University Of Virginia

Name : Ankith J Rai
SRN : PES1UG19CS069
SEC : B

1)

Ans)

- The mission of University of Virginia (VIA) is to develop and impart qualities of a leader in it's student's who are going to shape the future of the country and the world.

- The purpose for creating the ITS(Information Technology Services) was to provide resources and technology for the university community in order to achieve the university's mission.

- ITS provides services like management of IT infrastructure , policy and university records.

- ITS also provides information security to the database of the university. ITS is built in such a way that there is no denial/compromise on availability , integrity and confidentiality.

- ITS also coordinates the application's of the university.

2)

Ans)The reason's due to which universities attract cyber attacks are:

- The openness of the university as there are no or very less security protocols.

- The decentralized nature of the university leads it to become very hard to take decisions during emergency due to which resisting the attack becomes difficult.

- University’s have a lot of research intellectual property’s which have a high value in the market hence these attract malicious person’s like hacker’s to want them for making money by selling them.

- University’s also have financial information and PII(Personally Identifiable Information) of students and employees.

- University usually have a weak security protocols due to which it is a easy a easy target with high return.

3)

Ans)

The most common attack methods are:

- **Spear phishing :** Here a very large number of mails are sent to few targeted individual's mail which ask them to click a link which downloads malicious file into the system.

- **Unpatched systems :** In this type of attack, the system’s which have vulnerabilities are attacked.Usually a system is given an update (patch) to remove the known vulnerabilities in the system.As in an organization there are a lot of system’s hence it is very difficult and sometimes impossible to maintain a record on which system has been patched and which system has not bee.The attacker uses this vulnerability to his advantage.

- **Zero-day exploits :** In this attack, the vulnerability in the system is not known to the organization. Hence there is not update to remove this vulnerability.The attacker uses this and attack's the system.

Approaches used in mitigating the attacks:

- The most used approach to mitigate these kind of attack's is to used the Defence In Depth/ castle defence model.In this model there are multiple layer's in which in the inner most/ central layer(layer 0) most important resources and assets and data are kept and gradually as we move from the innermost layer towards the outer layer the importance of the resource kept within the layer keep's decreasing.

4)

Ans)The five objective's of the Phoenix Project are:

- **Determining the depth of intrusion of attack :** Mandiant, the security firm was called on to conduct investigation about the attack.But the investigation done by Mandiant was only a preliminary investigation hence a complete investigation needs to be done in order to have the complete information to go ahead.

- **Coming up with a redressal plan:** A remediation plan has been made in order to move forward and not face such activities in the future.In the plan all the system vulnerabilities are addressed and the method to patch them are also discussed.

- **Execution of redressal/remediation plan :** The execution of the plan has various activities such as tracking and monitoring the attacker’s activity’s , developing methods to protect data and applications, identifying and assessing the impacted stations, getting ready to support users during and after the go-phase and many more and then in the end the go-dark phase is initiated.

- **Defence mechanism:** In order to protect the UVA system’s from any further attack’s the defence mechanism has to to be improved and strengthened.

- **Restoration of services :** At the end of the go-dark phase all the system’s are tested and checked.

100% of effort’s needs to be put to accomplish these objectives as this matter deals with the personal information of students and employees and patents of the university.

5)

Ans)
The Internal stakeholders are:

a) Board of Visitors
b) Vice president of UVA
c) Deans of the University
d) Faculty
e) Retired faculty
f) Current staff
g) Retired staff
h) Students
i) Alumni

The External stakeholders are:

a) The Attorney General

b) Governor’s Office
c) The Press - like newspaper etc

In my opinion the project team should communicate with the each stakeholder using the network outside of the university server as the university sever has already been corrupted and communication on this server will lead to the attackers intercepting the message’s and this may lead to deleting of the evidences.

6)

Ans)
The risks inherent to this project are :

a) The possibility of leak of information that the attack has been detected and this makes the attacker’s pull out or stop the attack in order to avoid detection.

b) Conflicts in the schedule of the events taking place in the University which leads to a lot of inconvenience .

c) There can be incomplete system documentation or less factual documentation which leads to confusion in the Longer run.

d) The teams formed may not be as competent as expected which leads to loss of time and delay in the completion of project which needs to be complete in as less time as possible.

e) The management among teams might not be as smooth as expected due to which the project completion might take time.

The recommendation I would make to manage these risks are:

a) Make all the members of all the teams to swear to maintain secrecy about the detection of attack and about the ongoing project.

b) Proper system documentation with overview by another team.

c) Selecting team members with extremely good members who have shown their skills than on people who have no merit in handling the situation.

7)

Ans)

The success of the Phoenix project can be evaluated when another attack takes place on the university network.The success can be measured in terms of how the the updated security has held up to the new attack.We can also evaluate on the patches made after the previous attack have held up or not. We can also evaluate based on if all the vulnerability's have been closed or not. We can see, if the new attack has taken place to what extent has the attack breached the system and if the extent of intrusion is less or more than the previous attack.