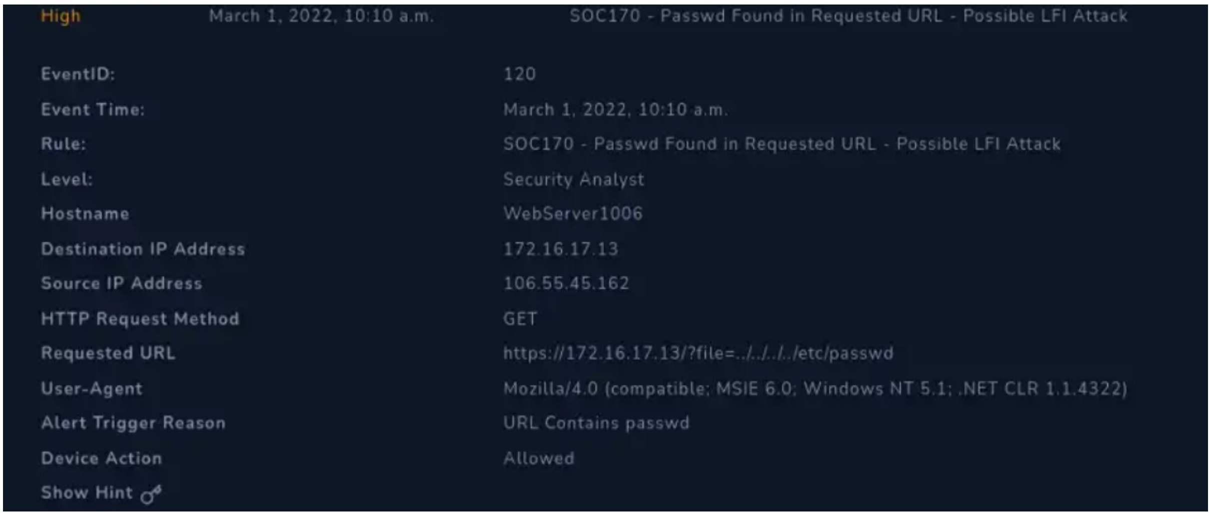
What is Local File Inclusion?

- Local File Inclusion (LFI) is a type of vulnerability that allows an attacker to include a file, usually through a script on a web server by manipulating the parameters that reference these files an attacker can access arbitrary files on the server, including sensitive ones such as password file.

How to detect LFI attacks?

- Look for patterns in the URL that may include an attempt to include a file
  - URL with "../../../file" or "../"

SOC170 - Passwd Found in Requested URL - Possible LFI Attack



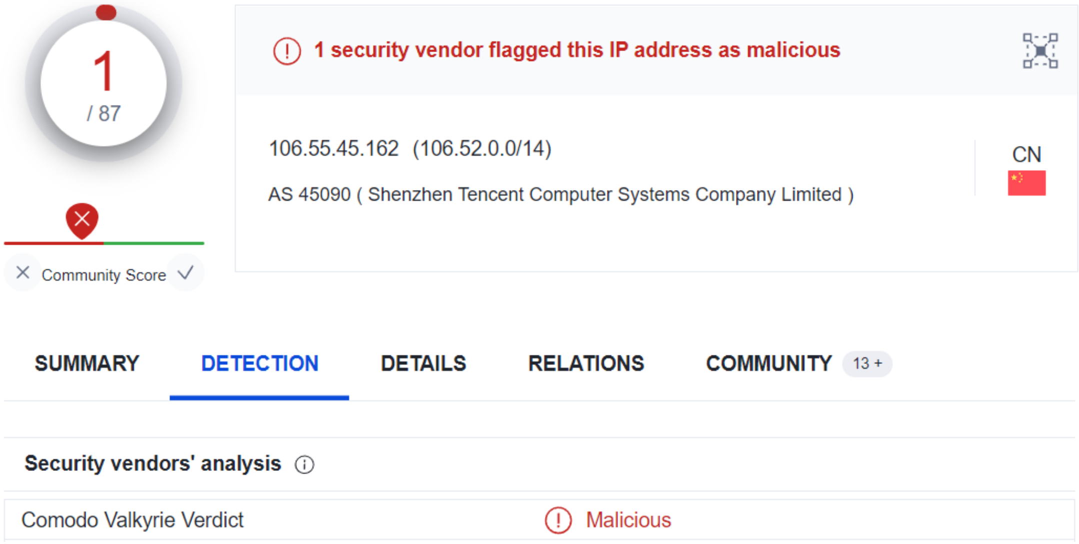
High March 1, 2022, 10:10 a.m. SOC170 - Passwd Found in Requested URL - Possible LFI Attack

EventID:	120
Event Time:	March 1, 2022, 10:10 a.m.
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
Show Hint	

The information gathered from the Alert.

