Penetration testing mini- report

summary

This test is about trying to exploit any ports that are open to vulnerabilities, and can easily be exploited by a hacker. This is a report on Vsftpd ver 2.3.4 which was one of the ports that was open and prone to exploitation. In this case, I tested metasploitable 2 to check if there are any vulnerabilities using Kali linux. Vsftpd is an ftp server program. File Transfer Protocol (FTP)is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server.

Vulnerabilities

Version 2.3.4 of vsftpd contained a backdoor that was slipped into the servers hosting the source code by an unknown person. The particular version of vsftpd included on the Metasploitable virtual machine contains a vulnerability that opens a backdoor shell. A backdoor shell is malicious software uploaded to a website without the knowledge of the website owner, allowing a hacker to remotely control functions of an infected site. In this case, it allows the user to obtain a root shell, view the contents of the files, modify things, and many more by attempting to login with a username ending with a :).

Potential impact of that vulnerability

Backdoors are very hard to weed out. Traditionally, detection involves using software scanners to search for known malware signatures in a server file system. This process is error prone, however. Backdoor shell files are almost always masked through the use of alias names, and in some cases, hidden through multiple layers of encryption. This kind of vulnerability can open doors to Data theft, website defacing, server hijacking, launching DDOS attacks, infecting website visitors, and many more. Even if a backdoor is detected, typical methods to reduce the severity of the issue (or even a system reinstallation) are unlikely to remove it from an application. This is particularly true for backdoors having a persistent presence in rewritable memory.

solution

To prevent backdoor attacks, you should install a powerful antivirus with top-notch malware detection and prevention capabilities, a firewall, and a network monitoring tool. Many backdoors are installed through RATs, Trojans, and other types of malware, so it is essential to install an antivirus tool capable of detecting such threats. The antivirus should also have a firewall and network monitoring as a part of the security suite.

conclusion

Considering the possibility of data theft, file seizure, and access backdoor controls, if a company has similar vulnerabilities as that of vsftpd v. 2.3.4. It is important to install firewalls for detecting such risks and antivirus for preventing backdoor attacks. It is also a good idea to reevaluate the risk assessments of the company to cater more towards acting against such attacks. That concludes the report on the vsftpd v2.3.4 port vulnerability.

References

https://www.imperva.com/learn/application-security/backdoor-shell-attack/

https://charlesreid1.com/wiki/Metasploitable/VSFTP

https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/