KARLSTAD UNIVERSITY

Final report

VT2026_DVAD25_49046_Etisk hackning

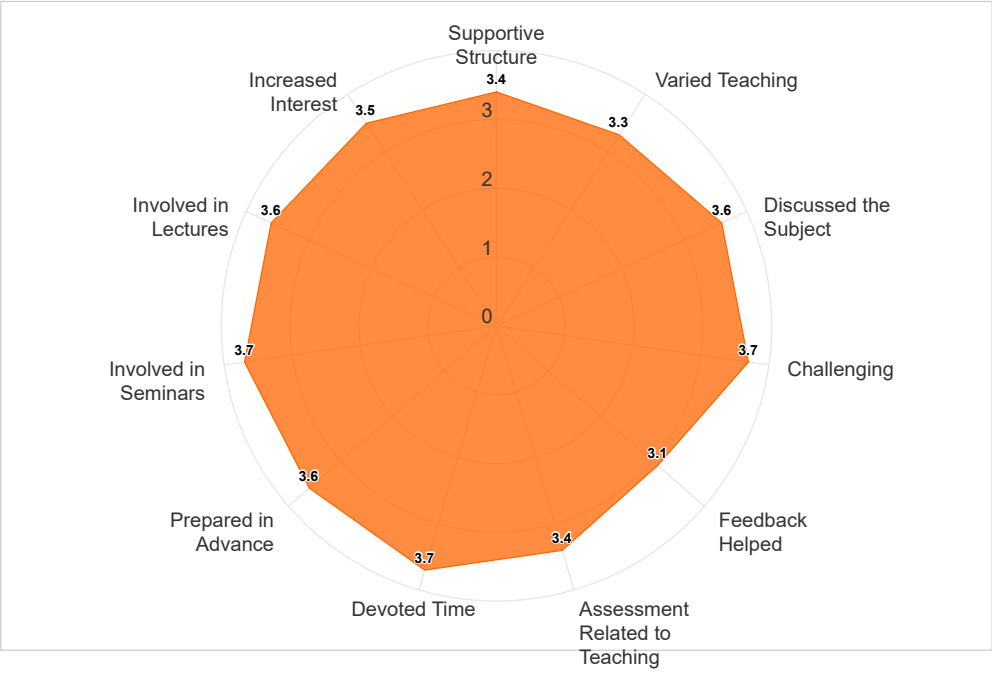
First time registred students: 69
Answer Count: 27
Answer Frequency: 39,13 %

The course evaluation could be answered during the period:

2026-03-23 - 2026-04-11

When collaborative courses, several course codes are shown below:

DVAD25 Etisk hackning, End date: 2026-03-29



KARLSTAD UNIVERSITY

Mean value for each question. Highest value = 4.

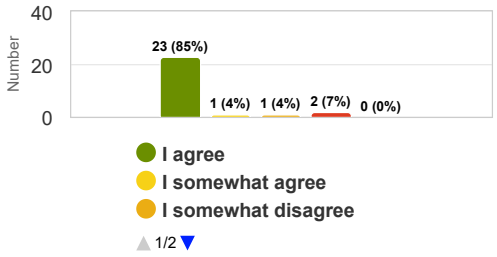
	Mean
Supportive Structure	3,4
Varied Teaching	3,3
Discussed the Subject	3,6
Challenging	3,7
Feedback Helped	3,1
Assessment Related to Teaching	3,4
Workload	2,0
Devoted Time	3,7
Prepared in Advance	3,6
Involved in Seminars	3,7
Involved in Lectures	3,6
Increased Interest	3,5

Results of learning

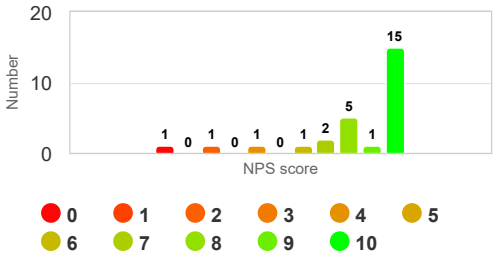
All in all, the course was valuable for me.

Courses that were considered valuable were related to personal development, acquisition of new knowledge and skills, understanding of something. Higher ratings can refer to students' perceived development (learned a lot, and it was useful). Lower ratings can refer to scanty development of knowledge and skills or not understanding certain themes or their parts, not understanding the necessity and significance of the course, problems in the learning environment.

	Mean
All in all, the course was valuable for me	4



How likely would you be to recommend this course to a friend or colleague?



Net Promoter Score (NPS) = 44,4

Promoters = 16 (59,3%)

Passives = 7 (25,9%)

Detractors = 4 (14,8%)

The Net Promoter Score (NPS) is a metric that measures student experience and predicts the effectiveness of a course. It calculates an NPS score based on a key question using a 0-10 scale, asking how likely students would recommend the course to others. Respondents are grouped into Promoters, Passives, or Detractors based on their score, and the NPS is calculated by subtracting the percentage of Detractors from the percentage of Promoters. The NPS is a core metric for course evaluation programs and is trusted by educational institutions to engage their students and improve their learning experience performance.

KARLSTAD UNIVERSITY

Course supervisor's comments

The feedback was mostly positive, despite the course's continued growth: 69 students registered for the first time, 67 were active, and 27 responded (39%), down from 62% in 2025. The number of active students has risen from 22 in 2024 and 36 in 2025. I was concerned that this scale would affect a course built around practical work and discussion, but the responses do not show a marked decline in quality. The cyber range worked very well and was more stable than in 2025. Only one manual intervention was needed to reset the containers, with negligible downtime.

In response to earlier requests for clearer solutions and more teaching during flag reports, I strengthened the flipped-classroom format: students investigated challenges before class, while the sessions spent more time on solutions, alternative approaches and discussion. Discussion of the subject scored 3.6 and involvement in seminars and practicals 3.7. Some students valued this approach; others still wanted more introductory teaching. Feedback helped scored 3.1, and some comments called for earlier feedback on reports.

I used students' Git/README reports during the discussions, and some of my working notes were initially shown accidentally. A few students found the display of identifiable work and notes uncomfortable, which is reflected in the course feedback. I understand this concern and see that this will no longer happen. Individual follow-up meetings with selected students took place only after all flags had been submitted, too late to offer much support during the course. The larger cohort also made the interval between the Sunday midnight submission deadline and Monday's 10:00 flag-report lecture unsustainable for reviewing reports.

The course updates were:

- a stronger flipped-classroom structure, connecting students' independent challenge work to more extensive teacher-led flag-report discussions.
- longer discussions of intended and alternative solutions, tools, vulnerabilities and common mistakes in the flag-report sessions.
- increased use of students' Git/README reports as examples for discussion, including an experiment with displaying my working notes. This practice needs to change as described below.
- individual follow-up meetings with selected students after all flags had been submitted.

Quoting the feedback of selected students:

- "This course had the perfect balance of gaining knowledge through the classes and through self-learning and researching to find the various solutions."
- "You really learned a lot from this course! Loved the practical part. The most fun class I've taken."
- "The course taught me a lot. Everything was well structured and organized. I liked that we had to do basically everything ourselves."

The Use of AI Tools:

The rules for using AI tools in DVAD25 were reformulated this year, and their use was limited. The policy was presented at the course opening and included in Canvas. It read:

"Dear all,
It is imperative to exercise caution when utilizing tools such as ChatGPT, Gemini, and Bing's CoPilot.
While these resources can provide valuable support, they should not replace the foundational skills of critical analysis and problem-solving, which are crucial in our field and a fundamental part of DVAD25. Dependence on artificial intelligence to understand complex concepts can undermine the development of independent thinking, which is necessary for a computer science professional. Be aware that AI tools do not always provide accurate or reliable information, and their responses may not always be correct.

Practical implications for DVAD25:
One of our goals is for you to learn how to reason as a security tester, and experimentation is a fundamental part of this process. Therefore, answers such as "I asked the AI bot, and it told me to do that" will not be accepted, and you risk losing points for the flags you captured by following instructions from AI chatbots.
You can use AI tools to learn more about attack tools, their uses, and limitations, as well as to assist with code. We may call you for an oral examination if we suspect AI tools were used beyond acceptable margins (e.g., to solve to challenge). To avoid any suspicion, remember to pay additional effort to your git repo reports.
You may use these tools (wisely) to assist your learning, but ensure they supplement rather than replace the academic effort required in your studies."

STUDENT FEEDBACK:

The comments below retain the students' wording, with minor typographical corrections. References to an unrelated named teacher/course and details of some exercises have been redacted.

Q. What enhanced your learning in this course?

- You really learned a lot from this course! Loved the practical part. The most fun class I've taken.
- The CTF style of it is super fun and engaging!
- The CyberRange is a really great opportunity to try and learn yourself!
- I had no previous experience in cyber security so this course taught me how to approach cybersecurity/hacking challenges. It also teaches you what tools can be used, and how you can use them.
- This course had the perfect balance of gaining knowledge through the classes and through self-learning and researching to find the various solutions. What enhanced my learning personally was the hints given to complete the various challenges, the tools and links provided to us through Canvas and personal research. With those, I could complete all of the challenges.
- Hands on experience, discussing different ways of solving the challenges during the flag reports, the good atmosphere in class created by Leo
- An envoriment where I could apply the theory I learned
- Having all materials present from the start, and the scoreboard, pushing me to try harder
- The course also provides a heavy list of links you can use to solve the solutions, but also dig deeper if you're interested in learning more.
- Hints
- Flag Reports
- the practiacle CTF, The utter fear of being placed on leo's shit list, memes.
- Leo! He is the best! <3
- leonardo, and google
- Mängder av timmar för att förstå sig på hur man löser utmaningarna mha google, artiklar. Medium var en bra webb plats för att djupa ner sig mer för att lösa uppgiften.
- it was mostly just self learnng, over the wire was not really that usefull to be honest but the usefull links on canvas was great, it allowed you to narrow down the scope for each flag and focus on learning the neccessary tools/concept.
- This being a fully practical course (except ethics) i had to learn everything myself from online resources.
- The way the course is structured, it's either learn what's necessary or fail.
- Unfotunately I wasn't able to learn anything through the course. Whatever, I learned was by doing everything myself. There were no proper theoretical lectures, where we got to learn the different concepts and tools related to the course.

