Why you should learn maldev

Become better at red team

Learning maldev gets you a bag of handy techniques which you can use to:

1. Partially automate red team engagements
2. Create custom payloads / tools
3. Be better at defence evasion

Become better at blue team

Learning maldev gives you exposure to various tips, tricks and techniques which are used by malware. You can write better detections once you understand how malware developers think.

Linux Maldev 101

Learn malware development
for Linux platform

Syllabus

- Common framework
  - Writing HTTP client and server
  - Command and control using HTTP
  - Preparing payload framework

Syllabus

- Initial compromise
  - Automated network scanning
  - Common methods for initial compromise
  - Automating initial compromise

Syllabus

- Building the payload
  - Single stage payload
  - Multi-stage payload
  - Extensible payload
  - Writing dynamic extensions

Syllabus

- Automating MITRE ATT&CK TTPs
  - Execution
  - Persistence
  - Privilege escalation
  - Lateral Movement
  - Defense evasion

Syllabus

- Combining the pieces
  - Automating end to end attack chain

Prerequisites

- Prior experience with Linux
- Prior experience with bash shell scripting
- Prior experience with C++14 or above

Register now!

https://arishtisecurity.com/training/malware-development