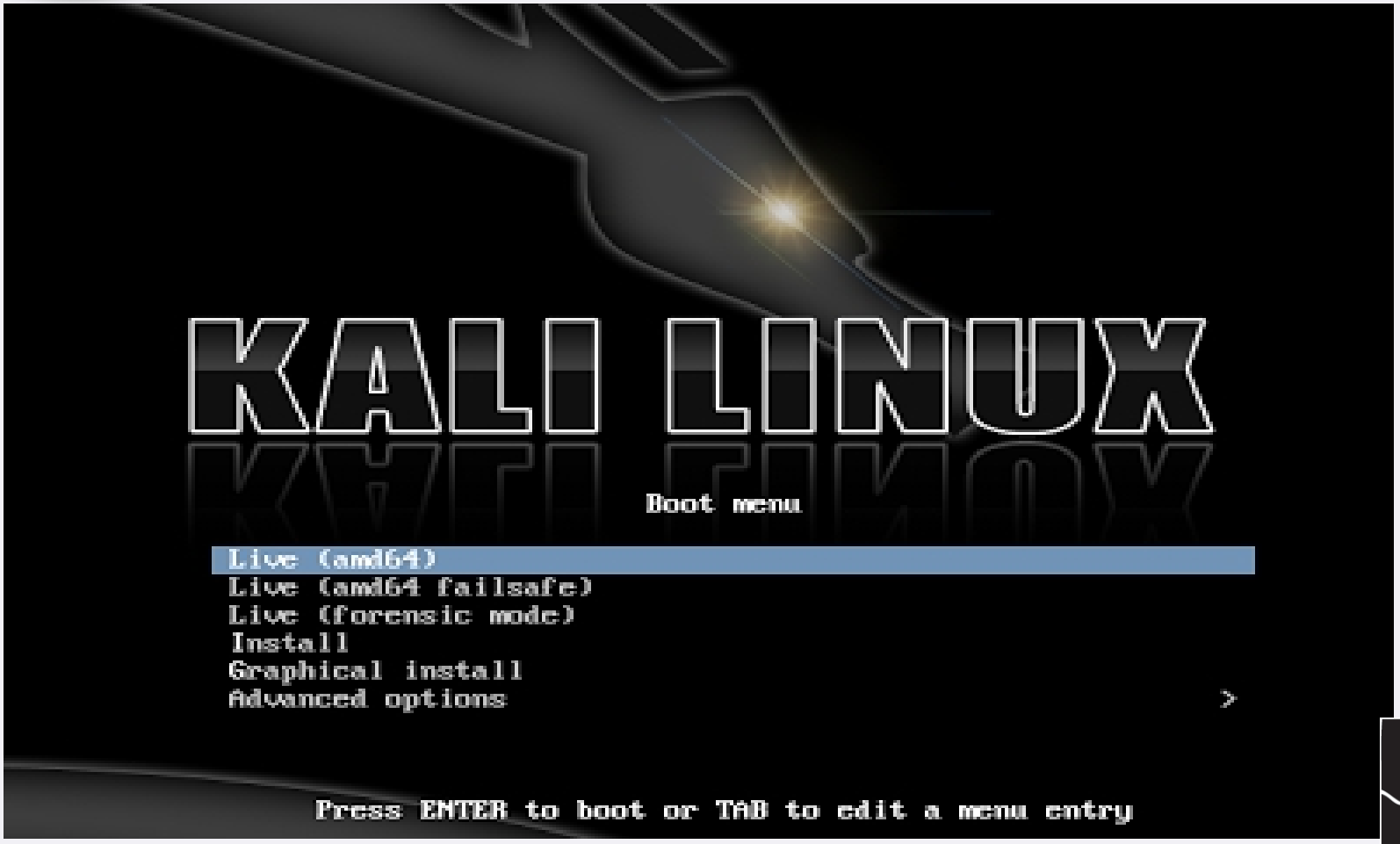
Sicurezza IT non solo nel significato tecnico:confidenzialità,integrità,disponibilità,

autenticita

OpensourceDay Udine

OpenSourceDay 2013

- Kali fornisce i più potenti strumenti per il penetration test attualmente presenti, sono installati tutti i software necessari per tentare di hackerare un pc o un sito web, per poter cosi testare la sicurezza dei nostri sistemi.
- Basata su Debian GNU/Linux pensata per l'informatica forense e la sicurezza informatica
- Kali Linux is based on Debian and uses a customized GNOME Shell
- Piattaforme:i386, x86-64, ARM
- Sito: kali.org (Offensive Security)
- docs.kali.org - documentation site
- forums.kali.org – Discussion Forums
- bugs.kali.org – For reporting bugs
- git.kali.org - monitor the development of Kali Linux


KALI LINUX
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Install
Graphical install
Advanced options
>
Press ENTER to boot or TAB to edit a menu entry

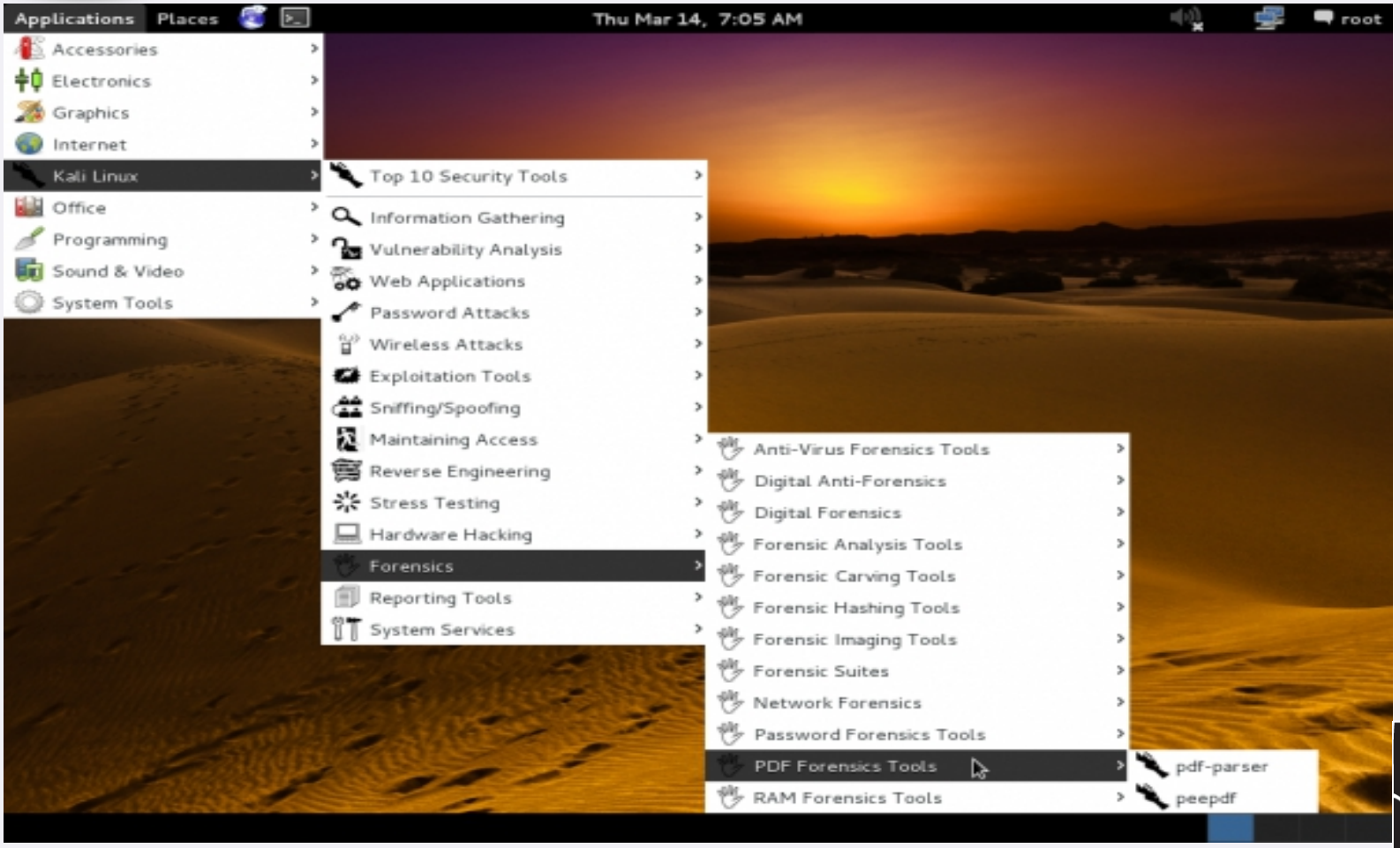
Security<->Forensics

Security IT prepara/previene/riduce i rischi

L'informatica forense è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, l'impiego ed ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo giuridico. (Wikipedia)

Forensics=investiga,analizza,recupera

Quindi per le indagini giudiziarie...e non solo---> il PC considerato come fonte di prova.


Applications
Places
Thu Mar 14, 7:05 AM
root
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
Anti-Virus Forensics Tools
Digital Anti-Forensics
Digital Forensics
Forensic Analysis Tools
Forensic Carving Tools
Forensic Hashing Tools
Forensic Imaging Tools
Forensic Suites
Network Forensics
Password Forensics Tools
PDF Forensics Tools
RAM Forensics Tools
pdf-parser
peepdf

Compiti e categorie

Compito generale della computer forensics:

- Analizzare i dati senza alterarli
- Garantire le prove acquisite
- Acquisire le prove senza alterare o modificare il sistema informatico
- Network-forensics, mobile-forensics,

introdusion - forensics e computer forensics

KALI LINUX

Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

Screenshot | Go Back | Continue

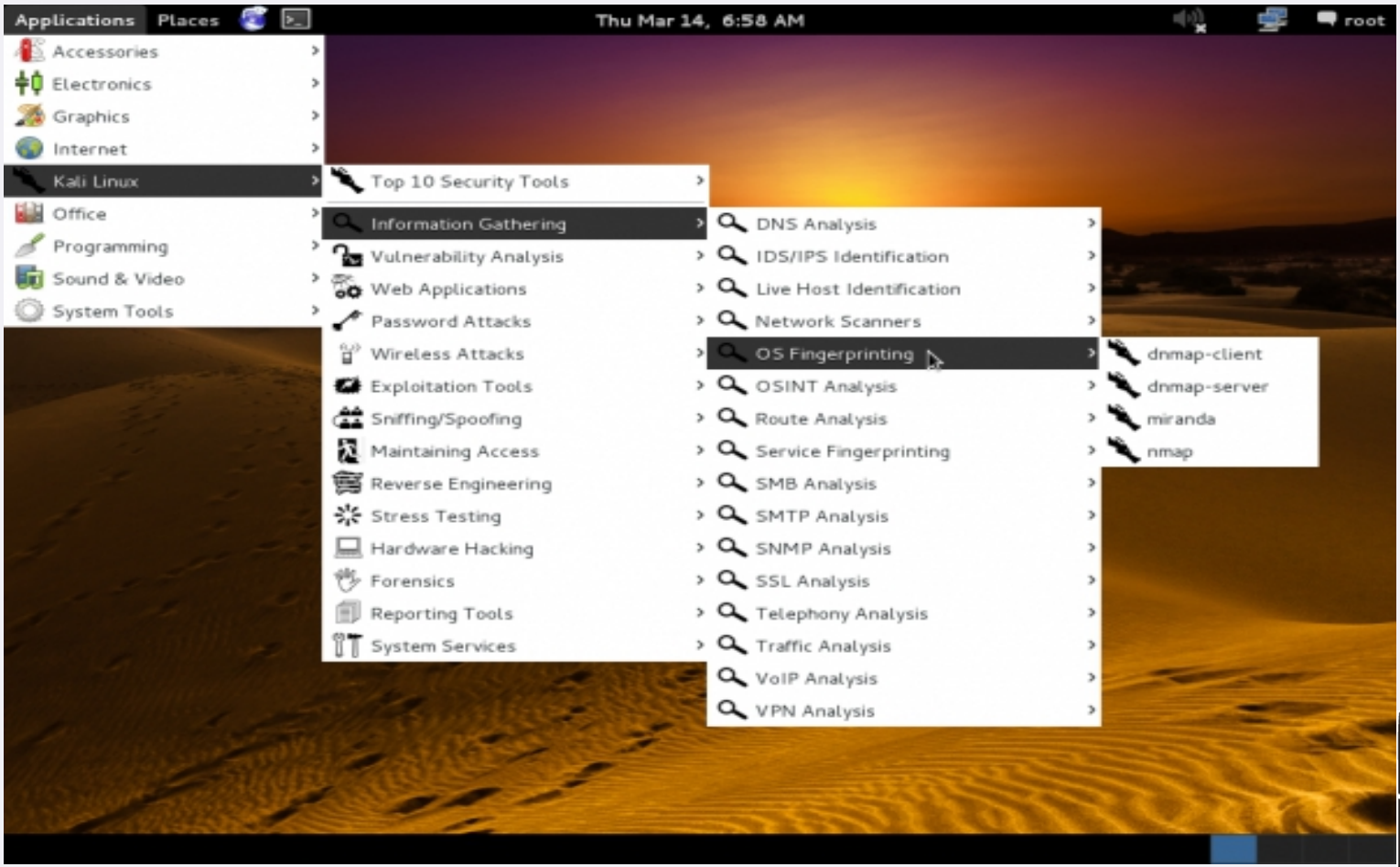
Perchè Linux

Linux permette di montare le unità e i supporti removibili in modalità sola lettura(read-only)

Gnu/Linux supporta un enorme quantità di Filesystem diversi.

E' opensource il sorgente è visionabile da chiunque

Il mondo Linux dispone di numerosi tools per la forensics


Applications
Places
Thu Mar 14, 6:58 AM
root
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
DNS Analysis
IDS/IPS Identification
Live Host Identification
Network Scanners
OS Fingerprinting
OSINT Analysis
Route Analysis
Service Fingerprinting
SMB Analysis
SMTP Analysis
SNMP Analysis
SSL Analysis
Telephony Analysis
Traffic Analysis
VoIP Analysis
VPN Analysis
dnmap-client
dnmap-server
miranda
nmap

Cracker= colui che si ingegna per eludere blocchi imposti da qualsiasi software al fine di trarne guadagno distribuendoli

Hacker=persona che si impegna a superare sfide intellettuali per aggirare le limitazioni che gli vengono imposte

Lamer=aspirante Cracker con knowhow IT limitate..ma anche una persona che si crede hacker in grado di distruggere pc altrui..

Penetration test

-processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. L'analisi comprende più fasi ed ha come obiettivo evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità che ne hanno permesso l'accesso non autorizzato. L'analisi è condotta dal punto di vista di un potenziale attaccante e consiste nello sfruttamento delle vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere al sistema.

