IBM Global Services

Computer Forensics

Douglas G. Conorich
Global Solutions Manager
Managed Security Services
conorich@us.ibm.com
817-962-5426

© 2003 IBM Corporation

Agenda

- Why Create a Computer Forensics Capability
- First Response – Investigative Principles
- Models for Intrusion Analysis
- File System
- Anatomy of an Attack
- Logs
- Analysis Tools

© 2003 IBM Corporation

Why Create a Computer Forensics Capability

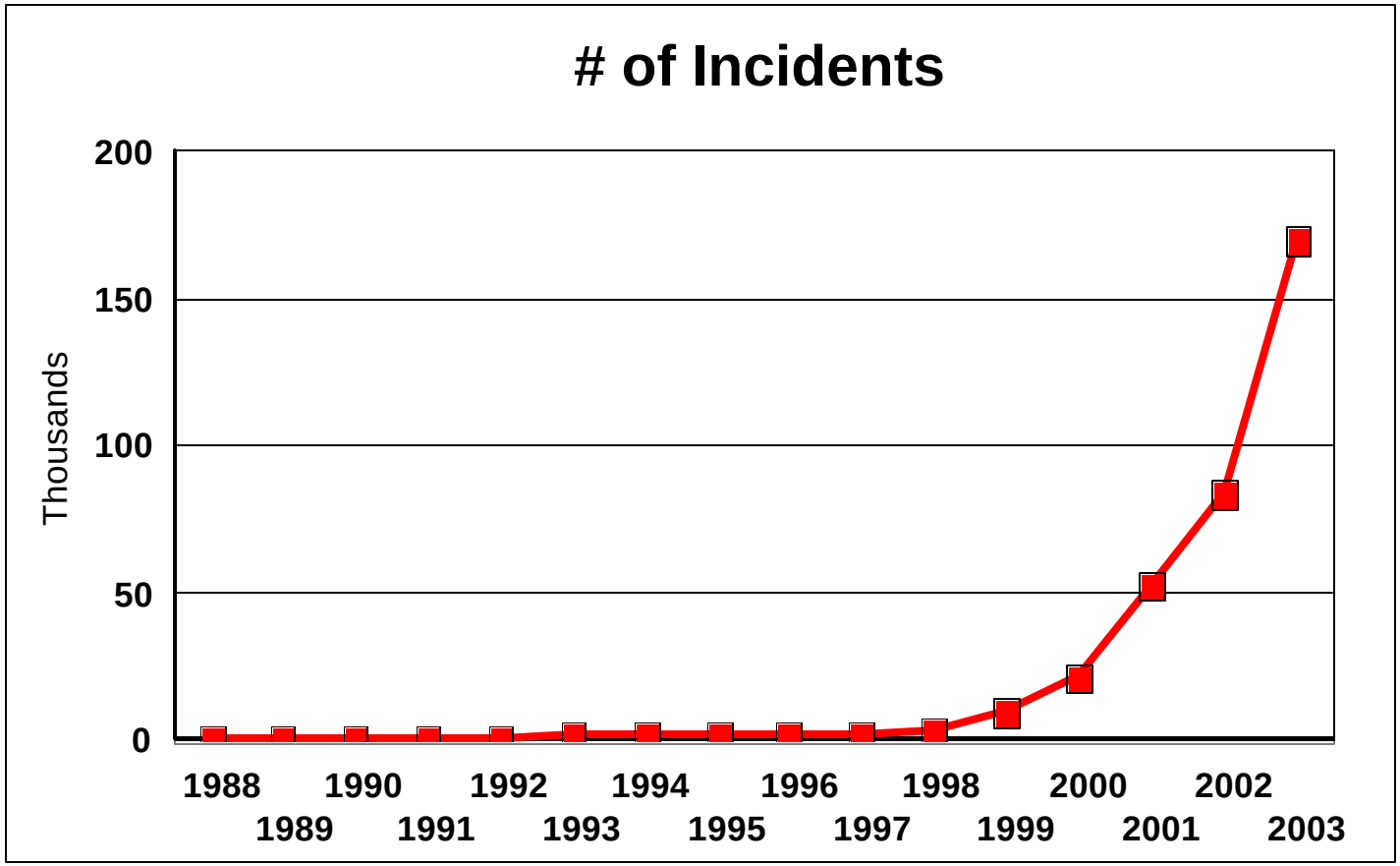
© 2003 IBM Corporation

Support internal investigations

- Theft and Embezzlement
- Hacking
- Email Abuse
- Software Piracy
- Internet Abuse
  - Pornography / Kiddie Pron Investigations
  - Stalking / Harassment

© 2003 IBM Corporation

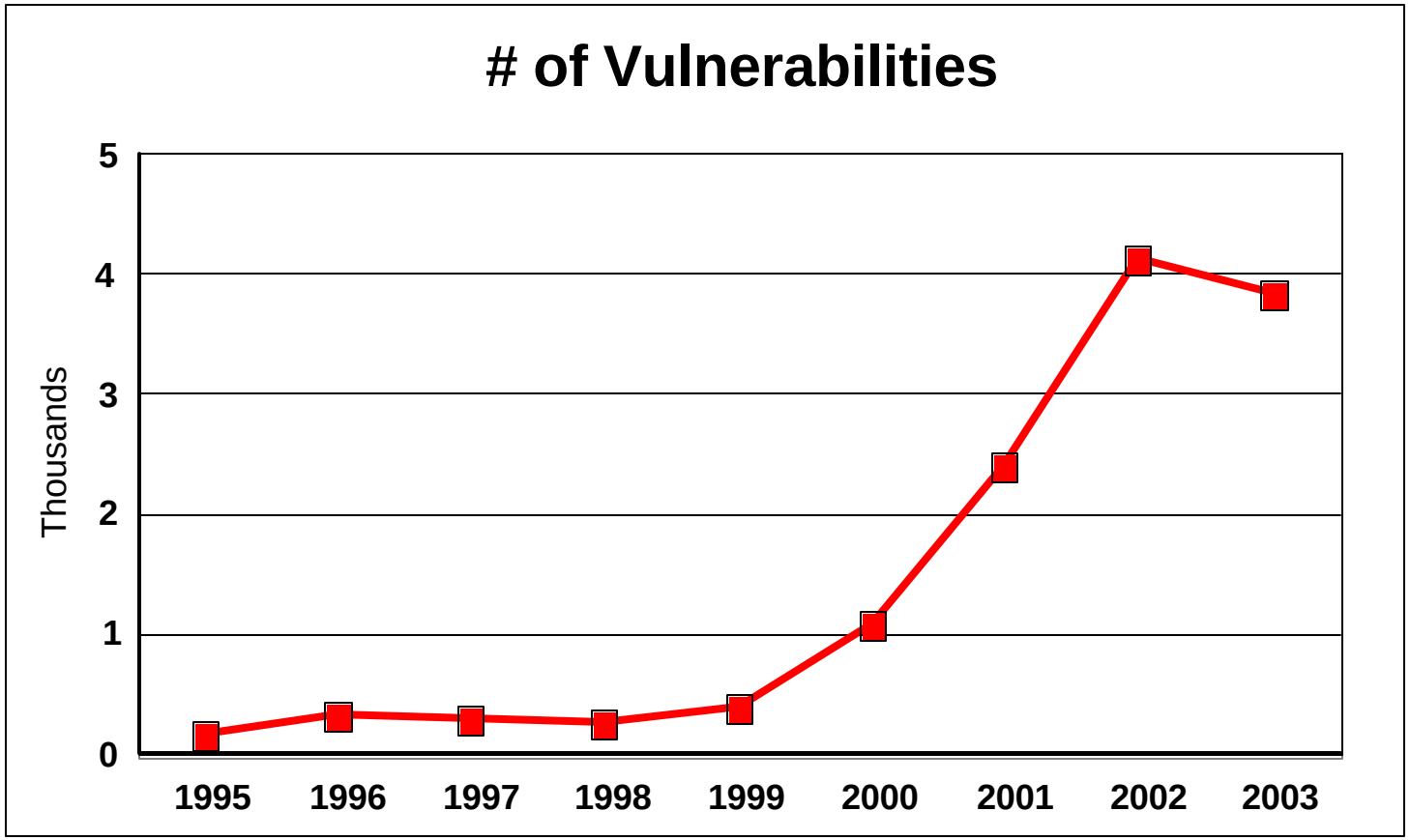
Number of Incidents



2003 Q1 = 42,586

© 2003 IBM Corporation

Number of New Vulnerabilities



2003 Q1 = 959

© 2003 IBM Corporation

And It's Probably Worse Than We Think….

- DOD Controlled Study (circa 1996)

Machines Attacked:	38,000
Machines Penetrated:	24,700 (65%)
Attacks Detected:	988 (4%)
Attacks Reported:	267 (27%)

© 2003 IBM Corporation

Roll Your Own or MSSP

- Driven by your organizational culture and economics
- Regulatory restrictions
- Number of cases requiring forensics
- Cost of development vs. consultants
  - Training
  - Retension
  - Multi-tasking
  - Software and hardware
- Flexibility
- What does management want

© 2003 IBM Corporation

Forensic MSSP's

- Cost can range from $100/hr to $500/hr
- Can be on retainer
- Provide instant expertise and credentials
- Latest forensic tools and hardware
- Availability may vary

© 2003 IBM Corporation

First Response – Investigative Principles

© 2003 IBM Corporation

What Type of Response?

Incident Management

Computer Forensics

© 2003 IBM Corporation

Terms

- **Incident Management** – The overall management process for handling the investigation and response to a critical incident. This can also be termed as the program management of an incident.

- **Forensic Investigation** – The detailed examination of all the physical and logical residue of a crime to scientifically determine the exact mechanism of that incident and/or to obtain evidence and process electronic evidence that will be use in a subsequent criminal investigation.

© 2003 IBM Corporation

Differentiation

- Forensic – An argumentative exercise, belonging to a court of law or public discussion and debate….
- Objectives differ:

  Conduct forensics to prosecute a perpetrator

  Conduct forensics to recover a business

© 2003 IBM Corporation

Initial Response

- The goal of your initial response is two-fold:
  - Retrieve enough information to CONFIRM that in incident has occurred.
  - Retrieve the VOLATILE data on the system that will no longer be there after you power the system off.

© 2003 IBM Corporation

Investigation Principles

- Did a crime REALLY occur?
- NEVER ASSUME!
  - "It's just a web page defacement…"
- Use the, "I don't believe you" ("Show Me") method of investigation
  - Until something has been proven beyond a doubt don't use it to guide your investigation
  - Always have two to three separate solid data points before you believe it
- STPA!

© 2003 IBM Corporation

STPA

STOP!!

Think, Plan, Act…

© 2003 IBM Corporation

Did a Crime Really Occur?

- Many incidents really are not
- Review all sources of information
- Determine the total situation

© 2003 IBM Corporation

Determine the total situation

- What system(s) were attacked?
- What method(s) was used in the attack?
- When did the attack start?
- What was the source of the attack?
- What damage was caused by the attack?
- How was the attack discovered?
- Is the system secure now?
- Who else know about the attack?

© 2003 IBM Corporation

The Issues

- Systems are Huge, Complex and Change Rapidly
- Things can hide anywhere
- Very little technical knowledge
- Knowledge and experience are important
- Gathering data is easy, Analysis is harder
- Storage
- Continuity of business functions
- Threat of destruction of data
- Loss of reputation or revenue

© 2003 IBM Corporation

Lemmas

- Speed is of the essence but don't overdo
- Anything you do to a system disturbs it
- You can never trust the system
- Your policies must always be considered
- Resign yourself to failures
- Prepared to be surprised

© 2003 IBM Corporation

Requirements for Digital Detectives

- Technical awareness
- Technical implication of actions
- Understand how data can be modified
- Clever, open-minded and devious
- Highly ethical
- Continuous education
- Knowledge of history
- Always use redundant data sources when drawing conclusions

© 2003 IBM Corporation

Software

- Many options
- Linux
  - Coroner's Toolkit, @Stake
- Windows-based programs
  - Encase
  - FTK
  - NTI
  - Maresware
  - DTSearch
  - Dibbs
  - Vogon

© 2003 IBM Corporation

When Faced with a"Situation"...

CRIME SCENE CRIME SCENE CRIME SCENE CRIME SCENE

- Secure and isolate
- Record the scene
- Conduct a systematic search for evidence
- Collect and package evidence
- Maintain chain of custody

CRIME SCENE CRIME SCENE CRIME SCENE CRIME SCENE

© 2003 IBM Corporation

Searching for Evidence

- Preserving state
- We can never know the past
- Even the present is tricky
- Always collect data in accordance with the Order of Volatility

© 2003 IBM Corporation

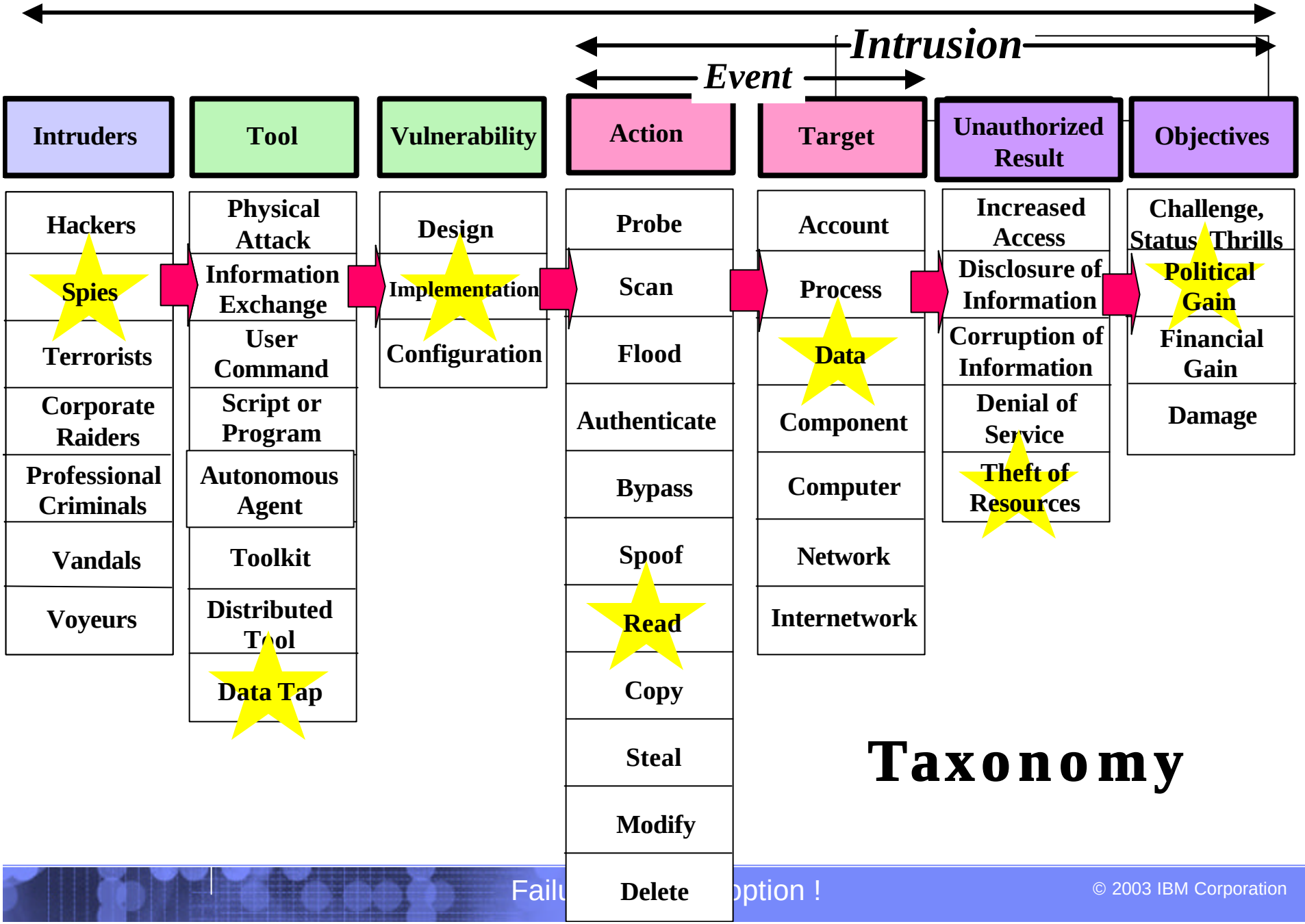
Order of Volatility

- Registers, peripheral memory, caches
- Memory (Kernel, Physical)
- Network state
- Running processes
- Hard Disk
- Floppies, backup media, etc.
- CD-ROMs, printouts, etc.

© 2003 IBM Corporation

Models for Intrusion Analysis

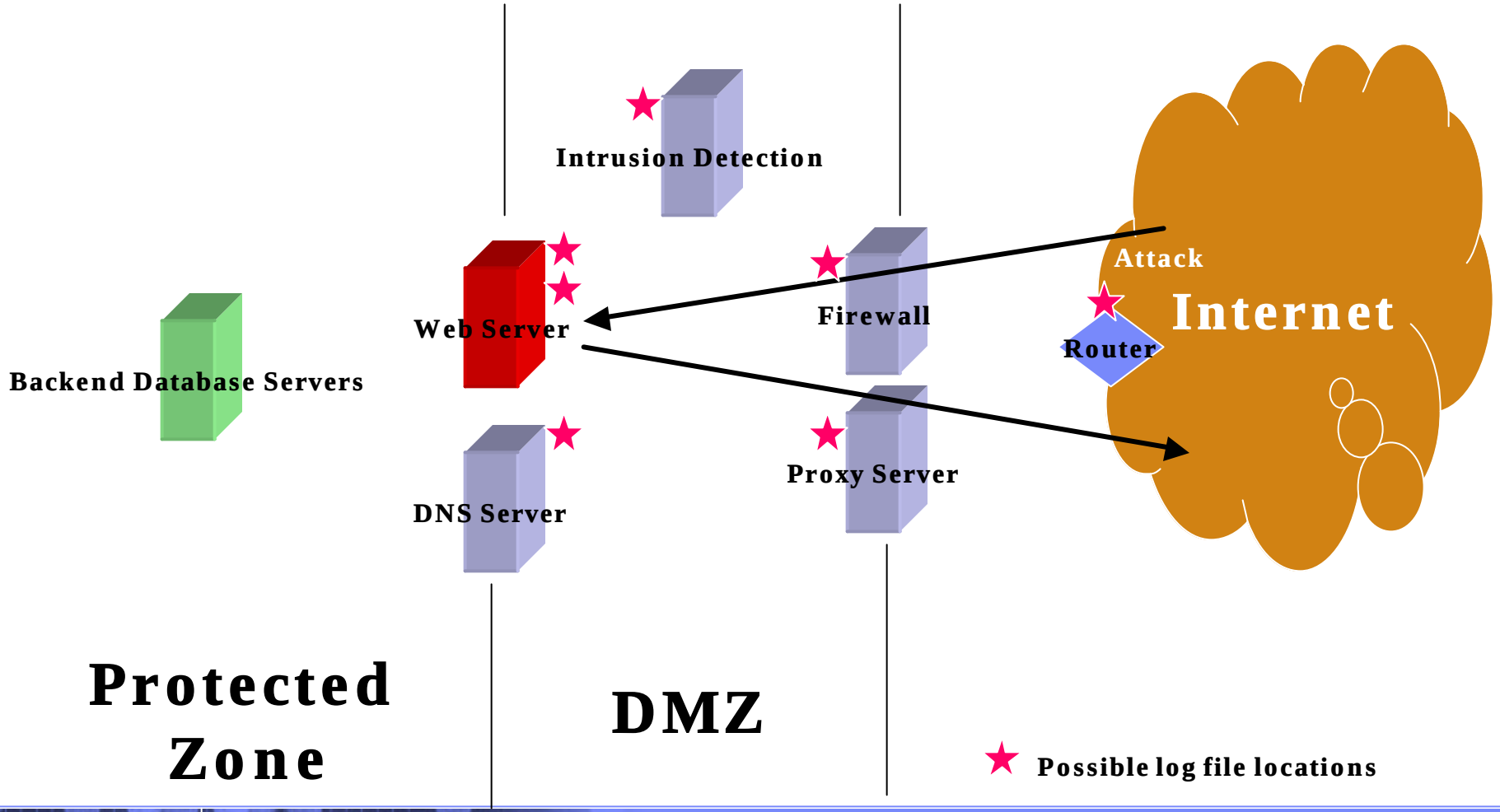
Incident



Taxonomy

© 2003 IBM Corporation

Architecture of an Attack



© 2003 IBM Corporation

IBM Global Services

Anatomy of a Hack

© 2003 IBM Corporation

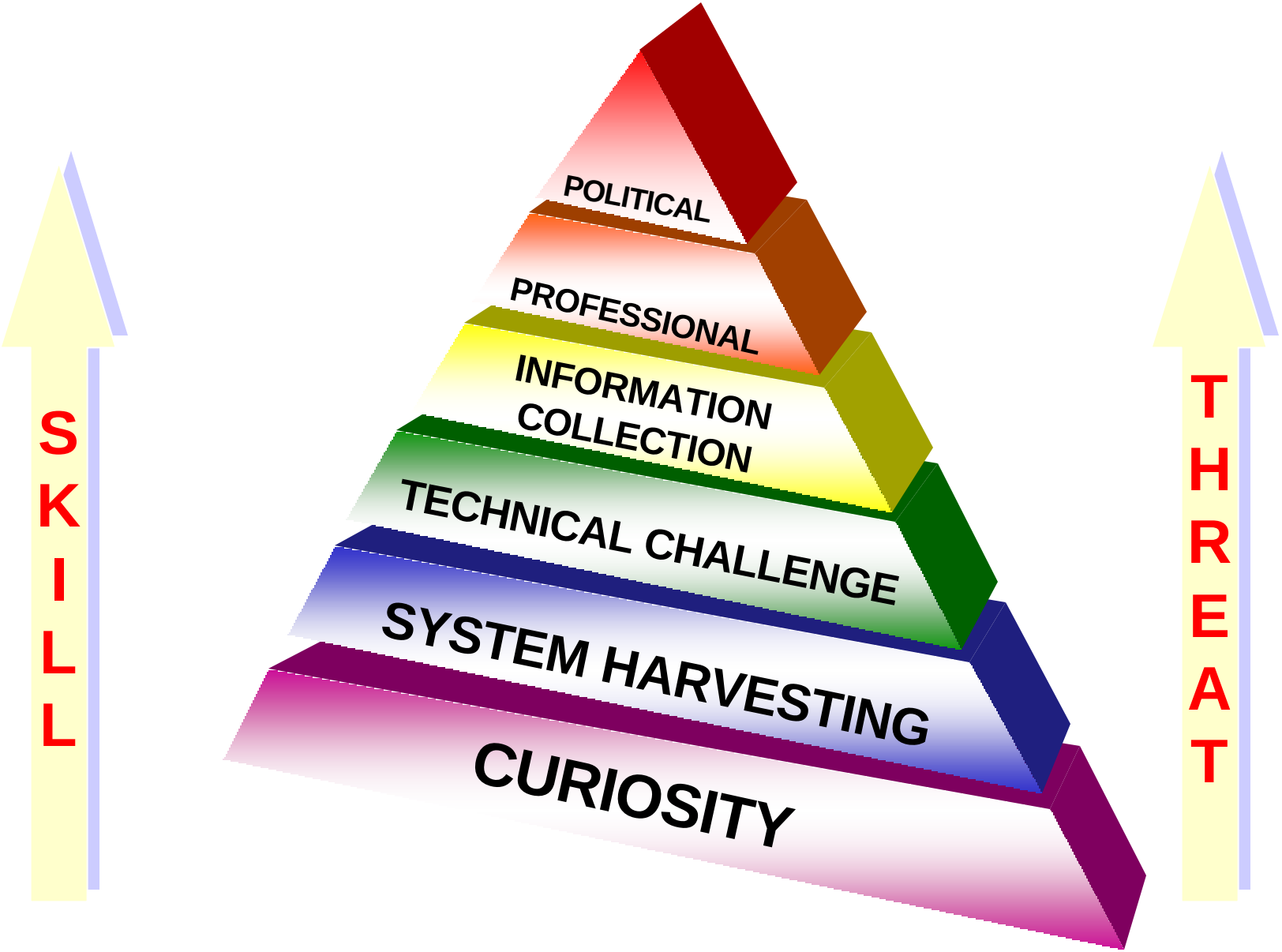
Chris Calvert

Overview

- Motive & Skill
- Reconnaissance
- Vulnerability mapping
- Initial access
- Privileged access
- Covert access

© 2003 IBM Corporation

Hacker Motive &



© 2003 IBM Corporation

Methodology

- Network is specifically targeted
  - Corporate identity / ownership (ibm.com)
  - Associated with identity / cause

Or

- Network is target of opportunity
  - Identified by automated tools
  - Vulnerable
  - Purely random

© 2003 IBM Corporation

Target Reconnaissance

- Open source information
- Internet technology
  - Passive
  - Active
- Usenet (System Admins)

© 2003 IBM Corporation

Internet Technology

- DNS / nslookup
- Whois

} **Passive**

- Traceroute

- Finger, showmount, rpcinfo, xdpyinfo
- Ping mapping
- Port scanners (nmap)
- Vulnerability Scanners

} **Active**

© 2003 IBM Corporation

Automated Attacks

- The rate of attack is increasing:
  - MTTA ranges from 45 sec to 24 hours
  - Average MTTA ***1 hour!***
- The big three defences:
  - Firewalls
  - Intrusion Detection Systems
  - Security Auditors

Essential, but have to audit in real-time!

© 2003 IBM Corporation

DNS Network Tools

whois -h whois.arin.net NETBLK-EC17-1-YAHOO1

whois -h whois.arin.net NETBLK-EC17-1-YAHOO1

```
Yahoo (NETBLK-EC17-1-YAHOO1)
   3420 Central Expressway
   Santa Clara, CA 95051
   US

   Netname: EC17-1-YAHOO1
   Netblock: 64.58.76.0 - 64.58.79.255
   Maintainer: YHOO

   Coordinator:
      Balling, Derek  (DB1428-ARIN)  tech-contact@yahoo-inc.com
      +1-408-530-5062

   Domain System inverse mapping provided by:

   NS1.YAHOO.COM 204.71.200.33
   NS5.DCX.YAHOO.COM 216.32.74.10

   Record last updated on 13-Dec-2000.
   Database last updated on  17-Jan-2002 19:56:07 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```


© 2003 IBM Corporation

Traceroute

USFPTU2 - SecureCRT

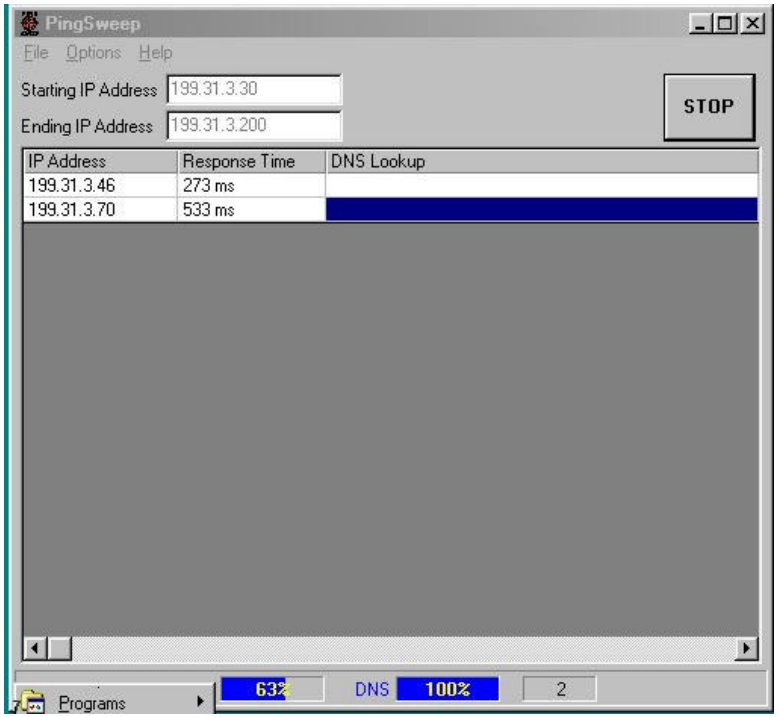
File Edit View Options Transfer Script Window Help

