TÉCNICAS DE INVASÃO

APRENDA AS TÉCNICAS USADAS POR HACKERS EM INVASÕES REAIS_

CRIADO POR
BRUNO FRAGA

EDITORA Labrador

TÉCNICAS DE
INVASÃO

CRIADO POR
BRUNO FRAGA

TÉCNICAS DE INVASÃO

APRENDA AS TÉCNICAS USADAS POR HACKERS EM INVASÕES REAIS_

Compilação
Thompson Vangller

EDITORA Labrador

Coordenação editorial
Erika Nakahata

Preparação de texto
Leonardo do Carmo

Projeto gráfico, diagramação e capa
Maurelio Barbosa

Revisão
Maurício Katayama

Dados Internacionais de Catalogação na Publicação (CIP)
Angélica Ilacqua CRB-8/7057

Fraga, Bruno

Técnicas de invasão : aprenda as técnicas usadas por hackers em invasões reais / Bruno Fraga ; compilação de Thompson Vangller. – São Paulo : Labrador, 2019.
296 p.

ISBN 978-65-5044-019-0

1. Hackers 2. Computadores – Medidas de segurança 3. Redes de computadores – Medidas de segurança I. Título II. Vangller, Thompson.

19-2005 CDD 005.8

Índice para catálogo sistemático:
1. Computadores : Técnicas de invasão

Editora Labrador
Diretor editorial: Daniel Pinsky
Rua Dr. José Elias, 520 – Alto da Lapa
05083-030 – São Paulo – SP
Telefone: +55 (11) 3641-7446
contato@editoralabrador.com.br

www.editoralabrador.com.br
facebook.com/editoralabrador
instagram.com/editoralabrador

Hello, friend!

AGRADECIMENTOS

À minha filha, Alice, que me deu todo o impulso para chegar até aqui. Aos meus pais, que me criaram com carinho e amor. À minha esposa, Beatriz, por sempre me apoiar e perder várias noites de sono comigo. E ao Bruno Fraga, por ter aparecido em minha vida como um coelho branco que eu decidi seguir.

Thompson Vangller
Aluno e compilador do livro, com base no Treinamento

Morpheus: Finalmente. Bem-vindo, Neo. Como você deve ter imaginado, eu sou Morpheus.

Neo: É uma honra conhecê-lo.

Morpheus: Não, a honra é minha. Por favor, venha. Sente-se. Eu imagino que deva estar se sentindo um pouco como Alice. Escorregando pela toca do coelho... Hum?

Neo: É, eu acho que sim.

Morpheus: Vejo isso em seus olhos. Você é um homem que aceita o que vê, porque pensa estar sonhando. Ironicamente, não está muito longe da verdade. Você acredita em destino, Neo?

Neo: Não.

Morpheus: Por que não?

Neo: Porque eu não gosto da ideia de não poder controlar a minha vida.

Morpheus: Eu sei exatamente o que quer dizer. Deixe que eu diga por que está aqui. Está aqui porque sabe de alguma coisa, uma coisa que não sabe explicar, mas você sente. Você sentiu a vida inteira que há alguma coisa errada com o mundo... você não sabe o que é, mas está ali, como uma farpa em sua mente, deixando-o louco. Foi essa sensação que o trouxe a mim. Você sabe do que eu estou falando?

Neo: Matrix?

Morpheus: Você quer saber o que é Matrix? Matrix está em toda parte. Está à nossa volta. Mesmo agora, nesta sala aqui. Você a vê quando olha pela janela ou quando liga a televisão. Você a sente... quando vai trabalhar, quando vai à igreja, quando paga seus impostos. É o mundo que acredita ser real para que não perceba a verdade.

Neo: Que verdade?

Morpheus: Que você é um escravo, Neo. Como todo mundo, você nasceu em cativeiro. Nasceu numa prisão que não pode ver, sentir ou tocar. Uma prisão... para a sua mente. Infelizmente, não se

pode explicar o que é Matrix. É preciso que veja por si mesmo. Esta é a sua última chance. Depois disto, não haverá retorno.

[*Morpheus abre a mão esquerda, revelando a pílula azul.*]

Morpheus: Se tomar a pílula azul, fim da história. Vai acordar em sua cama e acreditar no que você quiser.

