Hands On Lab: Unit 10

MICS-252, Fall 2024

Incident Response Linux

Prepared by: Karl-Johan Westhoff

email: kjwesthoff@berkeley.edu

UC Berkeley School of Information

MICS Course 252 Fall 2024 (Kristy Westphal)

1 Introduction

We are given a snapshot of some files from a Linux host which has been compromised.

2 Process

2.1 Open source information

Linux version 7.1 is mentioned, assuming this means the Red Hat Distribution 7.1, code named "Seawolf", released in 2001 [1]

2.2 Look at the files

It looks like we were issued the contents of Linux system 'var' folder (or parts thereof). In Linux the /var folder contains variable data files. This includes spool directories and files, administrative and logging data, and transient and temporary files [2]. Folder content is show in 1 the most interesting folder are the 'tmp' folder holding temporary files and of course the log folder (as hinted in the assignment)

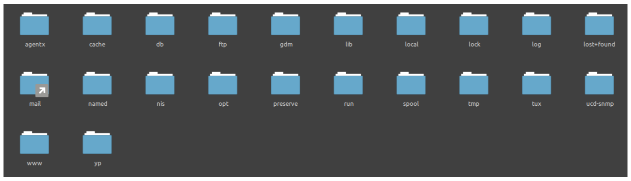

Figure 1: *We are given the 'var' folder from a compromised Linux host*

The 'tmp' folder is empty so focusing on the log folder going forwards.

References

[1] Wikipedia contributors. *Red Hat Linux — Wikipedia, The Free Encyclopedia*. `https://en.wikipedia.org/w/index.php?title=Red_Hat_Linux&oldid=1240829700`. [Online; accessed 27-October-2024]. 2024.

[2] The Linux foundation. *Chapter 5. The /var Hierarchy Linux foundation*. `https://refspecs.linuxfoundation.org/FHS_3.0/fhs/ch05.html`. [Online; accessed 27-October-2024].