What is Command Injection?

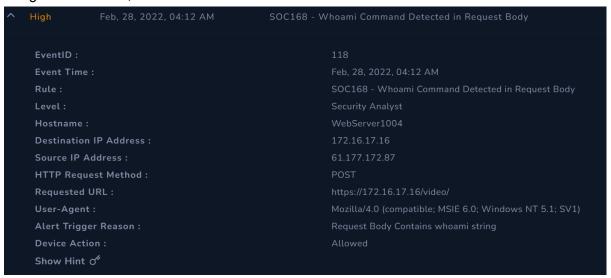
- Command injection is a type of vulnerability that allows an attacker to execute arbitrary commands on the host operating system via a vulnerable application.
- This can occur when an application passes unsafe user supplied data (e.g. form input) to a system shell without proper validation or sanitization.
- An attacker can use command injection to gain unauthorised access to sensitive data, execute malicious code or disrupt the intended functionality of the application.

How to detect command injection?

- One way to detect command injection vulnerabilities in a web application is to search the source code for keywords that may indicate the use of system commands with unsanitized user input
- Some keywords to look for include:
 - o "Whois", "dir", "ls", "cp", "cat", "type"
 - o "System", "etc", "exec", "shell_exec"
 - o "Whoami"

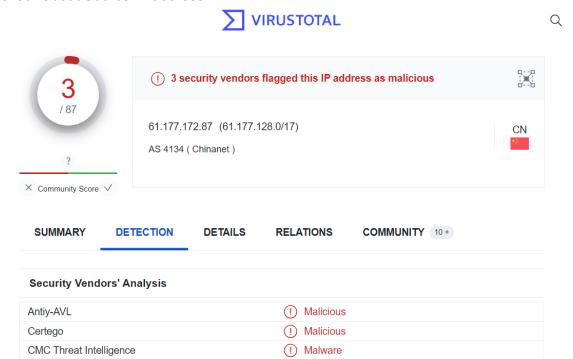
SOC168 - Whoami Command Detected in Request Body

Here is the generated alert,



- Source IP address (61.177.172.87) attempted "Whoami" command injection attack on Web server 1004 (172.16.17.16).
- Request URL: https://172.16.17.16/video/

Let's check about Source IP address:



This IP address was flagged as malicious. Also attackers make lots of attacks by using this IP address.



Lets, look into the Log Management

DATE	ТҮРЕ	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb. 28, 2022, 04:12 AM						€
Feb. 28, 2022, 04:11 AM						€
Feb. 28, 2022, 04:13 AM						€
Feb, 28, 2022, 04:14 AM						€
Feb, 28, 2022, 04:15 AM						⊕

- There are several command injection ware made by this attacker(61.177.172.87).
- All attempts are responded with 200 HTTP Status with different HTTP response sizes.
- We are able to see that all the command injections made by the attacker were executed. By checking the command line History on web server 1004

28.02.2022 04:11 ls

28.02.2022 04:12 whoami

28.02.2022 04:13 uname

28.02.2022 04:14 cat /etc/passwd

28.02.2022 04:17 cat /etc/shadow

Playbook Answers:



- Yes, we need Tier 2 Escalation
- The Attack was successful
- The Direction of Traffic : Internet to company network
- NO, this is not a Planned Test
- This is Command injection attack
- It is a Malicious Traffic