Cat Scan II Big Dog

Executive Summary

The company *Big Dog* has asked us to assess the risks and vulnerabilities that their assets are exposed to, as well as purpose any mitigation methods and sensors to help protect their valued assets. The assets that were presented to us were as follows listed from most important to least:

- Privacy (P)
- Proprietary (IP)
- Financial(F)
- Financial/Accounting(F)
- Security Management(SM)
- Systems(S)

With certain devices having access and housing certain important data, it is important to protect these assets from exploitable vulnerabilities by using sensors such as EXE/Script Sensor, HTTP Advanced Sensor, SSH Script Sensor, Windows Update Status (Powershell) Sensor, HTTP Advanced Sensor, to manage each system and protect them from possible attackers.

Overview

In order to obtain the information used to assess the risks and vulnerabilities of each device on the network, we first need to run an operations system scan on the network using a tool called zenmap, so that we can search for vulnerabilities dealing with the particular operating system associated with those devices. Doing this will provide insight on the types of attacks that could be faced for each device and will allow us to take the appropriate mitigation process to help secure all of the company's valuable assets. The following data is what i have gathered in accordance with the operating system scan for each device:

Device	Operating System
Linux	Linux 4.15 - 5.6
Windows systems	Windows 10 1507 - 1607
Windows server	Windows server 2016 build 10586 - 14393
kali	unknown

The scan provided us with the above results. Using an online tool called *NVD* (National Vulnerability Database), we can look up their CVE numbers (Common Vulnerabilities and Exposures). These CVE numbers will provide us with potential vulnerabilities to look at and to score them based on the priorities of *Big Dog's* assets.

Vulnerabilities

Windows housing multiple assets that are important to this company. The windows workstations house all the financial data(F) and security management(SM) which fall into the umbrella of privacy for *Big Dog* and its users. Therefore we will take a look at those systems first and what vulnerabilities they may contain. From the table in the Overview section, we can see that the windows systems are currently running the Windows 10 1507-1607 version. This version of windows is highly susceptible to remote execution code vulnerabilities, which essentially means that through and open or unprotected ports such as port 139 which is open on one of the windows machines systems. Attackers are able to use customized code to breach open ports on a machine which gain them access to anything on the system they want. For example, port 139 is in charge of messages between the machine and a server which are left unprotected, which anyone could access and exploit. But there are multiple examples of different ways that remote code execution can be used to exploit different devices on a network, so we will be taking a look at 3 for these windows systems.

Scripting Engine Memory Corruption is a type of remote code execution that allows the attacker to infiltrate a system's memory data and corrupt it as much as they'd like. Using the online resource NVD (National Vulnerability Database) and seeing the CVE numbers(Common Vulnerability and Exposures) we can see how critical this vulnerability is to *Big Dog* using CVSS (Common Vulnerability Scoring System). Inserting the required fields and how they would affect the confidentiality, integrity, and availability of systems on our own machine we get a base score of 8.3. Which means that if left monitored or mitigated this could pose a threat to *Big Dog* and its assets. The aforementioned categorized lists will all affect the privacy of the users, the financial data as well as the management systems that are stored on the windows systems, leading to the high score of 8.3.

The next vulnerability we will look at on the windows systems is Windows Storage Services Elevation of Privilege, which means that when a system does not properly monitor their file operations, for example authentication logs, then an attacker can gain access to a device on the system and use that to gain more privileges such as the admin privileges located on the windows devices in *Big Dog*'s network. Once again using the CVSS calculator we get a base score of 7.8. This vulnerability is ranked lower than the previous because of the circumstances needed to execute this type of attack, as the attacker needs to use a bit more complex coding and requires some sort of pre established privilege to access the machine. This vulnerability also affects the windows server as well.

The final vulnerability we will look at for the windows systems are windows security feature bypassing. This vulnerability will allow attackers to bypass security measures by impersonating the main component of the operating system or the “Kernel”, allowing them access to all the data on the machine. Using the CVSS calculator again, we can see that our score for thai vulnerability is an 8.8, once again compromising all three categories of confidentiality, integrity, and availability.

Linux being another device on the network that is a development tool for *Big Dog*’s Intellectual Property (IP) is a device that should be another priority for securing second as it does house one of the more important assets to the company but it does not house as many combined priorities as the windows systems. Although it isn’t the main priority for securing, it is still important to discuss the vulnerabilities as it is still an important part of the network to protect. The vulnerability that affects the Linux device is called an integer-overflow vulnerability. Which means that when malicious attackers allow local users to access a small database that can’t contain them to grant them all privileges linux users can have; including administrative privileges. Once again using the CVSS calculator we can see how it would affect *Big Dog*’s functionality of the device and the data it holds. The CVSS calculator shows a score of 8.8 for the risks it poses.

Finally, we come to the Kali machine. As we can see from the table provided in the above section, doing an operating system scan did not uncover the Kali Linux machine's exact operating system version. Kali Linux is a type of operating system that is hard to do an outside scan of its operating system because of the security measures that Kali has to mitigate attacks and vulnerabilities such as the ones above resulting in the case where we are unable to use the CVSS calculator to do any meaningful analysis of any vulnerabilities. That being said we can still take measures to ensure even more security for the device which will be discussed in the next two sections.

Table of Devices

This section will be dedicated to providing the recommended sensors for each device, The recommended Thresholds, the IoC's (Indicators of Compromise), and the SIL's (Safety Integrity Levels) for each device on the network.

Devices	Sensors	Thresholds	SIL's	IoC's
Windows 1&2	EXE/Script Sensor	N/A	Level 3	Incorrect Value of memory stability

Windows 1&2	HTTP Advanced Sensor	2(warning)
		3(error)
			Level 3	Too many failed authentication attempts

Linux	SSH Script Sensor	80% of disk space used up (warning) 90% of disk space used up (error)	Level 3	Unusual disk space usage
WinServer	Windows Update Status (Powershell) Sensor	N/A	Level 3	Latest Updates Not Being added

Kali	HTTP Advanced Sensor	2(warning)
		3(error)
			Level 3	Too Many failed authentication attempts

One of the sensors we recommend using for the Windows systems is the EXE/Script Sensor as it will help us monitor the integrity of the memory on the system using a custom script for the probe to test the stability and status of the data. Using the custom scripting we can set numerical or physical updates on whether or not data files, or any other important segments of memory are corrupted or have full integrity. HTTP Advanced Sensor for PRTG is another sensor for the Windows device we recommend using because it will allow us to monitor the amount of times users have failed their authentication. The thresholds above are an example of some thresholds to put as a warning and an error/ lockdown, of an account if the user's account has failed authentication 2 times for a warning and 3 times to lock the user out of the account. The Windows Server can be monitored more for updates as most of its critical vulnerabilities have patches to them from updates of a more current build of windows.

SSH Script Sensor is the sensor we recommend for the linux machine. Secure Shell Protocol or (SSH) Script sensor monitors the amount of data usage in the devices hard drives and memory. The vulnerability we are monitoring deals with when the attacker moves user data to a smaller database than they can handle, so this sensor will monitor all the disk usage and if it approaches 80% the sensor will send a warning and 90% for error messages. Putting the eros messages before 100% allows time for preventative measures before the damage cant be reversible.

Kali being a more secure system that is usually meant for network security in general, it requires that the sensitive data that it carries is protected and monitored to a degree as well. So we are recommending another authentication type sensor, HTTP Advanced Sensor, in order to monitor the same things as the windows systems. To ensure that the authorized users are the ones using the devices in charge of security for the network.

Recommendations & Industry Best Practices

The recommendations for all the windows systems including the windows server is to regularly apply security updates and patches to fix known vulnerabilities, using the “Principle of Least Privilege” which is essentially ensuring that all users have only the permission necessary to perform the assigned tasks, Enforcing Strong Authentication methods such as MFA (Multi-factor authentication) and password expiration, Monitoring auditing systems and event logs for any suspicious activity amongst the devices, and finally, isolating potentially malicious or untrusted code or processes, to ensure the security of the unaffected data. Enacting all these mitigation responses are not only recommended but also industry best practices for securing the windows systems.

Recommendations for Linux systems for the integer-overflow vulnerability are as follows. Using the technique “Data Execution Prevention” which prevents certain memory sectors of the linux device from being activated, meaning that it won’t be as easy to overflow databases with access to memory. Monitoring the data usage and the data type and looking for when any operation in a system is about to exceed the recommended threshold, will ensure that if there are any IoC’s related to data usage or even accidental over use of data will be managed. FInally updating Linux OS and installing patches as it will help prevent easier access to databases.

Conclusion

To conclude this report, using the investigative tools such as zenmap to investigate vulnerabilities on the network, using auxiliary and supportive tools such as the NVD database and CVSS calculators to assess the risk of the vulnerabilities and how they can be exploited, and finally enacting the mitigation and monitoring utensils; *Big Dog* will have a more secure network and the ability to monitor for Indicators of Compromise and possible attacks on the network.

Work CIted

You are viewing this page in an unauthorized frame window. NVD. (n.d.). https://nvd.nist.gov/vuln/detail/CVE-2018-0983

Microsoft CVE-2020-1057: Scripting engine memory corruption vulnerability. Rapid7. (n.d.). https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1057/

Common vulnerability scoring system version 3.1 calculator. FIRST. (n.d.). https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

You are viewing this page in an unauthorized frame window. NVD. (n.d.-a). https://nvd.nist.gov/vuln/detail/CVE-2018-0983

Microsoft CVE-2017-0213: Windows com elevation of privilege vulnerability. Rapid7. (n.d.-a). https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0213/

You are viewing this page in an unauthorized frame window. NVD. (n.d.-a). https://nvd.nist.gov/vuln/detail/CVE-2018-0902

Karedia, R. (2021, March 3). *What is the security feature bypass vulnerability & update affecting Windows customers worldwide?*. Checkmate. https://niiconsulting.com/checkmate/2021/03/what-is-the-security-feature-bypass-vulnerability-update-affecting-windows-customers-worldwide/

You are viewing this page in an unauthorized frame window. NVD. (n.d.-a). https://nvd.nist.gov/vuln/detail/CVE-2018-8781

What is is integer overflow and underflow?. Infosec. (n.d.). https://resources.infosecinstitute.com/topics/secure-coding/what-is-is-integer-overflow-and-underflow/

PRTG Manual: EXE/Script Sensor. Paessler. (n.d.). https://www.paessler.com/manuals/prtg/exe_script_sensor

PRTG Manual: Windows Updates Status (PowerShell) sensor. Paessler. (n.d.-b). https://www.paessler.com/manuals/prtg/windows_update_info_sensor

PRTG Manual: SSH script sensor. Paessler. (n.d.-b). https://www.paessler.com/manuals/prtg/ssh_script_sensor

PRTG Manual: HTTP advanced sensor. Paessler. (n.d.-b). https://www.paessler.com/manuals/prtg/http_advanced_sensor#:~:text=PRTG%20Manual%3A%20HTTP%20Advanced%20Sensor%20%20%20,priority%20for%20the%20sensor.%20This%20s%20...%20

Xu, L., Xu, M., Li, F., & Huo, W. (2020, September 8). *Elaid: Detecting integer-overflow-to-buffer-overflow vulnerabilities by light-weight and accurate static analysis - cybersecurity*. SpringerOpen. https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00058-2#:~:text=Integer%20overflow%20is%20one%20of%20the,it%20must%20be%20a%20real%20vulnerability.&text=Integer%20overflow%20is%20one,be%20a%20real%20vulnerability.&text=is%20one%20of%20the,it%20must%20be%20a