Trabalho de Conclusão de Curso

A Importância da Criação de uma Ferramenta de Conscientização de Segurança da Informação

Evérton Borges da Silva
ebs@ic.ufal.br

Orientador:
Prof. Dr. Leonardo Viana Pereira

Maceió, 16 de Agosto de 2022

Evérton Borges da Silva

A Importância da Criação de uma Ferramenta de Conscientização de Segurança da Informação

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação do Instituto de Computação da Universidade Federal de Alagoas.

Orientador:

Prof. Dr. Leonardo Viana Pereira

Maceió, 16 de Agosto de 2022

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação do Instituto de Computação da Universidade Federal de Alagoas, aprovada pela comissão examinadora que abaixo assina.

Prof. Dr. Leonardo Viana Pereira - Orientador
Instituto de Computação
Universidade Federal de Alagoas

André Lage Freitas - Examinador
Instituto de Computação
Universidade Federal de Alagoas

Jorge Artur Peçanha de Miranda Coelho - Examinador
Faculdade de Medicina
Universidade Federal de Alagoas

Maceió, 16 de Agosto de 2022

Catalogação na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 - 1767

S586i Silva, Evérton Borges da.
A importância da criação de uma ferramenta de conscientização de segurança da informação / Evérton Borges da Silva. – 2022.
26 f. : il.

Orientador: Leonardo Viana Pereira.
Monografia (Trabalho de conclusão de curso em Ciência da Computação) – Universidade Federal de Alagoas, Instituto de Computação. Maceió, 2022.

Bibliografia: f. 25-26.

1. Segurança da informação. 2. Interfaces de usuário (Sistemas de computação). 3. *Phishing* (Crime por computador). 4. Aquisição de conhecimento. I. Título.

CDU: 004.056.53

Agradecimentos

Agradecimento especial a minha mãe e ao meu pai que tiveram paciência durante toda a minha jornada dessa graduação e sempre me incentivaram a estudar. Sou muito grato por todo o suporte que foi me dado desde os primeiros dias de vida, essa vitória é deles também! Obrigado aos meus irmãos e todos os familiares que são presentes em minha vida.

Quero agradecer aos meus mentores professora Aline Ramos, professor Eduardo Setton e professor Heitor Ramos que sempre me incentivaram durante toda a minha graduação.

Obrigado ao professor Leonardo Viana que aceitou o convite de me orientar nesse TCC e me apoiou durante toda a graduação. Ele foi um dos primeiros professores que conheci na UFAL.

Agradeço a Beatriz Barboza e ao Cristiano Varady por toda a orientação e paciência durante o projeto no LCCV. Aprendi muito nesse período.

Sou grato aos meus amigos Ariany Franca, Ana Ferreira, Bruno Severo, Edla Vitória, Guilherme Medeiros, Hyuri Maciel, Jéssica Almeida, Joilnen Batista, Rodrigo Pinheiro, Roseane Tavares, William Kleber que tiveram comigo durante esse ciclo de graduação e conhecem de perto minhas lutas diárias.

'Este é o nosso mundo agora... o mundo do elétron e do interruptor, a beleza da transmissão. Sim, eu sou um criminoso. Meu crime é a curiosidade. Meu crime é julgar as pessoas pelo que elas dizem e pensam, não pelo que aparentam. Meu crime é ser mais esperto que você, algo pelo qual você nunca vai me perdoar. Eu sou um hacker e este é o meu manifesto. Você pode parar este indivíduo, mas você não pode parar todos nós... afinal, somos todos parecidos".

– Manifesto hacker de 1986

Abstract

Every day new types of cyber attacks and digital threats appear, we need each day to find solutions to combat these digital pests as well. The number of people using the Internet grows every year, it is the duty of security professionals and those who have knowledge to bring awareness to these users and make the worldwide computer network a safer place. It is not protecting from the Internet is protecting on the Internet. The development of awareness tools is important for the propagation of knowledge. And even more important is having conversations about information security indoors, in the office and in the friends wheel. Stay alert and vigilant!

Keywords: Security, Information, User, Cheat, Phishing, Awareness.

Resumo

A cada dia surgem novos tipos de ataques cibernéticos e ameaças digitais, precisamos que a cada dia se encontrem soluções para combater essas pragas digitais também. O número de pessoas utilizando a Internet cresce a cada ano, é dever dos profissionais de segurança e daqueles que tem conhecimento trazer conscientização para esses usuários e tornar a rede mundial de computadores um lugar mais seguro. Não é proteger da Internet é proteger na Internet. O desenvolvimento de ferramentas de conscientização é importante para a propagação do conhecimento. E ainda mais importante é ter conversas sobre segurança da informação dentro de casa, no escritório e na roda de amigos. Continuem atentos e vigilantes!

Palavras-chave: Segurança, Informação, Usuário, Enganar, Phishing, Conscientização.

Contents

List of Figures

1

Introdução

1.1 Motivação

Em 1969 surgiu a primeira conexão entre dois computadores, isso aconteceu em um laboratório nos Estados Unidos. E em 1987 foi liberada para uso comercial, dando início a uma nova era de informação. Segundo Hintzbergen et al. (2018) quando o receptor recebe um dado que tem algum significado é chamado de informação. O número 30 é só um dado e pode ser válido em vários contexto, mas quando dizemos que a temperatura são de 30° estamos dando um significado a ele que é de temperatura.

Hoje a informação pode ser acessada via computadores de mesa, notebooks, smartphones e quaisquer outros dispositivos que tenham conexão com a Internet ou não. Inúmeros artigos científicos de várias áreas da ciência, notícias do Brasil, do planeta e até fora dele, filmes novos e antigos, imagens de obras de arte que antes só poderiam ser vistas no museu, esses são alguns exemplos das informações que temos na Internet e todas elas estão dentro de um aparelho que cabe dentro do nosso bolso. A maioria dessas informações são acessadas pelo modelo cliente-servidor, onde o cliente faz requisições para um servidor que está executando algum tipo de aplicação Andrew Tanenbaum and Wetherall (2021).

O mundo cada vez mais conectado e o grande avanço da tecnologia traz muitos benefícios à humanidade. A conexão com várias pessoas ao redor do mundo, automação de tarefas repetitivas são alguns dos exemplos. E tem o lado ruim também, onde criminosos se aproveitam para tirar vantagens de usuários desinformados, aplicando golpes na internet. Podemos citar a venda de mercadorias que não existe, roubo de dados pessoais e vários outros golpes que surgem todos os dias. Os usuários são a vulnerabilidade que nenhum tipo de programa pode ser instalado para se defender de criminosos que convencem um funcionário de dar informações confidenciais da empresa Weidman (2014). Que não se confunda proteger o usuário na Internet com proteger o usuário da Internet, pois a Internet é um lugar incrível, mas é preciso sempre estar atento e vigilante para os perigos que nela possam conter.

1.2 Objetivos

O nosso trabalho tem como objetivo a construção de Produto Mínimo Viável (MVP) de uma ferramenta online e gratuita para testar os conhecimentos do usuário em relação a segurança da informação. Na plataforma o usuário realizará testes para verificar quais as atitudes que ele tomaria em determinados cenários, assim evitando ser vítima de criminosos.

Além disso, o nosso projeto tem a finalidade de conscientizar os usuários a tomarem medidas de prevenção contra esses tipos de ataques cibernéticos, dando dicas como se prevenir e ensinamentos sobre a área de segurança da informação. Queremos que essas ações promovidas pela plataforma possam evitar dores de cabeças futuras e que possam ajudar esse usuários. Nosso objetivo é conscientizar os visitantes e que eles consigam disseminarem o conhecimento que aprenderam para outros usuários em seu ciclo familiar e de amigos.

2

Segurança da Informação

2.1 Fundamentos

A segurança das redes de computadores começou a se tornar mais relevante com o avanço da Internet e a popularização dos computadores, os perigos digitais vêm crescendo ao longo dos anos. Vale ressaltar que a invasão das redes telefônicas vieram antes da Internet (Andrew Tanenbaum and Wetherall, 2021).

Na segurança da informação foram definidos três pilares: Confidencialidade, Integridade e Disponibilidade. Essas três propriedades são conhecidas como CIA (Confidentiality, Integrity e Availability).

Confidencialidade é quando a informação só está disponível para usuários autorizados (Andrew Tanenbaum and Wetherall, 2021). Quando um criminoso consegue escalar privilégio dentro da rede, de forma ilícita, temos uma quebra de confiança daquela informação.

