Analysis; Routing Attacks &Traffic Redirection

3-1 Traffic analysis

3-1-1 Introduction to Traffic Analysis

هذا الموضوع مهم جدا

Before the Traffic Analysis, we should know what the **Network Traffic Basics?**

Network traffic refers to the amount of data moving across a network at a given point of time. Network data is mostly encapsulated in network packets, which provide the load in the network. **The proper organizing of network traffic helps in ensuring the quality of service in a given network**. **Network traffic is also known as data traffic.**

Proper analysis of network traffic provides the organization with the following benefits:

1. Identifying network bottlenecks الاختناقات- There could be users or applications that consume high amounts of bandwidth.
2. Network security - Unusual amount of traffic in a network is a possible sign of an attack. Network traffic reports provide valuable insights افكار into preventing such attacks.
3. Network engineering - Knowing the usage levels of the network allows future requirements to be analyzed.

For more details, see the link below:

https://www.techopedia.com/definition/29917/network-traffic

Network Traffic Analysis can be defined as the process of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or general network operations and management.

Network Traffic Analysis using manual and automated techniques to review granular-level مستوى التقسيماتdetail and statistics within network traffic.

The Main purpose for traffic analysis is discover the pattern of traffic between parties.

According to (Northcutt, 2014)**, Traffic analysis is a special type of inference attack technique تقنية الهجوم المعتمدة على الاستنباط that looks at communication patterns between entities in a system (from attacker point of view).**

In traffic analysis messages are intercepting and examining in order to deduce يتم استخلاص information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

الفقرة تالية فكرية للمناقشة

The size of packets being exchanged يتم تبادلها between two hosts can also be valuable information for an attacker, even if they (attackers) aren't able to view the contents of the traffic (being encrypted or otherwise unavailable). Seeing a short flurry مضطربة of single-byte payload packets

with consistent pauses توقفات ثابتةbetween each packet might indicate an interactive session between two hosts. Large number of sustained packets مستمرةover time tend to indicate file transfers between hosts, also indicating which host is sending and which host is receiving the file. By itself, this information might not be terribly damaging تلف رهيب to the security of the network, but a creative attacker will be able to combine this information with other information to bypass intended security mechanisms.

Attackers would commonly use traffic analysis in addition to some other method of attack, **it is most useful for reconnaissance استطلاع the victim network to find vulnerable hosts or to determine characteristics of someone else's system**. However, in the case of insiders or authorized users, you have the "inference problem” مشكلة الاستدلال about data they are not authorized to access, wherein حيثauthorized users are able to make valid conclusions, based only on data they are authorized to access.

Fortunately, traffic analysis can also be used as a defensive technique by identifying anomalies شاذ in traffic patterns. Using traffic analysis, administrators can baseline الخط الاساسthe traffic to and from hosts on the network over time, in a graphical format (line charts or other graphs). As a daily routine, the administrator can review these charts and see patterns in network activity to and from hosts and networks, including packet quantity, packet sizes, bandwidth utilization, connections per hour, etc. After becoming familiar with the baseline utilization of the network, an administrator will be able to quickly spot anomalies يلاحظ الشذوذ in connections between hosts and networks such as port-scans, DoS attacks, significant increases in bandwidth

utilization, and other factors that might indicate hosts that are under attack or have become compromisedمخترق .

Typically, network traffic analysis is done through a network monitoring or network bandwidth monitoring software/application. The traffic statistics from network traffic analysis helps in:

- Understanding and evaluating the network utilization.
- Download/upload speeds.
- Type; size; origin; destination and content/data of packets.

Network security staff uses network traffic analysis to identify any malicious or suspicious packets within the traffic. Similarly, Network Administrations seek to monitor download/upload speeds, throughput الانتاجية, content, etc. to understand network operations.

Network traffic analysis is also used by attackers/intruders to analyze network traffic patterns and identify any vulnerabilities to break in or retrieve sensitive data.

