Exploit Mixins a11y.text Exploit Mixins Working with Exploit Mixins a11y.text Working with Exploit Mixins Exploit::Remote::Tcp a11y.text Exploit::Remote::Tcp Code: lib/msf/core/exploit/tcp.rb Provides TCP options and methods. Defines RHOST, RPORT, ConnectTimeout Provides connect() , disconnect() Creates self.sock as the global socket Offers SSL, Proxies, CPORT, CHOST Evasion via small segment sends Exposes user options as methods â€“ rhost() rport() ssl() Exploit::Remote::DCERPC a11y.text Exploit::Remote::DCERPC Code: lib/msf/core/exploit/dcerpc.rb Inherits from the TCP mixin and has the following methods and options: dcerpc_handle() dcerpc_bind() dcerpc_call() Supports IPS evasion methods with multi-context BIND requests and fragmented DCERPC calls Exploit::Remote::SMB a11y.text Exploit::Remote::SMB Code: lib/msf/core/exploit/smb.rb Inherits from the TCP mixin and provides the following methods and options: smb_login() smb_create() smb_peer_os() Provides the Options of SMBUser, SMBPass, and SMBDomain Exposes IPS evasion methods such as: SMB::pipe_evasion, SMB::pad_data_level, SMB::file_data_level Exploit::Remote::BruteTargets a11y.text Exploit::Remote::BruteTargets There are 2 source files of interest. Code: lib/msf/core/exploit/brutetargets.rb Overloads the exploit() method.â€™ Calls exploit_target(target) for each Target Handy for easy target iteration Code: lib/msf/core/exploit/brute.rb Overloads the exploit method. Calls brute_exploit() for each stepping Easily brute force and address range Metasploit Mixins a11y.text Metasploit Mixins The mixins listed above are just the tip of the iceberg as there are many more at your disposal when creating exploits. Some of the more interesting ones are: Capture â€“ sniff network packets Lorcon â€“ send raw WiFi frames MSSQL â€“ talk to Microsoft SQL servers KernelMode â€“ exploit kernel bugs SEH â€“ structured exception handling NDMP â€“ the network backup protocol EggHunter â€“ memory search FTP â€“ talk to FTP servers FTPServer â€“ create FTP servers Next Exploit Targets Prev Exploit Format