International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 7|| July 2017 || PP.40-45

Disaster and Recovery Approachfor Various Online Attacks

[*]Aakanksha Chopra
[*]*Assistant Professor (IT),Department of Information Technology, Jagan Institute of Management Studies (JIMS), Rohini Sec-5,Affiliated to GGSIP, Dwarka, Sector-16, New Delhi, India*

Abstract: *Information Security has become a monstrous issue to worry about every network today. Attackers these days are smart enough to attack any vulnerable data or the data having a minute loophole. Earlier attackers were from outside the organization but today they might be working within the organization also. They not only have a motive to misuse the data but they also breach security by using automated tools to investigate network systems and hence exploits any vulnerable security point and try to gain malicious access to that network. Also due to weak security policies, data, code and many processes of organizations various internal and external breach takes place. Firewall is a hardware or software device which is designed to permit or refuse network transmission based upon certain protocols but still, various security problems keep on arising. To further gain and invigorate the network from illegitimate entry the concept of Intrusion Detection System (IDS) and Intrusion Protection System (IPS)is applied. This paper is a review paper on distinct Disaster and Recovery Approach for Online Attacks, Intrusion Detection System (IDS) and Intrusion Protection System (IPS)and their different types.*

Keywords: *Online- attacks, Intrusion, Detection, Prevention, Host-based, Network- based, Anomaly, Signature.*

I. INTRODUCTION

According to George K. Kostopoulos [4], *Vulnerability* in any system is the result of an intentional or unintentional omission or of an inadvertent design mistake that directly or indirectly leads to compromise in the systems *integrity, availability, and confidentiality*. Generally, vulnerabilities may mask in each planate of security such as- *computer and storage security, communications security, information access security, or operational and physical security.* The Vulnerabilities must be taken good care in each of information systems.The majorcomponents are ***people, hardware, and software***. There are many types of vulnerabilities which could be avoided by secure coding as most of the vulnerabilities are caused due to insecure codes only like Fig.1.

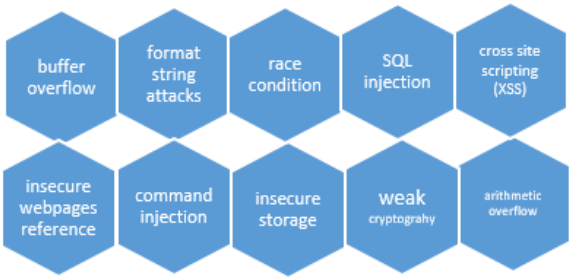

Fig.1: types of vulnerabilities due to insecure code.

An Intrusion is an act of maliciously trying to access some private data. However, intrusions can occur not only on the Internet but also in the intranets, where security is very fragile. Security can be intensified through intelligent mechanisms of authentication applied at both user side and server side [4.] Darryl White very well quoted "You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable." Looking at the statistics and increasing percentage of intranet attacks the inside system has become more vulnerable. Hence, a Disaster Recovery Plan should be adopted by all the organizations.

A disaster recovery plan binds both the hardware and software which are enforced to run captious applications and the associated processes to transform smoothly in the event of a natural or human−caused disaster. To apply Disaster recovery plan productively, we need to first assess our mission−associated processes and captious applications before constructing the extravagant recovery plan. CISCO Disaster Recovery paper illustrates on critical steps for best- practice disaster recovery: Management Awareness, Disaster Recovery Planning, Resiliency and Backup Services, and Vendor Support Services.[3]David Burns [5] have explained the concept of IDS and IPS and they have elaborated on "commonly detected attacks by a network IDS on different

layers. They also described common network anomalies on most OSI layers detected by IDS. They have also shown how IDS and IPS sensors work and set an alarm to detect and prevent the systems from any malicious acts."This paper is an extension of the previous paper of author [Refer 2]. Since the complexity of threats and corresponding solutions at an all- time high, organizations need to rethink their security strategies. This paper focuses on Intrusion Detection System, Intrusion Prevention System, Intrusion Detection and Prevention Systems, types of intrusions detection system, HIDPS, NIDPS. It also describes integrating security into the network itself so the network can firstly, continuously monitor and analyze files and identity subsequent malicious behavior whenever it may begin. Secondly, help organizations scale enforcement by having Disaster Recovery Plan, expanding the surface on which network device can be placed. Thirdly, methods to prevent various online attacks. It also explains concepts of vulnerability, exploit, risk, and threat.

II. INTRUSION DETECTION SYSTEM (IDS)

An intrusion means knowingly using someone's information without permission. Intrusion is a way someone interrupts system resources without any permission causing damages and attacks. It also involves various online attacks, cybercrimes, security threats, and security breach and security insights. It may lead to humongous attacks like DOS, Spoofing identity, hijacking, back doors, password guessing and much more [2].
*Intrusion Detection System (IDS)*is a security control or countermeasures network traffic and keep inquiring about network security. If IDS detects any menace then it alerts the system or networkadministrator. Intrusion Detection Systems were proposed in 1988, to detect intrusions. Three IDS models were been proposed based on the approach: Anomaly Detection, Misuse Detection, and Hybrid Detection [6.]IDS are a set of techniques andmethods that are used to detect incredulous activities both at the network and host level. There are two maintypes of Intrusion Detection System- Host Based Intrusion Detection Systems (HIDS) and Network BasedIntrusion Detection Systems (NIDS).

III. INTRUSION PREVENTION SYSTEM(IPS)

Intrusion Prevention System (IPS) is a security control or countermeasure that has the capability to *detect* and *prevent* misuse and abuse of, and unauthorized access to, networked resources and security. IPS is a forward combination of IDS, personal firewalls, and anti-viruses etc. The purpose of an Intrusion Prevention System (IPS) is not only to detect an attack which is trying to intrude, but also to stop it by responding automatically such as ceasing the process,logging off the user, anddebilitating the connection etc. Similar to IDS, IPS can be divided into two types, i.e. Host-Based Intrusion Prevention Systems (HIPS) and Network-Based Intrusion Prevention Systems (NIPS).An IPS or IDS detects and produces alerts because of a number of factors that include legitimate malicious activity, misconfiguration, environmental changes, and so on. Security controls are classified in one of the following terms-True positive, false positive, true negative, false negative [5.]Back in 1980, James Anderson (James, 1980) proposed the concept of intrusion detection. Then in 1988, three IDS models were been proposed based on the approach to detect intrusions: Anomaly Detection, Misuse Detection, and Hybrid Detection (Denning, 1987). Anomaly Detection based IDS produces a high rate of false positives. Misuse Detection produces smaller number of false positives, but the problem is that signature databases need to be regularly updated as their detection capability is based on them [6.]

When dealing with intrusion prevention it's important to understand difference between *vulnerability*, *exploit*, *risk*, and *threat*.***Vulnerability*** is a weakness that compromises either the security or the functionality of a system. Like- *Insecure communications, Poor passwords,Improper input handling.*An ***exploit*** is the mechanism used to leverage a vulnerability to compromise the security functionality of a system. Like- *Executable code, Password-guessing tools, Shell or batch scripts.* A ***threat*** is defined as any circumstance or event with the expressed potential for the occurrence of a harmful event to an information system in the form of destruction, disclosure, adverse modification of data, or DoS.There are three major types of threats to data- *altering, blocking, and snooping.*A ***risk*** is the likelihood that a particular threat using a specific attack will exploit a particular vulnerability of an asset or system that results in an undesirable consequence. Security engineers, administrators, and management will often try to determine risk in their business continuity and disaster recovery planning.

IV. DIFFERENT TYPES OF INTRUSION DETECTION SYSTEMS

IDSis majorly divided into two types- Anomaly Detection and Signature Detection. Against well-known attacks,the IDSdefinitely uses a database of delineated signatures formatching strings. But the canny hacker already has an idea about it and continues to fatigue the IDS byforging with new signature attacks, or by developing attacks that exploit new vulnerabilities. Anomaly-based intrusion detection is a method in the battle against intrusions, exploits, and misuse. Anomaly detection is not a cure-all alone. But when used in alliance with an effective Signature Detection method, Anomaly Detection is a viable and effective means of protecting your network infrastructure and your organization's ability to do business [7.]

Table 1: Anomaly Detection Vs. Signature Detection

Category	Anomaly Detection	Signature Detection
Definition	Anomaly detection technique store the system's normal behavior such as kernel information, systemlogs event, network packet information, software running information, operating system information etc. intothe database.	Signature detection scheme stores the sequence of pattern, the signature of attack or intrusion etc. into the database. It keeps check on intrusion activities in termsof packet headers and payload content. Used to checking for suspicious or malicious activity on the network. This method relies on its **database** of attacksignatures.
Behavior	If any abnormal behavior or intrusive activity occurs in the computer system which deviatesfrom system normal behavior then an alarm is generated.	When an attacker tries to attack or when an intrusion occurs then IDS matches the signatures of intrusion with the predefined signature that is already stored in the database. On the successful match, the system generates an alarm.
Flagging as intrusive	Anomalous activities that are not intrusive areflagged as intrusive. This will result in false-positive, i.e. false alarm. Anomaly-based intrusion detection triggers an alarm on the IDS when some type of unusual behavior occurs on your network. Intrusive activities that are not anomalous result in a false negative.	When one or more of these signatures match an alarm is triggered and the event is logged for further investigation.
Advantage/ Disadvantage	Ithas a more generalized approach when looking for and detecting threats to your network.	Signature-based intrusion detection is only as good asits database if a signature is not in the database, the IDS will not catch the attack.

Which is better?

Looking at the table it is clear that an anomaly detection method of intrusion detection has the embryonic to detect modern or unknown attacks.

V. INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)

Intrusion Detection and Prevention System (IDPS) is a procedure of controlling the events occurring in a system or network and evaluating them for feasible attacks, which are violations or threats of a misdemeanor of security policies of the system, and process of performing intrusion detection and attempting to stop detected possible incidents by techniques of prevention.IDPS is of following four different types [4]-

a. Host- based IDPS
b. Network- Based IDPS
c. Network Behavioe Analysis
d. Wireless IDPS

Table 2: Various types of IDPS

Type	Host- Based	Network-based	Network Behavior Analysis	Wireless IDPS
Protected Domain	A single host workstation or server.	Subnets and networked hosts	Subnets and networked hosts	Wireless networks and hosts
Examined Activities	Operating system application	Layers- network, transport and application	Layers- network, transport and application	Protocol activities and access authorization
Focus	Examines all activities including traffic flow and file properties	Focuses on blacklist detections, analyzes protocols	Focus on anomalous behavior	Focuses on hosts security and on traffic authorization

VI. POSSIBLE PREVENTION TECHNIQUES AND DETECTION MEASURES FOR ONLINE ATTACKS

This section elaborates on how various online attacks could be detected and prevented using anomaly detection, signature detection techniques also how the participants in the development of a secure information system work.

6.1. Denial of Service attack- These attacks are costly and most challenging for many websites –

6.1.1. Track the IP address which is flooding requests and making fake request [2.]

6.1.2. Have a tie up with internet service providers (ISP) to accept all the traffic from authentic users only-

i. They can keep a check on an IP address requesting same URL again and again.

ii. Fix a counter like structure which will restrict the number of access to a particular URL in a day, a week or a month; resulting in reducing the attacks.

6.1.3. Should have a stronger network security to block unnecessary network traffic to the systems

6.1.4. There should be ample backup and recovery measures

6.1.5. Prepare adequate standby system capacity- standby systems are the tangible insurance policy. Instead of losing data and huge amount of money it's better to save money in standby systems.

6.1.6. Use scanning tools which helps in identifying and analyzing security vulnerabilities in Network, Operating system and databases.
6.1.7. Can also perform penetration testing to check and assess the ability of network and system to stand against DOS and DOS attacks.
6.1.8. Anomaly detection technique of IDS should be applied to detect data originality from system themselves.

