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)

The principles that this scenario follows:

a) **Principle of Least Privilege:** An entity should be given only those privileges needed to complete its task.
b) **Fail-Safe Defaults:** Unless an entity is given explicit access to an object, it should be denied access.

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)

Tor does not offer encryption after the exit relay. The sender and the receiver need to share a key via TLS to encrypt their message if they want to secure it further.

3. What will happen in a memory overflow attack, if the return address section is changed to:

1) 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)

Program simply crashes.

2) new (virtual) address maps to a physical address, not protected by kernel, data is valid machine instruction? (5 points)

program continues to run, but it is not the one expected.

4. With AES key,

1) Could you provide communication confidentiality? (5 points)

AES key can provide confidentiality as it uses symmetric key encryption. The user with the valid key would be able to encrypt and decrypt the message.

2) Could you provide authenticity? Why? (5 points)

No, this is because an attacker could obtain a key using various tactics to gain access to an encrypted file or message stream between two individuals. An attacker could hijack a message stream and pose as a sender and receiver for the opposite parties (man-in-the-middle) resulting in a communication without authentication.

-2

5. 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)

It is a stateful firewall as it monitors all connection interactions until it is closed. Another reason to this is because it is examining the contents of the packets. Stateful firewall is much smarter and thus because of that it must be a stateful firewall. -2

6. For a desktop with capability of performing 10^8 (10 to the power of 8) decryptions per second, how many years in average does it take to crack a message encrypted under AES-128 algorithms? Show your calculation (10 points)

Total Number of AES-128 Keys = $2^{128} \approx 3.4 * 10^{38}$

$$Total\ Time¿\ Decrypt = \frac{Total\ Number\ of\ Keys}{Total\ Time\ Taken¿}\ decrypt¿$$

$$Total\ Time¿\ Decrypt = \frac{2^{128}}{(10^8 * 60 * 60 * 24 * 365)} = 1.079 * 10^{18}\ years$$ -2

7. How many layers of encryption are used in Tor networks? (10 points)

There are 3 layers of encryption in a Tor network which are as follows:

1) Entry Relay
2) Middle Relay
3) Exit Relay

8. Write the iptables command:

1) Set firewall http INPUT policy to DROP (5 points)

sudo iptables -A INPUT -p –-dport 80 -j DROP

2) Set firewall telnet OUTPUT policy to ACCEPT (5 points)

sudo iptables -A OUTPUT -p –-dport 23 -j ACCEPT

9. What is the difference of PGP certificate and x.509 PKI? (10 points)

In terms of key hierarchy, you have to request to a Certification Authority in order for them to issue you an X.509 certificate. On the other hand, we can create our own PGP.
In terms of key trust, X.509 supports only a sole key owner. It can support only one digital signature to confirm the key's validity. This does not work for PGP.

In terms of trust model, X.509 has a Hierarchical Trust Model. Trust originates from a 'trusted' CA, over which the guardian may or may not have control. A requestor provides a chain of authentication from the 'trusted' CA to the requestor's key. As for the signatures, each certificate has one signature, belonging to the issuer of the certificate.

While on the other hand PGP follows Web of Trust model. Each certificate can have multiple signatures; the first signature belongs to the issuer of the certificate.

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

ecause we can never know if the VPN server is compromised or not. And if it is than all the client's data will be leaked which will take away the whole purpose of using a VPN service. Now that we know this, it is always good to use good encryption before sending any data out to the VPN server. Also, another way to protect ourselves from such kind of attacks would be to simply use a good and reputable VPN service instead of something that is free and may not be as much trustworthy. This setup would be prone to man-in-the-middle attack.

-2