

A Step into the Computer Underground

**“By Understanding The Enemy
We Are Better Prepared To Defend Ourselves”**

by Brett Moore



Security-Assessment

.com

- Hackers, Crackers, Phreakers, Black Hats
- Males and Females, All Ages
- Computer Underground
- Warez Pirates
- Warez == Slang For Pirated Software



Security-Assessment

.com

- Internet Gives Worldwide Access To People With Similar Interests
- Credit Cards
- Free Software
- DVD Copies
- Pornography
- MP3 Music Files



Security-Assessment

.com

- Dialup access with modems
- BBS (Bulletin Board Systems)
- Online Handles (Alias)
- Leave Messages And Trade Files
- Free Long Distance Phone Calls



Security-Assessment

.com

- Stolen Credit Cards
- Stolen Calling Card Numbers
- Hacked PBX Systems
- Voice Mail Systems
- Blueboxing
- MF Tones To 'Talk' To The Exchanges



Security-Assessment

.com

- Phone Hackers == Phreaker
- Explored The Phone Systems
- John Drapner (Captain Crunch)
- 1960's, 1970's => 1990's
- 2600 Hertz MF Tone
- KP2 + CC + AC + # + ST



Security-Assessment

.com

- Software Has Been Pirated Since Before The Commodore 64
- Amiga, Mid 1980's
- Warez Scene (Community)
- Software Piracy (Warez Trading)



Security-Assessment

.com

- Multipart Process
- Obtain Software
- Software Cracking
- Software Distribution
- Supplier, Cracker, Distributor



OBTAIN

CRACK

DISTRIBUTE



Security-Assessment

.com

- Phreakers Provided Free Phone Calls
- BBS Sites For Distribution
- HQ's, Group Distribution Sites
- Courier Groups



Security-Assessment

.com

- Not Just Geeky Kids
 - Organised Groups
 - Different Countries
 - Peer Respect And Recognition
 - To Be The Top Group
 - Since Early 1980's
- RAZOR 1911
 - THC
 - TRSI
 - FAIRLIGHT
 - PARADIGM
 - 4-D (NZ)



Security-Assessment

.com

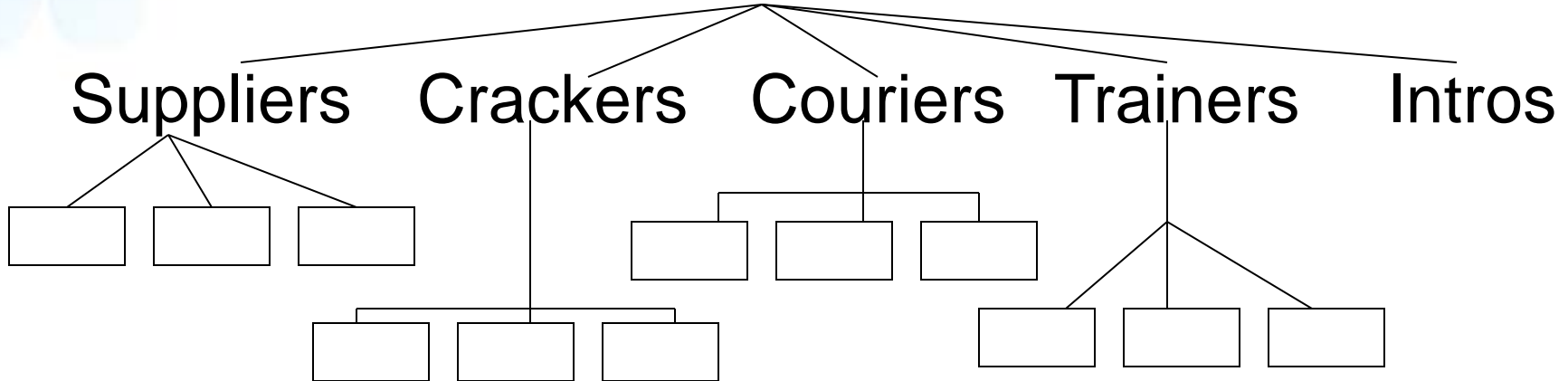
- Internet Savvy
- Replaced BBS's With FTP And Web Sites
- New Groups Formed
- Older Groups Expanded
- Groups Within Groups



Security-Assessment

.com

Group Leaders



Security-Assessment

.com

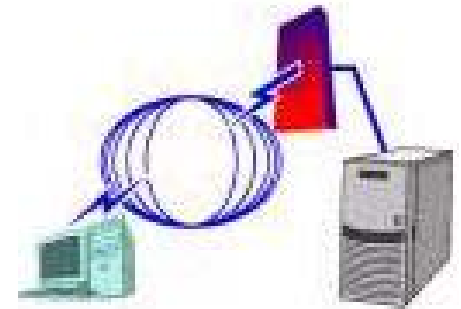
- Latest Technology
- Encrypted High Speed Links
- High Speed Is Expensive
- Hacking Techniques To Steal Bandwidth From Others



Security-Assessment

.com

- Scanners / Site Finders
- Unprotected FTP Sites
- Vulnerable Web Servers
- Distros – Private Distribution
- Pubstros – Public Distribution
- Scanstros – For More Scanning



Security-Assessment

.com

- Exploit Tools Allow Even Novice Hackers To Compromise Systems
- Available On The Internet
- Step By Step Instructions
- Access To More Tools
- “Just Press Go”



Security-Assessment

.com

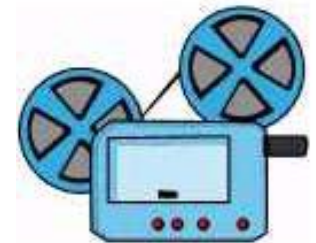
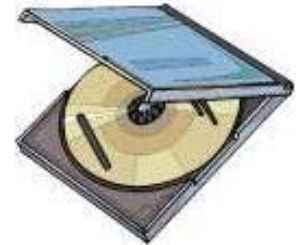
- Unlimited Time Resources
- FXP Transfers
- Automated Scanning
- Constantly Scanning
- Every Internet Connection Will Get Scanned



Security-Assessment

.com

- Not Just Games
- Software Applications
- DVD Movies
- Music MP3's
- Pornographic Images And Videos
- Distribution Process Is The Same



Inbox

- Folder List
- Outlook Today - [Personal Folders]
 - Calendar
 - Contacts
 - Deleted Items (20)**
 - Drafts
 - Inbox**
 - Infected
 - Journal
 - Notes
 - Outbox
 - Sent Items
 - Tasks

From	Subject	Received
Brett Moore	This Is Funny	Thu 13/09/2001 15...

From: Brett Moore **To:** brett@softwarecreations.co.nz
Subject: This Is Funny **Cc:**

jokes.exe (3 KB)

You gotta see this

Security-Assessment

.com

- A Virus Normally Requires Human Action To Spread
- May Already Be Infected Before Definitions Available
- Shutdown Anti Virus And Firewall Programs
- Some Can Auto Execute



Security-Assessment

.com

- Internet Worms Execute And Spread Automatically
- Search For An Infect Thousands Of Computers
- Old Worms Of 2001 Are Still Active
Sadmind, Code Red, Nimda
- Newer Worms
SQL Slammer, Apache Slapper



Security-Assessment

.com

- Hackers Use Virus And Worm Technology
- Virus Creation Kits
- Virus Scanners Are Important
- Employee Education About The Dangers Of Running Attachments



VX Heavens

- [Home](#)
- [News](#)
- [Library](#)
- [Sources](#)
- [Downloads](#)
- [Links](#)
- [Forum](#)

Virus sources

o.rar (o/100%-1.asm ... o/911.asm)	139933
a.rar (a/abdo.asm ... a/azusa.asm)	260776
b.rar (b/b1.asm ... b/byteme.asm)	312761
c.rar (c/c0t.asm ... c/cybtch-b.asm)	407486
d.rar (d/daboys.asm ... d/dwi.asm)	309639
e.rar (e/e1.asm ... e/extasy.asm)	149725
f.rar (f/faces.asm ... f/fumanchu.asm)	93715
g.rar (g/gadost.asm ... g/gv.asm)	107223
h.rar (h/hack-83.asm ... h/hydra8.asm)	141469
i.rar (i/ice1.asm ... i/ivkiller.asm)	159759
j.rar (j/j_1808.asm ... j/justice.asm)	165435
k.rar (k/kbm.asm ... k/kuku.bas)	66469
l.rar (l/lacimehc.asm ... l/lz.zip)	150825
m.rar (m/mad.asm ... m/myvir.asm)	342504
n.rar (n/naktruth.asm ... n/nymphmit.asm)	169323
o.rar (o/occido.asm ... o/ow9.asm)	148746
p.rar (p/pakbrain.asm ... p/pw17.asm)	321138
q.rar (q/qb.bas ... q/queen.pas)	10653
r.rar (r/random.asm ... r/rush_vir.asm)	99008
s.rar (s/s35.asm ... s/syslockm.asm)	315400
t.rar (t/t-1000.asm ... t/typo.asm)	204214



[Help to keep this site alive!](#)

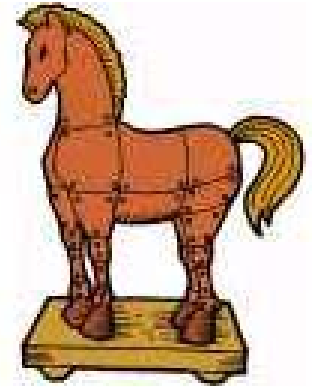
search

F2123752F2123752F2123752
 0732d3070732d3070732d30
 a5e616c2a5e616c2a5e616c
 f4e6c642f4e6c642f4e6c64
 e753d706e753d706e753d70
 f243b3d5f243b3d5f243b3c
 b2455226b2455226b245522
 b70306c5b70306c5b70306c
 42f3230642f3230642f3230
 75c2f2f575c2f2f575c2f2f
 72a482c272a482c272a482c
 F2123752F2123752F212375
 0732d3070732d3070732d30
 a5e616c2a5e616c2a5e616c
 f4e6c642f4e6c642f4e6c64
 e753d706e753d706e753d70
 f243b3d5f243b3d5f243b3c
 b2455226b2455226b245522
 b70306c5b70306c5b70306c
 42f3230642f3230642f3230
 75c2f2f575c2f2f575c2f2f
 72a482c272a482c272a482c
 F2123752F2123752F212375
 0732d3070732d3070732d30
 a5e616c2a5e616c2a5e616c
 f4e6c642f4e6c642f4e6c64

Security-Assessment

.com

- Backdoor Or Trojan Allows Access After A System Is Patched
- Run Commands, View And Edit Files
- Scanning
- Denial Of Service Attacks
- Proxies To Bounce Communications



Security-Assessment

.com

- Edit Web Script Or Create New
- Rootkits, Hard To Detect
- Listening Trojans Can Be Detected
- Netstat, Fport, Personal Firewalls
- Communication Over HTTP, TCP, ICMP
- Communication Encrypted



C:\>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1030	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2000	0.0.0.0:0	LISTENING
TCP	0.0.0.0:44334	0.0.0.0:0	LISTENING
UDP	0.0.0.0:135	**:	
UDP	0.0.0.0:445	**:	
UDP	0.0.0.0:1027	**:	
UDP	0.0.0.0:44334	**:	

