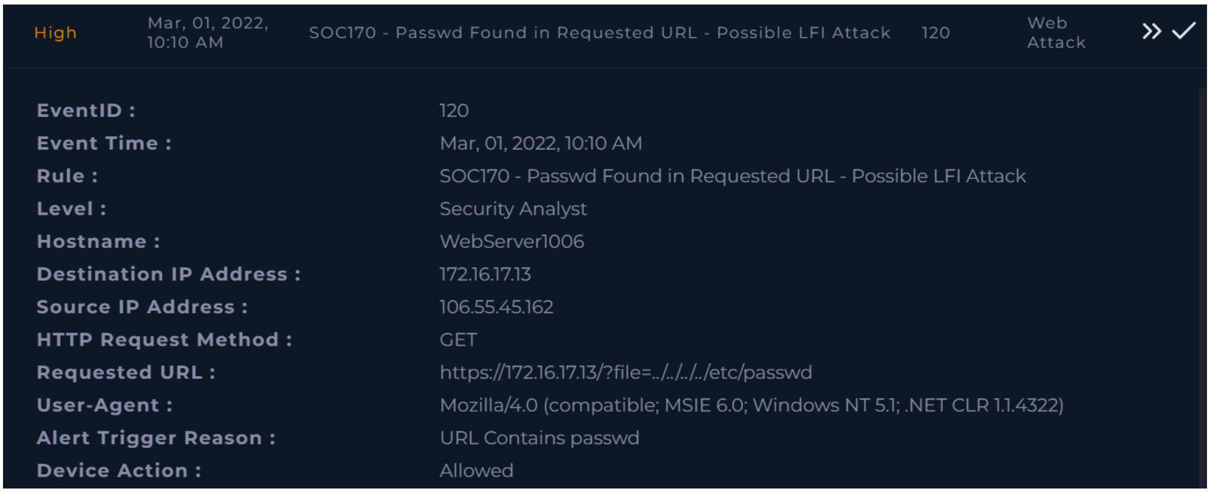
SOC170 – Passwd Found in Requested URL – Possible LFI Attack

Hello, Today I will write about investigation of “SOC170 - Passwd Found in Requested URL – Possible LFI Attack”

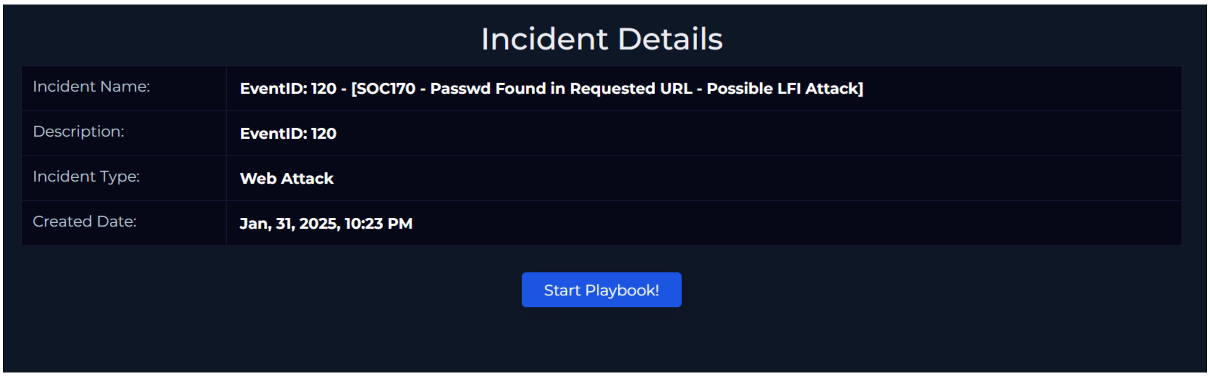
This is the alert that appears in our investigation channel.



High | Mar, 01, 2022, 10:10 AM | SOC170 - Passwd Found in Requested URL - Possible LFI Attack | 120 | Web Attack

EventID :	120
Event Time :	Mar, 01, 2022, 10:10 AM
Rule :	SOC170 - Passwd Found in Requested URL - Possible LFI Attack
Level :	Security Analyst
Hostname :	WebServer1006
Destination IP Address :	172.16.17.13
Source IP Address :	106.55.45.162
HTTP Request Method :	GET
Requested URL :	https://172.16.17.13/?file=../../../../etc/passwd
User-Agent :	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Alert Trigger Reason :	URL Contains passwd
Device Action :	Allowed

Let’s start with the playbook

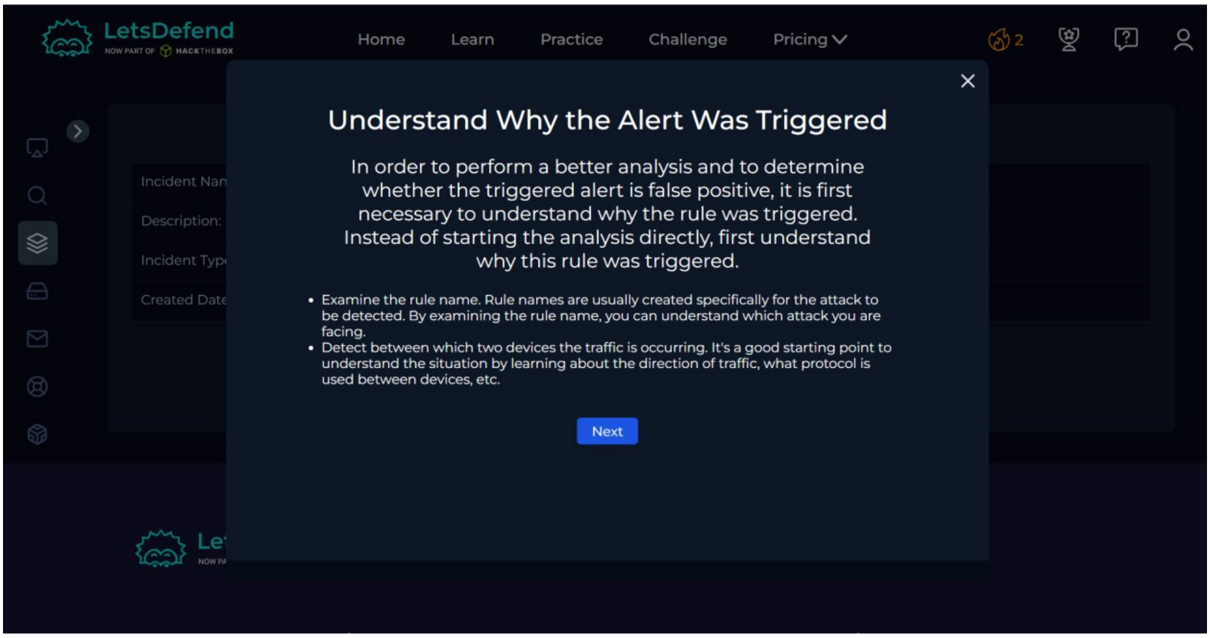


Incident Details

Incident Name:	EventID: 120 - [SOC170 - Passwd Found in Requested URL - Possible LFI Attack]
Description:	EventID: 120
Incident Type:	Web Attack
Created Date:	Jan, 31, 2025, 10:23 PM

Click on >> Start Playbook button

The first step of the playbook is asking us to understand why the alert was triggered



Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

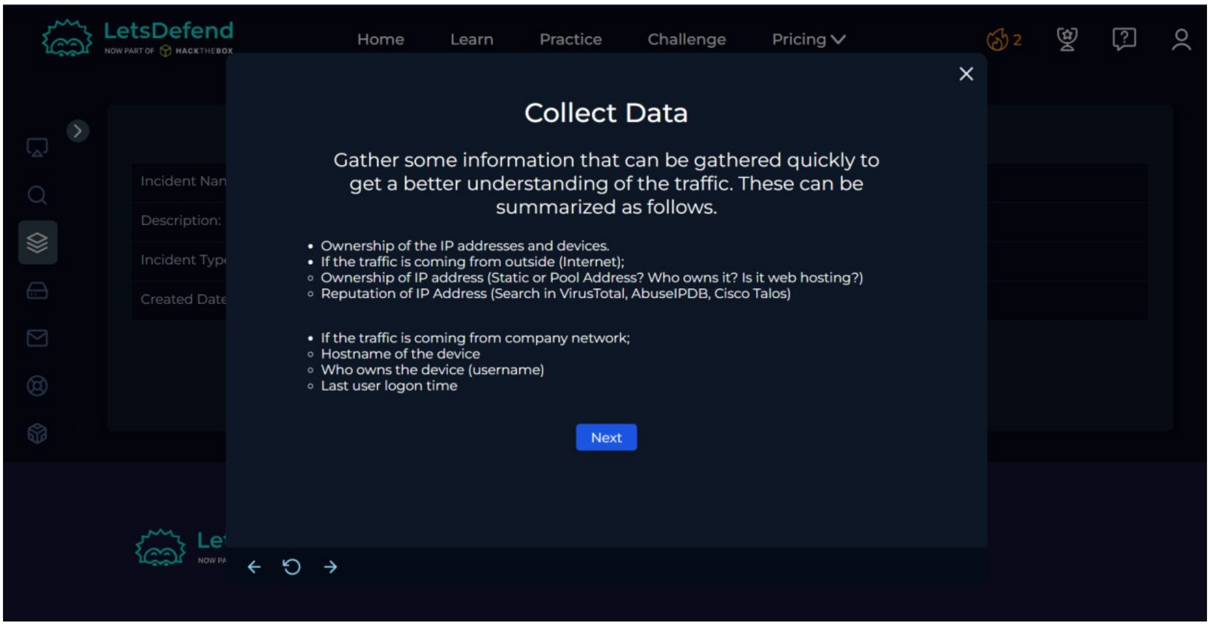
- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

Next

To understand the alert, we are supposed to examine the rule name.

The next step then asks us to determine the traffic path on which it is occurring.

The playbook's next phase instructs us to Collect data.



Collect Data

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

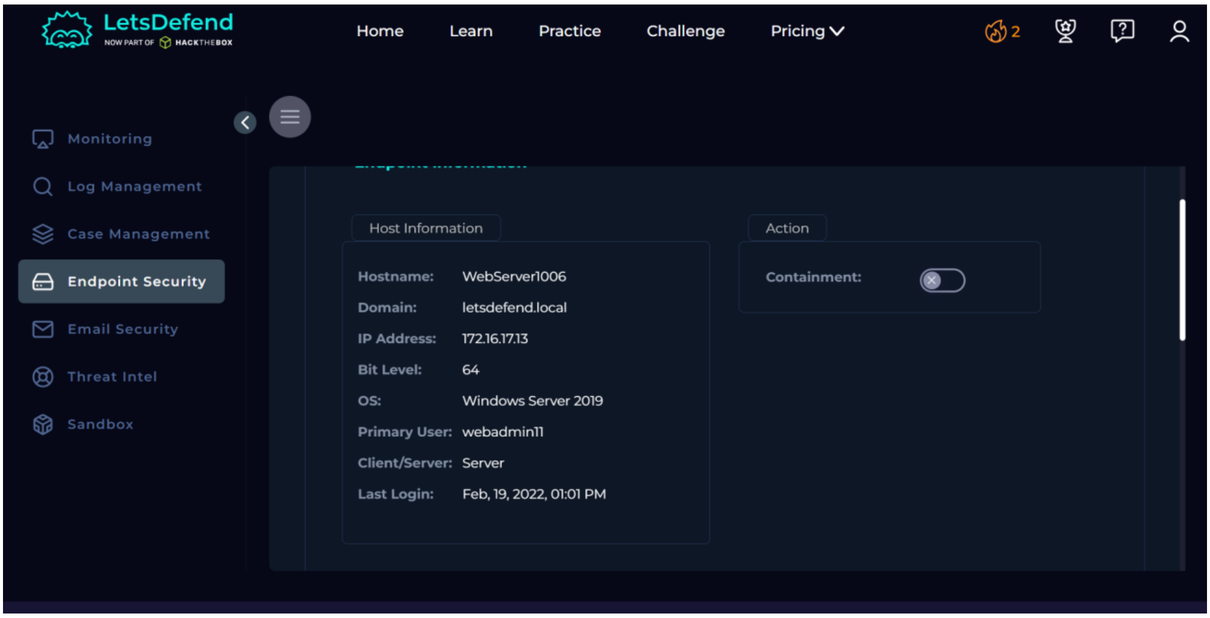
- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
  - Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
  - Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)

- If the traffic is coming from company network;
  - Hostname of the device
  - Who owns the device (username)
  - Last user logon time

Next

Let's find out the ownership of the IP addresses and devices.

After checking the Endpoint Security of the address 172.16.17.13 it displays that it belongs to webserver1006

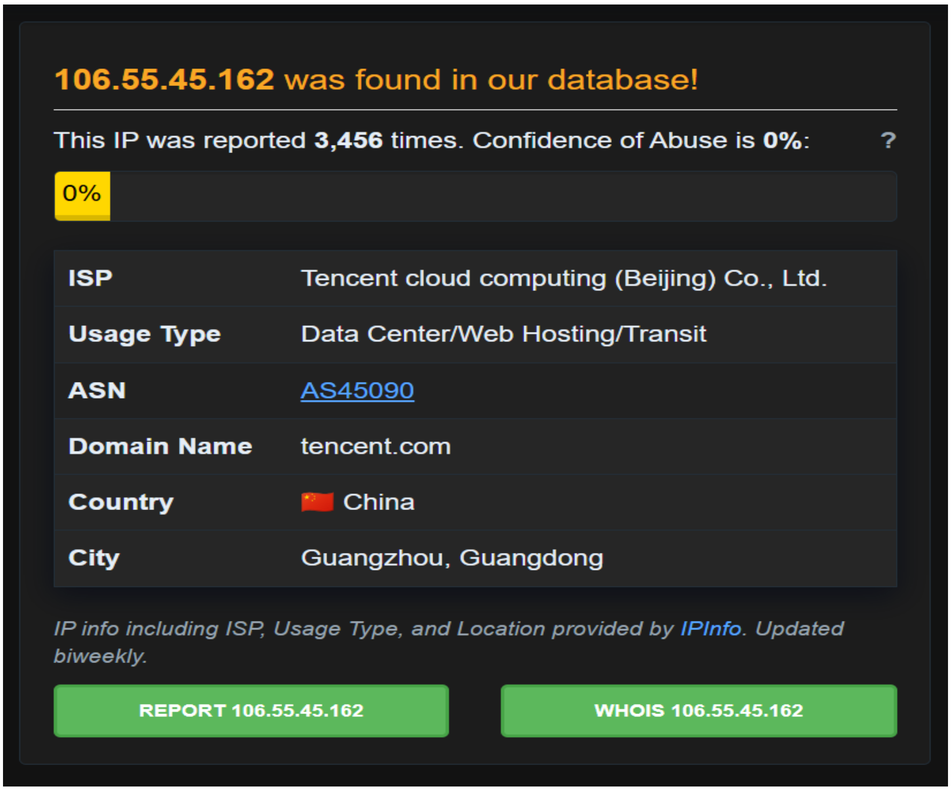


Hostname:	WebServer1006
Domain:	letsdefend.local
IP Address:	172.16.17.13
Bit Level:	64
OS:	Windows Server 2019
Primary User:	webadmin11
Client/Server:	Server
Last Login:	Feb, 19, 2022, 01:01 PM

