Disclaimer

This document provides a list of courses and resources for training purposes. Some of these resources are available for free or have a complimentary tier, while others require payment. We wish to emphasize that *we receive no sponsorship or endorsement* for promoting any of the items listed. Many of us have personally explored some of these resources for our own learning, but it's important to note that there's no obligation to purchase any of them. Consider this compilation as a knowledge repository of available options that we deem noteworthy.

Please be aware that this document was last updated in September 2023, so the pricing or tiers of some resources might have changed since. We aim to periodically review, refresh, and expand the content to keep it relevant.

If you've experienced any resources that aren't mentioned here and find them interesting or have any queries, please don't hesitate to reach out to us at **mentoring@women4cyber.dk**.

TryHackMe

Link: https://tryhackme.com/

Cost:

- free tier provides access to a significant amount of content and is sufficient to get started.
- VIP access to full content - Monthly: 12£/ month or Yearly 9£/ month
- https://tryhackme.com/why-subscribe

Beginner-friendly approach: TryHackMe is designed with beginners in mind. It offers a gradual learning curve, starting with easy challenges and gradually increasing the difficulty level. The platform provides a structured learning path, making it easier for newcomers to grasp fundamental concepts and build their skills step by step.

Hands-on learning: TryHackMe focuses on practical, hands-on learning rather than just theory. It provides virtual environments where you can practice real-world hacking techniques and apply security concepts. By actively engaging in tasks and challenges, you gain practical experience that enhances your understanding and skill development.

Wide range of topics: TryHackMe covers a broad spectrum of security-related topics, including penetration testing, network security, web application security, cryptography, and more. This diversity allows you to explore different areas of interest within the security field and find your niche.

Structured learning paths: Structured learning paths that guide you through different topics and skill levels. These paths help you navigate the learning materials efficiently, ensuring that you progress in a logical and structured manner. Whether you are a beginner or an experienced professional, you can find suitable learning paths to enhance your skills.

Interactive learning experience: The platform offers an interactive and gamified learning experience. You can participate in Capture The Flag (CTF) challenges, solve puzzles, complete tasks,

and collaborate with other learners through forums and chat rooms. This interactive approach keeps the learning process engaging and enjoyable.

Community and support: TryHackMe has a vibrant and supportive community of learners, including experienced professionals and fellow beginners. You can interact with others, ask questions, share knowledge, and learn from their experiences. The community provides a valuable support network and can help you overcome challenges and expand your knowledge.

HackTheBox

Link: https://www.hackthebox.com/

Cost:

- Free access to basic content.
- VIP 14$/month,
- VIP+ 20$/month
- https://www.hackthebox.com/hacker/pricing

Real-world simulations: HTB provides realistic virtual environments that simulate real-world scenarios and systems. These labs mimic various networks, machines, and vulnerabilities encountered in the field. By working on HTB machines, you gain practical experience and develop skills that directly apply to real-world security challenges.

Range of challenges: HTB offers a wide range of challenges, including both active and retired machines. These challenges cover different areas of security, such as web application security, network security, reverse engineering, cryptography, and more. The platform continually adds new challenges, ensuring that you can explore different domains and stay updated with emerging threats.

Active community and rankings: HTB has an active community of security enthusiasts, including professionals and beginners. You can collaborate, share knowledge, and learn from others through forums, chat rooms, and user profiles. Additionally, HTB provides a ranking system that allows you to track your progress, compare your skills with others, and even compete in Capture The Flag (CTF) events.

Practical learning and problem-solving: HTB emphasizes practical learning and problem-solving. Each machine presents a unique puzzle that requires you to perform reconnaissance, exploit vulnerabilities, escalate privileges, and secure the compromised system. By working on these challenges, you develop critical thinking, analytical skills, and a deep understanding of security concepts.

Networking and career opportunities: HTB can serve as a networking platform, connecting you with like-minded individuals, experienced professionals, and potential employers.

HackTheBox Academy

Link: https://www.hackthebox.com/

Cost:

- Free access to basic content.
- Student – 8$/month (For students and professors of universities and other academic institutions.)
- Silver Annual – 490$/year
- Silver – 18$/month (Get started in cyber)
- Gold – 38$/month (Advanced in cyber)
- Platinum – 68$/month (Master in cyber)
- https://help.hackthebox.com/en/articles/5720974-academy-subscriptions

Comprehensive learning materials: HackTheBox Academy offers a wide range of comprehensive learning materials, including video courses, tutorials, and documentation. These resources cover various security topics, such as penetration testing, web application security, network security, exploit development, and more. The materials are designed to provide in-depth knowledge and practical skills, helping you develop a strong foundation in different areas of security.

Practical hands-on approach: HackTheBox Academy emphasizes a hands-on learning approach. The courses and tutorials often involve practical exercises and labs that allow you to apply the concepts and techniques you learn. This interactive learning experience enhances your understanding and proficiency in real-world security scenarios.

Structured learning paths: HackTheBox Academy provides structured learning paths that guide you through different topics and skill levels. These paths help you navigate the learning materials efficiently, ensuring that you progress in a logical and structured manner. Whether you are a beginner or an experienced professional, you can find suitable learning paths to enhance your skills.

Integration with HackTheBox platform: HackTheBox Academy is integrated with the HackTheBox platform, which allows you to apply your knowledge and skills directly on practical challenges and machines. You can practice what you learn in the courses by solving challenges, working on machines, and participating in Capture The Flag (CTF) events.

Collaboration and community: HackTheBox Academy fosters a collaborative learning environment. You can engage with the community, discuss course topics, share knowledge, and seek help through forums and chat rooms. Collaborating with others and learning from their experiences can deepen your understanding and broaden your perspectives.

Offensive Security Proving grounds

Link: https://www.offsec.com/labs/

Cost:

- Play – Free (time limited to 3h a day)
- Practice: 19$/month or 199$/year
- https://www.offsec.com/labs/individual/

Realistic and challenging environments: The Proving Grounds provide realistic and challenging virtual environments for hands-on practice. These environments simulate real-world networks, systems, and applications, allowing you to experience and solve actual security scenarios. The challenges are designed to test your skills and push you to think creatively and critically.

Practical application of skills: The Proving Grounds focus on practical application rather than theory. You get to use the tools, techniques, and methodologies you learn in Offensive Security courses, such as the Penetration Testing with Kali Linux (PWK) and Advanced Web Attacks and Exploitation (AWAE). This hands-on approach allows you to refine your skills and gain practical experience in a controlled environment.

Feedback and guidance: As you work on challenges in the Proving Grounds, you receive feedback and guidance from the Offensive Security team. They provide insights, tips, and recommendations to help you improve your techniques and methodologies. This feedback helps you learn from experienced professionals and enhances your understanding of offensive security concepts.

Collaboration and community: The Proving Grounds foster collaboration and community interaction. You can join discussions, share knowledge, and learn from other security professionals in the Offensive Security forums. Engaging with the community allows you to exchange ideas, gain different perspectives, and expand your network.

Exam preparation: The Proving Grounds can be an excellent resource for preparing for Offensive Security certifications, such as the Offensive Security Certified Professional (OSCP) and Offensive Security Web Expert (OSWE) exams. The challenges and scenarios in the Proving Grounds align with the exam objectives, providing a valuable opportunity to practice and refine your skills before taking the certification exams.

PortSwigger Academy

Link: https://portswigger.net/web-security

Cost: Free

Focus on web application security: PortSwigger Academy specializes in web application security, providing comprehensive training and resources in this specific domain. It covers a wide range of topics, including web vulnerabilities, exploitation techniques, secure coding practices, and defensive measures.

Integration with Burp Suite: PortSwigger Academy is closely integrated with Burp Suite, a widely used web application testing tool. The platform offers hands-on exercises and labs that utilize Burp Suite for various security tasks.

Practical and interactive learning: PortSwigger Academy adopts a practical and interactive learning approach. The training materials include interactive labs, exercises, and challenges that allow you to apply the concepts and techniques in a simulated environment. This hands-on experience helps you develop real-world skills and strengthens your understanding of web application security.

Structured learning paths: PortSwigger Academy provides structured learning paths suitable for beginners, intermediate learners, and advanced practitioners. The learning paths guide you through a logical progression of topics, ensuring a well-rounded understanding of web security.

Educational resources and documentation: PortSwigger Academy offers comprehensive educational resources and documentation. These include tutorials, articles, cheat sheets, and videos that cover various aspects of web application security. These resources provide in-depth explanations, practical examples, and guidance to help you deepen your knowledge and overcome challenges.

APIsec University

Link: https://www.apisecuniversity.com/#courses

Cost: Free

This hands-on course provides detailed workshops on API hacking techniques and how to uncover vulnerabilities and logic flaws in APIs.

Immersivelabs

Link: https://cybermillion.immersivelabs.online/

Cost: Free

Hands-on, gamified learning: Immersive Labs provides a hands-on, gamified learning experience. It offers interactive labs and challenges that allow you to actively engage with real-world security scenarios.

Comprehensive content library: Immersive Labs has a comprehensive content library covering a wide range of security topics. From beginner to advanced levels, it offers modules and labs on subjects such as penetration testing, incident response, malware analysis, secure coding, and more.

Learning pathways and assessment: Immersive Labs provides structured learning pathways and assessments. It guides you through progressive modules, ensuring a logical and comprehensive learning experience. The assessments help you gauge your understanding and progress, allowing you to identify areas that need further improvement.

Skill validation and certification: Immersive Labs offers skill validation and certification options. By completing labs and challenges, you can earn digital badges and certificates that demonstrate your proficiency in specific security areas. These credentials can enhance your resume and credibility in the job market.

ISACA

Link: https://www.isaca.org/

Cost:

- Student - 25$

- Recent graduate - 68$
- Professional - 145$
- https://www.isaca.org/membership/become-a-member#grad

About ISACA: ISACA, the Information Systems Audit and Control Association, is a globally recognized organization that focuses on advancing knowledge and expertise in the fields of information technology governance, risk management, and cybersecurity.

ISACA Certification and Training: ISACA offers a range of globally recognized certifications, including the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified in Risk and Information Systems Control (CRISC). ISACA provides training and study materials to help professionals prepare for their certification exams.

Expertise and Research: ISACA is known for its extensive research and publications in the field of IT governance, risk management, and cybersecurity. Members have access to a wealth of resources, including research reports, whitepapers, and case studies.

Networking Opportunities: ISACA hosts conferences, seminars, and events around the world, offering members the chance to connect with peers, industry experts, and thought leaders. These networking opportunities can be invaluable for career growth and knowledge sharing.

Online Learning: ISACA offers a variety of online courses and webinars, making it convenient for members to continue their education and stay up-to-date with industry trends.

Professional Development: ISACA is committed to the professional development of its members. It provides resources for career advancement, mentorship programs, and job boards to help members find new opportunities in the field.

Community Support: ISACA has a thriving community of professionals who are passionate about IT governance, risk management, and cybersecurity. Members can engage in discussions, share insights, and seek advice from their peers.

Local Chapters: ISACA has local chapters in many regions, allowing members to participate in local events and activities, further enhancing their networking and learning experiences.

SANS

Link: https://www.sans.org/emea/

Cost: Some materials are for free

The SANS Institute is a globally renowned organization that specializes in cybersecurity education, training, and certification. SANS Institute ***primarily offers paid*** training and certification programs, and their courses are well-known for their high quality and expertise. However, SANS ***does provide some free resources and offerings*** to the cybersecurity community.

Here are some of the free resources and offerings provided by SANS - more can be found here https://www.sans.org/security-resources/?msc=main-nav

1. **Webinars:** SANS occasionally hosts free webinars on various cybersecurity topics. These webinars feature industry experts and provide insights into current threats, trends, and best practices.
2. **Reading Room:** SANS has a Reading Room on their website that offers a collection of whitepapers, research papers, and articles on cybersecurity topics. Many of these resources are available for free and cover a wide range of subjects.
3. **Cybersecurity Blog:** SANS maintains a cybersecurity blog where they publish articles, analysis, and commentary on cybersecurity issues. While not all content may be free, they often provide informative posts accessible to the public.
4. **Newsletters:** SANS offers several newsletters, such as "NewsBites," which provide cybersecurity news and insights. Some of these newsletters are available for free subscription.
5. **GIAC Advisory Board (GAB) Certification Papers:** The GIAC Advisory Board provides free certification papers on various cybersecurity topics. These papers can help professionals prepare for GIAC certifications.
6. **Security Awareness Resources:** SANS provides some free resources related to security awareness and training. These materials can be helpful for organizations looking to improve their employees' cybersecurity awareness.
7. **Cybersecurity Challenges:** SANS occasionally hosts cybersecurity challenges and competitions that are open to the public. These challenges can be an excellent way to test and enhance your cybersecurity skills.

EC-Council

Link: https://www.eccouncil.org/train-certify/certified-cybersecurity-technician-certification/

Cost: It is a partial scholarship, covering costs for e-courseware, practical hands-on labs, challenges and activities. Participants need to pay 199$ for certification and technology fee.

The **Certified Cybersecurity Technician** (CCT) certification aimes to equip individuals with the fundamental knowledge and skills needed to pursue a career in cybersecurity. It is intended for beginners or those with limited cybersecurity experience.

ISC2

Link: https://www.isc2.org/Landing/1MCC

Cost: Free training. Upon completing exam -$50 Annual Maintenance Fee.

$(ISC)^2$ is a globally recognized organization that offers various cybersecurity certifications, and it is dedicated to advancing the field of information security and promoting best practices in the industry. Their certifications cover a wide range of cybersecurity domains, and CISSP is one of the most well-known certifications within their portfolio.

If you register as candidate you will gain access to Online Self-Paced Training and voucher for free certification exam.