Cat Scan II Big Dog

Derek Mayen

Overview

The Client Cat has requires help with setting up PRTG sensors for her business and has asked us to recommend her some sensors and to describe the thresholds that would be an IoC. Through this document we will present our recommended sensors to install on the network to provide better security, and to alert of any suspected attacks that may occur. As well as explain what the thresholds will monitor and consider notable to become an alert.

Discovered Vulnerabilities & Sensors (Linux Machine)

Some vulnerabilities that were caught on the linux system were from DoS attacks. DoS or Denial of Service Attacks, are defined as a network attack that prevents legitimate use of server resources by flooding the network with requests.

One of the sensors we recommend is an Packet Sniffer Sensor as it will monitor the network for all traffic on the network And we will be able to customize the threshold for the the sensor , to help us know when there is a suspicious amount of traffic.

The Packet Sniffer Sensor monitors, among other things:

- Total traffic
- Port sniffer
- Web traffic (HTTP, HTTPS)
- Mail traffic (IMAP, POP3, SMTP)
- File transfer traffic (FTP, P2P)
- Infrastructure traffic (DHCP, DNS, ICMP, SNMP)
- Remote control (RDP, SSH, VNC)
- Other UDP and TCP traffic

Discovered Vulnerabilities & Sensors (Windows Machine)

For the Windows machine, the vulnerabilities that were caught were all exec code vulnerabilities. Exec Code or Remote Code Execution allows attackers to execute malicious code on systems and devices, regardless of their location, allowing them to insert their own back doors or ransomware or any other kind of malicious code into their target system.

Fortunately, these types of attacks are easier to make difficult on the attackers by doing some preventative measures such as updating software as soon as it comes out for example. In updating the software it helps prevent any previous vulnerabilities from being exploited further. And by monitoring the traffic with the sensor i have mentioned before, Packet Sniffer Sensor, it will be harder for any attacker to use RCE.

Work Cited

Simic, I. (2022, November 16). *【RCE attack】defintion, examples, and prevention*. Crashtest Security. https://crashtest-security.com/remote-code-execution/#:~:text=It%20is%20a%20way%20to%20remotely%20inject%20and,seize%2C%20modify%20or%20destroy%20data%2C%20install%20ransomware%2C%20etc.

Paessler AG. (2023, May 24). *Professional all-in-one packet sniffing tool*. Paessler. https://www.paessler.com/packet_sniffing?msclkid=f8509d08a64a1703599cf9b573e06880&utm_source=bing&utm_medium=cpc&utm_campaign=CAN_EN_Search-nonBrand_phrase_3&utm_term=ip+packet+sniffer&utm_content=ip-packet-sniffer

MozDevNet. (n.d.). *DoS attack - MDN web docs glossary: Definitions of web-related terms: MDN*. MDN Web Docs Glossary: Definitions of Web-related terms | MDN. https://developer.mozilla.org/en-US/docs/Glossary/DOS_attack