

# CS 455 – Computer Security Fundamentals

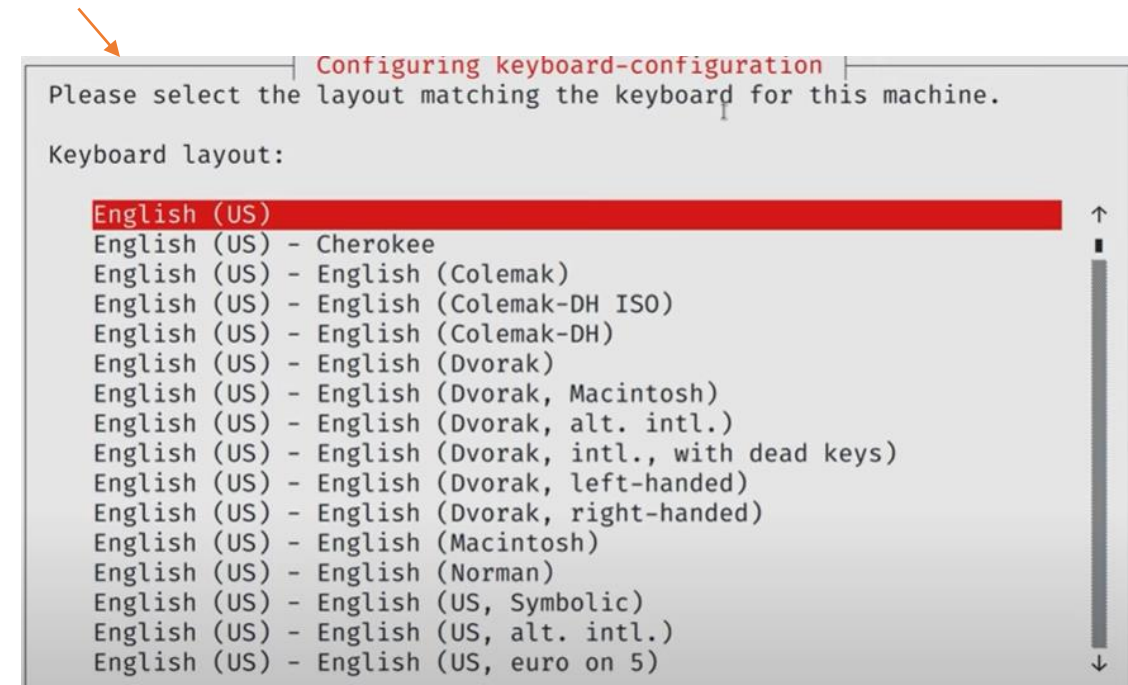
Dr. Chen-Yeou (Charles) Yu

# Computer Security Fundamentals

- A Quick Introduction to Kali Linux in AWS
  - ~~We will use this example to do our introduction first~~
    - ~~Install Kali Linux into AWS!~~
  - ~~Then, I will show you getting around with AWS~~
    - ~~SSH setup~~
    - RDP setup (GUI)

# A Quick Introduction to Kali Linux in AWS

- RDP setup
- Type the following in your “SSH” you just setup
- Assuming you are now using the SSH to connect the Kali Linux @ AWS
  - `sudo apt update`
  - `sudo apt install xfce4 xfce4-goodies -y`
    - You will see a confirmation for keyboard layout. Just use this one
- So for the server side “desktop environment” setup, we are done. Next up, we want to install xrdp as a kind of “system service”
  - `sudo apt install xrdp`
- xrdp is a service to facilitate our RDP connection



# A Quick Introduction to Kali Linux in AWS

- Now we are going to add an user who has the access right for this RDP service (in the cloud). Then, we will perform a connection from our local machine, my Kali Linux@VirtualBox to Kali Linux@AWS cloud

```
(kali$ kali)-[~]
$ sudo adduser charlesyu
Adding user `charlesyu' ...
Adding new group `charlesyu' (1002) ...
Adding new user `charlesyu' (1002) with group `charlesyu (1002)' ...
Creating home directory `/home/charlesyu' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for charlesyu
Enter the new value, or press ENTER for the default
    Full Name []: Charles Yu
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
Adding new user `charlesyu' to supplemental / extra groups `users' ...
Adding user `charlesyu' to group `users' ...
```

