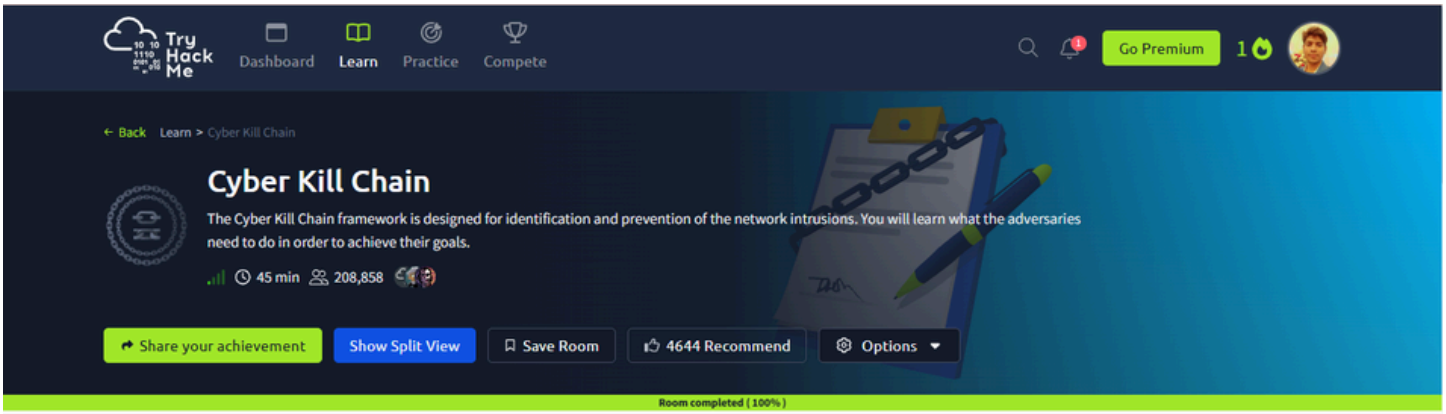
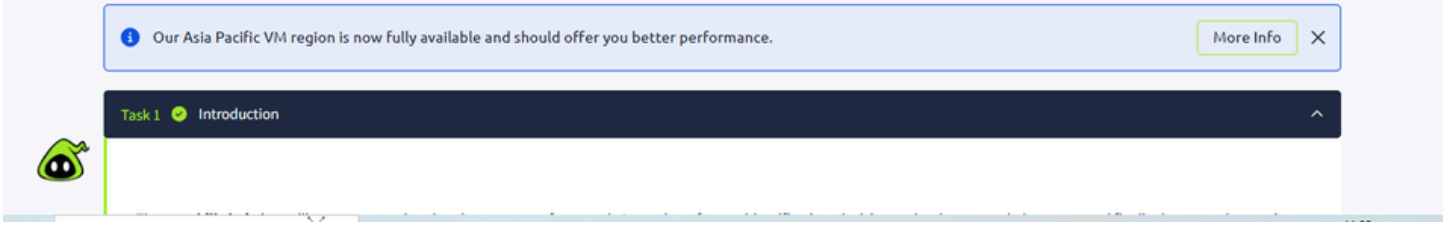




Task 1 Introduction

The term **kill chain** is a military concept related to the structure of an attack. It consists of target identification, decision and order to attack the target, and finally the target destruction.

Thanks to Lockheed Martin, a global security and aerospace company, that established the Cyber Kill Chain® framework for the cybersecurity industry in 2011 based on the military concept. The framework defines the steps used by adversaries or malicious actors in cyberspace. To succeed, an adversary needs to go through all phases of the Kill Chain. We will go through the attack phases and help you better understand adversaries and their techniques used in the attack to defend yourself.

So, why is it important to understand how Cyber Kill Chain works?

The Cyber Kill Chain will help you understand and protect against ransomware attacks, security breaches as well as Advanced Persistent Threats (APTs). You can use the Cyber Kill Chain to assess your network and system security by identifying missing security controls and closing certain security gaps based on your company's infrastructure.

By understanding the Kill Chain as a SOC Analyst, Security Researcher, Threat Hunter, or Incident Responder, you will be able to recognize the intrusion attempts and understand the intruder's goals and objectives.

We will be exploring the following attack phases in this room:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

Learning Objectives

In this room, you will learn about each phase of the Cyber Kill Chain Framework, the advantages and disadvantages of the traditional Cyber Kill Chain.

Outcome
As a result, you will be ready to recognize different phases or stages of the attack carried out by an adversary and be able to break the "kill chain."

Answer the questions below

Read the above.

No answer needed

✓ Correct Answer

Task 2 Reconnaissance

Reconnaissance is the research and planning phase of an attack against a system or victim. Adversaries use this phase to gather information about their target to inform their next steps. This information can include infrastructure details, employee data, business processes, and exposed technologies. Reconnaissance is often passive and undetected.

Poor recon typically leads to sloppy attacks, while well informed adversaries can create highly targeted, believable payloads that increase their chances of success.

A valuable piece of recon is **OSINT** (Open-Source Intelligence). With OSINT, adversaries gather insights about their target through publicly available information. Some public sources where OSINT data can be collected from include:

- Search engines
- Print and online media
- Social media accounts
- Online forums and blogs
- Online public record databases
- WHOIS and technical data

Reconnaissance Types

- **Passive Recon:** This involves having no direct interaction with the target. This may include WHOIS lookups, social media scraping, or reviewing breach data.
- **Active Recon:** This involves direct contact with the target with activities such as social engineering, port scanning, banner grabbing, or probing for open services.

Let's look at it from the attacker's perspective, who initially doesn't know what company he wants to attack.

A malicious attacker who names himself "Megatron" decides to conduct a very sophisticated attack that he has been planning out for years; he has been studying and researching different tools and techniques that could help him get to the last phase of the Cyber Kill Chain. But first, he needs to start from the Reconnaissance phase.

In order to operate in this phase, the attacker would need to conduct OSINT. Let's have a look at Email harvesting.

Email harvesting is the process of obtaining email addresses from public, paid, or free services. An attacker can use email-address harvesting for a phishing attack (a type of social-engineering attack used to steal sensitive data, including login credentials and credit card numbers). The attacker will have a big arsenal of tools available for reconnaissance purposes. Here are some of them:

- theHarvester: other than gathering emails, this tool is also capable of gathering names, subdomains, IPs, and URLs using multiple public data sources.
- Hunter.io: this is an email hunting tool that will let you obtain contact information associated with the domain.
- OSINT Framework: OSINT Framework provides the collection of OSINT tools based on various categories.

Answer the questions below

What is the name of the Intel Gathering Tool that is a web-based interface to the common tools and resources for open-source intelligence?

OSINT Framework ✓ Correct Answer

Answer the questions below

What is the name of the Intel Gathering Tool that is a web-based interface to the common tools and resources for open-source intelligence?

OSINT Framework ✓ Correct Answer

What is the definition for the email gathering process during the stage of reconnaissance?

email harvesting ✓ Correct Answer

Task 3 Weaponization

After a successful reconnaissance stage, "Megatron" would work on turning the raw information into actionable attack tools through crafting **malware** and **exploits** into a **payload**. Most attackers usually use automated tools to generate the malware or refer to the DarkWeb to purchase the malware. More sophisticated actors or nation-sponsored APT (Advanced Persistent Threat Groups) would write their custom malware to make the malware sample unique and evade detection on the target.

Before we proceed, let's define some key terminology.

Malware is a program or software that is designed to damage, disrupt, or gain unauthorized access to a computer.

Exploits are programs or code that take advantage of the vulnerability or flaw in the application or system.

A **payload** is a malicious code that the attacker runs on the system.

Continuing with our scenario, "Megatron" chooses to buy an already written payload from someone else in the DarkWeb, so that he can spend more time on the other phases.

In the Weaponization phase, the attacker can adopt the following tactics:

After a successful reconnaissance stage, "Megatron" would work on turning the raw information into actionable attack tools through crafting **malware** and **exploits** into a **payload**. Most attackers usually use automated tools to generate the malware or refer to the DarkWeb to purchase the malware. More sophisticated actors or nation-sponsored APT (Advanced Persistent Threat Groups) would write their custom malware to make the malware sample unique and evade detection on the target.

Before we proceed, let's define some key terminology.

Malware is a program or software that is designed to damage, disrupt, or gain unauthorized access to a computer.

Exploits are programs or code that take advantage of the vulnerability or flaw in the application or system.

