TEAMS Competition 2013
Scenario 1: Phishing, grades 6–8 Solutions

Questions

1. Which of the following methods best interrupts activities at Step 4 of the phishing cycle, when a hacker poses as the legitimate user?

2. Which graph represents the target ability of the new filtering program?

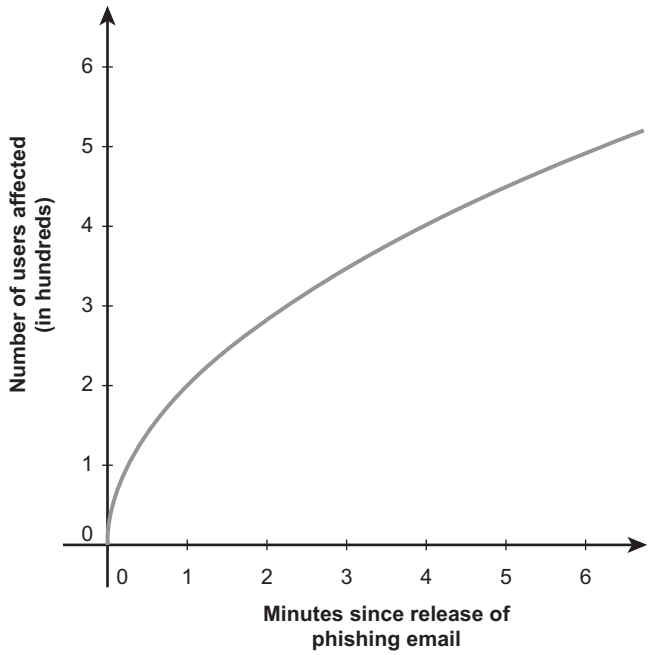
3. After 54 hours, how many people have responded to the phishing email by clicking on the link?

4. Exactly one hour after the release, how many email messages have bypassed the filters?

Solutions

1. E. implement a two-step login process, so users need to enter a password and other identifying information, such as preset security answers. [correct; this answer makes it harder for hackers to use stolen passwords]

2. D. [correct; this graph is a reflection about the line $y = x$]



3. C. 11,508 people [correct]

$n = 4t^2 - 3t + 6$
$n = 4(54)^2 - 3(54) + 6$
$n = 4(2{,}916) - 3(54) + 6$
$= 11{,}664 - 162 + 6$
$= 11{,}508$ people

4. B. 10,330 messages have bypassed the filters [correct]

$3t^2 - 8t + 10 = 3(60)^2 - 8(60) + 10$
$= 3(3{,}600) - 8(60) + 10$
$= 10{,}300$ messages have bypassed the filters

© Technology Student Association (TSA)

Questions

5. Determine the likelihood that the browser tool accurately identifies a suspicious link if the link is tested $t = 100$ times.

6. How many phishing attempts via mapped links remain undetected?

7. A phishing email is designed to attack user accounts with a series of email messages over a period of time. The sequence of attempts begins with five messages on day 1 and doubles each following day. How many total phishing emails will be delivered by the end of day 10?

8. Determine how many email messages the account receives after five hours.

Solutions

5. E. 92% accuracy [correct]

Likelihood of accurate identification

$$= 1 - \frac{108t - t^2}{t^2}$$
$$= 1 - \frac{108(100) - (100)^2}{(100)^2}$$
$$= 1 - \frac{10{,}800 - 10{,}000}{10{,}000}$$
$$= 1 - \frac{800}{10{,}000}$$
$$= 0.92 \cdot 100$$
$$= 92\% \text{ accuracy}$$

6. C. 405 phishing attempts remain undetected [correct]

$$\frac{45}{1{,}000} = \frac{x}{9{,}000}$$
$$45 \cdot 9{,}000 = 1{,}000 \cdot x$$
$$x = \frac{45 \cdot 9{,}000}{1{,}000}$$
$$= 405 \text{ phishing attempts remain undetected}$$

7. D. 5,115 phishing emails are delivered [correct]

$$S_{10} = \frac{a_1(1 - r^n)}{1 - r}$$
$$= \frac{5(1 - 2^{10})}{1 - 2}$$
$$= \frac{5(1 - 2^{10})}{-1}$$
$$= \frac{5(2^{10} - 1)}{1}$$
$$= 5(1{,}203)$$
$$= 5{,}115 \text{ phishing emails delivered}$$

