

Network Pentesting

Vivek Ramachandran

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

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

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

Pentesting Routers: Setting up the Lab

Router Pentesting

- Software vulnerabilities
 - Rare and fixed soon
 - Exploit Research
- Faulty by Design
 - Difficult to find for mature products
 - Reversing firmware images and testing
- Configuration Flaws
 - Very common
 - As secure as the knowledge of the Team implementing it

Configuration Flaws

- Attacking Administrative Services
 - SSH, Telnet
 - HTTPD
 - SNMP
- Routing Attacks
 - RIP
 - OSPF
 - BGP

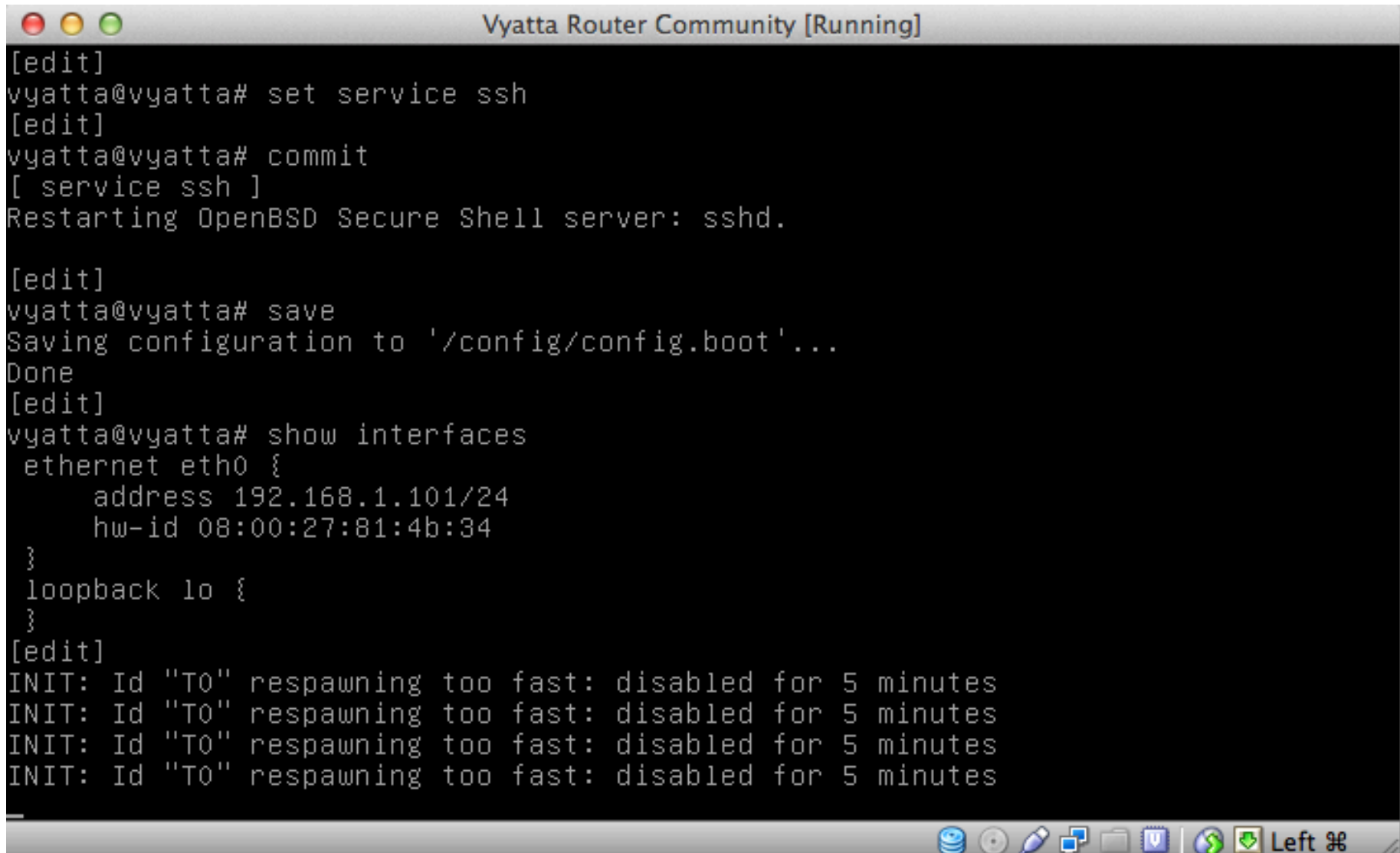
Vyatta



- Totally software based
- Free community edition

http://www.vyatta.com/downloads/documentation/VC6.5/Vyatta-QuickStart_6.5R1_v01.pdf

Installing Vyatta



A terminal window titled "Vyatta Router Community [Running]" showing the configuration of SSH service. The user enters commands to set the service, commit changes, save the configuration, and show interface details. The output shows the configuration for ethernet eth0 and loopback lo, followed by system messages about service respawning.

```
[edit]
vyatta@vyatta# set service ssh
[edit]
vyatta@vyatta# commit
[ service ssh ]
Restarting OpenBSD Secure Shell server: sshd.

