Trojans and Backdoors

Introduction

- A backdoor is a program that allows attackers to bypass normal security controls on a system, gaining access on the attacker's own terms.
  - Malware: Fighting Malicious Code

Introduction

- Backdoors simply give access. Trojan horses, pretend to be some useful program. Of course some tools are both backdoors and Trojan horses at the same time.
- A backdoor is only a Trojan horse if the attacker attempts to dress it up as some useful program. These are called Trojan horse backdoors, because they give access while pretending to be some benign program.

Different types of access

- *Local Escalation of Privilege*: This type of backdoor lets attackers with an account on the system suddenly change their privilege level to root or administrator. With these superuser privileges, the attacker can reconfigure the box or access any files stored on it.

Different types of access

- *Remote Execution of Individual Commands*: Using this type of backdoor, an attacker can send a message to the target machine to execute a single command at a time. The backdoor runs the attacker's command and returns the output to the attacker.

Different types of access

- *Remote Command-Line Access*: Also known as remote shell, lets the attacker type directly into a command prompt of the victim machine from across the network. The attacker can utilize all of the features of the command line, including the ability to run a series of commands, write scripts, and select groups of files to manipulate.

Different types of access

- *Remote Control of the GUI*: Rather than messing around with command lines, some backdoors let an attacker see the GUI of the victim machine, control mouse movements, and enter keystrokes, all across the network. With remote control of the GUI, the attacker can watch all of a victim's actions on the machine or even remotely control the GUI.

Installing backdoors

- gain access to the system through some common exploit, such as a buffer overflow or typical system misconfiguration.
- using an automated program such as the viruses, worms etc.
- tricking the victim user into installing it.
- Tricking users into running a malicious program by making it sound useful is really an example of a Trojan Horse technique

Starting Backdoors Automatically

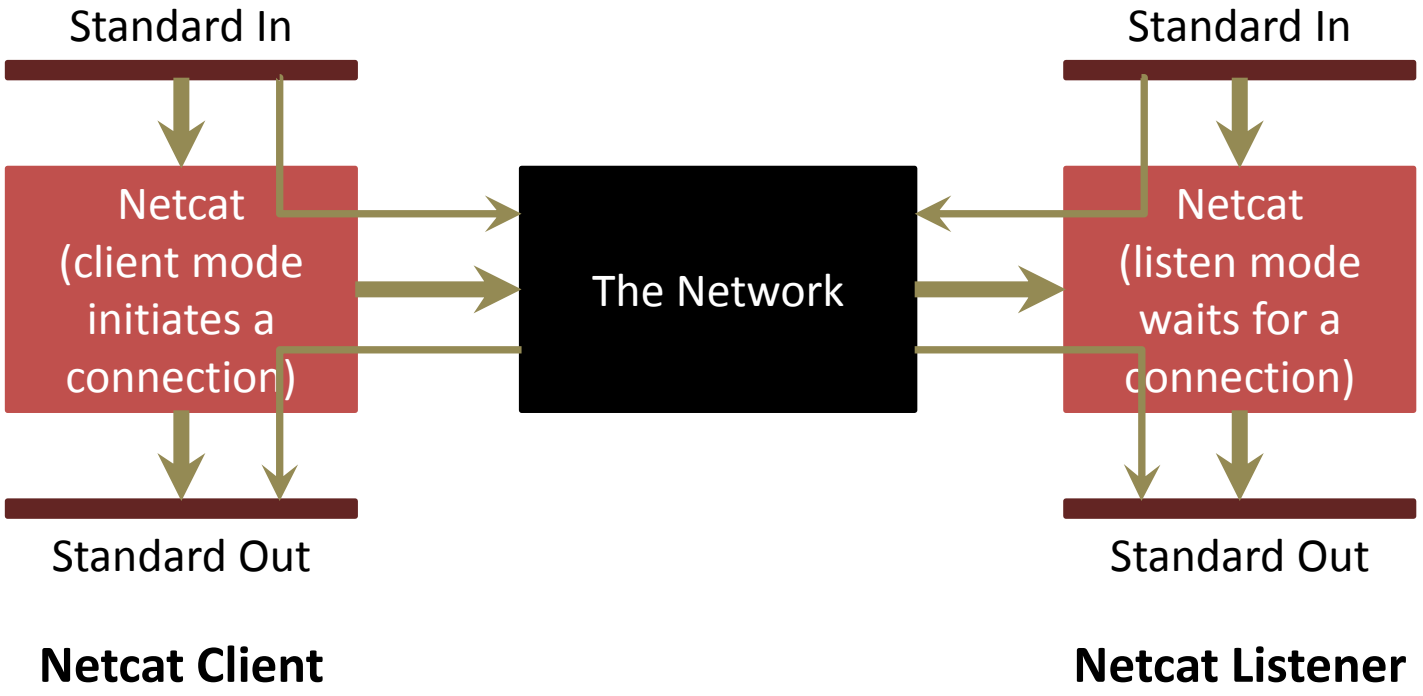
- Altering Startup Files and Folders
- Registry Abuses
- Undermining the Task Scheduler

- Modifying the inittab Config

Netcat

- Netcat takes Standard In and Standard Out and connects them to the network on any TCP or UDP port.
- Netcat operates in two modes: client mode and listen mode.
  - Client mode initiates a connection across a network.
  - Listen mode, listens for data to come in from the network.

