Faculdade de Engenharia da Universidade do Porto

Computer Hacking

O que são "maus" *hackers* (*crackers*)?

Projeto FEUP 1ºano -- Mestrado Integrado de Engenharia Informática e Computação:

Manuel Firmino da Silva Torres

José Manuel de Magalhães Cruz

Equipa 1MIEIC04_03:

Supervisor: João Correia Lopes

Monitor: Carlos Albuquerque

Estudantes & Autores:

Afonso Abreu up202008552@fe.up.pt

Fábio Sá up202007658@fe.up.pt

Inês Gaspar up202007210@fe.up.pt

João Malva up202006605@fe.up.pt

Manuel Rodrigues up202007554@fe.up.pt

Pedro Ferreira up202004986@fe.up.pt

Novembro 2020

Porto, Portugal

Resumo

O presente relatório visa compreender a relação entre o crescimento das novas tecnologias e o surgimento de mais cibercriminosos. A par da constante evolução do mundo, há quem se aproveite das fragilidades computacionais para benefício próprio, para obter informações de terceiros e fama: os *Crackers*.

No âmbito da Unidade Curricular "Projeto FEUP" comprometemo-nos a explorar esta vertente da Informática e a relacioná-la com a cibersegurança inerente ao século presente. Esta última, pilar preponderante para todos os utilizadores da Internet, é importante e necessária a qualquer Engenheiro na área. Ao saber as motivações dos *crackers*, as suas competências e objetivos, podemos compreender melhor a constante procura pela proteção dos dados pessoais.

Palavras-Chave

Hacker; White Hat hacker; Gray Hat Hacker; Black Hat hacker; Cracker; Cibersegurança*; Computer Cracking;* Informação*;* Ciberataque; Cibercriminoso.

Agradecimentos

Queremos agradecer, em primeiro lugar, ao nosso supervisor João Correia Lopes e ao nosso monitor Carlos Albuquerque, que nos ajudaram a compreender melhor os objetivos do trabalho.

Em segundo lugar, gostaríamos de agradecer aos núcleos de estudantes NIAFEUP, NEEEC e IEEE UP SB, pela disponibilidade prestada para partilhar informação relevante ao tema: *Computer Cracking*.

Para além disso, queremos agradecer às pessoas que participaram ativamente no questionário realizado a fim de obter dados estatísticos importantes para a avaliação do conhecimento geral acerca desta área.

Por fim, agradecemos aos coordenadores da unidade curricular Projeto FEUP, Manuel Firmino da Silva Torres e José Manuel de Magalhães Cruz, por terem tornado esta oportunidade possível, a fim de promover a integração e o conhecer, quer dos colegas de curso, bem como de toda a comunidade FEUP.

Índice

Lista de figuras

Lista de acrónimos

FEUP – Faculdade de Engenharia da Universidade do Porto;

IEEE UP SB – *Institute of Electrical and Electronics Engineers University of Porto Student Branch*;

MIT – *Massachusetts Institute of Technology*;

NEEEC – Núcleo de Estudantes de Engenharia Eletrotécnica e de Computadores (FEUP);

NIAEFEUP – Núcleo de Informática da Associação de Estudantes da Faculdade de Engenharia da Universidade do Porto;

VPN – *Virtual Private Network* (Rede Privada Virtual).

Glossário

Criptografia – codificação de dados;

Data Breaches - violação de dados; ocorre quando uma empresa/organização é vítima de uma falha de segurança relativa aos dados pelos quais é responsável. Resulta numa violação da confidencialidade, da disponibilidade ou da integridade dos dados;

Engenharia Inversa - processo de obtenção de conhecimento de princípios tecnológicos e o funcionamento de um objeto, dispositivo ou sistema, através da análise da sua estrutura, função e operação;

Exploits - na área da Informática, um *exploit* é um pequeno *software*, conjunto de dados ou uma sequência de comandos que tira partido de uma falha ou vulnerabilidade de um sistema, com o objetivo de causar danos ou erros, quer a nível de *software* ou *hardware* de um computador ou dispositivo eletrónico;

***Hack*er** - indivíduo que possui grandes conhecimentos informáticos e utiliza-os para diversos fins, consoante os seus objetivos;

Hardware - os processadores, fios e outros componentes físicos de um computador.

Malware - *software* malicioso que tem como objetivo infiltrar-se em sistemas informáticos para causar danos e roubo de informações particulares;

Software - conjunto de programas, processos, regras e, eventualmente, documentação, relativos ao funcionamento de um conjunto de tratamento de informações.

1. Introdução

Vivemos num mundo onde a tecnologia está já incrementada e enraizada de uma forma tão abrangente nas nossas rotinas, no qual pessoas desenvolvem técnicas em máquinas de elevado grau tecnológico para atingir determinados fins. Desta forma, é necessária a nossa atenção para aqueles que têm como objetivo o benefício próprio sem ter em conta os prejuízos causados.

Com base nesta questão, no âmbito da Unidade Curricular Projeto FEUP, foi-nos solicitada a realização de um Relatório de Engenharia cujo tema principal é *Computer Cracking* e comprometemo-nos a explorar dois subtemas adjacentes a este: *Hacking* e Cibersegurança. Assim, o nosso objetivo é dar a conhecer os conceitos ligados a estes dois subtemas e consequente explicação, tentando desacreditar alguns preconceitos relacionados com os *hack*ers.

Outro meio utilizado para enriquecer o nosso Projeto foi avaliar o nível de conhecimento geral acerca deste assunto, promovendo um inquérito a pessoas de diferentes faixas etárias (ao qual obtivemos 436 respostas). Estes dados permitiram-nos concluir a falta de conhecimento relativamente a esta área da informática. De facto, como resposta à primeira pergunta do inquérito (Figura 1) cerca de 88% dos inquiridos referiu saber o significado da palavra *hacking*. Contudo, numa pergunta seguinte (Figura 2) a maioria dos inquiridos (aproximadamente 75% da nossa amostra) associou-a a um conceito negativo.

Deste modo, vamos focar o nosso trabalho nos "maus" *hackers* e nas medidas de cibersegurança que minimizam os ataques informáticos.

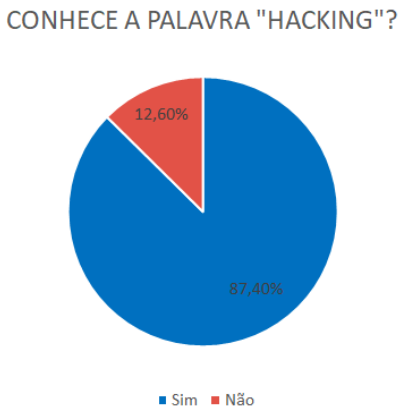

Figura 1 – Gráfico resultante das respostas à pergunta "Conhece a palavra *Hacking*?", realizado através do Google Forms. (436 respostas)

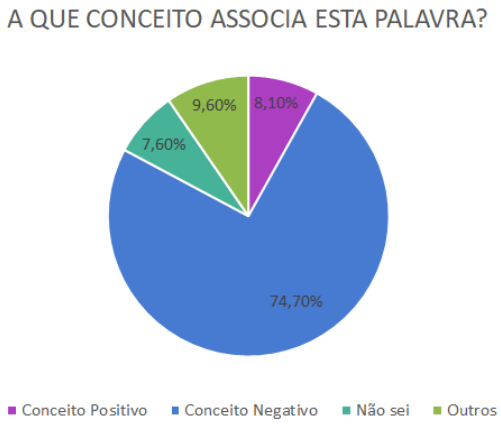

Figura 2 - Gráfico resultante das respostas à pergunta "A que conceito associa esta palavra?", realizado através do Google Forms. (396 respostas)

2. *Hacking*

O termo *hacker* não teve sempre o significado que hoje lhe atribuímos. Segundo Steven Levy[1], só em meados da década de 50 é que o termo começou a ser aplicado na área informática, através de um grupo de estudantes do MIT (conhecido como *Tech Model Railroad Club*) para se referirem a "partidas" na instituição. Nos tempos livres, os elementos do grupo dedicavam-se a desenvolver e construir miniaturas de comboios, que programavam para percorrerem maquetes de cidades. A partir dessa altura, o termo *hack* passou a ser utilizado para descrever uma solução inovadora e criativa para um determinado problema ou projeto que exigia muita dedicação e concentração, sendo o principal objetivo dos envolvidos a satisfação pessoal.

O conceito de *hacker* tal como o caracterizamos nos dias de hoje, surgiu apenas no início dos anos 80 e apresentava duas definições: por um lado, era usado para designar indivíduos que possuíam um grande conhecimento na área informática e sobressaíam (através das suas capacidades); por outro lado, também era usado para definir indivíduos igualmente capazes na área da programação que utilizavam os seus conhecimentos para atacar e violar a segurança de sistemas informáticos. Atualmente, a definição mais popular e que prevalece é a segunda.

[1] Steven Levy – jornalista americano escritor de livros sobre computadores, tecnologia, Internet, cibersegurança e privacidade.

2.1 Tipos de *Hackers* e seus motivos

Como foi supracitado, a palavra *hacker* adquiriu vários significados ao longo do tempo. Atualmente, o termo possui duas interpretações - por um lado pode servir de nome a alguém que é especialista na área de informática e computação, como também é usada para denominar um indivíduo que utiliza o seu conhecimento para atacar e criar esquemas fraudulentos com vista a prejudicar outros indivíduos, empresas ou organizações para auto benefício.

Devido à falta de consenso e à divergência no conceito, no final dos anos 90, a comunidade informática dividiu-se em: *White Hat Hacker* e *Black Hat Hacker*, também denominados "bons" e "maus" *hackers*, respetivamente. A principal diferença entre estes dois tipos de *hackers* é a questão ética.

Estas designações funcionam como uma espécie de analogia aos filmes antigos do *Wild West*, onde os chapéus permitiam distinguir os "heróis", chapéu branco, dos "vilões", chapéu preto. (Diogo de Carvalho Mendes, 2014)

À medida que o conhecimento se tornou acessível a um maior número de pessoas, começaram a surgir novos tipos de *hackers*, destacando-se os *Script kiddies* e *Gray Hat Hackers*.

2.1.1 *Script kiddies*

Geralmente, usa-se a expressão *Script kiddies* para nomear adolescentes que possuem alguns conhecimentos na computação e que o usam para vandalizar e explorar alguns ataques cibernéticos, motivados principalmente pela curiosidade e pela adrenalina. Aliás, segundo Daniel Silva, elemento do IEEE UP SB, os *Script kiddies* podem ser caraterizados como "jovens adolescentes que pegam em ferramentas pré-feitas e tentam usá-las para benefício próprio" (Daniel Silva 2020). Os ataques deste tipo de *hackers* geram pouco impacto, apesar de, com o passar do tempo, ganharem experiência e, consequentemente, obterem novos conhecimentos nesta área, tais como, por exemplo, novas ferramentas de *hacking*.

