UNIVERSIDADE ESTADUAL DE GOIÁS
CÂMPUS ITABERAÍ

AMANDA CLARA JONAS RIBEIRO
VITOR FREIRE RIBEIRO

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO SOBRE ENGENHARIA SOCIAL NO AMBIENTE ACADÊMICO

ITABERAÍ
2017

AMANDA CLARA JONAS RIBEIRO
VITOR FREIRE RIBEIRO

SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO SOBRE ENGENHARIA SOCIAL NO AMBIENTE ACADÊMICO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação da Universidade Estadual de Goiás – Campus de Itaberaí, sob orientação do profº Esp. Nádio Carlo de Souza Vieira.

ITABERAÍ

2017

DEDICATÓRIA

Eu Amanda Clara Jonas Ribeiro dedico este trabalho a minha mãe Maria de Fátima *(in memoriam)*, origem da inspiração para continuar este desafio, que não pôde estar nesse momento tão feliz da minha vida, mas que não poderia deixar de dedicar a ela, pois se hoje estou aqui, é por causa dela e por Deus! Devo muitas coisas a eles, por ensinamentos e valores passados. Ela não terá a oportunidade de presenciar a concretização desse sonho, mas tenho certeza que ajudou, apoiou e torce de onde ela está, para que alcance e tenha sucesso nessa nova jornada. Saudades eternas!

Eu Vitor Freire Ribeiro, dedico este aos meus pais Sandra Mendes Freire e Naim Ribeiro de Andrade, que nunca mediram esforços para que eu conseguisse chegar até aqui, dedico também a nossa Ex-Coordenadora de curso de Sistemas de Informação, Sheila da Silva Araújo, que sempre me auxiliou e apoiou nos momentos mais difíceis desse curso.

Dedicamos também às nossas famílias, por terem nos dado todo apoio que tanto precisamos nos momentos de perdas que, além disso, confiaram em nós.

Não poderíamos deixar também de dedicar, aos nossos amigos (as) que de alguma forma nos ajudou, que nos apoiaram e que sempre estiveram ao nosso lado, sempre nos levantando nos momentos de fraquezas, angústias e nas crises de ansiedade.

A estes dedicamos este trabalho, sem a ajuda, confiança e compreensão de todos, este sonho não teria se realizado.

Nosso muito obrigado. Vocês são tudo para nós!

AGRADECIMENTOS

Agradecemos primeiramente a Deus por nos ter concedido forças para que tenhamos chegado até aqui, também a nossa instituição que sempre nos propiciou tudo quando precisamos, ao nosso orientador que foi grande difusor de conhecimento durante esse período de graduação, por último e não menos importante, nossos professores e mestres que nos guiaram durante essa jornada.

“A nova fonte de poder não é o dinheiro nas mãos de poucos, mas informação nas mãos de muitos.”

(John Naisbitt)

RESUMO

O presente trabalho de conclusão de curso tem o intuito em abordar sobre segurança da informação com enfoque em engenharia social no meio acadêmico e assim demonstrar a vulnerabilidade das pessoas, sendo elas por falta de entendimento ou de instrução. Serão mostrados métodos e ferramentas da Engenharia Social utilizada para acessar a privacidade de vítimas. Buscamos, também, entender o psicológico e o que leva as pessoas a tais golpes e o porquê delas caírem no mesmo. Mostrando como são utilizadas e como se proteger. Explicando sobre todo o assunto de forma simples e sucinta para que todo leitor consiga entender, aprender e praticar o que está sendo exposto, tentando assim amenizar as ondas de crimes cibernéticos, para que todos consigam fazer sua parte, seja ela se ajudando ou ajudando ao próximo. Devido a uma grande quantidade de pessoas que são vítimas de ataques na internet através da engenharia social, iremos mostrar como e porque às pessoas caem nesse perigo, e também técnicas utilizadas pelos atacantes e algumas dicas simples para se prevenir.

Palavras-chave: Segurança da Informação, Engenharia Social, Vulnerabilidades, Conscientização.

ABSTRACT

The present work of course completion is intended to address information security with a focus on social engineering in the academic environment and thus demonstrate the vulnerability of people, because of lack of understanding or instruction. Methods and tools of Social Engineering used to access the privacy of victims will be shown. We also seek to understand the psychological and what drives people to such blows and why they fall into it. Showing how they are used and how to protect themselves. Explaining the whole matter in a simple and succinct way so that every reader can understand, learn and practice what is being exposed, thus trying to soften the waves of cybercrimes, so that everyone can do their part, whether it is helping or helping the next. Due to a large number of people who are victims of internet attacks through social engineering, we will show how and why people fall into this danger, as well as techniques used by attackers and some simple tips to prevent.

Keywords: Information Security, Social Engineering, Vulnerabilities, Awareness.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

Cert.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

DoS – *Denial of Service*.

SET – *Social Engineering Toolkit*.

Txt – Arquivo de texto.

Html – *HyperTextMarkupLanguage*.

Php – *Personal Home Page*.

ES – Engenharia Social.

IP – *Internet Protocol.*

RAM – *Random Access Memory.*

USB – *Universal Serial Bus.*

SSH – *Secure Shell*.

NTP – *Network Time Protocol.*

GPG – *GNU Privacy Guard.*

SQL – *Structured Query Language.*

SNTP – *Simple Network Time Protocol.*

SO – *Sistemas Operacionais.*

SUMÁRIO

INTRODUÇÃO

Quando se fala em segurança estamos falando em algo muito sério e sigiloso, onde hoje em dia muitas pessoas não têm noção do quanto estão sendo vulneráveis e dispersas sobre esse assunto, então a engenharia social no dizer de segurança da informação, é a manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais, com isso queremos mostrar que o elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano.

Com a disseminação da informação nos meios digitais em uma alta velocidade e o interesse que o ser humano tem em se relacionar e/ou socializar, despertou-se um interesse em explorar este campo utilizando o ambiente acadêmico. O objetivo desse trabalho é apresentar o tema sobre a segurança da informação na ótica da engenharia social e demonstrar vulnerabilidades das informações sobre as pessoas, sendo elas por falta de entendimento ou por falta de informação, com objetivo específico de o estudo abordar sobre duas linhas de pesquisa, sendo elas a parte técnica de segurança da informação e a parte psicológica dos engenheiros sociais e vítimas. Serão demonstradas etapas e ferramentas utilizadas para invadir a privacidade e às vezes até a vida de algumas vítimas. Sendo utilizados métodos de Engenharia Social computacionais em conjunto com as técnicas baseadas em pessoas no ambiente acadêmico. Busca-se, também, entender psicologicamente falando o que leva a pessoa a fazer isso para ganharem vantagens sobre os outros e o porquê as pessoas estão susceptíveis a esses ataques, mostrando assim a prática dessas ferramentas, como são utilizadas e como se proteger.

Tendo esse tema escolhido, pela notória quantidade de ataques e vítimas feitas por esses métodos, despertou-se a curiosidade para descobrir o porquê de um mundo tão evoluído tecnologicamente, a vítima esteja sujeita a tantos ataques que às vezes são considerados tão simples, tendo em vista alertar a todos dos perigos que cada um corre e formas que podem ser utilizadas para se protegerem desses ataques.

Baseando-se em livros, entrevistas com profissionais da área forense, da área de psicologia, fontes sobre o assunto de Engenharia Social, *hackers*, ataques cibernéticos, métodos forenses, dentre outros, usando material com conteúdo confiável e autoexplicativo, facilitando então o desenvolvimento do trabalho e ajudando a aprendermos mais durante esse período.

1 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação consiste sobre a proteção de algum dado valioso para determinado indivíduo ou organização. Pode se entender por informação todo conteúdo importante para um indivíduo e que tenha capacidade de armazenamento ou transferência, que serve para determinado propósito para o ser humano.

Segundo Alves (2006) a segurança da informação visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e oportunidades de negócios. Atualmente, informação digital é um dos principais produtos do mundo e devido à grande utilização, também é necessária que haja segurança. A segurança da informação pode ser afetada por vários fatores como o comportamento humano, pelo ambiente em que se encontra e o por pessoas que tem intuito de roubar, alterar ou destruir essas informações. Quando se diz sobre segurança da informação, logo têm que se pensar sobre suas características. Essas são consideradas os três pilares da segurança de informação, o que mantém essa segurança em pé, sendo elas demonstradas abaixo:

Figura 1- Pilares da Segurança da Informação.

- Disponibilidade: é o pilar responsável por garantir toda disponibilidade do sistema, seja no *hardware*, *software* e até mesmos os dados. Uma forma de garantir a

disponibilidade é através da redução de vulnerabilidades em sistemas computacionais, independente de qual seja.

- Integridade: é o pilar responsável por garantir que não haja nenhuma alteração de modo não autorizado no sistema durante o armazenamento ou processamento. Esse objetivo é responsável não só pelo sistema, mas também pelo *hardware*. É o termo usado quando o sistema funciona conforme o esperado.
- Confidencialidade: para garantir a confidencialidade, deve haver a segurança, para que não haja nenhuma divulgação ou perda indevida. Uma ação bem conhecida para que a confidencialidade seja aplicada é a criptografia, que é uma técnica para cifrar as informações até que estejam de forma ilegível, para que não haja acessos não autorizados, e caso haja, que não seja "visível".

De acordo com a entrevista feita com o profissional especialista em segurança da informação Nádio Carlo de Souza Vieira, pode-se notar que esses pilares são como uma base/alicerce, no qual precisa de todas as hastes para permanecer em pé.

Não existe um pilar mais importante que o outro, mesmo que um ataque não afete todos os pilares, é necessário que todos estejam de pé para que não haja uma queda na sua segurança de informação.

1.1 Ameaças da Segurança de Informação

São invasões de computadores, que costumam ser o tipo de ataque mais praticado/temido.

- **Scan**

É um ataque com o objetivo de identificar quais computadores estão ativos e quais serviços estão disponibilizados, ou seja, quais estão presentes na rede (como SO, atividade e serviços) e possíveis alvos para ataque.

- **Fraude**

A fraude, ou o *scam* (com "m"), um dos mais comuns deles é o *phishing*, conhecido como "pescaria ou *e-mail*", usado para envio de e-mails ou mensagens falsas com links suspeitos.

- **Worm**

Worms são vírus. *Malware* são *softwares* com o intuito de prejudicar o computador "hospedeiro", ou seja, são vírus entre diversos outros tipos de programas maliciosos. São perigosos pela sua capacidade de espalhar pela rede e afetar arquivos com sua rapidez.

1.2 Formas De Proteção De Ataques

São meios de segurança que visam controlar o acesso às informações de forma física e lógica.

- **Criptografia**: é um meio de converter os dados em um formato do qual seja impossível decifrá-lo, ou seja, impedir completamente a interpretação das informações, e elas só voltam ao estado nítido quando uma senha é inserida.
- **Assinatura digital**: Tem garantia de integridade dos dados por meio de criptografia, ou seja, seu acesso pode ser irrestrito e seu conteúdo não pode ser modificado.
- **Certificação**: uma certificação é como um atestado de autenticidade de um arquivo. Uma garantia de que o mesmo é válido.
- ***Honeyspot**:* É um *software* que age como um antivírus em tempo real, seu objetivo é proteger os dados de ameaças na *internet*. A diferença é que, em vez de mantê-lo em quarentena, por exemplo, o *honeyspot* engana esse invasor, fazendo-o acreditar que está tendo acesso real às informações.

2 ENGENHARIA SOCIAL

Atualmente o avanço da tecnologia está visível a cada dia. É quase impossível conhecer alguém que não tenha algum aparelho tecnológico ou redes sociais, e com isso cresce a vulnerabilidade das informações das pessoas pelo fato de exporem muito suas intimidades na rede. Uma pessoa com más intenções pode roubar sua casa, por saber que você não está lá, por meio de uma foto postada em alguma rede social. Essa é uma técnica muito antiga chamada de Engenharia Social.

O termo Engenharia Social só veio a ser popularizado nos anos 90, graças ao ex-*hacker* que ficou mundialmente famoso devido as suas trapaças na rede, inclusive invadindo sistemas do governo. Kevin Mitnick foi preso devido a um descuido em 1995, e após ser solto, deixou de lado a vida de *hacker* e lançou o livro "A Arte de Enganar" que conta como foi a sua vida de *hacker* durante esse período. Atualmente Mitnick colabora com órgãos governamentais, bancos e outras instituições ajudando assim a aumentar a segurança das mesmas.

Engenharia Social é uma técnica usada para ataques, usando métodos de persuadir as pessoas, para descobrir informações e dados importantes que podem ser usados de forma negativa para prejudicar a vítima. A ES pode ser considerada também, como uma arte, a arte de enganar, de manipular as pessoas, como diz o autor Hadnagy (2011) no seu livro *Social Engineering The Art Of Human Hacking*, que define a engenharia social como: [1]" [...] that social engineering is the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives." (HADNAGY, 2011, p. 23).

Diante das entrevistas feitas com profissionais da área psicologia, é possível notar que a Engenharia Social é uma técnica de manipulação psicológica, não é conhecida como Engenharia Social para psicologia e sim como a arte de persuasão.

Mitnik (2003) cita uma frase de Albert Einstein, dizendo que: "Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro". (MITNIK; SIMON, 2003, p.3).

Diante dessa frase que Mitnik entende-se que os ataques da engenharia social podem ter sucesso quando as pessoas são sem discernimento sobre as boas práticas da segurança. Uma pessoa vulnerável é aquela que está apta a ser invadida, ou seja, a serem atraídas por um

[1]Que a engenharia social é a arte ou, melhor ainda, a ciência, de habilmente manobrar os seres humanos para agir em algum aspecto de suas vidas, de usufruir das lacunas falhas do ser humano para benefício próprio, ou simplesmente por prazer.

inimigo. Essas vítimas são frágeis e incapazes de algum ato. Em sua maioria são mulheres, crianças e idosos que possuem maior fragilidade em relação a outras pessoas.

Na maioria das vezes esses ataques acontecem como, por exemplo: Pessoas que se passam por um profissional ou com apenas uma simples conversa no dia a dia, fazendo com que o atacante tenha acesso a informações das vítimas. Sobre as técnicas da Engenharia Social, muita das vezes também acontece através de informações falsas, sendo por qualquer meio de comunicação, como telefonemas, *e-mails* falsos com aplicativos de antivírus e conversas diretas, se dá também, através do carisma quando conquista a confiança da vítima, extraindo as informações necessárias para o ataque.

Aqui no Brasil se ouve muito falar sobre técnicas usadas por golpistas. Exemplo de uma delas é a do telefone, onde o golpista liga para vítima e finge estar com algum familiar, diz ainda que se a vítima não depositar uma quantidade de dinheiro, o familiar vai ser morto. De acordo com uma reportagem feita pelo Jornal Nacional em julho de 2015, só no centro-oeste do estado de São Paulo, o prejuízo chegou a 100 mil reais no ano de 2015 com essa técnica.

Técnicas *hackers* também são utilizadas com o mesmo intuito. De acordo com uma reportagem feita pelo *site* O Globo, o aposentando Edgar Silva Pereira que foi vítima de *hackers* que utilizaram engenharia social, o mesmo relatou ainda com uma brincadeira, que os *hackers* sabem mais dele do que ele mesmo. E esse tipo de crime só tem aumentado no Brasil, de acordo com o Centro de Estudos, Respostas de Segurança (Cert.br) que é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet brasileira. Houve um crescimento de 197% de 2013 para 2014, o aumento de *cyber* ataques reportados à entidade aumentou de 352.925 para 1.047.031.

De acordo com o *site* do Cert.br, durante o ano de 2015, o ataque reportado ao mesmo chegou a quase 700 mil, sendo de forma geral, sobre todo tipo de ataque, como mostra na figura a seguir:

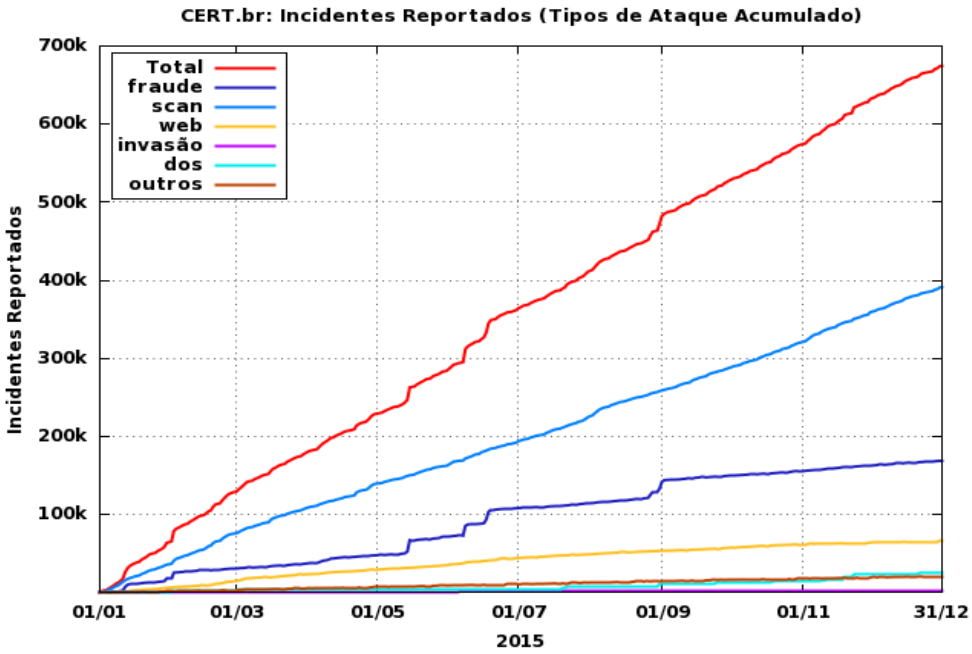

Figura 2- Ataques Acumulados.

Legenda:

- **Dos** (DoS– *Denialof Service*): Notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede;
- **Invasão**: Um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede;
- **Web**: Um caso particular de ataque visando especificamente o comprometimento de servidores *Web* ou desfigurações de páginas na Internet;
- ***Scan***: Notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;
- **Fraude**: Segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem;
- **Outros**: Notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que **não se deve confundir *scan* com *scam***. *Scams* (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

No dia 12 de maio de 2017, o mundo acordou alarmado, pois, houve um ataque mundial do vírus *ransomware*, o ataque foi nomeado de *wannacry*, termo inglês que traduzido para o português quer dizer “quero chorar”, as principais formas de execução desse vírus são: sites maliciosos, *links* suspeitos por *e-mails* e até mesmo aplicativos vulneráveis, também por *links* enviados pelo *Facebook* (que é um método muito utilizado para fazer vítimas de engenharia social). Os *hackers* utilizam deste meio para sequestrar todos os dados e arquivos do computador da vítima, paralisando assim o mesmo. Alegaram que só devolveriam os arquivos se receberem uma quantia estipulada de *bitcoin*, que é uma moeda digital.

Esse ataque foi de escala mundial, afetando 45 mil computadores em 74 países, com maior parte na Europa, onde foram atacados sistemas de hospitais, empresas de telecomunicações, bancos dentre outras empresas. A figura 3 mostra os países atacados no mundo:

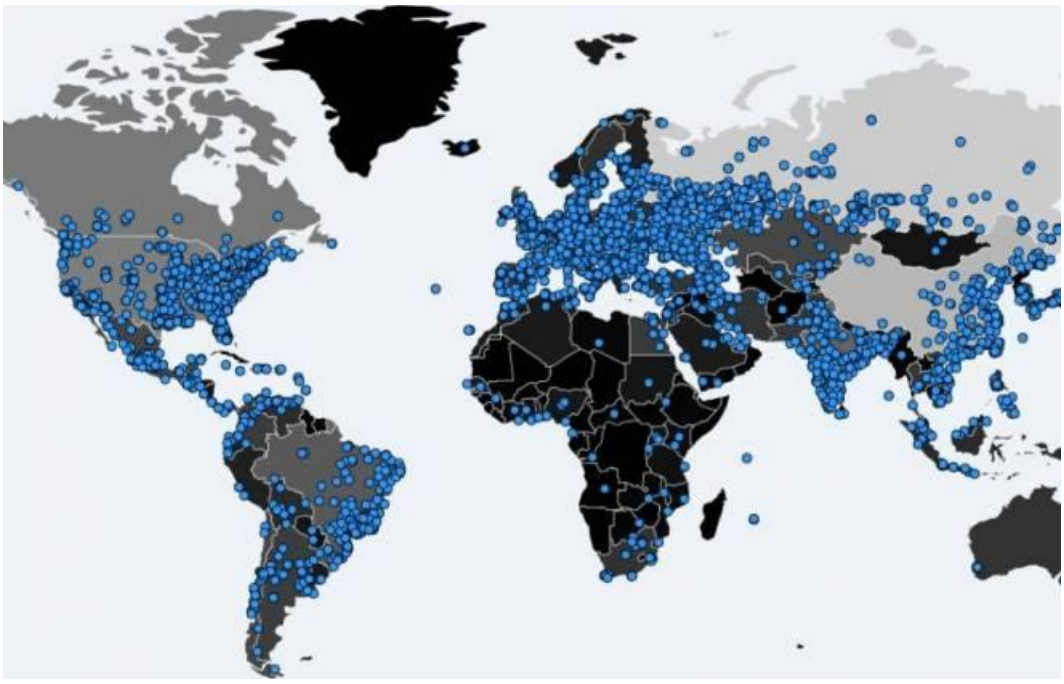

Figura 3- Países atacados.

Esses ataques mostram a vulnerabilidade das informações pessoas, até mesmo nas instituições onde trabalham, pois, uma simples técnica de Engenharia Social é capaz de fazer com que aja a perca de todos os dados de um computador ou até mesmo entregar dados importantes nas mãos de pessoas más intencionadas, o que pode causar grandes transtornos e problemas pela falta de cautela e pela falta de conhecimento.

Qualquer pessoa pode ser um engenheiro social, pois, os motivos giram em torno do comportamento humano, ou seja, qualquer ação que as pessoas fazem no dia a dia tem uma motivação ou uma razão para que sejam realizadas, como por exemplo: as pessoas que

praticam Engenharia Social com ataques diretos, sendo por rixa pessoal ou pela vontade de obter informações privilegiadas, sendo que com isso podem chantagear as vítimas com intuito de conseguir dinheiro ou oportunidades.

2.1 Tipos de Ataque

2.1.1 Ataque Direto

É quando se sabe quem é a vítima, ou seja, o atacante escolhe diretamente a vítima e busca capturar todos os dados necessários. Sendo que esse ataque pode ser executado com métodos computacionais e também com métodos pessoais.

2.1.2 Ataque Indireto

Não diferente do ataque direto, o ataque indireto também pode ser executado por métodos computacionais ou com métodos pessoais. O ataque indireto é quando não se tem uma vítima específica, ou seja, o atacante só ataca quem estiver susceptível no momento, um exemplo que se pode citar é: quando o atacante coloca um arquivo malicioso dentro de um *pen drive* e o deixa em algum lugar estratégico, onde a vítima por curiosidade usa-lo em algum dispositivo. Caso a vítima execute o arquivo malicioso o engenheiro poderá ter acesso ao dispositivo em que a vítima executou.

2.2 Processo da Engenharia Social

São sequências de processos que o Engenheiro Social usa para executar o ataque. Sendo elas:

2.2.1 Coleta de Informações

O engenheiro social busca extrair informações da vítima, seja com pessoas do mesmo ciclo de amizades, ciclo social ou acadêmico. Um exemplo é a troca de *e-mails*, redes sociais ou até de números telefônicos.

2.2.2 Desenvolvimento de Relacionamentos

Mitnik (2003) comenta que o relacionamento dentro do processo da Engenharia Social é da natureza humana confiar em nossos colegas, particularmente quando a solicitação passa no teste como sendo razoável. Os engenheiros sociais usam esse conhecimento para explorar suas vítimas e atingir seus objetivos.

Nessa etapa o engenheiro busca criar amizade com a vítima, até que a vítima confie no engenheiro social, para criar certa intimidade para o ataque.

2.2.3 Exploração de um Relacionamento

Quando o engenheiro já estiver conquistado à amizade/confiança da vítima, ele extrairá informações para o ataque.

2.2.4 Execução do Ataque

Após a coleta de todas as informações necessárias, onde já se criou um vínculo de amizade e confiança pela vítima, basta o engenheiro executar seu ataque.

2.3 Técnicas mais utilizadas

Existem várias técnicas utilizadas pelos engenheiros sociais para coleta de informações, sendo que as mais utilizadas são:

2.3.1 Análise do lixo

O lixo pode parecer algo descartável, onde qualquer outra pessoa não ira se interessar por ele, mas não para os engenheiros. No lixo existem várias informações ricas para os mesmos. As informações coletadas no lixo podem ter nomes de funcionários, telefone, senhas, telefones de clientes, transações efetuadas, entre outros. Ou seja, pode ser um dos primeiros passos para ataques de ES.

2.3.2 *Internet* e Redes sociais

Hoje, para descobrir informações de alguém basta pesquisar nas redes sociais. É uma das técnicas que engenheiros sociais usam para conhecer mais sobre seu alvo. Na internet e redes sociais há uma grande facilidade de encontrar informações como por exemplo: endereço, cargos, perfil pessoal, entre outros.

2.3.3 Contato Telefônico

Um exemplo de utilização dessa técnica é quando o engenheiro social se passa por um funcionário de uma empresa, fornecedor ou terceiros. Coletando informações de outros funcionários sem ser descoberto.

2.3.4 Abordagem Pessoal

É a técnica de abordagem no dia a dia, um exemplo é quando o engenheiro social vai até uma empresa e com sua técnica de persuasão, manipula algum funcionário até conseguir acesso facilmente do que deseja.

2.3.5 *Phishing*

Conhecido como “pescaria ou *e-mail* falso”, é umas das técnicas mais utilizadas por engenheiros sociais onde eles disparam milhões de *e-mails* com o intuito de que as vítimas façam o que se pede nos mesmos, a maioria desses *e-mails* falsos são de supostos bancos, Receita Federal, informando que estão irregulares. A maioria dos *Phishings* possuem algum anexo ou links que levam para a situação que o *Cracker* deseja.

2.3.6 Falhas Humanas

O ser humano tem muitas vulnerabilidades e algumas delas são: confiança, medo, curiosidade, instinto de querer ajudar, culpa, ingenuidade, entre outros. Com isso, o engenheiro social busca a confiança/intimidade da vítima para ela transmitir informações que ele precisa.

3 ANÁLISE COMPORTAMENTAL

Análise comportamental define-se como uma análise de todas as partes de um indivíduo, não só de comportamento/ações, mas sim de sentimentos, pensamentos e falas, sendo assim, estuda o comportamento humano a partir da interação entre organismo/ambiente. Segundo Baum (1994/1999) Skinner (1981) a análise comportamental são explicações de processos que não só envolve fatos atuais, mas sim ao decorrer do tempo/história esses processos de acontecimentos devem ser pesquisados e analisados, onde é com eles que explicam os determinados comportamentos do indivíduo. Existem três níveis de seleção de comportamento:

- Filogenético: São comportamentos adquiridos hereditariamente pela história de seleção da espécie.
- Ontogenético: São comportamentos adquiridos pela história vivencial do indivíduo, ou seja, sempre terá modificações de comportamento durante o tempo.
- Cultural: São restritos à espécie humana. São os comportamentos controlados por regras, estímulos verbais ou simbólicos, transmitidos e acumulados ao longo de gerações por meio da linguagem.

Já Metzger (1992) diz que a história comportamental é definida “em termos de exposições prévias a contingências tanto dentro quanto fora do laboratório”. Essa definição é muito abrangente, pois engloba os eventos extra experimentais como parte da definição de história comportamental, perdendo sua objetividade.

Outra definição também é da Wanchisen (1990). Segundo a autora, história comportamental diz respeito à “exposição a contingências respondentes e operantes cuidadosamente controladas em laboratório, antes da fase de ‘teste’ desejada”. Nessa definição são colocadas só as contingências no contexto experimental as quais o organismo foi exposto, antes de uma fase de teste específica.

A análise do comportamento se dá de modo bidirecional, ou seja, o comportamento do sujeito controla o ambiente e vice-versa, ou seja, fazer análise do comportamento é determinar as características/dimensões da ocasião.

De acordo com opiniões profissionais da área de psicologia, os engenheiros sociais se encaixam perfeitamente no nível Ontogenético, pois não sofrem de uma doença e sim de um desvio de personalidade adquirido com o tempo, podem ser definidos como pessoas que tendem a ser inteligentes, intensos, carismáticos e aprendem sobre o comportamento das vítimas ao observar suas reações, podem interferir em sentimentos variando discurso e comportamento. O engenheiro social tem um grande “poder” de persuasão onde usam suas

técnicas para fazer com que as vítimas soltem informações até mesmo sem perceber. Os principais alvos dos engenheiros sociais são a zona de conforto, negligência, compaixão, ansiedade e medo, por meio de conversa direta, persuasão, intimidação, coerção e extorsão.

Como dito, o engenheiro social explora a tendência natural de confiança do ser humano, e um meio evitar ataques não é só apenas combater por meios técnicos, mas também pelo meio pessoal, utilizando de conscientização e ate mesmo treinamento com as pessoas, pois segundo Mitnick (2003), quebrar a "*firewall* humana" quase sempre e fácil, não exige nenhum investimento além do custo de uma ligação telefônica, e envolve um risco mínimo.

3.1 Traços comportamentais e psicológicos que o torna suscetível a ataques de Engenharia Social

Nos traços comportamentais e psicológicos será citado sobre comportamentos e motivos do porquê as pessoas se tornam susceptíveis a ataques da Engenharia Social. Segundo Kevin Mitnik (2003):

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNIK, 2003, p.3).

Quando se fala em segurança não adianta ter todos os cuidados tecnológicos, de segurança se a maior vulnerabilidade são as próprias pessoas. Alguns fatores comportamentais e psicológicos que tornam as pessoas susceptíveis a ataques são:

- Vaidade Pessoal/Profissional: Pessoas são fáceis de agradar, de manter um relacionamento, ou seja, um simples elogio já ajuda a começar um relacionamento.
- Pessoas são curiosas: Qualquer enunciado chama atenção das pessoas, seja por marketing com pessoas famosas, por algo relacionado à saúde, por algo que a pessoa goste, etc...
- Gananciosas: O ser humano é ganancioso, quando se têm a oportunidades de ganhar dinheiro fácil e rápido se descuidam e pensando somente no dinheiro e deixando de lado a segurança.

- Autoconfiança: O ser humano tende a ter muita autoconfiança em si, como se o mesmo pensasse que nunca irá cair em uma ameaça na *internet*.
- Pessoas tendem a acreditar: As pessoas por si só acreditam em outras pessoas seja por boa vontade ou por falta de conhecimento no assunto.

4 KALI LINUX

Kali Linux é um Sistema Operacional (SO) com mais de 300 ferramentas para testes de invasão, penetração, *forense* entre outras e é utilizada por profissionais de segurança da informação. Era conhecido antigamente como *Backtrack*, criado pela equipe da *Offensive Security*. *BackTrack* era baseado no *Ubuntu*, enquanto hoje em dia *Kali Linux* é baseado no *Debian*.

O mesmo é um sistema gratuito, estável, confiável, múltiplos idiomas, customizável, tem suporte a inúmeros dispositivos *wireless* e pode ser complementado por uma vasta quantidade de aplicações desenvolvidas por terceiros.

Entrevistados neste trabalho relataram a utilização do Sistema Operacional *Kali Linux* por se tratar de um SO que oferece ferramentas diversas de *pentest*, como engenharia social e invasão. Sendo de código aberto, onde qualquer pessoa pode mudar seu código fonte, ou seja, de fácil utilização.

Pré-requisitos para instalação:

- 8 GB de espaço em disco para a instalação;
- No mínimo 512MB de RAM para as arquiteturas i386 e amd64;
- Suporte a boot pelo drive de CD-DVD / USB.

O Kali pode ser definido como "teste de penetração e auditoria de segurança", mas também existem muitas tarefas diferentes envolvidas por trás dessas atividades. Como por exemplo:

- Coleta de informações: Coleta dados da rede alvo e sua estrutura identificando computadores, seus Sistemas Operacionais e os serviços que eles executam.
- Análise de vulnerabilidade: Testa se um sistema local ou remoto é afetado por ameaças de vulnerabilidades conhecidas ou configurações inseguras.
- Análise de aplicativos da *Web*: Identifica configurações erradas e fraquezas de segurança na *web* aplicações.
- Avaliação de banco de dados: Existem ferramentas que testam vetores de ataque que vão desde injeção SQL para extração e análise de dados.
- Ataques de senha: Contém ferramentas de ataque de senha *online* até ataques *off-line* contra sistemas de criptografia ou *hashing*.
- Ataques sem fio: Kali é uma escolha óbvia para ataques contra múltiplos tipos de redes sem fio.

- *Reverse Engineering*: É um dos principais métodos de identificação de vulnerabilidade e usado também para analisar *malwares.*
- Ferramentas de exploração: Ferramentas que exploraram ou aproveitam uma vulnerabilidade, ou seja, da autoconfiança, curiosidade das pessoas e permitindo que controle de uma máquina remota (ou dispositivo).
- *Sniffing* & *Spoofing*: Usado para obter/extrair dados à medida que eles percorrem a rede, encontra ferramentas de falsificação que permitem representar um usuário legítimo.
- Exploração de postagens: Depois de ter obtido acesso a um sistema, mantém esse acesso ou ampliação do controle pela rede.
- Forense: Contêm várias ferramentas que permitem fazer tudo desde a triagem inicial até a imagem de dados, a análise completa e gerenciamento de casos.
- Ferramentas de Relatório: Ferramentas para ajudar a reunir as informações coletados da coleta de informações.
- Ferramentas de Engenharia Social: Existem ferramentas que ajudam explorar o comportamento humano como um vetor de ataque, ou seja, ser induzidos a tomar ações que comprometam a segurança do meio ambiente.
- Serviços do Sistema: Ferramentas que permitem que comece e pare aplicativos que são executados em segundo plano como serviços do sistema.

4.1 Características do Kali Linux

Mais de 300 ferramentas de teste de penetração: Contém várias ferramentas de invasão, exemplo:

- Software Livre: Como na versão antiga o Kali Linux é completamente gratuito.
- *Open Source Gittree*: A parte de desenvolvimento é disponível para todos verem e todas as fontes estão disponíveis para aqueles que desejam ajustar e reconstruir pacotes.
- FHS: Permite que todos os Usuários de Linux para localizem facilmente binários, arquivos de suporte, bibliotecas, etc.
- Ampla assistência em dispositivos sem fio: Criado para dispositivos sem fio como para outros, permitindo que seja compatível com vários dispositivos USB e outros dispositivos sem fio.

- Núcleo personalizado para corrigir injeção: A equipe de desenvolvimento faz análises sem fio para que o *kernel* tenha os últimos *patches* de injeção incluídos.
- Desenvolvimento seguro: É composto por um pequeno grupo de confiança, que só podem comprometer pacotes e interagir com os repositórios enquanto usam múltiplos protocolos.
- GPG assinou pacotes: Cada desenvolvedor individual assina seu pacote.
- Multilíngue: Contém suporte multilíngue, permitindo que mais usuários operem em qualquer idioma.
- Personalizável: Pode ser personalizado ao gosto do Usuário.
- Suporte ARMEL e ARMHF: O Kali está atualmente disponível para os seguintes dispositivos ARM e ARMHF.

4.2 Principais ferramentas para *Hackers* que contém no Kali Linux

4.2.1 Nmap

É uma ferramenta *free open source* utilizadas pelos *hackers*, utilizada para capturar informações específicas em máquinas, detecção de redes, análises e auditorias de segurança.

4.2.2 *Social Engineering Toolkit*

Também conhecido como SET, é desenvolvido para auxiliar em testes de penetração contra elementos humanos com ajuda da Engenharia Social, ou seja, utilizam pessoas porque são consideradas o elo mais fraco.

4.2.3 *Dnsenum*

É uma ferramenta para levantamento de informações de servidores DNS (*Domain Name System*, ou sistema de nomes de domínios), utilizado para pesquisar *hosts*, nomes de servidores, endereços IP (*Internet Protocol*), registros e outras informações, usando apenas de alguns comandos básicos.

4.2.4 *Nessus*

Criada pela *Tenable* é utilizada para realizar e analisar auditorias, executar escaneamentos, tem variedades de *plugins*, além de relatórios que podem ser gerados por meio de um *dashboard*.

4.2.5 *Cisco-Torch*

É utilizado para descobrir *hosts* da Cisco que usam protocolos SSH (*Secure Shell)*, Telnet, *Web*, NTP (*Network Time Protocol*) e SNTP (*Simple Network Time Protocol).* Utilizado também, constantemente para *forking* (bifurcação) para lançar a múltiplos processos de varredura em segundo plano. De acordo com o *HackingExposed Cisco Networks*, isso maximiza a eficiência na detecção de vulnerabilidades.

4.3 Aplicações *Web* (*Web Applications*)

São programas que rodam em servidores *web* e são acessados via *browser*.

4.3.1 *Nikto*

É um programa para analisar a vulnerabilidade de um *site*. É uma aplicação que verifica configurações do servidor, exerce uma análise que podem ser atualizados automaticamente, consulta versões desatualizadas e testam arquivos e programas perigosos que estão na *internet*.

4.3.2 *Parsero*

É um *script* que faz leitura do arquivo Robot.txt de um servidor *web* fazendo com que analise entradas não autorizadas, levando os navegadores de busca como Google, Bing, entre outros, onde arquivos ou diretórios hospedados no servidor não devem ser indexados pelo robô.

4.3.3 *Wapiti*

É uma ferramenta que analisa as páginas *web* nos quais possa injetar dados, testando as vulnerabilidades, permite também testes “*black-box*”, é um método que analisa recursos de uma aplicação sem verificar as estruturas internas.

4.3.4 Owasp Zap

É uma ferramenta gratuita e de fácil uso e foi desenvolvida por vários voluntários, a mesma está disponível em mais de 20 idiomas e tem a função de encontrar vulnerabilidades na segurança de aplicação de *web*. de encontrar vulnerabilidades na segurança de aplicações web.

4.3.5 *Veja*

É uma ferramenta *open source*, com funcionalidade de analisar vulnerabilidades e testes, detectar erros, análise de conteúdo, *Cross Site Scriping (XXS)* e *SQL injection*, desenvolvida em Java e de interface gráfica. Difere-se das outras ferramentas pelo seu *scan* que executa testes rápidos para detectar erros e vulnerabilidades e o fato de a ferramenta ser expansível, graças à sua *API Javascript*.

4.3.6 *Wireshark*

É uma ferramenta do Kali Linux que tem o intuito de analisar redes, obter riscos, captura, análise e filtragem de pacotes em tempo real, importação e exportação de arquivos e inspeção de centenas de protocolos.

5 FERRAMENTA SET *(SOCIAL ENGINEER TOOLKIT)*

A ferramenta SET (*SOCIAL ENGINEER TOOLKIT*) inclui ferramentas que permitem atacar ou testar um alvo, usando o ato de enganação. Além de ser simples de ser usada é muito fácil de ser encontrada na *internet*, como nos *sites: www.trustdSec.com/downloads*, Distribuição *Backtrack*, Distribuição de *Kali Linux*. A mesma é desenvolvida em *Python* e foi criada por David Kennedy, fundador da companhia *TrustdSec*. A *TrustedSec* foi criada pelo fato da indústria de segurança da informação ser carente de serviços de segurança (*Pentest*).

5.1 Objetivo da ferramenta SET

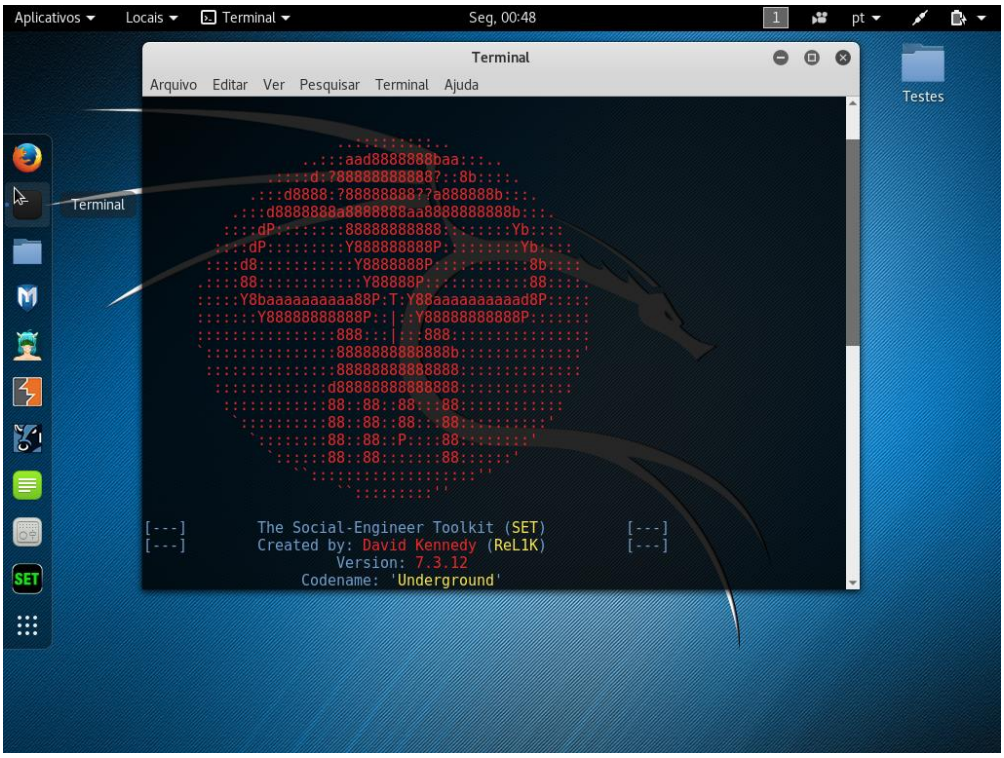

Figura 4– Inicialização da SET.

O objetivo da SET é fazer testes de penetração e trazer consciência para ataques de engenharia social. Ou seja, tem como objetivo e alvo fraquezas humanas, exploração de credibilidade, curiosidade, avareza, e a estupidez humana, sendo que seus ataques mais utilizados são com:

- *Email* falso/*Phishing;*
- Clonagem de *Website;*
- *QRCode.*

5.2 Tipos de Ataques

5.2.1 *Spear-Phishing Attack Vectors*

Este método é usado para realizar ataques de *e-mail*. Um exemplo é um PDF infectado no anexo a fim de comprometer o sistema. Relatado pelo policial federal na entrevista para este trabalho, esse é o tipo de ataque mais utilizado ultimamente.

5.2.2 *Website Attack Vectors*

É utilizado para realizar ataques em navegadores *web*, onde clona *sites*, intercepta a comunicação, criar abas nos navegadores, rouba credenciais, abre *poup-up* do Java para instalar *malwares*, entre outros.

5.2.3 *Infectious Media Generator*

O módulo de infeção dos dispositivos USB/CD/DVD irá criar um arquivo *autorun.inf* utilizando um *Payload* do *Metasploit*. Quando a USB/CD/DVD é inserida, ele será automaticamente executado se a execução automática estiver avançada.

5.2.4 *Create a Payloadand Listener*

O "*Payload*" normalmente é gerado pelo *Metasploit* resultado em um arquivo chamado "*msf.exe*", este arquivo pode ser renomeado e é necessário que a vítima realize o *download* e execute-o para o atacante ganhar acesso ao computador.

5.2.5 *Mass Mailer Attack*

Este método é usado para realizar ataques simultaneamente de forma aleatórias por *e-mail*, enviando *links* maliciosos, a fim de comprometer o sistema.

5.2.6 *Arduino-Based Attack Vector*

Esse ataque utiliza Arduido para programar e controlar o dispositivo. É uma plataforma de prototipagem eletrônica de *hardware* e *software* livres, com um micro controlador de placa única e suporte de entrada/saída.

5.2.7 *SMS Spoofing Attack Vector*

É um ataque onde criam mensagens via SMS e envia mensagens falsas para vítimas, na qual pode falsificar até a origem da mensagem.

5.2.8 *Wireless Access Point Attack Vector*

É um ataque onde é configurado um ponto de acesso sem fio falso e com isso direcionar a vítima para o tráfego de rede do atacante.

5.2.9 *QRCode Generator Attack Vector*

É um ataque onde cria um *QRCode* que quiser (malicioso) para ser redirecionado para um *site* falso.

5.2.10 *PowerShell Attack Vectors*

É um ataque onde você cria *malwares* para ataque, com esse ataque permite acesso total da máquina da vítima usado o *PoweShell* que contém de padrão no *Windows*.

5.2.11 *Third Party Modules*

É um ataque de terceiros, onde pode fazer clonagem de *sites* utilizando o modulo *Java AppletAttack*, e criação de *keylogers* e *Trjans* com o intuito de desconfigurar sistemas de segurança como antivírus e IPS.

6 TESTE EM AMBIENTE CONTROLADO

No dia 06 de outubro de 2017, na Universidade Estadual de Goiás, foi realizado um teste em ambiente controlado, para testar o comportamento e a vulnerabilidade das pessoas, e qual seria o grau de dificuldade para a captura de dados.

A escolha por esse dia deu-se a partir das entrevistas realizadas com psicólogos que permitiu o entendimento da necessidade de alcançar a confiança das vítimas, sendo o cenário propício para o teste.

A primeira etapa do ataque foi a “coleta de dados”, onde foi observado que havia sido aberto um questionário denominado Questionário Institucional, no portal da UEG (onde todos os alunos deveriam acessar o sistema para responder).

A segunda etapa foi o "Vetor de Ataque", quando foi planejada a forma que o ataque aconteceria, baseando-se em computadores, utilizamos a ferramenta SET (*Social-Engineering Toolkit*) do *Kali Linux*, onde foi clonado o portal da UEG (https://www.adms.ueg.br/auth/acesso/index). Com intuito de capturar os dados de *login* e senha do usuário que acessasse.

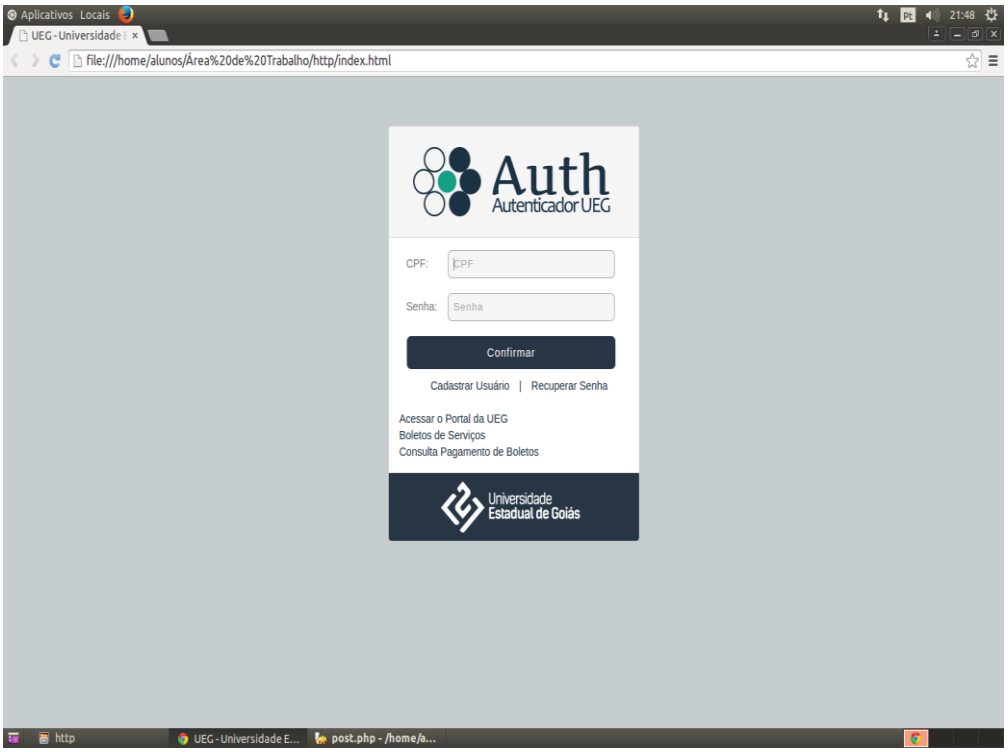

Figura 5– Clonagem Portal da UEG

De acordo com o planejamento, foi decidido que o teste seria aplicado em um dos laboratórios de informática da Universidade, pois seria um local onde poderia controlar o

ataque, e seria executado durante a aula do professor e orientador deste; tudo deveria ser preparado na etapa da execução.

A terceira etapa foi a "confiança", que se resume em ter certa confiança/intimidade com os alunos/vítima, com isso, foi preparado o ambiente, após a ferramenta ser desenvolvida e colocada como página principal do navegador Mozilla Firefox em todos os computadores. E no início da aula foi disponibilizado um pequeno tempo para que todos os alunos respondessem o questionário, tendo o laboratório à disposição.

O primeiro passo para criação do ataque foi instalação do *Kali Linux* em uma máquina virtual. Logo após a instalação, a máquina foi ligada e em seguida aberto a ferramenta SET (*Social-Engineering Toolkit*), e selecionar a opção *1) Social-Engineering Attacks*, que é a opção para ataques de engenharia social, como mostra figura abaixo:

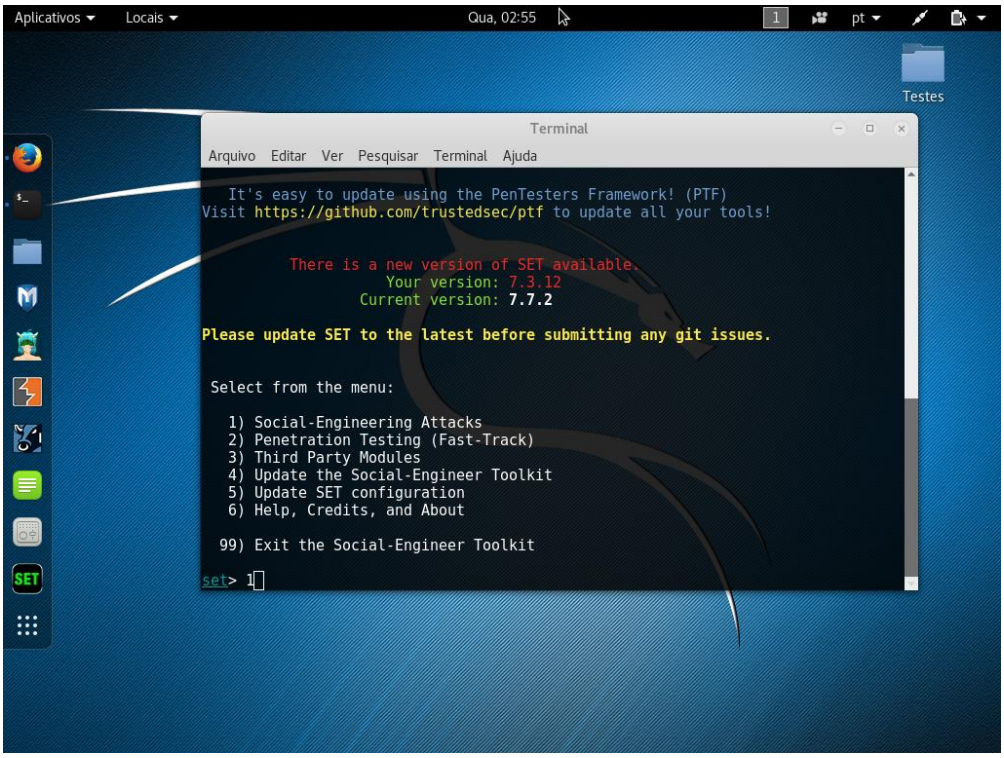

Figura 6- Escolha de ataque.

O segundo passo é selecionar a opção *2) Website Attack Vectors*, que é responsável por selecionar os vetores de ataque do *site*.

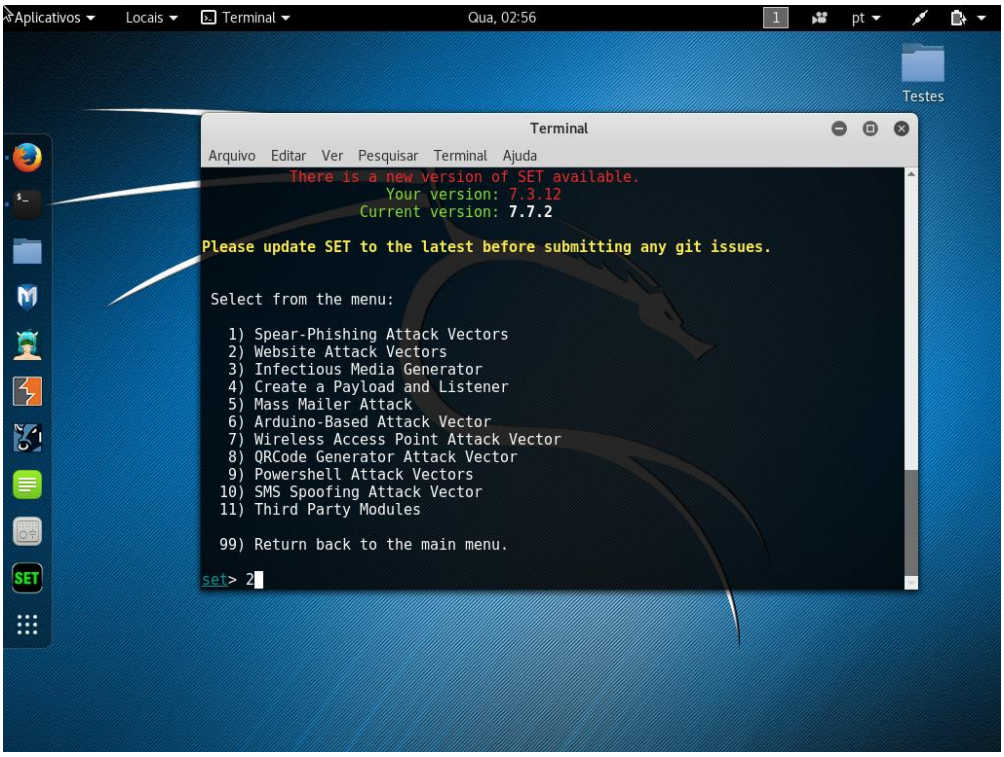

Figura 7 – Tipos de vetores de ataques.

O terceiro passo é selecionar a opção *3) Credential Harvester Attack Method*, que é a opção responsável pela coleta de credenciais.

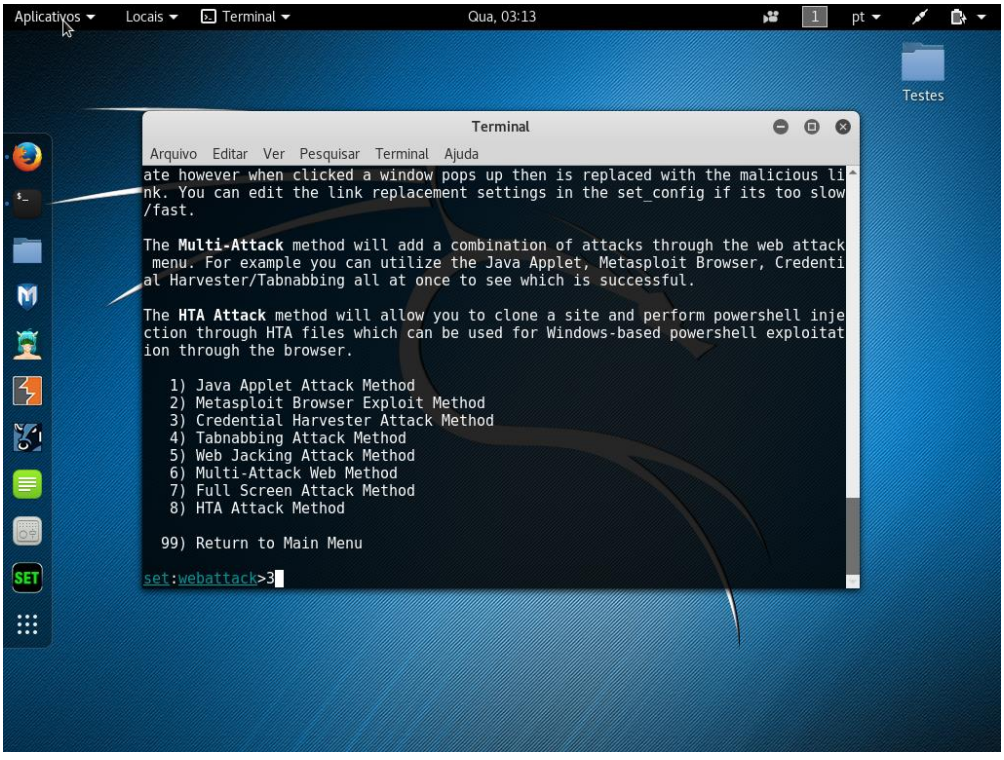

Figura 8– Colheita de credenciais.

O quarto passo é selecionar a opção *2) Site Cloner*, que é opção responsável pela clonagem do *site* desejado.

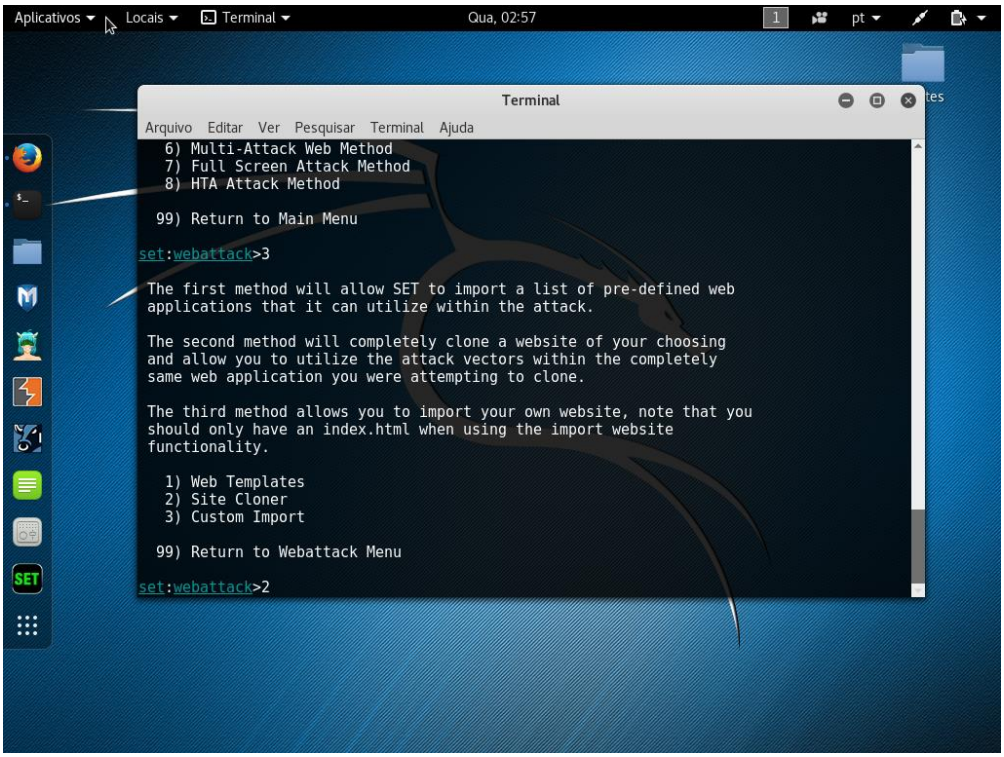

Figura 9– Clonagem do site

O quinto passo é digitar o IP do atacante, na qual os dados seriam enviados.

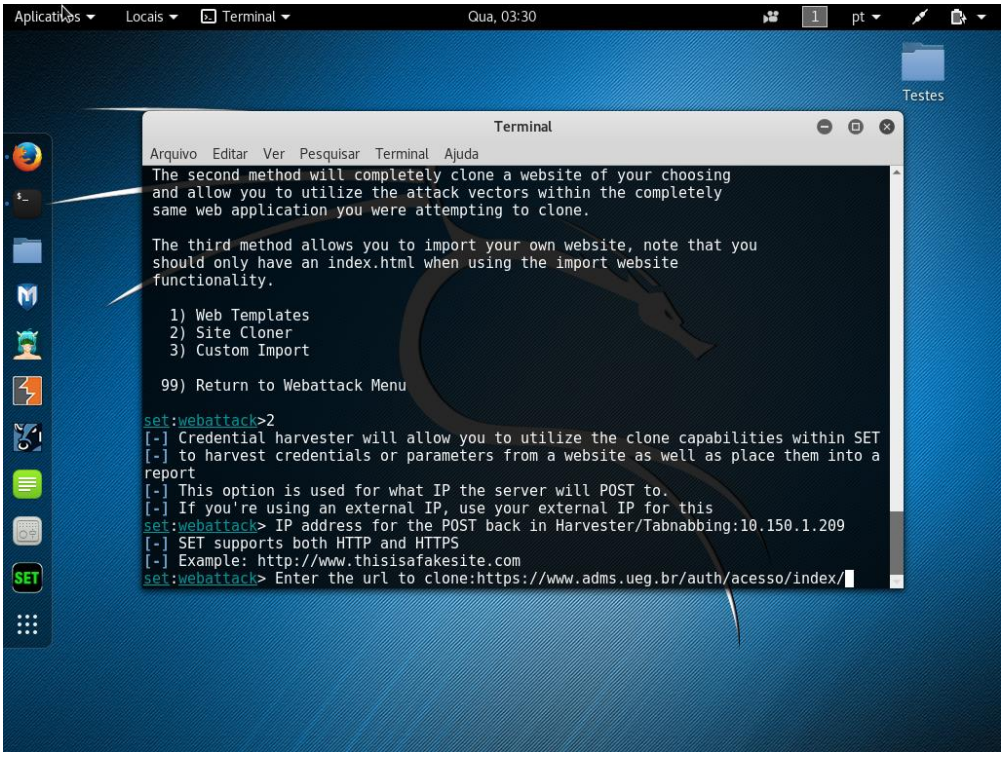

Figura 10– IP's de rede e site de destino.

Na pasta www/var/html do computador do atacante, foi gerado três arquivos, o primeiro arquivo é .txt, arquivo que estará as informações capturadas; o arquivo .html o responsável pela construção do *site* clonado e o arquivo .php, o arquivo responsável por ser aberto nos computadores, sendo conectado com o arquivo .html..

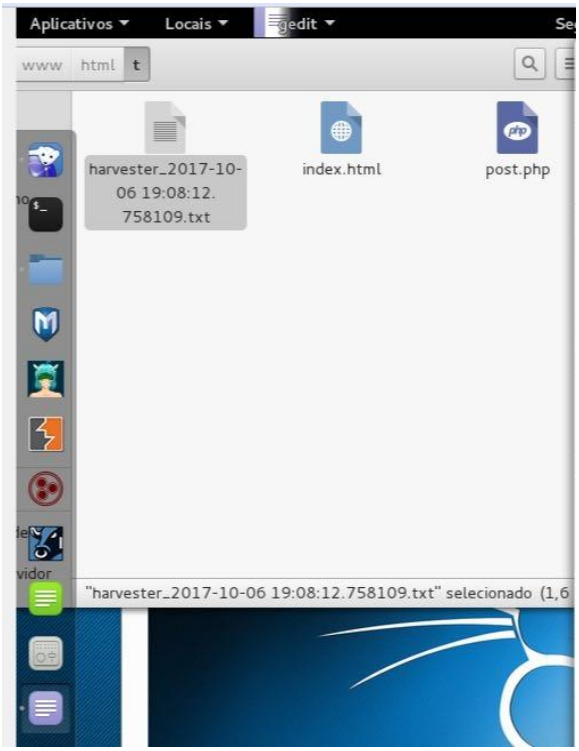

Figura 11– Arquivos criados após clonagem.

A quarta e última é a etapa da "execução", onde foi executado o teste, e foram colocados em todos os computadores do laboratório os arquivos de clonagem, a página de clonagem foi colocada como a página inicial da *internet*, para que sempre que abra o navegador, o *site* de clonagem seja aberto.

Após o teste ser realmente executado foi notado que todos os alunos acessaram o sistema sem perceber qualquer alteração, o professor abriu um espaço para que fosse explicado que estavam susceptíveis a ataques de engenharia social, verificou junto com os demais a página clonada e os detalhes que identificaram como falsa. Os alunos foram orientados que mudassem a senha imediatamente e também mostrada à forma que foi feito o teste com a ferramenta SET (*Social-Engineering Toolkit*) especificando passo a passo.

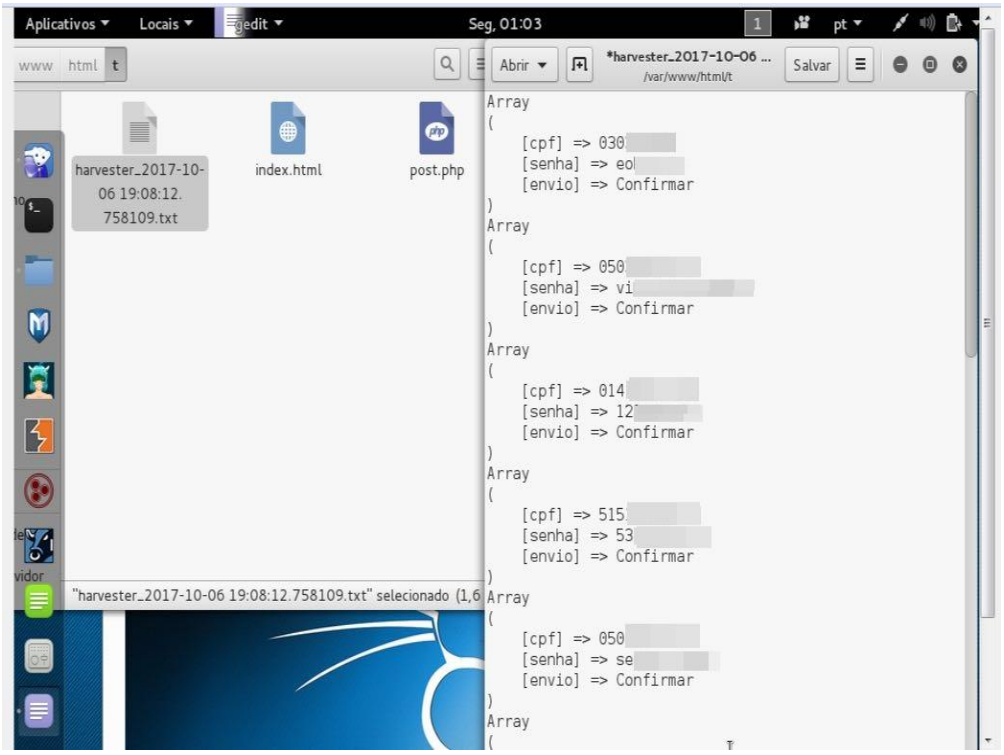

Figura 12– Dados capturados.

Foi concluído que, a Engenharia Social junto com a ferramenta SET (*Social-Engineering Toolkit*), além de ser muito fácil de usar, o resultado é muito satisfatório, conforme o teste executado foi identificado que as pessoas são fáceis de manipular e também são muito vulneráveis. A partir desses dados mostrados na Figura 12, observa-se que quando se trata de confiança/intimidade o engenheiro terá 100% de chances de concluir o que deseja, nota-se também que hoje em dia às pessoas estão muito dispersas em relação à segurança da informação, se auto tornando vítimas, onde na maioria das vezes nem imaginam que estão sendo manipulados.

7 BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE ACADÊMICO

Engenharia social é como um quebra cabeça, com a ajuda da falha humana um engenheiro social consegue juntar todas as peças facilmente. Uma pessoa não precisa ser especialista em tecnologia para saber se está sofrendo um ataque, basta saber se questionar em momentos cruciais e nunca divulgar informações confidenciais ou até mesmo informações não confidenciais sobre qualquer pessoa ou empresa que trabalha a não ser que conheça a pessoa para ter a necessidade de ter certas informações, onde um dos únicos meios de amenizar a ameaça da engenharia social é usar a conscientização para a segurança com as boas práticas de segurança da informação que definem as principais regras para o comportamento de todos no meio acadêmico, junto com sua educação e treinamento. É preciso antes de tudo, cercar o ambiente de informações elaborando e adotando boas práticas de segurança no intuito de minimizar os riscos a segurança. Algumas prevenções são:

- Treinar e educar os acadêmicos: Mostrar aos acadêmicos o quanto podem ser vulneráveis a diversas situações e fazer com que eles tenham consciência disso e fiquem mais espertos diante de certos acontecimentos, que fiquem cientes.
- Demonstrar o valor da Informação: Hoje em dia só dão valor depois que perdem algo, onde mostrará o valor das informações, onde a maioria delas é armazenada em dispositivos eletrônicos, com isso estão cada vez mais expostas a riscos.
- Desconfiar sempre: Ter muito cuidado ao falar informações para um estranho ao telefone. Não importa se a pessoa se apresenta de modo persuasivo ou formal, nenhuma informação deve ser fornecida além daquelas designadas como publicamente disponíveis depois ou até que você saiba quem está do outro lado da linha. Como Kevin Mitnick diz:

  > Essa é uma questão tão importante que a reitero em todo este livro: verifique, verifique e verifique novamente. Toda solicitação que não seja feita pessoalmente nunca deve ser aceita sem a verificação da identidade do solicitante, ponto. (MITNIK; SIMON, 2003, p.153).

- Tratar o lixo com respeito: As pessoas deveriam ter algumas atitudes não só em empresas, mas em casa e na Universidade também em questão do descarte do lixo, onde contém informações confidenciais. Antes desses descartes deveria passar primeiro por uma máquina cortadora de papel ou até mesmo serem queimadas e também ter um modo de apagar completamente as informações confidenciais dos dispositivos usados para armazenar os mesmos antes de descartá-los.

- Restringir acesso a informações: Quando se fala em informações devesse mantê-las em segurança e só poucas pessoas ter acessos a elas. Contém alguns sistemas onde tem controles em que se a pessoa tentar acessar um arquivo protegido fica registrado essas ações, sendo que dê certo ou não.
- Política de Segurança da Informação: As políticas de segurança são instruções que fornecem orientações de comportamento para pessoas para guardar as informações, e são muito importantes para não cair possíveis ameaças à segurança. Com isso configurar quantidades de tentativas de *login* para que se uma pessoa tentar acessar informações e ela errar uma determinada vez a conta seja bloqueada ou também exigir o uso de senhas difíceis.
- Utilizar antivírus e senhas difíceis: Esses métodos ajudam muito a dificultar que um engenheiro social acesse informações com uma conscientização para pessoas sobre seus comportamentos.
- Ter cuidado ao acessar contas/*e-mails* em computadores da Universidade: Maioria dos acadêmicos acessam contas e *e-mails* nos computadores da Universidade e a maioria não saiam corretamente dos mesmos, fazendo que outra pessoa acesse naturalmente suas contas.
- Não abrir certos dispositivos de armazenamento: Não conecte CD/DVD/USB se houver encontrado ou que você não sabe de onde vem em dispositivos eletrônicos, pode haver arquivos executáveis maliciosos neles.
- Não ter a mesma senha para várias contas: Isso faz com que fique mais fácil para engenheiros conseguirem acessar dados.
- Ter atenção aos *links* de acessos: Ou seja, prestar mais atenção quando for entrar em *sites* para não ser direcionado para outro destino, sempre ver se tem o https:// na barra de endereço.
- Perda de Confidencialidade: Não deixar nenhuma conta/*e-mails* já conectado no computador, fazendo com que facilite a invasão da confidencialidade.
- Atualização: Ameaças são descobertas todos os dias, e os sistemas e antivírus dos acadêmicos devem atualizar sempre para que seja contida as ameaças novas.
- *Firewall*: Sempre verificar se o *firewall* está ativado, pois esse programa age como uma barreira de proteção contra acessos maliciosos.
- Programas: Os acadêmicos devem sempre estar atentos sobre como baixam os programas, sendo nos computadores da Universidade ou no pessoal. Uma dica

> muito importante é que sempre quando se for baixar algum programa, baixar no *site* oficial do mesmo.

Esse capítulo de Boas Práticas da Segurança da Informação no Ambiente Academico deu-se através de pesquisas na *internet* e também através de opinião de profissional da área de Polícia Forense, Especialista em Segurança da informação e também profissionais na área de psicologia, sendo que esse capítulo poderá, em futuros trabalhos, se tornar material gráfico para melhor orientação da comunidade acadêmica.

8 CONSIDERAÇÕES FINAIS

A partir deste trabalho propôs como objetivo geral, mostrar a vulnerabilidade das pessoas pelo teste feito, criando uma cartilha de boas maneiras para que pessoas que talvez não conheçam e não entendem muito do assunto, possa se prevenir e evitar ataques.

Através das entrevistas feitas com o policial forense, psicólogos e especialista na área de segurança da informação foi possível comprovar do quanto o ser humano é frágil, e que pode sim ser considerado o elo mais fraco pelo fato de confiar nas pessoas.

As entrevistas com os profissionais foram muito empolgantes, pois os mesmos mostraram interesse sobre assunto, e se disponibilizaram para ajuda sempre que necessário, e assim mostrando que o presente trabalho seria realmente útil.

Foram encontradas dificuldades pela escassez de livros sobre os assuntos abordados, porém sempre que necessário o orientador e a Universidade deram apoio auxiliando em todos os aspectos.

Este estudo, embora suas limitações possam proporcionar grandes contribuições a seus leitores do meio acadêmico, uma vez que pode servir para o acréscimo de conhecimentos para trabalhos futuros, e para conscientização no ambiente acadêmico.

Almeja-se em trabalhos futuros a ampliação deste manual de boas práticas, a fim de construir um material gráfico-visual, que poderá servir de suporte a todos quanto desejar apreciar sua leitura.

Finalizando esse trabalho, permitindo a disseminação de conhecimentos mais amplos sobre o assunto, e com grande expectativa que todos que tenham acesso a este, também consigam ter um conhecimento maior.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, C.B. **Segurança da informação *vs* engenharia social.** Disponível em: <http://www.administradores.com.br/_resources/files/_modules/academics/academics_3635_20101207234707794d.pdf >. Acesso em: 15 de junho de 2017.

BOCK, A. M.B. **Psicologias, uma introdução ao estudo da psicologia.** Disponível em: <http://resgatebrasiliavirtual.com.br/moodle/file.php/1/E-book/Ebooks_para_download/Psicologia_do_Trabalho/Psicologia_-_Uma_Introducao_ao_Estudo_de_Psicologia.pdf >. Acesso em: 15 de junho de 2017.

Cert.br. **Sobre o Cert.br**. Disponível em: <https://www.cert.br/sobre/>. Acesso em: 16 de junho de 2017.

Cert.br. **Incidentes Reportados ao CERT.br.** Disponível em: <https://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque-acumulado.html>. Acesso em: 15 de junho de 2017.

E-tinet. **Ferramentas para hackers que podem ser usadas no KALI Linux.** Disponível em: <http://e-tinet.com/linux/27-ferramentas-hackers-kali-linux-parte-1/>. Acesso em: 06 de novembro 2017.

G1. **Golpe do falso sequestro aplicado por telefone ganha nova versão**. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2015/07/golpe-do-falso-sequestro-aplicado-por-telefone-ganha-nova-versao.html>. Acesso em: 16 de março de 2017

HADNAGY, Christopher, **Social Engineering The Art Of Human Hacking.** Disponível em: <https://www.pdf-archive.com/2014/06/02/social-engineering-the-art-of-human-hacking/>. Acesso em: 19 de maio de 2017.

HERTZOG, Raphaël; O'GORMAN, Jim; AHARONI, Mati (Org.). **Kali Linux Revealed: Mastering the Penetration Testing Distribution.** USA: OFFSEC PRESS, 2017. 344 p. Disponível em: <https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf>. Acesso em: 06 de novembro 2017.

Alerta Security. **Segurança da informação: entenda as principais ameaças.** Disponível em: <https://www.alertasecurity.com.br/blog/188-seguranca-da-informacao-entenda-as-principais-ameacas>. Acesso em: 19 de maio de 2017.

Olhar Digital. **Onda de ataques hackers se espalha pelo mundo; veja o mapa atualizado.** Disponível em: <https://olhardigital.uol.com.br/fique_seguro/noticia/onda-de-ataques-hackers-se-espalha-pelo-mundo-veja-o-mapa-atualizado/68259>. Acesso em: 19 de maio de 2017.

Olhar Digital. **Entenda o ciberataque que afetou mais de 45 mil PCs em 74 países.** Disponível em: <https://olhardigital.uol.com.br/fique_seguro/noticia/entenda-o-ciberataque-que-afetou-mais-de-45-mil-pcs-em-74-paises-hoje/68253>. Acesso em: 19 de maio de 2017.

Olhar Digital. **Entenda o que é Segurança da Informação e reduza riscos na empresa** Disponível em: <https://www.alertasecurity.com.br/blog/117-entenda-o-que-e-seguranca-da-informacao-e-reduza-riscos-na-empresa>. Acesso em: 19 de maio de 2017.

Psicologado. **O conceito de análise comportamental.** Disponível em: <https://psicologado.com/abordagens/comportamental/o-conceito-de-analise-do-comportamento>. Acesso em: 03 de setembro de 2017.

Profissionais TI. **Engenharia social: as técnicas de ataques mais utilizadas,** Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em: 17 de agosto de 2017.

Rede PSI. **Análise do comportamento e prática clínica**. Disponível em: <http://www.redepsi.com.br/2009/03/23/an-lise-do-comportamento-e-pr-tica-cl-nica/>. Acesso em: 05 de setembro de 2017.

Tecnicas de invasão. **Você sabe o que é o KALI Linux?** Disponível em: <https://tecnicasdeinvasao.com/linux/kali-linux/voce-sabe-o-que-e-o-kali-linux/>. Acesso em: 05 de novembro de 2017.

Tec Mundo. **Quem é Kevin Mitnick?.** Disponível em: <https://www.tecmundo.com.br/historia/1842-quem-e-kevin-mitnick-.htm>. Acesso em: 14 de março de 2017.

Terra. **SPAM/Hacker**. Disponível em: <https://duvidas.terra.com.br/duvidas/558/o-que-e-engenharia-social-e-que-exemplos-podem-ser-citados-sobre-este-metodo-de-ataque>. Acesso em: 14 de março de 2017.

Treinamento em Técnicas de Invasão. **Você sabe o que é o Kali Linux?.** Disponível em: <https://tecnicasdeinvasao.com/linux/kali-linux/voce-sabe-o-que-e-o-kali-linux/> Acesso em: 09 de Setembro de 2017.

Tech tudo. **O que é Ransowmare?**. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 19 de maio de 2017.

WEIL, P. e TOMPAKOW R. **Adoramos ler: O corpo fala.** Disponível em**:** <https://docs.google.com/file/d/0B5CK2xfgallpeWJQMHpvY05DR28/edit?pli=1> Acesso em: 27 de maio de 2017.

YouTube. **Engenharia Social (Segurança da Informação)**. Disponível em: <https://www.youtube.com/watch?v=cK1k0NABPhs> Acesso em: 20 de agosto de 2017.

ALBERTO ALVES, Gustavo. **Segurança da informação**: **Uma visão inovadora da gestão.** 1. Ed. Rio de Janeiro: Ciência Moderna Ltda, 2006 1 p.

BAUM, W. **Compreender o Behaviorismo: Ciência, Comportamento e Cultura**. Porto Alegre: Ed. Artes Médicas Sul, 1999.

HACKENBERG, T. D. Jacques Loeb, B. F. Skinner, and the Legacy of Prediction and Control. **The Behavior Analyst, v. 18**, n. 2, 1995, pp. 225-236.

HAYDU, Verônica Bender; FORNAZARI, Silvia Aparecida; ESTANISLAU, Célio Roberto (Org.). **Psicologia e análise do comportamento: conceituações e aplicações à educação, organizações, saúde e clínica.** Londrina: Humanidades Comunicação Geral, 2014. 560 p.

METZGER, B. (1992). **Stimulus control of behavioral history and s ubsequent □xed-interval performance.** (Unpublished doctoral dissertation). Departament o f Exper imental Psycholog y, West Virginia University, West Virg inia . p.15

MITNICK, Kevin D.; SIMON, William L. MITNICK - **A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: José Martins Braga, 2003. 286 p.

WANCHISEN, B. A . (1990). **Forgetting the lessons of history.** Behavior Anal yst, p.32.

APÊNDICE A – TRANSCRIÇÃO DAS ENTREVISTAS

ENTREVISTA 1

Nome: Alexandre de Moreira Vaz

Cargo: Perito Criminal

Tempo de Serviço: 10 Anos

Formação Acadêmica: Ciências da Computação.

1. Como você define um Hacker?

R- Definição atual, e que o hacker é uma pessoa com conhecimento técnico profundo sobre a área de computação, independente se ele e um desenvolvedor ou um grande conhecedor da área de suporte técnico ou de redes, e que costuma ter um conhecimento acima da média que possibilita que ele faça operações que a maioria das pessoas que estuda informática não consegue. Mas hacker e um nome que utilizamos basicamente para duas vertentes, pessoas que utilizam esses conhecimentos para algum trabalho útil (do bem) e pessoas que utilizam para um trabalho que vai prejudicar alguém, para cometimento de algum crime ou ação delituosa, mas nesse caso nós preferimos utilizar o termo cracker.

2. Dos vários casos já vistos nesta área, qual foi o que mais te surpreendeu? Por quê?

R- Vários casos são surpreendem porem houve um caso bem notório e conhecido onde um rapaz foi preso várias vezes, e vem atuando desde 2006 e é recorrente o caso de atuação dele com furto de dados sigilosos, dados de cartão de credito, invasão de contas bancarias de pessoas que recebem e-mails através de listas que são obtidas e vendidas na internet. Esse caso de reincidência foi bem surpreendente, pois fomos e prendemos o indivíduo, o mesmo ficou preso durante um tempo e começou a responder o processo, sai e continua novamente a realizar as ações delituosas, e assim continuamente várias vezes. O que o indivíduo fez, foi desenvolver as técnicas que ele utilizava, da década passada para cá, ele desenvolveu novas técnicas, novas metodologias de ataque e de furto e de engenharia social para conseguir esses feitos. E o mesmo foi pego cometendo um outro delito que acabou com que ele ficasse preso, onde foi mais importante esse outro delito do que os próprios delitos de desvio de dinheiros de conta bancarias e clonagens de cartão, foi encontrado no computador dele material pornográfico envolvendo crianças e adolescentes, e por isso ele ficou preso. E mais me

surpreendeu pelo fato de que nada mantinha ele preso em relação aos crimes de estelionato e furto e os crimes que agora estão enquadrados na nova lei de crimes cibernéticos.

3. Quais as ferramentas mais utilizadas por vocês forenses, sendo elas pagas ou gratuitas?

R- Nos utilizamos algumas ferramentas, sendo que algumas eu não posso comentar, mas outras sim, por exemplo, a *Forensic Toolkit* (FTK), que e uma ferramentas bem interessantes, mas nos utilizamos no momento principalmente ferramentas desenvolvidas na polícia federal, temos uma equipe excepcional, em termos percentuais nos temos na perícia um quantitativo de doutores e mestres muito grandes, e um dos locais do governo executivo onde existe mais doutores no país, então os mesmos conseguem por conta própria desenvolverem as ferramentas de análise forense e também compramos outras como para análise de equipamentos celulares, ferramentas que possibilitam a gravação de dados que estão trafegando pela rede, mas basicamente as ferramentas mais utilizadas são desenvolvidas dentro da própria polícia.

4. Como os usuários podem fazer para evitarem ataques?

R- Primeiramente o usuário deve ter consciência que não existe um sistema totalmente seguro em nenhum lugar do mundo. Segundo ponto, você deve ter consciência de que alguns sistemas são mais vulneráveis que outros, quanto mais conhecido e utilizado um sistema, mais vulnerável ele vai ser. Se você utiliza um sistema operacional como o Windows da Microsoft, com certeza você estará mais vulnerável a ataques do que um sistema como o Mac OS (Apple), que e utilizado por muitas pessoas mas o grupo de usuários e bem menor, por ser computadores caríssimos, que boa parte da população não terão acesso, então ai você terá uma quantidade menor de pessoas com intuito de criar um conjunto de códigos maliciosos para furtar dados. Terceiro você tendo um sistema operacional, você terá que ter as ferramentas que identifiquem, seja automaticamente ou seja em varreduras diárias ou semanais, possíveis ataques, seja com firewall ou com ferramenta integrada como e o caso atual da Microsoft, ou seja uma ferramenta comprada, não recomendo você a baixar qualquer ferramenta aleatoriamente sem ser em um site confiável, lembrando que se usar antivírus gratuito ele terá suas limitações, eu particularmente compro o antivírus, pois assim sei que terei mais benefícios um banco de dados mais amplo em termo de defesas existentes nessa ferramenta, por que ao invés de usar só como varredura, pode possibilitar que eu integre junto dela um firewall, pode possibilitar que eu crie filtros de endereços de IP, dentre outras

funções, então tendo o anti vírus mais seguro possível em termos de qualidade com que ele foi desenvolvido, e atualizado. Eu atualizo no mínimo cinco vezes por semana o antivírus, então aí você já tem uma ferramenta que vai fazer o seu muro inicial de bloqueio para ataques e uma outra ferramenta caso você deseje, pois e bom ter mais de uma ferramenta no computador. E o acesso a sites, e bom verificar se esses sites possuem segurança integrada, quando for transmitir dados, ver se tem o protocolo https, transmitindo via ssl, se os dados estão trafegando de forma criptografada, observar se tem um cadeado quando estiver acessando em qualquer tipo de browser, utilizar browsers que tenha alguma segurança integrada (Chrome, Opera). Outra coisa, e observar que quando você acessa um site qualquer, quando for fazer cadastro, ter senhas diferentes para quase todos sites, não usar nenhuma senha igual em todos sites. São as sugestões básicas para você evitar qualquer ataque. Tivemos um caso do Wanna Cry, que infectou milhares de computadores no mundo, onde muitas pessoas perderam seus dados por não fazerem backup.

5. Quais os ataques mais frequentes?

R- O mais frequente e o que a própria pessoa se deixa atacar, onde ela abre o próprio e-mail com um link ou arquivo malicioso e executar o mesmo, que vai rodar um código. E o phishing/scam enviados através de spams, e é o tipo de ataque que mais acontece, pois, ser o que mais dá resultado para as quadrilhas, por que as vezes tem empresas que tem muitas vulnerabilidades, mas pode não render nada para os atacantes. Temos casos de empresas que trabalham com muito dinheiro e tem suas falhas, mas é a minoria. O Brasil e um dos países que tem o sistema bancário mais seguro, porém os usuários se deixam invadir.

6. Qual é o comportamento da maioria dos Hackes/Crackers?

R- Eles geralmente pessoas egoístas, que não se preocupam com o bem do próximo, eles só pensam nos ganhos e na vida que eles vão levar sem trabalhar, são preguiçosos em termos de querer ganhar a vida realizando alguma coisa útil. Geralmente gostam muito de festas, e vida de ostentação, desperdiçam muito pois o dinheiro não e deles. São pessoas que dormem tarde e acordem cedo só pra startar os processos de envio de e-mails maliciosos.

7. Qual é a faixa etária dos hackers?

R- Normalmente são pessoas mais jovens, mas porem tem pessoas mais velhas de 30/40 anos.

8. Quais dispositivos são mais atacados?

R- Os próprios computadores pessoais, celulares tem muito ataque quando a pessoa acessando qualquer tipo de site sem antivírus, mas a maioria são os computadores pessoais e os computadores de empresas (Notebooks).

9. Em qual cidade/região teve mais ataque aqui no estado de Goiás?

R- Não há uma estatística, mas tem uma quadrilha de âmbito mundial onde parte dos líderes serem goianos.

10. Dentro de Goiás já houve algum ataque de grande impacto?

R- Nunca houve nada muito extraordinário, mas há ataques mesmo de volumes financeiros.

11. O que me fala sobre o Kali Linux, e o fato delas estar de tão fácil acesso para os usuários?

R- Qualquer ferramenta de código aberto, que tem possibilidades de mudar o código e fazer coisas incríveis com ela, mas a cada dia que se passa novas ferramentas são lançadas, e atualmente e apenas e um uso interessante que está sendo utilizadas até ser lançado outra.

ENTREVISTA 2

Nome: Lílian Barbosa de Morais

Formação Acadêmica: Psicóloga

Profissão: Docente e Psicóloga

CRP: 3686

1. Para você o que é Engenharia Social?

R- Nunca tinha ouvido falar sobre o termo, eu ouvi falar após ter sido procurada, onde fiz uma pesquisa sobre o que seria. Pensando em relação a psicologia, vocês trouxeram um termo novo que para nós já é um termo antigo, que é a capacidade de persuadir. Então engenharia social é isso, é a capacidade de persuasão de uma pessoa.

2. Pessoas que praticam a Engenharia Social podem ter um comportamento diferenciado de outras pessoas?

R- Não, geralmente essas pessoas tem o mesmo padrão de comportamento de qualquer outra pessoa. A gente não diferencia padrões de comportamento, em um contexto os comportamentos são os mesmos.

3. Você acredita que os engenheiros sociais podem ter algum distúrbio mental ou é desenvolvido lentamente com o tempo?

R- Só por ele ser Engenheiro Social não, as vezes ele escolher ser engenheiro social por ele já ter algum tipo de transtorno de personalidade.

4. Os principais objetivos desses Engenheiros Sociais em aplicar esta técnica, é por recursos financeiros ou por mera satisfação pessoal?

R- Pode ser os dois, mas levando pelo perfil da pessoa que vai praticar isso, e mais por uma questão de personalidade.

5. Como a psicologia lida com o perfil de pessoas que são Engenheiros Sociais?

R- Em geral, para psicologia são pessoas com perfil narcísico, que a gente chama de pessoas que elas estão em primeiro lugar, onde ela tem uma dificuldade de olhar o outro, sempre são as necessidades dela que tem que são satisfeitas, e são pessoas que estão mais nessas áreas de crime mesmo, para usar isso de uma forma negativa.

6. Pode ser considerada uma doença, característica pessoal ou desvio de personalidade?

R- É um desvio de personalidade.

7. Hoje em dia uma pessoa consegue obter informações pessoais de terceiros com facilidade, pois às pessoas são fáceis de manter contato, intimidade e até mesmo iludir para obter informações necessárias. Por que podemos considerar o ser humano o elo mais fraco?

R- Ele é o elo mais fraco por ser o único elo que a gente relaciona, por que a nossa inteligência que é o que nos diferencia dos outros animais de uma certa forma, ela nos deixa mais frágil, pela questão da vaidade, pela questão dos desejos, que são características do ser humano, deixa ele mais frágil, onde ele se vê mais apto a desenvolver certas coisas, a fazer certas coisas em função dessa vaidade e desses desejos.

8. Quais os aspectos que favorece o sucesso da Engenharia Social?

R- Primeiro é a própria capacidade dessa pessoa com esse perfil, que acaba sendo um perfil com personalidade que vai melhorando, na medida que ele vai praticando isso ele vai ficando melhor nisso. Juntamente com o outro lado, que é frágil, volátil que está a mercê do que o engenheiro social pode fazer.

9. Quais são os pontos positivos e negativos da Engenharia Social dentro da informática?

R- O que vejo de positivo e que são posturas que podem trazer coisas positivas para nossa sociedade, como obter certas informações que podem salvar vidas e que pode gerar coisas positivas em um contexto social é muito bom. Já negativo, entra na parte de pegar dados e informações e usar isso para prejudicar alguém, para trazer prejuízo de alguma forma para alguém ou para alguma empresa.

10. Você já trabalhou diretamente com casos em que o paciente tivesse características de um Engenheiro Social?

R- Na verdade, temos muitas pessoas assim no nosso dia a dia, pois isso não é uma personalidade rara, então no nosso dia a dia e no nosso trabalho sempre tem aquela pessoa que tem o perfil. Costuma ser uma pessoa muito doce, muito exagerada ao demonstrar afeto, que quer agradar demais, que quer se fazer muito prestativo e muito útil, que tem uma lábia muito

bom, uma comunicação muito boa. Então temos esse tipo de pessoa no nosso meio, o tempo todo, porém, o que se deve observar é o grau, tem alguns que usam isso num grau maior, onde trazem prejuízos maiores e outros não, ficam apenas nos níveis de fofoca e de coisas ruins do ambiente de trabalho.

11. Já viu algum caso na televisão, internet ou até mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- Não que eu não esperava, porem aquele caso do espião russo, foi muito inteligente naquilo que ele foi fazer, onde descobriu e conseguiu manter sigilo por tanto tempo, mas isso não me assusta.

12. Você já viu muitos casos de Engenharia Social, de modo geral, não somente na informática. Fale um pouco sobre algum caso que presenciou e possa falar?

R- Eu vivenciei no meu trabalho uma pessoa que tinha esse perfil, e ela fazia todo um jogo de manipulação, onde era uma sociedade e ela fazia esse jogo com as demais sócias com intuito de que ela fosse a sócia majoritária, então vivi isso na pratica com uma sociedade de quatro pessoas. Tínhamos uma pessoa com esse perfil, onde demoramos perceber, mas como duas das sócias eram psicólogas, isso foi notado, e conseguimos conduzir isso de uma melhor maneira.

13. Nosso trabalho tem o intuito de mostrar a vulnerabilidade das pessoas e conscientizá-las nesse quesito. Em sua opinião, quais os cuidados que a população deve adotar para evitar cair em tais fatos?

R- O primeiro cuidado e desconfiar sempre, pois nunca conhecemos uma pessoa por completo, se não conhecemos as pessoas que estão dentro da nossa casa, quem dirá as que estão fora. Ter sempre o cuidado de desconfiar, ter cautela, estar sempre atento nas intenções, gestos e comportamentos das pessoas. A pessoa mostra pelo comportamento o que ela quer, e se tivermos atenção nisso poderemos perceber.

ENTREVISTA 3

Nome: Kárita Rayane Silva Maia
Formação Acadêmica: Bacharel em Psicologia
Profissão: Psicóloga
CRP: 09/011118

1. Para você o que é Engenharia Social?

R- Não conhecia esse ato com esse termo de Engenharia Social. Hoje estudando um pouco do assunto entendo essa engenharia como o ato de buscar informações ou até mesmo levar pessoas tomar decisões pelo poder de convencimento do outro.

2. Pessoas que praticam a Engenharia Social podem ter um comportamento diferenciado de outras pessoas?

R- Podemos dizer que sim, pois a partir do momento que você toma por partido tentar convencer o outro de algo ou até mesmo tirar respostas em meio a algumas circunstâncias para tirar certa vantagem, você está tendo um comportamento racional daquilo que faz, mesmo vendo que isso prejudicaria o outro e te beneficiaria.

3. Você acredita que os engenheiros sociais podem ter algum distúrbio mental ou é desenvolvido lentamente com o tempo?

R- Todos nós estamos propensos a ter ou não um distúrbio mental, mas acredito que os engenheiros sociais podem vir ter um indicie maior de distúrbio mental. Visto que a partir do momento que se vê não obtendo os resultados desejados pode começar a desenvolver: depressão, manias, fobias.

4. Os principais objetivos desses Engenheiros Sociais em aplicar esta técnica, é por recursos financeiros ou por mera satisfação pessoal?

R- Aí já vai de cada indivíduo, mesmo com a busca por interesses financeiros a satisfação pessoal leva com que a pessoa cresça dentro dessa engenharia social. Podemos comparar com uma pessoa que partilha do tráfico de drogas, tem todo o retorno financeiro, mas o poder que cresce dentro do indivíduo faz com o que mesmo não queria sair desse meio.
Então podemos dizer que o poder gera consequências, e a engenharia social gera os dois.

5. Como a psicologia lida com o perfil de pessoas que são Engenheiros Sociais?

R- Podemos lidar com esse perfil com a psicologia reversa, que nada mais é que tentar obter pontos positivos encima daquilo que podemos considerar negativos no indivíduo. No caso dos engenheiros sociais tentaríamos mover a pessoa por uma ação contraria desse poder de persuasão, tentaríamos um lado reverso a persuasão.

6. Pode ser considerada uma doença, característica pessoal ou desvio de personalidade?

R- Pode ser tanto característica pessoal ou desvio de personalidade.

7. Hoje em dia uma pessoa consegue obter informações pessoais de terceiros com facilidade, pois às pessoas são fáceis de manter contato, intimidade e até mesmo iludir para obter informações necessárias. Por que podemos considerar o ser humano o elo mais fraco?

R- Por meio dessa falta de atenção gerada por essa era tecnológica que vivemos as pessoas começaram a abrir mais espaço em suas vidas quando o assunto é um contato pessoal. Hoje é muito fácil chegar na fila de um banco e começar a conversar com pessoas que você nunca viu e em poucos minutos você já conhece toda a vida da pessoa. Se alimentássemos o elo do convívio, do diálogo dentro de casa, com nossos amigos, estaríamos menos propensos a expor nossa vida com estranhos.

8. Quais os aspectos que favorece o sucesso da Engenharia Social?

R- Um bom poder de influência e um bom conhecimento do produto ou informação que está em questão.

9. Quais são os pontos positivos e negativos da Engenharia Social dentro da informática?

R- Acho que ponto positivo seria a interação de profissionais ligados à área e negativo seria o vazamento de informações ligadas ao indivíduo.

10. Você já trabalhou diretamente com casos em que o paciente tivesse características de um Engenheiro Social?

R- Sim, e com algumas sessões vi que o paciente usava dessa “Engenharia Social” inconscientemente.

11. Já viu algum caso na televisão, internet ou até mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- Pouco tempo vimos a justiça suspender os cartões do Santander free, pois eles prometiam um cartão sem nenhuma anuidade e quando os consumidores começavam a utilizar os cartões as faturas vinham com o valor da anuidade, e quando ligavam atrás de informações eles informavam que seria sem nenhuma anuidade se acumulasse R$ 100,00 de compras por mês. Não foi um fato que me surpreendeu, mas foi algo que acabou enganando muita gente.

12. Você já viu muitos casos de Engenharia Social, de modo geral, não somente na informática. Fale um pouco sobre algum caso que presenciou e possa falar?

R- Sim, nos presenciamos isso todos os dias quando entramos em comércios e até mesmo de promessas de promoções que enchem nossos olhos com a facilidade.

A pouco tempo uma determinada editora ligou na minha residência oferecendo um plano de assinatura de revista, quem atendeu foi minha vó que é a titular do cartão de credito, e com aqueles 5 minutos de bobeira fez a assinatura das revistas mal sabia ela que as consequências viriam mais tarde. Passado um ano eles ligaram para ela renovar a assinatura e ao falar que não queria eles disseram que a mesma teria que pagar uma taxa de cancelamento. Ela pagou mais 3 parcelas de 150 reais e após essas 3 parcelas eles ligaram novamente falando que ela teria que pagar mais 3 parcelas de 150 reais, pediram até o número do código de acesso do cartão de credito e a mesma passou esse número. Quando cheguei em casa e soube do ocorrido precisei ligar na operadora do cartão e fazer o cancelamento do mesmo.

13. Nosso trabalho tem o intuito de mostrar a vulnerabilidade das pessoas e conscientizá-las nesse quesito. Em sua opinião, quais os cuidados que a população deve adotar para evitar cair em tais fatos?

R- O principal cuidado é de nunca confiar em ofertas baratas demais ou muita facilidade para conseguir algo.

Pensar muito antes de tomar qualquer decisão pode ser um grande aliado para não cair em tais fatos. Tem coisas que devem ser guardadas para você ou no máximo para sua família e nunca expostas para terceiros, principalmente se você acabou de conhece-lo. Nem todo mundo olha com a mesma inocência que você está olhando.

14. No meio acadêmico casos de Engenharia Social podem ser considerados perda de tempo ou um caso sério?

R- Com certeza é caso sério, pois ter seus dados nas mãos de pessoas é muito perigoso, principalmente no meio acadêmico, onde qualquer informação capturada nas mãos de pessoas erradas, pode mudar o rumo do seu futuro acadêmico.

ENTREVISTA 4

Nome: Dayane de Moura Marques
Formação Acadêmica: Psicologia
Profissão: Psicóloga Social
CRP: 09/011259

1. Para você o que é Engenharia Social?

R- Manipulação psicológica pelo uso de imagem e/ou documentos sigilosos de outros.

2. Pessoas que praticam a Engenharia Social podem ter um comportamento diferenciado de outras pessoas?

R- Acredito que nem sempre.

3. Você acredita que os engenheiros sociais podem ter algum distúrbio mental ou é desenvolvido lentamente com o tempo?

R- Não. Cada caso é um caso, uma pessoa sem distúrbios também pode ter certos comportamentos para conseguir algo em algum momento da vida.

4. Os principais objetivos desses Engenheiros Sociais em aplicar esta técnica, é por recursos financeiros ou por mera satisfação pessoal?

R- As duas coisas, alguns por dinheiro, outros por satisfação pessoal.

5. Como a psicologia lida com o perfil de pessoas que são Engenheiros Sociais?

R- Difícil responder essa pergunta pois dificilmente esse tipo de perfil busca um psicólogo. O que deve ser feito é orientar as pessoas para não caírem no golpe, e acho importante falar mais sobre esse tema como forma de prevenção.

6. Pode ser considerada uma doença, característica pessoal ou desvio de personalidade?

R- Não é um diagnóstico, indivíduos e características nem sempre se encaixam.

7. Hoje em dia uma pessoa consegue obter informações pessoais de terceiros com facilidade, pois às pessoas são fáceis de manter contato, intimidade e até mesmo iludir

para obter informações necessárias. Por que podemos considerar o ser humano o elo mais fraco?

R- Com a chegada da internet as pessoas se apegam mais em pessoas virtuais do q em pessoas reais.

8. Quais os aspectos que favorece o sucesso da Engenharia Social?

R- Vítimas carentes, solitárias e desatentas.

9. Quais são os pontos positivos e negativos da Engenharia Social dentro da informática?

R- (A profissional optou por não responder essa pergunta).

10. Você já trabalhou diretamente com casos em que o paciente tivesse características de um Engenheiro Social?

R- Não.

11. Já viu algum caso na televisão, internet ou até mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- Sempre.

12. Você já viu muitos casos de Engenharia Social, de modo geral, não somente na informática. Fale um pouco sobre algum caso que presenciou e possa falar?

R- Muitas vezes acontece em mulheres, pessoas com tal perfil se aproxima da mesma para obter fotos comprometedoras e com isso manipular em troca de dinheiro ou até mesmo só para provocar desespero na vítima.

13. Nosso trabalho tem o intuito de mostrar a vulnerabilidade das pessoas e conscientizá-las nesse quesito. Em sua opinião, quais os cuidados que a população deve adotar para evitar cair em tais fatos?

R- Ficar mais atenta e não divulgar fotos comprometedora na internet ou deixar fotos e documentos sigilosos em computadores e celulares.

14. No meio acadêmico casos de Engenharia Social podem ser considerados irrelevantes?

R- Não! É caso sério, ninguém ira gostar de saber que suas informações estão nas mãos de outras pessoas, ainda mais quando se trata no meio acadêmico, onde os alunos fazem de tudo, por que realmente nunca conhecemos alguém a fundo e a capacidade de cada um.

ENTREVISTA 5

Nome: Maryanna Fernandes Lemes
Profissão: Psicóloga
Formação: Psicologia
CRP: 09/011090

1. Para você o que é Engenharia Social?

R- É um método, planejamento como o próprio nome diz, engenharia, para fazer com que as pessoas usem para chegar ao objetivo.

2. Pessoas que praticam Engenharia Social podem ter um comportamento diferenciado de outras pessoas?

R- Não

3. Você acredita que engenheiros sociais podem ter algum distúrbio mental ou é desenvolvido lentamente com o tempo?

R- Qualquer pessoa pode desenvolver algum Transtorno mental no decorrer da vida, seja engenheiro social ou não.

4. O principal objetivo destes engenheiros em aplicar esta técnica é por recursos financeiros ou por mera satisfação pessoal?

R- Depende de qual o objetivo que o engenheiro social planeja, ora financeiro ou pessoal.

5. Como que a psicologia lida com perfil de pessoas engenheiros sociais?

R- Lida em estudar e investigar sobre quais são os traços que compõem esse perfil

6. Pode ser considerada uma doença, ou característica pessoal, ou desvio de personalidade?

R- É necessário fazer uma avaliação psicológica para verificar, pois cada indivíduo enquanto engenheiro social é diferente um do outro, com objetivos diferentes.

7. Hoje em dia uma pessoa consegue obter informações pessoais de terceiros com facilidade, pois às pessoas são fáceis de manter contato, de ter intimidade até iludir e

obter informações necessárias. Porque podemos considerar o ser humano o elo mais fraco?

R- Depende do momento em que a pessoa está passando, se está mais vulnerável ou não, o que faz com que a atenção e concentração são fragilizadas e fáceis para as pessoas que aproveitam tais situações.

8. Quais são os aspectos que favorecem o sucesso da Engenharia Social?

R- Persuasão e atenção

9. Quais são os pontos positivos e negativos da Engenharia Social dentro da Informática?

R- Positivo é que há praticidade e agilidade nos processos.

Negativo é quando usa essa ferramenta para o crime.

10. Você já trabalhou diretamente com casos que clientes tivessem características de um Engenheiro Social?

R- Não

11. Já viu algum caso na televisão, internet ou até mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- Sim

12. Você já viu muitos casos de Engenharia Social, de modo geral, não somente na informática. Fale um pouco sobre os que você presenciou.

R- Não

13. Em sua opinião, quais os cuidados que a população pode adotar para evitar cair em tais fatos?

R- Ficar mais atento mesmo enquanto estivermos em situações de vulnerabilidade, apesar que nossas percepções das coisas estão fragilizadas nos tornando alvo de pessoas que usam a engenharia social para o crime.

14. No meio acadêmico casos de Engenharia Social podem ser considerados irrelevantes?

R- Relevantes. Com certeza! Por que a partir do momento que alguém tenha acessado as suas informações, isso estará afetado um dos pilares da Segurança da Informação, onde poderá usar isso contra você mesmo.

ENTREVISTA 6

Nome: Wandielly Ramaianne Silva do Carmo
Formação Acadêmica: Graduação em Psicologia - Universidade Federal de Goiás, Esp. Em Docência Universitária – FACER/Uni Evangélica. Pós-Graduanda em Terapia Cognitivo Comportamental – Instituto Capacitar.
Profissão: Psicóloga (atuação clínica e escolar)
CRP: 09/9661

1. Para você o que é Engenharia Social?

R- Para mim, Engenharia Social é o termo utilizado para classificar o comportamento de persuadir/enganar pessoas ou sistemas para apoderar-se de informações sigilosas ou comprometedoras.

2. Pessoas que praticam a Engenharia Social podem ter um comportamento diferenciado de outras pessoas?

R- Em geral, o comportamento do indivíduo que pratica a Engenharia Social tende a ser "acima de suspeitas". Coloca-se como uma pessoa prestativa, simpática. Tais indivíduos são estrategistas, apresentam-se como pessoas nas quais se pode confiar.

3. Você acredita que os engenheiros sociais podem ter algum distúrbio mental ou é desenvolvido lentamente com o tempo?

R- Pode ser desenvolvido ao longo do tempo. Nós aprendemos a nos comportar com base naquilo que fomos ensinados, através dos ciclos sociais em que estamos inseridos (família, amigos, trabalho, etc.) e também, através da observação do comportamento de outras pessoas. Sendo assim, as características apresentadas por um engenheiro social podem ser desenvolvidas ao longo do tempo, através da aprendizagem, até porque, os transtornos de ordem comportamental são desenvolvidos ao longo do tempo, na presença de um "gatilho ambiental". Entretanto, existem os transtornos da personalidade. O indivíduo que apresenta um transtorno da personalidade, têm comportamentos fixos em seu caráter, podendo incluir a engenharia social.

4. Os principais objetivos desses Engenheiros Sociais em aplicar esta técnica, é por recursos financeiros ou por mera satisfação pessoal?

R- Adquirir recursos financeiros, por si só, já é um comportamento provocativo de satisfação social. O indivíduo que coloca em prática as técnicas da engenharia social é reforçado pelos recursos financeiros aos quais pode ter acesso, mas, além disso, sente prazer ao conseguir acessar informações que não lhe pertencem. Ele se sente numa posição privilegiada em relação aos demais. Portanto, podemos dizer que os principais objetivos dos engenheiros sociais são a autossatisfação, o prazer de se sentir privilegiado em relação às outras pessoas, isto inclui a melhoria dos recursos financeiros. Estes engenheiros são seduzidos pela possibilidade de manipular as pessoas. Isto gera mais prazer do que obter recursos financeiros.

5. Como a psicologia lida com o perfil de pessoas que são Engenheiros Sociais?

R- No sentido de tratamento psicológico, acontece somente quando a pessoa deseja melhorar sua funcionalidade, ou seja, quando a prática da engenharia social começa a atrapalhar a vida da pessoa, o que raramente acontece. Geralmente, a psicologia, mais especificamente a Terapia Cognitivo Comportamental atua com o objetivo de aumentar o repertório de comportamentos sociais deste indivíduo, buscando diminuir a emissão dos comportamentos desadaptativos envolvidos na prática da engenharia social. Na clínica, os indivíduos que praticam a engenharia social não buscam atendimento por conta desta situação e, sim, por conta de outras demandas. A prática da engenharia social é altamente reforçadora para o indivíduo, é muito difícil que ele queira deixar este comportamento.

6. Pode ser considerada uma doença, característica pessoal ou desvio de personalidade?

R- Pode ser considerada uma característica pessoal ou desvio de personalidade. Como já explicado anteriormente, indivíduos que possuem transtorno da personalidade ou psicopatia/sociopatia, demonstra esta caraterística no seu caráter. Torna-se até redundante, já que esta característica pessoal do indivíduo é um comportamento de seu padrão de personalidade desviante (desviante se compararmos com amostras de seu ciclo social). Não é considerado doença porque não há alterações de ordem bio-fisiológica. É um padrão comportamental que a pessoa apresenta.

7. Hoje em dia uma pessoa consegue obter informações pessoais de terceiros com facilidade, pois às pessoas são fáceis de manter contato, intimidade e até mesmo iludir para obter informações necessárias. Por que podemos considerar o ser humano o elo mais fraco?

R- Nós, seres humanos, somos sociais. Precisamos estabelecer vínculos com outros seres da nossa espécie para obtermos satisfação de vida. A maioria de nós tem carência afetiva em algum grau, o que dá maior abertura para a ação dos engenheiros sociais. Além disso, há um aprendizado sobre confiança. Aprendemos a confiar/desconfiar das pessoas. Alguns se tornam alvos mais fáceis dos engenheiros sociais exatamente por terem uma carência afetiva e, talvez, isto os leva a confiar nas pessoas sem uma observação mais acurada. Há também a falta de informação. Muitos não têm conhecimento sobre a existência da Engenharia Social.

8. Quais os aspectos que favorece o sucesso da Engenharia Social?

R- A facilidade que os engenheiros sociais têm de manipular seus alvos. Um engenheiro social apresenta algumas características como simpatia, presteza, aparentam ser confiáveis e, a mais importante: são estrategistas. Sabem o momento certo de agir e como agir. São pessoas, no geral, frias e calculistas.

9. Quais são os pontos positivos e negativos da Engenharia Social dentro da informática?

R- Todos os padrões comportamentais têm os pontos positivos e negativos. Não é diferente com a Engenharia Social. Acredito que seja positivo quando a prática acontece com o objetivo de proteger informações ou identificar/corrigir falhas em programas de alta confidencialidade; neste caso, a engenharia social acontece para favorecer um grupo de pessoas.

Os pontos negativos se manifestam quando os engenheiros sociais o fazem com o intuito de prejudicar uma ou mais pessoas.

10. Você já trabalhou diretamente com casos em que o paciente tivesse características de um Engenheiro Social?

R- Ainda não.

11. Já viu algum caso na televisão, internet ou até mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- Alguns filmes abordam este tema, um exemplo é o filme "Prenda-me se for capaz", estrelado por Leonardo Di Caprio que, inclusive, é baseado em fatos reais. Tivemos um caso de grande repercussão no Brasil, do Marcelo Nascimento, que também inspirou uma obra cinematográfica intitulada como "VIP's".

12. Você já viu muitos casos de Engenharia Social, de modo geral, não somente na informática. Fale um pouco sobre algum caso que presenciou e possa falar?

R- Profissionalmente ainda não me deparei com algum caso explícito de Engenharia Social. Posso citar um caso que tem se tornado comum: o golpe do sequestro. O indivíduo liga para um cidadão, dizendo ter sequestrado um ente querido seu. Na verdade, o sujeito quer apenas retirar algumas informações pessoas como nome de parentes, endereço, etc.. Ao entrar em pânico com a situação, a vítima acaba por liberar os dados acreditando estar salvando a vida de outrem. Ou seja, o engenheiro social persuade a vítima a fazer/fornecer o que ele quer. Existem também casos comuns no WhatsApp, onde a vítima é convencida a fornecer fotos e informações. São muitas situações. Hoje, com o uso exagerado e inadequado das redes sociais, estamos nos tornando alvos cada vez mais fáceis para os engenheiros sociais.

13. Nosso trabalho tem o intuito de mostrar a vulnerabilidade das pessoas e conscientizá-las nesse quesito. Em sua opinião, quais os cuidados que a população deve adotar para evitar cair em tais fatos?

R- Redobrar o cuidado e atenção com seus dados pessoais. Ninguém tem bola de cristal, não dá para adivinharmos quando uma pessoa está má intencionada. Porém, existem alguns sinais que nos fazem ficar mais alertas. Seguir aqueles conselhos de avó: não dar dados pessoais a estranhos, mesmo que estes lhe pareçam familiares ou acima de qualquer suspeita. E o fato de se informar/ser informado da existência desta prática também auxilia nos nossos comportamentos de autocuidado. As pessoas pensam que engenheiros sociais dão golpes apenas em famosos ou ricaços. A prática da engenharia social é mais comum do que se imagina.

ENTREVISTA 7

Nome: Nádio Carlo de S. Vieira
Profissão: Docente e Analista de Sistemas
Formação: Graduação em Sistemas de Informação e Especialista em Segurança em Redes de Computadores

1. Para você o que é Engenharia Social?

R- Uma técnica antiga, porém, nos dias contemporâneos tomou essa nova roupagem denominada Engenharia Social. O ato de utilizar meios de comunicação tecnológicos, verbais ou corporais com persuasão (muitas vezes faltando com a verdade) para ganhar a confiança do interlocutor a fim de obter informações privilegiadas.

2. Quando se diz sobre Segurança da Informação, logo vem na memória os pilares, você acredita que exista um pilar mais importante que o outro quando se trata de ataques de engenharia social?

R- Os três principais pilares de segurança da informação – Disponibilidade, integridade e confidencialidade -formam um tripé. O tripé para se sustentar tem que estar todas as hastes íntegras, da mesma forma acredito não ter um maior que o outro, todos são importantes. O que vemos são determinados ataques que afetam mais um pilar determinado, já outros ataques podem afetar outro pilar. O que determina isso é a informação que está sendo alvo naquele momento e as ferramentas/técnicas.

3. Há diversos tipos de ataques virtuais, alguns relacionados com o acesso indevido a redes de computadores de terceiros e outros em forma de vírus embutidos em programas, mensagens eletrônicas e também ataques diretos como a engenharia social, qual desses fatos são mais fáceis das pessoas se tornarem vítimas?

R-Pela evolução que essa área tem, várias técnicas se tornam bem-sucedidas, porém a escolha dela depende do alvo e da análise do ambiente a ser atacado. Uma técnica que nunca saiu do ranking das mais eficazes é o *Phishing,* vindo da sua tradução de pescar, pode ser por email, dns, websites. Se trata de e-mails falsos ou sites que são direcionados para a vítima, se a mesma não identificar anormalidades, irá abrir os anexos ou clicar em algum link. Esta ação

já se entende que a vítima foi “fisgada”. Al clicar, o usuário pode ter instalado (sem ciência) um *rootkit* ou um trojan.

4. Quais são os pontos positivos e negativos da Engenharia Social dentro da Informática?

R- A engenharia social pode trazer pontos positivos para outras áreas, como técnicas de venda, oratória e outras. Na tecnologia da informação não identificou benefício dessa técnica. Vendo que a mesma pode ser utilizada para obter informações confidenciais, afetando a ética em TI e podendo encaixar como crime pelas leis vigentes em nosso país.

5. Você já trabalhou diretamente com casos de Engenharia Social?

R- Sim, no meu trabalho já recebi ligações de pessoas solicitando uma informação X, e se identificando. Após fazer algumas perguntas se segurança de cunho pessoa, essa mesma pessoa não soube responder, desligando o telefone logo em seguida.

Não precisar trabalhar somente em TI para ser conhecedor de casos e/ou participar de algum. Por exemplo: uma pessoa, com boa aparecia e dicção, pode chegar em um hotel e solicitar um quarto para hospedar, ao fazer o cadastro o mesmo sabe todas as informações decoradas e convicto daquilo. O atendente para evitar desgastes e/ou atrasos realiza o cadastro somente com os dados informados verbalmente. Fica a pergunta: Estes dados são verdadeiros? Se na ocasião hipotética, o hospede sair sem pagar, o hotel colocará como devedor a pessoa certa?

6. Quais as técnicas mais utilizadas pelos criminosos?

R- Engenharia Social como premissa para obter informações. A partir destas, determina o ataque de acordo com a informação e onde se encontra a mesma.

7. Qual ferramenta você considera a mais importante para proteção contra-ataques virtuais?

R- A ferramenta mais importante que conheço se chama “Conhecimento/Conscientização”. Ataques podem vir de todos os meios: internet, localhost, e-mail, pendrive, wi-fi, bluetooth. Camuflado de N formas, que se inovam a cada dia. O usuário deverá ficar atendo para os detalhes.

8. Qual ferramenta você conhece para ataques sociais?

R- Um dos mais usados kits de ferramentas usados no mundo e que tenho estudado no âmbito

da engenharia social se chama SET (Social Engineering Toolkit / Kit de ferramentas de engenharia social). Sua distribuição mais popular está na distribuição do Linux denominado Kali Linux.

9. Por que você acha que essa e a técnica mais utilizada?

R- Essa ferramenta sempre vem recebendo atualizações pela comunidade internacional de harckers por ser software livre. A ferramenta tem várias opções para elaborar uma boa engenharia social em websites, e-mails e arquivos infectados. Além de ter fácil acesso e não ter custo pela licença.

10. Por que você acha que as pessoas estão tão vulneráveis há essas técnicas?

R- A conectividade da população cresce de uma forma disparada. E as pessoas tem a tendência em evitar conflitos e socializarem facilmente nas mídias sociais, sempre que o interlocutor passa uma breve confiança.

11. Já viu algum caso na televisão, internet ou ate mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- Um documentário chamado VIPs, conta a história de Marcelo Nascimento da Rocha, um engenheiro social que se passou por jornalista, policial, guitarrista de rock, jogador de futebol e um dos maiores triunfos dos mesmos quando se passou pelo filho do dono das linhas aéreas GOL frequentando várias festas e ambientes de alta classe.

12. Na sua opinião, quais as principais medidas as serem tomadas para não ser vítima de tais ataques?

R-

- Se informar sobre os ataques da atualidade;
- Desconfiar de todos terceiros;
- Solicitar documento comprobatório;
- Não disponibilizar nas mídias sociais, informações pessoais;
- Não disponibilizar nas mídias sociais fotos e eventos em tempo real;
- Conscientizar as pessoas que estão em sua volta sobre os itens acima (pois as mesmas possuem informações sobre você).

13. Qual a técnica na sua opinião, que seria mais fácil para um engenheiro social usar no meio acadêmico?

R- Acredito que com a ajuda da Engenharia Social várias outras poderiam ser aplicadas no meio acadêmico, com professores e alunos. A engenharia social abre as portas da vulnerabilidade e identifica alvos fáceis ou não.

14. Já viu ou presenciou algum caso no meio acadêmico? Se sim fale um pouco sobre.

R- Já presenciei, o excesso de confiança que as pessoas no meio acadêmico podem ter um no outro, no qual cria ocasiões para necessitar de privilégios no sistema, e utilizar tais fins para outras finalidades.

ENTREVISTA 8

Nome: Nayume Pereira Demésio
Profissão: Técnica de Suporte à Usuários
Formação: Tecnologia em Redes de Comunicação – Pós Segurança e Gestão em Tecnologia da Informação

1. Para você o que é Engenharia Social?

R- Engenharia social é o termo utilizado para definir um método de ataque que utiliza da persuasão para conseguir informações importantes do indivíduo, que podem ou não ser utilizadas em benefício próprio.

2. Quando se diz sobre Segurança da Informação, logo vem na memória os pilares, você acredita que exista um pilar mais importante que o outro quando se trata de ataques de engenharia social?

R- Acredito que a junção dos três pilares (confidencialidade, integridade, disponibilidade) são essenciais quando se trata se defender de ataques de engenharia social.

3. Há diversos tipos de ataques virtuais, alguns relacionados com o acesso indevido a redes de computadores de terceiros e outros em forma de vírus embutidos em programas, mensagens eletrônicas e também ataques diretos como a engenharia social, qual desses fatos são mais fáceis das pessoas caírem?

R- Em forma de vírus embutidos em programas, mensagens eletrônicas e ataques em forma de engenharia social.

4. Quais são os pontos positivos e negativos da Engenharia Social dentro da Informática?

R- Os pontos negativos é que informações importantes podem ser capturadas por pessoas que podem agir de má-fé. Acredito que não haja pontos positivos da Engenharia Social dentro da Informática.

5. Você já trabalhou diretamente com casos de Engenharia Social?

R- Não, nunca trabalhei com caso de Engenharia Social.

6. Quais as técnicas mais utilizadas pelos criminosos?

R- As técnicas mais utilizadas são de obter informações por meio da persuasão, manipulação psicológica de modo a divulgar informações que podem ser confidenciais dento de uma instituição.

7. Qual ferramenta você considera a mais importante para proteção contra-ataques virtuais?

R- A ferramenta mais importante para proteção contra-ataques é orientação ao usuário. Orientá-lo a ter cuidado ao acessar sites, cuidado com os arquivos recebidos via e-mail, cuidado ao falar sobre informações da instituição à pessoas não relacionadas a ela.

8. Qual ferramenta você conhece para ataques sociais?

R- Ataques sociais podem ser feitos pessoalmente, ou online através de redes sociais.

9. Por que você acha que essa e a técnica mais utilizada?

R- Porque é a técnica mais fácil para se obter informações, de modo que possam ser utilizadas para quebrar senhas, acessar servidores. Os itens mais valiosos de uma organização são os ativos, que podem ser em forma de objetos ou informações.

10. Por que você acha que as pessoas estão tão vulneráveis há essas técnicas?

R- As pessoas estão vulneráveis, por inúmeros fatores, sendo por algum problema psicológico, sendo por problemas familiares. Sempre haverá um ponto fraco, que o engenheiro social poderá utilizar em benefício próprio.

11. Já viu algum caso na televisão, internet ou até mesmo pessoalmente sobre engenharia social que te surpreendeu?

R- O caso do Marcelo Nascimento da Rocha, um famoso ex-estelionatário brasileiro.

12. Na sua opinião, quais as principais medidas as serem tomadas para não ser vítima de tais ataques?

R- Orientar aos usuários a serem menos vulneráveis, e se protegerem ao máximo dessas pessoas.