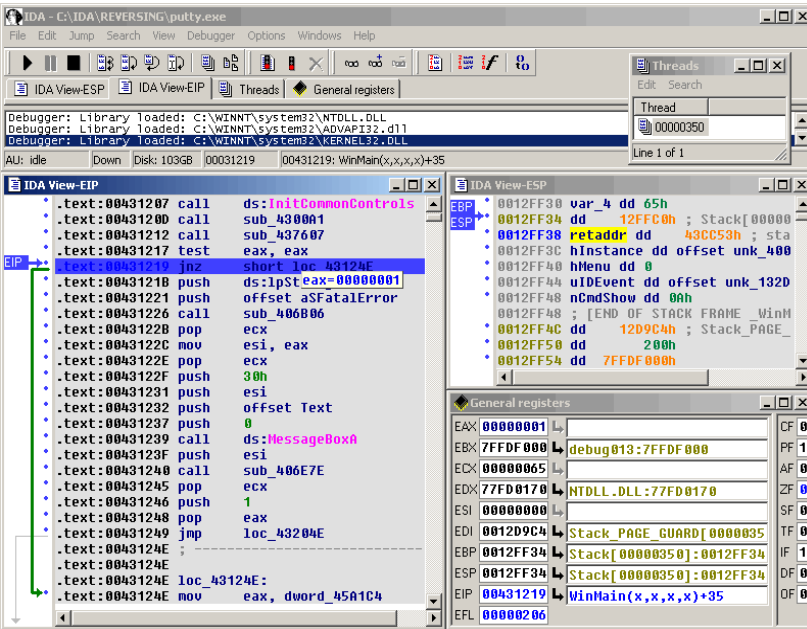




Vulnerabilidades de Software

Marcos Flávio Araújo Assunção
Fundamentos de Ethical Hacking

Tipos de falhas

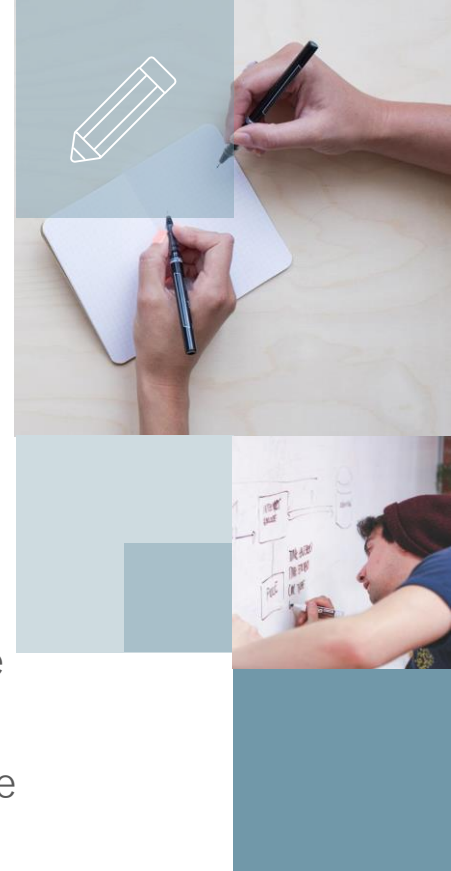


The screenshot shows the IDA Pro interface with the following components:

- Debugger:** Library loaded: C:\WINNT\system32\NTDLL.DLL, C:\WINNT\system32\ADVAPI32.dll, C:\WINNT\system32\KERNEL32.DLL
- General registers:** EAX: 00000001, EBX: 7FFDF000, ECX: 00000065, EDI: 77FD0170, ESI: 00000000, EDI: 0012D9C4, EBP: 0012FF34, ESP: 0012FF34, EIP: 00431219, EFL: 00000206
- Assembly code:**

```
.text:00431207 call ds:InitCommonControls
.text:0043120B call sub_4300A1
.text:00431212 call sub_437607
.text:00431217 test eax, eax
.text:00431219 jnz short loc_43124E
.text:0043121B push ds:ipSteax=00000001
.text:00431221 push offset a$FatalError
.text:00431226 call sub_406B06
.text:0043122B pop ecx
.text:0043122C mov esi, eax
.text:0043122E pop ecx
.text:00431230 push 30h
.text:00431231 push esi
.text:00431232 push offset Text
.text:00431237 push 0
.text:00431239 call ds:MessageBoxA
.text:0043123F push esi
.text:00431240 call sub_406E7E
.text:00431245 pop ecx
.text:00431246 push 1
.text:00431248 pop eax
.text:00431249 jmp loc_43204E
.text:0043124E loc_43124E:
.text:0043124E mov eax, dword_45A1C4
```

- As vulnerabilidades mais comuns encontradas em softwares são: Stack overflow, Heap overflow, String format, Heap spraying e Race Conditions
- Normalmente um debugger é utilizado para encontrar o “ponto falho” de um software
- Fuzzing é o nome dado à técnica de testar a entrada de dados de um software enviando seqüências aleatórias



Objetivos da exploração de **falhas**

Normalmente um atacante irá explorar uma falha remota para invadir um sistema e logo depois tentará a elevação de privilégios. O motivo para isto é que a maioria dos serviços hoje rodam no perfil de usuários com poucos privilégios como o nobody/guest.