2.1.2 *White Hat Hackers*

Os *White Hat Hackers* são indivíduos que se tornam especialistas na área da computação e, como tal, detêm o conhecimento necessário para aceder a redes informáticas. Todavia, usam-no para proteger, melhorar e fortalecer a defesa e eficácia dos sistemas de segurança. Assim, procuram as vulnerabilidades dos sistemas e corrigem-nas, reportando-as às entidades detentoras dos mesmos. É, por isso, frequente a maioria trabalhar para grandes empresas, que disponibilizam orçamentos na sua formação ou incentivam-nos a adquirirem novas técnicas de *hacking.*

2.1.3 *Black Hat Hackers*

Por sua vez, os *Black Hat Hackers* utilizam os seus conhecimentos para invadir dispositivos digitais e redes para fins maliciosos e ilícitos. Assim, conduzem ataques não autorizados contra sistemas de informação, violando-os e manipulando-os. São considerados cibercriminosos, sendo também conhecidos como *crackers*. São, geralmente, indivíduos que fazem uma pesquisa minuciosa e intensiva dos seus alvos antes de realizarem os ciberataques. Muitos dos ataques que empreendem baseiam-se nos seguintes: *phishing*, *malware*, compromisso de contas, DDoS, *botnets*, *data breaches,* entre outros.

Desta forma, podem dividir-se os *crackers* em dois tipos: os *crackers* de *software*, que são programadores que desenvolvem vírus e aplicações maliciosas, e os *crackers* criptográficos que se dedicam à quebra da criptografia. Os métodos mais utilizados são: força bruta, engenharia social, *exploits*, engenharia inversa, entre outros.

2.1.4 *Gray Hat Hackers*

Os *Gray Hat Hackers* partilham características dos dois grupos anteriores. Por um lado, ajudam a melhorar os sistemas de segurança, reportando erros que encontram às empresas ou organizações, tal como os *White Hat Hackers*. Contudo, invadem esses sistemas semautorização e, por isso, de forma ilegal, à semelhança dos *Black Hat Hackers*.

2.1.5 Motivações dos *Hackers*

As motivações dos *hackers* podem variar com o tempo e com o tipo de *hack*er. Geralmente, muitas pessoas que têm algum interesse na área da informática conhecem algumas ferramentas de *hacking* através da Internet ou por amigos e podem começar a criar ataques informáticos (tornando-se *Script kiddies*), movidas apenas pela curiosidade. Outros *hackers* atacam empresas e os seus sistemas a fim de passarem alguma mensagem, seja de cariz político ou ambiental, por exemplo. Este movimento designa-se por *Hacktivismo*.

Para além destas causas, alguns ataques informáticos são motivados pela guerra de informação, em que governos contratam *hackers* para que estes possam obter ou defraudar informações confidenciais de outros governos, de modo a favorecer os primeiros.

A indústria da espionagem também é responsável por vários ataques cibernéticos - alguns *hackers* e *crackers* utilizam os seus conhecimentos para se infiltrarem em sistemas de segurança e base de dados, com o objetivo de extorquir dados relevantes e/ou danificarem esses sistemas.

Para além disso, as motivações que são transversais a todos os *crackers* é a intenção de vandalizar e denegrir a imagem de instituições ou de pessoas, bem como a obtenção de fama e informações consideradas relevantes.

2.1.6 Competências necessárias de um *Hacker*

Nos últimos anos, o mundo tem assistido a um aumento das novas tecnologias, das suas capacidades e utilidades nos vários ramos da ciência. É expectável, portanto, que os *crackers* usem todas estas aliciantes ferramentas para benefício próprio. A Internet, armazém das mais poderosas informações capazes de alimentar qualquer mente mais curiosa, surge como um apoio contínuo e em parte gratuito para os autodidatas da área.

Motivados pela ganância do lucro, outrora pela notoriedade que tal ato despoletava nos primórdios dos sistemas informáticos, os *crackers* convertem o saber em ganhos pessoais e fraudulentos. O facto de terem acesso a informações confidenciais, típica ação proveitosa de

quem promove o constante roubo de identidade, está muitas vezes relacionado com a elevada qualificação, inteligência e estudo. Não é de todo comum, fácil ou simples conseguir encontrar lacunas, falhas e pontos fracos dos programas de *software* atuais. Bastante curioso, este tipo de cibercriminoso tem de ser hábil e demonstrar interesse na resolução de desafios aparentemente sem solução.

Para além dessas competências racionais, há outras de cariz mais técnico, articuladas com a constante obtenção de conhecimento. Os *crackers* devem ser poliglotas, dominando não só o inglês, como também algumas das restantes línguas faladas no mundo.

Devem também dominar as diversas linguagens de programação. Só com a confluência da interação homem-máquina, da capacidade da transposição da linguagem de alto nível para a linguagem de baixo nível passível de ser interpretada pelo computador, é que conseguem uma benigna adaptação a todo o tipo de situações. As mais recorrentes, aquelas que o *cracker* deve saber manipular e usar sem contratempos, são as linguagens C, C++, *Python*, *Perl* e *LISP*.

