What is IDOR?

- Insecure Direct Object Reference (IDOR) is a type of vulnerability that occurs when a user is able to access or modify resources that they are not authorised to access. vulnerabilities can be exploited to gain unauthorised access to sensitive information, such as user accounts, financial records.

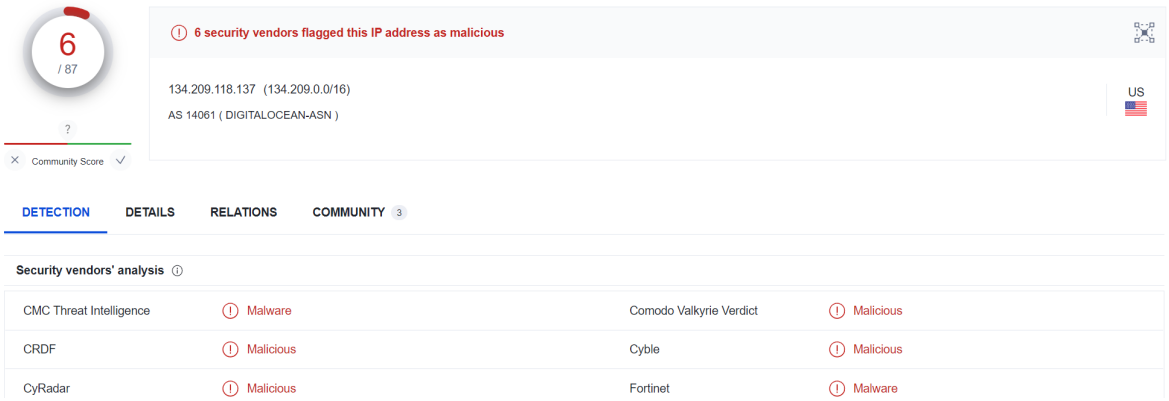
How to detect IDOR?

- If an application has a URL structure like this:
    - https://www.example.com/view_orders?id=12345
- An attacker could try changing the ‘id’ parameter to a different value, such as “id = 12346” and see if the application does not properly check the user’s authorization to view the order information, this could indicate an IDOR vulnerability.

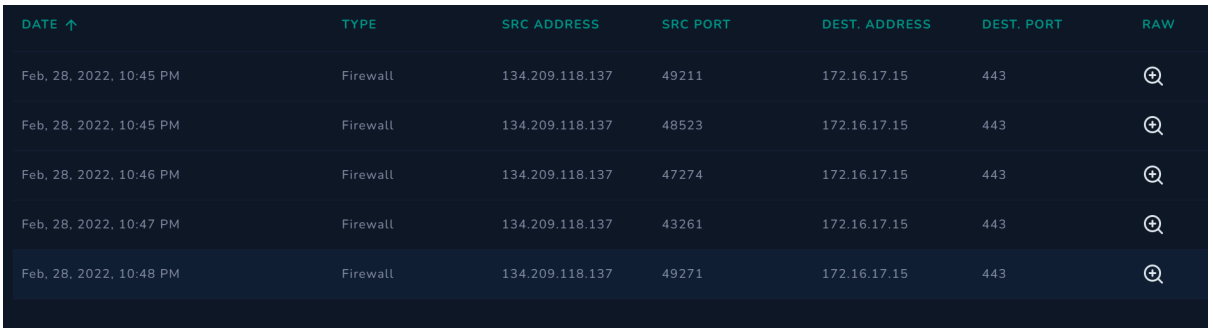
SOC169 - Possible IDOR Attack Detected:

- Source IP address: 134.209.118.137
- Destination IP Address: 172.16.17.15
- Requested URL: https://172.16.17.15/get_user_info/

I have done an investigation on 134.209.118.137 using VirusTotal, Cisco Talos and IBM xForce. There is a high rate of suspicious activities given by VirusTotal compared to others. This can be malicious traffic.

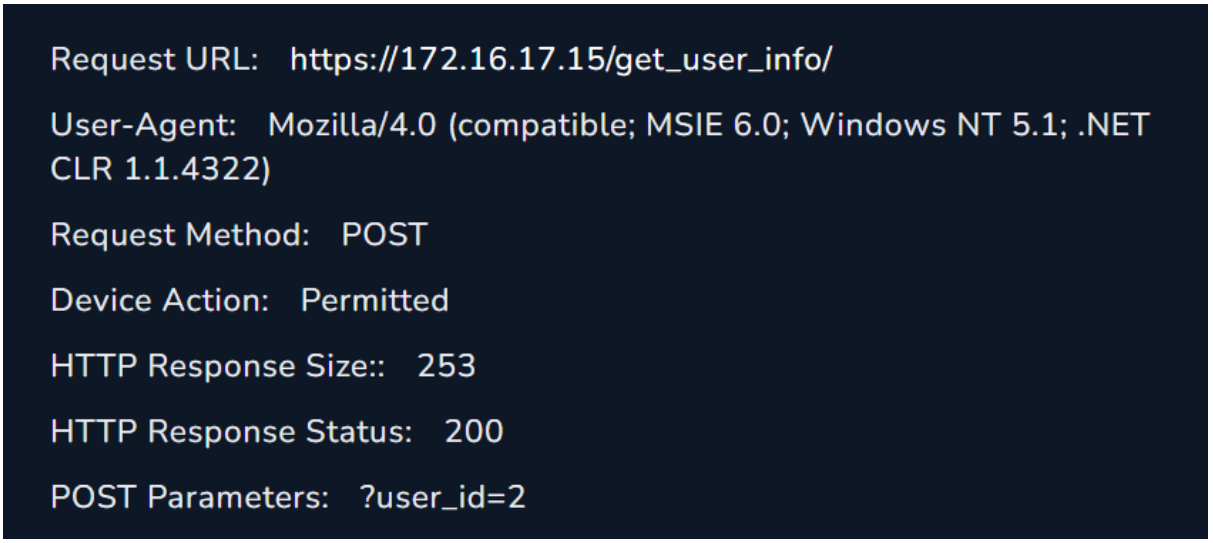


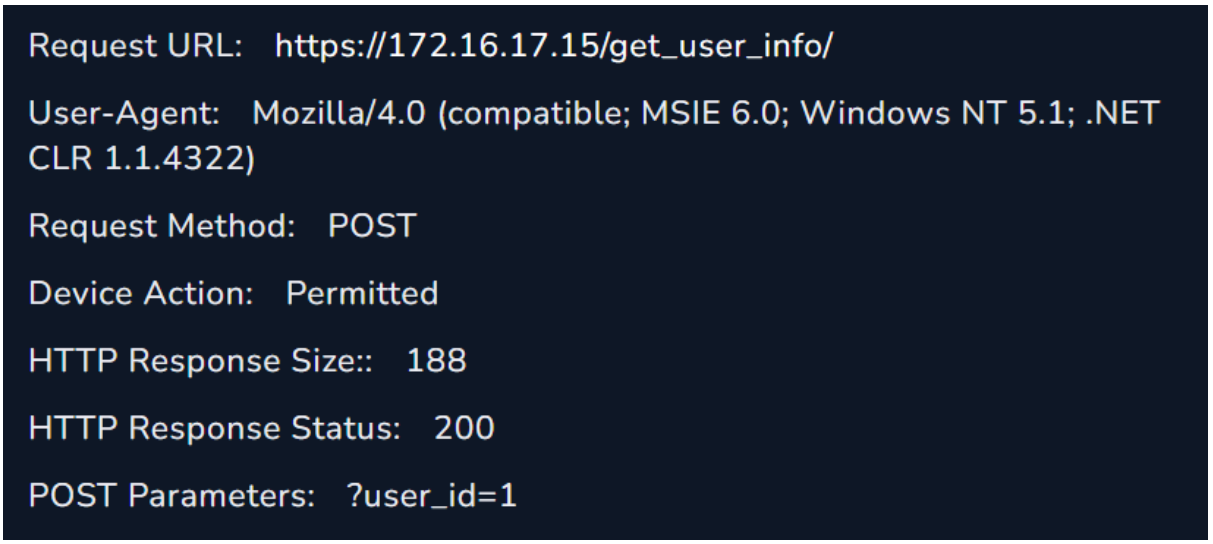
I looked into Log management for what are the activities made by this IP address (134.209.118.137).



DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 28, 2022, 10:45 PM	Firewall	134.209.118.137	49211	172.16.17.15	443	
Feb, 28, 2022, 10:45 PM	Firewall	134.209.118.137	48523	172.16.17.15	443	
Feb, 28, 2022, 10:46 PM	Firewall	134.209.118.137	47274	172.16.17.15	443	
Feb, 28, 2022, 10:47 PM	Firewall	134.209.118.137	43261	172.16.17.15	443	
Feb, 28, 2022, 10:48 PM	Firewall	134.209.118.137	49271	172.16.17.15	443	

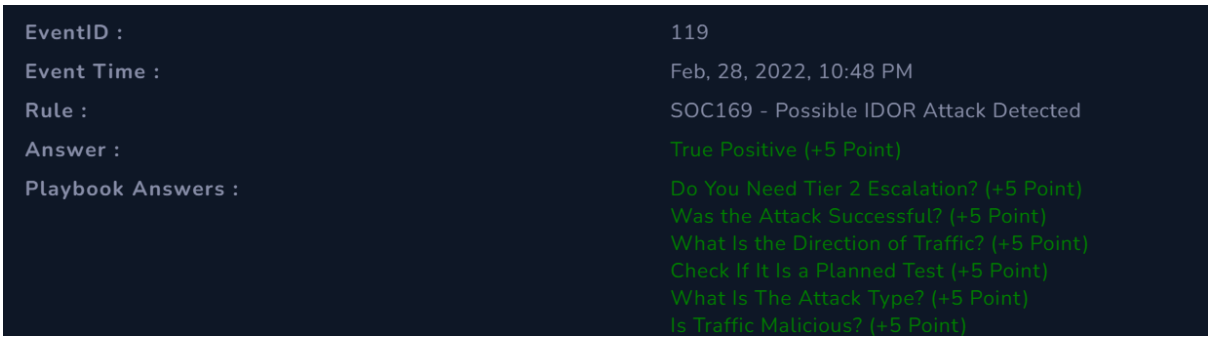
Here we can clearly see there are several requests asked by the attacker to the webserver1005. Attacker perform IDOR attacks by changing the “id” value from 1 to 5. To get the information about the user.





The attacker successfully got the information of another User by using the IDOR attack. We can say that by changes in HTTP Response size and also each request has HTTP Status 200 (OK).

Playbook answers:



- Yes, we need Tier 2 Escalation.
- The attack was successful
- The Direction of Traffic : internet to company network
- There is no information about Test. so, it was not a Planned Test
- Insecure Directory Object Reference (IDOR)
- Malicious Traffic