Netcat Backdoor Shell Listener

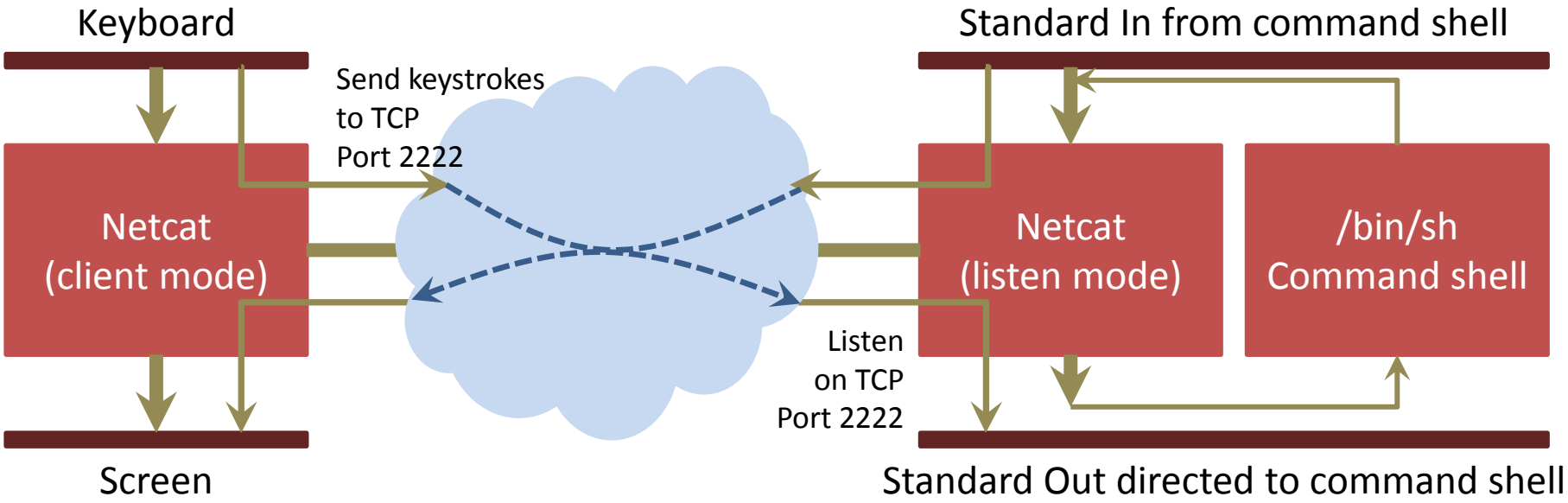


Netcat Backdoor Shell Listener

- nc [options] target_system_name [remote_port]
- nc –l –p 2222 –e cmd.exe

- -l: Listen Mode
- -L: "Listen Harder" Mode
- -u: UDP Mode
- -p: Local Port
- -e: Execute

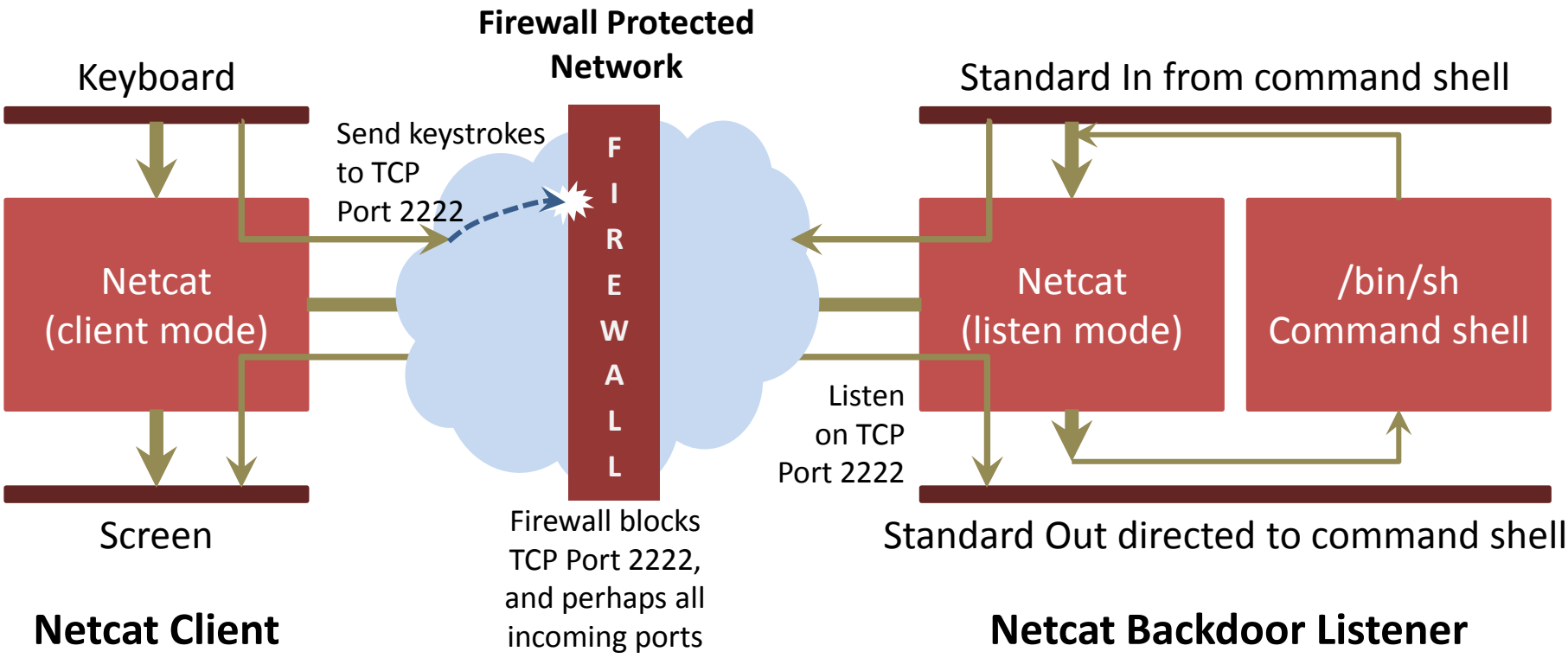
Netcat Backdoor Shell Listener



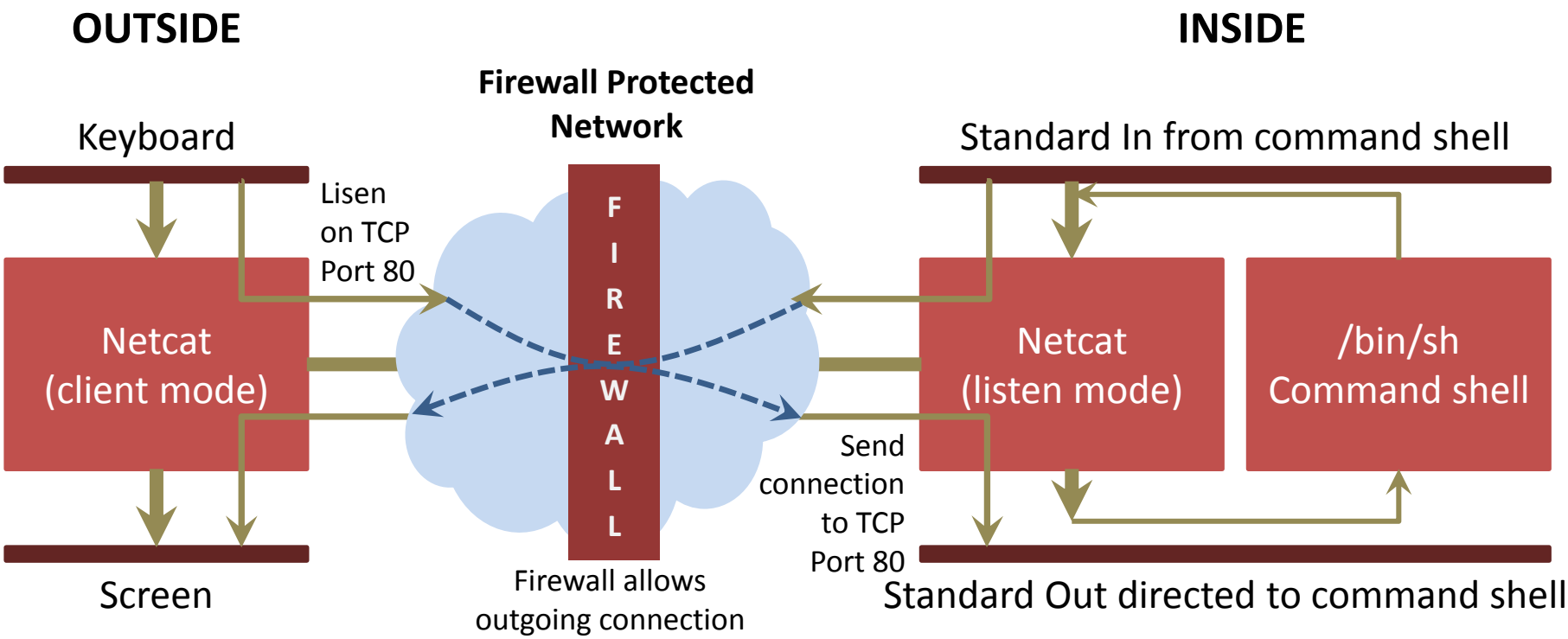
Netcat Client

Netcat Backdoor Listener

Limitation of Simple Netcat Backdoor Shell Listener



Shoveling a Shell with Netcat Backdoor Client



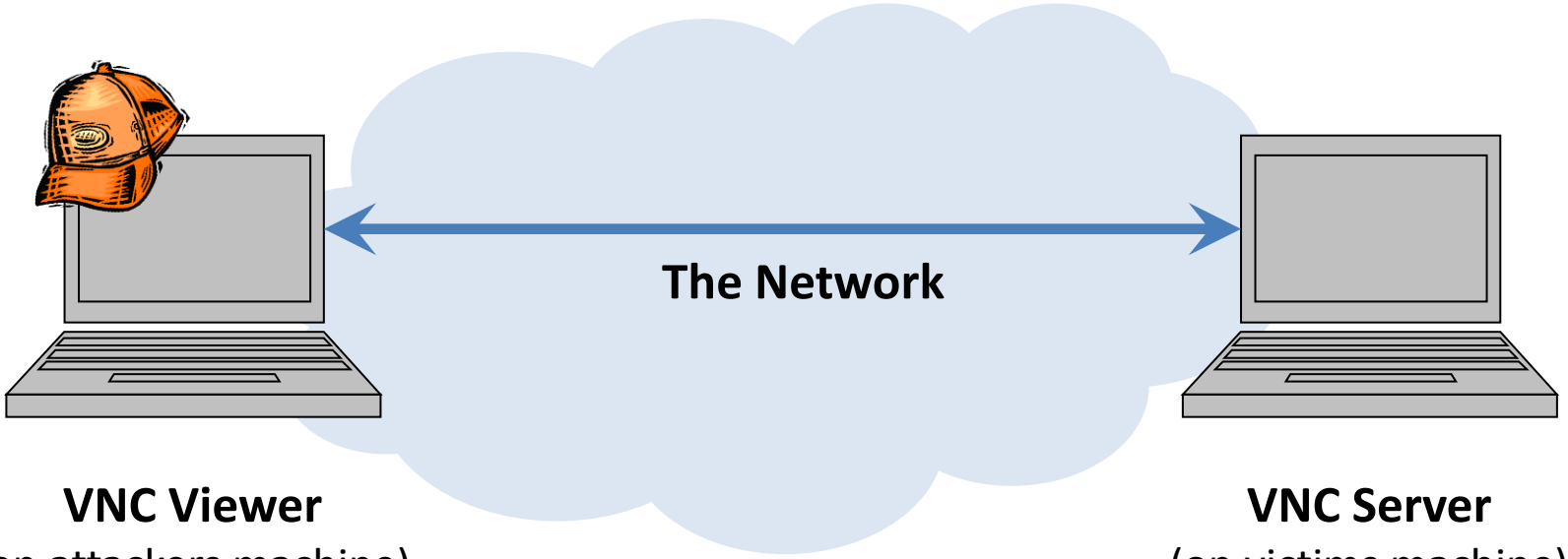
Defenses against Backdoor Shell Listeners

- carefully hardening your machine and applying patches on a regular basis
- make sure you deploy network firewalls that allow only those services for which you have an explicit business need
- conduct periodic port scans of your machines to find backdoor shell listeners that use TCP and UDP ports – nmap, netstat, fport, TCPview

GUIs Across the Network

- attackers desires control of the GUI, viewing the screen of the victim machine, moving its mouse, and sending in keystrokes

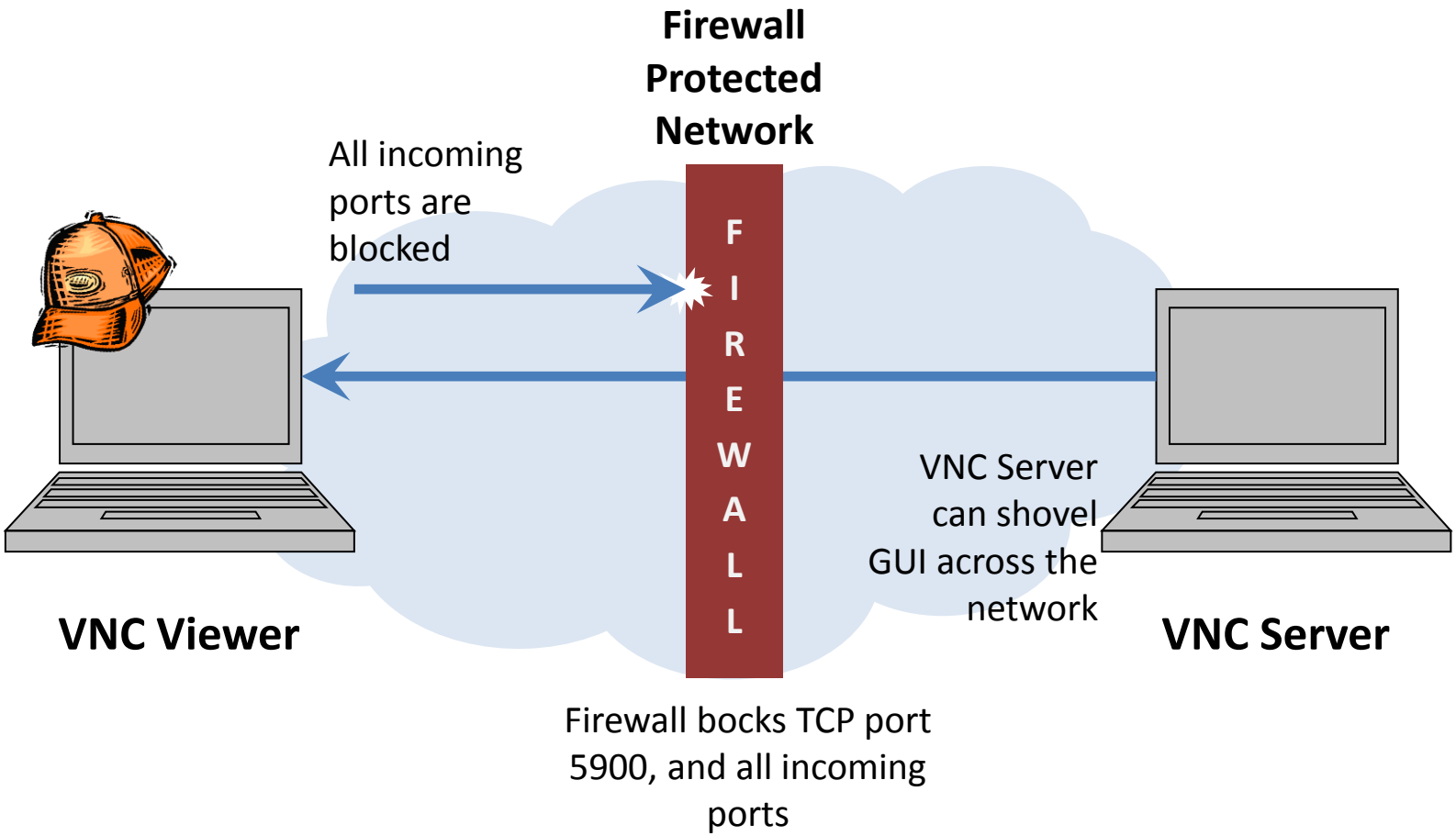
Controlling a VNC server using the VNC Viewer



VNC Viewer
(on attackers machine)

VNC Server
(on victims machine)

