Course: Hands-on Exploit Development

Module 3: Multi-staged exploits

Title: Assignment 3

Objective: Create a working exploit for Integard Pro 2.2.0.9026

- Develop this exploit for Windows 10 (x64)
- Use the existing exploit to understand where the vulnerability exists
- Using a bind tcp shell or reverse tcp shell payloads.
- Create a write-up or a short video explaining your methodology step by step.
- Send the link to write-up or video on csc@yaksas.in with the subject 'Assignment Submission: Integard Pro 2.2.0.9026

Tools required for this assignment

- Virtualization software (VirtualBox or VMWare)
- Linux
  - Kali Linux 2021.1 (VM)
  - Python 2.7
  - msf-pattern_create
  - msf-pattern_offset
  - msf-nasm_shell
  - Sublime Text or Notepad ++

- Windows
  - Target software -> Integard Pro 2.2.0.9026 | Download link: https://www.exploit-db.com/apps/adb9fb19c8cfe459d41cec7bd60456ed-IntegardSetup.exe
  - BurpSuite Community Edition
  - FoxyProxy Standard browser plugin
  - Firefox
  - Python 2.7
  - Immunity Debugger
  - Mona.py
  - Text Editor

Questions

- Where does the vulnerability lie and how to exploit it?
- How do you bypass the process of finding bad chars for this exploit?
- Which encoder did you use to encode the payload shellcode?