Capa

Slide 1 - Apresentação
Apresentar o Formato e Idéia do Encontro
Se Apresentar
Pedir para o Pessoal se Apresentar

Slide 2 - Ética Hackers

No prefácio do seu livro Hackers: Heroes of the Computer Revolution, de 1984, Steven Levy registrou os princípios da ética hacker:

Slide 3 - Pilares Ética Hacker
Compartilhamento
Abertura
Descentralização
Livre acesso aos computadores
Melhoria do mundo

Além desses princípios, Levy também detalhou a ética hacker no capítulo 2, The Hacker Ethic:

Slide 4 -
O acesso a computadores - e qualquer outro meio que seja capaz de ensinar algo sobre como o mundo funciona - deve ser ilimitado e total.
Esse preceito sempre se refere ao imperativo "mão na massa". Isto é, se um hacker precisa enviar várias mensagens para celulares sem pagar, ao invés de entrar várias vezes na interface web e enviar uma mensagem por vez, ele descobrirá como a interface web funciona e fará um programa automático para o envio de mensagens de forma mais ágil e com menos desperdício de tempo.

Slide 5 -
Toda a informação deve ser livre, pois o hacker precisa de informação para melhorar aquilo que precisa, a sua visão, ser melhorado.

O hacker busca a informação diariamente e tem prazer em passá-la para quem quer "pensar" e "criar" coisas novas.

Na sociedade de consumo de hoje, tudo é transformado em mercadoria e vendido.
Isso inclui a informação. Mas a informação, só existe na mente das pessoas.
Como não se possui a mente de outra pessoa, não podemos comercializar informações.
Uma analogia semelhante é a do velho índio Chefe Touro-Sentado ao dizer "a terra não pode ser possuída".

Slide 6 -
"Promover a descentralização", desconfiando de uma única autoridade.
Um hacker não aceita os famosos argumentos de autoridade e não acredita na centralização como forma ideal de coordenar esforços.

Isso é essencial a pratica, pois quanto mais disseminado o conhecimento e as técnicas dominadas por um, melhor será para o restante experimentar e produzir novas soluções.

Slide 7 -
"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.
Essa é a base da meritocracia.

Slide 8 -
"você pode criar arte e beleza com o computador"
visa a pluralidade do hacker, pois não só programas podem ser produzidos vários outros setores podem ter o seu trabalho aperfeiçoado e inovado com a utilização do computador.

Slide 9 -
"Computadores podem mudar sua vida para melhor"
visto que os computadores se tornaram parte essencial da vida das pessoas entrando para todas as áreas de conhecimento com potencial de melhorar a qualidade de vida como um todo.

Slide 10 - As Gerações de Hackers
Levy identifica vários "verdadeiros hackers" que influenciaram significativamente a ética hacker.

Slide 11 - 1ª Geração - Hackers de Software
Alguns "verdadeiros hackers" bem conhecidos:

John McCarthy:
Co-fundador da MIT Artificial Intelligence Lab e Stanford AI Laboratory. Ele é um dos "Pais Fundadores" da Inteligencia Artificial junto com Marvin Minsky, Allen Newell e Herbert A. Simon.
Participou do Comitê que desenvolveu a Linguagem de Programação ALGOL.
Inventor da liguagem de Programação LISP.
Inventor do "Garbage Collection", sistema amplamente usado para gerenciamento de Memória.

Bill Gosper:
Junto com Richard Greenblatt, pode-se considerar que ele fundou a comunidade hacker, e mantém um lugar de orgulho na comunidade Lisp.
Ele também é reconhecido por seu trabalho em representações em frações continuadas de números reais, e por auxiliar no algoritmo (que leva seu nome) para achar formas aproximadas de identidades hipergeométricas.

Richard Greenblatt:
Programador e projetista inicial da Máquina Lisp
Entrou para o MIT em 62. Juntou-se ao Famoso Tech Model Railroad Club, que é onde começa a "Comunidade Hacker". Começou a escrever um Compilador Fortran para o PDP-1 da DEC, assim como para toda a Familia PDP até o 6. Nunca terminou o compilador, mas trechos de seu

código fonte foram usados posteriormente.
Juntou-se ao AI Lab e lá foi merecidamente exaltado pela sua habilidade com Programação.
Passou tanto tempo programando para os PDP que bombou no 3 ano, tendo que largar o MIT e ir trabalhar. 6 meses depois foi contratado pelo AI Lab.

Richard Stallman:
Programador e ativista político, bem conhecido pelo GNU, Emacs e pelo Movimento de Software Livre.

Slide 12 - 2ª Geração - Hackers de Hardware
Levy também identificou os "hackers de hardware" (a "segunda geração", centrada principalmente no Vale do Silício) e os "hackers de jogos" (ou "terceira geração"). Todas as três gerações de hackers, de acordo com Levy, incorpora os princípios da ética hacker.

Alguns hackers da "segunda geração" de Levy inclui:
Steve Wozniak:
Um dos fundadores da Apple

Bob Marsh:
Designer do computador Sol-20

Fred Moore:
Ativista e fundador do Homebrew Computer Club

Steve Dompier:
Homebrew Computer Club membro e hacker que trabalhou com o início do Altair 8800

Lee Felsenstein:
Um hardware hacker e cofundador do Community Memory e do Homebrew Computer Club. Um designer do computador Sol-20

John Draper:
Uma figura lendária no mundo da programação de computadores.
Ele escreveu EasyWriter, o primeiro Processador de texto.

Slide 13 - 3ª Geração - Programadores de Jogos
A "terceira geração" praticante da ética hacker inclui:
John Harris:
Um dos primeiros programadores contratados para o On-Line Systems (que mais tarde se tornou Sierra Entertainment)

Ken Williams:
Junto com a esposa Roberta, fundou o On-Line Systems depois de trabalhar na IBM

Slide 14 - Normas

Slide 15 - Familia ISO 27000
Existem 27 Normas ISO 27000 prontas e 9 em Preparação nas séries da ISO 27000, e cada uma delas tem uma função específica.

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.

Slide 16 - ISO 27K mais conhecidas
ISO 27000 – São informações básicas sobre as normas da série.
Apresenta algum vocabulário e definições.

ISO 27001 – Bases para a implementação de um SGSI em uma organização.
Apresenta alguns requisitos que sugerem alguns procedimentos para uma boa Gestão da Segurança da Informação.

ISO 27002 – Certificação profissional, traz códigos de boas práticas para profissionais.
Esta é a Certificação que o Profissional faz o Exame para se Certificar.
Não confundir com a 27001 que é a Certificação a Empresa, assim como a ISO 9000 é para Gestão de Qualidade.

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.

Slide 17 - Os Pilares
A ISO 27000 pode ser resumida em alguns Pilares.

Disponibilidade
Garantia de que a informação esteja sempre disponível para o uso por aqueles autorizados pelo proprietário da informação.

Integridade
Garantia de 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 (criação, manutenção e destruição).

Confidencialidade
Garantia de que o acesso a informação se dará apenas para aqueles autorizados pelo proprietário da informação.

Autenticidade
Garantia de que a informação é proveniente da fonte anunciada e que não foi alvo de mudanças ao longo de um processo.

O mnemônico para facilitar a memorização do conceito é “DICA”, sendo: D para Disponibilidade; I para Integridade; C para Confidencialidade; e A para Autenticidade. Entender o significado de cada propriedade que integra a DICA é essencial para entender o conceito de segurança da informação e comunicações.

Para alguns, existe um 5º Pilar:
5. Irretratabilidade ou "não-repúdio"
Impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

Slide 18 - 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.

Slide 19 -
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.

Isso inclui comerciantes, intermediários que processam dados de cartão de crédito e estão ligados à rede da associação de cartões, assim provedores de serviço que hospedam sistemas de transações em ATM ou coletam e processam dados de cartão de crédito – gateways de pagamento.

Empresas que apenas emitem Cartões de Crédito e autorizam transações, como bancos e grandes varejistas, não precisam mostrar conformidade com o PCI DSS.

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

Slide 20 -
O PCI-DSS contempla 12 requerimentos básicos que têm o objetivo de:

Manter a rede de dados segura;
Proteger as informações de portadores de cartão de crédito;
Manter um programa de Gerenciamento de vulnerabilidades;
Implementar um forte controle de acessos;
Manter uma política de segurança de informações.

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.

Slide 21 -
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.

Slide 22 - Pentest
O Pentest ou Teste de Intrusão, simula tentativas de acesso a rede ou a sistemas por pessoas não autorizadas, em dois níveis: Interno e Externo.
É ideal que sejam realizados testes regularmente e após qualquer mudança significativa na rede de dados ou ambiente web.
Estes procedimentos são exigidos e/ou recomendados por diversas normas de segurança da informação.

O teste de intrusão apresenta a visão de um atacante real, apresentando informações que podem vir a ser utilizadas por pessoas com más intenções para obter vantagens ou acesso indevido a sistemas.

Existem algumas modalidades de Teste de Intrusão e a diferença entre elas está na quantidade de informações fornecidas aos nossos analistas especializados que irão executar os testes:

Slide 23 - Tipos de 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.

Slide 24 -
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.

Slide 25 -
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 acão da equipe de resposta a incidentes do alvo.

Slide 26 - Análise de Vulnerabilidades e Auditoria

Slide 27
Análise de Vulnerabilidades consiste em somente a identificação de falhas e vulnerabilidades conhecidas pelo scanners de vulnerabilidades.
Visam 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.

Geralmente a Análise de Vulnerabilidade não envolve Testes de Intrusão, ou seja, não há um ataque real para que se apresente possíveis dados sobre um determinado ambiente, mas apresenta real periculosidade, visto que, aos olhos do auditor, são informações que podem chamar a atenção de um real atacante e possivelmente serem exploradas.

Slide 28 - Legislação

Slide 29 - Lei Carolina Dieckmann
A Lei Carolina Dieckmann é como ficou conhecida a Lei Brasileira 12.737/2012, sancionada em 2 de dezembro de 2012 pela Presidente Dilma Rousseff, que promoveu alterações no Código Penal Brasileiro, tipificando os crimes informáticos.

Os delitos previstos na Lei Carolina Dieckmann são:

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.

A "Lei Carolina Dieckmann" entrou em vigor no dia 02 de abril de 2013.

Slide 30 – Etapas de um ataque