TDDE61 Ethical hacking

Mikael Asplund

LINKÖPING UNIVERSITY

Why this course?

- **July 2012** – Attackers had access to OPM's network.[357]
- **November 2013** – The first known adversarial activity begins in OPM's network that led to the breach identified by US-CERT in March 2014.[358]
- **December 2013 –** Adversarial activity to harvest credentials from OPM contractors begins by the attackers later identified in April 2015.
- **March 20, 2014** – US-CERT notified OPM of malicious activity and OPM initiates investigation and monitoring of adversary.
- **March 2014 to May 2014 –** OPM (under US-CERT guidance) investigated 2014 incident and monitored attackers.
- **April 25, 2014** – The domain "Opmsecurity.org" is registered to Steve Rogers (a.k.a. Captain America).[359] This domain was later used to exfiltrate data from OPM's network.
- **May 7, 2014** – The attacker poses as a background investigations contractor employee (KeyPoint), used an OPM credential, remotely accessed OPM's network and installed PlugX malware to create a backdoor. The agency's forensic logs show "infected machines" were accessed through a VPN connection, which was how background

https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

investigation contractors accessed OPM's network. At the time, OPM gave contractors a username and password and investigators would log in with this OPM credential.[360]

- **May 27, 2014** – OPM initiates "Big Bang" to eliminate attackers and complete remediation. This decision was made after OPM observed the attackers "load a key logger onto . . . several database administrators' workstations" and they got "too close to getting access to the PIPs system."[361] Meanwhile, the attacker that established a foothold on May 7, 2014 remained in the OPM network.

- **June 5, 2014 –** Malware is installed.[362] This malware installation appears to have been facilitated through the backdoor established on May 7, 2014.[363]

- **June 2014** – OPM contractor USIS self-detects a cyber-attack on its IT system and notified OPM.[364] USIS investigates and blocks and contains the attacker by early July, and invites US-CERT to USIS facilities to investigate by late July 2014.[365]

- **June 20, 2014** – Attackers conduct a remote desktop protocol (RDP) session indicating the attackers had escalated their access and began moving deeper into the network, contacting "important and sensitive servers supporting . . . background investigation processes." This RDP session was not discovered until 2015.[366]

- **June 23, 2014** – First known adversary access to OPM's mainframe, according to US-CERT.[367]

- **July to August 2014** – Attackers successfully exfiltrate OPM background investigation data. OPM contractor Brendan Saulsbury testified that forensic logs showed "they are sort of touching or accessing the data during the summer of 2014."[368]

https://oversight.
Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

- **July 29, 2014** – The domain "Opm-learning.org" is registered to Tony Stark (a.k.a. Iron Man).[369]
- **August 2014** – Following public reports of a data security breach at another contractor, OPM requested access to KeyPoint facilities and KeyPoint agreed.[370]
- **August 16, 2014** – The malware installed on June 5, 2014 appears to cease operational capabilities.[371]
- **October 2014** – Attackers move through the OPM environment to the Department of Interior data center where OPM personnel records are stored.[372]
- **December 2014** – Attackers exfiltrate 4.2 million personnel records.[373]
- **March 3, 2015 -** "wdc-news-post[.]com" is registered by attackers. Attackers would use this domain for C2 and data exfiltration in the final stage of the intrusion.[374]
- **March 9, 2015 –** Last beaconing activity to the unknown domain "opmsecurity.org" registered to Captain America, attackers switched their attack infrastructure to "wdc-"news-post.com" as their primary C2 domain for the remainder of the intrusion.[375]
- **April to June 2015** – Primary incident response and investigation period.

https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

"My SF-86 lists every place I've ever lived since I was 18, every foreign travel I've ever taken, all of my family, their addresses. So it's not just my identity that's affected. I've got siblings. I've got five kids. All of that is in there."[§]

— James Comey, Director of the FBI

"We cannot undo this damage. What is done is done and it will take decades to fix."[†]

— John Schindler, former NSA officer

LINKÖPING UNIVERSITY

https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

PEGASUS BY THE NUMBERS

GLOBAL SCALE

36 LIKELY OPERATORS

45 COUNTRIES WITH LIKELY INFECTIONS

10 OPERATORS WITH INFECTIONS IN ANOTHER COUNTRY

HUMAN RIGHTS

6 OPERATORS LINKED TO COUNTRIES WITH A HISTORY OF ABUSING SPYWARE TO TARGET CIVIL SOCIETY

CITIZEN LAB 2018

[Hacking Team Emails](#).

ForcedEntry (iOS exploit)

- PDF files disguised as GIF files – invokes PDF reader
- Uses JBIG2 image codec
- Integer overflow flaw allows JBIG2 bitmap to extend over regular memory
- Image compression format turns out to be Turing complete
  - ”Decompressing” the image stream makes allows changing arbitrary memory regions

https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please fo

Cost: ~10 billion EUR

1. Send $

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.

NotPetya

- Malware (claoms to be ransomware)
- Most probably developed by GRU (russian intelligence services)
- Used in 2017 to attack Ukraine
  - Electric grid
  - Central bank
  - Airports
  - …

NotPetya in 8 steps

1. Spread to new networks through imfected software (MeDoc)
2. Find and disable anti-virus
3. Steal credentials
4. Pivot to other machines in the network
5. Replace the boot sector
6. Reboot
7. The virus is now in control, encrypt the drive and show message
8. Clean up (anti-forensics)

NotPetya in 8 steps

1. Spread to new networks through imfected software (MeDoc)
2. Find and disable anti-virus
3. Steal credentials
4. Pivot to other machines in the network
5. Replace the boot sector
6. Reboot
7. The virus is now in control, encrypt the drive and show message
8. Clean up (anti-forensics)

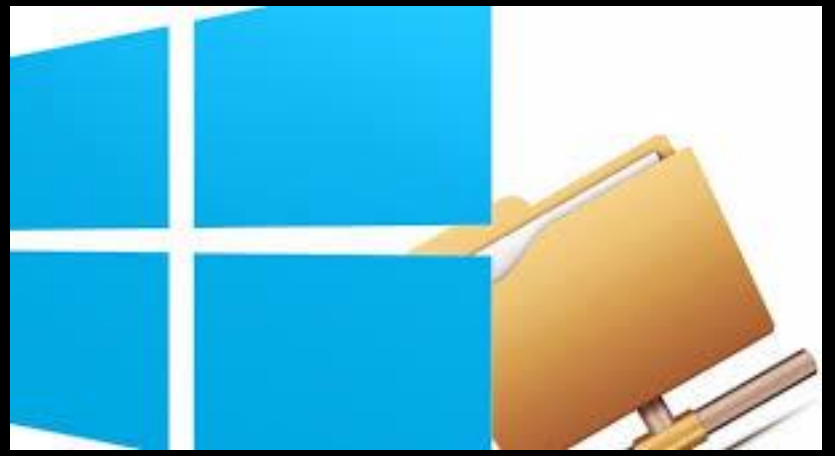
Step 1 (initial access)

- M.E.Doc
  - Tax program
  - 400 000 customers in Ukraine (90% of all business)
  - 1M installations
  - Automatic updates

- June 2017: M.E.Doc was infected with NotPetya
  - Quickly spread to most customer sites

Fourth step (pivoting)

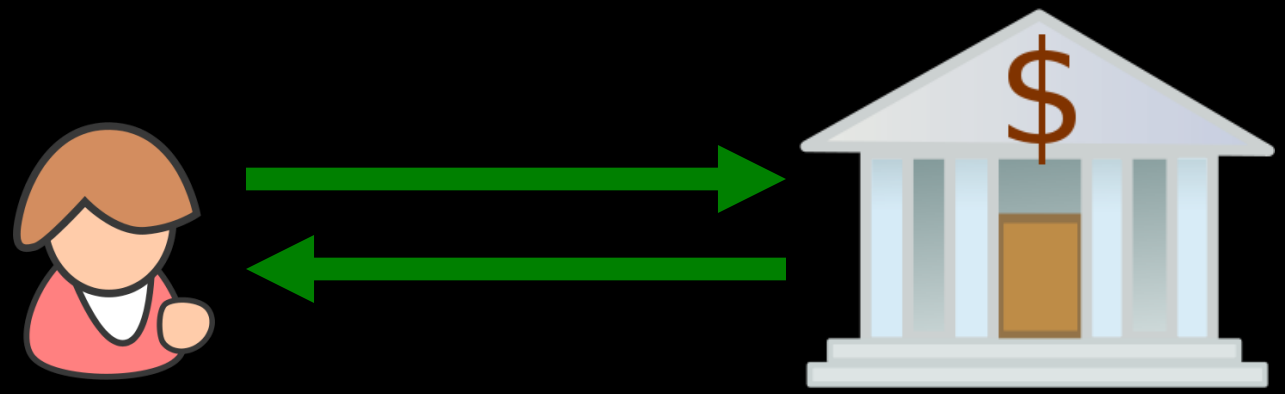
- Eternal blue: A cyberattack exploit
- Creator: US National Security Agency (NSA)
  - Stolen by the hacker group Shadow Brokers
- Spreads to network sharing protocol
  - SMBv1
  - Multiple bugs allowing remote execution



Secure connections

- Cryptography to ensure
  - Confidentiality
  - Integrity
  - Authenticity

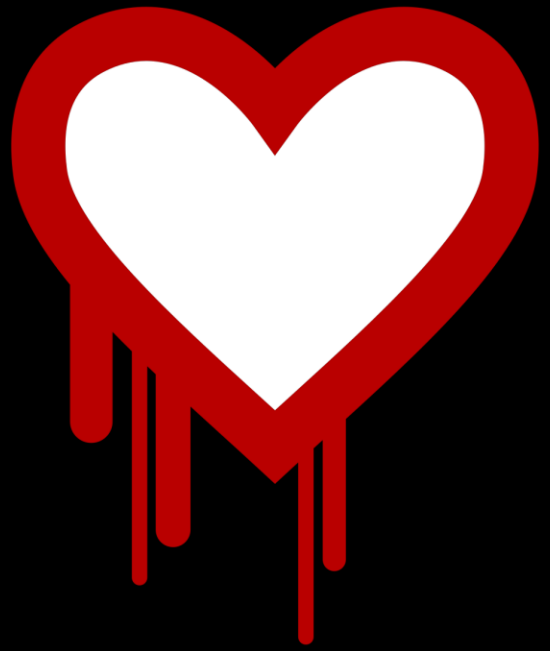
- Standard protocol TLS



Heartbeat

- Mobile units can suddenly loose their connection
- Use heartbeats to check if the other node is still there
- Computer A: Are you there, here is a message with 20 characters:
  ”ASFLKFQF#IN2FH!RO;&W”
- Computer B: Yes, I’m still here. You sent this message:
  ”ASFLKFQF#IN2FH!RO;&W”

Heartbleed



- Computer A: Are you there, here is a message with 20 characters:
  "A"
- Computer B: Yes, I'm still here. You sent this message:
  "A##SECRET###SECRET##"
- From the source code of OpenSSL:

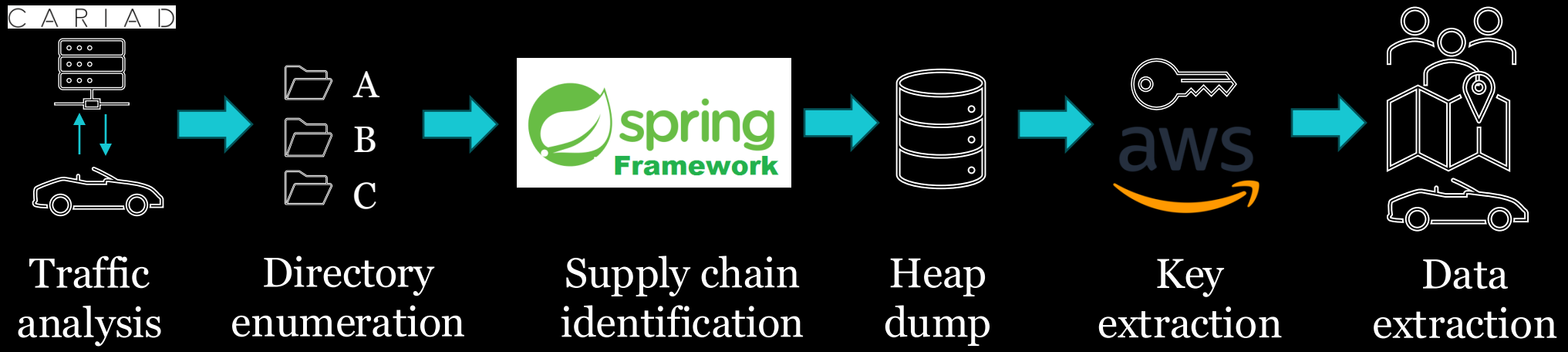
```
buffer = OPENSSL_malloc(1 + 2 + payload + padding);
bp = buffer;
memcpy(bp, pl, payload);
```

- (pl is pointer to the real message, payload is the given length, bp is a pointer to the message that will be sent)

VOLKSWAGEN DATA BREACH:

800,000 ELECTRIC CAR OWNERS' DATA LEAKED

Volkswagen data breach



[https://media.ccc.de/v/38c3-wir-wissen-wo-dein-auto-steht-volksdaten-von-volkswagen]

What’s the point?

Complex systems will inevitably have bugs

Some bugs are also security vulnerabilities

This course is not about developing new exploits

This course is about how to
think like a hacker

Why?

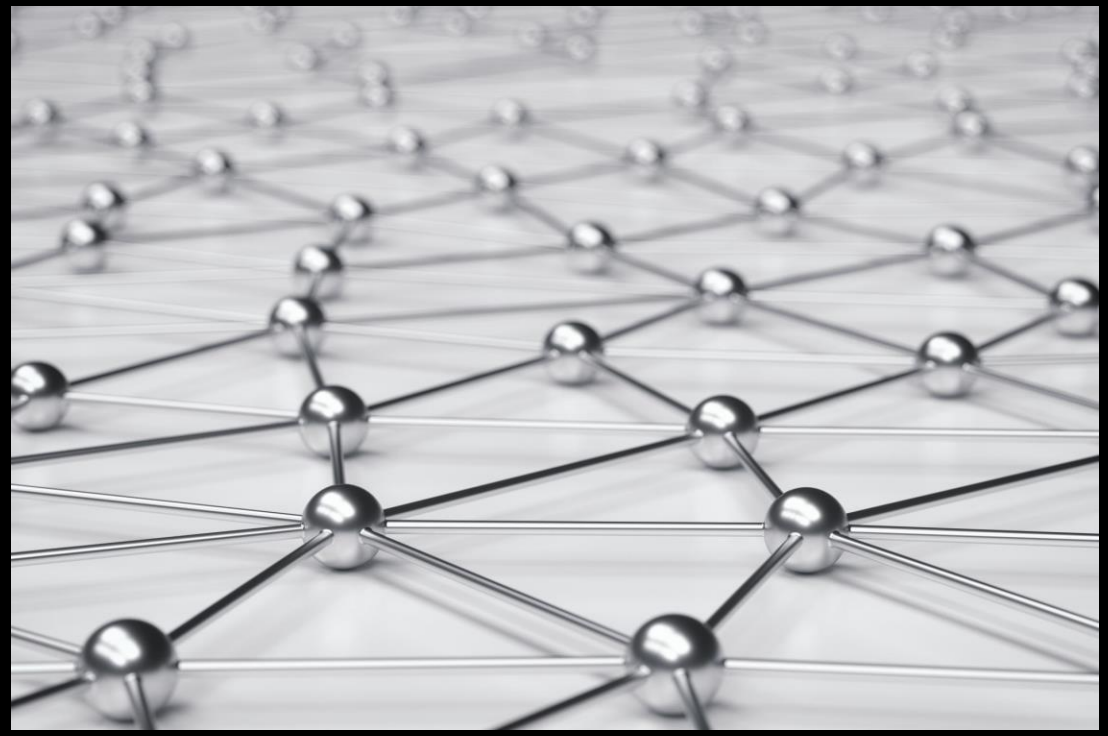
Reasons to know the craft of hacking

1. Work as a penetration tester
2. It takes a thief to catch a thief – learn how to detect and avoid attacks
3. Learn to make better software and systems

Course overview

Course organization

- Lectures
  - Normal lectures (few)
  - Guest lectures (with quizzes)
- Labs
- Ethics seminar

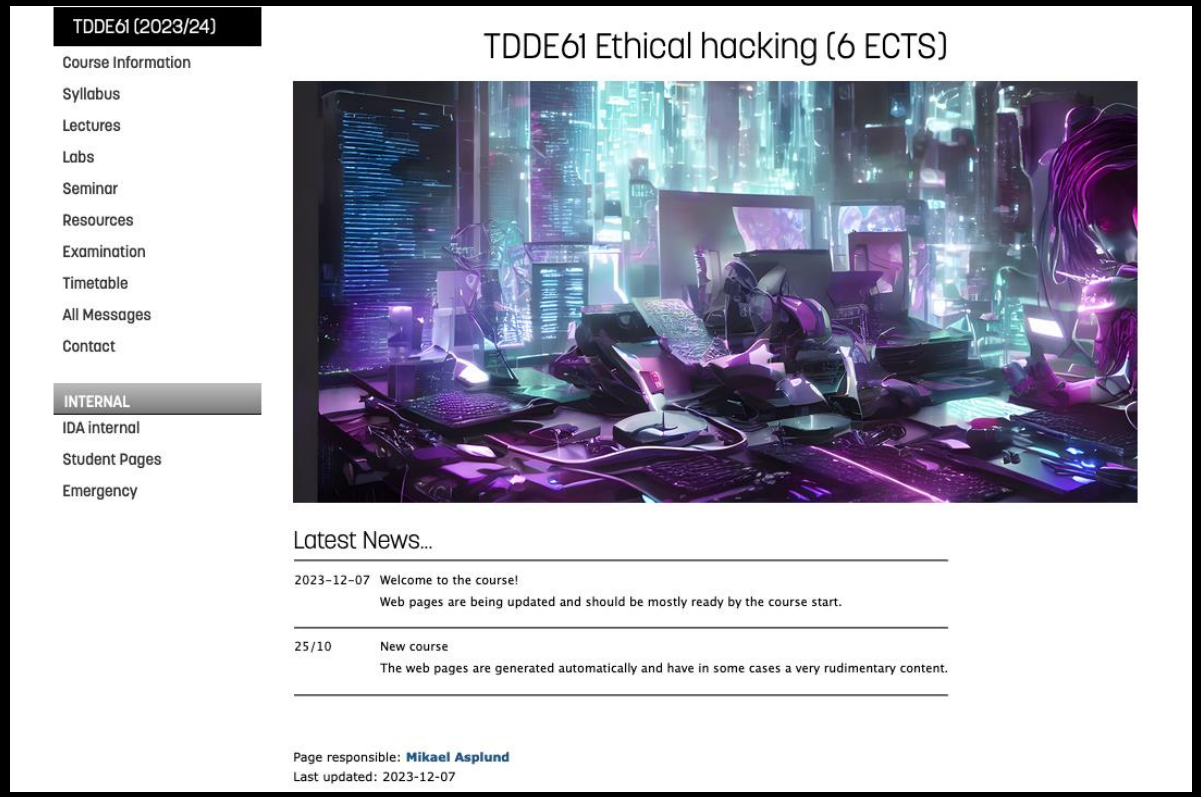


Examination

Exam code	Name	Credits	Grades
DAT1	Computer examination	0.5	U, G
LAB1	Computer labs	4.5	U, 3, 4, 5
UPG1	Seminar	0.5	U, G
UPG2	Online quiz	0.5	U, G

