Introducción a la cyberseguridad

Pentest / Retro-Ingeniería / RCE (ejecución de código a distancia)

Martin Tourneboeuf

April 13, 2021

ALMA: Atacama Large Millimeter/submillimeter Array

Contenido

Indice

Contenido

Indice

1. Paisaje cyber-seguridad
2. Buscar vulnerabilidades
3. Explotar vulnerabilidades

Descargo

Esta presentacion **no** es sobre:

Criminales

- Ver **Metasploit**: CLI

Antivirus

- Ver **Yara**: signaturas (estatico)
- Ver comportamental: serie de tiempo de io (dynamico)
- Protegen solo de ataques conocidos

Chronologia: Cyber, el terreno digital

Fecha	Terreno	Ejemplo	Lugar
-8000	Tierra	masa, baston	Africa, China
-2200	Mar	botes de papiro	Egipto
1911	Aire	avión de hélice	Francía
1957	Espacio	satélite espía	Russia, USA
2011	**Cyber**	gusano informático	Bielorrusia

StuxNet: aputa los sistemas SCADA, particularmente en el sector nuclear: (Israel + Usa -> Irán), 4 zero-day

Seguridad: humanos Vs humanos

	Safety	**Security**
Adversario	**Natural**	**Humano**
Definicion	Incontrolado / **aleatorio**	Un culpable **malicioso**
Herramienta	Guantes, Chaleco salvavidas	Cerradura, Cuenta en el extranjero
Digital	Linter, Tests, Watcher, Log	Review, Fuzz, Watcher, Reverse

Un terreno Asymetrico

Securidad

Attaquantes	Defensores
ratas	leviathan
5 ladrones	10.000 vecinos
1 virus	10e10 globulos blancos

Cyber

- **Nuevo terreno**, **barato**, al que llega primero **reclama**
- Se puede **apuntar lejos**
- Se puede **esconder**
- La **copia es gratis** => Se puede crecer rapido,

El attaquante puede probar su cargar sobre los AV => esta adelantado

El defensor debe comprobar que **toda** las entredas son segura

Mapa del los actores

- !!! Tu !!!
- Antivirus (servicios de seguridad)
- Empresa (admin sys ! no son cyberdefensores)
- Estado (cuida computadores mas essenciales que los tuyos, basicamente los suyos)

Vea aquí: el mapeo de los actores estatales del cyber en francía

Chile, Francia, USA, Japan

Diplomatie

Que es una vulnerabilidad informatica ?

Lo que permite

que un programa haga

algo que sus usarios no habian contemplado

Que es una vulnerabilidad informatica ?

Lo que permite

que un programa haga

algo que sus usarios no habian contemplado

"Un cyber-ataque se hace mediante la explotación de una vulnerabilidad"

Si es explotable pasamos de la safety a la security

Algunas vulnerabilidades conocidas

- **Indefinido:** comportamiento (spec)
- **Tipo:** confusión
  - imediato | pointer
  - con signo | sin signo
- **Entero:** Desbordamiento de enteros
- **Limite:** Fuera (out-of-bound)
- **Dato:** corupto o mal normalisado: Sql, Regex, Unicode
- **Característica:** secreta

Cyclo V: del pentest a la retroingeneria

El pentest, para ser realista, contempla:

0. (**Analisys** de riesgo: quien es el atacante)
1. **Anonimisación**
2. **Reconocimiento** de la superficie de exposición (alias: superficie de ataque) ex: puertos abiertos
3. **Retro-ingeneria** (analisys en laboratorio)
4. **Pruebas**
5. **Explotacion** (producion)
6. **Instalación** (persistir, esconderse, communicar, explorar, reproducirse, ...)

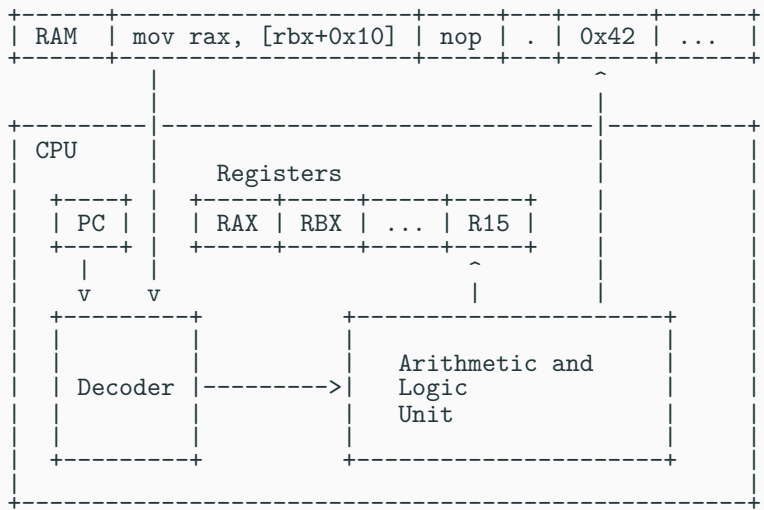
Es solo question de tiempo para cada etapa del ciclo en V

Demo: buscar vulnerabilidades

Shell, Firefox, Fuzz, IDA, Gdb

- El Fuzz (dynamic):
  - + puede usar el codigo como caja negra (barato)
  - − no encuentra todo
  - − encuentra siempre lo mismo: falta diversidad, 2 no valen mas que 1
- No olvides de donde vienes,
- Hypothesis, validacion y sus ventajas (yes no question)
- Si podia ejecutar codigo y ahora puedo ejecutar codigo, no gane nada !

Demo: Diagrama de un CPU



ROP: Return-oriented programming

Un tipo de baile en la RAM

Ver la emboscada 1999 (Sean Connery, Catherine Zeta-Jones)

Mitigation (Hagan la lista en casa)

- **Canary:** Stack-Cookie
- **DEP:** Data Exceution Prevention (NX for Linux)
- **ASLR:** Address space layout randomization
- **CFI:** Control Flow Integrity
- Higher levels: backup, isolation, trap

Y Alma ? Preguntas para el nuevo equipo de cyberdefensores

0. Attacantes potenciales, la carga final asociada
1. Superficie de exposición (servidores **y** servicios)
2. Como el atacante comunicara, se escondera, se anonimisara ...
3. Quien o que lo detectara
4. Hasta donde puede herir la empresa (ver mitigaciones)

Ver pentest@wikipedia

Links

- Intel software developer manual
- Simple CPU

Optimisaciones

```
                public print_all_points
print_all_points proc near               ; DATA XREF: LOAD
                endbr64
                push    rbp
                mov     rbp, rsp
                sub     rsp, 10h
                mov     [rbp-8], rdi
                mov     rax, [rbp-8]
                mov     rdi, rax
                call    internal_print_all_points
                leave
                retn
print_all_points endp
```

Figure 1: Debug

```
print_all_points proc near               ; DATA XREF: LOAD:0000000000000AD0↑o
                endbr64
                jmp     internal_print_all_points

print_all_points endp
```

Figure 2: Release

Calling conventions Intel 64 bits

N	Windows	Linux
1	RCX	RDI
2	RDX	RSI
3	R8	RDX
4	R9	RCX
5	[rsp+8]	R8
6	[rsp+10]	R9