Lab #3 : Reversing Networking Functions Plugin

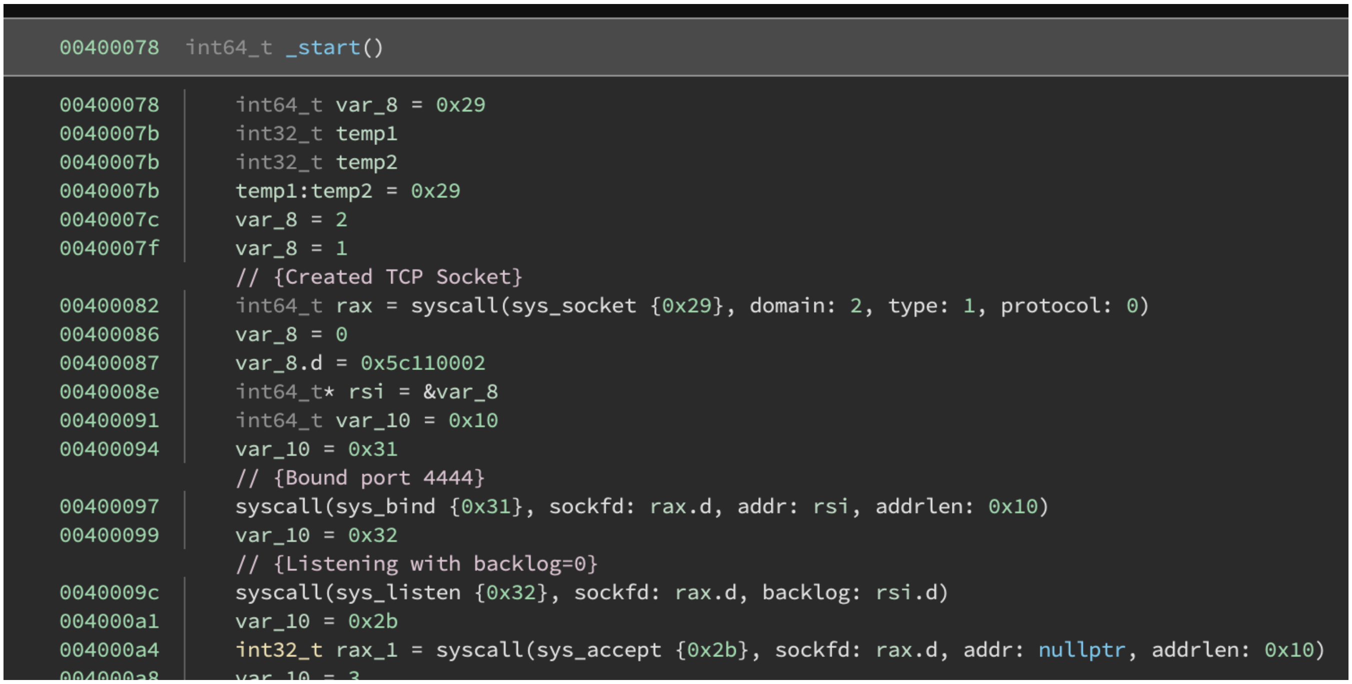
CSE4830 : Reverse Engineering

Networking Functions Plugin

In class, we discussed the various wrapper functions and system calls that enable networking on *nix operating systems. Further, we have been learning through the last few classes about the power of scripts to aid in static analysis. For this lab, you will construct a Binary Ninja plugin to automatically add comments for each networking function/system call in the binaries.

Lab Assignment

You are provided with a sample set of binaries, constructed from Metasploit single and staged payloads. The samples.tar.gz file includes a script to produce new samples with different options. Your plugin should automatically add comments to the binary for the wrapper functions and system calls that implement networking. It should include at a minimum: *socket, bind, listen, accept, connect, send/sendmsg, recv/recvmsg*. Your plugin should provide as much context as possible to the reverse engineer. A minimum sample outcome is depicted below. You may output the context in whatever format you believe is best for a reverse engineer to process.



```
00400078  int64_t _start()

00400078      int64_t var_8 = 0x29
0040007b      int32_t temp1
0040007b      int32_t temp2
0040007b      temp1:temp2 = 0x29
0040007c      var_8 = 2
0040007f      var_8 = 1
              // {Created TCP Socket}
00400082      int64_t rax = syscall(sys_socket {0x29}, domain: 2, type: 1, protocol: 0)
00400086      var_8 = 0
00400087      var_8.d = 0x5c110002
0040008e      int64_t* rsi = &var_8
00400091      int64_t var_10 = 0x10
00400094      var_10 = 0x31
              // {Bound port 4444}
00400097      syscall(sys_bind {0x31}, sockfd: rax.d, addr: rsi, addrlen: 0x10)
00400099      var_10 = 0x32
              // {Listening with backlog=0}
0040009c      syscall(sys_listen {0x32}, sockfd: rax.d, backlog: rsi.d)
004000a1      var_10 = 0x2b
004000a4      int32_t rax_1 = syscall(sys_accept {0x2b}, sockfd: rax.d, addr: nullptr, addrlen: 0x10)
004000a8      var_10 = 3
```

Figure 1: Expected Results for Networking Calls Plugin

Deliverables

1. Your plugin code compressed as a .tar.gz.
2. No report is necessary.

Extra Credit

[+20] You will present your plugins to the rest of the class. The best plugin (as voted by the class) will be submitted as a pull request to the binary ninja plugin repo.