INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E
TECNOLOGIA DE SÃO PAULO
CÂMPUS VOTUPORANGA

Kawam Oliveira Freitas
Pedro Henrique Veloso Gianeze

INVASÃO MOBILE

VOTUPORANGA
2020

Kawam Oliveira Freitas
Pedro Henrique Veloso Gianeze

INVASÃO MOBILE

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do diploma do Curso Técnico em Informática Integrado ao Ensino Médio do Instituto Federal de Educação, Ciência e Tecnologia, Câmpus Votuporanga.

Professor Orientador: Ubiratan Zakaib.

VOTUPORANGA
2020

FICHA CATALOGRÁFICA

Kawam Oliveira Freitas
Pedro Henrique Veloso Gianeze

INVASÃO MOBILE

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção do diploma do Curso Técnico em Informática Integrado ao Ensino Médio do Instituto Federal de Educação, Ciência e Tecnologia, Câmpus Votuporanga.

Professor Orientador: Ubiratan Zakaib.

Aprovado pela banca examinadora em xx de mês de 2020.

BANCA EXAMINADORA:

_____

Prof. D.r Cicrano da Silva (para feminino use Dra.)

_____

Prof. M.e Beltrano dos Santos (para feminino use M.ª)

_____

Prof. Esp. José Luis Brasil

EPÍGRAFE

RESUMO

ABSTRACT

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

O projeto consiste em criar um malware voltado para dispositivos móveis, no qual estará inserido um código malicioso que infectará o dispositivo da vítima, logo após ser instalado. O que permitirá que o atacante tenha acesso às informações encontradas no aparelho da vítima. O software malicioso em questão será desenvolvido utilizando o framework Metasploit e poderá ser enviado a dispositivos conectados à Internet, ou de forma direta. Para obtermos êxito na instalação desse aplicativo no dispositivo da vítima, utilizaremos técnicas de engenharia social — métodos de persuasão usado contra as pessoas para que elas façam algo que normalmente não fariam. Em suma, esse malware será uma prova de conceitos, desenvolvido para que se prove que tudo o que foi citado é possível que aconteça. Este aplicativo não causará nenhum dano ao dispositivo/usuário e não colherá nenhuma informação confidencial do alvo — para fins maldosos, apenas mostrará que é possível que se faça.

Como já citado anteriormente o objetivo principal deste projeto é a criação de um malware para dispositivos móveis, capaz de capturar dados pessoais, o qual será utilizado para evidenciar as vulnerabilidades, sendo possível conscientizar e informar um usuário que seu aparelho pode ser exposto ao não seguir normas de segurança.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

Desenvolver um malware para dispositivos móveis, capaz de capturar dados pessoais, o qual será utilizado para evidenciar as vulnerabilidades, sendo possível conscientizar e informar um usuário que seu aparelho pode ser exposto ao não seguir normas de segurança.

1.1.2 OBJETIVOS ESPECÍFICOS

- Aprofundar conhecimentos sobre Segurança da Informação.

- Aprimorar o conhecimento em Linux.
- Estudar as ferramentas que serão utilizadas.
- Disponibilizar aos usuários uma cartilha de segurança que os auxiliem a estar protegido na rede.
- Informar aos usuários sobre os diferentes tipos de ataques com os quais eles podem se deparar, como phishing, smishing, vishing, pretexting — técnicas de engenharia social.
- Fornecer a os usuários métodos de prevenção contra ataques de engenharia social.

1.2 JUSTIFICATIVA

Na sociedade contemporânea na qual vivemos, o contexto digital e a segurança da informação são tão relevantes quanto o contexto individual e a segurança pessoal, portanto as pessoas devem dar a mesma importância a eles. Contudo, tal relevância nem sempre é dada, principalmente no que se diz respeito à segurança da informação. Isso implica em cada vez mais usuários despreparados e desprotegidos, se tornando alvos fáceis para os criminosos. Assim sendo nosso projeto pode ser uma importante ferramenta de informação para os usuários. Pois, ao fornecermos uma situação de infecção de um dispositivo, mostramos ao usuário que ele também está sujeito a esse ataque e a qualquer outro, assim criando uma consciência no usuário sobre como ele se comporta no ambiente digital, além de — por meio da nossa pesquisa — informar a ele, meios de se precaver e orientar acerca do que fazer para se tornar um usuário responsável e protegido.

1.3 METODOLOGIA

Para atingirmos o objetivo principal deste projeto, utilizaremos as seguintes metodologias:

- Levantamento Bibliográfico: Este procedimento será utilizado para nos auxiliar na utilização das ferramentas necessárias para a conclusão do projeto.

- Pesquisa Exploratória: Por meio dessa análise será possível ter acesso a todos os dados que foram obtidos através das técnicas de engenharia social. Graças a este processo vamos conseguir reunir todos os problemas encontrados durante a pesquisa;
- Pesquisa Explicativa: Última fase, onde vamos registrar todos os dados e por meio dos problemas e das soluções obtidas chegaremos em uma solução incontestável para o problema apresentado.

1.4 ESTADO DA ARTE

Diversas abordagens já foram feitas sobre o tema invasão Android, porém utilizando ferramentas e metodologias diferentes.

No trabalho de Mendes (2017), ele utiliza uma abordagem diferente com a entidade OWASP que é um projeto aberto, o qual é mantido pela comunidade. O seu objetivo é criar documentos, ferramentas, tecnologias e metodologias para manter a segurança de aplicações. Um dos projetos oferecidos pela entidade é o OWASP Mobile Security Protect, que é responsável por oferecer recursos a desenvolvedores de aplicativos mobile para mantê-los seguros. O objetivo deste trabalho é detectar e analisar vulnerabilidades encontradas em aplicações mobile seguindo critérios da OWASP com o uso de ferramentas de pentesting.

Já no projeto de Junior (2016), foi utilizada a ferramenta MSFVENOM, com o intuito de realizar o ataque em um dispositivo com o sistema operacional Android na versão 3.0. Neste trabalho é visada a utilização do framework Metasploit para o desenvolvimento da ferramenta MSFVENOM, logo após um antivírus foi instalado no sistema operacional para detectar o impacto do software diante de um ataque deste nível.

No estudo realizado por Almeida (2013), foi constatado que com o crescente número de usuários do sistema operacional Android, a quantidade de vulnerabilidades encontradas vem crescendo de forma incansável. Levando isso em consideração, foi realizada um levantamento e uma análise sobre as vulnerabilidades encontradas na plataforma Android, tendo em vista todas essas falhas, foram pesquisadas e testadas ferramentas de proteção para ajudar a assegurar a segurança do sistema operacional.

O trabalho elaborado por Della Flora (2010) tem o intuito de evidenciar o uso do framework Metasploit no desenvolvimento de um exploit para realizar a exploração de vulnerabilidades. A vulnerabilidade explorada neste trabalho é denominada buffer overflow, que consiste em uma falha de segurança na qual se utiliza o estouro de dados, sobrecarregando uma variável do sistema.

Assim como foi constatado por Almeida (2013), Moura (2017) dá seguimento a essa linha de raciocínio, confirmando que com o crescente número de usuários de celulares com o sistema operacional Android, cada vez mais vai ampliar-se as falhas e vulnerabilidades encontradas no sistema. O objetivo do trabalho feito por Moura foi realizar uma vasta pesquisa para encontrar e detalhar o melhor payload para realizar ataques ao sistema operacional Android, e com isso são gerados backdoors com a ferramenta MSFVENOM e uma comparação foi feita entre eles.

2 ARQUITETURA ANDROID

O Android é um sistema operacional da Google, que foi desenvolvido baseado em Linux. O SO é destinado apenas para dispositivos móveis. O Android é composto por 6 camadas de software, são elas:

O kernel do Android é o núcleo do sistema, em seu desenvolvimento ele foi baseado no Linux 2.6. O kernel é responsável por fazer o intermédio entre o hardware e o software do dispositivo móvel, fazendo com que assim seja possível 20 realizar ações como gerenciamento de memória RAM/ROM, processador, controle de processos executados no sistema e gerenciamento de drivers.

No momento em que uma framework API aciona o hardware do dispositivo, a HAL é responsável por carregar módulos que sejam compatíveis e que possibilitem a configuração do hardware.

O Android Runtime é a camada responsável por executar várias máquinas virtuais Dalvik nos dispositivos, para toda aplicação executada no Android é criada uma máquina virtual (VM) para que não haja nenhuma interferência na execução nos processos do sistema. A ART também é responsável por simplificar o gerenciamento e diminuir o uso de memória no sistema.

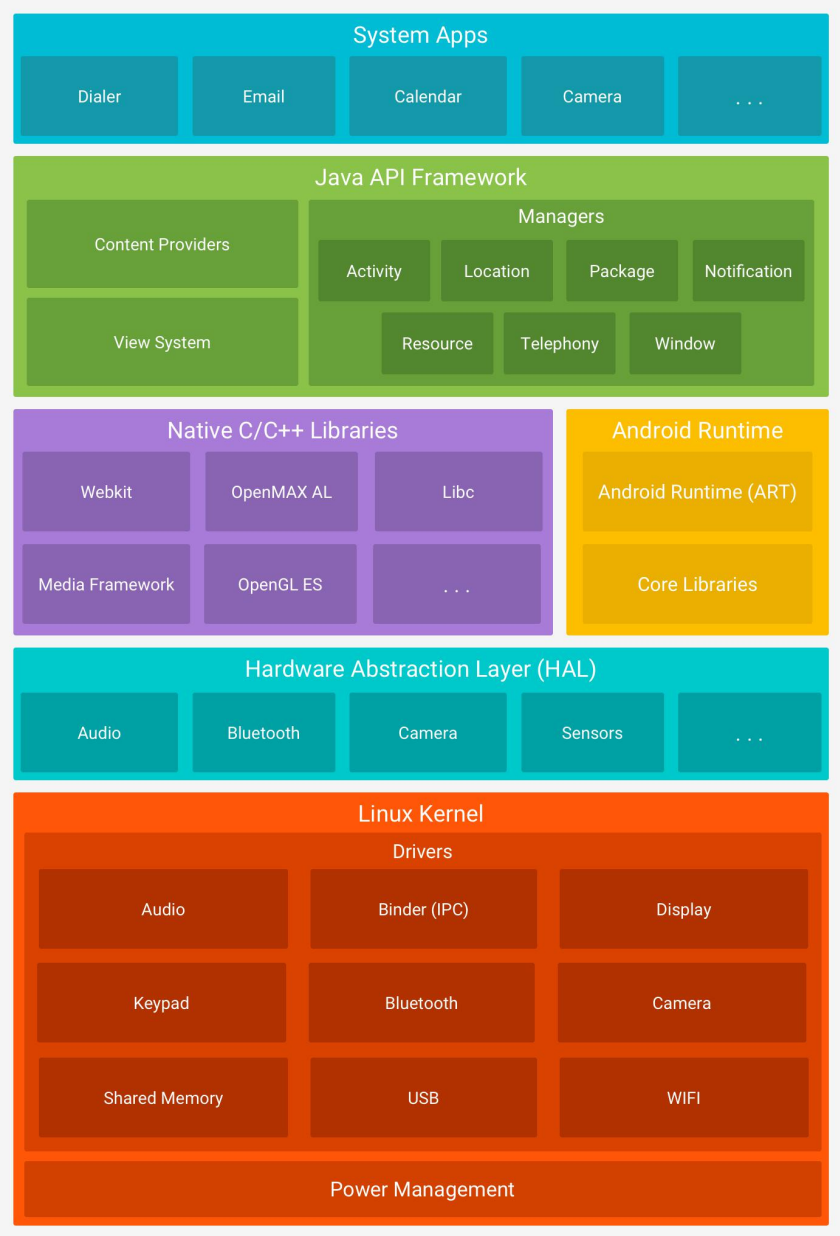
As bibliotecas C/C++ do Android são responsáveis por permitir o funcionamento correto de várias ferramentas do sistema, como a ART. Com elas também é possível visualizar imagens e objetos 2D ou 3D, fontes bitmap e vetorizadas e realizar

acessos ao banco de dados SQLite (banco de dados do Android). Várias funcionalidades disponíveis em navegadores web só são executadas por conta dessas bibliotecas.

Na camada de framework está disponível todo um conjunto de ferramentas e instrumentos que são necessários para o desenvolvimento de aplicativos para o Android, fazendo com que a utilização desses módulos fique mais simplista.

A camada de aplicação é onde fica contido a interface do usuário final e todos os aplicativos do sistema.

Figura 1 - Arquitetura do sistema operacional Android



Fonte: Android Developers (2020)

2.1 APK

O acrônimo “APK” vem da expressão em inglês Android Application Pack. Um APK é um arquivo compactado responsável por armazenar todas as informações necessárias para a instalação de um aplicativo, este tipo de arquivo encontra-se disponível apenas para dispositivos que possuem o sistema operacional Android.

Um aplicativo contendo a extensão “.apk” pode ser baixado diretamente da loja de aplicativos oficial do Android, a Google Play, porém este mesmo tipo de arquivo também pode ser encontrado em fontes não oficiais. Um aplicativo baixado de uma fonte não confiável, ou seja, fora da Google Play possui altas chances de não ser legítimo e possuir algum tipo de malware executando junto com ele.

Para evitar com que outros aplicativos fora da loja oficial fossem instalados em dispositivos com o sistema operacional Android, o próprio sistema e a Google Play disponibilizam uma ferramenta que impossibilita a instalação de aplicativos de outras fontes, porém todas essas funções de proteção podem ser facilmente desabilitadas pelo usuário caso necessário.

3 MATERIAIS E MÉTODOS

3.1 APARELHOS FUNDAMENTAIS

- Máquina virtual com o sistema operacional Kali Linux 64bits.
- Uma roteador com conexão a rede.
- Um aparelho celular Android.

3.2 SOFTWARES FUNDAMENTAIS

- Metasploit
- Ngrok (?)
- Kwetza (?)

4 METASPLOIT

HD Moore deu início a codificação da ferramenta em 2003, inicialmente desenvolvida na linguagem de programação Perl. O objetivo inicial do Metasploit era ser um jogo com a finalidade de simular um ambiente virtual totalmente vulnerável e explorável que se assemelhasse a um cenário real. Depois do lançamento, o jogo sofreu várias mudanças e foi se tornando gradualmente um framework, logo após estas mudanças a ferramenta foi totalmente reescrita na linguagem de programação 21 Ruby. Depois de se tornar oficialmente um framework de código livre, o seu principal objetivo se tornou desenvolver e configurar exploits e módulos auxiliares com o intuito de explorar falhas e vulnerabilidades.

4.1 EXPLOIT

Exploits são arquivos que possuem um código malicioso dentro deles. Existem vários tipos de exploits, mas cada um possui uma maneira diferente de atuar. Dentre os exploits existentes podemos destacar:

4.1.1 EXPLOIT LOCAL

Exploram vulnerabilidades de sistemas com o intuito de conseguir acesso ao usuário root (administrador) do software a ser atacado. Esta técnica consiste em obter acesso ao shell do sistema, e executar um script.

4.1.2 EXPLOIT REMOTO

Esses exploits necessitam apenas de um host para rodar o script. Esses arquivos são responsáveis por explorar vulnerabilidades remotamente para obter acesso ao sistema, normalmente para executar este tipo de arquivo são usadas vulnerabilidades existentes nos protocolos BIND, FTP, IMAP e POP.

1. BIND é um servidor DNS (Domain Name Service), geralmente é usado em sistemas Unix.

2. FTP é o protocolo de transferência de arquivos.
3. IMAP é um protocolo de responsável por gerenciar a transmissão de correio eletrônico.
4. POP responsável por transferir arquivos de um servidor para uma máquina local.

4.1.3 EXPLOIT DE APLICAÇÕES WEB

Esses exploits são responsáveis por explorar falhas em aplicações web, como, falhas no SQL.

4.1.4 EXPLOIT DoS/DDoS

Esses tipos de exploits são responsáveis por explorar uma vulnerabilidade realizando ataques DoS (Denial of Service) ou DDoS (Distributed Denial of Service), causando assim instabilidade e/ou travamentos no serviço atacado. A diferença entre um ataque DoS e DDoS está na proporção, enquanto o DoS utiliza apenas uma máquina para realizar o lançamento de vários processos no serviço escolhido para ser atacado, os ataques DDoS não utilizam apenas uma máquina, eles empregam várias máquinas zumbis para a execução do processo de ataque.

4.2 PAYLOAD

O payload é um código malicioso que é infiltrado por um exploit em uma falha do sistema atacado. Nele contém as instruções que vão ser executadas após ele ser 23 inserido no sistema, geralmente essas instruções são desenvolvidas utilizando a linguagem de programação Assembly.

5 ENGENHARIA SOCIAL

Segundo Mitnick e Simon (2003), a engenharia social se refere a um conjunto de práticas que utilizam da persuasão e da influência para manipular as pessoas. Aplicam-se os seguintes conceitos para Engenharia:

> aplicação de conhecimentos científicos e empíricos e certas habilitações especificam a criação de estruturas, dispositivos e processos para converter recursos naturais em formas adequadas ao entendimento das necessidades humanas(FERREIRA, 2009, p. 754).

E a seguinte definição para Social: “da sociedade ou relativo a ela, sociável” (FERREIRA, 2009, p. 1864). Então, quando há a junção destes dois termos Rosa et al. (2012, p. 3) dizem que a “Engenharia Social é a aplicação de conhecimentos empíricos e científicos de um modo sociável de acordo com as necessidades humanas para obter informações (como dados pessoais e contas bancarias)”.

Mitnick e Simon ainda complementam o que disseram anteriormente:

> Engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia (MITNICK; SIMON, 2003,p. 6).

Para Pais, Moreira e Varajão (2013), esse campo “trata-se de uma forma ilegítima de obtenção de informação sensível de um indivíduo ou de um colaborador de uma organização”. Geralmente, o atacante (Hacker, Cracker ou “engenheiro social”) se passa por uma pessoa com certa autoridade para conseguir ter acesso à informações confidenciais, as quais uma pessoa comum não teria, isso tudo para conseguir invadir o sistema. Ainda para esses autores, o “engenheiro social” utiliza de meios bem simples para enganar as pessoas, um telefone ou até mesmo à Internet, fazendo com que elas cedam informações confidenciais ou que quebrem algum protocolo de segurança instituído pela empresa. Ainda sob a visão destes autores, quando o “engenheiro social” faz uso das técnicas de Engenharia Social, ele está se aproveitando da tendência humana em confiar nas pessoas e para se aproveitar disso ele leva em consideração o princípio básico da Engenharia Social, o qual diz que o ser humano é o elo mais fraco dentre os mecanismos de segurança.

O website Security One (2011) apud Rosa et al. (2012) cita que o “ataque” do engenheiro social pode acontecer por meio de um bom papo numa mesa de bar ou até mesmo ao telefone e em alguns casos pode ser usada até sedução. O que vai

definir o sucesso do “ataque” será o nível de percepção da vítima abordada sobre o que realmente está acontecendo.

Dessa maneira, o “engenheiro social” não precisa elaborar um plano complexo com dia e hora marcada para efetuar o ataque, ele precisa apenas observar e analisar o momento para se obter informações de uma forma fácil. Seja em um encontro ou numa conversa casual, o engenheiro social tem apenas um objetivo que se baseia em extrair informações confidenciais ou pessoais, fazendo com que as vítimas não tenham percepção de que estão colaborando com o envio dessas informações.

Em Artigonal (2010) apud Rosa et al. (2012) a engenharia social não é só utilizada nos meios digitais, ela é uma ferramenta na qual exploram-se falhas humanas em empresas físicas ou jurídicas as quais possuem operadores do sistema de segurança da informação que tem poder de escolha parcial ou total sobre o sistema de segurança da informação seja ele físico ou virtual, entretanto deve-se frisar que as informações pessoais, não documentadas, conhecimentos, saberes, não são informações físicas ou virtuais, elas compõem um sistema que possui atributos comportamentais e psicológicos onde a engenharia social recebe auxílio de outras técnicas como leitura e linguagem corporal. A partir destas técnicas obtêm-se informações que não são físicas ou virtuais, mas sim comportamentais e psicológicas.

Conforme cita Mitnick, Simon e Wozniak (2002), existe um conjunto de características que influenciam fortemente a predisposição de um indivíduo ser alvo de técnicas de Engenharia Social.

- • Poder e autoridade: os alvos dificilmente questionam a autoridade de quem está se passando por seu “superior”. Assim fica fácil para que o “engenheiro social” tenha sucesso no seu ataque.
- Tendência natural para agradar e ser útil: diante uma situação com seu “superior”, a reação mais comum é a de ser cortês, na esperança de futuramente ser recompensado e elogiado pelos seus superiores, mostrando o quanto o indivíduo foi participativo e solícito. Uma vez que o indivíduo possa ser útil ao seu “superior”, muitas das barreiras que existem, se dissipam para o “engenheiro social”, fazendo com que o caminho até a informação desejada encurte.

- Ligação e similaridade: criar um ambiente de empatia pode facilitar a troca de informação. A estranheza pode surgir no alvo e isso pode dificultar o trabalho do “engenheiro social”, então procurar descobrir pontos de contato com o alvo tende a ser interessante, ou seja, descobrir os interesses, hobbies ou simplesmente o nome do seu interlocutor, são o suficiente para que o “engenheiro social” estabeleça um vínculo com o alvo, tornando o processo todo mais fácil.
- Reciprocidade: o interesse do alvo em benefícios futuros com base no serviço prestado ao seu “superior” pode ser uma vantagem muito útil ao atacante, uma vez que o alvo se torna mais propenso a colaborar, sabendo que em breve será recompensado
- Envolvimento e consistência: grande parte dos ataques costumam ser planejados com muita cautela e paciência de uma maneira a qual o “engenheiro social” procurará adequar-se ao cotidiano tanto da empresa quanto de suas possíveis vítimas. Ele precisará também adequar-se ao dia a dia das vítimas escolhidas e aos poucos tornar “invisível” sua presença dentro da empresa, ganhando desta forma a possibilidade de se movimentar livremente pelo ambiente interno da empresa, sem levantar quaisquer vestígios de sua estadia por ali.
- Baixo envolvimento: os funcionários de cargos mais baixos são um campo interessante para os “engenheiros sociais”. Os atacantes desresponsabilizam qualquer dano e consequência que seja causada pela ação da vítima. Com isso, busca-se relativizar o ocorrido, fazendo com que a vítima veja aquela ação como não nociva à empresa ou a ele próprio, como uma ação irrelevante para todos.

Junior (2006) fala sobre a existência de outros fatores que podem indicar se uma pessoa têm tendência a sofrer um golpe de um engenheiro social, sendo eles:

- Desejo de se tornar útil: as pessoas procuram serem educados ou tentar ajudar os outros;
- Criar amizades: ao ser elogiada, uma pessoa tende a “abrir sua guarda” e tornar-se mais suscetível a disponibilizar informações;
- Estender responsabilidades: geralmente as pessoas não consideram-se como únicas responsáveis pelas responsabilidades e atividades;

- Persuasão: definida pela capacidade de convencer o outro, em busca das respostas desejas para chegar a um objetivo.

Há uma grande gama de trabalhos que debatem sobre o ser humano ser “o elo mais fraco” na segurança da informação e os riscos que isso pode trazer às corporações caso não forneçam um treinamento adequado e eficiente.

“Eu não sou criptoanalista, nem matemático. Apenas sei como as pessoas cometem erros e elas cometem sempre os mesmos erros” (MITNICK; SIMON, 2005, p. 247).

Conforme Mitnick e Simon (2003) a maioria dos funcionários transferidos, demitidos ou rebaixados não causam problemas. Contudo, dentre centenas dos citados, basta um para que a empresa seja prejudicada. Estudos indicam que a maior ameaça a uma empresa vem de dentro e são as pessoas que têm um conhecimento grande do lugar no qual ficam e detêm acesso as informações valiosas. Com isso, o maior perigo para uma empresa vem dela própria, pois, alguns engenheiros sociais têm conhecimento sobre a empresa mesmo sem nunca ter trabalhado lá (por meio de conversas com algum funcionário demitido ou transferido) ou até mesmo um funcionário que não tenha muito conhecimento acerca da engenharia social pode causar danos calamitosos. Por já ter trabalhado na empresa conhece seu cotidiano, os pontos mais frágeis os quais poderá agir sob com mais probabilidade de sucesso, e dessa forma obter as informações de forma mais fácil. Já uma pessoa que nunca trabalhou na empresa terá uma dificuldade muito maior, uma vez que ele precisara fazer pesquisas e gastará muito mais tempo para obter sucesso em seu ataque do que um ex-funcionário revoltado.

Segundo a Sêmola (2014), o lixo pode ser uma fonte de informação rica para os engenheiros sociais, para obterem nome de funcionários, telefones, e-mail, senhas, contatos de clientes, fornecedores e transações realizadas.

Assim como Sêmola (2014), Mitnick e Simon (2003) citam outra ferramenta de pesquisa usada pelos engenheiros sociais: o lixo alheio. “Virar latas” é uma expressão que significa colocar a mãos na lixeira do alvo à procura de informações úteis. A quantidade de informações “inúteis” para um determinado alvo, podem se tornar extremamente úteis para o engenheiro social. Esse “agressor” retira do lixo os recibos de compras alheias, os quais contém nomes, documentos e endereços que as pessoas jogam no lixo de casa, nos lixos da rua ou até nos lixos de seu trabalho (sem nem pensar no risco ao qual estão se expondo). O melhor modo de se prevenir

acerca disso é não jogar nenhum tipo de comprovante, recibo ou extrato de conta bancária no lixo ou na rua. É recomendável que esses documentos sejam queimados, picados ou qualquer outro jeito que não seja possível a recuperação desses dados.

Como forma de contrapor o engenheiro social, Peixoto (2006) ratifica que se todo funcionário fosse questionador como uma criança, demonstrando interesse por tudo, ouvindo atentamente, estando atento a todos os fenômenos à sua volta e principalmente perguntando “porquê” para tudo que lhe dissessem, com certeza as organizações reforçariam seu elo mais fraco, o deixando mais apto e preparado para lidar com os engenheiros sociais. Ao levar a curiosidade característica das crianças para a vida adulta, o ser humano poderia ser alvo de muito menos ataques. Essa indagação por parte das crianças é inevitável, os pais ou a quem foi direcionada a pergunta muitas vezes não conseguem ou não sabem responder de uma forma clara para que a criança entenda ou não respondem realmente a pergunta da criança. Se esse anseio pelo saber fizesse parte do cotidiano dos funcionários dificultaria em muito para que o ataque do engenheiro social tenha 100% de eficácia, pelo fato de a maioria deles já terem algumas respostas prontas para algumas perguntas, mas não terem respostas para “todas” as perguntas. Essa enxurrada de perguntas feitas pelo alvo faria com que o “atacante” não se sinta tão seguro e comece a se sentir pressionado.

Porém, sabe-se que em muitas organizações esse hábito de questionamento não é aceito ou muito bem-vindo, o que faz com que grande parte dos funcionários apenas sigam ordens sem indagar o “porquê” daquilo.

5.1 PHISHING

O termo “Phishing” foi cunhado por volta de 1996 por cyber criminosos que roubavam contas da America Online (AOL) (UOL, 2014).

A Norton (2011) apud Rosa et al. (2012) considera o phishing como um golpe online de falsificação e que seus criadores são falsificadores e ladrões de identidade especializados em tecnologia. Eles utilizam spams, websites maliciosos, mensagens instantâneas e email como ferramenta para que as pessoas forneçam informações sigilosas, como números de contas bancárias e de cartões de crédito.

Segundo Leite e Pereira (2019), o termo phishing pode ser entendido como pescaria e é atualmente o tipo mais comum de engenharia social utilizado pelos cibercriminosos do mundo todo, devido ao fato de ser barato e conseguir atingir até milhões de contas. Esses autores definem o phishing em suma como uma “estratégia do envio de e-mails falsos, fazendo-se passar por instituições financeiras, propagandas de lojas conhecidas com anúncios atraentes, ou até mesmo comunicados governamentais”. (LEITE, PEREIRA, 2019, p. 2). Estes ataques não ocorrem apenas por e-mails, mas também podem ocorrer em formas mais simples, como anúncios nas redes sociais ou uma oferta de serviços que solicita os dados dos usuários para a execução do mesmo. Um exemplo de phishing que emprega este último exemplo é a imagem abaixo, que é uma oferta de cartões de crédito personalizados:

Após ver os exemplos acima, pode-se concluir que o phishing faz-se passar por um comunicado, notícia ou na maioria dos casos anúncios ou websites de fontes credíveis, focalizando o envio destes para usuários desinformados sobre o assunto.

Em Popper e Brignoli (2003) apud Alves (2010), phishing também é a criação de sites falsos que possuem o endereço (URL) muito semelhante ao original. Após preencher dados em sites como esses, os dados são automaticamente enviados para os criminosos. Por isso, é de extrema importância verificar se o website no qual está é o legítimo, para que se evite o roubo de suas informações.

De acordo com a Kaspersky, em 2018 os brasileiros foram os que mais sofreram ataques de phishing no mundo. Este levantamento mostrou que no ano de 2018 cerca de 23% dos usuários do país sofreram ataques, e em 2017 esta estatística sobe para 30% (KASPERSKY, 2018). Segundo Kaspersky (2019) o Brasil é o país que possuiu o maior número de usuários atacados por phishing no primeiro trimestre de 2019, com um crescimento de 3% em relação ao mesmo período de 2018. Isso ocorre pelo fato de que uma parcela esmagadora das pessoas na sociedade não possui o conhecimento necessário sobre segurança da informação para se proteger de ataques efetuados pelos engenheiros sociais, assim se tornando presas fáceis para esses criminosos.

5.1.1 PHARMING PHISHING

Segundo a Avast (2019) essa técnica apresenta-se de duas maneiras:

1. Os criminosos utilizam de algum método para instalar um vírus ou outro tipo de malware no computador do usuário, o qual redireciona o usuário para um site falso, mas muito parecido com o original – os conhecidos softwares crackeados;
2. Os criminosos transformam o pharming em um “redirecionador de links”, eles invadem um DNS e redirecionam os usuários que tentarem acessar o site legítimo para o falso.

Para Pereira (2016) essa técnica explora uma vulnerabilidade existente no servidor DNS conhecida também como DNS cache poisoning. O sistema DNS é o responsável por traduzir uma URL em um endereço que o computador consiga entender, um endereço IP, por exemplo, quando um usuário digitar www.google.com.br é o sistema DNS o responsável por traduzir essa informação para um endereço IP, no caso seria o IP 74.125.234.

De acordo com Paiva (2007) apud Pereira (2016) se o servidor DNS estiver vulnerável, o endereço digitado poderá ser direcionado para uma página falsa, a qual encontra-se hospedada em outro servidor e possui outro endereço IP. Esse processo é feito de forma instantânea, sem que o usuário saiba que está em um site ilegítimo. Segundo o autor, é muito difícil que o usuário perceba que caiu nessa técnica.

5.1.2 SPEAR PHISHING

Spear Phishing é um ataque de phishing que visa um alvo específico, sendo este alvo específico as grandes organizações e para realizar esse ataque é preciso um estudo minucioso por parte dos criminosos, Estabelecendo uma correlação com phishing, esse termo pode ser traduzido como “a pesca de arpão” (MARTINS, 2008).

De acordo com Deep (2019) o spear phishing deriva do phishing e é semelhante a ele, entretanto, essa técnica é potencialmente mais perigosa pelo fato de focalizar em uma empresa ou instituição. Neste método, o criminoso elabora um email a partir de assuntos e fontes que são comuns ao negócio da empresa e em alguns casos o

atacante foca em um departamento específico para que assegurar que no mínimo um de seus profissionais caia no golpe.

Em Computerworld (2012) apud Pereira (2016), olhando pelo lado empresarial, as novas tendências no cenário de spams e fraudes ultrapassam os emails enviados em massa e agora incluem o “spear phishing”, utilizados por criminosos que almejam alcançar alvos específicos de uma empresa.

Um ataque de spear phishing ocorre da seguinte maneira:

> Inicialmente é estabelecido o alvo, que geralmente pode ser um departamento, ou ainda instituições governamentais ou bancárias. Logo depois se faz um levantamento sobre as informações de cada funcionário em diferentes setores. […] Nesta fase o phisher se molda de acordo com o dia a dia da empresa, absorvendo os jargões e assimilando os processos e procedimento internos. Isso pode demorar vários dias, e até lá o phisher pode ser passar por várias pessoas da empresa, até que encontre a informação que deseja ou a pessoa certa para concluir seu ataque. Atingido o seu objetivo, o atacante passa a ter acesso a toda rede da empresa, com acesso a informações sigilosas e poder de realizar transferências ou pagamento por exemplo (PEREIRA, 2016, p. 20).

5.1.3 WHALING

Esse método pode ser traduzido para “caça às baleias” e no site da Avast (2018) está definido como “um ataque de phishing que visa um determinado indivíduo de alto valor” – os “whales” ou “bigfishes”, traduzindo, os peixes grandes. É o mesmo que spear phishing, mas com metas muito mais ambiciosas”. Ainda conforme o site, até mesmo os executivos seniores mais importantes podem sofrer com esse tipo de golpe.

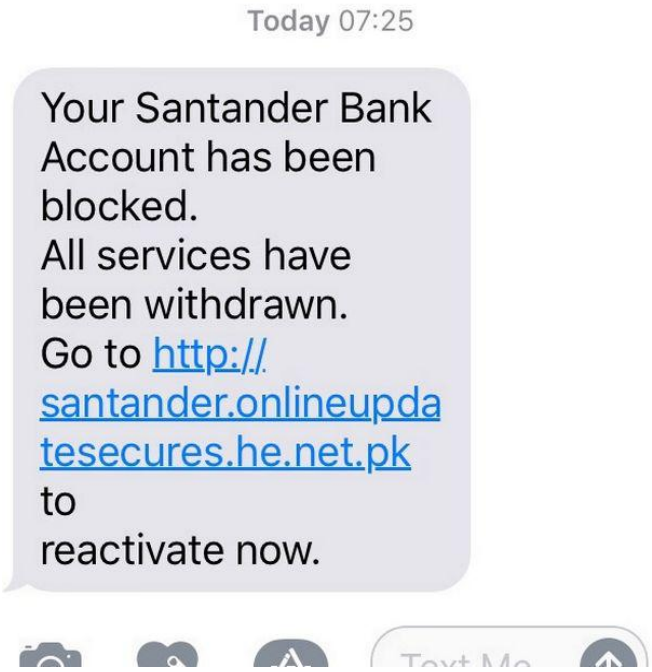
Assim como dito anteriormente, o whaling visa os “peixes grandes”, os CEO’s também estão inclusos. Os criminosos gastarão horas e horas para elaborar as melhores estratégias e o momento perfeito para realizar o ataque, isso tudo para aumentar suas chances de sucesso, uma vez que seu alvo possui um cargo muito alto e certamente possui conhecimento de informações confidenciais da organização (CISCO, 2018).

O exemplo mais comum de whaling é aquele em que um email é enviado para a caixa de entrada de um gerente de call center como se fosse uma mera reclamação de um usuário sobre um determinado serviço. No entanto, o conteúdo deste email é repleto de links de sites malicioso, os quais tentam roubar informações do alvo (DIÓGENES, MAUSER, 2016).

5.1.4 SMISHING

Como pode ser visto na figura X, Essa técnica consiste no formato via SMS do phishing. A Avast (2018) diz que o possível alvo recebe uma mensagem de texto que pede que ele clique em um link ou baixe um aplicativo. Contudo, ao realizar o que se pede, a vítima vai executar um malware em seu aparelho, que poderá capturar suas informações pessoais e enviá-las ao criminoso.

Figura x - SMS Perigoso



Fonte: AVG (2020).

De acordo com Neto (2018, p. 26):

> Smishing, ou SMS Phishing, é uma categoria de phishing na qual o atacante utiliza-se de SMS ou aplicativos de mensagens instantâneas para enviar a URL maliciosa, ao contrário do phishing tradicional que se utiliza de email como meio de divulgação do site malicioso.

5.1.5 VISHING

O vishing é a abreviação de “phishing por voz”, é a forma de áudio do phishing na web. O criminoso tentará persuadir a vítima pela chamada de voz para que ela lhe passe informações pessoais que poderão ser de grande valia para o criminoso futuramente, com as quais ele poderá roubar a identidade do alvo (AVAST, 2018).

Para Neto (2018, p. 28) “Vhishing, ou Voice Phishing, é uma categoria de phishing cujo atraque é realizado através de ligações telefônicas”. O criminoso liga para o alvo passando-se por um funcionário legítimo de uma empresa para solicitar informações sigilosas, persuadir o alvo a acessar um site falso ou configurar um servidor DNS malicioso em sua rede.

O intuito desse golpe é induzir o alvo a ligar para um número - pode ser utilizando a rede da operadora ou o sistema VoIP - e o fazer passar seus dados bancários ou digitá-los para um aparelho que reconheça os sons dos números e os registre. O contato feito via telefone é o método mais efetivo, pois por ser um contato direto (por voz), estimula a confiança do alvo a passar seus dados para o suposto “funcionário do banco” (CRESPO, SYDOW, 2007).

5.2 PRETEXTING

O nome Pretexting é originário da palavra “pretexto”, que é o que o atacante cria para obter as informações desejados por ele do usuário.

Neste método pode ser utilizado inúmeros outros métodos para persuadir o usuário a “entregar o ouro”. Pode ser usado desde uma pesquisa falsa ou até um perfil falso em uma rede social no qual ele criará uma relação de amizade com a vítima e use essa amizade para extrair qualquer dado que possa lhe ser útil (MAILFENCE, 2018).

De acordo com Baer (2008) apud Silva (2013), o pretexting é baseado na criação de um pretexto falso para obter informações da vítima. O cenário inventado pelo criminoso têm o objetivo de fazer com que o alvo não se sinta desconfortável ou tenha suspeitas de que seja um golpe, dessa forma ele realizará, sem grandes problemas, o desejo do engenheiro social. Geralmente, o impostor se passa por um funcionário real, que passa mais credibilidade e confiança para o alvo.

Essa técnica ocorre também por meio de ligações telefônicas, nas quais o criminoso diz ser outra pessoa para conseguir acesso a registros de chamadas ou demais informações de contas bancárias do alvo. Embora existam profissionais que atuam usando o pretexting, esse método não é usado só por eles, em certos casos os golpistas possuem relações com a vítima, por exemplo, um parente ou “amigo” (T-MOBILE apud FERREIRA FILHO, 2018).

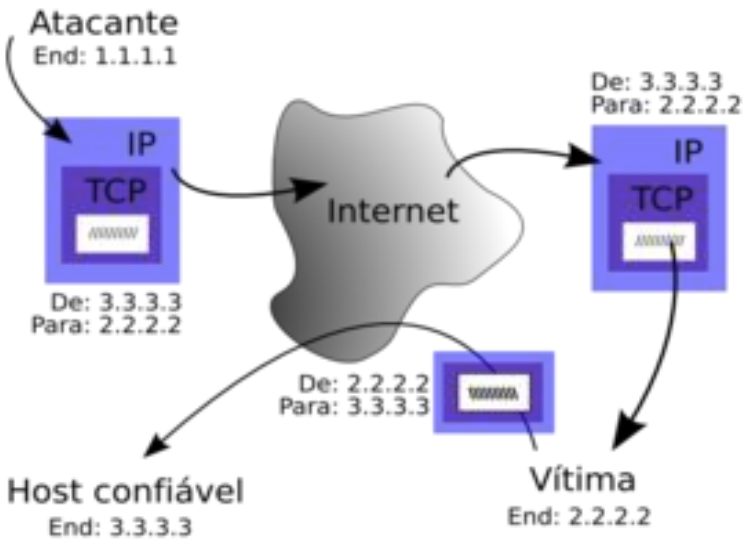
O pretexting nem sempre é maléfico, o que indicára se ele é benéfico ou não será o seu objetivo. O web site perveted justice é uma iniciativa de um grupo de pessoas , os quais fingem serem menores de idade com intenção de chamar a atenção de pedófilos e seduzi-los , fazendo com que assim seja possível sua prisão (SOCIAL-ENGINEER, 2018).

5.3 SPOOFING

A tradução do nome dessa técnica, segundo a Hostmidia é que “o spoofing vem do inglês, especificamente do termo ‘spoof’ e originalmente significava apenas 39 ‘fingir’ ou ‘imitar’ e não tinha uma conotação negativa, mas no jargão tecnológico, assumiu o significado de fazer falsificação.“

O spoofing é uma técnica na qual o criminoso finge ser outro aparelho ou usuário de uma rede com a intenção de acessar dados pessoais(como pode ser visto na figura X), espalhar malwares ou livrar-se das barreiras que os impedem de realizar seu ataque. As formas mais usuais deste método são o spoofing de IP, email e DNS (AVAST, 2019).

Figura X - Como funciona o spoofing



Fonte: Wikipédia (2018.)

Para Avast (2019):

> Essa prática é chamada de spoofing, um termo que engloba a falsificação de endereços IP (enviar mensagens para um computador usando um endereço IP que simula uma fonte confiável), de emails (falsificar o cabeçalho de um e-mail para disfarçar sua origem) e de DNS (modificar o servidor de DNS para redirecionar um nome de domínio específico para outro endereço IP).

Conforme dito por Popper e Brignoli (2003) apud Alves (2010), o spoofing de número telefônico é uma nova técnica que consiste em fraudar o sistema de identificação de chamadas, fazendo com que o número exibido no pelo identificador de chamadas seja aquele pretendido pelo engenheiro social. Dessa forma, ao tornar um número desconhecido em um conhecido aumentam-se as chances do alvo atender e de o engenheiro social colocar seu plano em prática.

5.4 FOOTPRINT

Conforme dizem Popper e Brignoli (2003) apud Alves (2010), o footprint objetiva descobrir informações acerca de algumas tecnologias que são utilizadas pela empresa, principalmente as que dizem respeito ao acesso remoto, Internet e extranet. Existem softwares próprios para isso, eles coletam as informações desejadas pelo engenheiro social. Essa técnica geralmente é usada como “válvula de escape” pelo criminoso quando ele não consegue obter as informações precisas por meio de outras técnicas de engenharia social devido à falta de conhecimento por parte dos alvos sobre o assunto de interesse do invasor.

5.5 TAILGATING

Para NSWorld (2018) o método tailgating é bem antigo e um de seus exemplos é quando o criminoso espera em um ponto estratégico, com suas mãos cheias de equipamentos, um dos funcionários até que ele chegue a uma área restrita. Quando esse funcionário credenciado abre a porta, o criminoso pede para que o funcionário segure a porta para ele, pois ele está com as mãos ocupadas e assim faz o funcionário, de forma inconsciente, sem se dar conta.

Exemplos como este mostram como uma pequena desatenção de um funcionário pode ser uma brecha para a ação do engenheiro social. Após adentrar a área restrita, o criminoso terá tempo de sobra para fazer o que bem entender.

Santos (2016) considera o tailgating como um dos melhores métodos para conseguir ter acesso as áreas restritas das empresas. Para aumentar a efetividade 41 do golpe, o criminoso pode fazer uso de disfarces que favoreçam sua situação, facilitando sua entrada nesses ambientes privados.

5.5.1 PIGGYBACKING

O piggybacking é muito semelhante ao tailgating. Essa técnica é usada, por exemplo, quando o engenheiro social utiliza de informações de uma organização terceirizada e as utiliza para se passar por funcionário legítimo da empresa realizando um serviço, utilizando um uniforme e até mesmo um crachá de identificação. As chances são muitos baixas de que alguém desconfie ou tente barrá-lo após passar para a área restrita, já que se ele está lá é porquê “ele pode” e isso deixa o caminho livre para que o criminoso trabalhe para cumprir seu objetivo naquela área (SANTOS, 2016).

5.6 QUID PRO QUO

Essa técnica é uma expressão latina que significa “tomar uma coisa por outra” e é a origem da palavra brasileira quiproquo No dicionário Collins (2019), esse método cria uma confusão na cabeça do usuário. Em um exemplo, o atacante liga para vários números dentro da empresa oferecendo um serviço.

Em determinado momento, algum dos funcionários realmente precisará daquele serviço oferecido e acreditará na ligação do criminoso. É durante a “prestação de serviço” que o engenheiro social consegue obter os dados dos quais precisa para agir futuramente.

“A tática mais comum envolve se passar por alguém da TI e abordar diversas vítimas encontrar alguém com um problema real de TI” (PROOF, 2018). Sob supervisão do engenheiro social, o alvo fornece códigos, desativa programas

essenciais e instala malwares pensando que está “resolvendo” o seu problema, quando na verdade está entrando em um problema pior ainda.

5.7 BAITING

Baiting é uma tática que já foi bastante utilizada antigamente, na época em que as mídias físicas de armazenamento eram muito utilizadas. Porém, mesmo sendo antigo este tópico merece menção, principalmente para conhecimento da equipe de TI da empresa (MAILFENCE, 2018).

Essa técnica explora a curiosidade e ganância do usuário oferecendo um brinde como um pendrive ou um DVD de um filme famoso ou até mesmo um CD de música, em um lugar bem visível em um escritório. Caso algum funcionário “morda a isca” e tente descobrir o conteúdo da mídia, introduzindo a unidade infectada em seu ambiente de trabalho, acaba por infectar seu computador, e potencialmente sua rede ou até instalando um malware sem nem ter ciência, deixando a empresa vulnerável a riscos desconhecidos (BUETLER, 2009).

6 SEGURANÇA DA INFORMAÇÃO

O conceito de segurança para Avizienis (2004), é um arranjo de atributos de confidencialidade, integridade e disponibilidade que precisa da existência concorrente de disponibilidade apenas para ações autorizadas, confidencialidade e integridade contra acesso não autorizado. Já Stoneburner (2002, p. E-1, tradução nossa) apresenta uma amplificação do conceito, a qual “Segurança em sistemas de informação é uma característica de sistema e um conjunto de mecanismos que 44 abrangem o sistema tanto lógica como fisicamente”. Abaixo, outro autor define o conceito e o objetivo de Segurança da Informação.

Para Fontes (2017, p. 12), a Segurança da Informação é “um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo de proteger a informação, possibilitando que o negócio da organização seja realizado e a sua missão alcançada”. O mesmo autor define para qual objetivo ela existe, a qual:

> “A Segurança da Informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos de informação para o funcionamento da organização. Sem a informação ou com uma informação incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimentos dos acionistas.” (FONTES, 2017, p. 12).

Existem diversos conceitos que caracterizam a Segurança da Informação. Abaixo é apresentada uma lista de conceitos abordados de forma mais ampla pelos autores citados anteriormente.

A confidencialidade é caracterizada pela “ausência de divulgação não autorizada de informações.” (AVIZIENIS, 2004, p. 3, tradução nossa). Para Goodrich (2010) , a confidencialidade se caracteriza pela proteção de dados, isto é, permitir que um usuário acesse à informação somente se ele possuir autorização. Já em Fontes (2017), a confidencialidade deve garantir que a informação seja acessada e utilizada exclusivamente por aqueles que a necessitam para conseguir realizar suas atividades profissionais na empresa. Para isso, é necessário haver uma autorização prévia. Para que se alcance uma boa confidencialidade, diversos outros conceitos estão envolvidos, tais como criptografia, controle de acesso, autenticação, autorização e segurança física.

- Para Goodrich (2010), a criptografia é caracterizada pela transformação da informação usando um segredo, o qual é chamado de chave de encriptação, para que assim as informações transformadas só possam ser lidas utilizando outro segredo, que é chamado de chave de desencriptação. Quando as chaves de 45 encriptação e desencriptação são iguais, elas recebem o nome de chaves simétricas. Quando elas são distintas, são nomeadas de chaves assimétricas.
- Segundo Goodrich (2010), o conceito de controle de acesso pode ser entendido como regras e políticas que limitam o acesso a informações confidenciais apenas às pessoas ou aos sistemas autorizados.
- A autenticação é a “integridade de um conteúdo e origem da mensagem, e possivelmente de alguma outra informação, como o tempo de emissão.” (AVIZIENIS, 2004, p. 14, tradução nossa). Na visão de Goodrich (2010), a autenticação é conceituada como a determinação da identidade ou papel de alguém. A autenticação pode ser efetuada combinando o que esse usuário

possui, o que ele sabe e quem ele é. Exemplo: smartphone, senha e impressão digital.

A integridade, segundo Avizienis (2004), é caracterizada pela falta de modificações inadequadas do sistema. De acordo com Fontes (2017), a integridade existe quando uma informação está correta, é verdadeira e ela não está corrompida. Goodrich (2010), cita outros três conceitos importantes quando o assunto é integridade: backup, checksums e códigos de correção de erros. Tais conceitos adicionais envolvem uma característica essencial para evitar alterações de dados: redundância, replicação de dados ou funções que possam ser detectadas como violações de integridade. Além de proteger os próprios dados é importante manter a integridade dos dados de cada arquivo, ou seja, informações de controle de acesso, de modificações, de proprietários, etc.

> Backup é a cópia e o arquivamento periódico de dados para que, em caso de alteração indesejada ou não autorizada, eles possam ser restaurados. Checksums são definidos como a computação de uma função que 46 mapeia o conteúdo de um arquivo para um número. Uma função checksum depende do conteúdo do arquivo de modo que qualquer alteração realizada sobre ele possui uma alta probabilidade de resultar num número diferente. Dessa maneira, é possível detectar alterações não permitidas em arquivos (GOODRICH, 2010, tradução nossa).

A disponibilidade é “prontidão para o serviço correto.” (AVIZIENIS, 2004, p. 3, tradução nossa). Em Goodrich (2010), a disponibilidade é um atributo da informação que permite que ela possa ser acessada e modificada a qualquer minuto por quem possui acesso. Para alcançar a alta disponibilidade existem dois conceitos fundamentais: redundância computacional e proteção fiscal. Para Fontes (2017), a disponibilidade deve garantir que a informação esteja acessível para o bom funcionamento da empresa e para que ela alcance suas metas e missão.

A legalidade, de acordo com Fontes (2017), é quando a informação está de acordo com as leis aplicáveis, regulamentos, licenças e contratos, assim como as normas éticas seguidas pela organização e desejadas pela sociedade.

A auditabilidade é quando “o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.” (FONTES, 2017, p.13).

Fontes (2010) cita que o não repúdio de autoria, por meios de alguns mecanismos, tem como objetivo garantir a autoria de um usuário, para que assim ele não possa negar o fato que gerou ou alterou uma informação.

Utilizando esses conceitos, a Segurança da Informação trabalha o máximo possível para minimizar os possíveis danos que possam ser causados pelos ataques, uma vez que, segundo Schell (2001), não existe ciência que consiga eliminar de forma definitiva todos os incidentes de segurança da informação, tendo como única opção o constante monitoramento e verificação.

7 VULNERABILIDADES

“Uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça” (MARCIANO, 2006, p. 50). Para o glossário de segurança da Internet, o IETF RFC 2828 (2000), vulnerabilidade é uma falha ou deficiência no projeto, desenvolvimento ou funcionamento de um sistema que pode ser utilizada como meio de violação das políticas de segurança do sistema. Mendes (2017, p. 21) diz que “com isso, podemos dizer que uma vulnerabilidade ocorre quando há uma fraqueza nas medidas protetivas do sistema que pode ser explorada por um usuário malintencionado”.

Conforme Quintão et al. (2010) muitos usuários têm a falsa impressão de estarem seguros quanto ao seu dispositivo móvel, pois eles, em sua maior parte, pensam que o seu dispositivo possui conexões ativas no momento em que realizam ligações ou enquanto navegam na Internet. Entretanto, o problema encontra-se na instalação de inúmeros apps, sem antes possuir um conhecimento prévio de suas funcionalidades e permissões necessárias para o seu bom funcionamento. Grande parte desses apps, rodam em segundo plano, ou seja, por “debaixo dos panos”. Tais apps possuem acesso à informações e dados do dispositivo por meio de processos e todo esse acesso aos dados e as informações ocorre sem que o usuário saiba, demonstrando assim, a vulnerabilidade do dispositivo do usuário.

Isto, para Amaral et al. (2017), “mostra que os dispositivos móveis podem estar sujeitos a várias ameaças, sendo que uma aplicação mal intencionada pode vir a explorar alguma vulnerabilidade do dispositivo móvel que o usuário não tem conhecimento.”. Esse autor ainda complementa dizendo que cada indivíduo deveria ter conhecimento do seu aparelho e das vulnerabilidades que o mesmo poderia ter, com o objetivo de proteger suas informações da melhor forma possível.

Para Almeida (2013), conforme citado por Amaral et al. (2017), o aumento do uso de smartphones está diretamente relacionado as inúmeras vulnerabilidades detectadas nesta plataforma, as quais são, de forma recorrente, exploradas por atacantes que utilizam técnicas como Phishing, Spyware, Bots, Root Exploits... Esse 48 cenário se torna pior pelo fato de que apenas alguns usuários utilizam ferramentas que aumentam o nível de segurança de seus aparelhos.

Neste âmbito, o estudo feito por Acker et al. (2010) conclui que os dispositivos móveis normalmente apresentam falhas de segurança no seu processo de desenvolvimento, sendo aconselhável que os usuários obtenham ferramentas capazes de contornar essas falhas em seus dispositivos. Com o intuito de frear a disseminação destas vulnerabilidades, foram criadas as CVEs (Commom Vulnerabilities and Exposures), uma base de dados pública e internacional que fornece informações sobre vulnerabilidades em diferentes dispositivos e plataformas móveis.

“Na prática, os atacantes utilizam diferentes ferramentas para identificar e explorar estas vulnerabilidades dos sistemas, como scanners de vulnerabilidades disponíveis no mercado e scripts automatizados de teste e invasão.” (FERRÃO; KREUTZ, 2017, p. 1).

Em Mueller e Schleier (2017), citado por Mendes (2017, p. 31) “em seu top 10, a OWASP dá resumo das categorias das principais vulnerabilidades no Android, divididos em categorias segundo seu guia, o Mobile Security Testing Guide (MSTG). São elas:”

1. **Uso Impróprio da Plataforma**: corresponde ao mal-uso de alguma feature ou falha em utilizar controles de segurança. No Android pode ser o mal-uso de intents, permissões, chamadas à API de terceiros ou até algum controle de segurança como Keychain (chaves de acesso privadas);
2. **Armazenamento Inseguro de Dados:** como o nome já diz, compreende o armazenamento de dados de maneira segura ou o seu vazamento não intencional. No Android, os dados podem ser vazados por exemplo, por meio de banco de dados SQLite, logs, XMLs com dados e cartão SD;
3. **Comunicação Insegura:** remete à problemas relacionados ao tráfego de rede do aplicativo, geralmente por não proteger os dados que estão sendo trocados com o servidor

4. **Autenticação Insegura:** os controles de autenticação são falhos, principalmente porque no mundo mobile, não se sabe se o usuário vai estar 49 online ou offline, assim dando margem, por exemplo, à execução de métodos no backend da aplicação
5. **Criptografia Insuficiente**: o código aplica criptografia à alguma informação sensível, porém esta criptografia é insuficiente para proteger estes dados;
6. **Autorização Insegura:** o aplicativo não faz as decisões corretas de autorização. Um exemplo disso seria um usuário com menos privilégio executando uma função de alto privilégio enquanto o aplicativo está em modo offline;
7. **Qualidade do Código:** nesta categoria haveriam todos os problemas relacionados à nível de implementação de código do lado do cliente, como buffer overflow, formatação de string e vários outros;
8. **Adulteração de Código:** modificação do código, memória dinâmica e dados do aplicativo por parte do atacante para obter vantagens pessoais ou monetárias;
9. **Engenharia Reversa:** compreende à análise de código binário, revelação de código fonte, algoritmos e outros recursos a nível de código da aplicação;
10. **Funcionalidade Estranha:** funcionalidades que foram utilizadas para propósitos de teste estão acidentalmente na versão release (lançamento) da aplicação. (MENDES, 2017. p. 31).

8 MALWARES

No campo da Segurança da Informação, malwares são bem conhecidos e perigosos também, sendo definidos como:

> Programa malicioso, código malicioso, software malicioso, ou simplesmente malware, são expressões que se referem a um programa que é inserido em um sistema, normalmente de forma encoberta, com a intenção de comprometer a confidencialidade, integridade ou disponibilidade dos dados da vítima, aplicativos ou o próprio sistema operacional. (DE MELO, 2011, p. 3).

Na visão de Fernandes Filho et al. (2011), atualmente é “difícil ‘enquadrar’ um exemplar de malware em uma única classe, devido à evolução destes códigos e à facilidade de se adicionar novas funcionalidades”. Para De Melo (2011), os malwares podem ser divididos, inicialmente, pela sua dependência ou não do hospedeiro. Os

softwares maliciosos dependentes são por exemplo: vírus, bombas lógicas e backdoors e os não-dependentes worms e zumbis. O modo como os malwares se replicam também é uma outra maneira usada para a classificá-los, vírus e worms são programas maliciosos que conseguem se replicar, por outro lado temos bombas lógicas, backdoors, zumbis, rootkits e keylogger. Existe ainda os malwares híbridos, que conseguem ter mais de uma característica ao mesmo tempo.

Para CERT.br (2018), algumas dentre as diversas formas que os malwares podem infectar ou comprometer um computador (ou um sistema computacional) são:

- Pela exploração de vulnerabilidades existentes nos programas instalados;
- Pela auto-execução de mídias removíveis infectadas;
- Pelo acesso à páginas web maliciosas;
- Pela ação direta de atacantes;
- • Pela execução de arquivos previamente infectados.

Existem diversos malwares, cada qual com sua funcionalidade, alguns deles são citados abaixo. As descrições abordadas a seguir baseiam-se nas definições de De Melo (2011) e Diorio (2018).

Vírus: Normalmente, os vírus infectam arquivos hospedeiros e se propagam através da disseminação desse arquivo. Geralmente, os vírus necessitam de uma ação e propagação que seja feita por uma entidade externa, como por exemplo os usuários.

Worm: Esses programas maliciosos espalham-se pela rede e comumente não necessitam que o usuário o ative, como é o caso do vírus. Outra característica é que os worms não precisam infectar arquivos do hospedeiro para os atacar e se disseminar, como também ocorre nos vírus. E ainda existem alguns worms que carregam dentro de si outro tipo de malware, que é descarregado na vítima após o worm conseguir se instalar no hospedeiro com sucesso.

Trojan: Cavalos-de-Tróia são malwares que buscam atrair a atenção do usuário para que ele instale um software “original e confiável”. Essas versões apresentam a mesma interface e funcionalidade do sistema original, entretanto elas também possuem funcionalidades extras para ocultar as ações ilegais.

Spyware: São programas desenvolvidos para monitorar e capturar as atividades do usuário e fornecê-las a terceiros. Spywares podem ser legítimos ou maliciosos, isso é definido pela forma que são instalados, o que eles fazem, o tipo de informação que monitoram e como os terceiros utilizam as informações recebidas. Existem

spywares que executam ações específicas, como os keyloggers (capturam e armazenam as teclas digitadas pelo usuário), screenloggers (capturam e armazenam a tela e as posições do cursor do usuário) e adwares (apresentam propagandas aleatórias para o usuário).

Ransonware: É um programa que bloqueia os dados armazenados em um equipamento, normalmente usando criptografia, e que exige pagamento de resgate para que esses dados sejam liberados novamente para que o usuário os acesse.

Bot: São programas que possuem mecanismos de comunicação e isso permite que os atacantes os controlem remotamente, possibilitando que eles usem a máquina infectada para executar ataques específicos, envio de spams ou propragação de malwares. Máquinas infectadas por um bot costumam ser chamadas de zumbi, pois são controladas remotamente sem o conhecimento do usuário final.

Backdoor: Tradicionalmente, as backdoors são “pontes” entre a máquina infectada e a máquina do atacante. Elas são usadas para a manutenção de uma máquina hospedeira, ou seja, para que o atacante não perca o vínculo com a máquina e tenha acesso á ela a qualquer momento.

Downloader: São programas que obtém acesso à rede e a usam para instalar um conjunto de outros malwares ou ferramentas que levem ao domínio da máquina comprometida. Para burlar os dispositivos de segurança que a vítima possui, é comum que esse software malicioso chegue ao alvo, anexado em mensagens de email eletrônico e ao serem executados, eles obtêm conteúdo malicioso de fontes externas (Internet).

Dropper: Droppers são similares aos Downloaders, a diferença se dá pelo fato de que eles não precisam buscar conteúdo em fontes externas, o código malicioso está inserido neles, sendo considerados “instaladores”.

Rootkit: São um conjunto de programas que permitem a ocultação da presença do invasor ou de um código malicioso. O objetivo de um rootkit é permanecer em uma máquina residindo no sistema sem ser encontrado, podendo conter exploits e outros malwares.

Para Diorio (2018), “ à medida que os malwares evoluem, outras classificações podem surgir ao longo do tempo. Além disso, um malware pode conter funcionalidades de múltiplas classes, tornando-o mais complexo e difícil de ser detectado e neutralizado”.

9 CONSIDERAÇÕES FINAIS

REFERÊNCIAS

ACKER, Eduardo Verruck; WEBER, Taisy Silva; CECHIN, Sergio Luis. **Injeção de falhas para validar aplicações em ambientes móveis**. In: Workshop de Testes e Tolerância a Falhas. 2010. p. 61-74.

ALMEIDA, Josiane. **ANÁLISE DA SEGURANÇA E DE FERRAMENTAS NA PLATAFORMA ANDROID.** 2013.

ALVES, Cássio Bastos. **SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL Como se proteger para não ser mais uma vítima**. **Brasília: UDF**, 2010.

AVAST. c-phishing. **Avast.** Disponivel em: https://www.avast.com/pt-br/c-phishing. Acesso em 08 jun. 2020.

AVAST. c-pharming. **Avast.** Disponivel em: https://www.avast.com/pt-br/c-pharming#topic-4. Acesso em 08 jun. 2020.

AVAST. o-spoofing. **Avast.** Disponivel em: https://www.avast.com/pt-br/c-spoofing. Acesso em 16 jun. 2020.

AVIZIENIS, Algirdas et al. Basic concepts and taxonomy of dependable and secure computing. **IEEE transactions on dependable and secure computing**, v. 1, n. 1, 2004.

BUETLER, I. **Social Engineering Test cases**. From Compass. Disponível em: https://www.hacking-lab.com/misc/downloads/Social_Engineering_V2.0.pdf. Acesso em 16 jun. 2020.

CANALTECH, 2018. Disponível em: https://canaltech.com.br/seguranca/phishing-golpe-usa-copa-do-mundo-para-roubar-cartao-de-credito-107888/ Acesso em 28 mai. 2020.

CAMURÇA, Francisco. Usuários compartilham no Twitter dados de cartão de crédito em troca de customização. **Welivesecurity**, 2019. Disponível em: https://www.welivesecurity.com/br/2019/05/30/usuarios-compartilham-no-twitter-dados-de-cartao-de-credito-em-troca-de-customizacao/ Acesso em 28 mai. 2020

CERT.br (2018). **Cartilha de Segurança para Internet**. Disponível em: https://cartilha.cert.br/. Acesso em 30 mar. 2020.

CISCO. **O que é Phishing**? 2018. Disponível em: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html. Acesso em 16 jun. 2020.

Acesso em: 14 set. 2018

CRESPO, Marcelo Xavier de Freitas; SYDOW, Spencer Toth. Novas Tendências da Criminalidade Telemática. **Revista de Direito Administrativo**, v. 246, p. 162-180, 2007.

COBUILD, Advanced English Dictionary. Copyright © HarperCollins Publishers. **Collins Dicionary**, Definição de 'quid pro quo'. Disponível em: https://www.collinsdictionary.com/pt/dictionary/english/quid-pro-quo. Acesso em 08 jun. 2020.

CURIOSIDADES, UOL. O que é phishing. **UOL**, 2014. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-e-phishing.html#rmcl. Acesso em 08 jun. 2020.

DELLA FLORA, Julio Cesar Liviero. **Desenvolvimento e aplicação de exploits utilizando o metasploit framework**. Revista Terra & Cultura: Cadernos de Ensino e Pesquisa, v. 26, n. 51, p. 113-124, 2018.

De Melo, L. P., Amaral, D. M., Sakakibara, F., de Almeida, A. R., de Sousa Jr, R. T., & Nascimento, A. (2011). **Análise de Malware: Investigação de Códigos Maliciosos Através de uma Abordagem Prática**. Minicursos do XI Simpósio Brasileiro de Segurança daInformação e de Sistemas Computacionais (SBSeg).

DEEP, Akash. How To Prevent Spear Phishing Attacks. **Hackernoon**, 2019. Disponivel em: https://hackernoon.com/how-to-prevent-spear-phishing-attacks-df35b11133b7. Acesso em 08 jun. 2020.

DIÓGENES, Yuri; MAUSER, Daniel. **Certificação Security+: Da prática para o exame SYO-401**. Novaterra Editora e Distribuidora LTDA, 2016.

DIORIO, Rafael Fernando et al. **Segurança da Informação e de Sistemas Computacionais: Um Estudo Prático sobre Ataques Utilizando Malwares**. Anais SULCOMP, v. 9, 2018.

Fernandes Filho, D. S., Afonso, V. M., Martins, V. F., Grégio, A.R.A., Geus,P.L.,Jino,M., dos Santos, R. D. C.(2011). **Técnicas para Análise Dinâmica de Malware**. XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg).

FERRAO, Isadora Garcia; KREUTZ, Diego. **Segurança na web: análise black-box de scanners de vulnerabilidades.** 1a Escola Regional de Engenharia de Software (ERES), p. 135-142, 2017.

FERREIRA, A. B. H. **Novo Dicionário Aurélio da Língua Portuguesa**. 4ª. Ed. Paraná: Positivo, 2009.

Ferreira Filho, C. T. M.; Corcovia, L. O.; Lima, L. O. Z.; Alves, R. dos S. AMEAÇAS DE ENGENHARIA SOCIAL À SEGURANÇA DA INFORMAÇÃO: FOCO EM PHISHING E PRETEXTING. **SIMTEC - Simpósio de Tecnologia da Fatec Taquaritinga**, v. 5, n. 1, p. 98-112, 21 dez. 2019.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introduction to computer security**. Pearson, 2011.

HOSTMIDIA. **O que é Spoofing e como se proteger?** Disponivel em: https://www.hostmidia.com.br/blog/spoofing/. Acesso em 16 jun. 2020.

IETF. IETF. Internet Engineering Task Force RFC 2828 **Internet Security Glossary**, maio 2000. Disponivel em: https://tools.ietf.org/html/rfc2828. Acesso em 01 abr. 2020.

JUNIOR, Eliezer de Souza Batista. **Uso de vírus desenvolvido no software MSFVENOM contra sistemas operacionais Android com utilização de mensagem SMS**. 2016.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social**. 2006. Disponível em: http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social. Acesso em 12 jun. 2020.

LEITE, Iago Piccoli; PEREIRA, Fagner Coin. ENGENHARIA SOCIAL. **Seminário De Tecnologia Gestão E Educação**, v. 1, n. 2, p. 11-14, 2019.

MARCIANO, João Luiz Pereira. **Segurança da informação: uma abordagem social**. 2006.

MARTINS, Diego de Oliveira. ***Phishing Scam: A fraude do Século 21***, 40 f. Universidade Federal do Rio de Janeiro, 2008.

MATSUNAGA, Igor. Os Principais Golpes de Engenharia Social. **nsworld**, 2018. Disponível em: https://nsworld.com.br/os-principais-golpes-de-engenharia-social/. Acesso em 12 jun. 2020.

MATSUNAGA, Igor. Homem cai em golpe de smishing e tem seu WhatsApp invadido. **nsworld**, 2019. Disponível em: https://nsworld.com.br/homem-cai-em-golpe-de-smishing-e-tem-seu-whatsapp-invadido/. Acesso em 15 jun. 2020.

MENDES, Dimas Albuquerque. **Análise de Vulnerabilidades em Aplicações Android com o Uso de Ferrramentas de Teste de Intrusão e a Metodologia OWASP**. 2017.

MITNICK, K., SIMON, W., WOZNIAK, S. **"The Art of Deception"**, John Wiley & Sons. 2002.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar. **Ataques de Hackers: Controlando o Fator**, 2003.

MITNICK, Kevin D.; SIMON, William L. **The art of intrusion**: the real stories behind the exploits of hackers, intruders, and deceivers. Indianapolis: Wiley Publishing, 2005.

MOURA, Anderson Henrique de. **A utilização do metasploit framework para obtenção de informações de um dispositivo móvel android**. 2017.

NETO, José Durval Carneiro Campello. **Panorama Atual de Smishing no Brasil**. 2018.

PAIS, Ricardo; MOREIRA, Fernando; VARAJÃO, João. **Engenharia Social (ou o carneiro que afinal era um lobo)**. 2013.

PEIXOTO, M. **Engenharia Social e a Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport. 2006.

PEREIRA, Cleber Guedes. **Phishing: conceitos e ações preventivas aplicadas à empresa**. 2016.

PROOF. **Engenharia Social.** 2018. Disponível em: https://www.proof.com.br/blog/ataques-de-engenharia-social/. Acesso em 16 jun. 2020.

QUINTÃO, P. MISAGHI, M. P. S. C. C. S. NOVAIS, E. B. -**Análise dos Desafios e Melhores Práticas Para Resguardar a Segurança e Privacidade dos Dispositivos Móveis no Uso das Redes Sociais** -2010. Disponível em: https://www.researchgate.net/profile/Mehran_Misaghi/publication/274706269_ANL HYPERLINK.

Acesso em 01/04/2020

RODRIGUES, Renato. Brasil é o País com mais usuários atacados por phishing. **Kaspersky**, 2019. Disponível em: https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/ Acesso em 28 mai. 2020.

RODRIGUES, Renato. Brasileiros são maiores vítimas de golpes phishing no mundo. **Kaspersky**, 2018. Disponível em: https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/. Acesso em 08 jun. 2020.

ROSA, Adriano Carlos et al. Engenharia Social: o elo mais frágil da segurança nas empresas. **REAVI-Revista Eletrônica do Alto Vale do Itajaí**, v. 1, n. 2, p. 29-40, 2012.

SANTOS, Daniel Pitanga dos. **A engenharia social no Brasil e seus riscos**. 2016.

SCHELL, Roger R. **Information security: science, pseudoscience, and flying pigs**. In: Seventeenth Annual Computer Security Applications Conference. IEEE, 2001. p. 205-216.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2014.

SILVA, Francisco José Albino Faria Castro. **Classificação Taxonómica dos Ataques de Engenharia Social**. 2013. 132 f. Dissertação (Mestrado em Segurança dos Sistemas de Informação) -Faculdade de Engenharia. Universidade Católica Portuguesa, Sintra

SOCIAL-ENGINEER.**The Social Engineering Framework**. 2018. Disponível em: https://www.social-engineer.org/framework/influencing-others/pretexting/. Acesso em 16 jun. 2020

SOUZA, Valter. o que é pretexting. **Mailfence** , 2018. Disponível em: https://blog.mailfence.com/pt/o-que-e-pretexting. Acesso em 08 jun. 2020.

SOUZA, Valter. engenharia social o que é baiting. **Mailfence** , 2018. Disponivel em: https://blog.mailfence.com/pt/engenharia-social-o-que-e-baiting/. Acesso em 08 jun. 2020.

STONEBURNER, Gary; GOGUEN, Alice; FERINGA, **Alexis. Risk management guide for information technology systems**. Nist special publication, v. 800, n. 30, 2002.

Tailgating Attack: A Physical Social Engineering Crime. Medium, 2020. Disponível em: *https://medium.com/@kratikal/tailgating-attack-a-physical-social-engineering-crime-f63da4195536*. Acesso em 08 jun. 2020.