É de realçar a influência do sistema operativo escolhido na altura da execução e aprendizagem na área. Embora o *hacker* tenha de ter um conhecimento alargado, de forma a abranger o maior número de programas de *software* possíveis, o sistema operativo Unix, ao contrário dos concorrentes Windows e macOS, é o mais utilizado neste tipo de situações: é gratuito, permite uma rápida personalização e é de código aberto. Assim é de prever que haja uma maior preferência por razões de velocidade, eficiência e segurança. Devido aos parâmetros assinalados, o *cracker* fica limitado somente pela sua própria capacidade e não pelo *software* utilizado aquando da intervenção antiética.

3. Cibersegurança

3.1 Definição

Cibersegurança refere-se a todo o conjunto de tecnologias, processos e práticas que têm como função proteger de ataques cibernéticos qualquer sistema informático, sejam eles *hardware*, *software* ou bases de dados. Tal como foi referido por Daniel Silva, membro da organização do IEEE UP SB, a cibersegurança consiste na "segurança/defesa de qualquer tipo sistema de informação, virtual ou não" (Daniel Silva 2020).

Estes ataques têm geralmente como objetivo aceder, alterar, ou destruir informações sensíveis de indivíduos ou empresas, quer seja para os próprios fins do *cracker*, para extorquir dinheiro ou simplesmente para perturbar a vítima.

Noutra perspetiva, Mário Mesquita e João Martins, membros do NIAFEUP, consideram que a cibersegurança consiste nas ferramentas e práticas que são utilizadas com o intuito de tornar os serviços informáticos (sites, programas, ...) seguros, combatendo o roubo de informações, bem como a proteção dos dados dos seus utilizadores (Mário Mesquita e João Martins 2020).

Normalmente, uma empresa de *software* tem uma equipa dedicada a este aspeto.

3.2. Importância

Atualmente, sabe-se que várias empresas e organizações despendem grandes quantidades de dinheiro, com vista a proteger os milhões de dados que circulam, quer na Internet, quer nos seus sistemas informáticos. De facto, a organização International Data Corporation fez um estudo onde previu que, mundialmente, se invistam 133 mil milhões de dólares até 2022 em soluções para fortalecer a cibersegurança.

Esta situação deve-se ao facto de várias organizações recolherem, processarem e armazenarem grande quantidade de dados. Muitos dos dados fornecidos são confidenciais e podem ser de vários tipos, podem ser propriedade intelectual, dados financeiros, informações pessoais ou dados cujo acesso não autorizado resulta em consequências negativas. A nível individual, um destes ataques pode gerar consequências prejudiciais para a vítima, quer seja roubo de identidade ou mesmo chantagem. Por sua vez, a RiskBased Security divulgou um relatório no qual revelou que cerca de 7,9 mil milhões de ficheiros foram expostos/comprometidos por *data breaches*, apenas nos primeiros noves meses de 2019. Assim, é fundamental que a sociedade esteja sensibilizada para estes perigos bem como para a melhor forma de preveni-los ou, pelos menos, minimizar os seus impactos.

3.3 Desafios da cibersegurança

A constante evolução da tecnologia aumenta os riscos relativamente à segurança informática, sendo por isso considerada o principal desafio da cibersegurança. À medida que surgem novas tecnologias, são simultaneamente descobertos novos meios de ataque. Por esta razão, torna-se cada vez mais difícil para as empresas e organizações acompanharem esta evolução. É essencial que todos os componentes da cibersegurança sejam regularmente atualizados com vista a melhorar a sua defesa contra esses eventuais ciberataques. Esta situação, está associada a outro problema: a falta de profissionais nesta área.

Porém, estes são cada vez mais necessários para analisar, gerir e resolver este tipo de incidentes. Desta forma, é muito frequente as organizações contratarem empresas de cibersegurança para as proteger ou fortalecer os seus sistemas. Contudo, esta opção não é acessível a todos, uma vez que representa um custo muito elevado, particularmente para empresas pequenas.

Outro desafio que já foi referido anteriormente é a quantidade de dados que uma organização pode armazenar. Isto constitui também um risco, na medida em que, quanto mais informações são recolhidas, maior é a probabilidade de um *cracker* realizar um ataque a esse sistema.

Assim, implementar novas medidas de cibersegurança apresenta-se como uma tarefa particularmente desafiante.

3.4 Medidas de proteção

Os ataques informáticos só podem ser defendidos se houver um completo esforço das organizações, pessoas ou tecnologias associadas. Algumas das principais medidas de proteção usadas em grandes empresas são:

- usar aplicações seguras, que guardam informações confidenciais e pessoais do utilizador. Normalmente esta segurança, que protege a integridade e privacidade dos dados armazenados, deve ser implementada antes do *design* da aplicação;
- a segurança operacional, que consiste no manuseamento dos dados. Deve ser eficaz ao ponto de determinar, com precisão, o local onde serão guardados todos os dados;
- as políticas de recuperação de dados após incidentes promovem métodos de proteção às empresas que tenham sido vítimas de perda ou exposição de informações pessoais;
- a educação dos utilizadores permite minimizar as falhas de segurança de mão antrópica. Qualquer indivíduo dentro de uma empresa ou instituição pode acidentalmente promover uma perda de proteção dos dados armazenados.

De acordo com os resultados do nosso inquérito, pudemos averiguar que os inquiridos estão bastante familiarizados com os métodos de proteção de dados. De facto, a panóplia de meios diferentes inferidos transparece que a amostra contacta, no seu quotidiano, com os seguintes tópicos de cibersegurança (Figura 3):

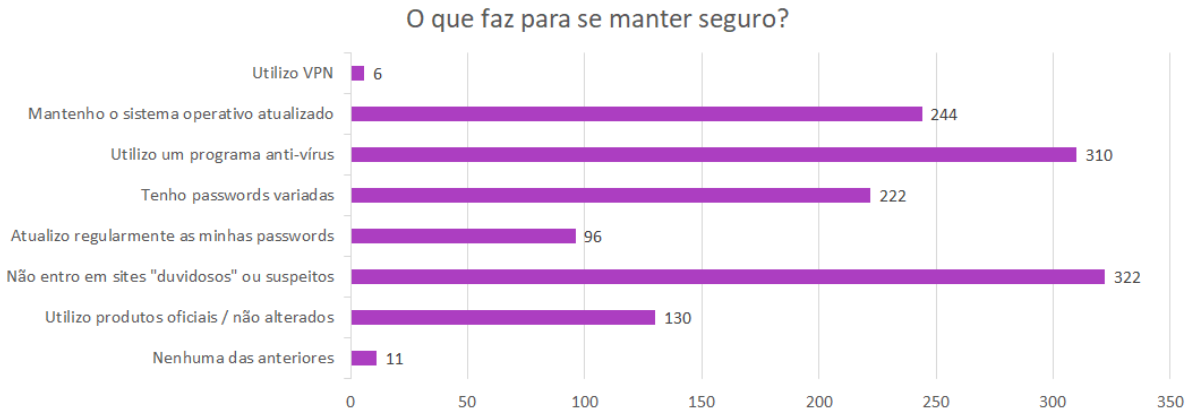

Figura 3 – Gráfico resultante das respostas à pergunta "O que faz para se manter seguro?", realizado através do Google Forms. (436 respostas)

4. Ataques mais comuns e prevenção

Existe uma extensa lista de diferentes ataques informáticos, cada um de natureza diferente e de diferentes níveis de danos associados à sua utilização.

Comecemos então por enumerar alguns exemplos desses ataques informáticos, associando-os de seguida, a diversas medidas para preveni-los.

4.1. *Botnet*

Tal como o nome indica, o termo significa “rede de robôs” que funcionam como um vírus. Este conjunto de *malware* é controlado por um agente externo, sendo geralmente o autor desse vírus. Os *botnets*, depois de incrementados no computador da vítima (através da execução de um *software*, por exemplo), podem realizar várias tarefas, mesmo sem que esta, utilizando o computador infetado, tenha perceção.

Utilizando *botnets* o atacante pode enviar *Spam*, realizar *Click Fraud* (cliques espontâneos em certas publicidades) e ainda roubar informações ou a identidade da vítima.

4.2. Ataques DDoS

DDoS é a sigla que indica em inglês as palavras *Distributed Denial of Service* (Negação de Serviço Distribuído). Este tipo de ataque informático carateriza-se na impossibilidade de um certo utilizador navegar na Web, fazendo com que o serviço do qual se pretendia fazer uso fique indisponível.

Os ataques DDoS são realizados enviando um grande conjunto de dados ao computador da vítima, sobrecarregando as capacidades da máquina de realizar todas as tarefas para as quais foi programada. Estes dados terão que ser suficientes para atingir o seu fim, ou seja, a indisponibilidade do serviço. Existe uma escala que avalia a severidade destes ataques, dependendo do dano que estes proporcionam no *hardware* atingido. O primeiro é chamado *self-recoverable* (pessoalmente recuperável): após o ataque o sistema é capaz de operar sem ter sofrido quaisquer danos colaterais. O segundo é chamado *human-recoverable:* significa a necessidade da ação humana no sistema para o normal funcionamento do mesmo (por exemplo: *reboot* do sistema). Finalmente, o ataque que gera mais danos é chamado *non-recoverable* (Não recuperável): o ataque teve uma severidade elevada que causa danos irreparáveis no hardware afetado.

Os ataques DDoS também podem ser provocados através da utilização de *botnets*.

4.3. Força Bruta

Assim denominado, porque este ataque é fortemente suportado na "força bruta" com que é realizado. Mais explicitamente, o *hacker* que utiliza este método usa um *software* que gera várias combinações para conseguir uma certa palavra-passe de um utilizador num determinado serviço. Para o conseguir, será necessário um número variável (dependendo do nível de segurança da palavra-passe escolhida) de tentativas até atingir o seu fim. É um ataque bastante popular na atualidade, devido ao facto de as palavras-passe utilizadas serem normalmente de caráter fraco, isto por não sermos capazes de memorizar uma grande quantidade de números com grandes dimensões e também pela continuidade de sites com meios de segurança mais datados, o que proporciona, por exemplo um número de tentativas de palavras-passe ilimitadas.

4.4. Engenharia Social

Ao contrário dos ataques abordados anteriormente, a engenharia social não depende muito das competências técnicas que o *cracker* possui, centra-se principalmente nas emoções humanas e na manipulação das mesmas.