6.2. Spoofing Identity- spoofing aims at deceiving the network so that it recognizes an unauthorized desktop system as if he was an authorized desktop system to gain access to the network and / or sensitive data. The victim may not be aware of the connection is not effective-
6.2.1. Should install properly configured firewalls at appropriate locations.
6.2.2. Perform constant monitoring on network traffics and potential intruders.
6.2.3. A stronger authentication technique should be used for authenticating messages transmitted within an authenticated session- not based on IP address but should be based on an encrypted identity that is unique for each new session
6.2.4. A *Signature Detection* scheme of IDS should be implemented. When an intruder tries to attack or when any intrusion occurs IDS matches the signatures of intruder with predefined signatures already stored in Database if it matches the IDS system generates an alarm and preventive measure could be taken [1.]

6.3. Hijacking- it is possible that once a user logs in to a remote computer using user ID and password then the connection will be stolen.
6.3.1. Should implement strong authentication policy for remote access so that after fixed period re-authentication for continuation should be asked for highly sensitive data.
6.3.2. Proper firewalls should be installed at appropriate points.
6.3.3. *Anomaly detection & Prevention*System*s*hould be installed for avoiding hijacking [1].
6.3.4. Promiscuous- mode[1] ***Network Intrusion Detection System*** could be used to analyze network packets. We can perform monitoring of network traffics also as this system "sniffs" all the packets on a network segment can be used to analyze the behavior.
6.3.5. Scanning tools could be used to do penetration testing to extract and identify vulnerabilities of hijacking attack.
6.3.6. Strong end-to-end encryption should be done for highly sensitive data.

6.4. Random Dialling/ War Dialling-
6.4.1. Adequate network security should be there so that all modems are authorized and controlled. For e.g.- on fixed intervals "wardialling" should be done to detect unauthorized modem.
6.4.2. All the modems should be centralized in a physically secured locations & it should be separated from network segment from other crucial and sensitive internal network. This separation helps restricting the attackers to gain unauthorized access to an internal network through modems.
6.4.3. The modems should be configured in "dial- back" mode so that remote network connection from modem will only be visible if remote server is preapproved.
6.4.4. Scanning tools could also be used on penetration testing could be done used or penetration testing could be done to identify vulnerability to war dialling risk.
6.4.5. An *Anomaly Detection* scheme of IDS should be implemented.

6.5. Backdrops/ Trapdoors-
6.5.1. We should make a provision to install a strict development system and change control procedures so as to insure that the systems are only used for testing purposes and it will as insure no backdoors have been included in system.
6.5.2. One should always accept systems from trusted sources who provides guarantee and certification that no product contains backdoors entry loopholes.
6.5.3. Always do regular integrity checks on programs used in production to ensure no alteration.
6.5.4. An *Anomaly Detection*and *Signature Detection* scheme of IDS should be implemented together.

6.6. Brute Force-
6.6.1. Substantial password policies should be enforced for eg.- acquiesce minimum password length and cyclic changes in passwords.
6.6.2. Vigorous encryption technology should be setup to safeguard user ID, passwords and confidentiality of data being exchanged.

6.6.3. Penetration testing should be done to determine vulnerabilities to malicious interferences and will help in estimating the strength of encryption.
6.6.4. Sufficient knowledge should be given to customers about managing and keeping passwords.
6.6.5. A*Signature Detection* scheme of IDS should be implemented together.

6.7. Exploiting known Security Vulnerabilities-
6.7.1. All the unused and unwanted programs and computer processes of servers and firewalls should be disabled so that attackers do not find any security weaknesses.
6.7.2. Newly invented security patches and updates on Operating system should be practiced.
6.7.3. Prime hardware and software merchants having hands-on on latest technology developments should be kept to defend from the recent attack techniques.
6.7.4. Significant penetration testing should be done to determine vulnerabilities like protocol defect/ fault or program bugs.
6.7.5. An *Anomaly Detection*and *Signature Detection* scheme of IDS should be implemented together.

