**SOC168 - Whoami Command Detected in Request Body**

**Incident Report: Command Injection Attack Detected**

**Event Overview**

A screenshot of a computer program

Description automatically generated

**Event ID:** 118  
**Detection Rule:** [SOC168 - Whoami Command Detected in Request Body]  
**Timestamp:** February 28, 2022, Multiple Events Between 01:11 AM - 01:15 AM

**Event Summary**

A potential **Command Injection Attack** was detected targeting the URL https://172.16.17.16/video/. Multiple HTTP POST requests were observed, each containing potentially malicious parameters designed to execute system-level commands on the target server. The firewall logged these activities as permitted, with HTTP response status codes of 200, indicating successful processing of the requests.

**Incident Details**

**Detected Commands**

Below is a summary of the observed requests:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Timestamp** | **Source Address** | **Command (POST Parameter)** | **HTTP Response Size** | **Response Status** |
| 01:11 AM | 61.177.172.87 | ?c=ls | 1021 | 200 |
| 01:12 AM | 61.177.172.87 | ?c=whoami | 912 | 200 |
| 01:13 AM | 61.177.172.87 | ?c=uname | 910 | 200 |
| 01:14 AM | 61.177.172.87 | ?c=cat /etc/passwd | 1321 | 200 |
| 01:15 AM | 61.177.172.87 | ?c=cat /etc/shadow | 1501 | 200 |

**Attack Analysis**

The detected commands suggest an attempt to:

1. Enumerate files and directories (ls).
2. Identify the current user (whoami).
3. Check the operating system and kernel information (uname).
4. Access sensitive system files such as:
   * **/etc/passwd**: A file containing user account information.
   * **/etc/shadow**: A file containing hashed passwords, which is highly sensitive.

The consistent 200 response codes and non-trivial response sizes imply that the commands were likely executed successfully, returning valuable information to the attacker.

A screenshot of a computer

Description automatically generated

**Observed Indicators of Compromise (IoCs)**

|  |  |
| --- | --- |
| **Indicator** | **Value** |
| **Source Address** | 61.177.172.87(Malicious IP) |
| **Destination Address** | 172.16.17.16 |
| **Destination Port** | 443 (HTTPS) |
| **Device Action** | Permitted |

VirusTotal result when I ran the malicious IP

A screenshot of a computer

Description automatically generated

**Impact**

If successful, the attack would expose critical system information:

* **Usernames and system users** via /etc/passwd.
* **Password hashes** via /etc/shadow, which could lead to brute force or password-cracking attempts.
* **System reconnaissance** data from whoami, uname, and ls, aiding further exploitation.

**Recommendations**

1. **Immediate Actions:**
   * Block the source IP 61.177.172.87 to prevent further malicious activity.
   * Review and sanitize input handling mechanisms in the application to mitigate command injection vulnerabilities.
2. **Long-Term Mitigation:**
   * Implement Web Application Firewalls (WAF) with rules to detect and block malicious commands in HTTP parameters.
   * Use parameterized queries or input validation to prevent arbitrary command execution.
   * Audit server logs for unauthorized access or tampering.
3. **Incident Response:**
   * Investigate whether sensitive data was accessed or exfiltrated.
   * Identify other potential vulnerabilities in the system.
   * Patch and update the web application framework and dependencies to fix security flaws.

**MITRE ATT&CK Mapping**

* **Tactic:** Execution
* **Technique:** Command and Scripting Interpreter (T1059)

**References**

1. MITRE ATT&CK Framework. *Command and Scripting Interpreter (T1059)*. Available at: https://attack.mitre.org/
2. Cisco Talos Intelligence. *Threat Intelligence Platform*. Available at: <https://talosintelligence.com/>
3. SANS Institute. *Incident Handling and Response*. Available at: <https://www.sans.org/>
4. Let's Defend. *SOC168 - Whoami Command Detected Lab*. Available at: <https://letsdefend.io/>