Caracterização de senhas utilizadas pela comunidade universitária como ponto de partida para o desenvolvimento de capacitação em cibersegurança

João Roberto Randel[1], Jorge Siqueira Serrão[1], Hugo Lima Romão[1], Felipe Leite Lobo[1], Marcelo Henrique Oliveira Henklain[1], Eduardo Luzeiro Feitosa[2]

[1]Departamento de Ciência da Computação – Universidade Federal de Roraima (UFRR)
Caixa Postal 15.064 – 91.501-970 – Boa Vista, RR – Brasil

[2]Instituto de Computação – Universidade Federal do Amazonas (UFAM) – Manaus, AM – Brasil

{felipe.lobo, marcelo.henklain}@ufrr.br, {hugo8romao, jrobertocunharr}@gmail.com, jorgefilhoz@hotmail.com, efeitosa@icomp.ufam.edu.br

Abstract. *The adoption of weak passwords occurs, in part, because secure practices increase the effort in using systems. When teaching about strong passwords, it is useful to start from the user's behavior and improve it, thus reducing his/her effort. In our study, we broke 242 hashes of passwords from users at a university to characterize them and then, propose learning objectives. We evaluated the effectiveness of the brute force (BF) and hybrid attacks (BF and dictionary) on a basic and a professional machine. BF was more effective, cracking 62.81% of passwords. They had 5 to 12 characters and did not meet minimum security requirements. We noticed that users need to learn how to create long passwords with different types of characters.*

Resumo. *A adoção de senhas fracas ocorre, em parte, porque práticas seguras aumentam o esforço no uso de sistemas. Ao ensinarmos sobre senhas fortes, é útil partir do comportamento que o usuário apresenta e aperfeiçoá-lo, reduzindo assim o seu esforço. Neste estudo, quebramos 242 hashes de senhas de usuários de uma universidade para caracterizá-las e, então, propor objetivos de aprendizagem. Avaliamos a efetividade dos ataques de força bruta (FB) e híbrido (FB e dicionário) em máquinas básica e profissional. A FB foi mais efetiva, quebrando 62,81% das senhas. Elas tinham de 5 a 12 caracteres e não cumpriam requisitos mínimos de segurança. Notamos que usuários precisam aprender a criar senhas longas e com tipos variados de caracteres.*

1. Introdução

No século XXI, o uso da Internet tem sido uma constante e seu impacto foi ampliado, em razão do distanciamento social imposto pela pandemia de COVID-19 (Guilherme et al., 2021). Na Internet, realizamos operações financeiras, interagimos com pessoas de modo profissional ou íntimo e armazenamos em nuvem os nossos documentos. Nesse cenário, as senhas continuam sendo umas das primeiras linhas de defesa para os nossos dados (Bošnjak and Brumen, 2019; Carvalho et al., 2022). Cumpre, portanto, perguntar: usuários usam senhas cuja força é compatível com os dados que elas protegem? Quais aprendizagens poderiam auxiliar usuários a projetar senhas mais seguras?

Essas questões ilustram a preocupação deste estudo de Educação em Computação (ver Bispo-Jr. et al., 2019), cujo objetivo foi caracterizar senhas de servidores de universidade públiaca do extremo Norte, por meio dos ataques de força bruta e híbrido, como ponto de partida para a formulação de objetivos de aprendizagem para o ensino de cibersegurança a essa população. Foi nosso objetivo secundário avaliar se *hardware* e tipo de ataque impactam na quebra dessas senhas, como forma de explicitar os riscos que os usuários enfrentam a depender dos recursos à disposição do atacante. Comparamos os ataques de força bruta e híbrido, cujo dicionário foi construído pelo primeiro autor.

A motivação desta pesquisa reside no fato de que o uso de senhas seguirá sendo adotado como estratégia de autenticação (Bošnjak and Brumen, 2019), afinal continua sendo o método de autenticação em sistemas web mais utilizado por usuários (Ji et al., 2017). Apesar de sua importância, raramente usuários utilizam senhas fortes, mesmo com campanhas de conscientização sobre ciberataques (Carvalho et al., 2017; Carvalho et al., 2022; Ruoslahti et al., 2021). Em parte, isso ocorre pelo esforço necessário para adotar comportamentos seguros, associado ao fato de que a "redução de risco", decorrente do comportamento seguro, não é uma consequência facilmente perceptível, pois ela implica em "nada ocorrer". O comportamento de risco, por sua vez, não resulta em prejuízo imediato e, ainda, tende a ser menos custoso para o usuário. Como regra, quanto maior a segurança de um sistema, menor a facilidade de utilizá-lo e vice-versa. Sabemos, porém, que comportamentos inadequados expõem os usuários a riscos (Guilherme et al., 2021). Por isso, precisamos auxiliá-los por meio de capacitações.

