Marcelo Nagy

Fundamentos de Cibersegurança

Como se defender contra ameaças online

AFD
Academia de Forense Digital

SUMÁRIO

INTRODUÇÃO

A internet é uma ferramenta poderosa e essencial em nossas vidas, seja para nos comunicarmos, nos informarmos ou realizarmos negócios. Porém, essa mesma ferramenta pode ser utilizada por indivíduos mal-intencionados para cometer crimes virtuais que afetam diretamente a segurança e a privacidade dos usuários da rede.

Nesse contexto, é imprescindível que todos nós tenhamos conhecimento sobre as principais ameaças virtuais e saibamos adotar boas práticas de segurança cibernética para nos protegermos contra esses ataques. Além disso, é fundamental que profissionais de cibersegurança estejam atentos a essas ameaças e trabalhem incansavelmente para garantir a segurança do perímetro cibernético de empresas, organizações e governos.

Neste e-book, intitulado "Fundamentos de Cibersegurança: como se defender contra ameaças online", abordaremos de forma clara e objetiva como a internet é utilizada para a realização de crimes virtuais e qual é a importância dos profissionais de cibersegurança na garantia da segurança do perímetro cibernético contra as principais ameaças virtuais. Além disso, destacaremos como o conhecimento adequado em cibersegurança pode auxiliar as forças de lei e profissionais do direito a esclarecer contravenções dessa natureza.

Apesar de ser um conteúdo introdutório na área, esperamos que este e-book possa contribuir para uma maior conscientização sobre a importância da segurança cibernética e para que o leitor esteja apto a adotar boas práticas de segurança cibernética e contribuir para a prevenção de crimes virtuais.

Boa leitura!

AGRADECIMENTO

Antes de tudo, eu gostaria de expressar minha profunda gratidão a todos aqueles que contribuíram para a realização deste e-book "Fundamentos de Cibersegurança" da Academia de Forense Digital. É com grande emoção que escrevo estas palavras, pois este trabalho não seria possível sem a ajuda de muitas pessoas importantes em minha vida.

Primeiramente, gostaria de agradecer ao meu filho Gustavo e minha esposa Rose, que sempre estiveram ao meu lado, me incentivando e me apoiando em todas as etapas da minha jornada. Sem o amor, o apoio e a compreensão deles, eu não teria a força necessária para seguir em frente com este projeto.

Também gostaria de agradecer a todos os meus alunos, que foram os principais motivadores para que eu começasse a escrever este e-book. Ao longo dos anos, tive a oportunidade de ensinar a muitos estudantes sobre cibersegurança e fiquei feliz em ver o interesse e a paixão que eles demonstraram por essa área. O feedback positivo e as perguntas desafiadoras que eles me fizeram me ajudaram a aprimorar meus conhecimentos e me inspiraram a compartilhá-los com um público mais amplo.

Por fim, não posso deixar de agradecer aos meus professores, que me guiaram e me inspiraram a seguir o caminho da segurança cibernética. Eles me ensinaram as habilidades técnicas necessárias para navegar neste mundo digital cada vez mais complexo e me mostraram a importância de se manter atualizado sobre as últimas tendências e ameaças. Sem o conhecimento e a orientação deles, eu não teria as habilidades necessárias para transmitir este conhecimento aos outros.

A todos que contribuíram para este projeto, gostaria de expressar minha gratidão mais sincera. Este e-book é um esforço coletivo e reflete a dedicação e o compromisso de todos os envolvidos em compartilhar seu conhecimento e experiência em cibersegurança.

Espero que este e-book possa ajudar a aumentar a conscientização sobre a importância da cibersegurança e fornecer a base necessária para as pessoas se protegerem de ameaças online cada vez mais sofisticadas.

SOBRE O AUTOR

Marcelo Nagy é um profissional de destaque na área de segurança da informação e forense digital, com vasta experiência em prevenção e investigação de crimes digitais e perícia judicial. Atualmente, é Diretor da STWBrasil, Chefe de Segurança da Informação na QualiSign S.A e Diretor da Academia de Forense Digital. Além disso, é curador e professor de pós-graduação na renomada Universidade Presbiteriana Mackenzie.

Como perito forense, Nagy colabora com o TRT-SP, TJ-SP e forças de lei do Estado de São Paulo, oferecendo sua expertise na identificação e análise de evidências digitais em casos jurídicos. Ele também é um consultor experiente em prevenção de crimes digitais, atuando em projetos importantes para a Rede Globo de Televisão.

Com sua vasta experiência em segurança da informação e forense digital, Marcelo Nagy é uma figura reconhecida e respeitada na comunidade de TI, e é um palestrante frequente em eventos nacionais e internacionais sobre segurança cibernética.

OBJETIVO

O objetivo deste e-book é fornecer aos leitores um entendimento claro de como a internet é utilizada para a realização de crimes virtuais e qual é a importância dos profissionais de cibersegurança na garantia da segurança do perímetro cibernético contra as principais ameaças virtuais. Além disso, o e-book tem como objetivo destacar como o conhecimento adequado em cibersegurança pode auxiliar as forças de lei e profissionais do direito a esclarecer contravenções dessa natureza. O conteúdo deste e-book visa capacitar o leitor a adotar boas práticas de segurança cibernética e a entender as principais técnicas e ferramentas utilizadas pelos cibercriminosos para realizar seus crimes virtuais. Com isso, espera-se que o leitor esteja apto a proteger suas informações pessoais e as informações da organização em que atua, bem como contribuir para a prevenção de crimes virtuais e a aplicação da justiça.

A internet tornou-se uma ferramenta essencial para a comunicação e o compartilhamento de informações em todo o mundo. No entanto, com o aumento do acesso à rede, também houve um aumento significativo de atividades criminosas virtuais. Os crimes virtuais, também conhecidos como cibercrimes, são aqueles que envolvem o uso de tecnologia da informação e da comunicação para cometer ações ilegais.

Diante desse cenário, torna-se fundamental a atuação dos profissionais de cibersegurança na garantia da segurança dos sistemas e informações de empresas e organizações em geral. Os profissionais de cibersegurança são responsáveis por desenvolver e implementar medidas de segurança cibernética, identificar e mitigar ameaças virtuais, bem como garantir a conformidade com as regulamentações e leis de proteção de dados.

Além disso, o conhecimento adequado em cibersegurança é essencial para auxiliar as forças de lei e profissionais do direito na investigação e esclarecimento de contravenções dessa natureza. Compreender as técnicas e ferramentas utilizadas pelos cibercriminosos pode ser uma peça-chave para identificar os responsáveis pelos crimes virtuais e garantir a aplicação da justiça.

Em resumo, a internet é um ambiente cada vez mais propenso a crimes virtuais, o que reforça a importância de medidas de cibersegurança robustas e da atuação de profissionais qualificados para a proteção do perímetro cibernético. A adoção de boas práticas de segurança, tais como a utilização de senhas fortes, a atualização regular de softwares e a conscientização dos usuários, também pode contribuir significativamente para a prevenção de crimes virtuais.

Definição de Cibersegurança

Cibersegurança é o conjunto de práticas, políticas, procedimentos, tecnologias e medidas de proteção que visam garantir a segurança dos sistemas, redes e dispositivos eletrônicos conectados à internet contra ameaças virtuais, como malware, phishing, hacking e outras formas de ataques cibernéticos. O objetivo da cibersegurança é garantir a confidencialidade, integridade e disponibilidade das informações e sistemas que são essenciais para o funcionamento de empresas, organizações, governos e indivíduos. A cibersegurança é uma área em constante evolução e exige a atualização constante das práticas e tecnologias utilizadas para garantir a proteção contra as ameaças cibernéticas cada vez mais sofisticadas.

Cibersegurança e Segurança da Informação estão relacionadas, mas não são exatamente a mesma coisa.

Segurança da informação refere-se a um conjunto de práticas, processos e medidas de proteção utilizadas para garantir a confidencialidade, integridade e disponibilidade das informações, independentemente de sua forma (digital ou física) ou do meio de armazenamento. O objetivo da segurança da informação é proteger as informações contra acessos não autorizados, perda, destruição ou alteração indevida, e isso inclui a proteção contra ameaças cibernéticas.

Por sua vez, a cibersegurança tem como foco a proteção dos sistemas, redes e dispositivos eletrônicos conectados à internet contra as ameaças cibernéticas, como malware, phishing, hacking, entre outros. A cibersegurança é uma parte importante da segurança da informação, pois as ameaças cibernéticas estão cada vez mais presentes e sofisticadas.

Assim, podemos dizer que a cibersegurança é um subconjunto da segurança da informação, mas ambas são essenciais para garantir a proteção das informações e sistemas em um mundo cada vez mais conectado digitalmente.

O termo HACKER

O termo "hacker" tem sido utilizado com frequência para se referir a indivíduos que utilizam habilidades e conhecimentos técnicos para invadir sistemas, redes e dispositivos eletrônicos com o objetivo de roubar informações ou causar danos. No entanto, essa definição não é totalmente precisa ou justa.

Originalmente, o termo "hacker" era utilizado para se referir a programadores experientes que se dedicavam a explorar e experimentar as capacidades dos computadores e sistemas, com o objetivo de entender melhor seu funcionamento e, eventualmente, melhorá-los. Os hackers originais eram considerados especialistas em programação e eram respeitados por sua habilidade técnica e sua dedicação à exploração de sistemas.

Com o tempo, o termo "hacker" acabou sendo utilizado de forma mais ampla para descrever indivíduos que exploram falhas de segurança em sistemas para benefício próprio, incluindo o roubo de informações, a disseminação de malware ou o uso indevido de recursos de computação. Esses indivíduos são geralmente considerados criminosos cibernéticos, e sua atividade é ilegal e prejudicial à segurança e privacidade dos usuários e organizações afetadas.

No entanto, é importante ressaltar que nem todo indivíduo que possui conhecimento técnico e habilidades em programação é um hacker mal-intencionado. Existem hackers éticos, que utilizam seus conhecimentos e habilidades para ajudar a identificar e corrigir falhas de segurança em sistemas e redes, e que trabalham em colaboração com organizações para melhorar a segurança e proteção das informações.

Em resumo, o termo "hacker" pode se referir tanto a indivíduos que utilizam seus conhecimentos para o bem, quanto a criminosos cibernéticos que exploram vulnerabilidades em sistemas para fins ilícitos. É importante diferenciar esses grupos e entender que a habilidade técnica e conhecimento não são, por si só, indicativos de más intenções.

O que diz a lei

A Lei Carolina Dieckmann, oficialmente conhecida como Lei nº 12.737/2012, é uma lei brasileira que trata dos crimes cibernéticos, também conhecidos como cibercrimes. Ela recebeu esse nome em homenagem à atriz Carolina Dieckmann, que teve fotos íntimas divulgadas na internet sem sua autorização em 2012.

A lei tipifica os crimes de invasão de computadores, violação de privacidade, roubo de senhas e outras condutas ilícitas praticadas por meio da internet. Ela prevê penalidades como detenção e multa para quem comete esses crimes. A lei foi sancionada em abril de 2012, após tramitar no Congresso Nacional por cerca de seis anos. Ela foi criada para atualizar a legislação brasileira em relação aos crimes cibernéticos, que estavam se tornando cada vez mais frequentes na época.

Entre as principais mudanças trazidas pela Lei Carolina Dieckmann estão a tipificação do crime de invasão de computadores, a criação do crime de divulgação de informações privadas e a previsão de agravamento de pena para crimes cometidos contra crianças e adolescentes.

A lei também estabelece que a polícia e o Ministério Público podem requerer informações sobre usuários de serviços de internet, como provedores e redes sociais, para investigação de crimes cibernéticos.

A Lei Carolina Dieckmann representa um importante avanço na legislação brasileira em relação aos crimes cibernéticos. Ela torna mais claras as condutas que configuram crimes na internet e estabelece penas mais rígidas para quem as comete. Com isso, espera-se que haja uma redução na prática desses crimes e que as vítimas possam ter mais proteção e justiça.

Essa Lei foi atualizada com a publicação da Lei 14.155, promulgada em 27 de maio de 2021, tipifica o crime de invasão de dispositivo informático no Código Penal Brasileiro. O texto da lei altera o artigo 154-A do Código Penal, que passou a ter a seguinte redação:

"Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa."

Com a nova redação, a lei torna crime a invasão de qualquer dispositivo informático, conectado ou não à internet, sem a autorização expressa ou tácita do proprietário. Isso inclui computadores, celulares, tablets, servidores, entre outros dispositivos.

Para que a conduta seja considerada crime, é necessário que haja violação indevida de mecanismo de segurança do dispositivo. Ou seja, se o dispositivo possuir senha de acesso ou qualquer outro mecanismo de segurança, a violação dessas medidas constitui crime.

Além disso, o objetivo da invasão também é relevante para a caracterização do crime. Se a invasão tiver como finalidade obter, adulterar ou destruir dados ou informações do dispositivo sem autorização do proprietário, ou ainda, instalar vulnerabilidades para obter vantagem ilícita, a conduta será considerada crime.

A pena para o crime de invasão de dispositivo informático é detenção de seis meses a dois anos, além de multa. Se a invasão causar prejuízo econômico à vítima, a pena pode ser aumentada.

A nova lei é um importante instrumento para coibir a prática de invasão de dispositivos informáticos, que pode causar danos significativos à privacidade e segurança dos usuários. A punição prevista na lei deve ser um alerta para quem pretende praticar esse tipo de conduta, especialmente no ambiente digital.

Tipos de HACKER

Existem vários tipos de hackers, cada um com habilidades e motivações diferentes. Aqui estão alguns exemplos:

Hackers White Hat: Esses são os chamados "hackers éticos", que usam suas habilidades para testar a segurança de sistemas de computador, redes e aplicativos em busca de vulnerabilidades que possam ser exploradas por hackers mal-intencionados. Eles trabalham em empresas de segurança cibernética ou em organizações que buscam proteger seus sistemas contra ataques.

Hackers Black Hat: Esses são os hackers mal-intencionados, que usam suas habilidades para invadir sistemas e redes com o objetivo de roubar informações, interromper serviços ou causar danos a organizações ou indivíduos. Eles podem ser criminosos que procuram obter lucro ou simplesmente pessoas que querem provar suas habilidades.

Hackers Gray Hat: Esses hackers não têm intenções necessariamente maliciosas, mas também não são totalmente éticos. Eles podem invadir sistemas para provar uma vulnerabilidade ou para chamar a atenção para uma questão de segurança, mas sem autorização prévia. Eles podem ser vistos como uma mistura dos dois primeiros tipos.

Script Kiddies: São hackers sem habilidades avançadas, mas que usam scripts e ferramentas prontas disponíveis na internet para realizar ataques simples. Eles geralmente não têm conhecimento profundo de como funciona a tecnologia e podem ser considerados uma ameaça menor.

Hacktivistas: Esses hackers usam suas habilidades para apoiar uma causa política ou social. Eles podem atacar sites governamentais ou corporativos para expor práticas injustas ou defender a liberdade de expressão. Eles podem ser considerados uma ameaça significativa para organizações que não estão alinhadas com seus ideais.

Hackers de Estado: Esses hackers são patrocinados pelo governo para realizar ataques cibernéticos em nome do estado ou para espionagem. Eles geralmente têm acesso a recursos avançados e habilidades técnicas superiores, tornando-os uma ameaça significativa para organizações e indivíduos.

Modus Operandi de um Hacker

O modus operandi, ou método de operação, de um hacker pode variar dependendo do seu objetivo e do tipo de sistema que ele está tentando invadir. No entanto, em geral, existem algumas etapas comuns que um hacker pode seguir durante um ataque:

Reconhecimento: Nesta fase, o hacker reúne informações sobre o alvo que deseja atacar. Ele pode usar técnicas de engenharia social para obter informações confidenciais ou explorar vulnerabilidades em sites ou sistemas relacionados para obter mais informações.

Varredura: Depois de reunir informações suficientes, o hacker inicia uma varredura para identificar vulnerabilidades no sistema. Ele pode usar ferramentas automatizadas para examinar portas abertas, serviços em execução ou outras informações do sistema que possam ser exploradas.

Exploração: Quando o hacker encontra uma vulnerabilidade, ele usa técnicas de invasão para explorá-la e ganhar acesso ao sistema. Isso pode envolver o uso de exploits conhecidos ou técnicas de engenharia social para obter acesso aos sistemas ou informações.

Manutenção de acesso: Depois de ganhar acesso ao sistema, o hacker pode instalar backdoors ou outros mecanismos para manter o acesso ao sistema mesmo após a exploração inicial.

Escalonamento de privilégios: Depois de obter acesso, o hacker pode tentar escalar seus privilégios para obter acesso a informações ou sistemas adicionais. Isso pode envolver a exploração de outras vulnerabilidades ou a obtenção de senhas ou credenciais de outros usuários do sistema.

Coleta de dados: Uma vez que o hacker tenha acesso a um sistema, ele pode coletar informações confidenciais, como senhas, informações financeiras ou de identificação pessoal.

Encobrimento: Para evitar ser detectado, o hacker pode tentar apagar ou ocultar evidências do ataque e garantir que seu acesso ao sistema permaneça oculto.

É importante lembrar que nem todos os hackers seguem este mesmo processo ou usam as mesmas técnicas. Alguns podem usar abordagens diferentes, dependendo do alvo ou das habilidades técnicas disponíveis.

Um simples 0-day

Um "0-day" é uma vulnerabilidade de segurança em um software que é desconhecida pelos desenvolvedores do software e pelo público em geral. Esse termo é utilizado porque os desenvolvedores do software têm "zero dias" para corrigir a vulnerabilidade antes que ela possa ser explorada por atacantes mal-intencionados.

Essas vulnerabilidades podem ser exploradas por atacantes para executar código malicioso ou assumir o controle de sistemas e dispositivos, levando a roubo de dados, interrupção de serviços ou outros tipos de ataques cibernéticos.

Para evitar que vulnerabilidades 0-day aconteçam, é importante seguir algumas práticas recomendadas de segurança:

Mantenha seu software atualizado: Mantenha seu sistema operacional e software sempre atualizados com as últimas atualizações e patches de segurança. As atualizações muitas vezes contêm correções para vulnerabilidades conhecidas ou desconhecidas.

Use software confiável: Utilize softwares de fontes confiáveis e evite instalar software de fontes desconhecidas ou não confiáveis.

Use antivírus e firewall: Utilize soluções de antivírus e firewall em seus dispositivos, pois eles podem ajudar a detectar e bloquear atividades maliciosas.

Pratique a segurança cibernética básica: Use senhas fortes e exclusivas, habilite a autenticação de dois fatores, evite clicar em links desconhecidos ou suspeitos em e-mails ou mensagens, entre outras práticas de segurança cibernética.

Realize testes de segurança: Realize testes de segurança em seu software e sistemas para identificar vulnerabilidades que possam ser exploradas pelos atacantes.

Seguindo essas práticas, você pode minimizar o risco de vulnerabilidades 0-day em seus sistemas e dispositivos. No entanto, é importante lembrar que nenhuma medida de segurança é 100% eficaz, e sempre há um risco de vulnerabilidades desconhecidas que possam ser exploradas pelos atacantes.

Mas afinal, o que é um Malware?

Um malware é um tipo de software malicioso que tem como objetivo danificar, controlar ou roubar informações de um computador ou dispositivo móvel. Malware é uma abreviação para "software malicioso".

O malware pode assumir várias formas, como vírus, worms, trojans, spyware, ransomware e outros tipos de software malicioso. Algumas das características comuns do malware incluem:

Propagação: O malware pode se espalhar rapidamente através de redes, dispositivos USB, e-mails, sites maliciosos ou outras formas de comunicação.

Dano: O malware pode danificar arquivos, sistemas, redes e dispositivos, causando perda de dados e interrupção de serviços.

Controle: O malware pode tomar o controle do sistema infectado, permitindo que o invasor execute comandos, roube informações, instale outros tipos de malware e até mesmo controle a câmera ou microfone do dispositivo.
Roubo de informações: O malware pode roubar informações confidenciais, como senhas, números de cartão de crédito, informações bancárias e outras informações pessoais.

Extorsão: O ransomware é um tipo de malware que criptografa arquivos do usuário e exige um resgate para recuperar o acesso a esses arquivos.

Nos anos 90 o termo "vírus" era frequentemente utilizado para se referir a qualquer tipo de software malicioso, incluindo vírus, worms, trojans e outros tipos de malware. Naquela época, o termo "malware" ainda não era tão comum.

Os vírus de computador foram os primeiros tipos de malware a se tornarem amplamente conhecidos e propagados nos anos 80 e 90. Eles se espalhavam através de disquetes e outros dispositivos de armazenamento removíveis e infectavam arquivos executáveis em sistemas operacionais como MS-DOS e Windows.

Os vírus foram amplamente cobertos pela mídia naquela época e geraram grande preocupação entre os usuários de computador. Por causa disso, o termo "vírus" acabou sendo usado de forma genérica para se referir a qualquer tipo de software malicioso que pudesse infectar um computador.

Com o tempo, outros tipos de malware, como trojans, spyware e adware, se tornaram mais comuns e o termo "malware" começou a ser usado com mais frequência para se referir a esses tipos de ameaças cibernéticas. Atualmente, o termo "vírus" é geralmente reservado para se referir especificamente a um tipo de malware que se propaga copiando a si mesmo para outros arquivos ou dispositivos, embora ainda possa ser usado de forma mais geral em alguns contextos.

Para evitar infecções por malware, é importante seguir algumas práticas recomendadas de segurança, como:

Manter o software atualizado: Atualize regularmente o sistema operacional e os softwares instalados com as últimas correções de segurança.

Usar software confiável: Instale apenas software de fontes confiáveis e evite abrir arquivos suspeitos ou desconhecidos.

Usar soluções de segurança: Instale e mantenha atualizado um software antivírus e firewall.

Evitar links e anexos suspeitos: Não clique em links suspeitos ou abra anexos de e-mails de fontes desconhecidas.

Fazer backups: Faça backups regulares dos seus arquivos e mantenha-os armazenados em um local seguro.

Ser cauteloso nas redes sociais: Evite divulgar informações pessoais em redes sociais, pois essas informações podem ser usadas por atacantes para realizar ataques de phishing e outros tipos de ataques.

Ao seguir essas práticas, você pode minimizar o risco de infecção por malware em seus sistemas e dispositivos.

Sobre Ciberextorsões

Ciberextorsão é um tipo de crime cibernético em que um indivíduo ou grupo usa ameaças ou intimidação para obter dinheiro ou outra vantagem de uma vítima. Na ciberextorsão, o criminoso ameaça causar algum tipo de dano ou prejuízo à vítima, como roubar ou expor informações confidenciais, danificar reputações, desativar sites ou sistemas, ou até mesmo prejudicar fisicamente indivíduos ou suas famílias.

Algumas formas comuns de ciberextorsão incluem:

Ransomware: O cibercriminoso infecta o computador da vítima com um tipo específico de malware que criptografa os arquivos do usuário e exige um resgate em dinheiro para desbloqueá-los.

Sextortion: O cibercriminoso ameaça divulgar informações pessoais ou comprometedoras, como fotos ou vídeos sexualmente explícitos, a menos que a vítima pague uma quantia em dinheiro.

DDoS: O cibercriminoso lança ataques de negação de serviço (DDoS) contra sites ou sistemas da vítima, exigindo um pagamento para cessar o ataque.

Ameaças físicas: O cibercriminoso ameaça causar danos físicos a indivíduos ou suas famílias, a menos que a vítima pague uma quantia em dinheiro.

Vazamento de informações: O cibercriminoso ameaça vazar informações confidenciais da vítima, como dados bancários ou informações de clientes, a menos que a vítima pague uma quantia em dinheiro.

Ameaças de reputação: O cibercriminoso ameaça difamar a reputação da vítima ou da empresa, publicando informações falsas ou prejudiciais na internet, a menos que a vítima pague uma quantia em dinheiro.

Para evitar ser vítima de ciberextorsão, é importante adotar medidas de segurança cibernética, como manter softwares atualizados, evitar clicar em links suspeitos ou abrir anexos de e-mails de fontes desconhecidas, usar senhas fortes e fazer backups regulares de dados importantes. Em caso de ameaças de ciberextorsão, é importante reportar o incidente às autoridades e buscar a ajuda de profissionais de segurança cibernética.

Ataques do tipo DDoS

Um ataque DDoS (Distributed Denial of Service) é um tipo de ataque cibernético que tem como objetivo tornar um site, aplicativo ou serviço indisponível para seus usuários legítimos, sobrecarregando-o com um grande volume de tráfego ou solicitações de conexão. Esse ataque é chamado de distribuído porque é realizado por um grande número de dispositivos, que podem estar localizados em diferentes partes do mundo e que, muitas vezes, foram infectados por malware e controlados remotamente por um atacante.

Os ataques DDoS geralmente são realizados usando redes de bots, também conhecidas como botnets, que são formadas por dispositivos que foram comprometidos por hackers e que podem ser controlados remotamente. Esses dispositivos incluem computadores pessoais, servidores, roteadores, câmeras de vigilância e outros dispositivos conectados à internet, que são vulneráveis a ataques porque possuem senhas fracas ou não foram atualizados com os patches de segurança mais recentes.

Quando um ataque DDoS é lançado, a rede de bots começa a enviar uma grande quantidade de tráfego ou solicitações de conexão ao site ou serviço de destino. Isso pode fazer com que o site ou serviço fique indisponível para seus usuários legítimos, pois não é capaz de lidar com o volume de tráfego recebido.

Em alguns casos, o ataque pode ser tão intenso que pode derrubar os servidores que hospedam o site ou serviço.

Existem muitos ataques DDoS de grande escala que já ocorreram ao longo dos anos, mas é difícil determinar qual foi o maior de todos, pois esses ataques estão se tornando cada vez mais sofisticados e intensos. No entanto, citaremos alguns dos ataques DDoS mais notáveis:

• Ataque DDoS contra a provedora de serviços de DNS Dyn em 2016: Este foi um dos maiores ataques DDoS já registrados, que afetou grandes empresas, como Twitter, Netflix, Reddit, Amazon, entre outros, deixando esses serviços inacessíveis para seus usuários.

• Ataque DDoS contra o provedor de hospedagem OVH em 2016: Este foi um ataque DDoS extremamente poderoso, que chegou a alcançar 1,1 terabits por segundo, tornando-se o maior ataque DDoS registrado até então.

• Ataque DDoS contra a provedora de serviços de segurança Cloudflare em 2020: Este foi um ataque DDoS muito intenso que atingiu um pico de 17,2 milhões de solicitações por segundo.

• Ataque DDoS contra a provedora de serviços de hospedagem GitHub em 2018: Este foi um ataque DDoS poderoso que atingiu um pico de 1,35 terabits por segundo.

Esses são apenas alguns exemplos de ataques DDoS notáveis que ocorreram nos últimos anos. É importante destacar que, independentemente do tamanho do ataque, os danos causados por um ataque DDoS podem ser significativos e duradouros, por isso é importante que as empresas estejam preparadas e tenham medidas de segurança eficazes para lidar com esses tipos de ameaças.

Os ataques DDoS podem ser realizados por diversos motivos, incluindo ativismo político, vingança pessoal, extorsão, concorrência desleal ou simplesmente para fins maliciosos. Os efeitos de um ataque DDoS podem variar desde a interrupção temporária de um serviço até prejuízos financeiros significativos para as empresas que dependem do serviço atacado.

Para se proteger contra ataques DDoS, as empresas podem adotar medidas de segurança como a implementação de firewalls, sistemas de detecção de intrusões e serviços de proteção DDoS. Além disso, é importante manter os sistemas atualizados e usar senhas fortes para proteger os dispositivos conectados à internet.

A tal da Engenharia Social

A engenharia social é uma técnica de manipulação psicológica usada para convencer as pessoas a divulgar informações confidenciais ou realizar ações que possam colocar em risco sua segurança ou a segurança de uma organização. É uma forma de ataque cibernético que não envolve diretamente a exploração de vulnerabilidades técnicas, mas sim a exploração da confiança e da ingenuidade das pessoas.

A engenharia social pode ser realizada de várias maneiras, incluindo a criação de perfis falsos em redes sociais, envio de e-mails de phishing, ligações telefônicas fraudulentas, dentre outras técnicas. O objetivo é sempre enganar a vítima e convencê-la a fornecer informações confidenciais ou executar uma ação que possa comprometer sua segurança ou a segurança de uma organização.

Os golpistas geralmente usam táticas psicológicas para manipular as vítimas, como a criação de uma sensação de urgência ou medo, o estabelecimento de confiança, a exploração de emoções como curiosidade e ganância, e outras técnicas para persuadir as vítimas a tomar uma ação específica.

Alguns exemplos de engenharia social incluem:

• E-mails de phishing: os golpistas enviam e-mails falsos que parecem ser de uma empresa legítima, solicitando que a vítima forneça informações confidenciais, como senhas, informações bancárias ou detalhes de cartão de crédito.

• Spoofing de identidade: os golpistas podem falsificar o número de telefone ou o endereço de e-mail para fazer parecer que estão entrando em contato de uma fonte confiável, como um banco ou uma empresa.

• Engenharia social física: os golpistas podem se passar por um técnico de informática ou outro profissional para acessar fisicamente um computador ou rede e instalar malware ou roubar informações confidenciais.

Para evitar ser vítima de engenharia social, é importante estar ciente das técnicas utilizadas pelos golpistas e manter-se vigilante. Algumas medidas de proteção incluem não clicar em links suspeitos, não fornecer informações confidenciais por telefone ou e-mail e verificar a autenticidade da fonte antes de tomar qualquer ação. Além disso, a conscientização e o treinamento em segurança cibernética podem ajudar a reduzir o risco de ser enganado por golpistas que usam a engenharia social como técnica de ataque.

Enganando com um Phishing

Esse é um bom exemplo de Engenharia social: Phishing é uma forma de ataque cibernético em que um indivíduo mal-intencionado tenta enganar uma pessoa ou organização para obter informações confidenciais, como senhas, informações bancárias, números de cartão de crédito, entre outros dados.

O phishing geralmente envolve o envio de um e-mail falso ou uma mensagem de texto que parece legítima e solicita que o destinatário clique em um link, baixe um arquivo ou forneça informações pessoais ou financeiras. Essas mensagens são projetadas para se parecer com comunicações oficiais de uma empresa ou organização confiável, como um banco, rede social, site de comércio eletrônico, entre outros.

Ao clicar no link ou fornecer informações solicitadas, a vítima acaba sendo redirecionada para um site falso que parece idêntico ao site real, mas na verdade é controlado pelo invasor. Nesse site, a vítima é solicitada a inserir informações confidenciais, que são então capturadas pelo invasor e usadas para fins mal-intencionados.

Os ataques de phishing também podem incluir o uso de mensagens de voz falsas ou mensagens diretas em redes sociais, com o objetivo de obter informações pessoais ou financeiras.

Os ataques de phishing são um problema sério na segurança cibernética, pois são fáceis de serem realizados e podem ser extremamente eficazes para enganar as pessoas. Para se proteger, é importante estar atento às comunicações suspeitas e nunca fornecer informações pessoais ou financeiras por meio de um link enviado por e-mail ou mensagem de texto. Em vez disso, é recomendado que as pessoas acessem o site oficial diretamente digitando o endereço na barra de endereços do navegador.

Envenenamento de DNS

O envenenamento de DNS (Domain Name System) é um tipo de ataque cibernético em que o invasor manipula o sistema de nomes de domínio para direcionar os usuários para sites maliciosos ou para obter informações confidenciais.

O DNS é o sistema que traduz os nomes de domínio em endereços IP. Quando um usuário digita um endereço da web em um navegador, o computador usa o DNS para encontrar o endereço IP correspondente e, em seguida, se conecta ao servidor da web para carregar a página. Se um invasor conseguir comprometer o DNS, ele pode redirecionar o usuário para um site falso que parece legítimo, mas que na verdade é uma armadilha para roubar informações do usuário.

Existem vários métodos de envenenamento de DNS, mas um dos mais comuns é conhecido como "envenenamento de cache". Nesse método, o invasor aproveita uma vulnerabilidade no servidor DNS para inserir informações falsas na cache do servidor. Essas informações falsas podem direcionar os usuários para um site malicioso em vez do site real que eles estão tentando acessar.

Outro método é conhecido como "envenenamento de registro". Nesse método, o invasor envia uma solicitação de DNS falsa ao servidor, fingindo ser o site que o usuário está tentando acessar. O servidor responde à solicitação com o endereço IP falso, levando o usuário para um site malicioso.

Os ataques de envenenamento de DNS podem ser devastadores, pois podem afetar muitos usuários em uma ampla área geográfica. Além disso, esses ataques podem ser difíceis de detectar e corrigir, já que a manipulação do DNS pode não ser óbvia para os usuários ou administradores de rede.

O envenenamento de DNS no modem de internet pode ocorrer se o invasor conseguir acessar o modem e alterar suas configurações de DNS. Isso pode ser feito através de técnicas de phishing, engenharia social ou exploração de vulnerabilidades de segurança conhecidas no modem.

Uma vez que o invasor tenha acesso ao modem, ele pode alterar as configurações de DNS para direcionar o tráfego para servidores DNS maliciosos. Esses servidores podem então fornecer informações falsas de DNS para redirecionar os usuários para sites maliciosos ou para capturar informações confidenciais.

Para se proteger contra o envenenamento de DNS, é importante que as organizações implementem práticas de segurança fortes, como a criptografia de dados, a autenticação de usuários e o monitoramento contínuo do tráfego de rede. Os usuários individuais também podem se proteger usando softwares de segurança e evitando clicar em links suspeitos ou abrir anexos de e-mails de remetentes desconhecidos.

Para se proteger contra o envenenamento de DNS no modem de internet, é importante manter o modem atualizado com as últimas atualizações de segurança e alterar as credenciais de login padrão para credenciais fortes e exclusivas. Além disso, é recomendado desativar o acesso remoto ao modem, a menos que seja absolutamente necessário, e nunca clicar em links suspeitos ou abrir anexos de e-mails de remetentes desconhecidos.

Mercado de Trabalho

O mercado de trabalho na área de cibersegurança tem crescido rapidamente nos últimos anos, impulsionado pela crescente ameaça de ataques cibernéticos a empresas, organizações governamentais e indivíduos.

A demanda por profissionais qualificados em cibersegurança é alta e continua a aumentar à medida que as organizações buscam proteger seus sistemas e dados contra ameaças cada vez mais sofisticadas.

Algumas das profissões mais comuns em cibersegurança incluem:

Analista de segurança cibernética: responsável por monitorar e analisar o tráfego de rede para identificar possíveis ameaças e vulnerabilidades de segurança.

Especialista em segurança de rede: responsável por configurar e manter as defesas de segurança de rede, incluindo firewalls, sistemas de detecção de intrusos e sistemas de prevenção de intrusos.

Especialista em segurança de aplicativos: responsável por identificar vulnerabilidades de segurança em aplicativos e softwares e implementar medidas para corrigir essas vulnerabilidades.

Especialista em segurança em nuvem: responsável por garantir a segurança dos dados armazenados em serviços de nuvem, incluindo a proteção contra violações de dados e ataques de hackers.

Os profissionais de cibersegurança geralmente precisam ter habilidades técnicas avançadas em áreas como redes, sistemas operacionais, bancos de dados e programação, além de conhecimento em estratégias de defesa e gerenciamento de riscos. Eles também precisam estar atualizados com as últimas tendências e técnicas de ataques cibernéticos para garantir que suas habilidades e conhecimentos sejam relevantes e eficazes.

O mercado de trabalho em cibersegurança é altamente competitivo, mas oferece oportunidades de crescimento e desenvolvimento profissional significativos para aqueles que estão dispostos a investir tempo e esforço em sua formação e especialização.

O que é um PENTEST?

Pentest (ou teste de penetração) é uma atividade realizada por profissionais de segurança da informação para avaliar a segurança de um sistema, aplicativo ou rede. O objetivo do teste de penetração é identificar possíveis vulnerabilidades que possam ser exploradas por invasores mal-intencionados.

Durante o teste de penetração, o profissional de segurança da informação simula um ataque cibernético, usando técnicas de hacking para explorar vulnerabilidades no sistema alvo. Isso pode incluir a realização de uma variedade de testes, como:

Varreduras de portas: para identificar quais portas estão abertas em um sistema e determinar se alguma delas pode ser usada como uma entrada para um ataque.

Identificação de vulnerabilidades: o profissional de segurança da informação procura ativamente por vulnerabilidades conhecidas em sistemas, aplicativos ou redes, como falhas de segurança em sistemas operacionais, servidores web ou aplicativos web.

Testes de invasão de rede: o profissional de segurança da informação tenta acessar redes e sistemas usando técnicas de hacking, como sniffing de tráfego, ataques de negação de serviço (DoS) e ataques de força bruta para senhas.

Engenharia social: o profissional de segurança da informação pode tentar enganar usuários do sistema para obter informações confidenciais, como senhas ou dados de acesso.

Após a conclusão do teste de penetração, o profissional de segurança da informação relata suas descobertas ao proprietário do sistema, aplicativo ou rede. O relatório de pentest inclui uma descrição detalhada das vulnerabilidades encontradas e sugestões para corrigi-las. O objetivo final do teste de penetração é ajudar a fortalecer a segurança do sistema, aplicativo ou rede, para evitar ataques cibernéticos e proteger dados sensíveis.

Sendo um Hacker Ético

Tornar-se um hacker ético envolve uma combinação de habilidades técnicas e conhecimento em ética e responsabilidade. Aqui estão algumas etapas que você pode seguir para se tornar um hacker ético:

Aprenda habilidades técnicas: Você precisará aprender habilidades técnicas para entender como funciona a segurança da informação e como explorar vulnerabilidades. Isso inclui aprender programação, redes, sistemas operacionais e outros tópicos relacionados.

Obtenha certificações: Existem várias certificações disponíveis para profissionais de segurança da informação, como Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP) e Offensive Security Certified Professional (OSCP). Essas certificações ajudam a validar suas habilidades e conhecimentos em segurança da informação.

Estude ética: É importante entender o que é certo e errado quando se trata de segurança da informação. Leia e estude sobre ética e responsabilidade em segurança da informação para garantir que você esteja agindo de maneira ética em todas as suas atividades.

Pratique em laboratórios virtuais: Antes de realizar qualquer teste de penetração em um sistema real, é importante praticar em um ambiente controlado, como um laboratório virtual. Isso permite que você aprimore suas habilidades e técnicas sem causar danos a sistemas reais.

Trabalhe em projetos de código aberto: Participe de projetos de código aberto para obter experiência prática em segurança da informação. Isso também ajuda a construir sua reputação como um profissional de segurança da informação.

Faça um curso de hacker ético: Existem vários cursos disponíveis online que cobrem ética hacker. Esses cursos ensinam as habilidades e conhecimentos necessários para se tornar um hacker ético e incluem tópicos como análise de vulnerabilidades, teste de penetração e ética em segurança da informação.

Adquira experiência em segurança da informação: Trabalhe em um emprego ou estágio relacionado à segurança da informação para adquirir experiência prática em teste de penetração e outras áreas de segurança da informação.

Lembre-se sempre de agir com responsabilidade e ética em todas as suas atividades relacionadas à segurança da informação. É importante seguir as leis e regulamentos aplicáveis e respeitar a privacidade das pessoas.

Tipos de PENTEST

Os tipos de Pentest (Teste de Penetração) podem variar de acordo com a abordagem, o escopo e os objetivos. Aqui estão alguns exemplos:

Black Box Pentest: Nesse tipo de Pentest, o testador não tem conhecimento prévio da infraestrutura, sistemas ou aplicativos que serão testados. O objetivo é simular um ataque de um hacker mal-intencionado.

White Box Pentest: Nesse tipo de Pentest, o testador tem acesso total ao ambiente a ser testado, incluindo credenciais de login, diagramas de rede e outros detalhes técnicos. O objetivo é realizar testes mais precisos e aprofundados.

Grey Box Pentest: Nesse tipo de Pentest, o testador tem acesso limitado à infraestrutura ou aplicativo a ser testado. O objetivo é simular um ataque de um hacker que obteve acesso limitado, por exemplo, por meio de credenciais roubadas.

Physical Pentest: Nesse tipo de Pentest, o testador tenta invadir fisicamente um ambiente, como uma sala de servidores, para avaliar a segurança física.

Social Engineering Pentest: Nesse tipo de Pentest, o testador usa técnicas de engenharia social para tentar enganar os usuários ou funcionários da empresa, a fim de obter acesso não autorizado a sistemas ou informações.

Wireless Pentest: Nesse tipo de Pentest, o testador tenta invadir redes sem fio para avaliar a segurança do Wi-Fi e outros dispositivos sem fio.

Web Application Pentest: Nesse tipo de Pentest, o testador avalia a segurança de um aplicativo web, procurando por vulnerabilidades como injeção de SQL, cross-site scripting, etc.

Mobile Application Pentest: Nesse tipo de Pentest, o testador avalia a segurança de um aplicativo móvel, procurando por vulnerabilidades como injeção de código malicioso, armazenamento de senhas em texto simples, etc.

Cloud Pentest: Nesse tipo de Pentest, o testador avalia a segurança de uma infraestrutura em nuvem, como AWS, Azure ou Google Cloud, buscando vulnerabilidades que possam comprometer a segurança dos dados armazenados.

A escolha do tipo adequado depende do objetivo e do escopo do teste de segurança a ser realizado.

Diferenças entre PENTEST e Análise de Vulnerabilidades

Pentest e Análise de Vulnerabilidades são duas técnicas de segurança cibernética distintas, embora complementares, com diferenças significativas entre si. Aqui estão algumas das principais diferenças entre os dois:

Escopo: A Análise de Vulnerabilidades concentra-se em identificar e documentar vulnerabilidades em um sistema, aplicativo ou rede, enquanto o Pentest procura explorar essas vulnerabilidades para determinar se é possível comprometer a segurança do sistema.

Objetivo: O objetivo da Análise de Vulnerabilidades é fornecer uma lista de vulnerabilidades identificadas para que a equipe de segurança possa corrigi-las. Já o objetivo do Pentest é avaliar a capacidade de defesa do sistema e fornecer informações sobre a eficácia das medidas de segurança existentes.

Metodologia: A Análise de Vulnerabilidades geralmente é um processo automatizado, que usa ferramentas de software para identificar vulnerabilidades conhecidas. O Pentest, por outro lado, usa uma metodologia mais manual e personalizada, com testadores de segurança usando técnicas de hacking para identificar e explorar vulnerabilidades que podem não ser detectadas por ferramentas automatizadas.

Envolvimento Humano: A Análise de Vulnerabilidades pode ser realizada sem a necessidade de envolvimento humano, pois é feita principalmente por meio de ferramentas de software automatizadas. O Pentest, por outro lado, envolve testadores humanos que usam técnicas criativas e personalizadas para avaliar a segurança do sistema.

Resultados: A Análise de Vulnerabilidades geralmente produz uma lista de vulnerabilidades identificadas, enquanto o Pentest produz um relatório mais completo, que inclui uma avaliação da segurança geral do sistema, bem como recomendações para melhorias.

Em resumo, a Análise de Vulnerabilidades e o Pentest são técnicas distintas, com objetivos e metodologias diferentes. Enquanto a Análise de Vulnerabilidades é usada principalmente para identificar vulnerabilidades, o Pentest é usado para avaliar a capacidade de defesa do sistema contra ataques reais. Ambos são importantes para garantir a segurança cibernética de uma organização e devem ser usados em conjunto como parte de uma abordagem abrangente de segurança cibernética.

Como fazer um PENTEST

Já foi demonstrado nesse e-book que o PENTEST, ou teste de penetração, é um processo utilizado para avaliar a segurança de um sistema, aplicativo ou rede, simulando um ataque real com o objetivo de identificar vulnerabilidades e fraquezas que possam ser exploradas por hackers ou outros invasores. Para fazer um PENTEST corretamente, siga estas etapas:

Definir o escopo: Determine o que será testado, incluindo o tipo de sistema, aplicação ou rede, bem como o alcance do teste.

Coletar informações: É importante coletar informações sobre o sistema ou aplicativo que será testado. Esta etapa envolve a busca de informações como endereços IP, URLs, nome de usuário, senhas e outras informações relevantes que possam ajudar a realizar um teste mais completo.

Identificar vulnerabilidades: Nesta etapa, o objetivo é identificar vulnerabilidades no sistema ou aplicativo. Os testadores devem usar ferramentas e técnicas para explorar vulnerabilidades conhecidas e desconhecidas e avaliar a sua gravidade e impacto potencial.

Explorar vulnerabilidades: Esta é a etapa onde os testadores tentam explorar as vulnerabilidades identificadas para determinar se elas podem ser efetivamente exploradas por um invasor.

Relatar resultados: Os testadores devem documentar todas as vulnerabilidades encontradas e suas respectivas recomendações para correção. O relatório deve incluir uma descrição detalhada dos problemas encontrados, bem como informações sobre como corrigi-los.

Validar correções: Após as vulnerabilidades serem corrigidas, é importante validar que as correções foram efetivas e que as vulnerabilidades foram remediadas corretamente.

Além disso, é importante que o PENTEST seja realizado por profissionais qualificados e experientes em segurança da informação e que siga as normas e boas práticas estabelecidas pelo mercado, como a norma NIST SP 800-115 ou a metodologia OWASP Testing Guide.

Para realizar um PENTEST de qualidade, algumas dicas preciosas devem ser seguidas.

Antes de iniciar o pentest, certifique-se de entender completamente o escopo do teste, incluindo os sistemas, aplicativos e redes que serão testados, bem como as restrições e limitações de tempo e recursos.

Utilize uma metodologia de teste bem definida, como a metodologia OWASP Testing Guide ou a norma NIST SP 800-115, para garantir que o teste seja completo e abranja todas as áreas necessárias.

Antes de iniciar o teste, faça uma análise de risco e identifique as principais ameaças e vulnerabilidades que o sistema pode enfrentar. Isso pode ajudar a focar os esforços do teste e priorizar as áreas mais críticas.

Embora as ferramentas de varredura automatizadas possam ajudar a identificar vulnerabilidades comuns, é importante que os testadores realizem testes manuais para encontrar vulnerabilidades mais avançadas e não detectadas por ferramentas automatizadas.

Mantenha um registro detalhado de todas as etapas do teste, desde a coleta de informações até a exploração de vulnerabilidades e documentação das descobertas. Isso pode ajudar a garantir que todas as vulnerabilidades sejam corrigidas e evitar problemas futuros.

Após concluir o teste, é importante relatar as descobertas de maneira clara e objetiva, destacando as vulnerabilidades encontradas e fornecendo recomendações para corrigi-las.

Certifique-se de seguir as melhores práticas de segurança durante todo o processo de pentest, incluindo o uso de senhas seguras, autenticação de dois fatores, criptografia de dados e outras medidas de segurança.

Conclusão

É importante destacar que o e-book do treinamento "Fundamentos de Cibersegurança" da Academia de Forense Digital é uma excelente introdução ao mundo da cibersegurança, cobrindo os principais conceitos e práticas para proteger sistemas e redes contra ataques cibernéticos. Este treinamento fornece aos alunos uma base sólida para avançar em sua carreira em cibersegurança.

No entanto, a cibersegurança é uma área em constante evolução, com novas ameaças e vulnerabilidades surgindo regularmente. É por isso que a Academia de Forense Digital oferece cursos adicionais, como o "Cyber Security Essentials" e o "Cyber Security Pentest", para ajudar os profissionais de segurança a se manterem atualizados com as últimas tendências em cibersegurança.

No curso "Cyber Security Essentials", os alunos aprendem sobre as ameaças mais comuns em cibersegurança, incluindo malware, phishing, ransomware e engenharia social, bem como as melhores práticas para prevenir e mitigar essas ameaças. Aprende também a explorar vulnerabilidades de ambiente Windows, Linux, Wifi, e ambientes WEB.

Já o curso "Cyber Security Pentest" fornece aos alunos uma visão aprofundada do teste de penetração, uma técnica utilizada para avaliar a segurança de sistemas e redes, simulando ataques cibernéticos para identificar vulnerabilidades e fraquezas.

Convidamos você a explorar os cursos adicionais oferecidos pela Academia de Forense Digital para aprimorar suas habilidades em cibersegurança e se tornar um profissional mais completo na área. Com nossos cursos, você terá acesso a instrutores experientes e a um conteúdo atualizado, para se manter à frente das ameaças em constante evolução do mundo cibernético.

Referências Bibliográficas

• "Cibersegurança: Como se proteger em um mundo conectado" de Daniela Costa e Juliana Nolasco (Editora Alta Books, 2021).

• "Fundamentos de Segurança da Informação: com base na ISO 27001 e ISO 27002" de Vinicius Serafim (Editora Brasport, 2019).

• "Segurança em Redes de Computadores e Internet: Fundamentos, Tecnologias e Protocolos" de Paulo Lício de Geus (Editora Bookman, 2016).

• "Manual Prático de Segurança da Informação: Fundamentos, Normas e Padrões Internacionais" de José Eduardo Cavalcanti e Vanessa Andrea de Oliveira (Editora Brasport, 2019).

• "Cybersecurity: Guia prático para proteger sua empresa contra ataques cibernéticos" de Marcos Mazzoncini (Editora Novatec, 2019).

• "OPENAI. ChatGPT: modelo de linguagem natural". Disponível em: https://openai.com/. Acesso em: 01 mar. 2023.

O MAIOR CENTRO DE TREINAMENTOS EM FORENSE DIGITAL DO PAÍS

Acesse nosso site
www.academiadeforensedigital.com.br