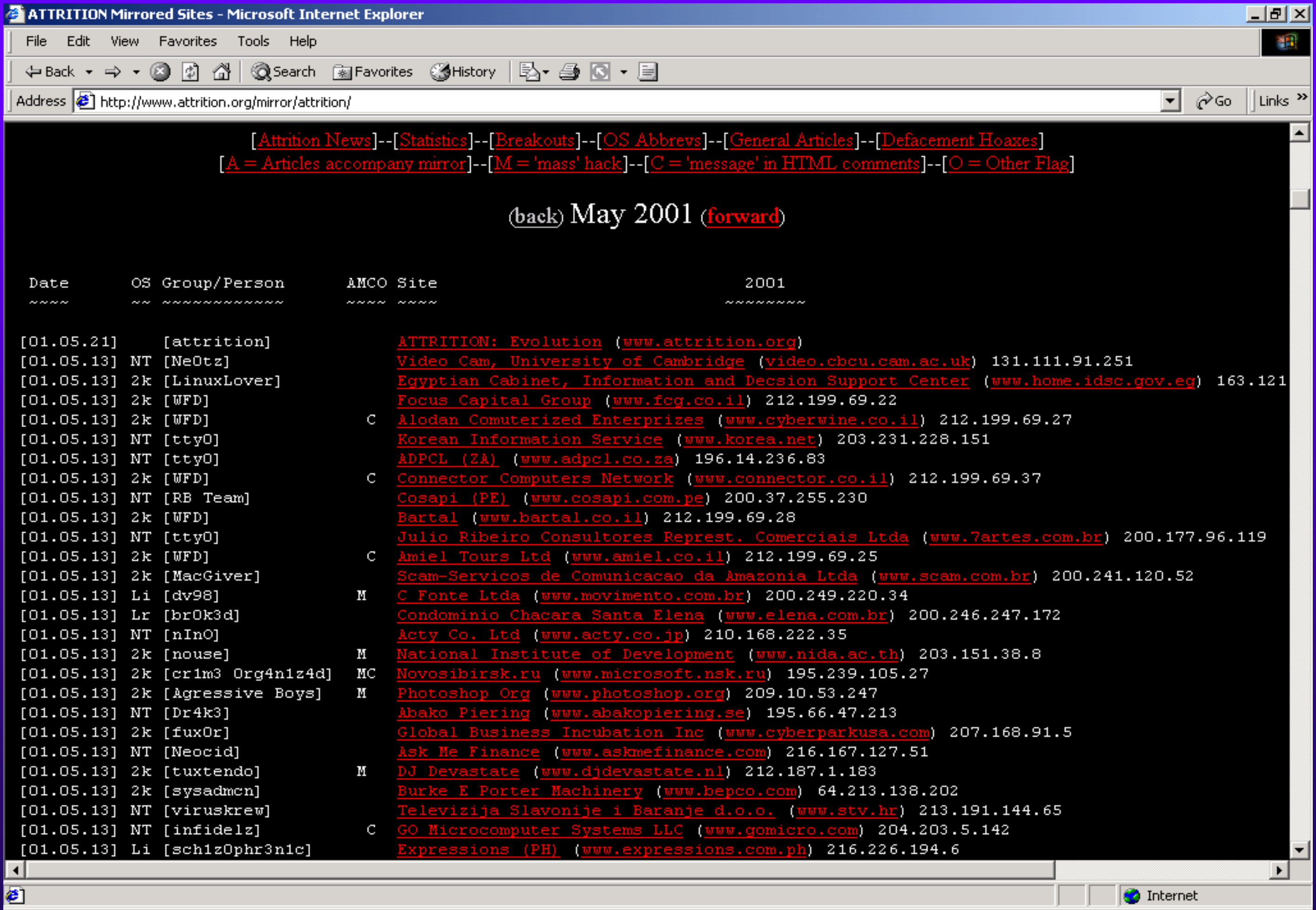
Chapter 11 Phase 5: Covering Tracks and Hiding

Attrition Web Site

- Contains an archive of Web vandalism attacks http://www.attrition.org/mirror/attrition



Address http://www.attrition.org/mirror/attrition/

[Attrition News]--[Statistics]--[Breakouts]--[OS Abbrevs]--[General Articles]--[Defacement Hoaxes]
[A = Articles accompany mirror]--[M = 'mass' hack]--[C = 'message' in HTML comments]--[O = Other Flag]

(back) May 2001 (forward)

```
 Date       OS Group/Person       AMCO Site                                  2001
 ~~~~       ~~ ~~~~~~~~~~~~~      ~~~~ ~~~~                                ~~~~~~~~

[01.05.21]     [attrition]             ATTRITION: Evolution (www.attrition.org)
[01.05.13] NT [Ne0tz]                  Video Cam, University of Cambridge (video.cbcu.cam.ac.uk) 131.111.91.251
[01.05.13] 2k [LinuxLover]             Egyptian Cabinet, Information and Decsion Support Center (www.home.idsc.gov.eg) 163.121
[01.05.13] 2k [WFD]                    Focus Capital Group (www.fcg.co.il) 212.199.69.22
[01.05.13] 2k [WFD]                 C  Alodan Comuterized Enterprizes (www.cyberwine.co.il) 212.199.69.27
[01.05.13] NT [tty0]                   Korean Information Service (www.korea.net) 203.231.228.151
[01.05.13] NT [tty0]                   ADPCL (ZA) (www.adpcl.co.za) 196.14.236.83
[01.05.13] 2k [WFD]                 C  Connector Computers Network (www.connector.co.il) 212.199.69.37
[01.05.13] NT [RB Team]                Cosapi (PE) (www.cosapi.com.pe) 200.37.255.230
[01.05.13] 2k [WFD]                    Bartal (www.bartal.co.il) 212.199.69.28
[01.05.13] NT [tty0]                   Julio Ribeiro Consultores Represt. Comerciais Ltda (www.7artes.com.br) 200.177.96.119
[01.05.13] 2k [WFD]                 C  Amiel Tours Ltd (www.amiel.co.il) 212.199.69.25
[01.05.13] 2k [MacGiver]               Scam-Servicos de Comunicacao da Amazonia Ltda (www.scam.com.br) 200.241.120.52
[01.05.13] Li [dv98]               M   C Fonte Ltda (www.movimento.com.br) 200.249.220.34
[01.05.13] Lr [br0k3d]                 Condominio Chacara Santa Elena (www.elena.com.br) 200.246.247.172
[01.05.13] NT [nIn0]                   Acty Co. Ltd (www.acty.co.jp) 210.168.222.35
[01.05.13] 2k [nouse]              M   National Institute of Development (www.nida.ac.th) 203.151.38.8
[01.05.13] 2k [cr1m3 Org4n1z4d]    MC  Novosibirsk.ru (www.microsoft.nsk.ru) 195.239.105.27
[01.05.13] 2k [Agressive Boys]     M   Photoshop Org (www.photoshop.org) 209.10.53.247
[01.05.13] NT [Dr4k3]                  Abako Piering (www.abakopiering.se) 195.66.47.213
