TDDE61 Ethical hacking
Lecture 3: Lab preparation

Mikael Asplund

LINKÖPING UNIVERSITY

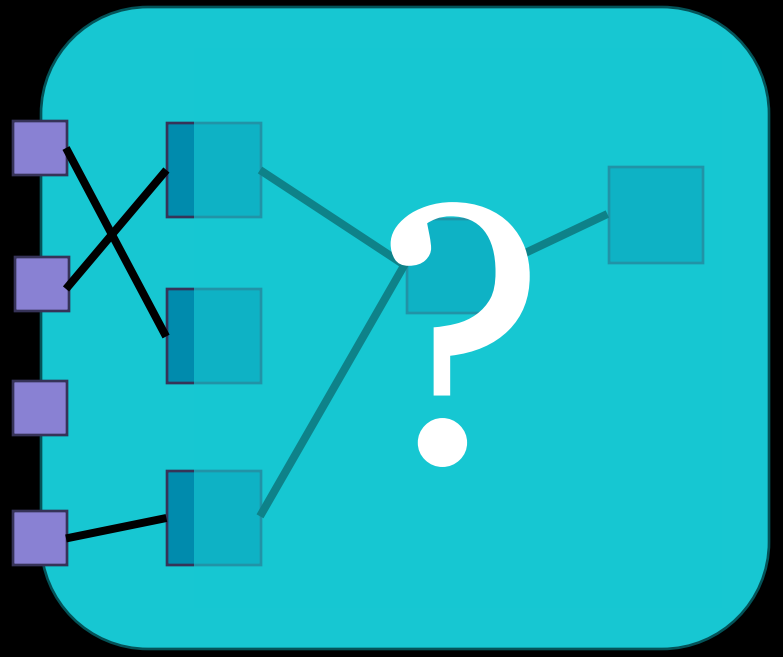
Working together

Lab servers

- 3 Dell PowerEdge R7615 servers each with
  - AMD Epyc 9523p CPU with 32 cores (64 threads)
  - 768GB RAM
  - 7TB disks
  - Dual-Port 25Gb/s SFP+-based network card

Lab setup

- Each pair will get their own ”world” to play around with
  - (Unless we get performance issues)
- Each world will have a range of 255 “external” IP addresses (D network)
  - 10.20.W.0/24, W=World number
- Within each world - a 10.0.0.0/22 network
  - Undisclosed network topology



Machines in the world

- Can be running different operating systems
- Can have several services running
- Might try to hide from you and evade your attacks
- Might not always be running

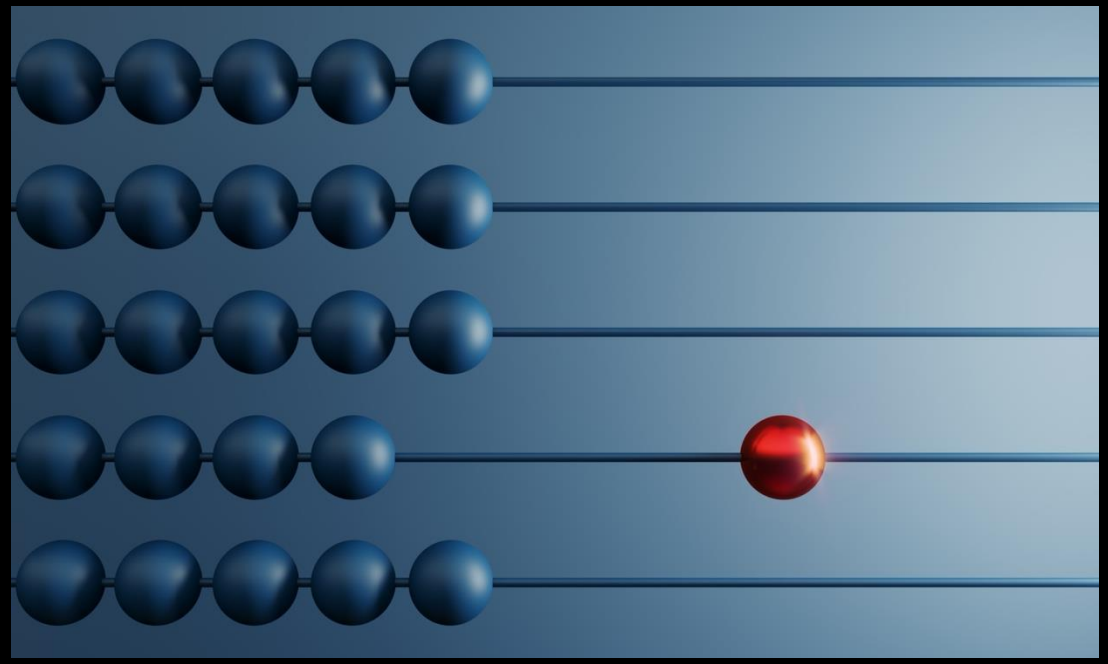
Flag points

- Flags for VT1: 40 points
  - Feb 5 - March 21
- Flags for VT2: 60 points
  - March 31 – May 29
- Flags in VT2 are more complex…

Nr	Topic	Points
1	Tutorial flag	4
2	Web crawling	6
3	Database hacking	9
4	Password cracking	4
5	Security by obscurity	8
6	Remote exploitation	9

Flags and grades

- Grade 3:
  - At least 20/100 points
  - All flags passed
- Grade 4:
  - At least 50/100 points
  - Al flags passed
- Grade 5:
  - At least 80/100 points
  - All flags passed

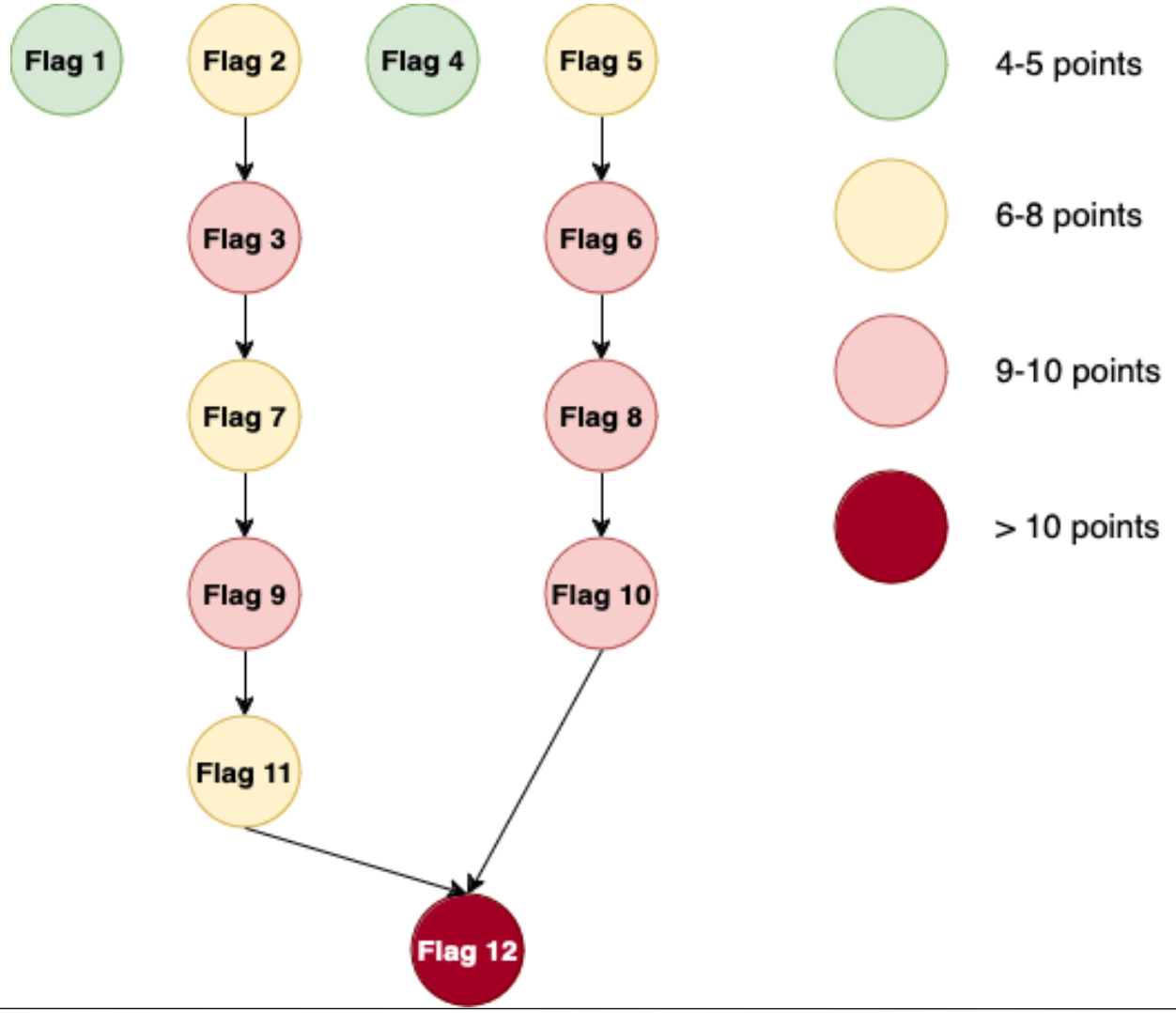


Hint point deduction

- Cumulative!
- End of March, 24/40 points have been automatically deducted
- Full solution available on-demand (after last hint)
  - Full deduction of points

Time of announcement	Flag number	Hint	Point deduction
2025-02-19 17.00	2	1	2
2025-02-21 17.00	2	2	2
2025-02-26 17.00	3	1	2
2025-02-26 17.00	4	1	2
2025-02-28 17.00	3	2	4
2025-03-05 17.00	5	1	1
2025-03-07 17.00	5	2	5
2025-03-12 17.00	6	1	1
2025-03-14 17.00	6	2	2
2025-03-21 17.00	6	3	3

Flag dependencies

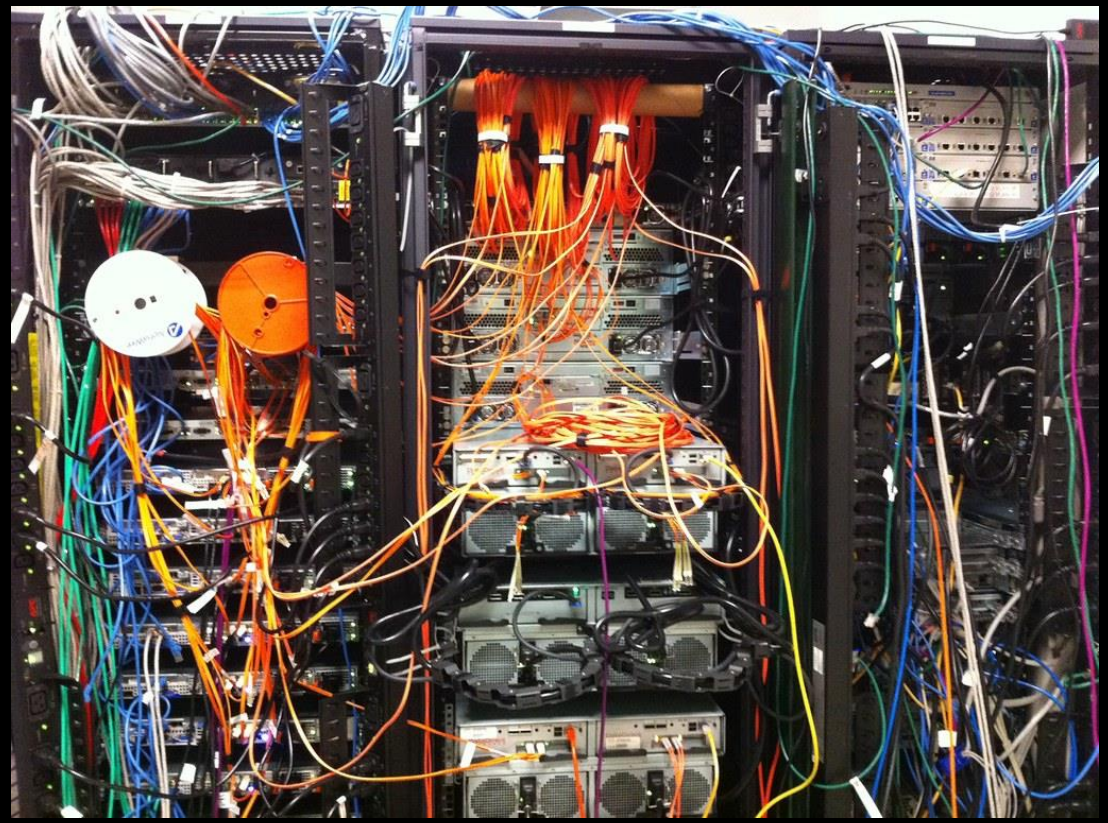


On **your world** you are free to

- Do port scans
- Intercept network traffic
- Decrypt (if you can)
- Launch exploits
- Insert own traffic
- Modify compromised hosts (including installing software)
- Use compromised hosts for computing tasks related to the labs
- Crack passwords
- Escalate your privileges
- Exfiltrate data
- Poke at the virtualization environment*

*Poking at the virtualization environment

- Servers are supposed to be transparent
  - There *should* be no way in for you into these machines
- Virtualization security is hard
  - There might be gaps
- You can try to find the gaps
  - Tell us if you find any
  - Do not take advantage!

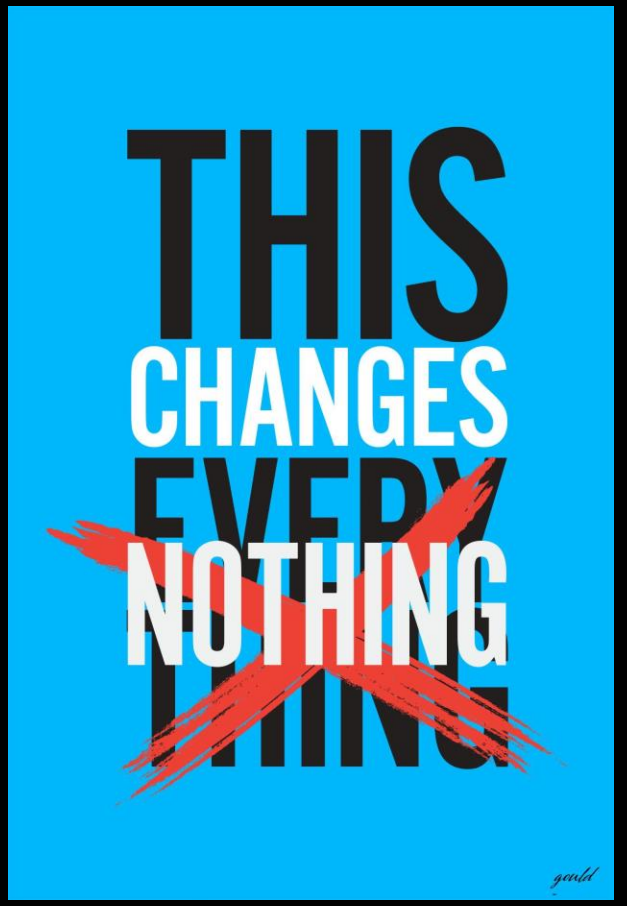


Internet access

- Is open from Kali VMs (web traffic only)
- Is blocked from within the world

Be prepared for disturbances

- Machines will reboot and be reset every day
  - You need to develop scripts to automate your attacks
- System configurations can change
- Network topologies can change



Stick and carrot

- Stick:
  - If you find a new vulnerability and take undue advantage – you will fail the course (and be reported)
- Carrot:
  - If you find a new vulnerability and tell us you will be rewarded with additional bonus points

Point policy for misconfigured flags

- If you find a flag with a method which is subsantially easier than the original design, the following policy will be applied.
  - Submitting the flag and informing us about the issue will reward you a number of points which is less than the full points for the flag.
  - After we patch the issue, you can again find the flag in the intended manner.
  - You receive full points for the flag so that the total points you receive is higher than the original number of points for the flag.

You are NOT allowed to

- Target **any** IP outside your given range
  - This includes port scanning and sniffing traffic
- Hinder other students
- Use compromised machines for other tasks (e.g., cryptomining)

We are watching you…

- Your activities are logged

- Breaking the rules can lead to
  - Failing the course
  - Being reported to the disciplinary board
  - Being reported to the police
  - Sending you to David Byers

Penetration testing basics

Penetration testing steps

Pre-engagement

Defining the scope

- Black-box, grey-box or white-box testing
- Systems that can be compromised or not
- Setting expectations (including timing)

Do the legal work

- Get-out-of-jail card
- Probably you are required to sign a Non-disclosure Agreement (NDA)

Intelligence gathering

- OSINT– Open Source Intelligence Gathering
- Collect data from:
  - Social media
  - Public records
  - Online services
- No actions on the actual system

Engagement

Mitre ATT&CK

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

https://attack.mitre.org/

Mitre ATT&CK

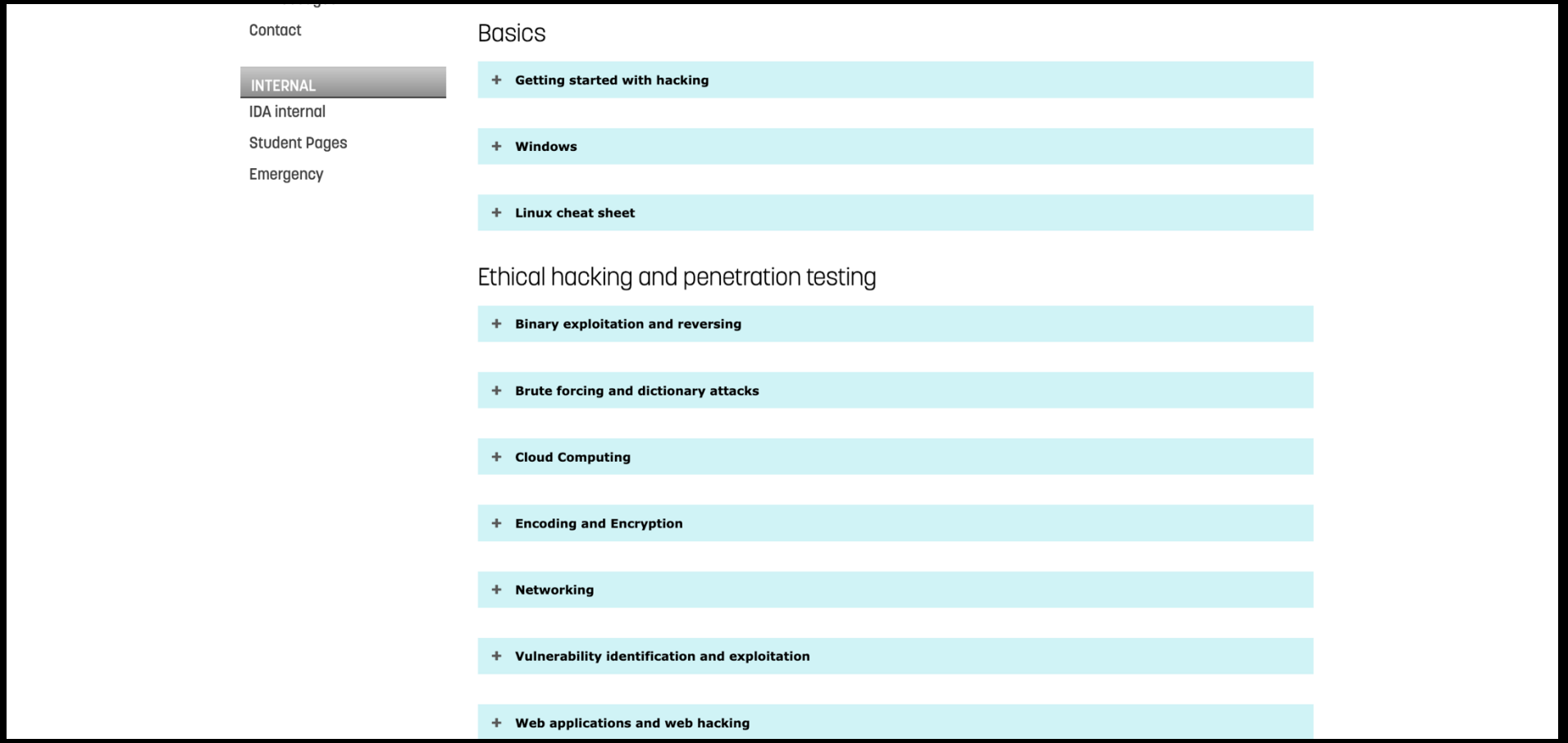
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

