OBE December 2021

Date and time of Exam :- 15th Dec. 2021, 9:00AM

Examination Roll Number :- 19234757006

Name of Program :- Master of Computer Application

Semester :- V

Unique Paper Code (UPC) :- 223402501

Title of Paper :- Cyber Security

Name of the Dept. :- Dept. of Computer Science

Email-ID :- anubhav.mca19.du@gmail.com

Mobile No. :- 9044490197

No. of Pages used :- 3

(2). Before diving into the question, lets understand what hacking is :- A commonly used hacking definition is the act of compromising digital devices and network through unauthorised access to an account or computer system. It is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals. Hacking refers to the misuse of devices like computer, smartphone, tablets and networks to cause damage to or corrupt systems, gather information on users, steal data or documents, or disrupt data-related activity.

(a). For the scenario when someone accidently finds someone's password and uses it to get into the system, the act committed by the former will be considered hacking as they are accessing the system deliberately and without any authorization, without intimating the original owner of the system. As is clear from the above information, regardless of the further plans of the person with the password their unauthorized access to the system will be considered as hacking.

(b). For this scenario, when someone sends me a 'game' and when I ran it, it logs me into an IRS server, it will

19234757006

be considered as hacking because it is a delible-rate and intentional process. The IRS server hold descriptions of semantic web services at two different levels and a knowledge level description of components is represented internally in OCML. As the user gets logged into the server without authentication is considered hacking although one can argue whenever the user was aware in advance of the process or not only then can one judge their intention.

(c). 1. Screened Host Firewall Architecture :-

It combines a packet filter router with an application proxy server named a baston host. The bastion host limits the ~~Server~~ network traffic and minimizes the traffic load on the internal network. It is the main target to the attackers because it maintains the copy of cached data of the attacker can gain some information of the internal network on targeting the signal bastion host.

2. Screened Subnet Firewall Architectures :-

It allows a demilitarized zone (DMZ) to provide security to the internal network DMZ is a two or more internal bastion host or network servers connected to the screened subnet to provide services through the

external or untrusted network. A screened subnet protects the DMZ systems and information from the external networks by providing an intermediate security. It protects the internal trusted network by limiting the access gain to the external systems.

- Thus, It can be concluded that screened subnet firewalls offers more security than screened Host firewall.