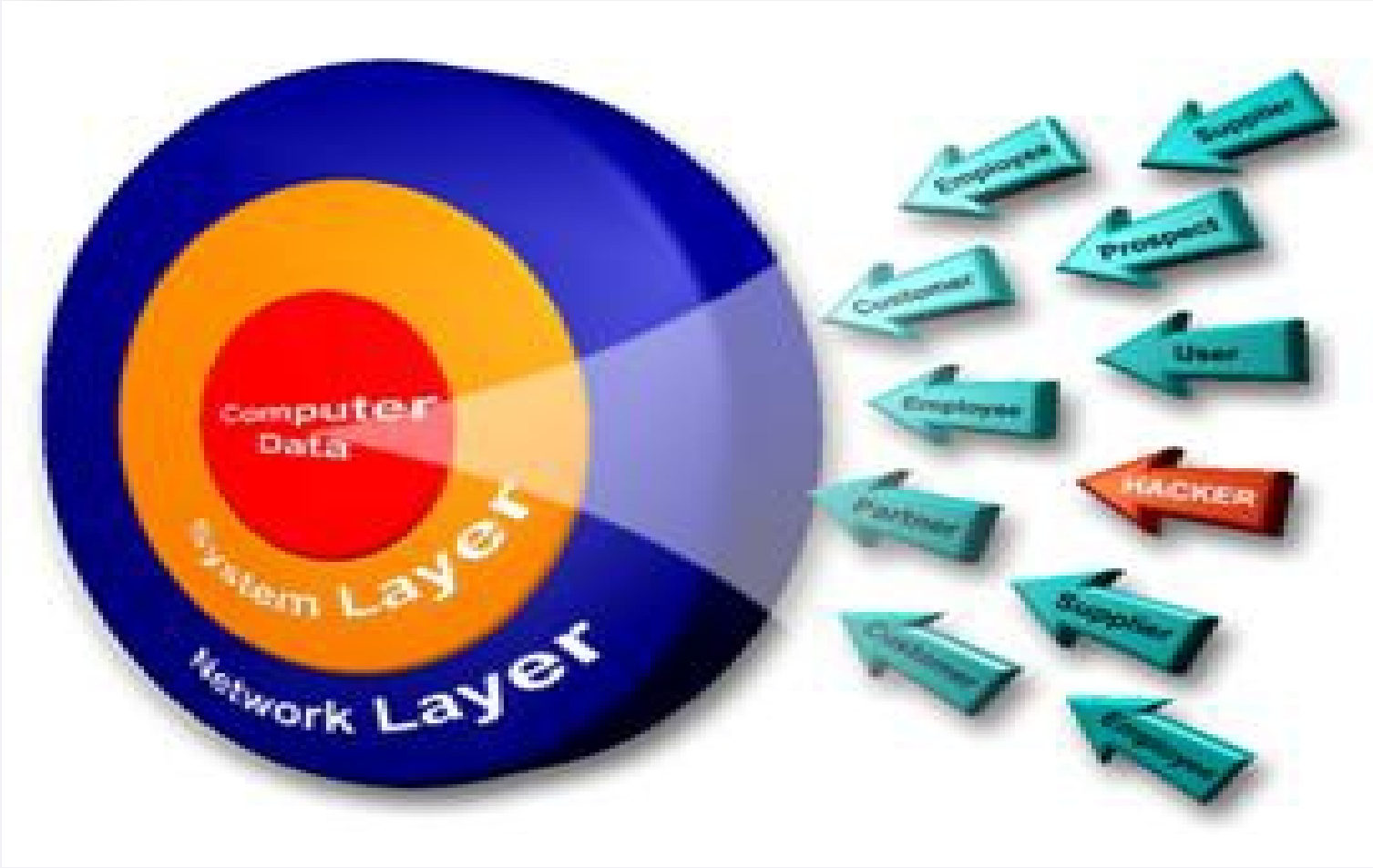
OpenSourceDay 2013

Le metodologie adottate hanno il comune obiettivo di fornire una conoscenza dettagliata sullo stato di sicurezza dei sistemi informatici presi in esame e permettono di:

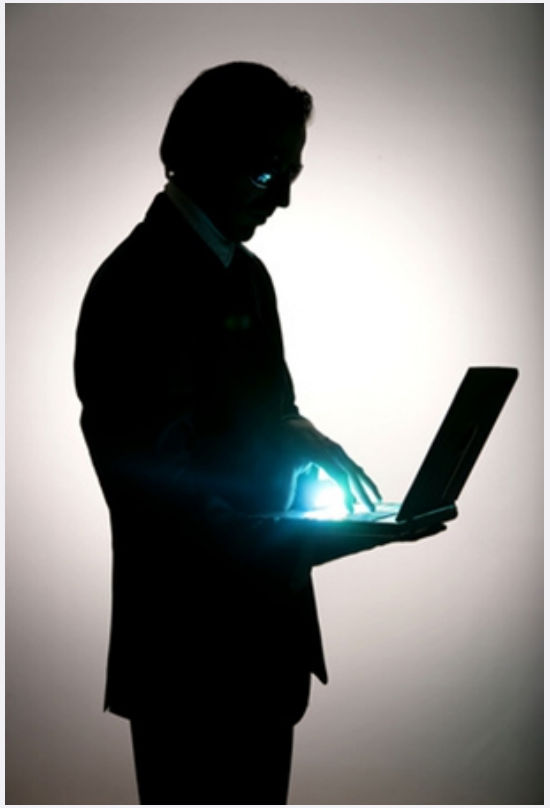
verificare che non sia possibile ottenere accessi non autorizzati a sistemi ed informazioni;

valutare se, per un utente con privilegi minimi, sia possibile accedere ad informazioni per le quali non ha l'autorizzazione necessaria;

verificare che un determinato software non permetta, ad un malintenzionato, di ottenere accessi.

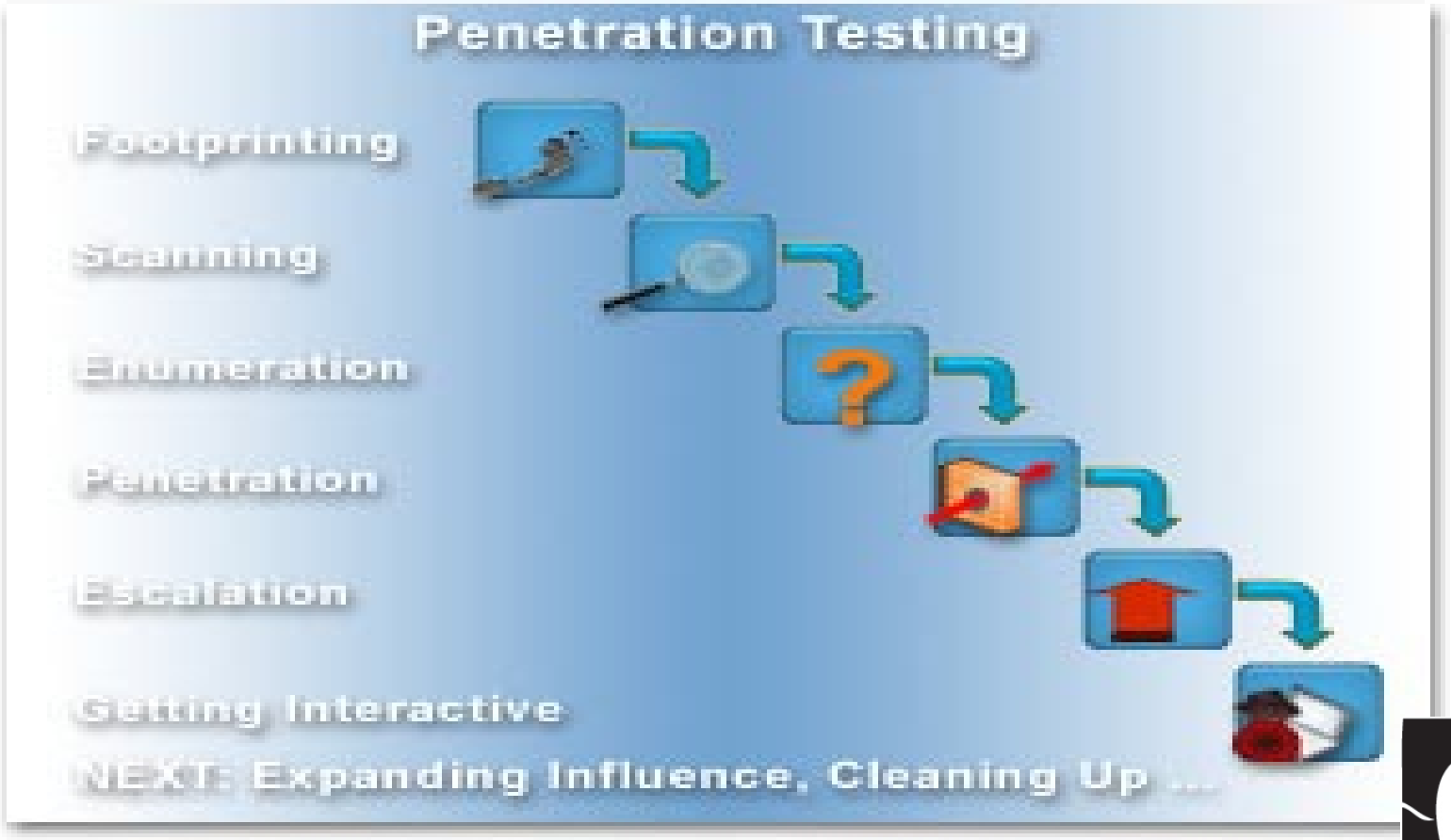

Computer Data
System Layer
Network Layer
Prospect
User
Employee
HACKER
Partner
Supplier

L'analisi viene svolta a fronte di un accordo commerciale/tecnico. Chi svolge questa attività è chiamato penetration tester o auditor e oggi anche con il più moderno nome ethical hacker, visto che si tenta di aggredire il sistema con le stesse logiche utilizzate da un hacker.



Possiamo riassumere l’intera attività di penetration testing in sei fasi principali:

- Information Gathering;
- Vulnerability Assessment;
- Exploitation;
- Privilege Escalation;
- Maintaining Access;
- Reporting;


Penetration Testing
Footprinting
Scanning
Enumeration
Penetration
Escalation
Getting Interactive
NEXT: Expanding Influence, Cleaning Up ...

