Cristobal Escobar

CPTS 327

Final Report

December 14, 2024

**Title:** Exploiting vulnerabilities in Windows XP

**Status:** Completed

**In previous Milestone:**

During the first milestone I set up my VMs, Kali and Windows XP, I connected both environments and then I started looking for vulnerabilities using nmap. Some of these vulnerabilities include Microsoft RPC, Microsoft Windows netbios-ssn and Windows XP microsoft-ds.

**Second Milestone:**

For milestone 2, I play around with Wireshark trying to learn how to use it, I learned a bit about how to monitor network between my Kali Linux and my Windows XP, in this part I was able to see all packages and protocols send and receive between both VMs. Then I started looking for vulnerabilities using nmap some of my findings were NetAPI, EternalBlue, VNC Injection and Add User (these can be found in nmap\_results.txt). Then I started looking for payloads to exploit the found vulnerabilities some of them include payloads for NetAPI and Eternal blue, I tried sending them, but I wasn’t able to get anything. I spent time trying to figure out the reasons, I tried disabling Firewall and other security settings in my Windows XP, but I wasn’t able to make more progress.

**Last Milestone:**

In this milestone, I did some research on what the reasons were why the payloads crashed all the time, I found that for EternalBlue I wasn’t setting the payload correctly, and for NetAPI I couldn’t find anything, I tried adjusting the payloads differently, but it still didn’t work. Using EternalBlue I successfully established a meterpreter session which granted me access to a bunch of Windows XP documents (.doc, xls. txt, etc). I was able to get into the administrator file and download all the files (saved in folder AdminFiles), I tried looking for passwords files, but I couldn’t find anything. Also, I was able to get some hashes after using metasploit post modulo hashdump, I saved the hashes (hashes.txt) and run John the Riper, after trying different things I successfully crack a password (can be seen in one of the screenshots).