2. Fundamentação teórica

2.1. Teoria sobre o comportamento aplicada ao ensino

Neste estudo, adotamos a teoria analítico-comportamental e, por isso, partimos do pressuposto de que o comportamento é um fenômeno natural, que consiste em um sistema de interações entre ambiente e ações de uma pessoa (Zilio and Neves-Filho, 2018). Nessa perspectiva, para intervir sobre esse fenômeno, é importante caracterizá-lo (Skinner, 2005/1953), de modo a evidenciar como o usuário se comporta concretamente e o que, se ensinado para ele, pode ajudá-lo a aumentar a força de suas senhas.

Seguimos, assim, um princípio pedagógico baseado na Análise do Comportamento (AC) de partir do que o aluno já conhece para o aprendizado de novos comportamentos, que sejam relevantes em sua realidade de vida (Kienen et al., 2021). Esses comportamentos, definidos como alvos do ensino, são os objetivos de aprendizagem. Destacamos que, ao partirmos do que o aluno já sabe, reduzimos o seu esforço no processo de aprendizado, tornando mais provável que ele apresente em contexto natural, fora da sala de aula, o comportamento ensinado. Entendemos, portanto, que se almejamos que as pessoas adotem comportamentos mais seguros, precisamos ensiná-las a fazer isso e, especialmente, arranjar condições ambientais que tornem mais prováveis esses comportamentos (Hartwig and Reuter, 2021). Esse é o desafio e, para lidar com ele, este estudo é o nosso ponto de partida. Ressaltamos que pesquisas sobre caracterização de comportamentos inseguros podem auxiliar na identificação de oportunidades de intervenção, pois explicitam concretamente, para determinada amostra de usuários, quais comportamentos precisam ser aprendidos, justificando, então, o ensino.

2.2. Força da senha

Existem padrões mínimos do que qualifica uma senha como forte. Elas devem ser (a) tão extensas quanto for possível, (b) devem utilizar todos os tipos de caracteres à disposição do usuário, (c) não devem ser utilizadas para autenticação em mais de uma conta, (d) precisam ser trocadas periodicamente e, a rigor, deveriam (e) ser aleatórias.

Dois estudos recentes podem explicitar o que afirmamos. Bošnjak and Brumen (2018), por exemplo, sugerem o uso de senhas com muitos caracteres, pois em seu estudo foram as mais difíceis de quebrar a partir de ataques de força bruta e de dicionário. No estudo de Ji et al. (2017), os pesquisadores também encontraram evidências de que senhas mais extensas tendem a ser mais fortes, mas destacaram que aquelas que possuem maior variabilidade de conjuntos de caracteres (letras minúsculas e maiúsculas, números e caracteres especiais) são ainda mais robustas. São estudos como esses que orientam a definição de políticas do que seria o ideal em termos de senhas fortes.

Apesar das recomendações existentes, a dúvida persiste sobre qual é a solução mais eficiente para que senhas fortes passem a ser adotadas pelos usuários. Trata-se aqui da busca de ajuste entre segurança e usabilidade. Para tanto, primeiro precisamos descobrir que senhas os usuários adotam, para identificar o que falta ser aprendido ou aperfeiçoado. Destacamos que algumas recomendações de especialistas em segurança sugerem comportamentos de alto custo (baixa usabilidade), que não consideram o que o usuário faz no seu cotidiano e quais dificuldades possui. Entendemos ser pouco realista que um usuário mude o comportamento de padrão inseguro (ex.: senha “12345”), para seguro de alto custo. Por isso, tentar resolver o problema do comportamento seguro pressupõe, de um lado, identificar como os usuários-alvo se comportam e por quais motivos agem assim e, de outro, como podemos determinar que uma senha é forte. Na seção de trabalhos relacionados e neste estudo, avaliaremos como usuários se comportam.

Com relação à força da senha, Glory et al. (2019) propõe a medida de entropia, que consiste em uma medida de sua imprevisibilidade. Quanto maior a entropia, maior o grau de desorganização da senha, tornando-a menos susceptível a um ataque. Geralmente, o valor da entropia é apresentado em termos de bits. Senhas com entropia entre 28-35 bits, são fáceis de serem decifradas. Entre 36-59, temos um grau razoável de dificuldade da senha. As senhas mais difíceis de serem quebradas, são aquelas com entropia superior a 60 bits. Nessa perspectiva, um comportamento seguro de “projetar senha” seria aquele que produzisse como resultado uma senha com entropia, no mínimo, igual a 60 bits. A equação a seguir explicita como a entropia é calculada. $Entropia = Comprimento\_da\_senha\ x\ log_2(Tamanho\_conjunto\_caracteres)$

O comprimento da senha corresponde ao número total de caracteres que ela possui, enquanto o tamanho do conjunto de caracteres (T) tem relação com a quantidade de caracteres possíveis em uma senha. Por exemplo: uma senha como ‘casa’ tem apenas letras latinas minúsculas. Uma vez que existem apenas 26 letras latinas, esse é o tamanho do conjunto de caracteres possível. Mesmo a senha ‘casa’ não usando todos esses caracteres, um atacante precisará testar todos eles em um ataque de força bruta. Por isso que consideramos o total de letras latinas minúsculas. É fácil entender que uma senha como ‘Casa’ já é mais forte só por incorporar as 26 letras latinas maiúsculas. Se adicionarmos caracteres especiais e números, chegaremos ao total de 94 caracteres. Para além deles, conforme expressão matemática da entropia, a outra variável que pode ser alterada é o comprimento da senha, cujo aumento produz melhora na entropia.

