Test Name : S22_MidSem_System and Network Security_3rd March 2022_11:00 AM

Name : Sudipta Halder - sudipta.halder@students.iiit.ac.in

Test Start Time	Marks Scored	Total Questions
03/03/2022, 11:00:23	17.0 / 20.0	15

Attempted Questions	Correct Questions	Incorrect Questions
15	14	1

Skipped Questions	Pending Evaluation
0	0

List of Sections

Explain the following attacks briefly

Marks per question : 1.0 | Marks Scored : 1.0

Q No.	Q. Type	Status	Marks	
1	Essay	✔	0.0	Hide Answer

Briefly explain the Replay attack

Characters: 730 , Words: 125

A replay attack occurs when a cyber criminal evasdropes on a secure network communication, intercepts it and then fradulently delays or resends it to the reciever to misdirect the receiver into doing what the hacker wants. The added danger of replay attack is that a hacker doesn't need advanced skills to decrypt a message after capturing it from the network. The attack could be succesful by simply resending the whole thing. Receiver will think that the message is coming from sender, but it is actually coming from attacker. Replay attack can be dangerous in banking transacyions. For eaxmple, if sender says receiver to send 200000 rupees once, but due to replay attack if attacker sends it 4 times, it will be a big problem.

Q No.	Q. Type	Status	Marks	
2	Essay	✔	1.0	Hide Answer

Briefly explain the Denial of Service attack

Characters: 670 , Words: 107

A DOS attack is a security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, networks, services or other information technology resources. Attacker in these these types of attacks typically floods web servers, systems or networks with traffic that overwhelmes the victim's resources and makes it difficult or impossible for anyone else to access them.

One version of DOS attack is Distrubuted Denial of Servie attack(DDOS). In that case, the attacks are done by attacker machine in a distributed way. Actually, attcker sets up a distributed system (for eg. bots) which performs those attacks in a distributed manner.

Q No.	Q. Type	Status	Marks	
3	Essay	✔	0.0	Hide Answer

Briefly explain the Forgery attack (impersonation attack)

Characters: 684 , Words: 114

Impersonation attck is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol. The goal of a strong identification or entity authentication protocol is to make negligible the probability that for a given party A, any party C, distinct from A, carrying out the protocol and playing the role of A, can cause another party B to complete and accept A's identity. Usually these types of attacks come from individuals tergeting high level executives. The goal of these attacker is to transfer money to a fradulent account, share insensitive data or reveal login information to attack company's network.

Choose the correct statement(s)

Marks per question : 1.0 | Marks Scored : 4.0

Q No.	Q. Type	Status	Marks

1 | Multiple Choice - Single Answer | ✖ | 0.0 | Hide Answer

Statements with respect to Overflow:

1) Most integer overflow vulnerabilities are caused by the misuse of overflowed values in sinks (e.g., memory allocation functions malloc).
2) Runtime Integer CHecking (RICH) is a static analysis tool to detect integer overflow attack.

- Option 1) is correct and option 2) is wrong.
- Option 1) is wrong and option 2) is correct.
- Both 1) and 2) are correct.
- Both 1) and 2) are wrong.

2 | Multiple Choice - Single Answer | ✔ | 1.0 | Hide Answer

Statements with respect to Control-Flow Intergrity (CFI):

1) CFI ensures that program execution follows a valid path through the static Control-Flow Graph (CFG)
2) Shadow Stack keeps a copy of the stack in memory
3) CFI can not be coupled with a protected shadow stack

- Only 1) and 2) are correct
- Only 1) and 3) are correct
- Only 2) and 3) are correct
- All 1), 2), and 3) are correct

3 | Multiple Choice - Single Answer | ✔ | 1.0 | Hide Answer

Statements with respect to Return Oriented Programming (ROP):

1) ROP can bypass Address Space Layout Randomization (ASLR).
2) ASLR randomizes the base addresses of memory and code segments so that the adversary can no longer predict start addresses of instruction sequences.
3) ROP allows an adversary to induce arbitrary program behavior without injecting any malicious code.

- Only 1) and 2) are correct
- Only 1) and 3) are correct
- Only 2) and 3) are correct
- All 1), 2), and 3) are correct

4 | Multiple Choice - Single Answer | ✔ | 1.0 | Hide Answer

Statements with respect to Heap-spraying attack:

1) It increases likelihood of success because the exact addresses of objects in the heap is not required to be known.
2) Attackers should be able to allocate objects whose contents they control in an application's heap.
3) Heap-spraying attack can not be detected through runtime interpretation and static analysis.

- (●) Only 1) and 2) are correct
- ( ) Only 1) and 3) are correct
- ( ) Only 2) and 3) are correct
- ( ) All 1), 2), and 3) are correct

5	Multiple Choice - Single Answer	✔	1.0	Hide Answer

Statements with respect to StackGaurd:

1) StackGuard provides an integrity check for function call activation records, making programs largely immune to stack smashing attacks.
2) The detection method in StackGuard is to place a "canary" word next to the return address on the stack.

- ( ) Only 1) is correct and 2) is wrong.
- ( ) Only 1) is wrong and 2) is correct.
- (●) Both 1) and 2) are correct.
- ( ) Both 1) and 2) are wrong.

Protocol design

Marks per question : 1.0 **Marks Scored : 3.0**

Q No.	Q. Type	Status	Marks	
1	Multiple Choice - Single Answer	✔	1.0	Hide Answer

In a Protocol P, sender performs the following operation. *Protocol A:* $y = Enc_{k1}\ (x \parallel H(k2 \parallel x))$, where x is the message, H is a hash function such as SHA-1, Enc is a symmetric key encryption algorithm, "‖" denotes simple concatenation and k1 and k2 are secret keys which are only known to the sender and the receiver.

Does Protocol A support **Integrity?**

- (●) Yes
- ( ) No

2	Multiple Choice - Single Answer	✔	1.0	Hide Answer

In a Protocol P, sender performs the following operation. *Protocol A:* $y = Enc_{k1}\ (x \parallel H(k2 \parallel x))$, where x is the message, H is a hash function such as SHA-1, Enc is a symmetric key encryption algorithm, "‖" denotes simple concatenation and k1 and k2 are secret keys which are only known to the sender and the receiver.

Does Protocol A support **Confidentiality?**

- (●) Yes

No

3	Multiple Choice - Single Answer	✔	1.0	Hide Answer

In a Protocol P, sender performs the following operation. *Protocol A: y = Enc_{k1} (x ‖ H(k2 ‖ x))*, where x is the message, H is a hash function such as SHA-1, Enc is a symmetric key encryption algorithm, "‖" denotes simple concatenation and k1 and k2 are secret keys which are only known to the sender and the receiver.

Does Protocol A support **Non-repudiation?**

Yes

No

Key exchange

Marks per question : 5.0 | **Marks Scored : 5.0**

Q No.	Q. Type	Status	Marks	
1	Essay	✔	5.0	Hide Answer

Suppose A and B use Diffie-Hellman key exchange. Let the common prime and primitive root shared between A and B are q=71 and α=7, respectively. If the private key of A is X_A=69 and private key of B is X_B=15, then find:
1) The public values computed by A (i.e., Y_A) and B (i.e., Y_B).
2) Compute the shared secret key (K) between A and B.

PS: DON'T JUST WRITE THE FINAL ANSWERS, DERIVE THEM.

Characters: 236 , Words: 59

q = 71

alpha = 7

Xa = 69

Xb = 15

Ya = alpha ^ Xa mod q

= 7 ^ 69 mod 71

= 61

Yb = alpha ^ Xb mod q

= 7 ^ 15 mod 71

= 23

key (K) = Yb ^ Xa mod q = 23 ^ 69 mod 71 = 34

key(K) = Ya ^ Xb mod q = 61 ^ 15 mod 71 = 34

Hence, Result

Ya = 61

Yb = 23

key(K) = 34

Code

Marks per question : 2.0 | **Marks Scored : 2.0**

Q No.	Q. Type	Status	Marks	
1	Multiple Choice - Single Answer	✔	2.0	Hide Answer

Which attacks are possible in the code shown in figure?
1) It allows remote attackers to execute arbitrary code
2) Cause a Denial of Service (memory corruption)

```
<form id="testfm">
<textarea id="child" value="a1" ></textarea>
<input id="child2" type="checkbox" name="option2" value="a2">Test check<Br>
<textarea id="child3" value="a2" ></textarea>
<input type="text" name="test1">
</form>

<script>

var startfl=false;


function changer() {
 // Call of changer function will happen inside mshtml!CFormElement::DoReset call,
after execution of this function crash in DoReset will happen when accessing freed
CInput element
   if (startfl) {
       document.getElementById("testfm").innerHTML = ""; // Destroy form contents,
free next CInput in DoReset
       CollectGarbage();
   }


}

document.getElementById("child2").checked = true;
document.getElementById("child2").onpropertychange=changer;
startfl = true;
document.getElementById("testfm").reset(); // DoReset call

</script>
```

- ○ Only 1)
- ○ Only 2)
- ◉ Both 1) and 2)
- ○ None of these

Misc

Marks per question : 1.0 | **Marks Scored : 2.0**

Q No.	Q. Type	Status	Marks	
1	Multiple Choice - Single Answer	✔	1.0	Hide Answer

To execute a successful buffer overflow attack, an attacker should able to perform:
1) Overwrite the return address.
2) Should be able to inject the source code.
3) Able to determine the location of the code.

- ○ Only 1) and 2) are correct

Only 1) and 3) are correct

Only 2) and 3) are correct

All 1), 2), and 3) are correct

2 | Multiple Choice - Single Answer | ✔ | 1.0 | Hide Answer

If you want to change the state of ASLR in a Linux system, then which file should you look into?

/proc/sys/kernel/randomize_va_space

/etc/pwd

/proc/sys/random_address

/proc/sys/kernel/random