Final assignment 4

1. A user who is signed up to a blog application as an “author” should not have administrative privileges that allow them to add or remove users. They should only be allowed to post articles to the application. Which 9-principles this is following? (10 points)
2. Tor network has a sender, a receiver, and three relay nodes. Which communication stage (in terms of the communication between one node and another node.) is not protected by Tor network? (10 points)
3. What will happen in a memory overflow attack, if the return address section is changed to:
4. new (virtual) address maps to a physical address, not protected by kernel, but the data in the address is not valid machine instruction? (5 points)
5. new (virtual) address maps to a physical address, not protected by kernel, data is valid machine instruction? (5 points)
6. With AES key,
7. Could you provide communication confidentiality? (5 points)
8. Could you provide authenticity? Why? (5 points)
9. The recent machine learning technique drives an intelligent firewall. It can detect attack’s stages by monitoring and analyzing the packet trace and pattern (e.g., a traffic burst within a short period of time at midnight implies a attack is happening). Is such a firewall stateful or stateless? Explain (10 points)
10. For a desktop with capability of performing 10^8 (10 to the power of 8) decryptions per second, how many yearsin average does it take to crack a message encrypted under AES-128 algorithms? Show your calculation (10 points)
11. How many layers of encryption are used in Tor networks? (10 points)
12. Write the iptables command:
13. Set firewall http INPUT policy to DROP (5 points)
14. Set firewall telnet OUTPUT policy to ACCEPT (5 points)
15. What is the difference of PGP certificate and x.509 PKI? (10 points)

10. Since VPN encrypts the inner-layer messages, is it secure to send messages without additional user-side encryption? Why? (10 points)