If the traffic is coming from outside (Internet);

Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)

We can clearly see that that it is a Static Address. We are able to determine that the device is being web hosted on the Tencent Cloud Computing Beijing Co. LTD using Cisco Talos and AbuseIPDB



106.55.45.162 was found in our database!

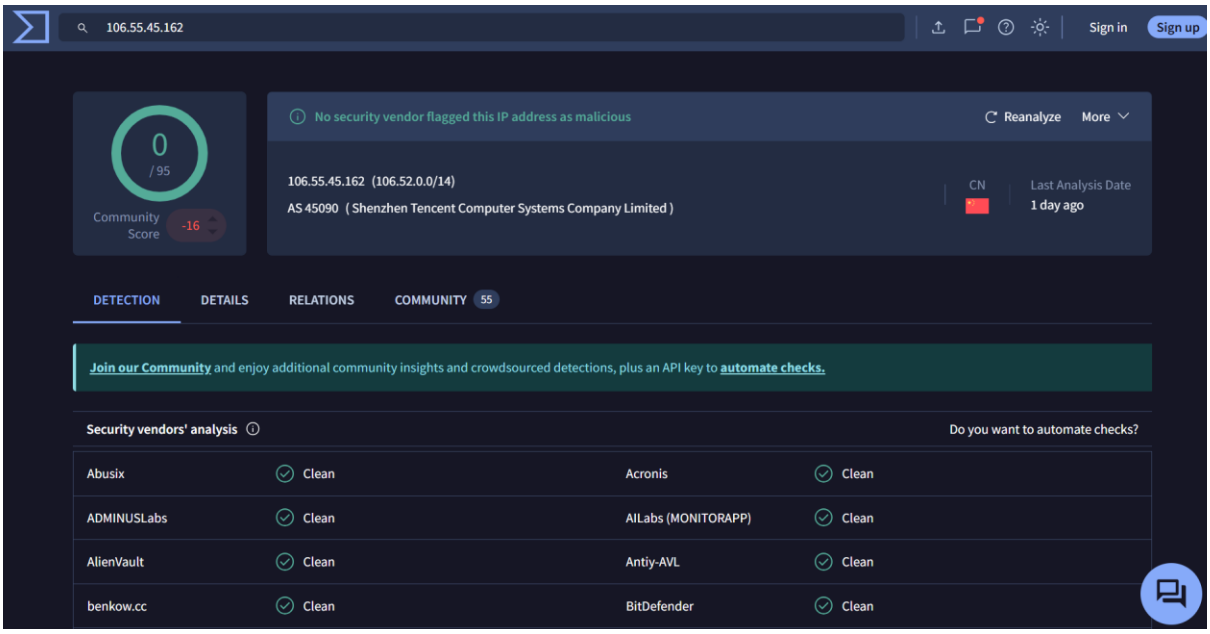
This IP was reported **3,456** times. Confidence of Abuse is **0%**: ?

0%

ISP	Tencent cloud computing (Beijing) Co., Ltd.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS45090
Domain Name	tencent.com
Country	🇨🇳 China
City	Guangzhou, Guangdong

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

The Reputation of the IP Address is **Suspicious**



0 / 95

Community Score -16

No security vendor flagged this IP address as malicious

106.55.45.162 (106.52.0.0/14)
AS 45090 (Shenzhen Tencent Computer Systems Company Limited)

CN

Last Analysis Date
1 day ago

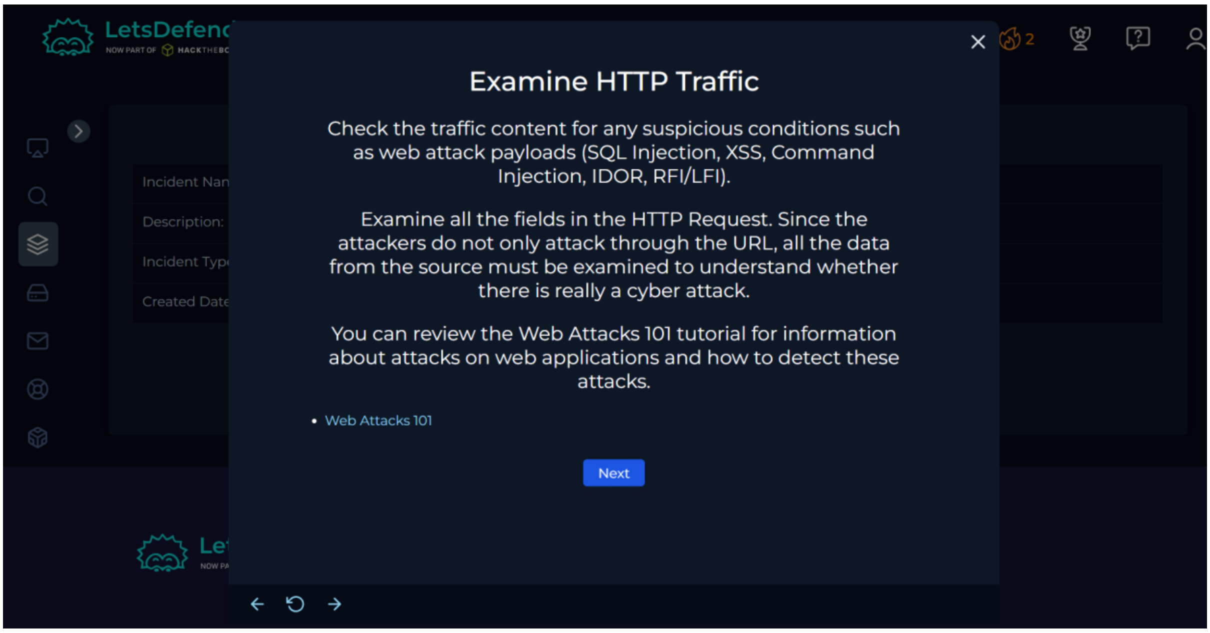
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean

Then we examine the HTTP Traffic by simply looking at the IP address reputation and the log analysis performed in log management.