[*Morpheus abre a mão direita, revelando a pílula vermelha.*]

Morpheus: Se tomar a pílula vermelha, fica no País das Maravilhas, e eu vou mostrar até onde vai a toca do coelho.

[*Neo pega a pílula vermelha.*]

Morpheus: Lembre-se – eu estou oferecendo a verdade, nada mais.

[*Neo toma a pílula vermelha.*]

Morpheus: Venha comigo.

The Matrix – Adentrando a Toca do Coelho

COMENTÁRIOS DO COMPILADOR

Construí esta obra a partir das videoaulas do curso online Técnicas de Invasão e de pesquisas realizadas na internet. As informações coletadas de fontes externas foram modificadas para melhor entendimento do leitor. A citação da fonte pode ser encontrada no rodapé da página.

O propósito desta obra é o de servir como um guia à introdução de Pentest, podendo ser utilizado também como um manual de consulta para realizar ataques clássicos.

O que realmente espero é que o leitor entenda a essência dos acontecimentos e o modo como o atacante pensa, pois as metodologias e ferramentas utilizadas podem mudar com o tempo, já que, todos os dias, novas atualizações de segurança surgem e novas vulnerabilidades são descobertas.

Sobre o *Técnicas de Invasão*

O Técnicas de Invasão é um projeto idealizado por Bruno Fraga. O objetivo do projeto é conscientizar o leitor sobre os riscos e ameaças existentes no mundo virtual e oferecer cursos altamente desenvolvidos para introdução de testes de invasão.

Apresenta, de modo inteligente e organizado, todo o processo de uma invasão, desde o princípio, e ensina passo a passo as metodologias e técnicas clássicas utilizadas por hackers. Além disso, busca alertar o aluno sobre riscos, apresentando dicas de proteção e pensamentos de hackers maliciosos.

O que há neste livro?

Este livro cobre as metodologias e técnicas clássicas empregadas por hackers, utilizando ferramentas do Kali Linux e outras ferramentas disponíveis na web, como o Shodan, Censys, Google Hacking etc.

Quem deve ler este livro?

Este livro é destinado a profissionais de segurança da informação, administradores de sistemas, engenheiros de software, profissionais de TI que buscam o conhecimento em técnicas de invasão, curiosos e pessoas que desejam iniciar uma carreira em TI.

O que é necessário para realizar os testes?

Para aprender de maneira eficiente todo o conhecimento que o livro apresenta e realizar os testes, é necessário ter:

- uma máquina virtual/física com o sistema operacional Kali Linux;
- uma máquina virtual/física com o sistema operacional Windows;
- uma máquina virtual/física com o sistema operacional Metasploitable;
- acesso à internet.

Recomenda-se, também, que o leitor tenha conhecimento básico de comandos Linux.

Observação

Cuidado com as aplicações dos conhecimentos ensinados neste livro, pois o uso de muitas ferramentas, técnicas e metodologias ensinadas aqui pode levar à prisão do indivíduo que as executou.

Realize os testes em um ambiente em que você seja o responsável e tenha controle, por exemplo, utilizando máquinas virtuais, rede LAN, seu IP público e domínio.

Na criação deste livro, o uso dessas ferramentas não infringiu nenhuma lei.

SUMÁRIO

APÊNDICES

D. CÓDIGOS DE STATUS ICMP

Segurança da informação[1] está relacionada à proteção de um conjunto de dados, no sentido de preservar o valor que esses dados possuem para um indivíduo ou uma organização.

São características básicas da segurança da informação os atributos de *confidencialidade*, *integridade* e *disponibilidade*, não estando essa segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

O conceito de segurança de computadores está intimamente relacionado ao de segurança da informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Atualmente, o conceito de segurança da informação está padronizado pela norma *ISO/IEC 17799:2005*, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas *ISO/IEC 27000* foi reservada para tratar de padrões de segurança da informação, incluindo a complementação

ao trabalho original do padrão inglês. A *ISO/IEC 27002:2005* continua sendo considerada formalmente como *17799:2005* para fins históricos.

Conceitos

A segurança da informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa; isto é, aplica-se tanto às informações corporativas como às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isso, ser estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem a utiliza, pelo ambiente ou infraestrutura que a cerca, ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (confidentiality, integrity and availability) – *confidencialidade, integridade* e *disponibilidade* – representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a *irretratabilidade* e a *autenticidade*.