https://attack.mitre.org/

Some useful tools

- Nmap
- Netcat
- Burpsuite and skipfish
- gobuster
- Sqlmap
- Nessus
- Metasploit
- Hydra
- Mimikatz
- Bash
- Powershell
- cURL and wget
- Tcpdump and wireshark
- Python
- ssh
- …

www.ida.liu.se/~TDDE61/resources



Post-engagement

Report writing

- Explain to the customer what you have done and how
- Can any successful attacks be prevented? How?
- For whom are you writing?
  - Executive summary
  - Detailed info

Other post-engagement activities

- Get feedback
- Learn
- Validate and re-test
- Clean-up

More detailed instructions

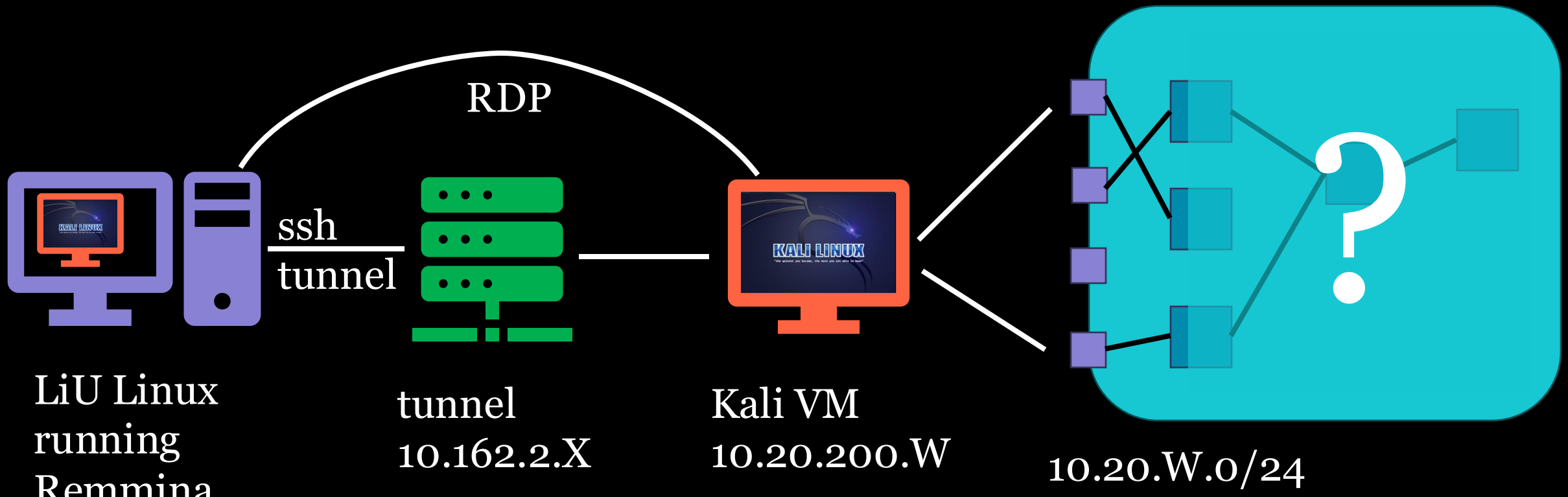
Steps to complete

- Sign up in webreg
- Setup the lab environment (two options exist)
- For every flag:
  - Find the flag (with hints if needed)
  - Submit the flag (CTFd)
  - Submit a writeup (Lisam)
  - Demonstrate the flag to your lab assistant
- Done!

Information provided:

- Username (your liuid)
- Password
- World number
- Tunnel IP
- IP start
- Tunnel number (option 2 only)
- Local tunnel IP (option 2 only)
- Remote tunnel IP (option 2 only)
- Callback IP (option 2 only)

Accessing the world option 1

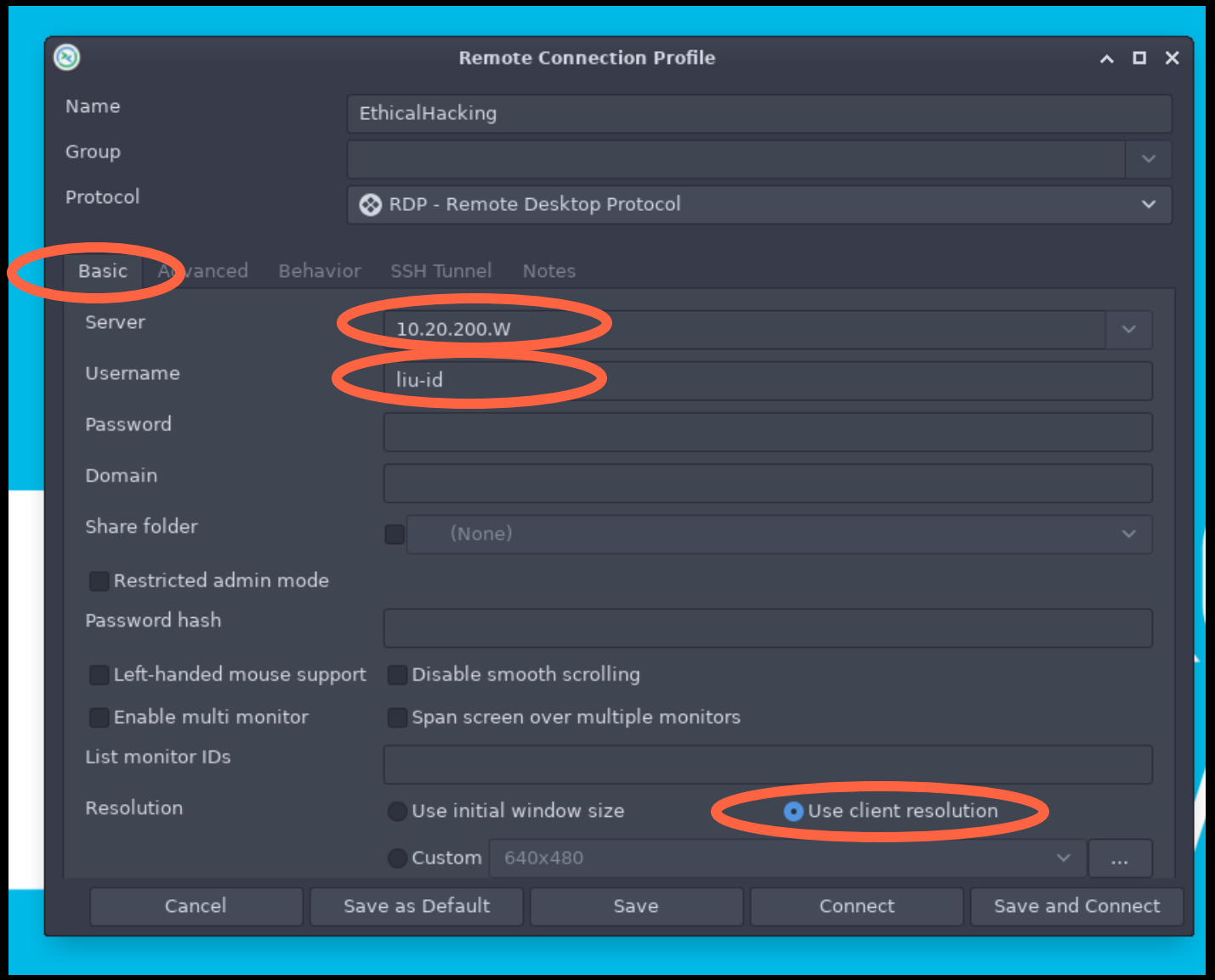


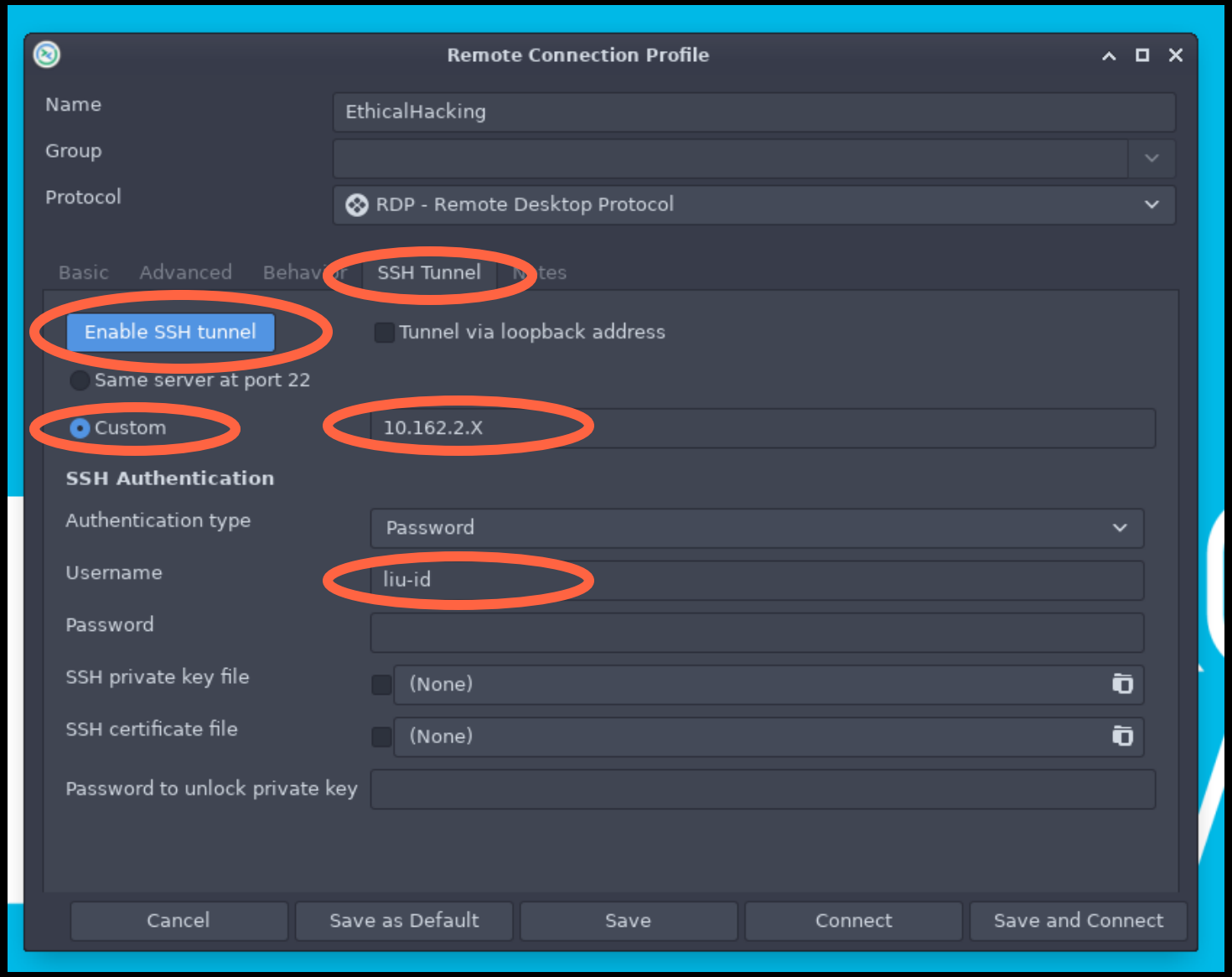
X = 4/5/6, W = world number

Accessing the world from LiU linux

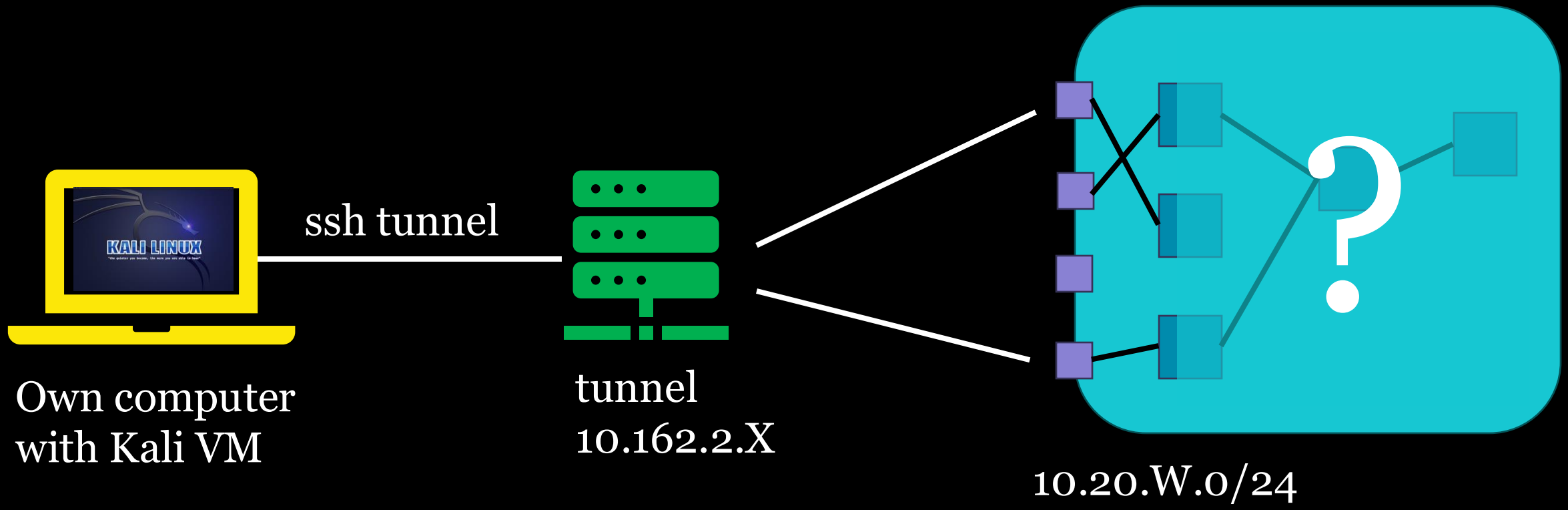
- Start Remmina
- Create new connection
- Under “Basic tab”:
  - Add Server 10.20.200.W
  - Add username (liuid)
  - Choose “Use Client resolution”
- Under “SSH Tunnel”
  - “Enable SSH tunnel”
  - Select “Custom”
  - Enter Server 10.162.2.X
  - Authentication type “Password”
  - Username (liuid)
- Save and Connect

- W – World number
- X – Tunnel IP


Remote Connection Profile
Name
EthicalHacking
Group
Protocol
RDP - Remote Desktop Protocol
Basic
Advanced
Behavior
SSH Tunnel
Notes
Server
10.20.200.W
Username
liu-id
Password
Domain
Share folder
(None)
Restricted admin mode
Password hash
Left-handed mouse support
Disable smooth scrolling
Enable multi monitor
Span screen over multiple monitors
List monitor IDs
Resolution
Use initial window size
Use client resolution
Custom
640x480
...
Cancel
Save as Default
Save
Connect
Save and Connect


Remote Connection Profile
Name
EthicalHacking
Group
Protocol
RDP - Remote Desktop Protocol
Basic
Advanced
Behavior
SSH Tunnel
Notes
Enable SSH tunnel
Tunnel via loopback address
Same server at port 22
Custom
10.162.2.X
SSH Authentication
Authentication type
Password
Username
liu-id
Password
SSH private key file
(None)
SSH certificate file
(None)
Password to unlock private key
Cancel
Save as Default
Save
Connect
Save and Connect

Accessing the world option 2



X = 4/5/6, W = world number

Accessing the world from own VM

- Only partially supported
- Install a VM on your own laptop (Kali is strongly recommended)
- Setup local tunnel and routing (sudo required)
  - Script to download from web page
- Start ssh tunnel
  - ssh –w0:T liuid@10.162.2.X –f true
  - liuid – your liuid
  - T – tunnel number
  - X – 4/5/6 (tunnel IP)
  - (ignore message about home directory)

setup-network.sh

```
TUNNEL_IP=10.162.2.X
LOCAL_TUNNEL_IP=10.0.99.Y
REMOTE_TUNNEL_IP=10.0.99.Z
LOCAL_DEV=eth0
ip link del tun0
ip tuntap add mode tun dev tun0 user mikael
ip addr add $LOCAL_TUNNEL_IP/31 dev tun0
ip link set tun0 up
ip route add $REMOTE_TUNNEL_IP dev tun0
ip route add 10.20.0.0/16 via $REMOTE_TUNNEL_IP dev tun0
```

Callback addresses

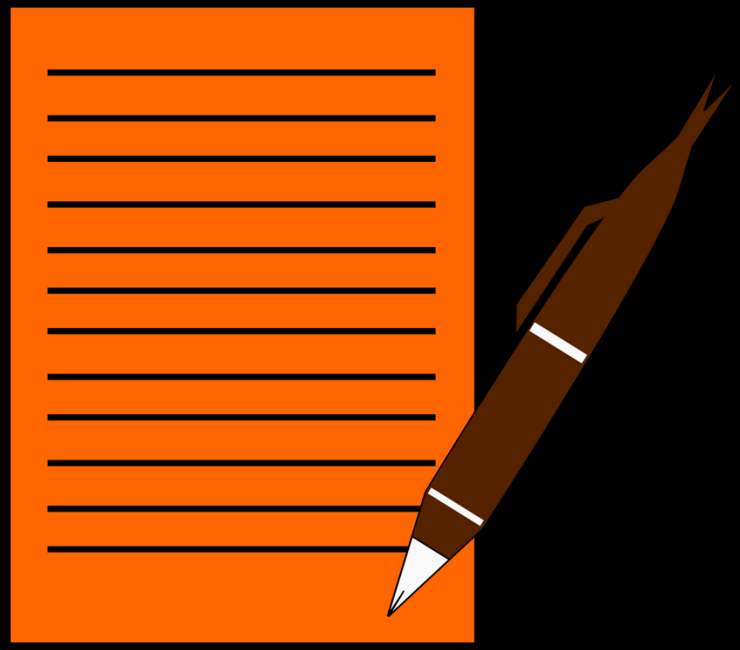
- For LiU Kali VM
  - 10.20.200.W is accessible from within the world
- For own Kali VM
  - 10.20.W.10 or 10.20.W.11 (depending on which student)
- **DO NOT ATTACK THESE ADDRESSES!**

Demonstrations

- Demonstrate the flag to your lab assistant
- No strict timing requirement
  - Don’t do all the last week
- Both students in a pair need to be able to explain

Writeups

- Write what you did and why you did it that way
- Submit it in Lisam at most 1w after the flag
- 1-2 pages
- Free format



Questions?