[01.05.13] 2k [fux0r]                  Global Business Incubation Inc (www.cyberparkusa.com) 207.168.91.5
[01.05.13] NT [Neocid]                 Ask Me Finance (www.askmefinance.com) 216.167.127.51
[01.05.13] 2k [tuxtendo]           M   DJ Devastate (www.djdevastate.nl) 212.187.1.183
[01.05.13] 2k [sysadmcn]               Burke E Porter Machinery (www.bepco.com) 64.213.138.202
[01.05.13] NT [viruskrew]              Televizija Slavonije i Baranje d.o.o. (www.stv.hr) 213.191.144.65
[01.05.13] NT [infidelz]            C  GO Microcomputer Systems LLC (www.gomicro.com) 204.203.5.142
[01.05.13] Li [sch1z0phr3n1c]          Expressions (PH) (www.expressions.com.ph) 216.226.194.6
```

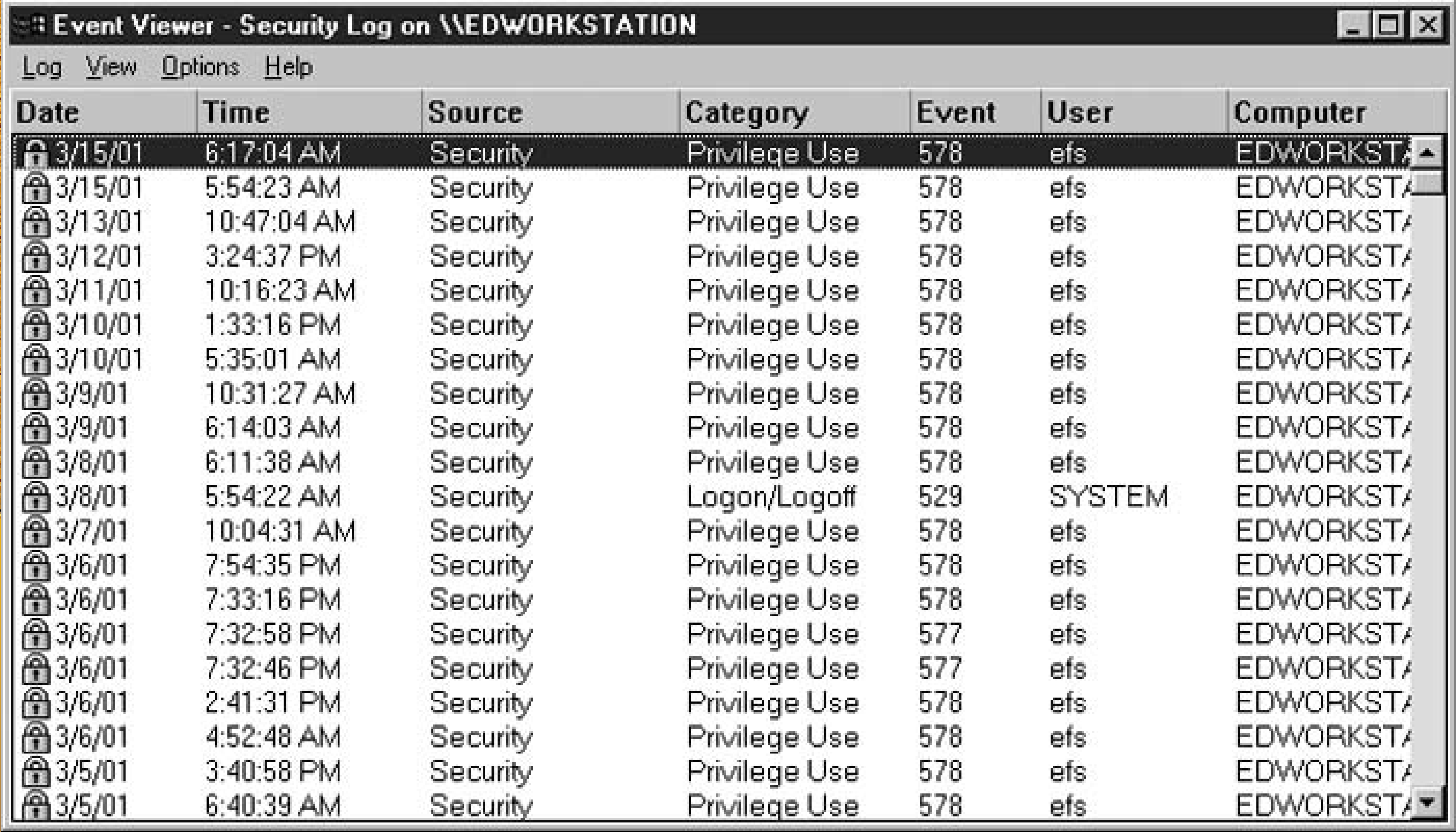
- Most attackers, however, wish to keep low profile

Hiding Evidence by Altering Event Logs

- Attackers like to remove evidence from logs associated with attacker’s gaining access, elevating privileges,and installing RootKits and backdoors
  - Login records
  - Stopped and restarted services
  - File access/update times

Event Logging in Windows NT/2000

- Security-related events such as failed login attempts or failed access to files are stored in file SecEvent.Evt
- System events such as inability in starting a system service are stored in file SysEvent.Evt
- Application events related to applications such as databases or web servers are stored in file AppEvent.Evt



Event Viewer - Security Log on \\EDWORKSTATION

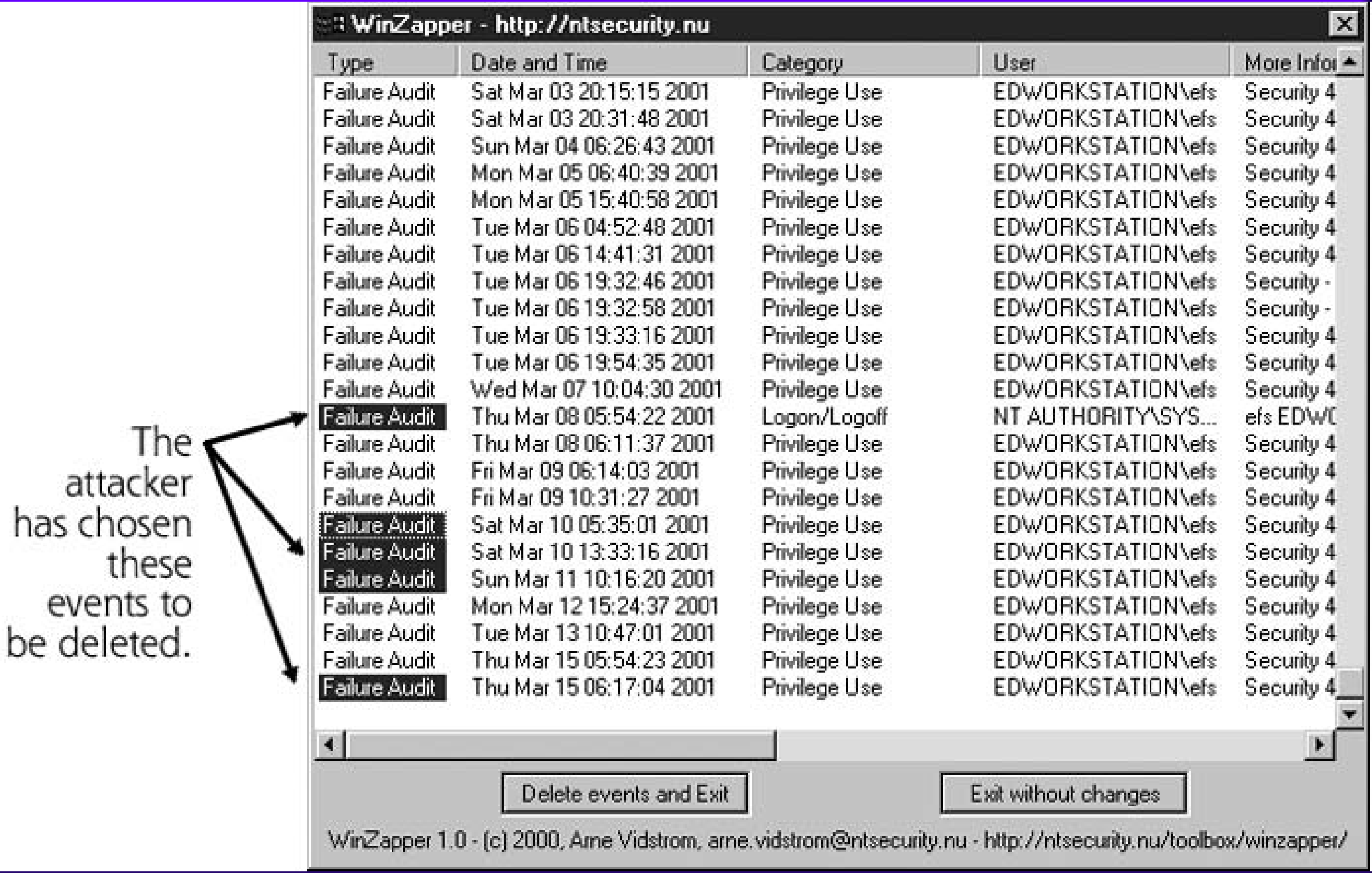
Date	Time	Source	Category	Event	User	Computer
3/15/01	6:17:04 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/15/01	5:54:23 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/13/01	10:47:04 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/12/01	3:24:37 PM	Security	Privilege Use	578	efs	EDWORKSTA
3/11/01	10:16:23 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/10/01	1:33:16 PM	Security	Privilege Use	578	efs	EDWORKSTA
3/10/01	5:35:01 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/9/01	10:31:27 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/9/01	6:14:03 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/8/01	6:11:38 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/8/01	5:54:22 AM	Security	Logon/Logoff	529	SYSTEM	EDWORKSTA
3/7/01	10:04:31 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/6/01	7:54:35 PM	Security	Privilege Use	578	efs	EDWORKSTA
3/6/01	7:33:16 PM	Security	Privilege Use	578	efs	EDWORKSTA
3/6/01	7:32:58 PM	Security	Privilege Use	577	efs	EDWORKSTA
3/6/01	7:32:46 PM	Security	Privilege Use	577	efs	EDWORKSTA
3/6/01	2:41:31 PM	Security	Privilege Use	578	efs	EDWORKSTA
3/6/01	4:52:48 AM	Security	Privilege Use	578	efs	EDWORKSTA
3/5/01	3:40:58 PM	Security	Privilege Use	578	efs	EDWORKSTA
3/5/01	6:40:39 AM	Security	Privilege Use	578	efs	EDWORKSTA

Figure 11.1 Windows NT Event Viewer

Altering Event Logs in Windows NT/2000

- opening or editing event log files cannot be done with a standard file editing tool
- Deleting event log files possible but may cause suspicion
- WinZapper tool allows attacker to selectively delete security events

  http://ntsecurity.nu/toolbox/winzapper



WinZapper - http://ntsecurity.nu

Type	Date and Time	Category	User	More Infoi
Failure Audit	Sat Mar 03 20:15:15 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Sat Mar 03 20:31:48 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Sun Mar 04 06:26:43 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Mon Mar 05 06:40:39 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Mon Mar 05 15:40:58 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Tue Mar 06 04:52:48 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Tue Mar 06 14:41:31 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Tue Mar 06 19:32:46 2001	Privilege Use	EDWORKSTATION\efs	Security -
Failure Audit	Tue Mar 06 19:32:58 2001	Privilege Use	EDWORKSTATION\efs	Security -
Failure Audit	Tue Mar 06 19:33:16 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Tue Mar 06 19:54:35 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Wed Mar 07 10:04:30 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Thu Mar 08 05:54:22 2001	Logon/Logoff	NT AUTHORITY\SYS...	efs EDW(
Failure Audit	Thu Mar 08 06:11:37 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Fri Mar 09 06:14:03 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Fri Mar 09 10:31:27 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Sat Mar 10 05:35:01 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Sat Mar 10 13:33:16 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Sun Mar 11 10:16:20 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Mon Mar 12 15:24:37 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Tue Mar 13 10:47:01 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Thu Mar 15 05:54:23 2001	Privilege Use	EDWORKSTATION\efs	Security 4
Failure Audit	Thu Mar 15 06:17:04 2001	Privilege Use	EDWORKSTATION\efs	Security 4

WinZapper 1.0 - (c) 2000, Arne Vidstrom, arne.vidstrom@ntsecurity.nu - http://ntsecurity.nu/toolbox/winzapper/

The attacker has chosen these events to be deleted.

Figure 11.2 WinZapper tool lets an attacker selectively delete events from Windows NT/2000 event logs

Altering System Logs in Unix

- Unix log files are stored in files specified in /etc/syslog.conf (eg. /var/adm/messages)
- Attackers can alter log files via editors such as vi or emacs

Altering Accounting Files in Unix

- utmp, wtmp, and lastlog files are the main accounting files in Unix
  - Written in special binary format
  - Can be edited using tools such as remove, wtmped, marry, cloak, logwedit, wzap, and zapper
    - http://ftp.technotronic.com/unix/log-tools
    - Tools included in RootKits

Unix Shell History Files

- stores a complete list of all commands entered by the user at the Unix command prompt
- Usually stored in users’ home directories
- Attacker may configure the length of the shell history file to be zero but may raise suspicion
- Careful attacker will remove unwanted lines from the history file via ASCII editor

Defenses for Log and Accounting File Attacks

- Activate logging on your critical systems
- Set proper permissions on the log files, utmp, wtmp, lastlog, and users’ shell history files
- Setup a a separate logging server
  - Add line “syslog 514/udp” to /etc/services on logging server
  - Modify /etc/syslog.conf on critical server to redirect desired message types to logging server
  - Hostname and IP address of logging server should be added to /etc/hosts on critical server to thwart DNS attack
  - In Windows NT/2000, replace EventLog service with an NT-compatible version of syslog to centralize logging
    - Kiwi syslog for NT http://www.kiwi-enterprises.com

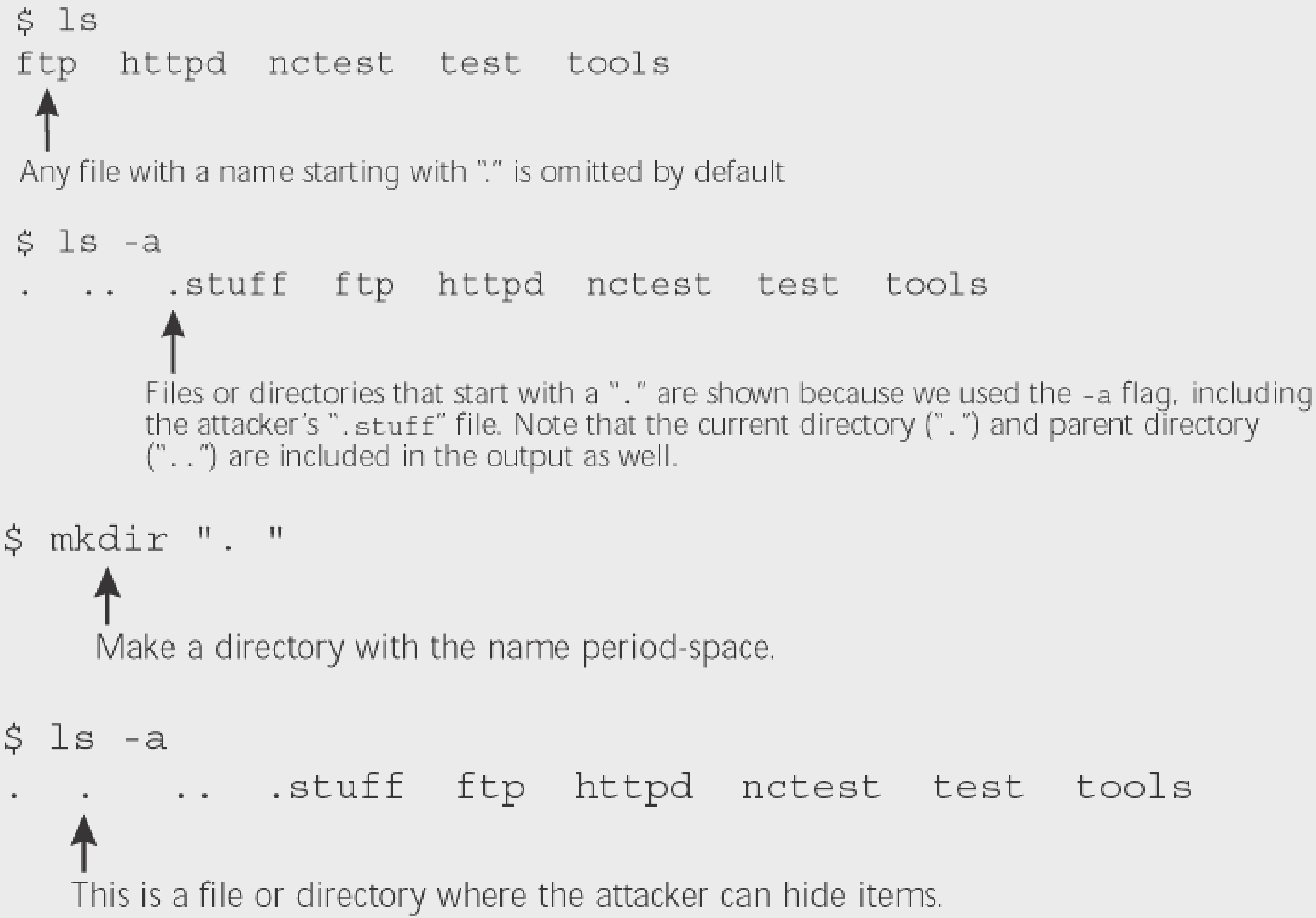
Defenses for Log and Accounting File Attacks (cont.)

- Encrypt log files http://www.core-sdi.com/english/freesoft.html
- On Linux systems, make log files append only

```
$ chattr   +a   [log_filename]
```

- Store logs on write-once media such as CD-ROM

Creating Hidden Files and Directories in UNIX



```
$ ls
ftp  httpd  nctest  test  tools
```

Any file with a name starting with "." is omitted by default

```
$ ls -a
.  ..  .stuff  ftp  httpd  nctest  test  tools
```

Files or directories that start with a "." are shown because we used the -a flag, including the attacker's ".stuff" file. Note that the current directory (".") and parent directory ("..") are included in the output as well.

```
$ mkdir ". "
```

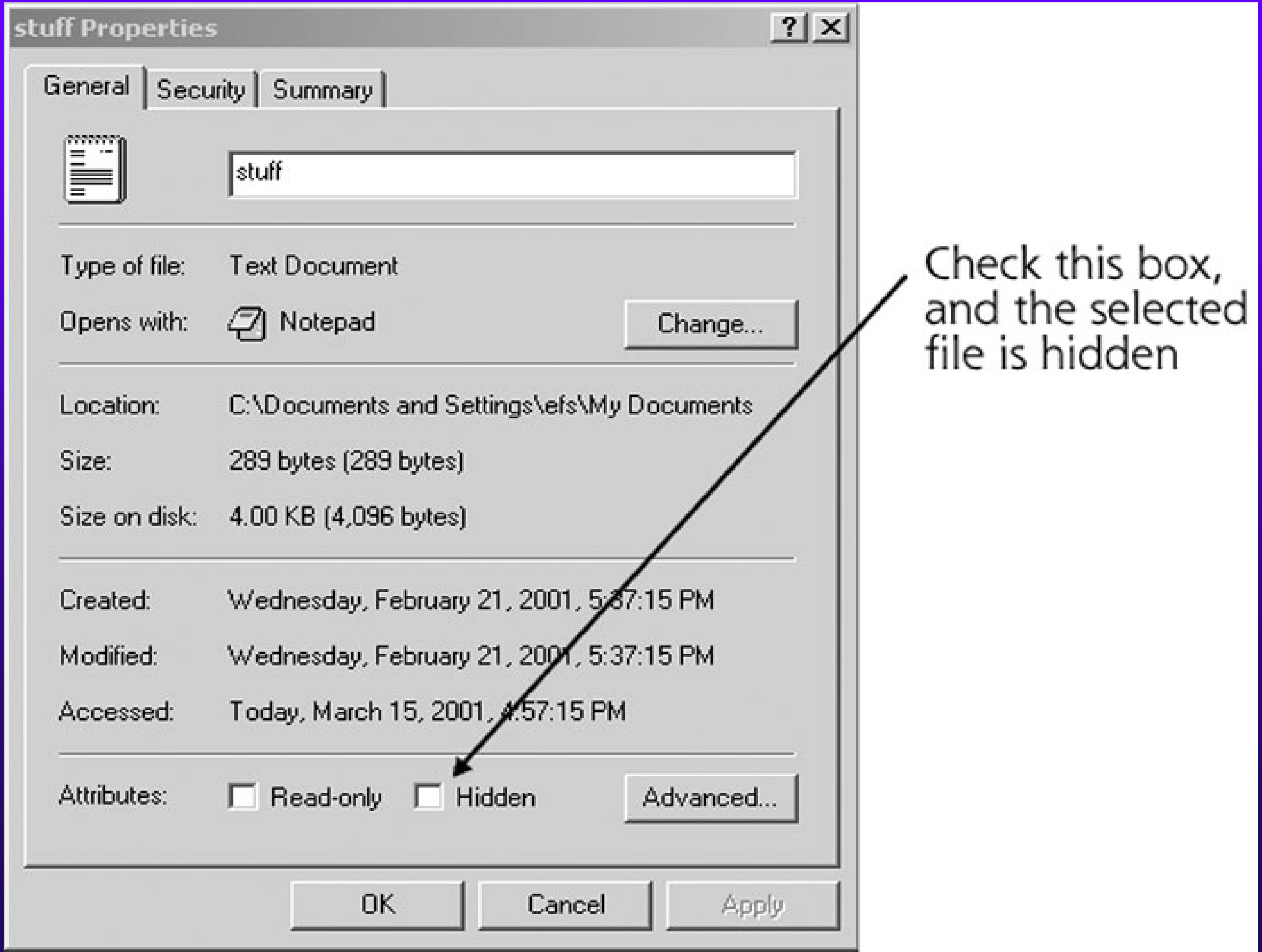
Make a directory with the name period-space.

```
$ ls -a
.  .   ..  .stuff  ftp  httpd  nctest  test  tools
```

This is a file or directory where the attacker can hide items.

Creating Hidden Files in Windows NT/2000

- Right-click on file or directory in Windows Explorer and selecting “properties”



stuff Properties

stuff

Type of file: Text Document

Opens with: Notepad

Location: C:\Documents and Settings\efs\My Documents

Size: 289 bytes (289 bytes)

Size on disk: 4.00 KB (4,096 bytes)

Created: Wednesday, February 21, 2001, 5:37:15 PM

Modified: Wednesday, February 21, 2001, 5:37:15 PM

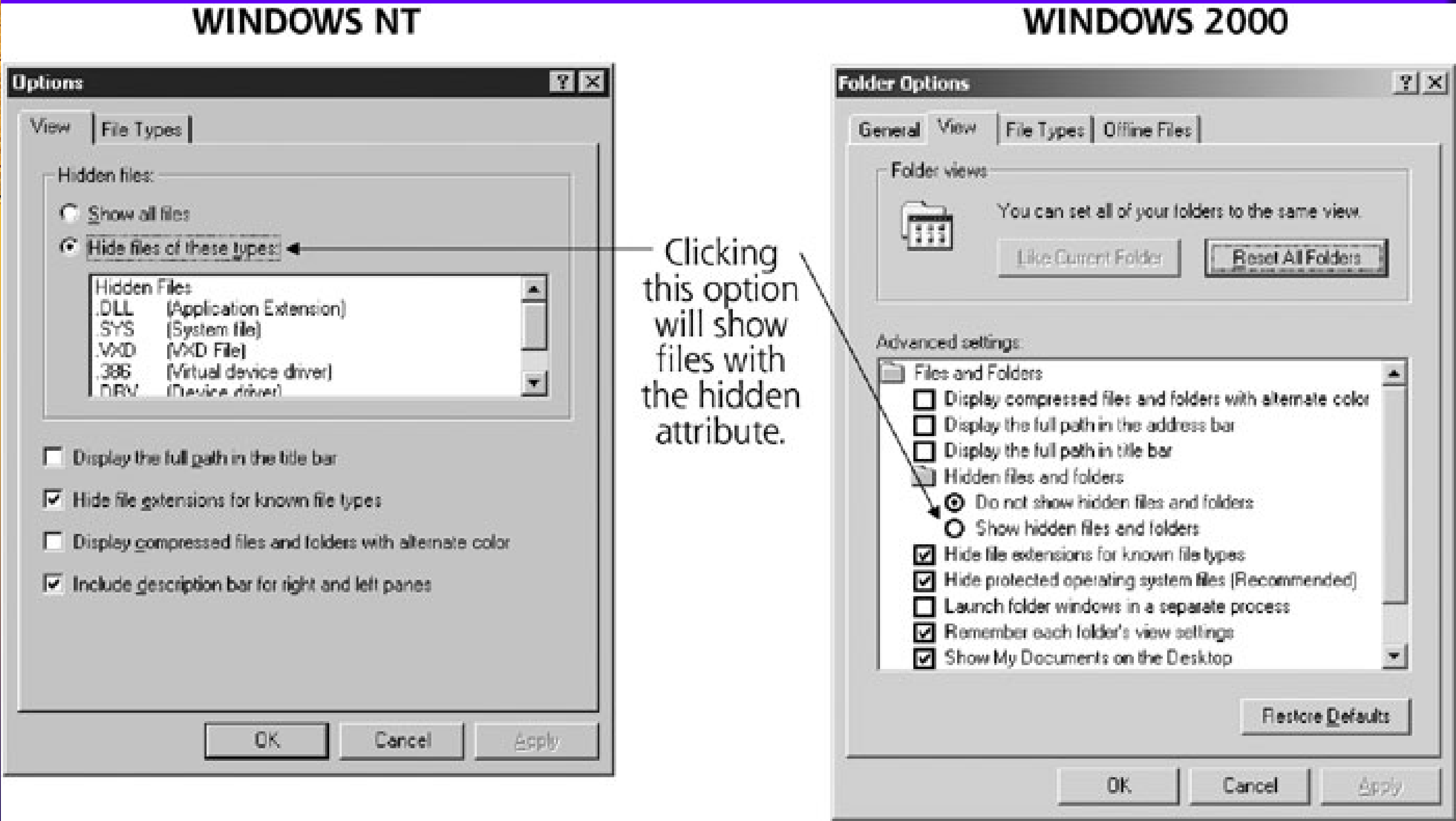
Accessed: Today, March 15, 2001, 4:57:15 PM

Attributes: □ Read-only □ Hidden

Check this box, and the selected file is hidden

Showing Hidden Files in Windows NT and Windows 2000

- ♦ On WinNT’s Windows Explorer, click on “view” menu to show all files
- ♦ in Win2000’s Windows Explorer, click on folder options



WINDOWS NT

Options ? ✕

View | File Types

Hidden files:

○ Show all files

● Hide files of these types:

Hidden Files	
.DLL	(Application Extension)
.SYS	(System file)
.VXD	(VXD File)
.386	(Virtual device driver)
.DRV	(Device driver)

□ Display the full path in the title bar

☑ Hide file extensions for known file types

□ Display compressed files and folders with alternate color

☑ Include description bar for right and left panes

OK | Cancel | Apply

Clicking this option will show files with the hidden attribute.

WINDOWS 2000

Folder Options ? ✕

General | View | File Types | Offline Files

Folder views

You can set all of your folders to the same view.

Like Current Folder | Reset All Folders

Advanced settings:

Files and Folders

□ Display compressed files and folders with alternate color

□ Display the full path in the address bar

□ Display the full path in title bar

Hidden files and folders

● Do not show hidden files and folders

○ Show hidden files and folders

☑ Hide file extensions for known file types

☑ Hide protected operating system files (Recommended)

□ Launch folder windows in a separate process

☑ Remember each folder's view settings

☑ Show My Documents on the Desktop

Restore Defaults

OK | Cancel | Apply

Hiding Information in Windows NT/2000

- NTFS allows every file to have multiple streams of data associated with it
- The normal contents of a file that can be seen and accessed by users is a stream itself
- Other data can be attached and hidden as separate stream using “cp” program in Windows NT Resource Kit

```
C:\>  cp stuff.txt notepad.exe:data
C:\>  erase stuff.txt
C:\>  notepad.exe
C:\>  cp notepad.exe:data   stuff.txt
```

Defenses from Hidden Files

- Use file integrity checking tools such as Tripwire to check contents of files and directories to verify that no additional data, files or directories have been hidden in them
- Use host-based IDS tools and anti-virus tools to check for presence of hidden file and generate alert message

Covert Channels

- Communication channels that disguises data while it moves across the network to avoid detection
- Require a client and server
- Can be used to remotely control a machine and to secretly transfer files or applications

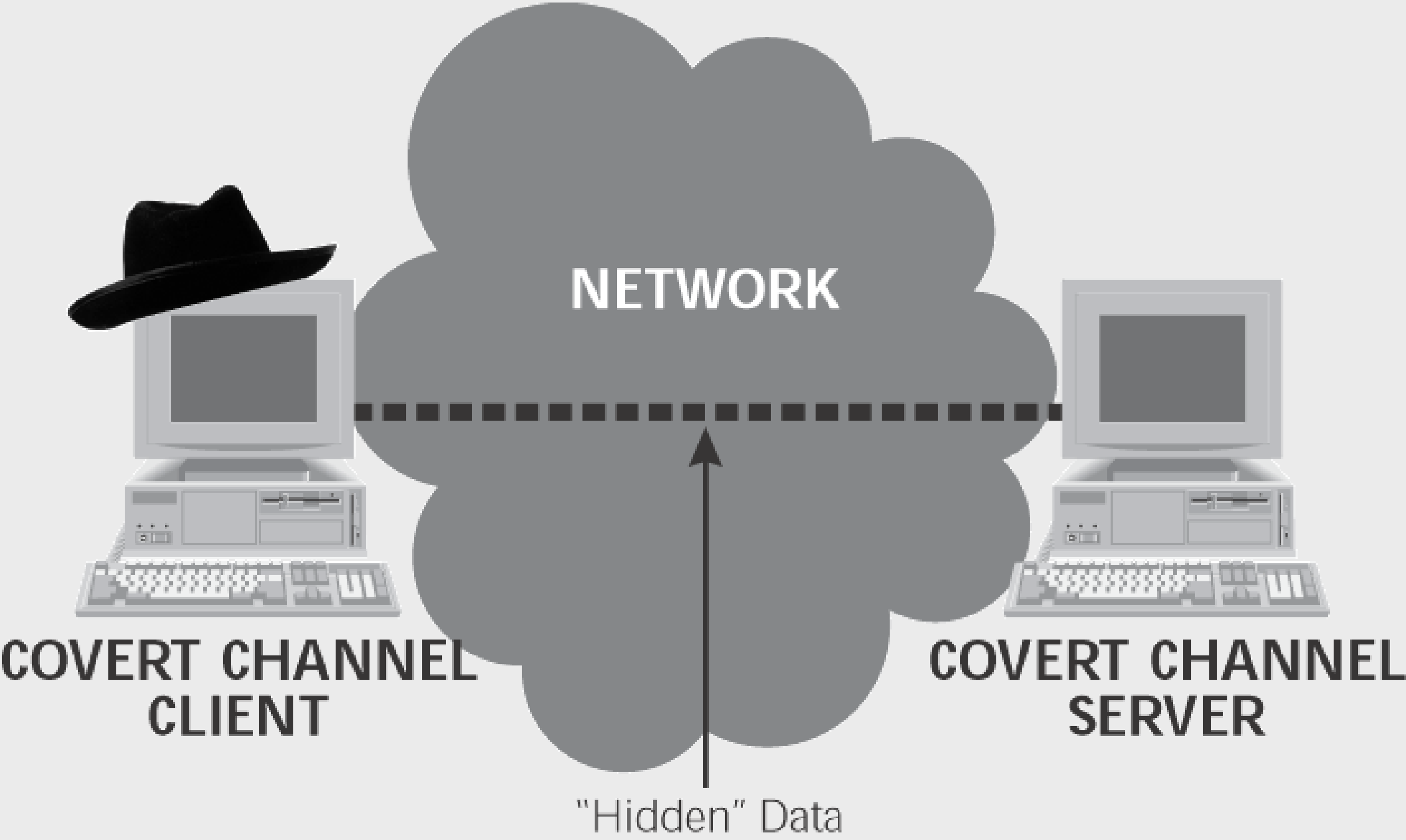


Figure 11.5 A covert channel between a client and a server

Techniques Used to Get a Covert Channel Server Installed

- Perform a buffer overflow on victim and install a backdoor
- Email an unsuspecting user an executable which installs a covert channel server
- Install covert channel as a contractor or employee with administrative privilege

Tunneling

- Carrying one protocol inside another protocol
  - Eg. Tunneling AppleTalk traffic over IP
- Any communications protocol can be used to transmit another protocol
  - SSH protocol used to carry telnet, FTP, or X-Windows session
- Used by covert channels
  - Loki
  - Reverse WWW Shell

Loki

- Covert channel using ICMP as a tunnel to carry interactive communication with a backdoor listener
- More stealthy and difficult to detect than other backdoor programs that listen on a given TCP/UDP port
- Description and source code available at http://phrack.com
- Loki client wraps up attacker’s commands in ICMP and transmits them to the Loki server (lokid)
- Loki server upwraps the commands, executes them and wraps the responses up in ICMP packets
- Lokid must be run with root privilege

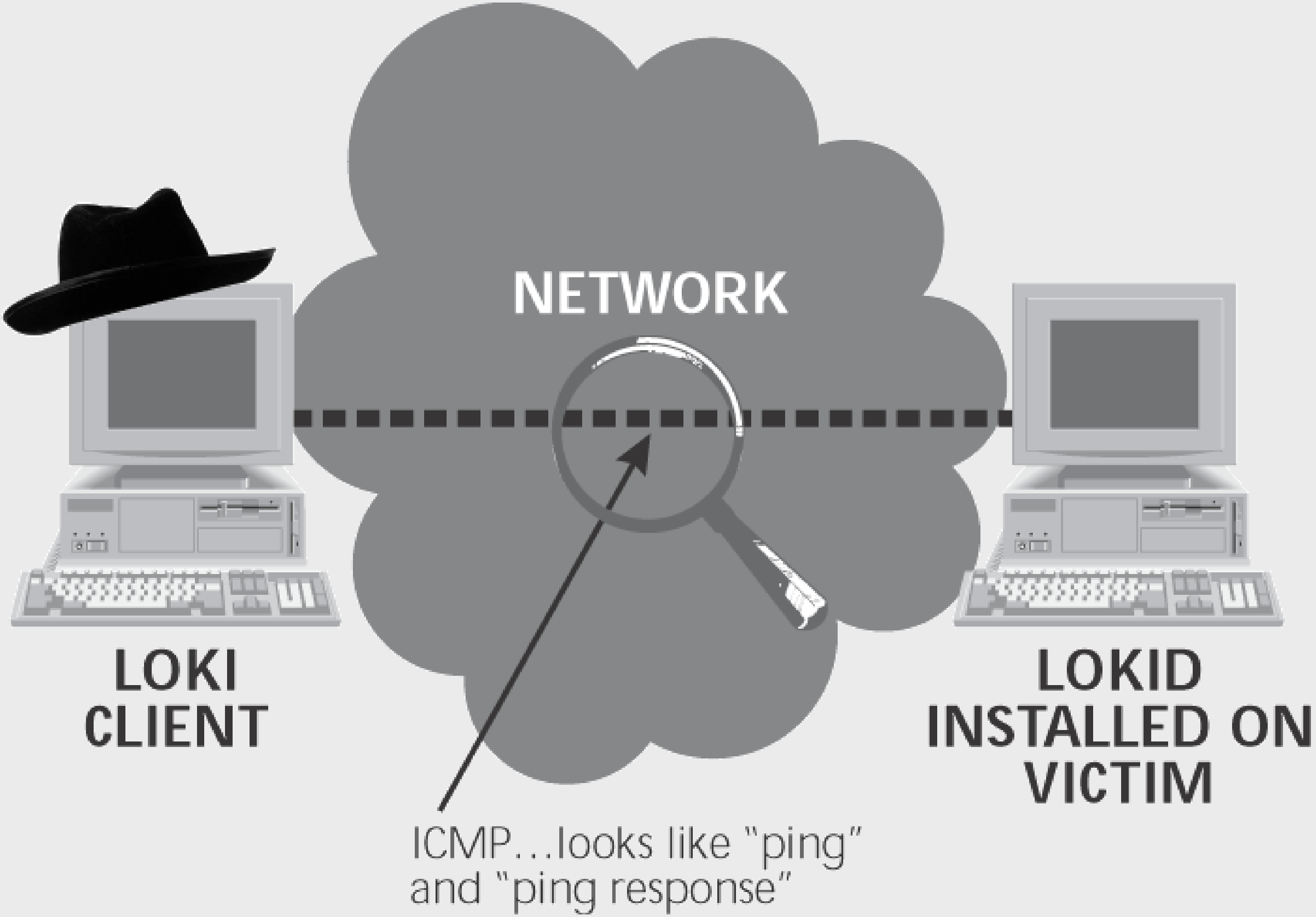

NETWORK
LOKI CLIENT
LOKID INSTALLED ON VICTIM
ICMP…looks like "ping" and "ping response"

Figure 11.6 Loki hides data inside ICMP messages

Loki (cont.)

- can only be detected via the presence of Loki daemon process running as root on the victim and the presence of bidirectional ICMP traffic
- Can disguise its packets as DNS queries and responses by running over UDP port 53
- Supports protocol-switching by typing “/swapt” on client to toggle between ICMP and UDP port 53
- Supports encryption of ICMP payload information

Reverse WWW Shell

- Uses HHTP as a covert channel
- Allows an attacker to remotely access a victim machine with a command-line prompt
- A Reverse WWW Shell server and Perl interpreter must be installed on the victim machine
- A Reverse WWW Shell master software and Perl interpreter must be installed on the attacker’s machine
- Can sneak past firewall
- Perl code available at http://thc.pimmel.com

Reverse WWW Shell (cont.)

- Every minute, Reverse WWW Shell server will contact the master to retrieve commands issued by the attacker
- Reverse WWW Shell server executes the commands, sends the results to Reverse WWW Shell master (via http request), and retrieves the next command (via http reply)
- Victim machine appears to be a web client sending HHTP Get commands while attacker’s machine appears to be a web server

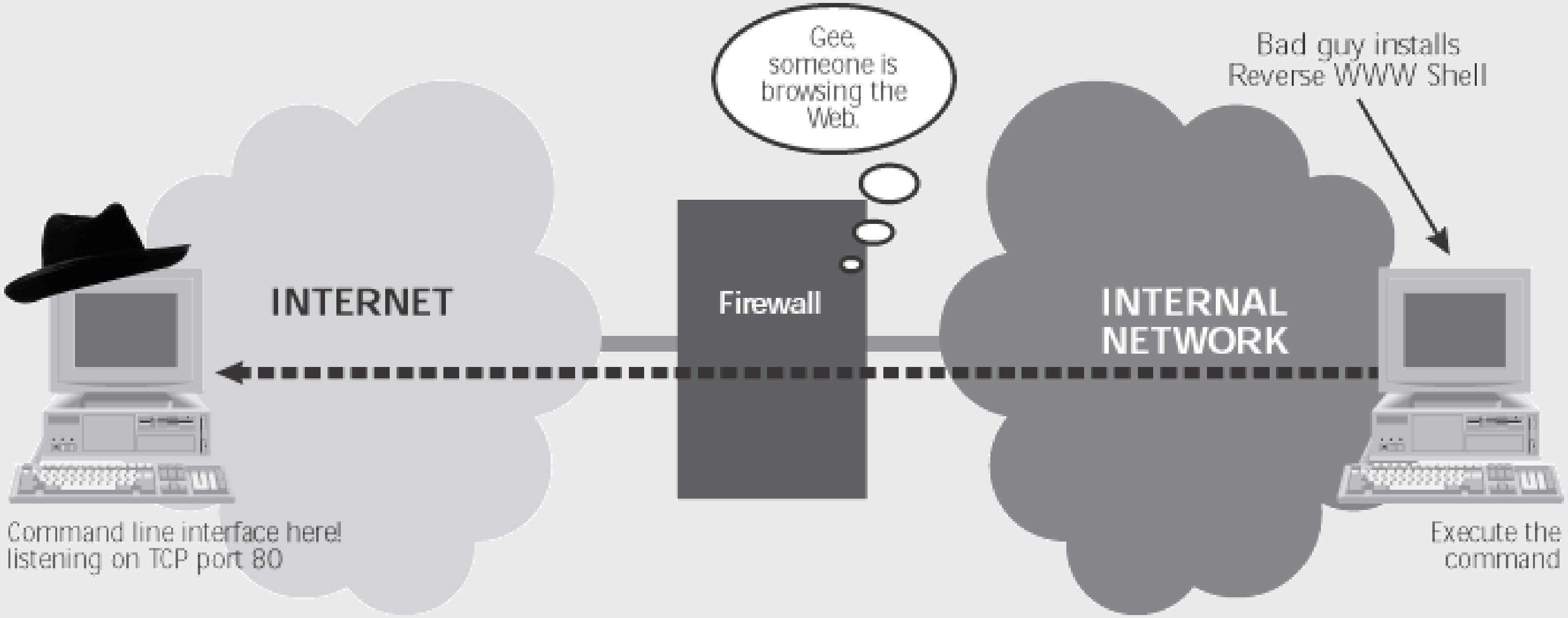

Gee, someone is browsing the Web.
Bad guy installs Reverse WWW Shell
INTERNET
Firewall
INTERNAL NETWORK
Command line interface here! listening on TCP port 80
Execute the command

Figure 11.7 Reverse WWW Shell looks like outgoing Web access, but is really incoming shell access

Protocols used for Covert Channels

- ICMP
- HTTP
- Telnet
- SMTP
- FTP
- Streaming audio
- SSH

Covert_TCP

- http://www.psionic.com/papers/covert
- Uses TCP and IP headers to create covert channels
- Data can be hidden in various fields
  - IP Identification field
    - One character embedded per packet
  - TCP sequence number
    - One character embedded per SYN request and Reset packets
  - TCP acknowledgement number
    - One hidden character per packet is relayed by a "bounce" server
- Can send data over any TCP source/destination ports
  - Can bypass firewall if use ports such as 25 or 53

<table>
<tr><td>V</td><td>HI</td><td colspan="2">Service</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="4"><i>Identification</i></td><td colspan="2">Flags</td><td colspan="2">Fragment</td></tr>
<tr><td colspan="2">Time to</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source IP Address</td></tr>
<tr><td colspan="8">Destination IP Address</td></tr>
<tr><td colspan="6">IP Options (if any)</td><td colspan="2">Padding</td></tr>
<tr><td colspan="8">Data</td></tr>
<tr><td colspan="8">.....</td></tr>
</table>

<table>
<tr><td colspan="6">Source Port</td><td colspan="6">Destination Port</td></tr>
<tr><td colspan="12"><i>Sequence Number</i></td></tr>
<tr><td colspan="12"><i>Acknowledgment Number</i></td></tr>
<tr><td colspan="2">Hle</td><td colspan="2">Rsvd</td><td colspan="2">Code</td><td colspan="6">Window</td></tr>
<tr><td colspan="6">Checksum</td><td colspan="6">Urgent Pointer</td></tr>
<tr><td colspan="10">IP Options (if any)</td><td colspan="2">Padding</td></tr>
<tr><td colspan="12">Data</td></tr>
<tr><td colspan="12">.....</td></tr>
</table>

Figure 11.8 The IP and TCP headers

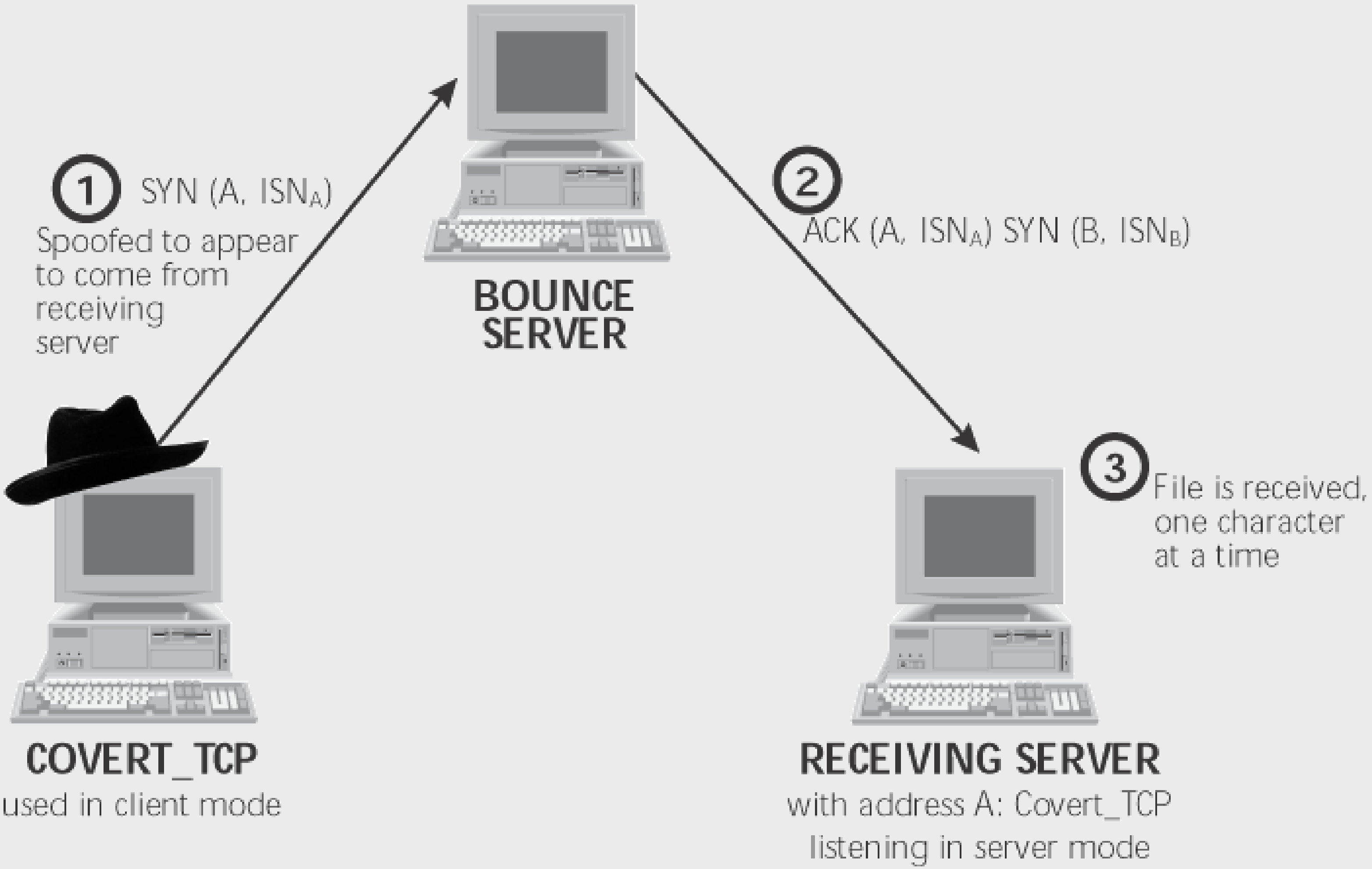

1 SYN (A, ISN$_A$)
Spoofed to appear to come from receiving server
BOUNCE SERVER
2 ACK (A, ISN$_A$) SYN (B, ISN$_B$)
3 File is received, one character at a time
COVERT_TCP
used in client mode
RECEIVING SERVER
with address A: Covert_TCP listening in server mode

Figure 11.9 Using Covert_TCP with a bounce server

Defenses against Covert Channels

- Don’t let attacker get root or administrator access on hosts
  - Harden OS
  - Install latest security patches
- Install network IDS
  - Loki and other covert channels can be detected by Snort