**Cat Box Brute Force Attack Playbook Report**

**Overview**

The Client Cat has requested help with setting up PRTG sensors for her business and has asked us to recommend 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**

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. This type of attack can cause a lot of problems for the company. DoS attacks flood the servers with false traffic with the goal of overflowing the server with requests. Sensors and Log monitoring are some effective ways of mitigation for this type of vulnerability.  
  
 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. This type of attack, although easier to prevent, if not prepared for beforehand, can have a massive impact on the company, as sensitive data could be compromised.

**Recommendations & Mitigation**

One of the sensors we recommend is a Packet Sniffer Sensor as it will monitor the network for all traffic on the networkAnd we will be able to customize the threshold for the sensor , to help us know when there is a suspicious amount of traffic. With this sensor, it will make monitoring logs and setting thresholds easier. The threshold that’d be best recommended is a threshold that validates the authenticity of the request by users, effectively ensuring that the traffic that is intended for the network is authentic.

For the windows machine, 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. Securing user accounts using password protection and 2 factor authentication is another way to make things difficult for attackers to breach the network.

**Conclusion**

In reviewing the vulnerabilities of the machines on the network, we have seen the vulnerabilities and are able to set the proper protocols and thresholds to properly prepare and mitigate the risks involved. Securing the network with the recommended sensors as well as updating the software will go a long way in protecting the data of this company.

**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