8. C. 3,483 messages [correct]

$$2n^3 + 15n^2 - 4n + 23 = 2(10)^3 + 15(10)^2 - 4(10) + 23$$
$$= 2(1{,}000) + 15(100) - 40 + 23$$
$$= 2{,}000 + 1{,}500 - 40 + 23$$
$$= 3{,}483 \text{ messages}$$

© Technology Student Association (TSA)

Questions

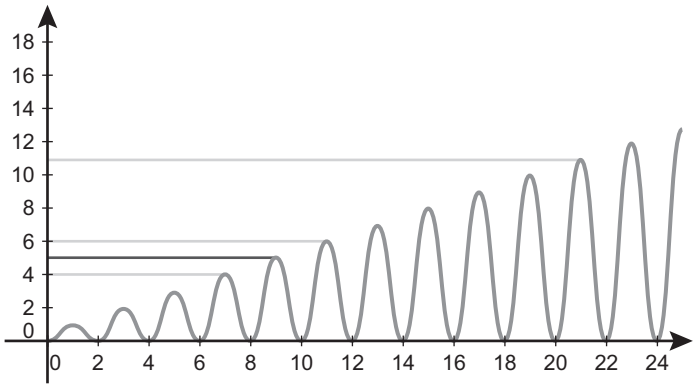
9. To the nearest hundreds place, estimate the number of users affected by a phishing email attempt occurring at 9 a.m.

10. How many permutations are possible?

Solutions

9. C. 500 users [correct]

For this grade band, this is basically a graph-reading question. The graph below shows the estimates corresponding to the answer choices (red is the correct answer).



10. D. 456,976 permutations [correct]

$26^4 = 456{,}976$ permutations

 © Technology Student Association (TSA)

TEAMS Competition 2013
Scenario 2: Web Application Attacks Solutions

Questions

11. How many attack attempts does the hacker make on application B?

12. How many targets has the hacker identified after the fifth worm attack?

13. How many adjustments are required to reduce the threat of vulnerability to attacks to zero?

14. If four applications on the social networking site use the register_ globals feature, how many remote code execution attacks are likely to occur?

Solutions

11. A. 320 attack attempts [correct]

The total attack attempts can be represented by $A + B = 1{,}600$. Since A received 4 times the attacks as B, $A = 4B$. Substitute $A = 4B$ into the equation $A + B = 1{,}600$ and solve for B.

$$\begin{aligned} A &= 4B \\ A + B &= 1{,}600 \\ 4B + B &= 1{,}600 \\ 5B &= 1{,}600 \\ B &= 320 \text{ attack attempts} \end{aligned}$$

12. D. 80 targets [correct]

4, 9, 15, 22, x
The sequence shows the interval of increase of 1 between each attack.
First interval increase = 5
Second interval increase = 6
Third interval increase = 7
Fourth interval increase = 8
The sequence, then, is 4, 9, 15, 22, 30
The fifth number in the sequence is 30
4 + 9 + 15 + 22 + 30 = 80 targets

13. C. 15 adjustments [correct]

To find the number of adjustments required to reduce the threat to zero, set the likelihood, y, equal to zero and simplify the equation.

$$\begin{aligned} 120 - 8x &= y \\ 120 - 8x &= 0 \\ 120 &= 8x \\ x &= 15 \text{ adjustments} \end{aligned}$$

14. D. 81 attacks [correct]

Find $g(4)$.

$$\begin{aligned} g(x) &= 3^x \\ g(4) &= 3^4 \\ &= 81 \text{ attacks} \end{aligned}$$

© Technology Student Association (TSA)

Questions

15. Of the following options, which type of webpage is the most at risk to a cross-site scripting attack?

16. What is the maximum number of "red flags" that the program catches at time $x = 10$ seconds?

17. What is the average number of attacks per day?

18. A user enters the numerical expression $\frac{2(3) + 4}{3 + 1}$ into the variable cell. What is the numerical output that results from the hacker's intrusion?

19. Which error message is the most effective in preventing a hacker from guessing a valid username?

Solutions

15. B. the login page of an interactive game [correct; this type of webpage requires heavy user input]

16. A. 15 flags [correct]

Solve the given equation for $x = 10$.

$$\begin{aligned} f(x) &= -x^2 + 20x - 85 \\ f(10) &= -(10)^2 + 20(10) - 85 \\ &= -100 + 200 - 85 \\ &= 15 \text{ flags} \end{aligned}$$

17. B. 3 attacks per day [correct]

Find the rate of change for the number of attacks between day 2 and day 7.

$$\begin{aligned} \frac{y_2 - y_1}{x_2 - x_1} &= \frac{16 - 7}{5 - 2} \\ &= \frac{9}{3} \\ &= 3 \text{ attacks per day} \end{aligned}$$

18. B. 0.4 [correct]

Simplify the input expression and substitute it for x in the function $g(x)$.

$$\begin{aligned} \frac{2(3) + 4}{3 + 1} &= \frac{10}{4} \\ &= \frac{5}{2} \end{aligned}$$

$$\begin{aligned} g\left(\frac{5}{2}\right) &= \frac{1}{\frac{5}{2}} \\ &= \frac{2}{5} \\ &= 0.4 \end{aligned}$$

19. A. "This username/password combination is not valid" [correct; this statement does not state which is valid, the username or the password]

 © Technology Student Association (TSA)

Questions

20. A hacker receives nine error messages. Approximately how many tries does it take for the hacker to figure out a given username?

Solutions

20. B. 188 tries [correct]

Solve $f(x)$ for $x = 9$.

$f(x) = 3x^2 - 5x - 10$
$f(9) = 3(9)^2 - 5(9) - 10$
$= 3(81) - 45 - 10$
$= 243 - 55$
$= 188$ tries

© Technology Student Association (TSA)

TEAMS Competition 2013
Scenario 3: Wireless Network Breaches Solutions

Questions

21. How many times has the company changed its key after the third week of using WEP encryption?

22. Determine the percent likelihood of being hacked when the company switches to WPA.

23. A casual user is within the range of the business's wireless signal. How does the network name now appear on the wireless network sensor?

24. How many possible targets must the scanner identify for the hacker to complete one successful attack?

25. What is happening when each wave peaks?

Solutions

21. D. 30 times [correct]

Substitute 3 for x in the equation and simplify.

$$f(x) = 2x^2 + 4x$$
$$f(x) = 2(3)^2 + 4(3)$$
$$= 18 + 12$$
$$= 30 \text{ times}$$

22. B. 20% [correct]

$$f(x) = \frac{3(x + 500) - 280}{x + 10}$$

$$f(60) = \frac{3(60 + 500) - 280}{60 + 10}$$

$$= \frac{3(560) - 280}{70}$$

$$= \frac{1400}{70}$$

$$= 20\%$$

23. E. none of the above [correct; the network name does not appear]

24. C. 6 possible targets [correct]

Set $f(x)$ equal to 1 and solve for x.

$$f(x) = 1 = 5(x - 6) - (x - 7)$$
$$1 = 5x - 30 - x + 7$$
$$1 = 4x - 23$$
$$24 = 4x$$
$$x = 6 \text{ possible targets}$$

25. A. there are more Internet users during this time period at the bus stop [correct]

© Technology Student Association (TSA)

Questions

26. What percentage of businesses uses MAC filtering?

27. Using 3.14 for pi (also used in its Greek form as π), what is Smith & Co.'s total area (in miles) of wireless coverage?

28. Given the area of the building, what is the smallest WLAN transmitter diameter that includes the entire building?

29. Which of the following passwords is the **strongest** choice?

30. What is the value of x as the hyperbola reaches the bottom of its curve?

Solutions

26. A. 40% [correct]

To find the percent of businesses that use MAC filtering, find the total number of businesses. Then divide the number of MAC filtering businesses by the total number of businesses.

$$\frac{1{,}400}{2{,}100 + 1{,}400} = 40\%$$

$$\frac{1{,}400}{3{,}500} = 0.4$$

$$0.4 \cdot 100 = 40\%$$

27. C. 50.24 mi² [correct]

The outer limit of the business's coverage is represented by the equation $(x - 3)^2 + (y - 2)^2 = 16$
The circle has a radius of 4. The area of a circle is found using the equation $A = \pi r^2$. Substitute 3.14 for π and 4 for r and simplify.

$$\begin{aligned} \text{Area} &= \pi \cdot r^2 \\ &= 3.14 \cdot 4^2 \\ &= 3.14 \cdot 16 \\ &= 50.24 \text{ mi}^2 \end{aligned}$$

28. C. 50 feet [correct]

The diameter of the circle needed for this problem is found by calculating the distance from opposite corners of the rectangle. The Pythagorean Theorem is used to find the measurement of the diameter.

$$\begin{aligned} a^2 + b^2 &= c^2 \\ 30^2 + 40^2 &= c^2 \\ 900 + 1{,}600 &= c^2 \\ 2{,}500 &= c^2 \\ c &= 50 \text{ feet} \end{aligned}$$

29. D. X@nder3L [correct; this password includes the name *Xander*, but it changes a letter to a symbol and it adds a number and a letter, both of which make it harder to guess]

30. E. infinity [correct]

The graph approaches zero, but never crosses the x-axis.

© Technology Student Association (TSA)

TEAMS Competition 2013
Scenario 4: Wi-Fi Hotspots Solutions

Questions

31. Which ordered pair below represents the location of the hacker?

32. Clara plans to check her personal email and browse the Web while relaxing in one of the locations. Although she does not mind paying for Wi-Fi, she doesn't want to pay a lot to use it. In addition, security is not the highest concern regarding her choice in network. Which Wi-Fi network is the **best** choice for Clara, based on her security needs, risk tolerance, and spending preferences?

33. Which of the following statements is true?

34. To the nearest tenth, what is the speed of the business traveler's Internet connection?

35. In terms of the number of attacks made, at what point are the two firewalls equally effective?

Solutions

31. C. (3,−2) [correct]

32. B. Nelson's Bookstore [correct; this location offers the best blend of low cost and reasonable protection for Clara, who is only planning to check personal email and surf the Web]

33. A. Andy is four times more likely to be hacked than Diane [correct]

To find out how much more likely Andy is to be hacked, divide the chance of Andy getting hacked by the chance of Diane getting hacked.

$\frac{60\%}{15\%}$ = 4 times more likely to be hacked than Diane

34. D. 37.8 megabits per second [correct]

The traveler's speed is reduced by 30%. Find the traveler's Internet connection speed by subtracting the reduction from 100% and then multiplying the percent by the original speed.

$100\% - 30\% = 70\%$
$54 \cdot 70\% = 37.8$ megabits per second

35. C. 5 attacks [correct]

To find out the point at which the two firewalls are equally effective, set the equations equal to each other and solve for n.

$f(n) = 6n + 10$
$g(n) = 3n + 25$
$6n + 10 = 3n + 25$
$3n = 15$
$n = 5$

© Technology Student Association (TSA)

Questions

36. For a 10-hour period, how many more attacks must be blocked by your team's firewall program to meet the design goal?

37. After a year has passed, what is the percent difference in vulnerability for the user?

38. What is the percent difference in the user's vulnerability after three hours?

39. Which of the following behaviors reduces a user's vulnerability to cyber attacks through public Wi-Fi hotspots?

40. In five years, what is the expected rate of change (in percentage) of business travelers who are likely to use NAS devices?

Solutions

36. B. 10 attacks [correct]

Find the number of attacks blocked by the competing program after 10 hours. Then multiply that number by 5% to find out how many more attacks must be blocked to meet the goal.

$$\begin{aligned} r(t) &= 16t + 40 \\ r(10) &= 16(10) + 40 \\ r(10) &= 160 + 40 \\ r(10) &= 200 \\ 200 \cdot 0.05 &= 10 \text{ attacks} \end{aligned}$$

37. B. 27.58% [correct]

The user's vulnerability is reduced each month by installing updated patches monthly. The percent is reduced by 5% each month, so the percent of vulnerability is multiplied by (1 – 0.5) for each month. Find the percent of reduction after a year and subtract this from the original percent to find the percent difference.

$$\begin{aligned} 0.60 \cdot (1 - 0.05)^{12} &= 0.60 \cdot 0.54036 \\ &= 0.3242 \\ 0.3242 \cdot 100 &= 32.42\% \\ 60\% - 32.42\% &= 27.58\% \end{aligned}$$

38. B. 22% [correct]

Substitute 3 for ***t*** in the equation and simplify. Then find the difference by subtracting the user's vulnerability from the percent of a successful attack

$$\begin{aligned} f(3) &= -6(3) + 86 \\ &= -18 + 86 \\ &= 68 \\ 90\% - 68\% &= 22\% \end{aligned}$$

39. C. using encrypted website protocols [correct]

40. E. 23% [correct]

Substitute 5 for *t* in the equation and simplify.

$$\begin{aligned} f(5) &= 2(5)^2 - 7(5) + 8 \\ &= 2(25) - 35 + 8 \\ &= 50 - 35 + 8 \\ &= 23 \end{aligned}$$

 © Technology Student Association (TSA)