Exploiting Simple Buffer Overflows on Win32

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

Bad Characters

Bad Characters

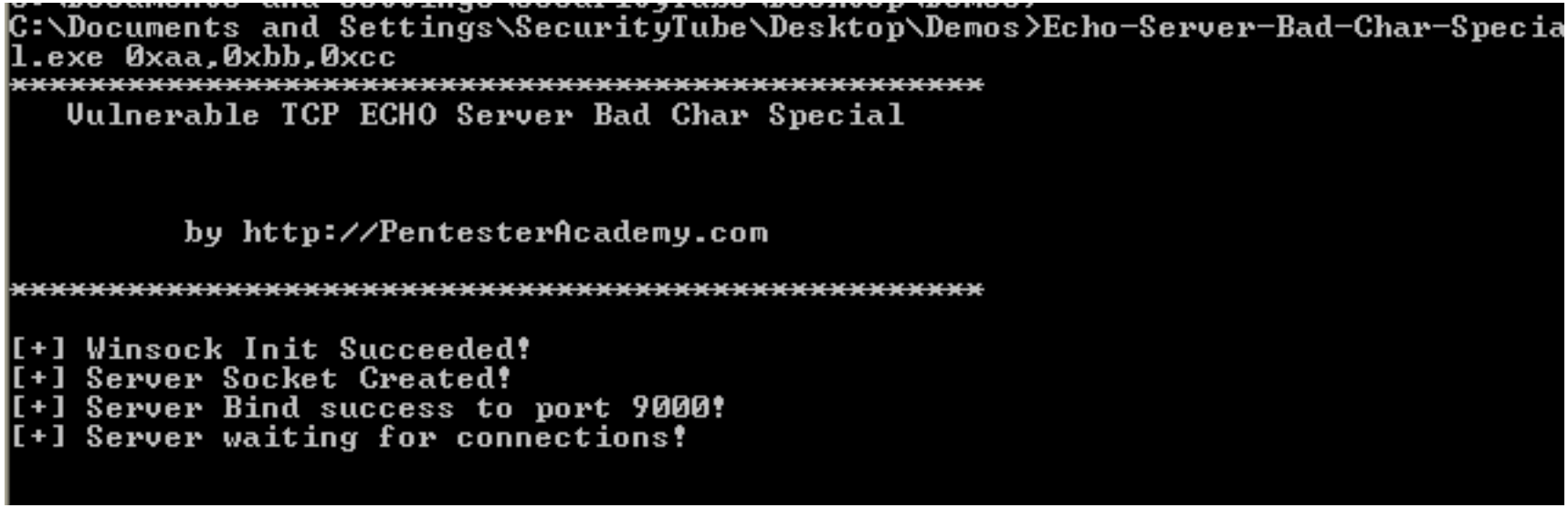
- Input sent to the program is filtered
- Input Delimiters
  - e.g. 0x00 for a string
  - e.g. 0x0a 0x0d for HTTP Header fields
- Will be Application and Developer Logic Specific

Why should this bother us?

- If our shellcode contains a bad character(s) then it will break the exploit

- How common are bad characters? VERY!!!

Generic Bad Character Program



Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

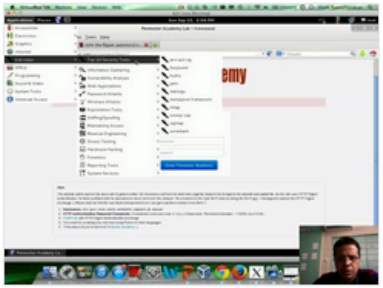
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

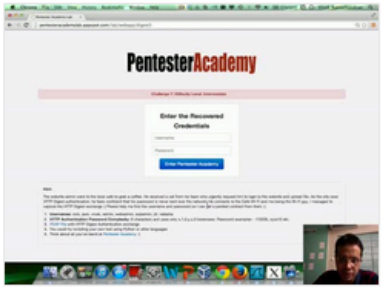
Start Learning Today!

Latest Videos

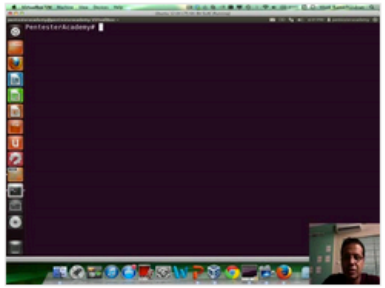
New content added weekly!



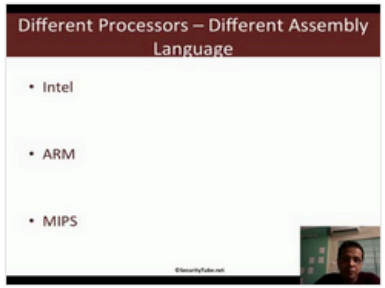
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux