Week 1: Virtualization and Architecture

03.05.2011, Garching

Due 10.05.2011

1 OS & services (lab task)

Choose your operating system and the services you want to offer on your honeypot and discuss your decisions with the group.

2 Create a virtual machine with VMware Server (lab task)

Create a virtual machine using VMware server, preferably picking the operating system you are planning to use.

3 Using VMware Server (lab task)

Make yourself familiar with VMware Server. For example, learn how to create a snapshot of your virtual machine and how to restore it.

4 Architecture (homework - 3 points)

Think of an architecture for the honeynet and describe it. Give reasons for your design decisions. Also address any security concerns within your architecture and offer solutions to these concerns. Hand in your suggestion in a written form by the beginning of our next session. Be ready to discuss your reasoning.

5 Vulnerabilities and threats (homework - 3 points)

Write a proposal containing the details of your planned operating system and services. This should include a reasoning for your choice and advanced logging capabilities of your system. Research known vulnerabilities to your OS and service(s) and add a short overview of weaknesses and known threats to your proposal. Be prepared to discuss your decisions and tell us about possible attacks on your honeypot.
6 Setup presentation (homework)

Prepare a 20 minute presentation for our meeting on 31.05.2011. This presentation should answer the following questions:

a) Which operating system (version) and services did you choose?

b) What vulnerabilities exist in your chosen setup?

c) Are these vulnerabilities exploitable? If so, to what end? (E.g. remote execution, denial of service, ...)

d) Choose a vulnerability and a single exploit for it. How does the chosen exploit work in detail?

e) Is there malware “in the wild” which makes use of these exploits? If so, give examples! If not, why is this vulnerability not being used by attackers?

Your presentation should include slides and you should be ready to answer questions afterwards. Any groups needing to borrow a laptop, coordinate with us before the session on 31.05.2011!

Submit your slides by the beginning of the session on 31.05.2011, regardless of which slot you are going to give your presentation in!