Select what you will do for your Something Awesome project

- [ ] I've made a blog page about which topic I have chosen for my project
- [ ] I've discussed it with my tutor if I'm unsure
- [ ] I've posted a summary comment to my blog page in the comments below
- [ ] I've also posted the summary comment into my Logbook

Start Planning Your Project

Picking a Security Engineering Project

You can pick anything security related. What we look for in particular is:

- Your security engineering understanding and growth over the duration of the project
- Personal analysis and reflections that make your journey and/or resources unique
- **Analysis:** The level of depth you have explored in your chosen project.
- **Reflection:** How you document issues you encounter and how you overcame that adversity.
- **Technicality:** The level of technical depth to demonstrate security understanding. [Required if COMP6841]
- Progression of your project proposal
- Impressive elements of your project - what cool stuff did you do?!

Advice on picking a project:

- Something you are really passionate about and want to learn more about
- Ensure that **if you are doing COMP6841 - you have technical components** within your project (It should be focused on security rather than learning to code)
- If you're not sure if your project is security related, ask your facilitator! We can make almost anything related and you'll still learn the same things and build the same skillsets.
- **If there is something not in the list provided, that is great and it is something you should consider doing**

Project Topics

The possible topics for your Security Engineering Project are categorised into three:

- Teach Something
- Analyse Something
- Build Something

A. Teach something

- Produce either
  - an online activity or
  - a case study,

which effectively teaches a concept from one of the core topics of this course listed below.

As you will start the project in Week 1 you should either pick a topic covered in Week 1, a topic you already know about, or a topic you are interested in and are happy to engage in self directed research to learn on your own before we cover the content in the regular flow of the course.

As part of your project you should identify the nature of your intended student audience, and actually test it out on people and use your materials to teach them to get evidence that your activity or case study is effective.

Project	Description
Your guide to security - Workbook - Document - Podcasts - Infographics	Everyone learns in different ways, and the way that someone else might understand security may be different to how it is explained to them at first. Not to mention that security is a vast topic with so much information and it can be confusing to know where to start in the first place. In creating your guide to security, consider a target audience, whether they are someone who has no understanding of security or intermediate and explain to them security concepts or fundamentals. You are essentially making a resource for a target audience where you should also consider a media that works best for you, whether it is a workbook, document report, podcasts or infographics. Some examples of may include and are not limited to: • What are the principles of Engineering? Applying an Engineering approach to security. • Measuring Security: Bits of Information, Bits of Security, Brute forcing • Risk, assessing • Command and Control, power structures, separation of power, checks and balances • Normal Accidents, Safety Culture • Security By Design • Asymmetric Cryptography • Symmetric Cryptography • Integrity, Hashing • Authentication, Identity, Biometrics, Impersonation • Attacks on PKI, Attacks on DNS • Cryptographic Protocols: e.g. online elections A lot of possibilities available here, research and present topics which you are interested in!

B. Analyse something using a security engineering approach

Analyse a real-world security design, operation and/or assurance scenario and evaluate it and make recommendations.

For example you might want to perform a threat model on a system, vaccination certificates in Australia or internationally, how your organisation or an organisation you know about carries out some of its secure operations, a security design from history, or any real world scenario similar to the sorts of scenarios we study in the weekly case studies, you can also analyse some Malware, a cryptographic algorithm, your own opsec/privacy posture. You could try and reverse engineer something. Some more examples are listed below:

Project	Description
Risk Assessments in GRC	Governance, Risk and Compliance is a key area many organisations are required to understand and invest towards such that they are operating with an understanding of risk. In doing this project, you will gain an understanding of the importance of risk, how it is measured and recommendations which are able to be provided across different organisations. The different frameworks are able to be explored and analysed for their efficiency and role.
Cryptography Research	Securing communication between parties through cryptography is diverse and as time has progressed, is increasingly complex. Consider researching into the wide range of cryptography methods and presenting your research and analysis in this field. If you are planning to solely research cryptography, you are expected to provide a great amount of

	depth on this single topic.
Consulting on a company providing security recommendations	Many consultancies provide security recommendations to ensure a stronger security posture in an organisation. Consider replicating this on a small or large currently operating organisation. Perform research to understand the security landscape they operate in. Cases may be hypothetical and assumptions are able to be made where information is not provided. Possibilities include and are not limited to providing a security posture analysis, recommendations and budgeting advice.
Analysing security in cinema	Security is depicted within a variety of movies, television shows, or short videos. Consider analysing security within these videos and providing a thorough analysis of its portrayal. How and what you choose to analyse is completely your choice and there should be no limitation, though there is an expectation of depth rather than summative of "what happened", as you provide your analysis and reflection of what you have identified.

C. Create something to demonstrate a concept or to help carry out an analysis

Code or build something which relates to A (teaching a course topic) or B (a tool to help carry out an analysis) above.

For example, you could build a working replica of an Enigma machine which could be used to demonstrate to students how the machine worked and/or could be cracked, or a password brute forcer, or a hardware device or cluster which can economically carry out a large number of computations. You could also build a steganographic tool, a rootkit, build your own CTF challenges, build something to do with NFC/RFID technology like scanning or cloning. Some more project ideas are listed below:

Technical Projects

Project	Description
NFC & RFID cards	The world of communication is evolving and how the technologies are used within society. Despite this, they also come with a variety of security vulnerabilities as they are used within society which you should explore. Students are required to go into technical depth by providing examples or proofs of concept to fulfil technical requirements. **Ethics:** Do not interact with any NFC / RFID card you do not have permission to test. This includes the university ID card - do not touch it!
Security in network layers	Networks are a significant part of how computers communicate with each other. These are usually done through a variety of layers within the OSI model which are also susceptible to a variety of security vulnerabilities. Within this project students, consider elaborating on networks and what vulnerabilities may exist within them. Students are required to go into technical depth by providing examples of these vulnerabilities or proofs-of-concept to fulfil technical requirements. **Ethics:** Only perform tooling on networks to which you can consent, or set up your own infrastructure.
Major recent vulnerabilities	Vulnerabilities, security mistakes that result in business impact, exist everywhere. Some are more notable than others or more well-known due to the scale of impact they have. The most common and recent vulnerability which was really impactful for a large number of companies was Log4j. There are many major security incidents out there and can include and not limited to Heartbleed, EternalBlue, and Log4j. Students are required to go into technical depth by providing examples of these vulnerabilities or code analysis or proofs-of-concept to fulfil technical requirements.
OWASP Top 10	The Open Web Application Security Project (OWASP) Top 10 is an awareness document to showcase the most critical web application-related security vulnerabilities which exist. Consider going into a large amount of technical depth on each of these areas, elaborate the significance of each, impact as well as techniques attackers would use using proofs-of-concept or examples to demonstrate what these vulnerabilities are and how they exist.
	There are so many games out there and individuals have constantly searched for ways to cheat in

Game Hacking	order to gain personal advantages. You should focus on a game that is older rather than newer. **Games like Valorant / League of Legends should be avoided** where older anti-viruses (if any) are much easier to overcome rather than those of newer games. Example: Wallhacks for CSGO amongst other features **Ethics:** Cheats performed should be done in a private lobby rather than in public servers in no way to harm other players' experiences.

Creating CTF Challenges	A CTF, or Capture the Flag, can be thought of as a cyber scavenger hunt. Here, individuals are rewarded flags for successfully completing tasks through points. Here, we are referring to Jeopardy-styled challenges where you are provided with a variety of challenges ranging from a multitude of topics each with a given amount of points. The harder challenges would typically be worth more points, and it's the team with the highest amount of points by the end of the CTF wins. Instead of completing these challenges, in this project you will be creating challenges from topics in which are interested, some of these include:
	
	• Web Application Security
	  ◦ SQL Injection
	  ◦ Cross-Site Scripting
	  ◦ Server-Side Request Forgery (SSRF)
	  ◦ Authentication vulnerabilities
	• Cryptography
	• Binary Exploitation
	• Reverse Engineering
	• Forensics
	• OSINT
	
	A lot of potential avenues to improve upon, there are a lot of different things you are able to do. In this project, document your methodology and mindset, what you tried and how you overcome challenges. For each challenge that you create, also create unique personalised writeups for each challenge, as well as other challenges which would be similar to it in the future to show your depth of understanding in the topic area. Analyse how you have made challenges harder and the defence mechanisms you have placed to increase difficulty.

Develop tooling (Red or Blue teaming)	All security teams need tooling and in a few instances there is a need for automation given the large number of assets an organisation may have and the need to check for vulnerabilities within all of them. There are a variety of tools that you are able to make, not limited to: • DIY WIFI Pineapple • Keylogger • Rubber Ducky • Fuzzer • Subdomain takeover tool • Rootkit (Difficult but rewarding - consult with your tutor for scope) We care a lot behind your security understanding and concepts behind your application utilises rather than your ability to code or debug code which we will not be marking. We will look, not only at the impressiveness of your project but also your understanding of the application of the tool, the problem it solves and deep technical analysis of it. For instance, in a keylogger what methodologies are able to be taken to hide it? Strong analysis and thorough personal reflections will strengthen your final project deliverable. Due to the popularity of these projects, a general idea of the HD of the following projects would include: • Keylogger - (HD requires hiding or discovery, and different types/implementations of keyloggers) • Rubber Ducky - (HD is based on payloads and what creative/impactful things you can do) • Fuzzer - (HD needs to implement AFL algorithms) **Ethics:** Offensive tooling must only be used on assets that you own or have consent to test.
End-to-End encryption chat	Communication between two or more parties is able to be listened to if there is a lack of encryption within the medium. In order to prevent this, applications implement end-to-end encryption methodologies which are used in order to ensure the security and privacy of all messages which are sent. In this project, develop an end-to-end encryption chat and provide thorough analysis and documentation to support how the application is safe to use and communicates with the other party successfully. We care a lot about your security understanding

	and concepts on the CIA triad (Confidentiality, Integrity, Availability) behind the strategy your application utilises rather than your ability to code or debug code which we will not be marking. Provide analysis and strong reflection on your understanding of these methods and possible attack vectors which have been considered and may still be successful or have been prevented.
OverTheWire	OverTheWire is a wargames platform to help learn and practice security concepts. Some wargames include Bandit, Leviathan, Natas, Krypton, Narnia and Behemoth. A description of each is listed below: • Bandit - absolute basics like linux commands - **this is not suggested and will not be marked for Something Awesome Projects** • Leviathan - focused around reverse engineering, so using tools such as GDB and strace/ltrace • Natas - basics of server-side web security wargames • Krypton - cryptography wargames • Narnia - a lot of regular vulnerabilities found, source codes provided • Behemoth - a lot of regular vulnerabilities found, source codes not provided In this project, document your methodology and mindset, what you tried and how they overcome challenges. Create unique personalised writeups for each challenge, as well as other challenges which would be similar to it in the future. Provide summaries of what you have learnt and the processes which were taken even though they may lead to rabbit holes. You are not expected to do all of them.
HackTheBox	HackTheBox is a platform to help learn and practice security concepts. There are a variety of machines that exist on the platform which would test your penetration testing skills. This is more advanced than OverTheWire and dives in a more intense rate and is recommended for individuals who are not beginners to penetration testing, but still wish to do a wargame-like something awesome project. There is a greater range of machines available, but you will have to pay in order to gain access to retired boxes. In this project, document your methodology and mindset, what you tried and how you overcome challenges. Create unique personalised writeups for each challenge, as well as other challenges which would be similar to it in the future. Provide summaries of what you have learnt and the processes which were taken even though they may lead to rabbit holes.
Attack/Defence CTF **(Very Difficult)**	In Attack-Defense your team has to defend their own servers against attacks as well as attack other team's servers to score points. Again, you will be looking for flags that will be automatically generated for every tick (depends on the CTF you are playing - in some events, ticks are 5 minutes, it may be more for others). Here, you are trying to create exploits to send to other teams and automate them to send them out to other teams as quickly as you can. Now, in the event you may see that other teams are getting flags from you (oh no)... so your system is vulnerable! Then, you would have to try to patch the vulnerability to stop other teams from using the same script against you. In this project delve into the knowledge and fundamentals of either Attack/Defence or both. An avenue is to consider how infrastructure is usually set up and do that yourself first before then going into the strategies used by both red and blue teamers. **Ethics:** Attacking methodologies should remain on assets that you own and have consent to test on.

Project Proposal Template

The project proposal is how the course will judge the progress of your own project. Illustrated below is a template that you should use in your Week 1 project update blog.

Project Goal:	*[What do you want to do?]*
	[What do you hope to accomplish? Clearly state the

Project Description (more depth):		*technical component if COMP6841]*	
Project Schedule	**Week 1**	*[What will you do in Week 1?]*	
	Week 2	*[What will you do in Week 2?]*	***Note:** Project Proposal Due Wednesday 9 am [With Week 1 Logbook]*
	Week 3	*[What will you do in Week 3?]*	
	Week 4	*[What will you do in Week 4?]*	
	Week 5	*[What will you do in Week 5?]*	***Note:** Mid-Term Progress* Video Due Wednesday 9 am [Week 4 Activity]
	Week 6	*-- Flexibility Week --*	
	Week 7	*[What will you do in Week 7?]*	
	Week 8	*[What will you do in Week 8?]*	***Note:** Final Report Deliverable Due Friday*
Project Deliverables/Outcomes:	*[What will the outcome and deliverables from your project?]*		

Additional Information

Use of ChatGPT	For this assessment task, you may use standard editing and referencing software, but NOT GENERATIVE AI. The use of generative AI such as ChatGPT is strictly prohibited in this assessment. You cannot use ChatGPT or any related generative AI tool to complete any of the weekly activities. If the use of generative AI is detected, it will be regarded as serious academic misconduct and subject to the standard penalties, which may include 00FL, suspension and exclusion.
Feedback	Your facilitator will give you feedback on your project update along with the feedback on your logbooks.

Back
Case Study 2 Prep: Drill

Next
Week 1 Reflection