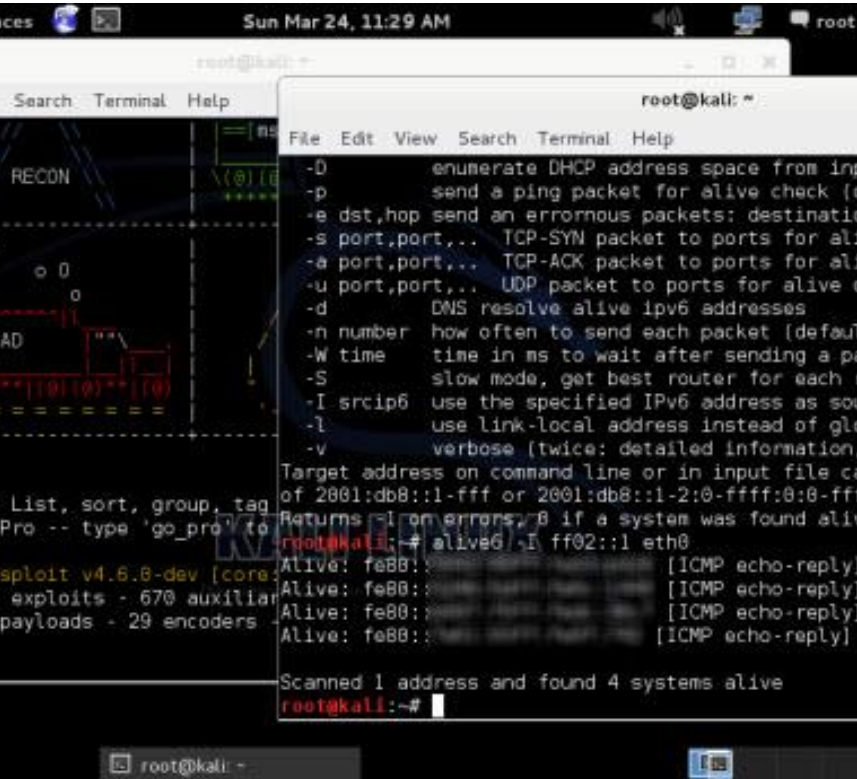
Falhas remotas

Ganhar acesso não autorizado ao sistema alvo (normalmente ao shell) ou causar Denial of Service

Falhas locais

Elevar os privilégios de acesso para root/system ou causar Denial of Service

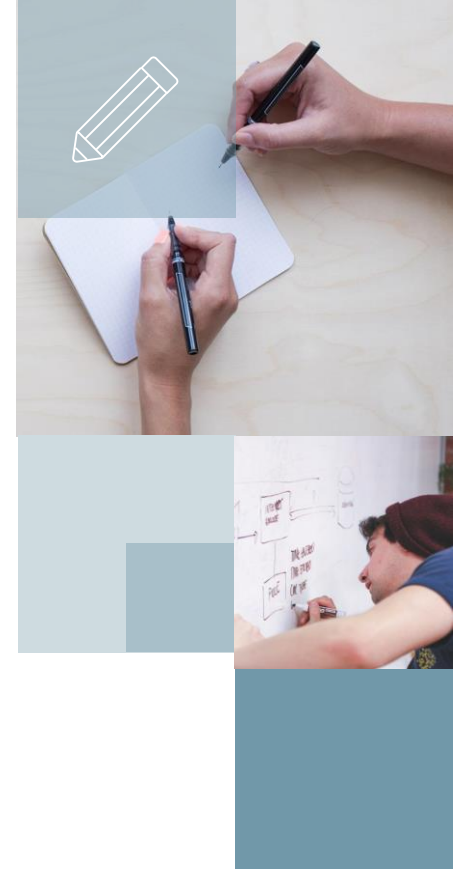




```
root@kali: ~  
File Edit View Search Terminal Help  
-D enumerate DHCP address space from input file  
-p send a ping packet for alive check (default)  
-e dst,hop send an erroneous packets: destination  
-s port,port,... TCP-SYN packet to ports for alive check  
-a port,port,... TCP-ACK packet to ports for alive check  
-u port,port,... UDP packet to ports for alive check  
-d DNS resolve alive ipv6 addresses  
-n number how often to send each packet (default: 1)  
-W time time in ms to wait after sending a packet  
-S slow mode, get best router for each route  
-I srcip6 use the specified IPv6 address as source  
-l use link-local address instead of global  
-v verbose (twice: detailed information, three: full packet details)  
Target address on command line or in input file can be:  
of 2001:db8::1-fff or 2001:db8::1-2:0-ffff:0:0-ffff  
Returns -1 on errors, 0 if a system was found alive  
root@kali: ~# nmap -sP 2001:db8::1-ffff:0:0-ffff  
Nmap scan report for 2001:db8::1  
Host is up (0.0000s latency).  
Not shown: 65535 ports filtered  
2001:db8::1: [ICMP echo-reply] (0.0000s latency)  
2001:db8::1: [ICMP echo-reply] (0.0000s latency)  
2001:db8::1: [ICMP echo-reply] (0.0000s latency)  
2001:db8::1: [ICMP echo-reply] (0.0000s latency)  
Scanned 1 address and found 4 systems alive  
root@kali: ~#
```

