Bilaal Williams

Executive Summary

In this vulnerability test we planted a malicious file on a website. Once downloaded this gave us access to the victim’s PC. This exploit requires the user to both download and open the file. Attackers accomplish these types of attacks using social engineering. There are many methods that an attacker may use to trick the victim into downloading the file. For instance, the file can be sent via email, or planted in a fictitious website designed by the attacker.

Mitigation

The first line of defense is the user. The user must be made aware of these types of attacks so they remain cautious about what types of websites they visit and what they choose to download. Company policy should explicitly state rules on downloading and a warning should be issued to the user each time they attempt to download files on the Internet. Some browsers such as Chrome block files that have payloads similar to the type used in this attack, but when the payload was appended to a legitimate file like putty, the warning was bypassed. This is why it is important to educate the user about malicious downloads and not simply rely on browser security and system rules.

In this attack, the remote shell only obtained privileges of the user who downloaded the file. It is important that privileges be limited on systems to only what is needed for each user. Although there are methods used by attackers to escalate privileges, it is important to make it as difficult as possible for an attacker to gain far-reaching access on the system.

System monitoring can identify a compromised PC, but it is extremely difficult to track if the client has many connections to remote hosts. Port monitoring can help to mitigate, and firewall rules should allow only specific ports to be opened.