Com o evoluir do comércio eletrônico e da sociedade da informação, a privacidade também se tornou uma grande preocupação.

Os atributos básicos (segundo os padrões internacionais) são os seguintes:

Confidencialidade – propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Integridade – propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

Disponibilidade – propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários

autorizados pelo proprietário da informação.

O nível de segurança desejado pode se consubstanciar em uma *política de segurança* que é seguida pela organização ou pessoa, para garantir que, uma vez estabelecidos os princípios, aquele nível desejado seja perseguido e mantido. Para a montagem dessa política, deve-se levar em conta:

- riscos associados à falta de segurança;
- benefícios;
- custos de implementação dos mecanismos.

Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

Controles físicos – são barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura (que garante a existência da informação) que a suporta. Há mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas etc.

Controles lógicos – são barreiras que impedem ou limitam o acesso à informação que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta à alteração não autorizada por elemento mal-intencionado.

Há mecanismos de segurança que apoiam os controles lógicos. São eles:

Mecanismos de criptografia – permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para isso algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

Assinatura digital – um conjunto de dados criptografados, associados a um documento com a função de garantir sua integridade.

Mecanismos de garantia da integridade da informação – usando funções de "Hashing" ou de checagem, um código único é gerado para garantir que a informação é íntegra.

Mecanismos de controle de acesso – palavras-chave, sistemas biométricos, firewalls e cartões inteligentes.

Mecanismos de certificação – atestam a validade de um documento.

Integridade – medida em que um serviço/informação é genuíno(a), isto é, está protegido(a) contra a personificação por intrusos.

Honeypot – é o nome dado a um software cuja função é a de detectar ou de impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o e fazendo-o pensar que está de fato explorando uma vulnerabilidade daquele sistema.

Há hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, antivírus, firewalls, filtros antispam, fuzzers, analisadores de código etc.

Ameaças à segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três características principais:

Perda de confidencialidade – ocorre quando há uma quebra de sigilo de uma determinada informação (por exemplo, a senha de um usuário ou administrador de sistema), permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.

Perda de integridade – acontece quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

Perda de disponibilidade – ocorre quando a informação deixa de estar acessível para quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, decorrente da queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

Aspectos legais[2]

A segurança da informação é regida por alguns padrões internacionais que são sugeridos e devem ser seguidos por corporações que desejam aplicá-la em suas atividades diárias.

Algumas delas são as normas da família ISO 27000, que rege a segurança da informação em aspectos gerais, tendo como as normas mais conhecidas a ISO 27001, que realiza a gestão da segurança da informação com relação à empresa, e a ISO 27002, que efetiva a gestão da informação com relação aos profissionais, os quais podem realizar implementações importantes que podem fazer com que uma empresa cresça no aspecto da segurança da informação. Há diversas normas ISO, e você pode conhecê-las no site *The ISO 27000 Directory*: www.27000.org.

Segurança da informação no Brasil – direito digital

> É o resultado da relação entre a ciência do direito e a ciência da computação, sempre empregando novas tecnologias. Trata-se do conjunto de normas, aplicações, conhecimentos e relações jurídicas, oriundas do universo digital. Como consequência desta interação e da comunicação ocorrida em meio virtual, surge a necessidade de se garantir a validade jurídica das informações prestadas, bem como transações, através do uso de certificados digitais.
>
> *Marcelo de Camilo Tavares Alves*[3]

No Brasil, há algumas leis que se aplicam ao direito digital, como:

A *Lei 12.737/2012*, conhecida como Lei Carolina Dieckmann, que tipifica os crimes cibernéticos.

> Art. 154-A. 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 3 (três) meses a 1 (um) ano, e multa.[4]

Essa lei é fruto de um casuísmo, em que o inquérito policial relativo à suposta invasão do computador da atriz Carolina Dieckmann sequer foi concluído e nenhuma ação penal foi intentada (porém os acusados foram mais do que pré-julgados). A lei passa, então, a punir determinados delitos, como a "invasão de dispositivos informáticos", assim dispondo especificamente o Art. 154-A.[5]

Deve-se esclarecer que a invasão, para ser criminosa, deve se dar sem a autorização expressa ou tácita do titular dos dados ou do dispositivo. Logo, o agente que realiza teste de intrusão (pentest, do inglês *penetration test*) não pode ser punido, por não estarem reunidos os elementos do crime. Caberá, no entanto, às empresas de segurança e auditoria adaptarem seus *contratos de serviços* e pesquisa nesse sentido, prevendo expressamente a exclusão de eventual incidência criminosa nas atividades desenvolvidas.