C:\>

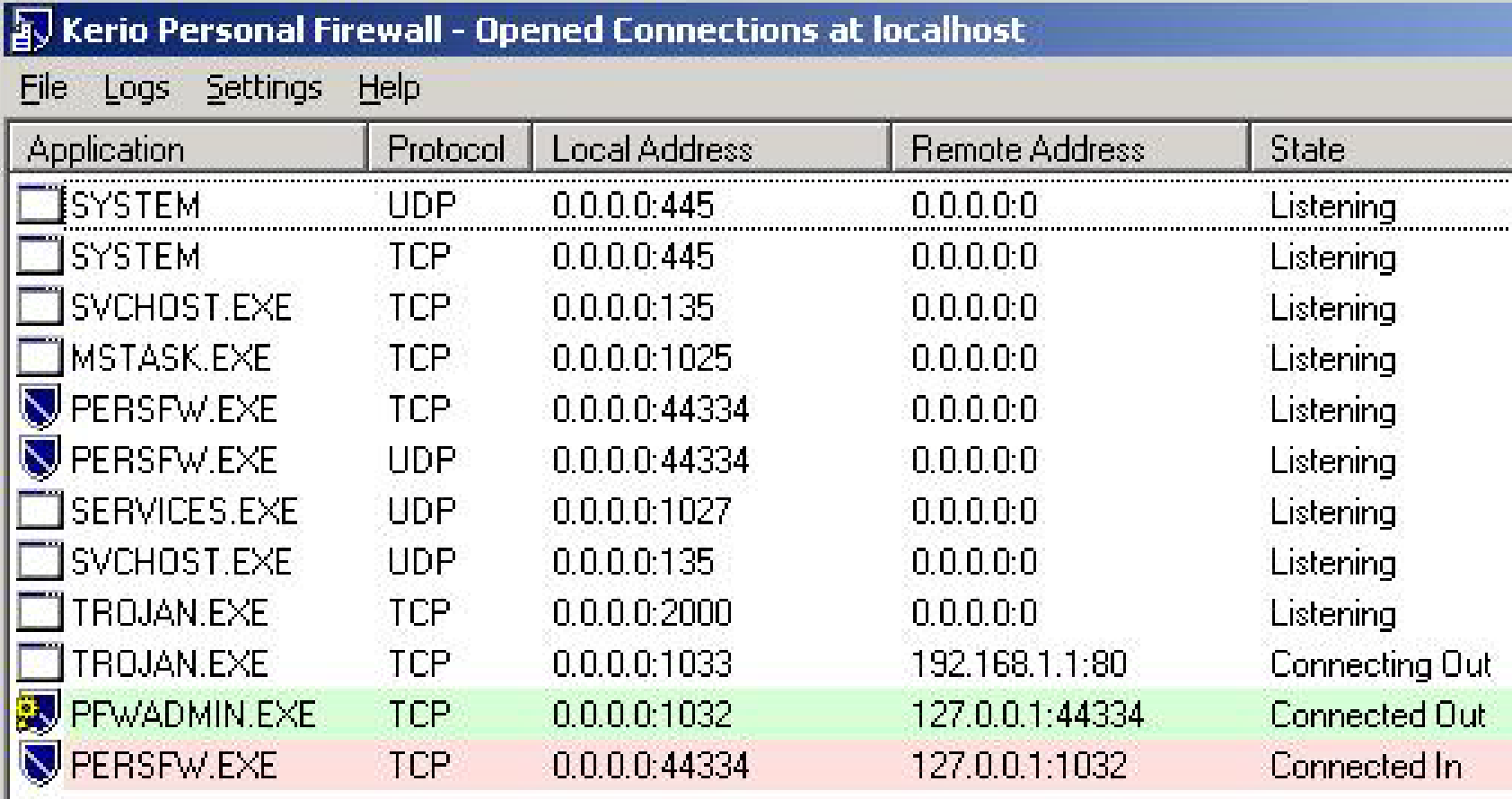
C:\WINNT\System32\cmd.exe





C:\Fport-2.0>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
<http://www.foundstone.com>

Pid	Process		Port	Proto	Path
396	svchost	->	135	TCP	C:\WINNT\system32\svchost.exe
8	System	->	139	TCP	
8	System	->	445	TCP	
640	MSTask	->	1026	TCP	C:\WINNT\system32\MSTask.exe
8	System	->	1029	TCP	
1064	OUTLOOK	->	1034	TCP	C:\PROGRA~1\MICROS~2\Office\OUTLOOK
1064	OUTLOOK	->	1035	TCP	C:\PROGRA~1\MICROS~2\Office\OUTLOOK
1208	trojan	->	1440	TCP	C:\sa.com\Exploits\trojan.exe
1208	trojan	->	2000	TCP	C:\sa.com\Exploits\trojan.exe
584	persfw	->	44334	TCP	C:\Program Files\Kerio\Personal Fir
	rsfw.exe				
396	svchost	->	135	UDP	C:\WINNT\system32\svchost.exe
8	System	->	137	UDP	
8	System	->	138	UDP	
8	System	->	445	UDP	
236	lsass	->	500	UDP	C:\WINNT\system32\lsass.exe
224	services	->	1028	UDP	C:\WINNT\system32\services.exe
296	IEXPLORE	->	1050	UDP	C:\Program Files\Internet Explorer\

Security-Assessment

.com



Application	Protocol	Local Address	Remote Address	State
<input type="checkbox"/> SYSTEM	UDP	0.0.0.0:445	0.0.0.0:0	Listening
<input type="checkbox"/> SYSTEM	TCP	0.0.0.0:445	0.0.0.0:0	Listening
<input type="checkbox"/> SVCHOST.EXE	TCP	0.0.0.0:135	0.0.0.0:0	Listening
<input type="checkbox"/> MSTASK.EXE	TCP	0.0.0.0:1025	0.0.0.0:0	Listening
 PERSFW.EXE	TCP	0.0.0.0:44334	0.0.0.0:0	Listening
 PERSFW.EXE	UDP	0.0.0.0:44334	0.0.0.0:0	Listening
<input type="checkbox"/> SERVICES.EXE	UDP	0.0.0.0:1027	0.0.0.0:0	Listening
<input type="checkbox"/> SVCHOST.EXE	UDP	0.0.0.0:135	0.0.0.0:0	Listening
<input type="checkbox"/> TROJAN.EXE	TCP	0.0.0.0:2000	0.0.0.0:0	Listening
<input type="checkbox"/> TROJAN.EXE	TCP	0.0.0.0:1033	192.168.1.1:80	Connecting Out
 PFWADMIN.EXE	TCP	0.0.0.0:1032	127.0.0.1:44334	Connected Out
 PERSFW.EXE	TCP	0.0.0.0:44334	127.0.0.1:1032	Connected In



Security-Assessment

.com

- IRC To Communicate With Trojans
- Zombie Computer – Under The Control Of A Hacker
- Trojan Connects To IRC And Awaits Commands
- Hacker Does Not Need To Know The IP Of The Compromised Computer



The screenshot shows a terminal window with a title bar that reads "[root] Well done. We reached the 200 infected." The terminal content is split into two columns. The left column shows IRC chat logs with timestamps and nicknames, such as "Election: it has to be done", "Election: this guy is taking up a slot and I want my movie", and "Election: I just keep hitting him till his movie times out". The right column shows network-related output, including IP addresses and connection status, such as "192.168.1.100", "192.168.1.101", and "192.168.1.102".



<Electron> it has to be done
 <Electron> this guy is taking up a slot and I want my movie
 <Electron> !login MS,O*GN6<]O7TT^+HX>#?_+QY./BT^+HM+.R
 X>#?Y^;ER<C']O7TT^+H_/QMGN6<Y./BT^+HM[:UI:2CKJVLKJ
 VLL;'OT.*QS,O*GN6<]O7TT^+H_/OZ<>#?MX>#?M+.RP+^^4V"
 P;2SLI7.D_#O[DC3X\NCV]?3#PL'VMG+T-'DX^+;VMG,=R\KM[.M!
 ?N3CXI[EG,/'P?/R\?;U]+2SLN'@wT4`
 <Electron> !udppacket 15000 66.68.188.47 random
 <X1-[13460]> **Electron** You are now authorized to use me...
 <X1-[13460]> [Currently Flooding] 66.68.188.47
 <Electron> **** [vV]Joel (3j7Rm2Yw@cs6668188-47.austin.tx.com)
 Quit (Ping timeout)
 <Electron> ah
 <Electron> cool
 <Electron> I will just keep hitting him till his movie times out
 <sigh> and i packet all the time?
 <Electron> I poacket occasionally
 **** **XS-[34849]** (~benzell@200.174.31.irc com-42393)
 quit [04:09] Connection reset by peer
 **** **XS-[53020]** (zbritneeo@irc. .com-28510.Reshall.Ber
 keley.EDU) join [04:09]
 <Electron> you packet all the time
 <Electron> time

@BotMonitor
 +Cable
 +sigh`
 +X1-[13460]
 sigh````
 X1-[15619]
 X1-[24381]
 X1-[33094]
 X1-[3348]
 X1-[33496]
 X1-[38861]
 X1-[46370]
 X1-[56808]
 X1-[61968]
 X1-[67391]
 X1-[69823]
 X1-[70586]
 X1-[73428]
 X1-[76877]
 X1-[80118]
 X1-[83854]
 X1-[90429]
 X1-[90904]
 X2-[30305]
 X2-[52151]
 X2-[6820]

Security-Assessment

.com

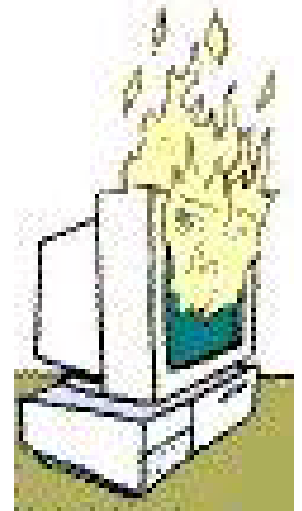
- 0 Day – Hole That The Vendor Is Not Aware Of
- No Patches
- White Hat == Good Guys
- Black Hat == Bad Guys
- Responsible Disclosure Of Security Holes



