Hadarics Kálmán, Dr. Leitold Ferenc: Szoftver sérülékenységek vizsgálata Metasploit keretrendszer felhasználásával

Az élet minden területén informatikai, info-kommunikációs eszközök vesznek körül bennünket. Ezek megfelelő működése elképzelhetetlen operációs rendszerek és különféle rendszerprogramok nélkül. Az utóbbi években jelentős átalakulásokat figyelhettünk meg a szoftverek fejlődésében, és a bennük talált biztonsági hibák jellegében. A szoftvergyártók is rájöttek, hogy nem elég egy adott szituációban megfelelően működő szoftvert készíteni, hanem már a tervezési fázisban komoly hangsúlyt kell fektetni, a majdani termék biztonságára. A Metasploit keretrendszer lehetőséget biztosít szoftverek biztonsági tesztelésére, a pillanatnyi szoftver és konfigurációs állapot figyelembe vételével. A keretrendszer teljes mértékben testre szabható, kiválóan használható tűzfal és egyéb biztonsági szoftverek védelmének vizsgálatára is.
Jelen cikkemben megvizsgálom az utóbbi évek szoftver sérülékenységeit, az aktuális trendeket ezen a területen, elemzem a leggyakoribb hibákat. Ezen túl bemutatom, hogy milyen módon lehetséges saját exploitokat készíteni, akár különböző elkerülési technikákkal, és a keretrendszer segítségével végrehajtani.