Acordo de confidencialidade – NDA[6]

Um contrato NDA (*non disclosure agreement*) é um acordo em que as partes que o assinam concordam em manter determinadas informações confidenciais. Para evitar que algum dos envolvidos ou mesmo terceiros tenham acesso a essas informações e as utilizem indevidamente, é possível firmar um NDA.

A principal vantagem desse acordo é a de diminuir as chances de que dados críticos a uma organização ou projeto sejam divulgados, já que um NDA define penalidades para quem descumpre as cláusulas de confidencialidade.

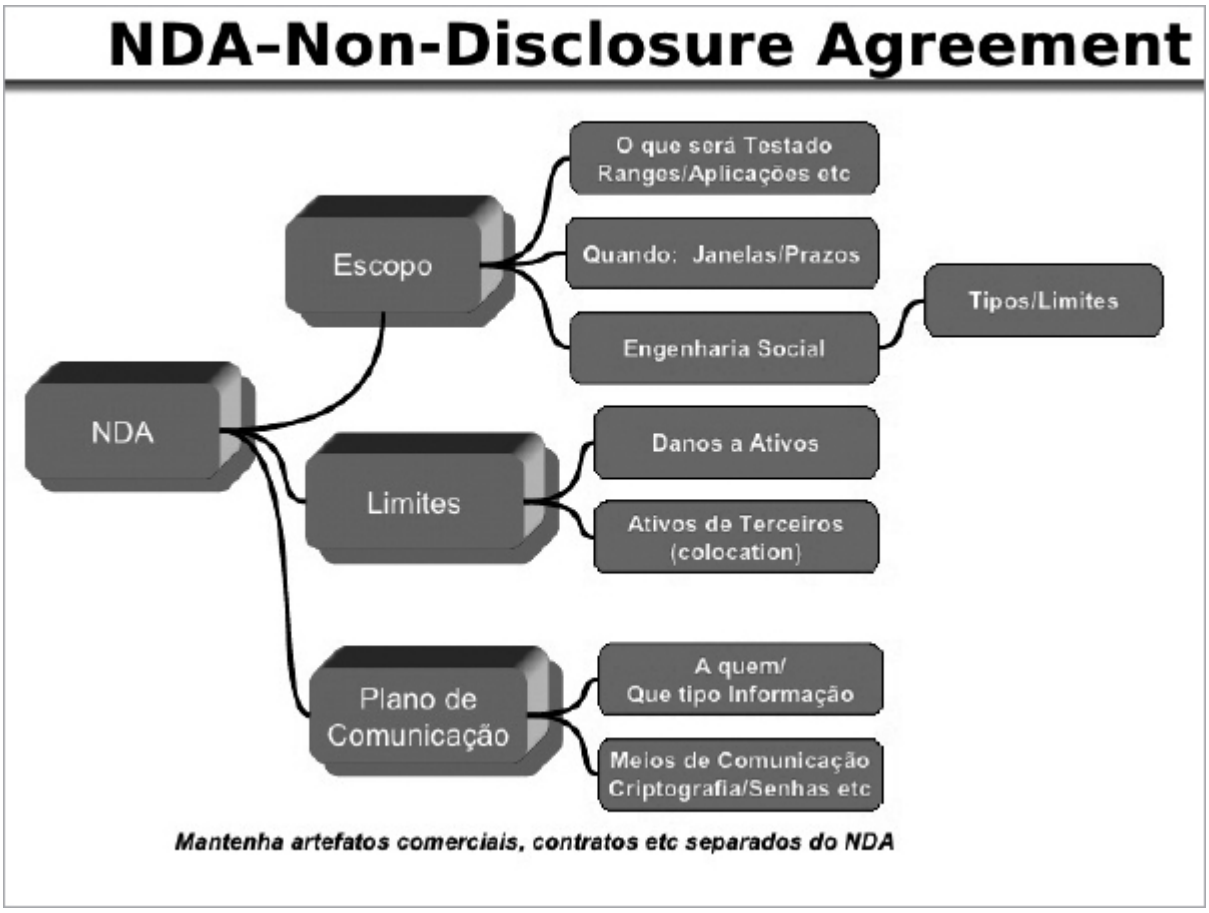
Além disso, um NDA facilita o "caminho jurídico" a ser tomado caso ocorra o vazamento de informações confidenciais, economizando tempo e recursos para a sua organização e aumentando as possibilidades de ganhar causas por quebra de sigilo.

A ISO 27002 define algumas normas para serem seguidas quanto ao código de prática para a gestão da segurança da informação; para implementá-la em uma organização, é necessário que seja estabelecida uma estrutura para gerenciá-la. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes de diversas partes da organização, com funções e papéis relevantes. Todas as responsabilidades pela segurança da informação também devem estar claramente definidas.

É importante, ainda, que sejam estabelecidos acordos de confidencialidade para proteger as informações de caráter sigiloso, bem como as informações que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes.

Estrutura de um acordo NDA

É de extrema importância para um analista pentest assinar um NDA, com detalhes das condições que a empresa vai disponibilizar e informações das quais esse analista tomará conhecimento.



Escopo – ele define o que será testado durante o processo de intrusão, quando e por quanto tempo será realizado. É importante essa definição para que ambas as partes não sejam prejudicadas. Essa importância se dá, por exemplo, porque durante um teste em períodos de pico de uma empresa a indisponibilidade de um sistema pode causar-lhe danos financeiros.

Limites – a definição de limites é uma etapa crucial, pois um ataque pode causar danos em sistemas e equipamentos que podem ser irreversíveis, causando um grande prejuízo financeiro para a empresa.

Plano de comunicação – define quem vai receber as informações encontradas e como elas serão disponibilizadas. Essa etapa requer muita atenção devido à possibilidade de as informações que um pentest pode encontrar serem altamente sensíveis.

Fases do processo de invasão[7]

As fases de um processo de invasão são basicamente divididas em três etapas:

Conhecer – resume-se em *coletar informações* do alvo que será invadido, através dos mais diversos meios, como coletar endereços de e-mails, pessoas que se conectam ao alvo, rastrear usuários, explorar o Google Hacking etc.

Analisar – a partir dos *dados coletados* na etapa anterior, vamos analisar cada dado para extrair o máximo de informação do alvo. Esta é a principal etapa para uma invasão bem-sucedida, a qual inclui, por exemplo, a realização de varredura de IP, serviços, sistema operacional, versões de serviços etc.

Explorar – esta etapa se resume em explorar todas as informações que foram analisadas para ganhar acesso ao alvo, como utilizar exploits, realizar ataques para quebras de senhas, engenharia social etc.

Ética e código de conduta[8]

A ética é impulsionada pelas expectativas da indústria de segurança da informação sobre o comportamento dos profissionais de segurança durante seu trabalho. A maioria das organizações define essas expectativas através de códigos de conduta, códigos de ética e declarações de conduta. No caso de testes de penetração, trata-se de fazer as escolhas certas, já que usamos poderosas ferramentas que podem fornecer acesso não autorizado, negar serviços e, possivelmente, destruir dados.

Você, sem dúvida, encontrará vários dilemas que vão exigir que considere o código ético e seu raciocínio moral, apesar das suas ações. Além disso, levando em conta as consequências que discutimos previamente, após a discussão, você deve ter as ferramentas certas para tomar a melhor decisão. Todas as nossas ferramentas de pentest podem ser usadas para fortalecer a segurança e a resiliência dos sistemas, mas, de fato, em mão erradas, ou quando usadas com más intenções, podem comprometer sistemas e obter acesso não autorizado a dados confidenciais.

Embora você queira fazer uso dessas ferramentas, deve se lembrar de que o objetivo do pentest é o de melhorar a segurança do sistema e da organização por meio das atividades. A execução de exploits e de acesso a esses recursos em sistemas que demonstram vulnerabilidades pode ser corrigida quando a extensão do problema é conhecida e compartilhada com aqueles que podem corrigi-la. Porém, se essa informação nunca chega a

alguém em uma organização e se a vulnerabilidade nunca for compartilhada com o fornecedor original do software, essas questões não serão corrigidas.

