Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

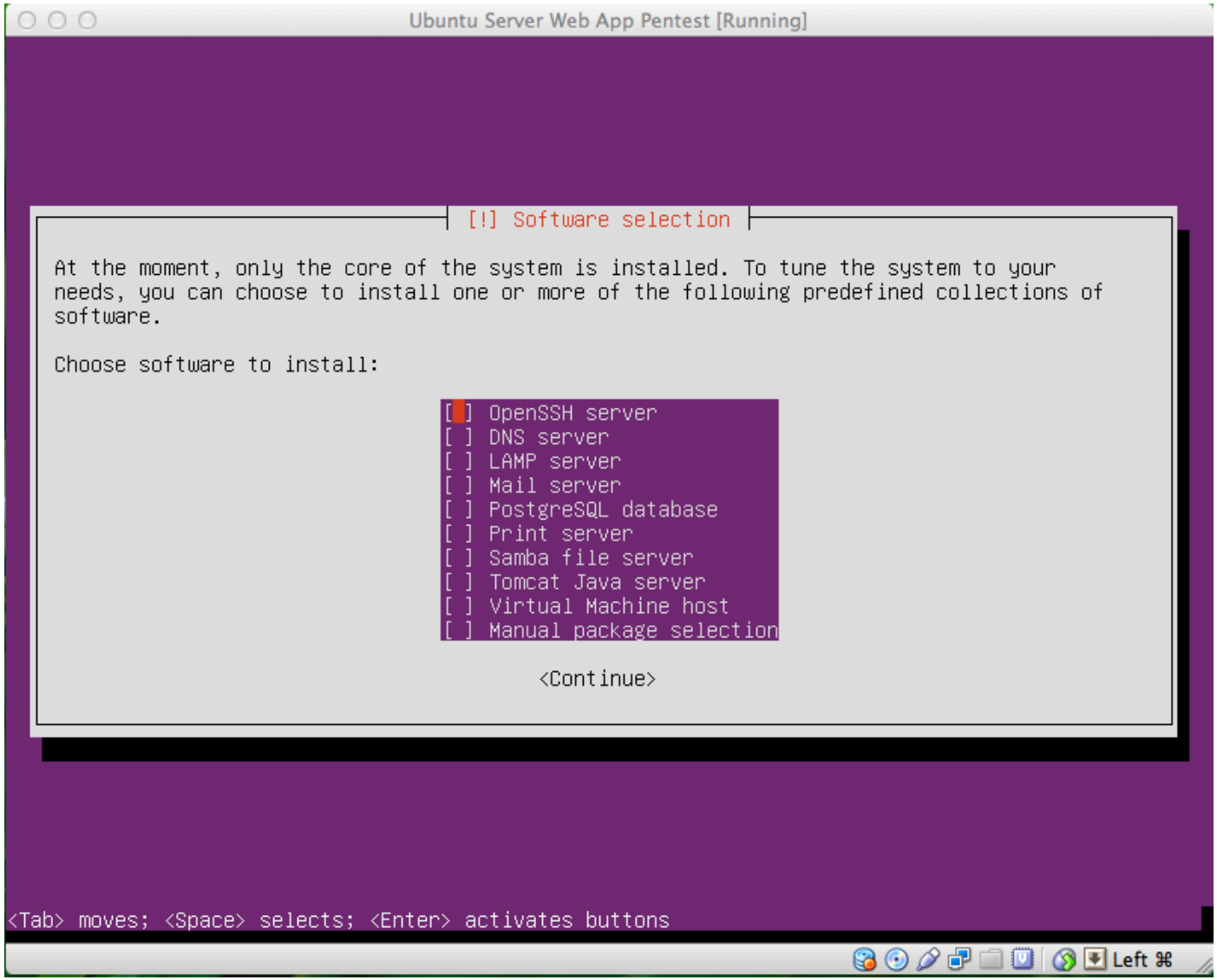
Pentester Academy: http://www.PentesterAcademy.com

Web to Shell on the Server

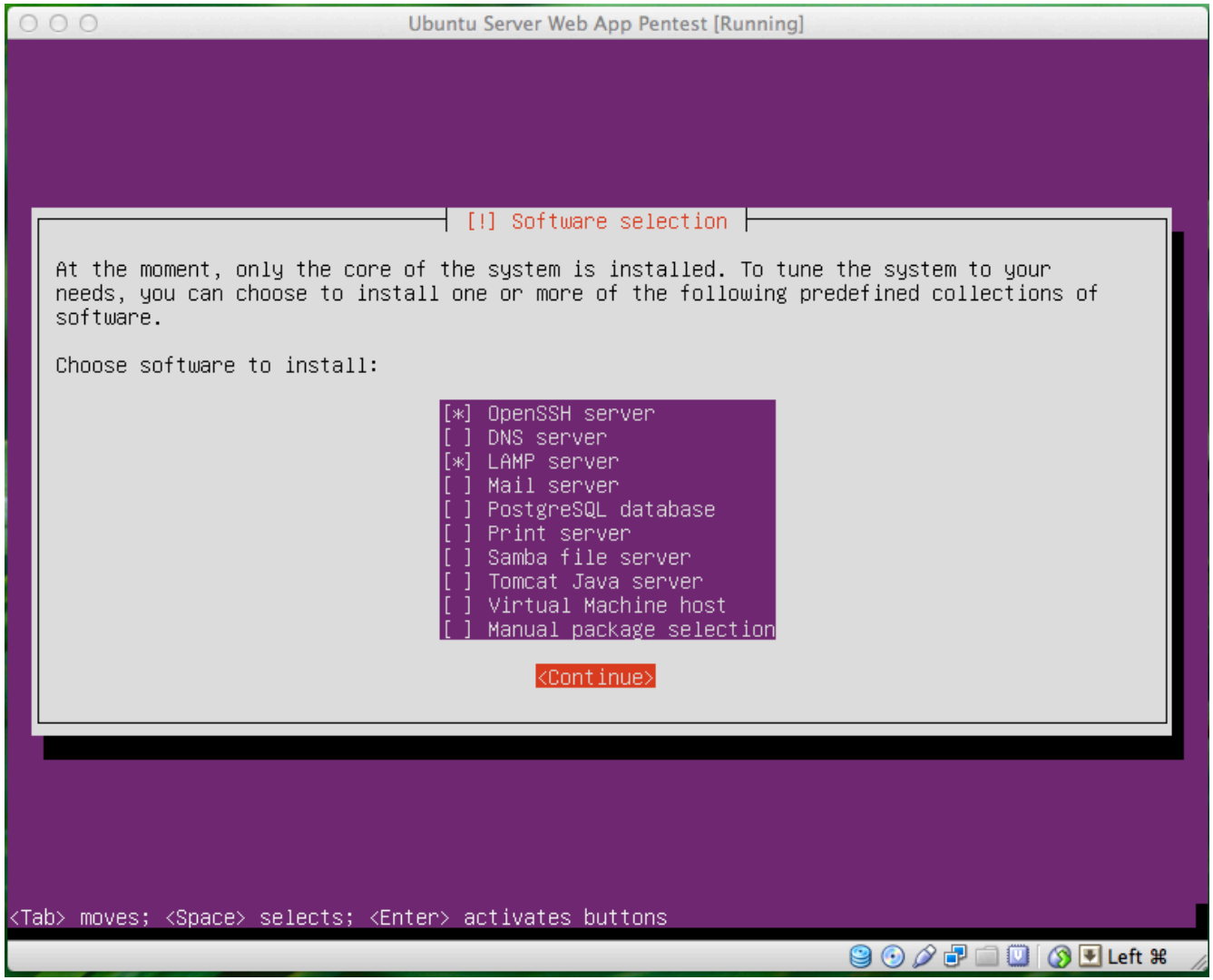
Web to Shell

- Upload backdoor on the server
- Execute commands on server
- Web to Shell
  - Command Injection
  - File Upload
  - …

Ubuntu Server Setup (12.04 LTS)



