Project: Project2/Week3/Day1

Submitted by: Navneet kaur

Title: Cat Scan II Big Dog

Executive summary: To help Cat's project Cat Scan II Big Dog project, first we make the list of all assets owned by the Big Dog organization. The list of assets includes 2 windows computers and Tablet which work as endpoints for the services like sales, marketing, Single window server on which Network monitoring tool PRTG is installed that monitors the whole network infrastructure and also SQL database runs on Server, Linux machines are used to develop important intellectual property for the company. I have used sensors like ping to check the communication in the network, SQL sensor to monitor the database, HTTPS to monitor the websites of organization, CPU performance and Runtime sensors and also set alerts for execution time to monitor the threshold of the device. In this scenario, SIL depends on MySQL database on server, firewall/antiviruses on endpoints and security on Host kali Linux machine because it has also a SQL database that needs to be watched.

Discussion: Cat is in charge of securing a business that uses a mix of Windows-based systems, servers, Windows 10 Workstations, and one Linux system. As she has other duties in the company, she has chosen to use a central monitoring system on the server, PAESSLER's PRTG. The system has been installed, and the systems that need to be monitored have been added to it. Her next step is to make sure that the appropriate sensors have been added to the systems for monitoring key items and that proper thresholds have been set for alerts. As one of the systems is a server, she wants to focus most of her attention there, but also remembering that the Windows Workstation and Linux system are used for development, and the Windows Server system has an SQL database that needs to be watched. The company has developers that work on Linux systems and these developers create important intellectual property (IP) for the company. All sales, marketing, and management functions in the company are performed on Windows systems. Test systems and IT systems (Kali 1 and 2) are also set up by IT.

Vulenerabilities:

Windows server: An Elevation of Privilege vulnerability exists when Diagnostics Hub Standard Collector allows file creation in arbitrary locations, aka "Diagnostic Hub Standard Collector Elevation Of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Microsoft Visual Studio, Windows 10 Servers.

CVE: CVE-2018-0952

Windows 10: Windows Print Spooler Elevation of Privilege Vulnerability

CVE-2022-30226

Linux: On Kali linux, all ports are closed it means no incoming connections are allowed, except for essential service such as SSH for remote access. Still some vulnerabilities like Misconfiguration, insider threats, social engineering attack.

Table of devices:

Devices	Sensor	Threshold	IoC	SIL	Attacks	Notes
Linux	**MySql**	**Checks execution time set 800 warning 900 max msec**	**Can be used to determine if service is suffering from a higher than normal load**	**low**	Test Logins or Brute Force Attempts, Creation of New Accounts, Unexpected Changes in System Configurations	**No ports open, less vulnerable**
Windows Server	**MySQL**	**Checks execution time set 800 warning 900 max msec**	**Immediate notifications when predefined threshold or events occur. This can include alerts for high resources usage, failed login or unusual activities related to MySQL.**	**7.8 High**	Unusual DNS Requests, Swells in Database Read/Write Volumes, Unusual System or Service Crashes	**5 open ports which are vulnerable**
Windows1	**Ping,** **HTTP**	**Max: 1919msec and min: 1 msec** **Downtime 75%**	**When no. of pings dropped on system** **Unable to load particular website in sensor**	**3.2 medium**	Unexpected Network Traffic Patterns, Reconnaissance Activity ,Spear-Phishing Attempts	Stopping and disabling the Print Spooler service disables the ability to print both locally and remotely.

Recommendation section:

For windows server:

http://www.securityfocus.com/bid/105048
http://www.securitytracker.com/id/1041466
https://www.exploit-db.com/exploits/45244/

Linux: to enhance the security of a linux, consider implementing other security measure:

1. Regularly applying updates and patches.
2. Employing a robust firewall solution to filter network traffic.
3. Utilizing IDS/IPS
4. Enforcing strong password policies and MFA.

Windows 10:

1. Keep OS up-to-date
2. Regular data backup
3. Monitor log activities
4. Secure web browsing.

References:

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows%2Bserver%2B1016%2Bstandard
https://geekflare.com/nmap-vulnerability-scan/
https://nira.com/nmap-vulnerability-scanning/
https://www.cvedetails.com/cve/CVE-2022-30226/
https://www.cvedetails.com/vulnerability-list/vendor_id-16215/BD.html

PPT link
https://docs.google.com/presentation/d/17NYGZ5bdC7Px919OPSjWboCvjmLuBJDl/edit#slide=id.p2