Client Interview:

What issues are you having?

We are having some funky stuff happening with an employee's computer, it was reported that processes not recognized were appearing. Boss was worried about our data being compromised.

Were any other devices affected?

Just that computer was affected that we know of. Data may have been pulled or other users might be compromised.

What software is the computer running?

It is a dev computer and runs webserver and apache.

How long have these issues been occurring?

This issue happened around 2 weeks ago.

What is the affected computer built on?

Ubuntu is the OS on the computer

Do you have a list of known users?

We do not have a list of known users. Only 2 users on the system would be root being the Boss or myself with the employee user.

Have you opened any ports?

Webserver port, sql database, SSH.

Memory Analysis:

At the beginning of the linux\_bash command execution of cow.bin was run. Analysis of this process only revealed its use in error.log for what is believed to have been a password rewrite

Suspicious processes PiMPz and SnwjT were found, they have PID 4544 and 13311. Finding these processes in linux\_psenv they have APACHE\_RUN\_DIR and utilize user www-data indicating the commands in bash\_history that use su www-data are linked to these processes.

Process lampiao.sh while initially does not have any suspicious commands run with it, upon researching this process it was discovered to be potentially linked to a capture the flag program with the goal of getting the root shell.

In linux\_pslist there are multiple sh processes running utilizing a PPID that belongs to PiMPz.

revshell7777.bin was found to be utilized 3 times in linux\_bash this being a reverse shell proves its been installed on the system, two times it was used in rm between those commands suspicious commands were run `which printf` was run 10 times each time with a different string that followed a pattern of "\10\0..."

The third time revshell7777.bin was used it was used in mv to /usr/sbin/updatephp

At the end of linux\_bash logkeys.log was found to have been executed, research shows this is a keylogger program which has been installed and run on the machine.

While searching through linux\_netstat both PiMPz and SnwJT were found to establish TCP port connections, 35551 and 4433 used for both processes, with what appears to be receiving ports indicating the system's network was hijacked to route traffic through a minitored interface

2 users were found to be used in linux\_bash tiago and benji. benji is only found once and in a less command for the user's .bash\_history ran in 2018 while taigo was switched to mutiple times but in the year 2020. It is possible that the date has been modified for these commands to create the belief benji is the susporcious user since tiago has user ID 1000.

In the 2018 commands lampiao.sh was run which through research is a rootkit installed on the system. When researching lampiao the sites that contained the program were all authored by tiago which further provides evidence that was the suspicious user. This program's goal from research is to get the root shell thus confirming that it should not be on the system.

Filesystem Analysis:

Though obtaining users with mysql it was found the 2 main users are benji and tiago.

tiago has user ID 1000 indicating it was created first while benji has ID 1001.

When pulling data related to lampiao it was shown that all files were accessed in 2018, this year is suspicious as its the only program to have been accessed at this time while everything else was in 2020.

At the begining of the command timeline it was shown that the initial user used was benji then root and lastly tiago.

Through error.log at the start t.php was attempted to be created then suddenly there are errors for commands in t.php showing it was attempted to have been run.

In this log the majority of commands were run in 2018 whic includes the SIGTERM errors returned.

After php-reverse-shell.php was saved these following commands were run

rm: cannot remove '/tmp/f': Operation not permitted

mkfifo: cannot create fifo '/tmp/f': File exists

sh: 1: cannot create /tmp/f: Permission denied

rm: cannot remove '/tmp/f': Operation not permitted

mkfifo: cannot create fifo '/tmp/f': File exists

sh: 1: cannot create /tmp/f: Permission denied

rm: cannot remove '/tmp/f': Operation not permitted

mkfifo: cannot create fifo '/tmp/f': File exists

sh: 1: cannot create /tmp/f: Permission denied

until a port connection succeeded on 1234.

Once the SIGTERM errors no longer appear there are multiple client denied by server config errors printed out.

towards the end of commands in error.log

PHP Notice: Use of undefined constant

was returned suggesting another .php file was executed which leads into errors for a cow.c program that ends the file with

Running ...

Received su prompt (Password: )

Root password is: dirtyCowFun

Enjoy! :-)

this return suggests that the root password was either adjusted or compromised.

With access.log there are again multiple suspicous executions in 2018 mainly a POST commands for intall.php

The multitude of GET commands run in 2018 suggest a copying of all or most of the files from the webserver.

For a POST command run in the access log there is a webaddress which provides sql scipting for password cracking using a dictionary attack format.

Scenario:

1. rootkit

Yes, PiMPz and SnwjT are rootkits installed on the system with PID's 4544 and 13311 respectively.

lampiao.sh is believed to be another rootkit installed on the system with the goal to get the root shell this process was found in the bash\_history for the system it has PID 294

2. keylogger

Yes, logkeys.log is a keylogger installed on the system this process was found in the bash\_history for the system.

3. reverse shell

Yes, revshell7777.bin is a reverse shell installed on the system this process was found in the bash\_history for the system.

4. ext4 extended attributes

Through running and discovering out of sequence inodes it reveals a number of them but fails to reveal much to prove information is being exfiltrated or an attempt to re-compromise the system on startup is happening.

5. New account with root privileges created

Through the client interview there should only be one user and the root access, upon inspection of users through MySQL there are 2 users, benji and tiago.

With tiago having user ID 1000 indicating tiago is supposed to be the primary user but though program research its possible tiago is the author of multiple malicious files found on the system while also tiago's last login being in 2018 a drastic change from a majority of commands being used in 2020.

Both users have read and write permissions indicating a suspicious user with elevated access.

6. Existing system account was modified to allow interactive logins

3 failed login attempts were found from an unkown account.

When searching the successful logins there were mutliple logins from benji and one from a proxy which is unidentified.

The majority of these logins occured from the ip 192.168.56.1

According to bash histories at some point someone used su to become tiago and showed the contents of both /etc/shadow and /etc/passwd through a "cat" command.

The SSH service was restarted.

7. Network was hijacked

netstat shows PiMPz and SnwJT processes have established connections with routing ports 35551 and 4433, which leads me to believe the network was hijacked to route traffic through a monitored interface.

Both these processes failed to show up in SQL file metadata suggesting they have since been removed or are a network service.

Multiple TCP connections from IP 192.168.56.104:59420 to 192.168.56.1:7777 suggest data was being moved over these ports as their connection was established to either python or bash

8. Software that supports file exfiltration or attack obfuscation

After finding the purpose for previously mentioned processes there were no other suspicious processes installed on the sytem that would support file exfiltration or attack obfuscation.

9. Suspicious volumes mounted

Searching mounted volumes using its volatility command there does not appear to be any suspicious volumns on the target system based on the output behaviour of the mount volatility command output.

10. kernel contains trojaned modules

Searching linux\_lsmod there are no suspicious loaded kernel modules in the target system.

None of the listed modules appeared to have any strange output are any strange parameters pasted into any of these modules.

11. Existing executable files replaced with malware versions

With command timeline revshell7777.bin was moved into updatephp directory under sbin thus overwriting it.

update-php was also accessed at the same time right before user directories and bash\_history was accessed.

This indicates a possiblity of the executable update-php was replaced with a malware version in this time frame.

12. Dictionary attack was performed

A user had looked into the contents of /etc/passwd and /etc/shadow to reveal user information on the system.

When analyzing the access.log there were multiple commands to access data on the system with a link to a known mysql dictionary attack program to attempt a password crack "http://sqlmap.org/".

13. A shared credential attack was performed

The output of the check\_fop volatility command returns nothing, thus there does not appear to have been a shared credential attack.

14. Network card has been put into promiscuous mode

ifconfig has returned that there are no network cards in promiscuous mode.

Interfaces "lo" and "eth0" have "False" for promiscuous mode, proving neither were put into promiscuous mode.

Recommendations to prevent future attacks:

It was determined there was a brute force login using sqlmap.

To prevent this type of compromise in the future it is recommended that you:

* Urgent: Require employees to update passwords to be stronger.
* Time out IP addresses.
* Install Snort or another intrusion detection system.
* Review Apache and MySQL logs periodically.
* Block MySQL key words like ‘;’ or ‘UNION’ from being passed into the webserver
* Educate employees on system security to protect their devices.