SEED Lab Environment Setup

CSE 565 Computer Security

Outline

- Environment Setup
  - We use SEED Ubuntu-20.04 VM
- Multiple VMs
- Best Practices

Environment Setup – x86

- For Windows/Linux User:
  - Download VirtualBox
    - https://www.virtualbox.org/
  - Follow the instructions
    - https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md

Environment Setup – Apple Silicon

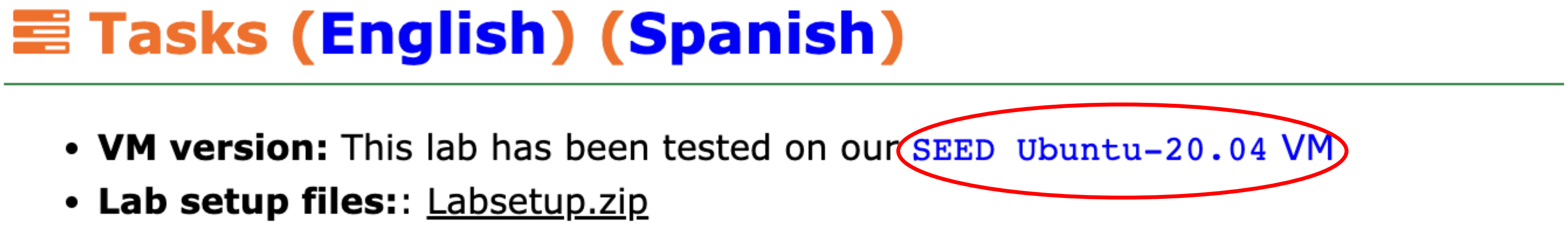
- For macOS User with Apple Silicon (M1, M2, etc.):
  - TBD

Environment Setup

- Lab Website
  - Secret-Key Encryption: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Encryption/
  - SQL Injection Attack: https://seedsecuritylabs.org/Labs_20.04/Web/Web_SQL_Injection/
  - Buffer-overflow Attack: https://seedsecuritylabs.org/Labs_20.04/Software/Buffer_Overflow_Setuid/
  - Sniffing and Spoofing: https://seedsecuritylabs.org/Labs_20.04/Networking/Sniffing_Spoofing/

Environment Setup Cont…

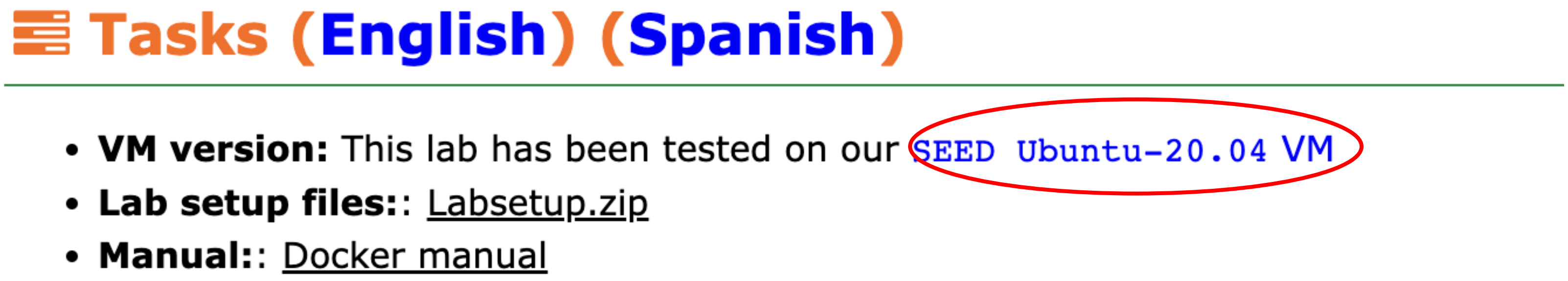
- Download the right VM
  - SetUID



Tasks (English) (Spanish)

- **VM version:** This lab has been tested on our SEED Ubuntu-20.04 VM
- **Lab setup files::** Labsetup.zip

  - Sniffing and Spoofing

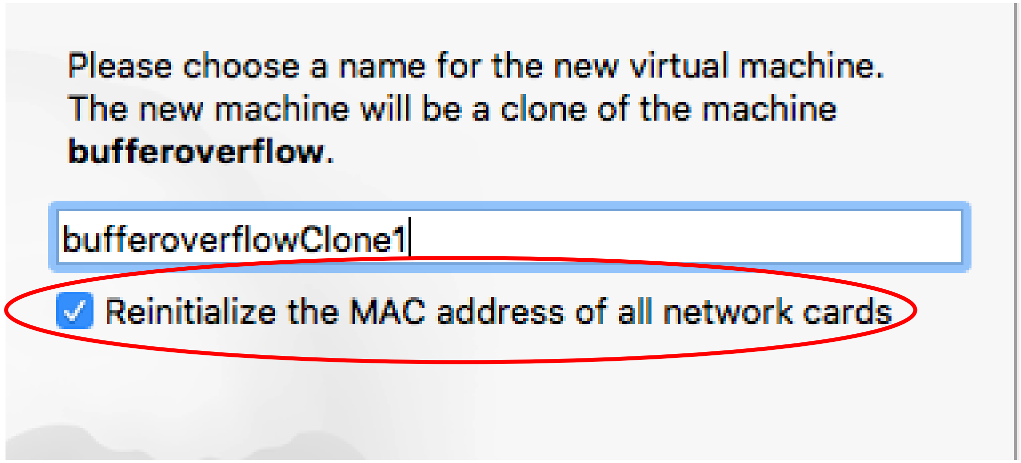


Tasks (English) (Spanish)

- **VM version:** This lab has been tested on our SEED Ubuntu-20.04 VM
- **Lab setup files::** Labsetup.zip
- **Manual::** Docker manual

Multiple VMs

- Clone your VM to create multiple VMs
  - Reinitialize MAC addresses

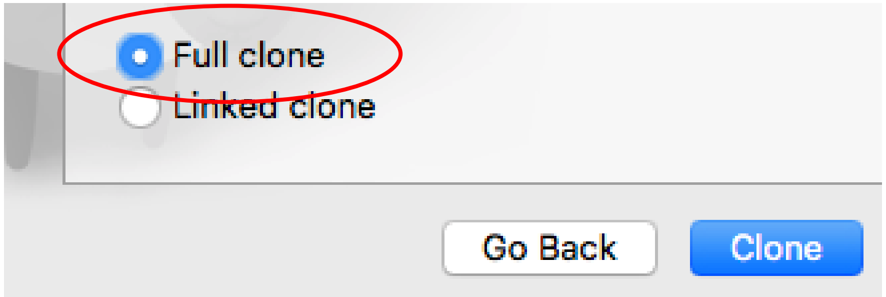


Please choose a name for the new virtual machine. The new machine will be a clone of the machine **bufferoverflow**.

bufferoverflowClone1

☑ Reinitialize the MAC address of all network cards

  - Full clone (Make sure you have enough disk space)

