

RECAP LAPORAN TRYHACKME

NAMA: DHYDAN DARWAN ROMMADHONA

KELAS: 3A

NIM: 2231740032

1. Cari dan masuk ke laman web tryhackme



2. Kemuan register atau login dengan mengisikan username,email, dan password atau Bisa langsung register dengan menggunakan akun google


Sign Up

Join over 4 million users and upskill in cyber security.

Username



Email Address

Password

☐ I'm not a robot  reCAPTCHA Privacy - Terms

Sign Up

Or

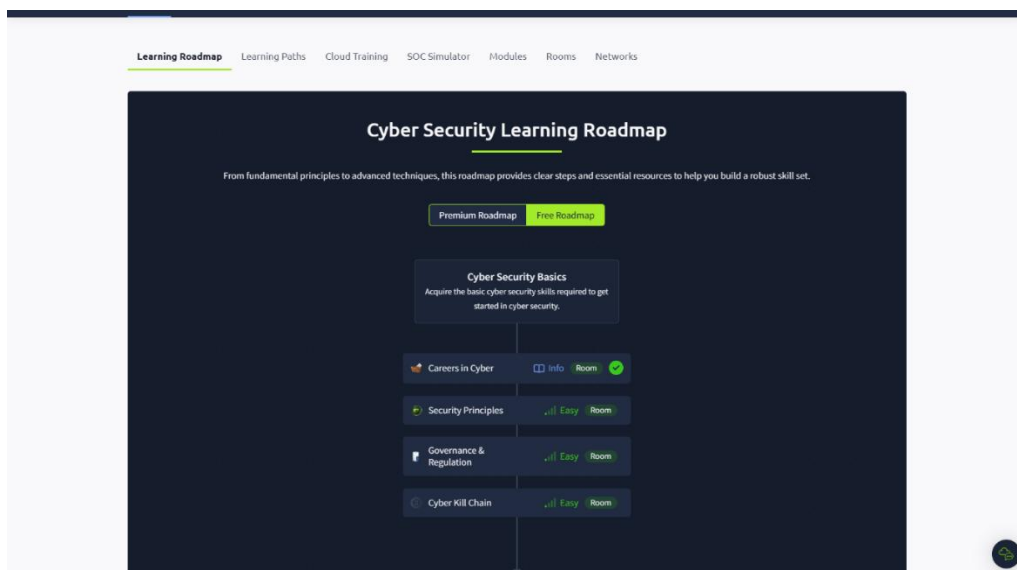
 Continue with Google  Continue with SSO

By signing up, you are agreeing to our [Terms and Conditions](#). Already have an account? [Log in](#).

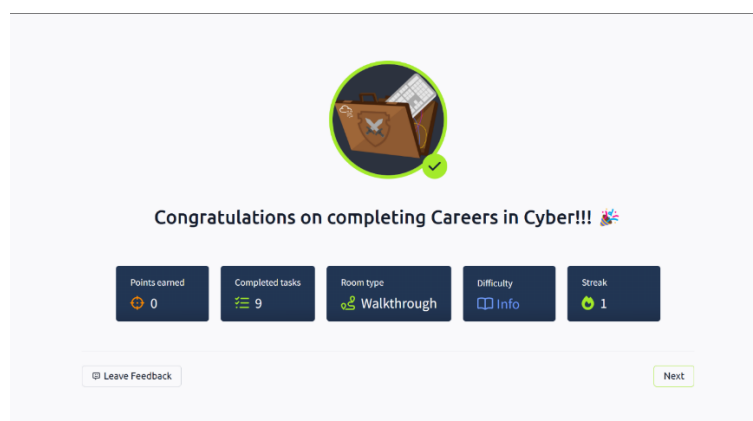
3. Ketika sudah masuk laman dashboard web tryhack pergi kelaman learn



4. Lalu scroll kebawah dan pilih roadmap pembelajaran yang free,dan klik salah satu icon pembeajaran dibawah untuk mempelajari topik-topik ilmu terkait



5. Kerjakan soal-soal dan quiz nya hingga muncul ucapan selamat dan di laman learn awal tadi muncul centang hijau pada topik persoalan yang di kerjakan tadi



6. Pilih topik selanjut nya yang mau dikerjakan

The screenshot shows the TryHackMe interface for the 'Cyber Kill Chain' room. The top navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other'. The room title 'Cyber Kill Chain' is prominently displayed, along with a description: 'The Cyber Kill Chain framework is designed for identification and prevention of the network intrusions. You will learn what the adversaries need to do in order to achieve their goals.' The room is rated 'Easy' and takes '45 min'. A progress bar at the bottom indicates 'Room progress (0%)'. The main content area shows a diagram of the Cyber Kill Chain framework with icons for Reconnaissance, Weaponisation, Exploitation, and Command & Control, connected by arrows. The 'Task 1 Introduction' tab is active.

7. Kerjakan soal-soal nya hingga semau page soal menjadi hijau

The screenshot shows the content of the 'Cyber Kill Chain' room. The top navigation bar includes 'Dashboard', 'Learn', 'Compete', and 'Other'. The room title 'Cyber Kill Chain' is prominently displayed, along with a description: 'The Cyber Kill Chain framework is designed for identification and prevention of the network intrusions. You will learn what the adversaries need to do in order to achieve their goals.' The room is rated 'Easy' and takes '45 min'. A progress bar at the bottom indicates 'Room progress (41%)'. The main content area features a diagram of the Cyber Kill Chain framework with icons for Reconnaissance, Weaponisation, Exploitation, and Command & Control, connected by arrows. The 'Task 1 Introduction' tab is active. The text describes the process of gaining access to a system through phishing emails and exploiting vulnerabilities. It mentions 'Megatron' who created two phishing emails, one with a fake Office 365 login page and another with a macro attachment that would execute ransomware. It also discusses 'lateral movement' and 'zero-day exploits'. The text concludes with a list of examples of how an attacker carries out exploitation: 'The victim triggers the exploit by opening the email attachment or clicking on a malicious link.', 'Using a zero-day exploit.', 'Exploit software, hardware, or even human vulnerabilities.', and 'An attacker triggers the exploit for server-based vulnerabilities.'

Answer the questions below

Can you provide the name for a cyberattack targeting a software vulnerability that is unknown to the antivirus or software vendors?

Submit

Room progress (46%)

The law applies to all business entities that conduct business in the European Union (EU) and collect/store/process the personal data of EU residents and are required to comply. It is one of the most stringent data privacy regulations worldwide and safeguards personal data during collection. Companies can only collect personal data for a legitimate reason and must inform the owner about its processing. Moreover, this also includes penalties and fines based on non-compliance in the following two tiers:

- Tier 1:** More severe violations, including unintended data collection, sharing data with third parties without consent, etc. Maximum penalty amounting to 4% of the organisation's revenue or 20 million euros (whichever is higher).
- Tier 2:** Less severe violations, including data breach notifications, cyber policies, etc. The maximum fine for Tier 2 is 2% of the organisation's revenue or 10 million euros (whichever is higher).

Payment Card Industry Data Security Standard (PCI DSS)
 PCI DSS is focused on maintaining secure card transactions and protecting against data theft and fraud. It is widely used by businesses, primarily online, for card-based transactions. It was established by major credit card brands (Visa, MasterCard & American Express). It requires strict control access to cardholder information and monitoring unauthorised access, using recommended measures such as web application firewalls and encryption. You can learn more about the standard [here](#).

Answer the questions below

What is the maximum fine for Tier 1 users as per GDPR (in terms of percentage)?

Woop woopl! Your answer is correct

Congratulations on completing Cyber Kill Chain !!! 🎉

Points earned 🏆 80	Completed tasks ✅ 10	Room type 👤 Walkthrough	Difficulty 📊 Easy	Streak 🔥 1
-----------------------	-------------------------	----------------------------	----------------------	---------------

[Leave Feedback](#) [Next](#)

Learning Roadmap

Cyber Security Learning Roadmap

From fundamental principles to advanced techniques, this roadmap provides clear steps and essential resources to help you build a robust skill set.

Premium Roadmap Free Roadmap

Cyber Security Basics
 Acquire the basic cyber security skills required to get started in cyber security.

- Careers in Cyber [Info](#) [Room](#) [✔](#)
- Security Principles [Easy](#) [Room](#)
- Governance & Regulation [Easy](#) [Room](#) [🔒](#)
- Cyber Kill Chains [Easy](#) [Room](#) [✔](#)

Fundamental skills
 Acquire the fundamental skills needed to enter any career in the industry.

8. Kerjakan semua soal hingga mendapat ucapan dan pada laman learn terdapat centang untuk topik yang di kerjakan tadi

TryHackMe

Dashboard

Learn

Compete


Other

Go Premium

1

D

Learn > Governance & Regulation



Governance & Regulation

Explore policies and frameworks vital for regulating cyber security in an organisation.

🟢 Easy ⌚ 120 min

Help

Save Room

👤 1730

⚙️ Options

Room progress (66%)

Task 1

🟢 Introduction

▼

Task 2

🟢 Why is it important?

▼

Task 3

🟢 Information Security Frameworks

▼

Task 4

🟢 Governance Risk and Compliance (GRC)

▼

Task 5

🟢 Privacy and Data Protection

▼

Task 6

🔴 NIST Special Publications

▲

NIST 800-53

NIST 800-53 is a publication titled **"Security and Privacy Controls for Information Systems and Organisations"**, developed by the National Institute of Standards and Technology (NIST), US, that provides a catalogue of security controls to protect the CIA triad of information systems. The publication serves as a framework for organisations to assess and enhance the security and privacy of their information systems and comply with various laws, regulations, and policies. It incorporates best practices from multiple sources, including industry standards, guidelines, and international frameworks.

Key Points

NIST 800-53 offers a comprehensive set of security and privacy controls that organisations can use to safeguard their operations, assets, personnel, and other organisations from various threats and risks. These include intentional attacks, unintentional errors, natural disasters, infrastructure failures, foreign intelligence activity, and privacy concerns. NIST 800-53 Revision 5 organises security controls into twenty families, each addressing a specific security concern category. You can learn more about the controls [here](#) (Section 2.2).

🟢 Woop woop! Your answer is correct

Congratulations on completing Governance & Regulation!!! 🎉

Points earned
🔥 112

Completed tasks
📋 8

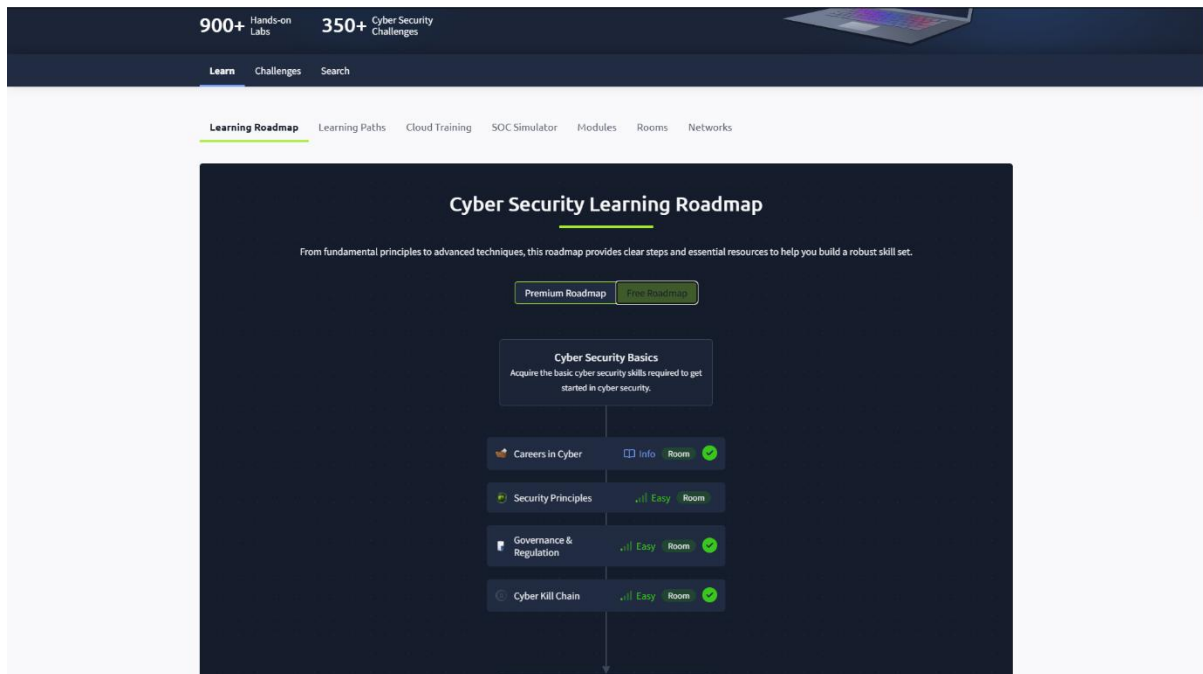
Room type
👤 Walkthrough

Difficulty
🟢 Easy

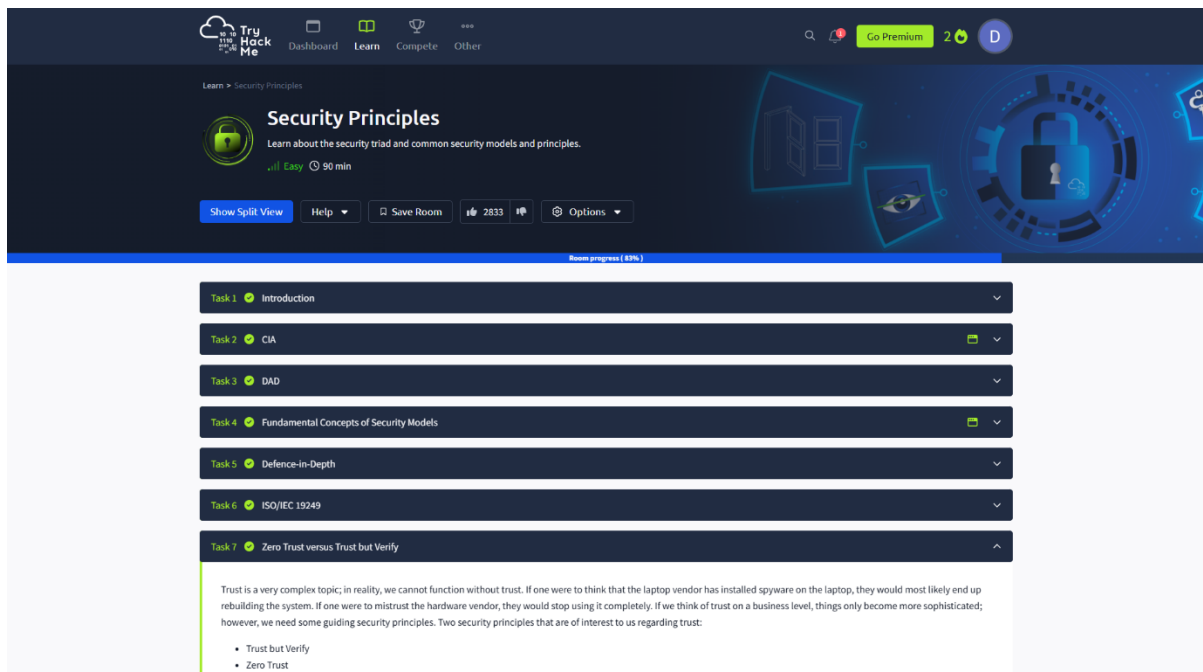
Streak
🔥 1

📝 Leave Feedback

Next

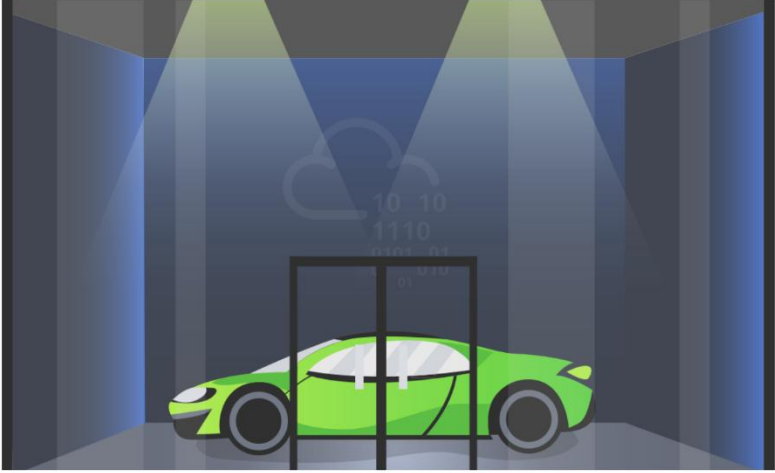


9. Kerjakan topik lain sehingga pada laman topik yang di kerjakan tadi muncul centang pada laman learn



Room progress (83%)

Task 8 Threat versus Risk




There are three terms that we need to take note of to avoid any confusion.

- **Vulnerability:** Vulnerable means susceptible to attack or damage. In information security, a vulnerability is a weakness.
- **Threat:** A threat is a potential danger associated with this weakness or vulnerability.
- **Risk:** The risk is concerned with the likelihood of a threat actor exploiting a vulnerability and the consequent impact on the business.

Away from information systems, a showroom with doors and windows made of standard glass suffers a weakness, or *vulnerability*, due to the nature of glass. Consequently, there is a *threat* that the glass doors and windows can be broken. The showroom owners should contemplate the *risk*, i.e. the likelihood that a glass door or window gets broken and the resulting

Woop woop! Your answer is correct



Congratulations on completing Security Principles!!! 🎉

Points earned56

Completed tasks9

Room typeWalkthrough

DifficultyEasy

Streak2

Leave Feedback

Next

10. Pastikan semua topik di learning roadmap ini sudah tecentang semua

Dashboard

Learn

Compete

Other

Learn

Experience our FREE, interactive cyber security learning path, designed for all skill levels. With hands-on exercises based on real-world scenarios—from hacking machines to investigating attacks—you can learn about cyber security and enhance your skills anytime, anywhere, all accessible through your browser.

900+

Hands-on Labs

350+

Cyber Security Challenges

TryHackMe

Get Premium

2

D

Learn

Challenges

Search

Learning Roadmap

Learning Paths

Cloud Training

SOC Simulator

Modules

Rooms

Networks

Cyber Security Learning Roadmap

From fundamental principles to advanced techniques, this roadmap provides clear steps and essential resources to help you build a robust skill set.

Premium Roadmap

Free Roadmap

Cyber Security Basics

Acquire the basic cyber security skills required to get started in cyber security.

Careers in Cyber

Info

Room

✓

Security Principles

✓

Easy

Room

✓

Governance & Regulation

✓

Easy

Room

✓

Cyber Kill Chain

✓

Easy

Room

✓