Network Pentesting

Vivek Ramachandran

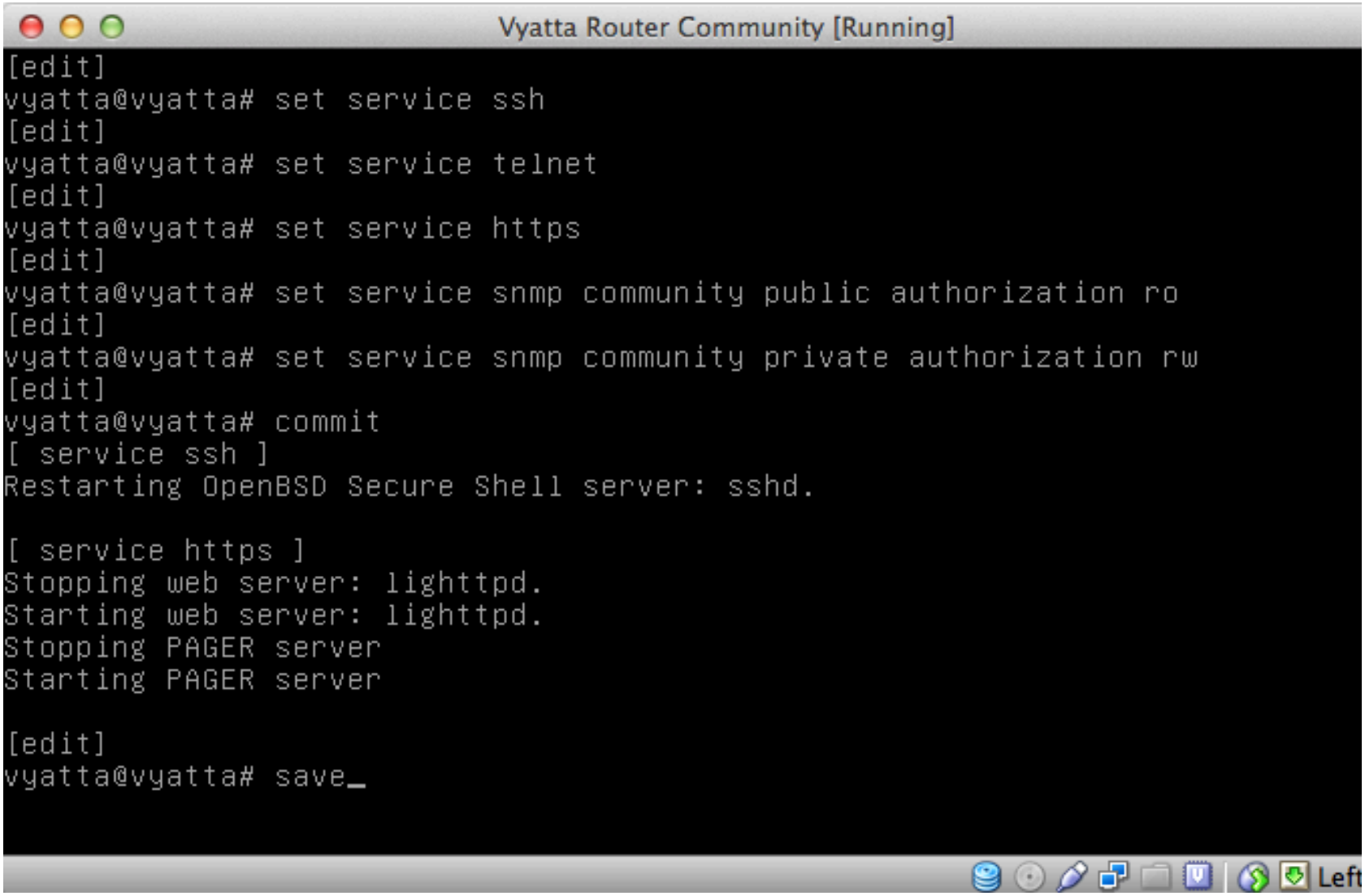
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

Pentesting Routers: Default Credentials on SSH, SNMP, Telnet etc.

Setting up the Lab



Scanning with Nmap

```
root@kali:~# nmap -sV -n 192.168.1.1

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-25 09:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00019s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
23/tcp  open  telnet   Vyatta router telnetd
80/tcp  open  http     lighttpd 1.4.28
443/tcp open  ssl/http lighttpd 1.4.28
MAC Address: 08:00:27:31:1D:17 (Cadmus Computer Systems)
Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http:
Nmap done: 1 IP address (1 host up) scanned in 12.39 seconds
```

Are there any UDP Services?

```
root@kali:~# nmap -sU -p 161 -n -sV 192.168.1.1

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-25 09:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00033s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server (public)
MAC Address: 08:00:27:31:1D:17 (Cadmus Computer Systems)
Service Info: Host: vyatta
```

Running Nmap Scripts

```
root@kali:~# nmap -sU -p 161 -n -sV -sC 192.168.1.1

Starting Nmap 6.25 ( http://nmap.org ) at 2013-05-25 09:25 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00054s latency).
PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server (public)
| snmp-hh3c-logins:
|_  baseoid: 1.3.6.1.4.1.25506.2.12.1.1.1
| snmp-interfaces:
|   lo
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 10 Mbps
|     Traffic stats: 133.75 Kb sent, 133.75 Kb received
|   eth0
|     IP address: 192.168.1.1  Netmask: 255.255.255.0
|     MAC address: 08:00:27:31:1d:17 (Cadmus Computer Systems)
|     Type: ethernetCsmacd  Speed: 100 Mbps
|     Traffic stats: 22.09 Mb sent, 24.34 Mb received
|   eth1
|     MAC address: 08:00:27:74:be:7d (Cadmus Computer Systems)
|     Type: ethernetCsmacd  Speed: 100 Mbps
|     Traffic stats: 0.48 Kb sent, 26.80 Kb received
|   eth2
|     MAC address: 08:00:27:51:10:07 (Cadmus Computer Systems)
|     Type: ethernetCsmacd  Speed: 100 Mbps
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

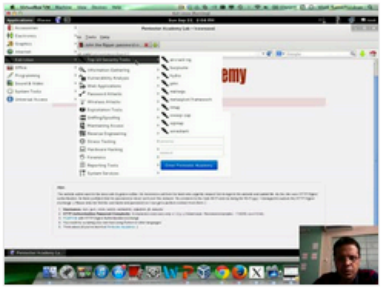
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

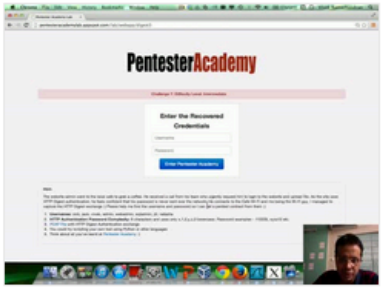
Start Learning Today!

Latest Videos

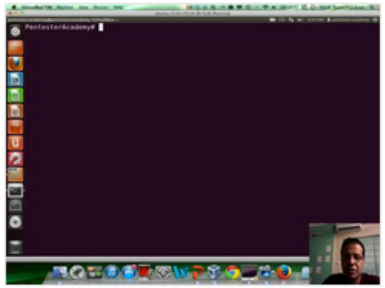
New content added weekly!



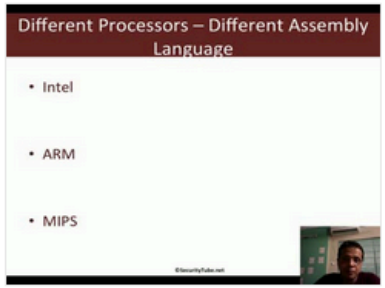
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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