Primeira Edição

Segurança cibernética

Grupo 12

Conteúdo

Introdução

Privacidade e segurança não são opostos; são dois lados da mesma moeda.
–Sebastian Thrun

Capítulo 1

Definição de Hacker

Um hacker é um indivíduo com profundo conhecimento em computação e tecnologia, utilizando suas habilidades para encontrar soluções inovadoras para problemas complexos. No entento, é crucial distinguir entre hackers éticos e mal-intecionados.

O termo "hacker"teve origem na década de 1970, associado aos primeiros programadores que desenvolviam softwares e sistemas complexos. A popularização do termo, inclusive com conotação

negativa, foi impulsionada por filmes como "Tron"e "WarGames"na década de 1980. Nessa época, surgiram os primeiros ataques cibernéticos a grandes organizações, levando à criação de leis sobre crimes de informática.

Temos alguns tipos de hackers:

White Hat (Ético): São especialistas em segurança da computação que realizam testes de invasão autorizados para encontrar e corrigir vulnerabilidades em sistemas. Eles geralmente, atuam como "mocinhos"da cibersegurança, contratados por empresas para fortalecer suas defesas. Um exemplo de ataque realizado por White Hats foi descoberta do bug Heartbleed no OpenSSL em 2014, que permitia o roube de informações confidencias de sites.

Black Hat (Malicioso): Invadem sistemas com intenções criminosas, visando lucro, diversão ou motivações políticas. Seus ataques podem envolver modificação de dados, distribuição de vírus e roubo de informações. São considerados os "vilões"da

cibersegurança e estão sujeitos a punições legais. O ataque de ransomware WannaCry em 2017, que afetou milhares de computadores globalmente, é um exemplo de Black Hat.

Grey Hat (Neutro): Atuam em uma área cinzenta, explorando vulnerabilidades sem autorização, mas sem intenções maliciosas. Podem invadir sistemas por curiosidade ou para alertar sobre falhas de segurança, mas suas ações podem ser consideradas ilegais. Um exemplo é o caso de Khalil Sreateh, que invadiu uma página do Facebook em 2013 para expor uma falha de segurança.

Script Kiddies: São hackers inexperientes que utilizam ferramentas e scripts desenvolvidos por outros, sem profundo conhecimento dos sistemas que atacam. Motivados por exibicionismo ou diversão, seus ataques geralmente têm impacto limitado.

Hacktivistas: Motivados por causa políticas ou sociais, usam suas habilidades para promover

suas ideologias. Seus alvos podem ser governos, organizações ou movimentos sociais.

Ética em Cibersegurança: A ética é fundamental na segurança da informação, guiando o comportamento e as decisões dos profissionais da área. Profissionais de cibersegurança tem acesso a informações confidenciais e devem agir com responsabilidades.

Princípios Éticos: Confidencialidade, Integridade e Responsabilidade.

Capítulo 2

Profissões da Cibersegurança

Red Team: Simulam ataques cibernéticos realísticos para identificar vulnerabilidades nos sistemas de uma empresa. Seu objetivo é avaliar a postura de segurança da empresa e auxiliar na melhoria das defesas. As atividades do Red Team são dividas em planejamento, execução, análise e recomendação.

Blue Team: Defendem ativamente os sistemas de uma organização contra ataques cibernéticos, monitorando, detectando, respondendo e mitigando ameaças. Seu foco é garantir a segurança, a confidencialidade, a integridade e a disponibilidade das informações. Suas atividades incluem monitoramento constante dos sistemas, detecção de ataques, resposta a incidentes e implementação de medidas de mitigação.

Forense Digital: Especialistas em investigar incidentes de segurança cibernética, analisando evidências digitais para rastrear autores e vítimas. Coletam, preservam, analisam e apresentam evidências digitais de forma válida e confiável. Seu trabalho é crucial para a aplicação da lei e da justiça no âmbito digital.

GRC (Governança, Risco e Conformidade: Profissionais que integram e otimizam os processos de cibersegurança nas empresas, garantindo a conformidade com leis, regulamentos e normas. Atuam

nas áreas de governança, risco e conformidade, definindo políticas, avaliando riscos e garantindo a conformidade com os requisitos legais.

DevSecOps: Integram a segurança em todas as etapas do ciclo de vida de desenvolvimento de software, automatizando a segurança e promovendo a colaboração entre equipes. Atuam nas áreas de desenvolvimento, segurança e operações, aplicando práticas e princípios de segurança por design e por padrão.

Capítulo 3

Conceitos Iniciais e Ameaças Cibernéticas

Vírus: Software malicioso que se replica e pode causar diversos danos, como corromper dados, apagar arquivos e causar lentidão no sistema.

Exemplos:

– Vírus de Boot: Infectam o setor de inicialização

do disco rígido.
– Vírus de Macro: Infectam arquivos que contêm macros, como documentos do Word ou Excel.
– Vírus Residentes: Permanecem na memória do computador, infectando outros programas.
– Vírus Polimórficos: Alteram seu código a cada replicação, dificultando a detecção.
– WannaCry: Ransomware que criptografa arquivos e exige pagamento em criptomoedas.
– ILOVEYOU: Espalhado por e-mail, replicava-se para todos os contatos da vítima.
– Stuxnet: Atacava sistemas de controle industrial, como usinas nucleares.

Como é transmitido:

É transmitido através de arquivos suspeitos, links maliciosos, dispositivos removíveis, downloads de fontes não confiáveis e brechas de segurança em softwares.

Medidas Preventivas:

– Usar um antivírus atualizado e confiável.
– Evitar abrir arquivos ou clicar em links suspeitos.
– Escanear dispositivos removíveis antes de usá-los.
– Fazer downloads apenas de fontes confiáveis.
– Manter os sistemas e softwares atualizados.
– Fazer backup de dados importantes.
– Desconfiar de e-mails suspeitos.

SPAM

Mensagem eletrônica não solicitada enviada em massa, geralmente com fins publicitários ou fraudulentos. Considerado uma forma de poluição digital, pode ser usado para espalhar malwares.

Spyware

Programa malicioso que se instala no computador e monitora as atividades do usuário sem seu consentimento, coletando informações pessoais e

confidenciais.

Worms

Semelhante a um vírus, mas com a capacidade de se replicar e propagar de forma independente, explorando vulnerabilidades em sistema e redes.

Phishing

Técnica que usa a engenharia social para enganar usuários, induzindo-os a fornecer informações confidencias, como senhas e dados bancários, por meio de e-mails, mensagens ou sites falsos.

Botnet

Rede de computadores infectados por malware, controlados remotamente por um cibercriminoso para realizar atividades maliciosas, como ataques DDoS e envio de SPAM.

Rootkit

Malware sofisticado que se instala no sistema operacional, obtendo acesso privilegiado e ocultando sua presença, permitindo o controle remoto do sistema e o roube de informações.

Cavalo de Troia

Disfarçado de um programa legítimo, engana o usuário para que o instale, abrindo portas para outros malwares ou permitindo o acesso remoto ao sistema.

Ransomware

Bloqueia o acesso aos dados ou ao dispositivo da vítima, exigindo um resgate para a liberação, geralmente em criptomoedas.

Engenharia Social

Usa técnicas de manipulação psicológica para en-

ganar pessoas, explorando suas emoções e confiaça para obter informações confidencias ou acesso a sistemas.

Capítulo 4

Como se Proteger

É fundamental estar ciente dos riscos online e das melhores práticas de segurança, educando e sensibilizando as pessoas sobre as ameaças e medidas de proteção. Adotar medidas preventivas ajudam a fortalecer a segurança digital. Veja algumas abaixo:

– Usar senhas fortes e únicas para cada conta ou serviço.
– Ativar a autenticação de dois fatores para uma camada extra de segurança.

– Manter os sistema operacionais, navegadores e aplicativos atualizados.
– Instalar um antivírus confiável em todos os dispositivos.
– Evitar clicar em links ou abrir anexos suspeitos, verificando a origem e a autenticidade dos mensagens.
– Usar redes Wi-Fi seguras e evitar redes públicas ou abertas, utilizando uma VPN para proteger a conexão.
– Fazer backup de dados importantes regularmente, armazenando-os em um local seguro.

Veja abaixo, algums dicas de como implementar as boas práticas de segurança em etapas:

– Avaliar a exposição a ameaças, identificando dados sensíveis, dispositivos utilizados, serviços online e os riscos mais prováveis.
– Escolher medidas de proteção adequadas às necessidades, considerando o tipo de atividade online, o orçamento, a complexidade da rede e os resultados esperados.

– Implementar e monitorar as medidas de proteção, instalando, configurando e revisando continuamente as medidas de segurança.