Quebrando o Cerco

Apresentação

Ética Hacker

Ética Hacker

- Compartilhamento
- Abertura
- Descentralização
- Livre acesso aos computadores
- Melhoria do mundo

Ética Hacker

O acesso a computadores - e qualquer outro meio que seja capaz de ensinar algo sobre como o mundo funciona - deve ser ilimitado e total.

Ética Hacker

Toda a informação deve ser livre, pois o hacker precisa de informação para melhorar aquilo que precisa, na sua visão, ser melhorado.

Ética Hacker

"Promover a descentralização",
desconfiando de uma única autoridade.

Ética Hacker

"Hacker devem ser julgados pelo seu hacking", ou seja, sua contribuição deve ser avaliada baseando-se somente no que foi produzido e não por critérios como idade, ter um diplomas acadêmicos, raça, cor, religião, posição ou outros.

Ética Hacker

"Você pode criar arte e beleza com o computador"

Ética Hacker

"Computadores podem mudar sua vida para melhor"

As Gerações de Hackers

1ª Geração

Hackers de Software

2ª Geração

Hackers de Hardware

3ª Geração

Programadores de Jogos

Normas

ISO 27000

A ISO 27000 foi baseada na British Standard (BS) 7799, um padrão publicado originalmente pelo British Standard Institute (BSI) em 1995. Foi escrita pelo Departamento de Industria e Comércio do Governo do Reino Unido e consiste de várias partes.

ISO 27000

ISO 27000 – São informações básicas sobre as normas da série.
ISO 27001 – Bases para a implementação de um SGSI em uma organização.
ISO 27002 – Certificação profissional, traz códigos de práticas para profissionais.
ISO 27003 – Diretrizes mais específicas para implementação do SGSI.
ISO 27004 – Normas sobre as métricas e relatórios do SGSI.
ISO 27005 – Diretrizes para o processo de gestão de riscos de segurança da informação.
ISO 27006 - Diretrizes de Serviços de Recuperação de Desastres.

ISO 27000

Disponibilidade
Integridade
Confidencialidade
Autenticidade

O mnemônico para facilitar a memorização do conceito é “DICA”. Entender o significado de cada propriedade que integra a DICA é essencial para entender o conceito de Segurança da Informação e Comunicações.

PCI-DSS

Em Setembro de 2006, algumas bandeiras de cartão de crédito, como Visa, Mastercard e American Express, criaram um Conselho, chamado PCI Council, para criar e recomendar boas práticas de Segurança de Dados, a PCI-DSS ou Payment Card Industry – Data Security Standard, a serem seguidas pelos estabelecimentos comerciais que aceitam Cartões de Crédito como forma de Pagamento, para proteger a privacidade dos consumidores portadores de Cartão de Crédito.

PCI-DSS

A obrigatoriedade de se adaptar ao Padrão se aplica a toda e qualquer Empresa que coleta, processa, armazena ou transmite informação de Cartão de Crédito.

Não estar em conformidade com a PCI-DSS pode incorrer em multas e até em descredenciamento dos estabelecimentos comerciais em aceitar cartões de crédito.

PCI-DSS

1. Instalar e manter um firewall para proteger dados de cartão de crédito.
2. Não utilizar senhas padrão ou outras configurações de segurança dos softwares utilizados.
3. Proteger dados de cartões de crédito armazenados.
4. Utilizar criptografia na transmissão de dados de cartões de crédito, manter um programa de Gerenciamento de Vulnerabilidades.
5. Utilizar regularmente programas anti-vírus.
6. Desenvolver e manter sistemas e aplicações seguras, implementar um forte controle de acesso.

PCI-DSS

7. Restringir acesso a dados de cartões de crédito por negócio e por pessoas que realmente precisam acessá-los.
8. Designar um único ID para cada usuário da rede e sistemas.
9. Restringir acesso físico aos dados de cartão de crédito, testar e monitorar a rede regularmente.
10. Rastrear e monitorar todos os acessos à rede e dados de cartões de crédito.
11. Testar a segurança de sistemas e processos regularmente, manter um programa de Gerenciamento de Vulnerabilidades.
12. Manter uma política que aborde a segurança das informações.

Pentest

Pentest

Blind ou Black Box
Neste ataque o Auditor não conhece nada sobre o alvo que irá atacar, porem o alvo sabe que será atacado e o que será feito durante o ataque.

Double Blind ou Double Black Box
Neste ataque o Auditor não conhece nada sobre o alvo, e o alvo não sabe que será atacado e tão pouco quais testes serão realizados.

Pentest

Gray Box
Neste ataque o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado e também sabe quais testes serão realizados. Este é o tipo de pentest mais realista possível, aproximando-se de um ataque real.

Double Gray Box
Neste ataque o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado, porém, não sabe quais testes serão executados.

Pentest

Tandem ou White Box/Crystal Box
Neste ataque o Auditor tem total conhecimento sobre o alvo, e o alvo sabe que será atacado e também o que será testado.

Reversal
Neste ataque o Auditor tem conhecimento total do alvo, porém o alvo não sabe que será atacado, e tão pouco quais testes serão executados. Este tipo de ataque é ideal para testes a capacidade de resposta e como está o timing de ação da Equipe de Resposta a Incidentes do alvo.

Análise de Vulnerabilidades e Auditoria

Análise de Vulnerabilidades

Análise de Vulnerabilidades consiste em somente a identificação de falhas e vulnerabilidades conhecidas pelo scanners de vulnerabilidades.
Visa somente mapear os programas e serviços que possam conter vulnerabilidades conhecidas, sem passar pela comprovação de que tal falha possa vir a acarretar em problemas e prejuízos a empresa.

Legislação

Lei Carolina Dieckmann

Art. 154-A
Invasão de 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.

Art. 266
Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.
Pena - detenção, de 1 (um) a 3 (três) anos, e multa.

Art. 298
Falsificação de documento particular/cartão. Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Etapas de um Ataque

Dúvidas?

garoa.net.br

gutemhc@gmail.com