Security-Assessment

.com

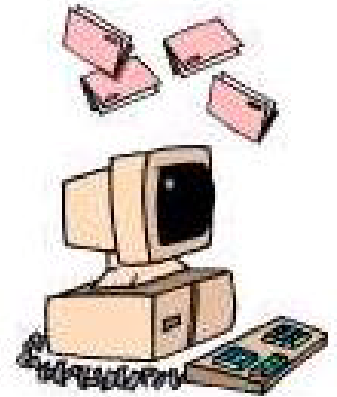
- March 2003, 0 Day Exploit In Use
- Attack On US Military Web Site
- Webdav – Distributed Authoring And Versioning
- Webdav – Enabled By Default



Security-Assessment

.com

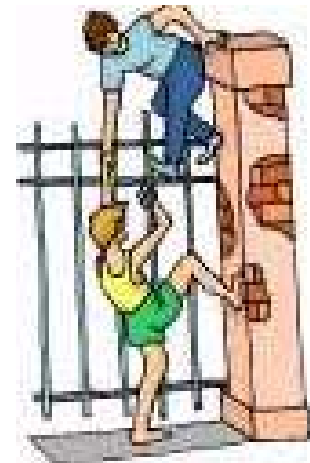
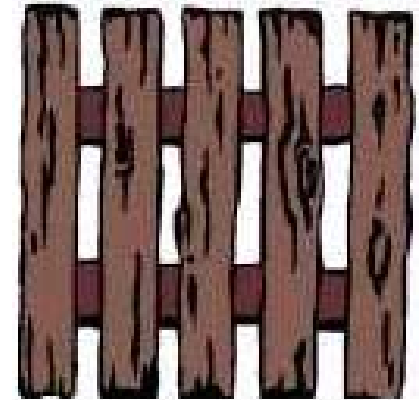
- Ensure Servers Are Up To Date With Security Patches
- Subscribe To Security Newsletters
- Conduct External Penetration Testing
- Running A Bare Minimum Server
- All Extra Services And Files Should Be REMOVED



Security-Assessment

.com

- Defence In Depth – A Multi-layered Approach To Security
- Do Not Rely On The First Fence!
- Web Servers Are The Most Commonly Hacked Servers
- Restrict Outbound And Internally Directed Traffic With Firewalls



Security-Assessment

.com

- Script Kiddies – Little Or No Real Hacking Skill
- Elite Hackers – Able To Create Exploit Tools, Worms, Rootkits And More
- Elite Hackers Will Share With Other Group Memembers
- Script Kiddies Gain Access To Elite Hacking Tools



S4t4n1c SOULS ownz YOUR BOX



Security-Assessment

.com

- Web Site Defacement – When The Main Page Is Changed
- Cyber-Graffiti
- Over 250 NZ Defacements So Far In 2003
- Zone-H.org Web Site Defacement Mirror
- WWW.CCIP.GOV.T.NZ



Security-Assessment

.com

- Denial Of Service Attacks – When Large Amounts Of Fake Traffic Cause Another Internet Connection To Become Unavailable



Security-Assessment

.com

- Information Theft
- Credit Card Fraud
- Identity Theft
- Industrial Espionage
- Blackmail / Extortion



Security-Assessment

.com

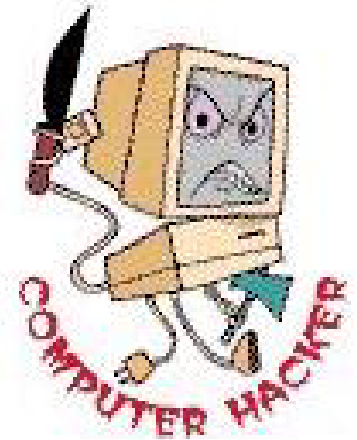
- Cost Is Difficult To Estimate
- Charged For FTP And DoS Traffic
- Email And Internet Access May Need To Be Shut Down
- Web Site Defacement Could Lead To Loss Of Customer Confidence



Security-Assessment

.com

- NZ Has Hackers!
- VeNoMouS – Linked With Overseas Groups, Arrested And Charged For Hacking Local Companies
- Crimes Ammendment Bill No 6
- Problems Will Arise Through Jurisdictional Disputes Across Countries



Security-Assessment

.com

- International Problem
- International Hackers
Hack Internationally
- No Borders, No Distance
- Size Doesn't Matter



BECAUSE THEY CAN!



Security-Assessment

.com

Presentation Slides And Speech Available
For Download From:

<http://www.security-assessment.com>

