It consultant and methodolgies

Business

IT Consultant & Methodologies Introduction As many people would agree, the computer age has brought with it many advancements in many areas. The most advanced section has been storage and transfer of information courtesy of the modern information systems (Arkin, 2010). However, it is clear that this advancement has brought with it several risks. It can be noted from the daily activities that this risks continue to increase as more people continue to gain access to vital information. As much as an information system needs to be a secure system that firms or individuals can confidently store their vital information with confidence, but in reality, things happen differently (Dittrich, 2012). The system tends to be configured in a manner that leaves loopholes that crackers might use to attack the system. These loopholes are categorized into four categories known as " attack methodologies." Poor configuration of the firm's network, which allows user's ordinary access to ICMP In this type of security risk, a cracker can attack the system using methodology one. Conventionally, ICMP is created to facilitate sending of error messages when non-transient error conditions are met therefore enabling a means to query the network (Arkin, 2010). In this case, an attacker will therefore try to exploit the open standards of the TCP/IP or OSI reference model. One common thing with ICMP is that it is a data component and it is used to build tunnels. This makes it vulnerable because everyone including potential crackers can access such information. It should also be noted that a lot of research has reached to the conclusion that ICMP is one of the key toolkits for malware. A weak password policy Using user's name as a password might sound as a brilliant idea for ensuring users remember the passwords, but in reality, it creates a serious security risk (Afayyadh, et al., 2010). In this situation, a cracker would exploit the system

using the fourth methodology. This methodology shows how an attacker can exploit the people, their routine, and procedures they undergo within an organization. One way of attaining this level is through “ social engineering” in this case a user is manipulated into giving out information by tricking them to believe that they ought to give out that information. Additionally, a cracker can achieve this objective by paying attention to the organization’s processes and procedures in the process getting to identify the existing loopholes that can be used by the cracker to attack. In this instance, application of the third methodology is also possible. Exploitation of the configuration, individual networks, and exploit nature of design and architecture can also enable accessibility by a cracker to the organization’s system using an existing user’s account. Back doors in the firm’s website that have not been secured Today’s internet is not safe anymore for online transaction. There are more crimes being committed on the internet on a daily basis courtesy of cyber-attack or cybercrime. A backdoor is a path to access a computer program while bypassing the security mechanism of the computer. In most cases crackers use worms to exploit such security vulnerabilities (Peterson & Turn, 1967). A website with unsecured backdoors can be very serious threat that a cracker can take advantage of to the organisation following the potential risks where a cracker can easily send malicious programs that will copy all the necessary information such as passwords and sent it the attacker. In this situation is where methodology three explains. The availability of weaknesses in architecture, functionality, design, and configuration of individual networks poses a great danger to the firm’s information and privacy. Failure to restore the system following a reinstall with all available service packs In this type of scenario, the attack

methodology likely to be deployed is methodology two. An attacker exploits the systems weaknesses in an operating system and when found they provide an avenue for malicious activities. A cracker can use this avenue to plant viruses into the system that will later be hard to detect as they are integrated into the operating system (Schwartz, 2012). Poor briefing of staff members on matters relating to information security procedures Social engineering is a type of an attack where the attackers disguises themselves and try to persuade a legitimate user into giving out sensitive information. This mode of attack is given under the fourth methodology. Information systems are vulnerable platforms that need to be protected to the fullest. This is because a small leak in vital information such as the security codes could lead to a massive loss in a very short period. It would be therefore advisable that the first step of introducing staff to an organisation’s information system, there should be clear set rules and policies that limit the amount of information shared or available to staff (Wilson, et al., 2009). The danger of relying on Microsoft system For this security risk attackers can exploit the firm through methodology two. In this case, the cracker or attacker usually pays attention to the operating system’s vulnerabilities to which they capitalise on to exploit and crack the operating system. Although, this phenomenon affects all operating systems, Microsoft is one most persistent cases (Finkle, 2011). This is can be observed when the company publishes identified vulnerabilities to which unfortunately most crackers have already exploited. One recent case of security risks with Microsoft is cookie jacking, which is a way crackers are able to access the cookies from the system they use it to source passwords (Finkle, 2011). References Afayyadh, B., Thorsheim, P., Josang, A. & Klevjer, H., 2010. Improving Usability of

Password Management with Standardized Password Policies. Queendland University of Technology, 7 June, pp. 1-8. Arkin, O., 2010. Ofir Arkin, ICMP Usage in Scanning – The Complete Know How,. [Online] Available at: http://www. sys-security. com/html/papers. html [Accessed 14 March 2013]. Dittrich, D., 2012. David Dittrich, The “ Tribe Flood Network” Distributed Denial of Service Attack Tool,. [Online] Available at: http://staff. washington. edu/dittrich/misc/tfn. analysis [Accessed 14 March 2013]. Finkle, J., 2011. Reuters: Microsoft latest securrity risks; cookiejacking. [Online] Available at: http://www. reuters. com/article/2011/05/25/us-microsoft-security-idUSTRE74O86F20110525 [Accessed 14 March 2013]. Peterson, H. E. & Turn, R., 1967. " System Implications of Information Privacy".. Proceedings of the AFIPS Spring Joint Computer Conference, XXX(68), pp. 291-300. Schwartz, M. J., 2012. Microsoft Attack Surface Analyzer Catalogs Threats. [Online] Available at: http://www. informationweek. com/security/application-security/microsoft-attack-surface-analyzer-catalo/240005089 [Accessed 13 March 2013]. Wilson, M., Stine, K. & Bowen, P., 2009. Information security training requirements: a role and performance based model. NIST special publication, 14 March, pp. 1-157.