

# Exploiting Simple Buffer Overflows on Win32

Vivek Ramachandran

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

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

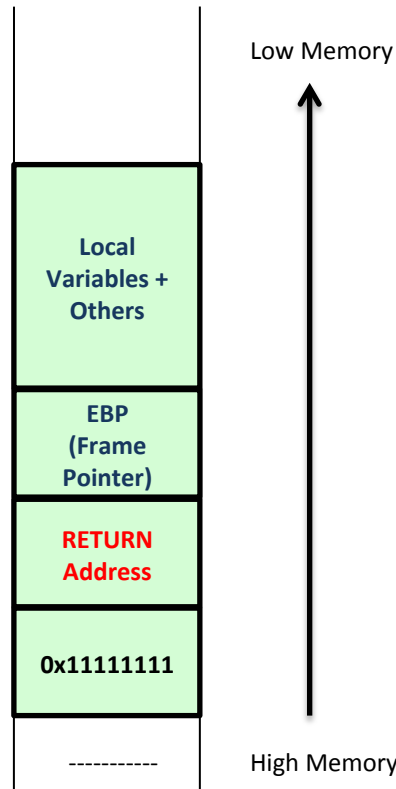
Pentester Academy: <http://www.PentesterAcademy.com>

# Overwriting the Stack with User Input

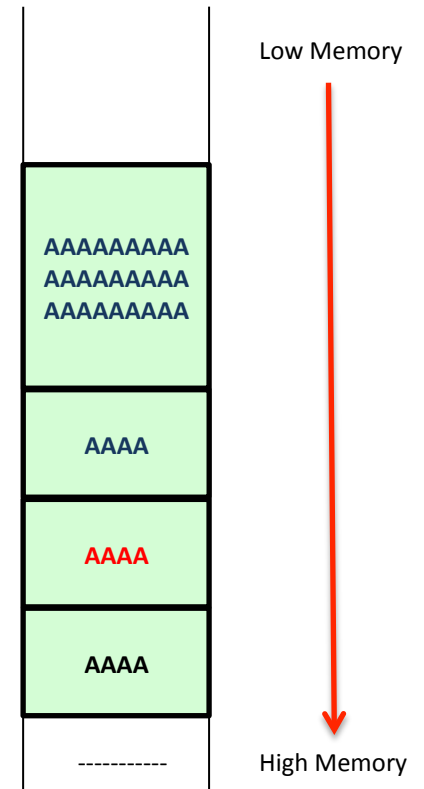
# Return to Shellcode

```
main(....)
{
    ....
    function(0x11111111);
    ....
}
```

```
function1(....)
{
    local variable definitions;
    ....
    return 1;
}
```



gets(buffer)



# Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



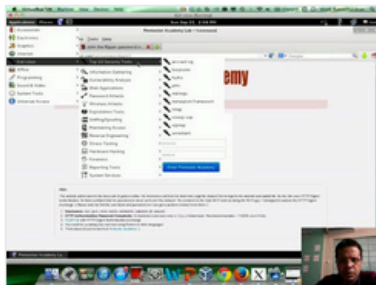
## Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

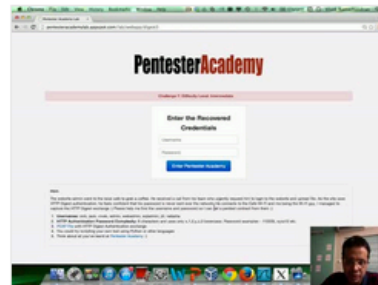
Start Learning Today!

## Latest Videos

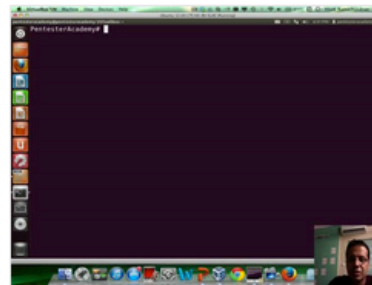
New content added weekly!



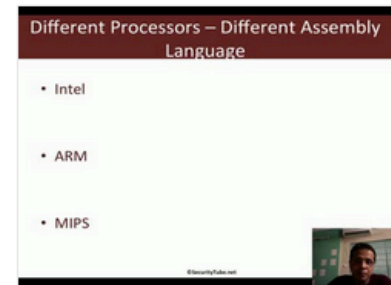
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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