2.1. Técnicas de ciberataque

De acordo com Bošnjak and Brumen (2018), ataques de força bruta são os mais conhecidos e aqueles que menos envolvem estratégias elaboradas. A força desse ataque depende, principalmente, do *hadware* do atacante: quanto mais potente, maior o potencial de sucesso, pois esse ataque requer um processo de tentativa e erro de todas as combinações possíveis de senha dentro de um conjunto de caracteres específico e para um tamanho de senha pré-determinado. Ataques de dicionário, por sua vez, partem do pressuposto de que os usuários tendem a escolher senhas previsíveis, como nomes comuns de pessoas ou de celebridades, nomes de lugares, times, carros e assim por diante. O atacante fornece, portanto, uma lista de palavras, com variações em seu formato de escrita, e procura por uma correspondência entre as senhas que está tentando quebrar.

Nos dois processos, ataque de força bruta e dicionário, o programa de computador do atacante trabalha a partir de uma lista de possíveis senhas, que são convertidas em código *hash*. Esse *hash* é, então, comparado com a lista de *hashes* a que o atacante conseguiu acesso e que está tentando quebrar. Cada correspondência encontrada equivale a uma senha quebrada.

Com base nos conceitos expostos, passamos a avaliar o que já foi pesquisado sobre a temática deste estudo. Seguimos, portanto, com a seção de trabalhos relacionados.

3. Trabalhos relacionados

Nesta seção apresentamos uma revisão da literatura, finalizando-a com o objetivo desta pesquisa. Vamos descrever estudos que caracterizam comportamentos de usuários acerca do uso de senhas e outros que investigam padrões de senhas quebradas em ataques.

Na linha de estudos sobre comportamentos de usuários, Guilherme et al. (2021) investigaram o perfil de internautas brasileiros em relação a condutas seguras. Participaram 207 pessoas, sendo 57% entre 18 e 25 anos, 53% com ensino médio completo, 33% com mais de 12h de tempo diário de uso de Internet e 37% sem treinamento em cibersegurança. A tarefa deles foi responder a um questionário. Verificou-se que, com a pandemia por COVID-19, mais de 50% passaram a usar a Internet com maior frequência (ex.: redes sociais, aplicativos de trabalho remoto). Em média, mais de 70% já fizeram *download* de programas de origem duvidosa, mais de 55% já compartilharam celular ou computador, mais de 29% já compartilharam dados de cartão de crédito em *app* de mensagem, mais de 40% sempre utilizam a mesma senha em mais de uma conta e mais de 19% já acessaram conta bancária em Wi-Fi público. Nota-se que os percentuais de ocorrência de comportamentos inseguros inspiram preocupação.

Seguindo nessa linha, muitos estudos realizaram ataques a bases de dados reais contendo apenas o *hash* das senhas, para identificar padrões de senhas quebradas. Bošnjak and Brumen (2018), por exemplo, investigaram quais técnicas de ataque são mais efetivas em termos de sucesso e consumo de tempo. Foi adotado um banco de dados de 151.136 senhas, sendo 16,77% delas criadas por universitários e as demais pelo computador. Os ataques foram de força bruta, de dicionário, combinados, híbridos e por regra. Ao final, 150.213 senhas foram quebradas em 35 horas e 44 minutos. Foi identificada uma diferença estatisticamente significativa entre a entropia das senhas quebradas (33,15) e aquelas que resistiram (68,23). Foi observada também correlação fraca, de 0,20, e estatisticamente significativa entre entropia da senha e tempo do aluno na universidade.

Ji et al. (2017), por sua vez, investigaram em que medida o uso de técnicas avançadas de ataques (envolvendo ataques de força bruta inteligente e de dicionário) seria efetivo para, em um número entre 109 a 1010 tentativas, quebrar cerca de 145 milhões de senhas, oriundas de 15 vazamentos de dados de diferentes plataformas. Avaliaram também como medidores de força de senha as classificariam. Por fim, examinaram se o vazamento de nome de usuário e e-mail poderia aumentar a chances de um atacante quebrar mais senhas. Verificou-se que o uso de múltiplas técnicas aumenta as chances de sucesso do atacante, pois nenhuma isoladamente é sempre eficaz e que houve 80% de sucesso na quebra de senhas, demonstrando que comportamentos inseguros são típicos. Nessa direção, foi identificado que muitos usuários utilizam dados relacionados ao seu e-mail e nome de usuário para a formulação de senhas. Ao examinar ferramentas *on-line* de verificação de força de senhas, foi demonstrado que algumas delas, a exemplo do Google Meter, tendem a classificar senhas fracas e que foram quebradas, como se fossem fortes. Isso representa um risco para usuários e demonstra a necessidade de capacitação das pessoas em segurança da informação, pois elas não podem depender apenas de ferramentas que avaliem a força de suas senhas, para tomar decisões.