6.8. Social Engineering-
6.8.1. Adequate security measures against illegitimate access from foreign parties.
6.8.2. Ample guidance to customers on security precautions should be provided.
6.8.3. An *Anomaly Detection*and *Signature Detection* scheme of IDS should be implemented together.

6.9. Password Guessing -
6.9.1. Strict password policies should be enforced for e.g.-acquiesce minimum password length and cyclic changes in passwords.
6.9.2. Disable used ID's after fixed number of failed logon attempts.
6.9.3. Precisely variate all default passwords on critical network components.
6.9.4. Give suitable guidance to customers on various security protection specifically on setting and managing passwords.
6.9.5. An *Anomaly Detection*and *Signature Detection* scheme of IDS should be implemented together.

6.10. Viruses-
6.10.1. Always use updated virus scanning tools.
6.10.2. Get certification from merchants that all products are virus free.
6.10.3. Policies should be made against the unwanted use of interest and electronic mails.
6.10.4. Formulate all information security policies.
6.10.5. Maximum use of distributed firewalls should be done.
6.10.6. Users should be given instructions on versions security procuration like opening e-mail attachments and use of internet or malicious websites and links.

6.11. Trojan Horses-
6.11.1. Routine integrity checks on all programs used in production should be done.
6.11.2. To make sure no Trojan horses enters the system one should forcefully place system development and change control procedures such that systems can normally be put into production only after thorough testing.
6.11.3. Formulate all information security policies.
6.11.4. Make best policies against unwanted use of internet and emails.
6.11.5. High level trainings should be given to internal members on security issues so that they always have a proactive approach against Trojan horses.
6.11.6. Users should be given instructions on versions security procuration like opening e-mail attachments and use of internet or malicious websites and links.

VII. CONCLUSION

The anomaly-based method is exquisite at providing the warning before potential intrusions could take place because it identifies any traffic behavior that is new or bizarre. These warnings can detect exploration attempts, backdoor entries, and certain natural failures in the network. For known attacks, signature detection generally provides the most accurate detection in the shortest time. In this way, known attacks, as well as those attacks whose signatures are not yet known and attacks that exhibit modified behavior, can be blocked.Hence, anomaly detection intrusion technique provides the best protection for your network when it is collated with a signature detection approach.

REFERENCES

[1] U. A. Sandhu, S.Haider, S.Naseer, and O. U.Ateeb, A Survey of Intrusion Detection & Prevention Techniques, 2011 International Conference on Information Communication and Management, IPCSIT vol- 16 (2011), IACSIT Press, Singapore, 66-67.

[2] A. Chopra, A Review Paper on Discrete Online Attacks, International Journal of Engineering, Business and Enterprise Applications (IJEBEA), 2016, ISSN (Print): 2279-0020, ISSN (Online): 2279-0039, 7-8.

[3] Cisco Disaster Recovery: Best Practices White Paper, 1992-2003

[4] George K. Kostopoulos, Cyberspace and Cybersecurity(Boca Raton London, New York, CRC Press, Taylor & Francis Group, 2013.)

[5] D. Burns, O. Adesina, and K. Barker, CCNP Security: Intrusion Prevention and Intrusion Detection System, Nov 22, 2011.Available at: http://www.ciscopress.com/articles/article.asp?p=1763920&seqNum=2

[6] M. A. Shibli, S. Muftic, Intrusion Detection and prevention System Using Secure Mobile Agents, IEEE INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY,(PP. 76- 82), PORTO PORTUGAL, JULY 2008.

[7] Dr. F. Gong, McAfee Network Security Technologies Group, White paper: Deciphering Detection Techniques: Part II Anomaly-BasedIntrusion Detection, March 2003.

International Journal of Engineering and Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

*Aakanksha Chopra "Disaster and Recovery Approachfor Various Online Attacks**"***
International Journal of Engineering and Science Invention (IJESI) 6.7 (2017): 40-45