**Runbook: Auditing Root Access and Command Execution on RHEL**

**1. Objective**

This runbook provides step-by-step instructions for auditing root access and tracking commands executed by users who switched to root. It uses auditd tools such as aureport and ausearch to comply with security policies like **NIST 800-53** and **CIS benchmarks**.

**2. Installing Auditd**

If auditd is not already installed, install it using:

sudo yum install audit -y # For RHEL 7/8

sudo dnf install audit -y # For RHEL 9

Ensure the auditd service is running:

sudo systemctl start auditd

sudo systemctl enable auditd

**3. Verify Audit Service Status**

Ensure the auditd service is running before proceeding:

sudo systemctl status auditd

If not running, start the service:

sudo systemctl start auditd

sudo systemctl enable auditd

**4. Audit Rules Configuration**

Audit rules define which events are recorded by auditd. The rules are typically stored in:

* /etc/audit/rules.d/ (Persistent rules)
* /etc/audit/audit.rules (Active rules loaded at boot)

**4.1. Adding New Audit Rules**

To add a new rule, edit or create a file in /etc/audit/rules.d/, e.g.:

sudo nano /etc/audit/rules.d/custom.rules

Add a rule, for example, to monitor changes to /etc/passwd:

-w /etc/passwd -p wa -k passwd\_changes

* -w /etc/passwd → Watch file /etc/passwd
* -p wa → Watch for write and attribute changes
* -k passwd\_changes → Add a key identifier

**4.2. Apply New Rules**

To apply the new rules without restarting the system:

sudo augenrules --load

To verify active rules:

sudo auditctl -l

**5. Identify User Sessions and Root Escalation**

**5.1. List User Login Events**

To identify users who logged in and switched to root:

sudo aureport -l -i

**6. Track Commands Executed as Root**

**6.1. List All Executed Commands**

To generate a report of commands executed on the system:

sudo aureport -x -i

**7. Track iptables Changes**

**7.1. Search for iptables Modifications**

To check for changes made to iptables rules:

sudo ausearch -c iptables

**8. Check for Policy Violations**

**8.1. Detect Audit Rule Violations**

To check for policy violations related to audit rules:

sudo aureport -k -i

**9. Detect Intrusions Using auditd**

**9.1. Identify Unauthorized Access Attempts**

Check failed login attempts:

sudo ausearch -m USER\_LOGIN --success no

**9.2. Detect Unauthorized File Access**

Monitor sensitive files (e.g., /etc/passwd):

sudo ausearch -f /etc/passwd

Generate a file access report:

sudo aureport -f

**9.3. Find Commands Executed by Suspicious Users**

List all executed commands:

sudo aureport -x -i

Search for a specific command:

sudo ausearch -c "bash"

**9.4. Monitor User Privilege Escalations**

Check sudo and su usage:

sudo ausearch -c sudo

sudo ausearch -c su

**9.5. Detect Audit Rule Changes**

Check for audit rule modifications:

sudo aureport -c

**9.6. Find Suspicious Network Activity**

Look for unauthorized firewall changes:

sudo ausearch -c iptables

**9.7. Track Kernel Security Events**

Identify security-related kernel events:

sudo aureport -k

**9.8. View System-Wide Events**

To check system reboots, crashes, or shutdowns:

sudo aureport -t

**9.9. Generate an Intrusion Report for a Specific Period**

To check today’s activities:

sudo aureport -l --start today --end now

**9.10. Find Users Who Switched to Root Between Specific Dates**

To list authentication events where users escalated to root (e.g., using su or sudo):

sudo aureport -au -i --start 2025-02-25 08:00:00 --end 2025-02-26 18:00:00

Example output:

Authentication Report

=============================================

# date time user term exe success event

1. 02/25/25 08:05:10 alice tty1 /bin/su yes 23001

2. 02/25/25 10:15:30 bob pts/0 /bin/sudo no 23002

3. 02/25/25 14:20:45 charlie pts/1 /bin/sudo yes 23003

* user → Shows who attempted privilege escalation.
* exe → Command used (/bin/su or /bin/sudo).
* success → yes or no (whether escalation was successful).

To get more details on a specific event (e.g., failed sudo attempt by bob with event ID 23002):

sudo ausearch -a 23002