Shoveling a GUI with VNC



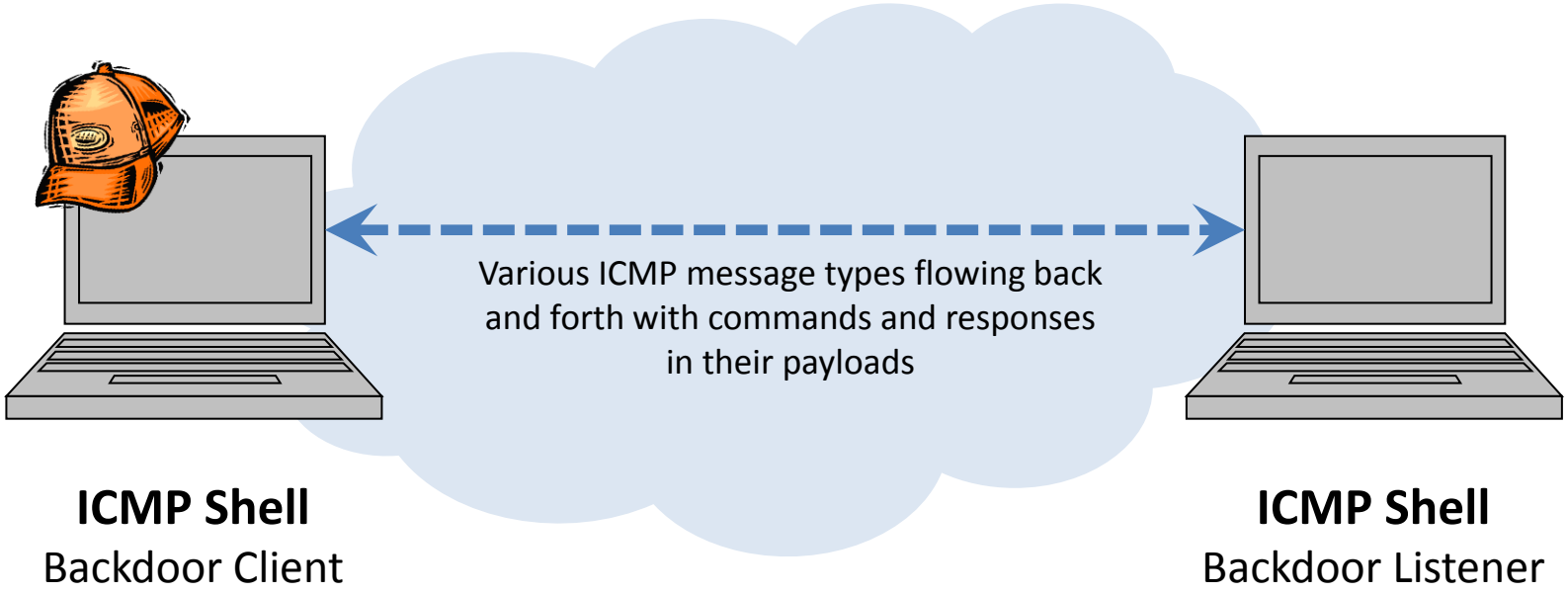
Remote Installation of Windows VNC

- Gain remote shell access
- Installs a copy of Windows VNC on his or her own local machine and configures it.
- Exports the registry keys associated with WinVNC from own system.
- Moves a copy of four files to the target system: Vnc.reg, as well as WinVNC.exe, Omnithread.dll, and VNCHooks.dll from the standard VNC installation.
- Using the remote shell to execute commands on the victim machine, the attacker loads the registry settings into the target system using the following command:
  - C:\> regedit /s vnc.reg
- Now, the attacker installs the VNC server running in Service Mode using this command:
  - C:\> winvnc –install
- Finally, the attacker executes one more command to start up the service:
  - C:\> net start winvnc

Backdoors without ports

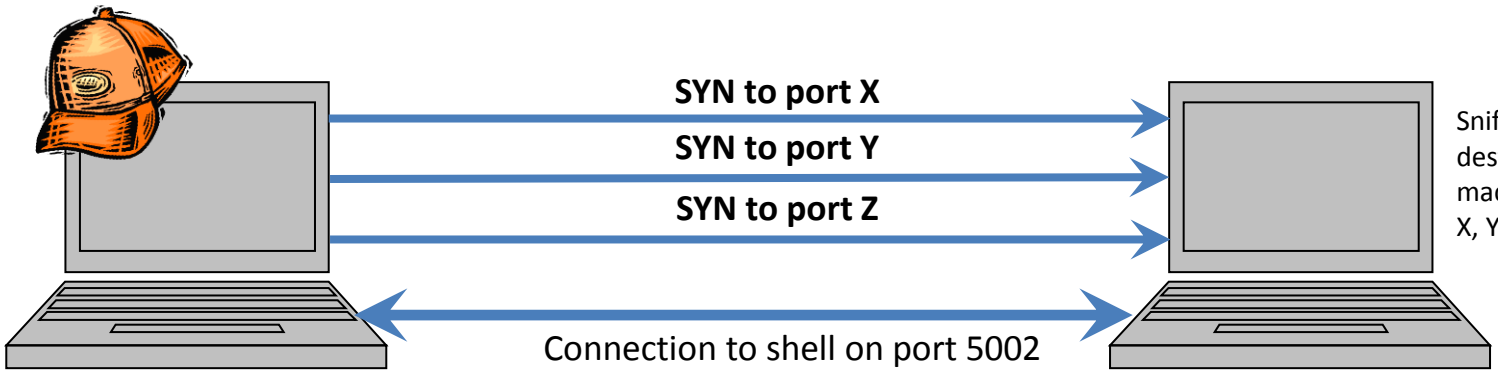
- ICMP backdoors

Using ICMP listeners for backdoors to avoid TCP and UDP ports



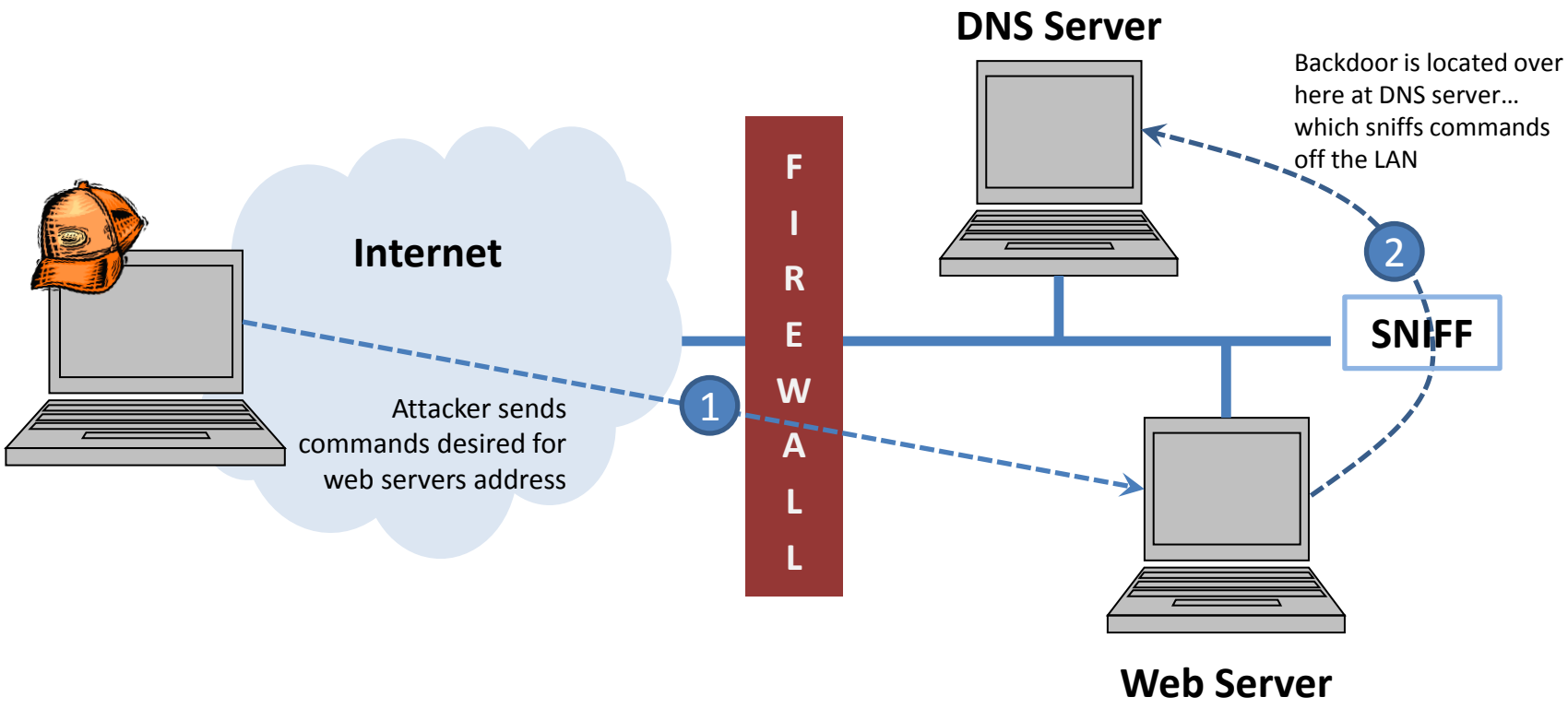
Non-promiscuous Sniffing Backdoors

The Cd00r non-promiscuous sniffing backdoor in action

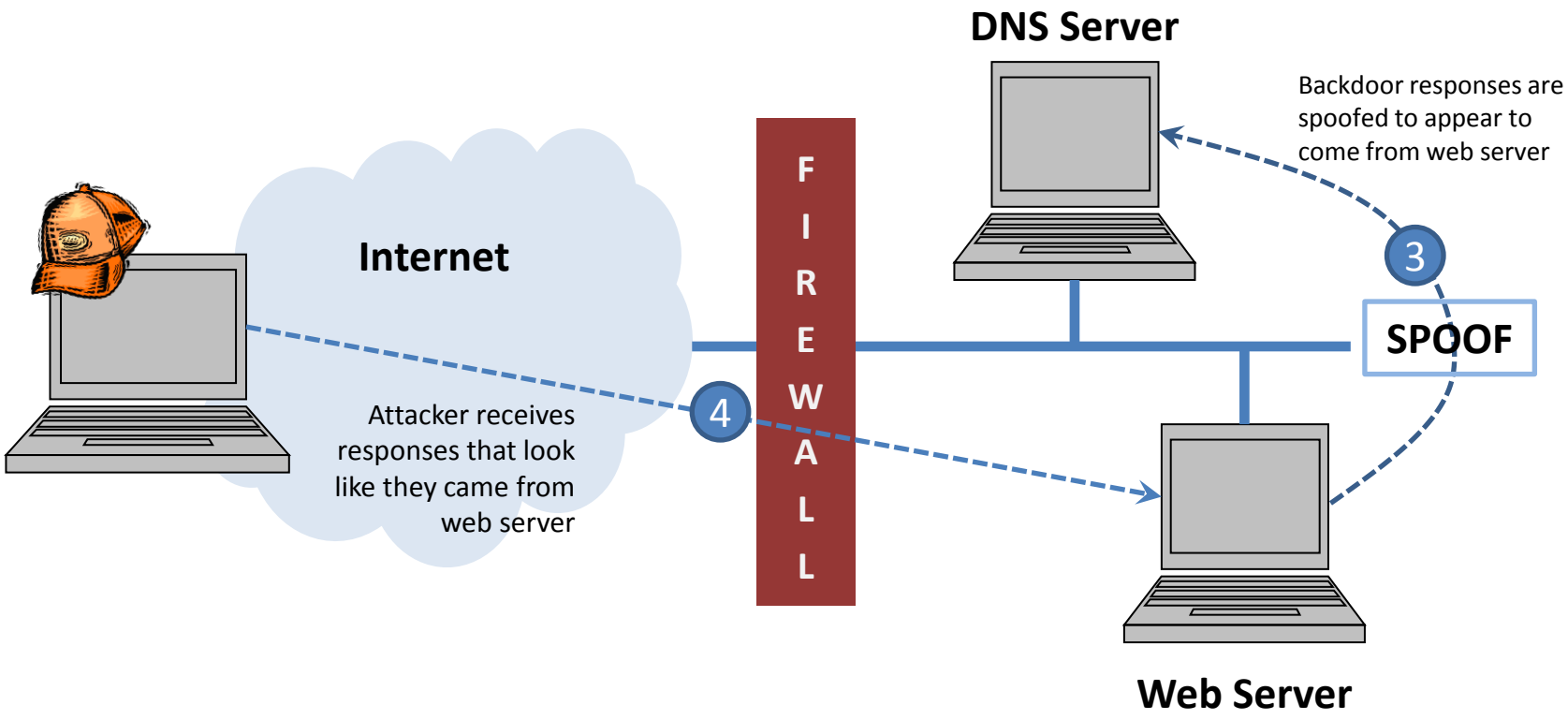


Promiscuous Sniffing Backdoors

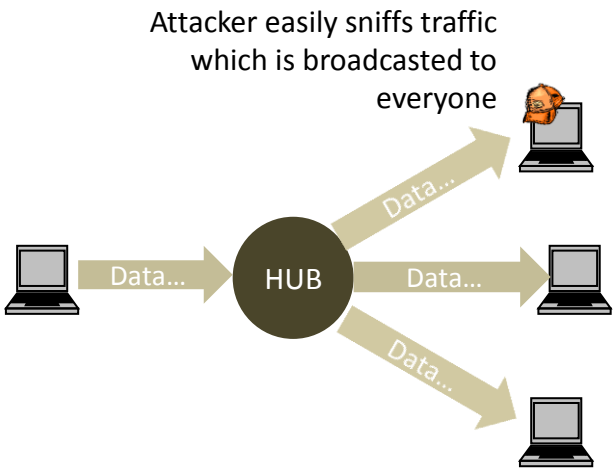
A promiscuous sniffing backdoor receiving commands



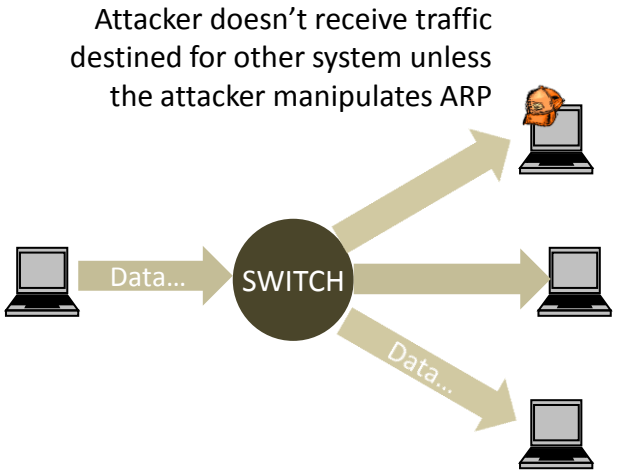
A promiscuous sniffing backdoor sending spoofed responses



Sniffing in a hub and switched environment

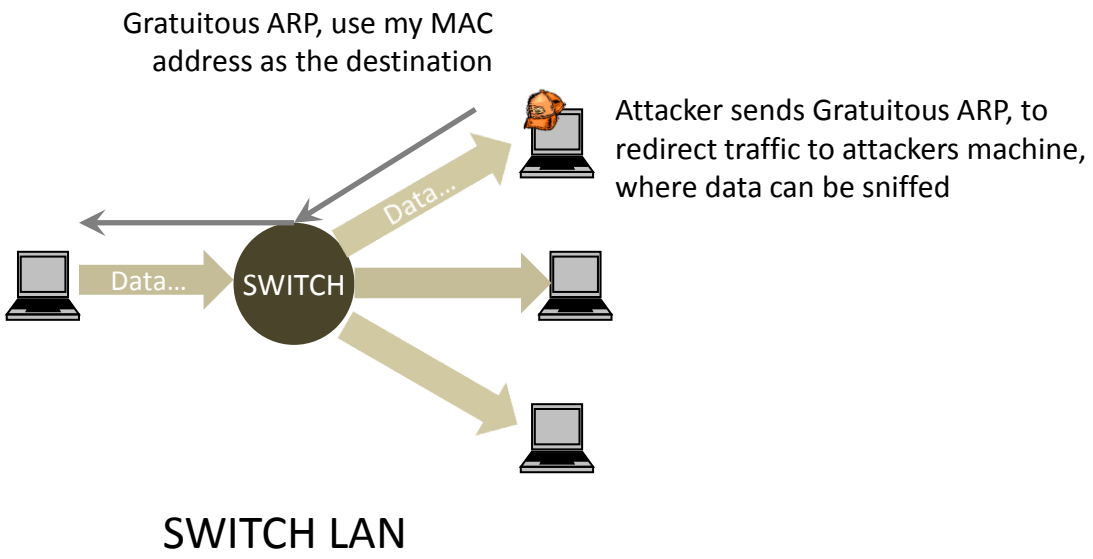


HUB LAN



SWITCH LAN

Using gratuitous ARPs to redirect traffic on a switched LAN



SWITCH LAN

Defences against Backdoors without Ports

- Linux
  - # ifconfig | grep PROMISC
  - # grep Promisc /var/log/messages
  - ip link
- Windows
  - Promiscdetect.exe
  - Sentinel
    - DNS Test
    - Etherping test
    - ARP test

- DNS Test
  - sends some packets on the LAN destined for various arbitrary IP addresses not on the LAN. Then, watches to see if any of these machines attempts a reverse DNS lookup on that IP address
- Etherping test
  - sends a ping packet to the suspect system's IP address, but uses a bogus destination MAC address. If the suspect system is not in promiscuous mode, it should ignore the packet, because it is not destined for this system's hardware address
- ARP test
  - sends an ARP request that asks which MAC address is associated with the suspect machine's IP address. but send this ARP request to a bogus MAC address, so the suspect system shouldn't see it on the LAN

Trojans

Introduction

- A Trojan horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality.

What's in a Name?

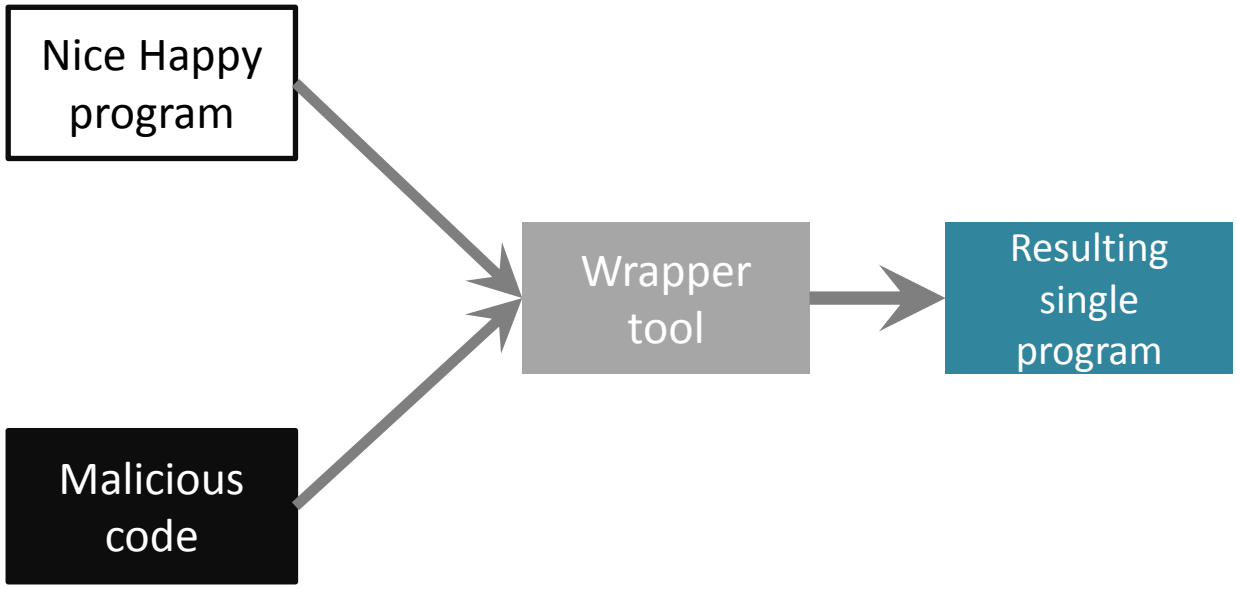
- Playing with Windows Suffixes
  - just_text.txt .exe
- Mimicking Other File Names
  - csrss.exe
  - services.exe
  - smss.exe
  - System
  - System Idle Process
  - winlogon.exe
- The Dangers of Dot "." in Your Path

