Cat Scan II Big Dog

By Robert Ajegbo

Executive Summary

Cat has been tasked with creating a monitoring system for the Big Dog organization. Big Dog has a network consisting of a Windows Server, Windows systems, Linux systems and Kali systems.

- The Windows Server acts as a file server for the company and it has PRTG on it. It also runs an SQL database as well as a website on IIS.
- The Linux systems are used by developers to create essential intellectual property for the company
- The Windows systems are used for all sales, marketing and management functions
- The Kali systems include Test and IT systems

- This report will explain some of the top risks and vulnerabilities found for the assets of the organization. I will also demonstrate recommended indicators of compromise (IoCs) to monitor for and also recommend some industry practices to better secure the Big Dog company.

Windows 2016 Server Vulnerabilities

CVE-2018-8136 (Windows Remote Code Execution Vulnerability)

- Risk: Successful attacker could execute arbitrary code with elevated permissions on a target system
- CVSS Base Score: 7.8 (High)
- Potential high impact on confidentiality, integrity and availability
- Mitigation: Install security update to correct how Windows handles objects in memory

CVE-2018-8142 (Windows Security Feature Bypass Vulnerability)

- Risk: Successful attacker could bypass security features and load improperly signed drivers into the kernel
- CVSS Base Score: 5.3 (Medium)
- Potential low impact on confidentiality, integrity and availability
- Mitigation: Install update that corrects how Windows validates kernel driver signatures

Ubuntu 20.04.6 (Linux) Vulnerabilities

CVE-2022-45919

- Risk: Successful exploitation could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service
- CVSS Base Score: 7.0 (High)
- Potential high impact on confidentiality, integrity and availability
- Mitigation: Updated software versions and fixes

CVE-2022-0812

- Risk: Allows attacker with normal user privileges to leak kernel information
- CVSS Base Score: 4.3 (Medium)
- Potential low impact on Confidentiality. No impact on integrity or availability
- Mitigation: Updated software and fixes

MS Windows 10 1507 Vulnerabilities

CVE-2023-35328 (Windows Transaction Manager Elevation of Privilege Vulnerability)

- Risk: Successful attacker could gain SYSTEM privileges
- CVSS Base Score: 7.8 (High)
- Potential high impact on confidentiality, integrity and availability
- Mitigation: Install latest security updates for OS

Table of Devices

Device	Vulnerability	Sensors	Threshold	SIL	Notes
Windows Server	CVE-2018-8136 CVE-2018-8142	• Ping • Memory usage	• Warning at 200ms and error at 500ms • Warning at 80% and error at 90%	• High	Monitor for abnormal network traffic and/or high memory usage
Linux Systems	CVE-2022-45919 CVE-2022-0812	• SNMP Disk usage • SNMP Memory usage	• Warning at 80% and error at 90% for each sensor	• High	Monitor for abnormal usage of Linux system components
Windows 10 Systems	CVE-2023-35328	• Network Traffic	• Set threshold based on network baseline (‘normal’ behaviour)	• High	Abnormal network traffic (Potential reconnaissance attempts and more)

Recommendations

Due to the high value of the organization, it is essential that further measures are taken

- Ensure that all devices are regularly maintained and updated with latest software and security updates
- Educate the various users (employees) of the importance of securing their data (use of strong passwords, multi-factor authentication, etc.)
- Establish a network baseline (‘normal’ network behaviour). This is essential to understand when there is potentially something strange occurring. Also helps to setup effective thresholds for sensors in PRTG
- Ensure that that all monitor data is backed up to an independent data center in case of emergencies (Network goes down or slows down)
- Monitor for abnormal logins and use of admin privileges (More often than not, there should not be anyone using their privileges outside ‘normal’ working hours)

References

‘. (2018, May 8). ' - Wiktionary. Retrieved July 13, 2023, from https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8136

CVE-2023-35328. (2023, July 11). MSRC portal. Retrieved July 17, 2023, from https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35328

CVE - Search CVE List. (n.d.). CVE. Retrieved July 11, 2023, from https://cve.mitre.org/cve/search_cve_list.html

Mohanakrishnan, R. (2022, February 3). *Top 10 Best Practices for Network Monitoring in 2022*. Spiceworks. Retrieved July 15, 2023, from https://www.spiceworks.com/tech/networking/articles/network-monitoring-best-practices/

November 2022 Linux Kernel 6.0.10 Vulnerabilities in NetApp Products. (2023, January 13). NetApp Product Security. Retrieved July 13, 2023, from https://security.netapp.com/advisory/ntap-20230113-0008/

NVD - Search and Statistics. (n.d.). NVD. Retrieved July 11, 2023, from https://nvd.nist.gov/vuln/search

Cat Scan II Big Dog

By Robert Ajegbo