Network Attacks

CSC 154

Passive Attacks vs. Active Attacks

- Passive attacks eavesdrop, collecting information;
- Active attacks take interactive actions like changing data, hence they are more malicious and will directly cause damage/change of flow;
- 4 Forms of active attacks: masquerade (hide identity), replay (after interception), modification of messages, denial of service;
- Active attacks generally after passive attacks, like surveillance;

- Defeating passive attacks should focus on detection;
- Defeating active attacks should focus on both detection and prevention;

Packet Sniffers

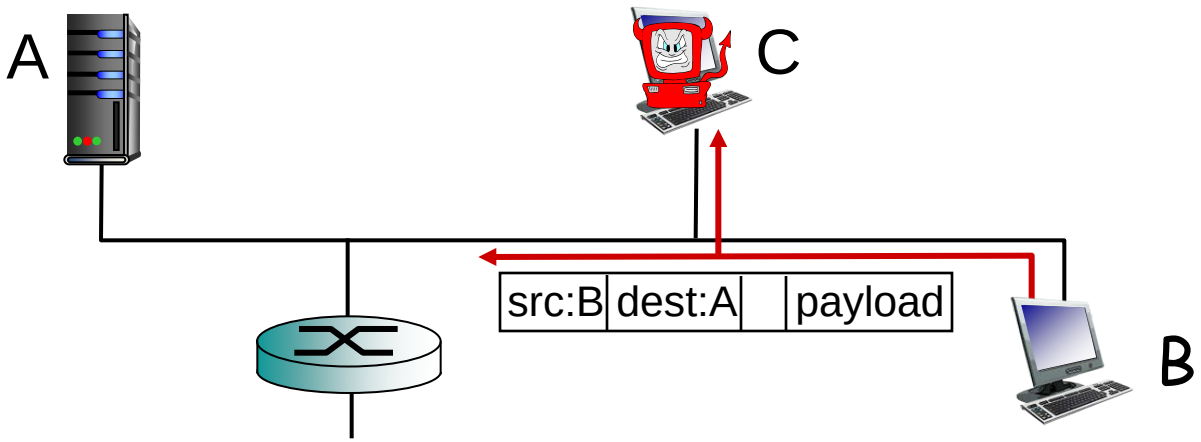
- Packet sniffers are discovering information by intercepting messages contained in network packets;
- Set hardware device in promiscuous mode;
- Packet sniffers are passive attacks, which do not alter data;
- Packet sniffers are hard to detect because they do not alter network traffic;

- Encryption can be used for prevention;
- Use one time passwords to help defeat;

Bad guys can sniff packets

packet "sniffing":

- broadcast media (shared ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- wireshark software used for end-of-chapter labs is a (free) packet-sniffer

One Time Password

- Attackers need your password into your system and perform malicious activities;
- They will have to type in the password, which further gets checked by your system;
- Your system will check by comparing the typed password with the one stored in system;
- One time password: the stored password get changed every time it is used;
- The password revealed by eavesdrop became “old”, which will fail in later password checking.

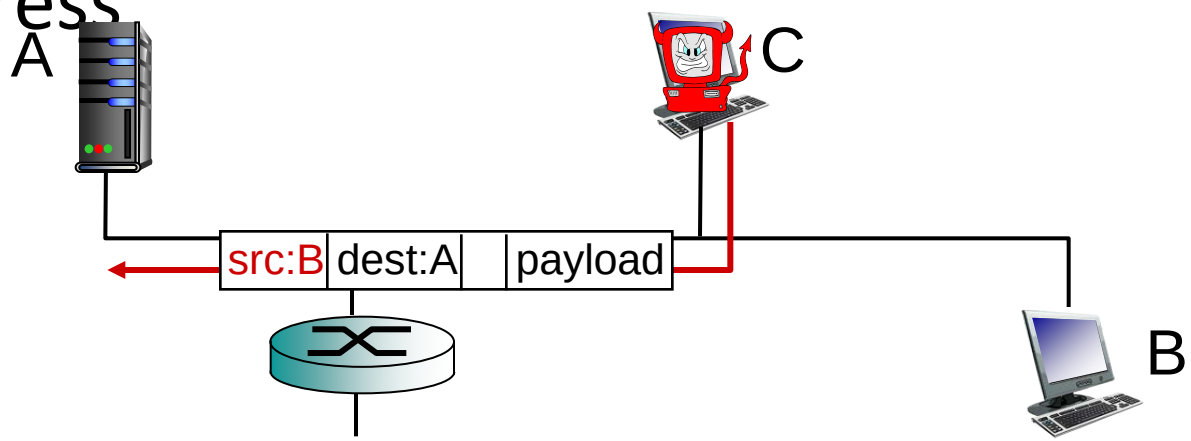
Spoofing

- Active attack, after passive attacks, to cheat for trust;
  - Hide real identity;
  - Perhaps no response;
- Camouflage IP and use internal IP; the hacker needs to know which (trusted) IP addresses to use;
- Spoofing can help enforce phishing attacks, like email spoofing;

- Use firewalls if you have trusted systems outside network;
- Cryptography and authentication prevent spoofing;

Bad guys can use fake addresses

IP spoofing: send packet with false source address



… lots more on security (throughout, Chapter 8)

Malicious Applets

- Small malicious programs, typically Java code, embedded in untrusted web pages and executed by browsers;
  - Log keystrokes;
  - Steal information (password, bank account, credit card);
  - Modifying files;
  - Spoofing emails;
  - Spread viruses;
  - Launch DDoS attacks;

- Disable Java to avoid;

War Dialers

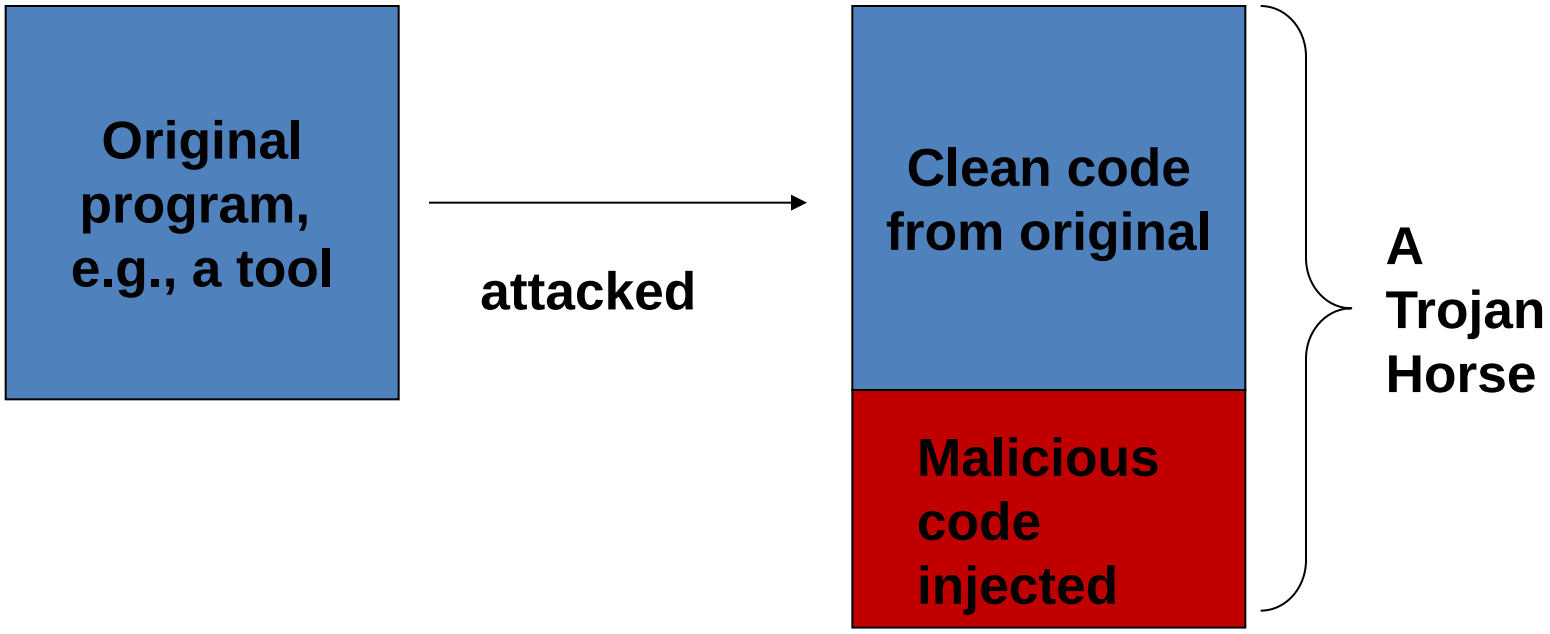
- Programs automatically dial telephone numbers and try to establish a connection via its dial-up;
- Break into a computer with unprotected logins or weak passwords;

- Change passwords frequently;
- Use strong passwords; Do not use dictionary words;
- Less vulnerability using Ethernet connection;

Logic Bomb

- Dormant until activated when certain conditions (data/time) satisfied;
  - Corrupts data until the system is unusable;
- Can be deployed by worm or viruses; or internal attacks from employees;
- Can be detected and removed by scanning;
  - Virus scanning;
  - Trip wire;
- Can be mitigated by hashing the original program;
  - a hash value is a unique value calculated one-way from the program content;
  - It's hard to reversely guess the content according to the hash value;
  - if content changes then hash value changes;

Trojan Horse



Logic bomb vs. Trojan horse

- Trojan horse is faking, and thus on top of, an existing program;

- Logic bomb is a separate program;

Virus, Worm vs. Trojan Horse

- Is a trojan horse virus or worm?
  - Virus;
  - Virus needs user interaction; worms NO;
  - trojan horse looks like real program;

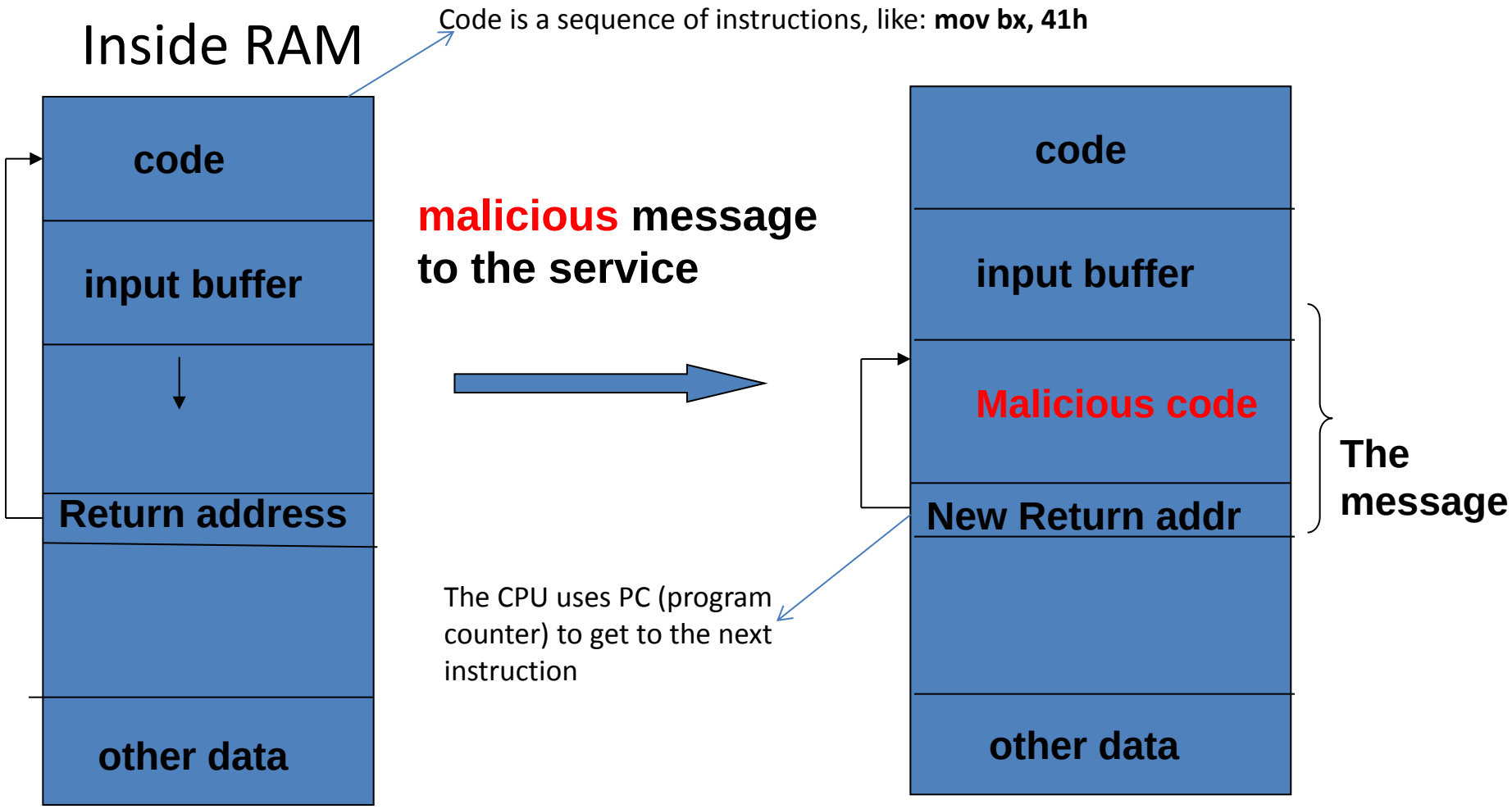
- Use antivirus to scan system for avoiding virus;
- Only run macro/code from trusted sources;
- Only download from trusted web-sites;

Buffer Overflow

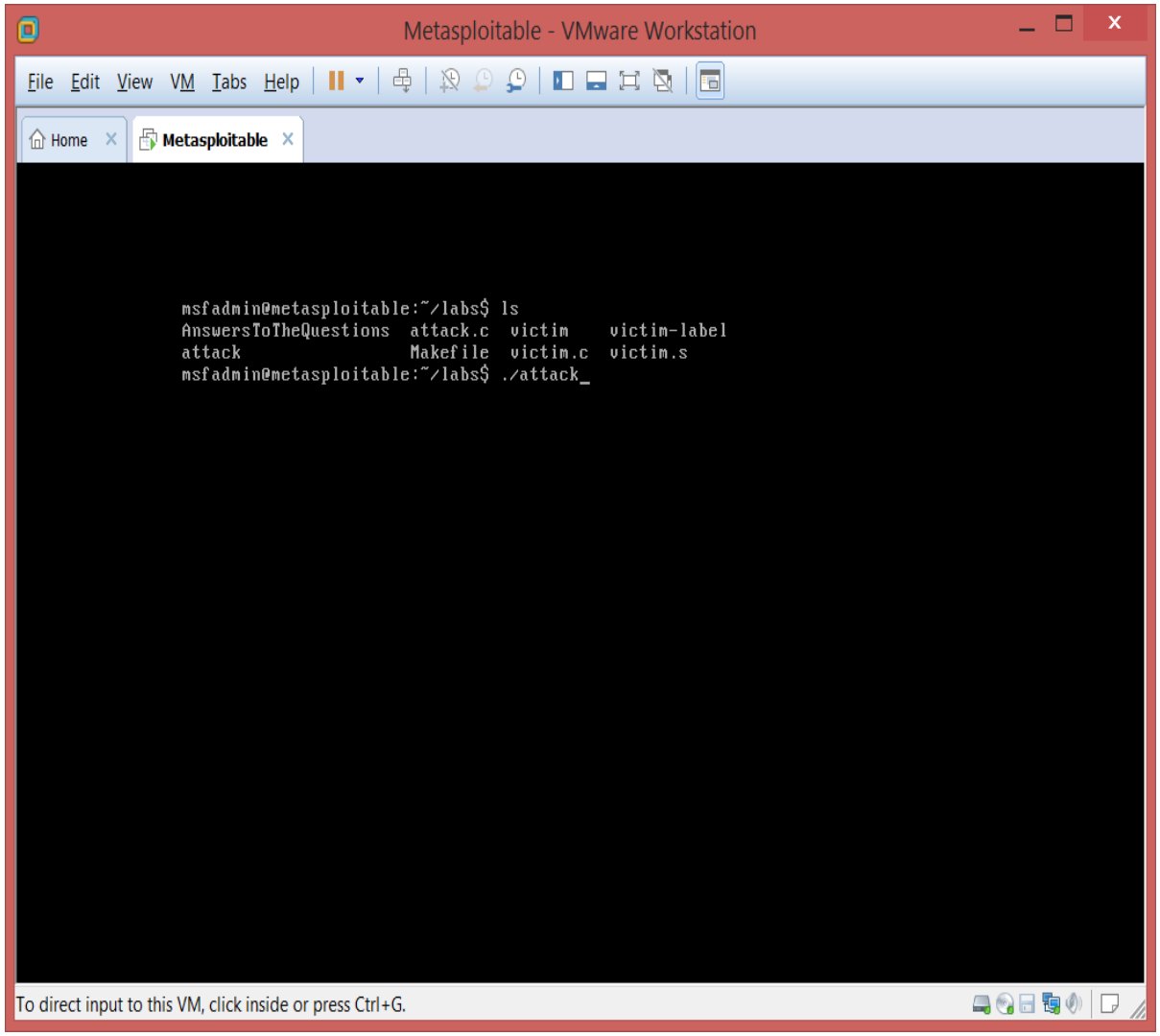
- More than 90% of real world hacking is via buffer overflow; like the various worms;

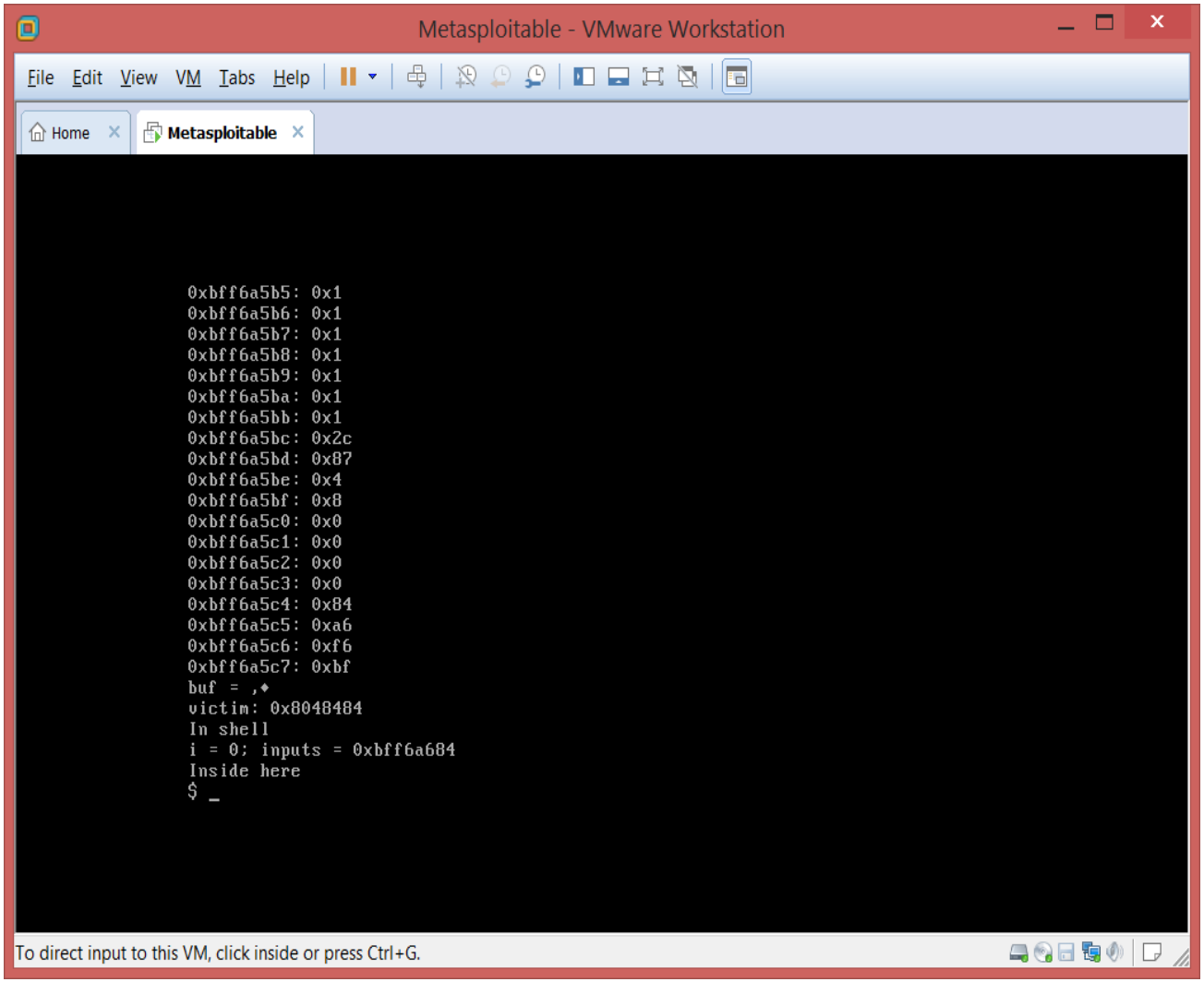
- Attacker sends more data than expected to the target
  - crash system (DoS) or gain control (buffer overflow);
  - usually subtly crafted;
  - when an Internet service is run, its stack contains the return address;
  - the attacker takes advantage of the stack and the return address is overwritten by over-long data ;
  - the changed return address will mislead the program execution to the malicious code that the attacker knows;

Buffer Overflow

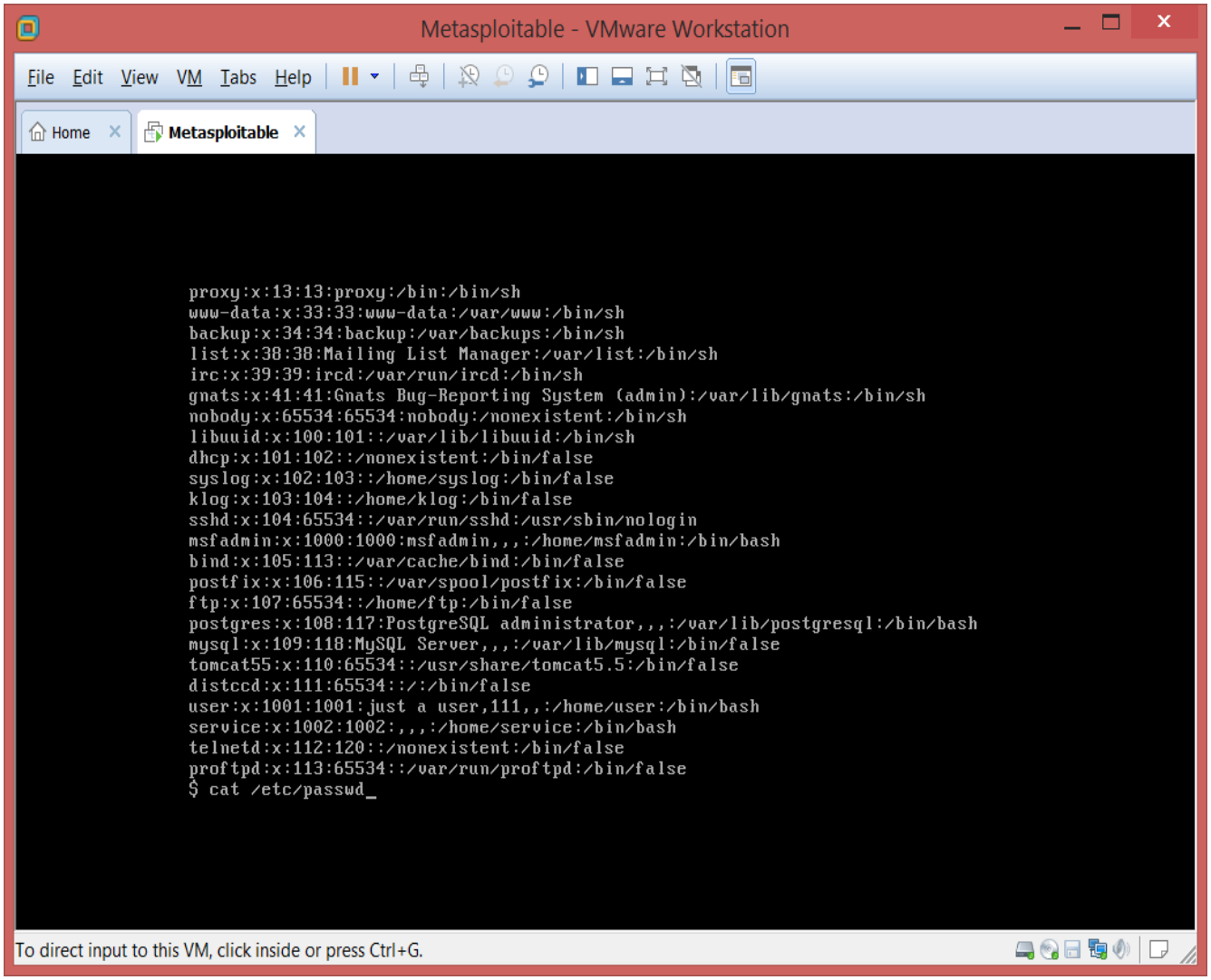


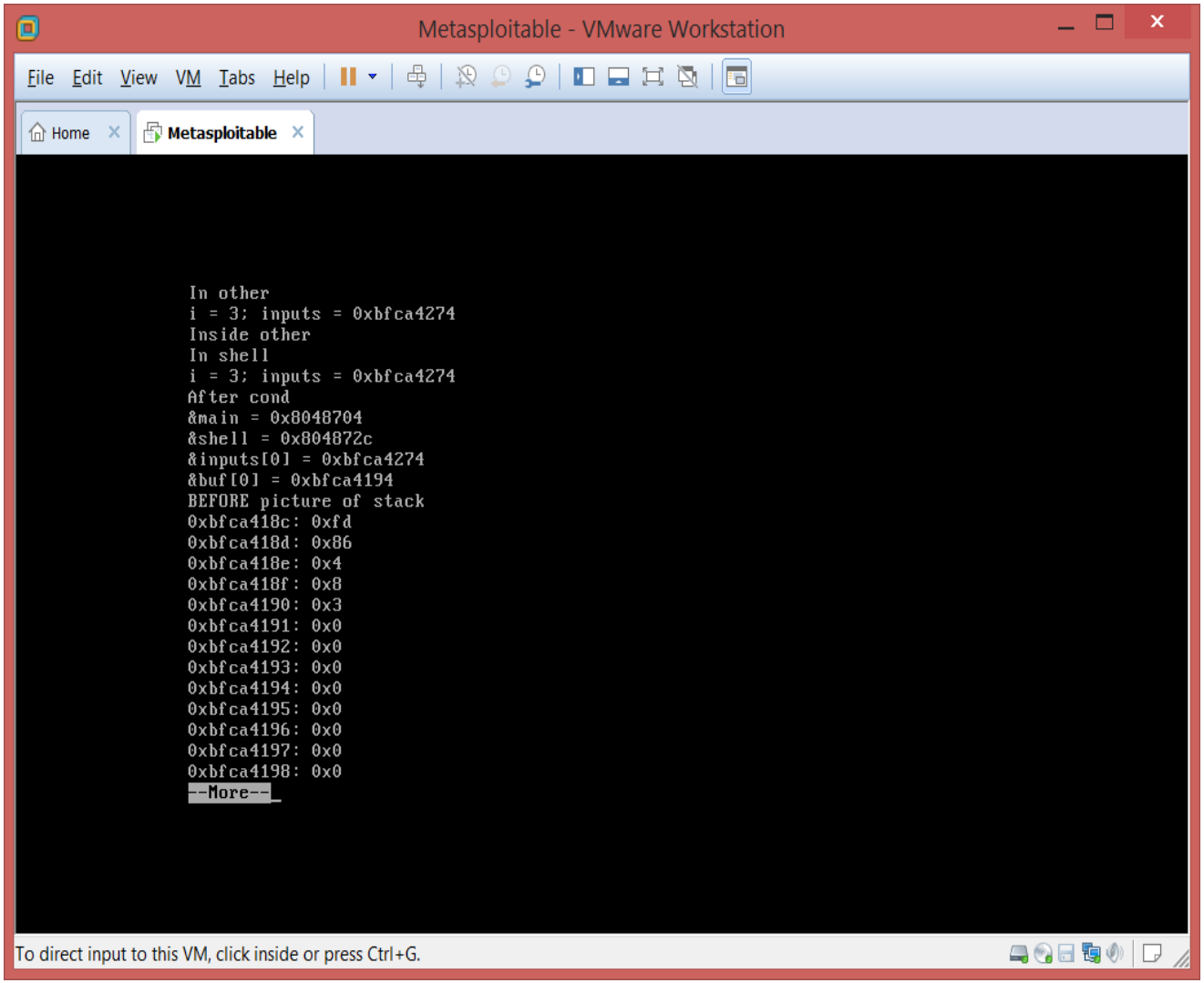
Demo Time (Virtual Machine-Metasploitable)


Metasploitable - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable
msfadmin@metasploitable:~/labs$ ls
AnswersToTheQuestions attack.c victim victim-label
attack Makefile victim.c victim.s
msfadmin@metasploitable:~/labs$ ./attack_
To direct input to this VM, click inside or press Ctrl+G.

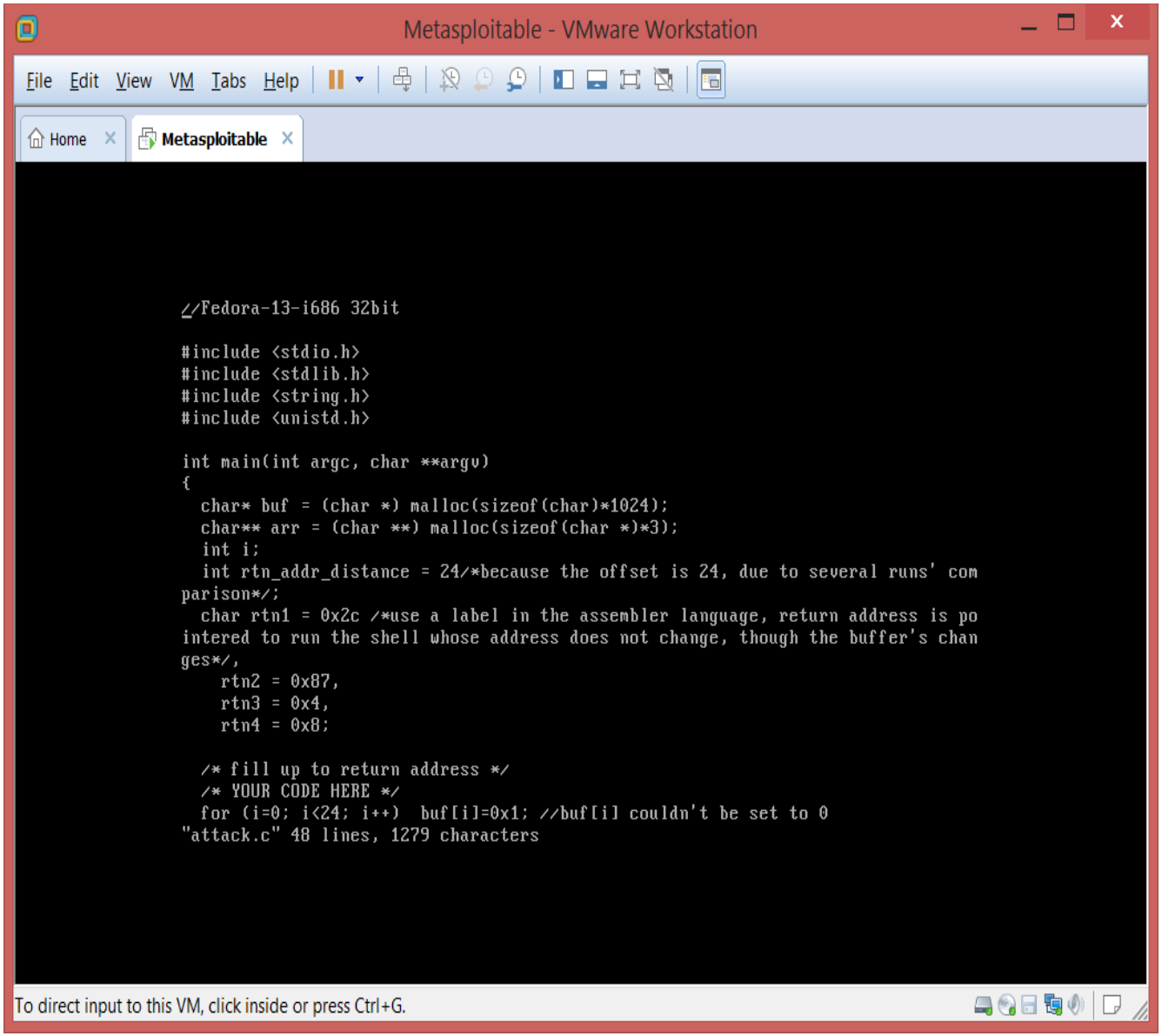


Get shell access after attack


Metasploitable - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
$ cat /etc/passwd_
To direct input to this VM, click inside or press Ctrl+G.



To predict where is the return address of shell



Attack code to craft new rtn address

A Revisit to DDoS

- DDoS uses controlled hosts, zombies, gained through buffer overflow, worm, botnets, etc.;
- Hardest attacks to defend; harder when they spoof IP addresses;
- Easiest to launch because they look like normal traffic;

- Limiting nonessential traffic; threshold;
- Load-balance;

Social Engineering

- Take advantage of human characteristics
  - psychological/behavioral biases
- Speak to unsuspecting employees for sensitive information;
  - Employees should be aware of the threat and risk;
  - Enterprise training and education;
- Security policies can be made to help;

Dumpster Diving

- Valuable information in garbage;
  - find information in garbage to help break into the computers;
  - Physical access to dumpster;
  - Enough time to sift through the items in dumpster;
  - Be patient;

- Sensitive documents should be shredded;

Password Cracker

- Situation:
  - passwords are encrypted;
  - Most encryption algorithms are now one-way
- Repeatedly attempting to identify the original password in clear text:
  - First to retrieve a username/password database file;
  - Then to repeatedly encrypt possible passwords, compare them to the entries in password column of the database file;
    - Usually based on brute-force engines;