Computer System Security Question Bank

Unit-1

Priyanka Tiwari
Asst Professor
(CSE)

SHORT QUESTIONS

① What is computer security?
② Define vulnerability
③ Differentiate b/w ransomware, virus, trojahorse, worm
④ What do you mean by zero day vulnerability?
⑤ What is control hijacking?
⑥ Define NOP slide.
⑦ Define canary.

LONG QUESTIONS

① What is computer security? For implementing a security plan what guideline one should follow.
② What are limitation of threat model assumption. What to do avoid limitation in threat model
③ Explain sample Attacks
④ Explain control hijacking attacks
⑤ Explain Buffer Overflow vulnerability.
⑥ " Integer " "
⑦ " Format String " .
⑧ Explain about defense mechanism from vuln. hijacking
⑨ Discuss some advance control attacks?

Unit-2

SHORT QUESTIONS

① Define privilege escalation attack
② Define confidentiality policy
③ Differentiate b/w DAC & MAC
④ What are subjects & objects in UNIX
⑤ Define terms euid, egid, ruid, rgid, suid, sgid.
⑥ What are the uses of suid/sgid bits.
⑦ What is NaCl?
⑧ Define Virtual Machine Monitor
⑨ Define covert channel

(10) Differentiate b/w Binary rootkit & library rootkit
(11) Define the term IDS

LONG QUESTIONS

(1) Explain Virtual Machine Isolation.
(2) What is VMM Introspection? How it is performed?
(3) Explain the concept of Bluepill & Redpill
(4) Explain about SFI approach.
(5) What are the purpose of rootkits?
(6) Discribe the types of rootkits.
(7) Explain the techniques for rootkit detection & recovery.
(8) Define IDS. Explain different types of IDS.
(9) Why confidentiality Policy is used? How many types of policies you have studied?
(10) How can bi confinement principles implemented?
(11) Briefly discribe about UNIX User IDs & Process IDs.
(12) Explain Jail Environment in FreeBSD.
(13) Explain the concept of SCI.

Unit-3

SHORT QUESTIONS

(1) Define access control.
(2) Differentiate b/w monolithic & component based design.
(3) Define the term identification, authentication & authorization.
(4) Who are different actors of access control.
(5) Differentiate b/w access control matrix & access control list.
(6) Differentiate b/w access control list & capabilities.
(7) ~~Explain the term~~ What are subject & object in Unix
(8) Define the term websecurity.

LONG QUESTIONS

1. Explain Cross Site Request Forgery attack & its defense techniques.
2. Explain Cross site scripting & its defense techniques.
3. Explain Goals of web security. What are the threat models of web.
4. Explain Document Object Model.
5. Explain the concept of Browser Isolation.
6. Explain Frame & Frame Busting.
7. Describe Gmail structure.
8. Explain the detailed concept of Access control.
9. How access control is implemented in windows.
10. What are the possible attacks on access control.
11. Explain Chromium security Architecture

Unit - 4

SHORT QUESTIONS

1. Differentiate b/w Encryption & Decryption.
2. Differentiate b/w Plain Text & Cipher Text
3. What is cryptography?
4. Differentiate b/w symmetric & asymmetric cryptosystem.
5. What is hash function?
6. What is digital signature?
7. List the protocol measures implemented for n/w security.
8. What is DNS.
9. Define the term Non Repudiation.

LONG QUESTIONS

1. Explain Following Protocols
   - IPSec
   - DNS
   - SSL/TLS
   - HTTPS
   - PGP
2. Explain symmetric key cryptosystem.
3. Explain Public Key cryptography.
4. Show the authentication procedure in RSA.
5. Elaborate RSA Encryption/Decryption.

⑥ Explain Hybrid Cryptosystem.
⑦ Explain the prouss of Digital Signature
⑧ What are digital certificates. How it it is issued?
⑨ Describe the prouss of DES.

Unit-5

SHORT QUESTIONS

① Define the term Firewall.
② What is Intrusion?
③ Define the term CIA.
④ List the layers of TCP/IP Model.
⑤ What is packet?

LONG QUESTIONS

① Describe Intrusion Detection system.
② Explain the concept of packet filtering.
③ what are the measures of routing security?
④ What are the weakness of Internet security?
⑤ Differentiate b/w Link Layer connectivity & TCP/IP connectivity.
⑥ Discuss the role of firewall in n/w security.