Systems Security

Exercise 3

Penetration tests - reconnaissance

Perform a reconnaissance, which is e preliminary phase for a penetration test. Use any chosen domain.

Any further phase of the tests is strictly forbidden. Penetration tests will be done later within the local network. Breaking this ban can cause serious restrictions and penalties (see materials form the lecture).

You should find the following information:

- Domain name
- IP address ranges
- Important serwers (DNS, mail, www, possibly others)
- Registrator of the domain
- One contact to an administrator
- Optionally telephone numbers

You should use at least following resources to gather information:

- Public web search services (onet, yahoo, google etc)
- Webpage of the chosen organization
- Whois database

The following programs should be employed, their usage must be documented:

- Web browser
- ***NetScan*** (**only** *whois* tab)
- ***WS Ping ProPack*** (**only** *whois* and *lookup* tabs)
- *nslookup* for retrieving data from DNS
- *tracert* to check whether discovered computers are really working and how they can be reached

During the exercise everyone must prepare a report, containing descriptions of every performed task and obtained information. A few most important screenshots can be attached to show used input parameters and the results. Failures should be included in the report, too. Failure reasons should be clarified. The report must be delivered at the end of the lab.

Prepared by Zbigniew Suski, translation: Janusz Borkowski