OSSEC HIDS Project

Host-Based Intrusion Detection
Suspicious Process Execution Detection

•••

Hyukjin Jeong

Project Overview

- Install and configure OSSEC on an Ubuntu Virtual Machine
- Detect suspicious login attempts (SSH brute-force simulation)
- Detect suspicious process execution using auditd + OSSEC
- Analyze alerts generated by OSSEC to understand HIDS behavior

What is a HIDS?

- Host-Based Intrusion Detection System
- Monitors authentication logs, system files, and suspicious activities
- Generates alerts based on predefined detection rules
- Lightweight and suitable for single-host monitoring

System Architecture

- Ubuntu 25.04 (ARM) running inside VMware Fusion (macOS)
- OSSEC installed in local mode
- Monitors:

  /var/log/auth.log for authentication and login events

  Audit logs (via auditd) for suspicious process execution

- Alerts stored in : /var/ossec/logs/alerts/alerts.log

Installation Process

- After installation, verified the following process:

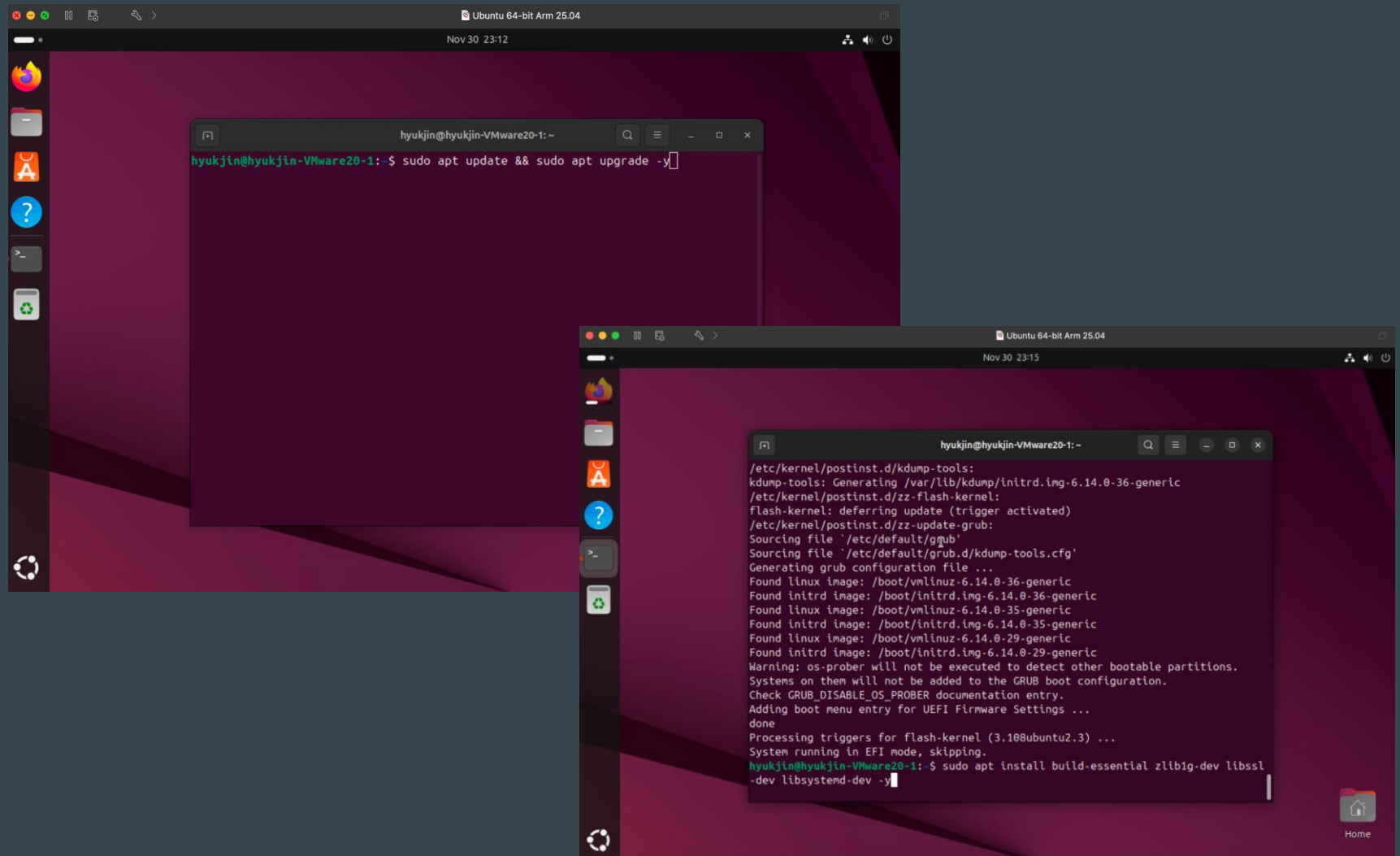
  ossec-monitord (monitoring)

