efeer Dashboard

PAM: Login session opened.

_id	1716373288.5432		
timestamp	2024-05-22T16:21:28.770+0600		
rule	level	3	
	description	PAM: Login session opened.	
	id	5501	
	mitre	id	T1078
		tactic	Defense Evasion Persistence Privilege Escalation Initial Access
		technique	Valid Accounts
	firedtimes	6	
	mail	False	
	groups	pam syslog authentication_success	
	pci_dss	10.2.5	
	gpg13	7.8 7.9	
	gdpr	IV_32.2	
	hipaa	164.312.b	
	nist_800_53	AU.14 AC.7	
	tsc	CC6.8 CC7.2 CC7.3	
agent	id	000	
	name	mmetroooo	
manager	name	mmetroooo	
full_log	May 22 15:21:26 mmetroooo su: pam_unix(su:session): session opened for user root(uid=0) by aomer(uid=0)		
predecoder	program_name	su	
	timestamp	May 22 15:21:26	
	hostname	mmetroooo	
decoder	parent	pam	
	name	pam	

data	srcuser	aomer
	dstuser	root(uid=0)
	uid	0
location	/var/log/auth.log	

MITRE ATT&CK® Information