A **payload** is a malicious code that the attacker runs on the system.

Continuing with our scenario, "Megatron" chooses to buy an already written payload from someone else in the DarkWeb, so that he can spend more time on the other phases.

In the Weaponization phase, the attacker can adopt the following tactics:

- Create an infected Microsoft Office document containing a malicious macros or VBA (Visual Basic for Applications) scripts.
- Create a malicious payload or a very sophisticated worm, implant it on USB drives, and then distribute them in public.
- Set up Command and Control (C2) infrastructure for executing the commands on the victim's machine or deliver more payloads.
- Infect the victim's host with a backdoor, which would provide a way to access the computer system, and bypass the security mechanisms.
- Tailoring phishing templates or OAuth-consent apps to look legitimate and dupe the victim.

Answer the questions below

What is the term for automated scripts embedded in Microsoft Office documents that can be used to perform tasks or exploited by attackers for malicious purposes?

Macro

✓ Correct Answer

Task 4 Delivery

Delivery is when Megatron decides to choose the method for transmitting the payload or the malware onto the target environment. There are plenty of options to choose from:

- Phishing email: after conducting the reconnaissance and determining the targets for the attack, the malicious actor could craft a malicious email that would target either a specific person (spear phishing attack) or multiple people in the company. The email would contain a malicious link or email attachment that would result into a compromise.
- USB drops offer the attacker a physical delivery medium into public places like coffee shops, car parks, or on the street. An attacker might decide to conduct a sophisticated USB Drop Attack by printing the company's logo on the USB drives and mailing them to the company while pretending to be a customer sending the USB devices as a gift.
- Watering hole attacks are targeted and designed to aim at a specific group of people by compromising the website they are usually visiting, redirecting them to a malicious website of the attacker's choice or creation. Victims would unintentionally download malware or a malicious application to their computer, resulting in a drive-by download. An example can be a malicious pop-up asking to download a fake Browser extension.

Answer the questions below

Answer the questions below

What do you call an attack targeting a specific group by infecting their frequently visited website?

Watering hole attack ✓ Correct Answer

Task 5 Exploitation

Exploitation is the moment the attacker's code executes on the target, taking advantage of a known vulnerability. In this phase, Megatron can opt to utilise a number of key techniques to gain access:

- Malicious macro execution: This may have been delivered through a phishing email, that would execute ransomware when the victim opens it.
- Zero-day exploits: These leverages on unknown and unpatched flaws in a system. These exploits leave no opportunity for detection at the beginning.
- Known CVEs: The attacker can choose to exploit unpatched public vulnerabilities found on the target environment.

After gaining access to the system, the malicious actor could exploit software, system, or server-based vulnerabilities to escalate the privileges or move laterally through the network.

Signs of exploitation to look out for include:

- Unexpected process spawns.
- Registry changes or new services created.
- Suspicious command-line arguments found in system logs.

Signs of exploitation to look out for include:

- Unexpected process spawns.
- Registry changes or new services created.
- Suspicious command-line arguments found in system logs.

Answer the questions below

What is the term for a cyber attack that exploits a software vulnerability that is unknown by software vendors?

Zero-day

✓ Correct Answer

Task 6 Installation

As you have learned from the Weaponization phase, the backdoor lets an attacker bypass security measures and hide the access. A backdoor is also known as an access point.

Once the attacker gets access to the system, he would want to reconnect back to the system if he loses the connection to it or if he got detected and got the initial access removed. Or if the system is later patched, they will no longer have access to it. That is when the attacker needs to install a **persistent backdoor.** A persistent backdoor will let the attacker access the system he compromised in the past. You can check out the Windows Persistence Room to learn how an attacker can achieve persistence on Windows.

The persistence can be achieved through:

- Installing a **web shell** on the webserver. A web shell is a malicious script written in web development programming languages such as ASP, PHP, or JSP used by an attacker to maintain access to the compromised system. Because of the web shell simplicity and file formatting (.php, .asp, .aspx, .jsp, etc.) can be difficult to detect and might be classified as benign. You may check out this great article released by Microsoft on various web shell attacks.
- Installing a backdoor on the victim's machine. For example, the attacker can use Meterpreter to install a backdoor on the victim's machine. Meterpreter is a Metasploit Framework payload that gives an interactive shell from which an attacker can interact with the victim's machine remotely and execute the malicious code.
- Creating or modifying Windows services. This technique is known as T1543.003 on MITRE ATT&CK (MITRE ATT&CK® is a knowledge base of adversary tactics and techniques based

As you have learned from the Weaponization phase, the backdoor lets an attacker bypass security measures and hide the access. A backdoor is also known as an access point.

Once the attacker gets access to the system, he would want to reconnect back to the system if he loses the connection to it or if he got detected and got the initial access removed. Or if the system is later patched, they will no longer have access to it. That is when the attacker needs to install a **persistent backdoor.** A persistent backdoor will let the attacker access the system he compromised in the past. You can check out the Windows Persistence Room to learn how an attacker can achieve persistence on Windows.

The persistence can be achieved through:

- Installing a **web shell** on the webserver. A web shell is a malicious script written in web development programming languages such as ASP, PHP, or JSP used by an attacker to maintain access to the compromised system. Because of the web shell simplicity and file formatting (.php, .asp, .aspx, .jsp, etc.) can be difficult to detect and might be classified as benign. You may check out this great article released by Microsoft on various web shell attacks.
- Installing a backdoor on the victim's machine. For example, the attacker can use Meterpreter to install a backdoor on the victim's machine. Meterpreter is a Metasploit Framework payload that gives an interactive shell from which an attacker can interact with the victim's machine remotely and execute the malicious code.
- Creating or modifying Windows services. This technique is known as T1543.003 on MITRE ATT&CK (MITRE ATT&CK® is a knowledge base of adversary tactics and techniques based on real-world scenarios). An attacker can create or modify the Windows services to execute the malicious scripts or payloads regularly as a part of the persistence. An attacker can use the tools like **ssc.exe** (sc.exe lets you Create, Start, Stop, Query, or Delete any Windows Service) and Reg to modify service configurations. The attacker can also **masquerade** the malicious payload by using a service name that is known to be related to the Operating System or legitimate software.
- Adding the entry to the "run keys" for the malicious payload in the Registry or the Startup Folder. By doing that, the payload will execute each time the user logs in to the computer. According to MITRE ATT&CK, there is a startup folder location for individual user accounts and a system-wide startup folder that will be checked no matter what user account logs in.

You can read more about the Registry Run Keys / Startup Folder persistence on one of the MITRE ATT&CK techniques.

In this phase, the attacker can also use the **Timestomping** technique to avoid detection by the forensic investigator and also to make the malware appear as a part of a legitimate program. The timestomping technique lets an attacker modify the file's timestamps, including to modify, access, create and change times.

Answer the questions below

What technique is used to modify file time attributes to hide new or changes to existing files?

Timestomping ✓ Correct Answer

What malicious script can be planted by an attacker on the web server to maintain access to the compromised system and enables the web server to be accessed remotely?

Web shell ✓ Correct Answer

Task 7 Command & Control

After getting persistence and executing the malware on the victim's machine, Megatron opens up the C2 (Command and Control) channel through the malware to remotely control and manipulate the victim. This term is also known as **C&C or C2 Beaconing** as a type of malicious communication between a C&C server and malware on the infected host. The infected host will consistently communicate with the C2 server; that is also where the beaconing term came from.

The compromised endpoint would communicate with an external server set up by an attacker to establish a command & control channel. After establishing the connection, the attacker has full control of the victim's machine. Until recently, IRC (Internet Relay Chat) was the traditional C2 channel used by attackers. This is no longer the case, as modern security solutions can easily detect malicious IRC traffic.

The most common C2 channels used by adversaries include:

- HTTP on port 80 and HTTPS on port 443, where this type of beaconing blends the malicious traffic with the legitimate traffic and can help the attacker evade firewalls.
- DNS (Domain Name Server), where the infected machine makes constant DNS requests to the DNS server that belongs to an attacker, this type of C2 communication is also known as DNS Tunneling

Important to note that an adversary or another compromised host can be the owner of the C2 infrastructure.

Answer the questions below

What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker.

DNS Tunneling ✓ Correct Answer

Task 8 Actions on Objectives (Exfiltration)

After going through six phases of the attack, Megatron can finally achieve his goals, which means taking action on the original objectives. With hands-on keyboard access, the attacker can achieve the following:

- Collect the credentials from users.
- Perform privilege escalation (gaining elevated access like domain administrator access from a workstation by exploiting the misconfiguration).
- Internal reconnaissance (for example, an attacker gets to interact with internal software to find its vulnerabilities).
- Lateral movement through the company's environment.
- Collect and exfiltrate sensitive data.
- Deleting the backups and shadow copies. Shadow Copy is a Microsoft technology that can create backup copies, snapshots of computer files, or volumes.
- Overwrite or corrupt data.

Answer the questions below

Answer the questions below

What technology is included in Microsoft Windows that can create backup copies or snapshots of files or volumes on the computer, even when they are in use?

Shadow Copy ✓ Correct Answer

Task 9 Practice Analysis

View Site

We really hope you enjoyed this room. In order to strengthen your knowledge, let's do a practice analysis.

Here is the real-world scenario for you to tackle:

The infamous Target cyber-attack, which led to one of the largest data breaches in history took place on November 27, 2013.

On December 19th, 2013, Target released a statement confirming the breach, stating that approximately 40 million credit and debit card accounts were impacted between Nov. 27 and Dec. 15, 2013. Target had to pay the fine of $18.5 million under the terms of the multistate settlement agreement. This is considered to be the largest data-breach settlement in history.

How did the data breach happen? **Deploy the static site** attached to this task and apply your skills to **build the Cyber Kill Chain of this scenario**. Here are some tips to help you complete the practical:

1. Add each item on the list in the correct Kill Chain entry-form on the Static Site Lab:

- exploit public-facing application

Room completed (100%)

Task 9 Practice Analysis

View Site

We really hope you enjoyed this room. In order to strengthen your knowledge, let's do a practice analysis.

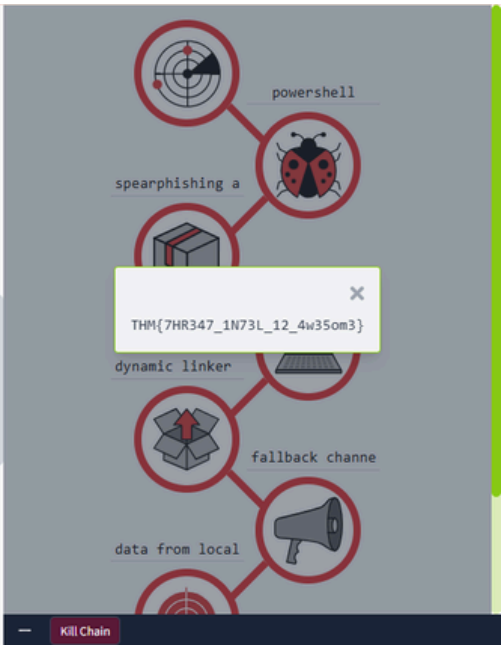
Here is the real-world scenario for you to tackle:

The infamous Target cyber-attack, which led to one of the largest data breaches in history took place on November 27, 2013.

On December 19th, 2013, Target released a statement confirming the breach, stating that approximately 40 million credit and debit card accounts were impacted between Nov. 27 and Dec. 15, 2013. Target had to pay the fine of $18.5 million under the terms of the multistate settlement agreement. This is considered to be the largest data-breach settlement in history.

How did the data breach happen? **Deploy the static site** attached to this task and apply your skills to **build the Cyber Kill Chain of [illegible]enario**. Here are some tips to help you complete the practical:

1. Add each item on the list in the correct Kill Chain entry-form on the Static Site Lab:



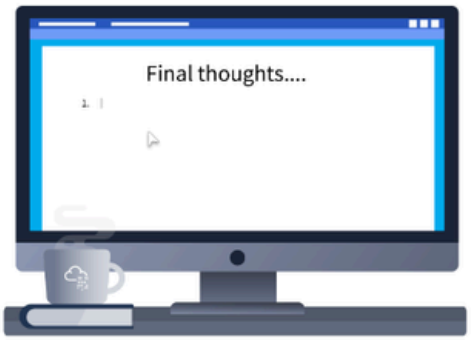
Answer the questions below

What is the flag after you complete the static site?

THM{7HR347_1N73L_12_4w35om3}

✓ Correct Answer

Task 10 Conclusion

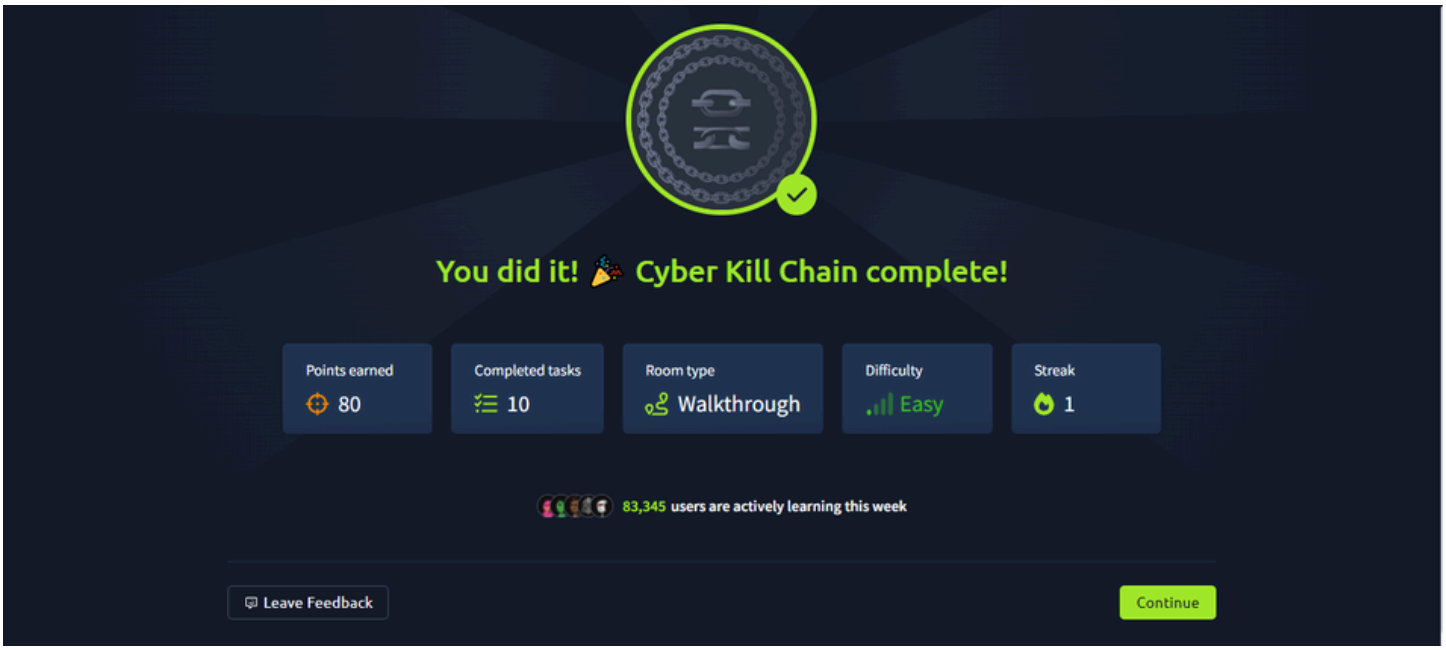


Cyber Kill Chain can be a great tool to improve network defence. Is it perfect and can it be the only tool to rely on? No.

The traditional Cyber Kill Chain or Lockheed Martin Cyber Kill Chain was last modified in 2011, which, if you remember, is the date of its establishment. The absence of updates and modifications creates security gaps.

The traditional Cyber Kill Chain was designed to secure the network perimeter and protect against malware threats. But the cybersecurity threats have developed drastically nowadays, and adversaries are combining multiple TTP (tactics, techniques, and procedures) to achieve their goal. Adversaries are capable of defeating threat intelligence by modifying the file hashes and IP addresses. Security solutions companies are developing technologies like AI (Artificial Intelligence) and different algorithms to detect even slight and suspicious changes.

Since the main focus of the framework is on malware delivery and network security, the traditional Cyber Kill Chain will not be able to identify Insider Threats. According to CISA, *"The Insider Threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization."*


You did it! Cyber Kill Chain complete!
Points earned
80
Completed tasks
10
Room type
Walkthrough
Difficulty
Easy
Streak
1
83,345 users are actively learning this week
Leave Feedback
Continue