APT : The Raise of

Cyber Crime

Let’s go

Niko, Andreas, Satria, Ramdhan & Agus.

#CyberSecurityMarathon2018

TABLE OF CONTENTS

01 ABOUT US

02 How A Criminal Might Infiltrate Your Network

03 Forensic Incident

04 Domesticate Malware

05 Hack Back

about us

Kami adalah kumpulan komunitas penggiat IT yang khususnya bergerak dibidang Security, yang ingin terus belajar & berbagi. Perkembangan ilmu dan teknologi mendorong kita untuk bersikap aktif dan inovatif.

LEARN MORE

Depok Cyber Security

How a Criminal Might Infiltrate Your Network

One of the great mysteries in security management is the modus operandi of criminal hackers. If you don’t know how they can attack you, how can you protect yourself from them? Prepare to be enlightened.

So? How criminal do it?

01 Time

02 Place

03 Mindset

At A Glance

Paths hackers can use to infiltrate networks
What patching and version states reveal
The dangers of elevated privileges

DEMO:
Penetrate the System

Digital Forensics

Find the bad guy!

Whoami?

- Known as вєтмєη / betmenwasdie
- Information Security Engineer, PT Noosc Global
- Penetration Tester, PT Xynexis International
- Research and Developer, DracOs Linux & GrombyangOS
- Active Contributor, Xfce4
- I was been a student, Binus & Budiluhur

Digital Crime is….

- Problematical
- Any crime where computer is a tool, target or both
- Offences against computer data or systems
- Unauthorized access, modification or impairment of a computer or digital system
- Offences against the confidentiality, integrity and availability of computer data and systems

Examples of Digital Crime

- Malicious Code
- Denial of Service
- Man in the Middle Attack
- Spam
- Phishing

Use Case

- SBY’s website hacked by Wildan aka MJL007 (2013)
- KPU’s website hacked by Dani Firmansyah aka Xnuxer (2014)
- Sultan Haikal vs Tiket[dot]com (2017)
- Ransomware “***WannaCry***” (2017)

What is Digital Forensics?

- Digital Forensics is the preservation, identification, extraction, interpretation, and documentation of computer evidence which can be used in the court of law.

Branches of Digital Forensics

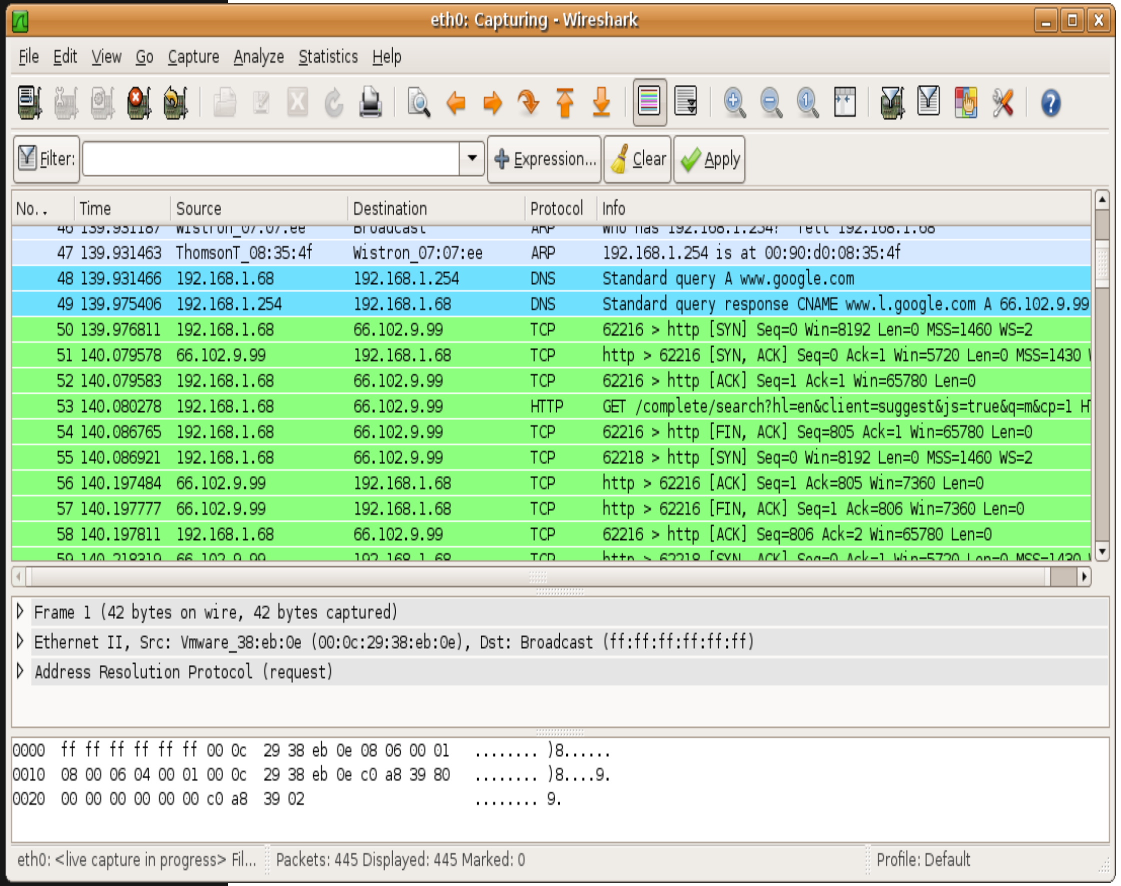
- Live Forensics
- Database Forensics
- Computer Forensics
- Network Forensics
- Mobile Forensics

Malware Forensics

Find the bad guy!

Tools in Used

- ➢ **Packet Capture and Analyzer**
- ➢ **Realtime Network Monitoring**


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

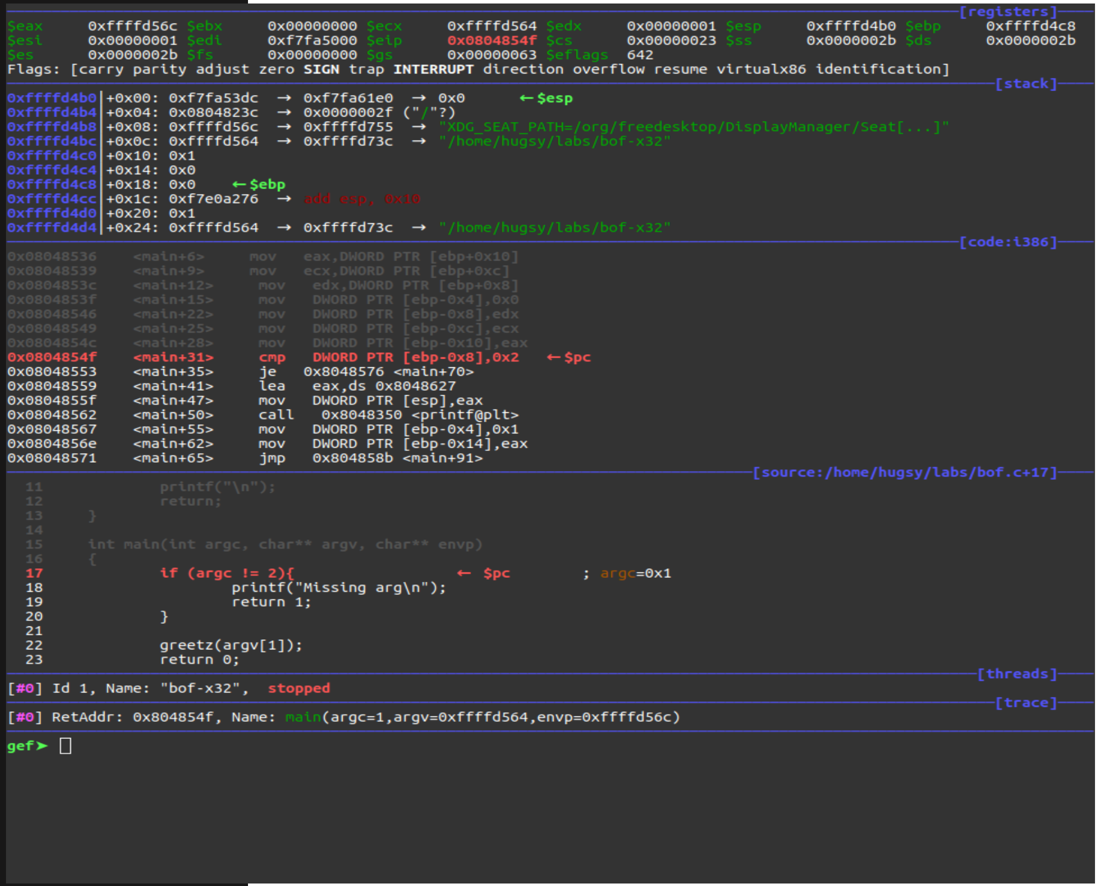
No.	Time	Source	Destination	Protocol	Info
46	139.931187	Wistron_07:07:ee	Broadcast	ARP	Who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.218319	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