- Source IP address : 106.55.45.162
- Webserver1006 : 172.16.17.13
- Requested URL : https://172.16.17.13/?file=../../../../etc/passwd

Let's investigate about source IP address with Virustotal and AbuseIPDB :



1 security vendor flagged this IP address as malicious

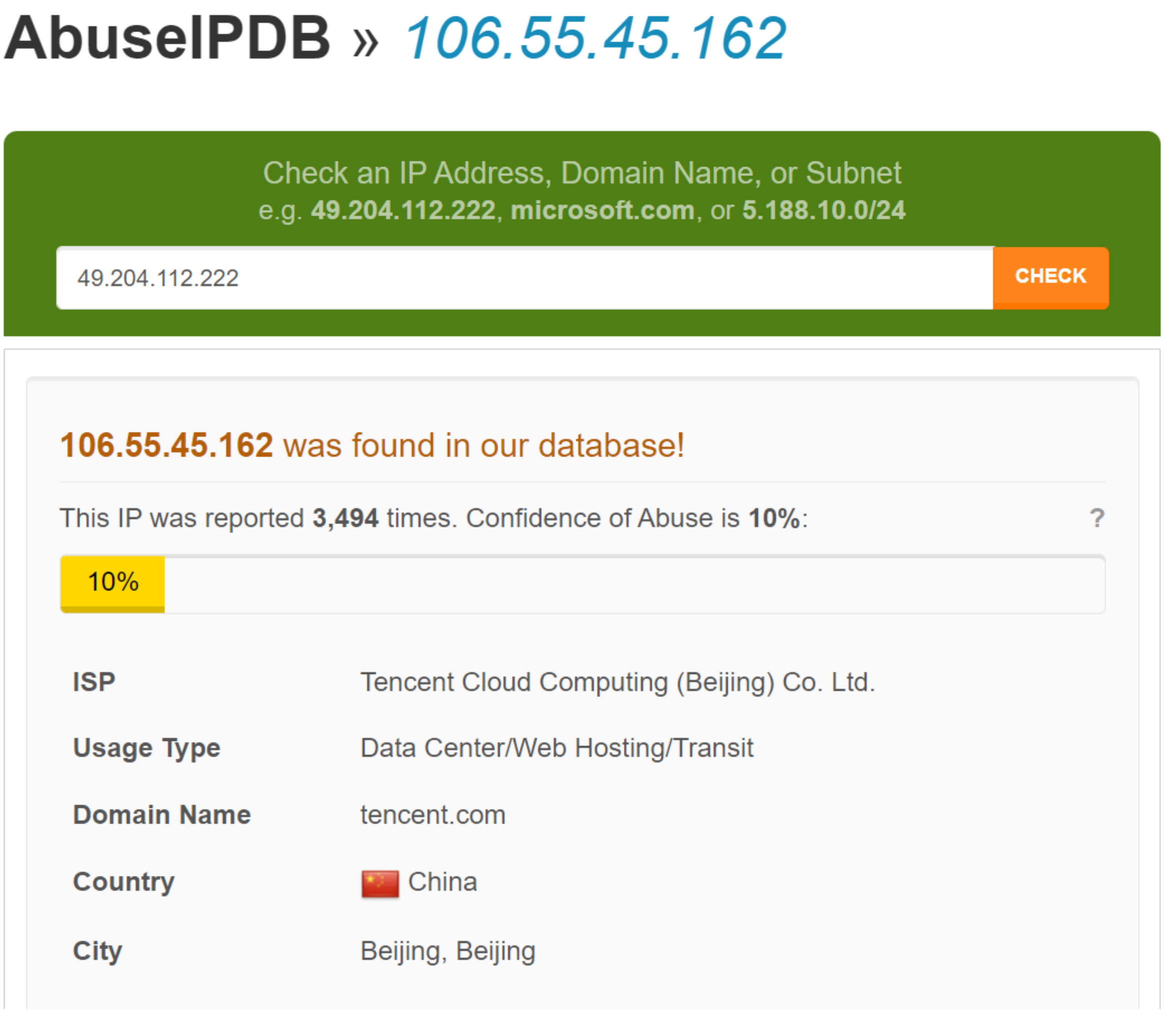
106.55.45.162 (106.52.0.0/14)

