(DEMB 13)

EXECUTIVE M.B.A. DEGREE EXAMINATION, MAY - 2015

First and Second Years

Paper – XIII : MANAGEMENT INFORMATION SYSTEMS

Time : 03 Hours **Maximum Marks : 75**

SECTION-A *(3 x 5 = 15)*

Answer Any Three of the following

1) a) Decision making with the help of data.

b) Design of system.

c) Control of projects.

d) Computer networks.

e) Query language.

f) Caribbean community.

SECTION-B *(3 x 15 = 45)*

Answer Any Three of the following

2) Bring out the significance of information resource management.

3) What are the stages in system development life cycle?

4) Distinguish between hardware and software.

5) Enumerate the future trend of DBMS.

6) Explain the computerisation at IFFCO.

7) Give an account of relational data base management systems.

SECTION-C *(15)*

(Compulsory)

8) We reach Nock in San Francisco's lower Haight after dark. Once inside, our pupils madly dilate as we try to catch the dynamics of this small, dark Cenozoic cave trimmed in airplane fuselage and grunge-clad patronage. Most don't take any notice; except a Medusalike young man sporting the stubby remnants of the recently shorn dreadlocks who rises from a floor cushion and extends his hand for a shake. He is Sirdystic, a hacker with whom I'd had only E-mail contact until now.

"Cool place," I offer.

"Yup." He gives a wry smile. "Cyber-Flintstones."

Soon, seven of us are slugging down room-temperature Guinnesses, which I'm buying. They all belong to the Cult of the Dead Cow, a 13-year-old, in-your-face hacking group whose members are young, rebellious, brilliant, and fed up with a mountain of perceived persecutions. They're misunderstood "white hat" good guys. Clueless federal agents are dogging them for no good reason, Privacy, Free speech. You get the picture.

But what they really hate is Microsoft Corporation, which, in the past year, has become the greatest of hacking targets. "We bring all these huge, gaping holes to their attention, and they don't listen," bellows Deth Veggie, a mammoth 24-year-old with rock-star looks.

Microsoft, they say, is more interested in marketing new systems than in securing them. Microsoft is breeding "dumbed-up" systems administrators who are so reliant on friendly, point-and-click interfaces that they fail to set basic security settings. Microsoft they say, hasn't learned from past mistakes made-and patched-in the Unix operating system.

"When we find a hole, we share that exploit with the rest of the world-and it takes Microsoft a long, long time to respond," says 22-year-old Tweetfish.

Hackers have posted the source code and techniques of myriad attacks against Microsoft products on World Wide Web sites and bullets in boards. They've got the

tools to crack passwords on NT and Windows 95 operating systems. And the techniques to grab those passwords from LAN Manager. Hackers know how to drop an Active X security level from high to none, essentially helping themselves to anything on the machine and the network it's connected to.

And the list goes on.

Why Microsoft? \ Why NT? First Microsoft is the biggest dog on the porch. Run, no less, by the richest guy on the planet. That's irresistible to many hackers. Also, compared with Unix which has been hacked and patched ad nausearn, NT makes for an exciting new playground.

In addition, Windows NT is quickly infiltering the enterprise. Microsoft is shipping more than 100,000 units of NT Version 4.0 every month. According to The Sentry Group, 85 percent of businesses and government agencies in the United States will use Windows NT as a desktop platform by next year.

In NT 5.0, Microsoft will introduce a three-tiered security architecture. MIT-developed RCF Kerberos authentication will replace the LAN Manager setup that hackers find so inviting. In addition, crypto-key infrastructure will be included to support digital certificates that authenticate users who access the system remotely. Moreover, in NT 5.0 data encryption will be supported, and administrators will have a central point from which to issue certificates and access controls.

Microsoft also maintains an electronic-mail address (secure@microsoft.com) to which anybody can send information about vulnerabilities. In addition, the company employs about 300 engineers who work only on security. And they listen to both hackers and customers, according to .Ed Muth, NT product manager. "We have demanding customers like banks and defense agencies who are not shy about telling us their security desires," he says.

"That's a bunch of marketing crock" Veggie says. "We try to contact Microsoft, and we always get the brush".

In any event, the bottom line is that the security problems most hackers ferret out aren't having a serious effect on Microsoft's ability to do business. Corporate America doesn't seem too spooked about Microsoft security, given the speed at

which they are deploying Windows NT. And that just keeps the hackers hacking away.

Questions:

a) Why are hackers like the Cult of the Dead cow hacking into Windows NT?

b) What is Microsoft doing about hacking and the security of Windows NT?

c) Is hacking by the cult of the dead cow and other “white hat” hackers ethical? Why or why not?

EEE