

Adatbiztonság gazdaságinformatikában

2011. november
19.
Budapest

Dr. Bencsáth Boldizsár
adjunktus
BME Híradástechnikai Tanszék
bencsath@crysys.hit.bme.hu



1. Security stakeholders

- Security chief (CIO, etc.)
 - Owners/managers
 - Employees
 - Internet Service Provider
 - Contracted professionals (security product vendors, ethical hackers, etc.)
 - Auditors
 - Outsider attackers
-
- Everybody has a different goal
 - Everybody has different permissions, possibilities
 - Something working in the classroom might not work in real-life

- Internal attackers
- Script kiddies
- Internet-wide scans (botnets, worms, etc.)
- Targeted attackers (with low budget)
- Professional targeted attackers (high budget)

Differences:

- What tools can they use (budget, knowledge)
- What time constraint they have
- How much computing, network resources they have
- How targeted is the attack
- What (how deep, sophisticated) is the main goal of an attack (e.g. just have a proxy -> ransom, multi-million dollar theft, obtaining millions of credit cards)

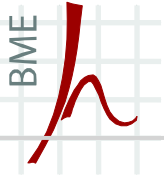
Point-of-View of the attacker

- The attacker focuses on errors rather than what is working
- Tries to find the weakest point
- Finds new ways to attack

This is why security testing, audits are important!

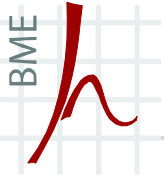
- If You learned security, You can avoid typical errors
- However, It is hard to identify system-wide problems at the first glance, during a large-scale development
- ... And nobody has enough time to do everything in a secure fashion

It is not impossible to do security testing against Your own work – just take a different hat and a bit different thinking,...



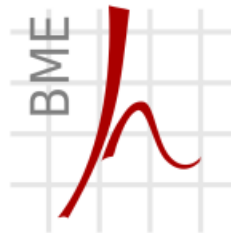
Some practical examples, tools

1. Kernel hack (Script-kiddie style) [VIDEO kernel_hack_2618](#)
(10 mins)



Kérdések?

KÖSZÖNÖM A FIGYELMET!



Híradástechnikai Tanszék

Dr. Bencsáth Boldizsár
adjunktus
BME Híradástechnikai Tanszék
bencsath@crysys.hit.bme.hu

