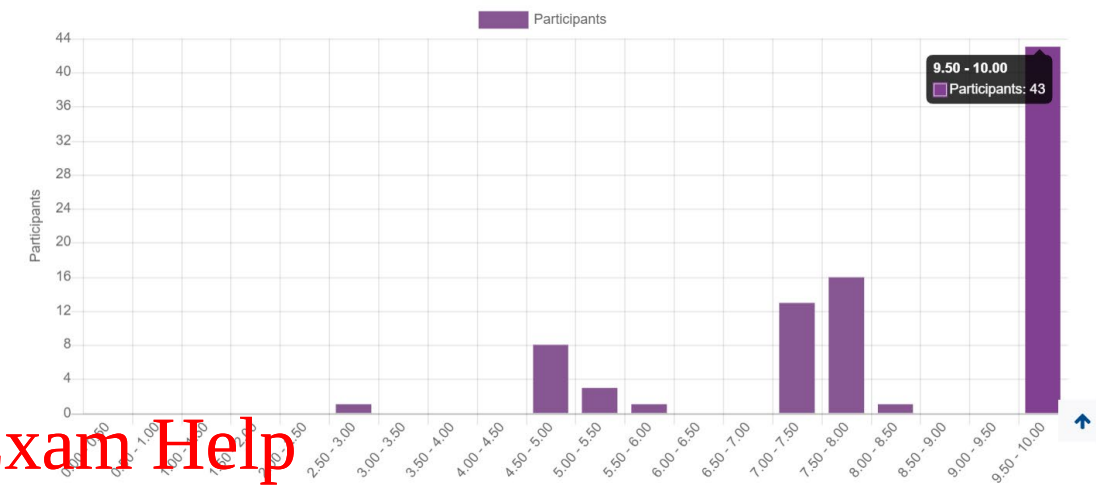
Quiz 2 - statistics

of participants: 87 / 100

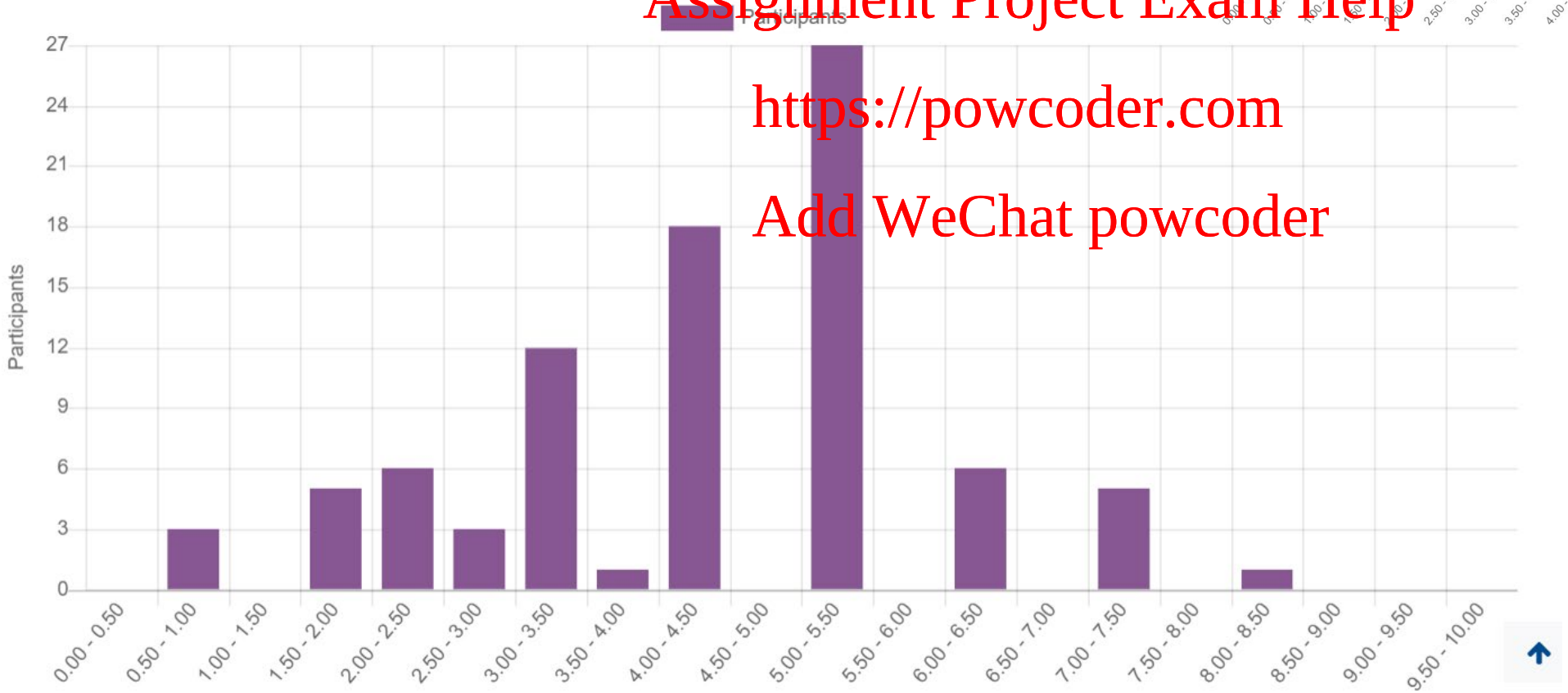
average: 5.24 / 10



Assignment Project Exam Help

https://powcoder.com

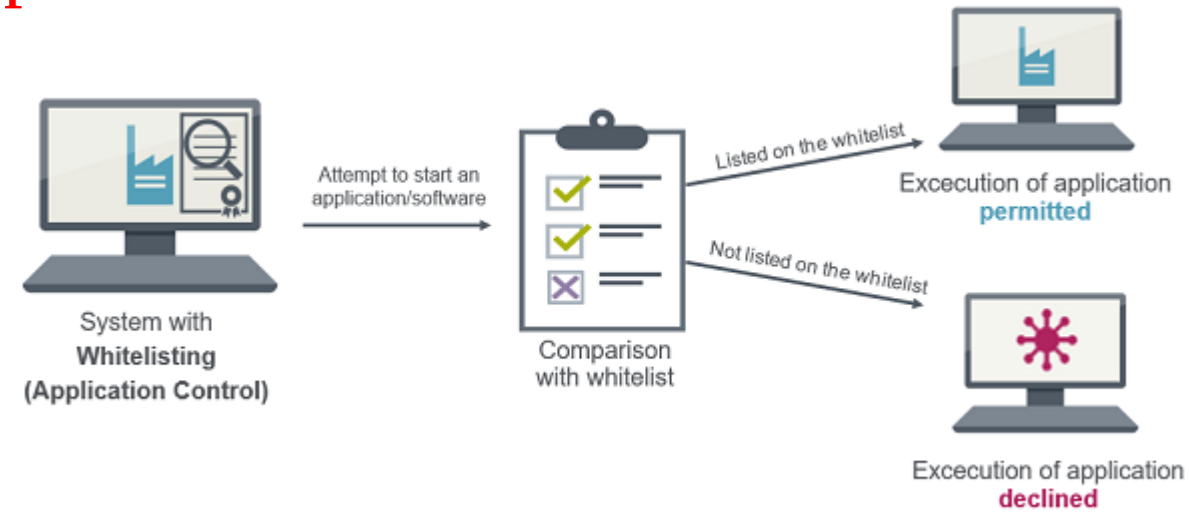
Add WeChat powcoder



A piece of software has been tested against a ‘whitelist’ of known program binaries, and no match is found. This implies that the given piece of software is:
(check everything that applies)

1) 100% malicious -20% of grade
2) 100% benign -20% of grade
3) potentially malicious 60% of grade
4) potentially benign 40% of grade
5) none of the above -20% of grade

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder



Choose the most appropriate word, out of the 4 offered choices, to complete the following statement: "National Institute of Standards and Technology (NIST) recommends the use of _____ in high-risk security environments, where the integrity (i.e., security) of individual or connected systems/computers is critical and takes priority over any restrictions that users might suffer in their choice or access to software."

1) software blacklisting
2) software whitelisting
3) static software analysis
4) dynamic software analysis

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

National Institute of Standards and Technology

Which type of computer virus is most likely to avoid detection by means of 'dynamic malware analysis'?

1) polymorphic virus
2) encrypted virus
3) metamorphic virus
4) stealth virus

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Metamorphism is a technique that mutates the dynamic binary code to avoid detection. It changes the opcode with each run of the infected program and does not use any encryption or decryption. The malware never keeps the same sequence of opcodes in the memory. This is also called *dynamic code obfuscation*. There are two kinds of metamorphic malware defined in [21] based on the channel of communication used: *Closed-world malware*, that do not rely on external communication and can generate the newly mutated code using either a binary transformer or a metalanguage. *Open-world malware*, that can communicate with other sites on the Internet and update themselves with new features.

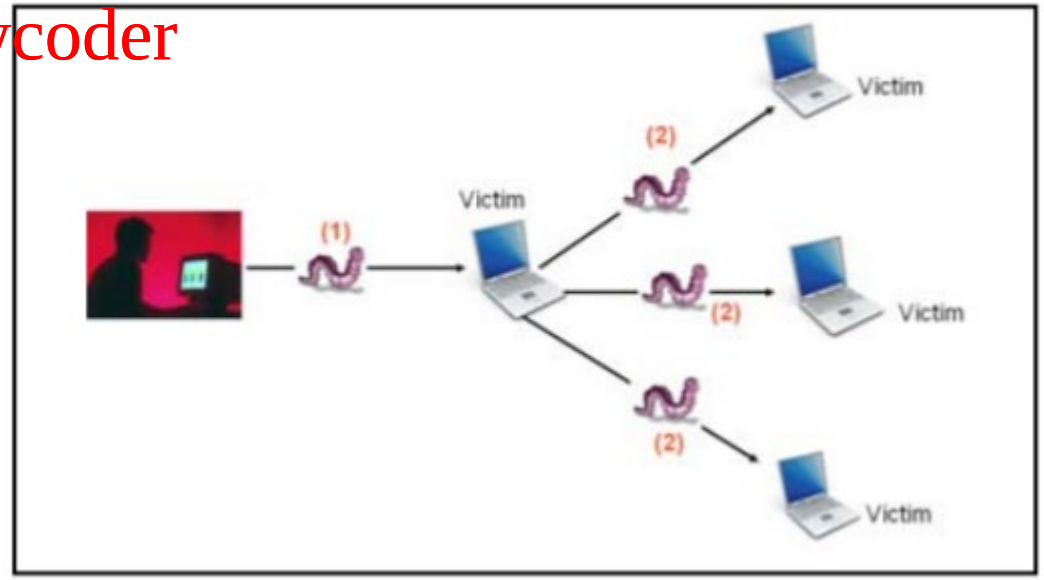
Philip OKane, Sakir Sezer, and Kieran McLaughlin. Obfuscation: The Hidden Malware. IEEE Security and Privacy, 9(5):41 – 47, September 2011

Which type of computer-worm ‘target discovery’ strategy is likely to result in the slowest initial rate of spread/infection?

1) random — slowest since (many) probed machines may not be vulnerable, but geographically most spread …
2) hit-list — fastest, since machines on the hit-list are almost certainly vulnerable …
3) topological — reasonably fast, but limited by the number of topological connections of infected machines …
4) local subnet — reasonably fast, but geographically limited to one network …

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Since the question did not talk about any extra/specific conditions for any of the strategies, you should assume that all strategies operate under the same conditions – e.g., no firewall present, each infected machine ‘probes’ the same number of other machines, etc.
So, if with random strategy 100 machines are probed, but only 30% are vulnerable, it means only 30 machines will be successfully infected.
On the other hand, if with hit-list strategy 100 machines are probed, and 99% are vulnerable, it means 99 new machines will be successfully infected.
Over time this results in much faster rate of infection with hit-list vs. random strategy …



Consider a computer worm that uses a combination of the 'random' and 'local network' propagation model. In particular, upon infecting a machine in a network, in each subsequent minute the worm attempts to infect 5 other local and 5 random non-local machines (10 machines in total).

Assume this worm infects one YorkU machine at time t=0. (There is no other infection involving this worm anywhere in the Internet at this time.) What is the maximum number of non-YorkU machines infected with this worm by the end of the 2nd minute?

Assignment Project Exam Help

How about the 'minimum' number ??

How about the 'average' number ??

1) 10

2) 20

3) 35

4) 55

Omission was made in my initial calculation – **the number should have been 85.**

Everybody will receive full grade for this question.

https://powcoder.com

Add WeChat powcoder

Note: one could claim that in this question, during the 2nd minute, some of the 5 non-York machines could be trying to infect (back) some of York machines, so 5*10 in the second expression would be an overestimation. While theoretically correct, this observation is not relevant since the question asks for 'maximum' (worst case) number of infected non-York machines – and the 'maximum' case happens when every non-York machine attempts to infect 10 other non-York machines …

The answer/logic would be different if the question asked for the minimum or the average number …

Solution – number of non-York machines infected:

1st minute: 0 old + 5 new infected = 5 infected machines

2nd minute: 5 old + 5*10 new infected + 6*5 = **85 infected machines**

5 non-York machines from 1st minute each infecting 10 new non-York machines

(1+5) York machines from 1st minute each infecting 5 new non-York machines