N_COM_DAD_A8 - Texto de apoio

Índice

1. INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

Queridos alunos, chegamos à última aula de nosso componente Comunicação de dados. Nesta última parte do componente, trabalharemos alguns conceitos fundamentais de segurança de redes e segurança da informação.

Durante décadas, as redes de computadores eram usadas somente por centros de pesquisa, universidades e funcionários de empresas que valiam-se de suas redes locais para compartilhar recursos. Neste cenário, como as condições de acesso eram limitadas e quase não havia acesso externo às redes, a segurança destas não precisava de maiores cuidados (Tanenbaum, 2010).

Nas últimas três décadas, as redes de computadores criaram uma revolução na utilização das informações, que agora são distribuídas (Forouzan, 2010). Essa revolução chamada Internet permitiu que qualquer pessoa no mundo acessasse serviços de compras/ pagamentos online, entretenimento ou trabalhassem remotamente de qualquer lugar do mundo. Segundo White (2012), toda essa interconectividade entre sistemas pode ser tanto maléfica quando benéfica, pois ao mesmo tempo em que temos uma sociedade cada vez mais conectada, oferecendo e consumindo serviços que estão a um clique do usuário, estamos também cada vez mais vulneráveis a incidentes de segurança da informação.

A preocupação com incidentes de segurança da informação levou o órgão de padrões do Reino Unido a publicar, em 1995, o padrão British Standard 7799 (BS7799) que trata a gestão de segurança da informação. Esse manual de boas práticas foi usado pela ISO (Organização Internacional de Normalização) para criar o padrão internacional de gestão de segurança da informação ISO/IEC 17799:2000 que, por sua vez, foi usado pela Associação Brasileira de Normas Técnicas (ABNT) para criar um padrão nacional (NBR ISO/IEC 27002:2013) com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações.

Apesar de o assunto segurança da informação ser muito abrangente, nossa disciplina de Comunicação de dados tratará, de maneira introdutória, o tema, apresentando a você conceitos básicos de segurança – como metas de segurança, ameaças, vulnerabilidades e classificação de ataques. Também veremos, ao longo da unidade, algumas técnicas usadas para mitigar eventuais problemas de segurança.

2. SEGURANÇA DEFINIDA POR METAS – MODELO CIDAL

Segundo Comer (2016), as redes não podem ser classificadas simplesmente como seguras ou não seguras, pois o termo não é absoluto. Apesar de todos os recursos e soluções disponíveis para prover proteção das redes de computadores, não é possível afirmar que uma rede é 100% segura. Segundo White (2012), nunca tivemos redes e sistemas de comunicação tão seguros como os que usamos hoje e, ao mesmo tempo, devido ao número crescente de ameaças, nunca estivemos tão vulneráveis a incidentes de segurança da informação.

Para entender melhor o paradigma acima, precisamos compreender que ameaça é uma possibilidade de ocorrer um ataque ou algum tipo de evento que cause danos a sistemas de informação e que vulnerabilidade é uma falha (proposital ou não) ou uma fraqueza que pode deixar os sistemas de computação em situação de risco ou suscetíveis a ataques. Considerando que não é possível conhecer ou prever todas as ameaças de redes existentes (até porque, todos os dias, ameaças novas podem surgir), especialistas de segurança da informação recomendam que políticas de segurança da informação usem como base a chamada Tríade CIA (Confidentiality, Integrity and Availability).

Chamada por Forouzan (2010) como metas de segurança, a Tríade CIA ou CID (confidencialidade, integridade e disponibilidade) representa os três principais pilares da segurança da informação. Esses pilares permitem aos especialistas de segurança cibernética e, até mesmo, aos desenvolvedores a priorizar ações que podem auxiliar na proteção de sistemas em rede. Os três elementos da tríade CID podem ser definidos como:

Confidencialidade: relacionado ao sigilo das informações, a confidencialidade deve garantir que pessoas não autorizadas não tenham acesso a informações armazenadas ou em transmissão em uma rede de computadores ou na Internet. O princípio da confidencialidade também costuma ser associado com a privacidade.

