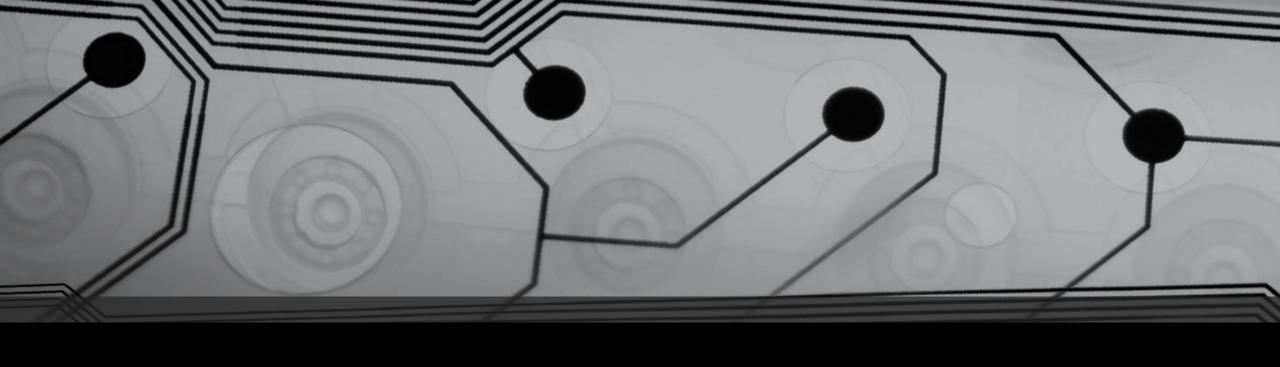


## Practical DEP + ASLR



# DEP

Automatic ROP Chain Building

### Ropper - Automated RopChain Building

- ./Ropper.py --file /bin/ls --chain "execve cmd=/bin/sh" --badbytes oooaod
  - https://anee.me/hackover-ctf-2016-ping-gnop-writeup-246f68b083aa
  - <a href="https://advancedpersistentjest.com/2017/07/31/writeups-rev75-simplephp-pwn100-bugs-bunny-ctf/">https://advancedpersistentjest.com/2017/07/31/writeups-rev75-simplephp-pwn100-bugs-bunny-ctf/</a>

#### Angrop - Automated Write/Read/Syscall

- https://github.com/salls/angrop
  - <a href="https://bannsecurity.com/index.php/home/10-ctf-writeups/34-openctf-2016-tyro-rop2">https://bannsecurity.com/index.php/home/10-ctf-writeups/34-openctf-2016-tyro-rop2</a>



#### **ASLR**

- Theory:
  - 32 bit No leak needed
    - ASLR bruteforce (Small space)
    - Buffer overflow/Format String/Arbitrary write
  - 64 bit Leak needed
    - Information Leak (Separate from write)
    - Buffer overflow/Format String/Arbitrary write

#### No awesome tools for this yet

- Read the write-ups!
  - ASLR 32bit Bruteforce
    - http://taishi8117.github.io/2015/11/11/stack-bof-2/
  - ASLR 64bit Bypass through .got/.plt
    - <a href="https://www.trustwave.com/Resources/SpiderLabs-Blog/Baby-s-first-NX-ASLR-bypass/">https://www.trustwave.com/Resources/SpiderLabs-Blog/Baby-s-first-NX-ASLR-bypass/</a>
    - https://sploitfun.wordpress.com/2015/05/08/bypassing-aslr-part-iii/
  - ASLR 32bit/64bit Bypass throuh ret2libc
    - https://sploitfun.wordpress.com/2015/05/08/bypassing-aslr-part-i/
    - https://sploitfun.wordpress.com/2015/05/08/bypassing-aslr-part-ii/