Linux 逆向

adamanteye

1. LLDB 使用

参考:

- GDB to LLDB command map - LLDB

运行:

```
(lldb) r(un)
```

附带参数运行:

```
(lldb) r(un) ans
```

下断点:

```
(lldb) br(eakpoint) s(et) --name/-n phase_2
(lldb) b phase_2
```

查看所有断点:

```
(lldb) br(eakpoint) l(ist)
```

删除断点:

```
(lldb) br(eakpoint) del(ete) 1
```

步进:

```
(lldb) s(tep)
```

步过:

```
(lldb) n(ext)
```

栈回溯:

```
(lldb) bt
```

查看通用寄存器:

```
(lldb) re(gister) r(ead)
```

为寄存器写入十进制值:

```
(lldb) re(gister) w(rite) rax 123
```

退出:

```
(lldb) q
```

2. Binary Ninja

注意默认以简化 Intel 格式显示 x86-64 汇编,可改为 AT&T 格式.