Network Intrusion Detection and Prevention in Organizations

Mohammed Al Madhi and Daniel Kearl

Final Project Team 14

University of Louisville - College of Business

Proposal

The focus of our project is on Network Intrusion Prevention and Detection. We plan to introduce the idea of network vulnerabilities and describe those that can be common in the workplace, then move on to describe methods of detection and prevention of these threats. There is also a small portion over recovery methods and topics that should be considered immediately after a threat has been brought under control. Finally, we will wrap up our research by attempting to relate it to the average employee, describing what they should be doing to keep their workplace network as secure as possible.

The following table of contents has been created with the paper and the presentation in mind, so if all goes to plan then both will be following it, though the presentation will likely do so more loosely. Our general plan is to approach this topic with the average person (as an employee of a business) in mind, hence the overview of networking and network vulnerabilities and tying things back into the average employee’s contribution to security.

Network security and intrusion prevention systems are never perfect, but with multiple layers of security, an organization is better protected against threats of network intrusion. Network intrusion occurs when someone attempts to gain access to the organization’s network for nefarious purposes, whether it is only to disrupt or to infiltrate. Well, how do we stop it? Using an Intrusion Detection and Prevention System (IDPS), the purpose of which is to prevent, identify, and report and harmful activities, is crucial to the information security of a business or other organization. In the case of an intrusion, the attacker might have gained access to data that may include clients’ and employees' private information, highlighting the importance of detecting and preventing intrusion attempts in such an environment.

TABLE OF CONTENTS

1. Basics of Network Vulnerability
   1. Overview

Network Systems attacks are increasing every day and many organizations are suffering from these attacks as they are the main target for network attacks. There are many reasons why attacks are mainly focused on organizations, one of the reasons include competitive intelligence in which the attacker wants to know the secrets to about the organization’s financials, products, services or other business secrets. Second type of attack include Denial of Service attack in which the attacker intends to harm or disable the organization’ network operations. In order to prevent these attacks from coming into your organization it is recommend that you have a Network Intrusion Detection System (IDPS), IDPS system monitors analyzes computer network traffics and notifies the network administrator in an event of an attack or suspicious activity on the network.

* 1. Common Configurations

Intrusion Detection and Prevention Systems (IDPS) can be deployed using a hardware or software sensor or agent and these are usually installed on the network gateways with other networks as those are great areas for scanning points where the network traffic converges for example it can be placed behind the firewall. The central machine is a system that stores data in a location in which it can be used for logging, alerting and reporting when a sensor detects an unusual activity.

1. Threats to Network Security

Network Security refers to the ability to protect network, however network security threats are potential risk that could or will negatively impact the organization network assets. Threats to network security are increasing daily and they are affecting many business organizations in many ways, and in order to prevent these from happening, we need to have proper configuration that could decrease the amount of network threats an organization receives. Based on our research we have included attacks/techniques that attackers use to try to gain access to your network some network attacks include

* 1. Network Attacks
     1. Phishing

According to the Principles of Information Security book, the definition of Phishing is “attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site.” Which means that the attacker will have you enter your personal information such as username and password or your credit card details; in which after that they could use these to lock your account or make an unauthorized purchases using your credit card details you provided while filling their phishing form out. In order to prevent phishing from happening to your organization a proper employee training is required and must be done quarterly in which to keep your team informed.

* + 1. Ransomware

Is a type of malware that will and can encrypt all your files on a Windows Operating System and which makes them inaccessible, and then will have a screen displayed asking for money in return for a key that will unlock your files. What’s dangerous about this malware is that if the computer infected is on network it would most likely infect all other computer connected on the same network as well which could cause a huge loss to the organization. In 2017 WannaCry a ransomware cyber-attack hit hundreds of United Kingdom National Health Service (NHS) computers many hospitals were force to delay surgery’s and cancel patient’s appointment, not only that but there are many other organization that has been hit such as FedEx and Nissan Automobile. To protect your organization from WannaCry or any future Ransomware, always have back-up, Secure host baseline, Threat Intelligence for firewall (IDPS), Anti-Malware for clients and mail server, and lastly User training as stated above in the Phishing section.

* + 1. Man-in-the-middle

According to the Principles of Information Security book “Man-in-the-middle attack (MITM) or TCP hijacking attack, an attacker sniffs packets from the network, modifies them, and inserts them back into the network.” One of the most common Man-in-the-middle attacks involves an attacker to set-up a fake Wi-Fi around Coffee shops, restaurants and or even shopping malls for people to connect to, these Wi-Fi’s pose and look as legitimate as the real Wi-Fi but once a person connected, then attacker will be able to steal logins, passwords and even credit card numbers on an unsecured host. To prevent MITM from happening according to the NIST There are Wireless IDPS sensors can that can detect when an attacker is trying to spoof a Wi-Fi, the IDPS Wireless sensors can Identify the physical location of the detected threat by using “triangulation” which estimates the location of the threat. Wireless IDPS sensors can be placed in multiple locations in the organization building and even in public, to protect users from any MITM attacks.

* + - 1. Packet/Network Sniffing

Packet/Network Sniffing are also known as packet analyzers are piece of hardware and or software that monitors traveling data over the networks, most organizations use these for legitimate purposes, although this can be used by an attacker to steal information from a network.

* + - * 1. Wireshark and Network Miner

Wireshark and Network Miner are similar programs that can be used to analyze packets on your network which then captures network data traveling through the network, both Wireshark and Network Miner are not a type of IDPS but they can be helpful to see what is going on in your network as these tools can be used by a Network Administrator to troubleshoot network problems and to examine security problems. It’s always important for a network administrator to have secured and encrypted network to prevent any unauthorized user from capturing and or sniffing your organizations data as this tool can also be used against your organization.

* + 1. DNS Spoofing

Domain Name Spoofing (DNS) Spoofing is an attack in which the cyber attacker tricks your computer into thinking its going to a legitimate website but its not, in which the attacker gains access to your DNS cache to steal your personal data/credentials if entered. In order for the organization to stay secured from such a threat, IT management team should monitor network traffic since if DNS request is going to an IP that isn’t a legitimate DNS server, then this shows that an employee is attempting to get around company’s DNS.

* + 1. DoS/DDoS

During a Denial of Service (DoS) attack the attacker sends a massive number of packet requests to a server, during which the server becomes overloaded with packets and cannot respond to any incoming requests which then the server crashes and wouldn’t be able to perform any normal functions. A Distributed Denial of Service (DDoS) attack is similar to a DoS attack but instead the attack comes from different areas, usually from bot computers which are controlled by the attacker(s). A DDoS attack is usually harder to combat as it comes from multiple locations using bot computers while a DoS attack usually comes from one IP address which could be blocked. In order for an organization to stay protected from DoS/DDoS attacks an organization must invest in an Anti DoS/DDoS tool which some of these tools are cloud base and do come with a free option such as Cloudflare, but its highly recommended to choose the best plan option as those are recommended for large or small organization.

* 1. Exploitation

According Webopedia Technical term for an exploitation is “an unintended and unpatched flaw in a software that exposes it to potential exploitation by hackers or malicious software code such as worms, viruses, Trojan horses and other forms of malware.”

* + 1. Misconfiguration

Attackers will find many ways to get into your system and if a system misconfiguration are one of the biggest threats to and organization as those could cause huge problem if left unpatched. There are many types of system configuration such as giving access to users that does not need it, leaving the system’s default account password blank and lastly and most importantly leaving your network password unsecured. It is always important to have proper system configuration to prevent any unauthorized access to your system, always have your system up to date, do not use default credentials, set proper user access and lastly implement a secured network access and location.

* + 1. Social Engineering

Social Engineering is exploiting human psychology into tricking them by using various techniques in order to gain access to system, data or building. Employees needs to be trained which is one way to prevent social engineering. The most used technique by social engineers is someone who poses as and IT staff and asks employees for their password in order to fix an issue with their account, an IT staff would never ask for an employee password in most cases. Thus, if the hacker is successful in gaining an employee password there would be a huge data loss that might include organizations records such as employee’s personal information, organization financial data, that is why training employees is required to keep your team informed.

1. Detection and Prevention

Intrusion detection and prevention system (IDPS) are hardware and or software that is implemented on a network that acts as security features, It is used to monitor network activities and looks for packets that possesses threats on an organization’s network. IDPS can prevent these attacks, in which it uses a web application firewalls that filters incoming network traffic such as malicious packets in order to keep the applications running and secure.

* 1. Physical Security
     1. Access Control

Access Control ensures that users have appropriate access that is designed to their job title, for example the organization’s security guards should not have access to the corporate Financial data, or the Financial Department should not have access to employee’s personal records, access control must be limited. non-employees must not have similar privilege access to the network as an employee there should be separate network, this ensures that organization devices are protected from rogue and to keep the corporate physical assets protected.

* + 1. Business Policy

An Organization must have policy for their Electronic devices and Network use and employees must accept the consequences for their misuse. Security Guidelines for user access, password requirements, confidentiality and the usage of their data.

* + 1. Employee Training

Employees are one of the greatest threats to the organization’s data and they have access by nature, employees do make mistakes which could lead to deleting, duplicating or accidentally modifying files, employees also need to understand the threats to network, make them aware and to prevent Phishing, Ransomware and Social Engineers as these are one of the biggest threats employees face, with proper training the less chance of an employee to fall for these threats.

* 1. Software Solutions
     1. Honeypots
     2. Firewalls
     3. Redundancy
        1. Load Balancing
        2. Parallelism
        3. Backup Sites
     4. Network Isolation
        1. Proxies
        2. VLANs
     5. Encryption
        1. Mechanics
        2. Data
        3. VPNs
  2. Maintenance
     1. Scheduled Downtime
     2. Update Management
        1. Testing
        2. Patching
        3. Deployment
     3. Hardware Upgrades

1. Recovery

Business must have a recovery plans that supports the organizations in an event of incidents. IT management must understand their roles and be prepared for recovery plans to protect their data, their business, clients and assets. Data is what holds most if not all the companies records such as customer information and other sensitive data, those must be backed up all the time and protected in any event.

* 1. Management
     1. Planning

Management plays a big role in maintaining an organization and enforcing Information Security policies. Management must have plans for recovery, in an event of an incident

* + - 1. DR Plans

Disaster Recovery Plan (DRP) focuses on the restoration of a system after an event of a disaster. DRP also consists of actions which must be taken before, during and after a disaster.

* + - 1. BCP

Business Continuity Plan (BCP) states the mission and the business functionality its purpose is to provide a continuity plan when recovering from a disruption, it also ensures that the organizations assets and personnel are protected and continuing to function. BCP is an important step in an organization, if an event of disturbance occurs the organization could potentially lose revenue if a continuity plan is not a requirement in that business.

* + 1. Evaluation
    2. Decision Making

1. References
2. Conclusion

Common configuration

S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi and S. Ventura, "SIP intrusion detection and prevention: recommendations and prototype implementation," 1st IEEE Workshop on VoIP Management and Security, 2006., Vancouver, BC, Canada, 2006, pp. 47-52.

K. Scarfone, P. Mell, Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology (NIST) (2007)

<https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901146>

Sources

Man in the middle <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>

Wireshark

<https://www.wireshark.org/>

DNS spoofing:

<https://threatpost.com/dns-spoofing-attacks/141880/>

DOS/DDOS ICE2A

Business Policy –

<http://www.corpcomputerservices.com/articles/it-policies-small-business>