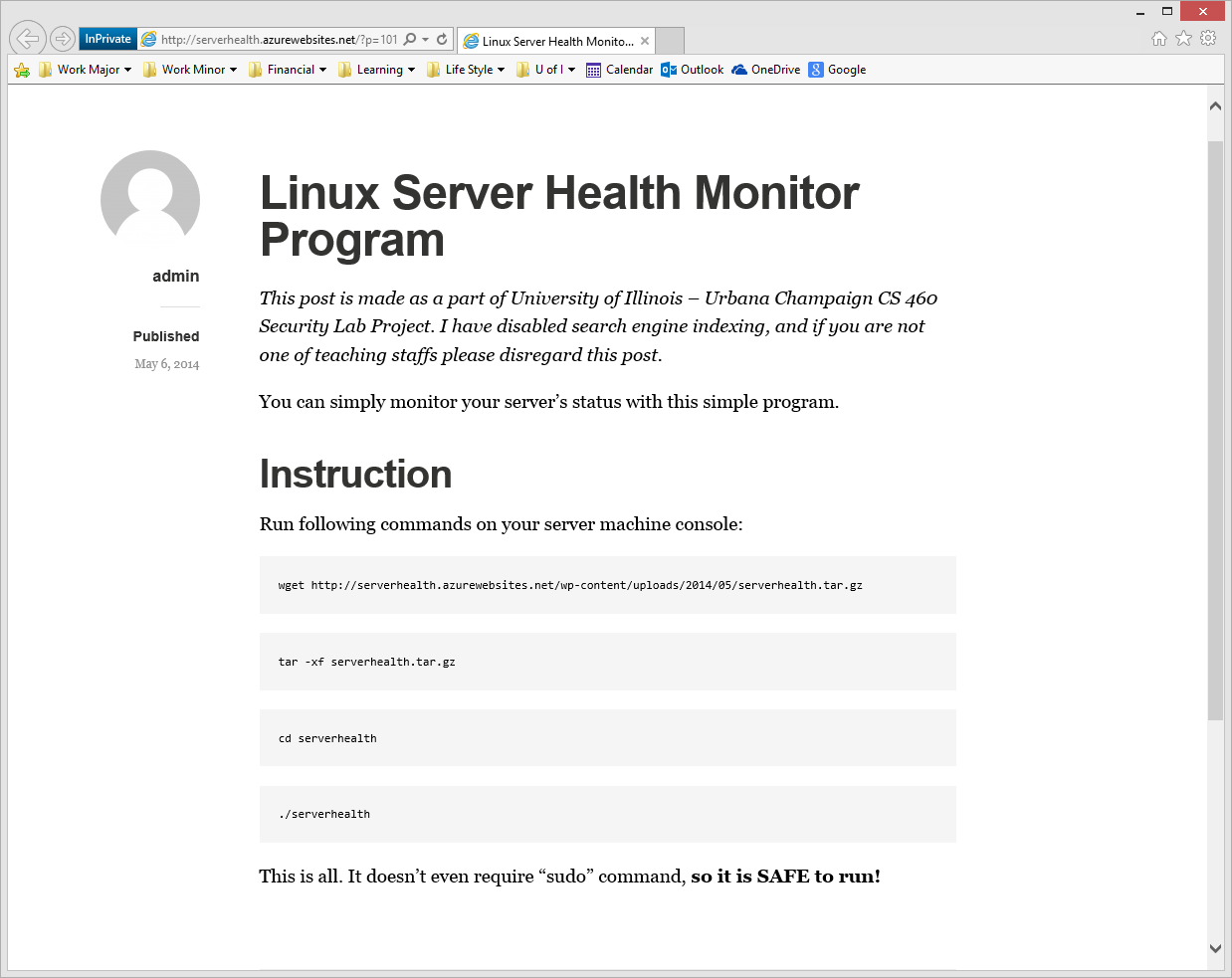
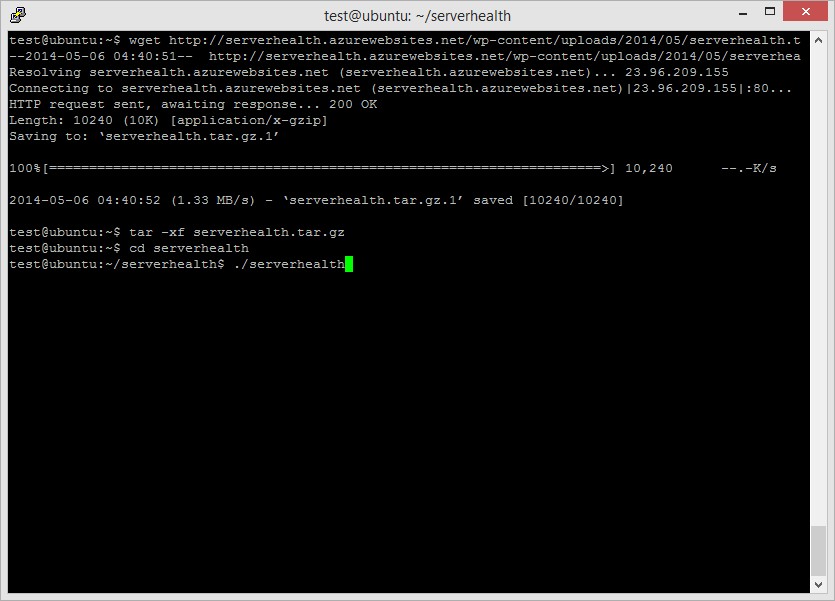
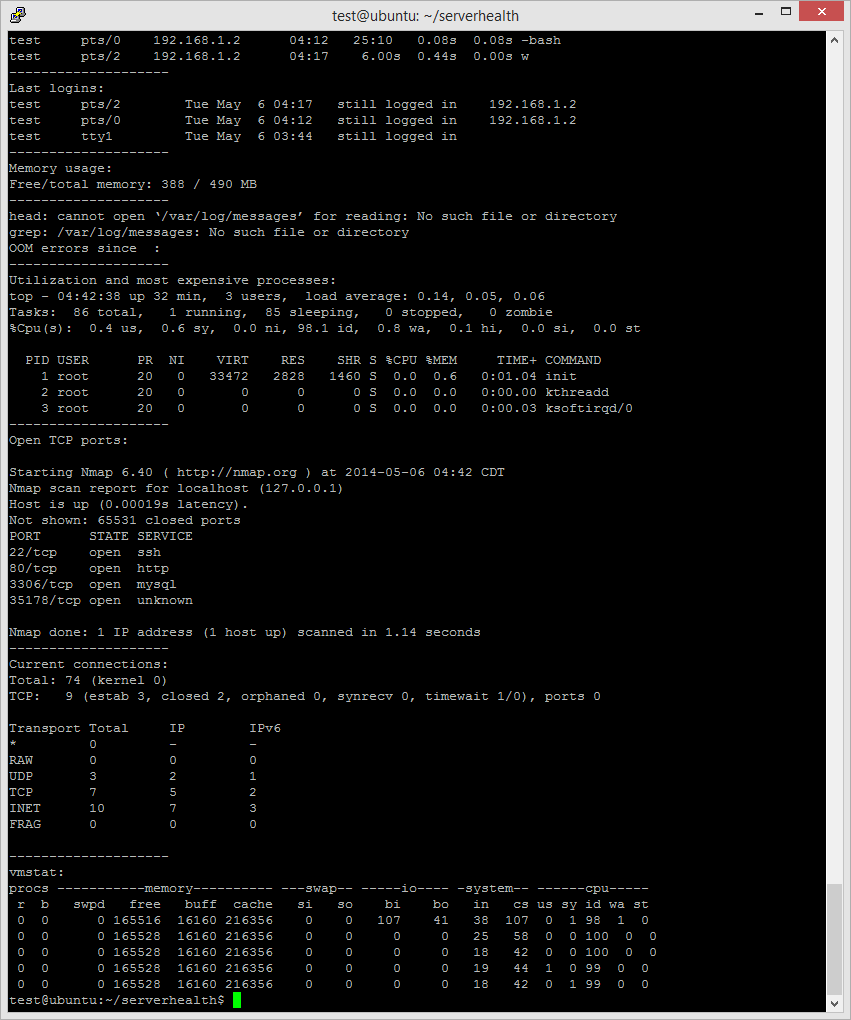
1. Trigger (<http://serverhealth.azurewebsites.net>)



