Tutorial Week 12

Questions

1. Which attacks rely on IP Spoofing? Which attacks, while made easier by IP spoofing, would still be possible without it?
2. Firewalls, Kerberos, RADIUS, PKI, IDS, VPN are among the security technologies we have encountered in this subject. Why is it not enough to just deploy these technologies without considering them in our security programme?
3. Why is it important to do a risk analysis before embarking on a large scale security programme?
4. Stateful packet inspection firewalls provide more sophisticated defence than proxy firewalls or packet filters but can themselves be subject to attack. What attack is a stateful packet inspection firewall most vulnerable to?
5. WPA2 supports the use of AES for encryption in a WLAN. Is AES a block or stream encryption protocol?
6. In a security environment an organisation needs to defend itself against many possible attackers. Who does KERBEROS defend the organisation against and how does it do it?
7. AES and DES are both block ciphers. Why is AES used in WPA2 but DES was not used in WEP?
8. A biometric system is subject to false accepts where it permits access by someone it should not, and false rejects, where it refuses access to someone it should. Which type of error is usually regarded as being more serious? Why?
9. WEP (Wireless Equivalence Privacy) experienced a number of problems that made it a less than satisfactory security solution. What were the problems?
10. WPA1 uses the same encryption algorithm (RC4) as WEP but is regarded as being much more secure. Why?
11. When purchasing goods via a website, why does the website need a digital certificate but not the person doing the purchasing? In what circumstances would the client need a certificate?
12. We have seen that probabilistic packet marking can be used to detect the sources of a Distributed Denial of Service attack. Is this sufficient to manage a DDoS? If not, what else is needed?
13. VPN tunnels can be compulsory or voluntary. Where would you expect each type of tunnel to be used?
14. Public Key Infrastructure links an identity of some kind to a public key. How does it do this? What are some of the weaknesses of PKI?
15. In constructing a digital signature, why do we encrypt the hash of a digital document rather than the document itself?
16. Diffie-Hellman hybrid key exchange and RSA can both be used to establish session keys across an insecure channel. How do the approaches differ?
17. We looked at three wireless network technologies and their security issues. What are the similarities in their security requirements? What are their differences?
18. What is a challenge-response authentication protocol? What are some examples we have seen in this subject?
19. What are the common firewall architectures? What are the common firewall types?