

Hacker jeopardy

birra @ esc2k07

by

naif - vecna - ascii - zen - mayem

+

24 latte di birra da 500ml

Regole

- 3 squadre con beep di prenotazione risposta
- Domande a risposta multipla (il 90% hanno una sola risposta valida, alcune più d'una)
- Chi indovina la risposta giusta beve 1 bicchiere di birra alla goccia
- Le squadre hanno un punteggio
- Le decisioni sui giudizi di chi ha risposto prima o giusto/sbagliato sono inappellabili

come funziona naptha ?

- E' un synflood asincrono
- E' un synflood sincrono
- E' un attacco UDP a moltiplicazione (stile smurf, ma diverso)
- Sfrutta la frammentazione
- Fa una full connect

cosa fa holyshit.c ?

- E' una race condition sul filesystem
- E' un exploit per solaris 10
- E' un rootkit per process hiding
- E' un trojan per forgiare le chiavi di sessione ssh prestabilite

qual'e' la legge italiana sul cybercrime ?

- la 615/99
- l'articolato Tanga
- la 547/93
- la 615 ter

ultima versione di NFS ?

- 2
- 3
- 4
- 5
- 5.5

quale' il codice di un NOP ?

- 0x41
- 0x90
- 0xFF
- 0x00

come si chiama il file di passwd di VMS ?

- passwd
- sysuaf.dat
- master.secret
- \$QSECOFR.DAT

KHS9NE ?

- codename processori sparc x86
- il primo gruppo di defacer (anni 80!)
- password di shimomura
- accesso di numero verde per compuserve

cos'ha lo stack dopo una chiamata a funzione ?

- return pointer
- frame pointer, parametri, variabili locali
- return pointer, frame pointer, parametri
- parametri, return pointer, frame pointer

chi ha fatto l'unico deface a securityfocus ?

- Sidewinder
- il gruppo TESO
- Mayhem (sobrio!)
- Fluffy bunny

Porta dei klogin ?

- 515
- 562
- 543
- 514
- e' stato ormai dismesso

half width unicode encoding

- %uFF27
- --
- %27
- %2527
- %u0027
- /con/con

il deCSS com'è stato pubblicato ?

- in un numero primo
- da VeriSign
- tramite rumore di fondo di un mp3
- steganografato in HTML
- cantato da Richard Stallman
- dipinto su una pergamena

qual'e' la lunghezza di una NUA

- 9
- arbitraria
- assegnata dal server
- 5+4

a che numero di BFi siamo arrivati ?

- 12
- BFi e' morta!
- 16
- 14

La password di default di DBSNMP

- tiger
- ABCDEFGHILMNOPQRSTUVWXYZ
- dbsnmp
- scott
- CHANGE_ON_INSTALL

Cos'è il Birthday Attack ?

- Un attacco a persone.linux.it
- Una torta di compleanno avvelenata
- Un paradosso statistico
- Una tipologia di DDoS
- L'attacco ai Root Server

La GRANT per usare “into outfile”

- outfile
- file_priv
- file
- file_out

cos'è il `net.inet.tcp.blackhole`

- uno stealth scan
- un insulto di EFNNet
- una `sysctl` di freebsd
- una tecnica anti DDoS
- un'estensione di iptables
- una `sysctl` di Linux

Lunghezza del TCP.SEQ

- 16
- 7 (strlen("TCP.SEQ") ?)
- 32
- 8
- dipende dai syn cookies

“cat /etc”, su solaris, cosa fa ?

- ls /etc
- open /etc/etc
- cat /etc/*
- stat /etc/
- invalid argument

STUN

- bypassa il nat
- Nick di Raoul Chiesa
- modalita' d'uso di openvpn
- Nick di Richard Stallman
- alias di stunel
- protocollo di http tunnelling

qual'e' l'ultima release di netbsd

- 4.0-rc1
- 3.1
- 3.0
- 3.4
- 2007 Enterprise

Porta di BGP

- non esiste
- 179
- 197
- dipende dall'implementazione (problemi di interoperabilit  tra Cisco e Juniper)
- quella posteriore

la libresolv implementa

- una libreria per risolvere i problemi
- una libreria grafica
- la libreria di risoluzione DNS
- la libreria di risoluzione IPv6
- la libreria di risoluzione della GNU

L'ultimo DDoS ai Root Server

- un mese fa
- tre mesi fa
- sei mesi fa
- un anno fa
- quattro anni fa
- dieci anni fa

Il DNS pinning/rebinding

- E' un attacco alle libresolv
- E' un attacco di dns poisoning
- E' un metodo di load balancing
- E' un attacco client side
- L'ha inventato kaminsky

Numero di edizione hackmeeting 2007

- 9
- 10
- 11
- l'hackmeeting e' finito nel 2004
- 0x0A

Capitan Crunch ?

- 2700
- 2600
- 2048
- 1999
- CCC

Steve Jobs

- boxava
- crackava password
- nuotava
- giocava a golf
- era un eroe

PDP-11

- Fa funzionare Internet
- Ha sistema operativo MVS
- Ha sistema operativo VMS
- Ci gira Linux
- Ci gira Unix
- Ci gira Multics

Solaris non e' disponibile su:

- x86
- Alpha
- sparc
- ppc
- PA risc

ALEX ALEX

- L'inventore del -j DROP
- -l -f user (su solaris)
- MafiaBoy
- C'e' stato 10 anni fa
- Non e' uno UNIX

Non e' uno UNIX

- IRIX
- IPSO
- SINIX
- IPX
- MINIX
- DARWIN

Cos'e' IPX ?

- Un modello di workstation SUN
- Il protocollo BOOTP
- Il protocollo nativo di VMS
- Il nick di Comer
- Una tecnica 3D FX
- Un modello di firewall Cisco

Il ponte sul logo

- SUN
- CISCO
- IRIX
- IPX
- SPARC 5

Come si fa una richiesta a identd

- PORTA LOCALE:PORTA REMOTA
- USERNAME:PORTA LOCALE
- con un browser
- con gentilezza
- con dig

numero syscall execve

- ||
- non ha numeri, si chiama “execve”
- 0x0A
- -||
- `sizeof(char) * 4`

Non serve pagine web

- `boa`
- `apache`
- `fasthttpd`
- `lighttpd`
- `thttpd`
- `Abyss`

L'header HTTP per fare una richiesta a un proxy in chain

- POSTPROXY
- Next-Host:
- Host:
- Max-Forwards:

Chi ha scritto su phrack?

- buffer
- sgrakkyu
- twiz

come funziona TOR

- agitando una bandoliera rossa
- routing a cipolla
- instradamento per cipolle
- forward multiplo
- instradamento per lamponi
- per magia nera

strace per solaris

- ktrace
- ltrace
- truss
- strace
- dtrace

come si attiva un'interfaccia su cisco

- ifup
- interface up
- enable
- no shutdown

L'op code di “int 3” su x86

- 0xCC
- 0xDD
- 0x90
- 0x69
- 0x666

Quale non e' un OS CISCO ?

- catos
- ios
- pix ios
- linux
- nokia

Cosa vorreste sovrascrivere ?

- %AIP
- %SYSYEM ROOT
- %RET
- %PET
- %COD
- %GCC

E' una SQL injection valida

- ' union show tables; '--
- ' union select name,passwd,null,null '--
- ' union(select(*)) '--
- ' inner join select name,passwd,null '--
- ' && select passwd != NULL

La tipologia di kazaa

- full p2p
- server centrali fissi
- server centrali eletti
- superclient
- mesh network

cosa significa EIGRP

- Exterior Internal Generic Routing Protocol
- Extra Internet Gre Routing Protocol
- External Interface Groaning Route Publically
- Enhanced Interior Gateway Routing Protocol

esiste il “one bit overflow” ?

- si, ma con altri nomi
- no
- e' un HOAX
- e' un modo sbagliato per dire “one byte overflow”
- si, ci hanno bucato sendmail

NX bit

- suid e sgid
- No dump
- Truss file
- Sticky file
- No execute
- No kill process

canary patch

- sshd
- apache
- phpmyadmin
- phpBB
- gcc

n3td3v, e':

- 3 persone, secondo un'analisi semantica
- una mailing list
- un newsgroup
- una syscall di knark
- gobbles

drwxr-x--t

- 10751
- 01551
- 01751
- 04751
- 00751

Google TiSP

- E' un servizio di ricerca per le aziende
- E' un water
- E' un hoax di Google
- E' un servizio di Technological interface Search Protocol

Debian etch ha tolto:

- pidof
- killall
- chgrp (si usa solo chown)
- chgrp (si usa solo chuid)
- pstree
- syslog

nmap

- E' un progetto nato nel 2000
- Implementa una tecnica di Antirez
- E' scritto da Naga & Alor
- linka le libpcap
- linka le libnet

Il nick di kevin mitnick

- nobody
- naif
- phish
- defcon
- condor
- mafiaboy

quale software fa steganalisi ?

- stegoelectric
- stegocrack
- stegdetect
- steguncover
- stegorape
- stegotellmetellme

tcpdump -e

- e' come tcpdump -l
- include le “extended information”
- mostra le excessive collision
- anonimizza il dump
- include l'header ethernet
- non e' piu' implementato

ps aux funziona su:

- Linux
- Mac
- Solaris
- IPSO
- HURD
- Plan9

Silvio Cesare

- scrisse su come patchare i kernel in /dev/mem
- scrisse come modificare una funzione non syscall
- scrisse il patching statico di vmlinux
- scrisse il patching dinamico di init
- Disse “alea iacta est”

Il bridge ethernet

- fa proxy arp
- parla IEEE 802.1d
- parla IEEE 802.1q
- E' stato inventato da Linux
- Non e' supportato da iptables (*)

L'editor “giusto”

- emacs
- vi

Questo quiz

- Rulezza