Integridade: esse pilar refere-se à confiabilidade das informações ou dos recursos da rede. A integridade deve garantir que, ao manipular, armazenar ou transmitir informações, mecanismos de controle devem ser implementados de maneira a assegurar que as informações não serão alteradas por entidades não autorizadas ou por falhas nos sistemas.

Disponibilidade: segundo Forouzan (2010), a informação é inútil se ela não estiver disponível, logo, a disponibilidade define que as informações e os serviços de uma organização precisam estar disponíveis para entidades autorizadas.

Além da tríade CID apresentada, outras duas metas foram acrescentadas, formando o modelo conhecido como CIDAL. As metas adicionadas são:

Autenticidade: garante a confirmação da identidade de um usuário de rede. Pilar que complementa a confidencialidade e o sigilo das informações, a autenticidade fornece mecanismos para garantir ou limitar o acesso às informações por parte dos usuários.

Legalidade: este pilar alerta que a manipulação e o acesso aos dados, bem como o uso da tecnologia de informática e comunicação deve estar de acordo com as leis vigentes do país.

3. TIPOS DE ATAQUES

Para garantir que os sistemas computacionais atendam às metas de segurança citadas no tópico anterior, é necessário conhecer e classificar os principais ataques à segurança da informação.

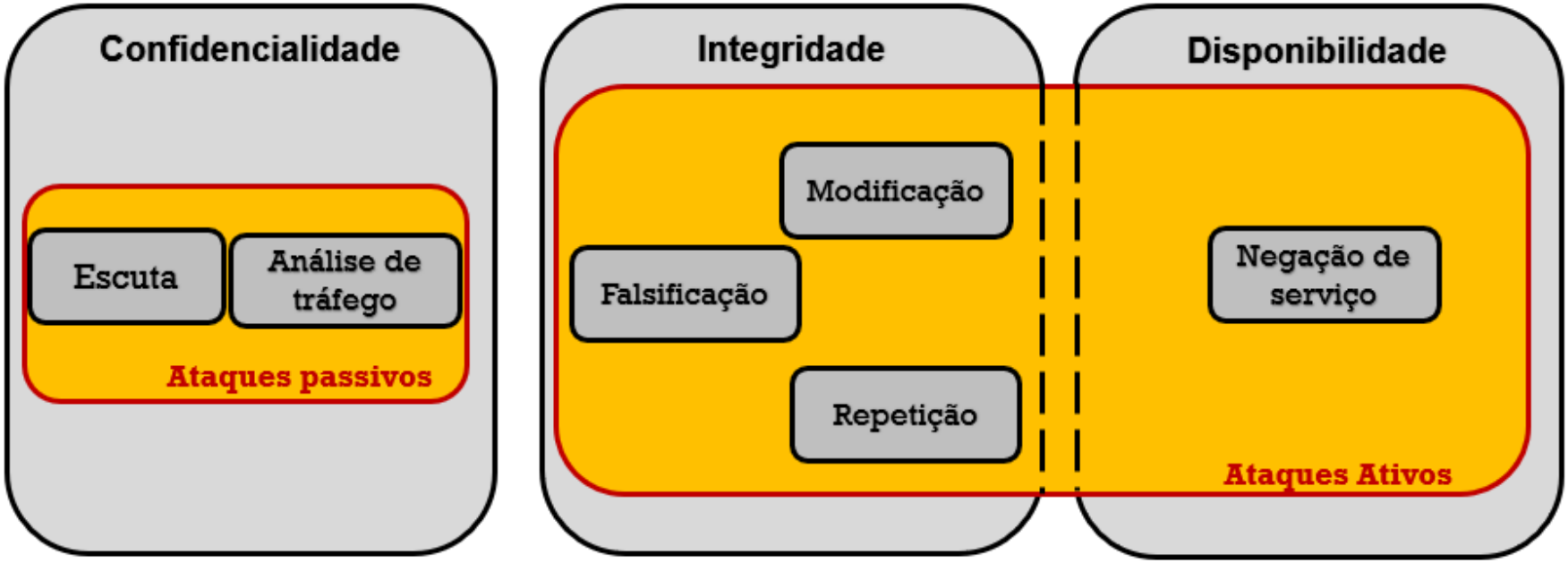
Diversas técnicas podem ser usadas para identificar ataques. Segundo a RFC 2828, os ataques podem ser classificados como passivos e ativos, bem como internos ou externos.