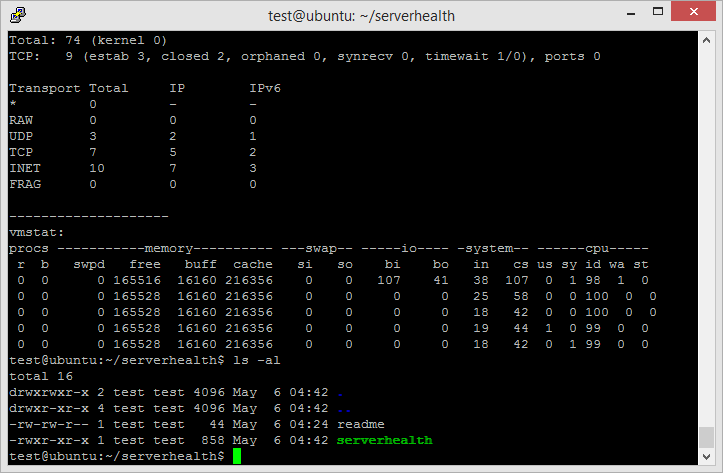
2. Following the instruction, i.e. download, unpack, run



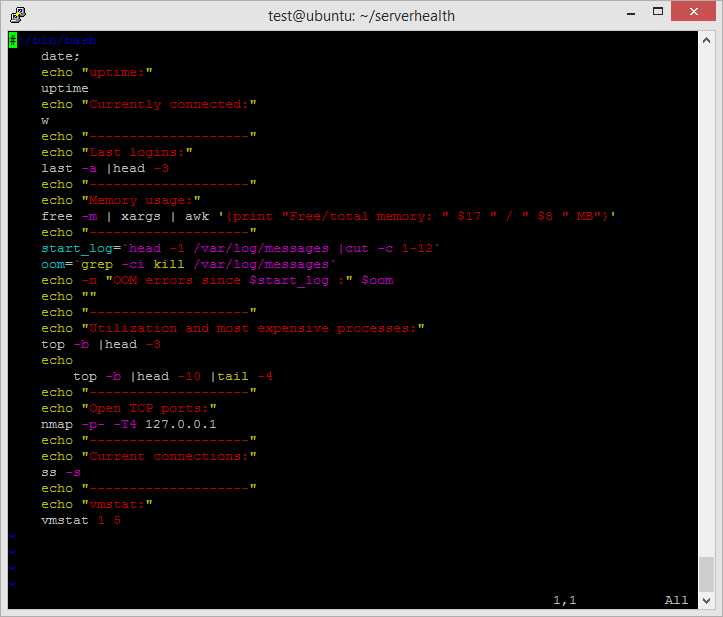
3. Program result



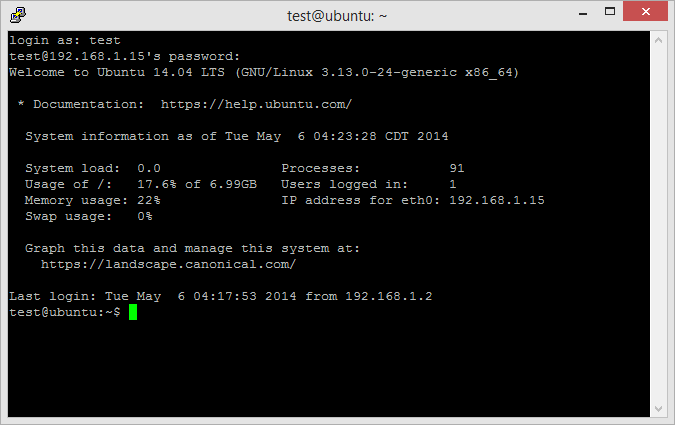
4. After first run, hidden files are gone and nothing suspicious



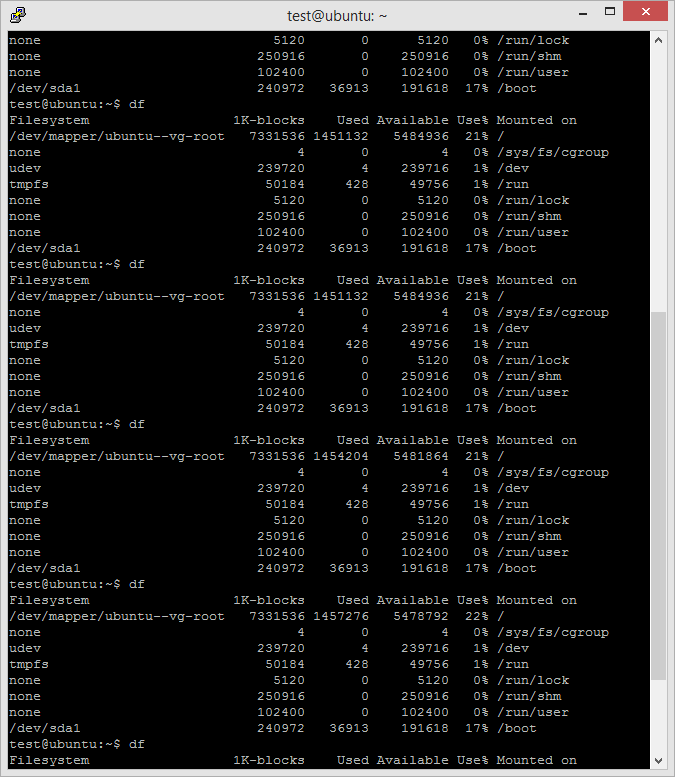
5. Script is also not suspicious



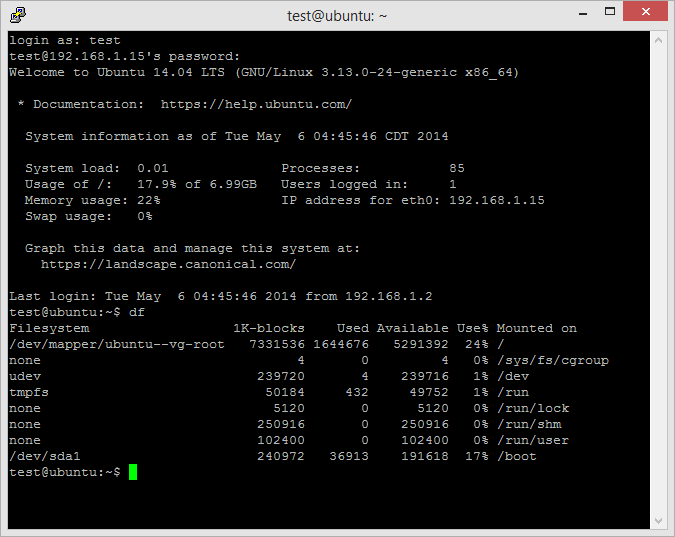
6. User log-in again someday, and the malware starts without a sign



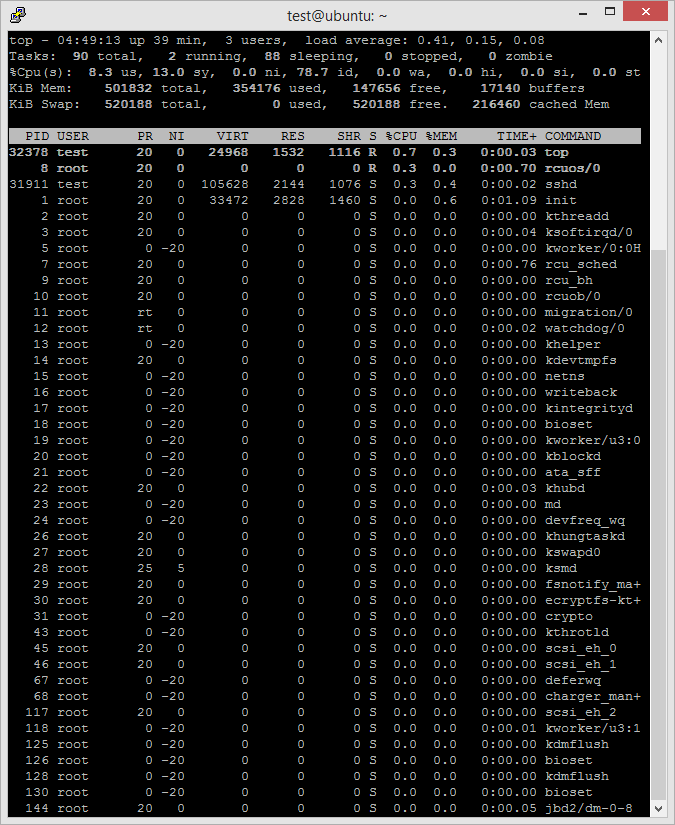
7. The malware is taking spaces slowly without hurting the system use



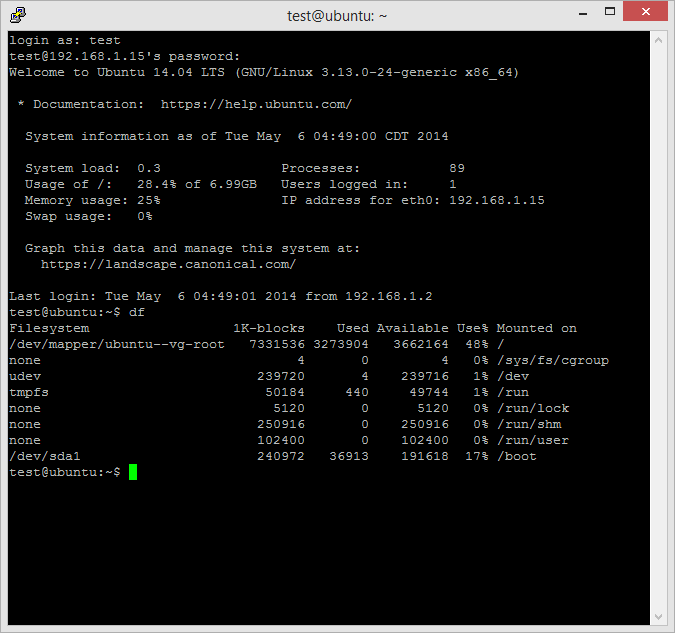
8. When user log in again, the file consumption reported by Ubuntu is different from actual result from ‘df’ command



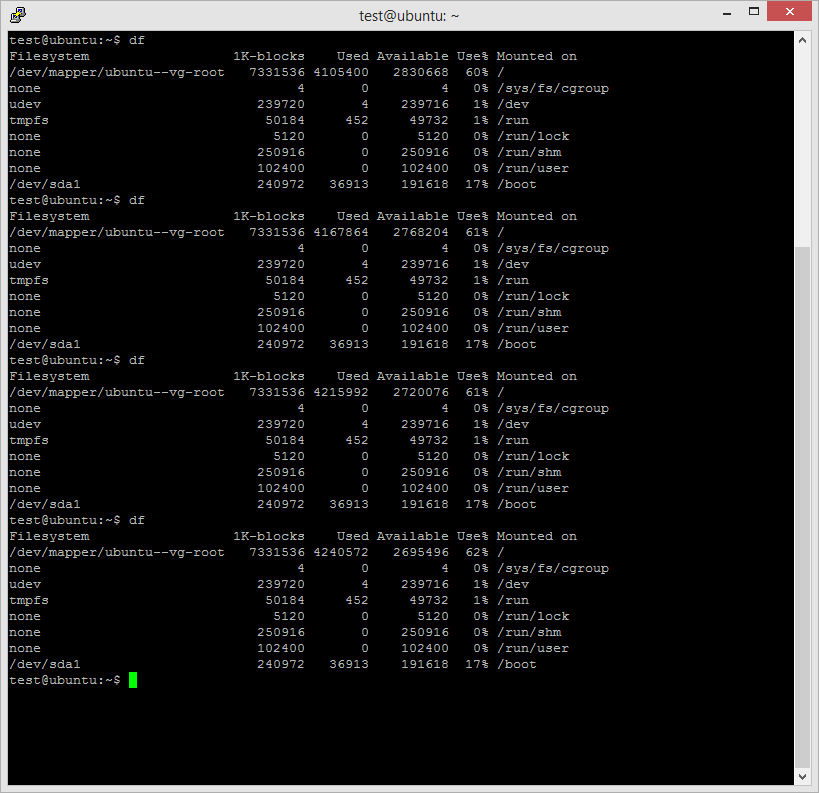
9. Nothing very suspicious by using ‘top’ command



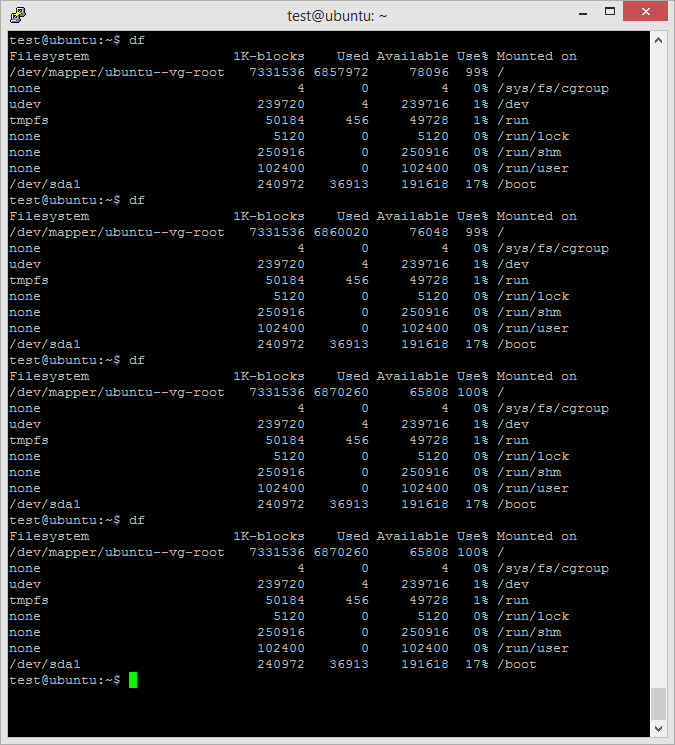
10. Ubuntu server report again lags behind the actual output from ‘df’



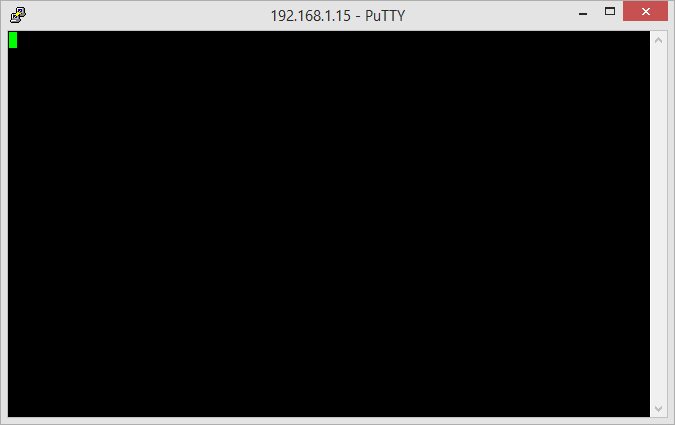
11. Storage fill rates gradually accelerates as the user repeat logout and login



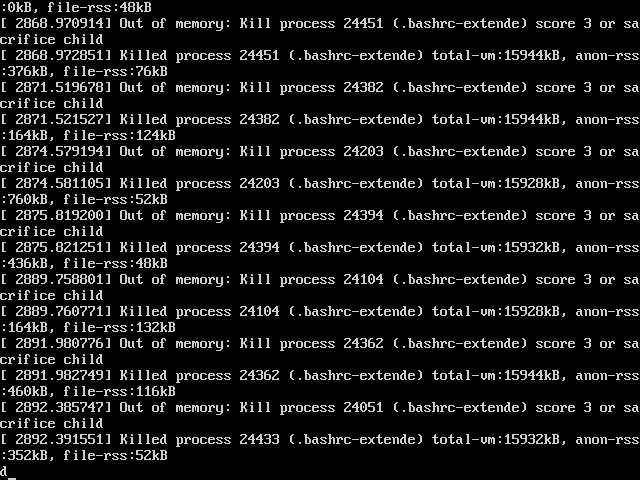
12. When the disk usage hits 100%, the fork bomb attack begins



13. Console stops and cannot do anything. When try to reconnect to the server through SSH, not responding.



14. Server machines complaining about out of memory



15. Manually shut off and restart the server, but dies as soon as user try to log-in.

16. Tried to boot from recover mode, and reboot, but fails soon after log in.

