Swimming in the Sea of ELF

AVTOKYO 2015 WORKSHOP

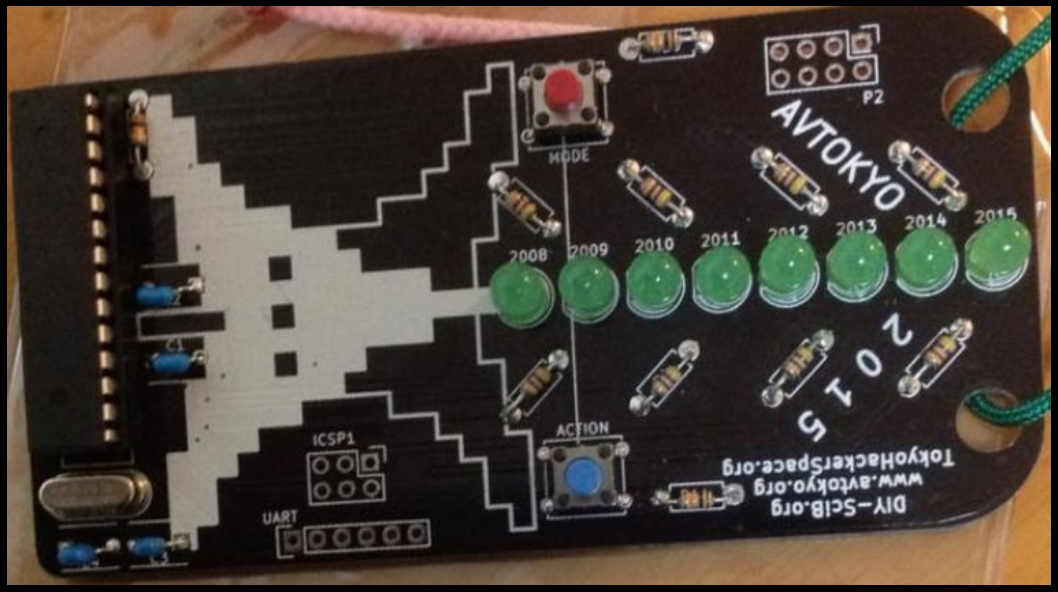
written by: @unixfreaxjp
presenters:
@ucq / IDA reversing
@unixfreaxjp / slides & all in UNIX shell reversing

November 14th, Shibuya, Tokyo, Japan

Thank's for directions from:
@tessy_jp, @moton, @sen_u @avtokyo

/ELF malware workshop

- WHY ELF?



/ELF malware by vuln top rank （システム脆弱性のELF感染順）

- shellshock < still number #1
- weak service credential (ssh/ftp/telnet)
  サービスの弱いログイン認証
- webapps remote injection vie vuln service exploitation
  コードインジェクション・ファイルアップロード
  (CMS/php, ElasticSearch,cPanel, Struts)
- Malvertisement (droids)
- others

/ELF malware by source

- Cyber crime botnet / サイバー犯罪系 (cDorked, mayhem, moose, etc)
- China ddoser (xor.DDOS, IptabLeX, etc)
- Youth hackers (skids) < irc ddos/pwn
- Spy tools (Finsisher, HackTeam etc)
- others

/ELF malware by device

- servers / vps
- network device (routers, switch, network & unmanaged security appliances)
- IoT (web camera, etc)
- Home/SOHO linux embedded devices
- droid phones
- desktop

Aimed target:

- DEFAULT CREDENTIALS
- OBSOLETE SECURITY

/ELF malware by platform

- x86 32bit
- x86 64bit
- ARM (and armel) 32bit
- MIPS (and mipsel) 32bit
- ARM (and armel) 64bit
- PPC 32bit
- SH 32bit
- Sparc

/ELF malware by function

- backdoor
- rootkit / pwn tool
- botnet (irc/shell or webshell)

FOR:

- ddoser
- infector to next linux nodes
- infector to clients
- bitcoin miner
- ransom

/workshop theme

- ELF malware analysis | ELFマルウェア調査
- Windows & UNIX shell | Windows上で調査 vs UNIX shell上の調査
- All is about **Tools** | ツール紹介
- Point: Audience interaction | 質問・説明・見せる事
- Agenda base | アジェンダ通りで実行
- Offline DEMO | オフライン経由のデモ

/agenda

- 色んなELFマルウェアの作り方、普通のELFと違い、隠せる方法とよく使われているのトリック、を説明する。
- ELFマルウェアバイナリーの調査やり方とツール紹介 ・ツールの説明 ・UNIX shellの上でELFのstatic vs dynamic調査連携方法 ・そしてリバースエンジナリング vs debugging方法 ・ELFファイルとメモリーforensics (Linux xBSD).

/agenda

- リアルケースELFマルウェア調査、仕組みTIPS/ヒント/トリック(デモ+説明）
  ・東ヨロッパ系ELFマルウェアPnScan, darkleech, mayhem,cDorkなど
  ・中国タイプELFマルウェア種類＋それぞれの種類の弱点
  ・skiddies系ELFマルウェア種類(なんでもIRC ddos)

/agenda

- ELF signatureアドバイサリー ・ClamAV ・Yara ・IOC
- サンプルケース説明/デモ
  (いくつかのリアル・ケースリバーシング)
- 発見仕方・調査流れの説明・調査目的/レポート・ヒント・TIPS・など
- Q & A

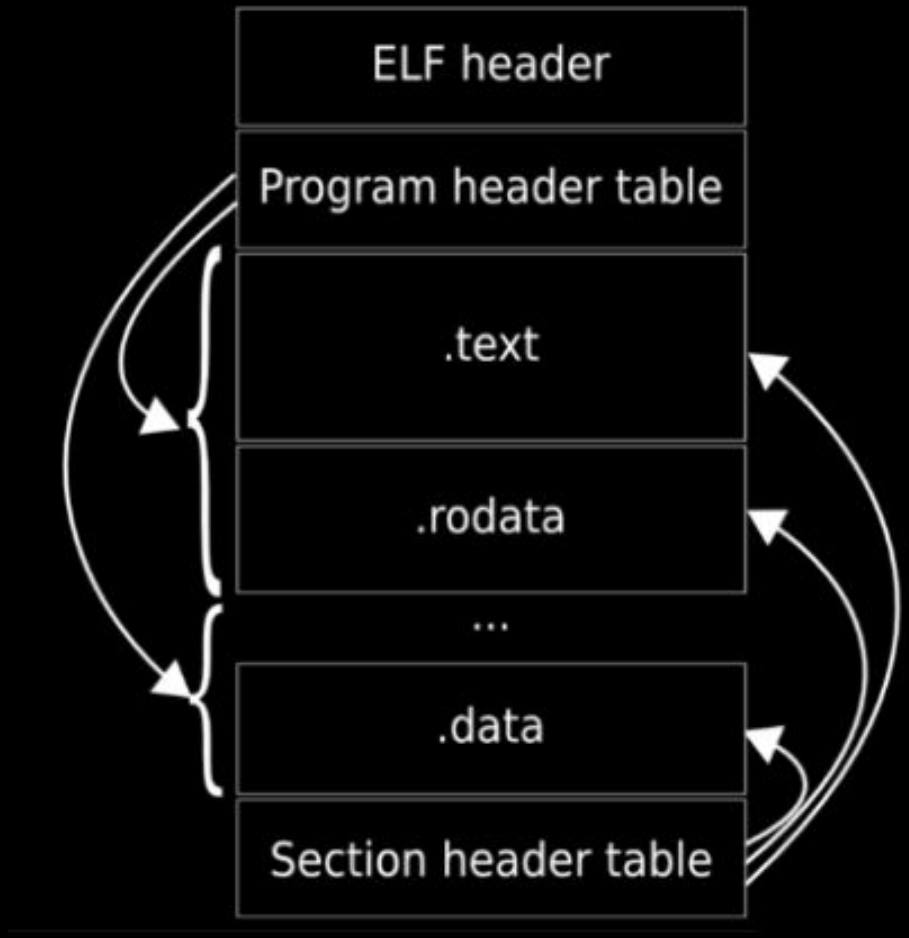
/BEFOREHAND...

- ELF malware does.. / ELFマルウェア目的
- ELF basics / ELFとは…w
- Linux execution basics / ELF実行仕組み
- Interception basics
- what needed to be noted in analyzing ELF in / いくつか注意点
  - using Windows tools
  - using shell tools
  - using online environments