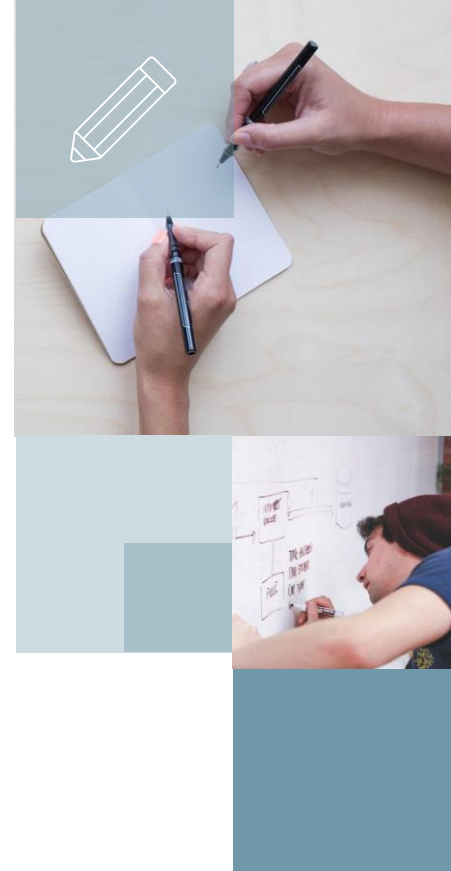
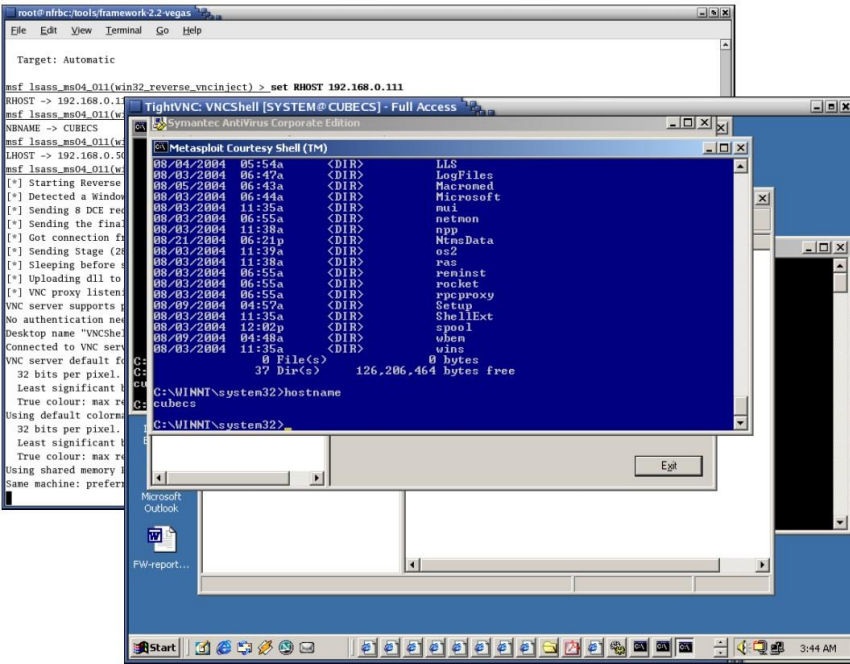
Distribuições próprias para **Penetration Test** que trazem coleções de exploits

- Kali Linux
- ArchAssault
- BackBox
- BlackArch Linux
- Knoppix STD
- Pentoo
- Parrot
- Samurai Web Testing Framework
- Matriux Krypton
- NodeZero



Exploits e Payloads

- Um Exploit é um software ou script que explora uma falha e injeta um payload
- Payload é o código que será executado na memória do Sistema comprometido
- Existem vários tipos de payloads: shell, vnc, meterpreter, etc.
- Frameworks de exploits são kits que facilitam o desenvolvimento e uso de exploits e payloads



Frameworks de Exploits

