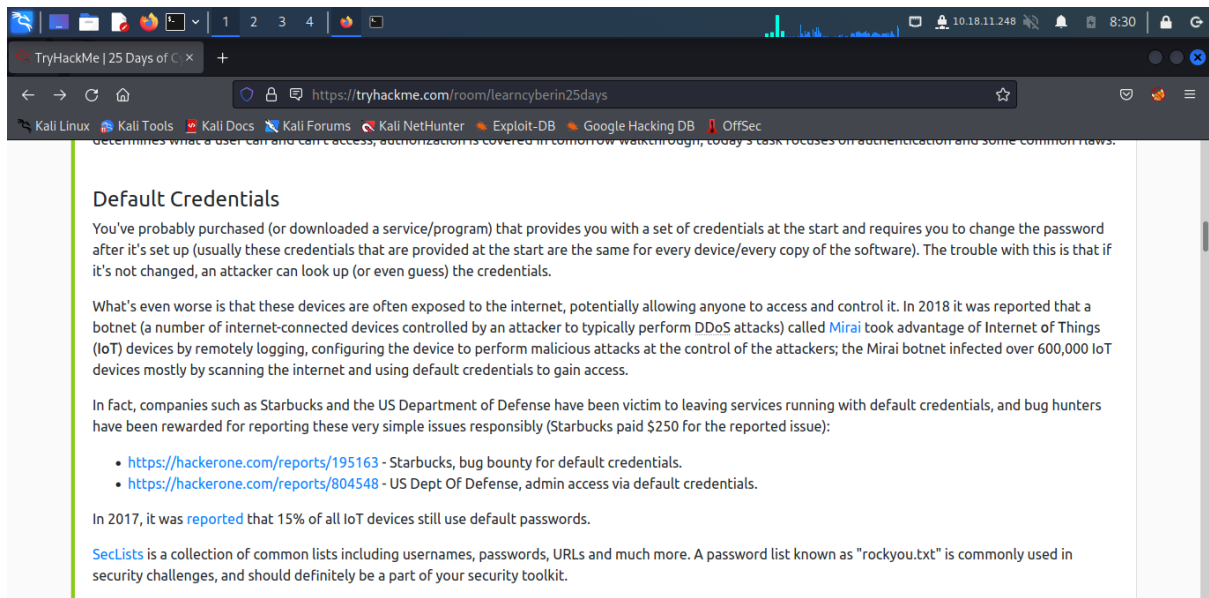


Day 3: Web Exploitation Christmas Chaos

Tool used: Kali-Linux, Firefox

Solution/walkthrough:

Question 1



The screenshot shows a web browser window with the URL <https://tryhackme.com/room/learnycyberin25days>. The page content is titled "Default Credentials" and discusses the importance of changing default credentials. It mentions that many IoT devices use default credentials, which can be exploited. It also lists some examples of default credentials and the consequences of not changing them, such as the Mirai botnet and Starbucks' security issue. The text includes several links to reports and a mention of SecLists.

Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called [Mirai](#) took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid \$250 for the reported issue):

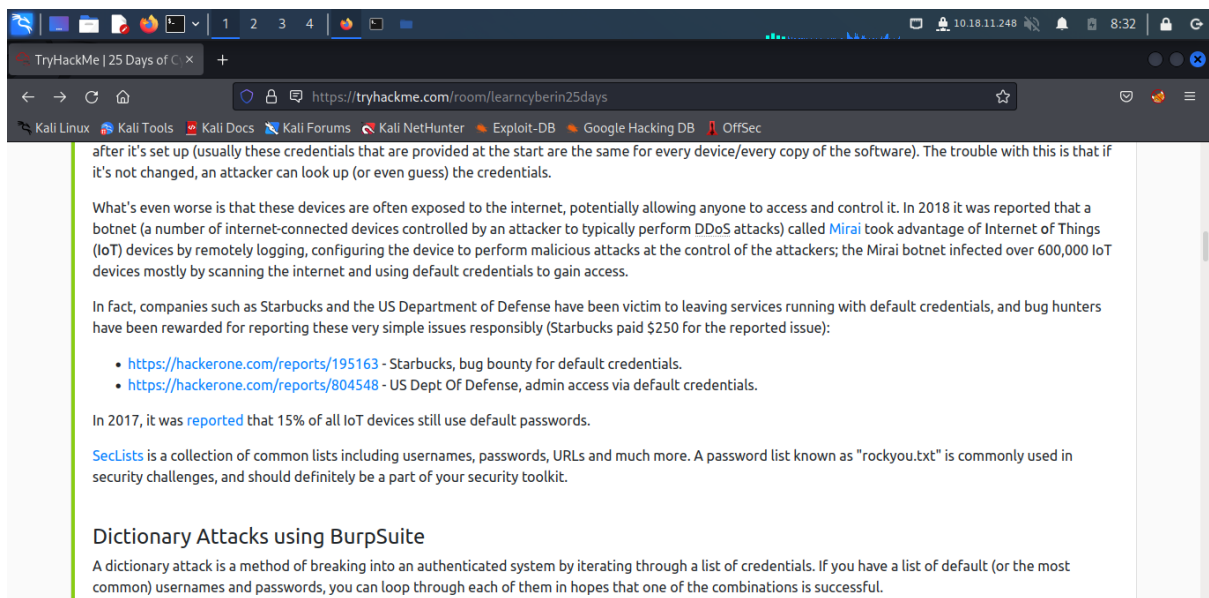
- <https://hackerone.com/reports/195163> - Starbucks, bug bounty for default credentials.
- <https://hackerone.com/reports/804548> - US Dept Of Defense, admin access via default credentials.

In 2017, it was [reported](#) that 15% of all IoT devices still use default passwords.

[SecLists](#) is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

Read the text and find the answer from the tryhackme text.

Question 2



The screenshot shows a web browser window with the URL <https://tryhackme.com/room/learnycyberin25days>. The page content is titled "Dictionary Attacks using BurpSuite" and discusses the importance of changing default credentials. It mentions that many IoT devices use default credentials, which can be exploited. It also lists some examples of default credentials and the consequences of not changing them, such as the Mirai botnet and Starbucks' security issue. The text includes several links to reports and a mention of SecLists.

after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called [Mirai](#) took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid \$250 for the reported issue):

- <https://hackerone.com/reports/195163> - Starbucks, bug bounty for default credentials.
- <https://hackerone.com/reports/804548> - US Dept Of Defense, admin access via default credentials.

In 2017, it was [reported](#) that 15% of all IoT devices still use default passwords.

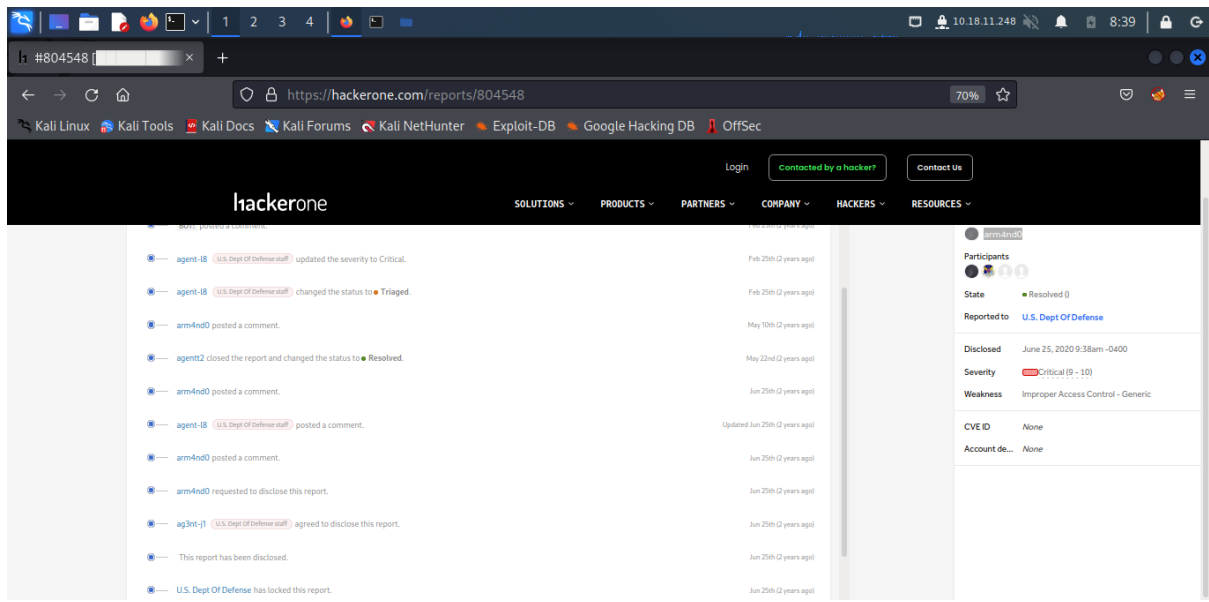
[SecLists](#) is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

Dictionary Attacks using BurpSuite

A dictionary attack is a method of breaking into an authenticated system by iterating through a list of credentials. If you have a list of default (or the most common) usernames and passwords, you can loop through each of them in hopes that one of the combinations is successful.

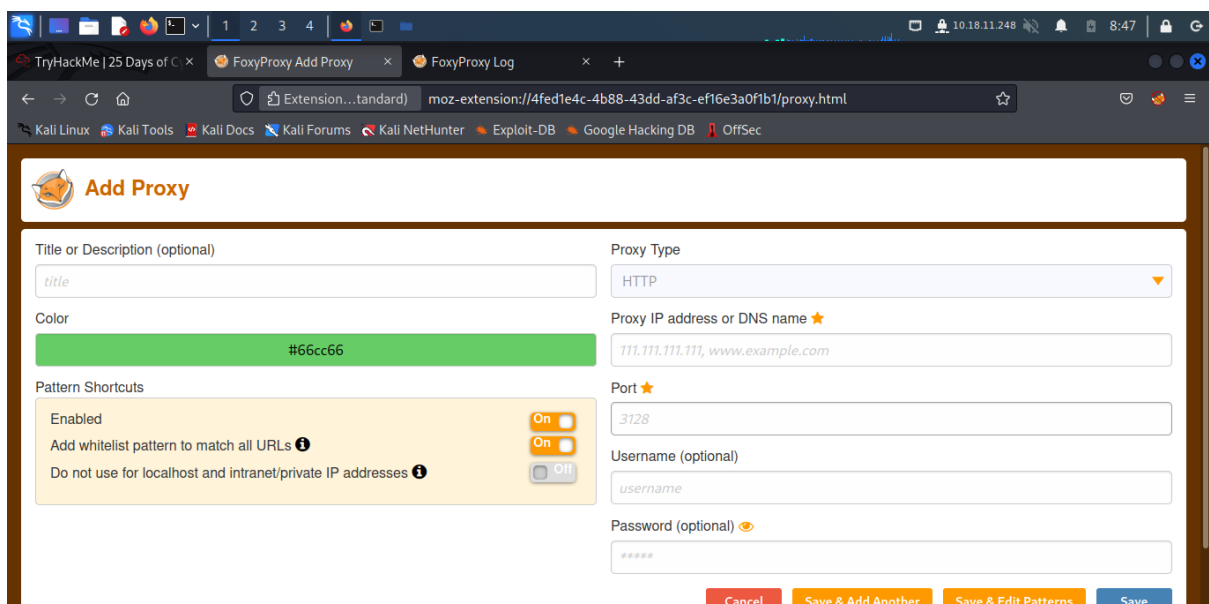
Read the text and find the answer from the tryhackme text.

Question 3



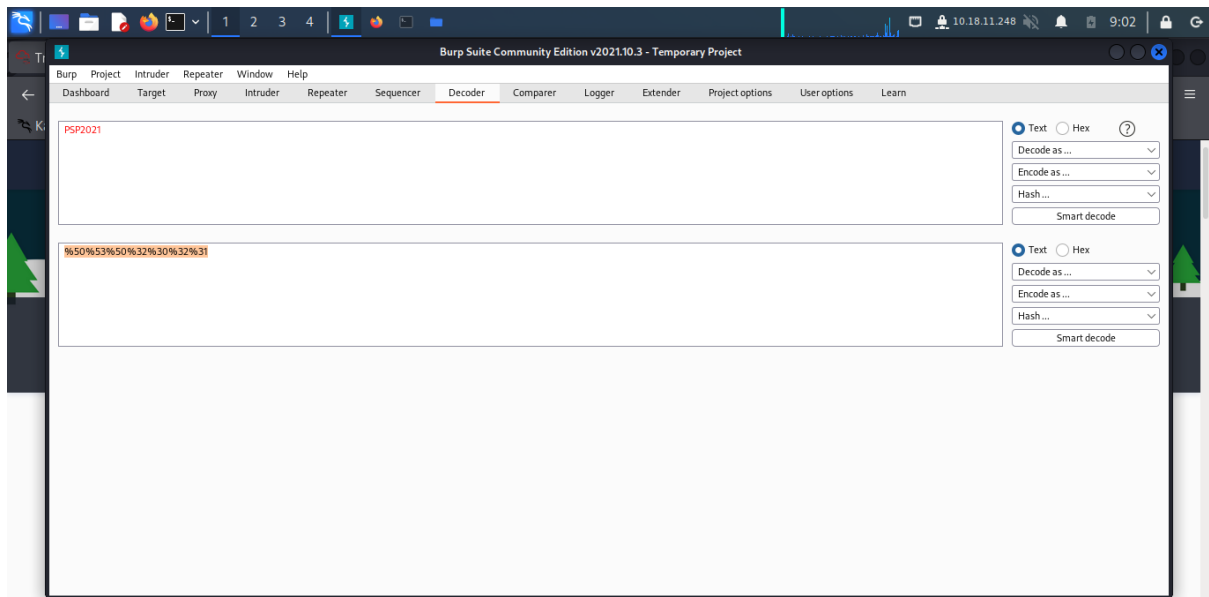
Read the report and find the answer.

Question 4,5



Open FoxyProxy Option and edit proxy. Then, the answer is shown.

Question 6



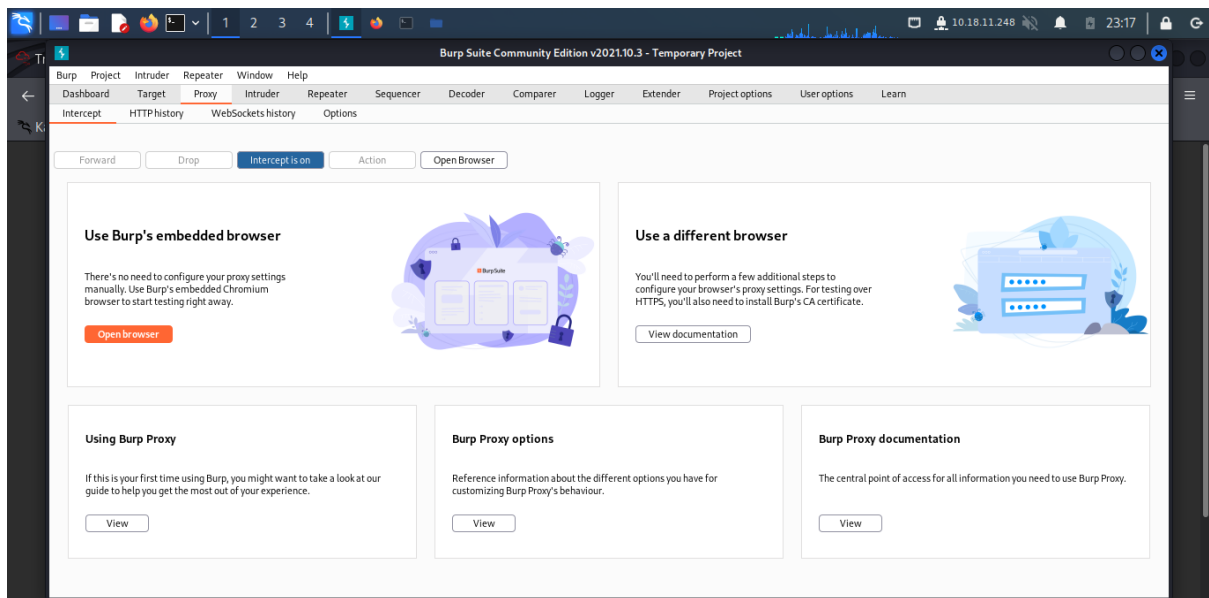
Open burp suite and press the decoder and type PSP0201 to encode the answer.

Question 7

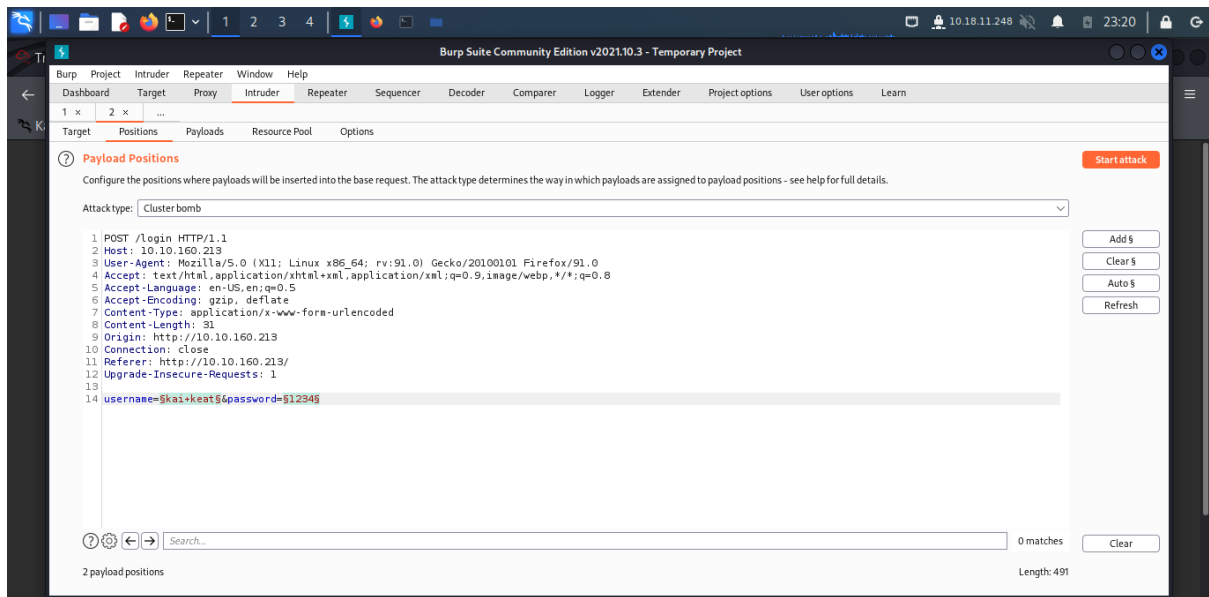
Cluster bomb – This uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

Research and find the answer.

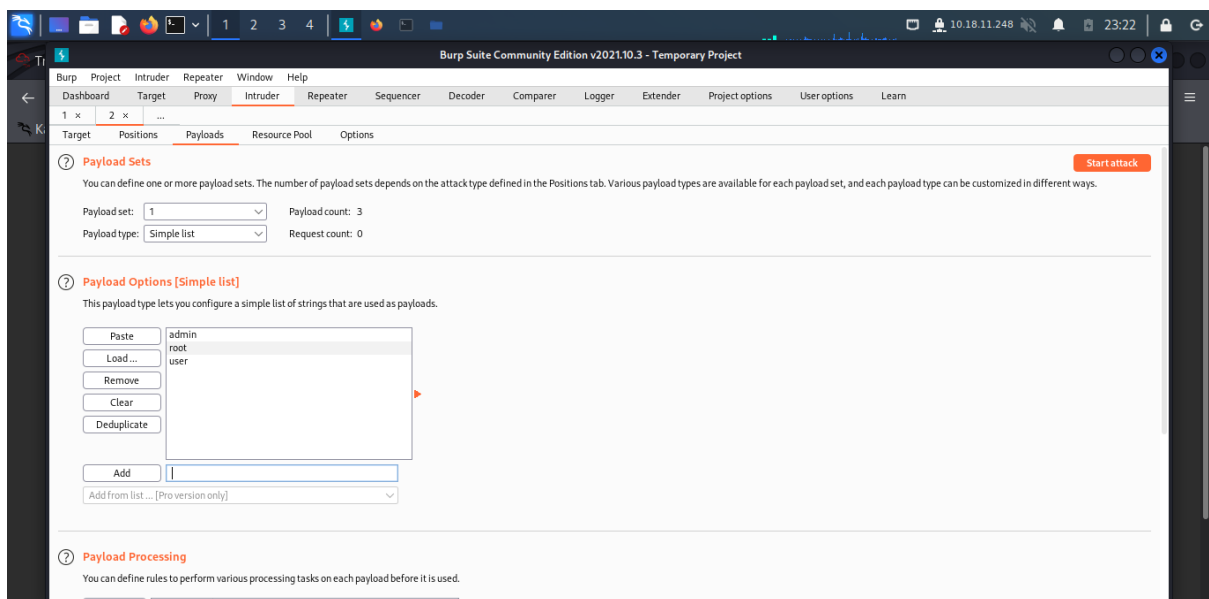
Question 8



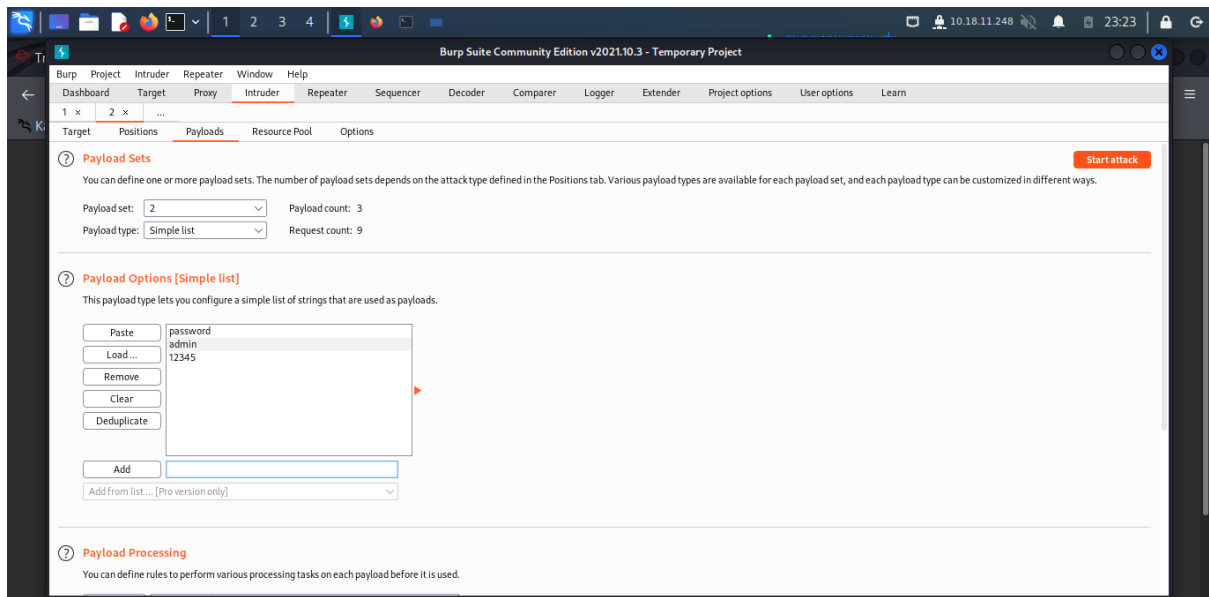
First, open burp suite and turn on intercept. Then, random put an input. Burp suite will send a request.



Next, send the request to intruder. Then, click into the position and select "Cluster Bomb" in the Attack type dropdown menu.

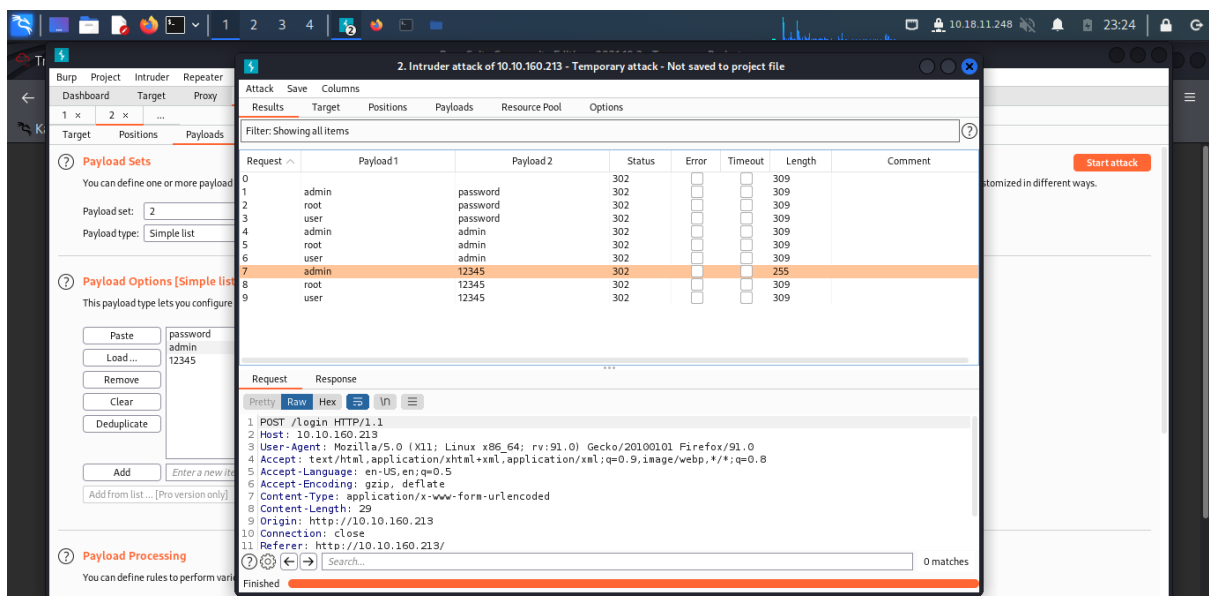


After that, click the "Payloads" tab, select Payload set 1 and at payload options, add a few common default usernames such as "admin", "root" and "user".

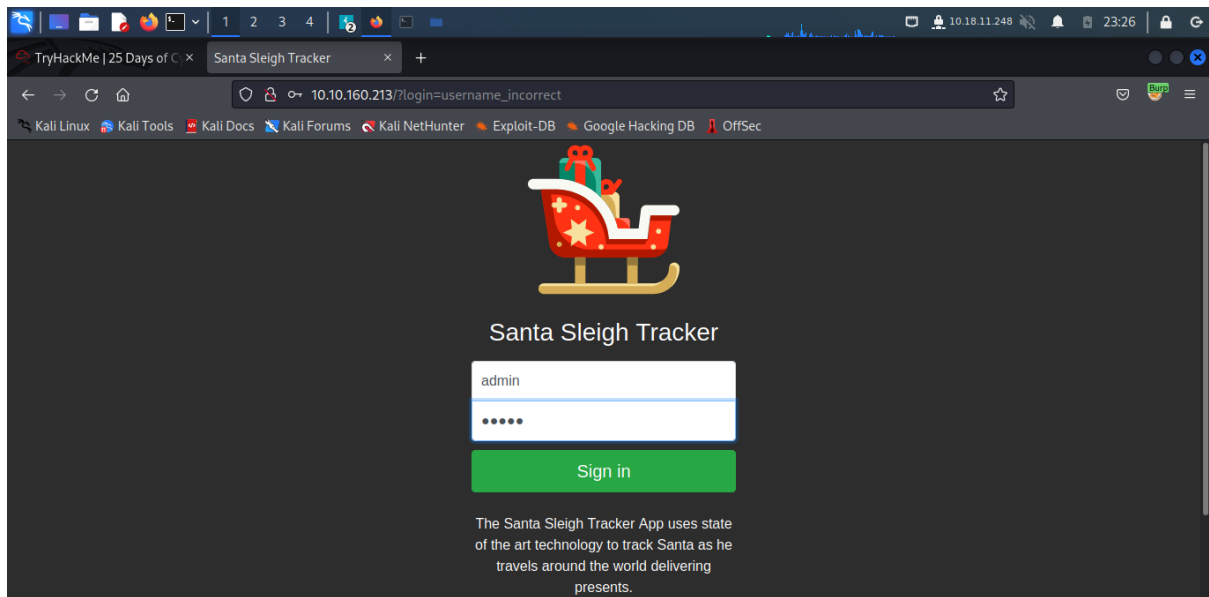


For set 2, add a few common default passwords such as "password", "admin" and "12345".

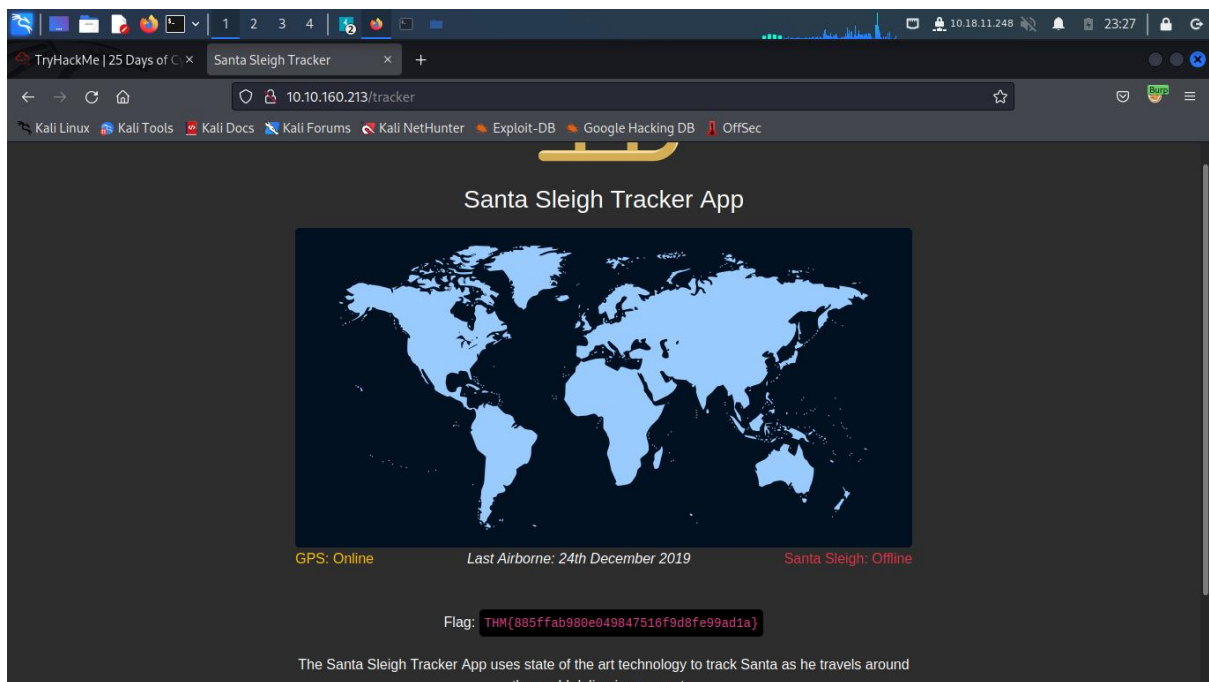
Then, click the start attack button.



The different pattern is shown.



Copy the username and password and log in it.



The flag is shown.