Finalmente, Carvalho et al. (2017) identificaram déficits de conhecimento sobre cibersegurança em alunos da educação básica e superior e nos docentes. Foram elaborados dois questionários. O primeiro, aplicado para todos os participantes, continha 10 situações típicas quando usamos a Internet, em relação às quais o participante tinha que identificar, entre as alternativas, aquela que correspondia ao tipo de ataque descrito ou à prática de segurança adequada diante da situação. O segundo questionário, apenas para os docentes, investigava se os professores já haviam ensinado cibersegurança em suas aulas e, em caso negativo, se julgavam pertinente que eles fossem capacitados nessa área. O conhecimento sobre vulnerabilidades tradicionais, como furto de identidade e *malwares*, foi adequado. Contudo, o conhecimento foi, respectivamente, baixo e insuficiente sobre (1) *spam*, (2) criptografia e (3) senhas seguras. Dos professores, mais de 50% afirmaram não ter ensinado nada sobre cibersegurança, em grande medida porque não se consideram preparados para abordar o tema, embora o avaliem como importante. Os autores concluíram que são necessárias mais capacitações em cibersegurança.

Com efeito, precisamos de mais estudos de caracterização dos comportamentos de "projetar e utilizar senhas", envolvendo usuários brasileiros, pois muitos estudos são internacionais (ex.: Ji et al., 2017; Bošnjak and Brumen, 2018). A produção desse conhecimento permite identificar o que o usuário sabe e o que precisa aprender, sendo útil para planejar capacitações (Kienen et al., 2021) sobre cibersegurança, que são cruciais para os cidadãos do século XXI (Ruoslahti et al., 2021; Švábenský et al., 2020). Assim, o nosso objetivo foi caracterizar senhas como ponto de partida para a formulação de objetivos de aprendizagem sobre cibersegurança. Avaliamos também se *hardware* e tipo de ataque impactam na quebra de senhas, para explicitar os riscos que os usuários enfrentam a depender dos recursos do atacante. Este estudo é o início do desenvolvimento de uma capacitação sobre criação de senhas seguras para a comunidade universitária.

4. Método

4.1. Aquisição de dados

Foi formalizado pedido para obtenção de base de dados de usuários inativos de universidade pública, contendo apenas *hashes* das senhas, sem qualquer dado pessoal. O

acesso a esse tipo de dado sensível é compatível com a Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018, conforme art. 7º, inciso IV. Nesses casos previstos em lei, o consentimento do titular dos dados não é necessário. Ademais, cumpre lembrar que, segundo Resolução n. 510/2016 do CNS, não precisam ser registradas e avaliadas pelo CEP/CONEP, "V – pesquisa com bancos de dados, cujas informações são agregadas, sem possibilidade de identificação individual". Ressaltamos que a base de dados não será compartilhada e que, após ter sido disponibilizada pelo setor de TI de universidade pública do Norte, na qual o estudo foi autorizado, ficou armazenada apenas nas máquinas necessárias para a realização dos ataques.

Obtivemos 242 *hashes* de senhas, que foram criadas por professores de diversos cursos e técnicos administrativos da universidade. A exceção das senhas vinculadas ao Departamento de Ciência da Computação, podemos afirmar que as senhas dessa base de dados foram criadas por usuários sem conhecimento especializado em computação.

4.2. Execução do ataque

Os ataques foram conduzidos utilizando o *software* hashcat v6.2.6 (Steube, 2022). Foram selecionadas duas configurações de máquina para a realização dos ataques: **(1) Computador de entrada:** CPU i7 4700HQ 2.4 Ghz, GPU NVIDIA GeForce GTX850M, Memória principal de 16 GB, Memória secundária de 1 TB HD e Sistema Operacional Windows 10 Home 64 bits; adquirido em 2015; **(2) Computador profissional:** CPU i7 11800H 2.3 Ghz, GPU NVIDIA GA107M GeForce RTX3050 Ti Mobile, Memória principal de 32 GB, Memória secundária de 1 TB SSD e Sistema Operacional Windows 11 Pro 64 bits; adquirido em 2023. Selecionamos dois tipos básicos de ataque: força bruta (FB) e híbrido (HB, força bruta e dicionário). Com base no estudo e achados de Bošnjak and Brumen (2018), definimos o tempo limite de execução do software de 36 horas.

