|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ASCII Table for Printable Characters** | | | | | | | | |
| Dec Hex Char  32 20  33 21 !  34 22 "  35 23 #  36 24 $  37 25 %  38 26 &  39 27 '  40 28 (  41 29 )  42 2a \* | Dec Hex Char  43 2b +  44 2c ,  45 2d -  46 2e .  47 2f /  48 30 0  49 31 1  50 32 2  51 33 3  52 34 4  53 35 5 | Dec Hex Char  54 36 6  55 37 7  56 38 8  57 39 9  58 3a :  59 3b ;  60 3c <  61 3d =  62 3e >  63 3f ?  64 40 @ | Dec Hex Char  65 41 A  66 42 B  67 43 C  68 44 D  69 45 E  70 46 F  71 47 G  72 48 H  73 49 I  74 4a J  75 4b K | Dec Hex Char  76 4c L  77 4d M  78 4e N  79 4f O  80 50 P  81 51 Q  82 52 R  83 53 S  84 54 T  85 55 U  86 56 V | Dec Hex Char  87 57 W  88 58 X  89 59 Y  90 5a Z  91 5b [  92 5c \  93 5d ]  94 5e ^  95 5f \_  96 60 `  97 61 a | Dec Hex Char  98 62 b  99 63 c  100 64 d  101 65 e  102 66 f  103 67 g  104 68 h  105 69 i  106 6a j  107 6b k  108 6c l | Dec Hex Char  109 6d m  110 6e n  111 6f o  112 70 p  113 71 q  114 72 r  115 73 s  116 74 t  117 75 u  118 76 v  119 77 w | Dec Hex Char  120 78 x  121 79 y  122 7a z  123 7b {  124 7c |  125 7d }  126 7e ~ |

1. List the TCP/IP layer that most closely aligns with the below technology:

nslookup \_\_Application\_\_\_

IP Address \_\_\_Network\_\_\_\_

Wires \_\_\_Physical\_\_\_

802.11 \_\_Data Link\_\_\_

TCP \_\_\_Transport\_\_\_\_

Port numbers \_\_\_Transport\_\_\_\_

Browser \_\_\_Application\_\_\_

MAC Address \_\_\_Data Link\_\_\_

Radio Waves \_\_\_Physical\_\_\_

1. What two TCP/IP layers will be different for wireless communications than for wired communications? Explain why the other layers remain the same.

Only Physical and Data Link layers will differ. The others stay the same because wireless communication only affects the local area network. All other communication outside of the local area network is the same as if it were a wired communication.

1. Matching:

\_C\_ Domain name A. Uniquely identifies a host. May change over time.

\_A\_ IP address B. Uniquely identifies a network adapter. Does not change.

\_B\_ MAC address C. Easy to remember by humans.

\_E\_ Subnet Mask D. Name for a set of wireless base stations.

\_D\_ ESSID E. Number that reveals a network address in an IP address

1. What do the following provide:
   1. ARP: It is the Address Resolution Protocol & translates IP addresses to MAC addresses and vice versa. It acts as the “phone book” for the local area network.
   2. DNS: Operates on port 53. Provides domain name resolution – it is the “phone book” that domain names into IP addresses.
   3. Router: Passes packets across the Internet towards their desired destination. Routers are most closely associated with the Network Layer in the TCP/IP stack
2. WEP, WPA, and WPA2 are used to solve what two problems we don’t have when we have strictly wired networks:

WEP, WPA, and WPA2 solve the problems of: controlling who can join a wireless network, and provide Confidentiality from people who have not joined the network but are in range of the wireless transmissions

1. For this piece of code, answer the following questions:

<HTML>

<HEAD></HEAD>

<BODY>

<FORM name="bio">

<P>

Last Name <INPUT type="text" name="last" value="Doe">

</P>

<P>

Age in Years <INPUT type="text" name="age" value="25">

</P>

</FORM>

</BODY>

</HTML>

1. What is the form name? bio
2. What is the name of the first input box? last
3. What is initially displayed for the value of Age in Years? 25
4. A webpage has a FORM which allows users to enter input. The webpage does not validate user input. Entering data results in a server-side script being executed that depends on this data. The script loops forever (infinite loop) if the user provides bad input. Who gets harmed more by the bad input? The user or the web server owner? Explain why?

Web server owner because the script will crash server, hence making the server inaccessible to others.

1. Explain the difference between TCP and UDP. Also provide an example of a service where TCP would make more sense to use than UDP and explain why.

TCP is a connection oriented protocol that is reliable. UDP is connectionless and there is no guarantee packets arrive at their destination. SMTP (email) is an example of a TCP protocol. You want assurance that your email packets arrived and in the proper order.

1. For the following URL, answer the following questions:

http://www.dominos.com/orderpizza.jsx?size=large&one=pineapple&two=sausage&three=mushrooms

* 1. What type of script is this using? Server side script
  2. What do you think this URL is requesting? Be specific.

One large pizza with 3 toppings to include pineapple, sausage, and mushrooms, from dominos.com.

1. In your own words describe the security benefits of employing Network Address Translation on a network.

NAT hides the IP addresses of the hosts behind the default gateway from people outside the network. This makes it harder for an attacker to target a specific host inside the network.

