ASH1925030M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:44AM (UTC-0500)
Submission ID: 1782992550
File name: ASH1925030M.pdf (173.71K)
Word count: 3203
Character count: 17505

Vulnerabilities of modern networks to intrusion

Sourav Barman
ASH1925030M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

In today's world, network security is critical in all sorts of networks. The network is used in offices, schools, and colleges, among other places. Furthermore, practically everyone is a part of a social network. Despite the fact that numerous network security solutions are in place, susceptible actions do occur from time to time. This article illustrates numerous network assaults that result in vulnerabilities, as well as intrusion detection and prevention solutions.

1 Introduction

1.1 Network security and common vulnerabilities

[3] A computer network is a group of connected computers that share resources. Network technology have been used in a variety of fields in recent years. Tax payments, e-commerce, and e-voting are examples. Client and host are the components of these application services. It's critical to protect these application servers and network devices from malicious intruders tapping or counterfeiting data.

Network security vulnerabilities are flaws within the system's software hardware. Network vulnerabilities are two types, either nonphysical or physical. Nonphysical network vulnerabilities commonly affect software or data. For example, an operating system might be vulnerable to network attacks if it's not updated for several years. If the software is running in its older version, malware could infect the Operating system.Physical protection, such as locking a server in a rack's closet or guarding an entry point with a turnstile, is just an example of physical network vulnerability.

The massive increase in cyber risks, combined with modern businesses' reliance on the stability and effectiveness of their IT infrastructure, has prompted a shift in mentality. Priorities are altering as "IT downtime" increases. Cyber assaults, particularly those targeted at networks, are real, according to recent polls, and are no longer an improbable occurrence that only affects a few exposed networks of high-profile enterprises.

As attacks become both more common and more tragic, professional IT information security can no longer ignore these difficulties inside the struggle to preserve and implement any provided IT information security; in many institutions, commercial success is tied directly to the reliable and safe activity of their networks.

Furthermore, while virus-based attacks are the most prevalent, unauthorized access and identity fraud attempts are also widespread, according to the annual F.b.i. Survey.

1.2 Types of Network Attacks

Active or passive attacks are both possible. In an "active attack," the attacker will take steps to modify system resources, such as breaking or bypassing security

systems. Typically, it leads to the disclosure of sensitive information, data change, or, at the most extreme, data loss. Active attacks include Trojan horses, viruses, and worms, introducing harmful code, stealing network data, and stealing login information. This kind of attack is extremely damaging to the system.

The following are examples of active attacks: Masquerade, Session Replay, Message Modification And service denial. A "passive attack" seeks to figure out what is going on. or to make use of some crucial knowledge that has no bearing on the outcome of the system's assets In this form of attack, the perpetrator is the one who initiates the attack. utilizes a sniffer program and waits for some sensitive data to be captured information that may be used in a variety of additional assaults Filtering the traffic, traffic analysis software, and packet sniffer tools Passive assaults use passwords as an example. The various kinds of Release of contents messages and passive attacks are examples of passive attacks. There are four primary types of network attacks. The attack might be active or passive, and it can fall into any of these four categories.

- Web-based Network Attacks;
- Phishing attack:
- Hijack attack; and
- Spoof attack.

1. Web-based Network Attacks:

   Internet-based network attack is a subset of network attack with its own set of characteristics. As a result, they are distinct from the previously mentioned incursion kinds. Below are a few examples of web-based attacks.

   - Injection :

   It is a type of web-attack technique in which the attacker will exploit the web applications that accept user data without their knowledge. Some of the injections are SQL, OS, and LDAP injection, which may be happened when the attacker sends the untrusted data to an interpreter as part of a command or query. Then the attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without any authorization.

   - Cross-Site Scripting (XSS) :

   When an online application collects anonymous data from the user through its cookie and transfers it to a web browser, this is known as cross-site scripting. This XSS allows the attacker to run their applications in the victim's browser, hijack logs or even redirect the user to malicious websites.

   - Security Misconfiguration :

When a network's security measures are not up to par, an unauthorized user or even an authorized user might become involved in vulnerable actions by accessing default accounts, underused pages, unpatched weaknesses, unsecured files and directories, and so on. Any system should have a secure configuration for the database server, web server, server application, and platform, among other things. As a result, the security configuration must be designed, implemented, and maintained. The security software, in particular, should be kept up to date.

2. Phishing attack:

   This form of assault is getting increasingly prevalent. An attacker develops a phony email account or website that looks exactly like a legitimate email address or website. Then he sends them an email containing the corruptible message or a link to a bogus website under their name. This bogus website appears to be identical to the real one. However, the user is unaware that when they begin to use it, the hacker collects the user's account information and login information, among other things, and subsequently misuses it.

3. Hijack attack:

   This sort of attack frequently occurs in the intervals between sessions. The attacker joins a running connection and secretly disconnects the actual party. Then, using the identity of the original disconnected party, he begins conversing with involved parties. Because the active participant is unaware that he is conversing with the attacker, he may exchange necessary information.

4. Spoof attack: This sort of attack frequently occurs in the intervals between sessions. The attacker joins a running connection and secretly disconnects the actual party. Then, using the identity of the original disconnected party, he begins conversing with involved parties. Because the active participant is unaware that he is conversing with the attacker, he may exchange important information with him.

2 History and development of (IDS)

Intrusion detection used to be a manual search for abnormalities before the invention of the current IDS. To accomplish so, log files were analyzed for actions that should or should not happen during standard computer and network functioning. Manually doing this operation is time and workforce intensive, strenuous, and perhaps incorrect. As a result, automatic log file readers were quickly developed, scanning for documented events suggesting irregularities or even infiltration by unauthorized personnel. However, not every anomaly represented a simple assault or infiltration, necessitating a complete analysis of the entire process. With more investigation, it was feasible to extract "attack patterns" from these abnormalities, developing the first automatic pattern recognition log file readers. However, it is essential to note that prior to the Internet age, most early ID Software (not Systems) was built, written, and not widely distributed because only a few organizations needed this

type of technology. According to the yearly F.b.i. The report, the source of assaults has switched from internal sources to the Internet; in 2003, 70As a result, the burgeoning IT security industry launched network-based intrusion detection, which works on the same pattern matching principle as host-based intrusion detection but monitors network traffic instead of reading log files to look for attack patterns in the TCP/IP packet stream.Until now, intrusion detection had been a post factum study of log files, providing forensic investigation and possible infrastructure improvements reasonably long after the actual incident.

Because of the availability of sufficient processing speed, it is now feasible to check for attack patterns after an event has occurred and monitor in "real-time" and trigger alarms if incursions are identified.

Due to market supply, the IT security industry has begun to transform previous prototype software into actual Intrusion Detection Systems, including user-friendly interfaces, methods for updating attack patterns, various methods of alerting, and some automatically triggered reactions or actual prevention methods, which can stop attacks in progress. Because of the financial losses incurred as a result of computer downtime, image loss, or even the compromise of private data, the need for being warned in the case of an attack and preventing the assault has grown in recent years. Particularly with the development of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, market demand for Intrusion Prevention Systems (IPS) rather than simple intrusion detection has become more robust. These Intrusion Prevention Systems are at the cutting edge of IDS technology right now, and they may be found as stand-alone devices or as part of current firewall systems. Another point to note is that the current trend in the IT security industry to move away from software-based solutions and appliance-based solutions has resulted in a shift in emphasis, for example, in the firewall industry, which now includes IDS and IPS as part of their solutions in some cases.

3 Methods of intrusion detection

3.1 Behaviour-based IDS

[1]Statistical Anomaly Detection is a technique for detecting statistical anomalies. Perforations are detected using a variety of ways. These assaults start by establishing a statistical baseline: what is usual for this system? They then collect and analyze additional statistical data. the departure from the starting point If a limit is reached, If the limit is surpassed, an alert will be sounded. The following are some examples of what a behavior-based IDS could detect:

1. Throughout a period, the number of unsuccessful login attempts at a sensitive host;

2. A flurry of unsuccessful login attempts: It is possible that an assault is underway or that the administrator just lost his password.

This introduces the issue of false positives (when an attack is identified when one is not taking place, e.g., a false alert) and false negatives (when an attack is overlooked because it falls within typical behavior parameters). It is possible that normal behavior and forbidden behavior overlap. As a result, legitimate users may diverge from the baseline, resulting in false positives (for example, if a user goes on vacation, works late at work, forgets their password, or begins to use a new program). A persistent attacker may gradually move the baseline over time such that his attack does not cause an alarm if the baseline is updated dynamically and automatically. Other disadvantages with behavior-based IDS include their difficulty in implementation, the fact that they may consume more resources than knowledge-based IDS, and the fact that they may require constant fine-tuning by administrators. There appears to be much research going on currently, but no commercial goods are known to be in use.

3.2 Host based IDS

Modern host-based Intrusion Detection Systems, which evolved from simple log file analyzers, are built as host-based software that operates in the background on supposed essential, sensitive hosts such as Mail Servers, DNS Servers, web servers, database servers, and so on. Host-based IDS are commonly seen in e-commerce setups where sensitive data is kept, or availability is crucial. The components are the actual host-based IDS program and an IDS management station, from which the application is operated, and alarms are transmitted for further action. Host-based IDS is used to detect attack patterns that are solely or more readily identified at the host level.

3.3 Network based IDS

An IDS that is network-based analyzes network traffic at the packet level. The components are the network-based IDS software, which runs on a dedicated host and is linked to network traffic through a network interface and an IDS management station, where the program is controlled, and warnings are issued. To avoid becoming a target for attack, it is common practice to "conceal" the system by putting the network interface into "stealth" or "promiscuous" mode, where the interface has no IP address, and the IDS probe cannot be answered by other hosts, but instead duplicates all getting passed traffic into its RAM. The packets are analyzed for attack signatures in both the header and payload, which are kept in the IDS Attack signature database, an essential component of any IDS program.If a match is detected, an alarm is sent through the SNMP trap or equivalent to the management station for further action. Some IDS, such as Tivoli, HP OpenView, and NetIQ, enable interaction with network and security management consoles due to the alarm delivery technique. Some IDS even allow an automated reaction to a detected attack, such as resetting the connection to the source IP or reconfiguring the firewall, for example, by blocking the relevant port.

4 Intrusion Prevention Systems (IPS)

According to many IDS users, seeing an attack as it happens is one thing, but blocking it is another. If one assumes that the most crucial goal of any IT security operation in this area is to avoid an attack and any subsequent disaster, IDS often falls short of this goal.Until recently, the best an IDS could do was send a reset package in the hopes of terminating an active attack session or reconfiguring a firewall by simply shutting the affected service's proper port. These safeguards were, of course, at least partially ineffective, for example, if the assault did not use a session-oriented protocol like UDP.

4.1 Definition of an IPS

Until recently, the best an IDS could do was send a reset package in the hopes of terminating an active attack session or reconfiguring a firewall by simply shutting the affected service's proper port. These safeguards were, of course, at least partially ineffective, for example, if the attack did not use a session-oriented protocol like UDP.there are two categories:

1. rate-based products
2. content-based

4.1.1 Rate-based IPS

Rate-based Intrusion Prevention Systems (RIPS) restrict traffic depending on network loads, such as too many packets, connections, or errors. A rate-based IPS kicks in when too much something blocks, throttles, or otherwise mediates the traffic. The most usable rate-based IPS is a mix of sophisticated configuration choices and various response technologies. Limit DNS server requests to 1000 per second, for example, and provide additional essential bandwidth and connection restricting rules.A rate-based Intrusion Prevention System can limit the amount of traffic routed to a specific port or service. If the threshold is surpassed, the IPS will block any future traffic from the source IP, but other users will utilize the service.

4.1.2 Content-based products

Content-based Intrusion Prevention Systems prevent intruders from accessing sensitive information. attack signatures and protocol-based traffic Anomalies are the result of the natural development of the universe. Firewalls and intrusion detection systems. They the following should be blocked:

- Worms
- Packets that do not comply with TCP/IP
- Suspicious behavior, such as port scanning, causes the IPS to block all traffic from that particular host in the future.

5 Summary

Hacking assaults, whether from within a network by a disgruntled employee or over an Internet connection by a hacker, are a reality in the IT industry. The same can be said for DoS and DDoS assaults, which are increasingly integrating distribution techniques from other known cyber attacks, such as a worm. According to the pattern seen in numerous polls, these attacks are more likely to increase rather than decrease. IDS/IPS are not meant to replace or compensate for the lack of an appropriate IT security management structure, nor can they compensate for the improper integration of other IT security requirements, such as defective key management or a lack of user knowledge of IT security concerns.Intrusion Detection Systems (IDS) may be thought of as a second line of defense for defending a network against assault, in addition to typical perimeter security procedures. It is getting increasingly difficult to enforce security access controls as a result of rising "deperimeterisation." Intrusion Detection Systems (IDS) can be used to detect assaults within a network, but they lack the ability to actively respond to an attack in progress. Intrusion Prevent Systems (IPS) combine IDS with firewall technologies to give a mechanism for responding to ongoing assaults.Only if all IT security components are professionally maintained, frequently reevaluated, manageable, and flexible enough to adapt to future changing needs can one assume that they are on the right track, as IT security is still, and likely always will be, a route to take rather than a destination to reach.

6 Conclusion

[2] An overview of detection and Prevention strategies, approaches, and technology for IDSs has been presented. Each strategy has advantages and disadvantages, so we must be cautious while choosing ways. For example, while pattern-based IDS is simple to create and relatively successful at inspecting known assaults, it struggles to identify novel attacks, attacks masked by evasion tactics, and various variations of known attacks. There have also been various rule-based techniques to detecting unknown assaults developed. Such tactics, on the other hand, may create a challenge of difficulty developing and updating knowledge for specific assaults. Furthermore, while heuristic-based techniques have the advantage of requiring no prior knowledge of assaults, they are inefficient in real-time applications due to their high computing cost.

References

[1] S Latha and Sinthu Janita Prakash. A survey on network attacks and intrusion detection systems. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 1–7. IEEE, 2017.

[2] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[3] Deris Stiawan, Mohd Idris, Abdullah Hanan Abdullah, et al. Characterizing network intrusion prevention system. *International Journal of Computer Applications*, 14(1):11–18, 2011.

ASH1925030M

ORIGINALITY REPORT

45%	30%	37%	32%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	faculty.kfupm.edu.sa Internet Source	18%
2	S. Latha, Sinthu Janita Prakash. "A survey on network attacks and Intrusion detection systems", 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017 Publication	9%
3	Submitted to Embry Riddle Aeronautical University Student Paper	3%
4	Submitted to University of Adelaide Student Paper	2%
5	Andreas Fuchsberger. "Intrusion Detection Systems and Intrusion Prevention Systems", Information Security Technical Report, 2005 Publication	2%
6	Submitted to Universiti Kebangsaan Malaysia Student Paper	2%
7	Submitted to University of Sunderland Student Paper	

		1 %
8	Submitted to Limerick Institute of Technology Student Paper	1 %
9	global.oup.com Internet Source	1 %
10	Submitted to NCC Education Student Paper	1 %
11	purplesec.us Internet Source	1 %
12	Submitted to Higher Education Commission Pakistan Student Paper	1 %
13	Submitted to University of Bradford Student Paper	1 %
14	Submitted to Manipal University Student Paper	<1 %
15	Submitted to Savitribai Phule Pune University Student Paper	<1 %
16	Submitted to Royal Melbourne Institute of Technology Student Paper	<1 %
17	www.coursehero.com Internet Source	<1 %

18	Aiman M. Osman, Anwar Dafa-Allah, Arafat Abdulgader Mohammed Elhag. "Proposed security model for web based applications and services", 2017 International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), 2017 Publication	<1%
19	Hajar Saif Alsaadi, Rachid Hedjam, Abderezak Touzene, Abdelhamid Abdessalem. "Fast Binary Network Intrusion Detection based on Matched Filter Optimization", 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020 Publication	<1%
20	Navdeep Kaur, Parminder Kaur. "Input Validation Vulnerabilities in Web Applications", Journal of Software Engineering, 2014 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925030M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 3

Sentence Cap. Remember to capitalize the first word of each sentence.

Article Error You may need to remove this article.

Sentence Cap. Remember to capitalize the first word of each sentence.

Missing "," You may need to place a comma after this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 4

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 5

Missing "," You may need to place a comma after this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 6

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 7

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sentence Cap. Remember to capitalize the first word of each sentence.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 8

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 9

PAGE 10