Examine HTTP Traffic

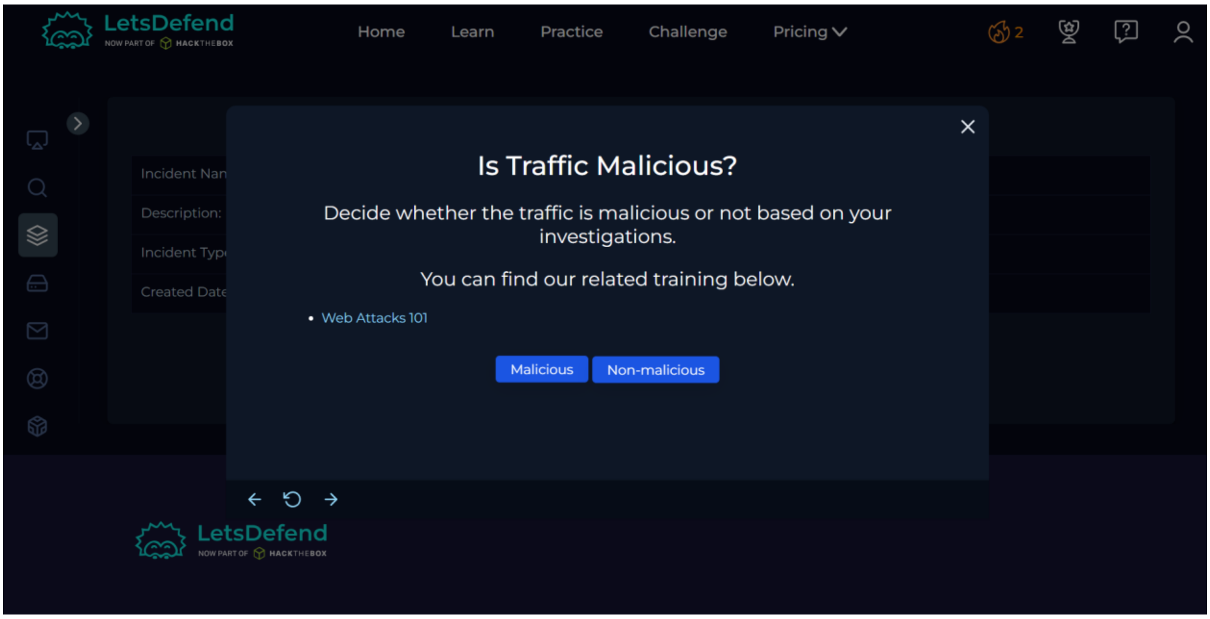
Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

- Web Attacks 101

Click on >> Next

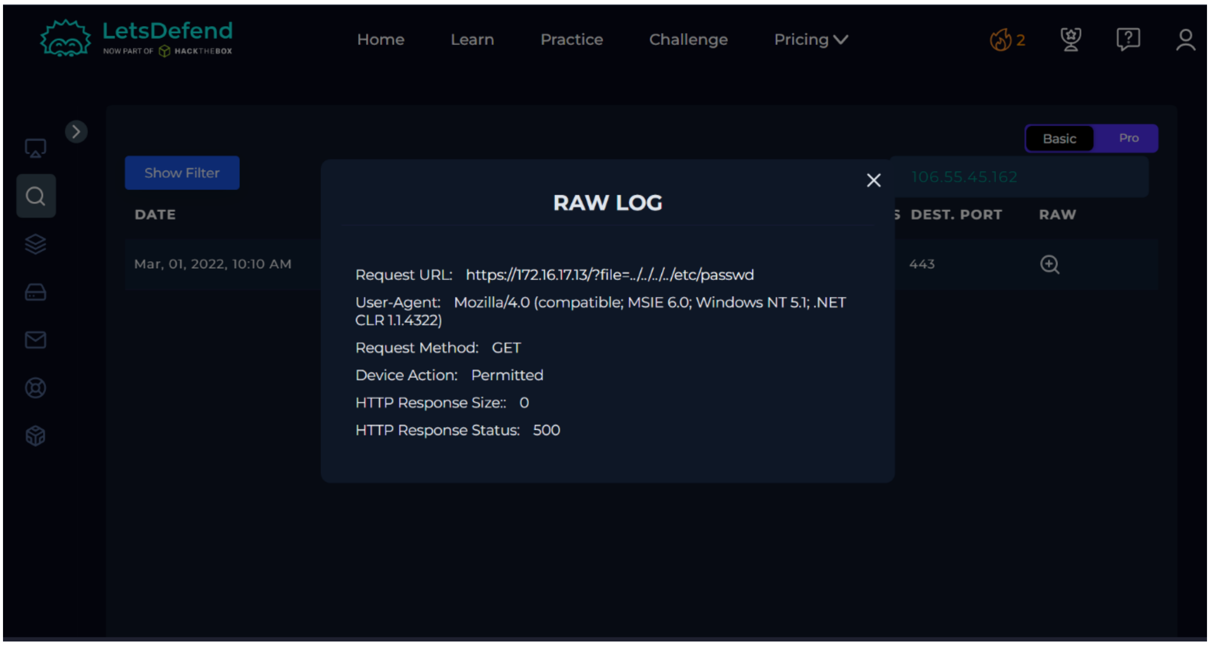


Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

Let’s find this out by searching the IP address 106.55.45.162 in log management section. In this log entry, we can clearly see that the attacker is trying to load a system file from the server using the URL parameter file.

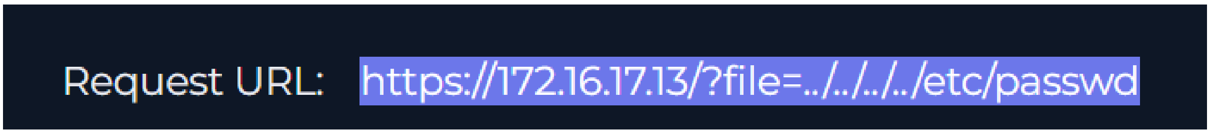


DATE		DEST. PORT	RAW
Mar, 01, 2022, 10:10 AM		443	

RAW LOG

```
Request URL:  https://172.16.17.13/?file=../../../../etc/passwd
User-Agent:  Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Request Method:  GET
Device Action:  Permitted
HTTP Response Size::  0
HTTP Response Status:  500
```

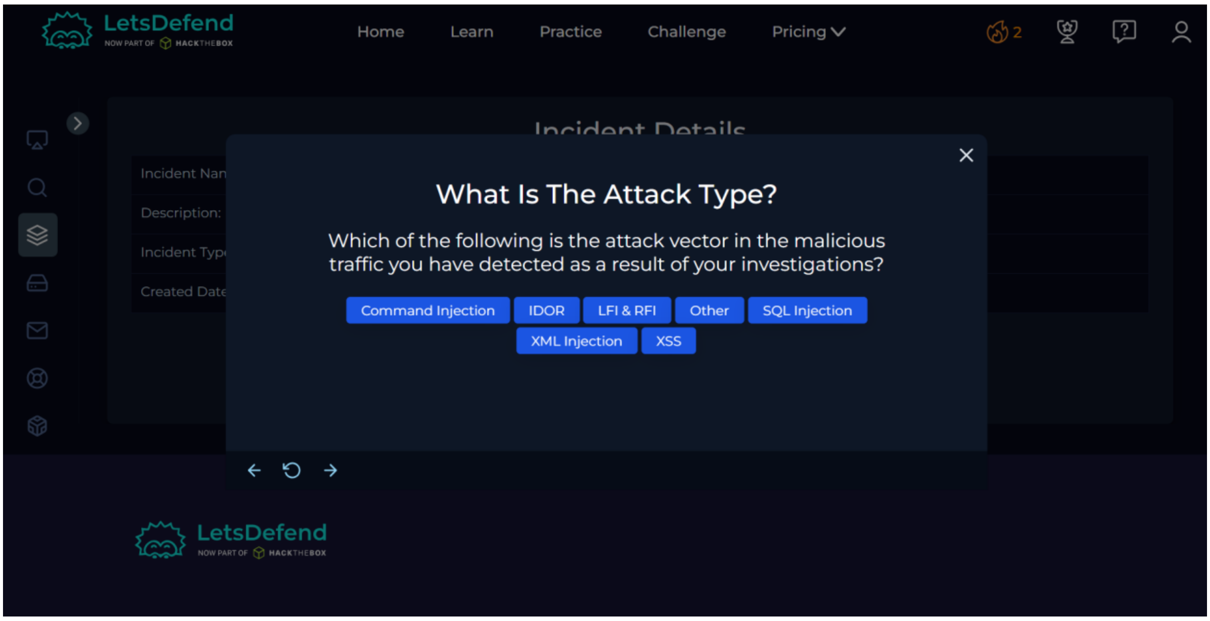
The request looks like this:



```
Request URL:  https://172.16.17.13/?file=../../../../etc/passwd
```

it shows a shows a classic Local File Inclusion (LFI) attack.

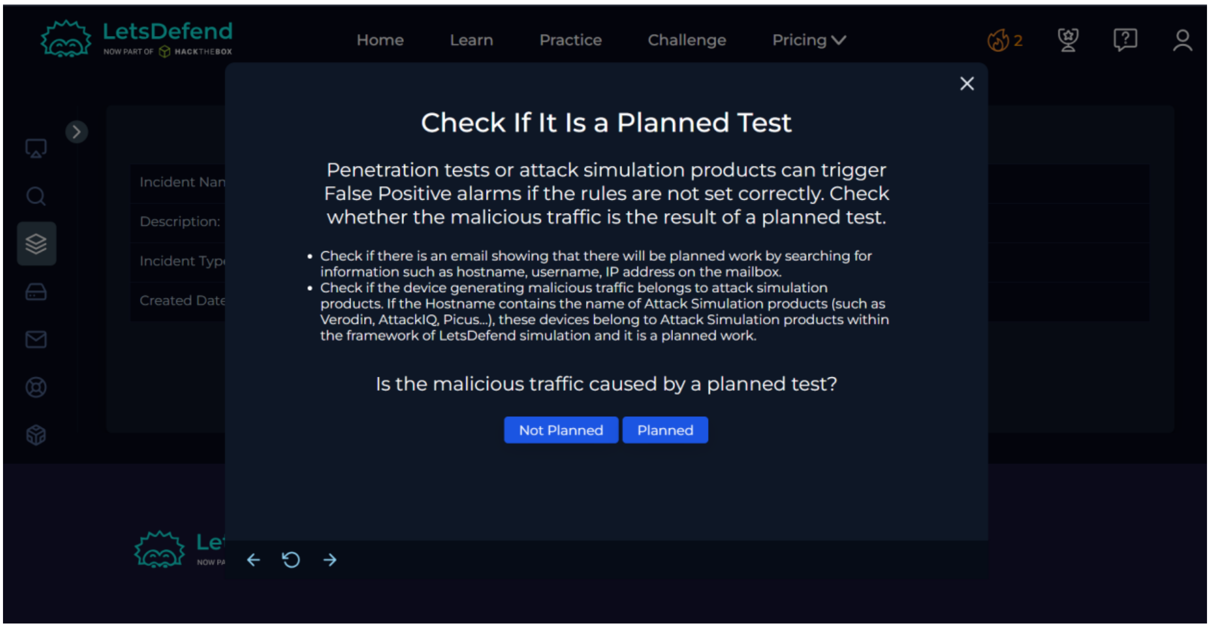
The attacker is using ../ (directory traversal) to climb out of the web folder and access a sensitive system file: /etc/passwd. This file stores user account information in Linux, so trying to load it is a clear sign of malicious intent.



What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

As discussed earlier, this is a LFI attack



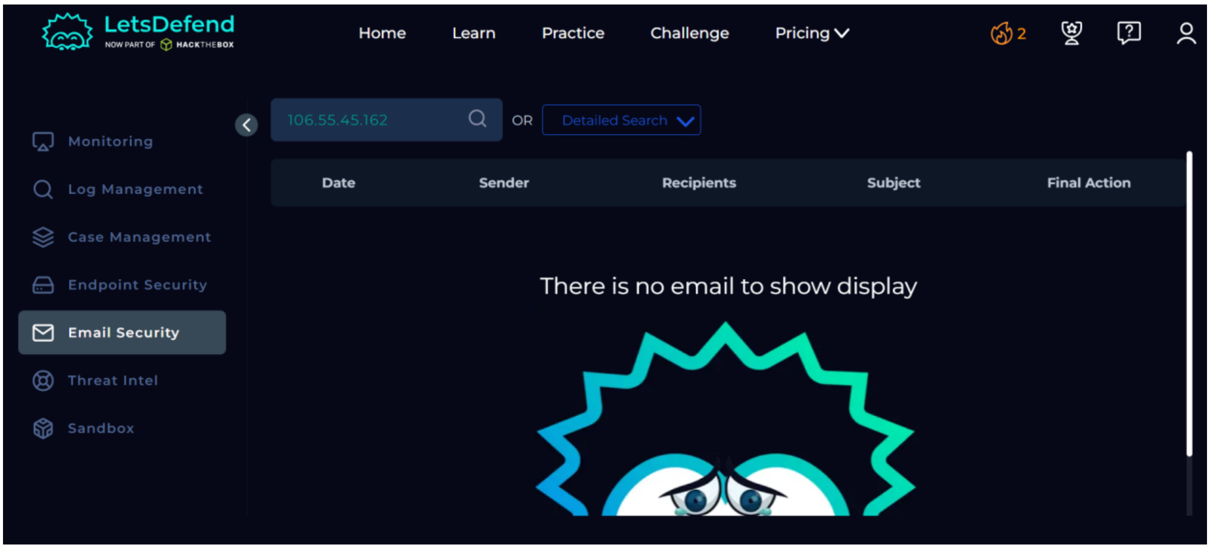
Check If It Is a Planned Test

Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

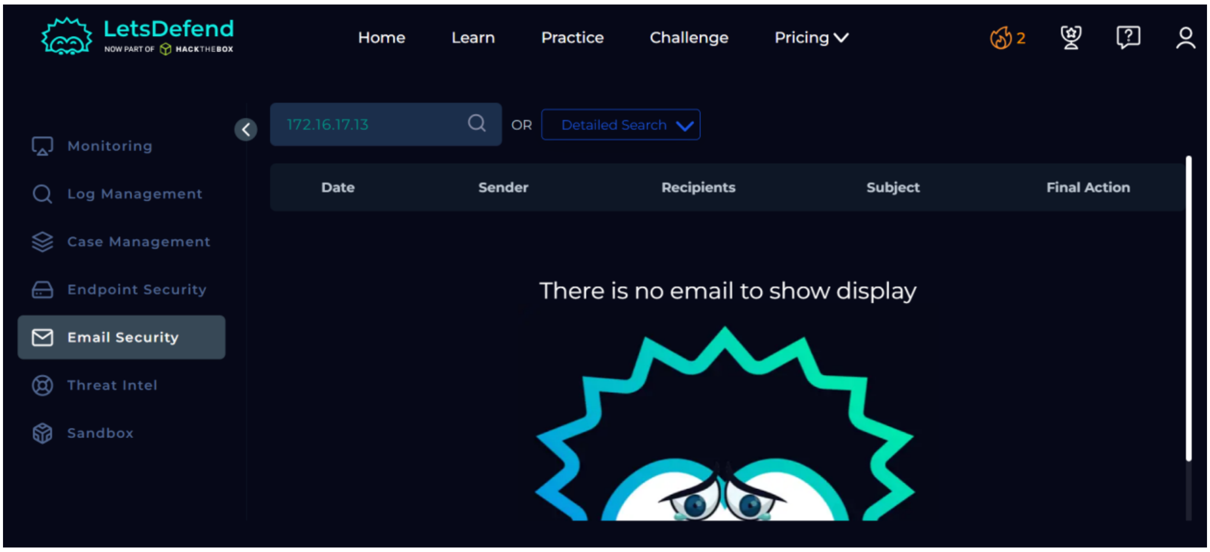
We can check this by using IP address in the Email Security.



106.55.45.162 OR Detailed Search

Date	Sender	Recipients	Subject	Final Action

There is no email to show display

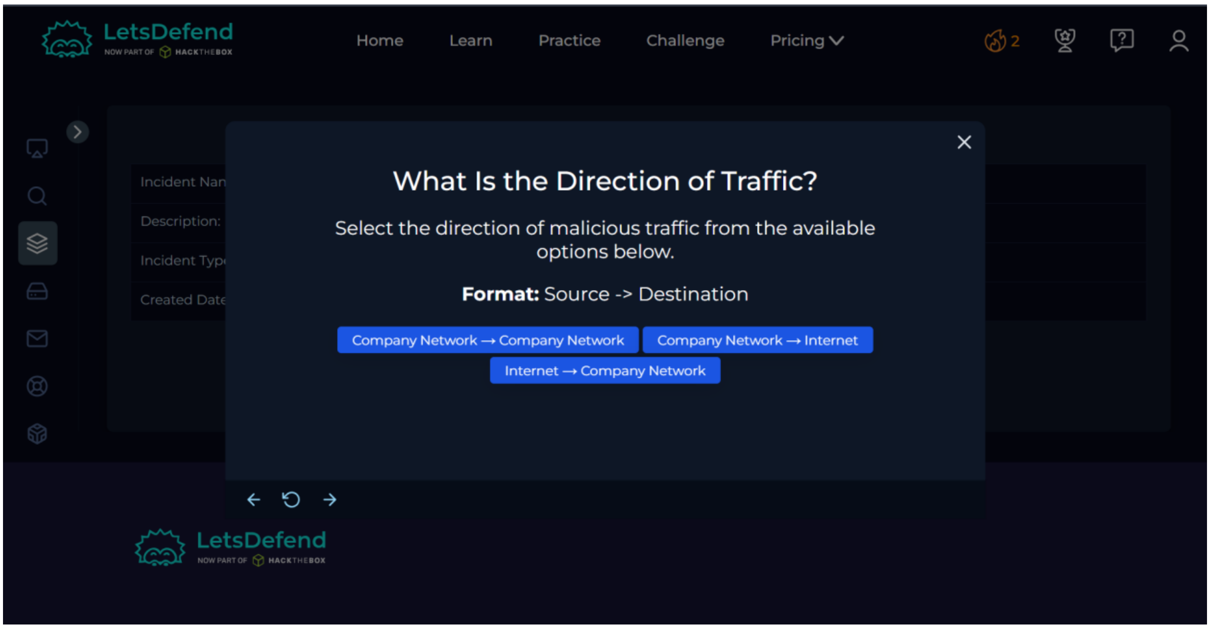


172.16.17.13

Date	Sender	Recipients	Subject	Final Action

There is no email to show display

After our search we found out that there is no email exchange related to this attack. So this is Not Planned



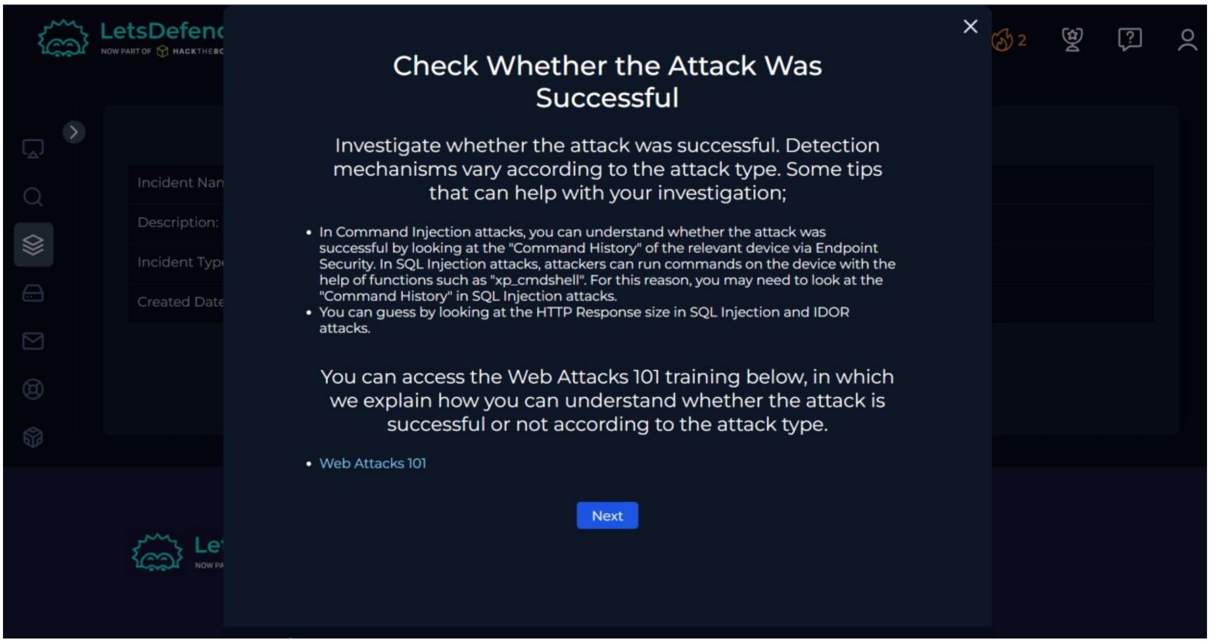
What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

To identify private vs public IPs, just check if the IP falls within the private ranges (10.x.x.x, 172.16–31.x.x, or 192.168.x.x). Any IP outside these ranges is a public IP. In simple terms: private IPs belong to internal networks, while public IPs are reachable from the Internet.

Click on >> Internet -> Company Network



Check Whether the Attack Was Successful

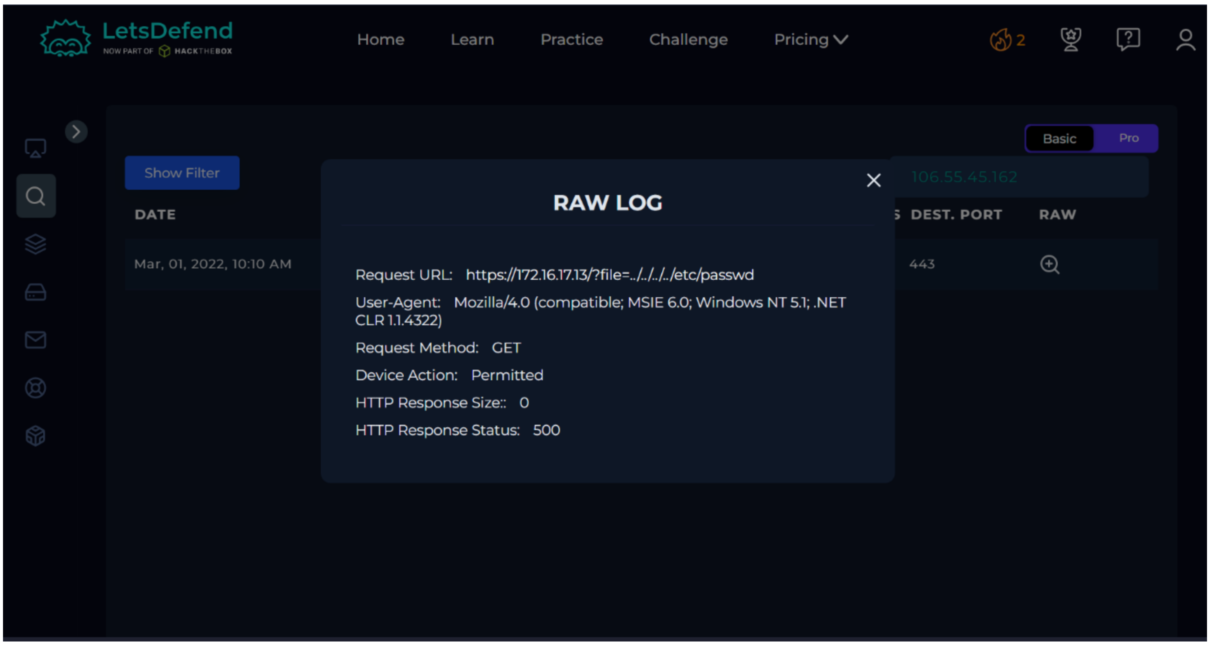
Investigate whether the attack was successful. Detection mechanisms vary according to the attack type. Some tips that can help with your investigation;

- In Command Injection attacks, you can understand whether the attack was successful by looking at the "Command History" of the relevant device via Endpoint Security. In SQL Injection attacks, attackers can run commands on the device with the help of functions such as "xp_cmdshell". For this reason, you may need to look at the "Command History" in SQL Injection attacks.
- You can guess by looking at the HTTP Response size in SQL Injection and IDOR attacks.

You can access the Web Attacks 101 training below, in which we explain how you can understand whether the attack is successful or not according to the attack type.

- Web Attacks 101

We can recall that the HTTP Response size was zero in our previous log analysis



DATE	DEST. PORT	RAW
Mar, 01, 2022, 10:10 AM	443	

RAW LOG

Request URL: https://172.16.17.13/?file=../../../../etc/passwd

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)

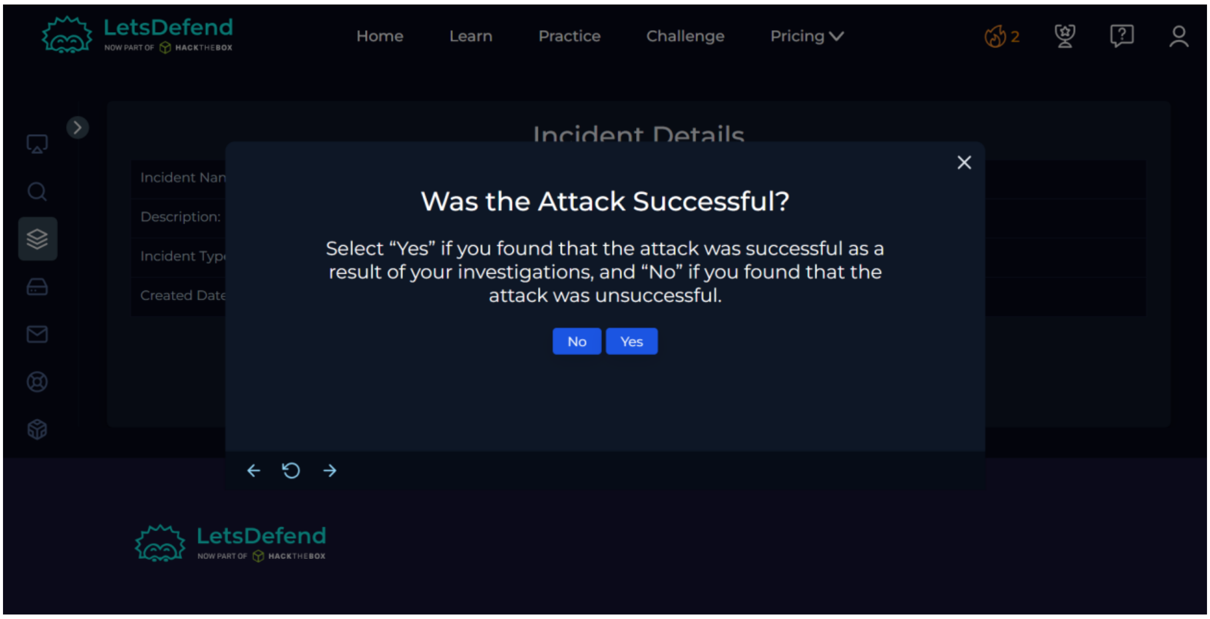
Request Method: GET

Device Action: Permitted

HTTP Response Size:: 0

HTTP Response Status: 500

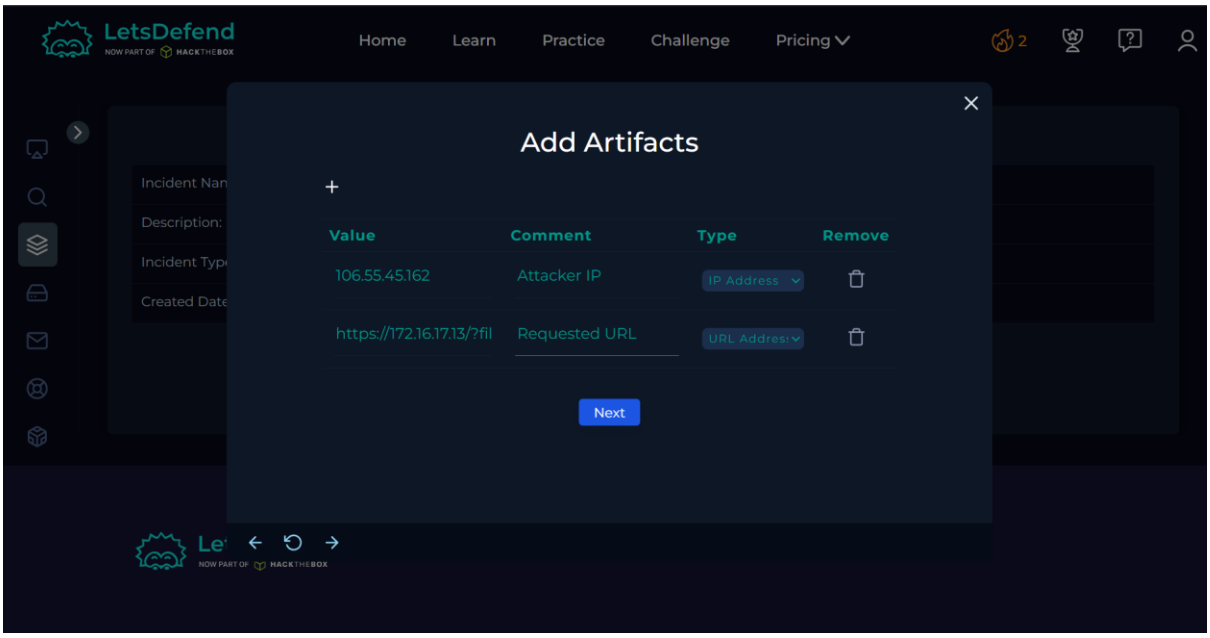
It means the server didn’t return any actual data. This indicates that the attacker’s request failed and the exploit was not successful.



Was the Attack Successful?

Select “Yes” if you found that the attack was successful as a result of your investigations, and “No” if you found that the attack was unsuccessful.

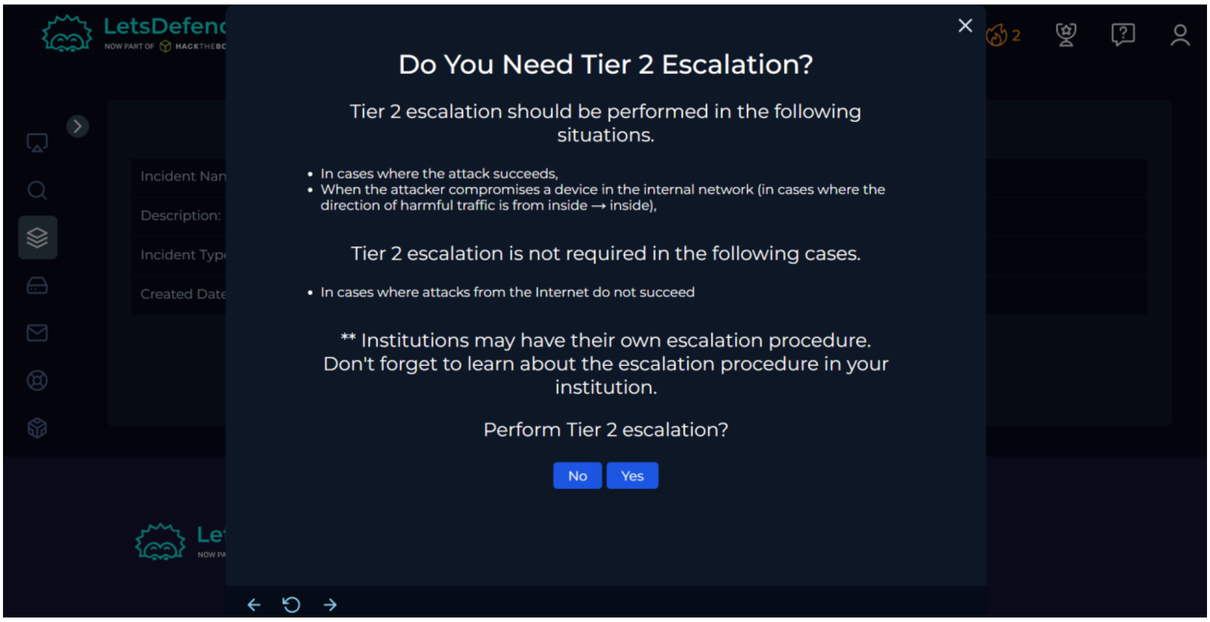
Click on >> No



Add Artifacts

Value	Comment	Type	Remove
106.55.45.162	Attacker IP	IP Address	🗑
https://172.16.17.13/?fil	Requested URL	URL Address	🗑

Add Artifacts then click Next



Do You Need Tier 2 Escalation?

Tier 2 escalation should be performed in the following situations.

- In cases where the attack succeeds,
- When the attacker compromises a device in the internal network (in cases where the direction of harmful traffic is from inside → inside),

Tier 2 escalation is not required in the following cases.

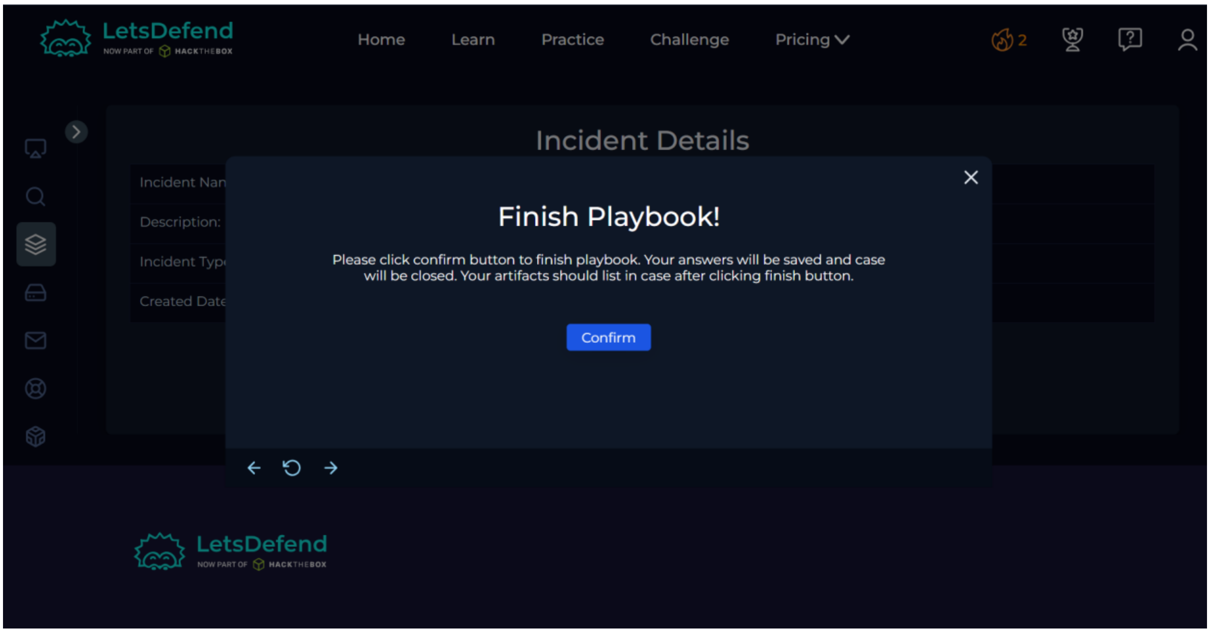
- In cases where attacks from the Internet do not succeed

** Institutions may have their own escalation procedure. Don't forget to learn about the escalation procedure in your institution.

Perform Tier 2 escalation?

As this attack was no successful and there was no communication regarding this, this alert does not require Tier 2 Escalation

Click on >> No



Finish Playbook!

Please click confirm button to finish playbook. Your answers will be saved and case will be closed. Your artifacts should list in case after clicking finish button.