Network security monitoring essay sample

Law, Criminal Justice

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Discovering DNS

A DNS acts as a database for hosting information. Top-level domains include. com, . edu, . gov, . mil, . org, . net, and . int. These top-level domains represent different institutions and organizations in the world. Domain name servers form a critical part in understanding network security monitoring. According to Shelly and Vermaat (2010), DNS allows computers to locate each other on the internet easily. DNS utilizes both the TCP port 53 and the UDP port 53 for the DNS communications (Bejtlich, 2004). The network analyst will thus require the understanding of the concept of DNS if they are going to analyze traffic (Bejtlich, 2004). Forms of network activity to be analyzed include normal, suspicious, and malicious activity. Thus, concepts of normal traffic, suspicious traffic, and malicious traffic need to be understood (Bejtlich, 2004).

- Normal Port 53 (UDP and TCP) Traffic

- Normal traffic is what is expected to be seen in normal activity via the UDP and TCP services using port 53.

- Suspicious Port 53 (UDP and TCP) Traffic

- Suspicious traffic will involve those packets that are caused by unknown

applications and protocols. This type of traffic is very different from the normal traffic and thus the analyst classifies them as suspicious as they do not conform to the normal traffic (Bejtlich, 2004). Prior to making any conclusions regarding the suspicious traffic, the analyst needs to examine issues such as statistical data, full content, and session information.

- Malicious Port 53 Traffic

- This may involve a case of zone transfer if an authorized party causes the malicious activity. Malicious traffic is normally characterized highly intrusive activity.

- Malicious Port 53 UDP Traffic

- This can be shown using the Tunnelshell program, which an intruder uses on a client victim to access the root server (Bejtlich, 2004). Once the intruder gains access, he or she can be able to exploit the system by developing tunnels that allow the intruder to have future remote access. Applications of tools that inspect network traffic can provide evidence of tunneling. This is done by checking the traffic against the expected structure for the protocol assigned to that port. For instance, tunneling can be identified by detecting DNS requests that do not originate from the DNS servers of the enterprise (Fry and Nystrom, 2009). This is because all clients need only use the internal DNS servers. However, this becomes a challenge when the intruder has used a client through his or her verified port to access the DNS servers.

- Malicious Port 53 TCP Traffic

- In a TCP malicious traffic, the intruder sets up a three-way handshake on the victim where malformed DNS inverse queries are done (Bejtlich, 2004).

Using Ethereal, the malformed queries are reported as attacks as they do not ask any proper question.

Harnessing the Power of Session Data

- According to Fry and Nystrom (2009), session data offers valuable information via its records, which form a vital part of monitoring. The session data is responsible for reducing the millions of packets into summaries of conversations or flows (Bejtlich, 2004). NetFlow is a good tool for recording session data (Fry and Nystrom, 2009). Using session data, the analyst can be able to know if the servers are compromised, locations that the intrusion occurred, and information that may have been lost via the intrusion.

- Session Data from a Wireless segment

- Session data from a DMZ Segment

- Possible information that can be gathered from a DMZ segment session data may include the intruder trying to send ICMP echo packets to a new system. Furthermore, any successful connections that are established will also be indicated in the session data. This can be justified by the presence of high packet and byte count, which shows a very interactive access (Bejtlich, 2004). More information can be gathered from the session data and servers with issues can be identified and addressed.

- Session data from VLANs

- New IP addresses connecting to others provides information of suspicious activity in VLANs. If information is being exchanged in the same VLAN, suspicions of abnormal activity may be less. The challenge in monitoring VLANs is that sniffing takes place on the firewall interface where mostly session data is not being collected. To address this problem, sensors can be

used that monitor the firewall interface activity.

- Session Data from External Segment

- Session data collected in the external segment represents the interface that connects the local area network (LAN) to the wired Internet (Bejtlich, 2004). Based on session data from the wireless segment, DMZ and the VLANs, compromised areas in the system can easily be identified. Thus, containment measures can be used to address the problem of intrusion.

References

Bejtlich, R. (2004). The Tao of network security monitoring: beyond intrusion detection. Boston:

Addison-Wesley.

Fry, C., & Nystrom, M. (2009). Security monitoring. Sebastopol, Calif.:

O'Reilly Media, Inc.

Shelly, G. B., & Vermaat, M. E. (2010). Discovering Computers 2010: Introductory. Cengage Learning.