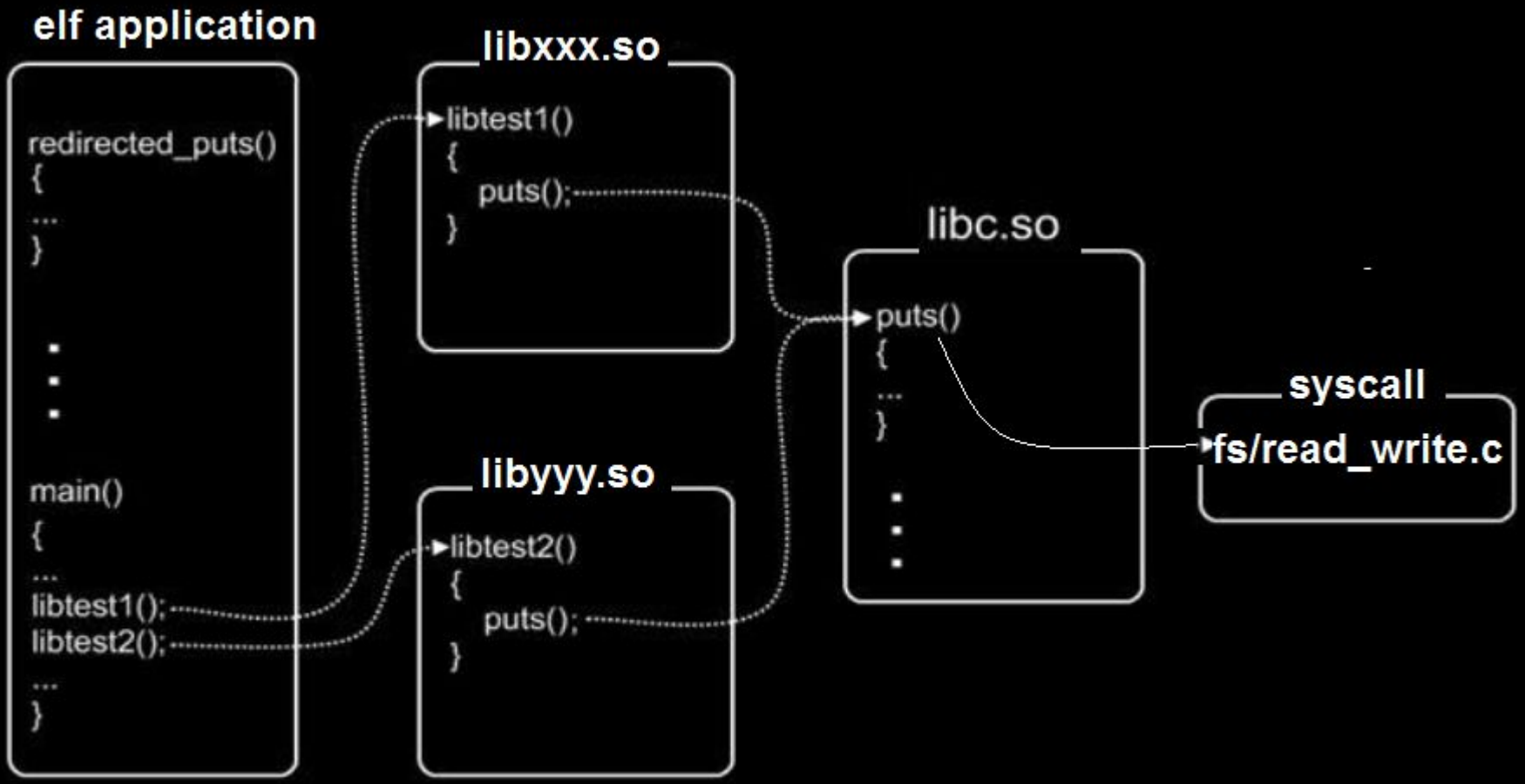
/ELF malware does:

- module interceptor (kernel / apps)
- static
- symbol stripping
- EP point hijack
- encryption
- exploitation
- rootkit
- botnet

