Manual do 7

“Caiu no gorpe do 7” rick joga a bct pros mnr do pcc
“tudo nosso nada deles #sóprogresso” perna de calibre
“os menor tem que chorar pra nois rir” p2
“sangue de puliça é nosso conbustiveu” chô da cdd
#tropadocomplexoCVRL1533

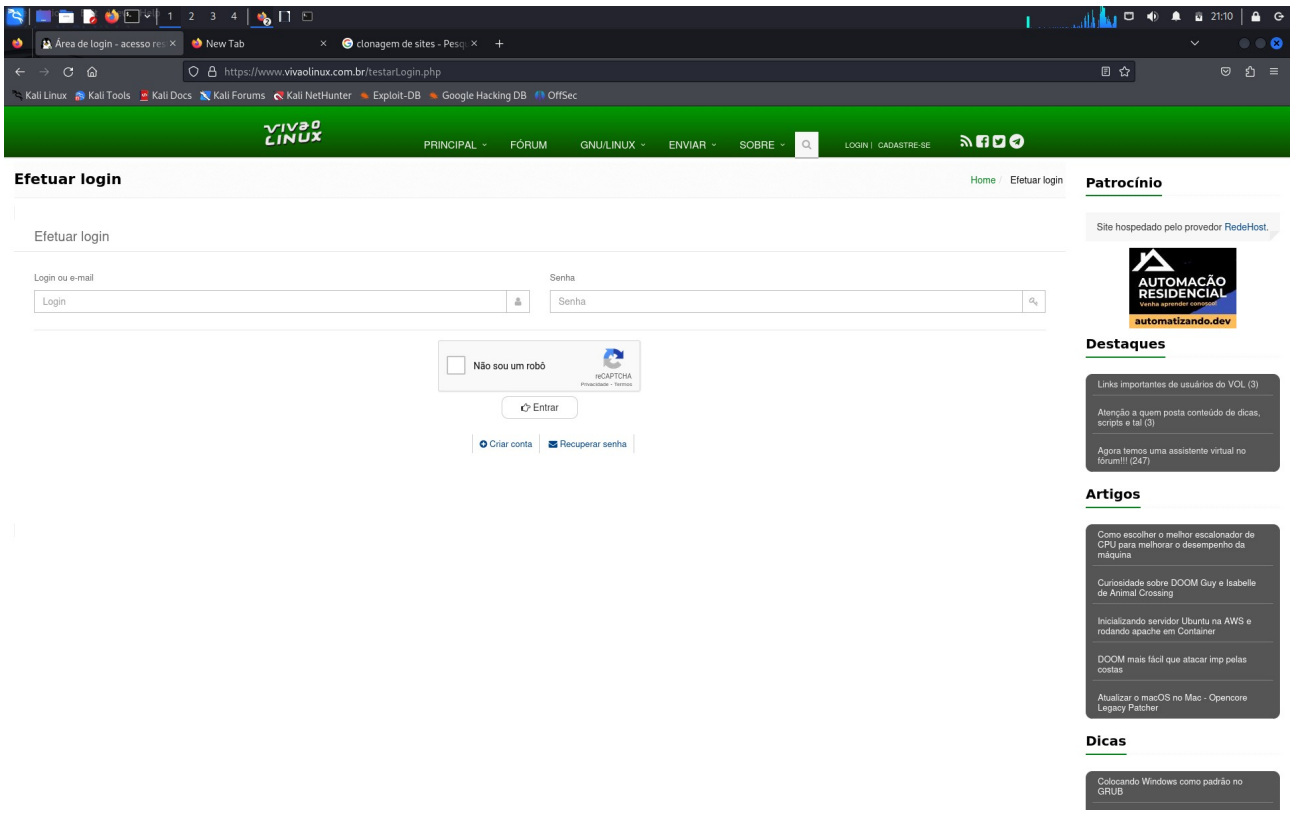
Phishing

Phishing é um golpe comum na internet em que **um criminoso se passa por uma pessoa ou empresa confiável** por meio de e-mail, site ou app para roubar dados sensíveis do usuário, como: nome de usuário, senha e cartão de crédito. Um mecanismo bastante comum é o uso de URL ou endereço de e-mail semelhantes ao da empresa.

Clonagem de Sites

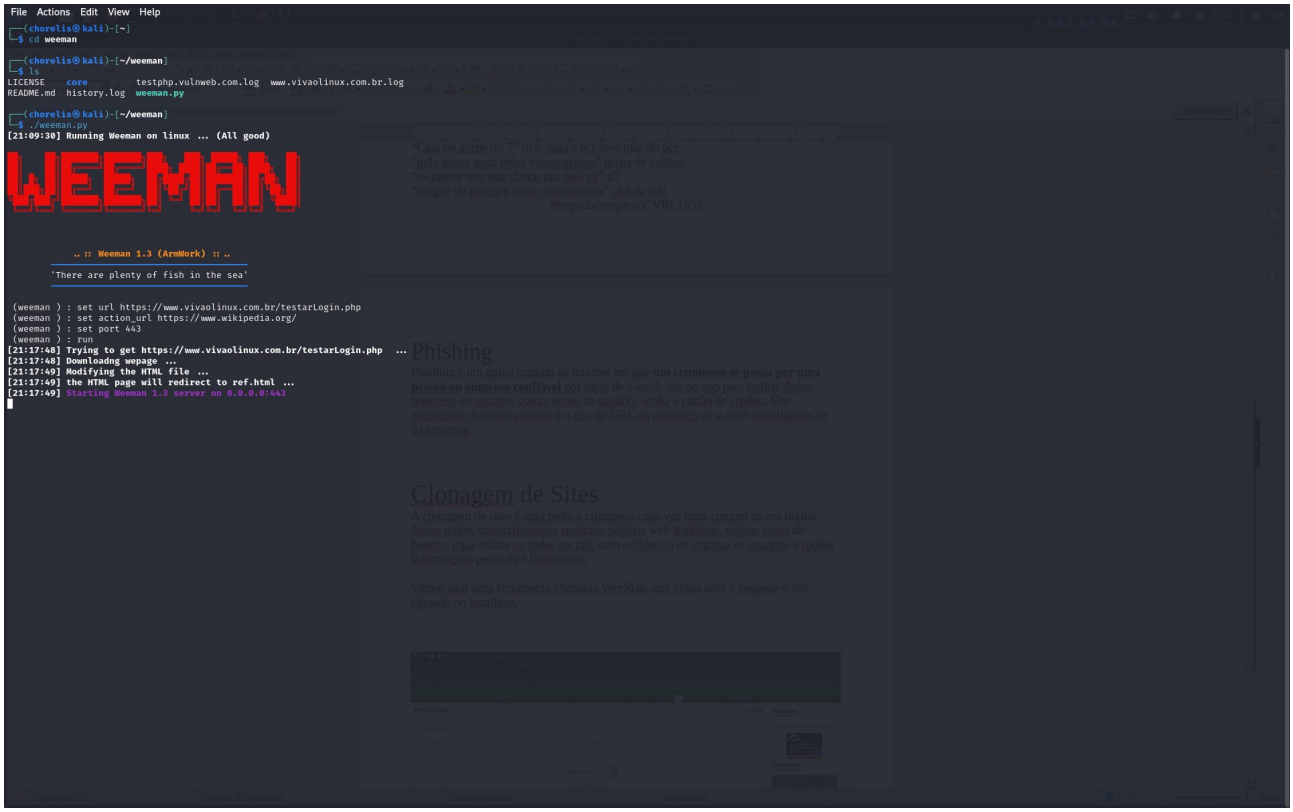
A clonagem de sites é uma prática criminosa cada vez mais comum na era digital. Nesse golpe, cibercriminosos replicam páginas web legítimas, muitas vezes de bancos, lojas online ou redes sociais, com o objetivo de enganar os usuários e roubar informações pessoais e financeiras.

Vamos usar uma ferramenta chamada WeeMan, que clona sites e hospeda o site clonado no localhost.



Esse site é o site original.

Vamos clonar ele para capturar algumas informações dos inputs desse site.



Depois de executatarmos o weeman executaremos os seguintes comandos.

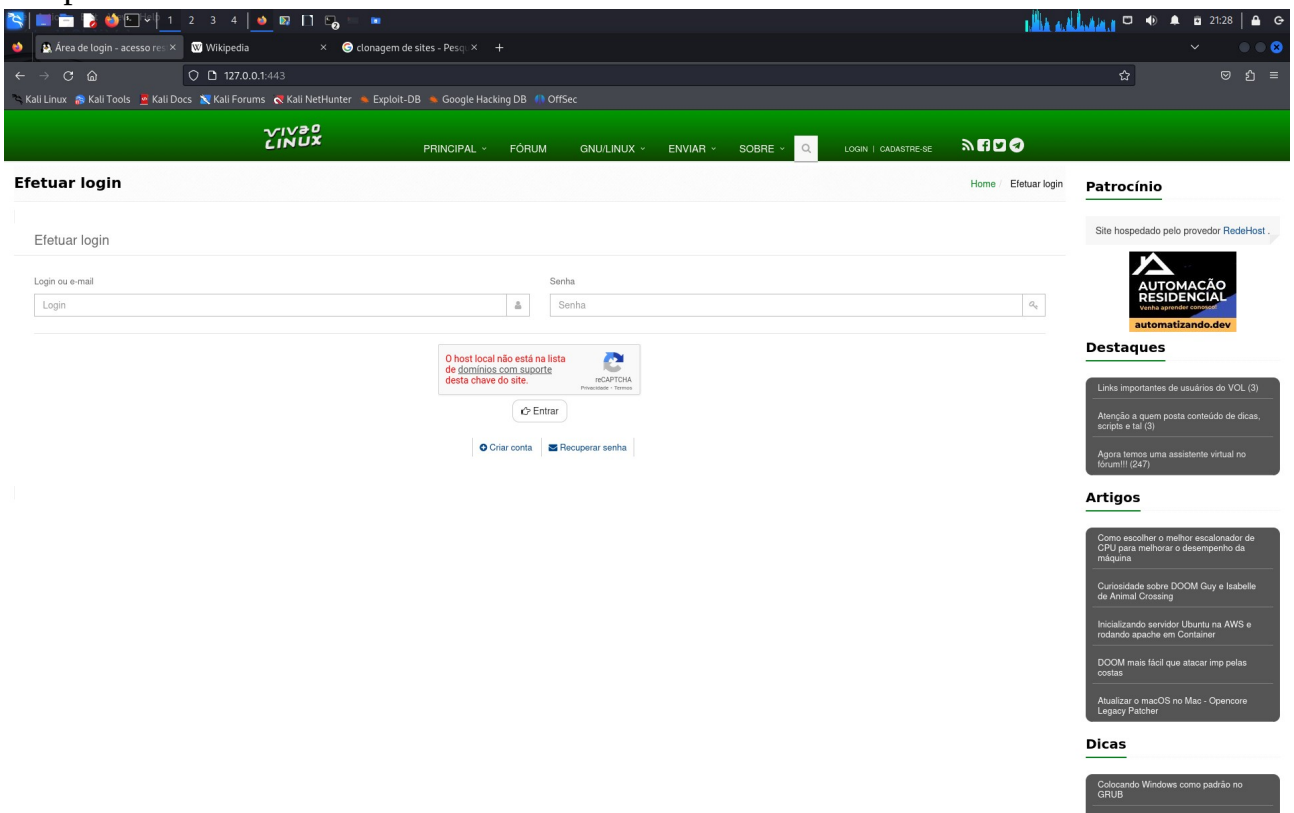
set url
: Serve para adicionar o site que você quer clonar.

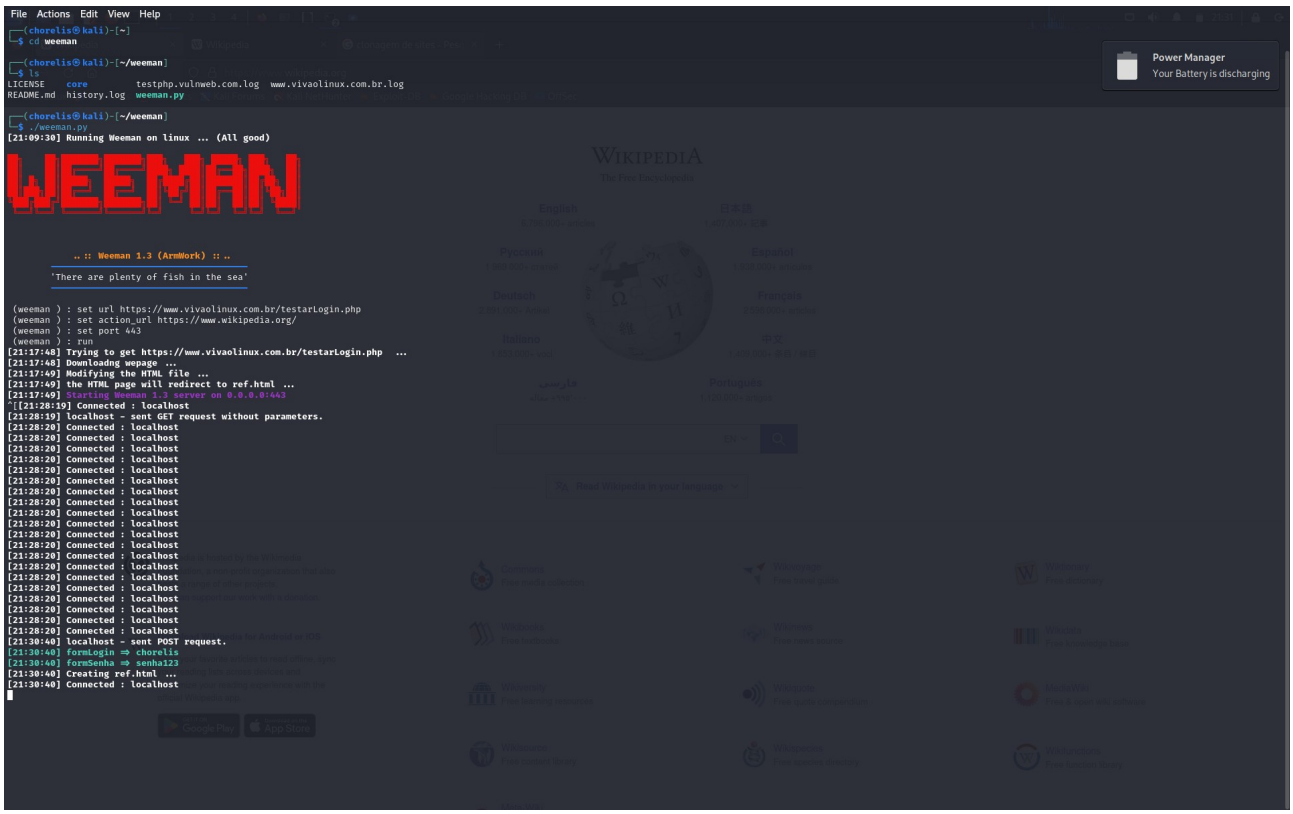
set port
: Serve para adicionar a porta que o site clonado ira rodar.

set action_url
: Serve para adicionar o site que a vitima será redirecionada após o phishing.

run
: Serve para começar o ataque.

Após isso o site clonado estará rodando no seu localhost.





Após a pessoa inserir os dados no site clonado e enviá-los, suas informações são capturadas pelo terminal do atacante.

Como se proteger desse tipo de ataque?

Verifique o URL: Sempre verifique se o URL do site é legítimo e seguro. Preste atenção a pequenas variações nos nomes de domínio, letras faltantes ou adicionais que possam indicar um site falso.

Pesquise a reputação do site: Antes de fornecer informações pessoais ou financeiras, pesquise a reputação do site e procure por comentários de outros usuários. Sites de revisão e fóruns podem fornecer insights valiosos sobre a legitimidade de um site.

Procure por sinais de segurança: Sites seguros geralmente têm um cadeado na barra de endereço e usam "https" em vez de "http". Esses sinais indicam uma conexão criptografada e mais segura.

Atenção aos pedidos de informações sensíveis: Desconfie de sites que solicitam informações sensíveis sem motivo aparente. Empresas legítimas geralmente têm políticas claras sobre o que é necessário e como usar suas informações.

Mantenha seu software atualizado: Mantenha seu navegador da web, sistema operacional e software de segurança atualizados para se proteger contra vulnerabilidades conhecidas.

Use autenticação de dois fatores (2FA): Quando disponível, ative a autenticação de dois fatores para adicionar uma camada extra de segurança à sua conta.

Fique atento a e-mails de phishing: E-mails de phishing muitas vezes tentam redirecioná-lo para sites falsos. Verifique sempre os remetentes e evite clicar em links suspeitos em e-mails não solicitados.

Eduque-se sobre golpes online: Mantenha-se informado sobre os diferentes tipos de golpes online e compartilhe informações com amigos e familiares para ajudá-los a evitar cair em armadilhas semelhantes.

Use uma solução de segurança confiável: Considere usar software antivírus e antimalware confiável para ajudar a proteger seu dispositivo contra ameaças online.