CSCE 629
Cyber Attack

[redacted]

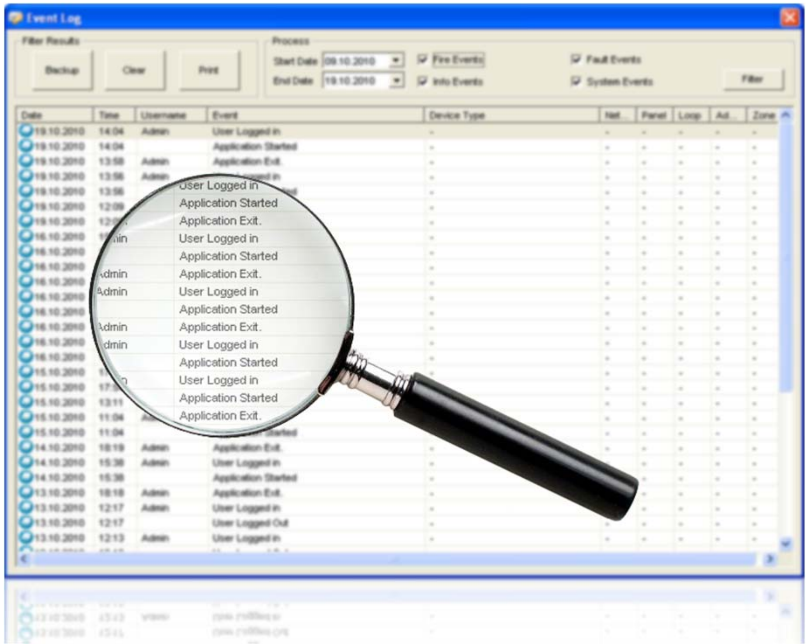
Covering Tracks
and

Hiding

Dr. Barry Mullins
AFIT/ENG
Bldg 642
Room 209
255-3636 x7979

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding
  - Altering Event Logs
  - Covert Channels

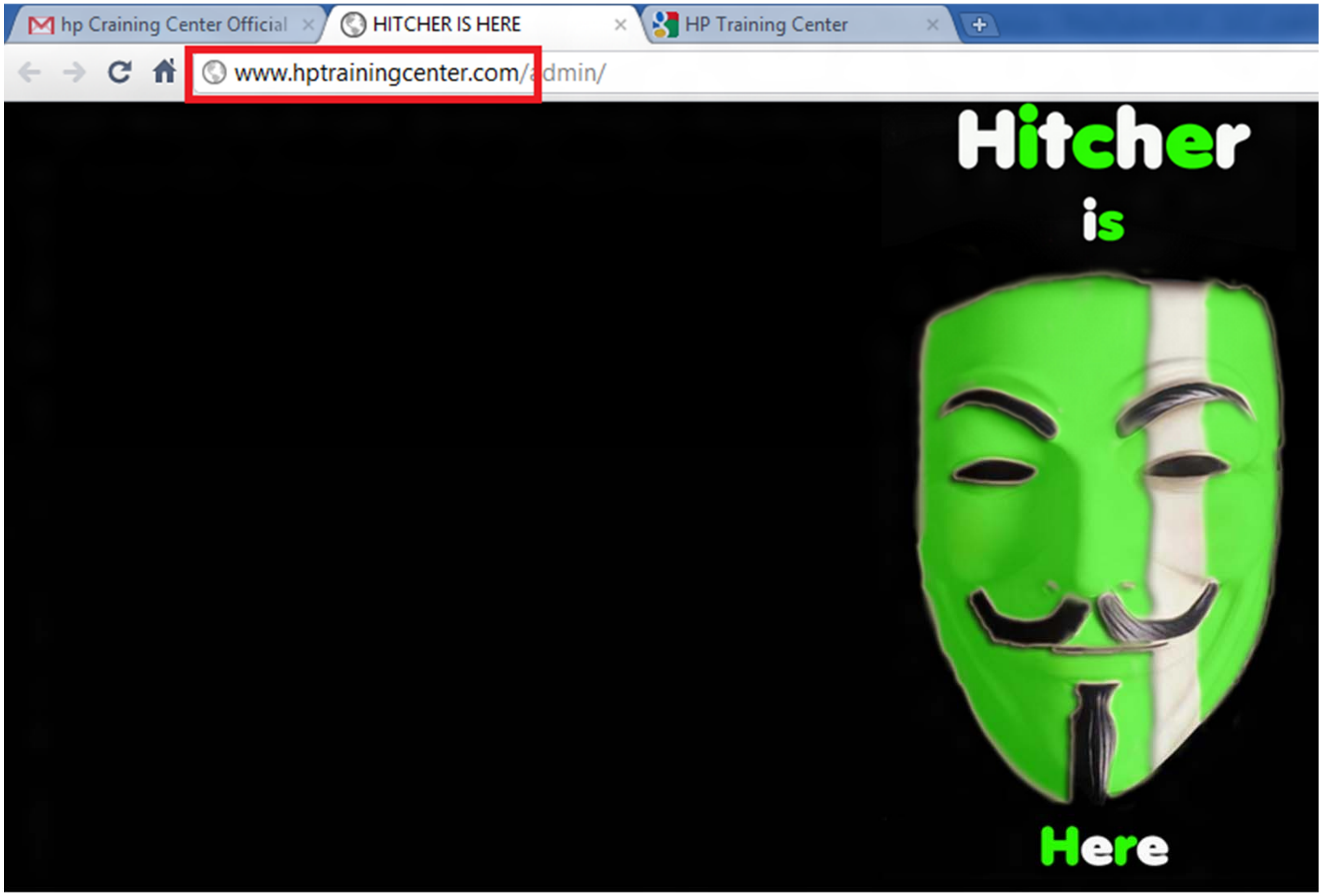


```
Date        Time   Username  Event                 Device Type  Net...  Panel  Loop  Ad...  Zone
19.10.2010  14:04  Admin     User Logged in        -            -       -      -     -      -
19.10.2010  14:04            Application Started   -            -       -      -     -      -
19.10.2010  13:58  Admin     Application Exit.     -            -       -      -     -      -
19.10.2010  13:56  Admin     User Logged in        -            -       -      -     -      -
19.10.2010  13:56                                  -            -       -      -     -      -
19.10.2010  12:09                                  -            -       -      -     -      -
19.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
16.10.2010                                         -            -       -      -     -      -
15.10.2010                                         -            -       -      -     -      -
15.10.2010                                         -            -       -      -     -      -
15.10.2010  13:11                                  -            -       -      -     -      -
15.10.2010  11:04                                  -            -       -      -     -      -
15.10.2010  11:04                                  -            -       -      -     -      -
14.10.2010  18:19  Admin     Application Exit.     -            -       -      -     -      -
14.10.2010  15:38  Admin     User Logged in        -            -       -      -     -      -
14.10.2010  15:38            Application Started   -            -       -      -     -      -
13.10.2010  18:18  Admin     Application Exit.     -            -       -      -     -      -
13.10.2010  12:17  Admin     User Logged in        -            -       -      -     -      -
13.10.2010  12:17            User Logged Out       -            -       -      -     -      -
13.10.2010  12:13  Admin     User Logged in        -            -       -      -     -      -
```

```
User Logged in
Application Started
Application Exit.
User Logged in
Application Started
Admin      Application Exit.
Admin      User Logged in
           Application Started
Admin      Application Exit.
dmin       User Logged in
           Application Started
           User Logged in
           Application Started
           Application Exit.
```

Attackers' Modus Operandi

- Some attackers want to draw attention to their cause
  - Defacing website
    - Attacker's presence is obvious immediately



Attackers' Modus Operandi

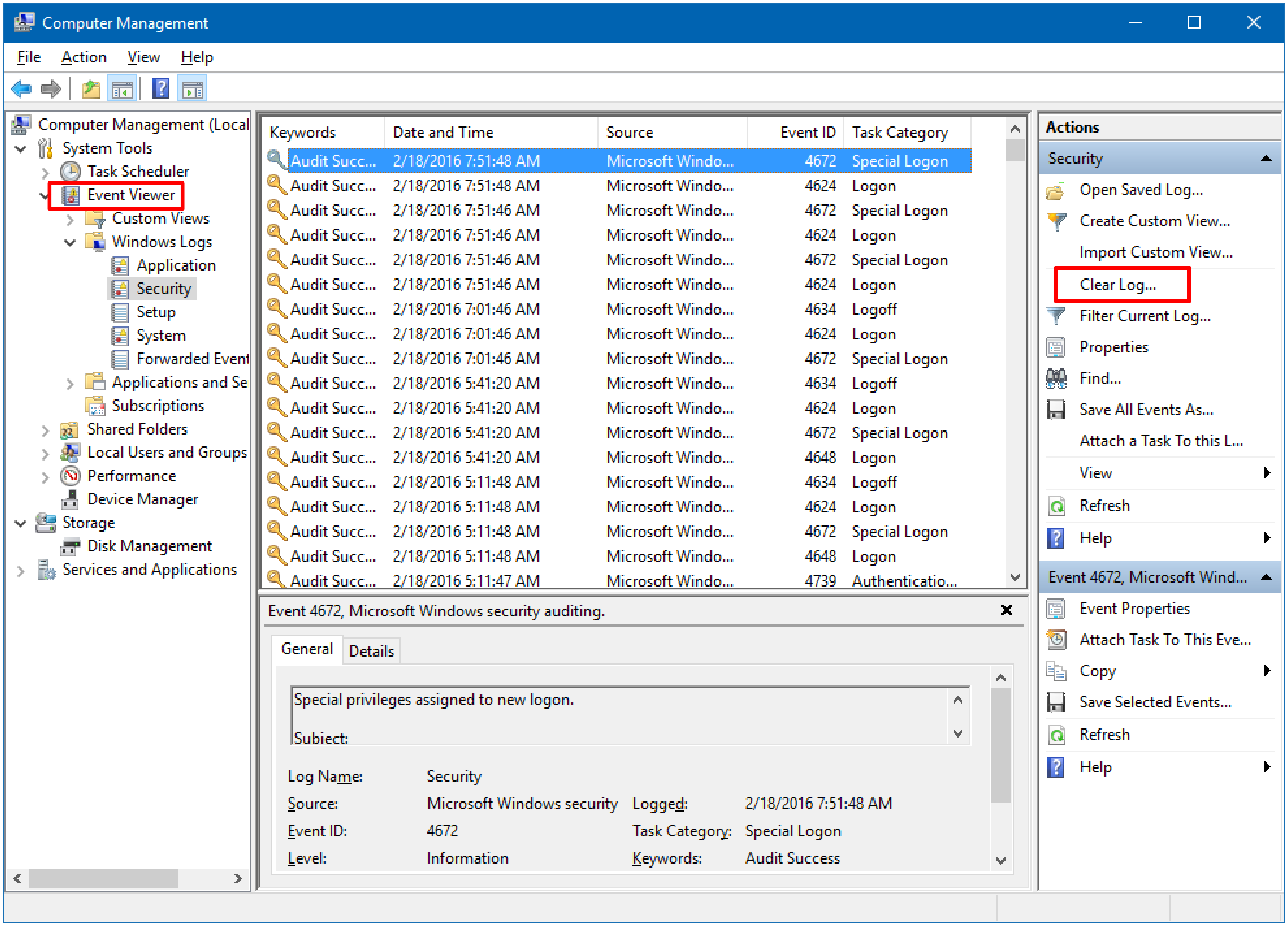
- Most attackers prefer more clandestine operations
- Prefer to maintain access for long period of time

- In order to hide the attacker's presence, the attacker
  - Installs rootkits
  - Modifies logs to remove evidence of
    - Gaining access to the machine
    - Elevating privileges
    - Installing a rootkit
  - Creates hidden files
  - Establishes covert channels

Event Logs in Windows

- Windows event logs are stored in
  - Win XP → **`C:\Windows\System32\Config`**
    - **`AppEvent.evt`** - Application-oriented events
    - **`SecEvent.evt`** - Security events
    - **`SysEvent.evt`** - System events (readable by all users)
  - Win 7, 10 → **`C:\Windows\System32\winevt\Logs`**
    - **`Application.evtx`** - Application-oriented events
    - **`Security.evtx`** - Security events
    - **`System.evtx`** - System events (readable by all users)
- Files are stored as binary information and are not directly editable
  - Files are write-locked on a running Windows system

Viewing and Clearing Event Logs



Keywords	Date and Time	Source	Event ID	Task Category
Audit Succ...	2/18/2016 7:51:48 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 7:51:48 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:01:46 AM	Microsoft Windo...	4634	Logoff
Audit Succ...	2/18/2016 7:01:46 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:01:46 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4634	Logoff
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4648	Logon
Audit Succ...	2/18/2016 5:11:48 AM	Microsoft Windo...	4634	Logoff
Audit Succ...	2/18/2016 5:11:48 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 5:11:48 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 5:11:48 AM	Microsoft Windo...	4648	Logon
Audit Succ...	2/18/2016 5:11:47 AM	Microsoft Windo...	4739	Authenticatio...

Event 4672, Microsoft Windows security auditing.

Special privileges assigned to new logon.

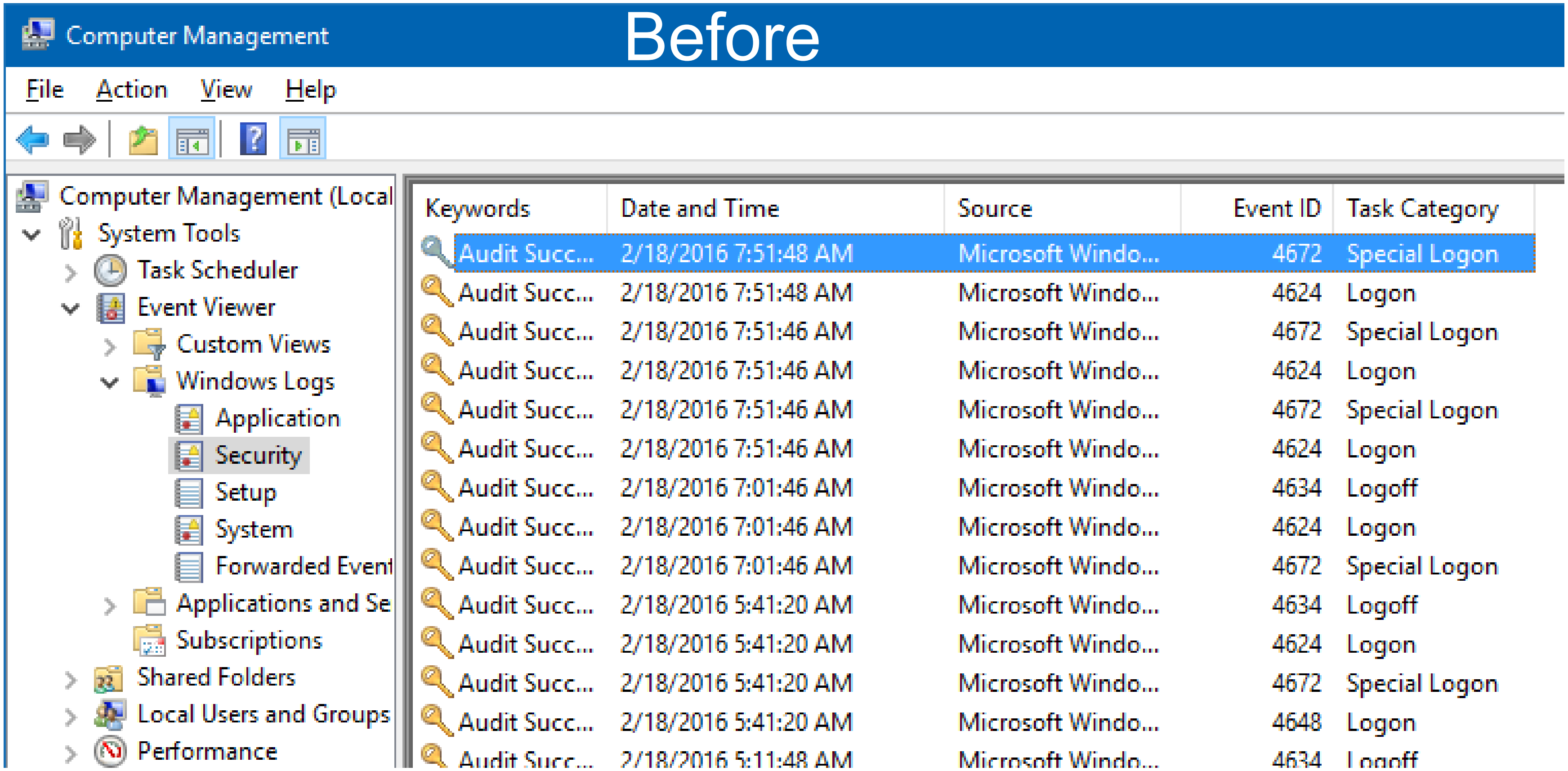
Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/18/2016 7:51:48 AM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success

"Attacking" Event Logs Windows 7-10

- Attacker with admin privileges can "clear" the log files

```
C:\>wevtutil cl security
```



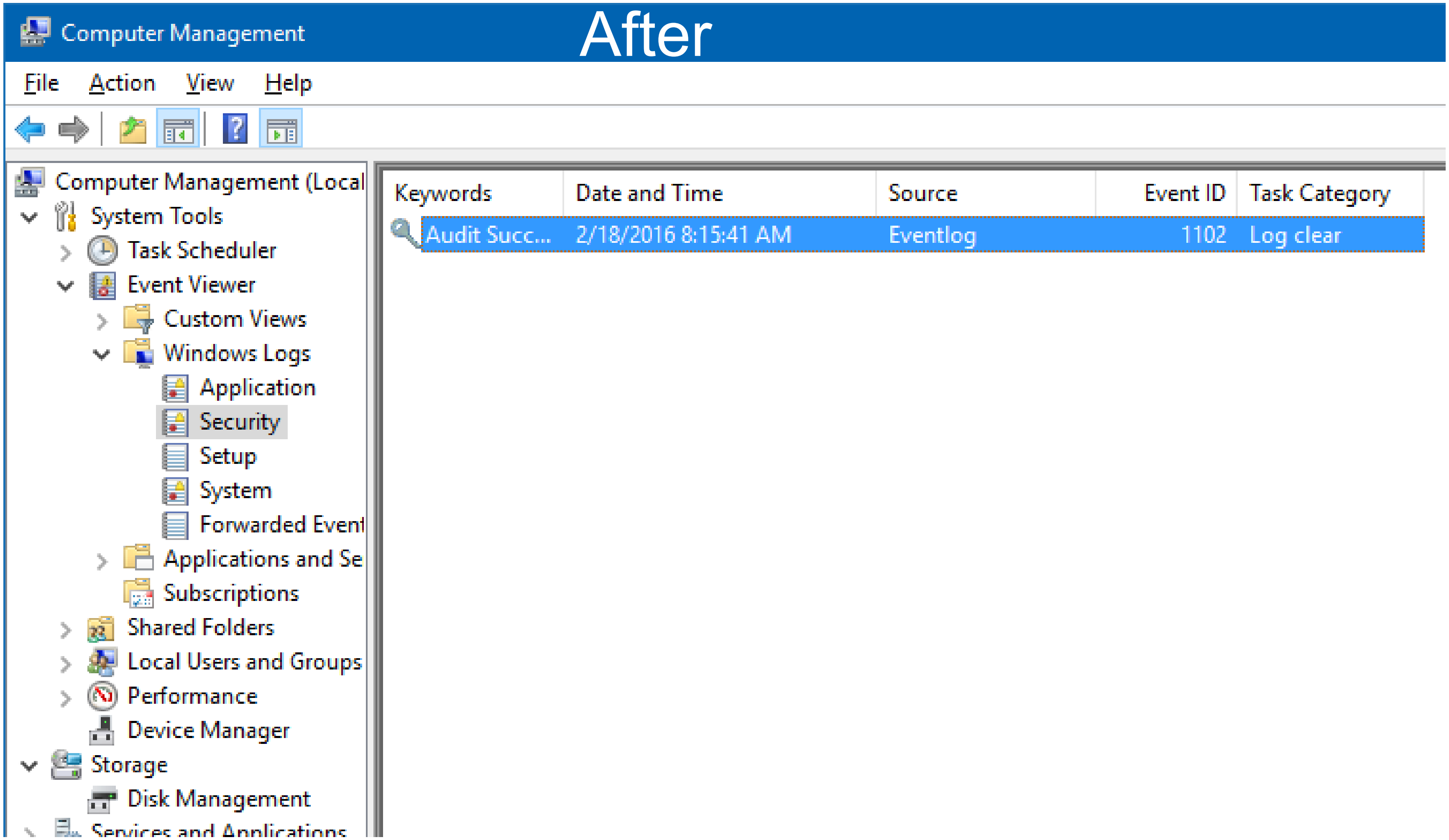
Before

Keywords	Date and Time	Source	Event ID	Task Category
Audit Succ...	2/18/2016 7:51:48 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 7:51:48 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 7:51:46 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:01:46 AM	Microsoft Windo...	4634	Logoff
Audit Succ...	2/18/2016 7:01:46 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 7:01:46 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4634	Logoff
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4624	Logon
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4672	Special Logon
Audit Succ...	2/18/2016 5:41:20 AM	Microsoft Windo...	4648	Logon
Audit Succ...	2/18/2016 5:11:48 AM	Microsoft Windo...	4634	Logoff

"Attacking" Event Logs Windows 7-10

- Attacker with admin privileges can "clear" the log files

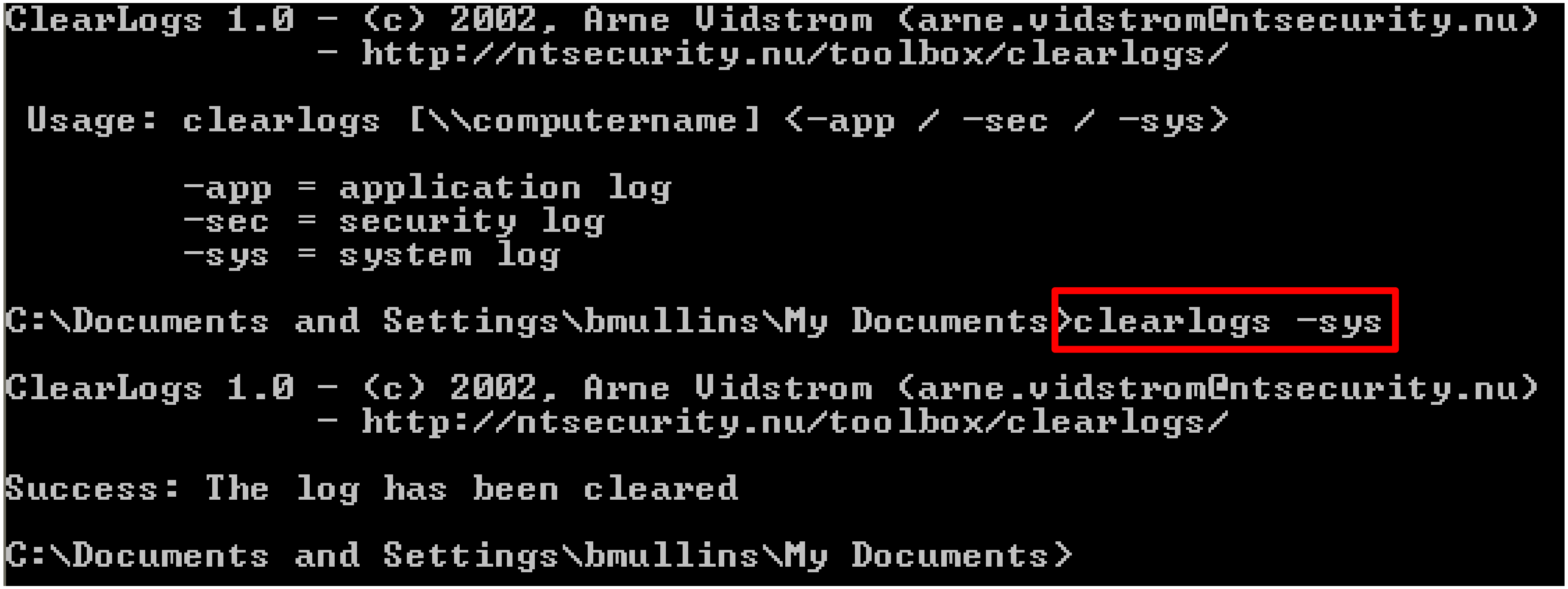
```
C:\>wevtutil cl security
```


After

Keywords	Date and Time	Source	Event ID	Task Category
Audit Succ...	2/18/2016 8:15:41 AM	Eventlog	1102	Log clear

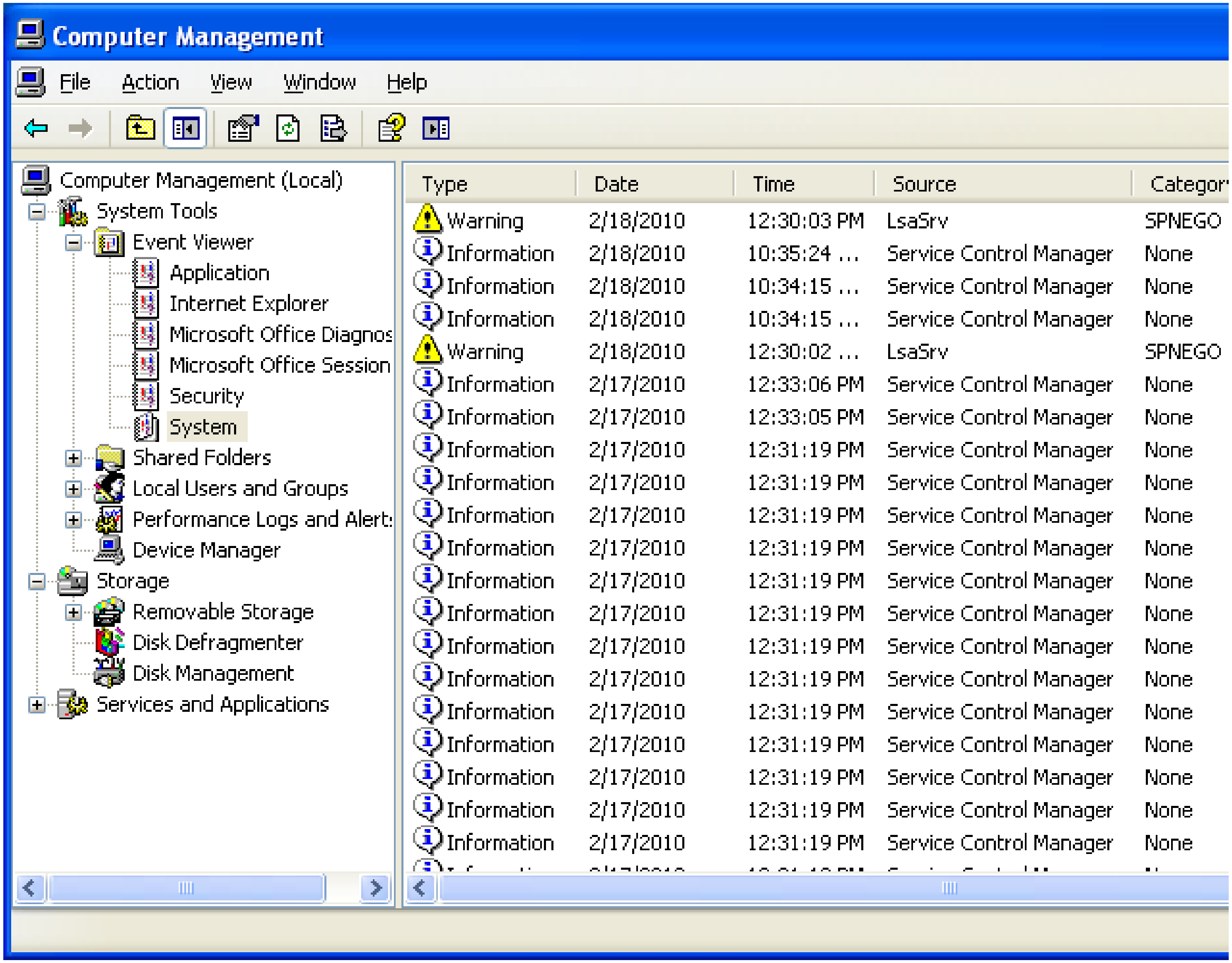
“Attacking” Event Logs Pre-Windows 7

- Clears the event log (Security, System or Application)
  - Windows NT 4.0 / 2000 / XP / 2003 / Vista
- Can also clear logs on a remote computer
- ntsecurity.nu/toolbox/clearlogs/



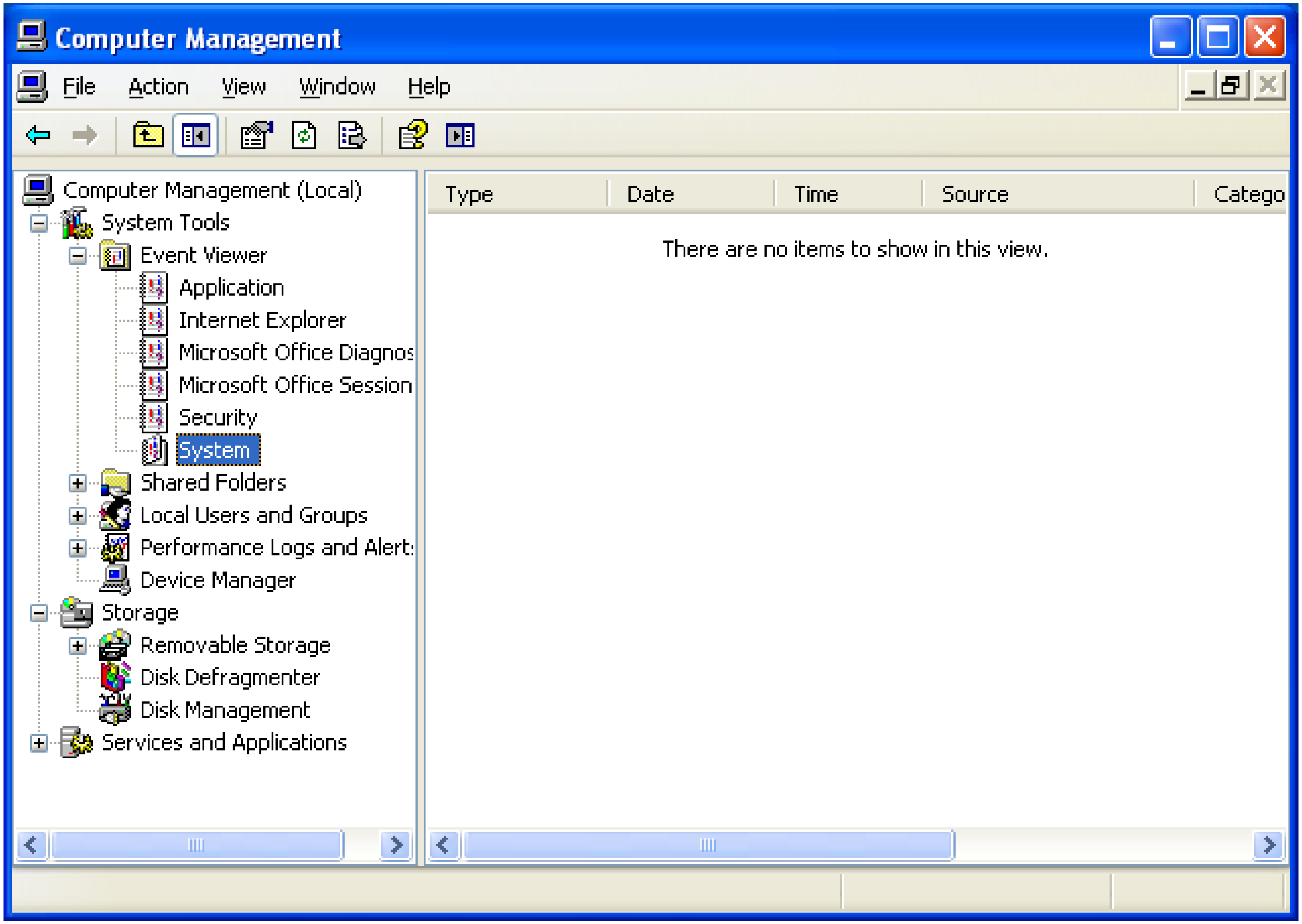
```
ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
              - http://ntsecurity.nu/toolbox/clearlogs/

 Usage: clearlogs [\\computername] <-app / -sec / -sys>

        -app = application log
        -sec = security log
        -sys = system log

C:\Documents and Settings\bmullins\My Documents>clearlogs -sys

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
              - http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared

C:\Documents and Settings\bmullins\My Documents>
```

Before Running `clearlogs -sys`



Type	Date	Time	Source	Categor
Warning	2/18/2010	12:30:03 PM	LsaSrv	SPNEGO
Information	2/18/2010	10:35:24 ...	Service Control Manager	None
Information	2/18/2010	10:34:15 ...	Service Control Manager	None
Information	2/18/2010	10:34:15 ...	Service Control Manager	None
Warning	2/18/2010	12:30:02 ...	LsaSrv	SPNEGO
Information	2/17/2010	12:33:06 PM	Service Control Manager	None
Information	2/17/2010	12:33:05 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None
Information	2/17/2010	12:31:19 PM	Service Control Manager	None

After Running `clearlogs -sys`



There are no items to show in this view.

Linux/Unix System Logs - ASCII

- Locations of main log file in **`/etc/rsyslog.conf`**
  - **`/var/log/auth.log`** → Authentication logs
  - **`/var/log/messages`** → boot messages / system messages
- Service logs
  - **`/var/log/httpd/error_log`**
  - **`/var/log/httpd/access_log`**
- Log files usually in ASCII
  - Edit using text editor
  - Use Perl or Python script if file is large

Accounting Files in Linux/Unix - Binary

- **utmp**: Currently logged in users /var/run/utmp
- **wtmp**: Past user logins /var/log/wtmp
- **lastlog**: Login name, port and last login time for each user
  - /var/log/lastlog
- Can only be edited using specialized tools:
  - **Last Door Log Wiper**
    - Wipes specific entries in arbitrary log files
    - If root, will also execute arbitrary commands without logging
  - **remove**
    - Changes last login time, location, and status by editing lastlog
    - Removes entries from utmp, wtmp, and lastlog
  - Numerous others including **RopeADope, Linux Log Eraser, wtmped, marry, cloak, logwedit, zapper**
  - www.packetstormsecurity.org/UNIX/penetration/log-wipers

Don't Forget Linux Shell History

- List of the most recent N commands stored in **~/.bash_history**
  - N=500 by default in bash
  - Written in ASCII and can be edited by hand with permissions of the user or root
- Attackers also delete or edit their shell history files
  - Attackers remove suspicious commands
  - Some even add commands to implicate some other user in the attack (divert attention)

I would like to present my client's
~/.bash_history from that evening.
I'd rather just confess to the murder.

Editing Shell History - A Problem

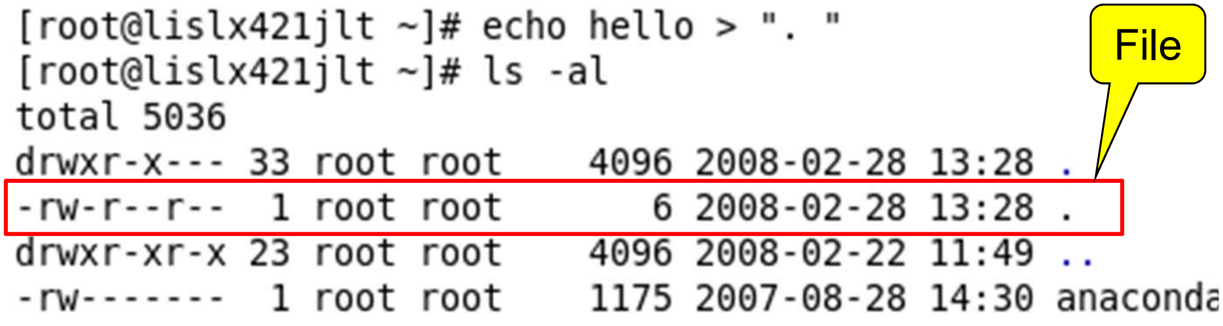
- Shell history is written when the shell is exited
- When editing shell history, the command used to invoke the editor is placed in the shell history file
- Attacker could edit the file, exit the shell, start another shell, edit the history file again to remove it…
  - … but it will be added again!
  - Chicken and egg problem
- Solutions
  - 1) Kill the shell, so that it cannot write the most recent shell history, including the command used to edit it
    - `# kill -9 [pid_of_the_shell_process]`
  - 2) Change environment variable HISTSIZE (for bash) to zero
    - `# export HISTSIZE=0`

Creating Hidden Files and Directories in Unix

- ❒ Easiest (and effective) way to hide files is to simply name them something like ". " or ".. "
  - ❖ There's a space after those periods
- ❒ Name a file "..." or even " " (That's a space!)
- ❒ Could also append a period "." to the beginning of the filename
  - ❖ These files are not displayed by the **ls** command
  - ❖ **ls –a** will display all files
- ❒ For example:

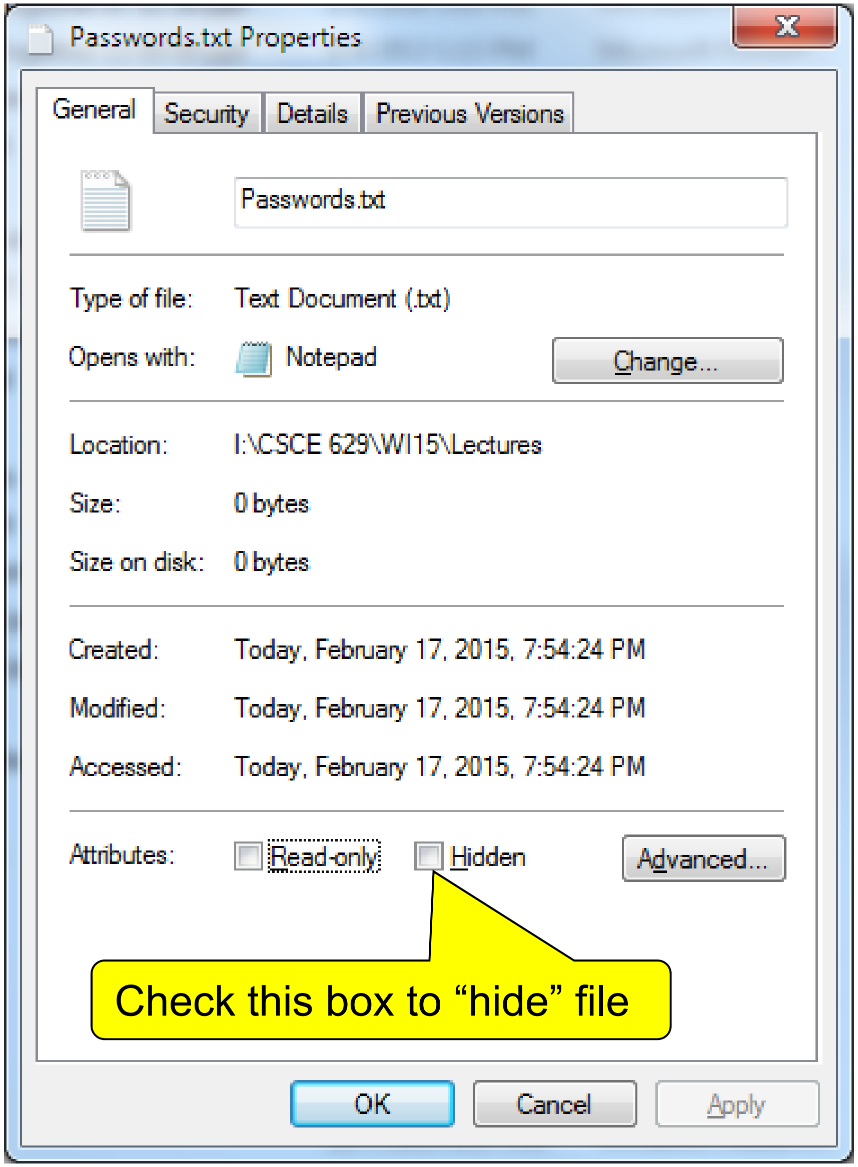
```
# ls
test.txt  files
# ls -a
. ..  .mystuff
test.txt  files
# echo hideme > ".. "
# ls -a
. .. ..  .mystuff  test.txt  files
```

File



```
[root@lislx421jlt ~]# echo hello > ". "
[root@lislx421jlt ~]# ls -al
total 5036
drwxr-x--- 33 root root    4096 2008-02-28 13:28 .
-rw-r--r--  1 root root       6 2008-02-28 13:28 .
drwxr-xr-x 23 root root    4096 2008-02-22 11:49 ..
-rw-------  1 root root    1175 2007-08-28 14:30 anaconda
```

Creating Hidden Files in Windows



Passwords.txt Properties

General | Security | Details | Previous Versions

Passwords.txt

Type of file: Text Document (.txt)

Opens with: Notepad Change...

Location: I:\CSCE 629\WI15\Lectures

Size: 0 bytes

Size on disk: 0 bytes

Created: Today, February 17, 2015, 7:54:24 PM

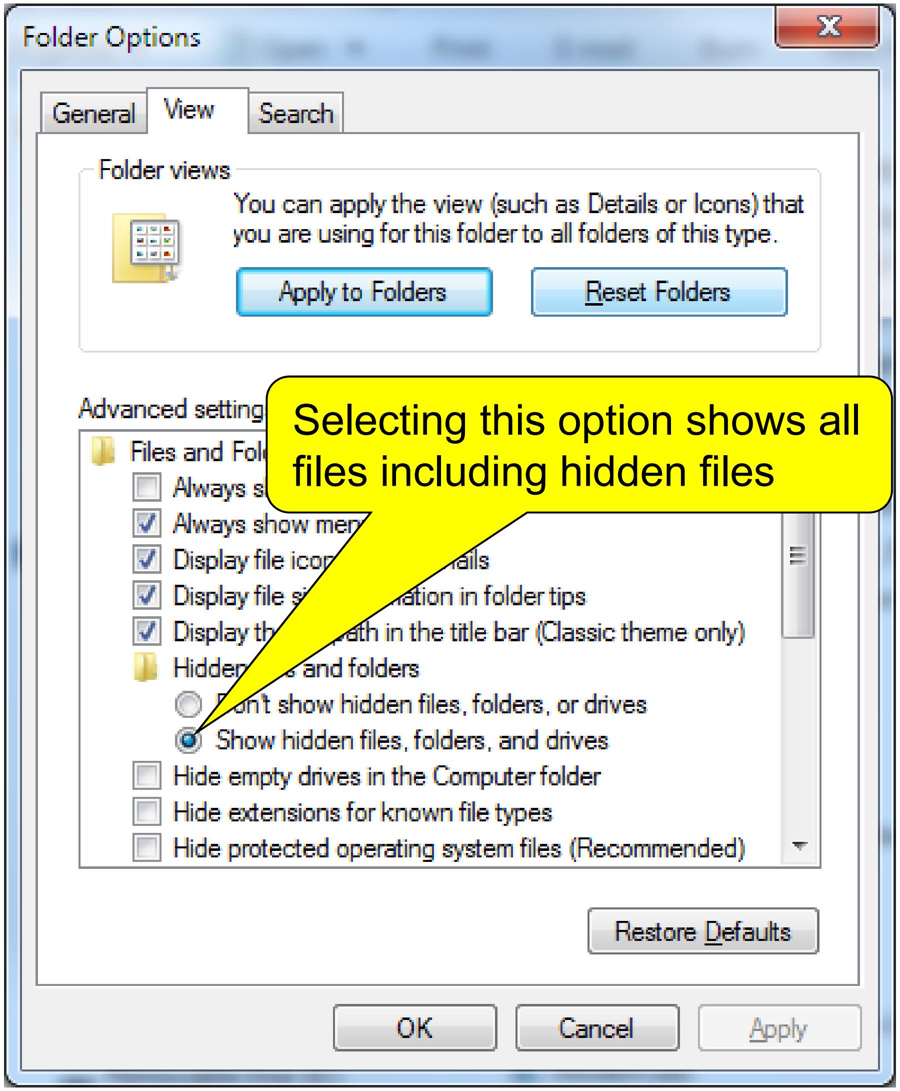
Modified: Today, February 17, 2015, 7:54:24 PM

Accessed: Today, February 17, 2015, 7:54:24 PM

Attributes: □ Read-only □ Hidden Advanced...

OK Cancel Apply

Check this box to “hide” file



Folder Options

General | View | Search

Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Apply to Folders Reset Folders

Advanced setting

Files and Fol

□ Always s

☑ Always show men

☑ Display file icon ails

☑ Display file si ation in folder tips

☑ Display th ath in the title bar (Classic theme only)

Hidden s and folders

○ Don't show hidden files, folders, or drives

● Show hidden files, folders, and drives

□ Hide empty drives in the Computer folder

□ Hide extensions for known file types

□ Hide protected operating system files (Recommended)

Restore Defaults

OK Cancel Apply

Selecting this option shows all files including hidden files

Hiding Files Behind Other Files

- Can append two or more files together

- **`copy /b cover.jpg + secret.txt hidden.jpg`**

- Appends **`secret.txt`** to the end of **`cover.jpg`** and names the new file **`hidden.jpg`**

- Can view **`hidden.jpg`** in an image viewer but if you open **`hidden.jpg`** in a text editor (e.g., notepad or notepad++) you will see the contents of **`secret.txt`** at the end

Hiding Files in NTFS Alternate Data Streams (ADS)

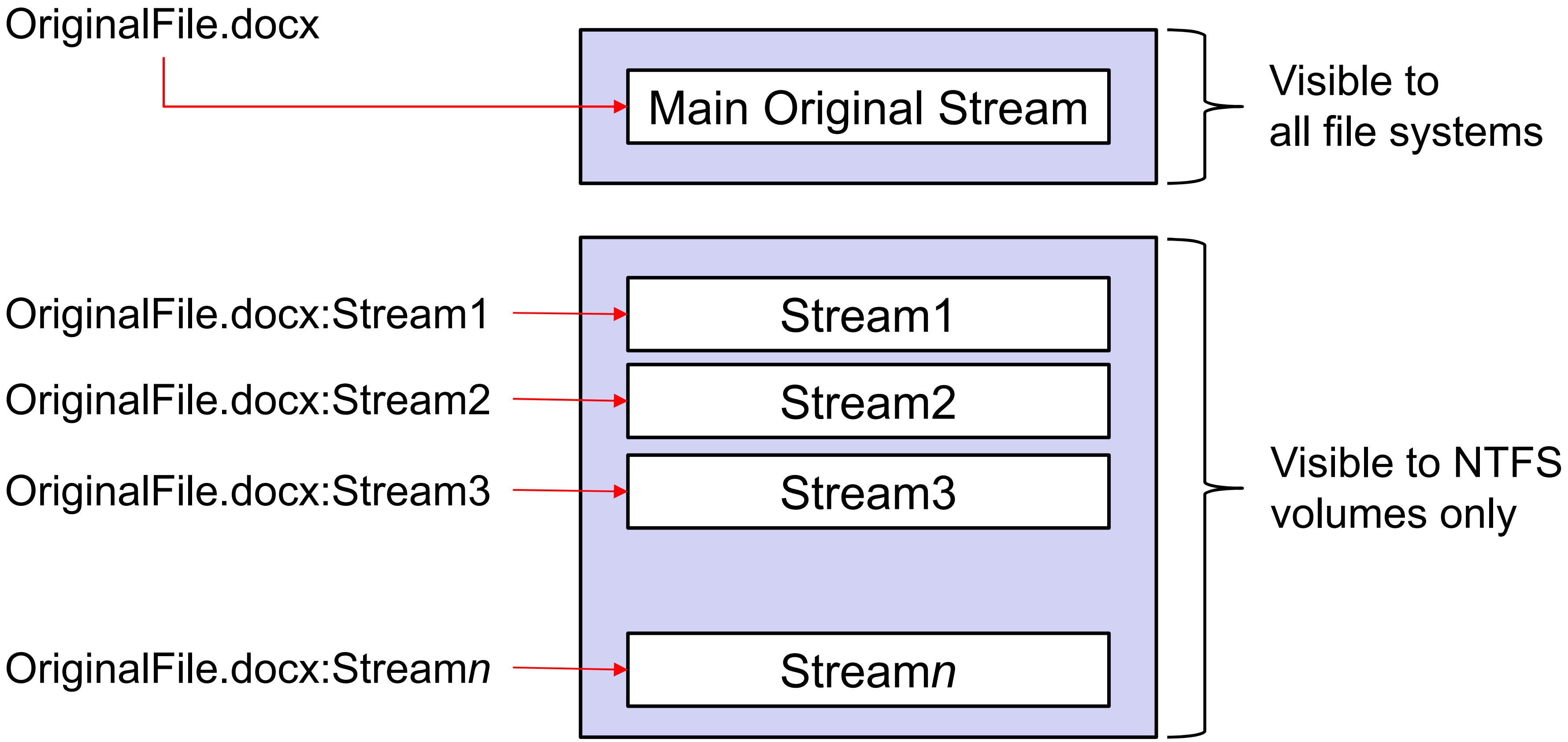
- Attacker's files can be hidden in a stream behind normal files or directories on the system
  - Such as .txt files, notepad.exe or word.exe (or anything else!)

- If system is running NTFS (New Technology File System), ADS is supported
  - ADS created to provide compatibility with the Macintosh Hierarchical File System which stored files in two parts—data and resource (how to use the data part)

http://www.bleepingcomputer.com/tutorials/windows-alternate-data-streams/

Hiding Files in NTFS
Alternate Data Streams (ADS)

- Multiple streams can be attached to each file or directory


OriginalFile.docx
Main Original Stream
Visible to all file systems
OriginalFile.docx:Stream1
OriginalFile.docx:Stream2
OriginalFile.docx:Stream3
OriginalFile.docx:Stream*n*
Stream1
Stream2
Stream3
Stream*n*
Visible to NTFS volumes only

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc781134(v%3dws.10)

Hiding Files in NTFS Alternate Data Streams (ADS)

- Legit uses of ADS
  - Metadata about file
  - Encryption information
  - Backup, maintenance, information on files and directories
  - Extended information about file activity
  - IE, Edge, Chrome and other browsers will add an ADS named Zone.Identifier to a file downloaded with info about the source
    - Some browsers even add other details about the file downloaded like source and referrer URLs

http://www.bleepingcomputer.com/tutorials/windows-alternate-data-streams/
https://www.jankyrobotsecurity.com/2018/07/24/accessing-alternate-data-streams-from-a-mac/

Hiding Files in NTFS

- Use the type command built into Windows

```
type stuff.txt > notepad.exe:anyfile.txt
```

- Pull file from stream and print to screen

```
more < notepad.exe:anyfile.txt
```

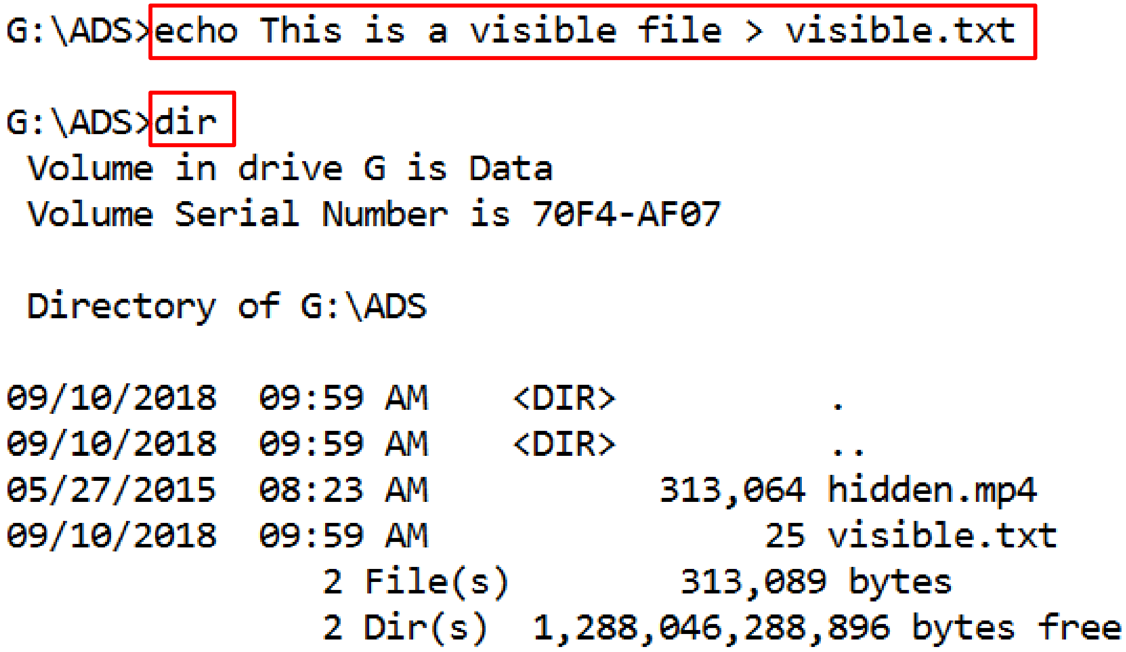
- Can also save to file

```
more < notepad.exe:anyfile.txt > newfile.txt
```

- Can even execute an ADS (Windows XP)

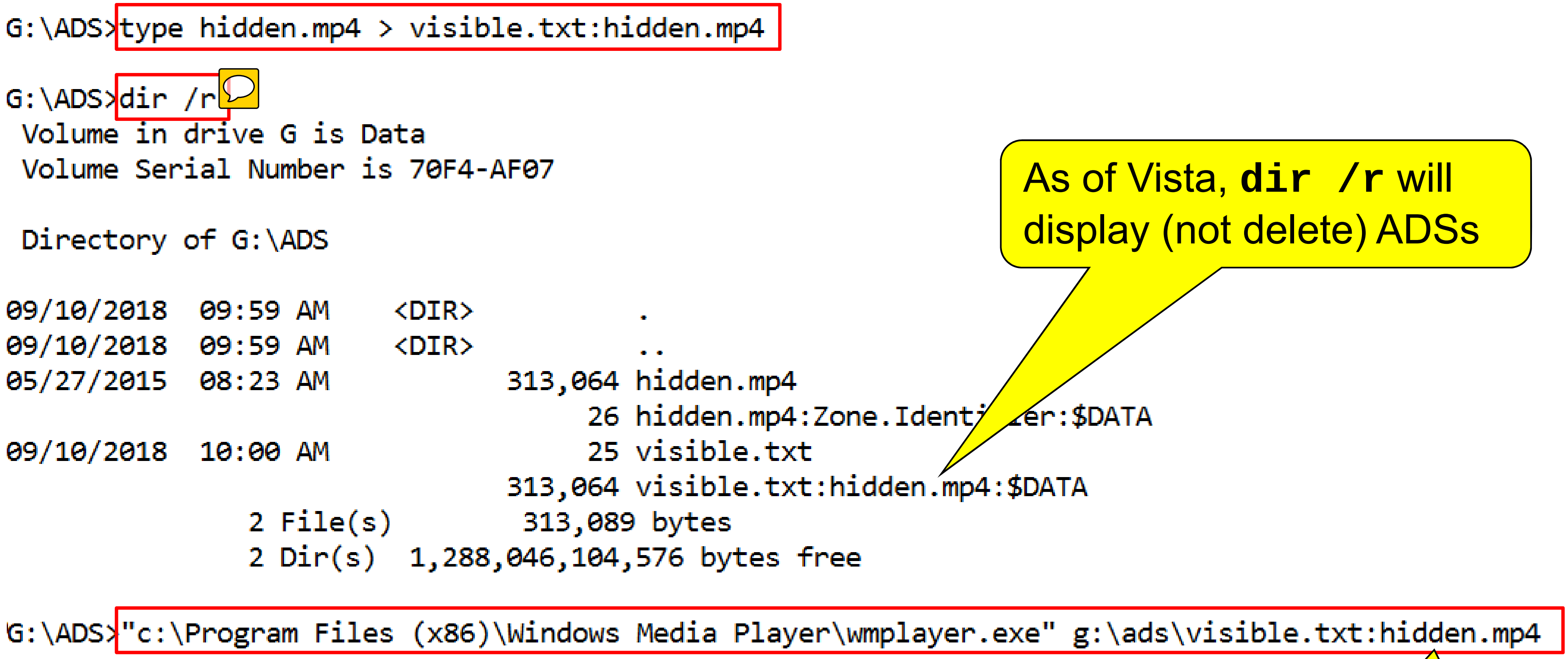
```
type evil.exe > good.txt:evil.exe
start .\good.txt:evil.exe
```

Example: Hiding Video Files in NTFS



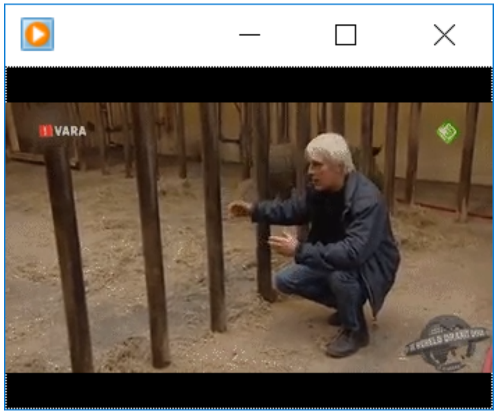
```
G:\ADS>echo This is a visible file > visible.txt

G:\ADS>dir
 Volume in drive G is Data
 Volume Serial Number is 70F4-AF07

 Directory of G:\ADS

09/10/2018  09:59 AM    <DIR>          .
09/10/2018  09:59 AM    <DIR>          ..
05/27/2015  08:23 AM           313,064 hidden.mp4
09/10/2018  09:59 AM                25 visible.txt
               2 File(s)        313,089 bytes
               2 Dir(s)  1,288,046,288,896 bytes free
```

Example: Hiding Video Files in NTFS



```
G:\ADS>type hidden.mp4 > visible.txt:hidden.mp4

G:\ADS>dir /r
 Volume in drive G is Data
 Volume Serial Number is 70F4-AF07

 Directory of G:\ADS

09/10/2018  09:59 AM    <DIR>          .
09/10/2018  09:59 AM    <DIR>          ..
05/27/2015  08:23 AM           313,064 hidden.mp4
                                    26 hidden.mp4:Zone.Identifier:$DATA
09/10/2018  10:00 AM                25 visible.txt
                               313,064 visible.txt:hidden.mp4:$DATA
               2 File(s)        313,089 bytes
               2 Dir(s)  1,288,046,104,576 bytes free

G:\ADS>"c:\Program Files (x86)\Windows Media Player\wmplayer.exe" g:\ads\visible.txt:hidden.mp4
```

As of Vista, **dir /r** will display (not delete) ADSs

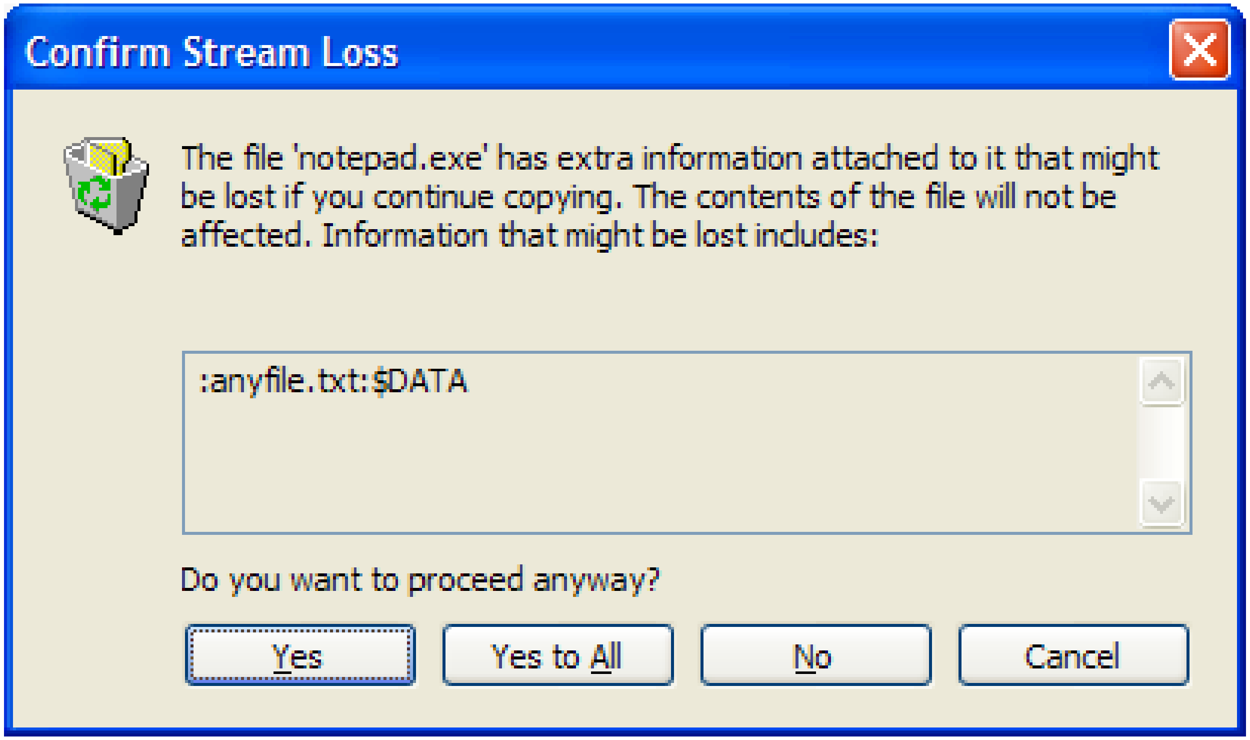


Can even play the hidden video

Alternate Data Streams in NTFS

- The hidden file in the stream will follow the other file around through normal copying between NTFS partitions

- Most, if not all, Internet protocols do NOT support ADS
  - The stream is removed during the copy



Confirm Stream Loss

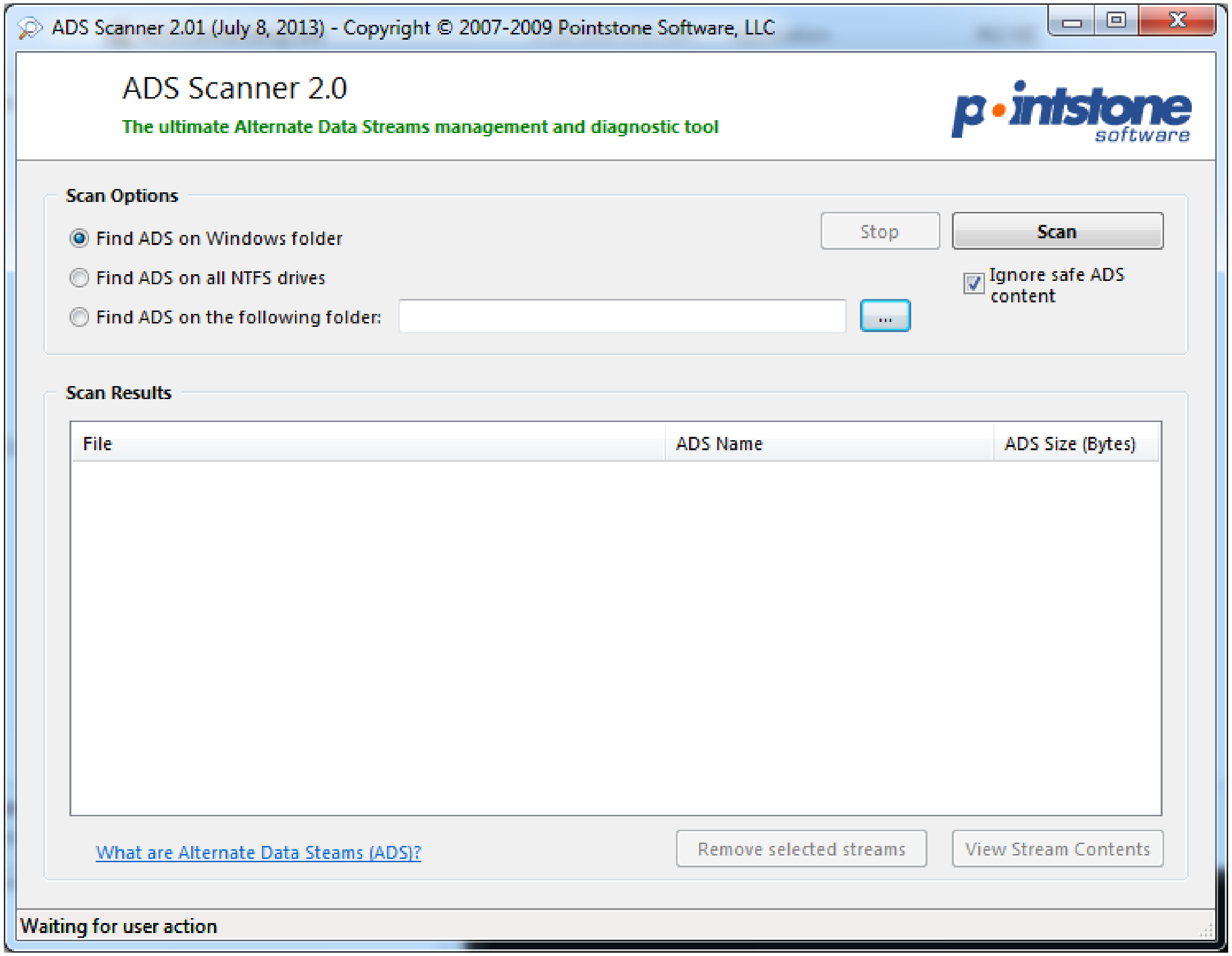
The file 'notepad.exe' has extra information attached to it that might be lost if you continue copying. The contents of the file will not be affected. Information that might be lost includes:

:anyfile.txt:$DATA

Do you want to proceed anyway?

Tools To Detect And Remove Streams

- LADS (List ADS) – command line - scans entire drive or given directory and lists the names and size of all ADSs it finds
- ADS Scanner 2 – www.pointstone.com/products/ADS-Scanner/



ADS Scanner 2.01 (July 8, 2013) - Copyright © 2007-2009 Pointstone Software, LLC

ADS Scanner 2.0

The ultimate Alternate Data Streams management and diagnostic tool

Scan Options

● Find ADS on Windows folder

○ Find ADS on all NTFS drives

○ Find ADS on the following folder:

☑ Ignore safe ADS content

Scan Results

File	ADS Name	ADS Size (Bytes)

What are Alternate Data Steams (ADS)?

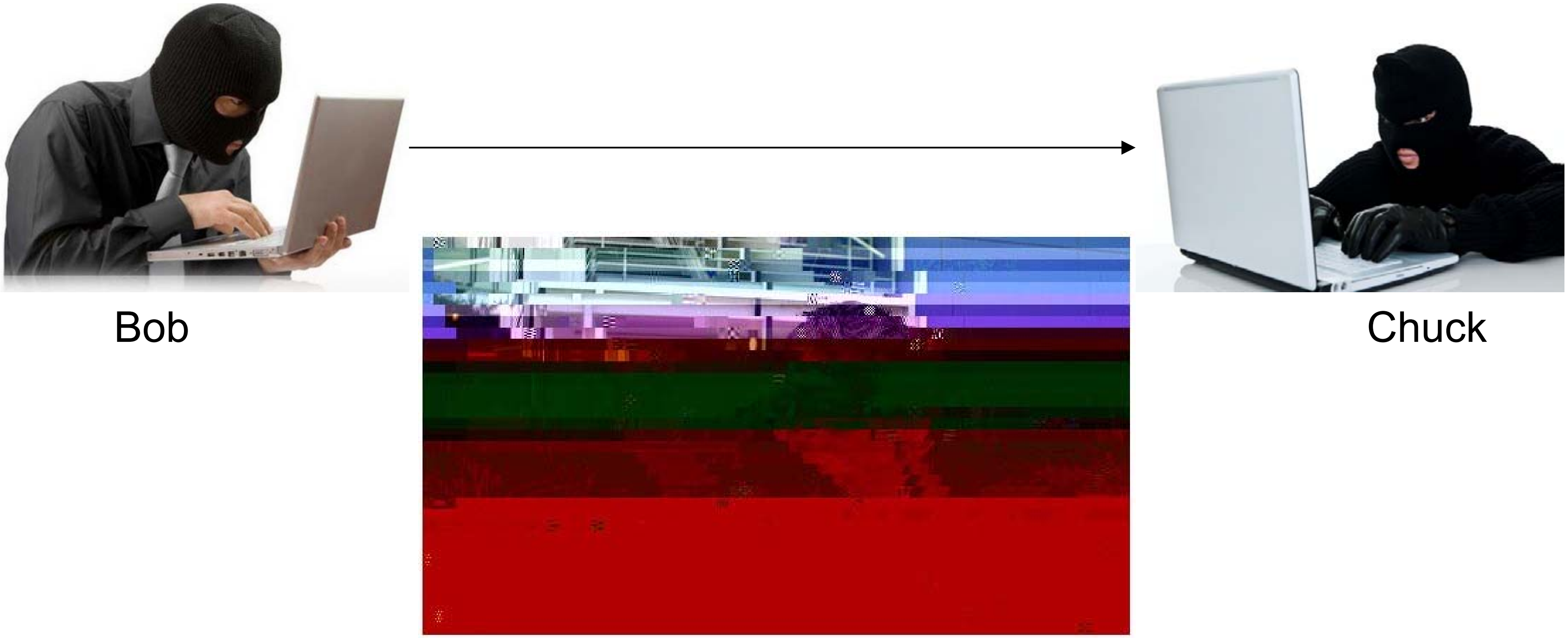
Waiting for user action

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding
  - Altering Event Logs
  - Covert Channels

Covert Channels – It Can Be Quite Easy

- Terrorist Bob purposely corrupts a file signature (magic numbers)
- Sends to terrorist Chuck who reverses the process
- Anyone intercepting the file will see it is corrupt and disregard

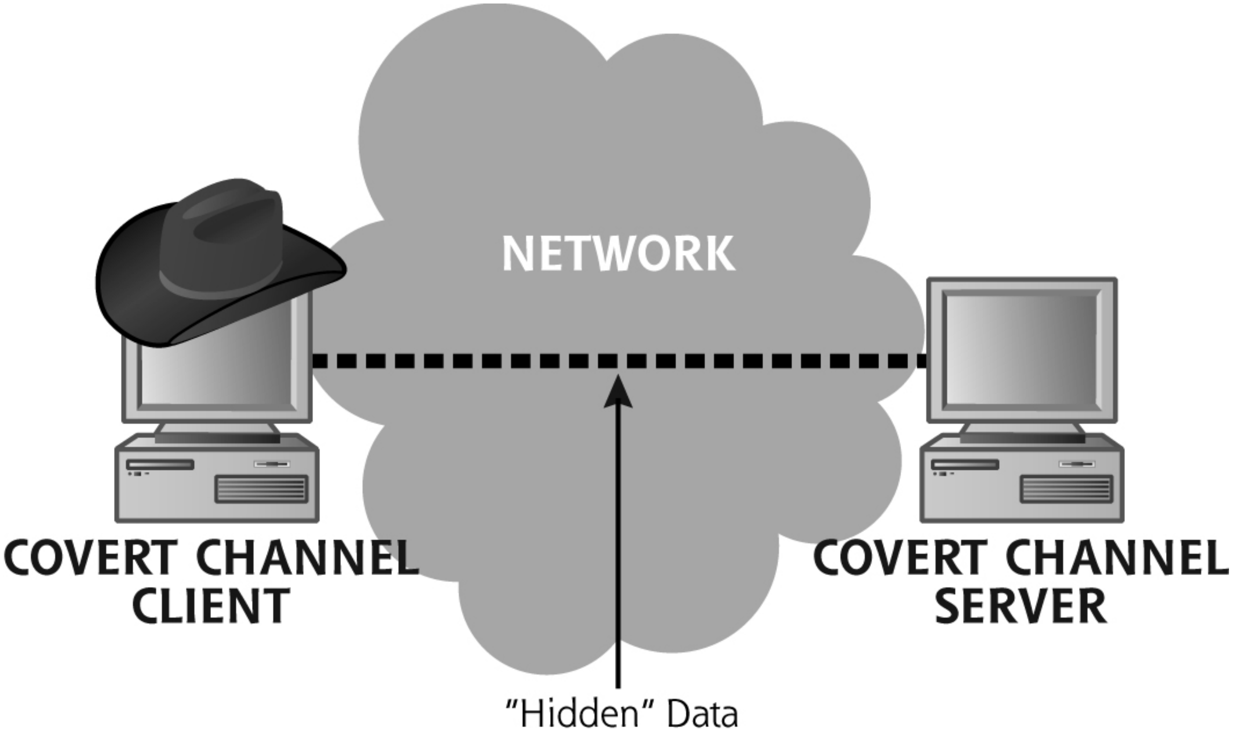


Tunneling and Covert Channels

- Attackers need a way to communicate with their evil programs
- You can carry any protocol on top of any other protocol
  - First protocol is encapsulated inside packets of second protocol
    - Network only sees second "outer" protocol
    - FTP over SSH
    - IP inside of IP
    - VPNs

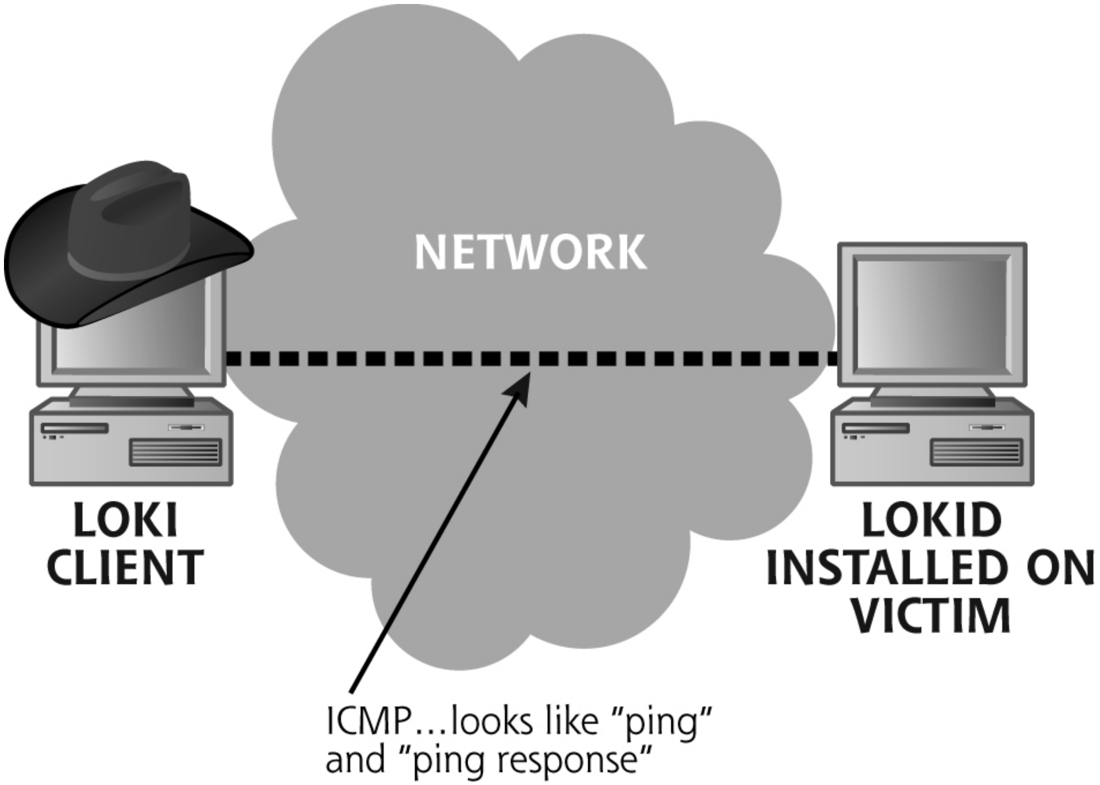
Tunneling and Covert Channels

- Covert channels require
  - Server on the victim machine
  - Client on the attacker's machine
- Attacker wants to hide the fact that he is moving data or issuing commands to the victim



Covert Channels Using ICMP: Loki

- Pronounced "Low Key" – and it's covert… Get it?
- Tunnels shell sessions over innocuous-looking protocols
  - ICMP (looks like ping)
  - UDP port 53 (looks like DNS queries and responses)
- Think of it as a telnet over ICMP (ping)
- Offers a command shell on the victim machine to attacker

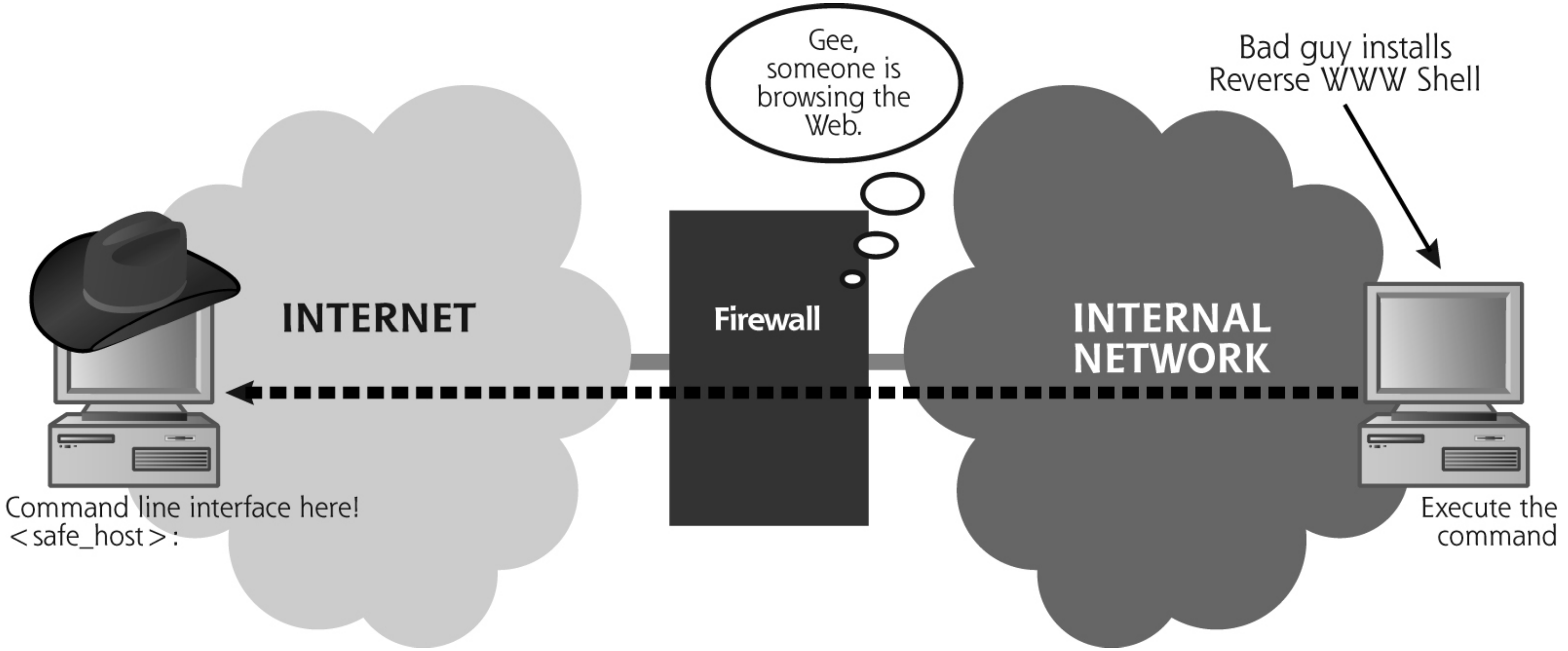

NETWORK
LOKI CLIENT
LOKID INSTALLED ON VICTIM
ICMP…looks like "ping" and "ping response"

Covert Channels Using ICMP: Loki

- Can also encrypt traffic
- Code at www.phrack.org/issues.html?issue=51&id=6
- Very effective for covert sessions
  - ICMP messages do not require an open port
  - Only trace of the Loki daemon is a root-level process and ICMP packets going back and forth
  - What if ICMP is blocked…

Covert Channels Using HTTP: Reverse WWW Shell

- Get a command shell on a machine behind a firewall
- Requires the attacker to place a server on an internal host


Gee, someone is browsing the Web.
Bad guy installs Reverse WWW Shell
INTERNET
Firewall
INTERNAL NETWORK
Command line interface here!
<safe_host>:
Execute the command

Covert Channels Using HTTP: Reverse WWW Shell

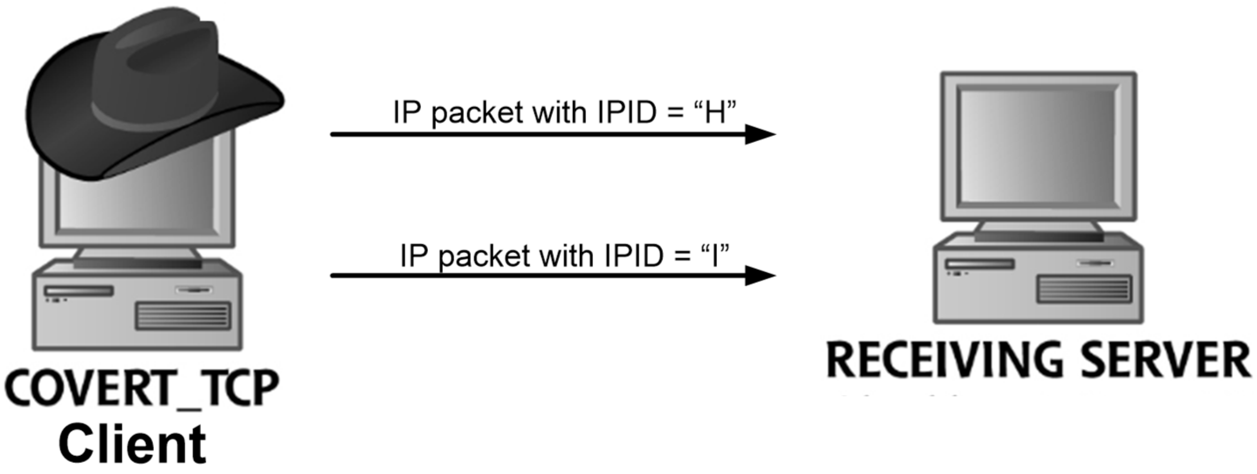
- At certain time intervals (e.g., 60 sec), the server "surfs" out to pick up commands
- Looks like an HTTP “GET” going out to the Internet
- Shell runs on internal host with input from external system!
- Attacker has to wait the 60 seconds before command is executed
  - Attacker could shorten this interval but not too short
    - Shorter intervals may be noticed as something suspicious
- freeworld.thc.org/releases.php

Covert Channels Using TCP/IP Headers

- Creates a covert channel using unused fields in TCP or IP header
- Covert_TCP is a Linux tool that implements a covert channel using either the TCP or IP header
- Designed to transfer ASCII files in
  - IP Identification field
  - TCP Sequence Number field
  - TCP Acknowledgement Number field
- Client and server are the same executable
  - Client sets up TCP connection and sends packets (no payload)
- Sends one byte per packet
- https://github.com/cudeso/security-tools/blob/master/networktools/covert/covert_tcp.c

Covert_TCP Modes

- IP ID Mode



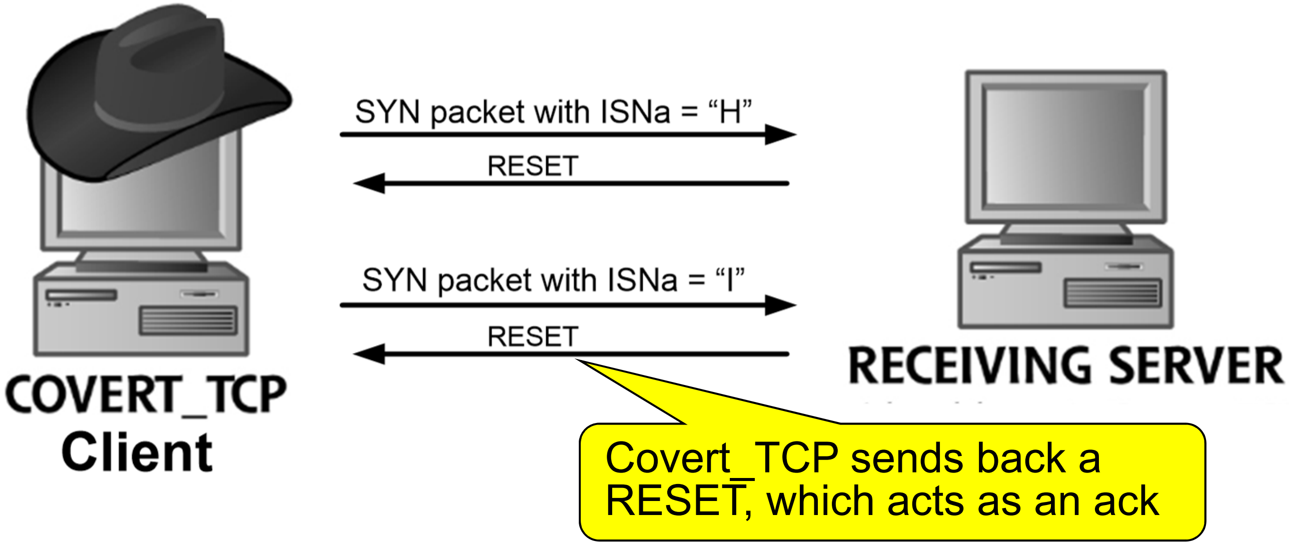
COVERT_TCP Client

IP packet with IPID = "H"

IP packet with IPID = "I"

RECEIVING SERVER

- TCP Seq # Mode



COVERT_TCP Client

SYN packet with ISNa = "H"

RESET

SYN packet with ISNa = "I"

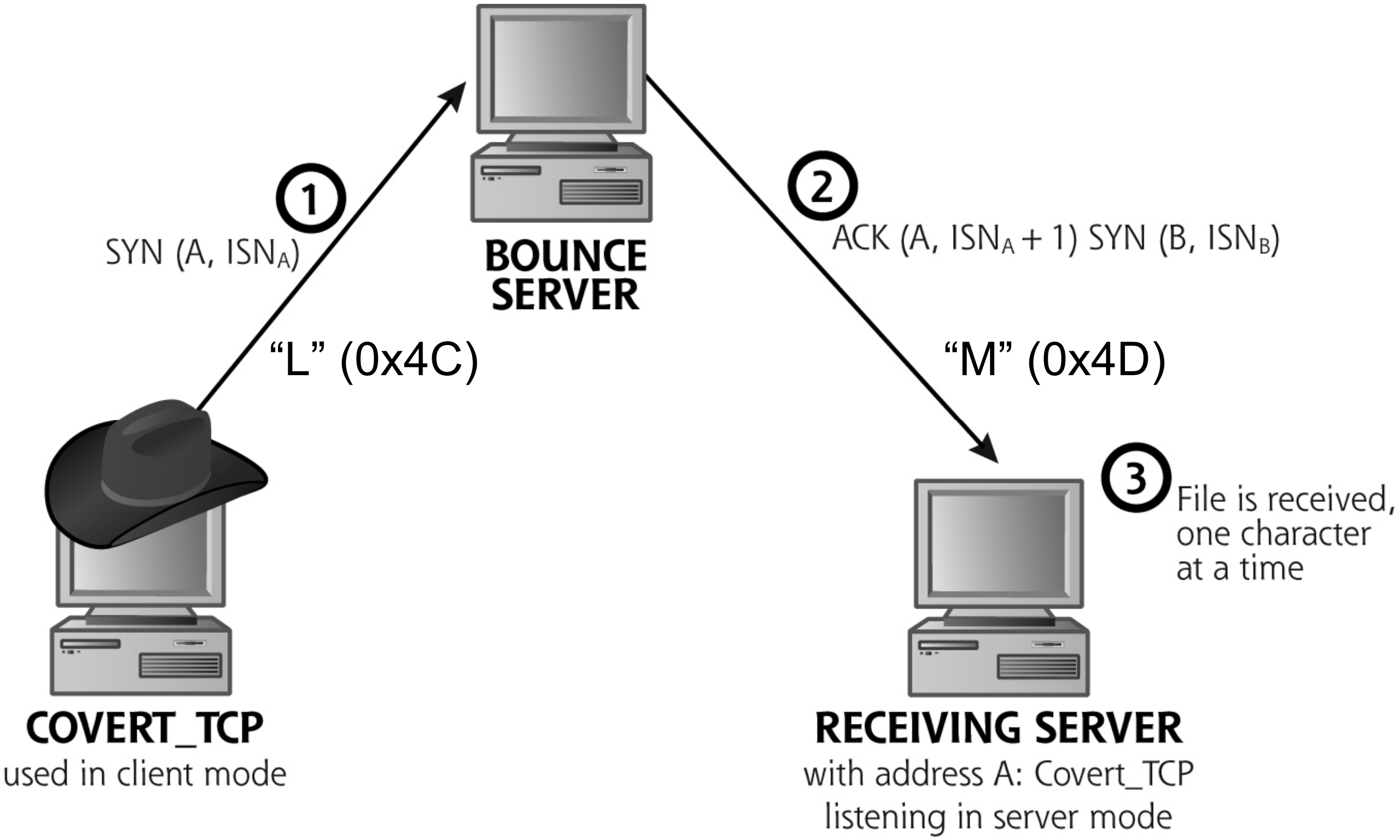
RESET

RECEIVING SERVER

Covert_TCP sends back a RESET, which acts as an ack

Covert TCP Bounce Mode

- TCP Ack Mode (also known as "bounce" mode)
  - ISNa needs to be one less than ASCII char to be transmitted
    - Send "L" (0x4C) if you want the server to recv "M" (0x4D)

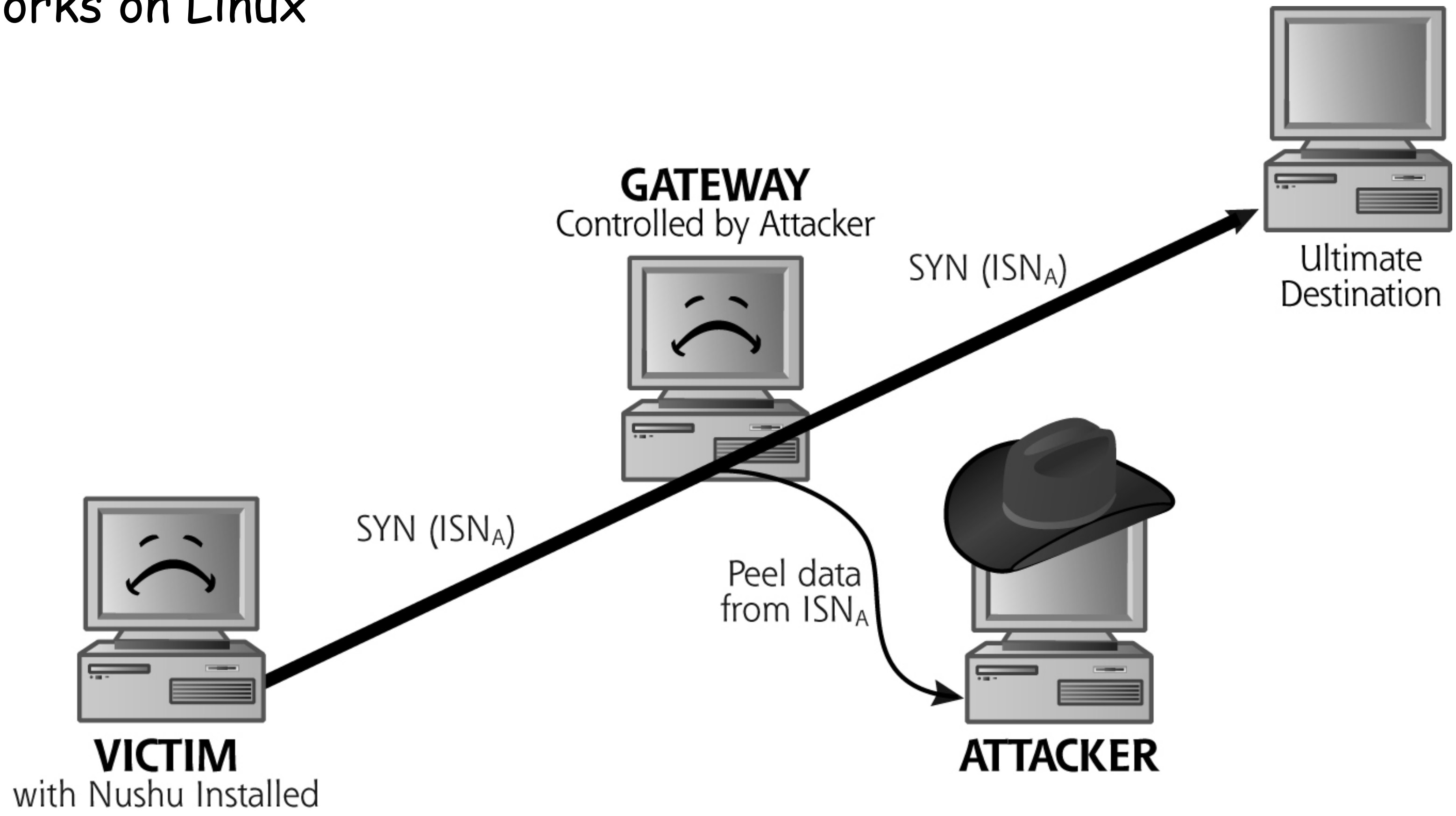

1
SYN (A, ISNA)
"L" (0x4C)
BOUNCE SERVER
2
ACK (A, ISNA + 1) SYN (B, ISNB)
"M" (0x4D)
3
File is received, one character at a time
COVERT_TCP
used in client mode
RECEIVING SERVER
with address A: Covert_TCP listening in server mode

Passive Covert Channels

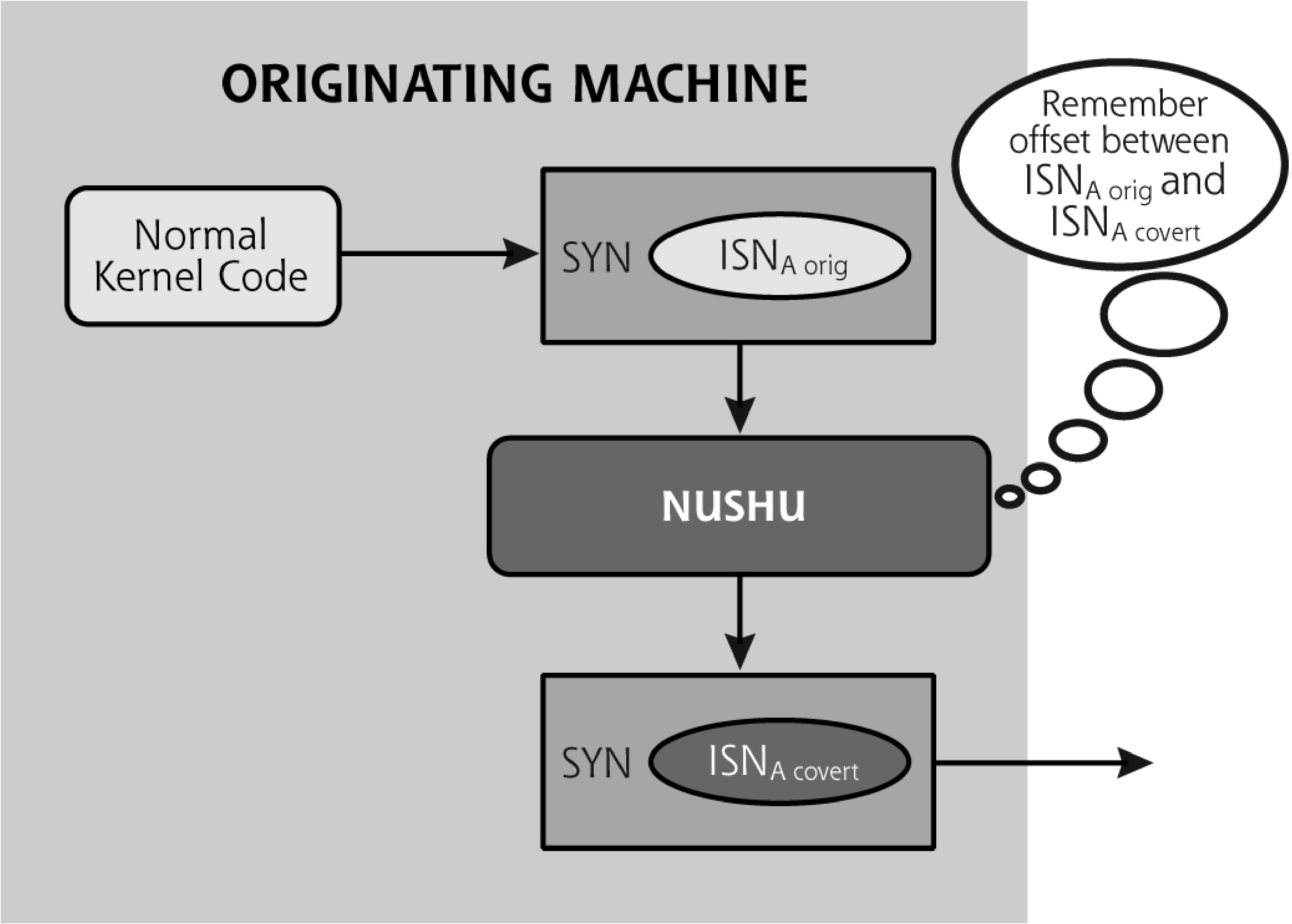
- Most covert channels generate their own packets hiding the data inside those packets
  - Covert_TCP, Loki, ICMP tunnel, etc.
- Passive covert channels use existing packets inserting their data inside
- Technique implemented in Nushu
  - Named after a secret language created by Chinese women centuries ago
  - Characters disguised as decorative marks or as part of artwork

Passive Covert Channels in Action

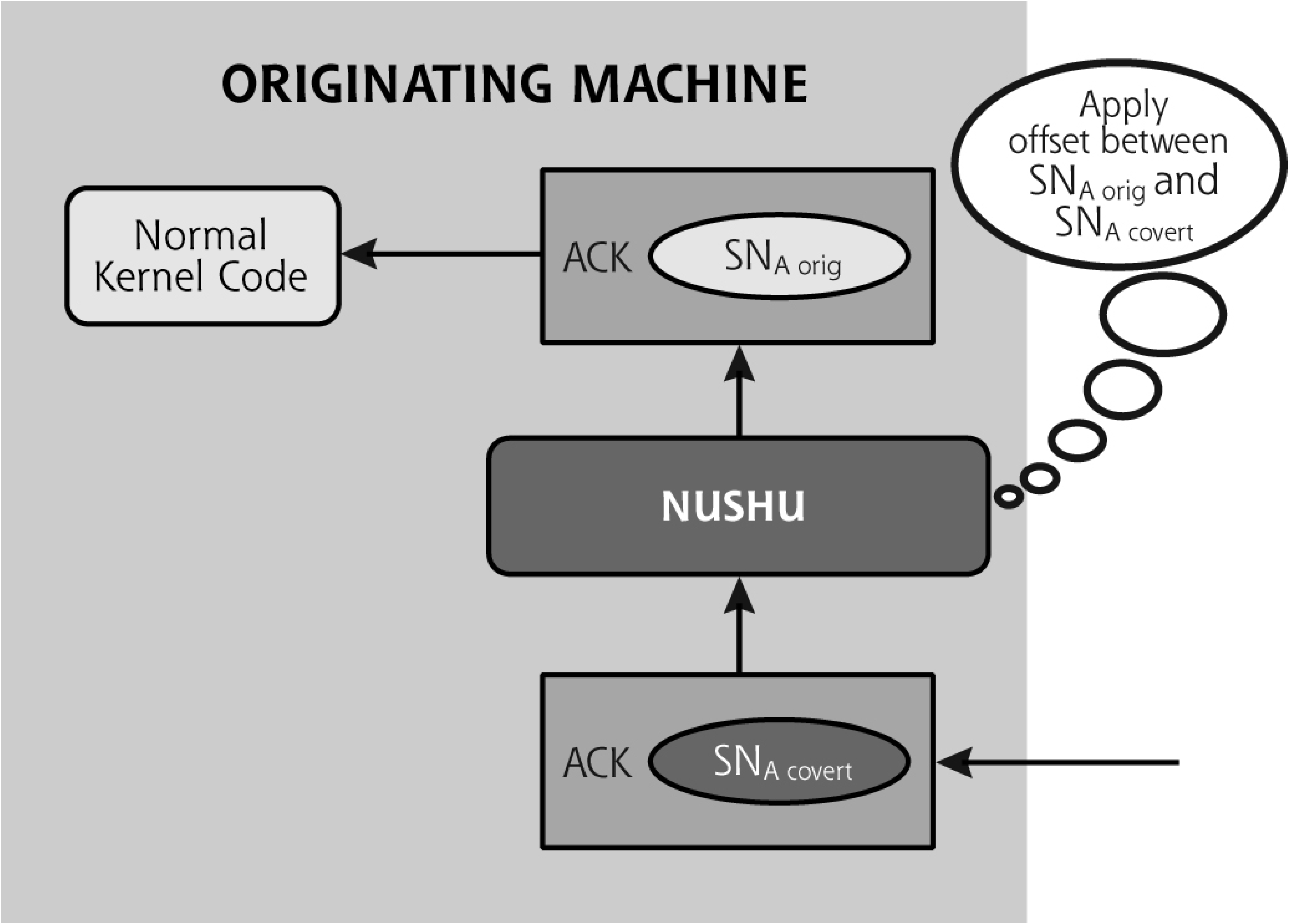
- Send data inside of SYN packets by tweaking ISNa to include data
- Strip data off while its on its way to destination using a gateway controlled by the attacker and running Nushu server
- Works on Linux



Substituting ISNA

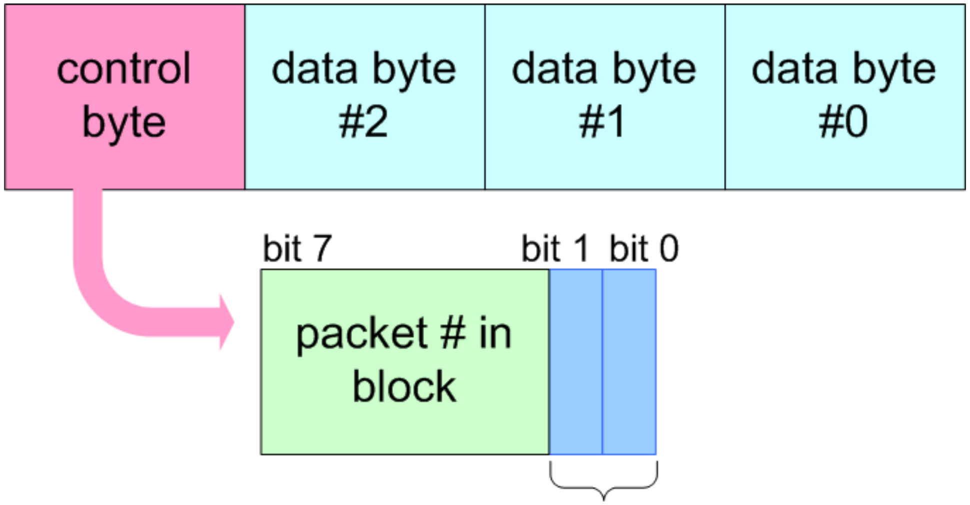


Dealing with ACKs



Nushu - Data Format

- Format for the initial sequence number (ISN) in the SYN packet
  - Can only carry 3 bytes per new TCP connection
  - Still a "reasonable" data channel if someone is surfing the web
- Interesting anomaly
  - Local tcpdump of packets have different sequence numbers than network-sniffed packets!



control byte

data byte #2

data byte #1

data byte #0

bit 7

bit 1

bit 0

packet # in block

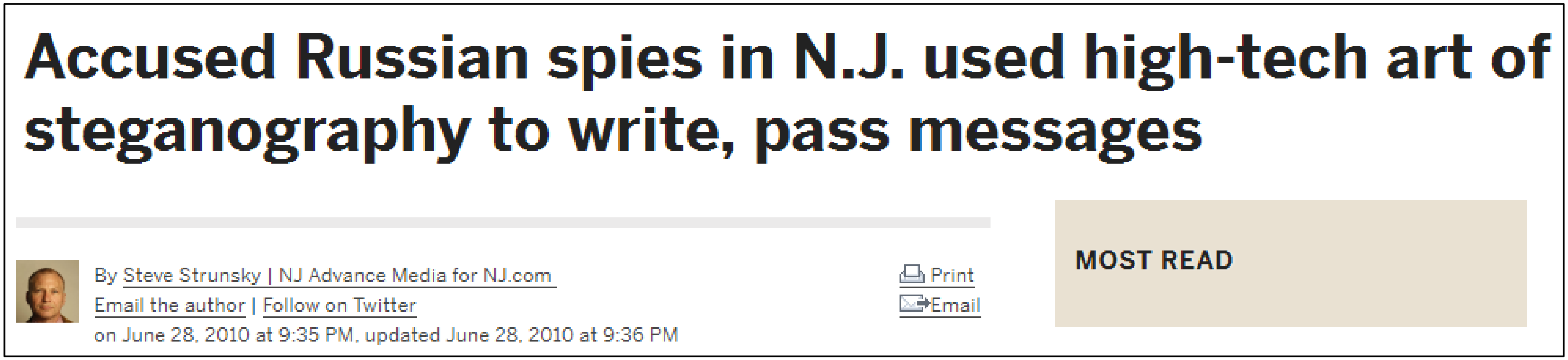
# of actual data bytes sent in this packet:
00: no data (control packet)
01: b0 is valid
10: b0 & b1 are valid
11: b0, b1 & b2 are valid

Covert Channels Using Steganography

- Steganography
  - From the Greek word steganos meaning “covered”
  - the Greek word graphie meaning “writing”
- Steganography is the process of hiding a secret message within an ordinary message and extracting it at its destination
- Although information can be hidden in almost any type of file, multimedia files are the most common carriers
- Digital images are good candidates for carriers
  - Commonly used -- not suspicious
  - Easily transported
  - Compression errors (noise) can mask errors introduced by payload
  - Anyone else viewing or listening to the file will fail to know it contains hidden/encrypted data

Steganography Uses

- Legitimate uses
  - Watermarking for copyright protection
  - Tagging images
- Illegitimate uses
  - Espionage
  - Concealing evidence
  - Covert communication



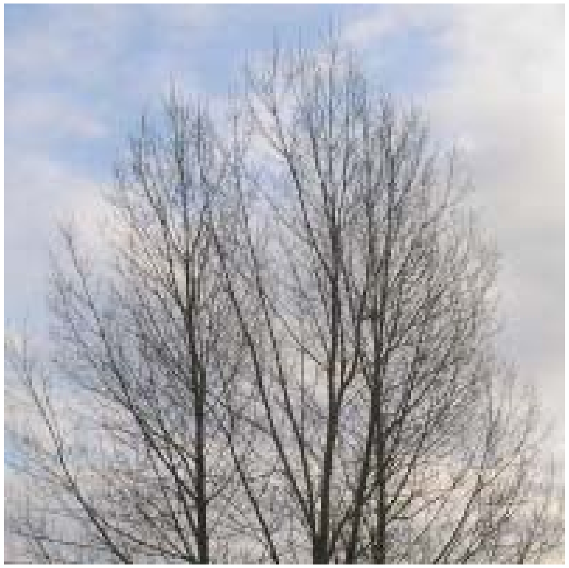
Accused Russian spies in N.J. used high-tech art of steganography to write, pass messages

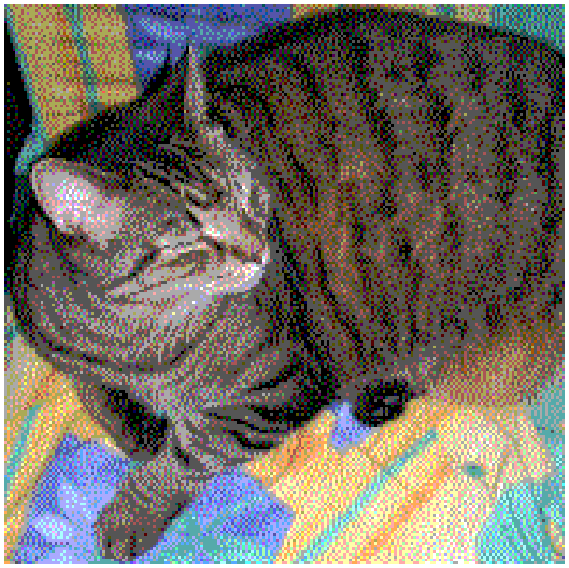
By Steve Strunsky | NJ Advance Media for NJ.com
Email the author | Follow on Twitter
on June 28, 2010 at 9:35 PM, updated June 28, 2010 at 9:36 PM

http://www.nj.com/news/index.ssf/2010/06/accused_russian_spies_in_nj_us.html

Steganography Example

- Picture of the cat is embedded in the picture of the tree
  - Do you see the cat in the tree?





Steganography vs. Cryptography

- Crypto – Observer can see there is a message but cannot read it
- Stego – Observer doesn’t even know the message exists
- Steganography deals with the concealment of a message, not the encryption of it
- Steganalysis → Identifying the existence of a hidden message
  - Not extracting the message

Steganography - Hiding Techniques

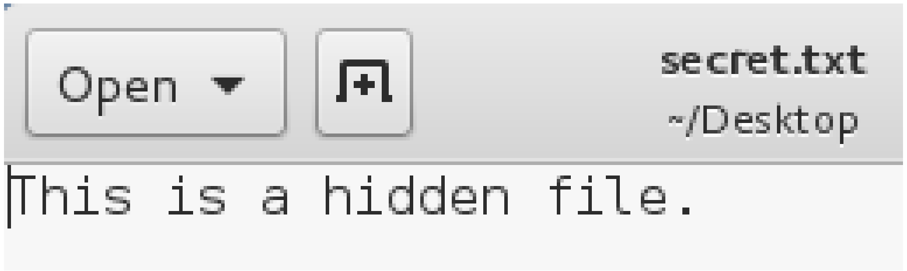
- Append information to a file
- Hide in unused portions of file header (PE header) or Code Cave
- Disperse hidden message/file throughout the file using algorithm
  - Modification of LSB (Least Significant Bit)
  - Many other techniques!
- Can be as simple as un-cropping a image

StegHide - One Tool… of many

- Supports (JPG, BMP, WAV, AU)
  - Linux (Kali: **`apt install steghide`**) or Windows XP
  - steghide.sourceforge.net/index.php

`carrier_image.jpg`

`secret.txt`



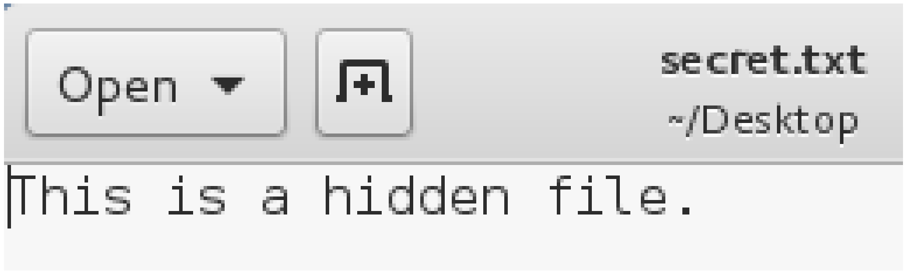
```
This is a hidden file.
```

Steganography - StegHide Embedding

```
# steghide embed -cf carrier-image.jpg -ef secret.txt
-sf stegofile.jpg
Enter passphrase:
Re-Enter passphrase:
embedding "secret.txt" in "carrier-image.jpg"... done
writing stego file "stegofile.jpg"... done
```

carrier_image.jpg

secret.txt



This is a hidden file.

Steganography - StegHide Detecting

```
# steghide info stegofile.jpg
"stegofile.jpg":
  format: jpeg
  capacity: 1.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "secret.txt":
    size: 23.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

Steganography - StegHide Extracting

```
# steghide extract -xf out.txt -sf stegofile.jpg
Enter passphrase:
wrote extracted data to "out.txt".
```