

RMF Workbook Summary - Zakiya

Control ID	Control Name	Lab Title	RMF Step	What Was Implemented	Command/Tool Used
AC-2	Account Management	IAM Lab	Implement	User/group creation + folder permissions	PowerShell
AU-6	Audit Review	Threat Detection Lab	Implement/Assess	Sudo monitoring using auditd	auditctl, ausearch
AU-12	Audit Generation	Threat Detection Lab	Implement	Persistent audit rule on sudo	/etc/audit/rules.d/sudo.rules
AU-2	Audit Records	Threat Detection Lab	Implement	Enabled auditd and reviewed logs	auditctl, ausearch
SI-4	System Monitoring	System Hardening Lab	Monitor	Logged firewall and service configuration	ufw, services.msc, secpol.msc
AC-7	Failed Login Detection	Threat Detection Lab	Assess/Monitor	Monitored failed login and auth.log	journalctl, aureport, grep
RA-5	Vulnerability Scan	Vulnerability Lab	Assess	Performed system vulnerability scan	lynis, Nessus Essentials