[edit]
vyatta@vyatta# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyatta@vyatta# show interfaces
  ethernet eth0 {
    address 192.168.1.101/24
    hw-id 08:00:27:81:4b:34
  }
  loopback lo {
  }
[edit]
INIT: Id "TO" respawning too fast: disabled for 5 minutes
INIT: Id "TO" respawning too fast: disabled for 5 minutes
INIT: Id "TO" respawning too fast: disabled for 5 minutes
INIT: Id "TO" respawning too fast: disabled for 5 minutes
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



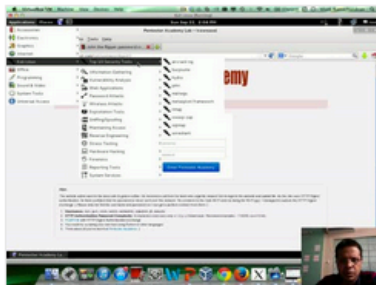
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

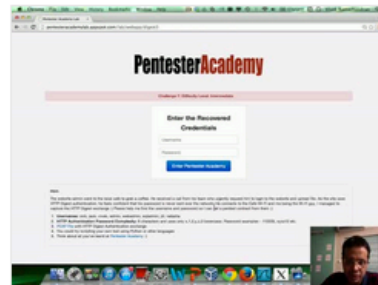
Start Learning Today!

Latest Videos

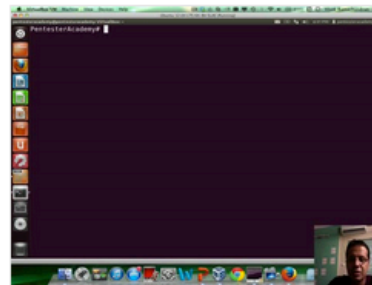
New content added weekly!



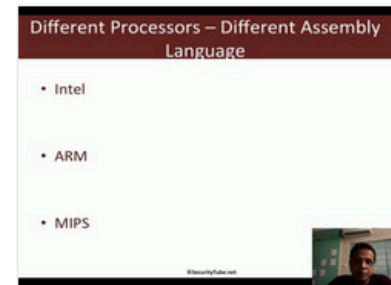
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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

Twitter and Facebook



Security Tube

@SecurityTube

Comprehensive, Hands-on, Practical and Affordable infosec training. Join students from 73+ Countries:

PentesterAcademy.com Securitytube-Training.com

CyberSpace · securitytube.net

19,964
TWEETS

8,576
FOLLOWING

37,554
FOLLOWERS



Edit profile



Next Gen InfoSec Trainin

SecurityTube

✓ Like

You like this.

You and 36,320 others like SecurityTube.