Q-1: personal education, training and awareness must

Business

Q-1:” Personnel’s education and training do not affect the server securityarchitecture”. Do you agree on the previous statement? Why? Please discuss youropinion considering the all components of the server security architecture. Describethe differences between security awareness, training, and education in terms ofthe goals, the target group, the level, the test measure, and the teachingmethods? Explain theresponsibilities of Computer Security Incident Response Team (CSIRT)? AnswerPersonaleducation and training affects the server security architecture. This isbecause for a clearer server security architecture, practices and police mustbe offered in combination e, g personal education, training and awareness mustbe incorporated as a combination to produce a better and sound securityarchitecture. Thesecurity architecture in this case provides the needed framework for integratingthe existing security tools, people, users to provide the needs of the organizationand provide a security direction as a basis for a future decision making.

Allthese are laid down to match the strategic vision of the organization. The most important aspects of asecurity Thestrategic process involved in planning and developing the security architecturemodel is to maximize the use available resources to minimize the cost andspending. In this case, complexity in unnecessary and only increase costs whenmultiple security are deployed. Here security controls must be tactical innature and implemented through a perceived need though this may require timeand more monetary spending as compared to security architectures which arestrategically designed. Securityarchitecture has a primary response goal of providing a clear and defined meansof control. This is a time and money saving

applications. Data security modeland data classification provide a working solution that brings requirementsinto manful categories helping to bring about a predefined control.

This savestime and money when consistently applied. Data classification modelThis is adata classification component designed to promote sharing of information. Because information needs to be classified correctly. It helps to inidentification of critical information and the required security controls. Information can be classified high, medium, low or unclassified. When criticaland sensitive information in under classified, it may be compromised andintercepted in transmission.

Over classification can also lead to complexityand may undermine the credibility of the classification system Data security modelThisclassification component directs and helps end users in ensuring thatinformation systems and data are secured in an appropriate manner. Here the requirementsof security and the classification level are defined basing on each company’schoice of implemented technologies. In this model, security is most importantconcern and how information is secured. Securityawareness can be defined as a view that users should be in position to knowthat threats, risks and dangers exist.

When a user is able to perceive athreat, then he/she is aware of the threat. Here users should also be aware ofthe kinds of applicable measures that should be used to protect themselves incase of such dangers. The major important reason of carrying out informationsecurity awareness is to effectively reduce security hazards. Securityawareness focuses on how users

respond in regards to information security andhow information van be transferred to users in regards to information securitythat influences user's behavior. Usersecurity training is a means making known the fundamental learning experiencesneeded that is given to employees to bring about the much needed performanceimprovements to attain the organizations objectives. UserEducation is concerned about giving knowledge and tools to grow and expand CIRT agroup of trained professionals responsible for handling security incidents sothat they can be easily removed, investigated and contained. This group isusually a small number from the same organization. Roles: Studying abuses casesCIRT teamprovides the platform in developing real abuse cases.

They share articles onattack mechanisms and available security flows so that necessary measures canbe put in place. RiskanalysisThe teamcan provide test scenarios on software testing basing on their experiences. Here they provide an interaction between developers and the incident managementteam. The testing element helps the team find any software coding errors. Penetrative testingThe CIRTteam also provides penetrative testing as part of their roles. Ifvulnerabilities are found at the penetrative testing stage, the software mayalso be sent back to the developers so that the know security flow can befixed. Providing feedbackon development practices.

The teammay propose a certain curriculum for educating developers, managers, executivesand others about security issues and enabling developers know about theattacker exploits including the corresponding

solutions and mitigations. Q-3: Acompany Vortex® works mainly in currency exchange. The company has more than10000 customers, and 700 employees. The company has 25 servers in differenttypes (database, web server, productactivation server, etc.). Two servers are still unoccupied.

The companyemployees utilize different operating systems such as Windows XP, Windows 8. 1, Windows Server 2012, and Debian Linux. The client computers used in the workingenvironment are mix of computers provided by the company, employees BYOD (bringyour own devices) computers, and mobile devices. The clients are connectedthrough both cable and Wi-Fi. The internet connection comes from two differentISPs. A lot of time is spent on setting up local user accounts on everyemployee’s computer and to troubleshoot third party applications installed bythe employees.

