

2000


:

:

تقرير خاص


أمن الحاسوب والإنترنت

كيف يقتحم العابثون الحواسيب...
وكيف يكشف عنهم
< م. سبيل >

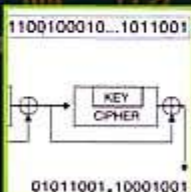


كيف تُؤمن حماية حاسوبية


- 1 جدران الحماية، < م. تشرنوبل >، < م. بيلور >
- 2 شهادات توثيق رقمية، < م. نور >
- 3 صندوق مامون (اللغة البرمجة) جافا، < م. كزايك >



تعمية من أجل الإنترنت
< م. زيمريان >



القضية ضد سن تشريعات
تُفتد تقانة التعمية
< م. ريلست >



1998/2

.1997 cyberviolation

()

()

...

(*)

RAM

(1)

< P.C.>



hacking

الشركة Rt66

.hackers

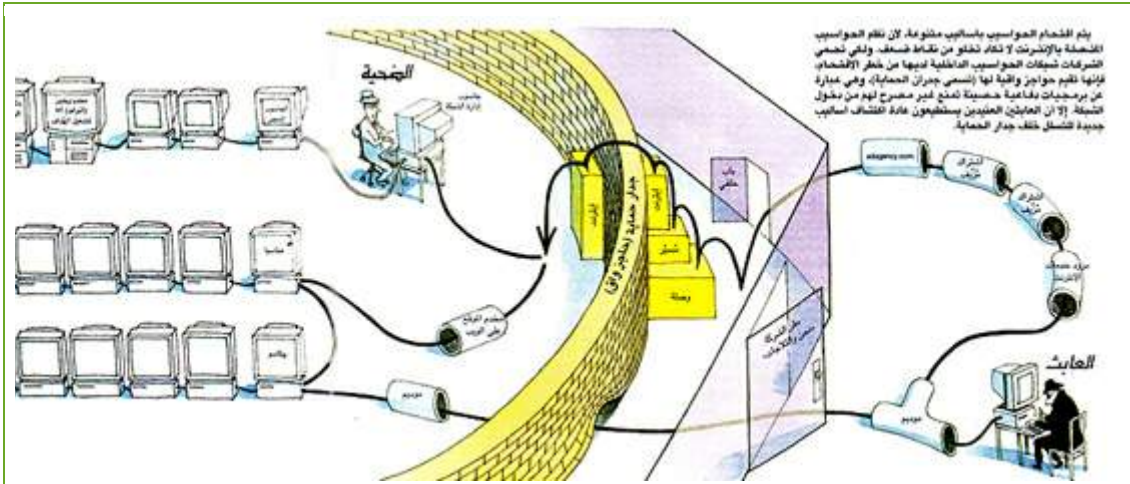
الإنترنت Chat Relay Internet

الراديو CB radio

line-on

Unix

.Wars Star



()

« »

!

"RTFM" :