A integridade garante que a informação chegue ao seu destino sem modificação (Andrew Tanenbaum and Wetherall, 2021) e só será modificada por usuários com permissões de escrita. O ataque Man in the Middle pode comprometer esse pilar, onde o criminosos vai interceptar os dados no meio da comunicação e a informação deixará de ser integra.

A disponibilidade é a propriedade que torna informação acessível a qualquer momento que o usuário necessite utilizar (Hintzbergen et al., 2018). Uma forma de ameaça a essa propriedade é o ataque de negação de serviço ou denial of service (DoS).

2.2 Risco, Ameaça, Vulnerabilidade

Precisamos diferenciar os termos risco, ameaça e vulnerabilidade. Risco, segundo (Hintzbergen et al., 2018) é quando um ativo pode ser comprometido através de uma ameaça por uma vulnerabilidade existente no sistema. Ameaças são potenciais causadores de danos

aos ativos do usuário. Vulnerabilidade é uma brecha de segurança que pode comprometer a tríade da segurança da informação (CIA), segundo (Alexandre Moraes, 2021). Podemos fazer a analogia de uma casa sem teto, onde a chuva pode ser uma ameaça, a vulnerabilidade é estar sem telhado e o risco é molhar toda a parte de dentro. No mundo digital uma ameaça é uma brecha de segurança em determinado programa e o risco é ele não ser corrigido com atualizações e ficar exposto a algum tipo de ataque. Com isso o criminoso pode explorar essa vulnerabilidade e o risco é dele obter informações do usuário.

2.3 Programas Maliciosos

Os programas maliciosos (Malicious Software) ou malwares são programas que tem o objetivo de causar algum tipo de dano em computadores, smartphones, tablets e qualquer outro dispositivo que tenham software embutidos, explorando qualquer tipo de vulnerabilidade. Podemos citar algum desses malwares:

a) Vírus de computador, assim como o vírus biológico, precisa de um hospedeiro para continuar se proliferando. Quando a vítima executa o programa de computador em que o vírus está anexado, ele começa a executar as ações maliciosas para as quais foi desenvolvido.

b) O worm, diferente do vírus de computador, não necessita de um programa hospedeiro para se proliferar. Só é preciso a execução desse worm para ele tentar infectar outros dispositivos na rede (CERT.br, 2012).

c) Cavalo de Tróia ou Trojan não se replica como os vírus e worms. Assim como os gregos enviaram um cavalo de madeira para a cidade de Troia disfarçado de um presente, que parecia inofensivo, dentro estavam vários soldados. Para não serem detectados, os trojans são anexados em programas legítimos (Weidman, 2014), como em documentos, vídeos, anexo de e-mails e outros. Eles ficam escondidos, aguardando serem executados pelo usuário, logo vão causar danos ao dispositivo da vitima. Um dos perigos desse malware é a abertura de portas dos fundos (backdoor) no computador alvo, dando acesso ao cibercriminoso.

d) Spyware é um tipo de malware espião. Dependendo da finalidade para qual foi criado, ele vai registrar as atividades no dispositivo do usuário. Esse rastreio vai desde a coleta das teclas pressionamento (keylogger) até o rastreio de atividades no dispositivo.

e) Ransomware é outro tipo de malware. Ransowm vem do inglês que significa "resgate". Essa praga digital bloqueia o acesso ao dados do dispositivo da vítima através da criptografia [1]. Na tela ficará mostrando as instruções para a liberação do ativo.

[1] https://www.kaspersky.com.br/resource-center/threats/ransomware/

Para todas essas ameaças é bom sempre estar prevenido. Mantendo os softwares de anti malwares e o sistema operacional atualizado. Além disso, ter o cuidado de não executar programas de origem duvidosa.

3

Engenharia Social

3.1 Engenharia Social

O ataque de engenharia social é a forma mais fácil de obter informações sobre um alvo. Quando se usa quaisquer técnicas de manipulação para obter informações pessoais se enquadra nesse ataque, podendo usar ou não auxílio de ferramentas computacionais (Moreno, 2019). Os criminosos que tentam aplicar golpes em suas vítimas são considerados estelionatário (CERT.br, 2012). Todo o ataque de engenharia social existe um objetivo específico, onde esse objetivo pode ser conseguir acesso ao sistema de uma empresa para se obter dados (Ivaturi and Janczewski, 2011).

3.2 Coleta de Informações

Segundo (Moreno, 2019) a coleta de informação é o primeiro passo de um ataque de engenharia social, onde se coleta informações relevantes sobre o alvo. Após isso, ganha-se a confiança, prepare-se como será feito o ataque e a ação é realizada. Em nosso trabalho iremos apresentar algumas formas de obter informações.

3.2.1 Pretexting

É a ação que o criminoso utiliza para persuadir as vítimas, fazendo que elas entreguem algum tipo de informação ou executem algo (Hadnagy, 2010). O atacante cria uma identidade falsa para obter os dados, essa identidade pode ser um suporte técnico de um determinado serviço. A vítima pode acabar caindo no golpe, pois não teve nenhum tipo de instrução/ensinamento sobre esses tipos de crime.

3.2.2 Quid pro Quo

O criminoso usa essa técnica para enganar a vítima, onde oferece algum tipo de incentivo, que não existe ou ele não irá fornecer, em troca de informações (Ivaturi and Janczewski, 2011). A vítima age por impulso a aceitar essa "oferta" imperdível, pois não pode ter outra "oportunidade" dessa.

3.2.3 Trashing

O método trashing também é conhecido como Dumpster Diving. Onde o criminoso vasculha o lixo da organização em busca de algum tipo de informação. Podem ser coletadas vários tipos de informações de uma empresa dentro do lixo (Granger, 2001). Documentos impressos, discos rígidos são alguns exemplos de coisas que podem ser encontradas, caso não exista um descarte consciente desses dados.

3.2.4 Shoulder Surfing

É a técnica de ver por trás dos ombros. A vítima pode estar distraída fazendo algum tipo de ação, como estar digitando suas credenciais ou escrevendo uma mensagem sigilosa, e o criminoso aproveitar para obter esses dados. Mas esse método pode ser mais sofisticado utilizando binóculos e câmeras escondidas.

3.2.5 OSInt

É possível obter informações de um usuário ou organização sem utilizar nenhum tipo meio ilícito, só usando dados fornecidos pelo próprio alvo. A técnica de Open Source Intelligence é a busca inteligente de informações de indivíduos e/ou Organizações em fontes abertas, em sua grande maioria via Internet, mas pode não ser por ela também (Sood and Enbody, 2014). Esses dados são obtidos através de fontes legais e por mídias sociais (Weidman, 2014). As redes sociais são um grande local para a coleta dessas informações. Os usuários mais desavisados deixam a privacidade de lado e permitem que seus dados fiquem expostos.

De acordo com (Silva et al., 2013) 70% das pessoas que participaram da pesquisa tinham o Registro Geral(RG) disponível na internet e 30% tinham o CPF, muitos desses dados são provenientes de concursos. Em outro resultado interessante, mostrou que dos 70% dos participantes que têm o perfil de Facebook ativo, desses 40% tem a data de aniversário exibida publicamente, onde não é necessário ser amigo(a) para visualizar esse dado.

Em um estudo feito (da Silva Geraldo and Takeda, 2019) com 132 amostras válidas, apontou que 30% das pessoas postam fotos com colegas de trabalho, 55% não e 15% não soube informar em redes sociais. Outro dado importante é que 54% costumam colocar o local de trabalho e o cargo contra 45% que não expõe essa informação e 1% não soube informar. Sabemos que

o LinkedIn é uma rede social profissional que conecta profissionais às empresas, mas nela pode conter criminosos em busca de informações.

3.3 Segurança Lógica

Segurança lógica são todos os mecanismos lógicos que impedem o acesso direto à informação. Políticas de segurança da informação, controle de usuário, configurações de rede são exemplos de segurança lógica. A criptografia, assinatura digital e anti-malware são algumas das ferramentas que auxiliam a segurança lógica (Fraga, 2019).

3.4 Segurança Física

Segurança física é quando existe o impedimento de acesso direto a informação por meios físicos (Fraga, 2019). Não adianta todas as configurações de segurança lógica, softwares atualizados e backup para um ativo (servidor), se a segurança física é negligenciada, deixando o controle de acesso físico aberto para qualquer usuário entrar. De acordo com (Hintzbergen et al., 2018) a segurança física não começa dentro da sala que está o ativo, ela começa desde o lado de fora das instalações do negócio. Paredes, portões, cercas elétricas, guardas de segurança, sensores de presença, câmeras são exemplos de segurança física.