Como profissionais de penetração, temos obrigações éticas e contratuais, de maneira que precisamos nos assegurar de que operamos de uma maneira que não viole esses códigos e não corrompa a confiança dessa profissão.

Para isso, é importante que você tenha o entendimento das suas ações. Para que possa entender o que é necessário para realizar testes de penetração, é importante entender o código de conduta e ética nesta área profissional. Há muito mais para saber a respeito desse tema além do que será descrito neste livro; isso é apenas o começo, a indicação do caminho por onde ir.

Para realizar os testes descritos neste livro, é necessário dispor de um ambiente de teste do qual você tenha o controle de forma legal, para que possa se divertir e aplicar todo o conhecimento disponível sem causar danos reais a uma empresa ou pessoa física.

Precisamos operar profissionalmente, assegurando que temos o conhecimento e o consentimento das partes interessadas para realizar os testes, de modo que nós não devemos realizar testes além do escopo do projeto, a menos que sejam autorizados. Sendo assim, gerencie todos os projetos com eficiência e proteja qualquer propriedade intelectual confiada a você.

Divulgue responsavelmente, compartilhando suas descobertas com as partes interessadas em tempo hábil, nunca tome decisões sozinho, sempre trabalhe em equipe e comunique a informação a quem de fato pertence e às partes interessadas. Não subestime o risco; sempre que você identificar um, não avance, pois pode causar problemas em alguma estrutura.

Conheça a diferença entre não divulgação, divulgação completa, divulgação responsável ou coordenada.

Avance na profissão, compartilhe seu conhecimento com profissionais pentesters e profissionais de segurança. Técnicas de ferramentas em testes de penetração em paralelo com a tecnologia evoluem continuamente, então, trabalhar sempre para avançar nesse campo, compartilhando a informação, é essencial para o crescimento profissional.

Use todas as ferramentas apresentadas neste livro com responsabilidade, pois de fato são ferramentas poderosas.

EC-Council – Código de ética

Por meio do programa de certificação Ethical Hacker – CEH (Certified Ethical Hacker) –, o membro estará vinculado a esse código de ética, que é destinado a profissionais de pentest. A versão atual pode ser encontrada no site EC-Council: www.eccouncil.org/code-of-ethics.

Veja alguns dos principais pontos desse código de ética:[9]

1. Privacidade – mantenha privadas e confidenciais as informações obtidas em seu trabalho profissional (em particular no que se refere às listas de clientes e informações pessoais do cliente). Não colete, dê, venda ou transfira qualquer informação pessoal (como nome, endereço de e-mail, número da Segurança Social ou outro identificador exclusivo) a um terceiro sem o consentimento prévio do cliente.

2. Propriedade intelectual – proteja a propriedade intelectual de outras pessoas confiando em sua própria inovação e esforços, garantindo, assim, que todos os benefícios sejam adquiridos com o seu originador.

3. Divulgação – divulgue às pessoas ou autoridades adequadas os perigos potenciais para qualquer cliente de comércio eletrônico. Esses perigos podem incluir comunidades da internet ou o público que você acredita estar razoavelmente associado a um determinado conjunto ou tipo de transações eletrônicas, software ou hardware relacionado.

4. Área de expertise – forneça serviços nas suas áreas de competência, e seja honesto e direto sobre quaisquer limitações de sua experiência e educação. Certifique-se de que você é qualificado para qualquer projeto no qual você trabalha ou se propõe a trabalhar por uma combinação adequada de educação, treinamento e experiência.

5. Uso não autorizado – nunca use conscientemente softwares ou processos que sejam obtidos ou retidos de forma ilegal ou não ética.

6. Atividade ilegal – não se envolva em práticas financeiras enganosas, como suborno, cobrança dupla ou outras práticas financeiras impróprias.

7. Autorização – use a propriedade de um cliente ou empregador somente de maneiras adequadamente autorizadas, e com o conhecimento e consentimento do proprietário.

8. Gerenciamento – assegure uma boa gestão de qualquer projeto que você liderar, incluindo procedimentos efetivos para promoção de qualidade e divulgação completa de risco.

9. Compartilhamento de conhecimento – contribua para o conhecimento de profissionais de comércio eletrônico por meio de estudo

constante, compartilhe as lições de sua experiência com outros membros do conselho da CEH e promova a conscientização pública sobre os benefícios do comércio eletrônico.

