

INSTITUTO TECNOLÓGICO DE SAN JUAN DEL RÍO



Tópicos de Ciberseguridad

P R E S E N T A:

Equipo Ladrillo

INGENIERÍA EN SISTEMAS COMPUTACIONALES

00401010	EB 59	jmp hackame.401068	
00401012	90	nop	
00401013	90	nop	
00401014	90	nop	
00401015	90	nop	
00401016	B8 0D204000	mov eax,hackame.40200D	
00401018	50	push eax	
0040101C	E8 27020000	call <JMP.&printf>	
00401021	83C4 04	add esp,4	
00401024	B8 01000000	mov eax,1	
00401029	E9 63000000	jmp hackame.401091	
0040102E	8B45 0C	mov eax,dword ptr ss:[ebp+c]	
00401031	83C0 04	add eax,4	
00401034	B9 04204000	mov ecx,hackame.402004	402004:"34309812"
00401039	51	push ecx	
0040103A	8B08	mov ecx,dword ptr ds:[eax]	
0040103C	51	push ecx	
0040103D	E8 0E020000	call <JMP.&strcmp>	
00401042	83C4 08	add esp,8	
00401045	83F8 00	cmp eax,0	
00401048	0F85 0B000000	jne hackame.401059	
0040104E	B8 C8000000	mov eax,C8	
00401053	8905 00204000	mov dword ptr ds:[402000],eax	
00401059	8B05 00204000	mov eax,dword ptr ds:[402000]	
0040105F	81F8 C8000000	cmp eax,C8	
00401065	0F85 13000000	jne hackame.40107E	
00401068	B8 29204000	mov eax,hackame.402029	402029:"Acceso Concedido"
00401070	50	push eax	

En x96dbg cambiamos ese salto hasta donde dice acceso concedido, y listo