```
[calvert@usfptu2 calvert]$ traceroute www.yahoo.com
traceroute: Warning: www.yahoo.com has multiple addresses; using 64.58.76.223
traceroute to www.yahoo.akadns.net (64.58.76.223), 30 hops max, 38 byte packets
 1  204.146.27.17 (204.146.27.17)  0.312 ms  0.260 ms  0.229 ms
 2  204.146.27.2 (204.146.27.2)  1.229 ms  1.094 ms  1.111 ms
 3  207.25.252.129 (207.25.252.129)  1.790 ms  0.803 ms  0.725 ms
 4  den-edge-20.inet.qwest.net (63.145.64.33)  1.778 ms  1.801 ms  1.671 ms
 5  den-core-02.tamerica.net (205.171.16.41)  1.813 ms  1.655 ms  1.617 ms
 6  sea-core-01.tamerica.net (205.171.8.82)  31.686 ms  31.793 ms  31.785 ms
 7  p5-0.sttlwa1-cr1.bbnplanet.net (4.25.88.1)  58.150 ms  57.870 ms  58.319 ms
 8  p0-0.snjpca1-br2.bbnplanet.net (4.24.4.178)  57.925 ms  57.792 ms  57.918 ms
 9  p1-0.snjpca1-cr2.bbnplanet.net (4.24.9.146)  57.950 ms  57.945 ms  58.153 ms
10  p0-0.exocom13.bbnplanet.net (4.24.234.138)  58.746 ms  58.890 ms  58.747 ms
11  bbr01-g6-1.snva02.exodus.net (64.15.160.145)  46.431 ms  46.386 ms  46.467 ms
12  bbr01-p3-0.sntc05.exodus.net (216.32.132.17)  73.867 ms  73.794 ms  73.932 ms
13  bbr02-p1-0.stng02.exodus.net (209.185.9.114)  91.883 ms  91.940 ms  91.962 ms
14  bbr02-p5-0.stng01.exodus.net (209.185.9.1)  93.128 ms  92.626 ms  92.581 ms
15  dcr03-g10-0.stng01.exodus.net (216.33.96.161)  92.549 ms  93.294 ms  92.728 ms
16  csr22-ve243.stng01.exodus.net (216.33.98.26)  93.151 ms  93.078 ms  93.292 ms
17  216.35.210.126 (216.35.210.126)  93.755 ms  93.024 ms  93.844 ms
18  w2.dcx.yahoo.com (64.58.76.223)  92.012 ms  92.083 ms  91.990 ms
[calvert@usfptu2 calvert]$
```

Ready | ssh2: 3DES | 30, 28 | 36 Rows, 87 Cols | Linux | NUM

Scanners

- Port Scanners
  - Port (stealth)
  - Ping map
  - Nmap
- Vulnerability Scanners
  - ISS
  - Nessus
  - Arirang



© 2003 IBM Corporation

Usenet

From: Urbans
Topic: Re: Secure FTP
Message: 1 of 3
Sent: Wed, 11 Aug 1999 19:50:45 -0700
See Also: Linux Networking OS

In article <7n988v$hk4$1@nnrp1.deja.com>, Greg.Drake@ramstein.af.mil wrote:

> *Is anyone aware of a Secure FTP server for Linux? Sent via Deja.com http://www.deja.com/ Share what you know. Learn what you don't.*

I remember there being something on the ssh site (www.ssh.org I think) about something called sftp. I don't know if there is an sftpd or not.

Nick Urban

Reply to this message

From: Andy
Topic: SecureFTP
Message: 2 of 3
Sent: Fri, 22 Oct 1999 10:26:57 -0400
See Also: Linux Networking OS

Hi all,

I've got ssh2 setup nicely on my linux box, and i want to allow only secure telnet and ftp. ssh2 comes with an sftp client for connection to an ssh server for ftp, but i can't seem to find any clients for windows...i'd really like to seal off unencrypted ftp and telnet but i can't unless i can direct the people that need to connect to a secure client. Any one know of any?

Thanks Andy

Reply to this message

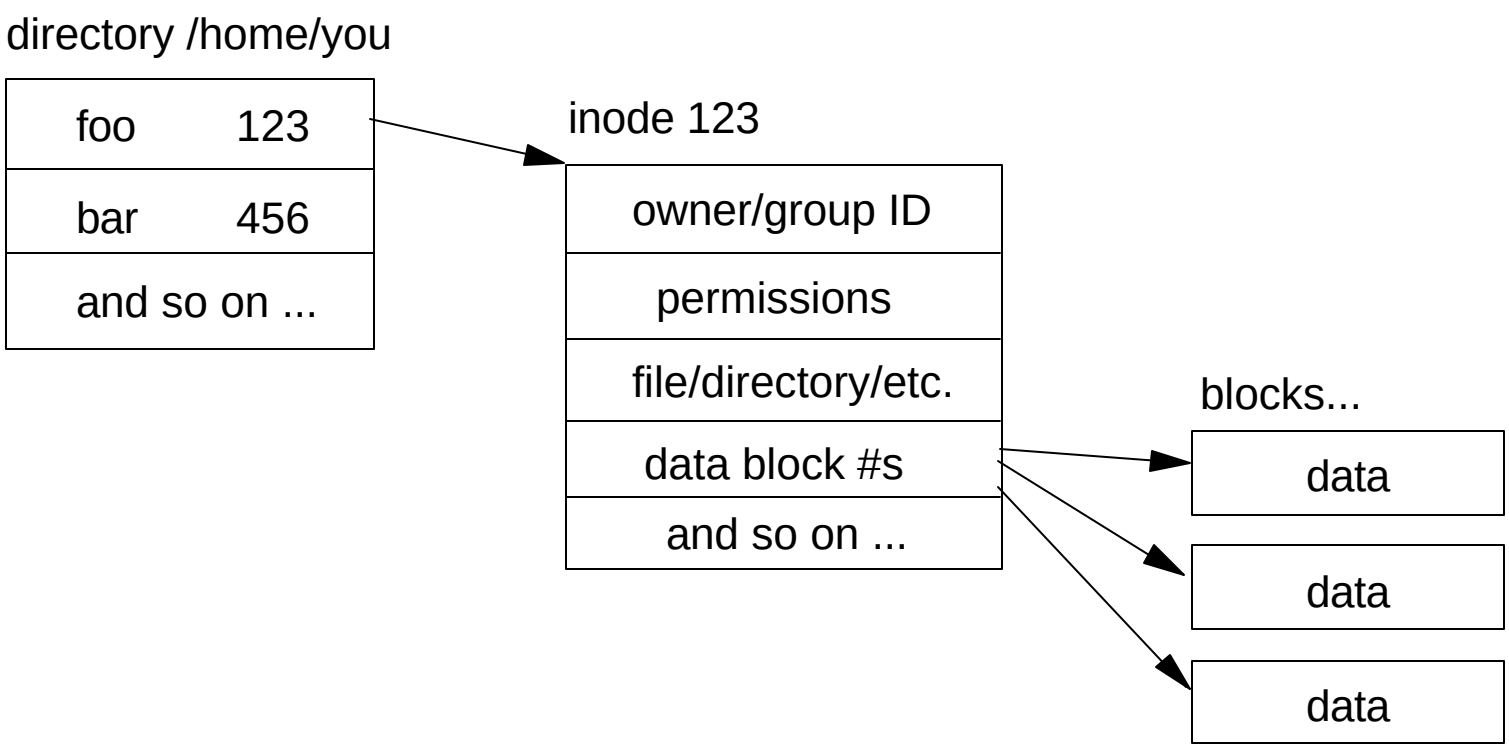
© 2003 IBM Corporation

IBM Global Services

File System

© 2003 IBM Corporation

UNIX File System Basics



© 2003 IBM Corporation

UNIX File Types

- Regular file (most files)
- Directory (a file)
- Symbolic link (alias for a file)
- Device (terminal, disk, memory)
- Inter-process communication: named pipe, socket

© 2003 IBM Corporation

UNIX file attributes

- Ownership: numeric user and group ID
- Permissions: R/W/X for owner, group, other
- Type: file, directory, symlink, device, etc.
- Reference count (0,1,2, etc.)
- File size in Bytes
- Time stamps (MAC times):

  last file Modification time

  last file Access time

  last status Change

© 2003 IBM Corporation

Unusual File System Properties

- Everything is placed in 1 logical tree.
- Devices are accessible through file system
- Directories are files (user can't write)
- File names can contain anything but / and null
- Files may contain "holes" (no data is written - read back as all zero blocks)

© 2003 IBM Corporation

Unusual File System Properties - continued

- Multiple references / multiple places
- Zero references - file exists after removal
- Zero link file is deleted when closed
- No built-in undelete provision like MSDOS
- Typically, only 0.5KB of wasted space at the end of a file

© 2003 IBM Corporation

IBM Global Services

Anatomy of an Attack

© 2003 IBM Corporation

Fidelity

Increasing Fidelity

Assessment	Incident
	Situation Assessment
	Threat Assessment
Data Relation	Data Mining
	Consolidation
	Correlation
Data Manipulation	Normalization
	Filtering
	Collection

© 2003 IBM Corporation

TCP Wrapper-style alert

- Activity at some unlikely hour

  Feb 9 03:56:17 wilma in.rlogind[2271]:connect from joe@betty

- Email inquiry:

  Joe was not working at 3 AM

- An intruder has compromised Joe's account ... and possibly more.

© 2003 IBM Corporation

Sign of trouble - no login record

- No login record

  % last | more sergey ttyp1 barney Wed Feb 8 16:45 -16:45

  rob ttyp1 freddy Wed Feb 8 09:08 -09:08

-
- Either no login record was written - entrance via backdoor, or
- The record was wiped out

© 2003 IBM Corporation

Some traces in file access times

- Output from "ls -lautR /"
- - massaged and sorted by time