Open SSH + LAMP

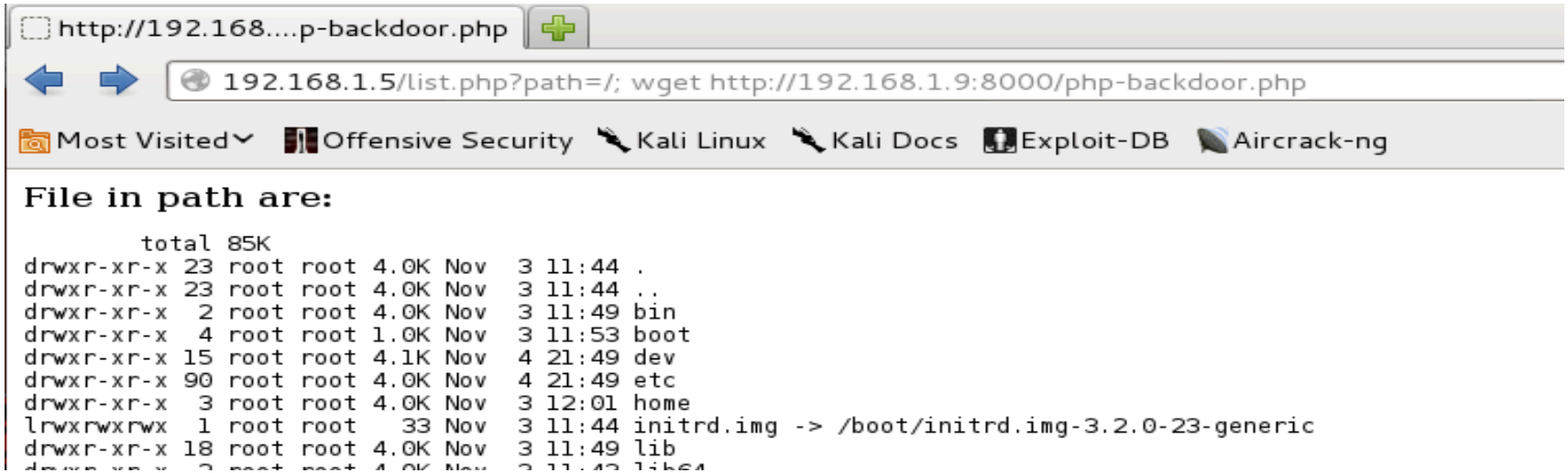


Upload

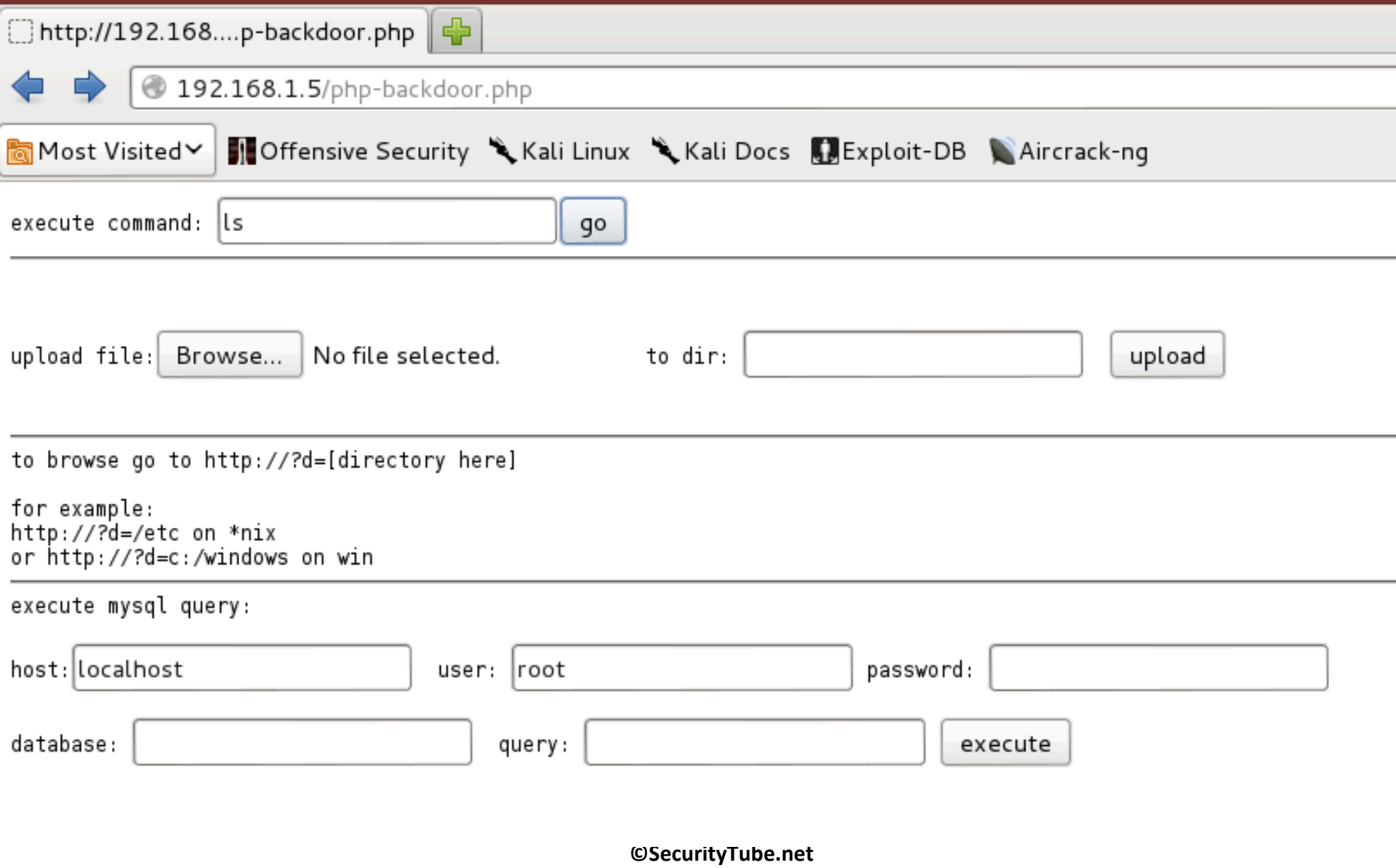
```
root@kali:/usr/share/webshells/php#
root@kali:/usr/share/webshells/php# ls
findsock.c          php-findsock-shell.php  qsd-php-backdoor.php
php-backdoor.php    php-reverse-shell.php   simple-backdoor.php
root@kali:/usr/share/webshells/php#
root@kali:/usr/share/webshells/php#
root@kali:/usr/share/webshells/php#
root@kali:/usr/share/webshells/php# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...



