Assembly para Pentesters

Assembly: Syntax Intel vs AT&T

Existem duas sintaxes diferentes para programar em assembly (Intel ou AT&T).

Vamos destacar algumas diferenças entre elas:

Na AT&T sempre usamos % para registradores e $ para números e podemos definir o tamanho com Q = 8 bytes | W = 2 bytes e B = 1 byte

No curso vamos trabalhar somente com a sintaxe Intel

Exemplo de Instruções

MOV	Move
ADD	Adiciona
SUB	Subtrai
INC	Incrementa
DEC	Decrementa
CALL	Chama
JMP	Salta
JNE	Salta se não for igual
CMP	Compara

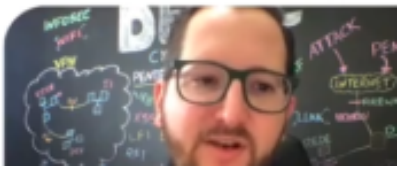
```
MOV EBX, 0x74e89010
CALL EBX
```

PUSH	Coloca na stack (topo)
POP	Retira da stack (topo)
NOP	No Operation (\x90)
INT3	Interrupção (breakpoint)
XOR	Instruções lógicas

```
MOV EAX, [ESP]
ADD ESP, 4
POP EAX
PUSH 41424344h
```

EXEMPLOS:

```
SUB ESP, 4
MOV [ESP], ABCD
XOR EAX, EAX
```



Instruções para Instalação das Ferramentas Necessárias

- Immunity Debugger
- Dev-C++
- outros...