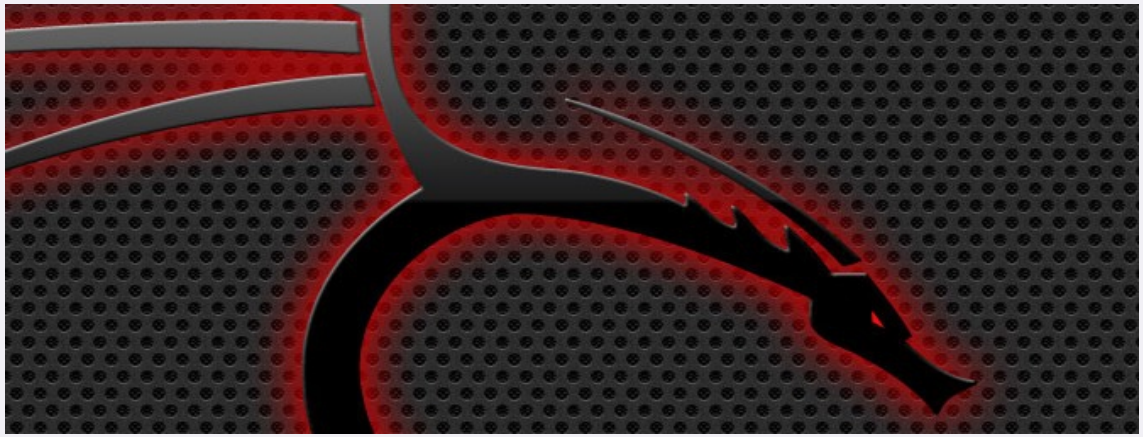
Information:google whois www

Service Enum.: vpn snmp port scan.dns

Penetration SQL

Maintaining Access:Trojans

House Keeping: cleaning up - rootkits



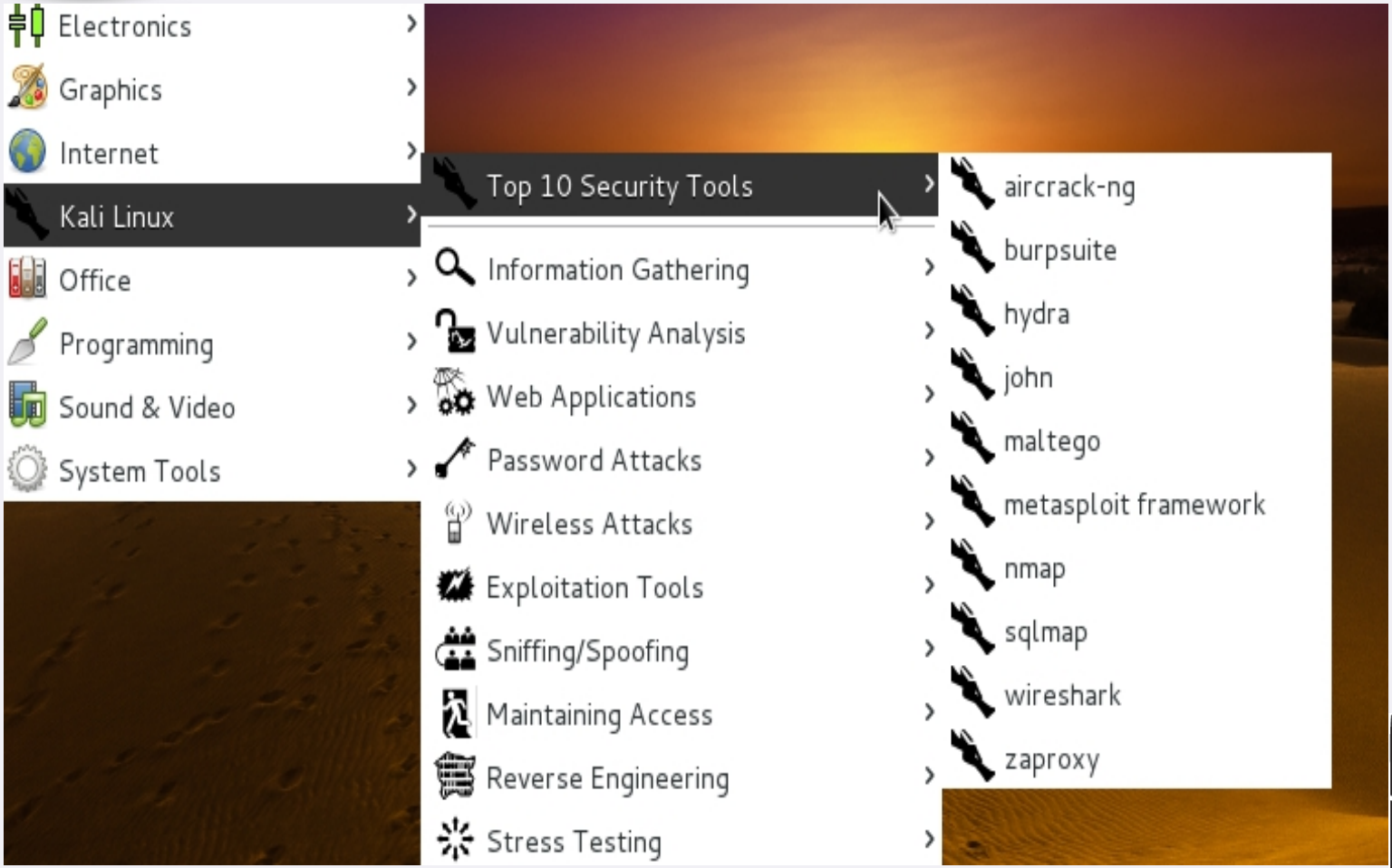
Google dork

Google ha una sua sintassi con delle regole precise. Tale sintassi permette di sfruttare al meglio le query. Tuttavia anche la scelta di parole chiave deve essere mirata ed il meno generica possibile. Google ha un singolare comportamento con le parole chiave: se infatti queste vengono ripetute più volte, il risultato della query cambia, e si hanno molti più risultati rispetto al singolo inserimento.

intitle: Trova le pagine contenenti nel proprio titolo la parola chiave specificata. Esempio:intitle:xhtml

allintitle: Restituisce le pagine che contengono nel titolo tutte le parole specificate. Esempio:allintitle:xhtml

Index of /admin intitle:"Index of etc/shadow


Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
aircrack-ng
burpsuite
hydra
john
maltego
metasploit framework
nmap
sqlmap
wireshark
zaproxy

