Hacking

Além dos Códigos: Navegando no Mundo do Hacking com Segurança e Expertise

Dedicatória

Quero agradecê-lo e parabenizá-lo por adquirir esse livro "Além dos Códigos: Navegando no Mundo do Hacking com Segurança e Expertise".

Este livro ensinará como você pode se proteger dos ataques de hacking mais comuns - sabendo como o hacking realmente funciona! Afinal de contas, para evitar que seu sistema seja comprometido, você precisa estar um passo à frente de qualquer hacker criminoso. Você pode fazer isso aprendendo como hackear e como fazer um contra-hack.

Neste livro, há técnicas e ferramentas usadas por hackers criminosos e éticos - tudo o que você encontrará aqui mostrará como a segurança das informações pode ser comprometida e como você pode identificar um ataque em um sistema que está tentando proteger. Ao mesmo tempo, você também aprenderá como minimizar os danos ao seu sistema ou interromper um ataque em andamento.

Obrigado por fazer o adquirir esse livro. Espero que você goste dele!

Índice

Introdução Sumário

- - - - X

Capítulo 1: Hacking 101

- - - - X

Sempre que você se depara com a palavra hacking, provavelmente a associa ao envio de um programa criptografado para outro usuário e, em seguida, conseguir acesso não autorizado a um computador remoto.

No entanto, o termo hacking era utilizado para definir qualquer ato de mexer no hardware ou software de um computador além de seu uso pretendido, a fim de aprimorá-lo e descobrir como os dispositivos eletrônicos podem funcionar eletronicamente.

Embora essa definição tecnicamente ainda seja válida, o hacking definitivamente tomou um rumo completamente novo, especialmente quando se trata de como uma pessoa pode acessar o computador de outra pessoa. Antes de pensar que o hacking se resume a superar seguranças para causar estragos no dispositivo digital de outra pessoa, você pode precisar saber sobre os tipos de hackers que existem nos dias de hoje.

Quem Hackeia?

Hackers são tipicamente divididos nas seguintes categorias:

Hackers black hat

Também conhecidos como hackers criminosos ou crackers, essas pessoas são aquelas que obtêm acesso malicioso a outro sistema de uma pessoa para ganho próprio. Eles geralmente invadem dispositivos eletrônicos e modificam, roubam ou excluem arquivos críticos para seu benefício pessoal.

Hackers white hat

Hackers white hat, ou hackers éticos, descobrem maneiras de explorar o sistema de um dispositivo para aprender como as pessoas podem se defender contra possíveis ataques. Esses hackers éticos também se certificam de que os serviços de segurança que eles emitem estão atualizados. Eles fazem isso ficando de olho e procurando ativamente por novas explorações e novas vulnerabilidades do sistema.

Hackers éticos também se certificam de descobrir novas maneiras de aprender como um dispositivo eletrônico pode ser manipulado para maximizar sua eficiência. Por esse motivo, eles constroem comunidades que lhes permitem compartilhar seu conhecimento para melhorar a forma como as pessoas usam seus dispositivos.

Hackers grey hat

Como o nome sugere, eles são motivados por hacking white hat e black hat - são aqueles que empregam tanto técnicas ilegais quanto legais para explorar ou melhorar um sistema. No entanto, se um hacker grey hat explora o sistema de outra pessoa, ele geralmente se certifica de informar o proprietário das explorações feitas e, em seguida, oferece sugestões sobre o que pode ser feito para reforçar a segurança do sistema. Depois de conseguir identificar os hackers que você provavelmente encontrará, você será capaz de entender a

motivação que eles têm para hackear e os tipos de hacks que eles provavelmente criarão.

Hacking é para Todos?

Embora o hacking seja geralmente atribuído a pessoas que sabem programar, qualquer pessoa pode aprender a hackear. Ao

mesmo tempo, é importante ter em mente que não há uma única maneira de aprender a hackear - hacks para melhorar ou atacar sistemas são

criados por meio da evolução contínua do conhecimento do usuário sobre como um sistema deve funcionar. Enquanto você lê isso, pode contar com a possibilidade de que uma nova maneira de proteger ou atacar um dispositivo ou rede já tenha sido criada.

Se você tem um computador ou um telefone celular, então você é o melhor candidato a ser um hacker. Você tem a motivação certa para aprender a mexer com um sistema e melhorar a forma como o usa. Como você conecta com outros usuários por meio de downloads, mensagens, compras online ou uploads, você precisa prestar atenção especial em como pode proteger seu próprio sistema. Para fazer isso, você precisa aprender como um hacker black hat pensa, começando pela motivação que eles têm ao atacar um sistema, até os rudimentos de um ataque. A partir desse ponto, você entenderá que tem muitas medidas preventivas quando se trata de impedir uma invasão não autorizada e até mesmo lançar um contra-ataque.

O Que Você Obterá Aqui?

Este livro lhe fornecerá informações sobre as estratégias comumente utilizadas por hackers black hat, o que permitirá que você teste as vulnerabilidades do seu próprio sistema e como você pode cair em diferentes armadilhas preparadas para a maioria dos usuários por aí. Aqui, você aprenderá como as pessoas se tornam candidatas a se tornarem vítimas potenciais de hackers criminosos e como você pode se proteger contra tais ataques. Neste ponto, você entende a ideia - está a caminho de se tornar um hacker ético.

Como sua principal preocupação é a sua própria segurança e garantir que você compreenda por que os ataques ocorrem através de diferentes sistemas, você também precisará aprender como os ataques são realizados inicialmente. Você será capaz de entender como hackers criminosos penetram em dispositivos aprendendo ferramentas, técnicas e ataques que eles usam em sua área. Uma vez que você compreende como um dispositivo eletrônico pode ser comprometido, terá uma ideia melhor do que pode fazer para evitar que isso aconteça.

É Difícil Aprender e Entender?

Embora o hacking exija **muita** prática, não é uma atividade difícil de se envolver. Contanto que você saiba como usar um computador e consiga seguir as instruções que encontrará neste livro, poderá testar ou até mesmo realizar hacks que você lerá nos capítulos posteriores.

Se você ainda não sabe programar, não se preocupe – encontrará instruções detalhadas sobre qual software de codificação, sistema operacional e outros mais adiante. No entanto, se você deseja se destacar no hacking e quer desenvolver suas próprias medidas de segurança ou testar uma versão de um ataque, então ter habilidades de codificação é essencial.

Habilidades Necessárias

Para se tornar um bom hacker ético, você precisa ter as seguintes habilidades:

Habilidades intermediárias em informática

Isso significa que você precisa ter habilidades que vão além de criar um documento do Word ou apenas navegar na internet. Para ser um hacker, você precisa saber como usar diferentes linhas de comando do Windows, configurar uma rede ou editar o registro do seu computador.

Boas habilidades em redes

Como muitos, se não a maioria, dos ataques de hackers são realizados online, você precisa dominar conceitos e termos de redes, como:

- Senhas WEP vs WPS
- NAT
- Endereços MAC
- Roteadores
- Portas

- VPN
- IPv6
- DNS
- Sub-rede
- DHCP
- IPs privados e públicos
- IPv4
- Modelagem OSI
- Pacotes
- TCP/IP

Uso de um sistema operacional Linux

Quase todos os hackers terão que usar o sistema operacional Linux, pois ele permite programas e ajustes que não são possíveis nos sistemas operacionais Windows e Mac. Quase todas as ferramentas de hacking que você pode encontrar também fazem uso desse sistema operacional.

Virtualização

Antes mesmo de tentar testar um ataque em um sistema ao vivo, você precisa ter certeza de que sabe o que está fazendo. Para garantir que está fazendo as coisas certas, talvez queira experimentar um hack primeiro em um pacote de software de virtualização, como o Workstation. Usar estações de trabalho virtuais fornecerá um ambiente seguro para seus testes de hack e impedirá que você cause danos ao seu dispositivo involuntariamente.

Tcpdump ou Wireshark

O tcpdump é conhecido como um analisador de protocolo de linha de comando ou um sniffer, enquanto o Wireshark é conhecido como a ferramenta mais popular disponível que realiza a mesma função.

Conhecimento em Tecnologias e Conceitos de Segurança

Qualquer hacker deve ser capaz de entender os conceitos e tecnologias mais importantes relacionados à tecnologia da informação. Por esse motivo, você precisa estar familiarizado com a tecnologia e conceitos sem fio, como Secure Sockets Layer (SSL), firewalls, Intrusion Detection System (IDS), Public Key Infrastructure (PKI) e assim por diante.

Habilidades de Scripting

Ter a capacidade de criar e editar scripts permite que você crie suas próprias ferramentas e consiga ser independente das ferramentas desenvolvidas por outros hackers. Ao ser capaz de construir suas próprias ferramentas, você se capacita a desenvolver defesas melhores à medida que hackers criminosos criam hacks mais avançados. Para fazer isso, você precisa tornar-se proficiente em pelo menos uma das linguagens de script comumente usadas, como Ruby on Rails ou Python.

Habilidades em Banco de Dados

Se você quiser entender como os hackers infiltram os bancos de dados do seu sistema, precisa garantir que sabe como os bancos de dados funcionam. Isso significa que você precisa dominar um sistema de gerenciamento de banco de dados, como Oracle ou MySQL.

Engenharia Reversa

A engenharia reversa permite que você converta um pedaço de malware ou um exploit semelhante em uma ferramenta de hacking mais avançada. Com essa habilidade, vem a compreensão de que quase todos os exploits feitos por hackers derivam de outros exploits existentes - uma vez que você entende como funciona um recurso de malware ou exploit, terá uma compreensão melhor de como outros hacks funcionam contra um sistema.