3-1-2 Network Traffic Monitoring

is the process of reviewing, analyzing and managing network traffic for any abnormality process عمليات شاذة that can affect network performance, availability and/or security.

Network traffic monitoring is a network management process that uses various tools and techniques to study computer network-based communication /data /packet traffic.

The key objective behind network traffic monitoring is to ensure availability and smooth operations on a computer network.

Network monitoring incorporates network sniffing and packet capturing techniques in monitoring a network. Network traffic monitoring generally requires reviewing each incoming and outgoing packet.

Some of the technologies that incorporate network traffic monitoring include:

- Firewalls
- Intrusion detection and prevention systems
- Network monitoring, managing and performance software
- Anti-virus/Anti-malware software

3-1-3 Packet Analyzer

A packet analyzer is a computer application used to track, intercept and log network traffic that passes over a digital network. It analyzes network traffic and generates a customized report to assist organizations in managing their networks. **Packet analyzers also may be used by hackers to intrude التطفل on networks and steal information from network transmissions.**

A packet analyzer is also known as a sniffer, network analyzer or protocol analyzer. A network manager must be vigilant يقظto analyze and protect network traffic from threats and low performance. Managers should troubleshoot the network often to ensure that it provides an efficient and fast network traffic environment.

A packet analyzer shows the complete status of all network activities by providing a complete picture of bandwidth and resources utilization. If a resource is using too much bandwidth, the network

manager can release يحرر the resource by interrupting بقطع the process. However, newly deployed نشر application and network nodes may have some configuration and working issues, but these can be solved within seconds using the packet analyzer. **Every action of a packet analyzer is performed in real time**.

Q: How the attacker can use the Packet Analyzer to attack the network?

3-1-4 Building a Common Understanding of Network Security

(Timothy Shimeall, 2016) said that there are two basic approaches to building a common understanding of network security:

1) **Bottom up**, where analysts start with events of interest (possibly identified from network flow data) and then pivot ينتقل to other pieces of network information, (possibly firewall records or IDS alerts), to add context for the analysis. For example, a web service outageانقطاع (identified from network flow data by failed attempts to contact the server), the analyst may examine IDS alerts (to find attempted or successful attacks against that service) or server logs (to find other indications as to why the outage occurredحدوث الانقطاع .
2) **Top-down**, where analysts examine broad general patterns of usage within network traffic. For example, there is a common pattern of network traffic behavior known as the diurnal curve النهاري المنحني, where traffic usage in a network ramps up تصعد at the beginning of the workday at about 8:30 a.m. and continues throughout خلال the day until about 4 p.m. followed by a natural drop off هبوط at the end of the workday. This curve is offset تتغير depending on the local time.

When examining this curve, for example, analysts should look for departures from the diurnal curve, sudden interruptions, or a sudden high spike تصاعد . In the event of anomaly pattern, an analyst might then turn to other data sources to drill down for better understand the divergence الاختلافات المتشعبة. For example, an examination of firewall records might help analysts identify interruptions as blocked traffic or network connections.

No matter which approach a defender uses, network attackers are often good at hiding behaviors with respect to any single data source. For example, if network attackers have styled their attacks so that they can't be detected through antivirus software or common IDS rules, analysts must then rely on network flow analysis, changes in service behaviors, or log file entries.

Bibliography

Northcutt, S. (2014). Traffic Analysis. *Security Laboratory: Methods of Attack Series*, https://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis.

Timothy Shimeall. (2016, September 16). *CERT Network Situational Awareness*. Retrieved October 15, 2017, from https://insights.sei.cmu.edu/sei_blog/2016/09/traffic-analysis-for-network-security-two-approaches-for-going-beyond-network-flow-data.html

Q: How the Packet size can be useful for attacker in Traffic analysis?

Q: How Traffic Analysis can be useful for Network Administrator?

Q: What are the main tasks should be followed by Network Administrator? Why?