Exercise-1

1. Read the following three bug reports. For each of them, decide whether an attack exploiting it violates confidentiality, integrity, availability, or some combination thereof. Give reasons for your decision.

Solutions:

(A) Windows SMB Remote Code Execution Vulnerability:

This Vulnerability mainly about Microsoft Server message block application, which is limited to handle only few requests. WannaCry is a ransomware, which attacks this application, and further it spreads to other remote systems inside a network. This Vulnerability mainly happens via crafted packets sent by the remote attackers. All Resources inside the attacked environment are impacted which leads to **loss of confidentiality.** On the other hand, attacker can be able to modify all the protected items by this attack, which is going to be serious consequences that leads to **loss of integrity.** Accessibility of resources, network bandwidth consumption and disk space, which are reasons to repeated exploitations and leads to **loss of availability**.

(B) Heartbleed vulnerability:

This Vulnerability will allow hackers to access sensitive data, which consists of credentials and private keys on affected devices. This vulnerability also affects the communications protocols SSL and TSL. In this attack, hacker will disclose some memory portion of the client/server that consists of personal information. By these assumptions, this vulnerability might **affect the confidentiality.**

(C) Cisco IOS XR Software Border Gateway Protocol Vulnerability:

This Vulnerability is seen in the CISCO IOS XR Software where its functionality will be infected while implementing the Border Gateway Protocol. Many attackers will try to perform Denial of Service Situations on targeted Systems. There will be multiple restarts resulting in this condition in BGP that leads to reset of multiple sessions. Therefore, this is an explanation for **Availability Impact.**

2. Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicefs , and Bob and Cyndy can read it. Cyndy can read and write the file bobfs , which Bob owns, but Alice can read and execute it. Only Cyndy can read and write the file cyndyfs , which she owns. Assume that the owner of each of these files can execute it. Note that there are four kinds of access rights in this question: read, write, own, and execute.

Solutions:

(A) Access control matrix:
  - ➢ Alice owns the file alicefs whereas Bob and Cyndy can read the file alicefs.
  - ➢ Bob owns the file bobfs and Alice and Cyndy can read the file bobfs whereas Alice can execute the file bobfs and Cyndy can write the file bobfs.
  - ➢ Cyndy owns cyndyfs and she can write and read the file cyndyfs.
  - ➢ Owner of each file can execute their responding file.

Users/Files	alicefs	bobfs	cyndyfs
Alice	ox--	rx--	----
Bob	r---	ox--	----
Cyndy	r---	rw--	oxrw

  - ➢ – Own, X – Execute, R –Read, W – Write.

(B) Cyndy gives Alice permission to read cyndyfs, and Alice removes Bob's ability to read alicefs.
  New Access control matrix:

Users/Files	alicefs	bobfs	cyndyfs
Alice	ox--	rx--	r---
Bob	----	ox--	----
Cyndy	r---	rw--	oxrw

  - ➢ – Own, X – Execute, R –Read, W – Write.

3. Consider the set of rights {read, write, execute, append, modify, own, truncate}.

(A) write accommand delete_all_rights (p, q, d). This command causes p to delete all rights the subject q has over an object d.

Solution:

- ➢ command delete_all_rights(p,q,d)
- ➢ delete read from A[q,d];
- ➢ delete write from A[q,d];
- ➢ delete execute from A[q,d];
- ➢ delete append from A[q,d];
- ➢ delete modify from A[q,d];
- ➢ delete own from A[q,d];
- ➢ delete truncate from A[q,d];
- ➢ end

(B) Modify your command so that the deletion can occur only if p has modify right over d.

Solution:

command delete_all_rights(p,q,d)

   if modify in a[p,d] then

- ➢ delete read from A[q,d];
- ➢ delete write from A[q,d];
- ➢ delete execute from A[q,d];
- ➢ delete append from A[q,d];
- ➢ delete modify from A[q,d];
- ➢ delete own from A[q,d];
- ➢ delete truncate from A[q,d];
- ➢ end