Report for pwn1 at 2024-05-15

Summary

Enumeration

Binary Information

File Name	Path	Format	Bit
pwn1	app/testFile/pwn1	ELF	32-bit

Security of the Binary

Basic Security Features			
Linked	**Stripped**	**RELRO**	**Canary**
dynamically linked	no	full	no

Advanced Security Mechanisms		
NX	**PIE**	**RPath**
yes	yes	no

Security Meta-Information		
RunPath	**Symbols**	**Fortify Source**
no	yes	no

Strings

- Stop! Who would cross the Bridge of Death must answer me these questions three, ere the other side he see.
- What... is your name?
- .note.gnu.build-id

Vulnerable Functions

- gets

Libraries

- linux-gate.so.1
- libc.so.6
- /lib/ld-linux.so.2

Assembly Code

```
assembly
xor ebp, ebp
pop esi
mov ecx, esp
and esp, 0xfffffff0
push eax
push esp
push edx
call 0x5f2
add ebx, 0x19e0
lea eax, [ebx - 0x1660]
push eax
lea eax, [ebx - 0x16c0]
push eax
push ecx
push esi
push dword ptr [ebx + 0x48]
call 0x570
hlt
mov ebx, dword ptr [esp]
ret
nop
nop
nop
nop
nop
mov ebx, dword ptr [esp]
ret
nop
nop
```

```
nop
nop
nop
nop
call 0x6f9
add edx, 0x199b
lea ecx, [edx + 0x58]
lea eax, [edx + 0x58]
cmp eax, ecx
je 0x648
mov eax, dword ptr [edx + 0x34]
test eax, eax
je 0x648
push ebp
mov ebp, esp
sub esp, 0x14
push ecx
call eax
add esp, 0x10
leave
ret
nop
lea esi, [esi]
repz ret
lea esi, [esi]
call 0x6f9
add edx, 0x195b
push ebp
lea ecx, [edx + 0x58]
lea eax, [edx + 0x58]
sub eax, ecx
mov ebp, esp
push ebx
sar eax, 2
mov ebx, eax
sub esp, 4
shr ebx, 0x1f
```

```
add eax, ebx
sar eax, 1
je 0x692
mov edx, dword ptr [edx + 0x4c]
test edx, edx
je 0x692
sub esp, 8
push eax
push ecx
call edx
add esp, 0x10
mov ebx, dword ptr [ebp - 4]
leave
ret
mov esi, esi
lea edi, [edi]
push ebp
mov ebp, esp
push ebx
call 0x600
add ebx, 0x1907
sub esp, 4
cmp byte ptr [ebx + 0x58], 0
jne 0x6e2
mov eax, dword ptr [ebx + 0x38]
test eax, eax
je 0x6d6
sub esp, 0xc
push dword ptr [ebx + 0x54]
call 0x5b0
add esp, 0x10
call 0x610
mov byte ptr [ebx + 0x58], 1
mov ebx, dword ptr [ebp - 4]
leave
ret
mov esi, esi
```

```
lea edi, [edi]
push ebp
mov ebp, esp
pop ebp
jmp 0x650
mov edx, dword ptr [esp]
ret
push ebp
mov ebp, esp
push ebx
sub esp, 0x14
call 0x600
add ebx, 0x18a7
sub esp, 0xc
lea eax, [ebx - 0x1640]
push eax
call 0x550
add esp, 0x10
sub esp, 8
lea eax, [ebx - 0x162d]
push eax
lea eax, [ebx - 0x162b]
push eax
call 0x590
add esp, 0x10
mov dword ptr [ebp - 0xc], eax
jmp 0x74f
movsx eax, byte ptr [ebp - 0xd]
sub esp, 0xc
push eax
call 0x5a0
add esp, 0x10
sub esp, 0xc
push dword ptr [ebp - 0xc]
call 0x540
add esp, 0x10
mov byte ptr [ebp - 0xd], al
```

```
cmp byte ptr [ebp - 0xd], 0xff
jne 0x73f
sub esp, 0xc
push 0xa
call 0x5a0
add esp, 0x10
nop
mov ebx, dword ptr [ebp - 4]
leave
ret
lea ecx, [esp + 4]
and esp, 0xfffffff0
push dword ptr [ecx - 4]
push ebp
mov ebp, esp
push ebx
push ecx
sub esp, 0x40
call 0x600
add ebx, 0x1820
mov eax, dword ptr [ebx + 0x44]
mov eax, dword ptr [eax]
push 0
push 0
push 2
push eax
call 0x580
add esp, 0x10
mov dword ptr [ebp - 0xc], 2
mov dword ptr [ebp - 0x10], 0
sub esp, 0xc
lea eax, [ebx - 0x1620]
push eax
call 0x550
add esp, 0x10
sub esp, 0xc
lea eax, [ebx - 0x15b5]
```

```
push eax
call 0x550
add esp, 0x10
mov eax, dword ptr [ebx + 0x40]
mov eax, dword ptr [eax]
sub esp, 4
push eax
push 0x2b
lea eax, [ebp - 0x3b]
push eax
call 0x530
add esp, 0x10
sub esp, 8
lea eax, [ebx - 0x159f]
push eax
lea eax, [ebp - 0x3b]
push eax
call 0x510
add esp, 0x10
test eax, eax
je 0x82f
sub esp, 0xc
lea eax, [ebx - 0x1584]
push eax
call 0x550
add esp, 0x10
sub esp, 0xc
push 0
call 0x560
sub esp, 0xc
lea eax, [ebx - 0x1564]
push eax
call 0x550
add esp, 0x10
mov eax, dword ptr [ebx + 0x40]
mov eax, dword ptr [eax]
sub esp, 4
```

```
push eax
push 0x2b
lea eax, [ebp - 0x3b]
push eax
call 0x530
add esp, 0x10
sub esp, 8
lea eax, [ebx - 0x154d]
push eax
lea eax, [ebp - 0x3b]
push eax
call 0x510
add esp, 0x10
test eax, eax
je 0x891
sub esp, 0xc
lea eax, [ebx - 0x1584]
push eax
call 0x550
add esp, 0x10
sub esp, 0xc
push 0
call 0x560
sub esp, 0xc
lea eax, [ebx - 0x1534]
push eax
call 0x550
add esp, 0x10
sub esp, 0xc
lea eax, [ebp - 0x3b]
push eax
call 0x520
add esp, 0x10
cmp dword ptr [ebp - 0x10], 0xdea110c8
jne 0x8c2
call 0x6fd
jmp 0x8d4
```

```
sub esp, 0xc
lea eax, [ebx - 0x1584]
push eax
call 0x550
add esp, 0x10
mov eax, 0
lea esp, [ebp - 8]
pop ecx
pop ebx
pop ebp
lea esp, [ecx - 4]
ret
nop
nop
nop
nop
nop
nop
nop
push ebp
push edi
push esi
push ebx
call 0x600
add ebx, 0x16b7
sub esp, 0xc
mov ebp, dword ptr [esp + 0x28]
lea esi, [ebx - 0xfc]
call 0x4d4
lea eax, [ebx - 0x100]
sub esi, eax
sar esi, 2
test esi, esi
je 0x945
xor edi, edi
lea esi, [esi]
sub esp, 4
```

```
push ebp
push dword ptr [esp + 0x2c]
push dword ptr [esp + 0x2c]
call dword ptr [ebx + edi*4 - 0x100]
add edi, 1
add esp, 0x10
cmp esi, edi
jne 0x928
add esp, 0xc
pop ebx
pop esi
pop edi
pop ebp
ret
lea esi, [esi]
repz ret
```

Code Analysis

Pseudo C Code

ChatGPT Analysis

Exploit

Fuzzing

Buffer Overflow

Format String

Credits

This report was generated using automated tools and the expert analysis of security researchers.