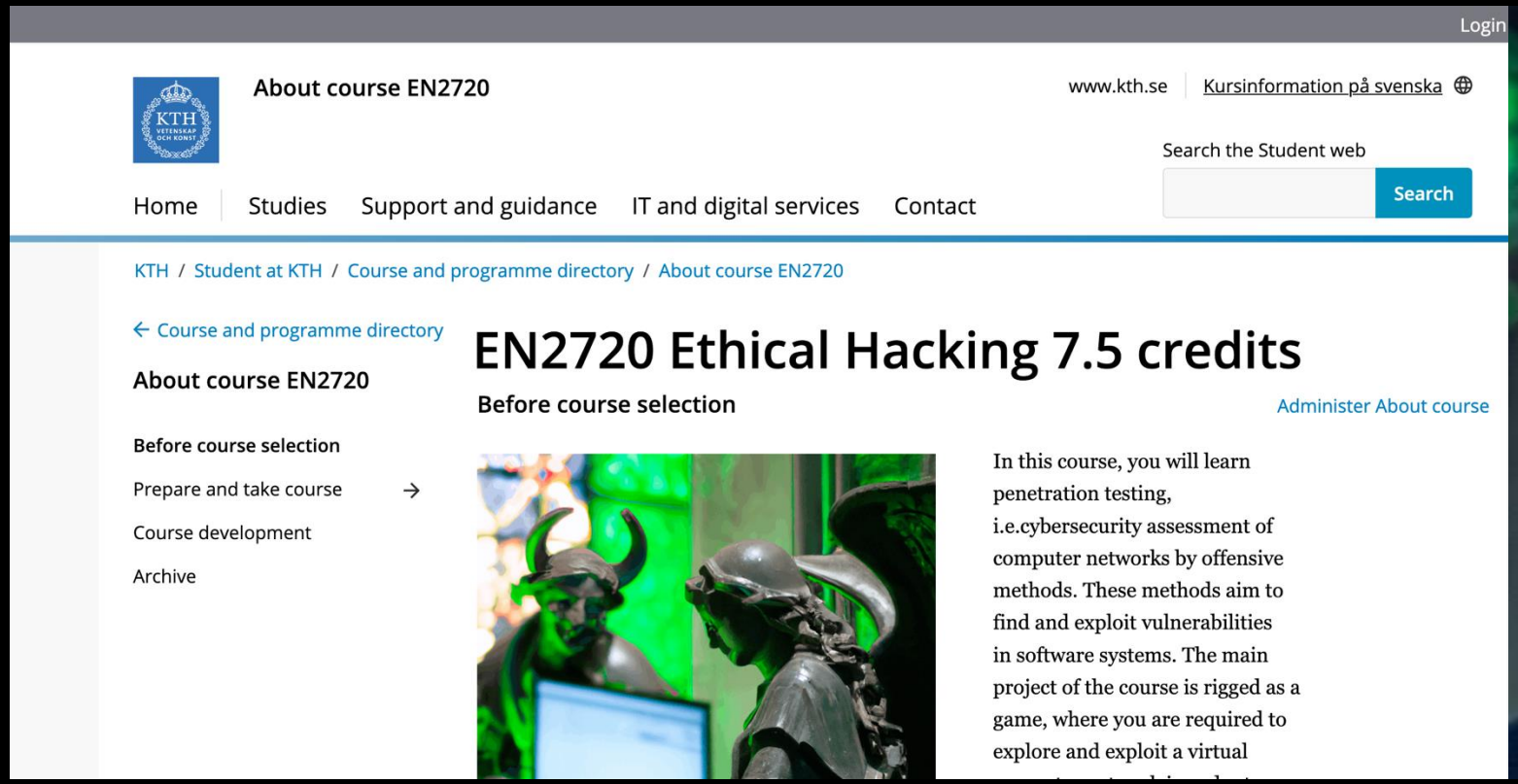
Course web pages

- www.ida.liu.se/~TDDE61
  - All public information here
  - Mostly updated by now
- Lisam/other resource
  - Submission of flags
  - Hints will be published here
  - Quizzes



Big thanks!

To the KTH team, especially Pontus Johnson and Nikolaos Kakouros

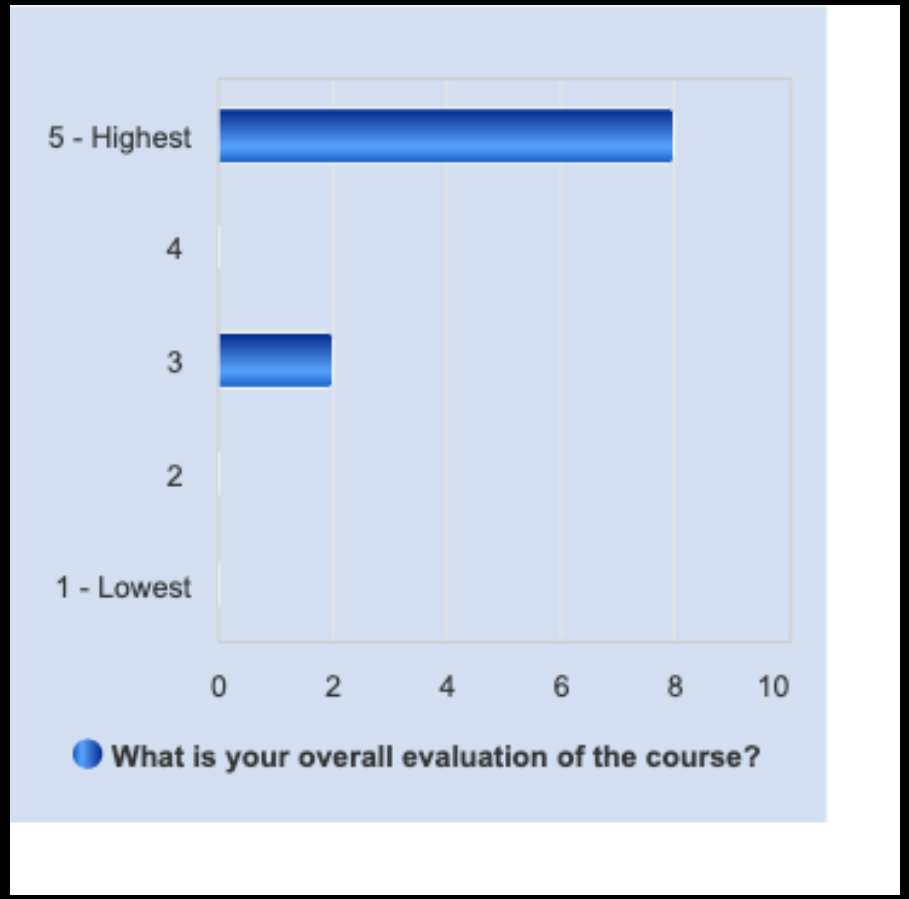


~~First~~ Second time trying

- Completely new type of course for LiU
- Completely new lab setup
- Help us make it as good as possible

Course evaluation and changes

- New lab rooms!
- Lab environment more stable
- Schedule improvement



People

- Mikael Asplund, examiner
- Roland Plaka
  - Lab assistant groups A and C
- Charilaos Skandylas
  - Lab assistant group B and D
  - Technical lab development

Exam on laws and regulation

What I don’t want…

government technology

AI CYBERSECURITY DATA WORKFORCE MORE

Special: Communities Constituents Engagement

CYBERSECURITY

FBI Arrests Student, Employee in University Hacking Case

A yearlong investigation into a hack against Florida’s Embry-Riddle Aeronautical University computers led federal authorities and police to an employee and student, who were allegedly using a program designed to capture administrator passwords.

