Binary Analysis Course

MAX ‘LIBRA’ KERSTEN

What is it?

- A public and free course providing step-by-step insights
  - It provides conceptual insights with the help of practical cases
  - Fully focused on free and open-source software
- The course contains
  - Background information
  - Conceptual explanations
  - Practical cases
  - Malware analysis
  - Automation scripts
  - Report writing tips

Console - Scripting

```
TalismanStackStringDecryption.java> Running...
TalismanStackStringDecryption.java> Stack string starting at 0x10002401
TalismanStackStringDecryption.java> Stack string ended, since no suitable scalar value could be found at 0x10002460!
TalismanStackStringDecryption.java> --------------------------------------------------------------------------------
TalismanStackStringDecryption.java> US-ASCII: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> ISO-LATIN-1: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> UTF-16BE: 䜀氀漀戀愀氀尀䐀攀氀匀攀氀昀⠀─㠀⸀㠀堀⤀
TalismanStackStringDecryption.java> UTF-16LE: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> UTF-8: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> Length in bytes: 46
TalismanStackStringDecryption.java> --------------------------------------------------------------------------------
TalismanStackStringDecryption.java> Finished!
```

Console - Scripting

```
xorddos_array_decryption.java> Running...
xorddos_array_decryption.java> cat resolv.conf
xorddos_array_decryption.java> sh
xorddos_array_decryption.java> bash
xorddos_array_decryption.java> su
xorddos_array_decryption.java> ps -ef
xorddos_array_decryption.java> ls
xorddos_array_decryption.java> ls -la
xorddos_array_decryption.java> top
xorddos_array_decryption.java> netstat -an
xorddos_array_decryption.java> netstat -antop
xorddos_array_decryption.java> grep "A"
xorddos_array_decryption.java> sleep 1
xorddos_array_decryption.java> cd /etc
xorddos_array_decryption.java> echo "find"
xorddos_array_decryption.java> ifconfig eth0
xorddos_array_decryption.java> ifconfig
xorddos_array_decryption.java> route -n
xorddos_array_decryption.java> gnome-terminal
xorddos_array_decryption.java> id
xorddos_array_decryption.java> who
xorddos_array_decryption.java> whoami
xorddos_array_decryption.java> pwd
xorddos_array_decryption.java> uptime
xorddos_array_decryption.java> Finished!
```

```
undefined __Z8aCheckAVv(void)

{
  bool bVar1;
  char *pcVar2;
  undefined uVar3;

  pcVar2 = __Z8aDecryptPc(&_aAV00);
  bVar1 = __Z7aPathAVPc(pcVar2);
  uVar3 = bVar1 != false;
  pcVar2 = __Z8aDecryptPc(&_aAV01);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x2;
  }
  pcVar2 = __Z8aDecryptPc(&_aAV02);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x3;
  }
  pcVar2 = __Z8aDecryptPc(&_aAV03);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x4;
  }
  pcVar2 = __Z8aDecryptPc(&_aAV04);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x5;
  }
```

```
undefined __Z8aCheckAVv(void)

{
  bool bVar1;
  char *pcVar2;
  undefined uVar3;

                    /* Decrypted value: "AVAST Software" */
  pcVar2 = __Z8aDecryptPc(&_aAV00);
  bVar1 = __Z7aPathAVPc(pcVar2);
  uVar3 = bVar1 != false;
                    /* Decrypted value: "Avira" */
  pcVar2 = __Z8aDecryptPc(&_aAV01);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x2;
  }
                    /* Decrypted value: "Kaspersky Lab" */
  pcVar2 = __Z8aDecryptPc(&_aAV02);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x3;
  }
                    /* Decrypted value: "ESET" */
  pcVar2 = __Z8aDecryptPc(&_aAV03);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x4;
  }
                    /* Decrypted value: "Panda Security" */
  pcVar2 = __Z8aDecryptPc(&_aAV04);
  bVar1 = __Z7aPathAVPc(pcVar2);
  if (bVar1 != false) {
    uVar3 = 0x5;
  }
```

Where can I find it?

- On my website: maxkersten.nl/binary-analysis-course/
- If you have questions, suggestions, or simply want to state you dislike Java
  - @Libranalysis on Twitter
  - /in/ThisIsLibra on LinkedIn
  - @ThisIsLibra on Telegram