Tool

Aircrack-ng – For wireless Cracking

Burpsuite – For Web Applications Pentesting

Hydra – For online Brute-Forcing of Passwords

John – For offline Password Cracking

Maltego – For Intelligence Gathering

Metasploit Framework – For Exploitation

Nmap – For Network Scanning

Owasp-zap - For finding vulnerabilities in web applications

Sqlmap – For exploiting SQL injection Vulnerabilities

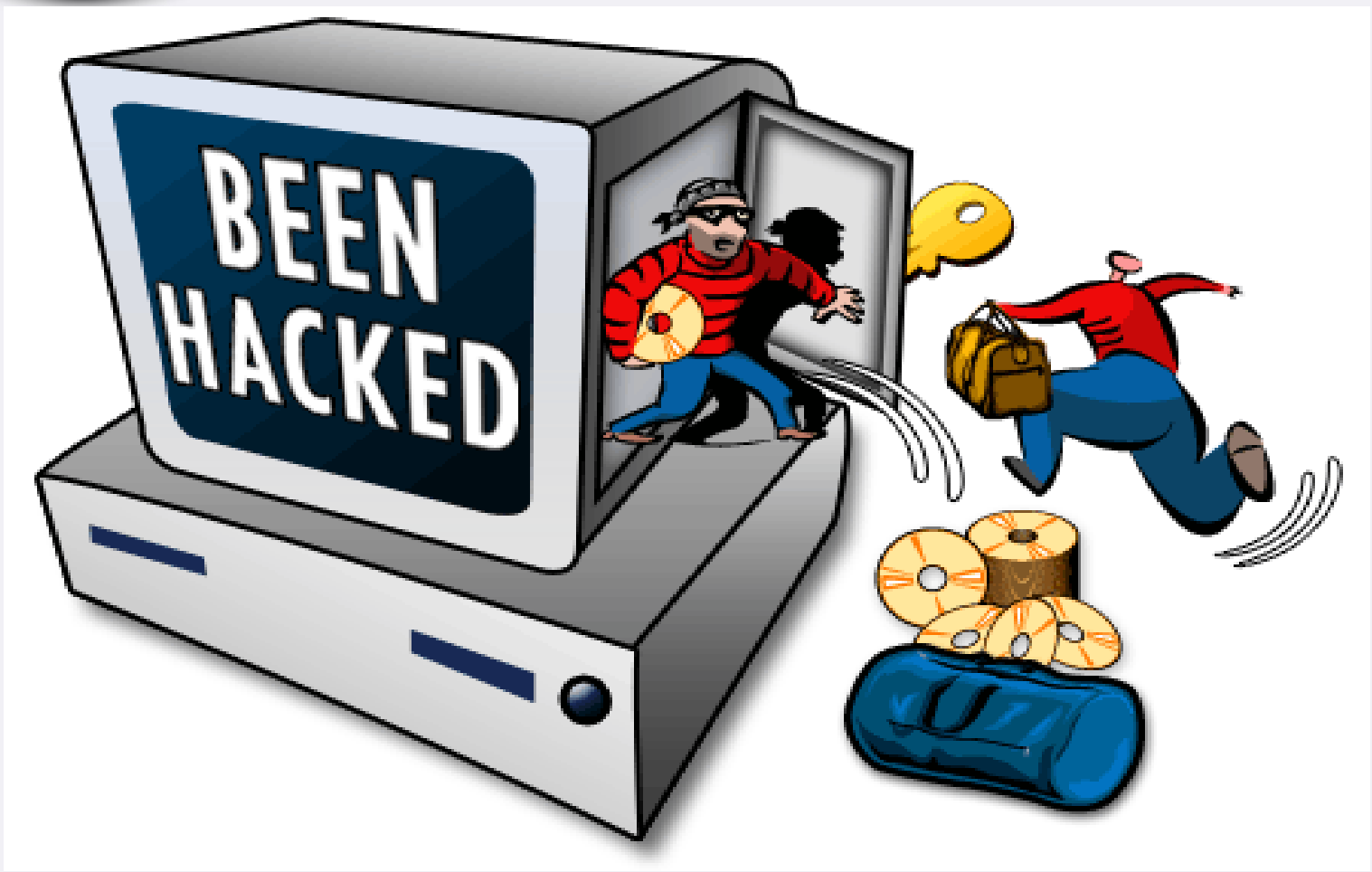
Wireshark – Network Protocol Analyzer


Applications
Places
Thu Mar 14, 6:59 AM
root
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
CMS Identification
Database Exploitation
IDS/IPS Identification
Web Application Fuzzers
Web Application Proxies
Web Crawlers
Web Vulnerability Scanners
burpsuite
cadaver
davtest
deblaze
fimap
grabber
joomscan
nikto
padbuster
proxystrike
skipfish
sqlmap
vega
w3af
wapiti
webscarab
webshag-cli
webshag-gui
websploit
whatweb
wpscan
xsser
zaproxy

Attacchi più frequenti

Injection Cross-site scripting(XSS) Verifica credenziali

Security Misconfiguration..quali filtri?..lasciamo il default.....è più facile comprare una scatola che gestire un processo di analisi e sviluppo...si deve accertare che gli input da parte dell'utente al browser dell'applicazione sia controllato attraverso validazione degli input prima di essere inviati alle pagine di output.


BEEN
HACKED

Pochissimi sono i veri Progetti di Sicurezza IT crittografia,Autenticazione,...

Spesso si vede la“Messa in Sicurezza” di un Sistema IT tramite “Cerotti”si sente spesso..se il sistema fosse stato progettato e implementato bene fin dall'inizio non avrebbe bisogno di cerotti che hanno funzionalità temporanea

Revisionare il codice è il modo più efficace di verificare se un'applicazione è sicura.I test possono solo verificare che un'altra applicazione non è sicura.