3.5 Táticas de Engenharia Social

Existem algumas técnicas para realizar o ataque de engenharia social e ser mais sucedido em obter os dados da vítima. Se o criminoso tem o objetivo de coletar as informações daquele usuário ele vai aguardar o tempo necessário. Iremos citar algumas das táticas mais utilizadas abaixo:

a) Autoridade: Enganar o usuário se passando por uma autoridade no assunto, podemos citar um técnico de suporte técnico, ou exercer um cargo superior.

b) Intimidação: Receber ameaças do criminoso caso não realize algum tipo de ação que ele ordenou.

c) Consenso / Prova Social: Fazer algo por ter consciência que outras pessoas já fizeram.

d) Escassez: Receber uma oferta de um produto que está com poucas unidades e com um bom preço.

e) Urgência: Receber um e-mail dizendo que sua conta bancária será bloqueada em alguns dias ou horas.

f) Familiaridade/Gosto: Falar de interesses em comum com a vítima.

g) Confiança: Ganhar confiança da vítima ao aos poucos até ela se sentir confortável de fornecer os dados.

3.6 Phishing

O ataque de phishing é um tipo de fraude, onde o usuário recebe um e-mail que tenta enganar e obter informações pessoais e financeiras dele. É difícil prender esses criminosos, por isso é importante os usuários ficarem atentos e não responder a e-mails que solicitam dados pessoais (Hintzbergen et al., 2018). Os e-mails enviados são descartáveis e não são vinculados ao nome do atacante, onde esses podem usar seus próprios servidores. As mensagens normalmente contém tópicos e temas atuais para chamar mais atenção do usuário como avisos judiciais, cartão de crédito, eleições, prêmios dentre outros (CERT.br, 2012). Exemplos de páginas falsas que podem ser recebidas por e-mail são de empresas de comércio eletrônico, grandes instituições financeiras, redes sociais (Facebook, Instagram), solicitação de recadastramento(CERT.br, 2012).

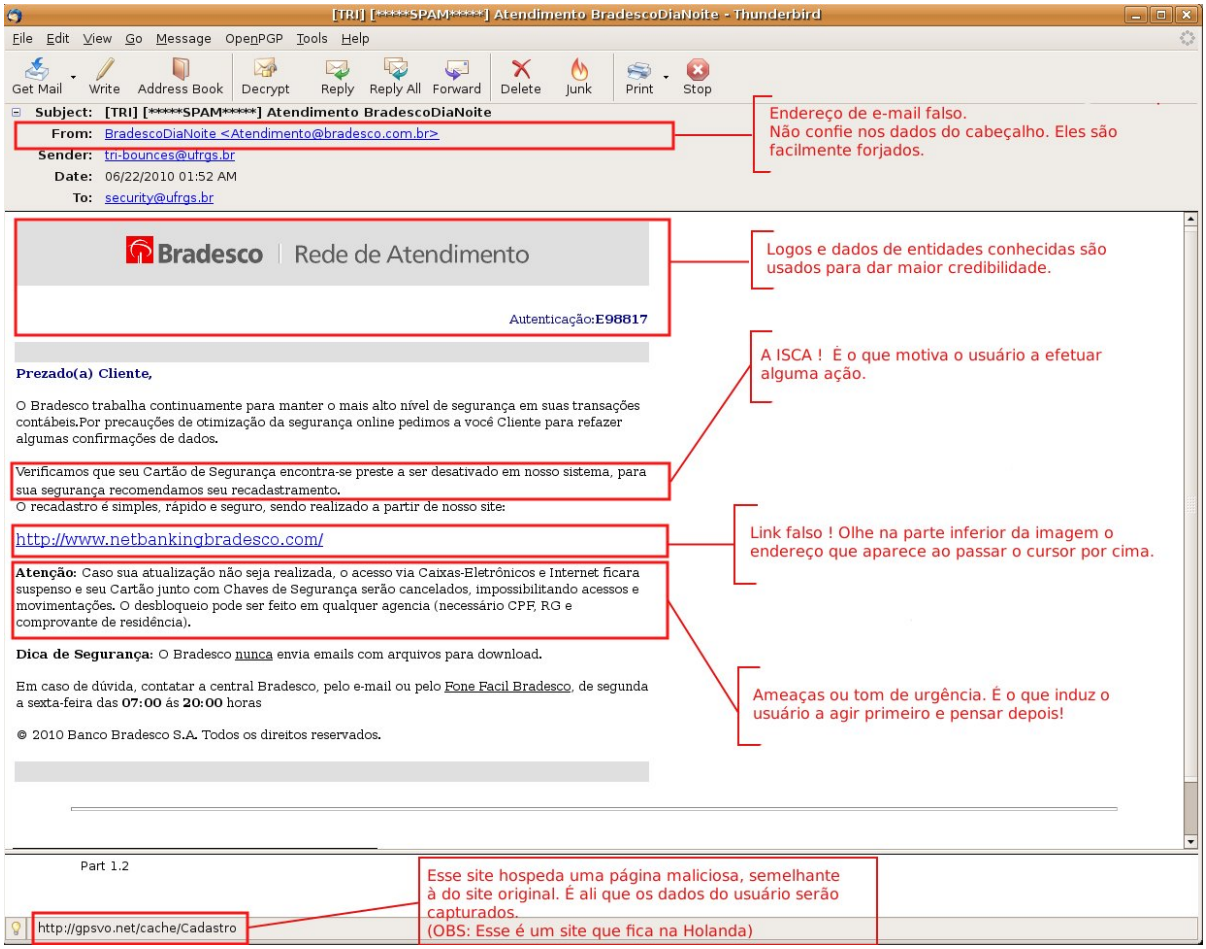

Figure 3.1: Características de um phishing

Além de links maliciosos, os e-mails podem conter um arquivo mal intencionado. Para enganar usuários o payload (carga útil) é escondido em programas executáveis conhecidos e legítimos que ao serem abertos pela vítima será executado e junto dele o código malicioso em segundo plano, esses arquivos são conhecidos como cavalo de tróia ou trojan (Weidman, 2014).

Segundo o relatório de KnowBe4 (2021), no top 10 global de categorias de phishing mais clicados estão Business (Negócios) 24%, Online Services (Serviços Online) 19%, Human Resources (Recursos Humanos) 16%, IT (Tecnologia da Informação) 11%, Banking and Finance (Bancos e Finanças) 8%, Coronavirus/COVID-19 Phishing 8%, Mail Notifications (Notificações de Correio Eletrôncio) 4%, Holiday (Feriados) 4%, Phishing for Sensitive Information (Phishing para Informações Confidenciais) 3% e Social Networking (Rede Sociais) 3%.

3.6.1 Vishing

Também chamado de voice phishing, é uma variação do phishing que utiliza a tecnologia de comunicação de voz, onde os criminosos ligam para suas vítimas para realizar o ataque (cis) e obter informações pessoais. Essas ligações são normalmente feitas usando a tecnologia Voice Over Internet (VOIP).

3.6.2 Smishing

É uma outra variação de phishing, podendo ser chamado de SMS phishing, onde são enviados Short Mensage Service (SMS) para tentar enganar a vítima. De acordo com o relatório (Pro) durante o ano de 2020 esse ataque cresceu cerca de 300%.

3.6.3 Spear Phishing

É um ataque de phishing direcionado. O atacante vai escolher bem suas vítimas, aquelas que possam fornecer informações valiosas para realizar o ataque. Usuários que têm maiores privilégios dentro da rede de computadores são os mais visados.

4

Conscientização

4.1 Conscientização na Segurança da Informação

Vários relatórios apontam um crescimento de ataques cibernéticos no ano de 2021. Segundo o infográfico de (ISACA, 2021) as empresas relataram um crescimento de 35% de ciberataques, sendo o ataque de Engenharia Social é o mais frequente com 14%. Muitos dos e-mails tinham relação com vacinas ou seguro emergência no Brasil. Houve um crescimento de 22% no volume de ataques de phishing em 2021, em uma pesquisa realizada por (PhishLabs, 2022). Quando o atacante é bem-sucedido em seu ataque, de acordo com o relatório de (Verizon, 2021) apontou que os dados comprometidos são credenciais (85%), dados pessoais (17%), outros (9%) e dados médicos (4%). Apesar desses números, segundo o relatório da CyberSafe e da National Cybersecurity Alliance (Karppinen and Ince, 2021), 67% dos participantes se acham preparados para identificar um e-mail malicioso e 38% se sentem como um alvo de cibercriminoso.

4.2 A Importância da Conscientização do Usuário

Devido ao crescimento de ataques que têm como alvo o ser humano, devemos criar maneiras de proteger esses usuários. Logo precisamos realizar a conscientização deles para que sejam menos propícios a cair em um desses ataques de engenharia social. O ano de 2021 foi um ano pandêmico, as pessoas necessitaram ficar em casa e trazer trabalho para casa. Vários golpes foram lançados envolvendo falsa central telefônica e do falso funcionário do banco[1].

O Observatório de Crimes Cibernéticos (OCC) lançou um ebook chamado "É bom demais para ser verdade?" (Alesandro Gonçalves Barreto, 2022), onde relata os golpes e delitos mais

[1] https://g1.globo.com/jornal-nacional/noticia/2021/04/16/golpes-e-fraudes-por-telefone-e-e-mail-disparam-no-brasil-durante-a-pandemia.ghtml/

comuns na Internet. Estão na lista as fraudes envolvendo o mensageiro de mensagens instantâneas WhatsApp e a rede social Instagram. Além do PIX que é o recente meio de pagamento eletrônico que foi lançado em 2020. Todos esses crimes tem algo em comum, os alvo são usuários das plataformas digitais.

Um dos golpes do Whatsapp é o SIM SWAP, onde o número da vítima é clonado pelo criminoso. Se o usuário não configurou a autenticação de duas etapas no aplicativo, o atacante terá acesso ao Whatsapp da vítima. Com acesso ao aplicativo, o criminoso pode disparar mensagem falsas para a lista de contatos da vítima pedindo "emprestado" dinheiro. Para evitar esse tipo de ataque é preciso ativar a confirmação em duas etapas do próprio WhatsApp, assim, será necessário de PIN quando for registrar o número de telefone no aplicativo.

O mais importante é saber o que medir e como medir o nível de conscientização em segurança da informação desses usuários (Kruger and Kearney, 2006). A conscientização pode começar a ser realizada por meio de treinamentos periódicos dentro da organização de trabalho e simulações de ataques por órgãos responsáveis. Mas a conscientização deve ir além, deve ser parte da cultura do usuário saber identificar e como agir nessa situação. De acordo com o relatório da CyberSafe e da National Cybersecurity Alliance (Karppinen and Ince, 2021) 64% dos participantes não tiveram nenhum tipo de treinamento. E ainda segundo a pesquisa, os participantes que tiveram acesso aos treinamentos, 73% mostraram interesse em aprender mais sobre o assunto quando a informação é disponibilizada a eles.

Podemos citar outras medidas para ajudar no fortalecimento das defesas desse usuário e no ambiente que ele está alocado, entre eles podem ser:

a) Ter cuidado com os links em e-mail e mensagens, pois podem levar usuários a páginas falsas.

b) Usar senhas fortes e diferentes para cada site que exige autenticação. Ative o fator de autenticação em duas etapas.

c) Instalar somente programas legítimos em seu dispositivo. Programas de procedências duvidosas podem conter malwares.

d) Conectar em redes confiáveis e seguras. Não confie em redes abertas. Na dúvida é melhor se conectar nos dados móveis.

e) Instalar atualizações do sistema operacional é importante para a correção de bugs e falhas.

f) Revisar os dados pessoais que estão públicos em suas redes sociais;

Essas medidas devem ser inseridas no dia-a-dia do usuário. A ferramenta que estamos propondo irá mensurar o conhecimento sobre o assunto, a atitude e o comportamento em determinada situação como é proposto em (Kruger and Kearney, 2006). Se cada usuário levar o

tema de segurança da informação para as rodas de conversas de amigos e familiares podemos ter uma redução no número de ataques de engenharia social.

A importância da conscientização é grande, mas é precisar saber o que fazer após o crime ser cometido. Baseado em um estudo feito por (Öğütçü et al., 2016) mostrou que 46% das pessoas que sofreram um ciber crime não tinham relatado para as autoridades. É uma porcentagem alta, a pesquisa ainda revelou que 40.4% não sabem a quem recorrer nessas situações.

4.3 Configuração do Ambiente de Ataque

Será demonstrado como pode ser realizado um ataque de phishing em poucos passos. Estaremos utilizado o sistema operacional (s.o.) open source chamado Kali Linux que é baseado na distribuição Debian. Dentro desse s.o. existem diversas ferramentas direcionadas para executar tarefas sobre segurança da informação [2], dentre elas a que iremos utilizar em nosso experimento para a criação de páginas falsas. Será utilizado o programa chamado VirtualBox para emular nosso sistema operacional do Kali Linux. Essa ferramenta será responsável pela criação de uma maquina virtual (virtual machine) com as seguintes configurações:

a) Memória Principal: 2048 MB;

b) Processador: Intel Core i5 com 2 núcleos;

c) Disco Rígido: 60GB;

A criação de vms nos traz os benefícios de necessitar de espaço físico de somente uma máquina física e de suas configurações (processador, memória e disco rígido). Outra vantagem é que podemos realizar downloads de imagens prontas de vms , mas tomando os cuidados de fazer em sites confiáveis e é importante a verificação de integridade desse arquivo.

4.4 Criação do Phishing

Para a criação do ataque de phishing, iremos utilizar a ferramenta do Kali-Linux chamada Social-Engineer Toolkit (SET) que é uma ferramenta de código aberto escrita em Python. Vamos utilizá-la para demonstrar em um ambiente controlado a criação de páginas falsas dos principais domínio da Internet e de como acontece o ataque de phishing.

4.4.1 Criando Páginas Falsas

É preciso iniciar o Social-Engineer Toolkit (SET) no Kali-Linux e selecionar algumas opções para fazer a criação de páginas falsas. Na figura 4.1 podemos ver a tela inicial da ferramenta.

[2] https://www.kali.org/docs/introduction/what-is-kali-linux/

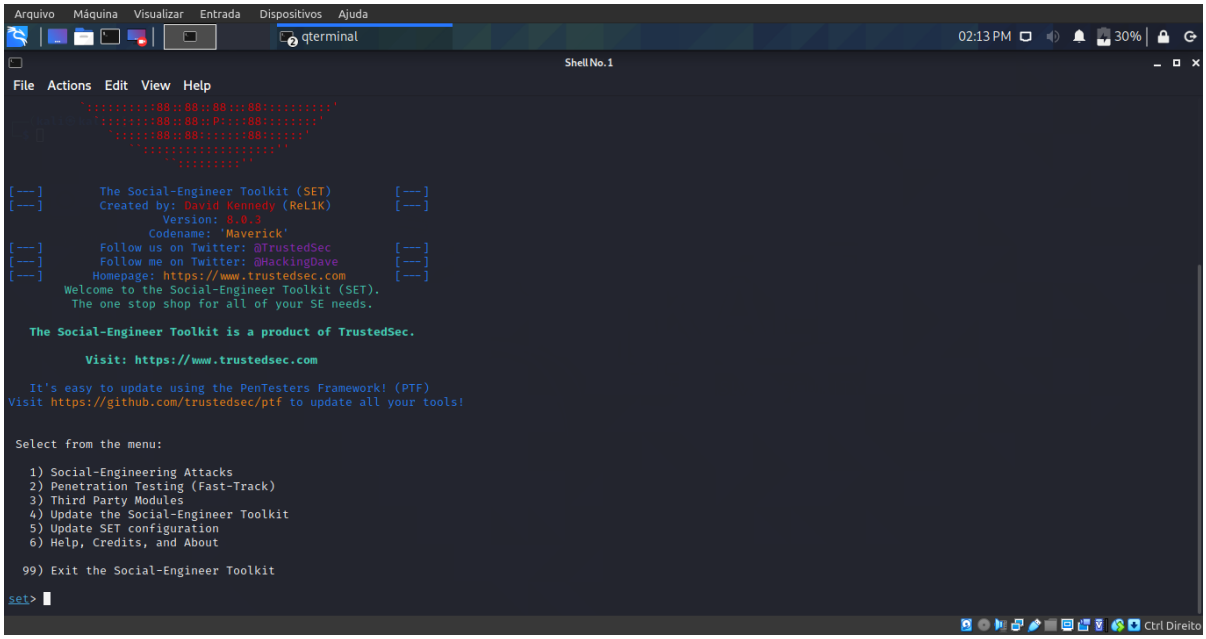

Figure 4.1: Tela inicial da ferramenta SET

Iremos utilizar um template do Twitter para realizar nossos testes. Mas como pode ser visto na figura 4.2, podemos usar outros templates. A ferramenta nos dá a opção de clonar outras páginas web.

