IV Year II Sem I Mid Examination.

Name : Prince Patel Roll No : 17BK1A05A7

Branch : CSE -B year : IV

Time : 2:00PM to 3:30PM Date : 5-5-2021

Invigilators Name : K.Venkat Krishna Duration : 90 Min

Subject : ~~Comput~~ ~~Cyber~~ forencics
Computer

Questions:—

(1) (a) List categories of Cyber Crime ?

(b) Analyse worm vs Virus counter measures ?.

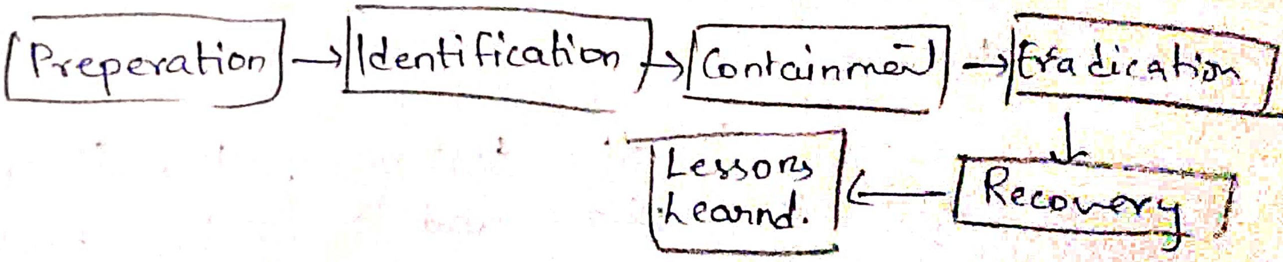
(2) Describe phase after detection of incident ?
(a)

(2) a)

(Ans) During the initial phase you need to take the least intrusive investigation.

→ Incident Response phase is taken after the detection.

→ Incident Response can be broken down into six phases that are :-



(1) Preperation :-

Preperation is straight forward as making sure you have a trained incident response team either employed, retainer or atleast someones business card you know who to call.

(2) Incident :-

An incident is initially identified ~~as~~ in any number of ways leading you to start your response plan with only slight awarness of what incident may be.

(3) Containment :-

containment often happens concurrently with identify or immediately following. Damaged systems removed from production, devices are isolated, comprinised accounts are locked.

(4) Eradication :-

Eradication is exactly what sounds like Removing and remediating any damage discovered in identified phase. This is normally done by Restoring system from backup.

(5) Recovery :-

Recovery is the testing of the fixes in the eradication phase and transistion back to normal operation.
Vulnerabilities are removed and compramised account passwords are changed.

(6) Lessons learnd :-

This phase is one that most of organisations skip but it is most importanb to prevent future incedents from analysig the previously occured incident.

(1)(a) Categories of cyber crime?-

Ans) few categories of cyber crime are:

(1) DDOS Attack :-

Distributed diniel of Service is attack on the network to ~~no~~ take the websites down and then hacker can hack once the network is done.

(2) Phising :-

This type of ~~back~~ attack occurs when hacker sends user Malicious files or url to the user via Email or other media and steals data when user access that Malicious url or file.

(3) Botnets :-

Botnets are networks from compramised computers which are controlled by hackers from remote area. They use this computers generally ~~fo~~ for doiy illigal things.

(4) Trojans :-

This are the virus which usually hides on some trusted files and reaches to user without his knowledge and steals Data.

(5) (c) Social Engineering:

Social engineering involves criminals making direct contact with you usually by phone or Email. They gain your confidence usually by acting as ~~Cons~~ customer service agents or bank agents then try to extract your personal Data slowely.

(1)(b)

Ans) Worm Vs Virus Counter Measures.

	Virus	Worm
1	Self Replicating program that attaches itself to other programs and files.	(1) illigitimate programs that replicate themselves usually over network.
2	Disrupt normal computer usage, corrupt user Data etc.	(2) Installs Backdoors on Vitim computer, slow down user network etc.
3	Countermeasures: 1) Antivirius 2) Update patches 3) Secure policy 4) firewall protection	(3) Counter Measures: 1) Antivirus 2) Update security patches 3) Update policy 4) Enable firewall.