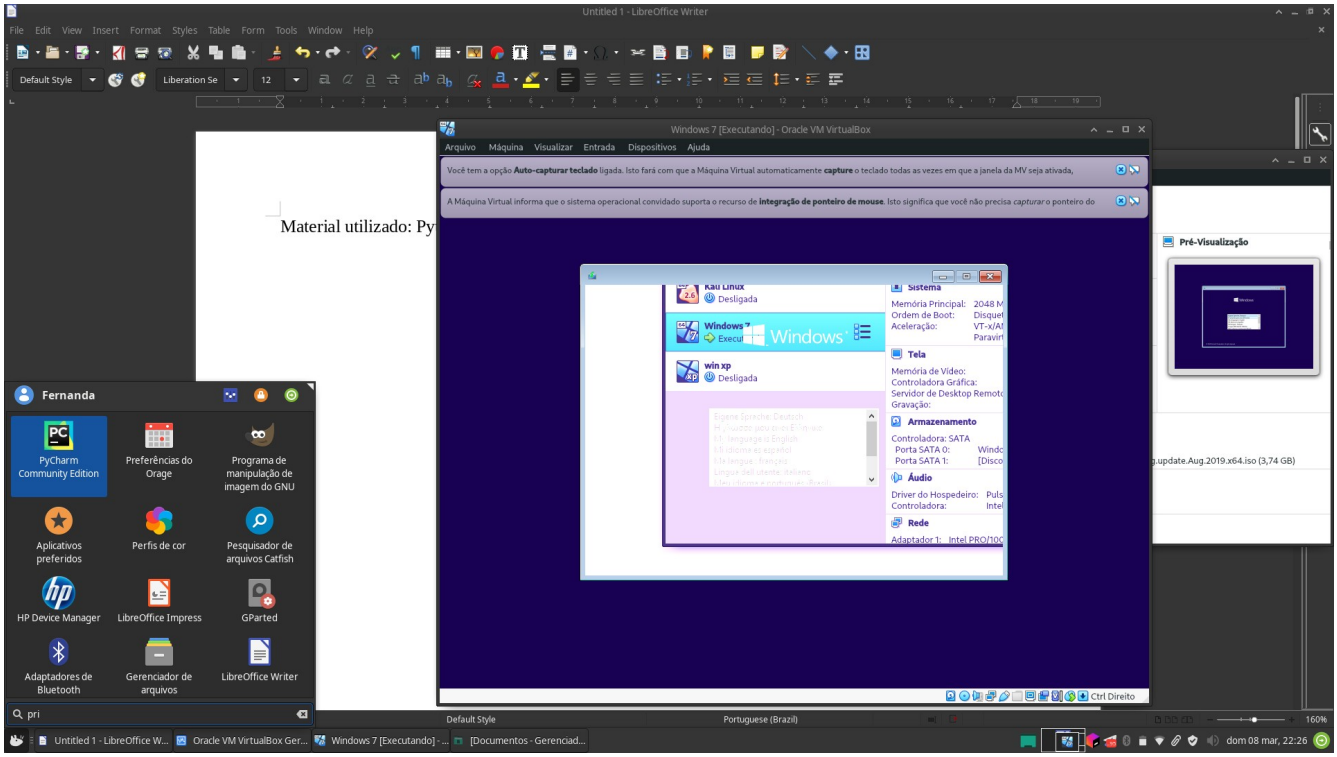
Material de estudo utilizado: Python para pentesters.
Linguagem utilizada: python
Versão: 2.7
Desculpa ruim mas um fato por ter deixado para última hora:



Não consegui executar uma VM e meu notebok travava e devia reiniciar, houve mais de 7 tentativas sem sucesso, somente conseguindo executar o Kali Linux em modo LIVE e ainda assim dando erro e travando, sem capacidade de utilizar um outro computador pelo local.
Devido a isso, não consegui executar e simular realmente o ataque, entretanto explicarei detalhadamente o que era suposto de acontecer, como, bibliotecas, entreoutros.

Cenário
Nos dias hodiernos, a maior parte dos usuários de computadores e notebooks (entreoutros) utilizam em suas maquinas o Windows, sendo o padrão da maior parte dos computadores vendidos. Por isso há uma maior distribuição de vírus para Windows, esse não será diferente.
Não podemos esquecer, também que a técnica de phishing, mesmo que muito conhecida por usuários, ainda ocorre muito on-line. Nesse caso, iremos o utilizar também.

O malware

O que precisa: ser baixado e executado uma vez como administrador.
Por que em python? Por ser mais difícil de ser capturado por um antivirus por ser script e não ter assinatura em assembly, mas infelizmente o código é menos protegido.
Bibliotecas importadas:
Socket; Time; Subprocess, Tempfile; OS

Por que o python? Porque é mais dificil do antivirus, firewall e etc detectar.

Aqui será feito o server eu client será utilizado o netcat (no kali linux – nc lvp PORTA), esse malware tem como objetivo permitir a execução de código remoto por uma conexão reversa por TCP.
O Socket é importado por utilizar conexões de redes.
O Time é importado pois uso a função sleep para dar uma “pausa de segundos.
O Subprocess é importado para executar códigos dentro do sistema operacional, independente do SO.
O IP é o ip de onde o trojan se conectara, no caso, é o meu linux.
A porta será para “driblar” o firewall, para ele acreditar que algo está ocorrendo mesmo quando não é (achar que está visualizando uma página, por exemplo)
Recv(1024) ← Vai receber os códigos recebidos da central

desisti. Desculpa. Eu nem lembro onde está sua outra tag, o engraçado é que fiz. Obrigada pelas ajudas, anjo.