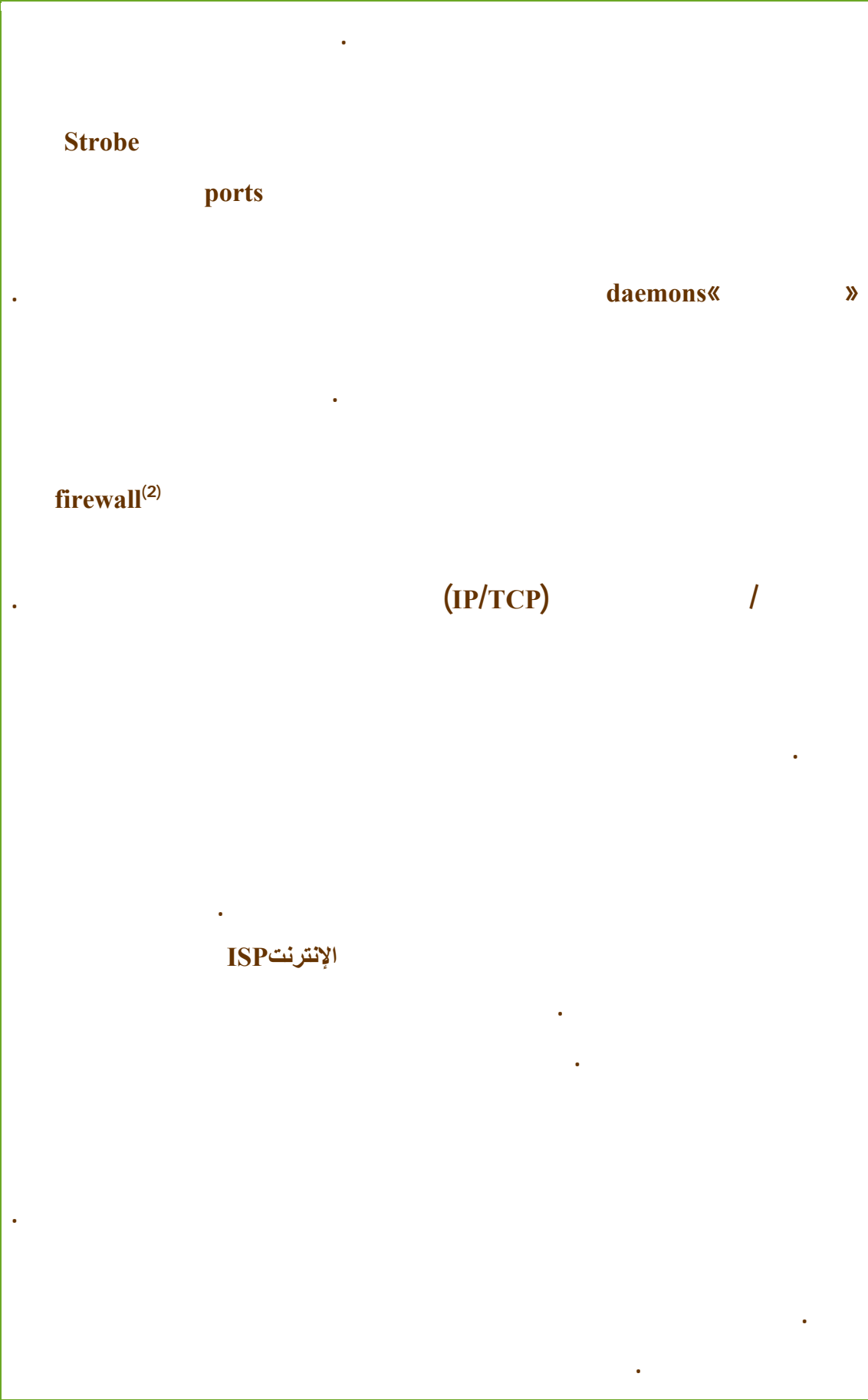
finger « »

ريفرجيروس com.refrigerus

telnet « »

root expn« »

server mail



(3)

.SYN flag synchronize

destination () source

.()

SYN

ACK

SYN

ACK /

.handshake way-three

FIN

ACK

packets FIN premature أوانها FIN

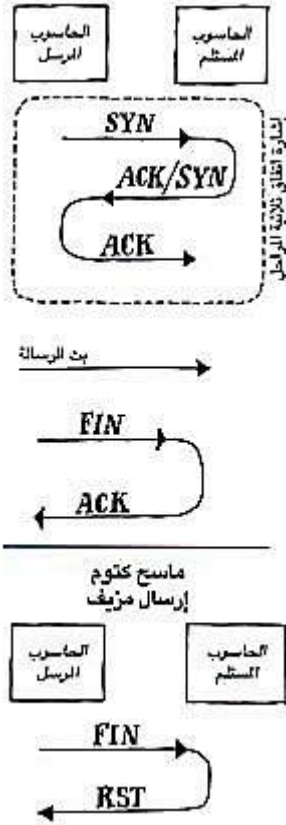
.RST) reset) « »

.logs

يستطيع FIN scanner

).

(.



SYN

.()

ACK

SYN.

FIN

FIN

.(RST (

.

.

.C

.

C

(.

) Linux

.

.

.

) (4)

.(

.

.

.

.

(5)

snapshot

FIN

encrypted

daemon shell-secure

31.659

FIN

EtherPeek

31.659

FIN

()

account

down shut

com.refrigerus whois « »

()

Us R Refrigerators

31.659

! »
crash 31.659

«

corrupt

"""nslookup

program server-name

«nslookup»

50

"""whois

:

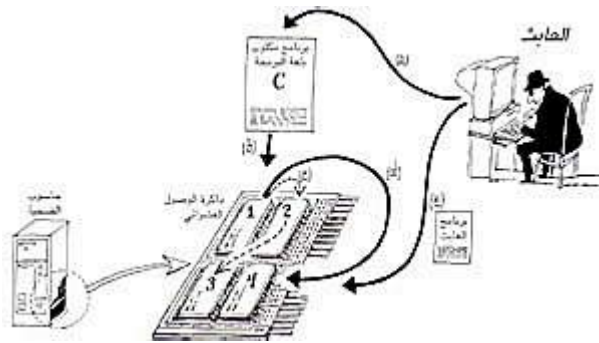
.«

»

com.refrigeratorz

FIN

FIN



buffer

()

overflow

C

(a)

C

1

(b).

(c). 3 2

1

(d). 4
(e)

« »

) ShokDial

»

(

«

2:57

«.6.3

Irix

»

يونيكس Unix

force brute

()

.

.

.

."nancy"

5

shell root

«! »

.

FTP protocol transfer file

« »

.

sniffer

)

.

(

.

."DiEd0gB"

revenge« »

who « »

.

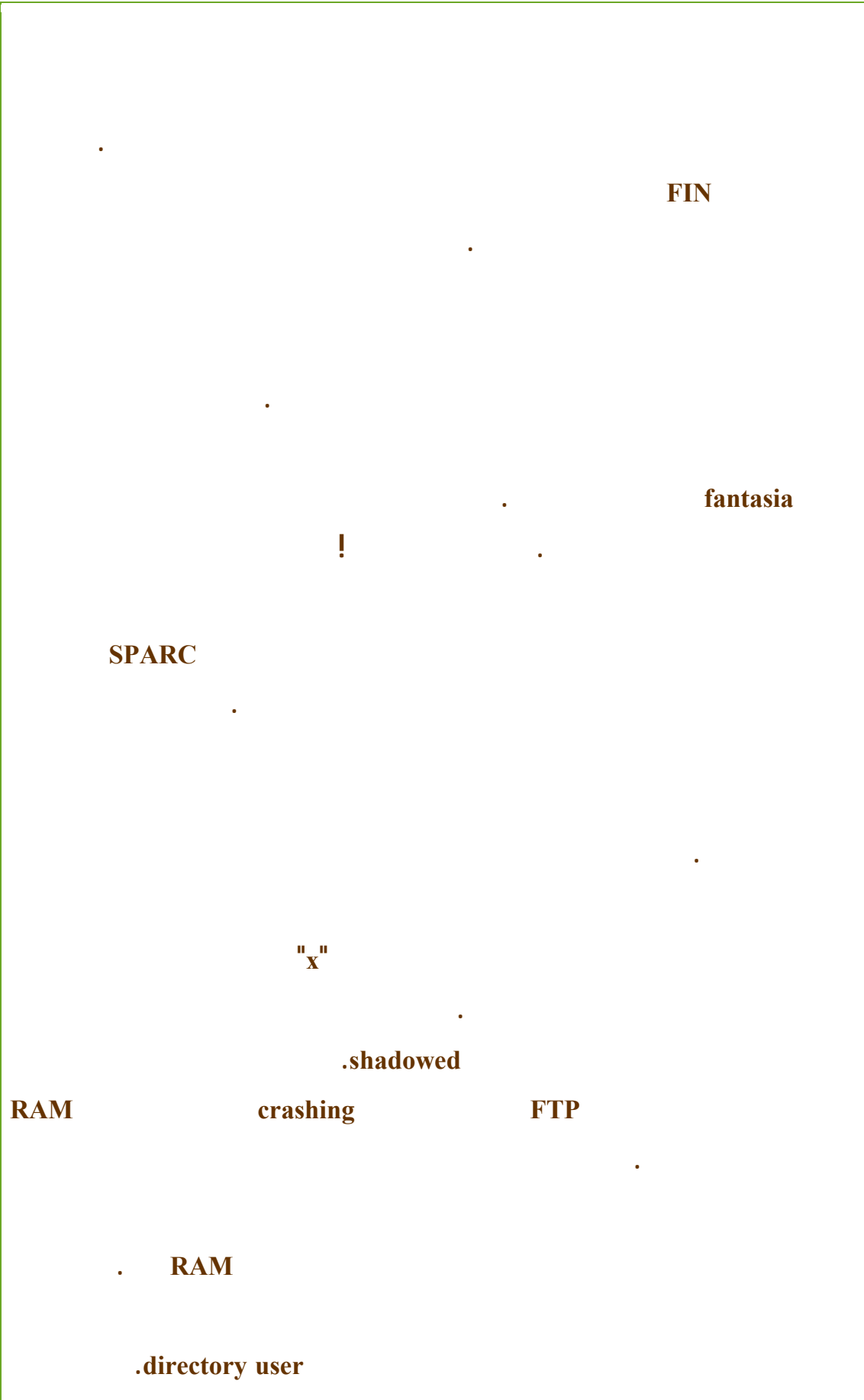
picasso« »

"revenge"

.

