INTEZER

ATT&CK matrix

for Linux cloud servers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion		Credential Access	Discovery	Lateral Movement	Collection	Command and Control		Exfiltration	Impact
Exploit Public-Facing Application	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Clear Command History	Scripting	Bash History	Account Discovery	Application Deployment Software	Automated Collection	Commonly Used Port	Standard Application Layer Protocol	Automated Exfiltration	Account Access Removal
Valid Accounts	Exploitation for Client Execution	Bootkit	Process Injection	Compile After Delivery	Space after Filename	Brute Force	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Connection Proxy	Standard Cryptographic Protocol	Data Compressed	Data Destruction
Trusted Relationship	Source	Create Account	Setuid and Setgid	Connection Proxy	Timestomp	Credential Dumping	Network Service Scanning	Remote File Copy	Data from Network Shared Drive	Custom Command and Control Protocol	Standard Non-Application Layer Protocol	Data Encrypted	Data Encrypted for Impact
	Local Job Scheduling	Hidden Files and Directories	Sudo	Disabling Security Tools	Valid Accounts	Credentials in Files	Network Sniffing	Remote Services	Data Staged	Custom Cryptographic Protocol	Uncommonly Used Port	Data Transfer Size Limits	Defacement
	Scripting	Kernel Modules and Extensions	Sudo Caching	File and Directory Permissions Modification	Web Service	Exploitation for Credential Access	Password Policy Discovery	SSH Hijacking	Input Capture	Data Encoding	Web Service	Exfiltration Over Alternative Protocol	Disk Content Wipe
	Space after Filename	Local Job Scheduling	Valid Accounts	File Deletion	Application Access Token	Input Capture	Permission Groups Discovery	Third-party Software	Data from Cloud Storage Object	Data Obfuscation		Exfiltration Over Command and Control Channel	Disk Structure Wipe
	Third-party Software	Port Knocking	Web Shell	Hidden Files and Directories	Revert Cloud Instance	Network Sniffing	Process Discovery	Application Access Token		Domain Fronting		Scheduled Transfer	Endpoint Denial of Service
	Trap	Redundant Access		HISTCONTROL	Unused/ Unsupported Cloud Regions	Private Keys	Remote System Discovery			Domain Generation Algorithms		Transfer Data to Cloud Account	Firmware Corruption
	User Execution	Server Software Component		Indicator Removal on Host	Execution Guardrails	Account Manipulation	System Information Discovery			Fallback Channels			Inhibit System Recovery
		Setuid and Setgid		Install Root Certificate	Exploitation for Defense Evasion	Cloud Instance Metadata API	System Network Configuration Discovery			Multi-hop Proxy			Network Denial of Service
		Systemd Service		Masquerading	Binary Padding	Steal Application Access Token	System Network Connections Discovery			Multi-Stage Channels			Resource Hijacking
		Trap		Obfuscated Files or Information	Indicator Removal from Tools		System Owner/ User Discovery			Multiband Communication			Runtime Data Manipulation
		Valid Accounts		Port Knocking			Cloud Service Discovery			Multilayer Encryption			Stored Data Manipulation
		Web Shell		Process Injection			Network Share Discovery			Port Knocking			System Shutdown/ Reboot
		Account Manipulation		Redundant Access			Software Discovery			Remote Access Tools			Transmitted Data Manipulation
		Implant Container Image		Rootkit						Remote File Copy			