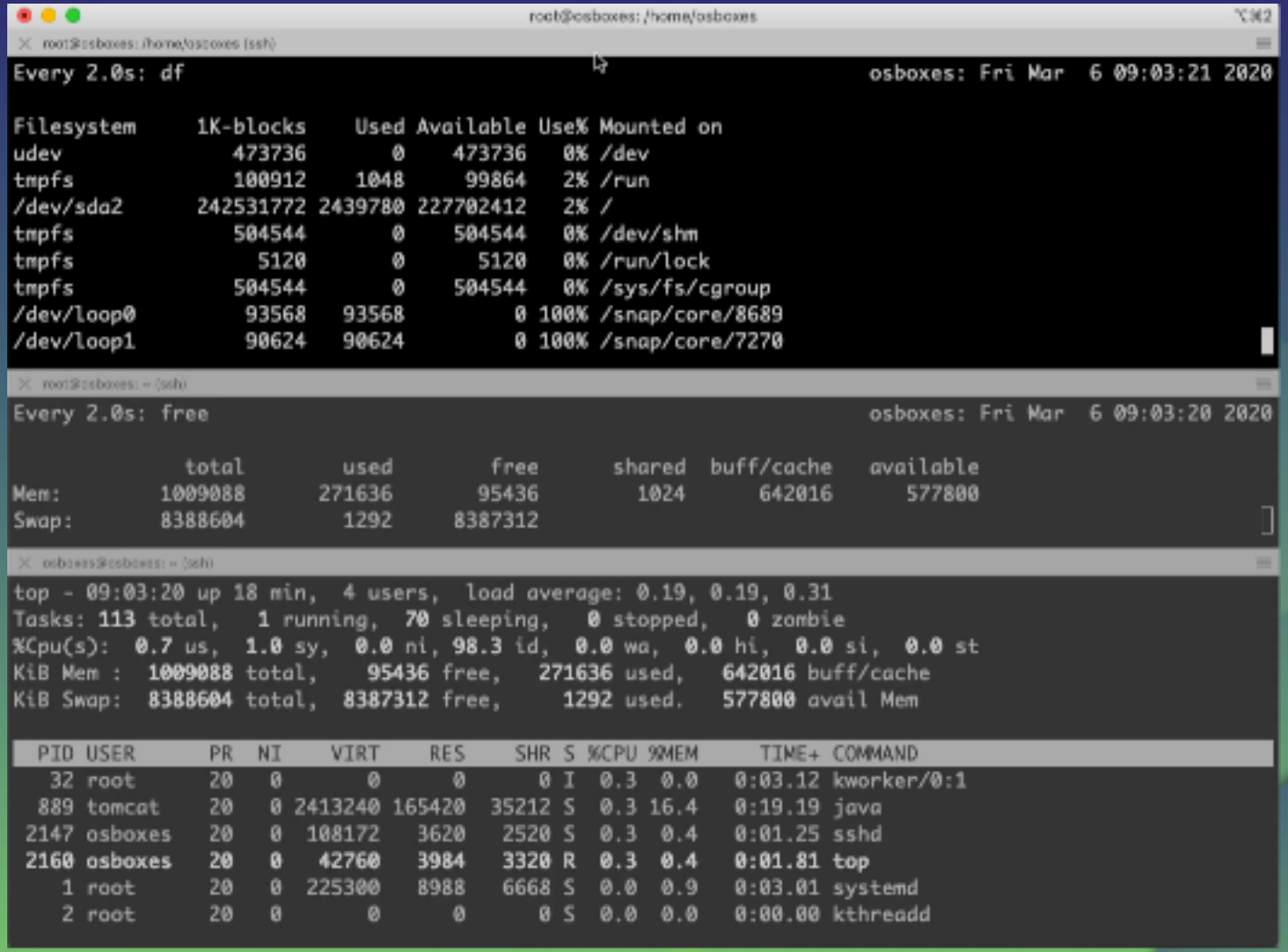
The ZIP BOMB (2 / 4)

- Major of packaged software is packed as a ZIP file: .jar, .war, .docx, .xlsx….
- Some Application Servers auto deploy them when put files in specific path
- What if we put a ZIP bomb renamed as a valid packed Application for a Tomcat?


root@osboxes: /home/osboxes
Every 2.0s: df
osboxes: Fri Mar 6 09:03:21 2020
Filesystem 1K-blocks Used Available Use% Mounted on
udev 473736 0 473736 0% /dev
tmpfs 100912 1048 99864 2% /run
/dev/sda2 242531772 2439780 227702412 2% /
tmpfs 504544 0 504544 0% /dev/shm
tmpfs 5120 0 5120 0% /run/lock
tmpfs 504544 0 504544 0% /sys/fs/cgroup
/dev/loop0 93568 93568 0 100% /snap/core/8689
/dev/loop1 90624 90624 0 100% /snap/core/7270
Every 2.0s: free
osboxes: Fri Mar 6 09:03:20 2020
total used free shared buff/cache available
Mem: 1009088 271636 95436 1024 642016 577800
Swap: 8388604 1292 8387312
top - 09:03:20 up 18 min, 4 users, load average: 0.19, 0.19, 0.31
Tasks: 113 total, 1 running, 70 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.7 us, 1.0 sy, 0.0 ni, 98.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 1009088 total, 95436 free, 271636 used, 642016 buff/cache
KiB Swap: 8388604 total, 8387312 free, 1292 used. 577800 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
32 root 20 0 0 0 0 I 0.3 0.0 0:03.12 kworker/0:1
889 tomcat 20 0 2413240 165420 35212 S 0.3 16.4 0:19.19 java
2147 osboxes 20 0 108172 3620 2520 S 0.3 0.4 0:01.25 sshd
2160 osboxes 20 0 42760 3984 3320 R 0.3 0.4 0:01.81 top
1 root 20 0 225300 8988 6668 S 0.0 0.9 0:03.01 systemd
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd