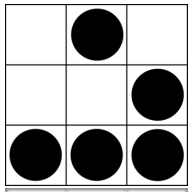


Sicurezza Informatica:

Hacker, Aziende, Rischi e Strumenti.

Come districarsi in mezzo a tutto questo?

Alessio L.R. Pennasilico

mayhem@alba.st

twitter: mayhemspp

FaceBook: alessio.pennasilico

27 Aprile 2011

$ whois mayhem

Security Evangelist @ Alba st

AIS Group Accord ATTUA PROGECO

Progetti:

CrISTAL, Hacker's Profiling Project, Recursiva.org

Board of Directors:

AIP Associazione Informatici Professionisti

AIPSI Associazione Italiana Professionisti Sicurezza Informatica

ILS Italian Linux Society

CLUSIT

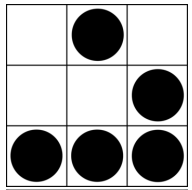
LUGVR Linux Users Group Verona

OPSI Osservatorio Permanente Sicurezza Informatica

Metro Olografix, OpenBeer, Sikurezza.org, Spippolatori.com

Agenda

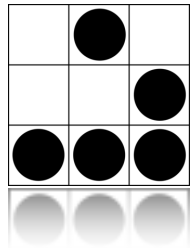
- ✓ Cosa è un hacker
- ✓ La cultura hacker
- ✓ Hacker in azienda
- ✓ Cosa si aspetta una azienda da voi?
- ✓ Penetration test



Hacker

Video: Marco 1.0

Jargon file

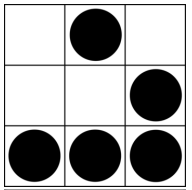


hacker: n.

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

The Hacker Foundation

The Hacker Foundation connects independent technology projects with the financial, managerial and legal resources necessary to make their projects a reality.



Alba S.T.

Di cosa ci occupiamo?

Gestione dell'infrastruttura:

Switching, Routing, Firewalling, Bridging, Wireless

Servizi a valore aggiunto:

VoIP, Monitoring, Consulenza, Security

Chi lavora per noi?

Persone giovani, dinamiche, fantasiose,

assetate di conoscenza.

Chi crede che nessun problema sia irrisolvibile,

che anche l'eleganza di una soluzione sia importante.

Chi non lavora per noi?

tanto fa lo stesso!

funziona anche cosi'!

si, in effetti si poteva fare meglio…

ho sempre fatto così ed ha sempre funzionato...

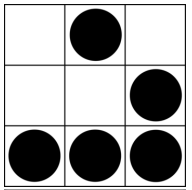
OpenSource

Sviluppiamo software con licenza GPL

Otteniamo visibilità

Otteniamo supporto dalla comunità

Non perdiamo clienti, li acquisiamo



Presentarsi ad un'azienda

Mittente

diavoletta76@hotmail.com

tenerello82@yahoo.com

lalloelalla@libero.it

maraiadesfa@tin.it

Presentazione

La mail con allegato il CV deve contenere un testo formale di accompagnamento al CV.

Allegati

1 MB è la dimensione massima di file permesso.

Un CV di 8 MB denota scarso rispetto e conoscenza di Internet e dell'uso dell'e-mail.

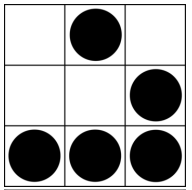
Curriculum Vitae

Le grandi aziende prediligono l'utilizzo del modello europeo

http://www.lavoro.gov.it/Lavoro/Europalavoro/SezioneCittadini/Orientarsi/EuropassCurriculumVitae/

Presentarsi

L’abito fa il monaco.



Competenza

Cosa fa l'azienda per me?

Ci interessa che i nostri tecnici siano competenti.

Formarli è nel nostro interesse!

Maggior soddisfazione, minor turn-over.

Corsi tecnici di formazione e di aggiornamento.

Laboratori di test e ricerca interni.

Certificazioni Vendor

Competenze specifiche per prodotto

Ready2GO

Visibilità per l'azienda

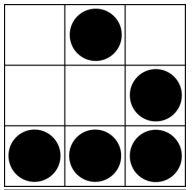
Sconti per l'azienda

Certificazioni independent

Più articolate, più generiche

Prestigiose per il possessore

Non immediatamente spendibili



Patrimonio dell'umanità

Il mercato tradizionale

Attribuisce il valore alle merci

La ricchezza si misura dalla capienza del magazzino

L'obiettivo è la produzione di un oggetto

Il mercato dei servizi

Sono le competenze ad avere valore

Sono le informazioni a costituire ricchezza

L'obiettivo è avere le idee che ci caratterizzano

Il patrimonio di molte aziende si basa

sulle loro ricerche

sulle loro informazioni

sui dati che possiedono

Cosa ha valore?

