

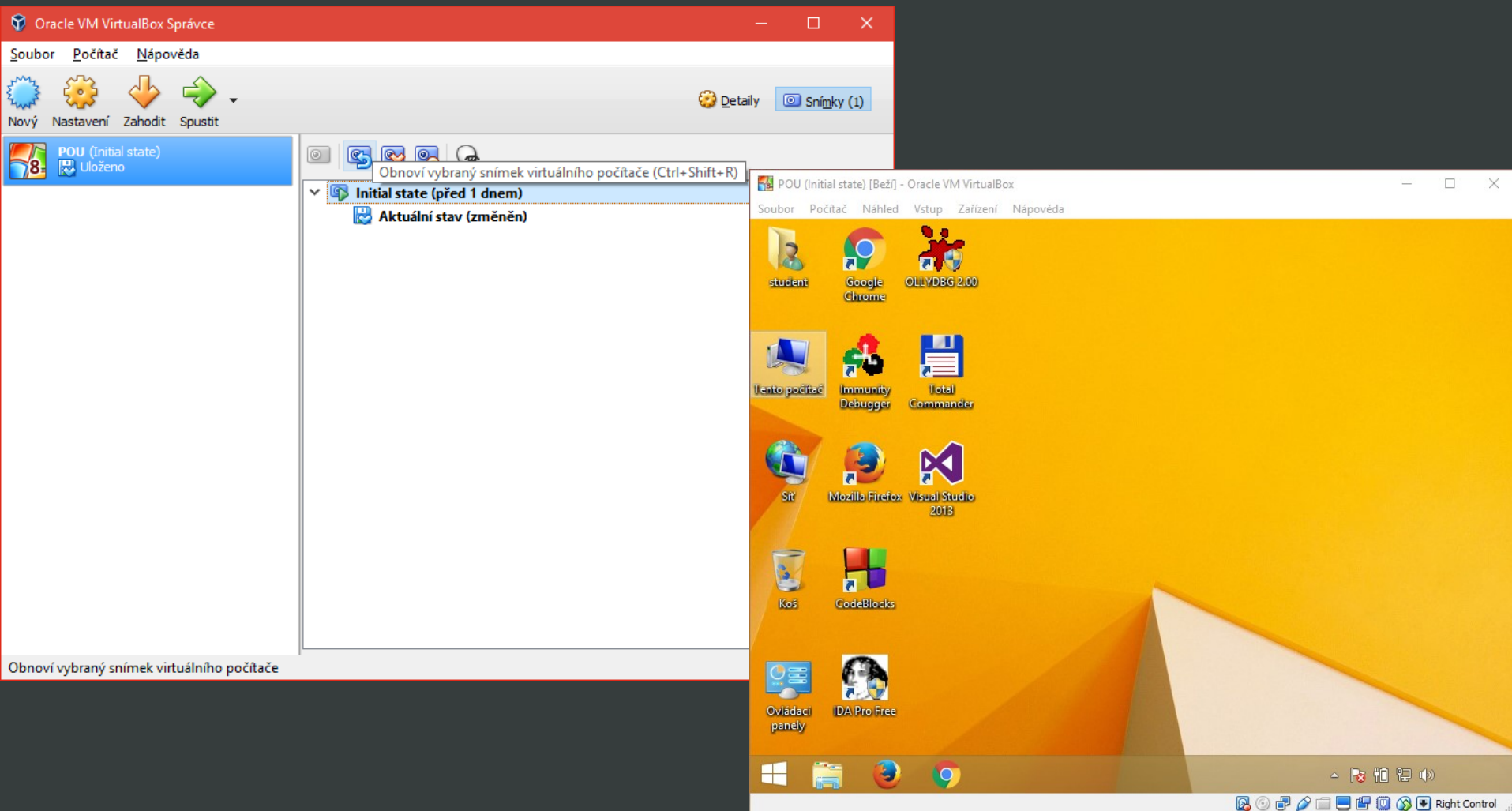
Fakulta elektrotechniky a informatiky
Vysoká škola báňská - Technická univerzita Ostrava

Cvičení 1

POČÍTAČOVÁ OBRANA A ÚTOK - POU

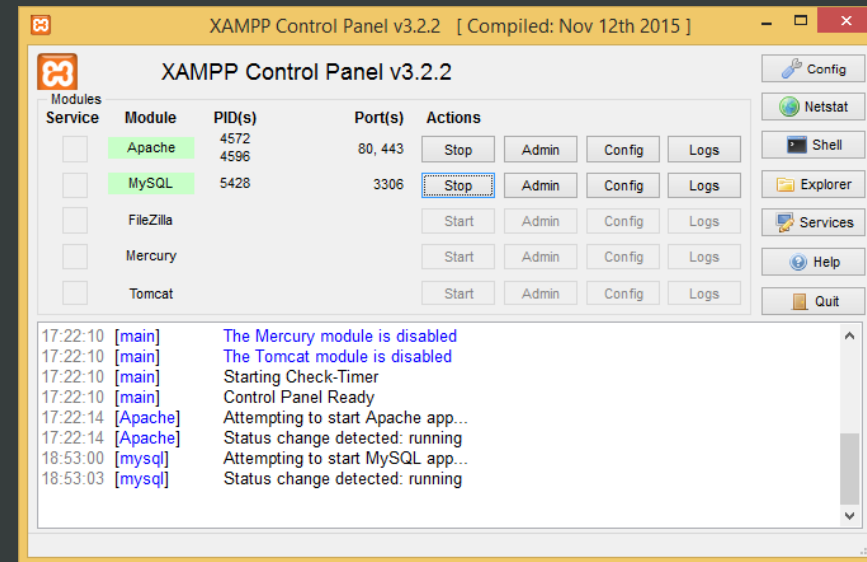


VirtualBox + Windows 8



XAMPP

- populární prostředí k vývoji v jazyce PHP
- snadno instalovatelný balík služeb
 - Apache (webový server)
 - MariaDB (relační databáze)
 - PHP (skriptovací programovací jazyk)
 - Perl (interpretovaný programovací jazyk)

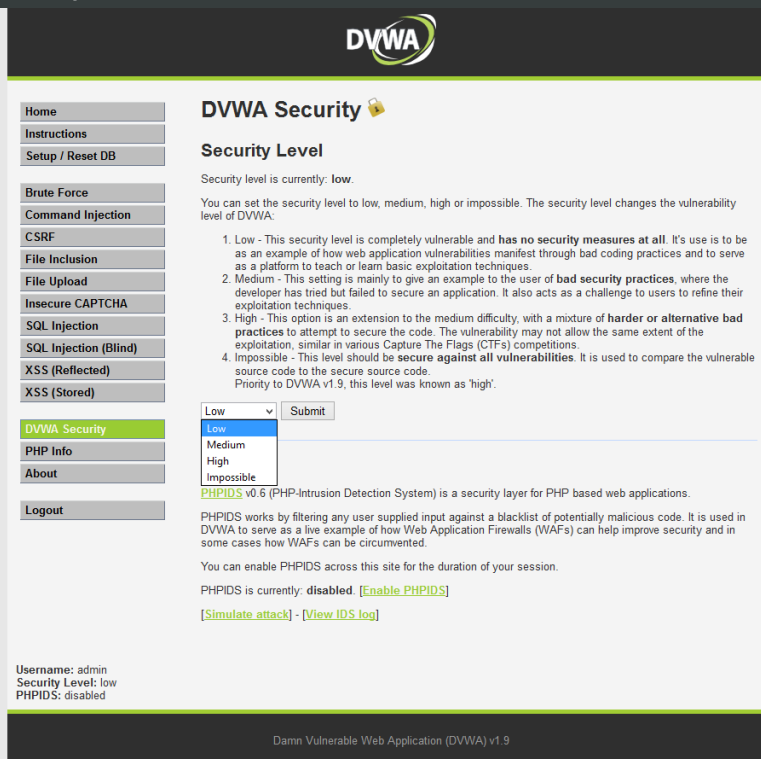


<https://www.apachefriends.org/index.html>

DVWA

- PHP/MySQL zranitelná webová aplikace
- k testování dovedností v oblasti bezpečnosti

<http://www.dvwa.co.uk/>



The screenshot shows the DVWA Security page. On the left is a navigation menu with items like Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), XSS (Reflected), XSS (Stored), DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled "DVWA Security" and "Security Level". It states "Security level is currently: low." and provides a list of four security levels: 1. Low (completely vulnerable), 2. Medium (bad security practices), 3. High (extension to medium difficulty), and 4. Impossible (secure against all vulnerabilities). A dropdown menu is open, showing "Low" selected, with "Medium", "High", and "Impossible" as options. Below the menu is a "Submit" button. The page footer shows "Damn Vulnerable Web Application (DVWA) v1.9".