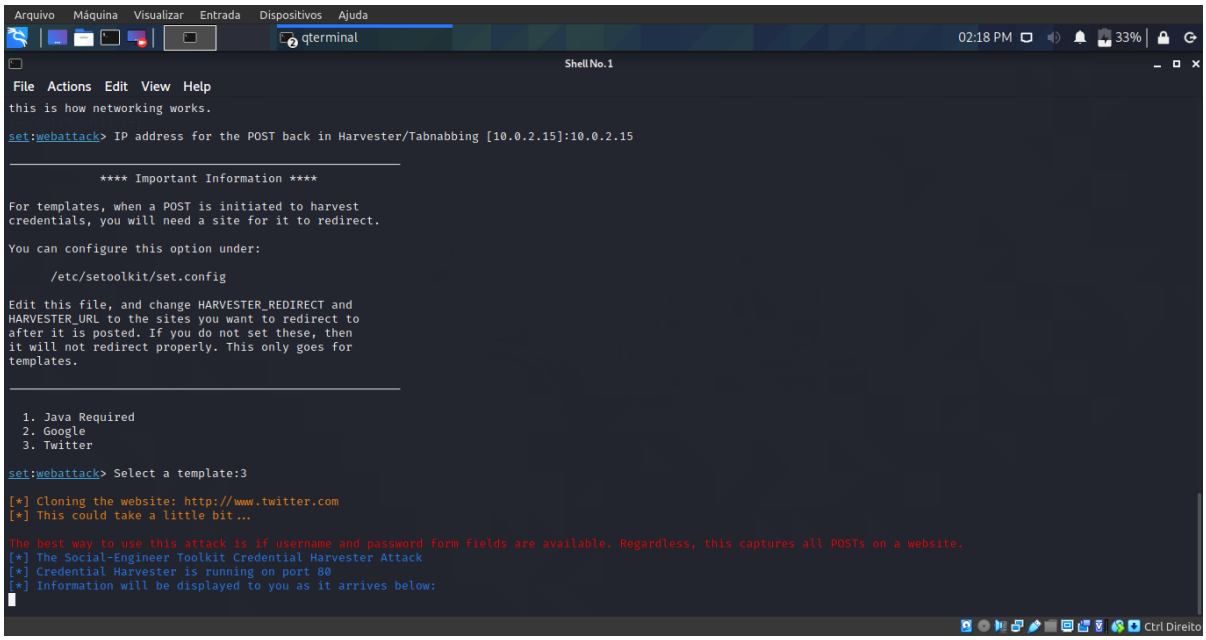

Figure 4.2: Escolha do template do Twitter

Podemos ver na figura 4.3 uma página falsa do Twitter, onde essa pode ser acessada via IP do próprio Kali-Linux. É possível fazer uma resolução DNS e alterar esse IP para um nome parecido com o nome original. Assim o ataque fica mais convincente, mas estamos em um

ambiente de testes e o objetivo é demonstrar o que se pode fazer com a ferramenta SET. Esse IP pode ser acessado por qualquer máquina na rede. Caso queira que essa página esteja disponível na Internet, precisaríamos de um IP público.

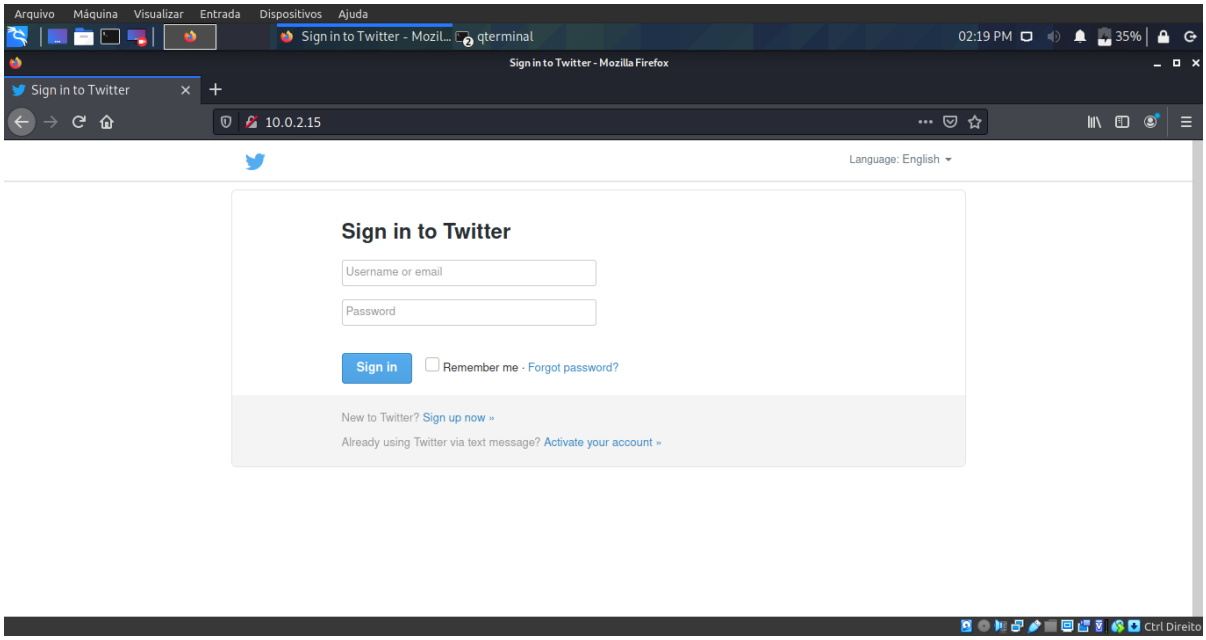

Figure 4.3: Página falsa do Twitter

Quando o usuário entrar com suas credenciais de login e senha, essas serão capturadas pela ferramenta, podemos verificar o nome e a senha em texto sem codificação na figura 4.4 e o usuário será redirecionado para a verdadeira página do Twitter (https://twitter.com/). Para a vítima esse redirecionamento pode ser percebido ou não. É importante verificar se aquele site das redes sociais, do banco ou qualquer outro que exija credenciais correspondem a URL legítima.

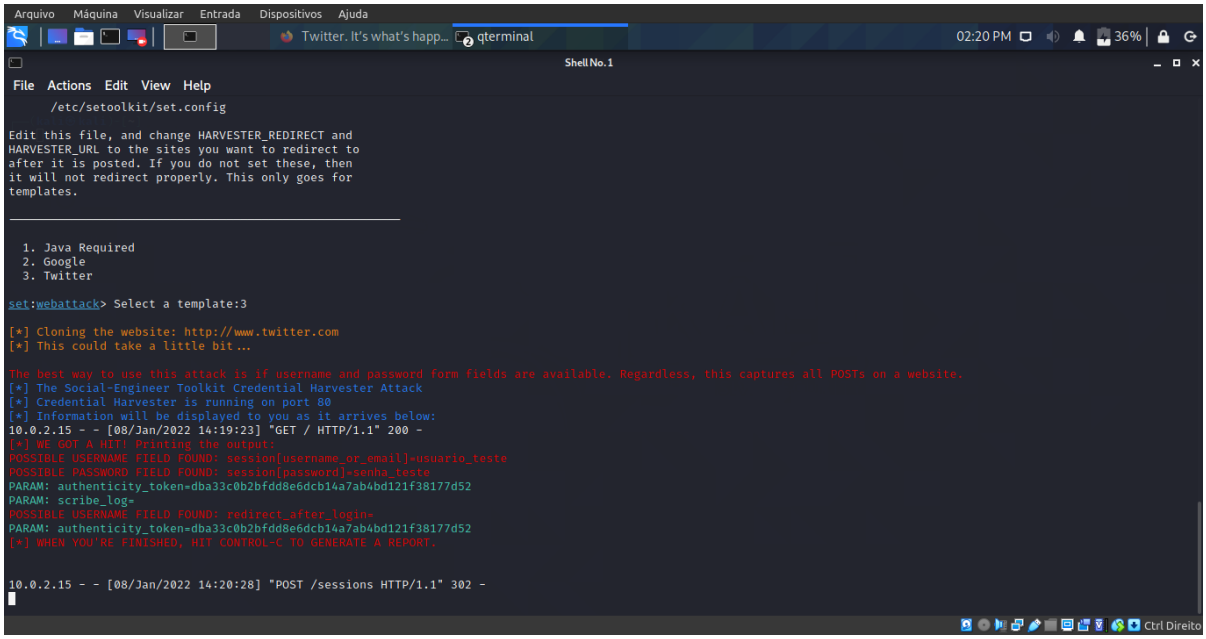

Figure 4.4: Captura das credenciais do usuário

Por isso a importância de usar sites com o protocolo HTTPS. Os domínios com HTTPS indica que terá autenticação entre o cliente e servidor e a proteção de integridade dos dados (Andrew Tanenbaum and Wetherall, 2021). Normalmente utiliza a porta 443, diferente do HTTP que usa a 80 como padrão.

4.4.2 Enviando um Phishing

O link pode ser colocado no corpo do e-mail e uma história deve ser inventada para o alvo achar necessário se conectar a sua conta do Twitter. Nessa história vai conter uma isca e ameaça ou urgência para o usuário tentar se conectar rapidamente.

5

Metodologia

5.1 Desenvolvimento da Ferramenta de Conscientização

Foi utilizado o framework web Django que é escrito na linguagem Python para o desenvolvimento de nossa aplicação. Python é uma linguagem de interpretada e com tipagem dinâmica, usada em diversas áreas da computação como desenvolvimento web, ciência dos dados, jogos entre outros. Na classificação das linguagem mais utilizadas Python aparece em primeiro lugar, segundo TIOBE Programming Community no mês de fevereiro de 2022[1]. E de acordo com PYPL PopularitY of Programming Language[2] no mês de fevereiro de 2022, tutorial de Python foi a linguaguem mais buscada no Google. Vamos utilizar a versão 3.8, versão atual da linguagem está na 3.10.

Django é gratuito e de código aberto, além disso é rápido, seguro e escalável. "Django incentiva o desenvolvimento rápido e um design limpo e pragmático"[3]. O framework usa o conceito Model, View e Template (MVT) como padrão de projeto. O Model é responsável gerenciamento de dados no banco de dados. O View faz a ligação entre o Model e Template, é responsável por controlar as ações da aplicação. E os Templates são as páginas HTML para a visualização e interação com o usuário.

Foi criado um modelo chamado "Question", onde é criado um objeto de cada questão. O atributo "question" é onde fica a descrição do cenário que o usuário é submetido. O "answerYes" contém a afirmação, isso que dizer que o usuário concorda com o cenário que lhe é apresentado. o "answerNo" é negação, será escolhido caso o usuário não concorde com o questionamento. O "answerIDontKnow" foi criado para acolher os usuários que não foram apresentados a determinados assuntos e/ou não presenciaram determinada situação.

[1] https://www.tiobe.com/tiobe-index/
[2] https://pypl.github.io/PYPL.html
[3] https://www.djangoproject.com/

```
1  class Question(models.Model):
2      question = models.CharField(max_length= 300, null=True)
3      answerYes = models.CharField(max_length=200, null=True)
4      answerNo = models.CharField(max_length=200, null=True)
5      answerIDontKnow = models.CharField(max_length=200, null=True)
6
7      answerCorrect = models.CharField(max_length=200, null=True)
8
9      help = models.CharField(max_length= 200, null=True)
10
11     def __str__(self) -> str:
12         return self.question
```

Umas das nossas principais *Views* tem a função de escolher os cenário para serem mostrados aos usuários. Esses são escolhidos de forma aleatória, assim gerando novo questionário para cada novo usuário. Por enquanto temos no total 18 questionamentos, mas o usuário só será testado em 10.

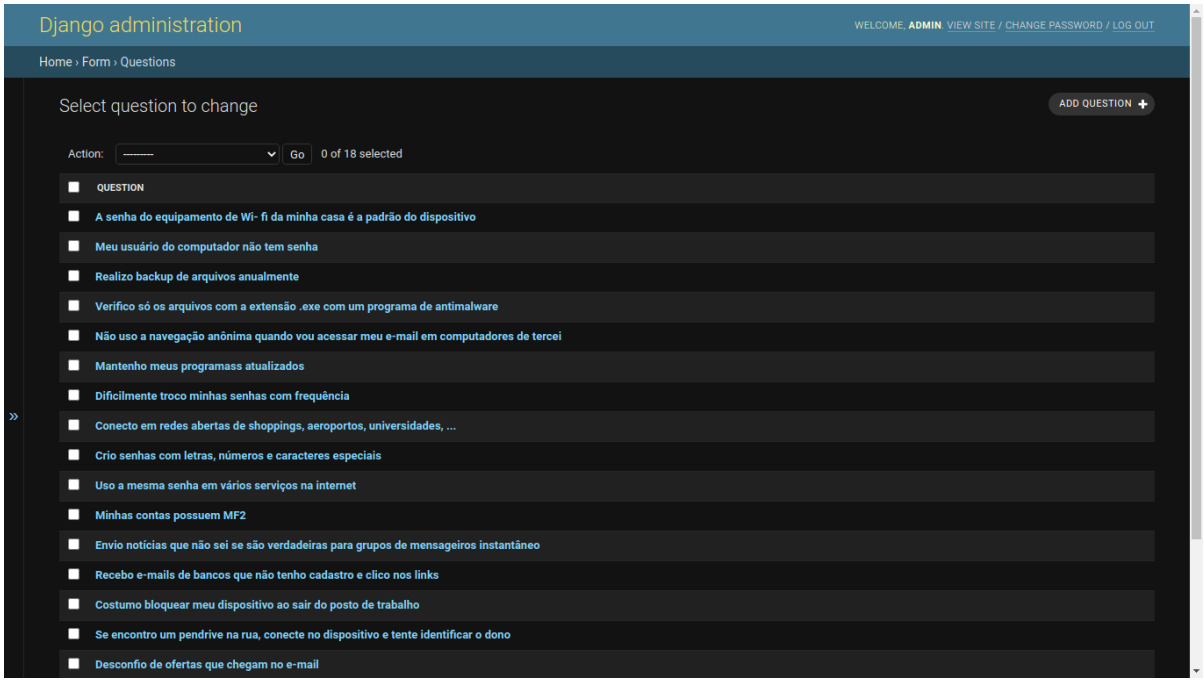

Figure 5.1: Banco de dados contendo todos cenários

Na interface web do usuário, ele será submetido a 10 cenários, que tentam reproduzir ambientes reais. Poderá ser escolhido entre as opções "Sim" que se refere ao "answerYes", "Não" é o "answerNO" e "Não aprendi sobre isso" é o equivalente a "answerIDontKnow" no models.

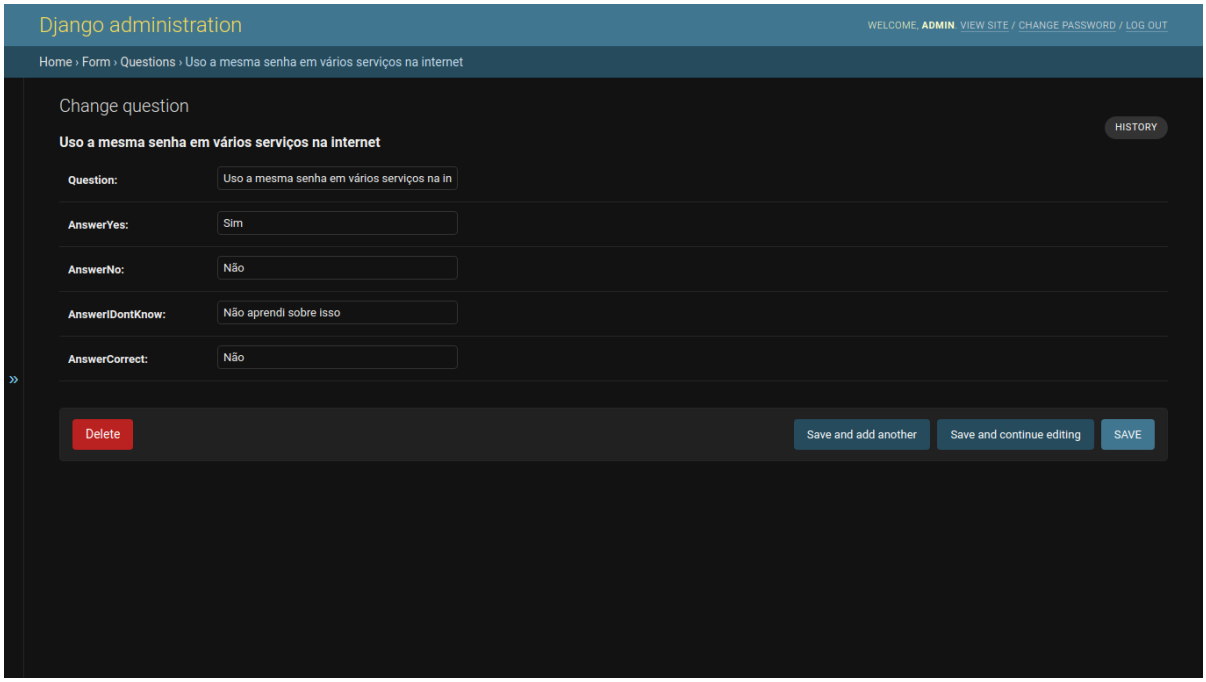

Figure 5.2: Cenário

O conjunto de cenários será feito de forma aleatória para cada usuário e a partir de um banco de dados que contém 18 cenários até o momento da publicação do nosso trabalho. Não será preciso se identificar ou fazer login na plataforma. Também Não é possível pular ou voltar.

A interface da página de resultado mostra alguns valores. **Porcentagem de Acertos** é feito utilizando média aritmética do número de acertos dividido pelo total. **Total de questões, Respostas Corretas e Respostas Erradas** são o próprio valor da variável. Decidimos que todas os questionamentos tem o mesmo valor, assim o valor de **Pontuação** fica como a soma de acertos.

5.2 Considerações

O servidor web será executado em uma máquina local com o IP 127.0.0.1 na porta 8000, poderíamos ter escolhido qualquer porta que estivesse disponível, escolhemos a padrão do sistema. Para o nosso trabalho a ferramenta só poderá ser acessado dentro da rede local onde o servidor está inserido. Limitando a nossa ferramenta de conscientização para alguns usuários. Mas nada impede dela ser disponibilizada na Internet, mas para isso é preciso fazer a hospedagem em algum domínio.

6

Resultados

6.1 Cenário

A plataforma testará os conhecimentos do usuário em relação aos principais tipos de ataque de engenharia social e sobre assuntos relacionados através de um questionário de múltipla escolha. Após o usuário chegar aos cenários que lhe são apresentados, será dado um resultado final e mostrará o quanto ele conseguiu pontuar. Isso não define sua capacidade de se defender ou não de ameaças na Internet, mas ajuda na conscientização dos usuários.

6.2 Implementação

A ferramenta tem uma interface inicial, onde vamos popular com diversos assuntos sobre segurança da informação. Na página temos as abas Segurança da Informação, onde vamos colocar as definições da área. Na aba de malwares será colocado os principais programas maliciosos conhecidos. Na aba de Dicas de Segurança vamos reunir as melhores práticas a serem adotadas pelos usuários. Além disso, temos o botão para a realização do Teste de Conscientização que é o objetivo do nosso trabalho.

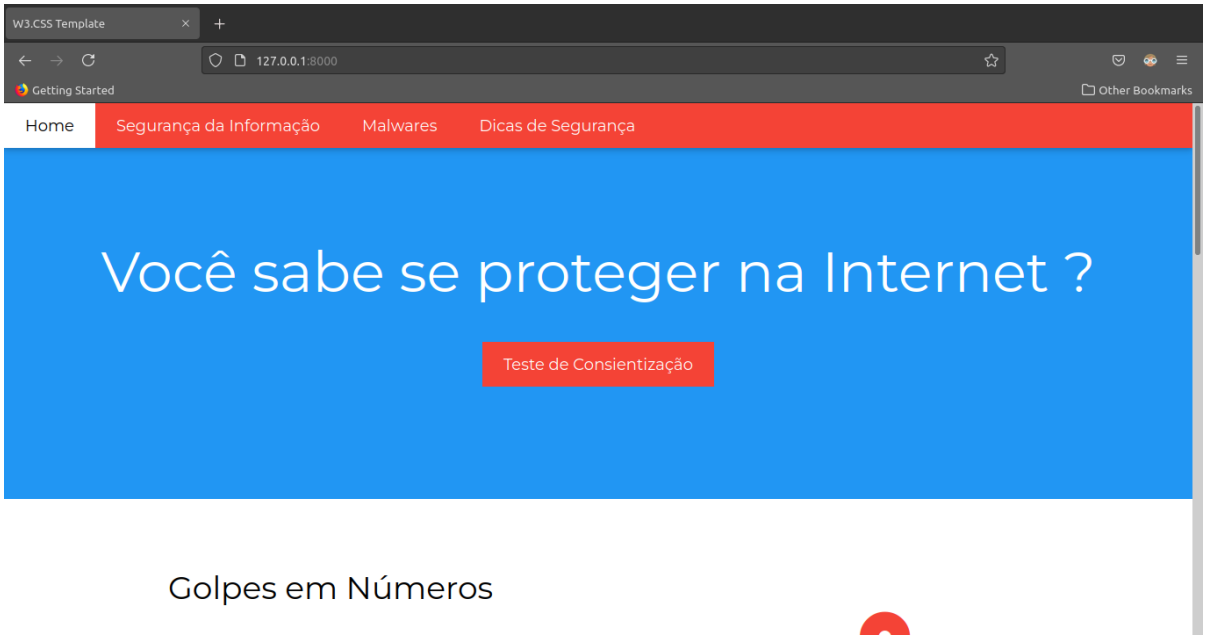

Figure 6.1: Interface inicial da aplicação Web

Antes de iniciar o questionário, o usuário será encaminhado para uma página que receberá os avisos necessários para realização do teste. Podemos ver na figura 6.2. Além disso, será informado que o teste não cobre todos os tipos de cenários e não emitirá certificado. A conscientização é um processo diário, onde é preciso ficar sempre atento aos velhos e aos novos golpes que surgem na Internet.

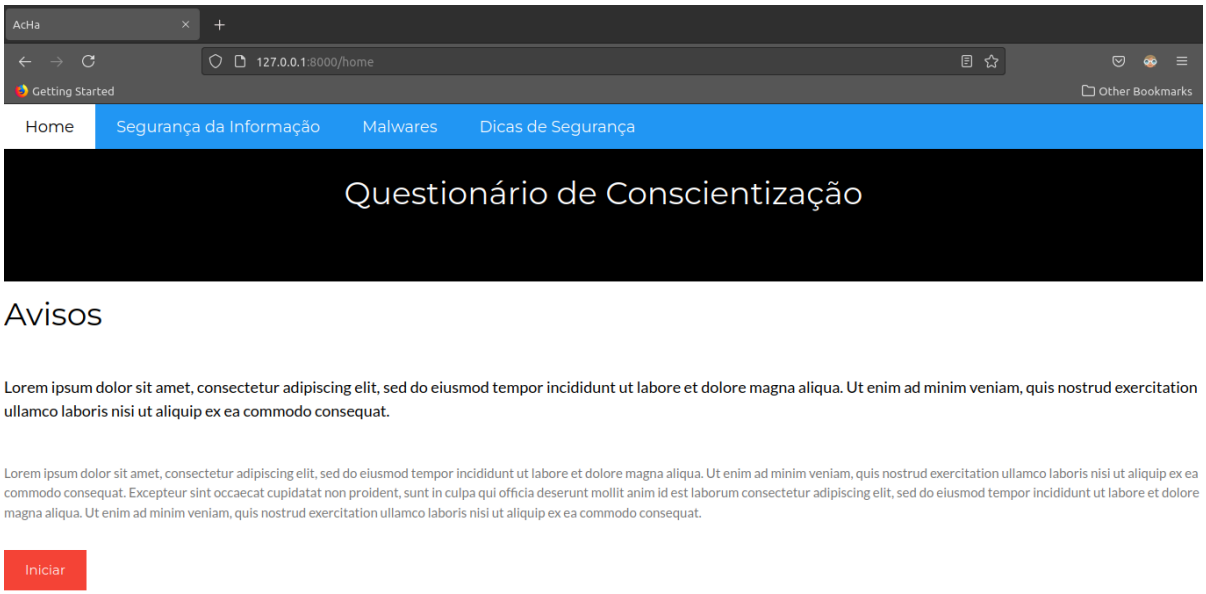

Figure 6.2: Tela de aviso

A ferramenta será composta com alguns cenários que o usuário irá testar seus conhecimentos. Desde ambientes para a criação de senhas fortes, conexão segura em redes sem fio e

cuidados com e-mails recebidos de contatos desconhecidos.

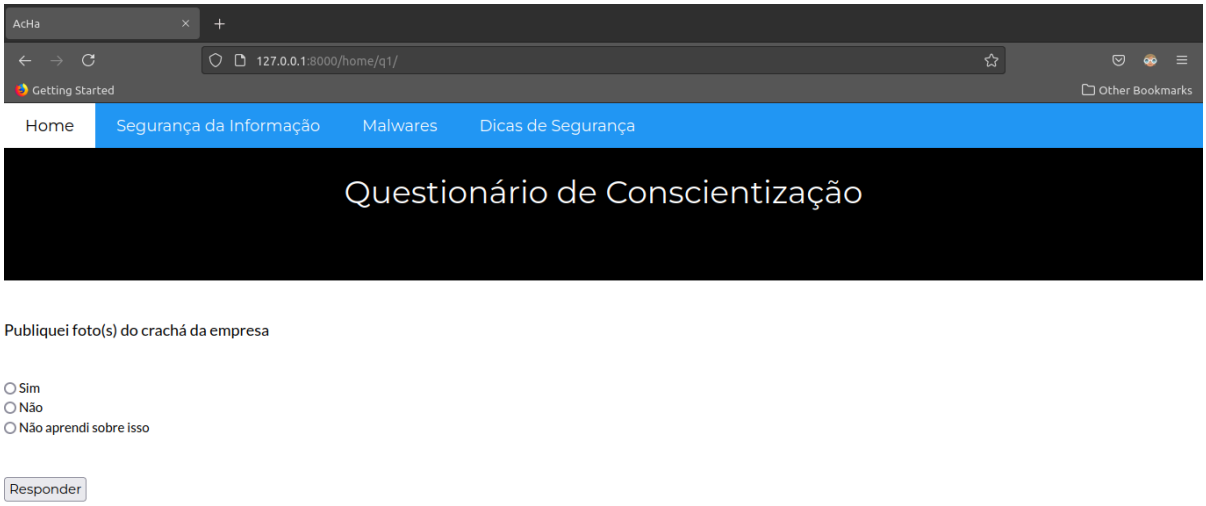

Figure 6.3: Tela inicial do questionário

Caso o usuário responda com sucesso, irá para o próximo cenário. Caso não obtenha êxito uma outra página será carregada informando as melhores práticas a serem feitas dentro daquela determinada citação.

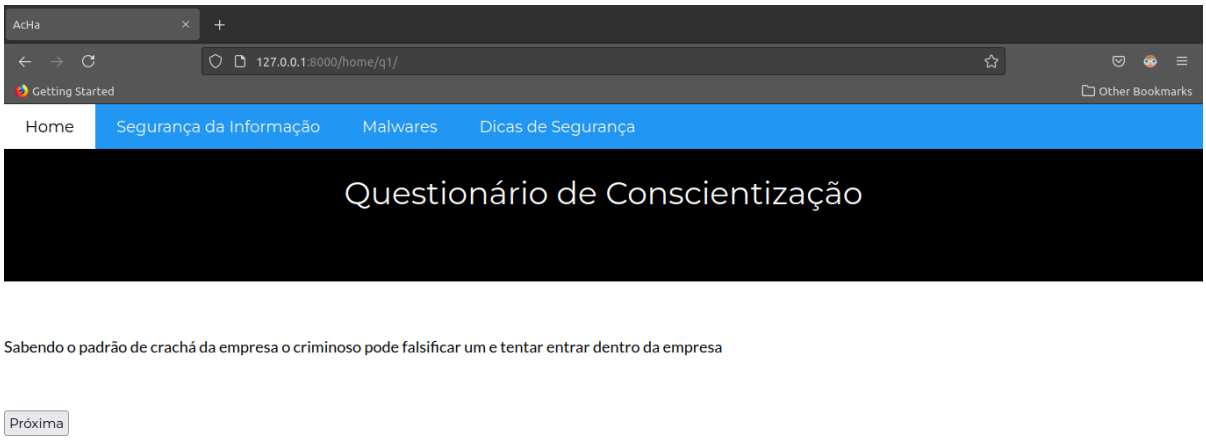

Figure 6.4: Tela de conscientização

6.3 Resultados

Podemos ver na imagem 6.5 o resultado final do usuário. Onde cada coluna representa um resumo da pontuação.

Resultado

Total questões	Pontuação	Respostas Corretas	Respostas Erradas	Porcentagem de Acertos
10	3	3	7	0.3

Figure 6.5: Resultado do usuário

7

Considerações Finais

7.1 Discussão

Com toda a tecnologia envolvida e já utilizada no dia-a-dia, sabemos que surgem novos ataques e ameaças todos os dias. Não existe ambiente 100% seguro, mas existem medidas que podemos fazer para nos prevenir. É importante ficar atentos e vigilantes em todos os momentos.

A plataforma deve ficar sempre disponível e o mais atualizada possível para atender as demandas dos usuários e do mercado.

7.2 Trabalhos Futuros

Para trabalhos futuros vamos adicionar gamificação na interface da plataforma para ficar mais amigável ao usuário. Assim o aprendizado será facilitado. Outra melhoria será a divisão dos cenários por nível do usuário, com isso podemos ter um progresso e a sensação crescimento dentro da plataforma.

Referências

Security brief: Mobile phishing increases more than 300continues. https://www.proofpoint.com/us/blog/threat-protection/mobile-phishing-increases-more-300-2020-chaos-continues. acessado em 16/01/2022.

Anotações do curso cybersecurity essentials português - brasileiro 0521 cga. https://lms.netacad.com/course/view.php?id=291924. acessado em 18/07/2021.

Natália Siqueira da Silva Alesandro Gonçalves Barreto. *É bom demais para ser verdade?* Observatório de Crimes Cibernéticos, 2022.

Victor Takashi Alexandre Moraes. *Segurança Em IoT: Entendendo os riscos e ameaças em IoT*. Alta Books, 2021.

Nick Feamster Andrew Tanenbaum and David Wetherall. *Redes de Computadores*. Pearson, 2021.

CERT.br. "cartilha de segurança para internet", 2012.

Vinicius da Silva Geraldo and Fábio Bento Takeda. Engenharia social: um perigo oculto em simples técnicas. *Revista Interface Tecnológica*, 16(1):242–253, 2019.

Bruno Fraga. *Técnicas de Invasão*. Novatec Labrador, 2019.

Sarah Granger. Social engineering fundamentals, part i: hacker tactics. *Security Focus, December*, 18, 2001.

Christopher Hadnagy. *Social engineering: The art of human hacking*. John Wiley & Sons, 2010.

Jule Hintzbergen, Kees Hintzbergen, André Smulders, and Hans Baars. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. Brasport, 2018.

ISACA. "infographic state of cybersecurity 2021", 2021.

Koteswara Ivaturi and Lech Janczewski. A taxonomy for social engineering attacks. In *International Conference on Information Resources Management*, pages 1–12. Centre for Information Technology, Organizations, and People, 2011.

Inka Karppinen and Ruya Ince. "the annual cybersecurity attitudes and behaviors report 2021", 2021.

KnowBe4. "top-clicked phishing email subjects", 2021.

Hennie A Kruger and Wayne D Kearney. A prototype for assessing information security awareness. *Computers & security*, 25(4):289–296, 2006.

Daniel Moreno. *Introdução ao Pentest*. Novatec Editora, 2019.

Gizem Öğütçü, Özlem Müge Testik, and Oumout Chouseinoglou. Analysis of personal information security behavior and awareness. *Computers & Security*, 56:83–93, 2016.

PhishLabs. "new phishlabs research reveals increase in phishing attacks", 2022.

Narjara Bárbara Xavier Silva, Wagner Junqueira de Araújo, and Patrícia Morais de Azevedo. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. *Revista Ibero-Americana de Ciência da Informação*, 6(2), 2013.

Aditya K Sood and Richard Enbody. Chapter 2 - intelligence gathering. In Aditya K Sood and Richard Enbody, editors, *Targeted Cyber Attacks*, pages 11–21. Syngress, Boston, 2014. ISBN 978-0-12-800604-7. **DOI** https://doi.org/10.1016/B978-0-12-800604-7.00002-4. URL https://www.sciencedirect.com/science/article/pii/B9780128006047000024.

Verizon. "2021 data breach investigations report", 2021.

Georgia Weidman. *Testes de Invasão: uma introdução prática ao hacking*. Novatec Editora, 2014.