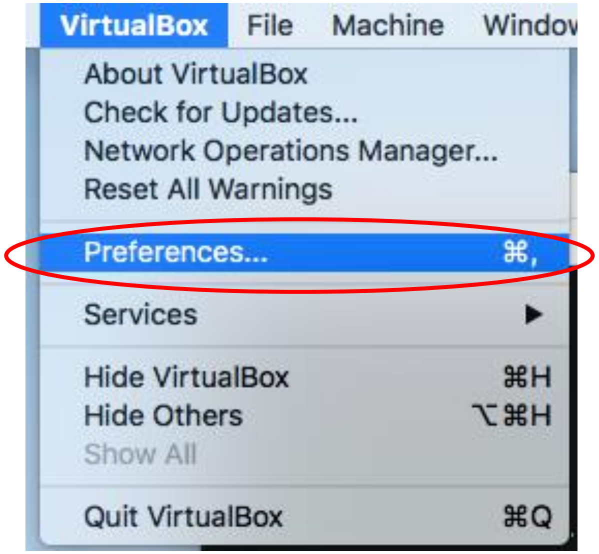


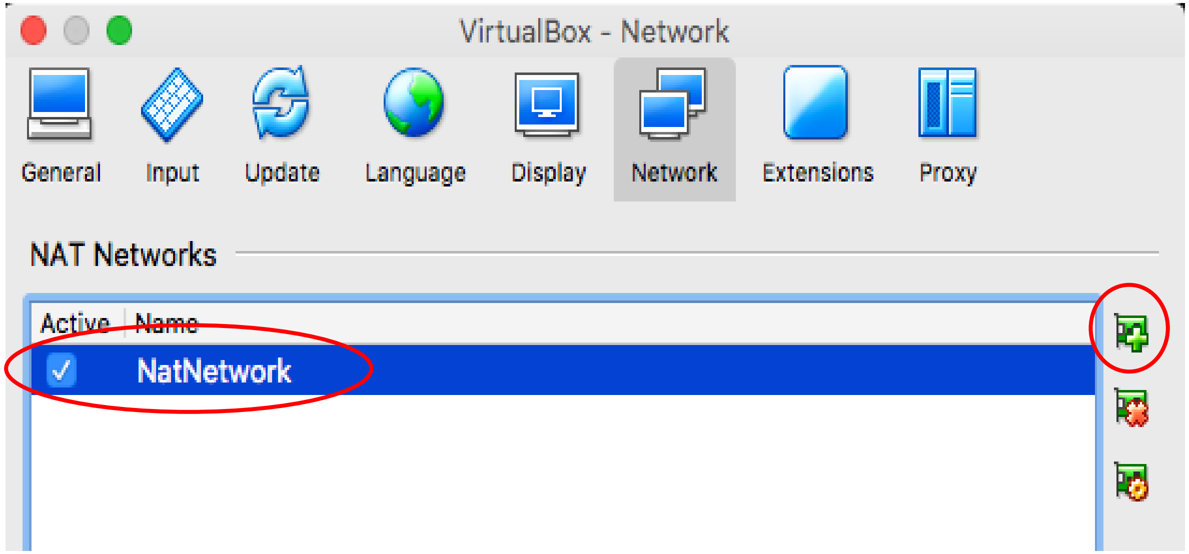
● Full clone

○ Linked clone

Multiple VMs Cont…

- NAT Network
  - Allows VMs to have assigned IPs. NAT networking forwards packets to VMs.
  - Create new NAT network



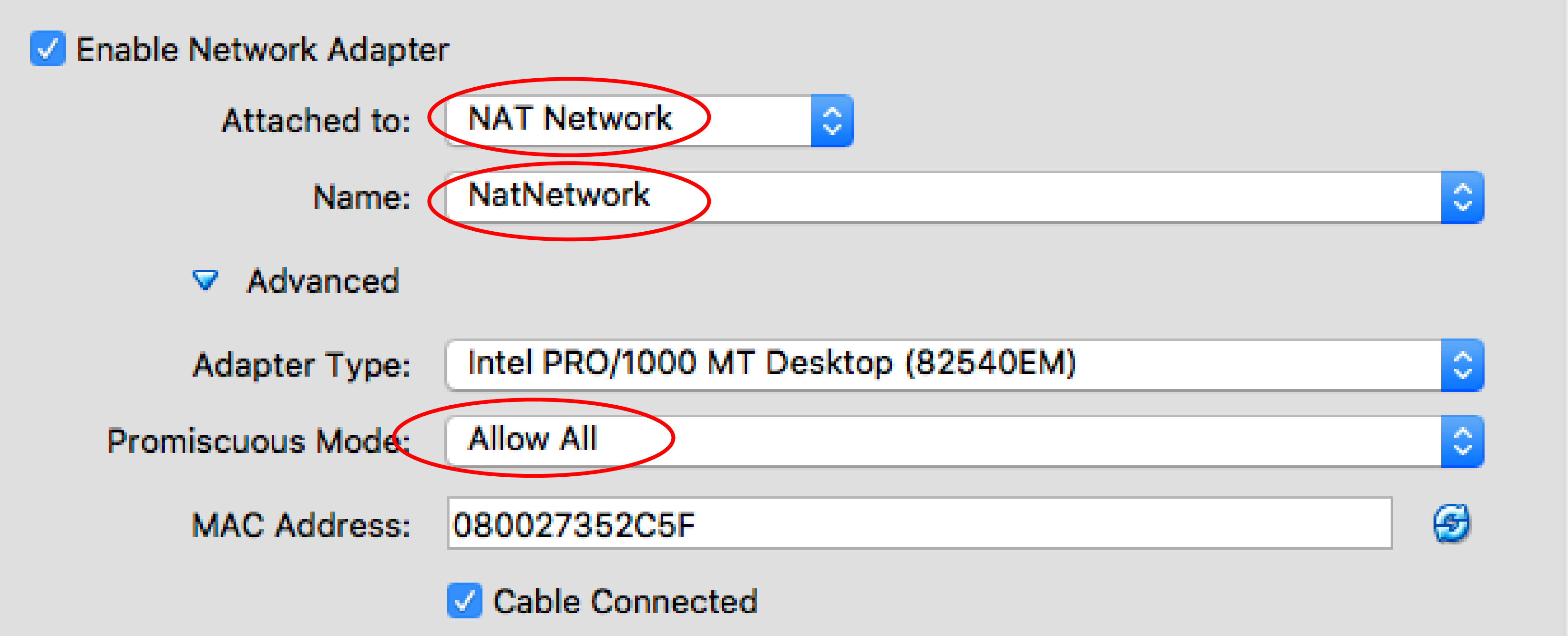


NAT Networks

Active	Name
✓	NatNetwork

Multiple VMs Cont…

- Assign your new NAT network to a VM



☑ Enable Network Adapter

Attached to: NAT Network

Name: NatNetwork

▽ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

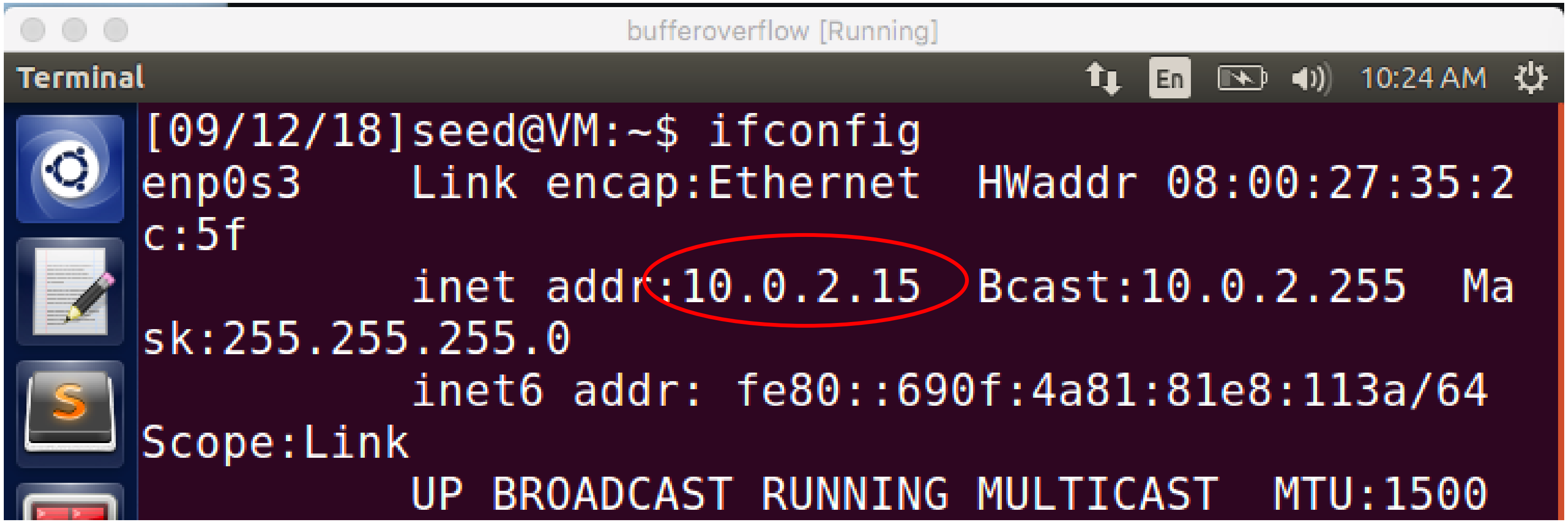
Promiscuous Mode: Allow All

MAC Address: 080027352C5F

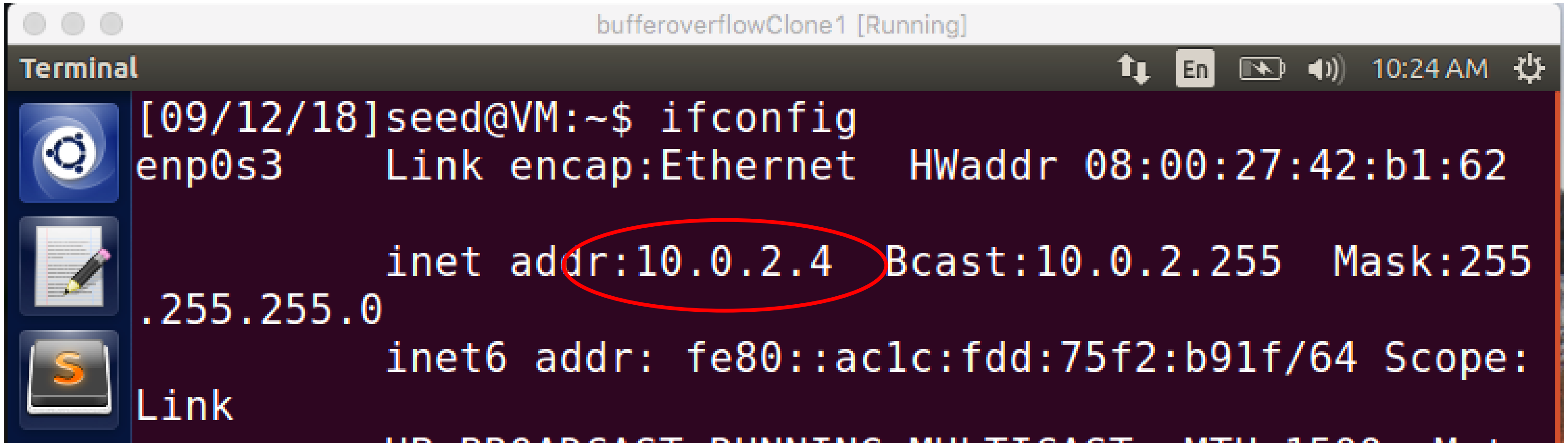
☑ Cable Connected

Multiple VMs Cont…

- Make sure your VMs have different IPs



```
[09/12/18]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:35:2
c:5f
          inet addr:10.0.2.15  Bcast:10.0.2.255  Ma
sk:255.255.255.0
          inet6 addr: fe80::690f:4a81:81e8:113a/64
Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500
```

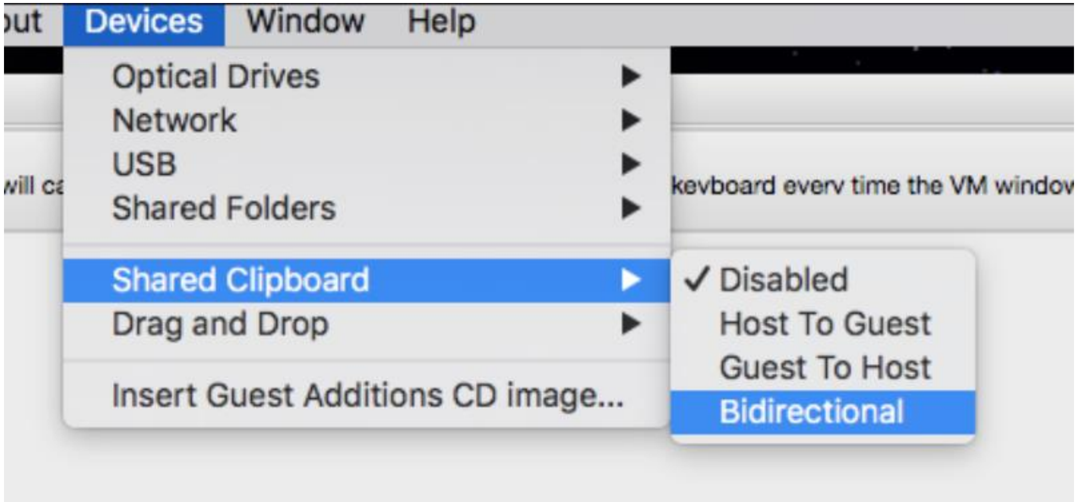


```
[09/12/18]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:42:b1:62

          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255
.255.255.0
          inet6 addr: fe80::ac1c:fdd:75f2:b91f/64 Scope:
Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
```

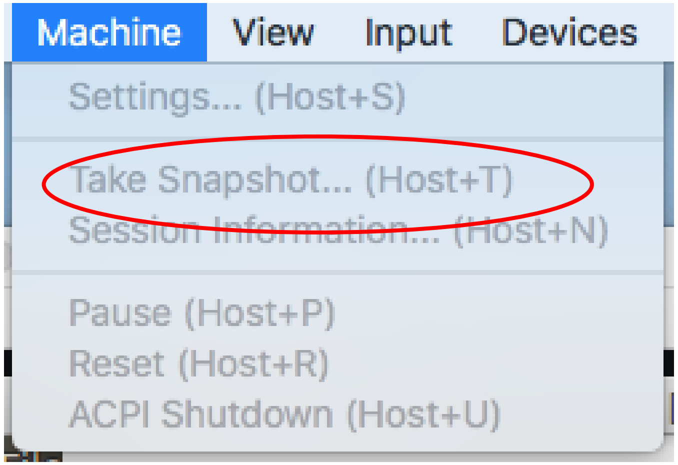
Best Practices

- Activate shared clipboard



Best Practices Cont…

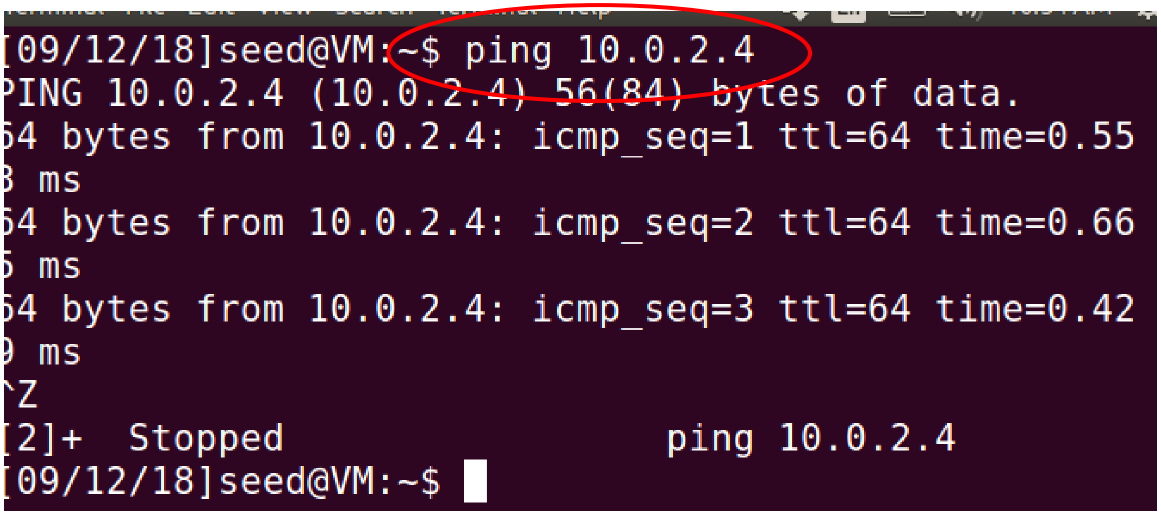
- Create snapshots regularly



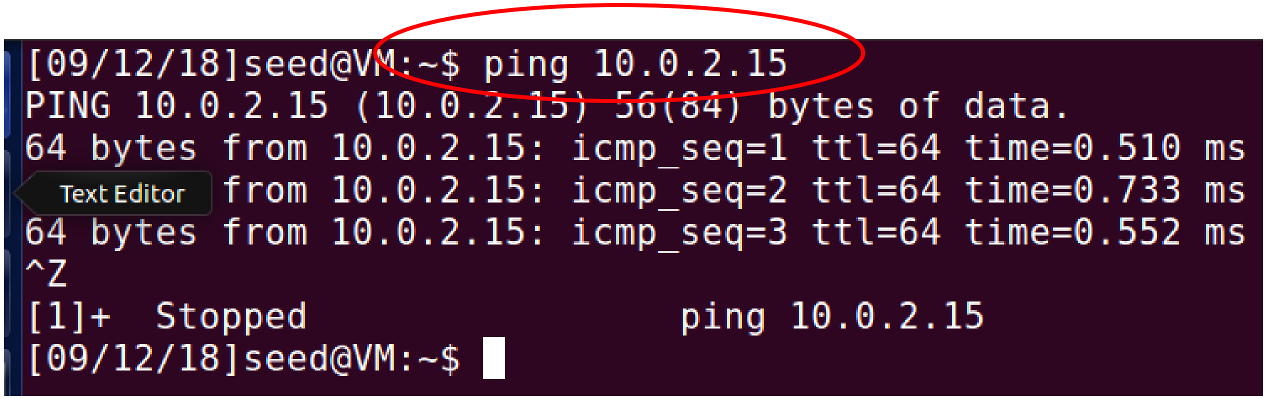
- Recover from system failures using the most recent snapshot

Best Practices Cont…

- Use ping to test connections



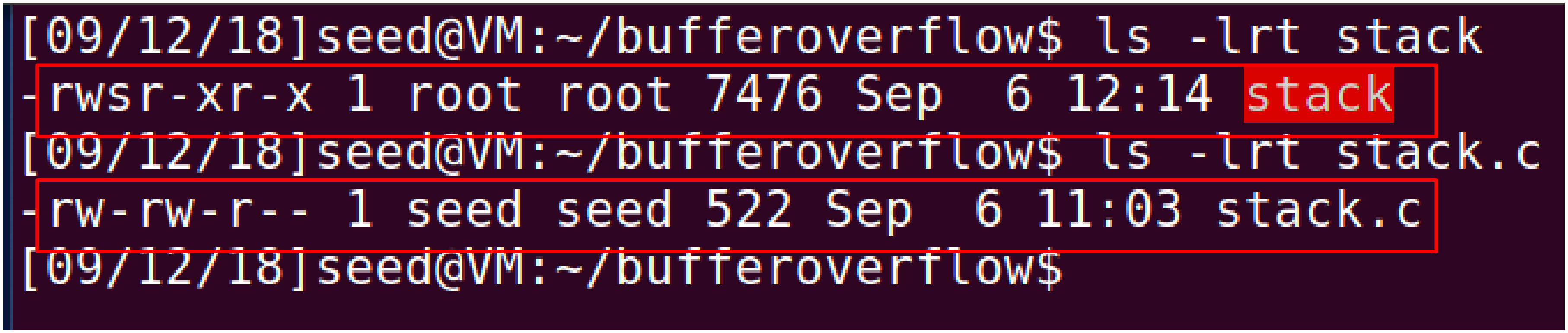
```
[09/12/18]seed@VM:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.55
3 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.66
5 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.42
9 ms
^Z
[2]+  Stopped                 ping 10.0.2.4
[09/12/18]seed@VM:~$ 
```



```
[09/12/18]seed@VM:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.510 ms
         from 10.0.2.15: icmp_seq=2 ttl=64 time=0.733 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.552 ms
^Z
[1]+  Stopped                 ping 10.0.2.15
[09/12/18]seed@VM:~$ 
```

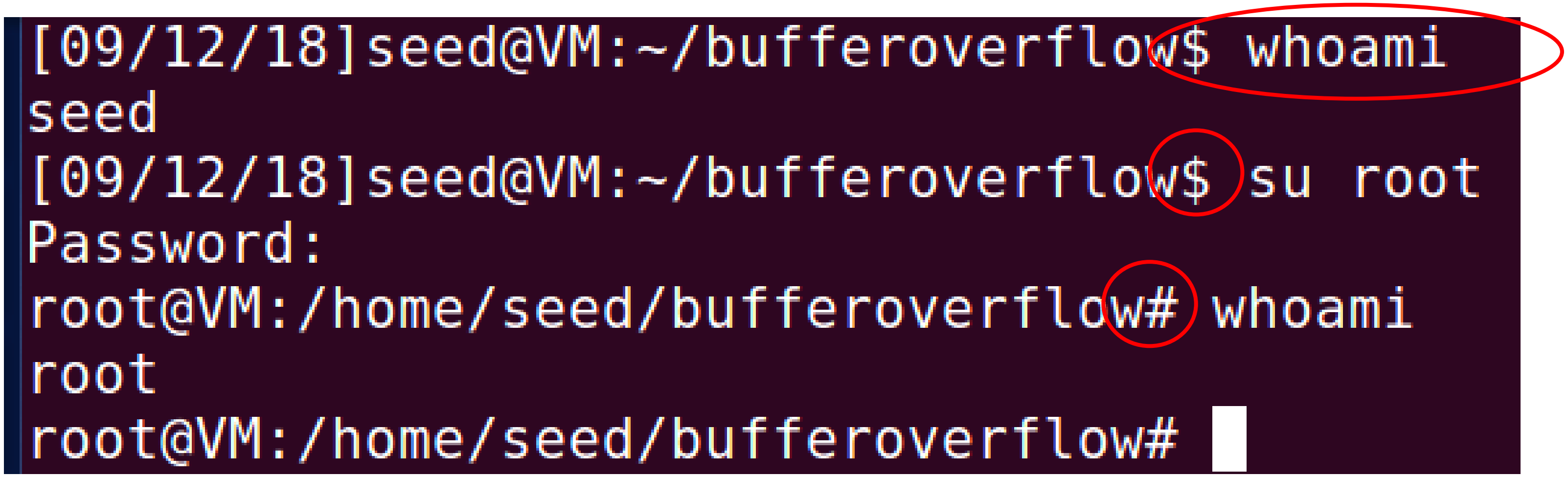
Best Practices (SetUid) Cont…

- Be aware of file permissions



```
[09/12/18]seed@VM:~/bufferoverflow$ ls -lrt stack
-rwsr-xr-x 1 root root 7476 Sep  6 12:14 stack
[09/12/18]seed@VM:~/bufferoverflow$ ls -lrt stack.c
-rw-rw-r-- 1 seed seed 522 Sep  6 11:03 stack.c
[09/12/18]seed@VM:~/bufferoverflow$
```

- Be aware of who the current user is



```
[09/12/18]seed@VM:~/bufferoverflow$ whoami
seed
[09/12/18]seed@VM:~/bufferoverflow$ su root
Password:
root@VM:/home/seed/bufferoverflow# whoami
root
root@VM:/home/seed/bufferoverflow# 
```

Resources

- SEED Lab User manual
  - Eg: Accounts, passwords, VM network configurations
  - http://www.cis.syr.edu/~wedu/seed/Documentation/Ubuntu12_04_VM/Ubuntu12_04_VM_Manual.pdf

- VM Customization
  - Make attacker, user desktops look different
  - http://www.cis.syr.edu/~wedu/seed/Documentation/Ubuntu12_04_VM/CustomizationInstruction.pdf

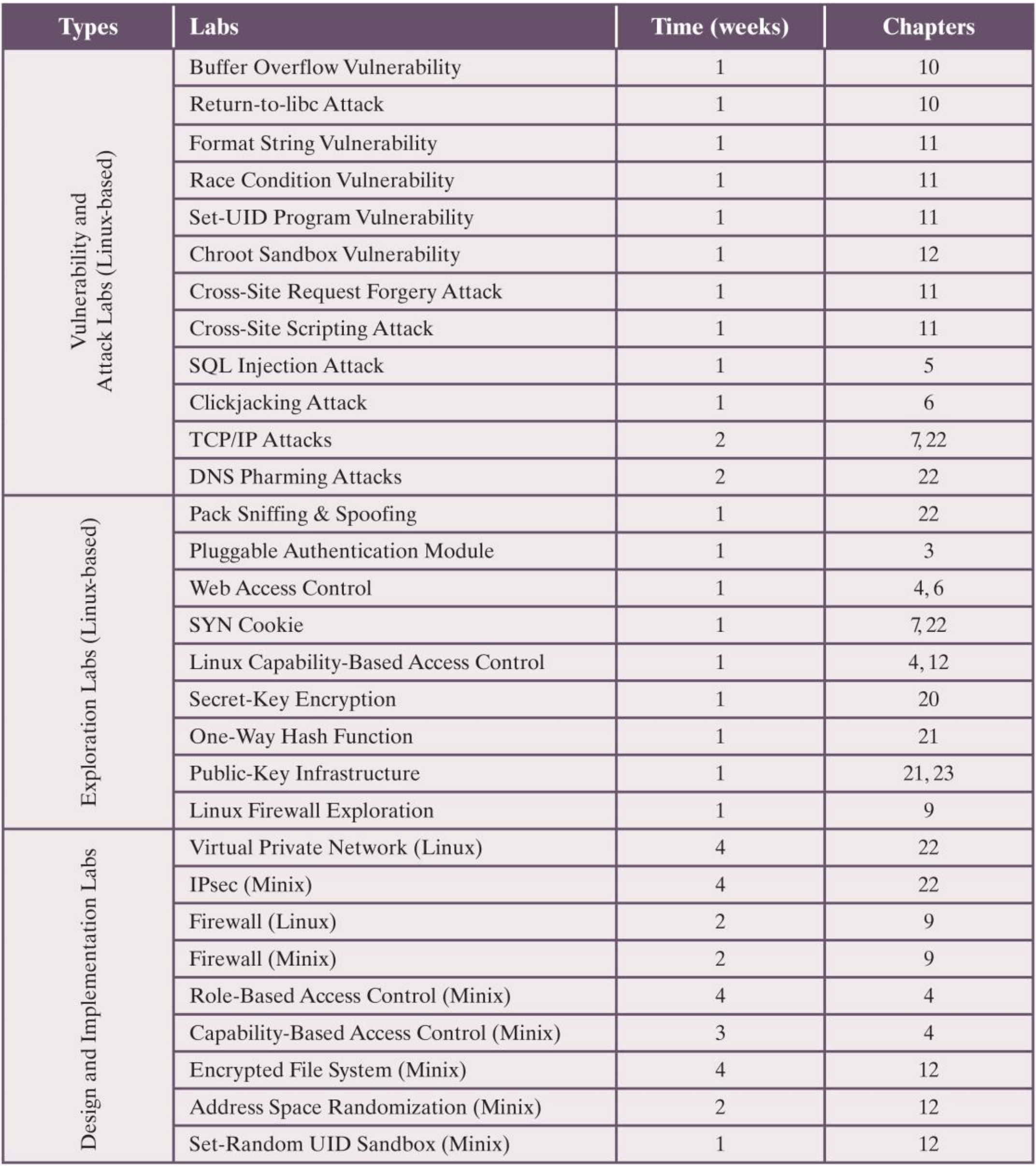
Report

- PDF submissions only

- Attach code in Appendix
  - List the important code snippets followed by explanation
- Screenshots are proof of task completion
  - Screenshot must show **relevant information**
    - Describe what you have done and what you have observed
    - Provide explanation to the observations that are interesting or surprising

Table A.1

Mapping of SEED Labs to Textbook Chapters



Types	Labs	Time (weeks)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	10
	Return-to-libc Attack	1	10
	Format String Vulnerability	1	11
	Race Condition Vulnerability	1	11
	Set-UID Program Vulnerability	1	11
	Chroot Sandbox Vulnerability	1	12
	Cross-Site Request Forgery Attack	1	11
	Cross-Site Scripting Attack	1	11
	SQL Injection Attack	1	5
	Clickjacking Attack	1	6
	TCP/IP Attacks	2	7, 22
	DNS Pharming Attacks	2	22
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	22
	Pluggable Authentication Module	1	3
	Web Access Control	1	4, 6
	SYN Cookie	1	7, 22
	Linux Capability-Based Access Control	1	4, 12
	Secret-Key Encryption	1	20
	One-Way Hash Function	1	21
	Public-Key Infrastructure	1	21, 23
	Linux Firewall Exploration	1	9
Design and Implementation Labs	Virtual Private Network (Linux)	4	22
	IPsec (Minix)	4	22
	Firewall (Linux)	2	9
	Firewall (Minix)	2	9
	Role-Based Access Control (Minix)	4	4
	Capability-Based Access Control (Minix)	3	4
	Encrypted File System (Minix)	4	12
	Address Space Randomization (Minix)	2	12
	Set-Random UID Sandbox (Minix)	1	12