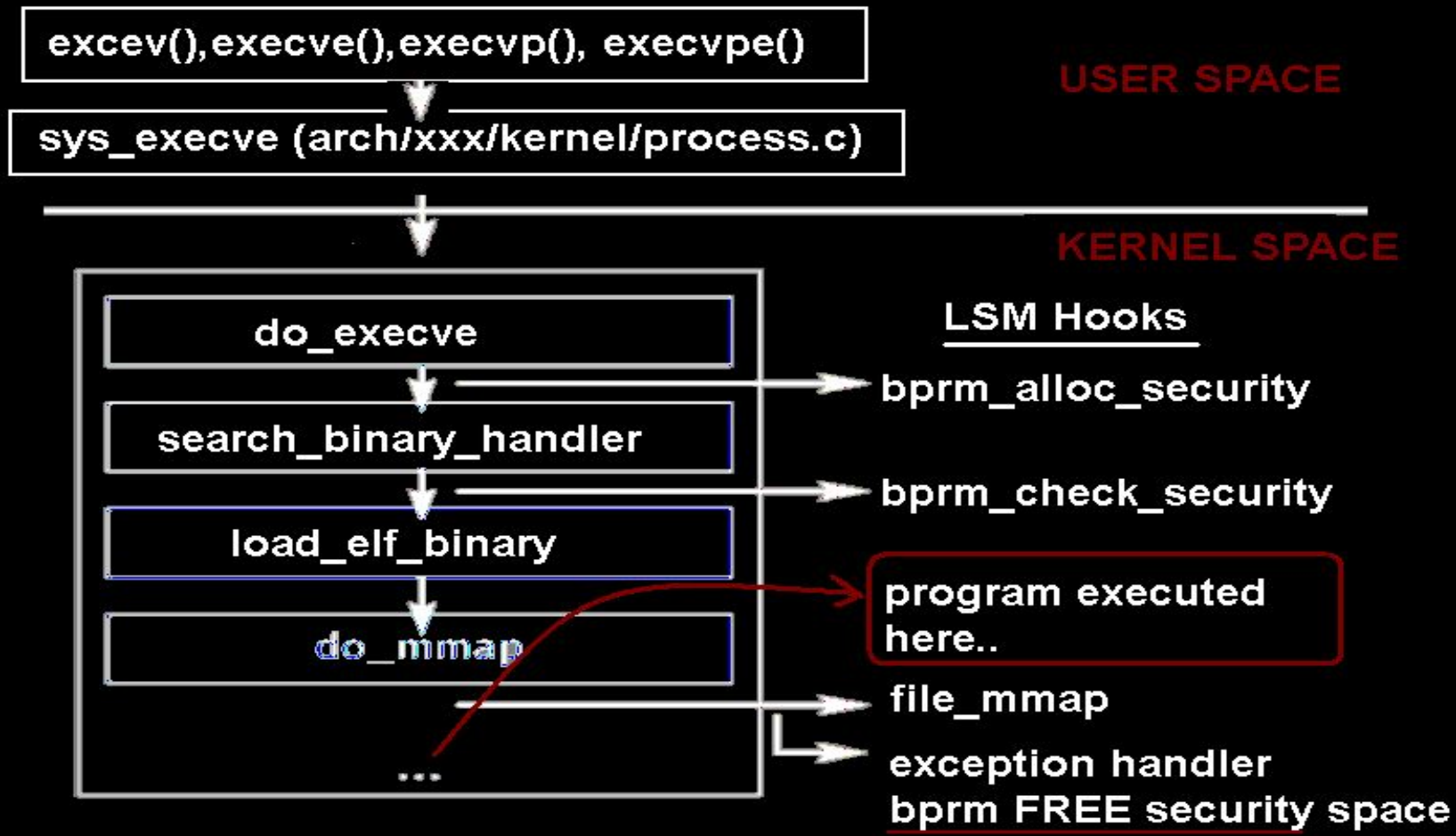
/ELF structure



/ELF exec w/link & libraries

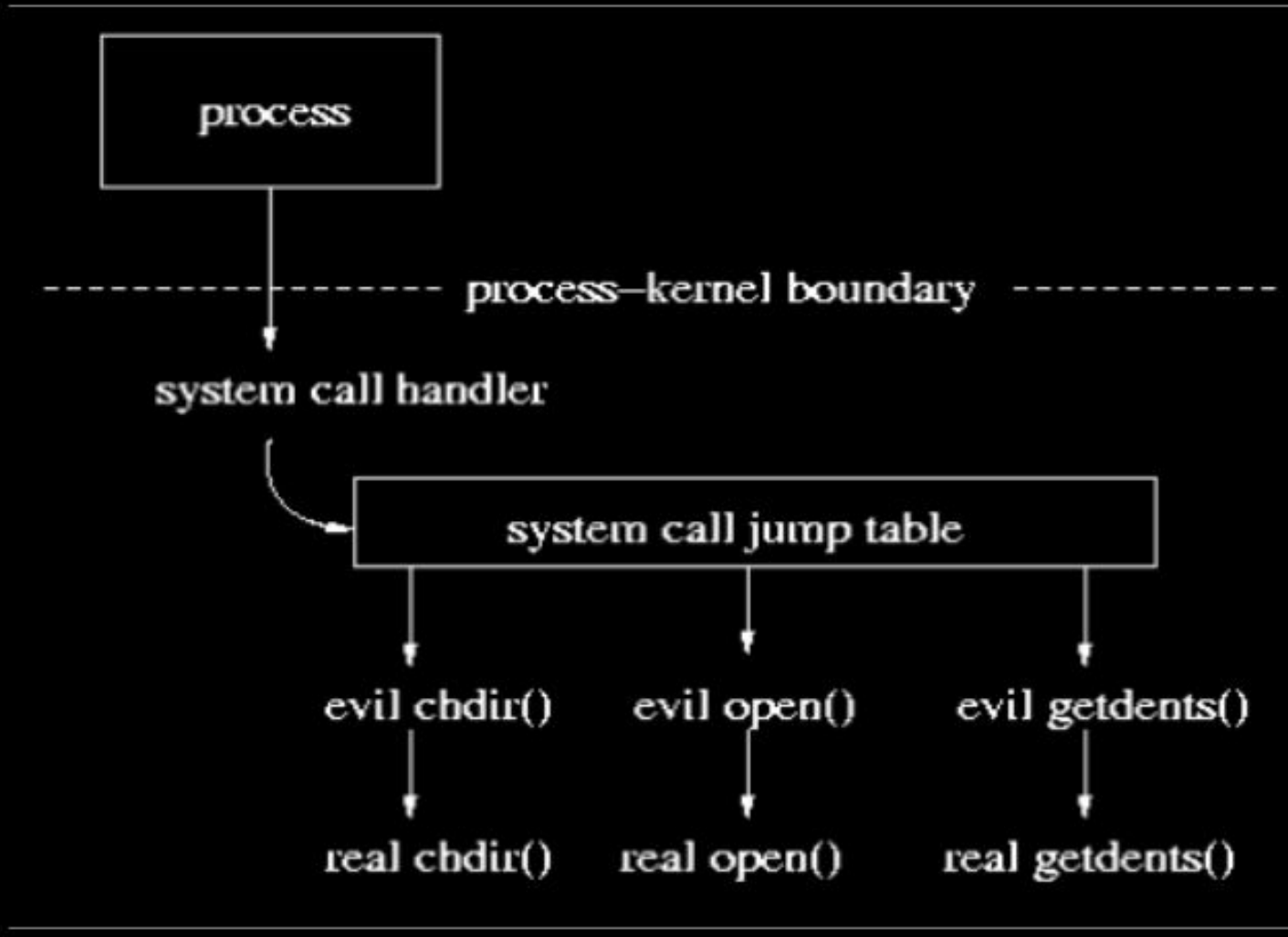


/ELF execution (mostly)

