ISSN: 2976-7466

Journal of Biosensors and Bioelectronics Research

SCIENTIFIC Research and Community

Review Article

Open Access

Guarding Networks: Understanding the Intrusion Detection System (IDS)

Pavan Navandar

Independent Researcher

***Corresponding author**
Pavan Navandar, Independent Researcher, USA.

Received: June 10, 2023; **Accepted:** June 17, 2023; **Published:** June 24, 2023

An Intrusion Detection System (IDS) maintains network traffic looks for unusual activity and sends alerts when it occurs. The main duties of an Intrusion Detection System (IDS) are anomaly detection and reporting; however, certain Intrusion Detection Systems can act when malicious activity or unusual traffic is discovered. In this article, we will discuss every point about the Intrusion Detection System.

What is an Intrusion Detection System?

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using an SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections.

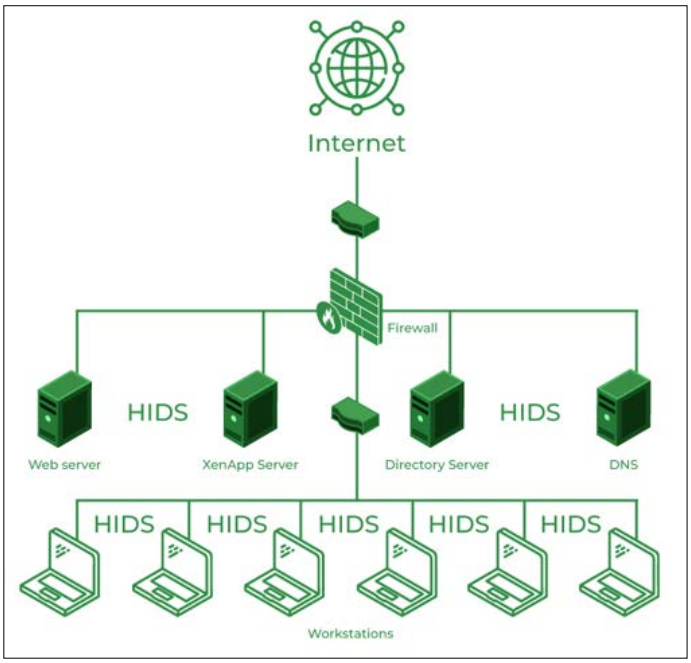
Working of Intrusion Detection System (IDS)

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Classification of Intrusion Detection System (IDS)

Intrusion Detection System are classified into 5 types:

- **Network Intrusion Detection System (NIDS):** Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.
- **Host Intrusion Detection System (HIDS):** Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



- **Protocol-based Intrusion Detection System (PIDS):** Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly

monitoring the HTTPS protocol stream and accepting the related HTTP protocol. As HTTPS is unencrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

- **Application Protocol-based Intrusion Detection System (APIDS):** An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols. For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.
- **Hybrid Intrusion Detection System:** Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system. The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Intrusion Detection System Evasion Techniques

- **Fragmentation:** Dividing the packet into smaller packet called fragment and the process is known as fragmentation. This makes it impossible to identify an intrusion because there can't be a malware signature.
- **Packet Encoding:** Encoding packets using methods like Base64 or hexadecimal can hide malicious content from signature-based IDS.
- **Traffic Obfuscation:** By making messages more complicated to interpret, obfuscation can be utilized to hide an attack and avoid detection.
- **Encryption:** Several security features, such as data integrity, confidentiality, and data privacy, are provided by encryption. Unfortunately, security features are used by malware developers to hide attacks and avoid detection.

Benefits of IDS

- **Detects Malicious Activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
- **Improves Network Performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
- **Compliance Requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
- **Provides Insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Detection Method of IDS

- **Signature-based Method:** Signature-based IDS detects attacks based on specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects based on the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system, but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.
- **Anomaly-based Method:** Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model. The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls

IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Placement of IDS

The most optimal and common position for an IDS to be placed is behind the firewall. Although this position varies considering the network. The 'behind-the-firewall' placement allows the IDS to have high visibility of incoming network traffic and will not receive traffic between users and network. The edge of the network point provides the network with the possibility of connecting to the extranet.

In cases where the IDS is positioned beyond a network's firewall, it would be to defend against noise from internet or defend against attacks such as port scans and network mapper. An IDS in this position would monitor layers 4 through 7 of the OSI model and would use Signature-based detection method. Showing the number of attempted breaches instead of actual breaches that made it through the firewall is better as it reduces the number of false positives. It also takes less time to discover successful attacks against networks.

An advanced IDS incorporated with a firewall can be used to intercept complex attacks entering the network. Features of advanced IDS include multiple security contexts in the routing level and bridging mode. All of this in turn potentially reduces cost and operational complexity.

Another choice for IDS placement is within the network. This choice reveals attacks or suspicious activity within the network. Not acknowledging security inside a network is detrimental as it may allow users to bring about security risk or allow an attacker who has broken into the system to roam around freely.

Conclusion

Intrusion Detection System (IDS) is a powerful tool that can help businesses in detecting and prevent unauthorized access to their network. By analyzing network traffic patterns, IDS can identify any suspicious activities and alert the system administrator. IDS can be a valuable addition to any organization's security infrastructure, providing insights and improving network performance [1-28].

