Hi

Anything suspicious in this log file?

Apr 25 19:36:53 ubuntu sshd[146770]: Failed password for root from 10.211.55.2 port 64223 ssh2
Apr 25 19:36:53 ubuntu sshd[146765]: Failed password for root from 10.211.55.2 port 64218 ssh2
Apr 25 19:36:53 ubuntu sshd[146773]: Failed password for root from 10.211.55.2 port 64226 ssh2
Apr 25 19:36:53 ubuntu sshd[146775]: Failed password for root from 10.211.55.2 port 64228 ssh2
Apr 25 19:36:53 ubuntu sshd[146776]: Failed password for root from 10.211.55.2 port 64229 ssh2
Apr 25 19:36:53 ubuntu sshd[146777]: Failed password for root from 10.211.55.2 port 64230 ssh2
Apr 25 19:36:53 ubuntu sshd[146762]: Failed password for root from 10.211.55.2 port 64217 ssh2
Apr 25 19:36:53 ubuntu sshd[146759]: Failed password for root from 10.211.55.2 port 64215 ssh2
Apr 25 19:36:54 ubuntu gdm-password]: gkr-pam: unlocked login keyring
Apr 25 19:36:56 ubuntu sshd[146767]: Failed password for root from 10.211.55.2 port 64220 ssh2
Apr 25 19:36:56 ubuntu sshd[146766]: Failed password for root from 10.211.55.2 port 64219 ssh2
Apr 25 19:36:56 ubuntu sshd[146774]: Failed password for root from 10.211.55.2 port 64227 ssh2
Apr 25 19:36:56 ubuntu sshd[146761]: Failed password for root from 10.211.55.2 port 64216 ssh2
Apr 25 19:36:56 ubuntu sshd[146769]: Failed password for root from 10.211.55.2 port 64222 ssh2
Apr 25 19:36:56 ubuntu sshd[146772]: Failed password for root from 10.211.55.2 port 64225 ssh2
Apr 25 19:36:56 ubuntu sshd[146768]: Failed password for root from 10.211.55.2 port 64221 ssh2
Apr 25 19:36:56 ubuntu sshd[146771]: Failed password for root from 10.211.55.2 port 64224 ssh2
Apr 25 19:36:56 ubuntu sshd[146770]: Failed password for root from 10.211.55.2 port 64223 ssh2
Apr 25 19:36:56 ubuntu sshd[146765]: Failed password for root from 10.211.55.2 port 64218 ssh2
Apr 25 19:36:56 ubuntu sshd[146773]: Failed password for root from 10.211.55.2 port 64226 ssh2
Apr 25 19:36:56 ubuntu sshd[146775]: Failed password for root from 10.211.55.2 port 64228 ssh2
Apr 25 19:36:56 ubuntu sshd[146762]: Failed password for root from 10.211.55.2 port 64217 ssh2
Apr 25 19:36:56 ubuntu sshd[146759]: Failed password for root from 10.211.55.2 port 64215 ssh2
Apr 25 19:36:56 ubuntu sshd[146777]: Failed password for root from 10.211.55.2 port 64230 ssh2
Apr 25 19:36:56 ubuntu sshd[146776]: Failed password for root from 10.211.55.2 port 64229 ssh2
Apr 25 19:37:00 ubuntu sshd[146767]: Failed password for root from 10.211.55.2 port 64220 ssh2
Apr 25 19:37:00 ubuntu sshd[146766]: Failed password for root from 10.211.55.2 port 64219 ssh2
Apr 25 19:37:00 ubuntu sshd[146774]: Failed password for root from 10.211.55.2 port 64227 ssh2
Apr 25 19:37:00 ubuntu sshd[146761]: Failed password for root from 10.211.55.2 port 64216 ssh2
Apr 25 19:37:00 ubuntu sshd[146769]: Failed password for root from 10.211.55.2 port 64222 ssh2
Apr 25 19:37:00 ubuntu sshd[146768]: Failed password for root from 10.211.55.2 port 64221 ssh2
Apr 25 19:37:00 ubuntu sshd[146772]: Failed password for root from 10.211.55.2 port 64225 ssh2
Apr 25 19:37:00 ubuntu sshd[146770]: Failed password for root from 10.211.55.2 port 64223 ssh2
Apr 25 19:37:00 ubuntu sshd[146765]: Failed password for root from 10.211.55.2 port 64218 ssh2
Apr 25 19:37:00 ubuntu sshd[146771]: Failed password for root from 10.211.55.2 port 64224 ssh2
Apr 25 19:37:00 ubuntu sshd[146773]: Failed password for root from 10.211.55.2 port 64226 ssh2
Apr 25 19:37:00 ubuntu sshd[146776]: Failed password for root from 10.211.55.2 port 64229 ssh2
Apr 25 19:37:00 ubuntu sshd[146762]: Failed password for root from 10.211.55.2 port 64217 ssh2
Apr 25 19:37:00 ubuntu sshd[146759]: Failed password for root from 10.211.55.2 port 64215 ssh2
Apr 25 19:37:00 ubuntu sshd[146775]: Failed password for root from 10.211.55.2 port 64228 ssh2
Apr 25 19:37:00 ubuntu sshd[146777]: Failed password for root from 10.211.55.2 port 64230 ssh2
Apr 25 19:37:01 ubuntu sshd[146767]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64220 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146767]: Disconnecting authenticating user root 10.211.55.2 port 64220: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146767]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146767]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146766]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64219 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146766]: Disconnecting authenticating user root 10.211.55.2 port 64219: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146766]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146766]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146774]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64227 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146774]: Disconnecting authenticating user root 10.211.55.2 port 64227: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146774]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146774]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146772]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64225 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146769]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64222 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146769]: Disconnecting authenticating user root 10.211.55.2 port 64222: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146769]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146769]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146772]: Disconnecting authenticating user root 10.211.55.2 port 64225: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146772]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146772]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146768]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64221 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146761]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64216 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146761]: Disconnecting authenticating user root 10.211.55.2 port 64216: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146761]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146761]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146768]: Disconnecting authenticating user root 10.211.55.2 port 64221: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146768]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146768]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146770]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64223 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146770]: Disconnecting authenticating user root 10.211.55.2 port 64223: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146765]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64218 ssh2 [preauth]
Apr 25 19:37:01 ubuntu sshd[146765]: Disconnecting authenticating user root 10.211.55.2 port 64218: Too many authentication failures [preauth]
Apr 25 19:37:01 ubuntu sshd[146765]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.211.55.2 user=root
Apr 25 19:37:01 ubuntu sshd[146765]: PAM service(sshd) ignoring max retries; 6 > 3
Apr 25 19:37:01 ubuntu sshd[146771]: error: maximum authentication attempts exceeded for root from 10.211.55.2 port 64224 ssh2 [preauth]

Yes, there is suspicious activity in this log file. There are numerous failed password attempts for the root user from the same IP address (10.211.55.2) and different port numbers. This activity suggests that someone is trying to gain unauthorized access to the root account by attempting to brute-force the password. The logs also show that the maximum authentication attempts were exceeded, and the system disconnected the user due to too many authentication failures.

You should investigate this issue further to determine if the IP address is known and if the attempts were legitimate or not. If the attempts were not legitimate, consider taking action to secure your system, such as blocking the IP address, enabling two-factor authentication, or implementing stricter security measures.