.

.



dump core

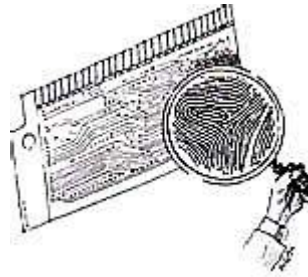
autopsy

.RAM

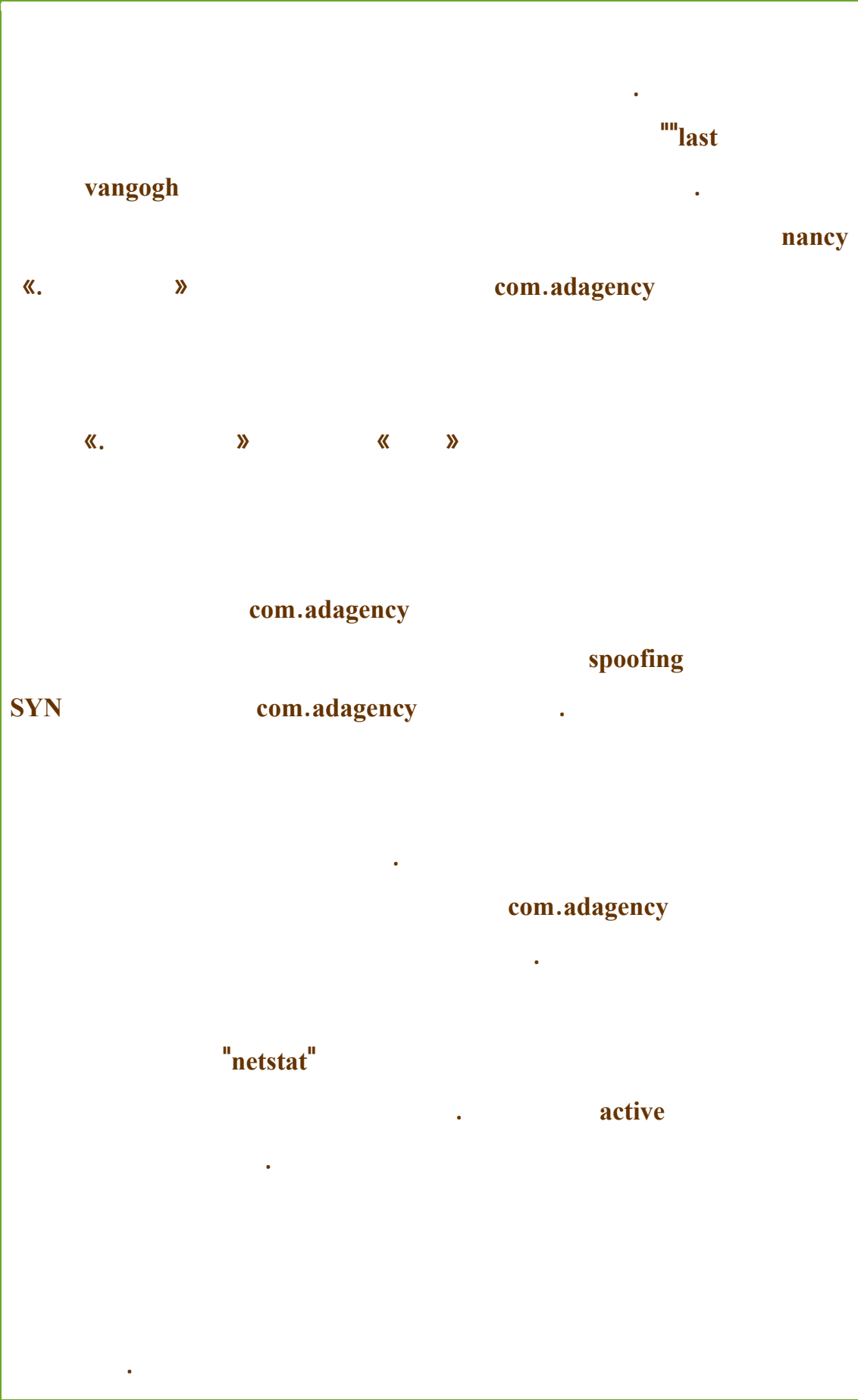
RAM

(buffer)

leak



(6)

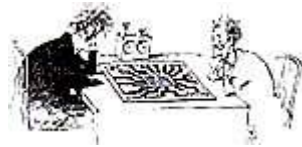


updating

« »

« »

« »



» page home

يُحْمَلُ upload

«

« »

.com.adagency

com.adagency

.

«

»

.

.

.

.

.

.

). .

(.

.

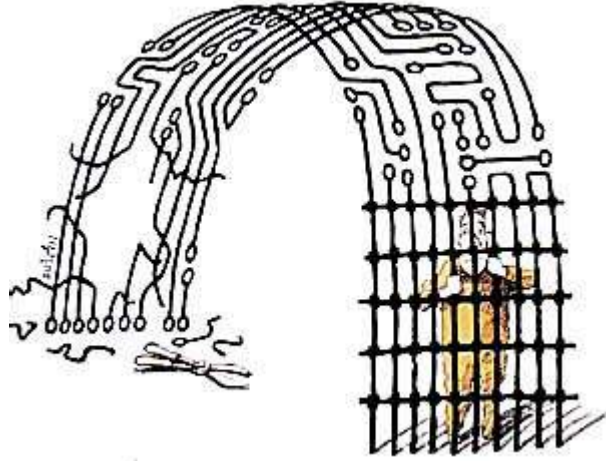
:

laptop

استرجاع retrieve

.«

»



»

«

FBI

culprit

dialer war

!

NT

sight-T

()

computer jail« »

.

.

...

8:17

.

.CNN

.

.

«

»

"telnet"

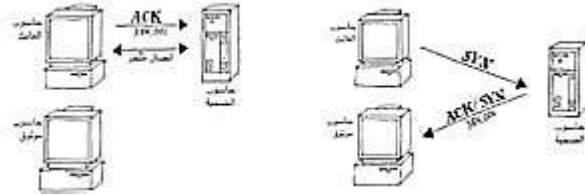
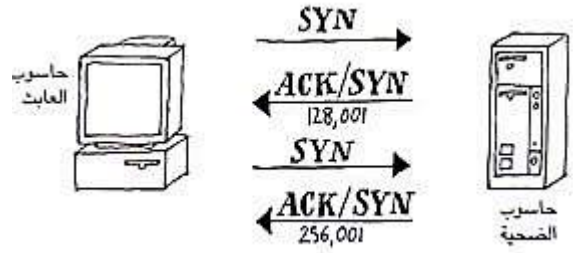
com.adagency

.

.

.

.



ACK / SYN] 50]

.)

. 128000

.()

:

.()

DiEd0gB

.com.adagency

.com.adagency

DiEd0gB

.

.

.

.

.

.

.

megabytes

.

.

(7)

«

»

Carolyn P. Meinel

) : » . 1998 « (

hacker

.(<http://www.happyhacker.org>) wargame
< .J >

مراجع للاستزادة

ESSENTIAL SYSTEM ADMINISTRATION. Second edition. A Eleen Frisch. O'Reilly & Associates, Sebastopol, Calif., 1995.

INTERNET FIREWALLS AND NETWORK SECURITY. Second edition. Chris Hare and Karanjit Siyan. New Riders Publishing, Indianapolis, 1996.

MAXIMUM SECURITY: A HACKER'S GUIDE TO PROTECTING YOUR INTERNET SITE AND NETWORK. Anonymous. Sams Publishing, Indianapolis, 1997.

THE GIANT BLACK BOOK OF COMPUTER VIRUSES. Second edition. Mark Ludwig. American Eagle Publications, Show Low, Ariz., 1998.

Additional information can be obtained at [http://www.geek-](http://www.geek-girl.com/)

[girl.com/](http://www.geek-girl.com/) bugtraq, <http://ntbugtraq.ntadvice.com/> ,

<http://rootshell.com/>, [http://](http://www.infowar.com/)

<http://www.infowar.com/>, <http://www.antonline.com/> and [http://www/](http://www.happyhacker.org)

[happyhacker.org](http://www.happyhacker.org) on the World Wide Web.

Details of EtherPeek and T-sight can be obtained at

<http://www.aggroup.com/> and <http://www.engarde.com/>, respectively.

(*) How Hackers Break In ... and How They Are Caught

scanner (1)

.() (2)

stealth (3)

. compile (4)

cyberbattles (5)

insinuate (6)
plea bargain(7)