References

1. Managing cyber risks in an interconnected world, Key findings from The Global
   a. State of Information Security Survey 2015. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.
2. NIST Cybersecurity Practice Guide, SP-1800-3: Attribute

Based Access Control,
   a. NIST. https://www.nccoe.nist.gov/sites/default/files/legacy-files/abac-nist-sp1800-3-draft-v2.pdf
3. NIST (2014) Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
4. EMV Payment Tokenization Specification - Technical Framework, Version 1.0,
   a. EMVCo, LLC https://www.emvco.com/specifications.aspx?id=263.
5. EMV and Encryption + Tokenization: A Layered Approach to Security. A First Data
   a. White Paper https://studylib.net/doc/8389165/emv-and-encryption---tokenization--a-layered-approach-to-...
6. What Every Card Not Present Merchant Should Know, Navigating Today's
   a. Challenging Payments Ecosystem. Verifi Inc, https://www.verifi.com/wp-content/uploads/2014/05/Verifi_eBook_web_noCNP.pdf.
7. Visa Best Practices for Tokenization Version 1.0, Visa Inc,
   a. https://usa.visa.com/dam/VCOM/global/support-legal/documents/bulletin-tokenization-best-practices.pdf.
8. Information Supplement: PCI DSS Tokenization Guidelines Version 2.0, August
   a. 2011, Scoping SIG, Tokenization Taskforce, PCI Security Standards Council,
   b. https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_
   c. Supplement.pdf
9. Tokenization Product Security Guidelines - Irreversible and Reversible Tokens
   a. Version 1.0, PCI Security Standards Council, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.
10. Implement Data Masking to Protect Sensitive Data: Part 1, Biswajit
    a. Maji, IBM, http://www.ibmbigdatahub.com/blog/implement-data-maskingprotect-sensitive-data-part-1.
11. Implement Data Masking to Protect Sensitive Data: Part 2, Biswajit Maji, IBM, http://www.ibmbigdatahub.com/blog/implement-data-maskingprotect-sensitive-data-part-2.
12. Data Masking Best Practice. an Oracle White Paper, Oracle Corporation,
    a. https://www.oracle.com/technetwork/database/manageability/data-masking-wp-12c-1964774.pdf.
13. Security is Not Just External - Don't Forget the "Other" Security, http://www.securityweek.com/security-not-just-external-dont-forget-other-security.
14. S Schober (2015) Real cost of data breaches still on the rise. http://www.cutimes.com/2015/03/01/real-costsof-data-breaches-still-on-the-rise.
15. W Long (2015) EU Data Protection Regulation: fines up to €100m proposed, http://www.computerweekly.com/opinion/EU-Data-Protection-Regulation-fines-up-to-100m-proposed.
16. L Whitfield (2015) ICO spells out £500,000 penalty plans, http://www.ehi.co.uk/news/EHI/5542/ico-spells-out%C2%A3500000-penalty-plans.
17. R Mckeane (2014) EU data protection reform: 12 things businesses need to know, http://www.theguardian.com/media-network/olswang-partner-zone/2014/dec/04/eu-data-protectionreform-business-fines.
18. D Worth (2013) Target takes $162m hit from cyber-attack data breach, http://www.privacyrisksadvisors.com/news/target-takes-162m-hit-from-cyber-attack-data-breach-by-danworth.
19. Poniman Institute (2015) The State of Data-Centric Security. http://www.banktech.com/pdf_whitepapers/incoming/1411503329_ponemon_infa_security.pdf.
20. M Greenway (2015) Data Obfuscation - managing data privacy in development and test environments. https://cdn2.hubspot.net/hubfs/2930497/Labs/Labs%20Products%20and%20Services/DSM%20Suite/PDFs/EN/Data_Security_and_impact_whitepaper.pdf?t=1507332164666.
21. Gartner (2013) Gartner Magic Quadrant for Data Masking Technology. https://www.gartner.com/en/documents/2636081.
22. M Rizvi (2023) Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Sciences 10: 055-060.
23. I Wiafe, FN Koranteng, EN Obeng, N Assyne, A Wiafe, et al. (2020) Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access 8: 146598-146612.
24. Bishtawi T, Alzubi R (2022) Cyber Security of Mobile Applications Using Artificial Intelligence. 1st International Engineering Conference on Electrical, Energy, and Artificial Intelligence https://www.researchgate.net/publication/368968557_Cyber_Security_of_Mobile_Applications_Using_Artificial_Intelligence.
25. Achi A, Kuwunidi Job G, Shittu F, Baba Atiku S, Unimke Aaron A, et al. (2021) Survey on The Applications of Artificial Intelligence in Cyber Security. Survey On the Applications of Artificial Intelligence in Cyber Security Article in International Journal of Scientific & Technology Research 9: 165-170.
26. Abbas NN, Ahmed T, Shah SHU, Omar M, Park HW (2019) Investigating the applications of artificial intelligence in cyber security. Scient metrics 121: 1189-1211.
27. Bhatele KR, Shrivastava H, Kumari N (2019) The Role of Artificial Intelligence in Cyber Security 170-192.
28. GA, S (2022) The Review of Artificial Intelligence in Cyber Security. International Journal for Research in Applied Science and Engineering Technology 10: 1461-1468.