IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INFORMATION PERTAINING TO NETWORK SECURITY RELATED DATA

S.Vimalathithan[1] M.Kanmani[2],W.Karishma[3], S.Vishali[4]
1 – Associate Professor , 2 – Assistant Professor, 3&4 – II year student
Mohamed Sathak A J College of Engineering, Chennai , India.

Introduction: Network security refers to a variety of measures, technologies, schemes, and procedures aimed at protecting computer networks and the data they transmit from unauthorized access, misuse, modification or demolition. Common network security measures include firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), encryption, access control, and monitoring and logging tools. Organizations of all sizes need to implement strong network security measures to prevent the loss or compromise of sensitive data, which can result in serious consequences such as financial losses, damage to reputation, and legal liability.

this paper discusses the challenges and importance of collecting security-related data in network systems, focusing on big data and 5G network systems. The 5V characteristics of security-related data are highlighted as a factor that makes data collection difficult in large-scale heterogeneous network systems. The paper focuses on collecting data for detecting network attacks, intrusions, and anomalies, reviews existing network data collection technologies, and evaluates their performance towards high-quality network security-related data collection.

Network security data collection:

Network security-related data refers to the type of data that can reflect the security status of a network system and can be used to detect network attacks by searching for abnormal network data. For example, Time to Live (TTL) is a type of network security-related data that can be used to detect Denial of Service (DoS) attacks.

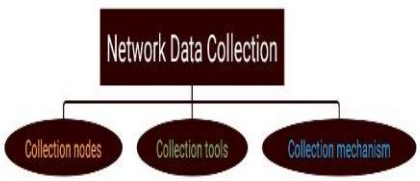


Figure 1:data collection technologies

Collection Nodes:

The common data collection nodes in a network system include routers, switches, gateways, IDSs/IPSs, firewalls, honey-pots, sensors, proxy servers/collecting servers, agents, mobile terminals, and distributed collection nodes. These nodes have different functions and are used for different purposes such as packet delivery, security, and data collection. Mobile terminals are often used due to their mobility and flexibility.

Figure: Collection nodes

Collection Tools

Network data collection tools can be classified based on software, hardware, and network protocol. Hardware-based tools provide high performance for large-scale systems but are inflexible and expensive. Network protocol-based tools are complex and not suitable for mobile devices. A universal data collector is needed that can be applied to different network nodes and systems. In the next section, different data collection tools are introduced in detail.

Figure3: Collection tools

A) SOFTWARE BASED DATA COLLECTION

Software based data collection tools refer to the use of computer programs and application to collect processes ,making the faster ,more efficient and less prone to errors

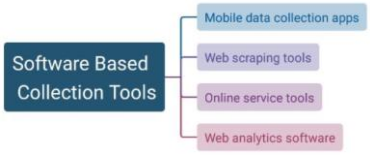


Figure 4: Software based collection tools

i) Mobile Data Collection Apps

Mobile data collection is a method of collecting data using mobile devices, such as smart phones or tablets, for the purpose of network security. It involves using software-based data collection tools to gather information about a network's security status, such as vulnerability assessments, compliance checks, or threat intelligence.

Mobile data collection typically works by installing a specialized app on a mobile device that is connected to the network being monitored. The app then uses various techniques to gather data, such as port scanning, network traffic analysis, or endpoint profiling. This data is then analyzed and presented to the security team, who can use it to identify and mitigate potential security threats.

ii) Web scraping tools:

Web scraping tools are software-based data collection tools that are used to extract information from websites and web applications. These tools can be used in network security to collect information about a target website or application, such as identifying potential vulnerabilities or analyzing the structure of the application.

Web scraping tools typically work by sending requests to a website or application and then parsing the response to extract the desired information. Web scraping tools can also automate the process of navigating through a website to collect data from multiple pages or sections of the site.

iii) Online survey tools:

Online survey tools are software-based data collection tools that can be used for a variety of purposes, including collecting information related to network security. These tools allow researchers or security

professionals to create and administer surveys that can be accessed online by participants, making it easy to collect data from a large number of people.

iv) Web Analytics Software

Web analytics software is a type of software-based data collection tool that is used to collect, process, and analyze data related to website usage and performance. In the context of network security, web analytics software can be used to monitor and analyze network traffic to identify potential security threats or vulnerabilities.

Web analytics software typically works by collecting data from website visitors, such as their IP address, device type, and browsing behavior. This data is then analyzed to provide insights into website usage patterns, user behavior, and the effectiveness of marketing campaigns.

B)Network Protocol Based Data Collection

Network protocol-based data collection technologies can provide a comprehensive understanding of the whole network system and are usually applied in the application scenarios of network management and network problem diagnosis.

i)SNMP

Simple Network Management Protocol (SNMP), which is widely used to monitor, control, configure, and manage network systems. SNMP consists of three key components: network devices, SNMP agents, and NMS. It enables network managers to troubleshoot problems and conduct MIB information polling for real-time analysis.

ii)TELNET

Telnet protocol as a network protocol that can be used to capture network data packets. A Telnet client can be configured to periodically establish Telnet connections with a router, which returns text-based results that can be analyzed to extract traffic data. Telnet-based data collection technology is faster and results in minimal data redundancy compared to SNMP protocol. However, using Telnet to collect network data requires root authority, which could pose potential network security problems

iii)IPFIX

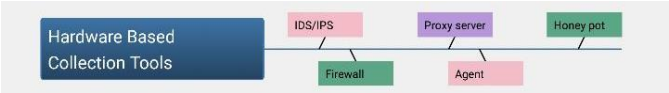
IP Flow Information Export (IPFIX), a universal standard that defines how IP flow information is to be formatted and transferred from routers, probes, and other devices to a collector for network measurement or traffic billing. IPFIX provides flexibility in allowing users to define the data types they need to convey and is used to format preprocessed reports in some traffic monitoring applications to detect distributed network anomalies and attacks. It can collect data at multiple scattered nodes of a network system, providing a comprehensive and objective understanding of the network system.

iv)Netflow

NetFlow is a data exchange mode introduced by Cisco mainly used for planning network traffic and managing traffic growth. NetFlow provides a higher level of abstraction by assembling related packets into groups called flows. Cisco provides NetFlow Collector (NFC) to collect NetFlow data, and other manufacturers offer similar collection software. It is a scheme that combines NetFlow protocol and device polling to capture and analyze packets in a Gigabit network.

C)*Hardware Based Data Collection*

Hardware-based data collection technologies are high-performance solutions, commonly used in scenarios such as IDS, but come at a high cost. AMD platforms have been found to yield better capturing results compared to Intel platforms due to better memory management and handling of bus contention. Other hardware devices used for data collection will be introduced next.



i)IDS/IPS

IDS/IPS based on hardware is a network security device used for detecting network intrusions and anomalies. It collects network data to detect attacks and anomalies, and there are two kinds of intrusion detection technologies: anomaly detection and misuse detection. The development of information technology and security requirements has led to an increasing amount of work on IDS/IPS.

ii)*Firewall*

Hardware-based firewalls are network security devices that monitor incoming and outgoing traffic based on pre-set rules. There are three categories of firewalls: Packet Filter, Application layer, and Proxy-based. Packet Filter firewalls examine packet headers, while Application layer firewalls identify protocols through Deep Packet Inspection. Proxy-based firewalls utilize proxy servers to provide authentication, logging, and account management functions. Integrating collecting functions into firewalls is preferable to detect attacks and anomalies originating from both inside and outside networks.

iii)*Proxy Server*

LANs can use proxy servers for network relaying and data collection. Proxy servers can record all transmitted data in detail and store them to disk as text-based traffic logs or even into a database, making them a practical data collection tool.

iv)*Agent*

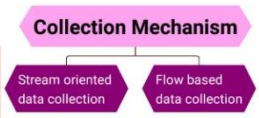
The system uses a hierarchical structure to gather information from multiple agents running on different hosts to identify anomalies and attacks in the network. It is an effective approach for detecting distributed network attacks.

v)*Honey Pot*

A honeypot is a security system that masquerades as a real system to divert attackers away from critical resources and record abnormal behavior. It can collect known or unknown attack data to prevent attacks on critical systems and can operate in encrypted network environments. However, deploying a honeypot system is expensive and requires careful configuration to effectively defend against attacks and record attack information.

D) Collection Mechanism:

A collection mechanism in network data collection refers to the method used to collect data from network devices or systems. The collection mechanism depends on the type of data being collected, the network topology, and the devices or systems involved.



1. *Stream Oriented Data Collection*

Stream oriented data collection in network security refers to the process of continuously collecting and analyzing data from network traffic in real-time. This data can include information such as packet headers, payloads, source and destination IP addresses, and protocol types.The goal of stream-oriented data collection is to identify and respond to security threats as quickly as possible. By analyzing network traffic in real-time, security analysts can detect anomalies, patterns, and potential attacks before they can cause significant damage.

Stream-oriented data collection can be performed using a variety of tools and technologies, such as network packet capture and analysis tools, intrusion detection and prevention systems (IDPS), and security information and event management (SIEM) systems. These tools can be used to monitor network traffic, detect potential security threats, and alert security analysts to take appropriate action to mitigate the risks.

Overall, stream-oriented data collection is an essential component of network security, as it allows organizations to proactively identify and respond to security threats in a timely manner.

2. *Flow Based Data Collection*

Flow-based data collection in network security refers to the process of collecting and analyzing data on network traffic flows. A network flow is defined as a unidirectional sequence of packets between a source and destination IP address, using the same protocol and transport layer port number.

Flow-based data collection focuses on identifying and analyzing the patterns of traffic flows, rather than analyzing individual packets. By collecting and analyzing flow data, security analysts can gain insights into network behavior, identify potential security threats, and take appropriate measures to mitigate the risks.

Flow-based data collection can be performed using various tools and technologies, such as flow-based network monitoring tools, network flow recorders, and network flow analysis software. These tools can capture flow data from different network segments and provide insights into network performance, user behavior, and potential security threats.

Overall, flow-based data collection is an important part of network security, as it allows organizations to monitor and analyze network traffic flows in real-time and detect potential security threats. By using flow-based data collection, organizations can better protect their networks and respond quickly to security incidents.

Algorithm for datacollection in network security:

- Define the data to be collected :according to our objective we need to collect data such as network traffic data, security alerts and other data that are relevant to network security.
- Identufy sources: Identify the sources that you can collect your data from like network servers, websites ,apps which generate the data you are in need.
- Data collection method: Determine which method can be used to collect the data, the method can be determined according to the data being collected and the environment of the data.
- Data collection variables: After determining the collection tool that can be used for your data, set up data collection parameters in order to filter data to avoid errors and data redundancy.
- Storing the data: Store the data in a centralized location like a database or a data warehouse.
- Analyze the data: By using several analyzing tools the collected data can be analysed for patterns or any security threats .
- Take action: If the analyzation ends in any potential ends in any possible security threats by the use of security policies or protocols rectify the problem immediate ly.
- Maintenance: Regularly monitor and maintain the data collection inorder to ensure protection over any future threats.

***Conclusion*:**

Collection of data related to network security is essential for the detection of network attacks and intrusions. In this paper we have discussed various network data collection technologies, we have mainly reviewed the data collection nodes ,collection tools and collection mechanism with their types. We have finally concluded the paper by explaining a simple algorithm for data collection and using the data against potential security threats.