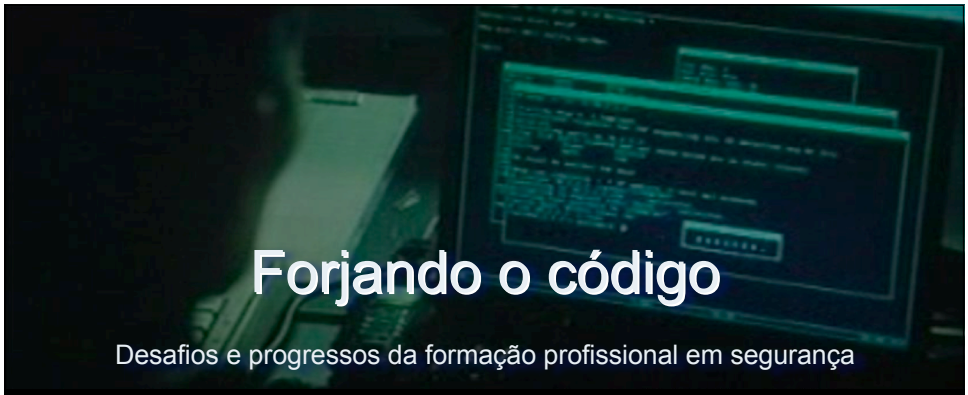


Forjando o código

Desafios e progressos da formação profissional em segurança

Adriano Mauro Cansian

unesp - universidade estadual paulista

adriano@acmesecurity.org

PGP KeyID: **0x3893CD2B**

Agenda

- Necessidades.
- Visões.
  - Academia, mercado, estudantes.
- Nossa experiência.
  - *Background*.
  - Visões, métodos e ênfases.
  - *Hacking revisited.*
  - Ética.
- Conclusões

Necessidades

Necessidades

- Choro:
- “ Nós precisamos de educação em segurança! ”
  - Mais e melhor !
- Até os mais desatentos descobriram isso !

O Campo é vasto

- Communications security
- Operations security
- Physical security
- Code security
- Personnel security
- Environmental security
- “You-name-it” security

Prática da segurança

Definida como:

- Proteção dos **atributos** de segurança da informação;
- Detecção de um comprometimento ou ataque sobre os **atributos**,
- Ser capaz de **reagir e corrigir** situações.

- Atributos:
  - Confidenc... blah, blah, blah...

Formalização

- 1970

  "providing satisfactory security controls in a computer system is in itself a system design problem requiring a combination of hardware, software, communication, physical, personnel, and administrative procedural safeguards ..."

  Ware, Willir H. - Security Controls for Computer System: Report for the Defense Science Board Task Force on Computer Security. **The RAND Co. (1970)**.

Pandemic !

- Três décadas depois:

*A **pandemic** (from Greek παν pan all + δήμος demos people) is an epidemic that spreads through human populations across a large region (for example a continent), or even worldwide.*

Visões

Visões (1)

- "*Computer security education*"
- O que isso significa não é lá muito claro...
- Academia, Mercado e Estudantes têm visões diferentes

Visões (2)

- As pessoas da academia são de Marte, e pessoas do mercado são de Vênus.
- E os estudantes... bem... :-)
- “Grandes habilidades” ?

Visões - Academia (1)

- Os princípios variam.
  - Geralmente visões da torre de marfim.
- Teóricos
  - Harrison, Ruzzo & Ullman, “***Protection in Operating Systems***”. Comm. of the ACM. 19 (8) (**1976**) pp. 461.
- Práticos
  - Saltzer & Schroder, “***The Protection of Information in Computer Systems***”. Proc.IEEE 63 (9) (**1975**) pp 1278.

Visões - Academia (2)

- **Meta:** ser capaz de aplicar princípios teóricos e práticos às mais variadas situações.
- Praticar "**a ciência e a arte**" da segurança de computadores.
- Traduzindo...
  - Bons instrutores: (deveriam) usar sua experiência, aliada a exercícios práticos, para incutir princípios a seus alunos.

Visões - Academia (3)

- O que se pensa:
- Os estudantes devem conhecer os fundamentos e aplicar os princípios, até obter sua formação.