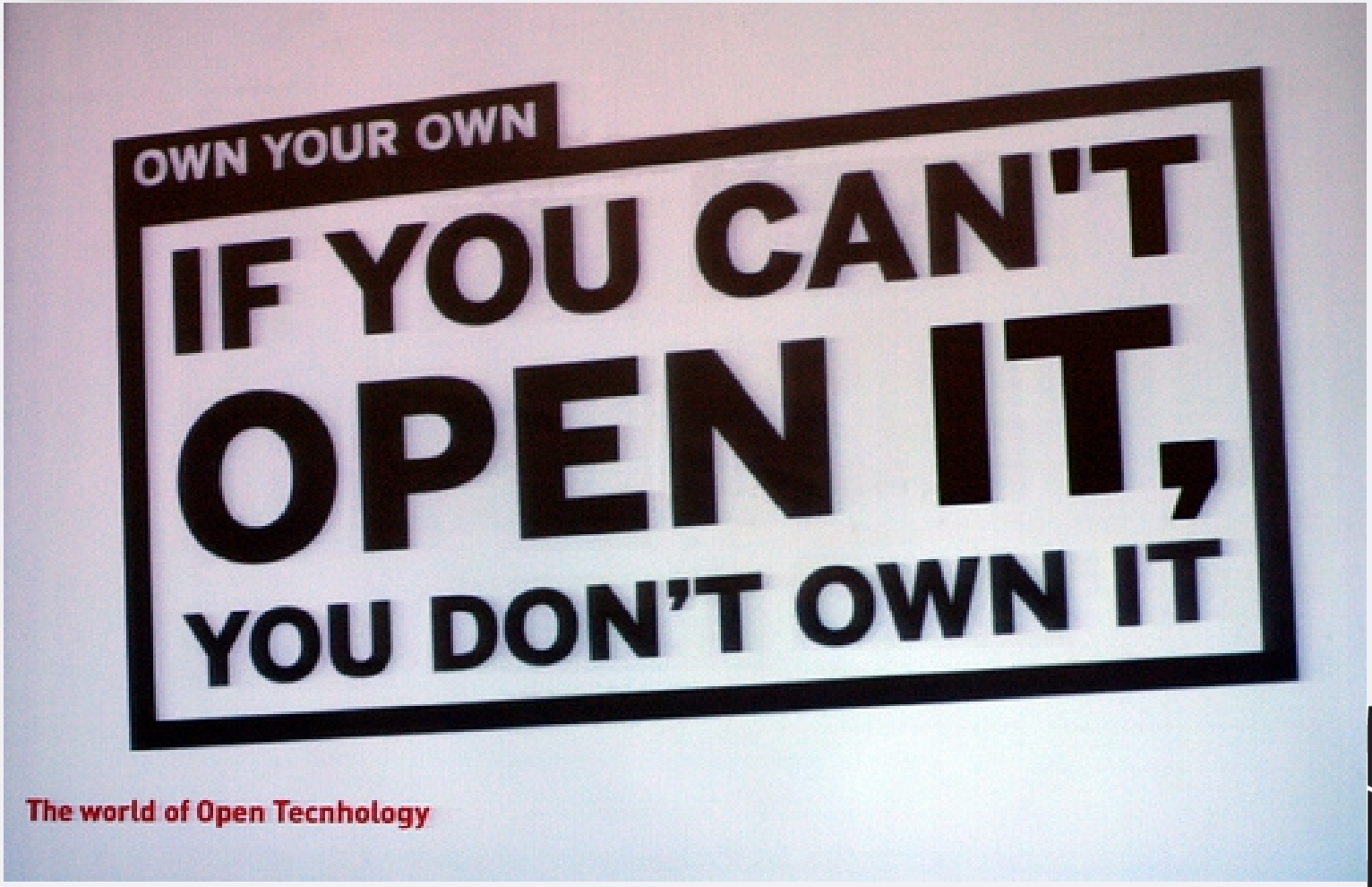
Avere un semplice firewall come molti di voi avranno, sia per default sui router o proprio in una macchina dedicata, alza notevolmente il livello di sicurezza all'interno di qualsiasi rete aziendale lan, ma vi informo che non vi è nulla che con il semplice acquisto garantisca la sicurezza della vostra infrastruttura. Cercare di fermare un ladro che ormai è entrato in casa è troppo tardi, dovremmo fermarlo a prima che entri.

Le politiche adottate in una qualsiasi rete si fonda su due variabili x e y e una costante k.Se assegniamo x=libertà e y=sicurezza otteniamo la relativa formula in cui LIBERTA' x SICUREZZA = K più diamo libertà alla lan e quindi ai membri che ne fanno parte e meno è alto lo standard di sicurezza.

- Rimozione account/dati di test prima dei passaggi in produzione
- Separazione degli ambienti di sviluppo e produzione in termini sistemistici e di personali
- Uso di tecniche di programmazione sicura
- La sicurezza richiede che non siano presenti funzionalità non richieste
- Approccio del minimo privilegio Sicurezza,qualità e progetti Sicurezza sempre valutata da capo e su tutto.


Applications
Places
Thu Mar 14, 7:04 AM
root
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
Android Tools
Arduino Tools
android-sdk
apktool
baksmali
dex2jar
smali

OpenSourceDay 2013



OpenSourceDay 2013

Le piattaforme sono gratis

Tempo, risorse, studio: no

...grazie per la vostra attenzione!