

Network Based IDS – Introduction & Experiences with Shadow

Data Security Nordic 2000
Tieturi



26.10.2000
japi@atbusiness.com
Senior Consultant, CISSP
AtBusiness Communications
<http://www.atbusiness.com/>



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 1

I have...

- ...some Unix experience
- ...some programming experience (C, C++, Perl, shell-scripts)
- ...concentrated in information security last 5 years
- ...been working in PKI-, LDAP- and VPN-projects lately
- ...studied and evaluated IDS-tools last 2 years
- ...looked at several NIDS-tools e.g. Dragon, RealSecure NFR, Snort, eTrust ID (SessionWall-3),...
- ...been running Shadow in our company network last 2 years
- ...some IDS-related links at
<http://www.atbusiness.com/staff/japi/security.html#ids>



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 2

Are you safe?

- How many network scans were targeted to your network last month?
a) more than 10 b) 1-10 c) none d) don't know
- How many serious break-in attempts?
a) more than 10 b) 1-10 c) none d) don't know
- How many succeeded break-ins?
a) more than 10 b) 1-10 c) none d) don't know
- Does your ecommerce-site have correct product information and pricelist?
a) yes b) no c) don't know
- Does your firewall protect you?
a) yes b) no c) don't know



Security Survey

<http://www.infosecuritymag.com/2000survey.pdf>

- Information Security Magazine annual survey
- Summer 2000 - 1,897 responses
- Outside breaches
 - Viruses/Trojans/Worms - 80%
 - Denial-of-Service - 37%
 - Exploits related to active program scripting - 37%
 - Attacks related to protocol weaknesses - 26%
 - Attacks related to insecure passwords - 25%
 - Buffer overflows - 24%
 - Attacks on bugs in Web-servers - 24%



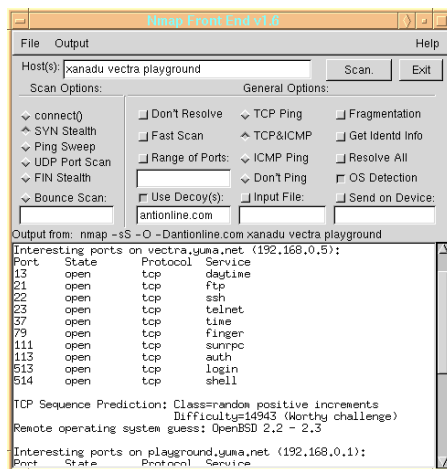
Hacker attack

- 1 Map the network and services
- 2 Find vulnerabilities
- 3 Break-in
- 4 Take over the system, install backdoors
- 5 Cover tracks, attack neighbor nodes
- 6 Steal, copy, destroy, change, blackmail,...
- 7 Use the system as a stepping stone when attacking other systems



nmap

<http://www.insecure.org/nmap/>



- Vanilla TCP connect() scanning
- TCP SYN (half open) scanning,
- TCP FIN, Xmas, or NULL (stealth) scanning
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments
- UDP raw ICMP port unreachable scanning
- ICMP scanning (ping-sweep)
- TCP Ping scanning
- Remote OS Identification
- Reverse-ident scanning



Nessus

<http://www.nessus.org/>



Nessus Report

Summary

- Number of hosts tested : 5
- Found 17 security holes
- Found 93 security warnings

bonsai.fr.nessus.org
 prof.fr.nessus.org
 dormeur.fr.nessus.org
 gateway.fr.nessus.org
 grincheux.fr.nessus.org

poppassd (106/tcp)
 pop-3 (110/tcp)
 unknown (135/tcp)
 netbios-ssn (139/tcp)

Security warnings

The remote registry can be accessed remotely using the login / password combination used for the SMB tests.

Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker.

Solution : filter incoming traffic to this port or set tight login restrictions.

Risk factor : Low
The domain SID can be obtained remotely. Its value is :

INTRANET : 5-21-20333150-368275040-1648912389

Save as... Save as HTML with Pies... Close

Hacker's toolkit - \$15.99



amazon.com

RATDOGS

HACKERS TOOLKIT V2.0 so you want to be a HACKER!!!

Price: \$15.99

Description: This CD-ROM contains many of the best hacking tools available today. It's a hacker's delight! 32 Bit Hacking & Cracking Tools. This is the NEW version... [read more](#)

ITEM INFORMATION

Exploits & security

Do not confuse this with the older version of Hackers toolkit Vol 1

This is the all new version

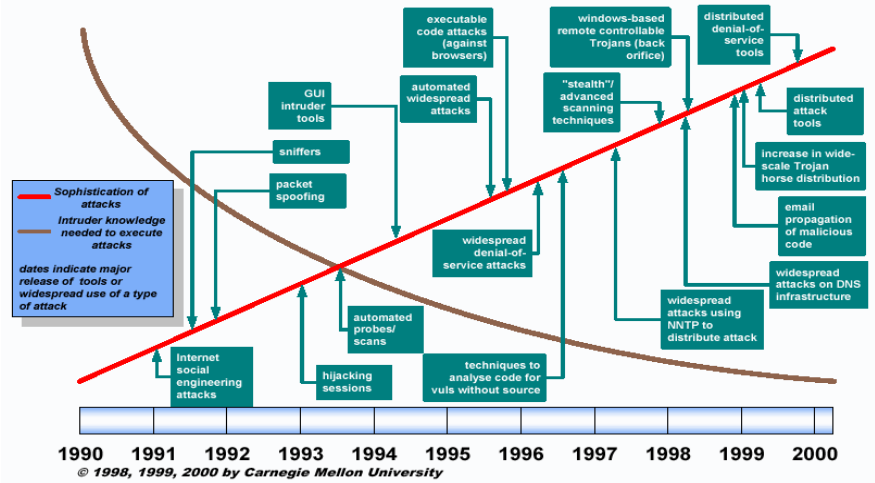
- ANTI VIRUS TOOLS
- IRC UTILITIES
- PASSWORD CRACKERS
- PROGRAM CRACKERS
- KEY LOGGERS
- PINEAKING TOOLS
- CODE WACKERS
- NOVELL

Plus Much More!

- WIN 95/98
- RWKERS
- FLOODERS
- CMP PROGRAMS
- C/P PROGRAMS
- CRACKERS
- LINK ZONE
- MAC PROGRAMS
- MAIL PROGRAMS
- IRC
- PORT SCANNERS
- IATLIES
- PORT BOMBERS
- SPOOFING
- SNIFFERS
- APPROPRIATE CRACKS

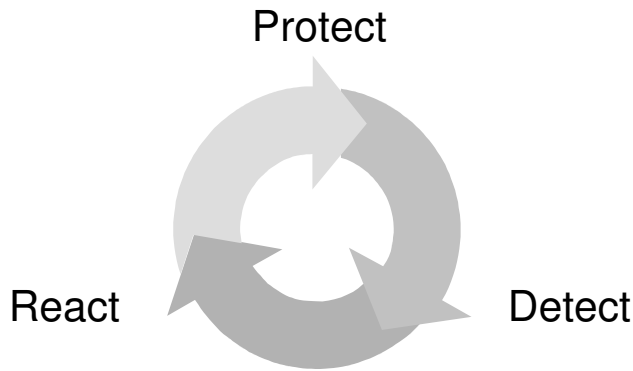
Hackers Toolkit 2.0 contains the most complete set of hacking & protection tools available today.

Attack Sophistication vs. Required Intruder Knowledge



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 9

Security is a process!



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 10

Detection tools

- Intrusion Detection Systems
 - Server-based
 - Workstation-based
 - Application-based
 - Network-based (NIDS)
- Vulnerability Scanners
- System Integrity Verifiers
- Log File Monitors
- Deception Systems (honeypots)



Why firewall alone is not enough?