192.168.1.5 - - [04/Nov/2013 11:32:32] "GET /php-backdoor.php HTTP/1.1" 200 -
```



Execute



Own ☺

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

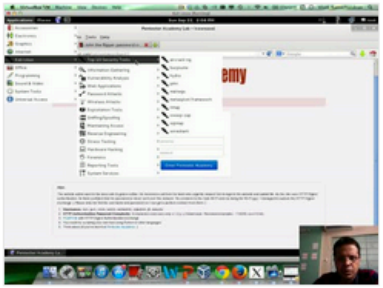
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

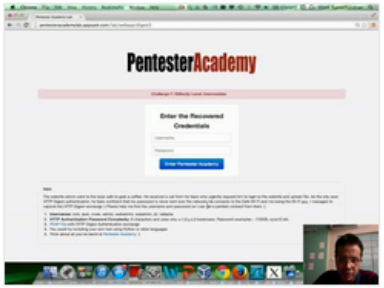
Start Learning Today!

Latest Videos

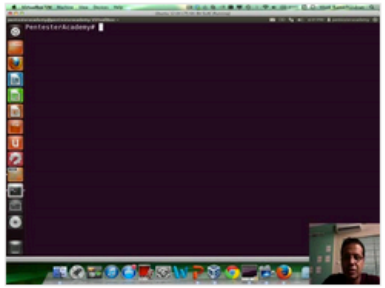
New content added weekly!



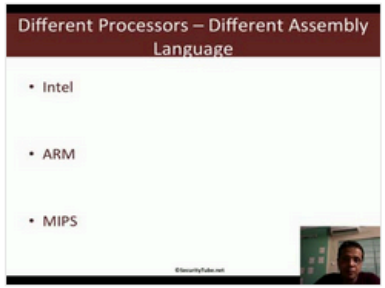
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux