== Engenharia Social ==

Por: Gênesis – O Hacker Cristão

Fórum – plughackers.net

-=[1]=-
.---------------.
| Introducao _____
`---'

Hoje em dia encontrar servidores bugados e muito comum, tornando o servico de "hackers" e "pseudos-hackers" muito trivial, na verdade existem correcoes para todas as falhas conhecidas (quando nao sao feitas rapidamente, bom quer dizer as vezes nao o que ocorre e que os ditos administradores, nao corrigem essas falhas, sabe-se la porque. (se alguem souber pq, me de um toque, eu devo ser ingenuo demais pois nao consigo ver um bom motivo para alguem que recebe para fazer a seguranca de um servidor nao baixar patches para corrigir as falhas do mesmo). Bom mais existem alguns poucos administradores que o fazem, algumas empresas fazem grandes investimentos em cima da seguraca de seus sistemas, mais enfim... Falhas na seguranca podem ser corrigidas, porem o ser humano pode ser facilmente, no dito popular "passado para tras", e eh em cima disto que age a Engenharia Social, fazendo com que pessoas inocentes facam todo o "trabalho sujo" dos "hackers". E um abraço para os manos arplhmd e tb p/ meu amigo Tiago Illan.

-=[2]=-
.---.
| Mitnick: ameaça é a engenharia social _____
`---'

Fonte: Site da revista Info Exame

Kevin Mitnick, o mais famoso hacker do mundo, deu o alerta esta semana de que não adianta nada as empresas se preocuparem com seus sistemas de segurança e deixarem de lado o principal perigo: a engenharia social.

Em uma entrevista ao site Infoconomy, Mitnick declarou que as empresas ficam expostas aos hackers porque não têm consciência das técnicas de engenharia social usadas pelos atacantes mais perigosos: a manipulação. ": A maioria das pessoas acha que, por não se considerarem ingênuas, não podem ser manipuladas.

"Mas nada está mais longe da verdade do que isto", disse. O hacker admitiu que muitas vezes se valeu de truques de manipulação que, aliados ao seu know-how em tecnologia, o levaram a quebrar diversos sistemas nos quinze anos em que se manteve nesta atividade.

Na opinião de Mitnick, bastava só persuadir funcionários mais desavisados a compartilharem informações vitais, como nomes de login e senhas - foi assim que ele afirma ter invadido a rede da Sprint, se passando por um engenheiro da Nortel Networks para o qual os funcionários passaram dezenas de logins e senhas para o acesso aos switches. "A ameaça da engenharia social é substancial", declarou o hacker ao site. "As pessoas deveriam saber que você pode comprar a melhor tecnologia do mundo, mas isto não protegerá sua empresa contra estas técnicas".

O especialista também considera um grave erro não treinar o pessoal da empresa para este tipo de procedimento, porque o funcionário não pode adivinhar o quão perigoso é passar informações por telefone a estranhos que se passam por profissionais de outras companhias ou da própria empresa.

Um dos complicadores, adiciona, é a postura dos próprios superiores, que ignoram procedimentos de segurança quando querem que um de seus funcionários execute uma tarefa imediatamente. "O funcionário nem vai questionar se a pessoa que ligou disser que quer algo a pedido do CEO da empresa", acredita. Mitnick ressalta que a técnica da manipulação não é apenas uma questão de sorte: geralmente os "engenheiros sociais" pesquisam profundamente seu alvo antes de atacar, para descobrir as culturas da empresa, sua estrutura coporativa e quem tem acesso a que tipo de informação.

Isto sem contar com tudo o que pode ser descoberto sobre uma empresa apenas ao se examinar sua lata de lixo. Resumindo, a recomendação do famoso hacker é a seguinte: "Treinem mais rigorosamente seus funcionários para que eles estejam alertas sobre o perigo da manipulação".

-=[3]=-
.----------------------------------.
| Exemplo de Engenharia Social _____
`---'

Certa vez me interesei por um host de uma empresa de medio porte (o q vc quer saber o nome??
esquece naum vou contar  scaneei tudo pra ver quais portas estavam abertas o q estava rodando
lá e se o mesmo possuia alguma falha conhecida, naum me lembro muito bem do resultado (isso foi
a algum tempo atras) mais posso dizer q tinha poucas portas abertas uma q me chamou a atenção
foi a 5950 q mais tarde descobri se tratar de um servidor de VNC (Virtual Network Computing) q
permite administração remota, tava rodando Conectiva Linux e pra minha infelicidade nenhuma falha
conhecida foi encontrada pelo scan 

O q eu fiz??? Bom observando q eu naum tinha praticamente nada a fazer, quase desisti, mais
ai veio algo em minha mente o VNC. Bom naum custava nada tentar, então abri o I.E. mesmo, e tentei
conectar apareceu um tela pedindo a senha, tentei
algumas senhas sem sucesso, mais decidi q se eu realmente fosse invadir aquele servidor o lugar

mais facil seria por ali, eu so precisava de uma senha, mais como eu faria para descobrir a bendita
senha???

Comecei então a fazer pesquisas sobre a empresa alvo para descobrir nomes de funcionarios,
endereços de e-mail, telefones e qualquer outra coisa q me fosse util, a primeira coisa q fiz
foi navegar pela home page da empresa em questão, facilmente consegui alguns endereços de e-mail
inclusive do administrador do site e o telefone da empresa atraves da pesquisa tanto no site
como no registro.br, o proximo passo foi dar uma olhada no codigo fonte da pagina, e pra minha
surpressa no lugar onde fica a meta name e aquelas coisaradas todas, tava o nome de outra
empressa e um nome provavelmete do responsavel pela page, estranho??? naum !!! De
cara percebi doq se tratava, simplesmente a empresa q eu tentava
invadir (q a partir de agora chamarei de Tabajara) havia contratado outra empresa (que chamarei
de Capivara, ah isso naum tem nada haver com o Casseta e Planeta pra fazer seu web site !!!

Por dedução vi q o VNC deveria esta sendo utilizado por Capivara para fazer a administração
do site de Tabajara pois o servidor devia se encotrar fisicamente no endereço da mesma.

Mais isso era tudo dedução, então eu precisava de provas mais concretas e de mais informações
q pudesem me ajudar a obter a senha, oq eu fiz?? Liguei pro
102 e perguntei o numero do telefone de Capivara (incompetentes naum colocaram isso nas metas
tags :p Bom com o numero nas mãos planejei um roteiro de como deveria ser meu dialogo

Com tudo planejado, precisaria so de um endereço de e-mail decente caso fosse necessario, fui
no zzn.com e abri um
endereço como se eu fosse funcionario de uma empresa, tipo meunome@nomedaempresa.zzn.com
(eh tem razão naum eh tão decente assim, mais e melhor q nada),
pronto ja tinha tudo q precisaria agora era so respirar fundo, pegar o tel e ligar.

O dialogo a seguir dificilmente vai ficar como o q foi usado, como eu ja disse isso foi ah algum
tempo, ah e os nomes usados abaixo tb são totalmente ficticios.

Capivara - Capivara Gisele Boa Tarde.

Eu - Boa Tarde !!! Aki quem fala eh o Claudio da Fulano Empreendimentos Imobiliarios

Capivara - Posso ajuda-lo em q Sr. ?

Eu - Bom sou funcionario da Imobiliaria Fulano de Tal e estou interessado em saber como
funciona o serviço de vcs, assim meu chefe quer colocar uma pagina no ar para q nossos
clientes possam acessar e ver quais os imoveis estao disponiveis tanto para locação
como para vendas esse tipo de coisa, e como aqui na firma naum tem um setor

adequado
para isso e como eu sou o q mais entende de informatica aqui acabou sobrando pra mim arrumar isso, então eu gostaria de tirar algumas duvidas sobre o serviço prestado por vcs.

Capivara - Entendo vou passar vc para o Valdir ele poderá atende-lo melhor. (Sorte minha pois este era o mesmo nome q estava no codigo fonte do site de Tabajara)

Eu - ok, obrigado e tenha um bom dia

Capivara - Valdir Boa tarde !!! em q posso ajuda-lo Sr. ?

Eu - Boa tarde !!! Valdir aqui quem fala e o Claudio... (ai eu repeti quase a mesma
conversa q tive com a atendente)

Capivara - Pode ficar a vontande para pergutar Sr.

Eu - Bom tenho varia duvidas, por exemplo aqui na firma temos o servidor q seria utilizado
para hospedar a pagina, como vcs fariam a atualização? Vcs viriam aqui sempre q preciso?
ou vcs usam algum tipo de conexão remota para isso?

Capivara - Sei mais primeiro preciso saber qual a configuração do seu servidor para saber se ele
e adequado para hospedar um site

Eu - Então o servidor ainda naum chegou aqui na firma ele foi comprado recentemente
então nao estou muito certo da marca mais sei q ele terá um HD de 100GB e 3GB de memoria RAM e tera acesso a Banda Larga

Capivara - E o Sistema Operacional vcs pretedem usar Windows?

Eu - Olha naum tenho certeza ainda, mais a tendencia e optarmos pelo Linux para diminuir o custo com licenças, o problema e q ninguem aqui sabe usar
o Linux.

Capivara - Fique tranquilo nossa empresa pode cuidar do seu caso tranquilamente, temos varios
casos semelhantes ao seu e sempre obtivemos sucesso, trabalhamos da seguinte forma: temos preferencia pelo Conectiva Linux a administração e feita por
nos mesmo entao nao existe a necessidade do cliente ter conhecimento avançado em Linux,
so o basico para poder nos ajudar em caso de emergencias e com algumas rotinas, mais para isso nos fazemos
o treinamento do funcionario q ficara responsavel por isso, primeiro sera mandado
um tecnico para fazer as configurações necessarias em seu servidor, a partir
de entao toda a manutenção e atualização será feita atraves de conexão remota.

Eu - Interessante, mais oq poderia ser esses casos de emergencias?

Capivara - São raros na verdade e quase impossivel de acontecer mas o mais comum se trata de
não conseguirmos logar usando a conexão remota, geralmente isso
e ocasionado pelo proprio cliente, então nos passamos um e-mail para o funcionario
responsavel pelo servidor na empresa em questão, informando do problema e de como
soluciona-lo.

Eu - Valdir quantas pessoas fazem parte da equipe q vai cuidar da administração do site?

Capivara - A principio a equipe e formada apenas por um funcionario da Capivara, so em alguns casos
a parte ocorre de ter mais de um funcionario envolvido no caso, esse funcionario q sera responsavel por entrar em contato com a empresa cliente sempre q necessario
e por fazer o gerenciamento do site.

Eu - No caso como foi vc que me atendeu você seria o responsavel pela administração da pagina?

Capivara - Isso, todos os contatos e administração seria feita por mim

Eu - Valdir obrigado pela sua atenção, mais eu tenho q atender um cliente importante aqui
e vou ter q desligar, gostaria q vc me passase um e-mail explicando melhor o serviço
e tambem uma tabela de preço pra eu poder passar isso para o meu chefe

Capivara - Certo qual e o seu e-mail?

Eu - Claudio@fulano.zzn.com

capivara - Estarei passando o e-mail o mais breve possivel

Eu - Obrigado Valdir, desculpa o incomodo, e tenha uma Boa tarde !!!

Capivara - Nos q agradecemos, tenha uma boa tarde tb !!!

2 minutos depois quando eu consegui me recompor da tremedera e repor as ideias fiz uma analize
em q essa conversa poderia me ajudar.

Essa conversa foi muito interessante para mim pois pude confirmar o uso do VNC para administração
remota e aprendi um pouco da rotina utilizada por Capivara para com seus clientes, ao receber o
mail de Valdir pude ver tb o padrão de escrita e estilo utilizado nos e-mails de Capivara, tinha
o enderenço de mail de Valdir sabia q se alguem de capivara tivesse q mandar algum e-mail para
Tabajara seria o Valdir e ja tinha tb boas ideias para o meu ataque a Tabajara


Abri outra conta de mail no zzn.com agora como pedro@capivara.zzn.com
Passei um e-mail parecido com esse para Tabajara:

To: contato@tabajara.com.br
from: pedro@capivara.zzn.com
Subject: Problema com conexão remota

Capivara LTDA

Venho por meio deste avisar que estamos tendo dificuldades para acessar o seu servidor atraves
do VNC, acredito que o problema esteja relacionado a senha q estamos utilizando, como vossa empresa
pode observar, não é o Valdir Rocha q está mandando o e-mail como de costume e sim o Pedro da Silva
, o motivo é que o Valdir foi para um congresso em Santa Catarina.

Estou tentando logar utilizando a senha: "seucraison" , da mesma forma como fui

instruido por
Valdir mais a senha e recusada, provavelmente essa seja a senha de outro cliente, a partir do
momento que ele me passou varios clientes de sua responsabilidade a troca de senhas pode ter ocorrido
naturalmente.

Como so quem tem acesso a essa senha e o Valdir, e não estamos conseguindo entrar em contato com o mesmo,
gostaria de pedir gentilmente a vossa empressa que confirme a senha já citada.

Caso ela realmente esteja incorreta mande-nos um e-mail com a senha correta urgentemente, pois precisamos fazer
algumas atualizações de segurança no seu servidor, e caso a senha esteja correta avise-nos para que possamos
tomar as medidas adequadas para resolver a situação.

Peço desculpas pelo trantorno sem mais para o momento.

agradeço desde já vossa colaboração,

Pedro da Silva

Em cerca de uns 20 minutos depois recebo o mail de Tabajara dizendo q a senha realmente estava
errada e q a correta seria: "pikachu" ,aew foi so abrir o VNC cliente e conectar no servidor com
a senha, e VOALA la estava o desktop de Tabajara inteirinho na tela de meu micro, o resto eh
historia 

-=[4]=-
.---------------------------------.
| Dicas para Engenharia Social _____________________________________
`---'

*Qualquer ataque deve ser planejado com antecedencia, detalhe por detalhe, para isso faça pesquisas sobre o alvo, colha tudo o q julgar util, como nomes, telefones, endereços de e-mail, estilo de escrita dos funcionarios, nomenclaturas usadas na empresa vc pode conseguir isso usando tais fontes:

-Pesquisa na propria home page da empresa visite pagina por pagina recolhendo o maior numero de endereços de e-mail, telefones, e as vezes e possivel encontrar nomes de funcionarios tb.

-Busque no Codigo Fonte da pagina por comentarios q lhe possam ser uteis.

-Entre no site registro.br e faça uma busca sobre o seu alvo assim vc pode descobrir quem e o administrador, endereço fisico da empresa, telefones, endereços de e-mail e mais algumas coisas.

-Pesquisa em historicos de listas de discussão, é possivel encontrar mensagens muito atraentes para o atancante, algumas mensagens são tão inocentes q o sujeito falta dizer "me invadam por aki q eu deixo" . Um jeito facil de pesquisar em historicos e utilizando o proprio www.google.com.br (como diz Narcotic "O Grande Oraculo") faça assim com alguns endereços de e-mail nas mãos faça uma busca usando esses endereços como palavra chave, simples e eficiente. Com isso tb vc pode observar estilos de escritas e assinaturas usados pela pessoa q vc pretende personificar.

-Se vc naum tiver voz de criança e for um pouquinho corajoso, ligue para a empresa e demostre interesse sobre os seus serviços, assim vc pode aprender

sobre as nomenclaturas usadas na empresa e ainda, confirmar alguns nomes e funções de funcionarios e oq mais sua mente insana conseguir imaginar. Ah aconselho naum fazer isso usando seu tel de casa pode acontecer do lugar ter Bina e se ficarem desconfiados de vc podem te localizar facilmente

-Coleta de lixo !!! eh isso mesmo procure no lixao da empresa por anotações de telefones, memorandos, manuais com politícas internas da empresa, cursos ou férias, manuais dos sistemas utilizados, qualquer coisa que contenha nome de usuários e senhas, Disquetes,CDs ou HDs aparentemente inutilizáveis, papel timbrado da empresa.

*Fakemail eh muito recomendado, use sua imaginação

*Sites clones tb sao bem vindos, vide os ultimos casos de sites clones, um da microsoft q pedia para fazer o download de um patche de seguranca, que na verdade era um trojan, e outro do banco Itau q pedia para o cliente renovar a senha e o final da historia vc ja sabe.

4.1 - Metodos utilizados

-Assuma a identidade de outra pessoa, q pode ser qualquer um na empresa desde um simples funcionario ate alguem com mais autoridade dependendo do q vc planejou.

-Use frases q dê a impressão q a pessoa precisa de vc um exemplo retirado do mail acima " precisamos fazer algumas atualizações de segurança no seu servidor".

-Faça com q o sujeito se sinta bem consigo mesmo (vide puxa-saco) assim fica mais facil de manipula-lo.

-Use frases q denotem q vc precisa dele assim ele se sente superior e vai tentar se " aparecer " e acaba falando mais doq devia, ex retirado do telefonema: " acabou sobrando pra mim então eu gostaria de tirar algumas duvidas."
"o problema e q ninguem aqui sabe usar o Linux."

-Ocupaçao Furtiva !!! Q??? Isso mesmo!!! E assim vc finge ser da companhia de telefone, eletrica ou dependendo do caso vc pode fingir ser alguem da manutenção, um funcionario novo ou ate mesmo o entegador de leite :p. Aew vc pode andar livremente pelo local de trabalho da vitima, o limite desse metodo e a sua imaginação e criatividade. Esse e o metodo mais dificil, (ta na cara né? pq diabos eu to escrevendo isso entao???) pois e necessario muita coragem e boa interpretação.

-=[5]=-
.---------------------.
| Como se proteger _____
`---'

*Treinamento de funcionarios

*Evite ao maximo dar informações da estrutura da sua empresa.

*Certifique-se de que a pessoa e realmente quem diz ser, no caso acima bastaria dar um simples telefonema para confirmar a procedencia do e-mail e acabar com todo meu plano.

*Cuidado com o q joga no lixo, procure inutilizar tudo.

*Resumindo tudo numa unica frase "desconfie ate da sua mãe" :p

-=[6]=-
.----------------.
| Finalizando ____
`---'

O grande lance da Engenharia Social e que ela vai ser sempre viavel e muito eficiente, haja visto que ate mesmo Adao e Eva foram enganados, e desde aquela ate os dias atuais, varias pessoas sao "feitas de *@3$$%*" o dia inteiro, baseado nisso duvido muito que algum dia isso seja diferente, entao tome cuidado pois o proximo pode ser voce 

Gênesis – O Hacker Cristão