Os ataques passivos são ataques de monitoramento usados para tentar aprender ou fazer uso das informações monitoradas sem afetar os recursos do sistema (por exemplo, escuta de transmissão de voz sobre IP). Muitas vezes, os ataques passivos podem ser usados para planejar um futuro ataque ativo. Os ataques ativos, por sua vez, envolvem algum tipo de modificação no sistema, afetando sua operação ou adulterando dados armazenados ou em transmissão.

Tanto ataques ativos quando passivos podem ser classificados como internos ou externos. Um ataque interno é caracterizado por um ataque iniciado dentro do perímetro de segurança, ou seja, um agente (usuário) que possui autorização para usar o sistema inicia o ataque de maneira voluntaria ou involuntária (por exemplo, realiza o download de um arquivo infectado e executa esse arquivo na rede, sem saber da ameaça). O ataque externo, por sua vez, como o nome diz, é realizado por algum agente fora do perímetro de segurança da rede.

Forouzan (2010) classifica os ataques em três grupos e associa essa classificação à tríade CID, criando uma taxonomia de ataques. Na Figura 1, temos a taxonomia de ataques relacionados à tríade CID proposta por Forouzan, associada à classificação de ataques citada na RFC 2828.

Figura 1 – Taxonomia de ataques relacionados às metas de segurança



Fonte: Forouzan (2010).

Na Figura 1, vemos que os ataques passivos são responsáveis por violações à confidencialidade das informações. Dentre os ataques que podem comprometer a confidencialidade, podemos citar:

Ataques de escuta: refere-se à interceptação de dados/ mensagens que podem ser confidenciais e estão trafegando por redes de comunicações. Neste tipo de ataque, o agente malicioso (atacante) pode usar o conteúdo da mensagem interceptada em seu benefício próprio.

Análise de tráfego: considerando que por meio de técnicas de criptografia (a criptografia será discutida mais adiante) uma mensagem transmitida por uma rede de comunicações pode se tornar ilegível, ainda assim, um agente malicioso pode ter interesse em interceptar as mensagens com o objetivo de obter padrões usados durante a transmissão. A análise de tráfego pode, por exemplo, fornecer ao atacante endereços de emissor ou do receptor de mensagens, bem como padrões de criptografia.

Os ataques ativos agem diretamente contra a integridade e disponibilidade dos dados. Quando analisamos a integridade dos dados, podemos citar os seguintes ataques:

Modificação: segundo Stallings (2008), modificação ocorre quando uma parte de uma mensagem legítima foi alterada ou as mensagens foram reordenadas para produzir um efeito não autorizado em benefício do atacante ou de terceiros. Esse ataque pode, por exemplo, alterar uma mensagem em que há uma proibição de acesso às instalações de uma empresa para uma mensagem de autorização de acesso.

Repetição: neste ataque, o agente malicioso captura e armazena mensagens enviadas por um usuário legítimo para enviá-las mais tarde. Neste tipo de ataque, o agente malicioso pode, por exemplo, reutilizar uma mensagem de ordem de pagamento para receber valores duplicados (Forouzan, 2010).

Falsificação: Nos ataques de falsificação, o agente malicioso se faz passar por outra pessoa para obter acesso a sistemas e/ou executar ações criminosas. Podemos citar, como exemplo de falsificação, o uso do número de cartão de crédito de terceiros para realizar compras on-line, ou o uso de nome de usuário e de senha de terceiros para realizar acesso a serviços na Internet.

Os ataques de modificação de repetição também são conhecidos como ataques de Man-in-the-middle (MitM), pois, nesse tipo de ataque, o agente malicioso intercepta as mensagens entre o emissor e seu receptor legítimo.

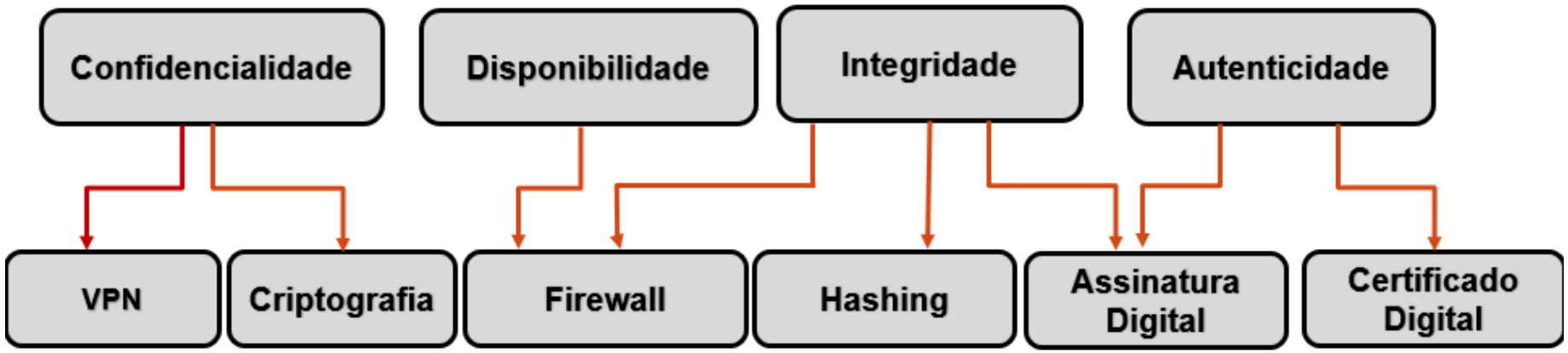
Por fim, quando analisamos a disponibilidade, temos o ataque ativo conhecido como negação de serviço.

Negação de Serviço: conhecido também como ataques de DoS (Denial of Service), neste ataque, o agente malicioso tem como objetivo causar dano ou interromper totalmente serviços disponíveis na rede. Ele pode desde cortar um cabo de rede ou mudar o endereço do servidor DNS de uma máquina, impedido que a vítima acesse à Internet. Os ataques de DoS podem acontecer de forma coordenada, com diversos computadores disparando milhares de solicitações a um servidor, por exemplo. Esse disparo em massa de solicitações pode deixar o servidor lento ou interromper o serviço devido à impossibilidade de responder a todas as solicitações. Tal ataque coordenado é conhecido como DDoS (Distributed Denial of Service).

4. TECNOLOGIAS DE MITIGAÇÃO DE ATAQUES

Ao longo dos anos, diversas técnicas, algoritmos e produtos de segurança foram desenvolvidos com o objetivo de mitigar ameaças e ataques a sistemas de informação. Conhecer os princípios dessas ferramentas e como elas podem garantir as metas impostas pelo modelo CIDAL são de extrema importância para os profissionais de TI. Na Figura 2, temos um resumo das principais técnicas que podem contribuir com as metas impostas pelo modelo CIDAL.

Figura 2 – Principais técnicas usadas para garantir as metas de segurança da informação



Fonte: Elaborada pelo autor.

Nos tópicos subsequentes, estudaremos as tecnologias apresentadas na Figura 2.

4.1. Funções de hash

A função hash é um algoritmo matemático que converte uma informação de entrada de tamanho variado em uma saída de comprimento fixo conhecida como valor de hash. Usada para garantir a integridade de mensagens transmitidas em rede, quando um host deseja transmitir uma mensagem, ele pode gerar um hash dessa mensagem e anexá-lo a ela. Ao receber a mensagem com hash, o destinatário deve executar o mesmo algoritmo de hash executado na mensagem original e verificar se o hash obtido a partir da mensagem recebida é idêntico ao hash recebido junto com a mensagem. Valores de hash divergentes indicam que a mensagem foi corrompida.

4.2. Criptografia

A palavra criptografia tem origem grega e significa “escrita secreta” (Tanenbaum, 2010). Considerado um dos componentes mais importantes na segurança de informação, a criptografia é usada para garantir a confidencialidade das informações, bem como para contribuir com a privacidade na rede. O uso dessa técnica permite mitigar ataques como escuta, modificação e repetição e limita a análise de tráfego, pois uma parte da mensagem se tornará ilegível.

Para entender como ocorre a criptografia de dados, faz-se necessário definir alguns termos usados por teóricos de sistemas criptográficos:

Texto claro: uma mensagem original antes de ter sido criptografada.

Texto cifrado: uma mensagem após ter sido criptografada.

Chave: conjunto curto de bits ou palavras usado para criptografar uma mensagem.

Algoritmo de criptografia: algoritmo que transforma um texto claro em texto cifrado.

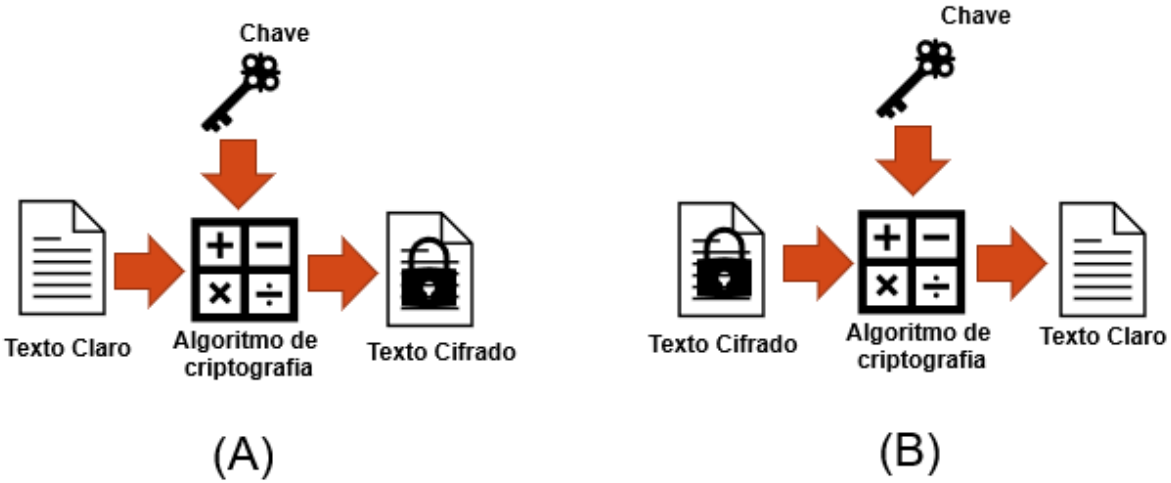
Algoritmo de decriptografia: algoritmo que transforma o texto cifrado em texto claro.

Cifrar: ação de transformar um texto claro em texto cifrado.

Decifrar: ação de transformar um texto cifrado em um texto claro.

Basicamente, a criptografia de dados é feita por um algoritmo matemático que, a partir de uma chave, cifrará uma mensagem em texto claro, transformando-a em uma mensagem em texto cifrado. Na Figura 3(A), temos uma representação dos elementos usados na criptografia de dados.

Figura 3 – Modelo simplificado de criptografia (A) e de decriptografia (B)



Fonte: Elaborada pelo autor.

O processo de criptografia é reversível, ou seja, um algoritmo pode transformar (decriptografar/ decifrar) uma mensagem de texto cifrado em texto claro desde que seja usado no processo o mesmo algoritmo que cifrou a mensagem e uma chave equivalente à chave usada no processo de criptografia.

Apesar das diversas técnicas de criptografia e independentemente da complexidade dos algoritmos, Forouzan (2010) classificou os algoritmos de criptografia em duas grandes categorias: cifras de chave simétrica e cifras de chave assimétrica.

Cifras de chave simétrica: neste sistema de criptografia, uma única chave é usada tanto para cifrar quanto para decifrar as mensagens, ou seja, o destinatário de uma mensagem cifrada só conseguirá decifrar a mensagem se conhecer a chave que foi usada no processo de cifragem.

Cifras de chave assimétrica: neste tipo de criptografia, para cifrar e decifrar uma mensagem, é necessário o uso de duas chaves distintas conhecidas como chave pública e chave privada. Amplamente usado por sites de e-commerce, os algoritmos de chave assimétrica funcionam da seguinte forma: quando um usuário deseja realizar um pagamento no site de e-commerce e enviará os dados de seu cartão de crédito de maneira segura, o site em que a operação está sendo realizada disponibiliza para o usuário uma chave pública que será usada para cifrar a mensagem.

A mensagem em texto cifrado é transmitida até o servidor do e-commerce que usará a chave privada para decifrar a mensagem recebida. Neste sistema, é impossível decifrar uma mensagem usando uma chave pública, fato que garante que a mensagem somente será decifrada pelo detentor da chave privada.

4.3. Certificado e assinatura digital

Uma assinatura digital é um método matemático que usa criptografia de chave assimétrica com objetivo de garantir a autenticidade e a integridade de uma mensagem, documento digital ou software.

No processo de assinatura digital, o signatário possui uma chave privada que será usada para assinar o documento. A veracidade do documento é verificada por meio da chave pública do signatário.

Assim como acontece fora do mundo digital, quando assinamos um documento (por exemplo, a compra de um imóvel ou um carro), além da assinatura, é necessário ir a um cartório comprovar que as assinaturas presentes no contrato são legitimas. Quem garante essa legitimidade é o funcionário do cartório.

Um processo semelhante acontece no mundo digital. Além da assinatura digital, fez-se necessária a criação de uma entidade que consiga verificar se aquela assinatura é legitima ou não. Essa entidade é chamada de autoridade de certificação (CA). Toda vez que uma mensagem, documento digital ou software é assinado digitalmente, a CA é a responsável por verificar a assinatura digital e emitir um certificado digital, comprovando a autenticidade do documento.

4.4. Firewall

Segundo Forouzan (2010), firewall é um dispositivo/ software instalado entre a rede interna de uma organização e o restante da Internet por onde todos os pacotes, entrando ou saindo da rede, devem passar. Os firewalls são configurados com regras que definem o tráfego permitido dentro e fora de uma rede. Eles podem ser classificados como:

Filtro de pacotes: nesse tipo de firewall, os pacotes são filtrados com base nas informações presentes na camada de rede ou de transporte dos pacotes. Todo pacote que chegar a um firewall de filtro de pacotes pode ter seu tráfego permitido ou negado com base em uma lista de permissões criada pelo administrador da rede. Por exemplo, se o administrador de redes quer proibir o acesso a determinado site que não está em conformidade com a política de uso da empresa, ele pode simplesmente configurar o firewall para negar (descartar) todos os pacotes de rede cujo endereço IP de destino seja o endereço IP do servidor do site.

Outra possibilidade é bloquear um serviço de rede com base em sua porta, por exemplo; o administrador de redes não quer permitir acesso remoto a terminais da rede por meio do protocolo Telnet (Protocolo de Interface de terminais e de aplicações através da Internet). Para impor essa proibição, basta o administrador de redes configurar o firewall para não permitir a passagem de pacotes cuja porta de destino seja a porta 23 (porta padrão do protocolo Telnet).

Servidores Proxy: atuando como um servidor intermediário entre hosts na LAN e a Internet, os servidores proxy, além de realizarem uma filtragem de pacotes na camada de transporte e na camada de rede, também inspecionam a camada de aplicação.

4.5. Redes privadas virtuais

A rede privada virtual ou VPN (Virtual Private Networks) é uma tecnologia selecionada por empresas para realizar acesso ou compartilhar recursos protegidos dentro da empresa usando a infraestrutura de redes públicas (Internet). Para garantir a privacidade e confidencialidade dos dados transmitidos pela Internet, as VPNs fazem uso de tecnologias de tunelamento e criptografia.

5. REFERÊNCIAS

COMER, D. Redes de Computadores e Internet. 2. ed. Porto Alegre: Bookman, 2016.

FOROUZAN, B. A. Comunicação de dados e Redes de computadores. 3. ed. Porto Alegre: Bookman, 2010.

RFC 2828 – Internet Security Glossary. Disponível em: <https://datatracker.ietf.org/doc/html/rfc2828> Acesso em: 15 jul. 2021.

STALLINGS, W. Criptografia e Segurança de redes: princípios e práticas. 4. ed. São Paulo: Pearson, 2008.

TANENBAUM, A. Redes de computadores. 5. ed. São Paulo: Pearson, 2010.

WHITE, C. M. Redes de computadores e comunicação de dados. 6. ed. São Paulo: Cengage, 2012.