Desenvolvimento de Exploits no Windows

OBJETIVO

~~~~~~

Aprender a identificar e explorar vulnerabilidades de buffer overflow em softwares e ao final escrever um exploit capaz de explorar a vulnerabilidade remotamente

1) Coleta de informações (Identificar o software e entender como funciona a comunicação)
2) Fuzzing (enviar diversos tipos de dados afim de testar o comportamento do software)
3) Identificar a vulnerabilidade (Atingir EIP)
4) Controlar EIP (validar espaço) → Controlar o fluxo do programa
5) Identificar BadChars (Caracteres Inválidos)
6) Identificar o endereço de retorno
7) Testar a execução
8) Gerar o shellcode
9) Exploit Final

Contexto

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Aplicação em rede rodando um Windows 10 Enterprise
atualizado com Antivirus e Firewall ativado

→ Vamos executar o netserver.exe no Windows e vamos entrar nele com o Karlinho Linux
→ A conexão será feita via nc:

```
nc -v 172.15.0.97 5800
```

Vamos interagir com um script em python:

```
#!/usr/bin/python
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("172.15.0.97",5800))
banner = s.recv(1024)
print (banner)
cmd = "HELP\r\n"
s.send(cmd.encode())
s = s.recv(1024)
print (r)
```

→ Executamos com python2