

TDDE61 Ethical hacking

Lecture 3: Lab preparation

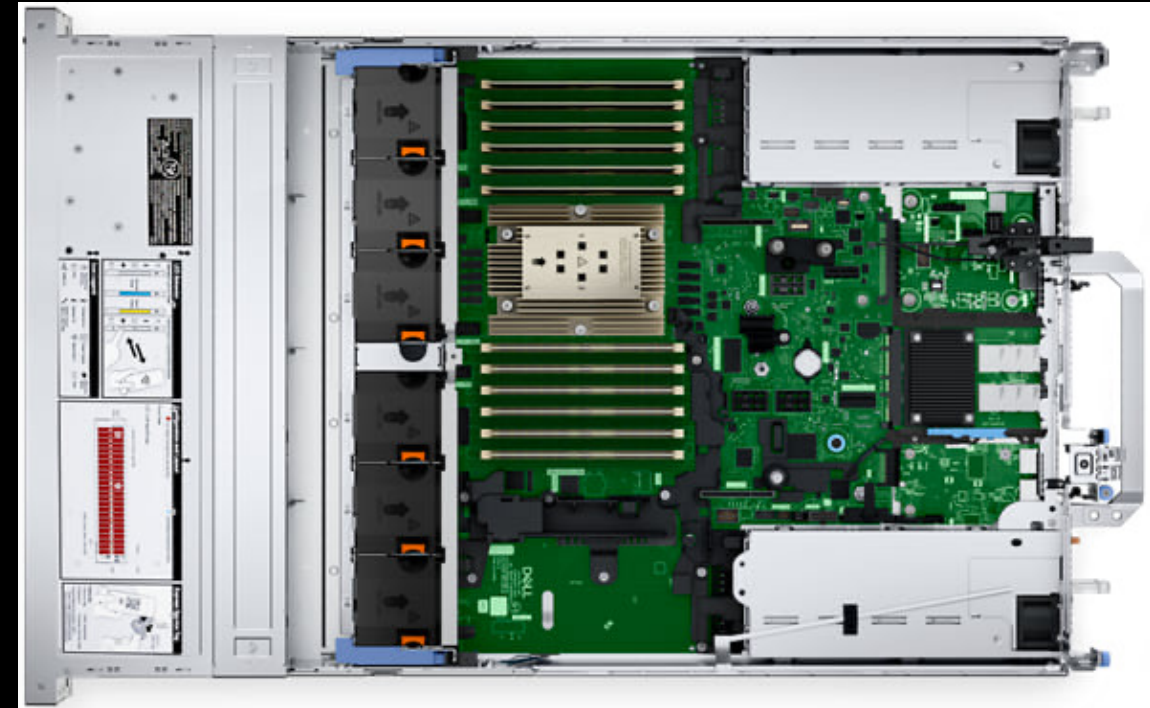
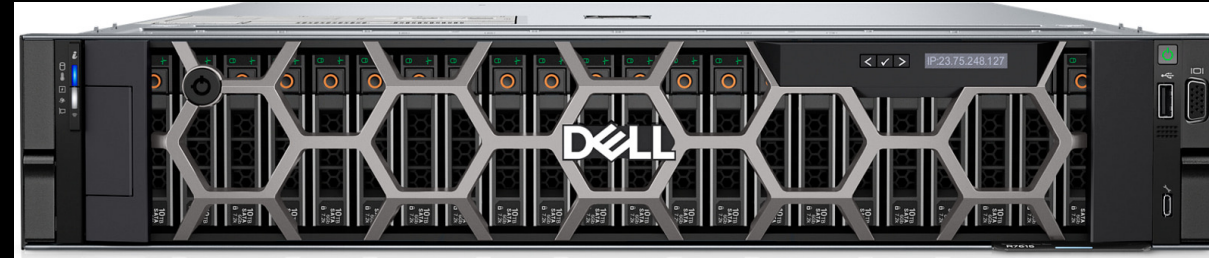
Mikael Asplund

Working together



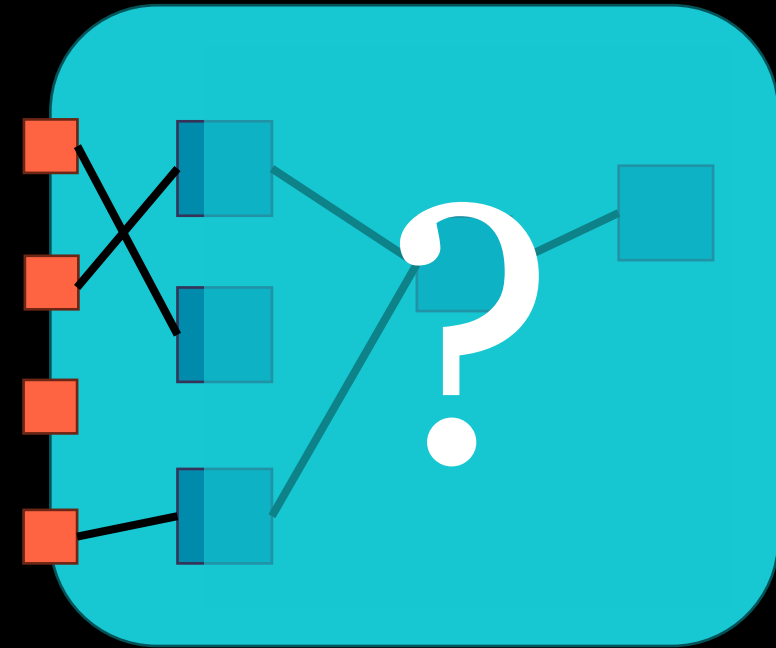
Lab servers

- 3 Dell PowerEdge R7615 servers each with
 - AMD Epyc 9523p CPU with 32 cores (64 threads)
 - 768GB RAM
 - 7TB SSD 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 10 IP addresses on the LiU network
 - VPN needed to connect even when on campus
- Within each world - a 10.0.0.0/16 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

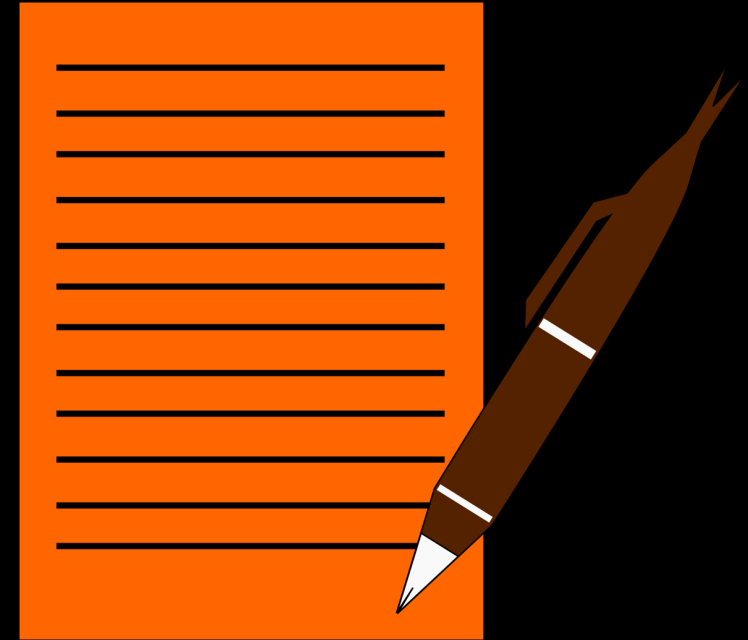
Be prepared for disturbances

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



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

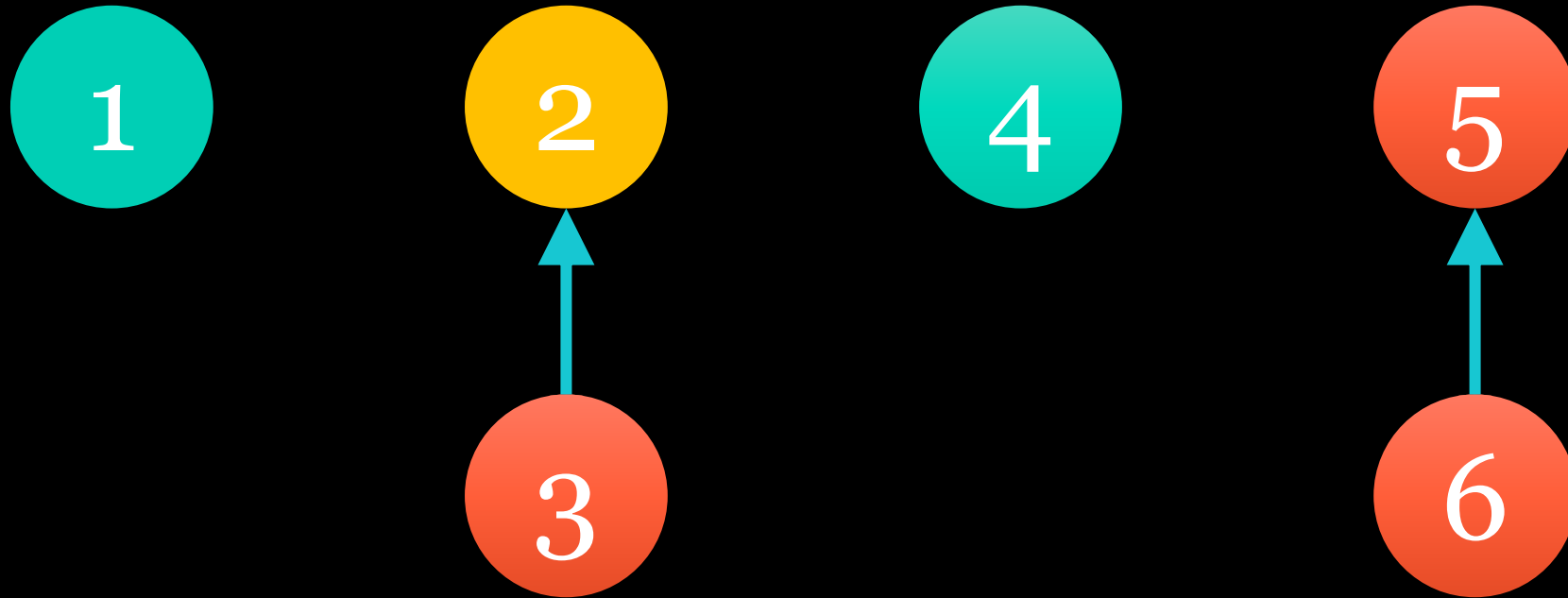


More on flags

- Flags for VT1: 40 points
 - Jan 29 - March 8
- Flags for VT2: 60 points
 - March 8 (25) – May 22
- Flags in VT2 will *probably* be 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

Flag dependencies VT1



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

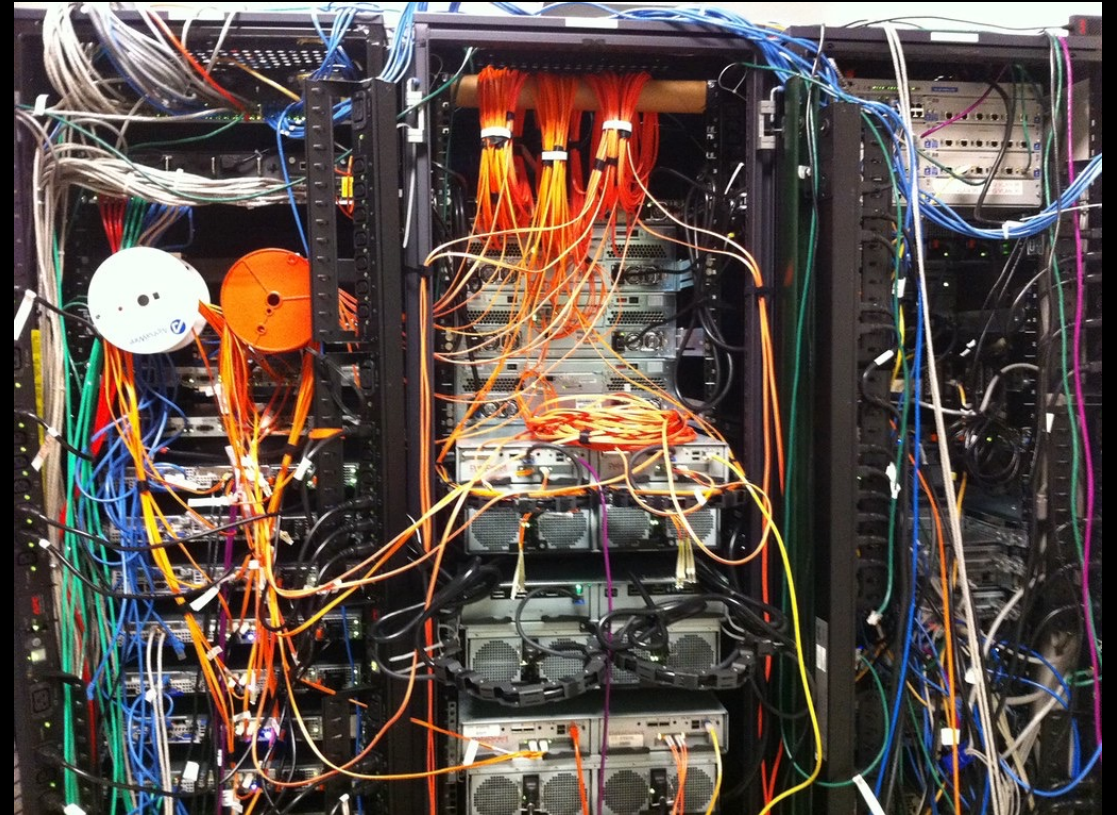
Hint	Time of announcement	Point deduction
2:1	2024-02-09, 17:00	2/6
2:2	2024-02-16, 17:00	2/6
3:1	2024-02-16, 17:00	2/9
3:2	2024-02-23, 17:00	4/9
4:1	2024-02-23, 17:00	2/4
5:1	2024-03-01, 17:00	1/8
5:2	2024-03-08, 17:00	5/8
6:1	2024-03-08, 17:00	1/9
6:2	2024-03-15, 17:00	2/9
6:2	2024-03-23, 17:00	3/9

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!



[Det här fotot](#) av Okänd författare licensieras enligt [CC BY](#)

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



You are **NOT** allowed to

- Target **any** IP outside your given range
 - This includes port scanning and sniffing traffic
 - Beware the LiU VPN
- 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

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

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

Contact	Basics
INTERNAL	+ Getting started with hacking
IDA internal	
Student Pages	+ Windows
Emergency	+ Linux cheat sheet
	Ethical hacking and penetration testing
	+ Binary exploitation and reversing
	+ Brute forcing and dictionary attacks
	+ Cloud Computing
	+ Encoding and Encryption
	+ Networking
	+ Vulnerability identification and exploitation
	+ Web applications and web hacking

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

Questions?

