Exploit Development Goals a11y.text Exploit Development Goals Exploit Development | Metasploit Unleashed Exploit Development Goals Examples a11y.text Exploit Development Goals Examples When writing exploits to be used in the Metasploit Framework, your developmentÂ goals should be minimalist . Offload as much work as possible to the Metasploit Framework. Make use of, and rely on, the Rex protocol libraries . Make heavy use of the available mixins and plugins . Just as important as aÂ minimalistÂ design, exploits should (must) be reliable . Any BadChars declared must be 100% accurate. Ensure that Payload->Space is the maximum reliable value. The little details in exploit development matter the most. Exploits should make use of randomness whenever possible. Randomization assists with IDS , IPS , and Anti-VirusÂ evasion and also serves as an excellent reliability test. When generating padding, use Rex::Text.rand_text_* (rand_text_alpha, rand_text_alphanumeric, etc). Randomize all payloads by using encoders. If possible, randomize the encoder stub. Randomize nops too. Just as important as functionality, exploits should be readable as well. All Metasploit modules have a consistent structure with hard-tab indents. Fancy code is harder to maintain, anyway. Mixins provide consistent option names across the Framework. Lastly, exploits should be useful . Proof of concepts should be written as Auxiliary DoS modules, not as exploits . The final exploit reliability must be high. Target lists should be inclusive. To summarize ourÂ Exploit Development Goals we should create minimalistic , reliable code that is not only readable , but also useful in real world penetration testing scenarios. Next Exploit Format Prev Exploit Development