12 Week Exam Study Guide

Vocabulary

1. Host
2. IP Address
3. Domain name
4. Packet
5. Router / gateway router
6. Injection attack
7. Cross-Site Scripting (XSS)
8. Cookie
9. Phishing
10. Port
11. Protocol
12. Hub
13. Switch
14. Subnet mask
15. Network address
16. MAC address (physical address)
17. ESSID/BSSID
18. Firewall
19. Access Control List (ACL)
20. Encryption (Symmetric, Asymmetric)
21. Hashing
22. Frequency analysis
23. One-time-pad
24. Digital signature
25. Certificate
26. Man-in-the-middle attack
27. Steganography
28. Embedded message, cover-medium, stego-medium

Concepts

1. Contrast IPv4 and IPv6. What is dotted quad notation?
2. How does network address translation (NAT) work? (On course Resources page see Network Demos and then click on NAT Demo)
3. What is traceroute? (Note traceroute doesn't show switches/hubs)
4. Everything that you do online leaves a digital trail. User activity can be tracked by:
    a. Server access/error logs
    b. Browser history
5. In an injection attack, the bad guy injects code, but the code is executed in the context of the victim. How do we protect against injection attacks?
6. How are cookies used and what do we gain by using them?
7. What are the 5 network layers? Understand basically what happens at each layer.
8. What are the differences between TCP and UDP?
9. Understand the connection between services, ports, protocols, and tools.
10. Memorize the table at the top of the next page, with the exception that the only port numbers you are expected to know are port 80 for HTTP, 443 for HTTPS, 22 for SSH, 53 for DNS:
11. The internet is a network of networks. What one thing must a host have to connect to a network? What 3 things does a host need to also play on the internet?
12. Understand how packets are sent:
    a. To other hosts in your network
    b. To hosts in other networks

(On course Resources page see Network Demos then click on Network-Internetwork Demo)

Service	Protocol	Port	TCP/UDP	Tools
"ping", check if node is alive	ICMP	--*	--	ping
World Wide Web	HTTP	80	TCP	browsers
Secure Web	HTTPS	443	SSL/TLS	browsers
Name Resolution	DNS	53	UDP	nslookup
Secure Remote Shell	SSH	22	TCP	ssh (PuTTY)
Remote Desktop (Windows)	RDP	3389	TCP	rdesktop (a Unix tool)
Secure Remote File Transfer	SFTP	22**	TCP	WinSCP
Dynamic Host Configuration***	DHCP	67/68****	UDP	builtin Windows DHCP client, dhclient
Network file & printer sharing	SMB	445	TCP	the file browser's "map network drive"

* Ping doesn't use the transport layer, so there's no associated port

13. What are the differences between wired and wireless networks? What stays the same?
14. What are the five pillars of IA? You should understand which pillar is being protected/attacked given a particular scenario.
15. Understand that there is an ever present trade-off between security and functionality. There are risks involved both in providing a service as well as in using it. We must weigh the risks involved against the benefits of the functionality.
16. Understand and be able to apply the risk equation: *risk = likelihood*impact* where likelihood is a function of vulnerabilities and threats.
17. What are firewalls used for and how do they work?
18. What is the difference between symmetric encryption (block ciphers), hashing, and asymmetric encryption (public key encryption)? What pillars of IA does each help to protect (how is each used)? How are these used in combination to achieve greater security?
19. What problem with symmetric encryption does asymmetric encryption solve?
20. What are the requirements for a good hash function?
21. Algorithms we've seen in class:
    a. Caesar Cipher and Vigenere Cipher – Symmetric encryption
    b. MD5 and SHA1 – Hash functions
    c. RSA – Asymmetric encryption
22. What is the difference between encryption and steganography? What pillars of IA does each help to protect?
23. How can we hide secret messages in image files without being noticed?