The company plans to move some of their used applications to thecloud, and the company needs this issue to be considered. It isrequired to: 1. Designcomplete server security architecture for the company Vortex®. The designshould produce secure servers, and build a secure working environment from bothinside and outside the company2. Developa flowchart that describes the design aspects for the entire design process. You can use IF-THEN approach. Hints: Youcan consider different factors and keywords in your design like:• Thenetwork design/ topologies for the 25 servers. Dividing the servers intodifferent network zones according the sensitivity and functionality of 2 theservers•Protection of the servers from the networking perspective.

Network-basedfirewalls, distrusted firewalls, and host-based firewalls• Theinstallation and the hardening process of the server OSs which needs a policyor a regulation document• User/customer authentication to the servers (from inside the company and fromoutside the company as well)• Serversmanagement plans by IT personnel• Securitytechniques for the database servers that are connected to database security onthe application layer• Securityawareness, training, and education for the employees• Advicesabout using cloud computing by Vortex®Thequestion has a broad scope, and you have to do your best to bring all thepossible design aspects. You need to apply what you have learned from the labassignments in the design of the server security architecture. AnswerInterconnectedcomputers bring large amounts of possibilities in the company Vortex for collaboration, intercommunication, remote access, social networking file and printer sharing. Networkcommunications in small to medium organizations is largely and often impairedmalicious attacks which target network equipment and users to disrupt networktraffic. The most common among those attacks is the denial of service attacks anduser or host compromise attacks. In a denialof service attack, the attacker sends large amounts of bogus data traffic tothe target computer with intentions of causing disruptions while consuminglarge amounts of bandwidth and in the end rendering the computer unable toprovide services to the intended legitimate users. In a host compromise attack, the attacker exploits vulnerabilities in a host thereby gaining control of it 2. When these two attacks are combined, they can be used to cause more distrustfulkind of attack called distributed denial of service attacks(DDoS).

The numberof DDoS have been on the rise recently on many popular e-commerce and gamingwebsites which have been targeting mostly the Domain name servers. The mostimportant solution that research has found on better countering them is throughdesign of secure servers and schemes of detecting and recovery using detectionfeatures like intrusion detection systems (IDS). Other methods range fromresistant schemes designed based on built capabilities to survive and resistnetwork attacks. All these measures have been proposed but has not solved theever increasing attacks yet hackers still launch successful attacks 2. The solutiontherefore resides in the design of secure network architectures and othernetwork schemes that are capable of avoiding and mitigating serious impacts ofthe attacks. The reasonsfor the security architecture design include; v For consumer trust andconfidencev Better business focusv Better and secureinformation exchangev Remote and secure accessto internal workings and operationsv Improved businessproductivityv Reduction in costsassociated with loss of information components of security architecturemodel componentsThesuccessful security model will be in position to put together a combination ofpolicies and also leading practices, user training and education, encompassingnew technologies, and awareness programs.

There are four different layersconsidered in the design of the server security architecture which areaddressed in the architecture, v Secure accessv Hardware and operatingsystemv Applicationsv Human aspects A number ofprograms like anti-virus, intrusion protection systems, firewalls play animportant role in the protection of the companies from any attacks coming fromwithin the organization or outside it. A holistic architecture will be

implementat Vortex® to achieve the highest from the security mechanisms that will be inclusiveof all the security elements. This architecture is coordinated and structuredto include the people, the network servers, the end user computers, which worktogether to completely ensure security at Vortex®. To alignthese components effectively, the security architecture needs will be driven bypolicy stating management’s performance expectations, how the architecture isto be implemented, and how the architecture will be enforced. This will enablethe architecture to guide management so that decisions are aligned andconsistent throughout the entire IT landscape.

The architecture also will bestrategic — it will be structured in a way that supports the organization’sbusiness goals. The ITdepartment will be in position to understand the design of the securityarchitecture and its main components, how to assess the architecture’s effectivenessand the all the needed frameworks in order to maximize any audit efforts 3. The followingareas of concern will also form part of an effective and carefully plannedsecurity architecture and will be evaluated during audits of the securityarchitecture; v Guidance in the areas ofincident response, baseline configuration, account creation and management, disaster recovery, and security monitoring.

v Identity management. v Inclusion and exclusion ofwho and what is subject to the domain of the security architecture. v Access and border control. v Validation and adjustmentof the architecture.

v Training. v Education The logical network zoningor separation of the serversThe 25servers will be positioned in logical division of network servers in the Vortexcompany. This division is done for better manageable network to reduce on datatheft, reduce attack surface and for compliance. The security zone will have a well-definedperimeter and strict protection of its boundaries because the systems that areit can highly be attacked. For example, an end user computer will be givendifferent security requirements in the architecture as compared to thefinancial accountant that store confidential financial reports in therestricted zone.

The zones must all comply to the general security rules andguidelinesv Each zone will only have oneseparate entry point as defined by the firewallv All outbound and inboundtraffic must be monitored at the system perimeterv All systems and groupsmust be identifiedv Only traffic that relatesto Vortex® will be allowed to leave and enter the system perimeterWhile thiscan be done smoothly, complexity must be limited by defining clear securityrequirements and defining a few or small network security zones The Goals: The goal isto reduce the attack surface in a zone, which can be achieved exposing a fewnumber of services coupled with a much more tremendous and strict accesscontrol methods that can be used to provide limited access to only identifiedgroups of users. This makesthe zones safe in case of an attack, which will essentially mean the attackermust compromise all the outer zones before accessing the inner zones where criticalinformation is stored thus highly increasing critical systems availability. Networksegmentation provides the following goals as part of a defense in depthv Minimal data breachv Limits attack surfacesv Divides

the system intocompartmentsv Increase the availabilityof the system Thenetwork zones and their attached trust levels Zone Trust level attached Restricted The highest rust Management Highest trust Extranet Medium Enterprise Medium External DMZ Low Internet Don’t trust Restricted ZoneThis is aplace for the all sensitive information breach of which of its confidentiality, integrity and availability has far reaching consequences to the company on itsreputation, competitiveness, and its market share prices.

The highest protectionwill be placed at this zone to detect and stop any attacks. The number ofcritical systems at this level will include; v Financial databasev User system databasesv Human resource databasev Intellectual property ManagementzoneThemanagement zone is the center of monitoring and control like performanceservers, security management and configuration management. Here some users havea higher access privilege than other users thus making systems in this zone aprime target of attackers. ExtranetZoneThis zonewill house highly trusted connections with third party partners in businesswhich also extends to the enterprise zone. Information and data flow from theinternal network and the external network must be filtered and monitored inorder to strictly allow company information to leave or enter the zone at theperimeter. The Vortex®has no control on systems that are outside its control in the external zone. Thisrequires that all third parties adhere to risk assessments to be able tounderstand their security position before any connection is being allowed tothem.

ExternalDemilitarized zone(DMZ)Theexternal DMZ is responsible for all devices that require internet connectivity. It provides access to systems that operate between enterprise zone and theinternet. All trafficis to be monitored that passes the extranet and the enterprise zones. Under the extranet zone, hardening isperformed on the systems to minimize attacks, these systems include; v email gatewayv External web serversv Web proxy serversv Remote service accessv FTP servers Intranet zoneThis zone is solely responsible for mediating betweenthe restricted zone, external zone and the internal zone. Application serverswill reside in this zone and end user's devices must authenticate to therestricted zone before being allowed access. Access of restricted zone from the internet will onlybe possible via a restricted and secure method like the virtual privatenetwork(VPN) Enterprise zoneThis is the platform for end user devices likecomputers, printers, mobile phones and tablets. Their protection is importantto reduce exposure of end user devices to the risks of malware. Zone control and data accessEach zone is attached a security level with atrust relationship which increases as to the inner most zone from the outerzones.

Data must be prevented from flowing unnecessarily by deploying securitycontrols between zones. This can have achieved by use of monitoring tools likeintrusion detection and prevention systems, inspection firewalls, continuous accesscontrols, and data loss prevention. The control security implementation withina zone will enable easy detection of malicious activity across systems securitywith in a zone (SecureArc, n. d.). Training and educationTraining is key and will be vital in establishinga secure architecture in support of the efficiency of system users. In somescenarios some

individuals may perceive security as a hindrance to the day today duties of their jobs and may not have an understanding of the risks theyface as a result of system use.

This can be attributed to the numerous changesin security updates and security architectures due to emerging securitythreats. Therefore, regular user training and educationkeeps security awareness visible in the minds of employees enabling them to beupdated on the value of the information in their hands and the current securitybest practices and company management expectations Hardware and software technologyThe deployed hardware and software in Vortex® used to monitorand manage this security architecture will be the center of the securityconcerns. Other security mechanisms will be put in place to protect the physicalhardware. Like locks, man traps, biometric devices at door entries and etc. Thisarchitecture will not only rely on technology and disregard the individuals whouse it. As technology changes and new solution are put in place, the possibilityis high this will also have an impact on the architecture.

The change must alsobe evaluated to determine if a related counter change in architecture need tobe performed The ForwardThisplanned security architecture will help the information technology teamefficiently manage a wide variety of risks consistently maximize industry bestpractices while allowing the management make better and informed decisions. This will improve flexibility and promote interoperability and integration inthe organistion. References1R. Mohan, “ Network Analysis and Application

Control Software based onClient-Server Architecture", International Journal of ComputerApplications, vol. 68, no. 12, pp. 34-39, 2013.

2M. Bloch, R. Narasimha and S.

McLaughlin, " Network Security for Client-ServerArchitecture Using Wiretap Codes", IEEE Transactions on InformationForensics and Security, vol. 3, no. 3, pp. 404-413, 2008. 3V.

Varadharajan and U. Tupakula, " On the Design and Implementation of anIntegrated Security Architecture for Cloud with Improved Resilience", IEEETransactions on Cloud Computing, vol. 5, no. 3, pp.

375-389, 2017. Q. 2 LabProlonged running of thecommand hping3 –rand-source 10. 0. 0. 204 –flood -S -L 0 -p 80 overloads fillsmemory in Kali and later makes it non responsiveSource addresses are randomIP addresses and later put metasloitable unreachable until a forcible restartwas performed. I wrote my custom exploit on Metasploitable 2 from Kali Linux.

Manually exploiting VSFTPD V2. 3. 4 on metasploitable 2The main purpose of FTP is to transfer data across the internet. It was exploiting a vulnerability with telnet with metasploit I ran the service VSFTPD V2.

3. 4 and worked as root which gave the privilegeaccess to the root shell on metasplibale 2. The vulnerable may not be available since it has already been removed on deployable systems. I attempted to exploit the vulnerability backdoor through connecting tometasplotable 2 VSFTPD service.

I manually used telnet to exploit the vulnerability in VSFTPD v2. 3. 4 andmetasploit. in this step I used telnet to connect to metasploit Here below I used nmap to scan for port 6200 to see that port 6200 was openand execute the malicious code. I was able to see that FTP was using root by use of the challenge idcommand followed by (;) I used themetasploit which had an exploit Here the backdoor exploit command was used Hacking and Gaining Access to Linux by Exploiting SAMBA ServiceI begin by finding open ports using the nmap command nmap -sS -Pn -A 10. 0.

0. 30 After finding samba open ports and its services, I send exploits creatingmeterpreter sessions. Here I used metasploit.

I had to first find the version of samba installedLunch the command msfconsole to start metasploit here are the modules foundThe exploit Hacking Samba and installing meterpreterThis is using interpreter to hack a Linux system and take control of itMeterpreter is a service that gives the attacker access on the victimsystem to create a functionality. It gives the attacker command shell capabilityand helps attackers extract information from the victim computer while alsocovering his tracks. I begin openingmetasploit search for any samboexploits issue the command > uselinux/samba/lsa_transnames_heapand then asks msf> exploit(lsa_transnames_heap) > sjow payloads I choose a specific pay from the long list of payloads which islinux/x86/shell_bind_tcpBecause its a reverse shell capable of running on systems of x86 and usestcpI use the command > set payload linux/x86/shell_bind_tcp Shows the payload is acknoledgedthe I set the LPORT and RHOST(Loacl host and the remote

host)> setg LPORT 8080 and> set RHOST 10. 0. 0. 30 And finally the exploit But the targetreturned that it was not a vulnerable samba server