Writing a Simple Fuzzer a11y.text Writing a Simple Fuzzer What is a Fuzzer? a11y.text What is a Fuzzer? A Fuzzer is a tool used by security professionals to provide invalid and unexpected data to the inputs of a program. A typical Fuzzer tests an application for buffer overflow , invalid format strings, directory traversal attacks, command execution vulnerabilities, SQL Injection, XSS, and more. Because the Metasploit Framework provides a very complete set of libraries to security professionals for many network protocols and data manipulations, it is a good candidate for quick development of a simple fuzzer. Metasploitâ€™sÂ Rex Library a11y.text Metasploitâ€™sÂ Rex Library The Rex::Text module provides lots of handy methods for dealing with text like: Buffer conversion Encoding (html, url, etc) Checksumming Random string generation The last point is extremely helpful in writing a simple fuzzer. This will help you writing fuzzer tools such as a simple URL Fuzzer or full Network Fuzzer. For more information about Rex, please refer to the Rex API documentation . Here are some of the functions that you can find in Rex::TextÂ : root@kali : ~ # grep "def self.rand" /usr/share/metasploit-framework/lib/rex/text.rb def self.rand_char(bad, chars = AllChars)

def self.rand_base(len, bad, *foo)

def self.rand_text(len, bad='', chars = AllChars)

def self.rand_text_alpha(len, bad='')

def self.rand_text_alpha_lower(len, bad='')

def self.rand_text_alpha_upper(len, bad='')

def self.rand_text_alphanumeric(len, bad='')

def self.rand_text_numeric(len, bad='')

def self.rand_text_english(len, bad='')

def self.rand_text_highascii(len, bad='')

def self.randomize_space(str)

def self.rand_hostname

def self.rand_state() Next Simple TFTP Fuzzer Prev Nessus via MSFconsole