KARLSTAD UNIVERSITY

Q. What would you do differently in the teaching of this course?

- Nothing that I can think of right now.
- Nothing really, think the course was ran great!
- Nothing.
- Really fun course, so I don't think there is any need to make any changes. Maybe offer the top students who completed all of the challenges in basically 24 hours some additional challenges? I wasn't one of them so you should maybe ask them :)
- Extra hard challenges for bragging/bonus points, more breadth in challenge types, maybe some signal/audio stuff or stego!
- Add more flags, not necessarily more servers but more flags like Lima, where you have a flag present on a server that you need to solve and not necessarily needing lateral movement.
- Wishlist would be forensics, cryptography and reverse engineering flags
- first of all i really liked the course i give it 5 out of 5. two thing i would change. first of the first week it would be nice to have two dependency path that are not realated to the same methods to solve it. so for example the alpha and bravo flag used dictonary attacks so if you for whatever reason got stuck here you did not have an altenative path. you are hard stuck. secound thing is I think the flag report was a missed oppertunity to learn alternativ solution. we mostly discussed the "attended way" of solve the flag. it would be nice to learn some of the alternative route the more experience student took (mostly the students from the hacking club). Because i assume you pretty much know almost all the ways to solve the flags so would be nice if it was covered more in detail.
- I whould tell the students that perform poorly their grade will not be the points but rather they will be entered in a CyberSecurity Death Math. where only 1 fourth passes and where the loser has to retake the course with a negative 100p
- Göra flag reports distans/ ändra flagg report momentet att inkludera en ny uppgift för hur Leonardo hade löst uppgiften. Inget med flaggorna utan bara ett mer momentet att få ut mer lärdom.
- Instead of providing a just a step-by-step overview/walkthrough at the cost of points, consider also organizing additional optional "lectures" where interested students can attend an have explained in person the solution, either by peers or teacher/TA. These sessions could go much more in details than what is possible during the flag reports with a full audience and helps also with learning the right mindset, especially to people that never touched this subject.
- Be more diverse when talking to students in class. It was very often the same prople that talked.
- Some more introduction in how CTFs work in the beginning would be great. Especially in the beginning I spent a lot of time trying very complex solutions. Then, I had to take a hint and the actual solution was quite simple.
- The only thing I'd change would be that before the challenges, some introductory lessons would be held, completing minor challenges together with the tutor and the class.
- Lectures that go thrugh the tools and how to use them, before the flags.
- I get the idea the student shuld learn on it's own, and in real life there wont be lectures on what tools to use and how to use them. But that statement can be applied to all studies (math, computer science, writing, fusics, electronics, etc)
- This is a course, I expect the professor / others to teach me...
- First of all, I would like to have proper lessons where the students properly learn the different concepts and tools, how they work, how everything is related, etc. Secondly, I would have given the students feedback on their work such as on their reports, rather than having the students give me multiple (approximately 15) reports, and not be satisfied with them and in the end fail them for something that could have been fixed after the first reports feedback.
- The course would benefit from including more structured teaching rather than focusing primarily on asking students to find flags. While the hands-on approach can be engaging, it assumes that all students already have a certain level of background knowledge. Without sufficient introductory teaching, it becomes difficult to keep up with the assignments and fully understand the objectives. The current format can feel overwhelming, especially when students are expected to complete tasks without first being given clear explanations or foundational concepts. Providing clear instruction, basic concepts, and guided examples before assigning tasks would make the course more accessible and effective. A better balance between teaching and practice would significantly improve the overall learning experience
- Actually teach how to hack before just giving the challenges, be more flexible/ supportive to students and won't show their personal notes in front of the whole class.
- Maybe not show everyones readme's without warning and not show your reviews of them. That is not how grading and reviews are typically done and people might feel uncomfortable with that. Especially given that this is a mandatory course so you have to do it even if you dont like it and then being ridiculed in class might lessen the inscentive to try to complete this course yourself without cheating with AI or stuff like that.
- Exclude the public shaming. Keep the bad notes to yourself and only showcase good solutions if any

---

Q. Recommendations for learning for future learners.

- Nah, awesome course though. Credits to the guys who made the cyber range and Leonardo who is a really great teacher. He understands the "vibe" so to speak :)
- This is the most fun course in the program.
- If you liked the topic, join KAUotic for more CTFs.
- DO NOT LEAVE STUFF FOR LAST MINUTE. While it definitely is possible to still pass the course leaving stuff for late into the week closer to deadlines, it severely hampers the learning imo.
- Get started on time! Don't postpone tasks.
- Start doing the Flags on mondays or tuesdays. Do not push it up until the end of the week because then you will stress and maybe lose simple points because you overlook simple stuff. Note everything you do because you might have to redo some work and it makes the final report writing so much easier.
- Start early, get familiar with the previous course if (time.exists()), don't end up on leo's shit list.
- Börja tidigt och skriv klart writeuppen så fort som möjligt
- lima is EZ, its fine to wait until the last moment to do it.
- Document every step, RTFMs, be creative with solutions, take your time studying tools/vulnerabilities/findings, don't overthink challenges (they are all text-book vulnerabilities) and start early each week. AI helps a little but more often than usual either refuses to help or sends you on wild goose chases, use it carefully and ALWAYS fact check it yourself.
- Don't think too complex. The actual solution is usually not too hard. You just need to find the right tool you need for the problem.
- Check the course useful links/materials.
- Metasploit is a really good tool which also have search function. Try to be ahead of the curve. The more pain you do early, the less pain you will have later on, where it might matter more. Also if Kilo and Lima are present, then you will probably need to dedicate more time to those flags, as they most likely will need it from you.
- Try picoCTF before getting access to the cyber range. It really helps getting to know Kali, tools and how to actually solve CTFs, but in a much more compact and less time consuming way. TryHackMe and HackTheBox are a bit more similar to the course itself, but also requires much more time, especially if you haven't tried CTFs before.
- Go thrugh the tool list and see what they recomend, just give everything to AI, and ask for maybe a 2-sentence answer for every tool. That will help you a lot!
- KEEP IN MIND!!! 99% of the course can be solved with tools, very few things require you to write your own tool/software, either use a tool or someone else already have the software for you!!!
- engage in high ethic and moral practices... like leo
- A lot of students might not have prior experience when it comes to developing various software based solutions and might not have stumbled upon how important it is to always prioritize security. Whatever kind of solution that a student ends up working on, security is something that is key. We might have students that end up working on networks, applications, software or websites. All of these can be vulnerable. What I personally noticed was that this course offers us a view onto all of these types of vulnerabilities, but also personal security such as the

importance of a secure password. It's hard to know what to protect against if you haven't had the chance to experience it yourself. This course gives you that chance by letting you experience how it is to be an attacker, so that you later can defend yourself against an external part. This is especially important in the time of artificial intelligence, where a lot of the time, you end up adding pieces and bits instead of coding the entire thing yourself. This can lead to a codebase with a lot of holes that attackers can use against you. This course is very important to future engineers, it doesn't hold your hand all the time and encourages you to find out a lot of the information yourself. But don't get discouraged, because the internet is constantly developing and attack patterns change. Instead of being discouraged, use it as a form of preparation against the unknown that you one day must defend yourself against.
- That be ready that all the load is on you, that in this course you will be both the teacher and student at the same time. And after going through this myself, I can say this with a 100% surety, that whatever time I spent on this course, the multiple hours, the slepless nights were all to waste. I was soo excited for this course throughout my years in this program, and was really looking forward, however it became one of worst course that I have had.

Q. Please explain your evaluation.

- The best course taken so far. Opened my horizons to something I never considered before.
- Awesome course! Fun and educational.
- As I've previously mentioned in my recommendation to future students, this course is one of the most exciting but also one of the most important courses I've taken to date. Having worked in the field as a developer of various sorts, the importance of being knowledgeable against attacks is key.
- The practical part in the course was very fun and all the hands on work really made me like the subject more.
- all of leonardos courses so far has been really good, fantastic teacher, don't let him leave, he is probably the only reason this course works as well as it does
- Cinema Absoluta
- best non-math course we've had so far.
- The course taught me a lot. Everything was well structured and organized. I liked that we had to do basically everything ourselves. The lectures with Leo were also very entertaining.
- You learn a lot and it's a fun way to learn.
- You cover meany tools and meany diferent aspects
- I loved the course - CTFs are closely related to these, so if you enjoy those, you will definitely find this course interesting. It also gives you a lot of information about the ethical aspects of hacking and vulnerabilities/exploits. My valuation is mainly based on what you learn from this course, and how you learn it. It's really different from learning something through just reading a book, compared with reading books/online sources as a complement to the practical work. In this course, you mainly read stuff to solve the challenges (practical work). You have an explicit reason why you're reading.
- Jag tycker att kursen har varit väldigt bra därför har jag gett den ett högt betyg. Men finns moment vilket kunde höja kursen. Ps den var redan bättre än XXX kurs
- The course was at times hard, but also really fun, anyone with a slight interest in cyber security will definitely come out even more interested upon the end of the course. Flag reports were good, but could possibly benefit with more students participating in the discussion.
- all in all, even though the stress of not finding flags made me lose hair at an alarming rate. the CTF is fun, the course is fun. and leo made the flag reports fun to attend by bringing up the memes people had in their git repos. in other words I think Leo does a very good job with this course, but plz consider the Cyber Death matches. This whould be very fun for me ☺☺☺
- The course as a whole was really enjoyable, though quite time consuming. I would highly recommend the course if it weren't for the public shaming during the flag reports which really was quite off-putting. The ethics part of the course was not relevant to the hacking assignments unfortunatly. Would have been fun to try to hack a machine as ethically as possible, as well as brute forcing your way in.
- I think I have explained enough.
- It was quite stressful given the time constraints, huge amount of challenges and self-learning required. It would have been much better if hacking concepts were all taught before having to do the challenges.

Q. Other opinions and comments about the course.

- 10/10 would take again
- Definitively worth. One of the better course at Uni for sure
- This was a really fun and challenging course. It was painful yes, but also very rewarding.
- Leo is kinda cool I guess
- Great course if you are interested in the topic and want to learn. You have to learn everything yourself and if someone does not have any interest in this subject that will be hard. Especially when there is no exam to rembember the answers for but instead practical.
- Lima was so much different that the rest of the challenges but still fun to solve (even if it made me loose my sanity for a week).
- Consider adding other themes like forensics or OSINT and (maybe optional, gives extra points) a windows machine to attack.
- The XXX machines are too easy to spot and ignore, they should be interactive and act as honeypots to throw you off in the solution.
- it whould be cool if the cyber range was available for longer.
- Rekommenderar att ändra lite på varje uppgift för att skapa variation och att slippa läckor för nästa år. Eventuellt ett extra moment för att testa kunskaperna man har lärt sig på plats i kau för att Leo ska lättare undersöka eleverna kunskap. Eller en liten tenta. Hade velat se en ny uppgift som involverade aningen behöver at nå en maskin från två eller 3 maskiner samtidigt vilket hade varit en utmaning. Eller en uppgift som kräver mer av verktyg som burpsuite eller något liknande vi gjorde i security 1 kursen. Bra kurs!
- Make it optional please.
- I learned a lot, but no thanks to the professors! I could just do hack the box...
- If I go a course I expect people to teach me!
- While the feedback regarding README quality is technically valuable, the delivery method is problematic. Publicly displaying personal notes to 'out' specific students for 'SUS' or poor work during class creates a negative learning environment. This feedback would be much more effective if delivered privately or anonymized to avoid public scrutiny of individual students. (This was written with the help of AI)
- I didn't like at all how the teacher outed a lot of people who had done a bad job. Notes on people's performance were shown to everyone in class, the teacher had written notes like "poor" and "wtf" by some of the reports.
- None, really disappointed.

SUMMARY AND NEXT STEPS:

The practical challenges and the more extensive flag-report discussions will remain central. I will continue discussing solutions, tools and alternative approaches, while considering where introductory examples would help students with less experience. I will also make room for students who do not usually speak in class, review the hints and their cost, and continue developing new exercises and better alignment between scenarios.

With 67 active students, the course needs a more sustainable review and support process. I will move the Monday flag-report lecture from 10:00 to 13:00 and consider adjusting the Sunday submission deadline. Lab supervisors will identify students who may need help earlier and arrange an initial meeting; unresolved concerns will be brought to me while there is still time for students to improve.

I will no longer display my assessment notes on individual reports. Student solutions can be discussed orally and anonymously; identifiable reports, including positive examples, will be shown only with prior permission. The cyber range worked reliably this year, and we will continue

developing its infrastructure, including features for student accountability.