Antecedentes

Los Sistemas de Detección de Intrusiones (IDS) son componentes esenciales en la infraestructura informática moderna para monitorizar e identificar tráfico de red no deseado y malicioso, como accesos no autorizados o sistemas mal configurados. Tradicionalmente, la mayoría de los IDS comerciales se basan en firmas, utilizando un conjunto de reglas para determinar qué constituye tráfico malicioso mediante la monitorización de patrones específicos. Sin embargo, si bien estos sistemas son muy efectivos contra amenazas conocidas, la detección basada en firmas falla cuando los vectores de ataque son desconocidos o cuando los ataques conocidos se modifican para eludir las reglas.

Además de su dificultad para identificar amenazas desconocidas o modificadas, los sistemas basados en firmas suelen estar plagados de falsos positivos en escenarios del mundo real. Esto es particularmente problemático en la detección de shellcode malicioso, donde los patrones binarios pueden ser difíciles de distinguir del tráfico de red benigno, llevando a que las firmas deban ser deshabilitadas y volviéndolas inútiles. Minimizar la tasa de falsos positivos es una preocupación importante, ya que un alto número de estos puede ahogar el código malicioso real y hacer que el sistema sea ineficaz.

La evolución y el uso extendido de los Sistemas de Información y Telecomunicaciones (ITS) han llevado a un rápido crecimiento del tráfico de red que necesita ser procesado y analizado. Para abordar estos problemas, han surgido métodos basados en aprendizaje automático (ML) y redes neuronales artificiales (ANN). Las ANN, inspiradas en el comportamiento de las neuronas biológicas, son algoritmos capaces de capturar relaciones altamente complejas y no lineales en los datos sin conocimiento previo. Han sido utilizadas en una amplia variedad de tareas de clasificación y en varios dominios de seguridad informática, incluyendo la detección de virus y el análisis de fallos de diseño de software.

Un tipo de amenaza común y crucial en las redes es el escaneo de puertos (PortScan). Este es a menudo el primer paso en un ciberataque, donde un atacante escanea sistemáticamente un rango de puertos de red en un sistema objetivo para identificar posibles vulnerabilidades, configuraciones de red, implementaciones de servidores y sistemas operativos. Identificar y enumerar máquinas activas y sus servicios mediante el envío de sondas y el análisis de sus respuestas es una fase indispensable del reconocimiento en ciberintrusiones. Los escaneos pueden ser internos (dentro de la red corporativa) o externos (desde fuera de la red). Los atacantes emplean diversas técnicas de evasión, como la reducción de la tasa de escaneo, para eludir los algoritmos de detección basados en el comportamiento. Por lo tanto, se requiere un enfoque más inteligente y adaptativo para la detección de intrusiones y la clasificación precisa del tráfico de red.

Estado del Arte

El Estado del Arte en la precisión de clasificación de datos en tráfico de red, la defensa dinámica y reducción de falsas alarmas, y la estadística de indicadores de escaneo (IoS), ha visto avances significativos con la aplicación de técnicas de Inteligencia Artificial.

Precisión de Clasificación de Datos en Tráfico de Red

Las Redes Neuronales Artificiales (ANNs) han demostrado ser muy eficaces para la detección de tráfico malicioso. Un enfoque novedoso utilizando ANNs para la detección de shellcode malicioso logró una precisión promedio del 98%, con una tasa de falsos positivos inferior al 2% en validaciones cruzadas repetidas, lo que demuestra la robustez, precisión y exactitud de la técnica.

En el contexto de la Seguridad del Internet de las Cosas (IoT), los modelos de aprendizaje automático (ML) y aprendizaje profundo (DL) han alcanzado una alta precisión en la predicción de ataques. Un estudio evaluó clasificadores como Random Forest (RF), ANN, Regresión Logística (LR) y Support Vector Machine (SVM) en un conjunto de datos en tiempo real (RT-IoT2022). RF mostró una precisión del 99.9%, mientras que ANN alcanzó el 99.8%. Esto subraya la capacidad de estos algoritmos para identificar diversos tipos de ciberataques en el IoT, incluyendo ARP_poisoning, DOS_SYN_Hping, MQTT_Publish, NMAP_FIN_SCAN, NMAP_OS_DETECTION y Thing_Speak.

Para mejorar la calidad de los modelos de ML, se ha propuesto la segmentación de datos cuando se analiza el estado de los sistemas de telecomunicaciones. Este método, que divide la muestra de datos en subconjuntos basados en factores que afectan las propiedades del tráfico, permite usar algoritmos de clasificación que tienen los mejores indicadores de calidad en segmentos de datos individuales. La segmentación de datos permite una mejor adaptación a los cambios en los rangos y distribuciones de las variables estudiadas a lo largo del tiempo, lo que es crucial ya que las propiedades del tráfico pueden cambiar durante el funcionamiento de los ITS. Al minimizar la función de pérdidas en cada subconjunto segmentado, se puede seleccionar el clasificador más adecuado para ese segmento específico, mejorando los indicadores de calidad de clasificación en condiciones operativas cambiantes.

En la detección de ataques de PortScan, el uso de algoritmos de ML también ha mostrado resultados prometedores. Un estudio que utilizó el conjunto de datos CICIDS2017 para detectar ataques de PortScan, encontró que el algoritmo JRip alcanzó una precisión del 99.84%, superando a OneR con 99.56%. Estos modelos se benefician de métodos híbridos de selección de características, como la combinación de filtrado por varianza y la relación de ganancia de información (IGR), para reducir el número de atributos a un conjunto óptimo de 13 características.

Además, un sistema de seguridad de red anti-mapeo dinámico ha logrado una precisión del 98% utilizando el modelo Bi-LSTM+Attention en el conjunto de datos UNSW-NB15, cubriendo varios tipos de ataques.

Defensa Dinámica y Reducción de Falsas Alarmas

La reducción de falsas alarmas es un objetivo central en el desarrollo de IDS. El enfoque basado en ANNs para la detección de shellcode no solo logró una sensibilidad perfecta, sino que también exhibió una excelente precisión (minimizando los falsos positivos), con una tasa de falsos positivos inferior al 2% en un conjunto de datos extremadamente grande de tráfico benigno. Esto es fundamental, ya que altos niveles de falsos positivos pueden hacer que un sistema de intrusión sea inútil.

Los métodos que se adaptan a las propiedades cambiantes de los datos y a la detección de puntos de cambio en las series de tiempo, como los propuestos por Lebedev y Rzayev, permiten mejorar la calidad de clasificación en entornos teleinformáticos con

condiciones de operación continuas y cambiantes. Al dividir la muestra en segmentos con diferentes propiedades de datos, los modelos pueden ser pre-entrenados y asignados con los mejores indicadores de calidad, lo que, a diferencia de los enfoques de ensemble, evita que algoritmos más débiles degraden el resultado general y reduce la intensidad de recursos. Este método también permite combatir las emisiones y el ruido, y formar subconjuntos localizados de manera compacta en el espacio de objetos, lo que puede aumentar los indicadores de calidad hasta en un 5%.

Las estrategias de seguridad anti-mapeo dinámicas han sido exploradas para contrarrestar el escaneo de red ilegal. Esto incluye la combinación de asignación dinámica de direcciones IP, ofuscación de puertos, camuflaje de tráfico y análisis de comportamiento para mejorar el sigilo y las capacidades anti-detección del sistema. Utilizando un modelo Bi-LSTM+Attention, se ha logrado una reducción del 30% en la tasa de falsas alarmas en comparación con el modelo LSTM tradicional. Este enfoque integra firewalls inteligentes y sistemas de prevención de intrusiones (IPS), empleando Modelos Ocultos de Markov (HMM) y redes LSTM para identificar y bloquear comportamientos de escaneo maliciosos, y optimizar las listas de control de acceso (ACL).

Otro enfoque proactivo para la detección de escaneos implica la monitorización y manipulación del tráfico DNS. Un método propuesto detecta escaneos internos y externos en redes corporativas correlacionando los flujos de red con las consultas y respuestas DNS precedentes, y reduciendo los valores TTL (tiempo de vida) de los Registros de Recursos DNS (RR). Este mecanismo es efectivo contra escáneres sigilosos y adaptativos, y su despliegue incurre en una sobrecarga insignificante en los tiempos de respuesta de DNS y de red. La reducción de los valores TTL de las respuestas DNS es crucial, ya que sin ella, los atacantes podrían aprovechar los registros DNS en caché para eludir la detección. Este enfoque ha demostrado ralentizar el éxito de los escaneos hasta 20,000 veces en la propagación de gusanos.