```
03:50:53   1422 -r--r--r-- root /usr/include/setjmp.h
03:53:26 344586 -r-xr-xr-x root /usr/lib/ccom
03:53:33 221215 -r-xr-xr-x root /usr/bin/as
03:53:36 303617 -r-xr-xr-x root /usr/bin/ld
```

- Look for unusual things like compiling code

© 2003 IBM Corporation

Results so far - not a whole lot

- Wrapper alert - Joe's account compromised
- "ls" access times - find intruder built and installed software
- "ls" modification times - no new or modified files
- "ps" output - no new or unusual processes

  % ps -aux
- Time for more drastic measures

© 2003 IBM Corporation

Finding a good baseline

- Purpose: to find out what has changed relative to some "known to be good" state
- Questions for different levels of desperation:

  How useful are the backups?

  Is a similarly configured machine available?

  Are system and application installation media available?

© 2003 IBM Corporation

Unmistakable rootkit signature

- "find / -type f -print | xargs md5 >file"

  finds trojan versions of:

du	(hide sniffer, logs and config files)
ifconfig	(hide sniffer activity)
login	(backdoor)
ls	(hide sniffer, logs and config files)
netstat	(hide intruder network connections)
ps	(hide sniffer processes)

- Plus config files, programs and a network sniffer log with login/passwd information.

© 2003 IBM Corporation

Hacker Tools

- Tools can make even unsophisticated intruders smart. Smart enough to:
  - exploit a vulnerability
  - wipe their login record
  - install Trojan Horses and viruses
- Tools do not stop intruders from making unsophisticated mistakes, such as leaving a trail of file access time stamps or stumbling over tripwires

© 2003 IBM Corporation

IBM Global Services

Logs & Searching

© 2003 IBM Corporation

Worth a thousand words. ..

```
Sep 2500:44:49 dionysis rpc.statd[335] :
gethostbyname error for
AX?X?Y?Y?Z?Z?[?[?ffff750
80497101b06874656762747 36f6d616e7972652
06520726f7220726f66
```


© 2003 IBM Corporation

Frankenstein Effect

- Goal – reanimation
- Complete dynamic state -processes, disk, network. ...
- Like the book -fiction
- Only very low-rez

© 2003 IBM Corporation

Logs -even bigger problems

- Turned off – by vendors and by users
- Enormous space required for larger systems even for minimal logging
  - Earthlink in the gigabytes/day;
- Rotation, destruction, and no backups

© 2003 IBM Corporation

Binary Logs

- Must use specialized software
- Difficult to write tools
- What you see is all you get
- Versions -data, viewers, OS, time of year
- Meanings change from host to host
- Unexploded munitions -side effects of reading arbitrary data into a program

© 2003 IBM Corporation

E.g. - a system login

Syslog -

```
Aug 19' 17:12:42 foo telnetd[666] :
connection from "10.6.6.6"
```

Last -

```
matt ttypO 10.6.6.1 Fri Oct 5 13:46 - 13:46 (00:00)
zen pts/O 10.6.6.2 Fri Oct 5 12:47 still logged in
```

lastcomm -

```
telnet root ttyp2 0.01 secs Fri Oct 5  11:12
```

Post-mortem analysis -overview

- What was logged.
- Chronological analysis of
  - What files were accessed.
  - What files were modified.
  - What deleted file information is available

© 2003 IBM Corporation

What was logged

A scream of agony in the middle of the night:

```
Sep 25 00:44:49 dionysisrpc.statd[335]: gethostbyname error for
[a very long non-conformant hostname. ..]
Sep 25 00:45:16 dionysisinetd[473]: extra conf for service te1net/tcp
(skipped)
Sep 25 00:45:28 dionysisin.te1netd[11554]: connect from 10.83.81.7
Sep 25 01:02:02 dionysisinetd[473]: pid 11554: exit status 1
Sep 25 17:31:47 dionysisin.telnetd[12031]: connect from 10.83.81.7
Sep 25 17:32:08 dionysisin.telnetd[12035]: connect from 10.83.81.7
```

(IP address information changed to protect the guilty)

© 2003 IBM Corporation

What was accessed, part 1/2

```
sep 25 2000 00:45:15
    size  mac permission  ownership       file name
   207600 .a. -rwx-xr-x   root    root    /image/usr/bin/as
    63376 .a. -rwxr-xr-x  root    root    /image/usr/bin/egcs
    63376 .a. -rwxr-xr-x  root    root    /image/usr/bin/gcc
    63376 .a. -rwxr-xr-x  root    root    /image/usr/bin/i386-redhat-1inux-gcc
     2315 .a. -rw-r--r-   root    root    /image/usr/include/_G_config.h
     1297 .a. -rw-r--r-   root    root    /image/usr/include/bits/stdio-1im.h
     4680 .a. -rw-r--r-   root    root    /image/usr/include/bits/types.h
     9512 .a. -rw-r--r-   root    root    /image/usr/include/features.h
     1021 .a. -rw-r--r-   root    root    /image/usr/include/gnu/stubs.h
    11673 .a. -rw-r--r--  root    root    /image/usr/include/1ibio.h
    20926 .a. -rw-r--r--  root    root    /image/usr/include/stdio.h
     4951 .a. -rw-r--r--  root    root    /image/usr/include/sys/cdefs.h
  1440240 .a. -rwxr-xr-x  root    root    /image/usr/1ib/gcc-lib{[...]/cc1
    45488 .a. -rwxr-xr-x  root    root    /image/usr/1ib/gcc-lib/[...]/collect.2
    87312 .a. -rwxr-xr-x  root    root    /image/usr/lib/gcc-lib/[...]/cpp
     5794 .a. -rw-r--r--  root    root    /image/usr/lib/gcc-
lib/[...]/include/stdarg.h
     9834 .a. -rw-r--r--  root    root    /image/usr/liblgcc-
lib/[...]/include/stddef.h
```


© 2003 IBM Corporation

What was accessed, part 2/2

```
Sep 252000 00.45,16
Size   mac   permission   ownership   file name
  1926 .a.   -rw-----     root  root  /image/us~/lib/gcc-lib/[...]/specs
205136 .a.   -rwxr-xr-x   root  root  /image/usr/bin/ld
176464 .a.   -rwxr-xr-x   root  root  /image/usr/bin/strip
  8512 .a.   -rw---r--    root   root /image/usr/lib/crt.1.o
  1124 .a.   -rw-r--r--   root  root  /image/usr/1ib/crti.o
   874 .a.   -rw-r--r--   root  root  /image/usr/lib/crtn.o
  1892 .a.   -rw-r--r--   root  root  /image/usr/lib/gcc-lib/[...]/crtbegin.o
  1424 .a.   -rw-r--r--   root  root  /image/usr/lib/gcc-lib/[...]lcrtend.o
769892 .a.   -rw-r--r--   root  root  /image/usr/lib/gcc-lib/[...]/libgcc.a
314936 .a.   -rwxr-xr-x   root  root  /image/usr/lib/libbfd-2.9.5.0.22.so
   178 .a.   -rw-r--r--   root  root  /image/usr/lib/libc.so
 69994 .a.   -rw-r--r--   root root   /image/usr/lib/libc_nonshared.a
     (m=modified, a=read access, c=status change)
```

Conclusion: intruder compiled simple C program.

© 2003 IBM Corporation

Modifications to existing files

```
Sep 25 2000 00:45:16
Size   mac  permission ownersbip    file name
   0   m.c  -rw-r--r-- root   root   /image/etc/hosts.allow
   0   m.c  -rw-r--r-- root   root   /image/etc/hosts.deny
3094   mac  -rw-r--r-- root   root   /image/etc/inetd.conf
      (m=modifed. a=read access, c=status change)
```

- Duplicate telnet service entry in inetd.conf.
- TCP Wrapper remote access control turned off.
- Suspicion: intruder configured a backdoor .

© 2003 IBM Corporation

Two new files: brick, xstat

- Not part of the RedHat 6.2 Linux distribution:

```
date and time            size  mac permission ownership   file name
Sep 25  2000  00:45:15  20452 m.c -rwxr-xr-x root root  /image/bin/brick
Sep 25  2000  00:45:16   3448 m.. -rwxr-xr-x root root  /image/usr/bin/xstat
```

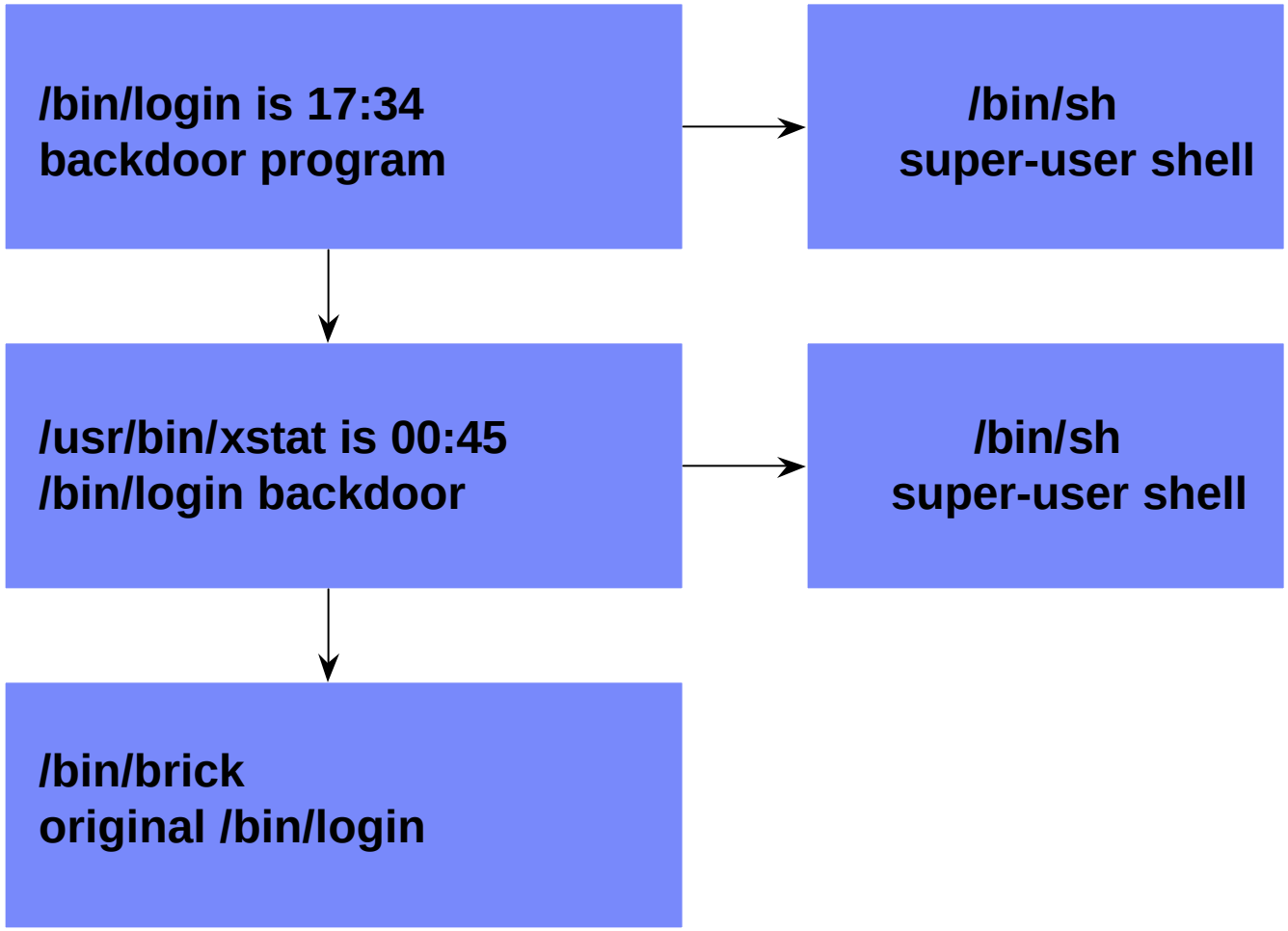
- /bin/brick is copy of RedHat 6.2 Linux /bin/login.
- What about the present /bin/login program ?

```
date and time              size mac  permission ownership  file name
Sep  25   2000 17:34:17    3448 ..c  -rwxr-xr-x root root  /image/usr/bin/xstat
Sep  25   2000 17:34:20  302207 ..c  -rwxr-xr-x root root  /image/bin/login
```

- /usr/bin/xstat is 00:45:16 login backdoor program.
- /bin/login is yet another login backdoor program.

© 2003 IBM Corporation

Login backdoor upon backdoor



© 2003 IBM Corporation

Deleted file analysis part 1/2

```
date and time          size mac permission ownership disk inode
Mar 07 2000 04:29:44 20452 m.. -rwxr-xr-x root root <image.hda8-30199>
Sep 25 2000 00:45:15 20452 .a. -rwxr-xr-x root root <image.hda8-30199>
Sep 25 2000 00:45.16 20452 ..c -rwxr-xr-x root root <image.hda8-30199>
```

Deleted file 30199 recovered with icat[1] is original /bin/login file. It even has the right inode number:

```
$ ls -fli /image/bin
...skipped...
inode permission ref ownership size last modify name
30197 -rwxr-xr-x   1 root root  4016 Mar 7 2000 dmesg
30198 -rwxr-xr-x   1 root root  7952 Mar 7 2000 kill
60257 -rwxr-xr-x   1 root root 12207 Aug 18 2000 login    backdoor:
30200 -rwxr-xr-x   1 root root 23600 Mar 7 2000 more
30201 -rwxr-xr-x   1 root root   362 Mar 7 2000 vimtutor
```

[l]Access file content by inode number, from the Coroner's Toolkit.

© 2003 IBM Corporation

Deleted file analysis part 2/2

Deleted files with inode numbers 22111-22113 were tentatively identified with fls[1] :

```
Sap 25 2000 00:45:16
size mac permission ownership file name            inode   comment:
0 mac -rw-r--r-- root root /image/tmp/ccpX2iab.ld <22113> (deleted)
0 mac -rw------  root root /image/tmp/cWxNYYa.o   <22112> (deleted)
0 mac -rw------  root root /image/tmp/ccXJHPza.c  <22111> (deleted)
```

Deleted file names are typical for compiler and linker temporary files.

Look at the file permissions. What is wrong here?

[1]List (deleted) directory entries, from the TCTutils software. ,

© 2003 IBM Corporation

Clues found so far

00:44:49 Break-in with rpc.statd exploit.
00:45:15 Relatively small program compiled.
00:45:16 First login backdoor installed. Original /bin/login program copied to /bin/brick.
00:45:16 Truncated hosts.allow/deny files.
00:45:16 Duplicate telnet service configured.
00:45:28, 17:31:47, 17:32:08 Telnet connections.
17:34:20 Second login backdoor installed. First login backdoor renamed to /usr/bin/xstat.

© 2003 IBM Corporation

No method is an Island

- Start with a time frame
- Must combine tactics to get an answer - Correlation is the key!
- Never will have enough, but could get enough...

© 2003 IBM Corporation

IBM Global Services

Analysis Tools

© 2003 IBM Corporation

Analysis Tools

- General file analysis tools:

  strings - show clear-text strings embedded in any file

  grep - search for specific strings

  file - identify content by looking at part of the data

  Program file analysis tools:

  nm - display compiler and runtime linker symbol table

  ldd - identify dynamic libraries used (can be dangerous)

  disassemblers, debuggers - for the really desperate

© 2003 IBM Corporation

Analysis Tools - continued

- lsof: lists opened by processes
  ftp://vic.cc.purdue.edu/pub/tools/unix/lsof
- ltrace: log every library routine call (output like strace).
  ftp://ftp.debian.org/debian/dists/unstable/main/source/utils/
  Guaranteed portable to SUNs.
- ttywatchers: real-time monitoring and more.
  ftp://coast.cs.purdue.edu/pub/tools/unix/ttywatcher
- tap: hook into streams-based tty systems
  ftp://coast.cs.purdue.edu/pub/tools/unix/ttywatcher
  Guaranteed portable to SUNs.

© 2003 IBM Corporation

Before an Incident

- Have a good security policy
- Learn thy system(s) - education
- Turn on logging and accounting
- Create a baseline
- Regularly audit your systems
- Know how to gather forensic data
- Backup
- Keep up with security patches and tools
- Know who to contact in an emergency

© 2003 IBM Corporation

Coroner's Toolkit (TCT)

- **TCT is a collection of programs that can be used for a post-mortem analysis of a UNIX system after break-in.**

© 2003 IBM Corporation

Coroner's Toolkit (TCT)

- Contents

  grave-robber tool that captures information,

  the ils and mactime tools that display access patterns of files dead or alive,

  the unrm and lazarus tools that recover deleted files, and

  the keyfind tool that recovers cryptographic keys from a running process or from files

© 2003 IBM Corporation

Coroner's Toolkit (TCT)

- **Runs on:**

  SUN Solaris,

  FreeBSD,

  RedHat Linux,

  BSD/OS,

  OpenBSD, and

  even runs on SunOS 4.x.

© 2003 IBM Corporation

Coroner's Toolkit (TCT)

- Where to get it:

  http://www.porcupine.org/forensics/

  http://www.fish.com/forensics/

  ftp://tct.earthlink.net/pub/

© 2003 IBM Corporation

Forensic resources

1. SANS Presentation on Windows Media Imaging
   http://sans.digisle.tv/audiocast_040302/Webcast_040302.pdf
2. Windows Forensic Acquisition Utilities
   http://users.erols.com/gmgarner/forensics/
3. Preservation of Fragile Evidence for First Responders
   http://www.csa.syr.edu/Jesse_Kornblum.pdf (Fred is on the FIRE CD)
4. Forensic and Incident Response Environment
   http://fire.dmzs.com/?section=main
5. Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000
   http://www.sans.org/rr/paper.php?id=647
6. Foundstone Initial Response to Windows NT/2000
   http://www.foundstone.com/pdf/ir-primer.pdf
7. Rob Lee (SANS) UNIX Forensics Techniques for Incident Response
   http://www.incident-response.org/incidentresponse.ppt
   (http://www.incident-response.org)
8. E-Evidence Info
   http://www.e-evidence.info/specific.html (Good resource and links)
9. The Sleuth Kit (Freeware Forensic analysis tools)
   http://www.sleuthkit.org/index.php

© 2003 IBM Corporation

© 2003 IBM Corporation