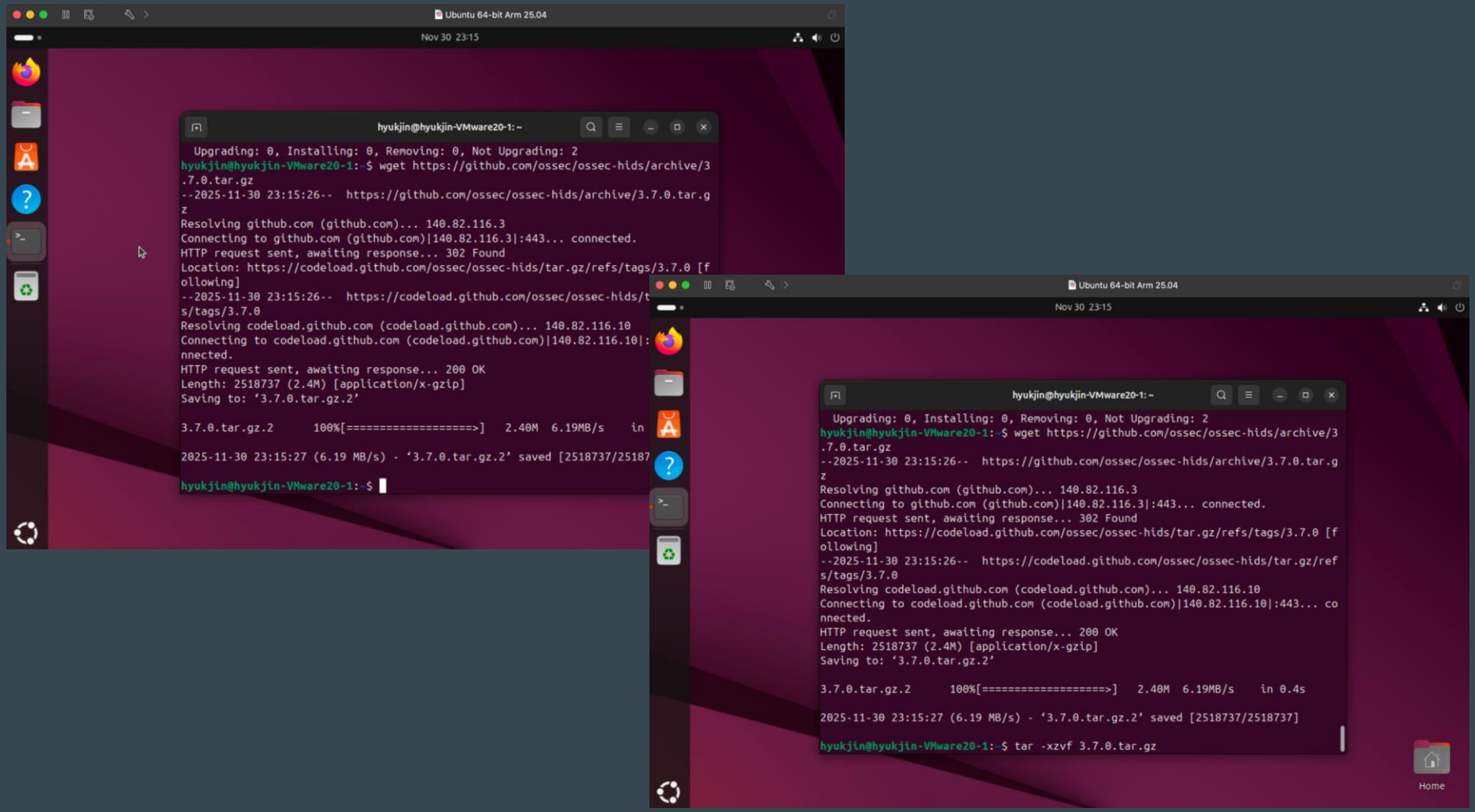
  ossec-logcollector (log watcher)

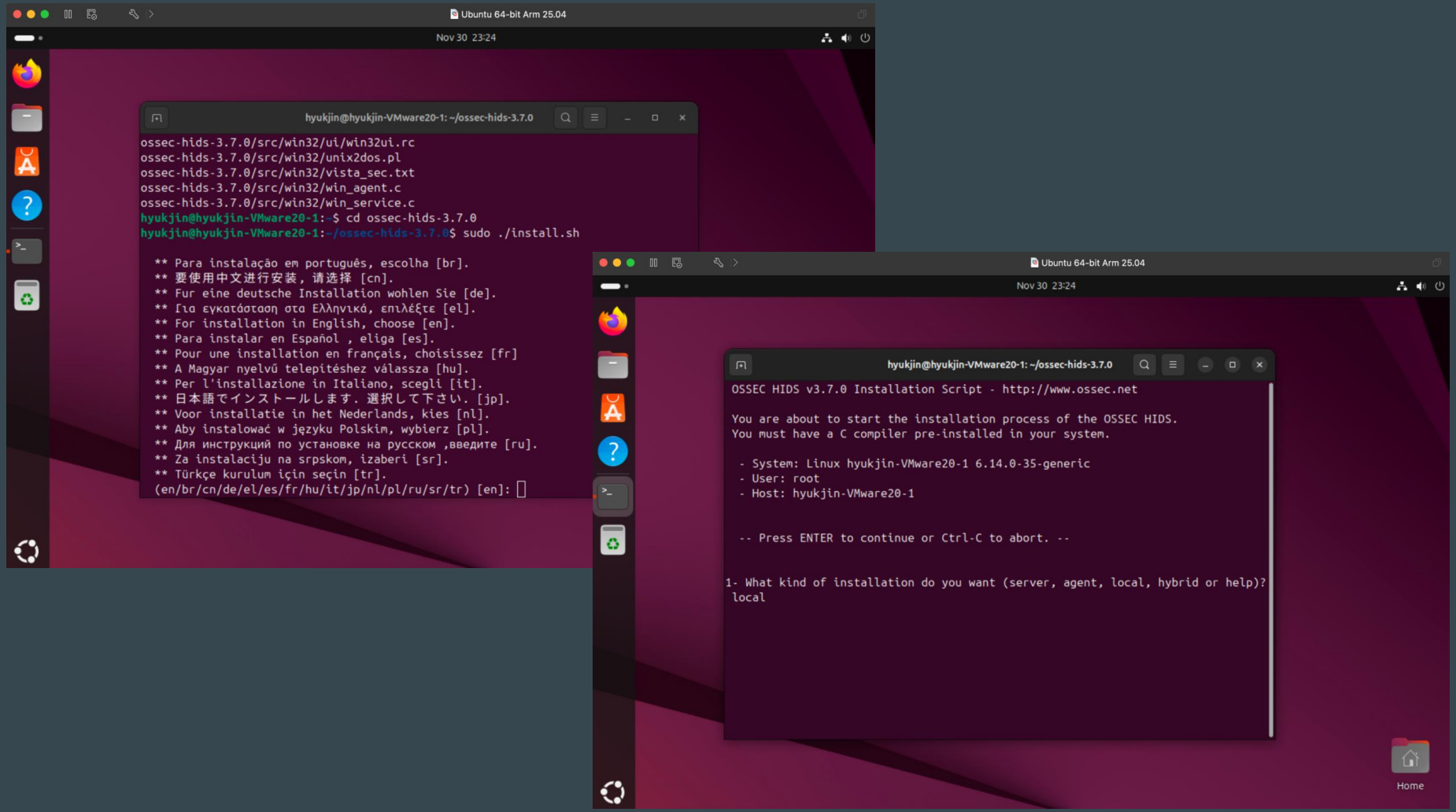
  ossec-syscheckd (file integrity)

  ossec-analysisd

  ossec-execd


Ubuntu 64-bit Arm 25.04
Nov 30 23:12
hyukjin@hyukjin-VMware20-1: ~
hyukjin@hyukjin-VMware20-1:~$ sudo apt update && sudo apt upgrade -y
Ubuntu 64-bit Arm 25.04
Nov 30 23:15
hyukjin@hyukjin-VMware20-1: ~
/etc/kernel/postinst.d/kdump-tools:
kdump-tools: Generating /var/lib/kdump/initrd.img-6.14.0-36-generic
/etc/kernel/postinst.d/zz-flash-kernel:
flash-kernel: deferring update (trigger activated)
/etc/kernel/postinst.d/zz-update-grub:
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/kdump-tools.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.14.0-36-generic
Found initrd image: /boot/initrd.img-6.14.0-36-generic
Found linux image: /boot/vmlinuz-6.14.0-35-generic
Found initrd image: /boot/initrd.img-6.14.0-35-generic
Found linux image: /boot/vmlinuz-6.14.0-29-generic
Found initrd image: /boot/initrd.img-6.14.0-29-generic
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
Processing triggers for flash-kernel (3.108ubuntu2.3) ...
System running in EFI mode, skipping.
hyukjin@hyukjin-VMware20-1:~$ sudo apt install build-essential zlib1g-dev libssl
-dev libsystemd-dev -y
Home


Ubuntu 64-bit Arm 25.04
Nov 30 23:15
hyukjin@hyukjin-VMware20-1: ~
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 2
hyukjin@hyukjin-VMware20-1:~$ wget https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz
--2025-11-30 23:15:26-- https://github.com/ossec/ossec-hids/archive/3.7.0.tar.gz
Resolving github.com (github.com)... 140.82.116.3
Connecting to github.com (github.com)|140.82.116.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/ossec/ossec-hids/tar.gz/refs/tags/3.7.0 [following]
--2025-11-30 23:15:26-- https://codeload.github.com/ossec/ossec-hids/tar.gz/refs/tags/3.7.0
Resolving codeload.github.com (codeload.github.com)... 140.82.116.10
Connecting to codeload.github.com (codeload.github.com)|140.82.116.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2518737 (2.4M) [application/x-gzip]
Saving to: '3.7.0.tar.gz.2'
3.7.0.tar.gz.2 100%[==========>] 2.40M 6.19MB/s in 0.4s
2025-11-30 23:15:27 (6.19 MB/s) - '3.7.0.tar.gz.2' saved [2518737/2518737]
hyukjin@hyukjin-VMware20-1:~$ tar -xzvf 3.7.0.tar.gz
Home


Ubuntu 64-bit Arm 25.04
Nov 30 23:24
hyukjin@hyukjin-VMware20-1: ~/ossec-hids-3.7.0
ossec-hids-3.7.0/src/win32/ui/win32ui.rc
ossec-hids-3.7.0/src/win32/unix2dos.pl
ossec-hids-3.7.0/src/win32/vista_sec.txt
ossec-hids-3.7.0/src/win32/win_agent.c
ossec-hids-3.7.0/src/win32/win_service.c
hyukjin@hyukjin-VMware20-1:~$ cd ossec-hids-3.7.0
hyukjin@hyukjin-VMware20-1:~/ossec-hids-3.7.0$ sudo ./install.sh
** Para instalação em português, escolha [br].
** 要使用中文进行安装，请选择 [cn].
** Fur eine deutsche Installation wohlen Sie [de].
** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
** For installation in English, choose [en].
** Para instalar en Español , eliga [es].
** Pour une installation en français, choisissez [fr]
** A Magyar nyelvű telepitéshez válassza [hu].
** Per l'installazione in Italiano, scegli [it].
** 日本語でインストールします. 選択して下さい. [jp].
** Voor installatie in het Nederlands, kies [nl].
** Aby instalować w języku Polskim, wybierz [pl].
** Для инструкций по установке на русском ,введите [ru].
** Za instalaciju na srpskom, izaberi [sr].
** Türkçe kurulum için seçin [tr].
(en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]:
Ubuntu 64-bit Arm 25.04
Nov 30 23:24
hyukjin@hyukjin-VMware20-1: ~/ossec-hids-3.7.0
OSSEC HIDS v3.7.0 Installation Script - http://www.ossec.net
You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
- System: Linux hyukjin-VMware20-1 6.14.0-35-generic
- User: root
- Host: hyukjin-VMware20-1
-- Press ENTER to continue or Ctrl-C to abort. --
1- What kind of installation do you want (server, agent, local, hybrid or help)?
local
Home

SSH Login Failure Detection

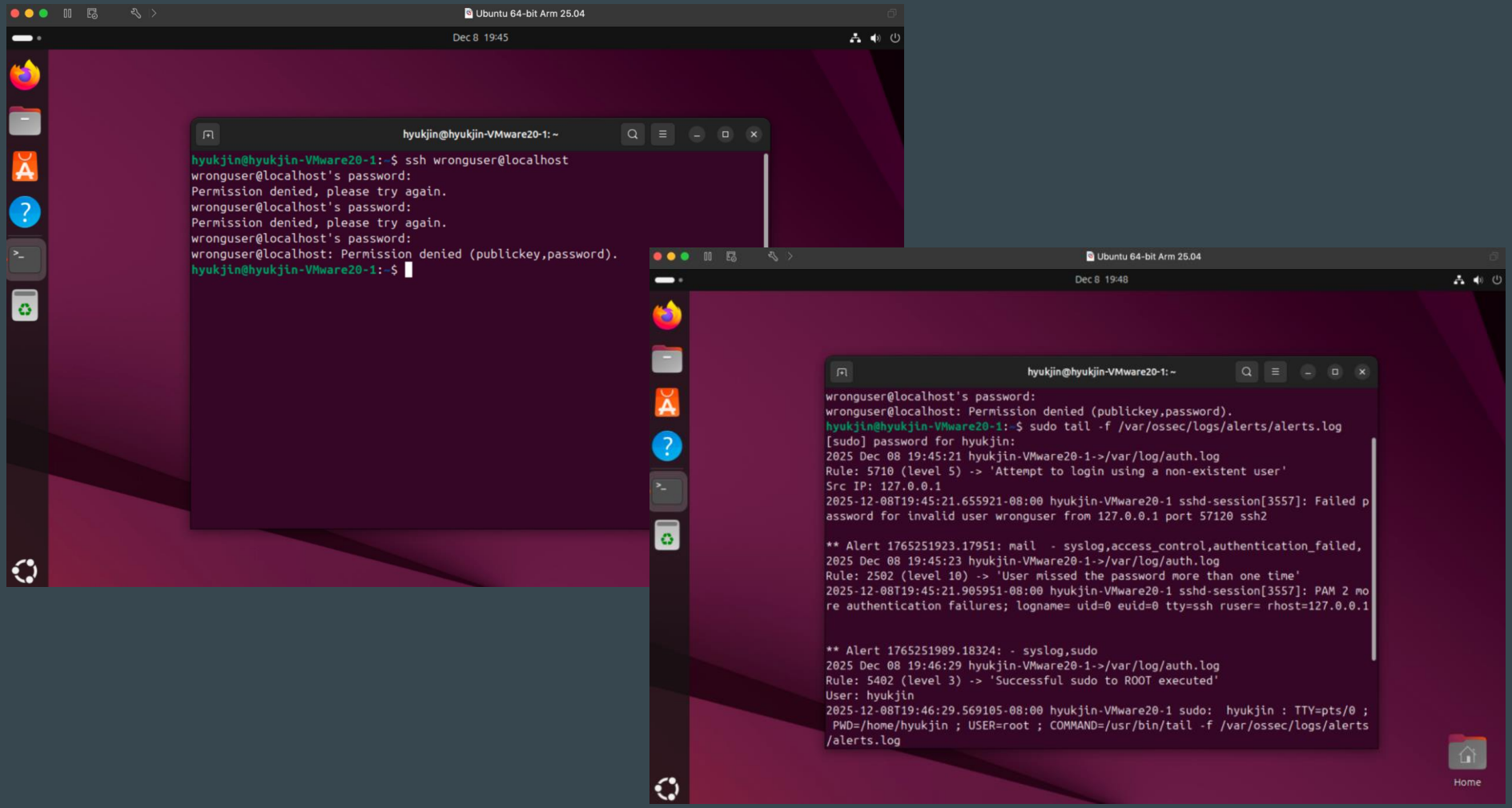
- Simulated brute-force attempts using invalid user:

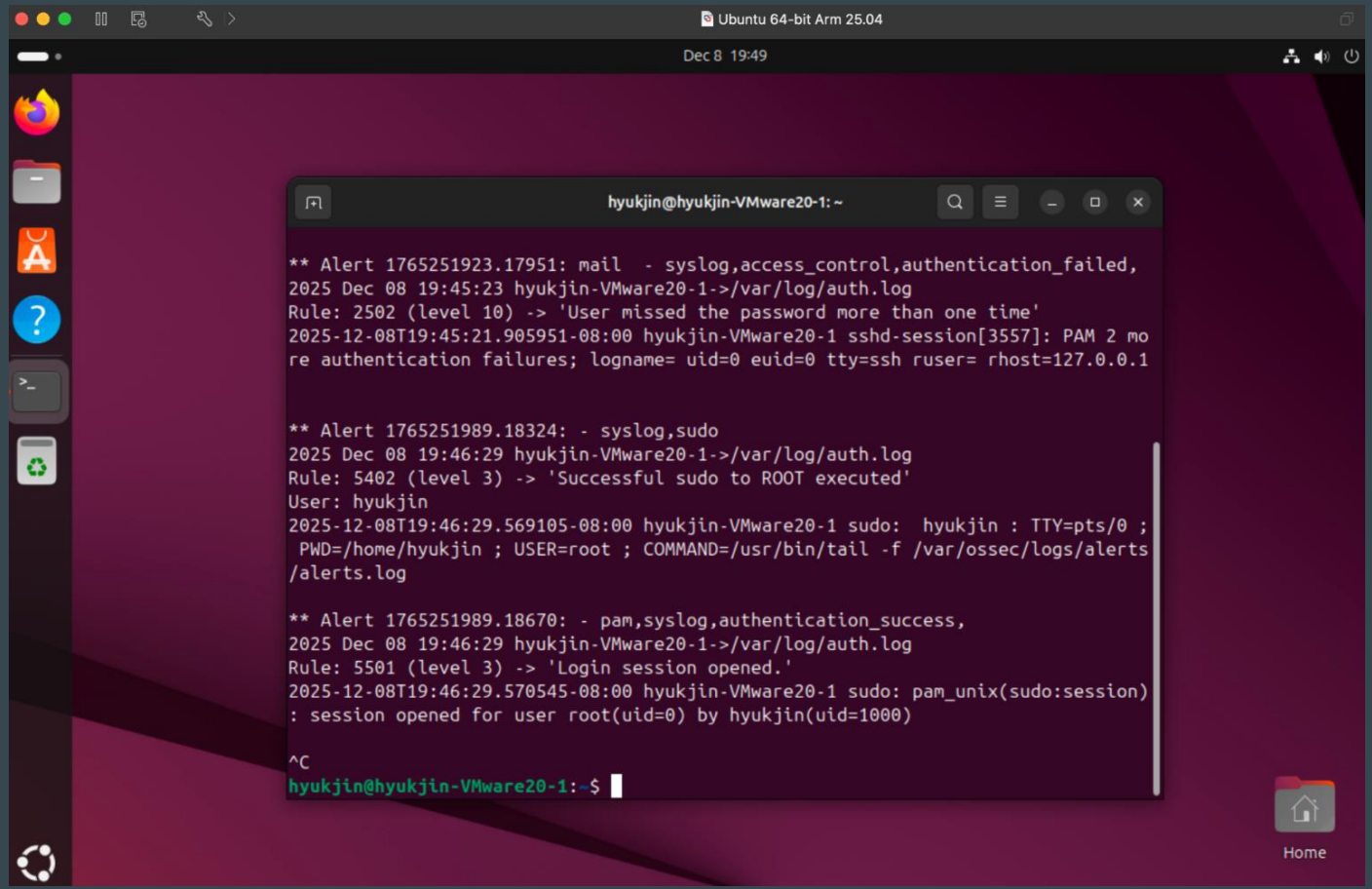
  Example: ssh wronguser@localhost

- OSSEC detected multiple failed login events, including invalid usernames and repeated authentication failures

  Example Alert:

  “Rule 5710 → Attempt to login using a non-existent user”

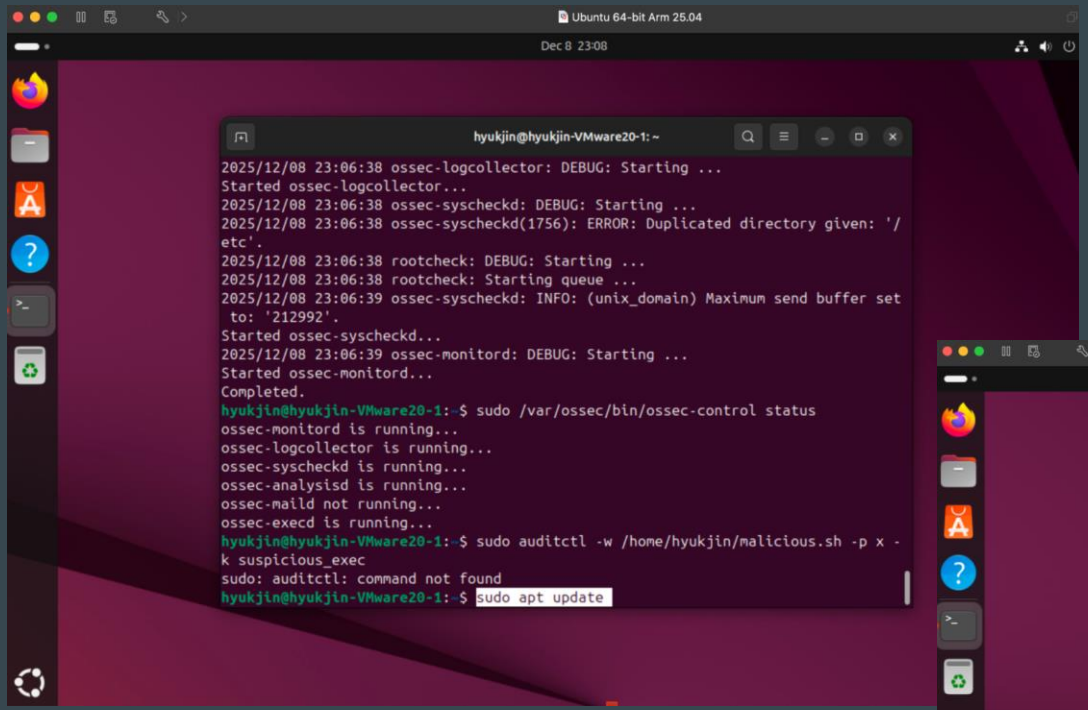

Ubuntu 64-bit Arm 25.04
Dec 8 19:45
hyukjin@hyukjin-VMware20-1: ~
hyukjin@hyukjin-VMware20-1:~$ ssh wronguser@localhost
wronguser@localhost's password:
Permission denied, please try again.
wronguser@localhost's password:
Permission denied, please try again.
wronguser@localhost's password:
wronguser@localhost: Permission denied (publickey,password).
hyukjin@hyukjin-VMware20-1:~$
Ubuntu 64-bit Arm 25.04
Dec 8 19:48
hyukjin@hyukjin-VMware20-1: ~
wronguser@localhost's password:
wronguser@localhost: Permission denied (publickey,password).
hyukjin@hyukjin-VMware20-1:~$ sudo tail -f /var/ossec/logs/alerts/alerts.log
[sudo] password for hyukjin:
2025 Dec 08 19:45:21 hyukjin-VMware20-1->/var/log/auth.log
Rule: 5710 (level 5) -> 'Attempt to login using a non-existent user'
Src IP: 127.0.0.1
2025-12-08T19:45:21.655921-08:00 hyukjin-VMware20-1 sshd-session[3557]: Failed password for invalid user wronguser from 127.0.0.1 port 57120 ssh2
** Alert 1765251923.17951: mail - syslog,access_control,authentication_failed,
2025 Dec 08 19:45:23 hyukjin-VMware20-1->/var/log/auth.log
Rule: 2502 (level 10) -> 'User missed the password more than one time'
2025-12-08T19:45:21.905951-08:00 hyukjin-VMware20-1 sshd-session[3557]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
** Alert 1765251989.18324: - syslog,sudo
2025 Dec 08 19:46:29 hyukjin-VMware20-1->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: hyukjin
2025-12-08T19:46:29.569105-08:00 hyukjin-VMware20-1 sudo: hyukjin : TTY=pts/0 ; PWD=/home/hyukjin ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.log
Home

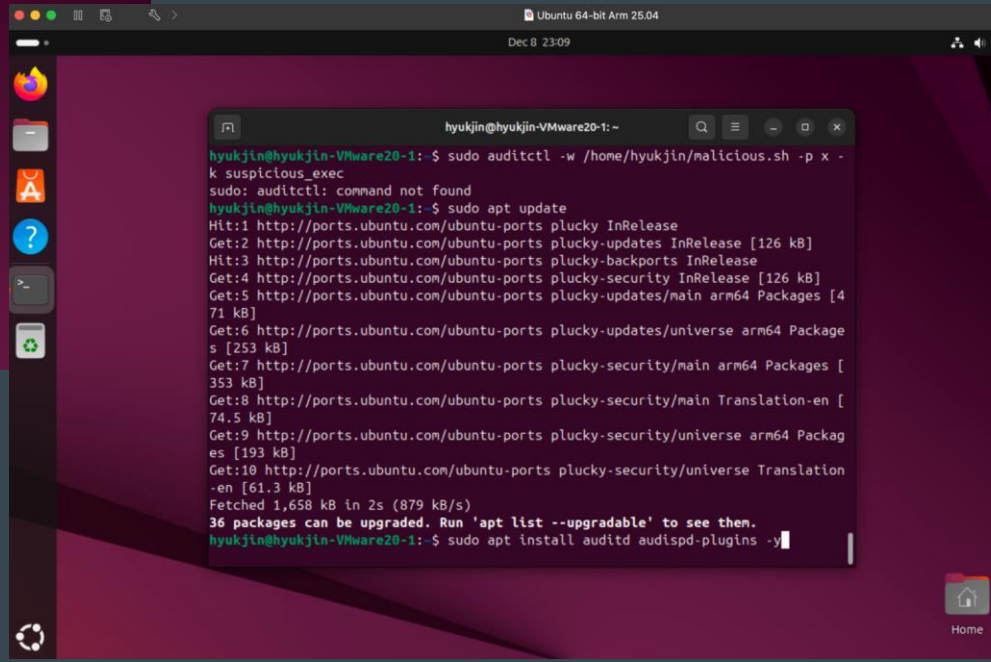

Ubuntu 64-bit Arm 25.04
Dec 8 19:49
hyukjin@hyukjin-VMware20-1: ~
** Alert 1765251923.17951: mail - syslog,access_control,authentication_failed,
2025 Dec 08 19:45:23 hyukjin-VMware20-1->/var/log/auth.log
Rule: 2502 (level 10) -> 'User missed the password more than one time'
2025-12-08T19:45:21.905951-08:00 hyukjin-VMware20-1 sshd-session[3557]: PAM 2 mo
re authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
** Alert 1765251989.18324: - syslog,sudo
2025 Dec 08 19:46:29 hyukjin-VMware20-1->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: hyukjin
2025-12-08T19:46:29.569105-08:00 hyukjin-VMware20-1 sudo: hyukjin : TTY=pts/0 ;
PWD=/home/hyukjin ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts
/alerts.log
** Alert 1765251989.18670: - pam,syslog,authentication_success,
2025 Dec 08 19:46:29 hyukjin-VMware20-1->/var/log/auth.log
Rule: 5501 (level 3) -> 'Login session opened.'
2025-12-08T19:46:29.570545-08:00 hyukjin-VMware20-1 sudo: pam_unix(sudo:session)
: session opened for user root(uid=0) by hyukjin(uid=1000)
^C
hyukjin@hyukjin-VMware20-1:~$
Home

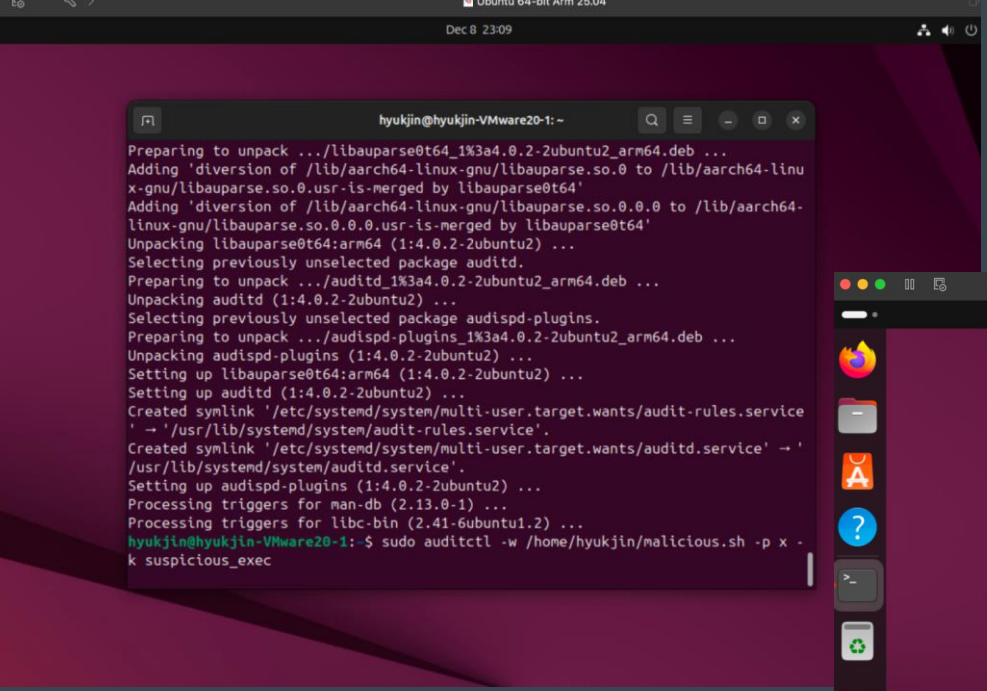
Suspicious Process Execution Detection (Auditd + OSSEC)

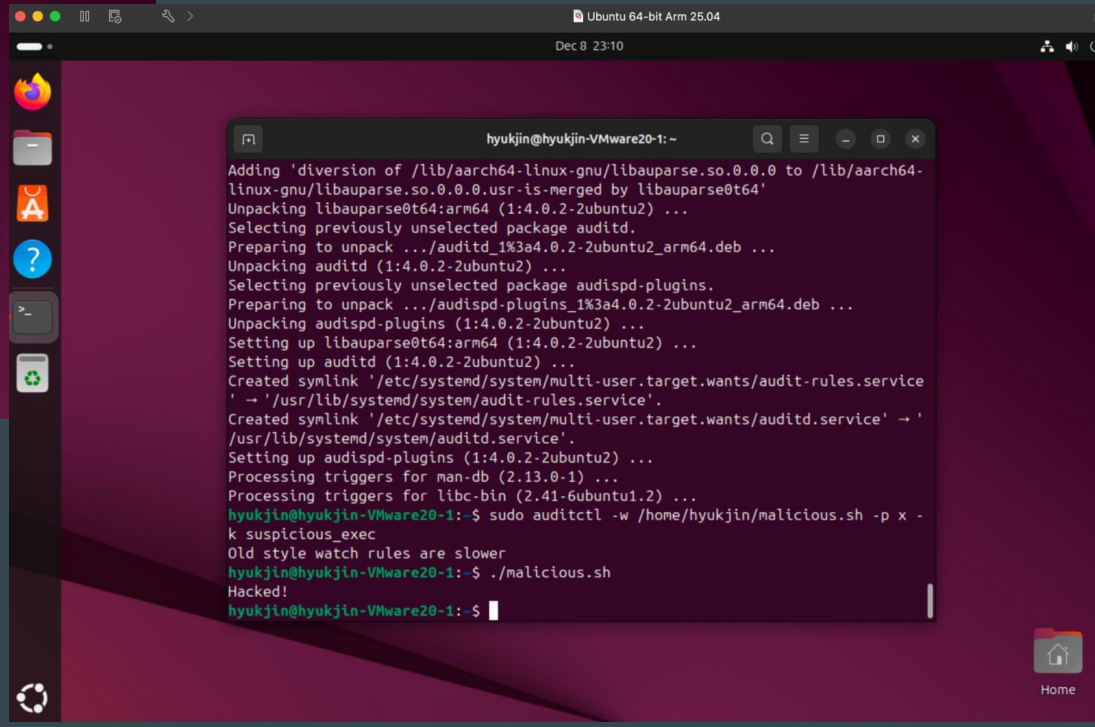
- Executed an unknown script to simulate attacker behavior
- auditd monitors process events using a watch rule
- OSSEC analyzes audit logs and applies custom rule 100100
- Expected alert:

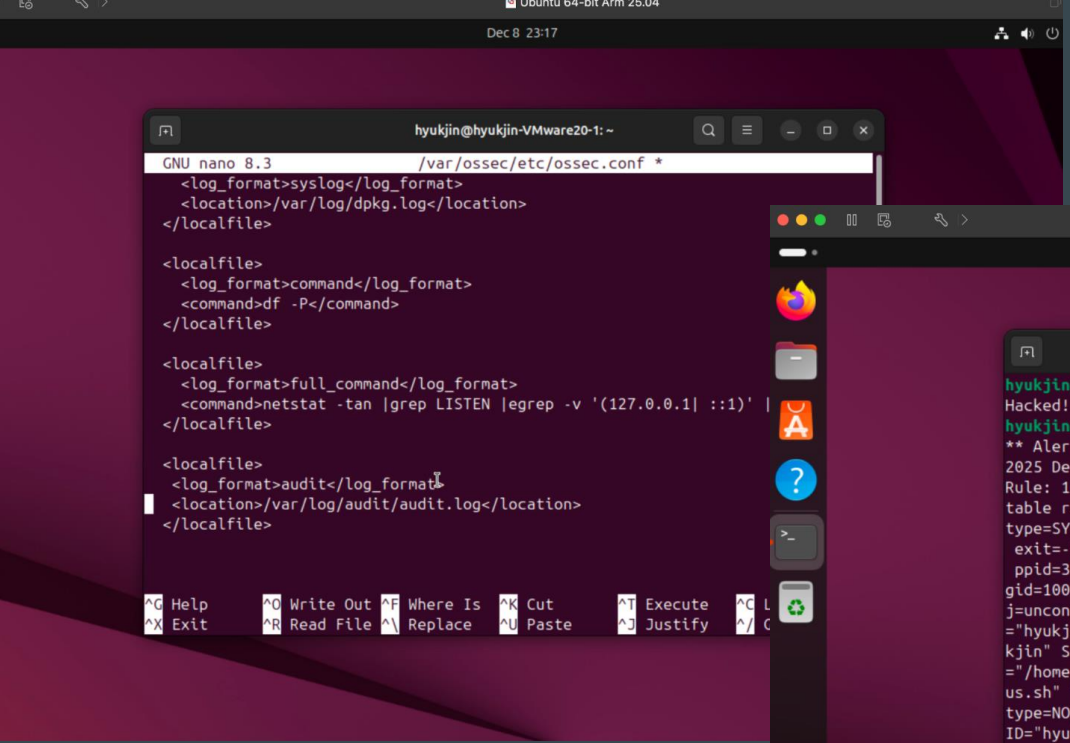
  “Rule 100100 → Suspicious process execution detected: Unknown executable ran”

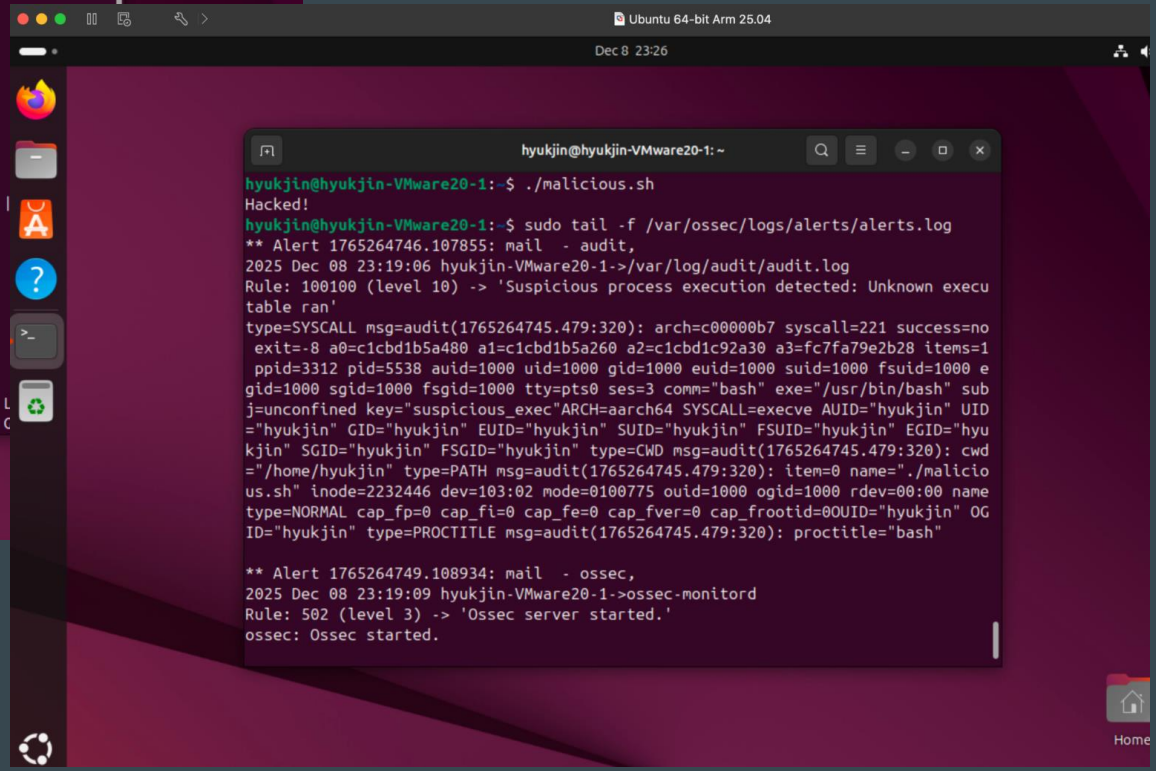

Ubuntu 64-bit Arm 25.04
Dec 8 23:08
hyukjin@hyukjin-VMware20-1: ~
2025/12/08 23:06:38 ossec-logcollector: DEBUG: Starting ...
Started ossec-logcollector...
2025/12/08 23:06:38 ossec-syscheckd: DEBUG: Starting ...
2025/12/08 23:06:38 ossec-syscheckd(1756): ERROR: Duplicated directory given: '/etc'.
2025/12/08 23:06:38 rootcheck: DEBUG: Starting ...
2025/12/08 23:06:38 rootcheck: Starting queue ...
2025/12/08 23:06:39 ossec-syscheckd: INFO: (unix_domain) Maximum send buffer set to: '212992'.
Started ossec-syscheckd...
2025/12/08 23:06:39 ossec-monitord: DEBUG: Starting ...
Started ossec-monitord...
Completed.
hyukjin@hyukjin-VMware20-1:~$ sudo /var/ossec/bin/ossec-control status
ossec-monitord is running...
ossec-logcollector is running...
ossec-syscheckd is running...
ossec-analysisd is running...
ossec-maild not running...
ossec-execd is running...
hyukjin@hyukjin-VMware20-1:~$ sudo auditctl -w /home/hyukjin/malicious.sh -p x -k suspicious_exec
sudo: auditctl: command not found
hyukjin@hyukjin-VMware20-1:~$ sudo apt update


Ubuntu 64-bit Arm 25.04
Dec 8 23:09
hyukjin@hyukjin-VMware20-1: ~
hyukjin@hyukjin-VMware20-1:~$ sudo auditctl -w /home/hyukjin/malicious.sh -p x -k suspicious_exec
sudo: auditctl: command not found
hyukjin@hyukjin-VMware20-1:~$ sudo apt update
Hit:1 http://ports.ubuntu.com/ubuntu-ports plucky InRelease
Get:2 http://ports.ubuntu.com/ubuntu-ports plucky-updates InRelease [126 kB]
Hit:3 http://ports.ubuntu.com/ubuntu-ports plucky-backports InRelease
Get:4 http://ports.ubuntu.com/ubuntu-ports plucky-security InRelease [126 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports plucky-updates/main arm64 Packages [471 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports plucky-updates/universe arm64 Packages [253 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports plucky-security/main arm64 Packages [353 kB]
Get:8 http://ports.ubuntu.com/ubuntu-ports plucky-security/main Translation-en [74.5 kB]
Get:9 http://ports.ubuntu.com/ubuntu-ports plucky-security/universe arm64 Packages [193 kB]
Get:10 http://ports.ubuntu.com/ubuntu-ports plucky-security/universe Translation-en [61.3 kB]
Fetched 1,658 kB in 2s (879 kB/s)
36 packages can be upgraded. Run 'apt list --upgradable' to see them.
hyukjin@hyukjin-VMware20-1:~$ sudo apt install auditd audispd-plugins -y
Home


Ubuntu 64-bit Arm 25.04
Dec 8 23:09
hyukjin@hyukjin-VMware20-1: ~
Preparing to unpack .../libauparse0t64_1%3a4.0.2-2ubuntu2_arm64.deb ...
Adding 'diversion of /lib/aarch64-linux-gnu/libauparse.so.0 to /lib/aarch64-linux-gnu/libauparse.so.0.usr-is-merged by libauparse0t64'
Adding 'diversion of /lib/aarch64-linux-gnu/libauparse.so.0.0.0 to /lib/aarch64-linux-gnu/libauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:arm64 (1:4.0.2-2ubuntu2) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a4.0.2-2ubuntu2_arm64.deb ...
Unpacking auditd (1:4.0.2-2ubuntu2) ...
Selecting previously unselected package audispd-plugins.
Preparing to unpack .../audispd-plugins_1%3a4.0.2-2ubuntu2_arm64.deb ...
Unpacking audispd-plugins (1:4.0.2-2ubuntu2) ...
Setting up libauparse0t64:arm64 (1:4.0.2-2ubuntu2) ...
Setting up auditd (1:4.0.2-2ubuntu2) ...
Created symlink '/etc/systemd/system/multi-user.target.wants/audit-rules.service' → '/usr/lib/systemd/system/audit-rules.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.
Setting up audispd-plugins (1:4.0.2-2ubuntu2) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for libc-bin (2.41-6ubuntu1.2) ...
hyukjin@hyukjin-VMware20-1:~$ sudo auditctl -w /home/hyukjin/malicious.sh -p x -k suspicious_exec


Ubuntu 64-bit Arm 25.04
Dec 8 23:10
hyukjin@hyukjin-VMware20-1: ~
Adding 'diversion of /lib/aarch64-linux-gnu/libauparse.so.0.0.0 to /lib/aarch64-linux-gnu/libauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:arm64 (1:4.0.2-2ubuntu2) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a4.0.2-2ubuntu2_arm64.deb ...
Unpacking auditd (1:4.0.2-2ubuntu2) ...
Selecting previously unselected package audispd-plugins.
Preparing to unpack .../audispd-plugins_1%3a4.0.2-2ubuntu2_arm64.deb ...
Unpacking audispd-plugins (1:4.0.2-2ubuntu2) ...
Setting up libauparse0t64:arm64 (1:4.0.2-2ubuntu2) ...
Setting up auditd (1:4.0.2-2ubuntu2) ...
Created symlink '/etc/systemd/system/multi-user.target.wants/audit-rules.service' → '/usr/lib/systemd/system/audit-rules.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/auditd.service' → '/usr/lib/systemd/system/auditd.service'.
Setting up audispd-plugins (1:4.0.2-2ubuntu2) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for libc-bin (2.41-6ubuntu1.2) ...
hyukjin@hyukjin-VMware20-1:~$ sudo auditctl -w /home/hyukjin/malicious.sh -p x -k suspicious_exec
Old style watch rules are slower
hyukjin@hyukjin-VMware20-1:~$ ./malicious.sh
Hacked!
hyukjin@hyukjin-VMware20-1:~$
Home


Ubuntu 64-bit Arm 25.04
Dec 8 23:17
hyukjin@hyukjin-VMware20-1: ~
GNU nano 8.3 /var/ossec/etc/ossec.conf *
<log_format>syslog</log_format>
<location>/var/log/dpkg.log</location>
</localfile>
<localfile>
<log_format>command</log_format>
<command>df -P</command>
</localfile>
<localfile>
<log_format>full_command</log_format>
<command>netstat -tan |grep LISTEN |egrep -v '(127.0.0.1| ::1)' |
</localfile>
<localfile>
<log_format>audit</log_format>
<location>/var/log/audit/audit.log</location>
</localfile>
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify


Ubuntu 64-bit Arm 25.04
Dec 8 23:26
hyukjin@hyukjin-VMware20-1: ~
hyukjin@hyukjin-VMware20-1:~$ ./malicious.sh
Hacked!
hyukjin@hyukjin-VMware20-1:~$ sudo tail -f /var/ossec/logs/alerts/alerts.log
** Alert 1765264746.107855: mail - audit,
2025 Dec 08 23:19:06 hyukjin-VMware20-1->/var/log/audit/audit.log
Rule: 100100 (level 10) -> 'Suspicious process execution detected: Unknown executable ran'
type=SYSCALL msg=audit(1765264745.479:320): arch=c00000b7 syscall=221 success=no exit=-8 a0=c1cbd1b5a480 a1=c1cbd1b5a260 a2=c1cbd1c92a30 a3=fc7fa79e2b28 items=1 ppid=3312 pid=5538 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=3 comm="bash" exe="/usr/bin/bash" subj=unconfined key="suspicious_exec"ARCH=aarch64 SYSCALL=execve AUID="hyukjin" UID="hyukjin" GID="hyukjin" EUID="hyukjin" SUID="hyukjin" FSUID="hyukjin" EGID="hyukjin" SGID="hyukjin" FSGID="hyukjin" type=CWD msg=audit(1765264745.479:320): cwd="/home/hyukjin" type=PATH msg=audit(1765264745.479:320): item=0 name="./malicious.sh" inode=2232446 dev=103:02 mode=0100775 ouid=1000 ogid=1000 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="hyukjin" OGID="hyukjin" type=PROCTITLE msg=audit(1765264745.479:320): proctitle="bash"
** Alert 1765264749.108934: mail - ossec,
2025 Dec 08 23:19:09 hyukjin-VMware20-1->ossec-monitord
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.
Home

Troubleshooting & Fixes

- Installed missing build dependencies (zlib, OpenSSL, headers, libsystemd) required for OSSEC build process
- Corrected syscheck configuration path issues caused by ARM specific directory differences
- Enabled auditd and OSSEC real time monitoring after verifying service failures
- Resolved duplicated configuration warnings during OSSEC startup

Conclusion

- Successfully installed and configured OSSEC HIDS on Ubuntu VM
- Detected SSH brute-force attempts through log monitoring
- Implemented suspicious process execution detection using auditd + OSSEC
- Learned practical HIDS implementation, rule configuration, alert interpretation, and troubleshooting

Thank you