(ISC)² – Código de ética

O código de ética da (ISC)² aplica-se a membros desta organização e titulares de certificação como o Certified Information Systems Security Professional (CISSP).

Embora este código não seja projetado especificamente para testes de penetração, ele é extremamente simples e tem um conteúdo abrangente para cobrir a maioria das questões éticas que você vai encontrar como profissional de segurança da informação. Verifique o código completo no site www.isc2.org/ethics

Veja alguns dos principais pontos deste código de ética:

1. Proteger a sociedade, a comunidade e a infraestrutura.

2. Agir com honra, honestidade, justiça, responsabilidade e legalidade.

3. Prover um serviço diligente e competente aos diretores.

4. Avançar e proteger a profissão.

De que lado?

Há uma discussão na área sobre qual chapéu um profissional da segurança está usando, ou seja, de que lado moral o profissional age com o conhecimento de técnicas de penetração. Normalmente, é definido como *White Hat* (Chapéu Branco), *Black Hat* (Chapéu Preto) e *Grey Hat* (Chapéu Cinza).

White Hat – os hackers White Hat optam por usar seus poderes para o bem. Também conhecidos como *hackers éticos*, podem ser empregados de

uma empresa, ou contratados para uma demanda específica, que atuam como especialistas em segurança e tentam encontrar buracos de segurança por meio de técnicas de invasão.

Os White Hat empregam os mesmos métodos de hacking que os Black Hat, com uma exceção: eles fazem isso com a permissão do proprietário do sistema, o que torna o processo completamente legal. Os hackers White Hat realizam testes de penetração, testam os sistemas de segurança no local e realizam avaliações de vulnerabilidade para as empresas.

Black Hat – como todos os hackers, os Black Hat geralmente têm um amplo conhecimento sobre a invasão de redes de computadores e a ignorância de protocolos de segurança. Eles também são responsáveis por escreverem malwares, que é um método usado para obter acesso a esses sistemas.

Sua principal motivação é, geralmente, para ganhos pessoais ou financeiros, mas eles também podem estar envolvidos em espionagem cibernética, hacktivismo ou talvez sejam apenas viciados na emoção do cibercrime. Os Black Hat podem variar de amadores, ao espalhar malwares, a hackers experientes que visam roubar dados, especificamente informações financeiras, informações pessoais e credenciais de login. Eles não só procuram roubar dados, mas também procuram modificar ou destruir dados.

Grey Hat – como na vida, há áreas cinzentas que não são nem preto nem branco. Os hackers Grey Hat são uma mistura de atividades de Black Hat e White Hat. Muitas vezes os hackers Grey Hat procurarão vulnerabilidades em um sistema sem a permissão ou o conhecimento do proprietário. Se os problemas forem encontrados, eles os denunciarão ao proprietário, às vezes solicitando uma pequena taxa para corrigir o problema. Se o proprietário não responde ou não cumpre com um acordo, às vezes os hackers Grey Hat publicarão online a descoberta recentemente encontrada, para todo o mundo ver.

Hackers desse tipo não são inerentemente maliciosos com suas intenções; eles estão procurando tirar algum proveito de suas descobertas. Geralmente, esses hackers não vão explorar as vulnerabilidades encontradas. No entanto, esse tipo de hacking ainda é considerado ilegal, porque o hacker não recebeu permissão do proprietário antes de tentar atacar o sistema.

Embora a palavra hacker tenda a evocar conotações negativas quando referida, é importante lembrar que os hackers não são criados de forma igual.

Se não tivéssemos hackers White Hat procurando diligentemente ameaças e vulnerabilidades antes que os Black Hat possam encontrá-las, provavelmente haveria muito mais atividades envolvendo cibercriminosos que exploram vulnerabilidades e coletam dados confidenciais do que existe agora.[10]

O processo de penetration test (pentest)[11]

Alguns anos atrás, não havia nenhum padrão para realizar o processo de *pentest*, e, com isso, quando não eram bem organizados, os processos não atingiam os objetivos propostos, devido ao descuido nos resultados, à má documentação e à má organização de relatórios.

Para solucionar esses problemas, profissionais experientes criaram um padrão chamado Penetration Testing Execution Standard (PTES), que possui sete sessões organizadas em um cronograma de engajamento.

Essas sessões cobrem um cronograma aproximado para o pentest do início ao fim. Ele inicia-se com o trabalho que começa antes de utilizar o Metasploit durante todo o caminho, até a entrega do relatório para o cliente, de forma consistente. As sessões são as seguintes:

1. Interações de pré-engajamento – envolvem o levantamento de pré-requisitos para o início do pentest, definem o escopo do processo de teste e desenvolvem as regras.

2. Coleta de informações – é a atividade associada à descoberta de mais informações sobre o cliente. Essas informações são úteis para fases posteriores do teste.

3. Modelamento de ameaças – a modelagem de ameaças utiliza a informação dos ativos e processos de negócio reunidos sobre o cliente para analisar o cenário de ameaças.

É importante que as informações de ativos sejam usadas para determinar os sistemas a serem direcionados para o teste e as informações de processos sejam utilizadas para determinar como atacar esses sistemas.

Com base nas informações de destino, as ameaças e os agentes de ameaças podem ser identificados e mapeados para as informações de ativos. O resultado é o modelo de ameaças que uma organização é suscetível de enfrentar.

4. Análise de vulnerabilidades – envolve a descoberta de falhas e fraquezas. Através de uma variedade de métodos e ferramentas de teste, você

obterá informações sobre os sistemas em uso e suas vulnerabilidades.

5. Exploração – usando as informações de vulnerabilidades e o levantamento de requisitos realizados anteriormente, é nesta etapa que exploramos de fato as vulnerabilidades para obter acesso aos destinos. Alguns sistemas têm controle de segurança que temos que ignorar, desativar ou evitar, e às vezes é preciso tomar uma rota completamente diferente para realizar a meta.

6. Pós-exploração – uma vez que conseguimos o acesso a um sistema, precisamos determinar se ele tem algum valor para o nosso propósito e precisamos manter o controle sobre o sistema. A fase pós-exploração explora essas técnicas.

7. Relatórios – é necessário documentar o nosso trabalho e apresentar ao cliente em forma de um relatório que apoie o cliente a melhorar sua postura de segurança descoberta durante o teste.

Para mais informações acesse o site oficial do PTES: www.pentest-standard.org.

Além dos PTES, devemos ter ciência de outras metodologias de teste. O Instituto Nacional de Padrões e Tecnologias (NIST) produz uma série de publicações relacionadas à segurança conhecida coletivamente como *NIST 800-115*, um guia técnico para teste de validação de segurança da informação, que foi publicado em 2008 e tem apenas uma pequena seção específica sobre testes de penetração.

O Open Source Security Testing Methodology (OSSTMM) possui um manual que foi publicado em 2010. Atualmente, há uma quarta edição em desenvolvimento, porém, para ter acesso a este manual é necessário ser membro, o que envolve a realização de alguns cursos e um programa de certificação de três níveis para essa metodologia.

O Open Web Application Security Project (OWASP) também possui um guia, o *OWASP Testing Guide v4*, cujo foco principal está em testes de segurança de aplicativos web, mas que tem um valor de grande peso em testes de penetração.

---

1. SEGURANÇA DA INFORMAÇÃO. *In*: WIKIPEDIA: a enciclopédia livre. [San Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: https://pt.wikipedia.org/wiki/Segurança_da_informação. Acesso em: 14 ago. 2019.

2. Videoaula TDI – Concepção – Aspectos Legais.
3. ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009, p. 3. Disponível em: https://docero.com.br/doc/xc0vec. Acesso em: 15 ago. 2019.
4. BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 14 ago. 2019.
5. LEI CAROLINA DIECKMANN. *In*: WIKIPEDIA: a enciclopédia livre. [San Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann. Acesso em: 23 ago. 2019.
6. Videoaula TDI – Concepção – Acordo de confidencialidade.
7. Videoaula TDI – Concepção – Fases do Processo de Técnicas de Invasão.
8. Videoaula TDI – Bootcamp – Ética e código de conduta.
9. EC-COUNCIL. Code of ethics. Disponível em: www.eccouncil.org/code-of-ethics. Acesso em: 14 ago. 2019.
10. SYMANTEC. What is the difference between Black, White and Grey Hat Hackers? Disponível em: https://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers. Acesso em: 14 ago. 2019.
11. Videoaula TDI – Bootcamp – O Processo de penetration test.