**Information Assurance and Security 2**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | October 26, 2024 | Name | Vallejos, Trissa May R. |
| Student ID. | 2021-00176-PQ-00 | Program | BSIT |
| **Activity 3 – Penetration Testing | Real-World Example Analysis** | | | |
| **Objective**: Analyze a real-world example of penetration testing revealing critical vulnerabilities, and summarize the improvements made as a result.  **Instructions:** Research and provide details on a real-world penetration testing case that led to important security improvements. Answer each question below in 5 -10 sentences.  **Questions to Answer:**   1. **Background of the Case**  * What happened? Describe the event or breach and the key details about the organization and data involved. - In 2016, there was an attack on the Democratic National Committee (DNC) that exposed vast amounts of confidential data, including opposition research on Donald Trump before he was elected President. A spear-phishing attack is one where hackers send a fake email to DNC members asking for login details, which the employees give out willingly. While on the network, the attackers were able to acquire and exfiltrate thousands of emails internal communications donor information confidential files days after the hack was discovered, however, those identifying as Guccifer 2.0 claimed not to be involved with Russia and instead said they were behind the heistᅳa massive election interference operation that led to WikiLeaks releasing sensitive data on the DNCᅳwhich in turn damaged politically Democratic US politicians during our last general presidential election cycle recess.   That breach was later discovered to be the work of two groups tied to Russian government-backed cyber espionage teams operating under codenames “Fancy Bear” and “Cozy Bear,” connected with Russia's intelligence services. This incident served to underline the dangers of using weak cybersecurity in political institutions and fueled fears that foreign countries could manipulate democratic processes. It also prompted extensive discussions about cybersecurity that underscored the threat to political data and persuaded this would not happen again.  1. **Penetration Testing Findings**  * What vulnerabilities were discovered? Explain the primary security issues that penetration testing, or post-breach analysis revealed.   The 2016 Democratic National Committee (DNC) cyberattack revealed several vulnerabilities in the DNC’s cybersecurity defenses. Attackers, suspected to be Russian hackers, gained access by using spear-phishing emails to trick staff into providing their login credentials. This phishing method exploited human vulnerability, bypassing technical defenses and allowing attackers to access internal systems. Once inside, they moved through the network exploiting poor password practices and a lack of multi-factor authentication to access sensitive files, emails, and databases.  One major security flaw was the lack of network segmentation, which could have limited the attacker's access to specific parts of the network, containing the damage. Additionally, the DNC’s detection systems were insufficiently configured, leading to a delayed response that allowed attackers prolonged access over months. The DNC was also unprepared for advanced persistent threats (APTs), which are complex, long-term cyberattacks aimed at extracting data without triggering security alerts.  Penetration testing and post-breach analysis concluded that a stronger security posture could have prevented the attackers’ deep infiltration. This included recommending better user awareness training, more robust email security measures, and implementing network segmentation alongside continuous monitoring solutions.   1. **Security Improvements**  * What actions were taken to improve security? Summarize the main security changes the organization made to prevent future breaches.   The Democratic National Committee (DNC) improved security after the 2016 hack by creating a number of defenses against similar assaults in the future. Since a spear-phishing attack caused the initial breach, one of the main steps was to improve cybersecurity training for staff members, particularly in the area of identifying phishing attempts. Regular phishing simulations were used to reinforce this training, which helped staff members identify questionable emails and protect their credentials. Also, the DNC implemented stronger authentication procedures, including multi-factor authentication (MFA), which provided an additional degree of protection to stop unwanted access even in the case that login credentials were made public. In order to proactively detect and fix system vulnerabilities and make sure that its infrastructure was impervious to possible attacks, the company also made an investment in penetration testing.   1. **Lessons Learned**  * What is the main takeaway? Identify the most important lesson or principle that this case highlights the value of penetration testing.   The DNC data breach underscores the importance of penetration testing and basic cyber hygiene in preventing cyberattacks. Hackers exploited a preventable weakness using a spear-phishing email to steal login credentials. Penetration testing could have identified these vulnerabilities early and reinforced the need for stricter security measures. Employee training on phishing recognition and multi-factor authentication would have further reduced risks. This incident shows that even well-funded organizations must prioritize foundational security practices. Regular testing and proactive security updates are essential to protect sensitive information. Additionally, the case highlights the role of private companies in supporting national cybersecurity, as they often manage critical infrastructure. Better collaboration between government and private sectors could mitigate damage from similar attacks.  **Deliverable**  Prepare a **brief report** or **slide presentation** summarizing your findings, including a reflection on the role of penetration testing in preventing similar incidents.  **References (APA Format):** Nakashima, E. (2016, June 20). Cyber researchers confirm Russian government hack of Democratic National Committee. *The Washington Post*. <https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html>  Fazzini, K. (2018, July 16). How the Russians broke into the Democrats’ email, and how it could have been avoided. CNBC. <https://www.cnbc.com/2018/07/16/how-russians-broke-into-democrats-email-mueller.html> | | | |