Este tipo de ataque distingue-se, assim, pelo facto de poder ter uma abordagem mais física, no qual, por exemplo, a pessoa se desloca a um determinado local com o objetivo de obter informações. Muitas vezes, é mais fácil aceder a um servidor fisicamente do que remotamente. Por esta razão, pode ser mais simples estudar o ambiente de trabalho de uma empresa ou corporação, vagueando e observando tudo aquilo que poderá ser útil para facilitar a sua concretização. Porém, nem todos os ataques de Engenharia Social se realizam desta forma, tudo o que implique o contacto (mesmo virtual) com outra pessoa está também incluído nesta classificação. Defender-se desta espécie de ataques tem, por conseguinte, uma grande dificuldade, devido ao facto de não depender de um *software* especializado em ataques informáticos, mas sim do comportamento das pessoas, que é maioritariamente imprevisível.

4.4.1 *Phishing*

Este ataque informático é um exemplo de Engenharia Social, caracteriza-se na tentativa de ganhar certos tipos de informações, normalmente pelo envio de e-mails, enquanto o autor se faz passar por uma identidade suficientemente credível, ludibriando por fim a vítima.

Este ataque é bastante comum na atualidade. Isto deve-se ao facto do *phishing* não precisar de nenhuma capacidade extraordinária no campo do *hacking*, apenas de uma alta fonte de credibilidade no seu processo. Uma frase que descreve de uma forma bastante

acertada este ataque é a seguinte: “It doesn’t matter how many firewalls, encryption software, certificates, or two-factor authentication mechanisms an organization has if the person behind the keyboard falls for a phish.” (Jason Hong, 2012) (traduzindo para português: “Não importa quantas *firewalls, software* de encriptação ou mecanismos de autenticação de dois fatores uma organização tem se a pessoa atrás do teclado é enganada por um *phish*).

4.5. Meios de segurança

Enumerar sistemas de segurança para cada exemplo de *hacking* não seria totalmente sensato uma vez que existem no momento diversos programas de *software* muito específicos para cada tipo de ataque. Para além disso, estes são elaborados tendo como base vários conceitos matemáticos e dessa forma, caracterizá-los iria contornar ligeiramente o tema deste trabalho.

Isso não invalida, no entanto, o facto dos ataques informáticos poderem ser prevenidos e como tal podemos enunciar várias medidas que deveriam ser tomadas pelos utilizadores ou até mesmo empresas de modo a tornarem os ataques cibernéticos menos frequentes.

- Não se deve utilizar as mesmas palavras-passe para diferentes serviços: se um *cracker* conseguir acesso a apenas uma conta de um certo serviço, as outras estarão consequentemente comprometidas. Para tal, são frequentemente utilizados gestores de palavras-passes.

- É de evitar as palavras-passe com poucos carateres e de sequências simples. Apesar de ser um conselho vulgar para as novas gerações, este tipo de situação ainda é muito recorrente.

- São necessárias atualizações das interfaces em vários serviços da Internet. Deste modo, a identificação de emails fraudulentos seria mais facilitada e intuitiva, o que faria com que situações de *phishing*, por exemplo, diminuíssem.

- Colocar algum tipo de informação no início de emails que comprova a sua veracidade é também uma técnica usada por empresas para combater o *phishing*.

- Nunca clicar em sites ou notificações que tenham um caráter duvidoso. Obviamente este vai ser um objeto de julgamento subjetivo, mas é de assumir que não vencemos coisa alguma de valor pela Internet.

4.6 Meios de segurança associados aos sistemas da FEUP

Para que cada pessoa possa prevenir-se individualmente tomando as medidas apresentadas em cima, o SIGARRA disponibiliza alguns mecanismos de defesa para que os estudantes da FEUP se sintam seguros, quando navegam neste site e nos outros sistemas ligados à faculdade (serviços, sites dos núcleos, entre outros).

4.6.1 Alteração da palavra-passe (password)

O SIGARRA possui um sistema de alteração de palavras-passe ao qual estabelece uma nova palavra-passe, que cumpra vários requisitos, tais como: possuir entre 8 e 32 carateres, não pode ser igual às últimas 5 palavras-passe anteriores, não pode conter carateres especiais (#, $, % &, /, &, etc.) e tem de conter números e letras. Consoante a qualidade da nova palavra-passe, o sistema retribui uma mensagem ao utilizar, indicando a força da palavra-passe, esta mensagem varia entre “Muito Fraca” a “Muito Boa”.

4.6.2 Recuperação de palavra-passe por SMS

Em caso de perda ou esquecimento da palavra-passe associada aos sistemas informáticos: Sigarra, Windows, Linux, correio eletrónico, rede sem fios, VPN e Tcpgate, é possível alterar a palavra-passe utilizando um telemóvel pessoal ativo, registado e associado ao serviço, através de SMS. A nova palavra-passe deverá obedecer às regras já referidas e será atualizada em todos os sistemas já referidos.

4.6.3 Anti-Spam

Nos serviços da FEUP está disponível para todos os utilizadores uma configuração de proteção anti-spam localizados no SIGARRA da mesma faculdade. Estes filtros de emails têm em conta normas definidas internacionalmente.

No configurador, o utilizador tem 3 opções das quais pode escolher:

- Na 1ª, as mensagens avaliadas como spam são enviadas para o separador “spam”, e serão eliminadas 15 dias depois;
- Na 2ª, os emails com caraterísticas de spam serão automaticamente eliminados à chegada;
- Na 3ª, o spam apenas será marcado no cabeçalho com a mensagem “X-Spam-Status: Yes”.

No entanto, em todas as opções anteriormente referidas, as mensagens avaliadas como spam serão marcadas com a mensagem “X-Spam-Status: Yes”, caso contrário serão marcadas com a mensagem “X-Spam-Status: No”.

Também todos os emails spam não poderão ser reencaminhados, para garantir maior segurança.

4.6.4 Antivírus/Antispyware

Este serviço apenas está disponível para computadores com os respetivos sistemas operativos: Microsoft Windows 2000, XP, 2003, Vista, 2008 e Windows 7 versão 32 e 64 bits. Para tirar proveito do antivírus é necessária a autenticação de um utilizador administrador e instalar o programa.

4.6.5 Auditor de segurança informática

Este serviço diagnostica, de forma sintética ou completa, o nível de segurança de uma determinada página Web. No final da auditoria, é enviado um relatório para o email do utilizador, indicando as principais falhas e alertas de segurança detetados, ao longo da avaliação.

4.6.6 Autenticação de utilizadores

A forma como os utilizadores são autenticados nos diversos serviços que a FEUP disponibiliza promove uma melhor garantia de privacidade. Para isso, o acesso requer credenciais fidedignas e disponibilizadas pela faculdade, que são pessoais e intransmissíveis.

4.6.7 CSIRT.FEUP

Este é o serviço disponível online que permite identificar e tratar os alertas de segurança de todos os utilizadores da rede em vigor na FEUP. O utilizador, ao reportar o ocorrido para https://csirt.fe.up.pt/, com as suas próprias credenciais de acesso, pode indagar acerca dos incidentes de segurança ocorridos e submetidos por este método.

4.6.8 Guia de segurança

A Faculdade disponibiliza um Guia de Segurança (do CICA) que permite aos utilizadores terem conhecimento de um conjunto de práticas importantes para manter a integridade dos sistemas informáticos.

4.6.9 Incidentes de Segurança Informática

Este serviço permite aos utilizadores realizarem pedidos de análise a incidentes de segurança informática. Os utilizadores devem descrever o incidente para o endereço eletrónico: incidente.seguranca@fe.up.pt, indicando as máquinas afetadas, o sistema operativo, o tipo de ataque e as áreas comprometidas.

4.6.10 Repositório de Chaves Públicas PGP

O Repositório de Chaves Públicas da FEUP permite guardar, nos seguros servidores da faculdade disponíveis em keysrv.fe.up.pt, as chaves que podem ser usadas para encriptar mensagens, emails e documentos enviados pelos serviços Web. Para isso, o utilizador que queira tirar partido deste serviço gratuito deve primeiramente ter um email pessoal e uma aplicação PGP, que gere a palavra-passe e a chave de segurança.

4.6.11 Teste de robustez de palavra-passe

A FEUP fornece acesso a um serviço que permite que o utilizador averigue a qualidade/robustez e o nível de segurança da sua palavra-passe. Assim, depois de se inserir a palavra-passe no programa, ele analisa-a e classifica-a segundo a escala seguinte: “Muito Fraca”; “Fraca”; “Aceitável”; “Boa”; “Muito Boa”. Se o nível desta for muito reduzido (caso seja uma palavra-passe muito vulgar ou contenha poucos carateres), o programa transmite avisos para melhorar a sua qualidade.

4.6.12 VPN

A VPN disponível no SIGARRA permite aos estudantes acederem a conteúdos que se encontram apenas na rede da FEUPnet remotamente e de forma segura, a partir de casa. Assim, o estudante apenas precisa de configurar a VPN, utilizando a sua conta TCPGate.

5. Conclusões

Com este Projeto, pudemos aprofundar e adquirir novos conhecimentos acerca do tema *Computer Cracking* bem como analisar as várias medidas que visam reduzir os impactos dos ciberataques.

Este trabalho permitiu-nos também averiguar as principais diferenças entre *hackers (White Hat Hackers)* e *crackers (Black Hat Hackers)*. São ambos indivíduos com grandes competências a nível de programação, mas enquanto que os primeiros se dedicam a melhorar e fortalecer a segurança dos sistemas informáticos, os segundos aproveitam-se das suas vulnerabilidades e tiram proveito próprio. Desta forma, verificamos que as principais distinções entre estes dois tipos de *hackers*, são a questão da permissão e a questão ética. De seguida, exploramos os ataques mais recorrentes e entre os quais destacamos: *botnet*, ataques DDoS, força bruta e *phishing*. Os efeitos destes ataques podem ser minimizados através da adoção de medidas de cibersegurança, como por exemplo: alteração frequente de passwords, não aceder a sites duvidosos, estar atento a e mails suspeitos, entre outros.

Referências bibliográficas

Raymond, Eric Steven. 2001. "How To Become A Hacker", Atualizado em 3 de janeiro de 2020, acedido em 18 de outubro de 2020. http://www.catb.org/esr/faqs/hacker-howto.html

Mendes, Diogo de Carvalho. 2014. “Técnicas de hacking para anonimização na Internet”. https://repositorio.ucp.pt/handle/10400.14/15325

Pinto, José Carlos Oliveira. 2009. “Sistema de detecção de intrusão em rede informática” https://recipp.ipp.pt/bitstream/10400.22/1978/1/DM_JosePinto_2009_MEEC.pdf

Skillville. 2019. "Hackers Vs Crackers", Acedido em 18 de outubro de 2020. https://skillville.in/blog/hackers-vs-crackers

Mote, Christopher. 2010. "Hackers, Crackers, Script-Kiddies, Cyber-Spies: Can you spot the bad guy?", Acedido em 18 de outubro de 2020. http://anthillonline.com/hackers-crackers-script-kiddies-cyber-spies-can-you-spot-the-bad-guy/

Erickson, Jon. 2008. "Hacking: The art of exploitation", acedido em 19 de outubro de 2020.

Leeson, T. Peter e Coyne, Christopher. 2005. "The Economics of computer hacking”, acedido em 24 de outubro de 2020.

Mitnick, Kevin, Simon, L. William. 2011. "Ghost in the Wires", acedido em 19 de outubro de 2020.

Centro Nacional de Cibersegurança Portugal, Junho 2020, acedido em 20 de outubro de 2020. https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2020__observatoriocibersegurança_cncs.pdf

TechTarget. 2020. “What is cybersecurity? Everything you need to know”, atualizado em abril de 2020, acedido em 18 de outubro de 2020. https://searchsecurity.techtarget.com/definition/cybersecurity

Kaspersky. 2020. “What is Cyber Security?”, acedido em 19 de outubro de 2020. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Cisco. 2020. “What is Cybersecurity?”, acedido em 19 de outubro de 2020. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

P.Dinesh. 2016. "Ethical Hacking and Cyber Security", acedido em 22 de outubro de 2020. https://www.academia.edu/26362650/Ethical_Hacking_and_Cyber_Security

Barber, Richard. 2001. "Hackers Profiled — Who Are They and What Are Their Motivations?", Atualizado em 7 de Fevereiro de 2020, acedido em 22 de outubro de 2020. https://www.sciencedirect.com/science/article/pii/S1361372301020176?via%3Dihub

Yermalovich, Pavel. 2020. "Ontology-Based Model for Security Assessment: Predicting Cyberattacks Through Threat Activity Analysis". Acedido em 23 de outubro de 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=36237466

Mirkovic, Jelena; Reiher, Peter. 2004. "A taxonomy of DDoS attack and DDoS defense mechanisms", acedido em 21 de outubro de 2020. https://dl.acm.org/doi/10.1145/997150.997156

Kaur, Navpreet. Dr. Jaswinder Singh. "Ethical Hacking in windows Environment", Acedido em 21 de outubro de 2020. https://zenodo.org/record/46485#.X57pmIj7REY

Liu, Jing; Xiao, Yang; Ghaboosi, Kaveh; Deng, Hongmei e Zhang, Jingyuan. 2009. "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures", Acedido em 21 de outubro de 2020. https://link.springer.com/article/10.1155/2009/6926544

Maryam M. Najafabadi, Taghi M. Khoshgoftaar, Clifford Kemp, Naeem Seliya e Richard Zuech. 2014. "Machine Learning for Detecting Brute Force Attacks at the Network Level ", Acedido em 23 de outubro de 2020. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7033609&tag=1

Hong, Jason. 2012. "The State of Phishing Attacks", acedido em 21 de outubro de 2020. https://dl.acm.org/doi/pdf/10.1145/2063176.2063197

CICA. 2020. "Serviços CICA - Segurança", acedido em 28 de outubro de 2020. https://sigarra.up.pt/feup/pt/web_base.gera_pagina?P_pagina=21237

Gregory L. Orgill; Gordon W. Romney; Michael G. Bailey e Paul M. Orgill. 2014. "The Urgency for Effective User Privacy education to Counter Social Engineering Attacks on Secure Computer Systems", acedido em 21 de outubro de 2020.

Apêndice A: Formulário do inquérito

Computer Cracking

No âmbito da Unidade Curricular (UC) "Projeto FEUP", pretendemos com este simples questionário avaliar a exposição ao tema: Computer Cracking. A sua resposta irá contribuir para uma estatística que irá constar no nosso relatório. Salientamos que as respostas são anónimas e apenas para fim de pesquisa.

Tempo estimado de questionário: 1 minuto.
Muito obrigado pela atenção e colaboração.
*Obrigatório

1. Idade (faixa etária): *

   Marcar apenas uma oval.

   - ◯ <18
   - ◯ 18 - 24
   - ◯ 25 - 40
   - ◯ >40

2. Conhece a palavra "hacking"? *

   Marcar apenas uma oval.

   - ◯ Sim
   - ◯ Não

3. Se respondeu sim, a que conceito(s) associa a essa palavra?

   Marcar apenas uma oval.

   - ◯ Conceito positivo
   - ◯ Conceito negativo
   - ◯ Não sei
   - ◯ Outra: _____

4. Considera que os seus dados se encontram seguros, quando utiliza a Internet? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Talvez

5. Sabe o que é a "cibersegurança"? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

6. O que faz para se manter seguro? *

Marcar tudo o que for aplicável.

- ☐ Mantenho o sistema operativo atualizado
- ☐ Utilizo um programa anti-vírus
- ☐ Tenho passwords variadas
- ☐ Atualizo regularmente as minhas passwords
- ☐ Não entro em sites "duvidosos" ou suspeitos
- ☐ Utilizo produtos oficiais / não alterados
- ☐ Nenhuma das anteriores
- Outra: ☐ _____

7. Considera o negócio do hacking / cracking rentável? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei

8. Por favor, coloque observações/dúvidas que gostaria de ver exploradas ou esclarecidas: