# Ethical Hacking konferencia az Arénában

***A NetAcademia Oktatóközpont idén immár ötödik alkalommal rendezte meg IT-biztonsági szakemberek részére az Ethical Hacking konferenciát. „Felkért előadóink 2012-ben is izgalmas témákkal és élő demókkal készültek. A gyakorló IT szakembereknek mindenképpen jó, ha találkoznak szakmai konferenciákon, hiszen biztonsági problémák minden rendszer működését veszélyeztethetik" – mondta Fóti Marcell, a NetAcademia ügyvezetője.***

■ ***Fóti Marcell*** (NetAcademia, vezető oktató, CEH, Trusted Security Advisor, MVP) ***„Cloudrendszerek biztonsága, avagy a felhő benéz az ablakon"*** című előadásában elmondta, hogy nagy az ellenállás számos vállakozás részéről, a felhőrendszer használatával szemben, de a felhőrendszerek árának drasztikus csökkenésével lassan minden adattárolás a felhőben lesz megoldva. Hekkelhetők-e, ezek a rendszerek – tette fel az előadó a kérdést és válaszként demókban olyan hákolmányokat mutatott be, melyek megmutatják a legveszélyesebb biztonsági réseket.

■ ***Hambalkó Balázs*** (IT biztonsági szakértő) ***„Adatok megszerzése többszörösen védett hálózatból, avagy nincs olyan, hogy kicsi SQL Injection"*** bemutatójában többféle védelemmel ellátott honlapról adatot szerzett, megkerülve a Web Application Firewallt (Illetve Filterezést), az IDS elől elbújva, és a nem teljesen hacker-barát honlapot is szóra bírva az SQL Injection típusú támadással.

■ ***Kovács Zsombor*** (IT Security Geek, CISSP, OSCP, OSWP, CEH) ***„Mobileszközök gyakori biztonsági buktatói, avagy egy iPad alkalmazás teljes átverése"*** előadásában elmondta, hogy fel kell készülni az eszközhöz fizikailag hozzáférő támadó esetére is. Egy konkrét példán keresztül mutatott be néhány buktatót, amiket kihasználva a szemfüles támadó kicselezheti a legbonyolultabb kriptográfiai eszközparkot is.

■ ***Deim Ágoston*** (Mind-Info, NetAcademia, CEH, ECSA, LPIC, MCP, CLE) ***„A tűzfalon túl, avagy hogyan kerüljünk a tűzfalon kívülre, belülre"*** című előadásában bemutatta, hogy mi ellen tud, és mi ellen nem képes egy tűzfal védelmet nyújtani. A tűzfalak felderítését, és a tűzfalon történő, nem engedélyezett forgalom átvitelének a bemutatása után, gyakorlati példával szemléltette az szakember a probléma lényegét. Az előadás végén az előadó felhívta a hallgatóság figyelmét arra, hogy hagyományos tűzfalak ideje lejárt.

■ ***Kovács László*** (Nemzeti Közszolgálati Egyetem, alezredes, egyetemi tanár) ***„Cyberharcosok, avagy hogyan lopjunk 100 millió dolláros kémrepülőt"*** előadásában beszélt arról, hogy 2011-ben Irán meghekkelt egy csúcstechnológiát képviselő amerikai pilótanélküli repülőgéprendszert, egy 100 millió dolláros kémrepülőt. Az előadó kifejtette, már nem csak arról van szó, hogy valaki meghekkeli a Vatikán hivatalos szerverét, vagy valamelyik bank rendszerét, így szerezve pénzt és kétes hírnevet. A hadviselés szerves részévé válik e technológia, és már kőkemény cyberhadviselésről kell beszélnünk.

■ ***Dr. Bencsáth Boldizsár*** (BME HIT CrySyS Lab, adjunktus, PhD.) ***„Tűzfalakon át DNS PHP kóddal, avagy a DNS-rendszer egy meglepő felhasználása"*** című előadásban elmondta, hogy előfordulhat, hogy egy megtámadott rendszerben a támadó már majdnem eléri célját, de mégis jól védett környezetbe kerül. Így csak rövidebb parancsokat képes futtatni és nem tud kitörni a tűzfal szorításából. Az előadó talán egy eddig nem alkalmazott módszert javasolt, a PHP nyelv DNS-kódba ágyazását, mely segítségével keresztül lehet vergődni a fent vázolt problémákon.

■ ***Balázs Zoltán*** (Deloitte, vezető tanácsadó, CISSP, CPTS, MCP) ***„Zombi tűzróka, avagy mire képes egy rosszindulatú böngésző kiegészítő"*** című demó bemutatóban a hallgatóság láthatta a „hacmebank" módosított működését, illetve a sütilopáson keresztül a GOOGLE 2 faktoros autentikációjának kijátszását. A saját fejlesztésű Firefox kiegészítő „zombi" módjára várja a parancsot egy szervertől, majd végrehajtja azt.

■ A standokat egyébként is érdemes volt körbejárni: Saját szemünkkel is láthattuk, sőt ki is próbálhattuk azt a kémegeret, amelynek belseje a szokásos mutatóeszköz hardveren kívül egy extra SIM-kártya foglalatot is rejtett. Így titokban bármikor belehallgathattunk a szobában folytatott beszélgetésekbe. Mivel a rejtettkamerás, és egyéb megfigyelő, lehallgatóeszközök mára már egészen apró méretekben is rendelkezésre állnak, érdemes lehet ezen elgondolkodni, ha valahonnan például egy egeret kapunk céges ajándékként.

***H. K.***


***Kémegér***