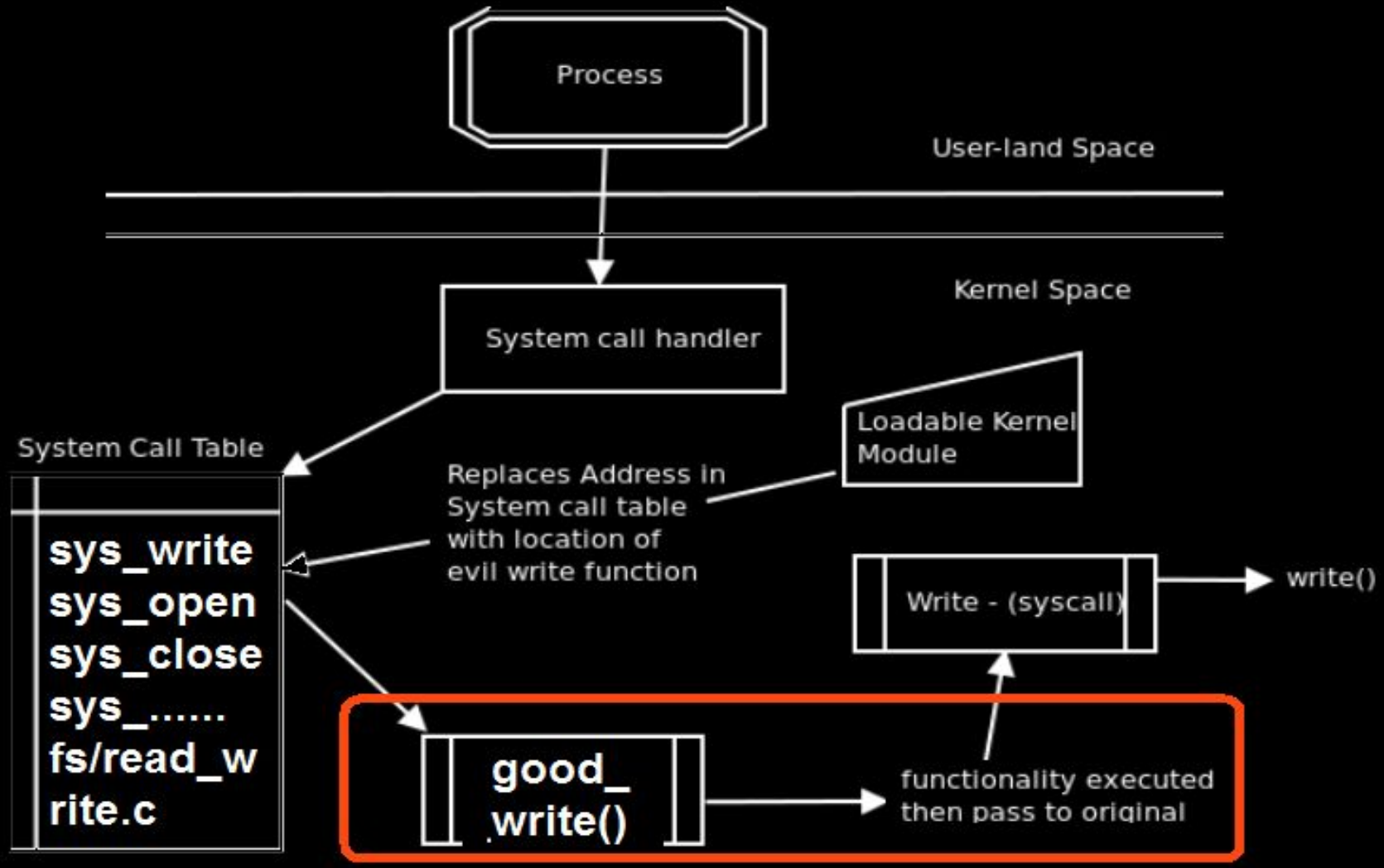


ref: nsa.gov/research/_files/selinux/
(modified by @unixfreaxjp for ELF malware research and education purpose