1. Assume the following:

Your IP address is 10.131.46.22

Port that your laptop uses to send information out: 41321

Your Gateway router IP address is 10.131.46.1

Port your Gateway router uses to send information out: 32765

ESPN.com server IP address is 192.168.22.135

You would like to go to ESPN.com to see the score of the Indians-Cubs game, so you type <http://www.espn.com/> in your web browser. Given the above information, and assuming your Gateway router employs Network Address Translation, if you typed netstat –an in an administrator shell after you went to espn.com, what would you most likely receive as a response (circle the correct answer):

* 1. TCP 10.131.46.22:32765 192.168.22.135:80 ESTABLISHED
  2. TCP 10.131.46.22:80 192.168.22.135:32765 ESTABLISHED
  3. TCP 10.131.46.22:41321 192.168.22.135:80 ESTABLISHED
  4. TCP 10.131.46.1:41321 192.168.22.135:80 ESTABLISHED
  5. TCP 10.131.46.1:32143 192.168.22.135:80 ESTABLISHED

1. In symmetric cryptography, a Chosen Plaintext Attack involves two known values that are combined to obtain a third unknown value. What are the two known values and what is the third unknown value?

The two known values in a Chosen Plaintext Attack are plaintext and ciphertext. The unknown value is the key.

Given the following set of commands run in a Windows Command Prompt, answer 13:

* Ipconfig

Windows IP Configuration

IPv4 Address: 10.53.37.113

Subnet Mark: 255.255.255.0

Default Gateway:

* Arp –a

Interface: 10.53.37.113

Internet Address Physical Address

10.53.37.1 00-0e-ed-3f-f5-bd

10.53.37.122 00-e3-f4-d1-15-90

10.53.37.153 00-e4-5f-44-5a-a8

10.53.37.99 12-98-ed-f1-78-bc

* Tracert –d 192.168.72.3

Tracing route to 192.168.72.3

1. <1 ms <1 ms <1 ms 10.53.37.1
2. <1 ms <1 ms <1ms 10.48.1.94
3. 2 ms <1 ms <1 ms 192.168.72.1
4. <1 ms < 1 ms 1 ms 192.168.72.3
   1. What is the IP address of the local host?

10.53.37.113

* 1. What is the MAC address of the local host’s Gateway router?

00-0e-ed-3f-f5-bd

* 1. What is the IP address of the destination host?

192.168.72.3

For questions 14-17, circle (T) True or (F) False:

1. (T / F) When hiding information in a picture file using steganography, it is better to hide the data in the least significant bits of a byte because those bits have less influence over the quality of the picture than higher order bits.
2. (T / F) An event-driven script executes immediately once a webpage loads.
3. (T / F) If I input the value <U>Watch Out!</U> into a website form, and the website displays this as Watch Out!, then I know the website is vulnerable to HTML injection attacks.
4. (T / F) Cookies are used to store user credentials (usernames, passwords, etc.) on the server side.
5. Fill in the blanks: Cross-Site Scripting is a combination of \_injection\_ and \_reflection\_. Sending an email with an embedded html link that when executed will transfer money from the victim’s bank account to your account if the victim is \_logged into\_ their bank account when clicking on the link, is an example of Cross-Site Scripting. The Cyber Security pillar of \_Integrity\_ is violated in this example because the amount of money in the victim’s account was modified.
6. Alice wants to send a confidential message to Bob using asymmetric encryption **AND** sign the message (also using asymmetric encryption) so that Bob can reasonably assume it came from Alice.
   1. What key would Alice use to encrypt the contents of the message to provide confidentiality?

Bob’s public key

* 1. What key would Alice use to sign/encrypt the message to provide authentication?

Alice’s private key

* 1. What key would Bob use to validate that the message came from Alice?

Alice’s public key

* 1. What asymmetric encryption algorithm is most commonly used across the Internet? RSA

1. If Eve intercepted the message in #19 AND was able to change the message while it was in transit to effectively say something different than what Alice had intended, what pillar of cyber security would Eve have violated?

Integrity

1. What pillar of Cyber Security is most associated with encryption?

Confidentiality

1. What is the biggest problem with symmetric key encryption? Explain your answer.

Key exchange (or key distribution) – With symmetric key encryption, there is one secret key. Only the sender and receiver should know this key. Securely getting this key to the receiver can be a challenge in symmetric cryptography.

1. Matching: Match the terms with the definitions below.
   1. Firewall
   2. Intrusion Detection System
   3. Intrusion Prevention System
   4. Email Security Gateway
   5. Defense in Depth

\_b\_ Similar to a firewall, it monitors network traffic for suspicious activity

\_a\_ Network security device that monitors incoming and outgoing network traffic

\_e\_ A strategy employed by network administrators to deploy multiple layers of defense

\_c\_ Monitors network traffic and takes action if malicious activity is detected

\_d\_ Prevents transmission of emails with malicious intent

1. Which of the following javascript statements would allow a user to provide input and save it to the variable r. Circle the correct answer.
   1. var r = input(“Enter a number”);
   2. var r = alert(“Enter a number”);
   3. var r = prompt(“Enter a number”);
   4. var r = ask(“Enter a number”);
2. What would be the value of x after the following lines of code were executed?

var x = 1;

var n = 0;

while(n < 4)

{

if( n < 3 )

{

x = x + n;

}

n = n + 1;  
}

x=4

OLD STUFF

For the next three questions, a network is a set of hosts with the same network address.

1. When host A needs to send a packet to host B, it calculates their respective network addresses by combining what values.

IPv4 address and subnet mask

1. If host A determines host B is on the same network, host A sends the packet with a destination \_MAC address\_ for host B and the destination MAC address for: the default gateway router.
2. If host A determines host B is on a different network, host A sends the packet with a destination \_IP address\_ for host B and the destination MAC address for: default gateway router.