AS 45090 (Shenzhen Tencent Computer Systems Company Limited)

CN

Security vendors' analysis

Comodo Valkyrie Verdict	Malicious



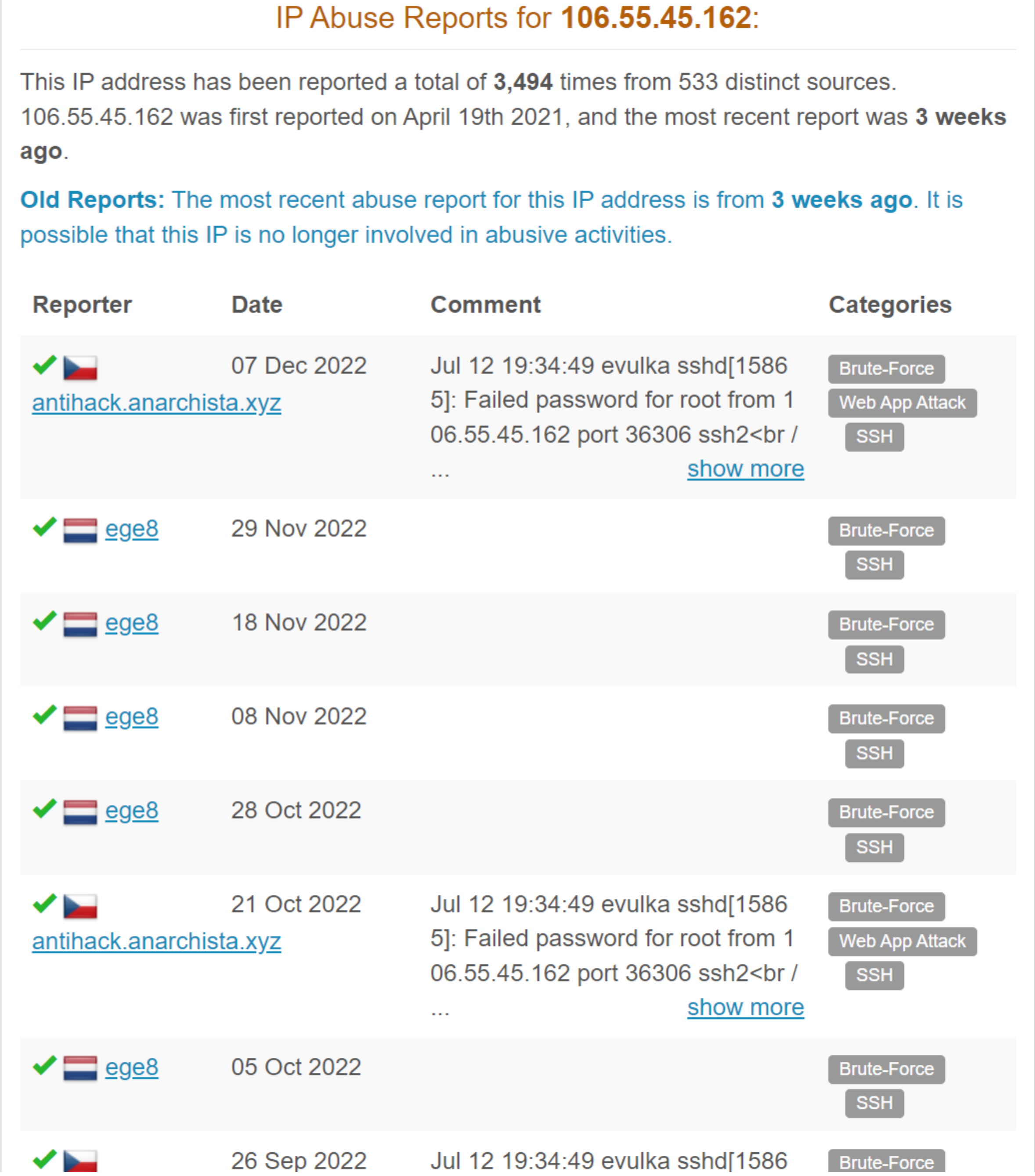
AbuseIPDB » *106.55.45.162*

Check an IP Address, Domain Name, or Subnet
e.g. **49.204.112.222**, **microsoft.com**, or **5.188.10.0/24**

106.55.45.162 was found in our database!

This IP was reported **3,494** times. Confidence of Abuse is **10%**:

ISP	Tencent Cloud Computing (Beijing) Co. Ltd.
Usage Type	Data Center/Web Hosting/Transit
Domain Name	tencent.com
Country	China
City	Beijing, Beijing



IP Abuse Reports for **106.55.45.162**:

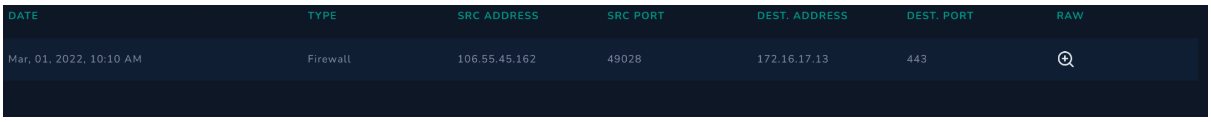
This IP address has been reported a total of **3,494** times from 533 distinct sources. 106.55.45.162 was first reported on April 19th 2021, and the most recent report was **3 weeks ago**.

Old Reports: The most recent abuse report for this IP address is from **3 weeks ago**. It is possible that this IP is no longer involved in abusive activities.

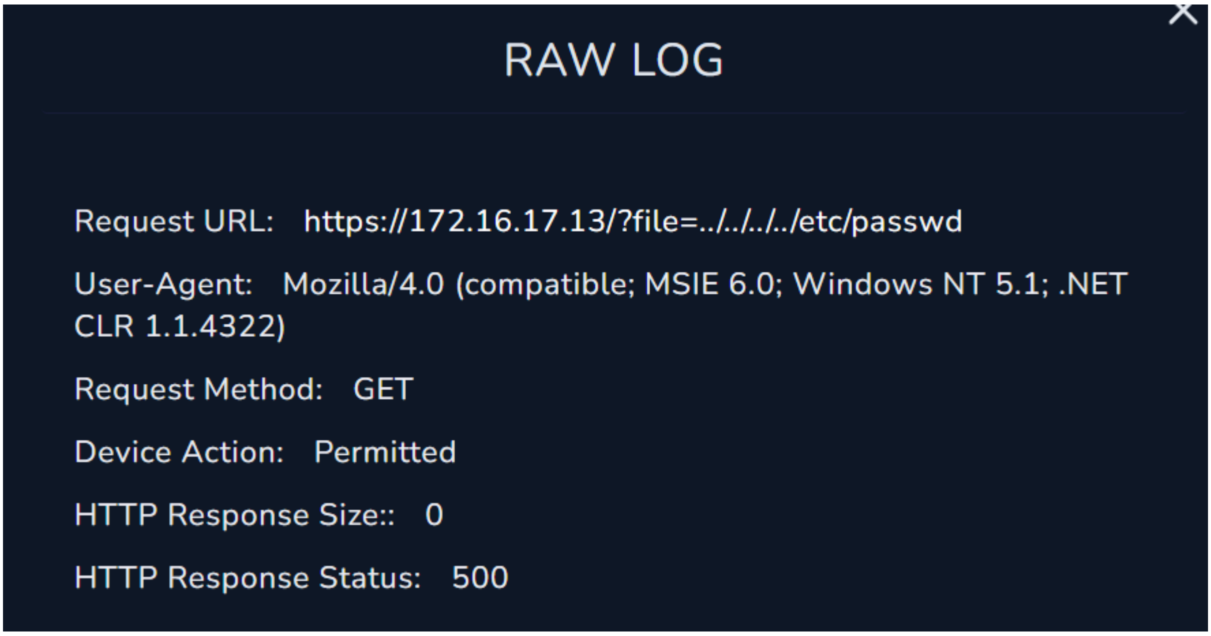
Reporter	Date	Comment	Categories
✓ antihack.anarchista.xyz	07 Dec 2022	Jul 12 19:34:49 evulka sshd[15865]: Failed password for root from 106.55.45.162 port 36306 ssh2<br / ... show more	Brute-Force Web App Attack SSH
✓ ege8	29 Nov 2022		Brute-Force SSH
✓ ege8	18 Nov 2022		Brute-Force SSH
✓ ege8	08 Nov 2022		Brute-Force SSH
✓ ege8	28 Oct 2022		Brute-Force SSH
✓ antihack.anarchista.xyz	21 Oct 2022	Jul 12 19:34:49 evulka sshd[15865]: Failed password for root from 106.55.45.162 port 36306 ssh2<br / ... show more	Brute-Force Web App Attack SSH
✓ ege8	05 Oct 2022		Brute-Force SSH
✓	26 Sep 2022	Jul 12 19:34:49 evulka sshd[1586	Brute-Force

From this result, we can see this ip address used for several malicious activities.

Now we can look into the log management,



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 01, 2022, 10:10 AM	Firewall	106.55.45.162	49028	172.16.17.13	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)

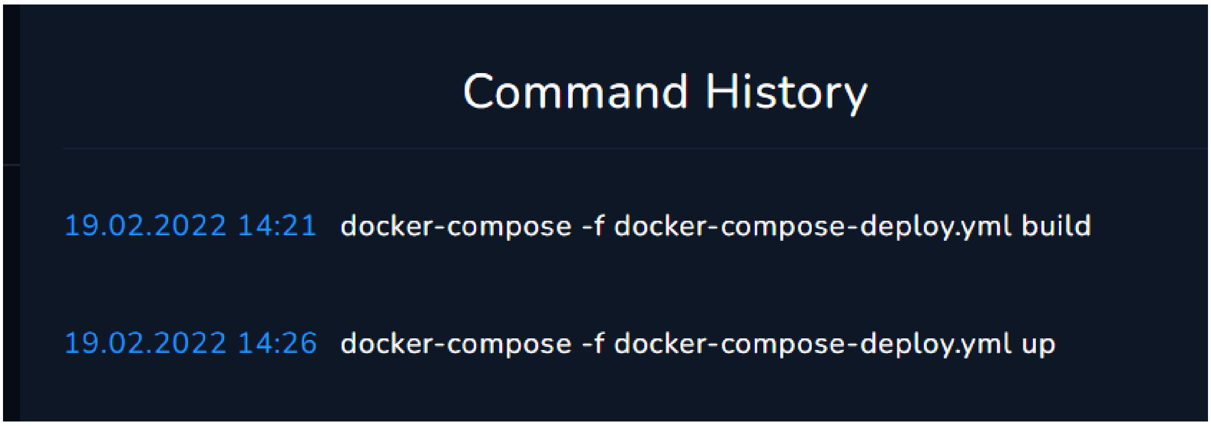
Request Method: GET

Device Action: Permitted

HTTP Response Size:: 0

HTTP Response Status: 500

Only one request was made by the attacker, and the request was responded with HTTP Response Status 500 (internal server Error) and Response Size with 0. Also no suspicious command.



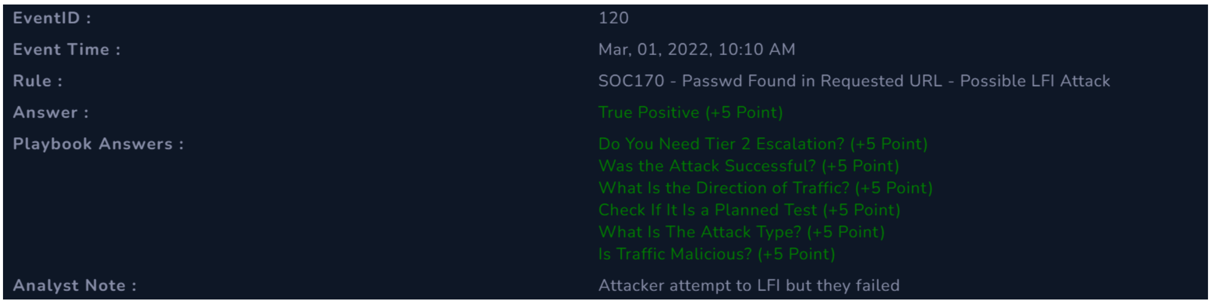
Command History

```
19.02.2022 14:21  docker-compose -f docker-compose-deploy.yml build

19.02.2022 14:26  docker-compose -f docker-compose-deploy.yml up
```

From this information, we can say that the attack attempt was unsuccessful .

PlayBook Answers:



EventID :	120
Event Time :	Mar, 01, 2022, 10:10 AM
Rule :	SOC170 - Passwd Found in Requested URL - Possible LFI Attack
Answer :	True Positive (+5 Point)
Playbook Answers :	Do You Need Tier 2 Escalation? (+5 Point) Was the Attack Successful? (+5 Point) What Is the Direction of Traffic? (+5 Point) Check If It Is a Planned Test (+5 Point) What Is The Attack Type? (+5 Point) Is Traffic Malicious? (+5 Point)
Analyst Note :	Attacker attempt to LFI but they failed

- No need to Tier 2 Escalation
- The attack Unsuccessful
- The Direction of Traffic : internet to company network
- Not a Planned Test
- Local File Inclusion
- Malicious Traffic