/bad ELF: module_intercept.ko



/good guys: kernel interception



/tools

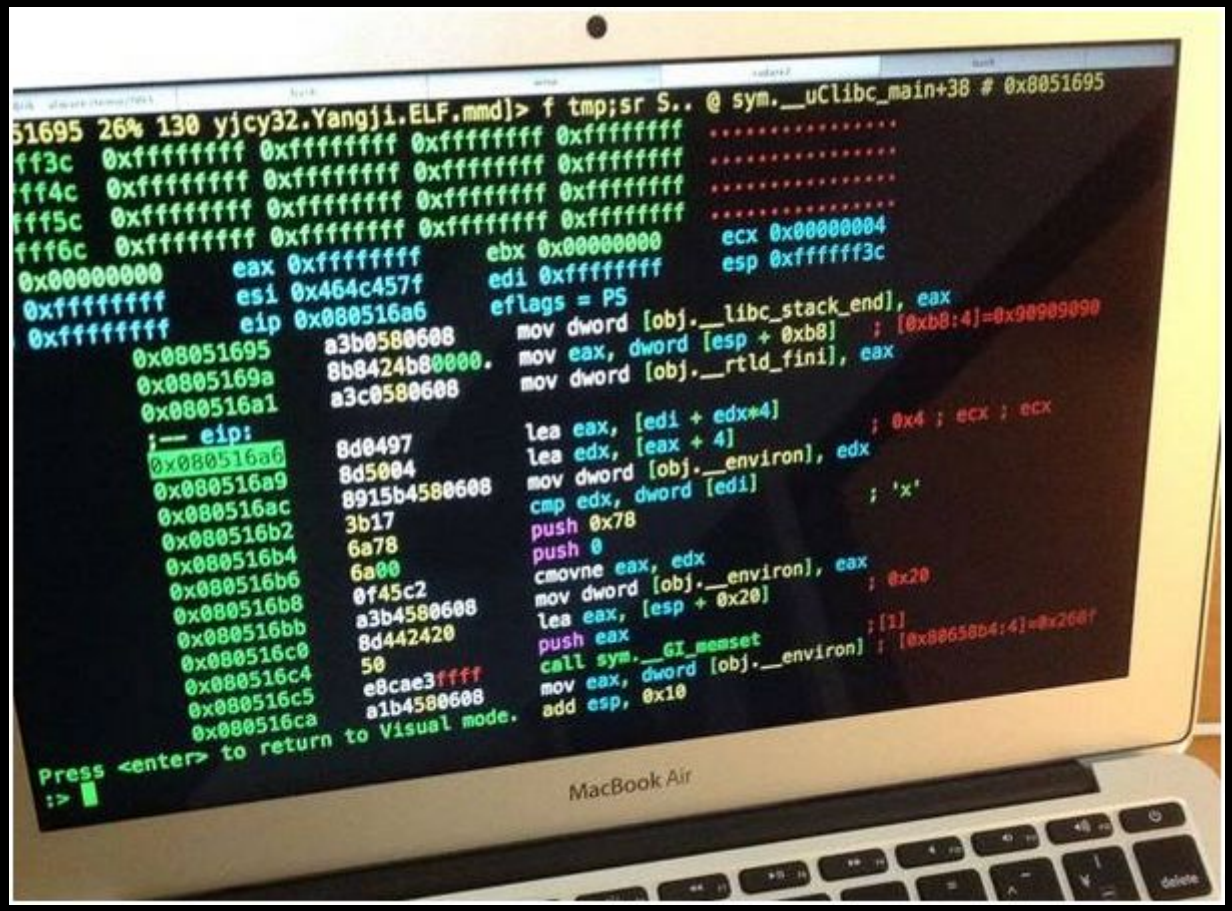
- readelf
- objdump
- gdb
- radare2 / IDA
- ptrace/ktrace/strace 何でもtrace
- emulators (disclosed in the workshop)
- kick em back toolset by: pots, traps, baits, lure..

/workshop

•START

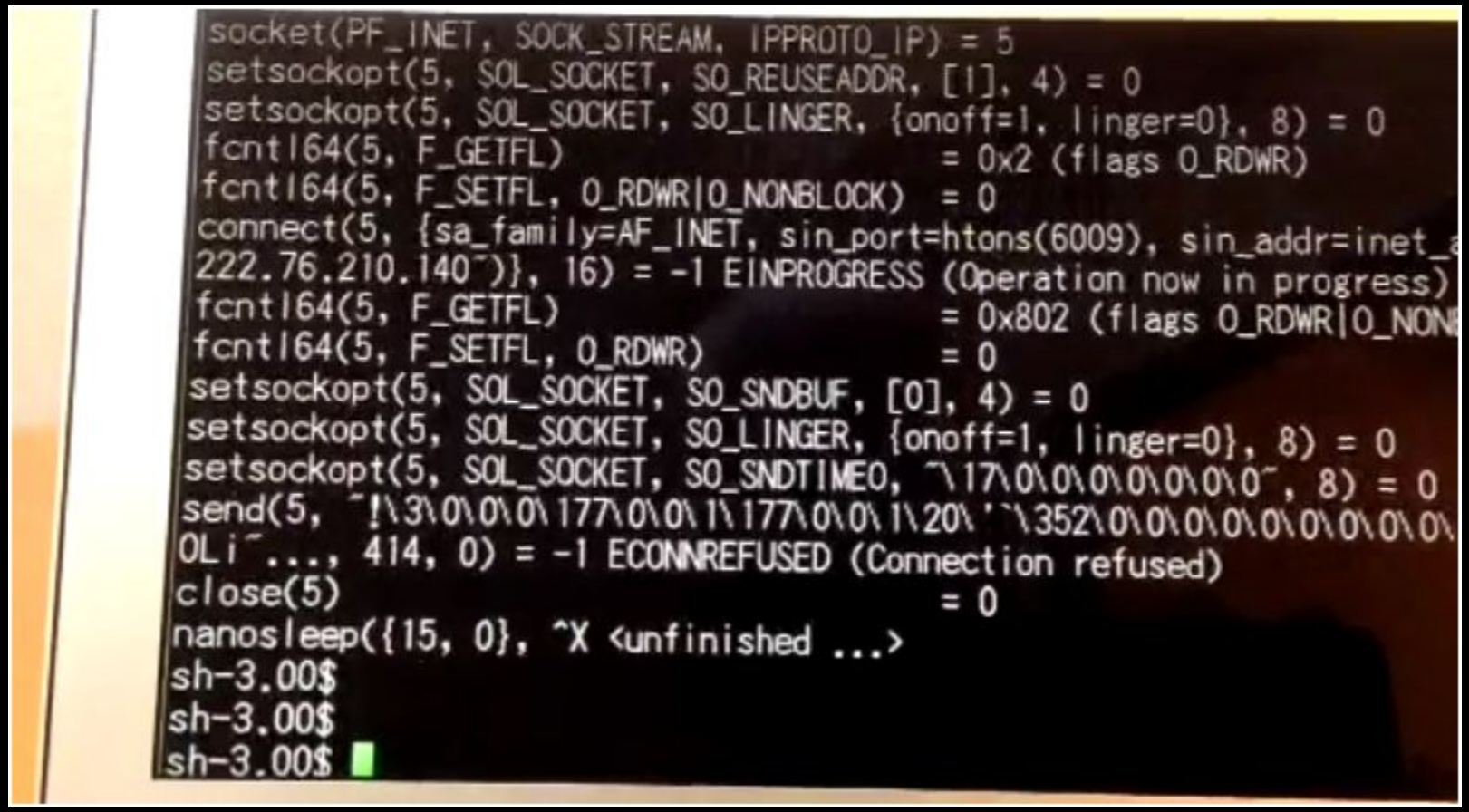
宜しくお願いします

/shell screenshots



static reverse vs dynamic reverse

/shell screenshots

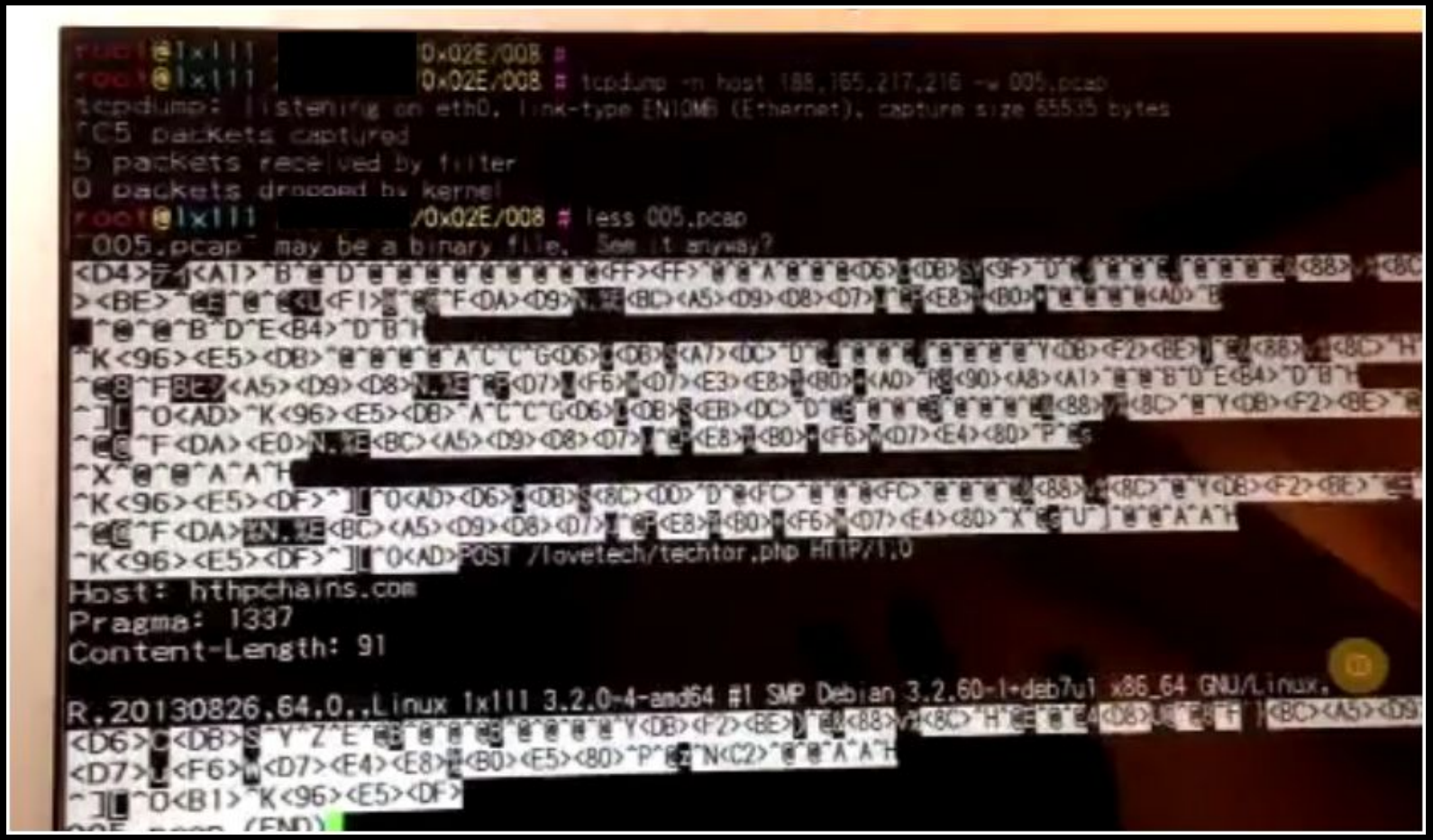


Debug the ELF malware

/shell screenshots

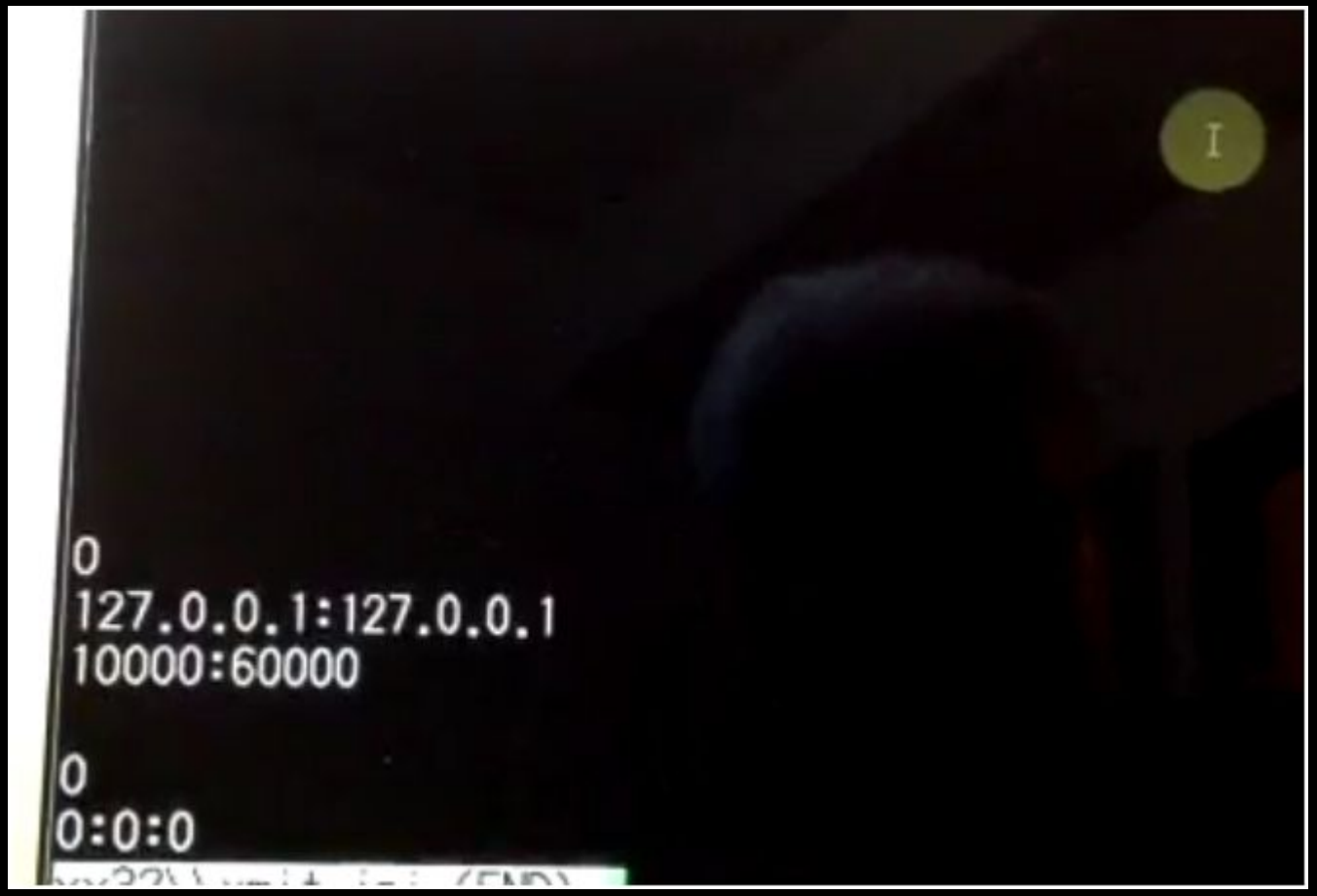
dissecting mayhem infections

/shell screenshots



cracking a CNC

/shell screenshots



dissecting malware config

/workshop momento

【ワークショップ】"Swimming in the sea of ELF"

1. 色んなELFマルウェアの作り方、普通のELFと違い、隠せる方法とよく使われているのトリック、を説明する。
2. ELFマルウェアバイナリーの調査やり方とツール紹介
   ・ツールの説明
   ・UNIX shellの上でELFのstatic vs dynamic調査連携方法
   ・そしてリバースエンジナリング vs debugging方法
   ・ELFファイルとメモリーforensics (Linux xBSD)
3. リアルケースELFマルウェア調査、仕組みTIPS/ヒント/トリック（デモ+説明）
   ・東ヨロッパ系ELFマルウェア：darkleech, mayhem,cDorkなど
   ・中国タイプELFマルウェア種類＋それぞれの種類の弱点
   ・skiddies系ELFマルウェア種類(なんでもIRC ddos)
4. ELF signatureアドバイサリー
   ・ClamAV
   ・Yara
   ・IOC
5. サンプルケース説明（いくつか0day.jpとmalwaremustdieリアルケース）
   ・発見仕方と調査流れの説明
   ・いくつ調査デモ
   ・調査目的/レポート
6. Q & A