Quello che ho prodotto?

Quello che posso produrre?

Le mie idee?

Il mio modo di lavorare?

Seneca

Le idee migliori sono patrimonio dell'umanità

64 DC

Jonas Salk

Scopre il vaccino antipolio

La regala all'umanità

Albert Bruce Sabin perfeziona il vaccino

Riconosce i meriti di Salk, regala il vaccino all'umanità

La ricerca scientifica

Il progresso della ricerca scientifica

è largamente basato sul lavoro fatto

precedentemente

da qualcun altro

Le opere d'arte

Quante opere d'arte sono il frutto di un percorso della cultura del genere umano?

Quante opere non sarebbero potute esistere?

Iliade/Odissea - Eneide - Divina Commedia

Il diritto d'autore

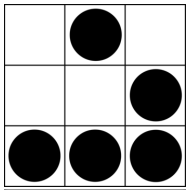
Il diritto naturale d'autore nasce nei primi anni del 1700 in Inghilterra.

In Italia, il primo riconoscimento di tale tipo di diritto si ha intorno al 1800, seguito poi da un testo unico nel 1882, sostituito nel 1925 dalla Legge Rocco e poi, nel 1941, dalla Legge sul Diritto 'Autore(L.d.A.), che è ancora il testo normativo di riferimento.

Sono seguite nel tempo molte modifiche.

Responsabilità

Voglio davvero essere io ad impedire alla razza umana di progredire?



Rischi

Analisi del rischio

Probabilità di un evento

Costi di un incidente (lavoro, immagine, etc)

Costi per prevenirlo

Valutare l'attacker

Non tutti gli attacchi hanno

la stessa probabilità di essere efficaci.

A seconda del "da cosa difendersi"

cambia il "come difendersi" ed i relativi costi

Script kiddies

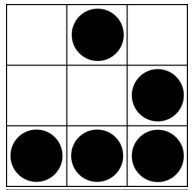
Difendersi da minacce standard, da programmi automatici, richiede programmazione, metodo e costanza.

Applicare le patch, cambiare le configurazioni di default, utilizzare password non banali spesso si dimostra sufficiente.

Black Hat

Difendersi da un attaccante motivato e probabilmente pagato richiede misure di sicurezza più profonde e policy più rigorose.

Il tentativo di attacco potrebbe, infatti, utilizzare strumenti ad-hoc e protrarsi per lungo tempo



Persone

Persone vs. Tecnologia

Installare un antivirus è necessario.

Si tratta di uno strumento automatico che ferma codice malevolo conosciuto.

Prima o poi qualcosa di indesiderato passerà:

per questo devo insegnare a non cliccare su ogni allegato!

Social Engineering

Parlare con le persone è spesso il metodo più veloce e redditizio per ottenere informazioni.

Pretendere di essere qualcun altro, chiedere dati a cui non si è autorizzati ad accedere è spesso banale.

Formazione

Formare, istruire, spiegare è l'unico strumento efficace per innalzare il livello di sicurezza attraverso il creare consapevolezza negli utilizzatori.

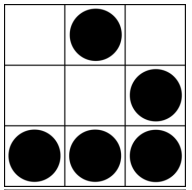
In-formare è indispensabile per completare le misure tecnologiche adottate.

The USB case

Un'azienda commissiona un PenTest.

Gli attaccanti spargono chiavette contenenti malware scritto appositamente nei dintorni dell'azienda.

I dati degli impiegati iniziano subito ad arrivare.



Tecniche di Attacco

Vulnerability Assessment

Il primo passo di un pen-test è creare una mappa degli host e dei device che compongono la rete, dei servizi pubblicati e delle loro possibili debolezze; viene definito Vulnerability Assessment.

nmap -h

* -sS TCP SYN stealth port scan (default if privileged (root))

  -sT TCP connect() port scan (default for unprivileged users)

* -sU UDP port scan

  -sP ping scan (Find any reachable machines)

* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)

  -sV Version scan probes open ports determining service & app names/versions

Some Common Options (none are required, most can be combined):

* -O Use TCP/IP fingerprinting to guess remote operating system

  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'

  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)

  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy

* -S <your_IP>/-e <devicename> Specify source address or network interface

Perchè diverse tecniche?