Estadísticas de Indicadores de Escaneo (IoS) en Tráfico de Red

La identificación de Indicadores de Escaneo (IoS) es fundamental para desarrollar sistemas de detección de intrusiones más efectivos. Investigaciones recientes han profundizado en las características del tráfico de escaneo de puertos, particularmente el generado por herramientas como Nmap. Los IoS incluyen características como:

• Distribución de puertos de destino: Nmap tiende a seleccionar puertos aleatorios de sus bases de datos específicas, a diferencia de otras herramientas como Metasploit, que pueden seguir un patrón ascendente. Analizar esta distribución ayuda a reconocer la herramienta utilizada y los comandos empleados.

• Puertos de origen: El número y la secuencia de puertos de origen utilizados pueden ser una firma para el tipo de escaneo (por ejemplo, SYN o Connect) y la herramienta (Nmap vs. Metasploit).

• Tamaño, duración y número de paquetes: Estas características varían según el tipo de escaneo y la configuración de la herramienta, y pueden ser utilizadas para caracterizar el tráfico de escaneo.

• Medidas estadísticas: Calcular la media, desviación estándar y varianza de los puertos de destino o de origen puede ayudar a detectar la selección aleatoria de puertos en Nmap y, por lo tanto, la presencia de un escaneo.

Herramientas como Nmap son ampliamente utilizadas para ataques de reconocimiento, mientras que Metasploit proporciona una infraestructura completa para pruebas de penetración y también puede generar tráfico de escaneo. El estudio del tráfico generado por estas herramientas revela patrones distinguibles, como la secuencia de puertos (aleatoria en Nmap por defecto, ascendente en Metasploit).

Las técnicas de escaneo varían e incluyen SYN, TCP Connect, Xmas, FIN, Null, ACK, Window y Maimon. La detección tradicional basada en firmas o comportamiento puede ser eludida por técnicas de escaneo nuevas, modificadas o sigilosas. Los detectores basados en el comportamiento, aunque diseñados inicialmente para gusanos, pueden ser vulnerables a escáneres lentos y sigilosos que utilizan perfiles de tiempo conservadores, eludiendo la detección al operar por debajo de ciertos umbrales. Esto resalta la necesidad de enfoques que utilicen IoS avanzados y análisis estadístico para identificar estas amenazas.

Referencias

1. Al-Khazaali, Z., Al-Ghabban, A., Al-Musawi, H., Sabah, A., & Al Mahdi, N. (2025). Characteristics of Port Scan Traffic: A Case Study Using Nmap. Journal of Engineering and Applied Sciences Department, 29(01). https://doi.org/10.31272/jeasd.2638

2. Arabiat, A., & Altayeb, M. (2024). Enhancing internet of things security: evaluating machine learning classifiers for attack prediction. International Journal of Electrical and Computer Engineering, 14(5), 6036–6046. https://doi.org/10.11591/ijece.v14i5.pp6036-6046

3. Guo, M., Ma, D., Jing, F., Zhang, X., & Liu, H. (2025). Dynamic Anti-Mapping Network Security Using Hidden Markov Models and LSTM Networks Against Illegal Scanning. Informatica, 49(12), 207–220. https://doi.org/10.31449/inf.v49i12.6903

4. Jafarian, J. H., Abolfathi, M., & Rahimian, M. (2023). Detecting Network Scanning Through Monitoring and Manipulation of DNS Traffic. IEEE Access, 11, Art. 3250106. https://doi.org/10.1109/ACCESS.2023.3250106

5. Kareem, M. I., Abood, M. J. K., & Ibrahim, K. (2023). Machine learning-based PortScan attacks detection using OneR classifier. Bulletin of Electrical Engineering and Informatics, 12(6), 3690–3696. https://doi.org/10.11591/eei.v12i6.4142

6. Lebedev, I., & Rzayev, B. (2023). Segmentation of data when analyzing the state of telecommunication systems. Indonesian Journal of Electrical Engineering and Computer Science, 29(3), 1473–1479. https://doi.org/10.11591/ijeecs.v29.i3.pp1473-1479

7. Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4, 95–99. https://doi.org/10.1016/j.icte.2018.04.003