# A Quick Introduction to Kali Linux in AWS

- Next up, we want to **add this newly added user, “charlesyu” into the xrdp group**, for example: (you need to replace my account for yours)
  - `sudo usermod -aG xrdp charlesyu`
- It's about the time to start the service!
  - `sudo systemctl start xrdp`
- If you are not sure if the system is running correctly, here is the command
  - `sudo systemctl status xrdp`

# A Quick Introduction to Kali Linux in AWS

- Here is the status. Active!

```
(kali@ kali)~$ sudo systemctl start xrdp
(kali@ kali)~$ sudo systemctl status xrdp
• xrdp.service - xrdp daemon
   Loaded: loaded (/lib/systemd/system/xrdp.service; disabled; preset: disabled)
   Active: active (running) since Fri 2023-04-14 01:18:07 UTC; 1min 17s ago
     Docs: man:xrdp(8)
           man:xrdp.ini(5)
  Process: 21048 ExecStartPre=/bin/sh /usr/share/xrdp/socksetup (code=exited, status=0/SUCCESS)
  Process: 21056 ExecStart=/usr/sbin/xrdp $XRDPOPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 21057 (xrdp)
    Tasks: 1 (limit: 1125)
  Memory: 1.1M
     CPU: 12ms
  CGroup: /system.slice/xrdp.service
          └─21057 /usr/sbin/xrdp

Apr 14 01:18:06 kali systemd[1]: Starting xrdp.service - xrdp daemon...
Apr 14 01:18:06 kali xrdp[21056]: [INFO ] address [0.0.0.0] port [3389] mode 1
Apr 14 01:18:06 kali xrdp[21056]: [INFO ] listening to port 3389 on 0.0.0.0
Apr 14 01:18:06 kali xrdp[21056]: [INFO ] xrdp_listen_pp done
Apr 14 01:18:06 kali systemd[1]: xrdp.service: Can't open PID file /run/xrdp/xrdp.pid (yet?) after start: Operation not permitted
Apr 14 01:18:07 kali systemd[1]: Started xrdp.service - xrdp daemon.
Apr 14 01:18:08 kali xrdp[21057]: [INFO ] starting xrdp with pid 21057
Apr 14 01:18:08 kali xrdp[21057]: [INFO ] address [0.0.0.0] port [3389] mode 1
Apr 14 01:18:08 kali xrdp[21057]: [INFO ] listening to port 3389 on 0.0.0.0
Apr 14 01:18:08 kali xrdp[21057]: [INFO ] xrdp_listen_pp done
```

# A Quick Introduction to Kali Linux in AWS

- Next up, you can start the xrdp-sesman, the “session manager”
  - `sudo systemctl start xrdp-sesman`
- Almost done now! Did you remember the steps when we are going to setup a brand new OS image in AWS?
  - The SSH setting!
  - **Now we are going to add one more entry in the “security group” for RDP!**
- Click the “**Security Group**” tab
- Try to ignore the one with “default” because it is there along with your account.
- Check the existing one! (See the next page)

# A Quick Introduction to Kali Linux in AWS

us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#SecurityGroups:

Agents Truman State Unive... COMPSAC THE FIRST IEEE SERV... Game Theory guillaume-chevalier... Non-Convex region US\_VISA jaungiers/LSTM-Ne... LaTeX Sequence Classifica... Other bookmarks

aws Services Search [Alt+S]

Savings Plans  
Reserved Instances  
Dedicated Hosts  
Capacity Reservations

▼ Images  
AMIs  
AMI Catalog

▼ Elastic Block Store  
Volumes  
Snapshots  
Lifecycle Manager

▼ Network & Security  
**Security Groups**  
Elastic IPs  
Placement Groups  
Key Pairs  
Network Interfaces

▼ Load Balancing  
Load Balancers  
Target Groups

▼ Auto Scaling  
Launch Configurations  
Auto Scaling Groups

**Security Groups (1/2)** Info

Filter security groups

Actions Export security groups to CSV Create security group

	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
<input checked="" type="checkbox"/>	-	sg-01d023506013fce97	Kali Linux-Kali Linux 2...	vpc-0c9f6edbc269509a5...	This security group w...	378253604690	2 Permission entries
<input type="checkbox"/>	-	sg-05f714967d552bb52	default	vpc-0c9f6edbc269509a5...	default VPC security g...	378253604690	1 Permission entry

sg-01d023506013fce97 - Kali Linux-Kali Linux 2023.1-AutogenByAWSMP--1

Details Inbound rules Outbound rules Tags

**Inbound rules (2)**

Filter security group rules

Manage tags Edit inbound rules

	Name	Security group rul...	IP version	Type	Protocol	Port range	Source	D
<input type="checkbox"/>	-	sgr-07ca388d372bb...	IPv4	RDP	TCP	3389	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-06f0c476645d79...	IPv4	SSH	TCP	22	0.0.0.0/0	-



# A Quick Introduction to Kali Linux in AWS

- You will see 2 inbound rules in there!
- In the beginning, we only have 1 rule which is for SSH, remember that?
- I click the [Edit Inbound Rules] to add 1 more rule for RDP
- For detail, check the next page.
- Yes! For teaching purposes, I open that to the world! 0.0.0.0/0
- For practices, you need to set your own IP address,  
or you project co-worker's IP address for better protection

# A Quick Introduction to Kali Linux in AWS

## Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

### Inbound rules [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sgr-07ca388d372bb8fc6	RDP ▼	TCP	3389	Custom ▼	<input type="text" value="0.0.0.0/0"/>	<input type="text" value=""/> <input type="button" value="Delete"/>
sgr-06f0c476645d79813	SSH ▼	TCP	22	Custom ▼	<input type="text" value="0.0.0.0/0"/>	<input type="text" value=""/> <input type="button" value="Delete"/>

Add rule

Cancel

Preview changes

Save rules

# A Quick Introduction to Kali Linux in AWS

- All right, once you have this setting done, we can connect our Kali Linux @ AWS EC2
- In my use case, for the demonstration purpose, I just type this from my Kali Linux in the VirtualBox:
  - `rdesktop [ip address]`
  - The ip address here means your IP Address in EC2 instance (Kali Linux)
- Have problem with IP address?
  - There is an “instances”
  - Choose the [Networking] tab

## ▼ Instances

### Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

# A Quick Introduction to Kali Linux in AWS

**New EC2 Experience**  
Tell us what you think

EC2 Dashboard  
EC2 Global View  
Events  
Tags  
Limits  
▼ **Instances**  
Instances  
Instance Types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Capacity Reservations  
▼ **Images**  
AMIs  
AMI Catalog  
▼ **Elastic Block Store**  
Volumes  
Snapshots  
Lifecycle Manager

**Instances (1/1)** Info

Find instance by attribute or tag (case-sensitive)

Connect Instance state Actions Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
KaliLinux	i-0c42e00490f1fa031	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c	ec2-18-218-230-188....	18.218.230.188

**Instance: i-0c42e00490f1fa031 (KaliLinux)**

Details Security **Networking** Storage Status checks Monitoring Tags

You can now check network connectivity with Reachability Analyzer. Run Reachability Analyzer

▼ **Networking details** Info

Public IPv4 address 18.218.230.188   open address	Private IPv4 addresses 172.31.41.240 Private IP DNS name (IPv4 only) ip-172-31-41-240.us-east-2.compute.internal	VPC ID vpc-0c9f6edbc269509a5
Public IPv4 DNS ec2-18-218-230-188.us-east-2.compute.amazonaws.com   open address	IPv6 addresses -	Secondary private IPv4 addresses -
Subnet ID subnet-065d4b6488ad86539	Carrier IP addresses (ephemeral) -	Outpost ID -
Availability zone us-east-2c	Answer RBN DNS hostname IPv4 Enabled	
Use RBN as guest OS hostname Disabled		

▼ **Network Interfaces (1)** Info

# A Quick Introduction to Kali Linux in AWS

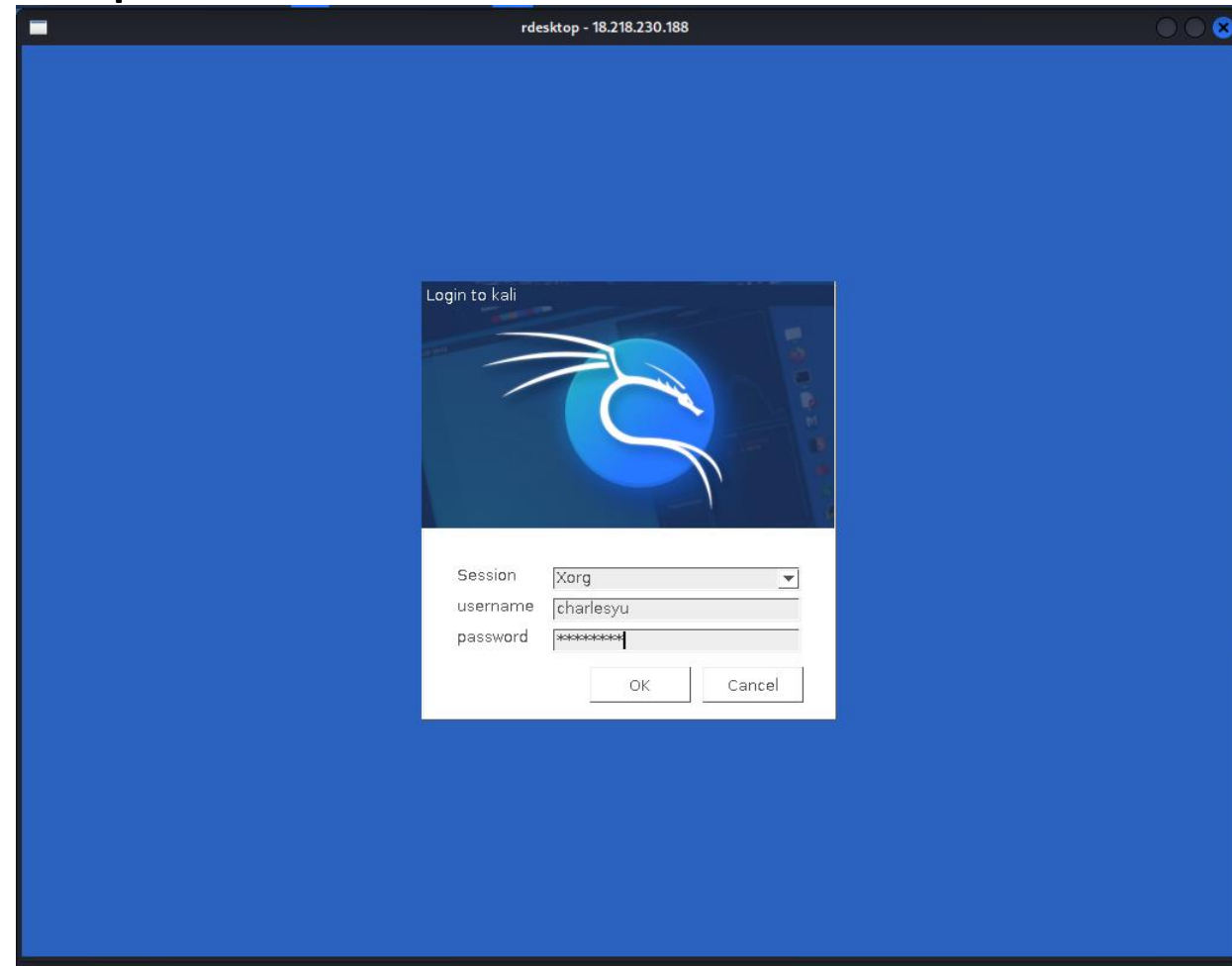
- This is it! This is the command I typed from my Kali Linux in my VirtualBox

```
(kali@kali)-[~]  
$ rdesktop 18.218.230.188
```

- Kali Linux (VirtualBox) –(Connect to)→ Kali Linux @ AWS EC2

# A Quick Introduction to Kali Linux in AWS

- There we go. This is the remote desktop
- I use the account / password,
- I just setup the login account / password info. in slide #4 and #5
- Use this info. to login to the RDP



# A Quick Introduction to Kali Linux in AWS

- Cool! Isn't it?
- Well, the ugly truth is that, it is not very cool 😊
- Actually, it is very slow in the UI responses
- There is another thing called VNC. If we have enough time, we will go through it.



# A Quick Introduction to Kali Linux in AWS

- We can log out first
- Then, we will go back to the Kali Linux in our VirtualBox
- This small screen will close up quickly





# A Quick Introduction to Kali Linux in AWS

- We are not satisfied! Change the resolution from the command line
  - `rdesktop 18.218.230.188 -u charlesyu -g 1920x1080`

• This looks  
Good.  
The  
resolution  
is much  
better



# A Quick Introduction to Kali Linux in AWS

- In the next 2 meeting, we will go through detail security settings in our EC2 instance.
- Then, we will quickly head to cryptography / key management