|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Decorative | | | | |
|  |  |  | |  |
| Big Dog  Risks & Vulnerabilities | | |
| Curtis Crawford | | 28 May 2024 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Decorative | | | | |
|  |  |  | |  | |
|  | Executive Summary  Big Dog is now in charge of a larger network with more systems, and along with the added responsibilities, comes a need for more protection and security. With a mixture of Windows & Linux systems, we’ll be using the PRTG monitoring system to monitor the network traffic and machines. There are specific sensors among the many that stand out and need to be watched closely. MySQL Database Query Sensors (2), for Linux & Windows, both need to be monitored for abnormal query rates with an SIL of 9. The SSH Sensor and any unusual login activity, at an SIL level of 8. Antivirus Status Sensor is a big one, as if it is disabled or outdated could cause tremendous harm, with an SIL of 9. Lastly a File Sensor, where anomalous file system changes could indicate unauthorized access; which I have assigned an SIL of 9. | |  | |

|  |  |  |
| --- | --- | --- |
|  | |  |
| DiscussionWindows Server While Windows Servers are at risk from countless types of attacks, I chose to prioritize the following as the most critical risks. DDoS: If the servers are attacked with the intention of shutting them down (DDoS), then accessibility becomes an issue. Malware: Any form of malicious software that an attacker might attempt to upload to our servers could result in, among many things, stolen or corrupted data, ransomware, and more. Linux Linux is typically a lot safer than Windows when it comes to security, but that doesn't make it invincible. If an attacker were to find a way into the system, I chose the following two risks as the most prevalent. Privilege Escalation: Let's say an attacker has basic user access but manages to escalate that to that of what Root can do, the possibilities of what that attacker can access and do are now endless. Linux is also at risk from attacks that could result in memory corruption. As Big Dog uses their Linux system to create intellectual property (IP), if that information were to become corrupted, the impact would be immense. | | |
|  |
| Windows Workstations Windows Workstations are mostly at risk of user-sided errors and social manipulation in my humble opinion. Someone downloads something they're not supposed to and now you've opened the door for an attack (unauthorized applications). If the user is allowed to surf the web, malicious websites are definitely a risk factor to be aware of. Phishing emails hoping to steal your user's information and employee's login details, the possibility of accidentally downloading Spyware, these have always been a huge threat as well. Kali Kali as a bare metal OS is actually a decent idea if you've got a good IT team that knows their command lines. The risk that comes with this of course is that Kali is known on the interwebs as the "hacker's OS". There's a lot of tools at the attackers dispense, and if the Kali machine becomes compromised while connected to the other systems via the network, we've just served the attackers dinner and desert. If the attackers have any intel on how our system works and knows that the Kali system is only used for IT, they might attempt Brute Force attacks on their passwords in an attempt to gain their privileges. With that being said, privilege escalation also comes into play as a user with IT privileges that's been compromised has the potential to escalate their privileges to that of a Root User; which could basically control the entirety of that machine and gain access to others across the network. | | |  |

|  |
| --- |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| Table of sensors | | | |
|  |  | |  |

recommendations:

## Ping Sensor

With minimal impact on your PRTG systems performance, having ping sensors would help in monitoring the health of your systems.  
  
“Hardware monitoring starts with a simple ping test. This is a simple way to check whether all servers are reachable. If the ping test fails, the server may be turned off, there may be a problem with a switch, or the error may be due to an unplugged or damaged cable. PRTG provides the [Ping sensor](https://www.paessler.com/manuals/prtg/ping_sensor) and the [Cloud Ping v2 sensor](https://www.paessler.com/manuals/prtg/cloud_ping_v2_sensor) for this purpose.” -blog.paessler.com

Disk Space Sensor

While the first thing you think of when it comes to monitoring your devices might not be disk space, this plays a huge role in the performance of your systems and depending on the circumstances, can potentially be an IoC.

“Planning for future capacity needs can be challenging. Monitoring disk space with PRTG gives you a single, easy-to-understand overview to help you stop unexpected resource shortages, locate “zombie” processes, and reduce overprovisioning instances. Monitoring can also show you which applications and processes use the most disk space, so you can make more informed resource allocation decisions.” -paessler.com

FTP Sensor

Monitoring your File Transfer Protocol is a good idea because it not only is it something you want to be working for your users, unexpected errors and problems could be an indicator of compromise.

“The FTP sensor monitors file servers via the File Transfer Protocol (FTP) and FTP over SSL (FTPS).” -paessler.com

References:

<https://blog.paessler.com/top-sensors-in-prtg-to-monitor-your-dell-hpe-and-ibm-server-hardware>

https://www.paessler.com/disk\_space\_monitor

https://www.solarwinds.com/server-application-monitor/use-cases/ftp-monitoring

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

<https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=A%20brute%20force%20attack%20is,and%20organizations%27%20systems%20and%20networks>.

<https://www.itforce.ca/blog/common-it-security-risks-how-to-counter-them-2022>  
  
<https://www.reddit.com/r/hacking/comments/v1mz1n/security_risks_of_using_kali_linux_on_baremetal/>  
  
<https://tuxcare.com/blog/memory-corruption-vulnerabilities-in-the-linux-kernel/>

Video Report:  
  
https://www.mediafire.com/file/8jc3loh2qhsj69l/Recording\_2024-05-28\_182838.mp4/file