- Firewall is a gatekeeper - we need a burglar alarm too
- Firewall doesn't recognize attacks attempted with allowed protocols: http, ftp, email, dns,...
- Firewall doesn't save enough history information
- Intranet is usually not protected with firewalls
- Firewall doesn't handle problems with protocols and applications
- How do you verify your firewalls configuration and function?
- Do you know all the services running in your network?
- Firewall software could have bugs also
- Multiple layer security is more effective



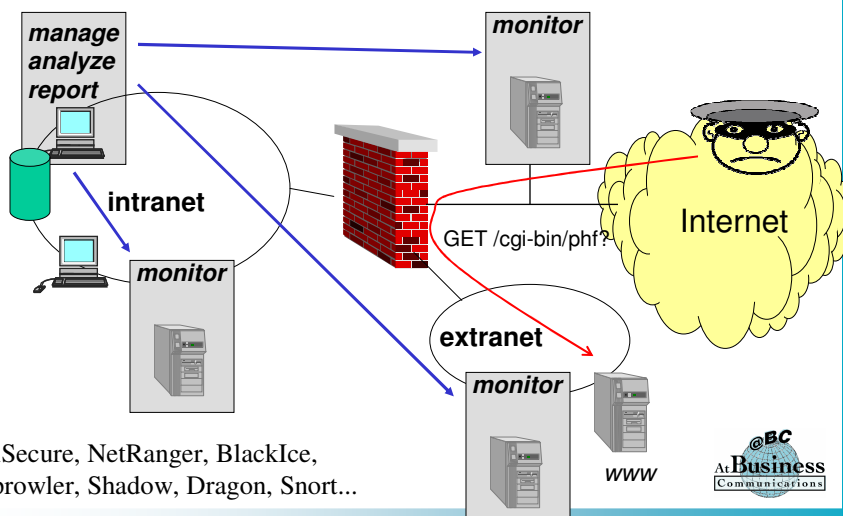
NIDS

Network Intrusion Detection System

- Listens to network traffic
- Notices known attacks
- Notices non-standard TCP/IP packets
- May launch protective actions
- Saves history
- Invisible for users and applications



Example NIDS setup



RealSecure, NetRanger, BlackIce,
Netprowler, Shadow, Dragon, Snort...

Good IDS-tool

- Invisible, needs few resources
- Reliable, fault-tolerant
- Easy to modify for different needs
- Adapt to changes, scalable
- Difficult to fool
- Notices abnormal behavior
- Easy to use, central administration
- Good reporting and analyzing features
- Large problem/fingerprint database



Why to have NIDS?

- Attacks are noticed in their early phase
- It's better that you find the problems instead of a hacker
- Traffic history of attack is saved => evidence
- Verify the adequacy of your security arrangements
- Makes it easier to negotiate security budget:-)



NIDS challenges

- Analyzing attacks require TCP/IP and security expert
- Fast networks
- Heavily loaded networks
- Switched networks
- TCP/IP problems: forged source IP's, flags,...
- Fragmented IP-packets
- Insertion attacks, "su ro^H^Hroot"
- Denial-of-service attacks against NIDS
- Encryption
- Keeping attack signatures up-to-date



NIDS challenges

```
[**] WEB-CGI-bash shell [**]
10/16-00:07:44.900000 0:E0:1E:7F:A:10 -> 0:0:D1:ED:50:A9 type:0x800 len:0x18F
xx.xx.xx.xx:1822 -> yy.yy.yy.yy:80 TCP TTL:122 TOS:0x0 ID:23276 DF
*****PA* Seq: 0x1055FEB Ack: 0x434B1054 Win: 0x2238
47 45 54 20 2F 78 2D 73 61 6A 74 69 6E 67 2F 63 GET /x-sajting/c
68 61 74 2F 69 6C 6D 65 65 74 2F 2F 62 61 73 68 hat/ilmeet//bash
66 75 6C 2E 67 69 66 20 48 54 54 50 2F 31 2E 31 ful.gif HTTP/1.1
0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 52 ..Accept: /*.*.R
65 66 65 72 65 72 3A 20 68 74 eferer: ht
```



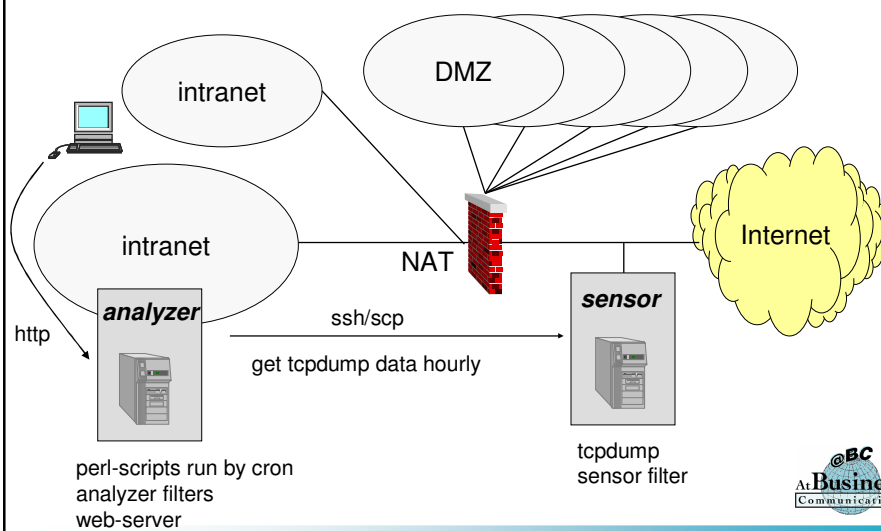
Shadow

<http://www.nswc.navy.mil/ISSEC/CID/>

- Free NIDS tool based on
 - Unix
 - tcpdump
 - Perl
- You need
 - 2 Unix boxes with lots of disk-space
 - Unix experience
 - tcpdump experience
- Design philosophy
 - No alarms, but system/security administrator checks the reports when appropriate
 - Checks (TCP/UDP/IP) headers only



Our setup



Filters

- Sensor filters define what packets are captured
 - all ip except mail and ftp-data
 - how much payload is save
- Analyzer filters define interesting packets
 - abnormal IP-traffic
 - ports scans
 - network mapping
 - non-http connections to web-servers
 - known attack-signatures
 - icmp.filter, ip.filter, udp.filter, tcp.filter, site.filter,...



Tcpdump filters

- tcp and (tcp[13] & 2 != 0)
 - tcp packet with SYN-bit on (13th byte of the tcpheader)
- tcp and (tcp[13] & 2 != 0) and (dst port 143)
 - imap
- ip and ip[19] = 0xff
 - Broadcast packets
- ip and dst port 111
 - Portmapper
- ip[12:4] = ip[16:4]
 - Same src and dst ip-address => land-attack
- icmp[0] != 8 and icmp[0] != 0
 - icmp-packets other than echo requests & replies



Example analyzer filter

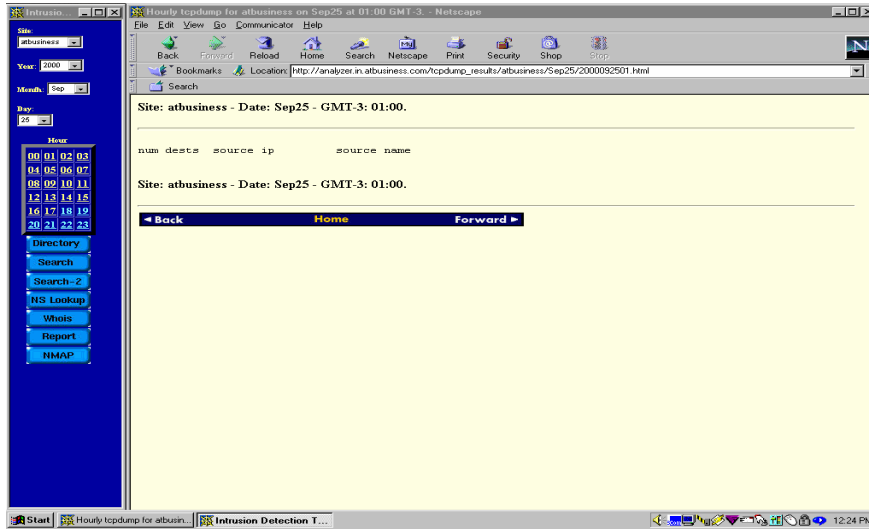
```
ip and (not src host fw.atbusiness.com) and  
(  
  (dst host www.atbusiness.com and  
  (  
    (tcp and ((tcp[13] & 2 != 0) and (tcp[13] & 0x10 = 0))  
      and (not dst port 80)  
      and (not dst port 443))  
  ))  
or  
  
(dst host imap.atbusiness.com and  
(  
  (tcp and ((tcp[13] & 2 != 0) and (tcp[13] & 0x10 = 0))  
    and (not dst port 143))  
))  
)
```



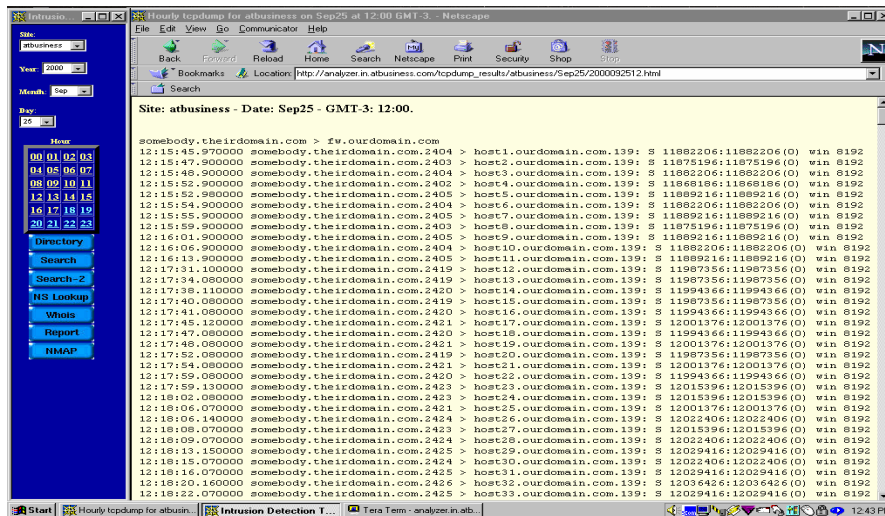
Shadow screendumps

A screenshot of a Netscape browser window. The address bar shows the URL 'http://analyzer.in.atbusiness.com/shadow/'. The main content area has a blue background with the text 'AtBusiness Intrusion Detection & Response Team using SHADOW' and the AtBusiness Communications logo. Below this, it says '(SANS Heuristic Analysis for Defensive Online Warfare)'. At the bottom, there is a graphic with the text 'team Shadow' and a stylized face. The browser's left sidebar shows a navigation menu with options like Directory, Search, Search-2, WS Lookup, Whois, Report, and NMAP. The taskbar at the bottom shows the Start button and several open windows, including 'Intrusion Detection T...'. The system tray shows the time as 12:21 PM.

No problems



Netbios scan



Whois he?

The screenshot shows a Netscape browser window with a 'Team SHADOW - WHOIS Form' open. The form contains a search field with the text 'somebody.theirhost.com' and a list of IP addresses with their corresponding domains. The list includes:

- 4834708 (0) win 1028
- 4834708 (0) win 1028
- 691291518 (0) win 1028
- 2645403 (0) win 1028
- 276032859 (0) win 1028
- 1474474547 (0) win 1028
- 156455543 (0) win 1028
- 0161 (0) win 1028
- 09 (0) win 1028
- 12104784188 (0) win 1028
- 1556 (0) win 1028
- 1474474547 (0) win 1028
- 029 (0) win 1028
- 401465 (0) win 1028
- 841290844 (0) win 1028
- 2645403 (0) win 1028
- 276032859 (0) win 1028
- 156455543 (0) win 1028
- 6911608016369 (0) win 1028
- 1639549311 (0) win 1028
- 401466698 (0) win 1028
- 376 (0) win 1028
- 451 (0) win 1028
- 376 (0) win 1028
- 0702899 (0) win 1028
- 7139476 (0) win 1028
- 5115186135 (0) win 1028
- 1177001595 (0) win 1028
- 451 (0) win 1028
- 3122 (0) win 1028

The browser's address bar shows the URL: http://analyzer.in.atbusiness.com/tcpdump_results/atbusiness/Sep24/2000092418.html. The page title is 'Site: atbusiness - Date: Sep24 - GMT-3: 18:00.' The browser's status bar shows 'Document: Done' and the time '12:54 PM'.

Example scan (t0rnkit)

timestamp	source.port	dest.port	flags	beginning: seq #	ending: seq #	(bytes)	options
18:10:14.155524	somebody.theirdomain.com.511	> host1.ourdomain.com.511	SF	694834708	694834708	(0)	win 1028
18:10:14.155524	somebody.theirdomain.com.511	> host2.ourdomain.com.511	SF	694834708	694834708	(0)	win 1028
18:10:14.155524	somebody.theirdomain.com.511	> host3.ourdomain.com.511	SF	1691291518	1691291518	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host4.ourdomain.com.511	SF	942645403	942645403	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host5.ourdomain.com.511	SF	1276032859	1276032859	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host6.ourdomain.com.511	SF	474474547	1474474547	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host7.ourdomain.com.511	SF	156455543	156455543	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host8.ourdomain.com.511	SF	1839000161	1839000161	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host9.ourdomain.com.511	SF	990107509	990107509	(0)	win 1028
18:10:14.165524	somebody.theirdomain.com.511	> host10.ourdomain.com.511	SF	2104784188	2104784188	(0)	win 1028

Normally source port is random

SYN + FIN is not normal

Fast repeating connections

Port used by t0rnkit



Shadow - advantages

- Free
- Flexible
- Easy to modify/expand with perl
- Lots of tools available to work with tcpdumps
- No alarms - only reports
- Saves all traffic
- Possible to use in complex environment – we have several "home nets", separate net addresses for fws and NAT in use.



Shadow - disadvantages

- Can't analyze IP payload
- Keeping filters up-to-date in large environment is difficult
- No real-time alarms
- Analyzing data requires lots of TCP/IP, Unix, Perl and tcpdump knowledge
- No real on-going development



Snort

<http://www.snort.org/>

- Based on tcpdump, analyzes also IP payload
- Lots of attack fingerprints available
- Saves only suspect traffic
- Very active development
- Lots of add-on tools
- Can analyze tcpdump-files created by Shadow
- Shadow sensor can be replaced by Snort
- Real-time alarms
- Difficult to configure for complex network



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 33

Shadow + Snort

- Snort can be used to get tcpdump data for Shadow
- Snort can be used to analyze Shadow tcpdumps
- IP-payload checked by Snort
- Real-time alerts by Snort
- Two systems see more than one!

- Our current solution is to run Shadow dumps through Snort daily
- Better solution would be to replace Shadow sensor by Snort and let it feed Shadow analyzer



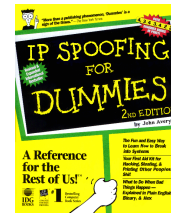
Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 34

Scans to our network

	Sep-1999	Mar-2000	Sep-2000
ftp		2	6
telnet		1	1
http		1	1
pop2		3	
pop3	1		1
imap	1		
dns		3	3
sunrpc	2	4	4
socks	1	1	
linuxconf		1	1
netbios	1		18
hack'a'tack	2	2	1
subseven	1	2	2
netbus	1	2	1
ringzero		1	1
udp port 1	1		
rpc.statd exploit			2
i0rn			1
	11	23	43

2000

Jan 16
 Feb 25
 Mar 23
 Apr 37
 May 32
 Jun 19
 Jul 31
 Aug 26
 Sep 43
 Oct 51 (24.10)



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 35

Response to scans

- Well-known companies get lots of scans per day
- NASA: 500.000 attacks per year
- I think that response to scans is worth while if you don't have to worry about serious attacks all the time
- Automate the reports and response as much as possible
- It's best that novice script-kiddies get a warning in the beginning of their "career", slap on the wrist



Copyright 2000 AtBusiness Communications Oy / Jari Pirhonen 13.4.2000 Page: 36

Recovering from the break-in (SANS)

- Remain calm; don't hurry.
- Notify your organization's management.
- Provide a game plan (with options if possible).
- Apply need-to-know.
- Use out-of-band communications; avoid email and other network-based communications channels.
- Take good notes, good enough to serve as evidence in a court of law.
- Contain the problem; pull the network cable.
- Back up the system(s), and collect evidence.
- Eradicate the problem and get back in business.
- Lessons learned, apply what you have learned.



Inform the administrators

Below is a log showing a connection attempts from a machine within your domain. The machines it connected to does not offer this "service" so this can only be assumed to be an IP space probe for vulnerable machines. Port 31789 belongs to trojan program called "Hack'A'tack".

We take this matter seriously, and hope that you will as well. Please take action on this issue as is appropriate and respond to this email-address with your actions. If possible, please sign your email digitally.

1. Apr 2000 (timezone is GMT + 2, Helsinki, Finland)

```
19:58:44.840000 hacker.evil.org.31790 > host1.ourdomain.com.31789: udp 1
19:58:44.840000 hacker.evil.org.31790 > host2.ourdomain.com.31789: udp 1
19:58:45.110000 hacker.evil.org.31790 > host3.ourdomain.com.31789: udp 1
19:58:45.110000 hacker.evil.org.31790 > host4.ourdomain.com.31789 : udp 1
19:58:45.120000 hacker.evil.org.31790 > host5.ourdomain.com.31789: udp 1
```

...



Real-world responses

"We identified the dialup account that was used for this port scan. The account belongs to an local hospital, but apparently is often 'stolen' (or perhaps used unauthorised from employees outside of the hospital). We will take this with their management - the account has been temporarily suspended. Thanks for letting us know."

"First, thank for you attention. This scanners were in computer room and they is students. This campus was disconnected from Internet. About this episode was reported to warden, rector of PSTU and FSB. Two students was stand off Internet."

"Sorry....our server is hacked. so... we are reinstalling the server..."

"We take a serious notice of this kind of hacking. The address that you are mail me about, is belong to a dial-up pool. We will find out which customer was used this address at this portion of time and will take care about that problem"

"Thank you for your report. While we are not allowed to give out specific information regarding subscriber identity, or specific action taken without legal process, we have identified the offending user and taken appropriate action against this account."



Real-world responses

"We already had complaints yesterday and contacted our customer immediately. They noticed a breakin on Sunday (10.09.2000) themselves and had blocked the host on router level. They are currently cleaning up the system and investigating the issue. Thanks for the notice and sorry for the inconveniences."

"The customer owning the machine used for the portscans has been warned, and he has ensured us to fix the security on his machine. If any new portscans from that machine will occur, we will disconnect the machine. Our apologies for the inconvenience."

"My apology for any inconvenience that may have caused you. We had a Linux test box that sat outside our firewall. Unfortunately it was hacked and used for hacking other sites. It is now shutdown. Again, my apology."

"Thank you for notification of this event. I want to assure you that we take such issues seriously as well. We allow some of our users to have personal machines in our IP address space, which this machine is one of. It appears that it was hacked, and we are tracing down how and by whom. Until such time as we can be sure that the incident will not repeat, this machine will be removed from the network. If you have any other @BC concerns, please feel free to contact me directly."



Planning

- Level of TCP/IP expertise in your company?
- Public Domain or commercial product?
- Where to put the sensors?
- Alarms or logs?
- How often and how the tool is updated?
- What does your security policy define?
- Who need to belong in CERT/CIRT?
- How to response?



First things first

5. Audit, response, investigation, IDS
4. Technology, products
3. Education
2. Security architecture, processes
1. Policies, guidelines

