BRAINWARE UNIVERSITY

Term End Examination 2022
Programme – B.Sc.(ANCS)-Hons-2020
Course Name – Threat Modeling, Risk Assessment and Management
Course Code - BNCSD501A
(Semester V)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) A hacker commits an ____attack by tracking one device into sending messages to the hacker instead of the intended recipient. Speculate the right one.

a) DNS Spoofing. b) ARP Spoofing.
c) DDoS attack. d) DOS Flood.

(ii) Cite which one does not fall among OWASP Top 10 Risks as:

a) Injection. b) Cross Site Request Forgery.
c) Spoofing. d) None of the above.

(iii) Discover the amount of information about the identity of the participants that is revealed in a transaction is measured by

a) The Nymity Slider. b) Privacy Impact Assessments.
c) Contextual Integrity. d) None of the above.

(iv) Advantages of _____to protects the user from getting bad data from a signed zone by detecting the attack and preventing the user from receiving the tampered data. Recognize.

a) DNSSEC. b) SYNC FLOODING.
c) IPSec. d) ACL.

(v) Online attacks against the login system, is termed as_____. Identify.

a) Threats to Passwords. b) Repudiation Attack.
c) All of the above. d) None of the above.

(vi) A model of biometric authentication consist authenticators with _____ for authentication measures with response. Discover.

a) Hardware b) Software
c) Sensors d) None of the above.

(vii) Developer must implement _____ to design to minimize DoS risks for Denial of Service Threat. Interpret.

a) Front Ends b) Back Ends
c) All of the above. d) None of the above.

(viii) Predict which Logs (Log analysis) must be protected for the following threat:

a) Tampering. b) Repudiation.
c) Information Disclosure. d) None of the above.

(ix) They do not have any real system knowledge, they only know how to follow instructions using different available tools. Analyze.

a) The undergraduate. b) The Expert.
c) The Script Kiddie. d) None of the above.

(x) Conclude that "SYNC Flood" attack is commonly famous for:

a) TCP/IP DoS ATTACK. b) ICMP Attack.
c) Both of the above. d) None of the above.

(xi) Identify the Causes for Threat Modeling are:

a) Find Security Bugs Early. b) Understand your Security Requirements.
c) Engineer and Deliver Better Products. d) All the above

(xii) To address Denial of Service threat, the Security Expert can utilize_____. Identify.

a) Networking Flooding. b) Synchronization.
c) Elastic resource. d) None of the above.

(xiii) Consider the subset of buffer overflow in which the attacker overwrites the program stack, leading to a change in control flow is termed as_____

a) Stack smashing b) SIPRNet
c) SDL d) RFC

(xiv) _____ is the act of denying responsibility for an action. Choose.

a) Repudiation b) Augthentication
c) Authorization d) None of the above.

(xv) It is one ideal cloud-based filtering service to protect one organization against spam, malware and other email threats. Locate.

a) Stepping stones. b) EOP.
c) Whiteboard Diagramming. d) None of the above.

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Illustrate the Threat Applicability for STRIDE-per-interaction scenario. (3)
3. Explain Access Control and various types of Access Control. (3)
4. Discover Information Disclosure Threat and how to mitigate the same. (3)

OR

Judge the different types of application of Elastic Resources. (3)

5. Classify Attack Tree? Explain one Attack Tree for spoofing a process. (3)

OR

Explain one Attack Tree for spoofing a data flow. (3)

6. Express about CAPTCHA. (3)

OR

Write about DNS Spoofing with an example. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. For the same institution offering such services, please draw State Diagram and explain as the Cyber Security Expert to focus the strategy for threat modelling. (5)
8. Discuss Tampering Threats from the perspective of an Attacker. (5)
9. Write about Attack Tree with an example for a real life Threat occurring in Cyber Space. (5)
10. Prepare and correlate Account Recovery Checklist for addressing Accounts and Identity. (5)
11. Explain Account Life Cycles. (5)

OR

Explain the attributes for modelling Social Engineering Attacks in Cyber Space. (5)

12. Justify Assets. Explain components of Asset-Centric Modeling. (5)

OR

Reframe Threat Trees for Spoofing an External Entity (Client/Person/Account). (5)

****