- ✓ tentare di non essere rilevati da un eventuale IDS
- ✓ tentare di "imbrogliare" un eventuale firewall
- ✓ tentare di sfruttare cattive implementazioni dello stack TCP/IP o del servizio per ottenere maggiori informazioni

nmap -sT

Esegue un 3way handshake completo per ogni porta da verificare.

E' il metodo di default dell'utente senza privilegi di root, poiché utilizza la connect() di sistema.

nmap -sS

SYN scan

Invia solamente il primo pacchetto con SYN=1, senza mai spedire il pacchetto con SYN=1 ed ACK=1.

E' necessario possedere i privilegi amministrativi per utilizzarlo.

nmap -sF

FIN scan

E' necessario possedere i privilegi di root per utilizzarlo.

Invia un pacchetto anomalo, con FIN=1, e resta in attesa di una risposta.

nmap -sN & -sX

E' necessario possedere i privilegi di root per poterli utilizzare. Entrambi generano pacchetti “inesistenti”.

Null scan invia un pacchetto con tutte le flag impostate a 0.

Xmas tree scan invia un pacchetto con le flag FIN, URG e PUSH impostate ad 1.

Tipo di servizi

Dopo avere scoperto quali porte sono aperte vogliamo determinare quali servizi rispondono su quelle porte, quale versione del servizio viene utilizzata e quali funzionalità sono disponibili.

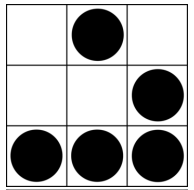
Ricerca Vulnerabilità

Dovremmo cercare delle informazioni relative ad eventuali bug o misconfiguration dei servizi trovati.

La maggior parte del lavoro, rispetto a servizi standard, può essere affidata ad appositi programmi.

Penetration Test

A partire dai dati raccolti durante il vulnerability assessment, attraverso ulteriori test, molto più complessi ed invasivi, dovremo scoprire le reali debolezze della rete in esame.



Hackers Approach

Diverso approccio

Effettuati questi ed altri test attraverso Internet potremmo considerare il test concluso.

Un elenco di server aggiornati e ben configurati potrebbe indurci a dire “la vostra rete per ora e' sicura”.

Altre tecniche

Un buon pen-tester non si ferma ai primi risultati, cerca una strada "alternativa".

Ad esempio verificare accessi wireless, dial-up o la possibilità di ottenere informazioni dagli utenti.

kismet

Kismet è uno sniffer orientato a rilevare reti wireless e collezionare i dati necessari per forzare l'eventuale chiave WEP o constatare la presenza di WPA.

Aircrack-ng

Individuata una rete su cui transita traffico criptato, sarà possibile utilizzare aircrack per trovare la corretta chiave WEP/WPA, che ci permetterà di accedere alla rete wireless analizzata.

Accessi Dial-up

Spesso le moderne reti aziendali permettono comunque degli accessi dial-up, per consentire connessioni remote ai propri dipendenti.

Apparati “pirata”

Non è raro il caso di dipendenti che collegano al proprio PC aziendale, all'insaputa dell'ufficio IT, modem che permettono un collegamento dall'esterno, per garantirsi un accesso da casa.

Lo stesso avviene con gli access-point.

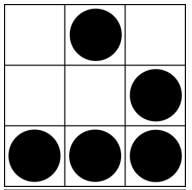
Thinking out of the box

Banca commissiona un PenTest.

Il Web banking risulta sicuro: normalizza l'input.

Bonifico cartaceo: campo note contenente javascript

Applicazione compromessa!



Conclusioni

Video: I signori della truffa

Le aziende

Vogliono persone motivate e brillanti

Danno peso alle certificazioni ed ai titoli

La cultura della ricerca e della condivisione può creare business nel nostro mercato

PenTest

La loro riuscita dipende dalle persone

Gli strumenti possono essere solo un aiuto

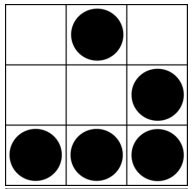
Un approccio "hacker" ne assicura la completezza

Web-O-grafia

http://catb.org/jargon/html/index.html
http://www.hackerfoundation.org/
http://www.schneier.com/crypto-gram-0606.html#6

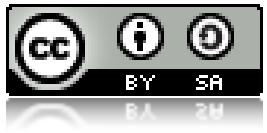
http://www.packetstormsecurity.org
http://www.securityfocus.com
http://www.sikurezza.org

$ google && apropos && man :)



Grazie per l'attenzione!

Domande?



Alessio L.R. Pennasilico

mayhem@alba.st

twitter: mayhemspp

FaceBook: alessio.pennasilico

27 Aprile 2011