O ataque de força bruta consistiu na geração de uma série de combinações de caracteres, as quais observaram as restrições de máscaras, que replicavam características de senhas comumente encontradas em vazamentos. Uma máscara define os tipos e a quantidade de caracteres que devem ser considerados na geração de uma combinação. Essas características são definidas a partir de grupos de caracteres (letras minúsculas, maiúsculas, dígitos e caracteres especiais). A máscara `?l?l?l?l?d?d?d?d`, por exemplo, define um espaço de busca para senhas de oito caracteres, formada por quatro letras minúsculas e quatro dígitos, respectivamente. Neste estudo, adotamos as máscaras disponibilizadas pelo próprio software *hashcat*, totalizando 25.044 máscaras. O comando utilizado no *hashcat* para a execução deste ataque foi:

```
hashcat -a 3 -m 111 -d 1 --runtime=129600 --workload-profile=4 -o
./result.txt hashes.txt masks.hcmask --potfile-disable --status >
logs.txt
```

O ataque híbrido consistiu em uma combinação de um ataque de força de bruta e de dicionário. A proposta desse ataque foi acelerar a quebra de senhas, em relação a um ataque isolado de força bruta. Nesse ataque, o *software* concatenava palavras do dicionário, sempre posicionadas à esquerda, com caracteres numéricos e especiais, posicionados à direita. O dicionário foi construído a partir de nomes comuns, segundo o Censo do IBGE de 2010, times de futebol disponíveis no site da CBF, combinações de letras de teclado e palavras tipicamente encontradas em vazamentos de senhas. Utilizamos o seguinte comando no *hashcat* para a execução deste ataque:

```
hashcat -a 6 -m 111 -d 1 --runtime=129600 --workload-profile=4 -o
./result.txt hashes.txt masks.hcmask wordlist.dict --potfile-disable --
status > logs.txt
```

4.3. Análise de dados

As análises envolveram cálculo de média, desvio padrão, contagem de frequência e cálculo de proporção. Utilizamos duas técnicas de estatística inferencial: teste Anova, testes T como *post hoc* e p-valor com correção de Bonferroni. Os nossos dados violaram o pressuposto de homoscedasticidade (semelhança da variância entre os grupos), mas ao conduzirmos testes com estatísticas não-paramétricas, obtivemos resultados similares àqueles encontrados com as estatísticas paramétricas (requerem o cumprimento de requisitos como normalidade), as quais preferimos por serem mais robustas.

Para a elaboração dos objetivos de aprendizagem, adotamos o procedimento simplificado para descrição de partes funcionais de objetivos intermediários, de natureza interpretativa, proposto pelas analistas do comportamento Cortegoso e Coser (2013). Começamos por identificar as características das senhas quebradas (ex.: baixa extensão) e os conceitos de segurança da informação relacionados aos ataques que realizamos, como aspectos da realidade (isto é, do ambiente) com os quais os usuários precisam aprender a lidar (ou seja, as ações). Com isso, elaboramos sentenças em que o verbo no infinitivo representa uma ação e o complemento, o ambiente. Cada sentença se refere a um comportamento a ser aprendido, isto é, a um objetivo de aprendizagem.

5. Resultados e Discussão

Começamos esta seção com os resultados de senhas quebradas. A Tabela 1 exibe a quantidade de senhas quebradas e a sua entropia, em função do tipo de *hardware* e ataque.

Tabela 1. Quantidade e entropia das senhas quebradas em função do hardware e ataque.

Condição	Quantidade Senhas Quebradas	% Total	Entropia			
			Média	DP	Mínimo	Máximo
1) HW-Básico e FB	119	49,17	32,41	7,76	16,61	41,68
2) HW-Pro e FB	152	62,81	35,07	8,64	16,61	48,70
3) HW-Básico e HB	59	24,38	34,46	12,96	16,61	62,04
4) HW-Pro e HB	67	27,69	33,47	12,45	16,61	62,04

Nota. HW = Hardware utilizado no ataque, que foi Básico ou Profissional; FB = Força Bruta; HB = Ataque híbrido (Força bruta e Dicionário); % Total = (Quantidade Senhas / 242) x 100.

Podemos notar que a estratégia mais efetiva foi o ataque de força bruta, executado a partir do *hardware* profissional. Esse resultado mostra que o grau de perigo de um ataque está relacionado com o poder computacional de que o atacante dispõe, bem como das técnicas que utiliza. O resultado que encontramos, com destaque para o ataque de força bruta em detrimento do híbrido, que combina duas técnicas, contraria os achados de Ji et al. (2017). Provavelmente, a escolha que fizemos no ataque híbrido, de limitar a concatenação de palavras apenas à esquerda, pode ter impactado negativamente a sua efetividade. Além disso, a lista de palavras pode ter sido limitada, principalmente, para lidar com situações nas quais a senha continha apenas letras, como iniciais de um nome.

Cumpre destacar também que, mesmo com um *hardware* básico e ataque de força bruta, foi possível quebrar 49,17% das senhas, sugerindo que mesmo computadores mais

simples podem oferecer risco aos usuários, quando utilizados em um ciberataque. Lembramos, porém, que, tanto Ji et al. (2017) quanto Bošnjak and Brumen (2018) obtiveram percentuais mais elevados de senhas quebradas, respectivamente, 80% e 99,39%. Embora esses estudos tenham combinado várias técnicas, Bošnjak and Brumen (2018) conseguiram em 32 horas e 21 minutos quebrar 97,53% das senhas apenas com o ataque de força bruta. Esse dado sugere que precisamos aperfeiçoar o comando utilizado no *hashcat*. Com efeito, o risco que o usuário sofre ao adotar uma senha fraca pode ser maior do que os nossos resultados podem permitir identificar.

Com relação às médias de entropia, não encontramos diferenças estatisticamente significativas entre as quatro condições por meio da ANOVA para amostras independentes ($F(gl = 3) = 1{,}723$; $p = 0{,}162$). Não obstante, é possível notar que, embora as menores médias de entropia sejam iguais para todas as condições, nos dois ataques híbridos, conseguimos quebrar senhas cuja entropia era 62,04, considerada indicativa de senha forte (Glory et al., 2019). Isso sugere que essa técnica pode quebrar senhas mais difíceis, com o mesmo tempo do ataque de força bruta. Também sugere que, apesar da importância das heurísticas sugeridas por especialistas sobre o que são senhas fortes, é importante que o usuário entenda o básico sobre os tipos de ataques para que, de forma autônoma, consiga ponderar os riscos das senhas que cria e adota. Destacamos que nenhuma das senhas quebradas cumpria os requisitos básicos, tipicamente, solicitados em sistemas web: conter, pelo menos, uma letra maiúscula, uma minúscula, um número e um caractere especial, atingindo o mínimo de oito caracteres ao todo.

A Tabela 2 exibe a caracterização das senhas quebradas em função do tipo de *hardware* e ataque. Com base na literatura revisada, selecionamos estas características: (1) quantidade de caracteres, (2) quantidade de letras, (3) quantidade de números, (4) quantidade de caracteres especiais, (5) quantidades de duplicações de letras, números ou caracteres especiais, (6) quantidade de casos de letras ou números consecutivos.

Tabela 2. Características das senhas quebradas.

Estatísticas	Condição				Médias Gerais
	1) HW-Básico e FB	2) HW-Pro e FB	3) HW-Básico e HB	4) HW-Pro e HB	
Caracteres					
Média	7,02	7,33	7,61	7,64	7,40
DP	1,07	1,17	1,62	1,52	1,35
Mínimo	5,00	5,00	5,00	5,00	5,00
Máximo	10,00	10,00	12,00	12,00	11,00
Letras					
Média	2,53	3,01	3,15	2,78	2,87
DP	1,98	2,18	2,98	2,98	2,53
Mínimo	0,00	0,00	0,00	0,00	0,00
Máximo	6,00	7,00	9,00	9,00	7,75
Números					
Média	4,48	4,28	4,46	4,87	4,52
DP	2,09	2,07	1,97	2,16	2,07
Mínimo	1,00	1,00	1,00	1,00	1,00
Máximo	10,00	10,00	8,00	8,00	9,00
Especiais					
Média	0,01	0,03	0,00	0,00	0,01
DP	0,09	0,21	0,00	0,00	0,08
Mínimo	0,00	0,00	0,00	0,00	0,00
Máximo	1,00	2,00	0,00	0,00	0,75
Duplicações					

Média	1,03	1,02	1,07	1,24	1,09
DP	1,00	0,95	0,87	1,00	0,96
Mínimo	0,00	0,00	0,00	0,00	0,00
Máximo	4,00	4,00	4,00	4,00	4,00
Consecutivos					
Média	0,24	0,26	0,17	0,16	0,21
DP	0,77	0,82	0,42	0,41	0,61
Mínimo	0,00	0,00	0,00	0,00	0,00
Máximo	7,00	7,00	2,00	2,00	4,50

Os dados da Tabela 2, na dimensão de quantidade de caracteres, sugerem que com os ataques híbridos (condições 3 e 4) conseguimos quebrar senhas mais extensas que nos ataques de força bruta (condições 1 e 2). Encontramos uma diferença estatisticamente significativa nessa direção ($F(gl = 3) = 4{,}620$; $p = 0{,}003$). Os testes *post hoc* indicaram que as diferenças estavam entre as condições 1 e 3 ($p = 0{,}023$) e 1 e 4 ($p = 0{,}009$). Com relação à quantidade de letras, não encontramos diferenças entre as condições ($F(gl = 3) = 1{,}267$; $p = 0{,}285$) e o mesmo ocorreu com a quantidade de números ($F(gl = 3) = 1{,}221$; $p = 0{,}302$), de caracteres especiais ($F(gl = 3) = 1{,}376$; $p = 0{,}250$), de duplicações ($F(gl = 3) = 0{,}904$; $p = 0{,}439$) e de letras ou números consecutivos ($F(gl = 3) = 0{,}402$; $p = 0{,}751$). Portanto, além do número de caracteres, não ocorreu uma distinção de padrões de senhas quebradas pelos *hardwares* e técnicas utilizadas. Esses dados, conforme já destacado, diferem dos achados de Jit el al. (2017). Uma hipótese para explicar eventuais diferenças em padrões de senhas, segundo esses autores, são fatores culturais (ex.: práticas de punição para desobediência às regras) e a finalidade de criação da senha (ex.: banco *versus* rede social). Isso pode ter contribuído para os resultados encontrados, além das limitações já explicadas sobre a configuração do ataque híbrido no *hashcat*.

Com base nesse conjunto de dados, temos elementos empíricos para caracterizar o comportamento dos usuários com os quais pretendemos trabalhar. Eles, tipicamente, adotam senhas com cinco a 12 caracteres. Eventualmente, criam senhas que podem não ter nenhuma letra ou nenhum número ou nenhum caractere especial, motivo pelo qual cada uma dessas dimensões tem quantidades mínimas iguais a zero. Ao examinar as médias gerais, podemos inferir que esses usuários adotam mais números do que letras e, em último lugar, usam caracteres especiais. Um aspecto positivo que nossos dados revelaram é que são pouco frequentes as duplicações de caracteres ou a criação de sequências de caracteres consecutivos, sejam letras (ex.: abc) ou números (ex.: 123).

Notamos, portanto, que de fato os usuários apresentam comportamentos inseguros em relação às senhas que criam e adotam, conforme achados de Guilherme et al. (2021). Uma hipótese para explicar esse comportamento é o fato de que o usuário não sabe projetar senhas seguras (Carvalho et al. (2017), podendo se esquivar dessa tarefa por considerar que apenas soluções muito complexas poderiam ajudá-lo a se proteger. Consequentemente, é necessário ensinar os membros da comunidade acadêmica a projetarem senhas seguras. Partindo dos comportamentos concretos apresentados pelos usuários investigados, identificamos que o aprendizado dos seguintes comportamentos, exibidos na Tabela 3, pode aumentar a sua segurança, pelo menos, em relação a ataques de força bruta e híbridos, cujos parâmetros sejam similares aos que adotamos.

Tabela 3. Objetivos de aprendizagem propostos para o ensino de princípios de cibersegurança.

Comportamento
1) Caracterizar os ataques de força bruta e de dicionário em termos de como quebram uma senha.

2) Identificar as propriedades de senhas que são facilmente quebradas por ataques de força bruta e de dicionário.
3) Caracterizar a força de uma senha em termos do cálculo de entropia e dos requisitos mínimos tipicamente exigidos em sistemas de autenticação.
4) Identificar as propriedades de senhas com entropia menor do que 60, com destaque para o não cumprimento de requisitos mínimos.
5) Avaliar potencial de segurança da senha, considerando propriedades de senhas susceptíveis a ataques de força bruta, de dicionário, com entropia menor do que 60 e que não cumprem requisitos mínimos de segurança.
6) Projetar senha com mais de 12 caracteres, com, pelo menos, uma letra maiúscula, uma letra minúscula, um número, um caractere especial, sem duplicações de caracteres ou sequências de letras ou números consecutivos e que priorize conjuntos de caracteres com maior número de possibilidades de variação, no caso, letras maiúsculas e minúsculas, caracteres especiais e números.

Sugerimos na Tabela 3 seis classes de comportamentos para orientarem a capacitação de usuários (professores e técnicos). Em síntese, esses comportamentos contribuem com a compreensão dos riscos a que estamos expostos, com a identificação dos tipos de senhas que devem ser evitadas, com o reconhecimento de senhas inadequadas e com a criação de senhas seguras, tendo por fundamento os comportamentos de projetar e utilizar senhas que os usuários já adotam. Estamos propondo, portanto, não exigir do usuário grandes mudanças comportamentais, mas sim um aperfeiçoamento de como ele age no cotidiano, reduzindo, desse modo, o seu esforço para agir com segurança. O ensino desses objetivos pode ser realizado pela combinação de aula expositiva com exercícios que envolvam caracterizar ou identificar fenômenos. Os comportamentos de avaliar e projetar senhas, por fim, podem ser favorecidos a partir de situações-problema que precisem ser solucionadas pelos aprendizes. Nos dois casos, avaliação do aprendizado e *feedbacks* constantes são cruciais (Kienen et al., 2021).

Limitações do estudo. A principal limitação deste estudo foi a pequena amostra de senhas. Uma alternativa é compor um banco de dados com senhas vazadas no Brasil ou relatórios de senhas mais comuns nesse país.

6. Conclusão

O objetivo deste estudo foi caracterizar senhas de servidores de universidade pública do extremo Norte por meio dos ataques de força bruta e híbrido, sendo nosso objetivo secundário avaliar em que medida *hardware* e tipo de ataque impactam na quebra de senhas. Verificamos que o ataque de força bruta foi mais efetivo, que comportamentos de projetar e utilizar senhas fracas são recorrentes e que, portanto, uma capacitação é importante, devendo focar no entendimento dos principais ataques e como se proteger.

Sugerimos em estudos futuros investigar se (e em que medida) o conhecimento de dados sobre as pessoas facilita a quebra de senhas, uma vez que existem evidências nessa direção (Aljohani et al., 2020; Tsai et al., 2016; Whitty et al., 2015). Adicionalmente, conduziremos um estudo sobre ensino de cibersegurança a partir dos objetivos de aprendizagem propostos. No momento, realizamos uma palestra e elaboramos uma cartilha (cujo acesso está disponível mediante solicitação aos autores). Contudo, ainda não avaliamos a eficiência dessas condições de ensino.

7. Referências

Aljohani, M., Alruqi, M., Alboqomi, O., and Alqahtani, A. (2020). An experimental study to understand how users choose password. In: *The 4th International Conference on*

Future Networks and Distributed Systems (ICFNDS) (ICFNDS '20). New York: ACM. https://doi.org/10.1145/3440749

Bispo-Jr., E. L., Raabe, A., Matos, E., Maschio, E., Barbosa, E. F., Carvalho, L. G., Bittencourt, R. A., Duran, R. S., and Falcão, T. P. (2019). Tecnologias na Educação em Computação: Primeiros Referenciais. *Revista Brasileira de Informática na Educação – RBIE*, *28*, 509-527. https://doi.org/10.5753/RBIE.2020.28.0.509

Bošnjak, L., Sreš, J., and Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. In: *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1161-1166). https://doi.org/10.23919/MIPRO.2018.8400211

Bošnjak, L., Sreš, J., and Brumen, B. (2019). Rejecting the death of passwords: Advice for the future. *Computer Science and Information Systems*, *16*(1), 313-332. https://doi.org/10.2298/CSIS180328016B

Carvalho, E. A., Reis, T. A., and Alves, F. J. (2017). Ensino de noções básicas de segurança da informação nas escolas brasileiras. In: *Anais do XXIII Workshop de Informática na Escola (WIE 2017)*. https://doi.org/10.5753/cbie.wie.2017.765

Carvalho, H., Ribeiro, J., Batista, D., and Pina, J. (2022). HashifyPass - Uma Ferramenta para Visualização de Hashes de Senhas. In: *Anais Estendidos do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (pp. 79-86). Porto Alegre: SBC. https://doi.org/10.5753/sbseg_estendido.2022.226940

Cortegoso, A. L., and Coser, D. S. (2013). Elaboração de programas de ensino: Material autoinstrutivo. EdUFSCar: São Carlos.

Glory, F. Z., Aftab, A. U., Tremblay-Savard, O., and Mohammed, N. (2019). Strong password generation based on user inputs. In: *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (p. 416-423). https://doi.org/10.1109/IEMCON.2019.8936178

Guilherme, L. P., Ferreira, M. F., Fonseca, G. M., and Lazarin, N. M. (2021). Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede. In: *Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro* (pp. 1-7). Porto Alegre: SBC. https://doi.org/10.5753/ersirj.2021.16972

Hartwig, K., and Reuter, C. (2021). Nudge or restraint: How do people assess nudging in cybersecurity - a representative study in Germany. In: *European Symposium on Usable Security 2021 (EuroUSEC '21)* (pp. 141-150). New York: ACM. https://doi.org/10.1145/3481357.3481514

Ji, S., Yang, S., Hu, X., Han, W., Li, Z., and Beyah, R. (2017). Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords. *IEEE Transactions on Dependable and Secure Computing*, *14*(5), 550-564. https://doi.org/10.1109/TDSC.2015.2481884

Kienen, N., Panosso, M. G., Nery, A. G. S., Waku, I., and Carmo, J. S. (2021). Contextualização sobre a Programação de Condições para Desenvolvimento de Comportamentos (PCDC): Uma experiência brasileira. *Perspectivas em Análise do Comportamento*, *12*(2), 360–390. Recuperado de https://www.revistaperspectivas.org/perspectivas/article/view/818

Ruoslahti, H., Coburn, J., Trent, A., and Tikanmäki, I. (2021). Cyber Skills Gaps – A Systematic Review of the Academic Literature. *Connections: The Quarterly Journal*, *20*(2), 33-45. https://doi.org/10.11610/Connections.20.2.04

Skinner, B. F. (2005). *Science and human behavior*. Cambridge, MA: The B. F. Skinner Foundation. (Trabalho original publicado em 1953). Recuperado de https://goo.gl/D7yLsb

Steube, J. HashCat. (2022). Recuperado de https://github.com/hashcat/hashcat

Švábenský, V., Vykopal, J., and Čeleda, P. (2020). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. In: *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. https://doi.org/10.1145/3328778.3366816

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. http://dx.doi.org/10.1016/j.cose.2016.02.009

Whitty, M., Doodson, J., Creese, S., and Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7. https://doi.org/10.1089/cyber.2014.0179

Zilio, D., and Neves-Filho, H. (2018). O que (não) há de "complexo" no comportamento? Behaviorismo radical, self, insight e linguagem. *Psicologia USP*, *29*(3), 374–384. https://doi.org/10.1590/0103-656420170027