ISEC 675: Information Systems Auditing

Summer Term 2023

Eric Webb

Professor Ling Wang

Assignment 2: Written Essays

**Written Essay 2-1:**

Performing security assessments are crucial for organizations to ensure integrity, confidentiality, and availability while also remaining compliant. By reviewing the vulnerability life cycle, organizations can mitigate risk by addressing risks factors such a nondisclosure, full disclosure, limited disclosure, and responsible disclosure. By performing security assessments on the seven domains of a typical IT infrastructure, organizations can properly implement controls, assess risk, and identify vulnerabilities. Security assessments can help organizations achieve compliance and mitigate risk in many forms such as disclosures type attacks, vulnerabilities, malicious code, phishing, underground economies, and spam. Addressing the different types of disclosures, risk from attacks, and the security assessments on the seven domains of a typical IT infrastructure, can help achieve compliance in an organization.

The vulnerability life cycle can be used for discovering, disclosing, and remediating vulnerabilities. But when vulnerabilities are discovered, organizations can mitigate risk factors by establishing different disclosures. It is important to know the distinct types of disclosures and when to implement them. To begin, Nondisclosure occurs when a vulnerability is discovered but not publicly disclosed. Typically, in this instance, sharing vulnerability with the public would lead to increased risk from the exploitation and is only released to trusted individuals. Full Disclosure occurs when organizations publicly disclose all the details about a vulnerability, including the technical aspects. Full Disclosures benefit the technical community by being transparent, facilitating timely patches, and encouraging organizations to take necessary action promptly. Limited Disclosure occurs when only parts about a vulnerability are shared. Limited Disclosure may be used when full details could jeopardize system security, such as waiting on a vendor to release patches. Responsible Disclosure occurs when organizations report vulnerabilities to the affected vendors or organizations. Responsible Disclosure provides an opportunity to develop and release patches before disclosing publicly and allows organizations to mitigate vulnerabilities before they become publicly known.

Significant risks to organizations can include attacks, vulnerabilities, malicious code, phishing, underground economies, and spam. Attacks such a social engineering attacks and man-in-the-middle attacks can lead to unauthorized access, theft, financial loss, and ruin reputation. Vulnerabilities such as the one found in the LOG4J vulnerability can be exploited and can potentially compromise data and disrupt operations (Cybersecurity and Infrastructure Security Agency, 2021). Malicious code such as malware and viruses can infect, steal, manipulate, and even remote-control systems. Phishing attacks such as spear fishing and whaling can trick employees into giving up sensitive information such as access credentials (National Cyber Security Centre, n.d.). Underground economies make money on stolen data, selling hacking tools, and offering illegal services (Internal Revenue Service, n.d.). This increases risk for organizations. Spam emails waste time but can also lead to security incidents such as being part of a phishing attempt.

By conducting security assessments across the seven domains of a typical IT infrastructure, organizations can identify vulnerabilities, implement remediation, and adhere to compliance (Kim, David, & Solomon, 2012). The User Domain focuses on individual users who have access to organizations' IT resources. The domain involves password policies, access controls, and user account management. The domain supports compliance by supporting that only authorized users have access to sensitive data. The Workstation Domain focuses on individual devices. Assessments in this domain evaluate the measures of antivirus, firewalls, and patch management. This domain can support compliance by ensuring that workstations meet security requirements. The LAN domain focuses on the infrastructure of the Local Area Network. This domain involves segregating internal networks, intrusion detection, intrusion prevention, and network access controls. This helps with compliance by identifying vulnerabilities in the LAN domain and facilitating the appropriate security controls. The WAN domain focuses on the Wide Area Network. Assessments in this domain evaluate the security of remote access, virtual private networks, and encryption mechanisms. This helps achieve compliance by ensuring confidentiality and integrity across open networks. The Application Domain focuses on the software. Assessments in this domain focus on identifying vulnerabilities, code reviews, and software testing. This helps maintain compliance by ensuring the security and integrity of software applications. The Physical Domain focuses on the physical IT infrastructure such as data centers and server rooms. Assessments in this domain evaluate the physical access controls, surveillance systems, and environmental controls. This helps maintain compliance by assessing physical security and implementing necessary controls to physically protect assets. Finally, the Data Domain focuses on data throughout its life cycle. Assessments in this domain include classification of data, encryption, backups, and retention policies. Assessments can help maintain compliance by ensuring appropriate data protection measures are in place like encrypting data in motion and at rest.

In conclusion, security assessments are crucial for organizations to maintain security and compliance. By being familiar with the vulnerability life cycle and addressing disclosure types, organizations can effectively mitigate risk. Addressing risks from attacks, vulnerabilities, malicious code, phishing, underground economies, and spam is essential to protecting sensitive information, preventing loss, and maintaining a good reputation. Security assessments conducted across the seven domains of a typical IT infrastructure enable organizations to identify vulnerabilities, implement remediation measures, and ensure compliance with regulations. By focusing on user management, workstation security, network infrastructure, remote access, software applications, physical infrastructure, and data protection, organizations can address security risks and meet requirements. These assessments play an important role in protecting organizations' assets, mitigating risks, and maintaining security and compliance.

**Written Essay 2-3:**

The Workstation Domain in IT Infrastructure is prone to various risks, threats, and vulnerabilities. One useful resource to mitigate these is the Common Vulnerabilities & Exposures (CVE) database, which provides lists of known vulnerabilities and exploits. By incorporating the CVE database, organizations can mitigate risks, threats, vulnerabilities, and misconfiguration at an operating system level.

When it comes to the Workstation Domain, common risks associated with it include unauthorized access, malware infections, and data breaches. Threats can be in the form of social engineering techniques such as spear phishing. Vulnerabilities can come from outdated software, unpatched systems, weak passwords, or misconfigurations. These vulnerabilities can be exploited to access systems, steal data, or disrupt operations. Being able to recognize these risks, threats, and vulnerabilities are beneficial to organizations by allowing them to implement proper security measures and mitigate breaches.

There are few good examples of well-known vulnerabilities and exploits from the CVE database workstation domain. The first being CVE-2021-34527 called Print Nightmare (Cybersecurity and Infrastructure Security Agency, 2021). These vulnerabilities allowed an attacker to exploit the Windows Print Spooler service and allowed attackers to execute arbitrary code with system privileges. Another example is CVE-2021-3156 called the Sudo Heap-Based Buffer Overflow (Cybersecurity and Infrastructure Security Agency, 2021). This vulnerability allowed attackers to use a buffer overflow to take advantage of the Unix like systems and escalate privileges, bypassing normal access controls. The last example is CVE-2020-1472 called Zero Logon (National Vulnerability Database, n.d.). This vulnerability affected Microsoft Windows Net Logon Remote Protocol (MS-NRPC) and allowed attackers to gain unauthorized access to a domain controller. Exploiting this vulnerability led to the compromise of domain credentials, compromising the security of workstations within the domain. These examples highlight the significance of monitoring the CVE database to stay informed about vulnerabilities and exploits.

Operating system-level risks, threats, and misconfigurations within the Workstation Domain can expose workstations to various security concerns, potentially leading to unauthorized access, data breaches, and operational disruptions. By understanding and addressing these risks, organizations can enhance their security posture and protect their sensitive information and assets. From an operating system level risk prospective, outdated operating systems that are no longer supported or lack necessary security patches pose significant risk. Using unlicensed or pirated operating systems can increase the risk of malware infections and unauthorized access. Risk can also come from misconfigurations such as weak or default passwords, improper user permissions, and even disabled security features. Workstations are a great target for threats to attack and exploit the host operating system. Malware such as viruses, worms, ransomware, and spyware can infiltrate workstation through phishing emails, websites, and removable media. This malware can specifically target operating system vulnerabilities to gain unauthorized access to workstations. vulnerabilities and misconfigurations at an operating systems level within the workstation domain are significant. These can include unpatched security vulnerabilities, weak encryption protocols, or insufficient access controls. By exploiting these vulnerabilities or misconfigurations, bad actors can escalate privileges, compromise sensitive data, or challenge the integrity of the workstations operating system. The consequences of workstation domain exposures can lead to sever consequences for an organization. This can lead to unauthorized access, data breaches, stolen intellectual property, or loss. Exploited workstations can be used as entry points of lateral movement in the network, this can potentially compromise the overall security posture of the network. Operational disruptions by exploiting a workstations operating system can lead to downtime, loss of productivity, or even reputational damage. To implement risk mitigation and enhance workstation security, organizations should adhere to robust security practices. This can include regular patch management to keep operating systems up to date, utilizing strong password policies, using multi factory authentication, and ensuring appropriate user access controls. There should be adequate endpoint protection such as antivirus, intrusion detection, intrusion prevention, and host-based firewalls, to detect and prevent malware infections. Regular security awareness training should be used to educate users on potential threats such as phishing, and to encourage responsible computer practices.

In conclusion, the Workstation Domain in IT infrastructure is susceptible to various risks, threats, and vulnerabilities. Utilizing resources such as the Common Vulnerabilities & Exposures (CVE) database can help organizations mitigate these risks. Risks associated with the Workstation Domain include unauthorized access, malware infections, and data breaches, while threats can take the form of social engineering techniques like spear phishing. Vulnerabilities stem from outdated software, unpatched systems, weak passwords, and misconfigurations. By recognizing these risks, threats, and vulnerabilities, organizations can implement proper security measures to mitigate breaches. Examples from the CVE database, such as Print Nightmare, Sudo Heap-Based Buffer Overflow, and Zero Logon, highlight the importance of staying on top of vulnerabilities and exploits. Operating system-level risks and misconfigurations within the Workstation Domain expose workstations to unauthorized access, data breaches, and operational disruptions. To address these issues, organizations should prioritize regular patch management, strong password policies, multi-factor authentication, and adequate endpoint protection.

**References:**

Cybersecurity and Infrastructure Security Agency. (2021, February 2). Sudo Heap-Based Buffer Overflow Vulnerability (CVE-2021-3156). Retrieved from https://www.cisa.gov/news-events/alerts/2021/02/02/sudo-heap-based-buffer-overflow-vulnerability-cve-2021-3156

Cybersecurity and Infrastructure Security Agency. (2021, June 30). PrintNightmare: Critical Windows Print Spooler Vulnerability. Retrieved from

https://www.cisa.gov/news-events/alerts/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

Cybersecurity and Infrastructure Security Agency. (2021, December 10). Apache Log4j Vulnerability Guidance. Retrieved from <https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance>

Internal Revenue Service. (n.d.). Cash Payment Limitations Chapter 8 [PDF file]. Retrieved from <https://www.irs.gov/pub/irs-utl/cashchapter8_210737.pdf>

Kim, David, dan Michael G Solomon. 2012. Fundamentals of Information Systems Security. Jones & Bartlett Learning, United State of America

National Cyber Security Centre. (n.d.). Whaling: How it works and what your organisation can do about it. Retrieved from <https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it>

National Vulnerability Database. (n.d.). CVE-2020-1472 Detail. Retrieved from <https://nvd.nist.gov/vuln/detail/cve-2020-1472>