Trojan Name Game Defenses

- by employing the antivirus tools
- ready to kill suspicious processes that usurp the names of legitimate processes – pskill
- lsof and Fport
- block executable e-mail attachments at your Internet gateway

Wrapper programs

- wrappers, binders, packers, EXE binders, and EXE joiners



Wrappers features

- combining two, six, nine, or even an arbitrary number of programs together
- addition of static files into the mix
- encrypting the malicious code portion of the resulting package
- morphing the decryption code so that it dynamically alters itself to evade detection, using polymorphic coding techniques

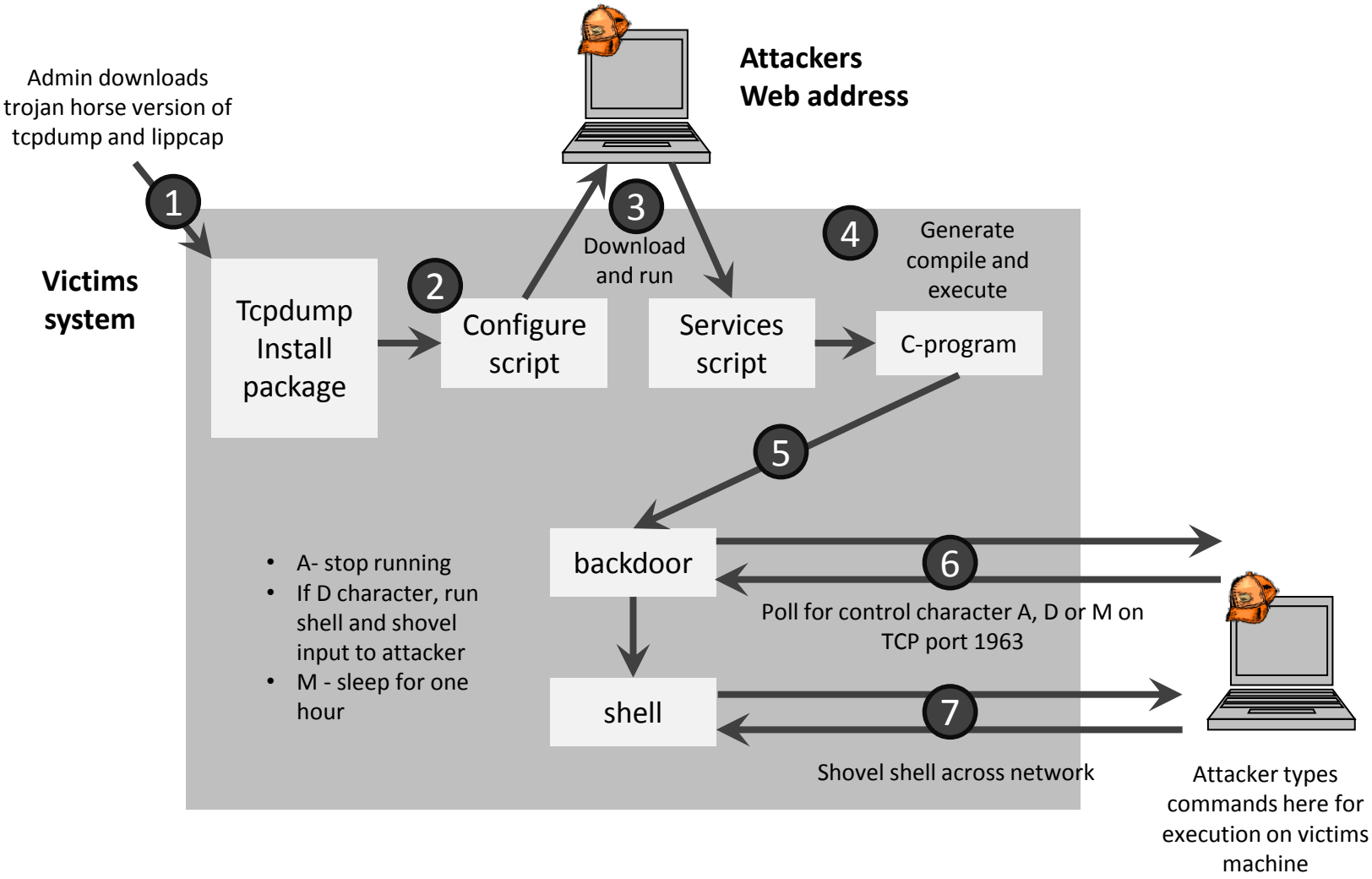
Wrapper Tools

- AFX File Lace
- EliteWrap
- Exe2vbs
- PE Bundle
- Perl2Exe
- Saran Wrap
- TOPV4
- Trojan Man

Trojaning Software Distribution Sites

- Trojaning Software Distribution the Old-Fashioned Way
  - software updates containing malicious code via the snail-mail postal service
- Going after Web Sites
  - Monkey.org, openssh.org, tcpdump.org, sendmail.org

The Tcpdump and Libpcap Trojan Horse Backdoor



Defences against Trojan Software Distribution

- user awareness,
- administrator integrity checks,
- carefully testing new software
  - should always test new tools before rolling them into production
- Check for included digital signature of the software, using a public key encryption package such as Pretty Good Privacy (PGP)

Poisoning the Source

- Code Complexity Makes Attack Easier
- Test? What Test?
  - www.eeggs.com
- The Move Toward International Development
- Defences against Poisoning the Source
  - encourage commercial vendors to have robust integrity controls and testing regimens for their products