Visões - Mercado (1)

- Precisa proteger seu investimento.
  - (Quase sempre) entende o valor da segurança da informação.
- Sabe que ela é feita com recursos humanos.
- Mas:
  - Quer recursos humanos bem formados.
  - Que funcionem efetivamente.
  - Com custo baixo.

Visões - Mercado (2)

- **Meta:** Um profissional que reduza as ameaças, com um custo mínimo de treinamento.
- Reconhece que entender e dominar princípios ajuda a desenvolver e implementar políticas e mecanismos.
  - “Huh? Você conhece TCP/IP?? Legal !”
- Mas, **os resultados finais é que importam** !

Visões - Governo

- Governos utilizam a segurança de computadores como uma das muitas ferramentas para proteger os interesses nacionais.
- Supondo que exista algum:
  - Interesse nacional...
  - Governo...

Visões - Estudantes (1)

- Expectativas:
  - Ser um CSI?
  - Ser o Robert Redford?
  - Ser um "***hacker***"?
  - **Meta:** Huh? Meta ?

Visões - Estudantes (2)

Quando vamos mexer com Linux ?

Quando vamos mexer com PDAS?

Vamos procurar viruses?

Quando vamos mexer com telefones?

Não é muita teoria ?

Quando vamos ver um "*case*" maior ?

Existe uma ferramenta para... ??

TCPdum... o quê ?

Quando vamos mexer com Mac?

Por que estamos estudando segurança da informação?

Por que não estamos fazendo coisas **mais** técnicas ?

Por que não estamos fazendo coisas **menos** técnicas ?

Tenho mesmo que saber tantos protocolos?

Quais as minhas perspectivas profissionais?

Quanto vou ganhar?

Precisa mesmo de TCP/IP ?

Precisamos de mais leis?

Nossa experiência

Nosso *Background*

- Laboratório de pesquisa em segurança de computadores e redes, fundado em 1995.
- UNESP - São José do Rio Preto, SP. Brasil.
  - www.acmesecurity.org
  - www.ibilce.unesp.br
- Desenvolvimento de atividades ligadas a Internet desde 1992.
  - Foco em pesquisa, mas com propósito de formar recursos humanos.
  - Universidade pública e gratuita.

Background dos estudantes (1)

- Prós:
  - Comprometidos.
  - Boa cultura geral.
  - Boa formação moral.
- Contras:
  - Poucas habilidades específicas.
  - Conhecimentos mistos e diversos
    - "Eu sei de quase tudo um pouco e quase tudo mal"
  - O que é ser um analista de segurança?

Background dos estudantes (2)

- Núcleo de conhecimento:
  - Nada se pode assumir.
  - *Background* de matemática heterogêneo.
  - *Background* de programação heterogêneo.
    - Quando sabem programar não sabem escrever ou falar.
  - Só usuários de Windows.
  - Funcionamento da Internet: “saber transversal”.
  - Alguns sequer sabem porquê (e se) querem trabalhar com segurança.

Desafio

- Transformar os heterogêneos.
- Lapidar.
- Fazer-se entender:
  - Montar uma estrutura que faça sentido aos estudantes.
    - Sem perder o rigor formal.

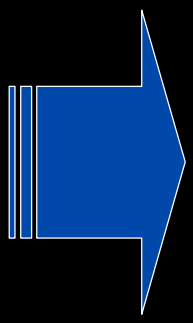
Como ensinamos

Como ensinamos?

- Fundamentos.
  - Protocolos.
  - Protocolos.
  - Protocolos.
- Ética.
- Técnicas de Segurança.

... com os melhores recursos

- Hardware.
- Software.
- Ambiente.
  - Físico.
  - Cultural.
  - Técnico.
  - Investigativo.
  - Instigativo.



Peopleware

...com o melhor material

Estudos de casos.

- É difícil obter dados de casos reais para ensino.

Exemplos de ensino.

- Ainda que se tenha os estudos de casos, as idéias e os exemplos reais, é preciso criar ambientes de ensino (imagens) para o treinamento.
- Grande consumo de tempo.

...com perspectivas

- Dificuldade de posicionar estudantes num ambiente de segurança real.
  - Estágios não são oferecidos num ambiente de produção.
  - O mercado tem medo dos estudantes.
- Como estagiários de mercado:
  - Estudantes em “atividades lúdicas”.
  - Os estudantes têm medo do mercado.

.. com o melhor cuidado (1)

- Problemas em potencial:
  - Por definição, **é impossível ensinar os estudantes como proteger e defender a sem ensina-los como atacar**.
    - Tanto em teoria como na prática.
  - Ensinar estudantes sobre assuntos potencialmente perigosos exige cautela.
    - Adotar salvaguardas para todos.

.. com o melhor cuidado (2)

- Ética.
  - **A maior preocupação.**
- Devem ser preparados para entender os efeitos de suas ações.
  - Poucos centros de formação incluem componentes de *"appropriate use",* a respeito da segurança de computadores.
- Incluímos pesadamente ética na formação, junto com os fundamentos.

Onde os *hackers* entram?

- ***Hackers* no sentido não pejorativo.**
- Levam computadores ao limite.
- *Hackers* precisam aprender ética como todo mundo.
- Ensinando ética a *hackers*, os aspectos positivos do *hacking* são **encorajados,** e os negativos são desencorajados.

Huh? Encorajar *hacking*?

- Sim, absolutamente, em vários níveis:
  - *Hackers* são curiosos, motivados e talentosos.
  - *Hackers* experimentam.
    - Características desejáveis em P&D.
- *Hackers* : por trás das maiores inovações.

- Não confundir "*hacking*" com crime eletrônico, *cracking*, vandalismo, etc...
  - Sentido não pejorativo e sim **apreciativo**.

Hacking revisited

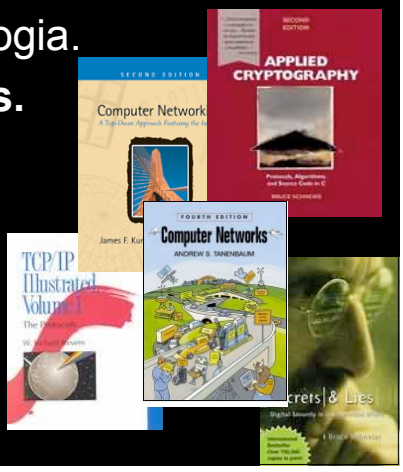
- *Hackers* entendem o valor da informação.
  - Muito interessados em integridade da informação, segurança e privacidade.
  - Capazes de entender as implicações das suas ações e das ações de outras pessoas.
- Temos certeza que que isso não cria mais "*hackers*" (pejorativo)
  - Mas sim reforça códigos de valores éticos como força de trabalho e conhecimento.

Exemplos de temas em ética

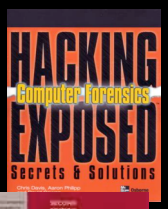
- **Valor da informação.**
- **Privacidade da informação.**
- **Segurança da informação**
- **"*Secrecy*"**

Muito além da ética

- A preparação técnica é feita sobre os fundamentos da tecnologia.
- **Nunca sobre produtos.**
- Sempre sobre idéias.
  - Ênfase nos protocolos.
  - Ênfase em *peopleware*.
  - Ênfase em conceitos.

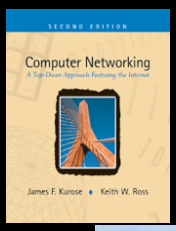


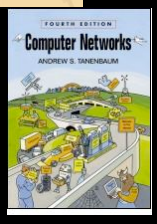
O melhor conjunto de habilidades

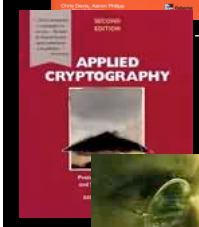


Capacidade criativa, investigativa e instigativa.

Sólidos conhecimentos ténicos acerca dos ambientes.

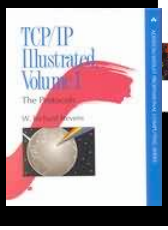


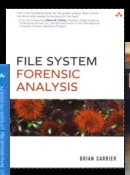


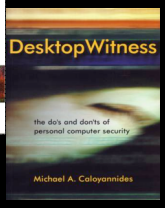


Sólidos conhecimentos dos fundamentos: protocolos, RFCs, códigos, falhas.

Comprometimento ético.







Conclusões

Lições aprendidas ao longo de 12 anos ensinando analistas de segurança

Lições aprendidas (1)

- Estudantes esperam:
  - Combinação de temas apropriados.
  - Materiais de estudos de casos e simulações.
  - Hardware e ambiente apropriado.
  - Material de ensino que os estimule.
- Estudantes precisam sentir que estão aplicando o que aprenderam, e quais os resultados de suas ações.

Lições aprendidas (2)

- O preço que se paga é alto.
- Segurança de computadores pode ser um tema caro, em termos de recursos e de tempo.
- O desenvolvimento de pesquisa auxilia no ambiente de preparação dos estudantes.

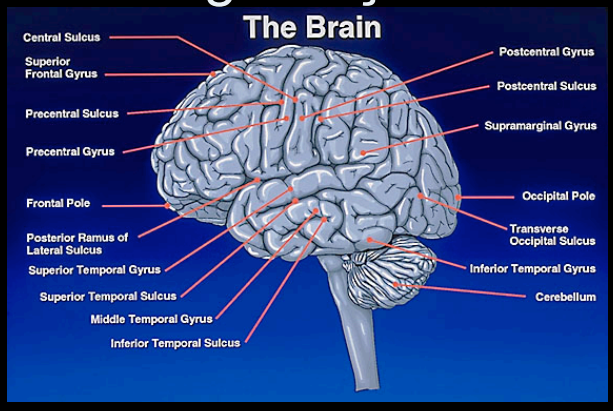
Lições aprendidas (3)

- **Elementos críticos:**
  - **Fundamentos** melhor do que produtos.
  - **Ética** equivale a um fundamento.
    - Item mais valioso.
  - Estudantes necessitam de orientação em sua carreira.
    - *Hacking* é uma habilidade a ser lapidada.
  - Meios e a motivação adequados:
    - Universidades (brasileiras) não possuem.
  - O governo não faz idéia do que estamos falando.

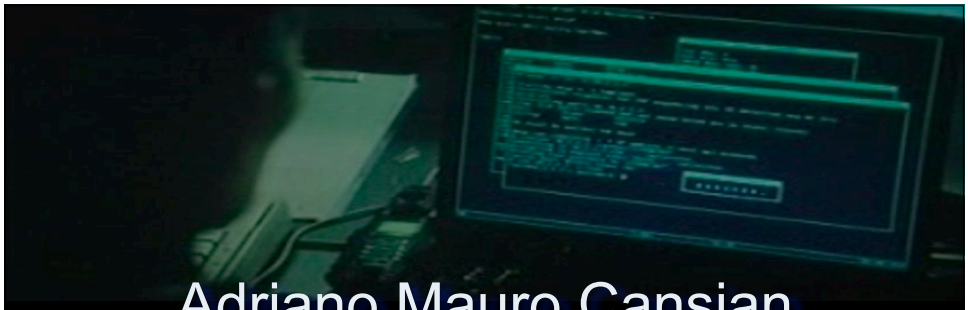
Lições aprendidas (4)

- "*A fool with a tool is still a foll*".
- **Pensar como *hacker* não cria criminosos.**
- Impossível aprender defesa sem aprender ataques.
- Ensinar a atacar não significa que ele vá atacar.
- Ensinar a atacar não cria criminosos.
  - "*commitment*" ético e moral.

A melhor ferramenta de segurança...



(desde que devidamente treinada)



Adriano Mauro Cansian

Laboratório ACME! de Pesquisa em Segurança de Redes
UNESP - Universidade Estadual Paulista
Campus de São José do Rio Preto
São José do Rio Preto, SP.
Tel. (17) 3221-2475 (laboratório) / 3221-2201 (secretaria)
http://www.acmesecurity.org

adriano@acmesecurity.org

PGP KeyID: **0x3893CD2B**