SecurityTube Linux Assembly Expert (SLAE^{64})

SecurityTube Linux Assembly Expert

Training: http://www.SecurityTube-Training.com

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

Vivek Ramachandran

SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{32,64} Course Instructor

Module 1: 64-Bit ASM on Linux

2. CPU Information

Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{64}, SLAE^{32} Course Instructor

http://SecurityTube-Training.com

Different Processors – Different Assembly Language

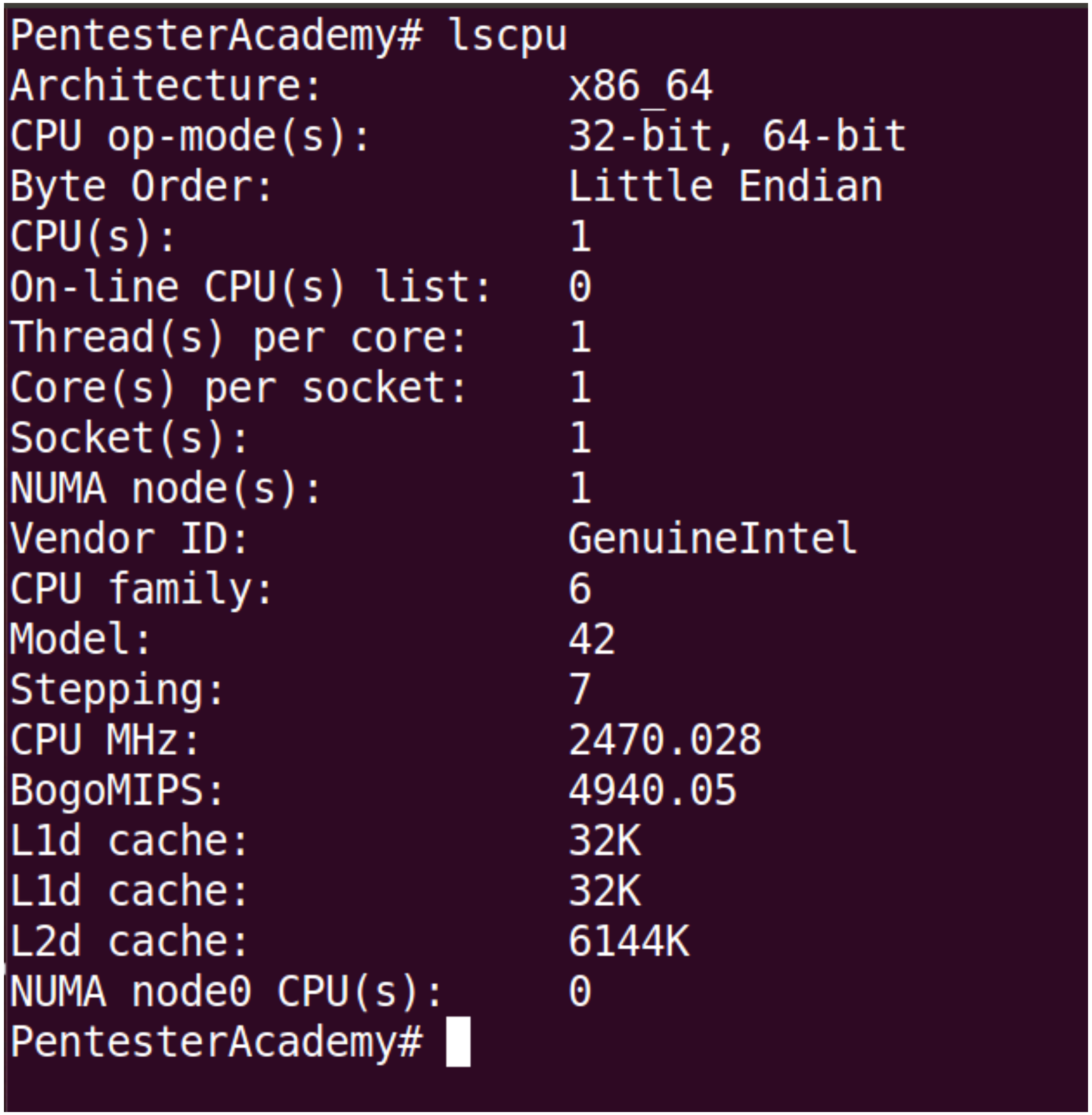
- Intel
- ARM
- MIPS

Intel Architecture

- IA-32

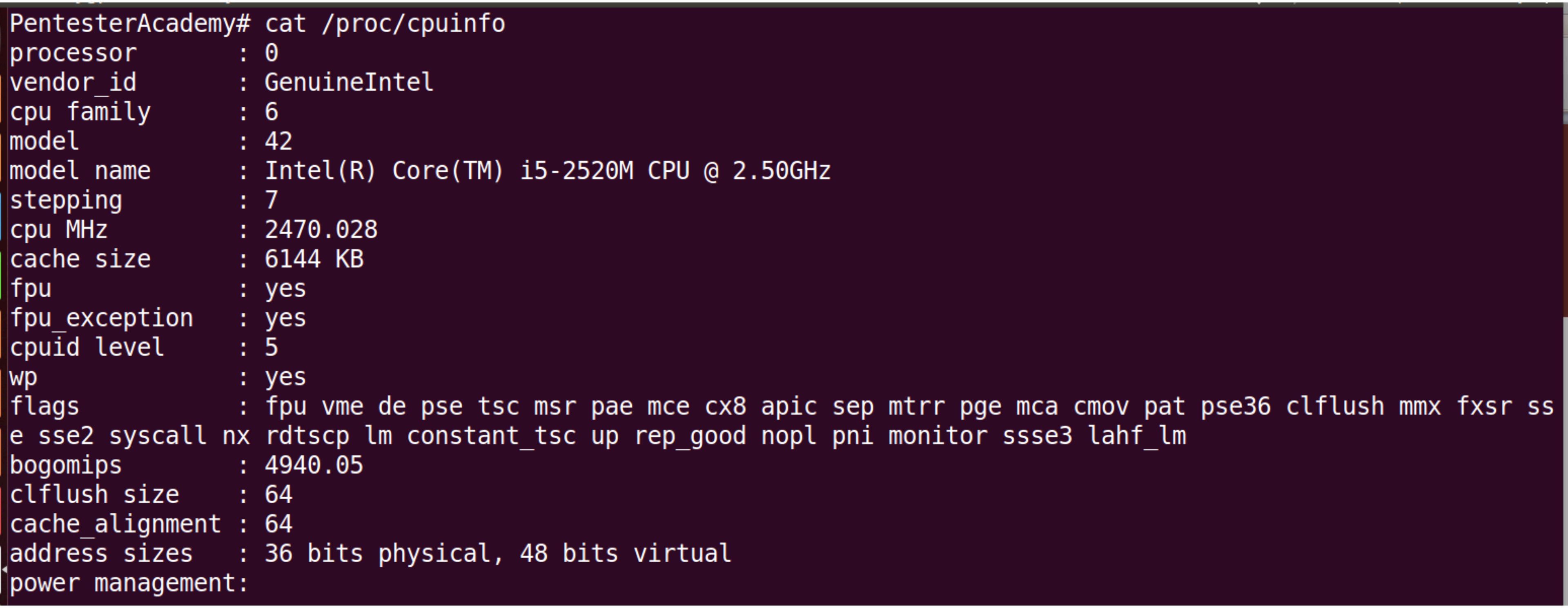
- X86_64

lspcu



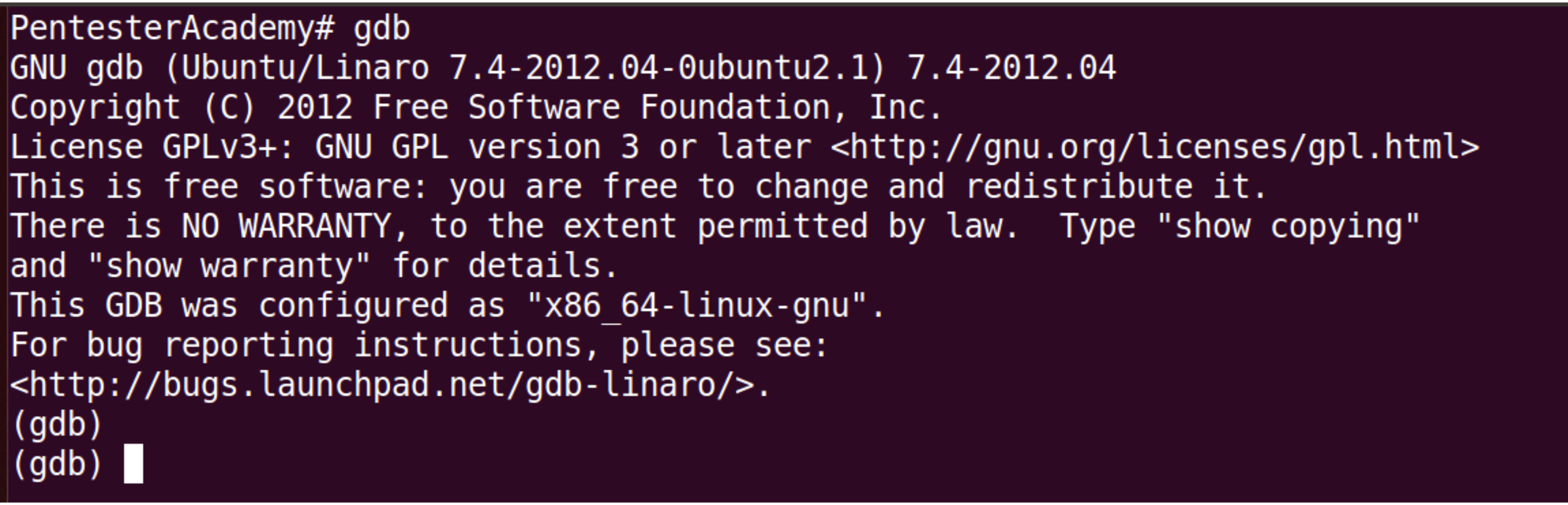
```
PentesterAcademy# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                1
On-line CPU(s) list:   0
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):             1
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 42
Stepping:              7
CPU MHz:               2470.028
BogoMIPS:              4940.05
L1d cache:             32K
L1d cache:             32K
L2d cache:             6144K
NUMA node0 CPU(s):     0
PentesterAcademy# 
```

Cat /proc/cpuinfo



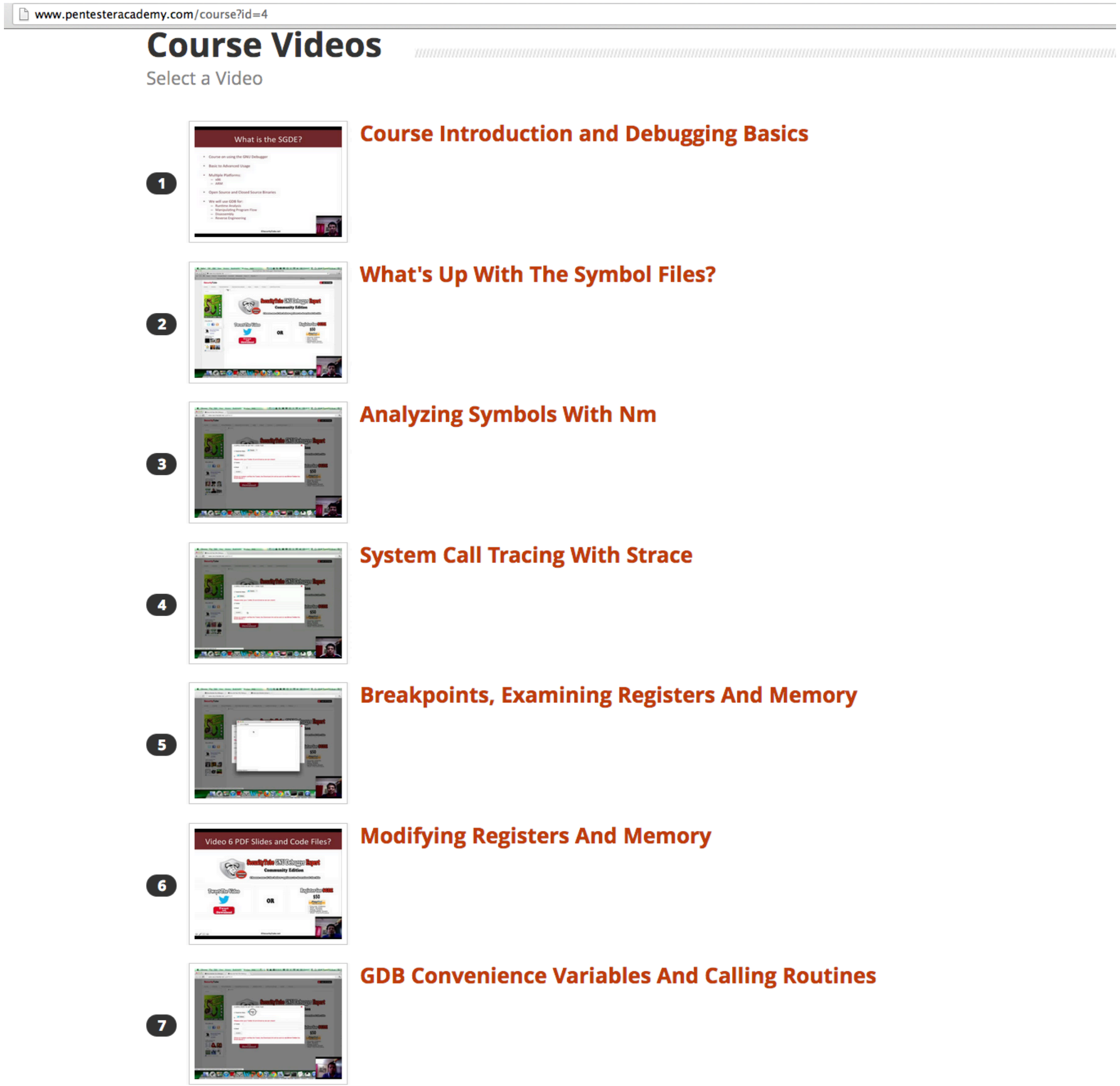
```
PentesterAcademy# cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 42
model name      : Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz
stepping        : 7
cpu MHz         : 2470.028
cache size      : 6144 KB
fpu             : yes
fpu_exception   : yes
cpuid level     : 5
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr ss
e sse2 syscall nx rdtscp lm constant_tsc up rep_good nopl pni monitor ssse3 lahf_lm
bogomips        : 4940.05
clflush size    : 64
cache_alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:
```

GDB – your best friend



```
PentesterAcademy# gdb
GNU gdb (Ubuntu/Linaro 7.4-2012.04-0ubuntu2.1) 7.4-2012.04
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
For bug reporting instructions, please see:
<http://bugs.launchpad.net/gdb-linaro/>.
(gdb)
(gdb) █
```

GDB Series on Pentester Academy



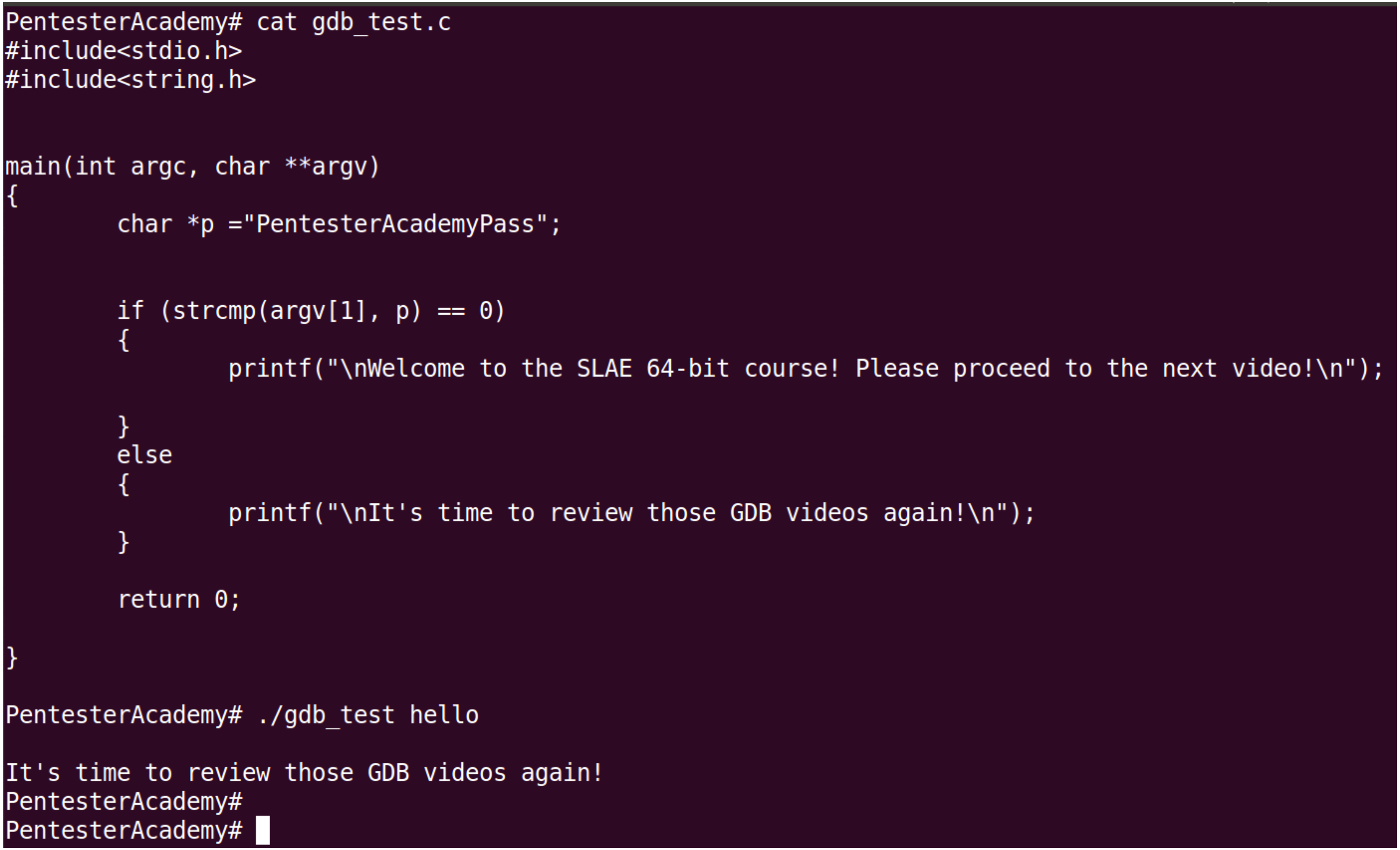
www.pentesteracademy.com/course?id=4

Course Videos

Select a Video

1. Course Introduction and Debugging Basics
2. What's Up With The Symbol Files?
3. Analyzing Symbols With Nm
4. System Call Tracing With Strace
5. Breakpoints, Examining Registers And Memory
6. Modifying Registers And Memory
7. GDB Convenience Variables And Calling Routines

GDB Test



```
PentesterAcademy# cat gdb_test.c
#include<stdio.h>
#include<string.h>


main(int argc, char **argv)
{
        char *p ="PentesterAcademyPass";


        if (strcmp(argv[1], p) == 0)
        {
                printf("\nWelcome to the SLAE 64-bit course! Please proceed to the next video!\n");

        }
        else
        {
                printf("\nIt's time to review those GDB videos again!\n");
        }

        return 0;

}

PentesterAcademy# ./gdb_test hello

It's time to review those GDB videos again!
PentesterAcademy#
PentesterAcademy# 
```