November 30, 2018 • T.S. Jarmusz, The News-Journal

Stay on top of the latest state & local government technology trends.

Sign up for GovTech Today. Delivered daily to your inbox.

Email Address*

Edmonton · New

Student charged with cyber crimes in U of A malware breach

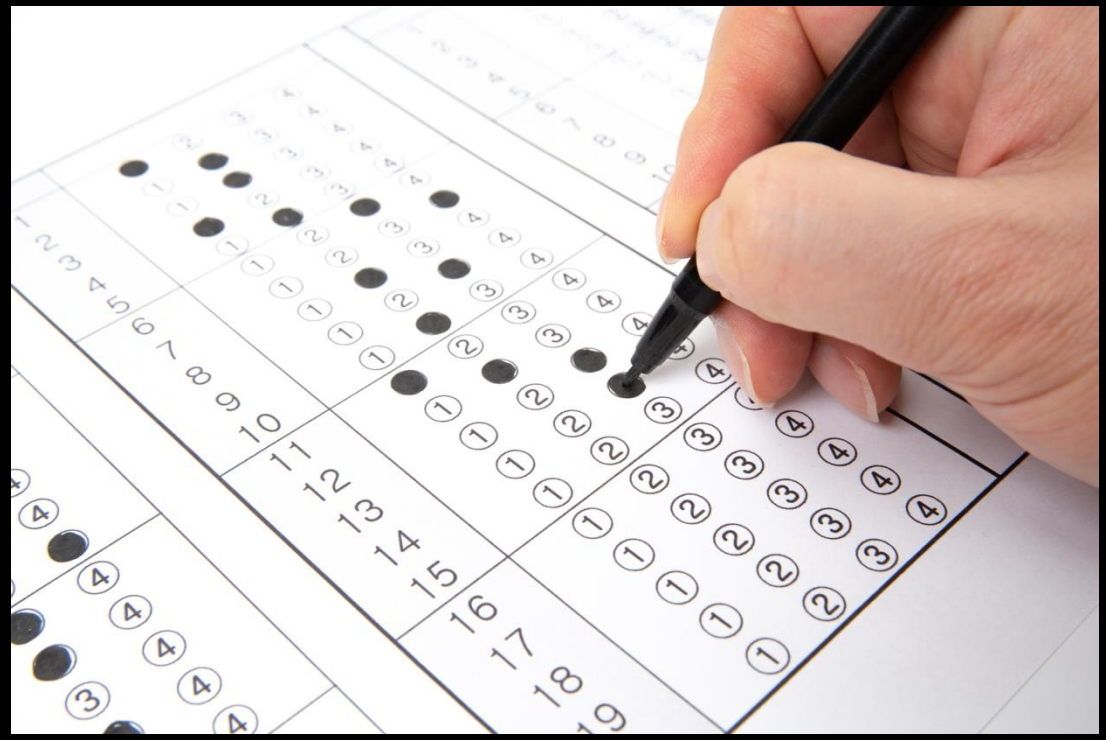
'We have not in recent memory sustained an incident of this scale or magnitude'

Emily Fitzpatrick, Natasha Riebe · CBC News · Posted: Jan 05, 2017 2:18 PM EST | Last Updated: January 6, 2017

More than 300 university computers and more than 2,000 passwords belonging to University of Alberta

Exam on laws and regulation

- Passing the exam is **required** to access the cyber labs
- Held next Thursday January 30 at 14.00-16.00
- Retake: February 7 10.00
- 15 multiple choice questions
  - 10 fully correct answers needed to pass



Preparing for the laws and regulation exam

- Go to the lecture on Tuesday January 28
- Read the material

Labs

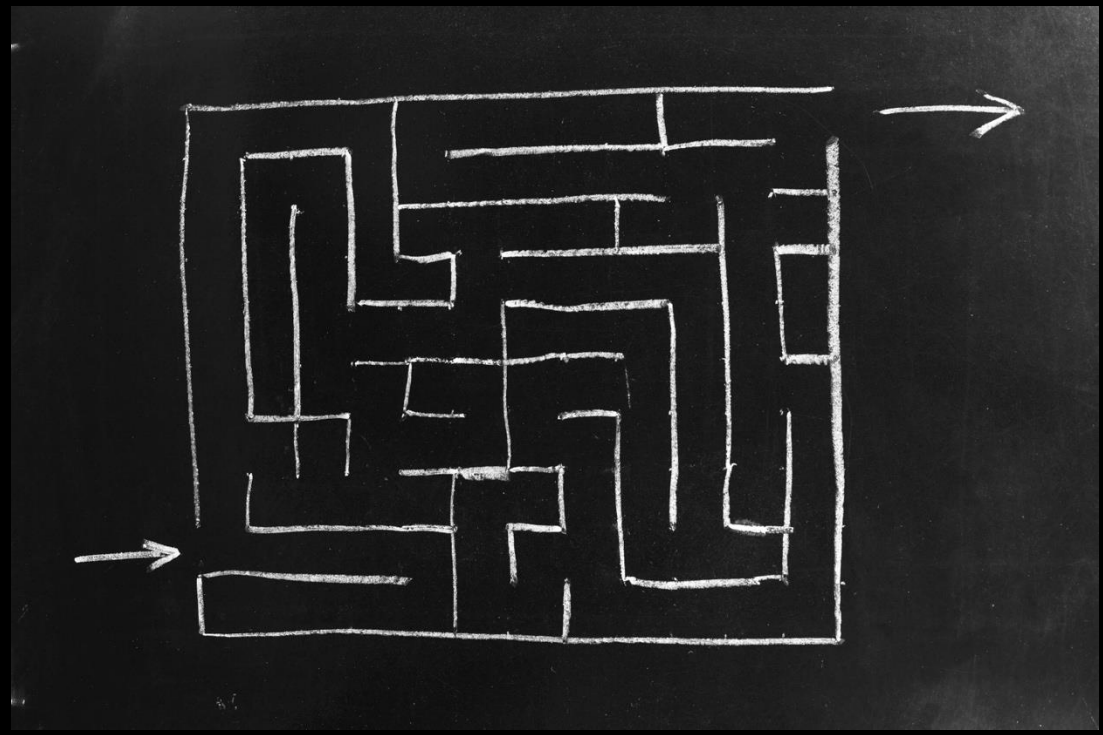
Capture the flag

- Work in pairs
- Your task is to find a set of flags
  - flag{febe1fe0f22d3b3f0b1982e880c5af5ac3e2af0b1514b8}
- Each flag gives 4-14 points
- Total number of points: 100


By Lydia Liu

How to find your way

- A penetration tester will not be told what vulnerabilities to find
- Similarly, we do not provide step-by-step instructions
- Plenty of resources available



Hints

- Available for all flags except the first
- Reduces the points
- Published at predefined times
- Full solution
  - On demand only
  - All points removed
  - Must still complete the flag

More info about the labs

- Lab preparatory lecture
  - January 29 10-12

- Web pages
  - https://www.ida.liu.se/~TDDE61/labs

Seminars

Should the police be allowed to hack the phones of suspected criminals?

Is it ok to do a port scan on a remote server?

What about reverse engineering a web service?

Seminar on ethics

- Discuss ethical questions related to penetration testing and ethical hacking
- 16 different groups, 6-7 students per group
- One 2h seminar per group
- 10-15 minutes per student

Steps for the seminar

1. Register in webreg. Deadline: 2025-02-03
2. Select a topic. Deadline: 5 days before the seminar
3. Write a 1-2 page reflection and upload it. Deadline: 3 days before the seminar
4. Read the other reflections. Deadline: 1 day before the seminar
5. Prepare a short opposition. Deadline: 1 day before the seminar
6. Attend the seminar, present your reflection, oppose on one reflection and engage in active discussions on the other topics

Topics

- The Stuxnet worm
- The EncroChat infiltration
- Usage of the Pegasus spyware
- The Snowden leak
- Bulletproof hosting like the one provided by the Cyberbunker
- Hacktivism activities such as the call for cyber operations against Russia in connection to the war against Ukraine
- Avoiding copyright infringement protection to keep video games from being shut down, e.g., the Pretendo project

Guest lectures

Guest lectures

- Purpose: To widen perspectives and get to know how it works in reality
- Typically 45mins
- After each lecture: Quiz
- At least five guest lectures
- More information will come

What happens next?

What happens next…

Date	Time	What	Who
Tuesday January 28	8-10	Lecture on laws and regulation	M. Asplund & D. Byers
Wednesday January 29	10-12	Lab preparation lecture	M. Asplund
Thursday January 30	14-16	Exam on laws and regulation	You…
Wednesday February 5	-	You will get access to the labs	Those who passed the exam
Wednesday February 5	10-12	Ethics lecture	M. Asplund
Feb 6 or Feb 7	-	First lab	Those who passed the exam
Friday February 7	10-12	Retake exam	Those to didn’t pass the exam