

University of Wales

Trinity Saint David

Antoci Bianca

1817784

MODULE CODE/ COD Y MODIWL: ACCC5003

NETWORK OPERATING SYSTEMS AND SECURITY

Security Policy and Management

Assignment 2

Table of Contents

Introduction	3
Problem analysis	4
Basic requirements of ensuring confidentiality, integrity and availability of a network system	4
Understanding the nature of a network security breach	6
Basic principles of auditing and testing a network system	8
Conclusion	10
Recommendations	11
References	12

Introduction

In the face of the new global crisis, many companies have abandoned conventional working routines favoring remote working conditions. There is an overt shift in working culture and patterns. Staff is now spending more on ensuring they have private working facilities such as WIFI systems and home offices. Networks have been profoundly affected by this new change in patterns. Securing this network is easier said than done as with every added person comes an added risk to the system. This paper seeks to identify the etiology of an attack, the nature it was executed, how it could have been used to compromise data, and the ways it can be prevented in the future. The paper will also elaborate on how a system can be audited to show vulnerable spots and methods to repair the vulnerabilities [1].

Problem analysis

“Basic requirements of ensuring confidentiality, integrity and availability of a network system” [16]

A secure network makes sure that the system is accessible to execute its designated task. This is provided by preserving it from attacks that stem from within and outside the organization [2]. Conventional security measures are narrowed down to a few requirements. They are user device protection, user identification, and point results for security; with new members' inclusion into a network, the threat to the network increases. Measures include monitoring of application traffic. This helps avoid hazards such as stealing of intellectual property or personal data. The basic fundamentals must be defended from service disruption. Such would result in a network being made unavailable for the intended use. Other outcomes would include service theft when an unauthorized user accesses a system to access unauthorized services. Many organizations do not invest in infrastructure beyond point results like firewalls. To defend the full network, security must be addressed in all layers and a complete networking life cycle. Protect networking affects securing the application traffic as it travels a network. Areas to be covered by the system are perimeter security and communications security. Perimeter security protects networks from outside attacks. Such security measures include firewalls and intrusion detection. Communications security measures provide data confidence, integrity, and non-repudiation. This can be facilitated using secure socket layers or using virtual private networks. Secure networking protects the elemental infrastructure from attacks. Platform security is when each accessory is available to achieve its

intended function. This ensures that the devices do not become an individual point of collapse. Network security plans should have antivirus verify, host intrusion detection, and endpoint compliance. This ensures actions check user devices for needed security software. Several aspects have to be taken into account when identifying ways a network can be compromised. The technology aspects include the hardware and software systems that make the network being used. Each added device becomes a vulnerability point that can be exploited. The human element is another factor to consider. Persons trained to identify malware, suspicious links and are always cautious about updating security features on their software and other devices are much less likely to suffer a security breach. Untrained persons are more vulnerable to be attacked if they do not consider the safety measures to be adopted. A poorly maintained network with minimal user identification systems is more likely to suffer an attack, whereas regularly maintained systems, with regular updates, are less likely to suffer attacks [3], [4].

“Understanding the nature of a network security breach” [16]

The cyber breach was initiated by a staff member who set in motion a three-pronged intrusion. This was an A.R.P. attack based on the 'man-in-the-middle' attack. An Address Resolution Protocol attack is when a malicious attacker sends falsified A.R.P. messages over a local area network [5]. The A.R.P. attack leads to a linking of the attackers' mac address with the I.P. address of a legitimate PC or service on the network. Once connected, the malicious party has access to any data going through the device. The party can then intercept, modify, or even stop data in transit. This could be any data from social media feeds to bank transactions worth millions. A.R.P. spoofing attacks are commonplace when local area networks when computers on a LAN network are compromised. Several exploitations can be devised from this attack. Basic attacks are often exploited to steal sensitive information. Other outcomes of this compromise are Denial of Service attacks (D.o.S). This attack often leverages A.R.P. spoofing to link several I.P. addresses to the targets mac-address and thus overload the computer with traffic [6]. This can cause such an inconvenience that the right signals do not get through, causing lagging through the whole network. Session hijacking can be exploited by using A.R.P. spoofing to steal sessions and I.D.s, thus granting attackers access to private data and systems. If this were a security network, identities would be leaked and exploited by malicious parties. Man-in-the-middle attacks are used to intercept and modify any traffic between teams. Data is manipulated and altered once the A.R.P. spoofing is done. This attack was probably planned by an external party that took advantage of a vulnerable system. It is unlikely that the staff member knew what they were doing though this is not entirely

improbable. The attack resulted in password cracking and access to personal data. Data is set to be sold to a darknet website on what is likely to be a “sucker’s list” to be exploited for malicious intent. There are several preventive measures one can control to facilitate security against such attacks. Packet filtering involves inspecting packets as they are transmitted across a network. They are useful as they help filter out packages and block the ones with conflicting source information. They work by identifying those packets from outside the system that shows source addresses from inside the network and vice versa. One human aspect that can improve security is to avoid trust relationships. Companies that rely on protocols that depend on trust relationships should be relied on as little as possible. They count on I.P. addresses for authentication. This makes it easier for hackers to run A.R.P. attacks while in place [7]. This makes it seem as if the attack was initiated internally while initiated outside the network. A.R.P. spoofing detection software can help in A.R.P. spoof detection. They work by inspecting and certifying data before it is transmitted. These applications also block data that seems to be spoofed [8]. The basic details should go through some intense scrutiny. A test approach can be used to identify several concerns that arise. For example, odd email addresses, social media invites, and several settings made on the network. Making the network public, using weak passwords, not updating software regularly, and leaving personal computers turned on when one goes to the workspace are ways to compromise a network. The organization should adopt a system to demonstrate better compliance with data protection legislation better. This is more comprehensive than endpoint protection but accommodates perimeter, communications, and platform security [9].

“Basic principles of auditing and testing a network system” [16]

A data security audit is a means of estimating even if an organization acquiesces with its data protection duties, find data protection risks, and bring forward recommendations for best practices [10]. An audit can be facilitated when the organization understands some factors beforehand. Such are the categories of particular data they have, the operations they use to process and deport the data, how to protect the data, the presence and nature of regulations and considerations, response to incidents promptly, and the best approach to make learned risk-based agreements and assessment of current systems, new projects, and actions, and choice of new I.T. products [11],[12]. These measures help dissect the data's nature, the dangers within the network, whether overt or otherwise, and how these risk points can be secured. Having proactive access ensures companies are superior arranged to adapt to adjustment in technology. Such regulations are cloud ISO 27018, which outlines the cloud insurance policies of personally identifiable information (PII). There are also big legal and administrative adjustments, like the new General Data Protection Regulation GDPR.

The principles of data security are a clearly defined strategy. This represents the volume of security measures to be audited, the system's scope, the endpoint provisions applied, and the level of security needed to be optimized. The organization's wide controls describe the extent of the organization's network, the types of connections present, and the end-users proficiency and vulnerabilities. Processes and procedures explain the system in which the data is managed and processed. One is the continuous analysis of the capability of the

data privacy and security program. The process of conducting a data protection audit can vary depending on the scope and detail of the task being done, however, there are common steps that can be adopted through each system. Identifying the process required for making an audit sets priorities and objectives beforehand. Determining the audit subject also narrows down the areas of focus to ensure a thorough analysis. This could be a security audit, maintenance audit, or checking for updates. Audit objectives are also key to understanding the scope of investigation. The three stages determine the analysis scope; this established the analysis levels to be facilitated to designate the area to cover. Performing the audit planning is key as it sets a strategy beforehand to understand the nature of the system, the potentially vulnerable areas, and how to delegate tasks. The audit procedures and steps for data gathering are the next phases. Conclusion of the exercise and writing endnotes are the final phase. These help record findings as well as set a date for the last audit. They take into account the updates, recommendations as well as replacements to be done by the client company [13], [14], [15].

Conclusion

Network security is a broad genre with various subgenres that all have unique but relatable risks and consequences. What drives data security is modern economic trends that depend on consumer behaviour and consumer patterns. Several laws force companies to handle personal data with the utmost safety, such as the new General Data Protection Regulation, which is considered the most progressive law on data protection in the last 20 years. There is an undeniable human aspect to data security breaches; an unsuspecting staff member clicks on a link that leads to an attack, or a company I.T. manager preferring endpoint security measures only perhaps for cost-related reasons, leading to a vulnerable network system. The consequences of such challenges can result in unsafe data, multiple attacks, and an overall falter of the entire network system. The steps stated above are thus adopted to mitigate such occurrences from happening.

Recommendations

- Understand the nature of the data, methods of processing, and ways to store it
- There are several aspects to network security; examples are the human aspect, hardware aspect, and software aspect.
- Vigilance is key to mitigate potential vulnerabilities.
- Endpoint solutions are not adequate for full network security.
- Prepare a plan to establish security and routine maintenance.
- Malicious parties can exploit local area networks to compromise systems.
- The damage done by network exploitation can be irreversible and should be prevented at all costs.
- The security of a network system should be readily addressed and evaluated to prevent breaching.

References

- [1] Barday, K.A., Brannon, J.B., Sabourin, J.L., Karanjkar, M.S., Jones, K. and Beaumont, R.A., OneTrust L.L.C., 2019. *Data processing systems and methods for auditing data request compliance*. U.S. Patent 10,318,761.
- [2] Abdelmoumin, G. and Hazzazi, N., 2020. Distributed Operating System Security and Protection: A Short Survey. In *17th International Conference on Information Technology–New Generations (ITNG 2020)* (pp. 145-151). Springer, Cham.
- [3] Tayyaba, S., Khan, S.A., Tariq, M. and Ashraf, M.W., 2020. Network Security and Internet of Things. In *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital* (pp. 198-238). I.G.I. Global.
- [4] Ye, Y., Yan, L., Ren, S. and Zhang, Q., 2019, June. Research on Network Security Protection Strategy. In *2019 International Conference on Robots & Intelligent System (ICRIS)* (pp. 152-154). IEEE.
- [5] Al Anani, A., 2020. A.R.P. Spoofing.
- [6] Shanmugam, T. and Malarkodi, B., 2019, July. Analysis of Recent Challenges and Solutions in Network Security. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 902-907). IEEE.

- [7] Viscuso, M., Johnson, B., Saunders, A., Ruef, A. and McFarland, J., Carbon Black Inc, 2019. *Systems and methods for tracking and recording events in a network of computing systems*. U.S. Patent 10,185,822.
- [8] Chevalier, R., Plaquin, D., Dalton, C. and Hiet, G., 2019, December. Survivor: a fine-grained intrusion response and recovery approach for commodity operating systems. In *Proceedings of the 35th Annual Computer Security Applications Conference* (pp. 762-775).
- [9] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. and Faruki, P., 2019. Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, 21(3), pp.2671-2701.
- [10] Priyadarshini, S.B.B., Bagjadab, A.B. and Mishra, B.K., 2019. Security in Distributed Operating System: A Comprehensive Study. *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies*, pp.221-230.
- [11] Wang, Q., 2020. Strategy of Enterprise Network Security Protection Based on Cloud Computing. *MS&E*, 750(1), p.012234.
- [12] Malisencu, D., 2019. Attacks analyze in the computer networks.
- [13] Ward, B.C., Skowyra, R., Jero, S., Burow, N., Okhravi, H., Shrobe, H. and Khazan, R., 2019. Security Considerations for Next-Generation Operating Systems for Cyber-Physical Systems.
- [14] Diamantopoulou, V., Tsohou, A. and Karyda, M., 2019, August. General data protection regulation and ISO/IEC 27001: 2013: synergies of organisations'

compliance activities. In *International Conference on Trust and Privacy in Digital Business* (pp. 94-109). Springer, Cham.

[15] Celdrán, A.H., Pérez, M.G., Mlakar, I., Calero, J.M.A., Clemente, F.J.G., Pérez, G.M. and Bhuiyan, Z.A., 2020. PROTECTOR: Towards the protection of sensitive data in Europe and the US. *Computer Networks*, 181, p.107448.

[16] University of Wales, Trinity Saint David, "Network Operating System and Security(ACCC5003_LON)"[Online].

Available:https://moodle.uwtsd.ac.uk/pluginfile.php/48795/mod_resource/content/6/ACCC5003_NOS%20Assignment_2.pdf