🔑 Core Windows Security EventCodes (MUST KNOW)

EventCode	Meaning	SOC Use
4625	Failed login	Brute-force detection
4624	Successful login	Account activity
4672	Special privileges assigned	Admin logon
4634	Logoff	Session tracking
4648	Explicit credentials used	Lateral movement
7045	New service installed	Persistence
4697	Service installed	Persistence
4798 / 4799	Group membership change	Privilege escalation

Sysmon Event IDs (VERY important)

Sysmon has **its own Event IDs** (not Windows Security ones).

Sysmon ID	Meaning	Why SOCs Care
1	Process creation	Malware execution
3	Network connection	C2 traffic
7	Image loaded	DLL hijacking
11	File created	Payload drops
13	Registry change	Persistence
22	DNS query	Beaconing

Must-Know Linux SOC Search Queries (Beyond “Failed password” & `sudo`)

Linux does **not** rely on numeric EventCodes like Windows. SOC detection on Linux is **pattern + context based**.

Below is a **SOC-grade, must-know table** for Linux searches.

🔐 Authentication & Access (HIGH PRIORITY)

Purpose	SPL Query	Why SOCs Care
Failed SSH logins	`index=security_logs "Failed password"`	Brute-force attacks
Invalid users	`index=security_logs "Invalid user"`	Enumeration attempts
Successful SSH login	`index=security_logs "Accepted password"`	Account activity
Root login	`index=security_logs "session opened for user root"`	Privilege abuse
Login from new IP	`index=security_logs "Accepted password"`	Lateral movement

👤 Privilege Escalation

Purpose	SPL Query	Why SOCs Care
sudo usage	`index=security_logs sudo`	Admin activity
sudo failures	`index=security_logs "authentication failure" sudo`	Privilege escalation attempts
su to root	`index=security_logs "session opened for user root"`	Unauthorized privilege use

⚙️ System & Persistence Indicators

Purpose	SPL Query	SOC Value
New user created	`index=security_logs "useradd"`	Persistence
User added to sudo	`index=security_logs "usermod" sudo`	Privilege escalation
Cron job creation	`index=security_logs "CRON"`	Scheduled persistence

System service start	`index=os_logs systemd`	Malware persistence
Package install	`index=os_logs apt install`	Unauthorized software

🌐 Network & Recon (Basic)

Purpose	SPL Query	SOC Value
SSH connections	`index=security_logs sshd`	Connection tracking
Port scanning traces	`index=os_logs "connection refused"`	Recon
DNS resolution	`index=os_logs "named"`	C2 detection (later)