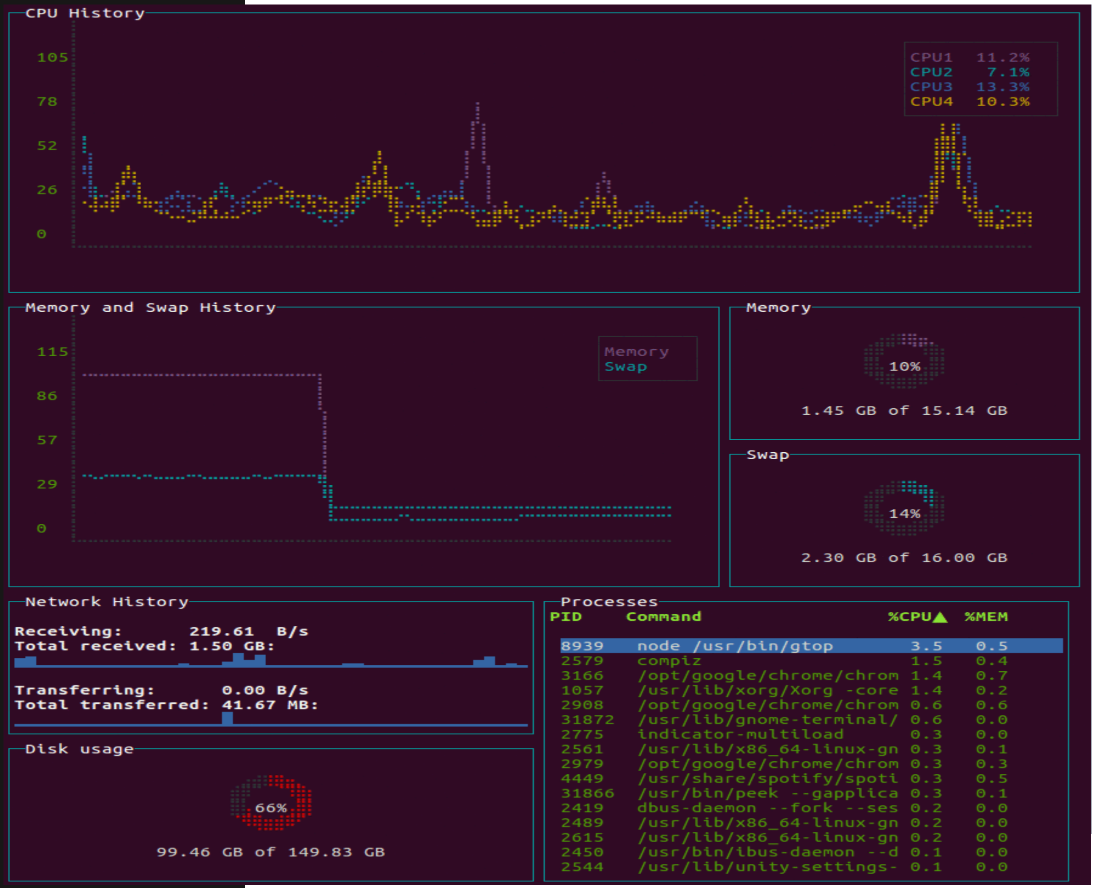
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

- ➢ **GDB (Gnu Debugger)**
- ➢ **Disassembler**



```
──────────────────────────────────────────────────────────────────────────────────────────────────────────[registers]──
$eax     0xffffd56c $ebx     0x00000000 $ecx     0xffffd564 $edx     0x00000001 $esp     0xffffd4b0 $ebp     0xffffd4c8
$esi     0x00000001 $edi     0xf7fa5000 $eip     0x0804854f $cs      0x00000023 $ss      0x0000002b $ds      0x0000002b
$es      0x0000002b $fs      0x00000000 $gs      0x00000063 $eflags  642
Flags: [carry parity adjust zero SIGN trap INTERRUPT direction overflow resume virtualx86 identification]
──────────────────────────────────────────────────────────────────────────────────────────────────────────────[stack]──
0xffffd4b0│+0x00: 0xf7fa53dc  →  0xf7fa61e0  →  0x0       ←$esp
0xffffd4b4│+0x04: 0x0804823c  →  0x0000002f ("/"?)
0xffffd4b8│+0x08: 0xffffd56c  →  0xffffd755  →  "XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat[...]"
0xffffd4bc│+0x0c: 0xffffd564  →  0xffffd73c  →  "/home/hugsy/labs/bof-x32"
0xffffd4c0│+0x10: 0x1
0xffffd4c4│+0x14: 0x0
0xffffd4c8│+0x18: 0x0     ←$ebp
0xffffd4cc│+0x1c: 0xf7e0a276  →  add esp, 0x10
0xffffd4d0│+0x20: 0x1
0xffffd4d4│+0x24: 0xffffd564  →  0xffffd73c  →  "/home/hugsy/labs/bof-x32"
─────────────────────────────────────────────────────────────────────────────────────────────────────────[code:i386]──
0x08048536     <main+6>      mov    eax,DWORD PTR [ebp+0x10]
0x08048539     <main+9>      mov    ecx,DWORD PTR [ebp+0xc]
0x0804853c     <main+12>      mov    edx,DWORD PTR [ebp+0x8]
0x0804853f     <main+15>      mov    DWORD PTR [ebp-0x4],0x0
0x08048546     <main+22>      mov    DWORD PTR [ebp-0x8],edx
0x08048549     <main+25>      mov    DWORD PTR [ebp-0xc],ecx
0x0804854c     <main+28>      mov    DWORD PTR [ebp-0x10],eax
0x0804854f     <main+31>      cmp    DWORD PTR [ebp-0x8],0x2    ←$pc
0x08048553     <main+35>      je     0x8048576 <main+70>
0x08048559     <main+41>      lea    eax,ds 0x8048627
0x0804855f     <main+47>      mov    DWORD PTR [esp],eax
0x08048562     <main+50>      call    0x8048350 <printf@plt>
0x08048567     <main+55>      mov    DWORD PTR [ebp-0x4],0x1
0x0804856e     <main+62>      mov    DWORD PTR [ebp-0x14],eax
0x08048571     <main+65>      jmp    0x804858b <main+91>
────────────────────────────────────────────────────────────────────────────────[source:/home/hugsy/labs/bof.c+17]──
  11                  printf("\n");
  12                  return;
  13          }
  14
  15          int main(int argc, char** argv, char** envp)
  16          {
  17                  if (argc != 2){                  ← $pc        ; argc=0x1
  18                          printf("Missing arg\n");
  19                          return 1;
  20                  }
  21
  22                  greetz(argv[1]);
  23                  return 0;
────────────────────────────────────────────────────────────────────────────────────────────────────────────[threads]──
[#0] Id 1, Name: "bof-x32",  stopped
──────────────────────────────────────────────────────────────────────────────────────────────────────────────[trace]──
[#0] RetAddr: 0x804854f, Name: main(argc=1,argv=0xffffd564,envp=0xffffd56c)
───────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
gef➤ 
```

- ➢ **Application Resources Monitor**
- ➢ **CPU Usage Monitor**
- ➢ **Memory Usage Monitor**



```
1.45 GB of 15.14 GB

2.30 GB of 16.00 GB

Receiving:        219.61  B/s
Total received: 1.50 GB:

Transferring:          0.00 B/s
Total transferred: 41.67 MB:

99.46 GB of 149.83 GB

Processes
PID    Command                    %CPU▲  %MEM

8939   node /usr/bin/gtop          3.5    0.5
2579   compiz                      1.5    0.4
3166   /opt/google/chrome/chrom 1.4    0.7
1057   /usr/lib/xorg/Xorg -core 1.4    0.2
2908   /opt/google/chrome/chrom 0.6    0.6
31872  /usr/lib/gnome-terminal/ 0.6    0.0
2775   indicator-multiload         0.3    0.0
2561   /usr/lib/x86_64-linux-gn 0.3    0.1
2979   /opt/google/chrome/chrom 0.3    0.3
4449   /usr/share/spotify/spoti 0.3    0.5
31866  /usr/bin/peek --gapplica 0.3    0.1
2419   dbus-daemon --fork --ses 0.2    0.0
2489   /usr/lib/x86_64-linux-gn 0.2    0.0
2615   /usr/lib/x86_64-linux-gn 0.2    0.0
2450   /usr/bin/ibus-daemon --d 0.1    0.0
2544   /usr/lib/unity-settings- 0.1    0.0
```

DEMO:
Digital Forensic Analysis

APP
sinarmas

Reversing.ID

Domesticate Malware

Taming the Beast to the Deepest Part of Operating System

Why Crafting a Malware?

FINANCIAL GAIN

Stealing resource: money, bank account, credit card, cryptocurrency

NATIONAL SECURITY

1. A surveillance to citizens
2. Sabotage other country

PROTECT INTEREST

Protect certain content from modification or disadvantage

How to be Infected

- Spam or phishing emails containing attached files.
- Infected removable drives
- Bundled with other software
- Visiting any compromised or infected websites.
- Old and unpatched systems
- Downloading software, especially illegal one, from untrusted source.

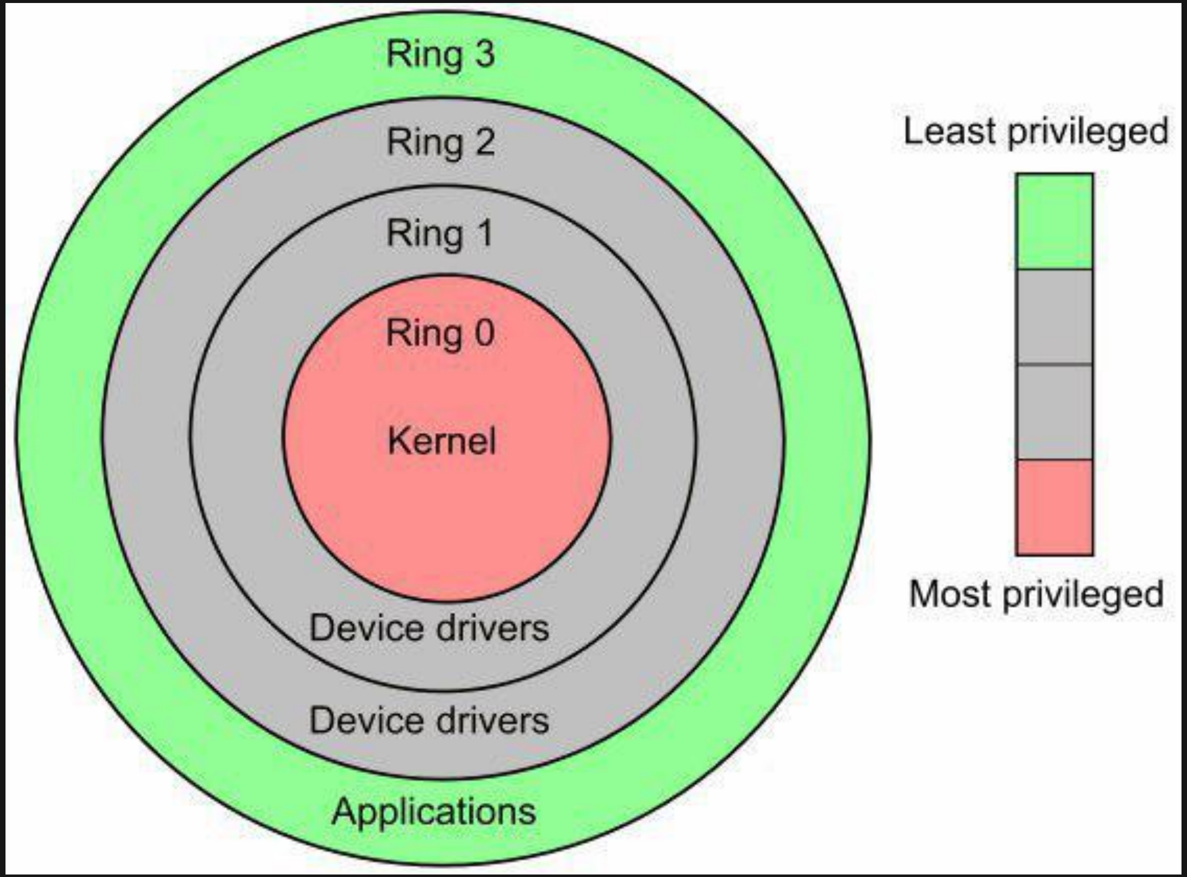
Linux Rootkit Kernel Module

Level Rootkit

01 **User mode rootkit**

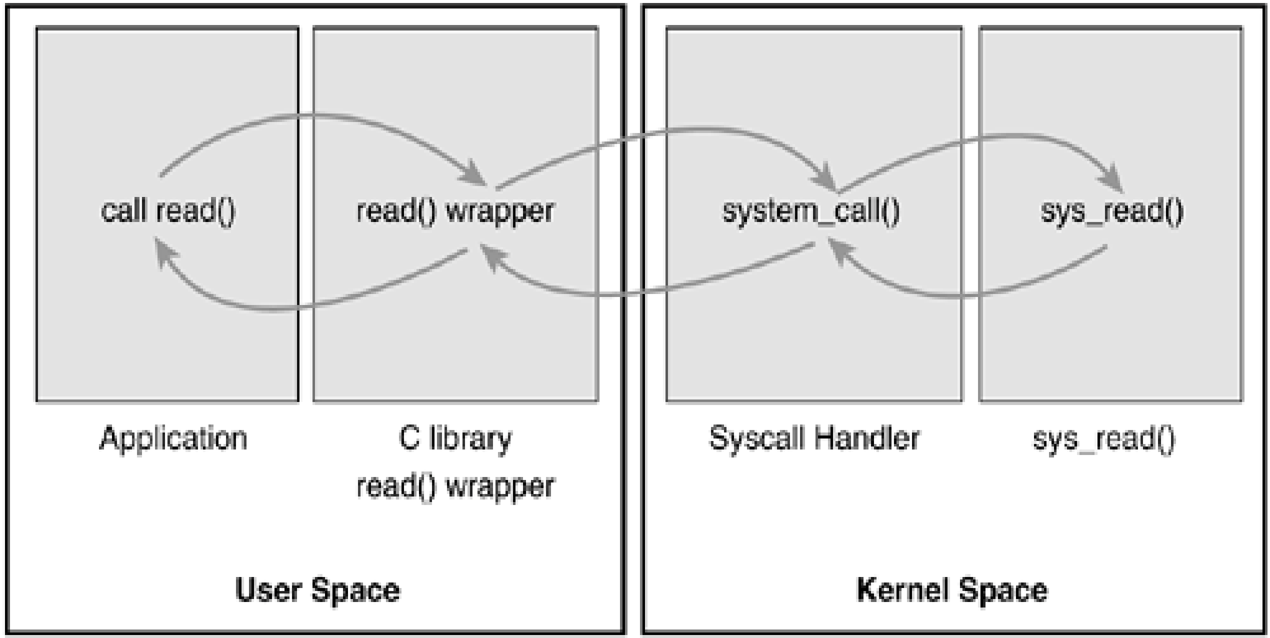
02 **Kernel mode rootkit**

Kernel mode (ring0)

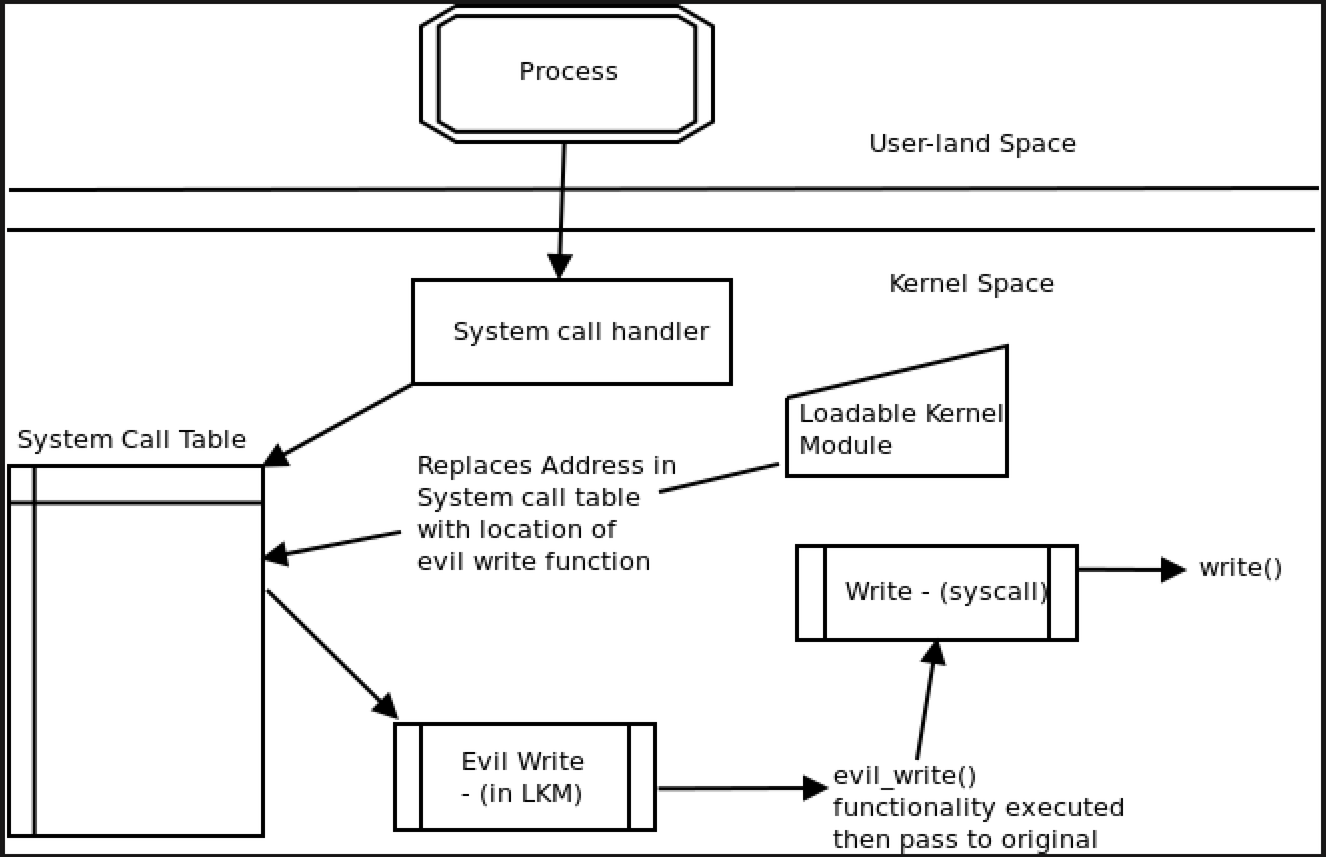


Linux Kernel Module

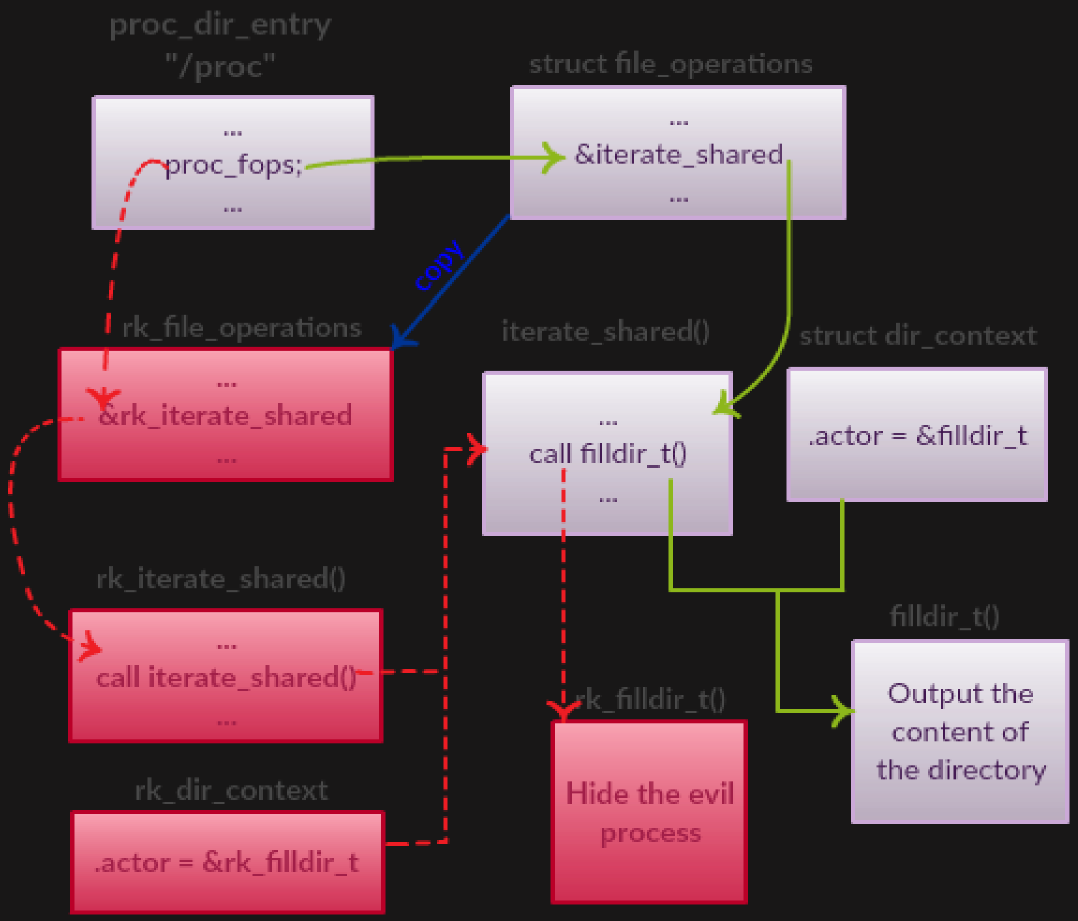
Syscall Hijack



Syscall Hijack



VFS Hijack


proc_dir_entry
"/proc"
...
proc_fops;
...
struct file_operations
...
&iterate_shared
...
copy
rk_file_operations
...
&rk_iterate_shared
...
iterate_shared()
...
call filldir_t()
...
struct dir_context
.actor = &filldir_t
rk_iterate_shared()
...
call iterate_shared()
...
filldir_t()
Output the content of the directory
rk_filldir_t()
Hide the evil process
rk_dir_context
.actor = &rk_filldir_t

Legitimate course of action
What happens during hijacking

Rootkit gain access root

```
get_root() {
                commit_creds(prepare_kernel_creds(0));
                return;
}
```

D E M O: Rootkit Reverse Engineering

TRIPLE ONE
GLOBAL

IndoXploit

OUR HINT SO FAR

IP Attacker

Protocol

C&C Command

DEMO:
Time for Revenge

Bonafidz
STUDIO

id
cloudhost