Onde estão as ferramentas de segurança do Brasil ?

Ronaldo Vasconcellos

H2HC 5, 9 de novembro de 2008

Agenda

- Trilha sonora
- Por que a pergunta?
- E por que o Ronaldo?
- O ecossistema
- Problemas
- Conclusões

Trilha sonora

Nobody But Me (1968)

The Human Beinz

Por que a pergunta?

- Por que a pergunta **agora**?
  - pr0j3kt m4yh3m br4z1l
  - i sh0t t3h wh1t3h4t

Por que a pergunta? (2)

- Estão certos? Errados?
  - Não é o assunto da palestra
  - Assunto: O que pode ter causado o surgimento do pr0j3kt m4yh3m br4z1l
- Pontos de vista
  - Whitehats tem certeza de que estão certos
  - Blackhats tem certeza de que estão certos
  - Todos tem certeza de que estão certos

E por que o Ronaldo?

- Por que alguém precisava tocar no assunto
  - H2HC 4 (som de grilos)
- Medidas anti-bullying não funcionam!
- Whitehat que dá valor a hackers
- Não pretendo representar whitehats, recriminar não-whitehats
  - Minha opinião, não represento ninguém.


Extreme Confidence

Ecossistema de segurança

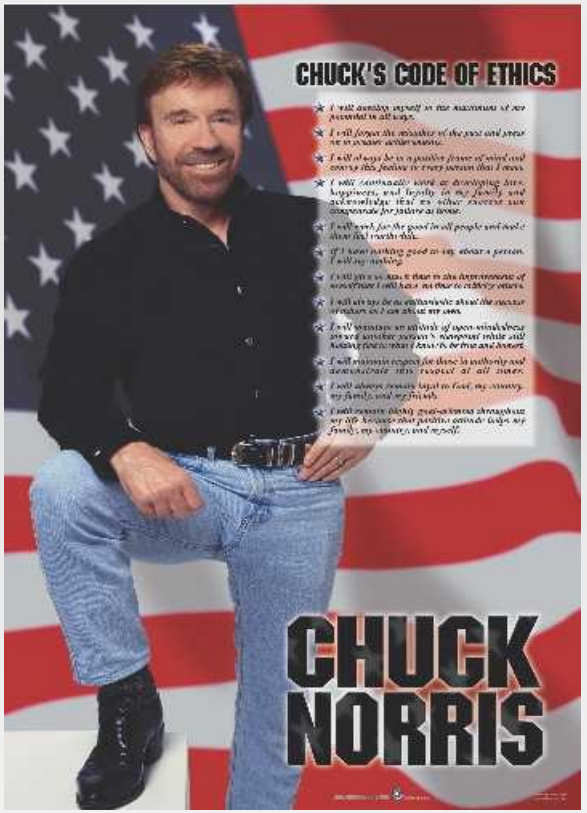
- Comunidade não-whitehat
- Comunidade whitehat
- Academia
- Empresas
- Grupos de segurança

Ecossistema de segurança (2)

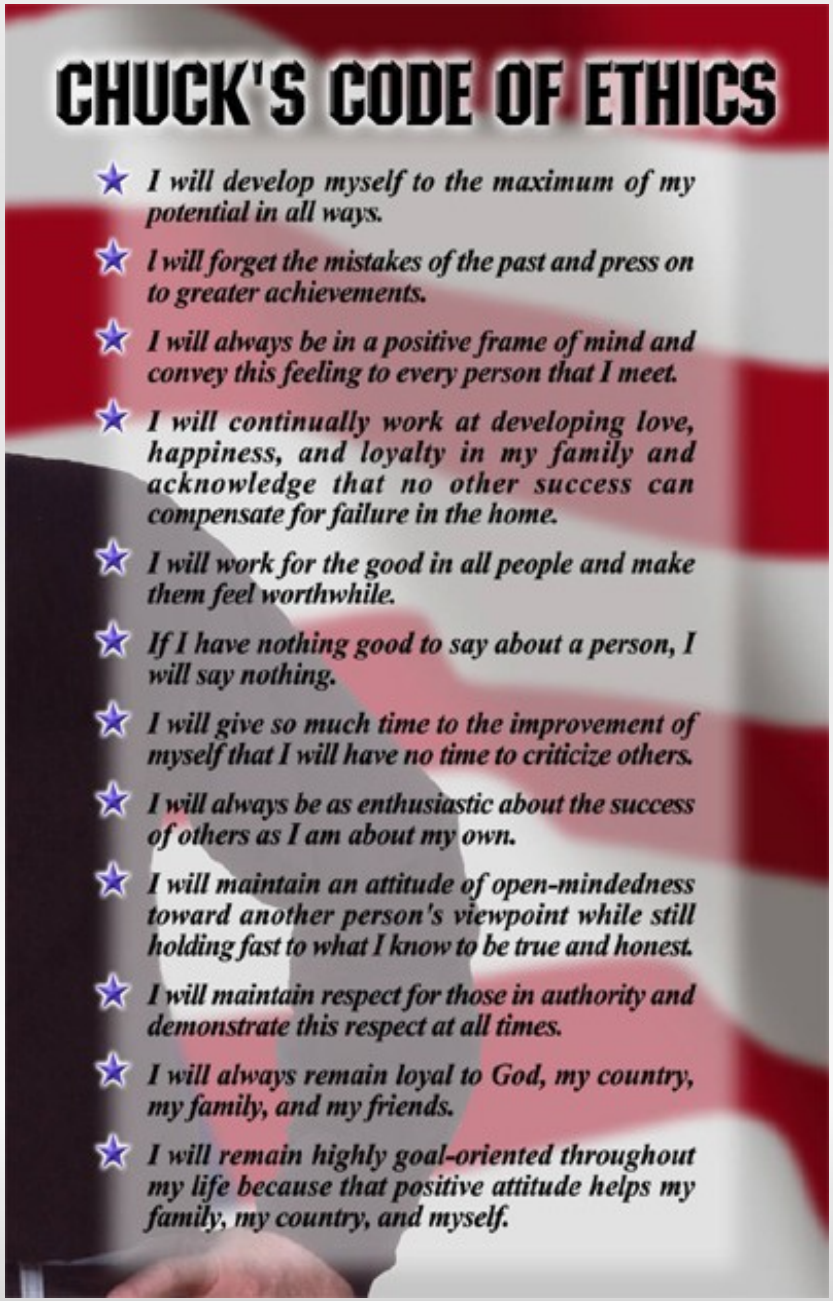
- Não-whitehats / hackers maliciosos
  - Todos na mesma prateleira, embora não seja correto.
  - Crime organizado online existe sim
    - Brasileiro é hacker por natureza. Lei de Gérson.
  - Eventos abertos
    - Relativamente recentes - H2HC, uCon
    - Revista 2600 ”Pelego's Bar at Assufeng, near the payphone. 6 pm”
    - Whitehats brasileiros não valorizam ou admitem participar.

Ecossistema de segurança (3)

- Whitehats
  - Tão radicais quanto os blackhats
  - Códigos de ética demais
    - (ISC)², ISSA, ISACA, SANS GIAC, ”hacker ético”
    - Brasileiro é anti-ético por natureza
    - Ética é mais do que um código escrito por estrangeiros
    - Ética tem mais a ver com educação, valores e índole
      - Não vai aprender no trabalho
      - Se você não aprendeu com a vida e com os pais esqueça



Ecossistema de segurança (4)



Ecossistema de segurança (5)

- Whitehats (2)
  - Chuck Norris code of ethics poster
    - http://www.chucknorris.com/html/shopping3.html
  - Incoerências
    - Sua caixa de ferramentas é cheia de ferramentas hackers - Nmap, Metasploit, etc.
    - Aparente desprezo por qualquer atividade hacker brasileira
    - Entretanto...

Ecossistema de segurança (6)

- Whitehats (3)
  - Participar da DEFCON é legal, participar da Black Hat é legal (Las Vegas!)
  - Evento não precisa se ”esconder” no final de semana
  - Brasileiros em geral: TUDO de fora é melhor

Ecossistema de segurança (7)

- Academia
  - Universidades e centros de pesquisa
    - Federais e estaduais principalmente
    - Unicamp, USP, UFSC, UFPE, etc.
    - Provavelmente os melhores programadores do Brasil
  - Eventos
    - CGI.br GTS (½ corporativo), SSI (morto), SBC SBSeg
    - Formalidade acadêmica
    - Honeypots, honeypots, honeypots...

Ecossistema de segurança (8)

- Academia (2)
  - Existem hackers, mas aparentemente não aproveitam o potencial
  - Referências: quase sempre estrangeiros
  - Muita teoria, poucos produtos que você use
    - Framework, paradigma, palavras o sucesso!
  - Eventos ”hacker” para esta comunidade
    - FISL, eventos ”livres”
  - Eventos bem divulgados como H2HC colaboram

Ecossistema de segurança (9)

- Empresas
  - Profissional de segurança ”pasteurizado” (Paulo T.)
  - Formação em faculdades de primeira linha, certificação CISSP (vendor neutral)
    - Sem isto você é periferia para RH
  - Não assuma que só existem não-hackers
    - Caminhos diferentes na vida

Ecossistema de segurança (10)

- Empresas (2)
  - À espera do próximo all-in-one
    - Eles não tem o tempo que muitos tem
  - Alguns cairam na área de segurança por acaso
  - Um chefe para deixar feliz
  - Nem tudo em segurança é divertido

Ecossistema de segurança (11)

- Grupos de segurança
  - CERT.br, CERT.org, CAIS, CTIR Gov, etc.
- Não se engane: cada um cuida de seus clientes
- Embora alguns prestem serviços públicos eles foram criados com algum propósito
- Missão é cuidar de sua própria parte da internet
- Cada um tem um ponto de vista sobre vocês

Ecossistema de segurança (12)

- Grupos de segurança (2)
  - Do seu ponto de vista não-whitehat no Brasil é criminoso potencial
  - Realmente tratam de muitos problemas
  - Se hackers brasileiros não criam produtos
    - ”Eles” continuam a usar ferramentas hacker de fora
    - Eles não tem razões para acreditar que haja alguma coisa de útil no Brasil. Sem reputação.
    - H2HC evoluiu mas ainda pode ajudar a quebrar o estigma hacker = botnets | phishing | defacements | carders

Alguns problemas

- Poucos ”espaços de convivência” populares no Brasil
  - Lista CISSPBR – deveria ser apenas CISSP
  - ISTF
  - Lista GTS-L (fechada) – muito formal, longos períodos de silêncio
  - Listas SecurityGuys (malas!), PericiaForense (DoS no mailbox)
- Concepção errada: lista de CISSP considerada (e aceita) como principal lista do Brasil.

Alguns problemas (2)

- Ego
  - Msc, PhD vs. CISSP, CISA, CISM, etc.
    - Certificação não é título
  - Certificações não substituem talento
  - Reputação se constrói, mesmo sem certificações

Alguns problemas (3)

- Ego (2)
  - Enough already:

```
Re: Ferramenta Y

Escrevi sobre este assunto em meu blog há 6 meses
atrás. O post está no link:

http://blog.example.com

Atenciosamente,
John Doe da Silva, CISSP

> Prezados,
> Como altero o parâmetro X da ferramenta Y?
```

Alguns problemas (4)

- Ego (3)
  - Chega!
  - Se ninguém além de bots visitam seu blog...
    - Talvez ele seja irrelevante
    - Talvez fazer um comentário de uma linha com um link para outro post de blog não seja valorizado
    - Fique na sua. Link na assinatura é mais apropriado.
    - Enchente de informações. Você precisa se destacar.

Alguns problemas (5)

- É interessante assinar as poucas listas do Brasil para saber o que acontece
- Se você não gosta da lista saia
- Não gosta de não-whitehats? Não venha na H2HC.
- Não gosta de engravatados e assuntos nada emocionantes? Não vá no CNASI, SecurityWeek.

Alguns problemas (6)

- Lá Eles! (gíria de baianos)
- Cada um no seu quadrado!

Alguns problemas (7)

- Poucos eventos conseguem reunir todos os chapéus
- YSTS 1.0, YSTS 2.0
  - Para mim a balança pesa mais para hacker
- Entretanto
  - Palestrantes do lado academia, do lado corporativo, do lado hacker em harmonia
  - Adriano Cansian (GTS), Emmanuel Goldstein (2600), Anderson Ramos (ISC)², dum_dum

Alguns problemas (8)

- Mais
  - Apoio da ISSA
  - Mais do que um logotipo
- Por que funciona?
  - Os participantes se sentem especiais
  - Nome engraçado, apenas 1 dia, infeliz segunda-feira, mas funciona assim mesmo
  - Organização

Alguns problemas (9)

- Mais uma vez: brasileiro padrão espera tudo de fora
  - Acho que você não é um índio
  - Open Source não é traduzir interface e manual!
  - Não seja um índio, você sabe inglês
  - Todos já sabem que é livre. Chega de traduzir, jesuíta.

Alguns problemas (10)

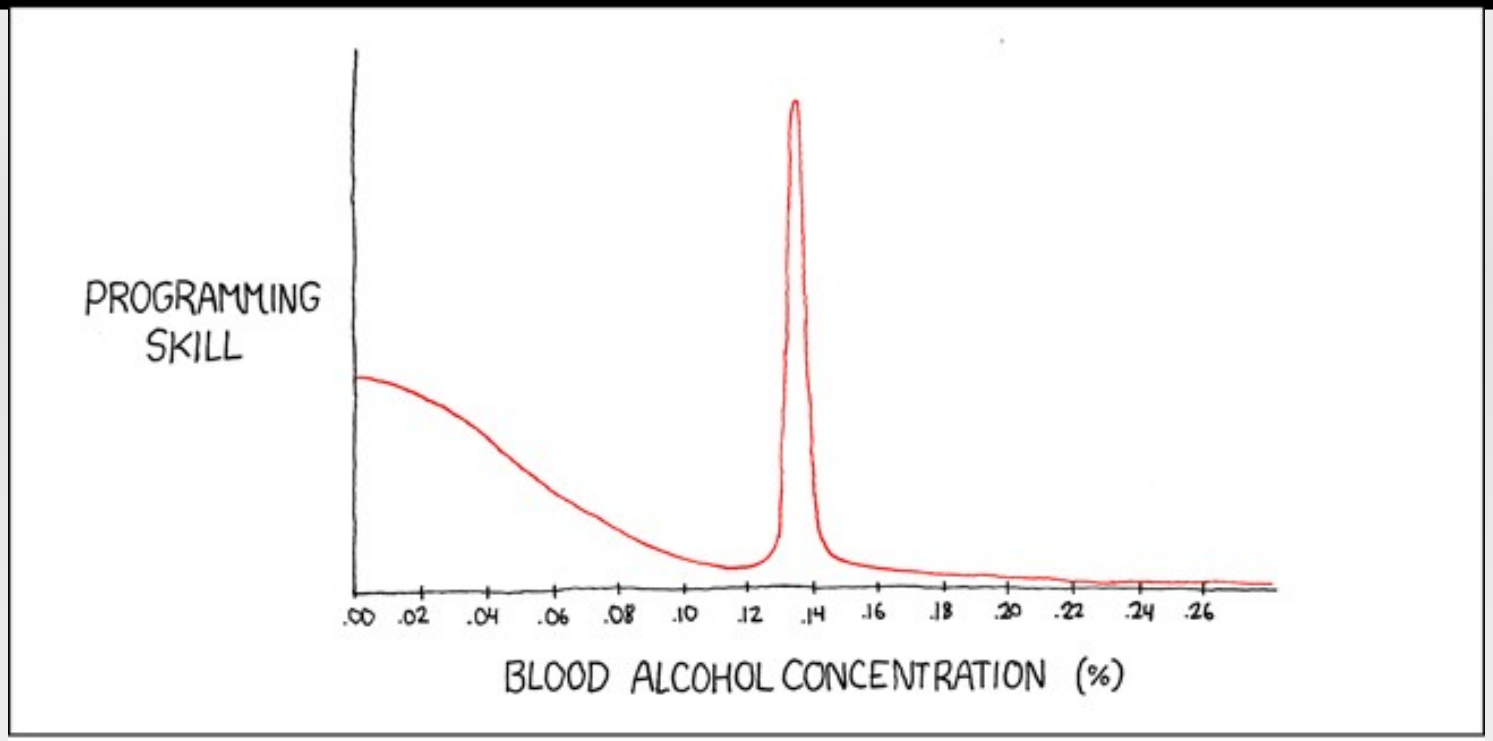
- Quer ajudar o Software Livre? Esqueça o Babelfish
  http://meiobit.pop.com.br/meio-bit/software/quer-ajudar-o-software-livre-esqueca-o-babelfish
- Quer apoiar o Open Source? Então pare de encher o saco e coloque a mão na massa
  http://meiobit.pop.com.br/meio-bit/open-source/quer-apoiar-o-open-source-entao-pare-de-encher-o-saco-e-colo
- Upcoming changes to the CISSP exam and the drama associated with it
  http://www.cccure.org/modules.php?name=News&file=article&sid=1338

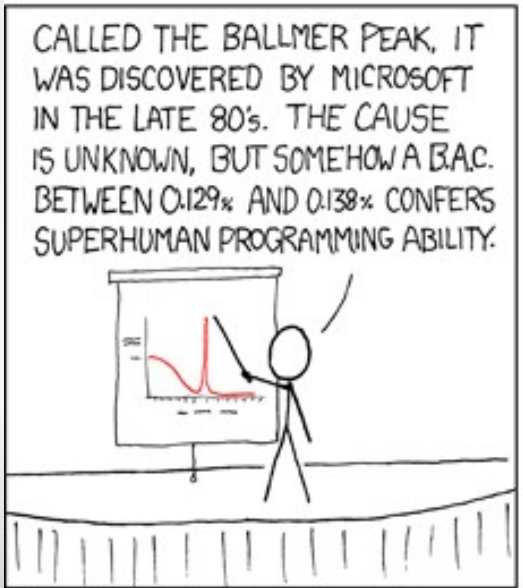
Alguns problemas (11)

- Mais uma vez: brasileiros não são éticos por padrão
  - Bico calado se a conta vem errada pra menos, notas falsas em diárias de viagem, computador ”vem com Windows”, Lei de Gerson, carteira de estudante (ingressos caros pra tudo - mistério!), ...
  - Políticos não são mais corruptos, simplesmente tem acesso a mais dinheiro. Você rouba chopp do garçon.

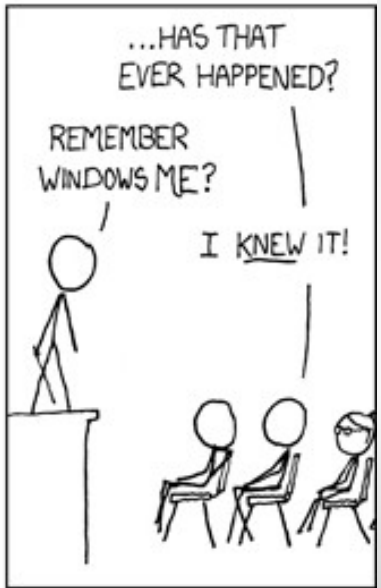
Alguns problemas (12)

- Mais uma vez: brasileiros não são éticos por padrão (2)
  - Incoerência
    - Celular desbloqueado, cópia de DVDs, Wii / Xbox 360 desbloqueado, Windows XP ”desbloqueado”, iPhone funcionando no Brasil, etc.
    - Hackers já estão por toda parte.


PROGRAMMING SKILL
.00 .02 .04 .06 .08 .10 .12 .14 .16 .18 .20 .22 .24 .26
BLOOD ALCOHOL CONCENTRATION (%)


CALLED THE BALLMER PEAK. IT WAS DISCOVERED BY MICROSOFT IN THE LATE 80's. THE CAUSE IS UNKNOWN, BUT SOMEHOW A B.A.C. BETWEEN 0.129% AND 0.138% CONFERS SUPERHUMAN PROGRAMMING ABILITY.


HOWEVER, IT'S A DELICATE EFFECT REQUIRING CAREFUL CALIBRATION— YOU CAN'T JUST GIVE A TEAM OF CODERS A YEAR'S SUPPLY OF WHISKEY AND TELL THEM TO GET CRACKING.


...HAS THAT EVER HAPPENED?
REMEMBER WINDOWS ME?
I KNEW IT!

Idéias

- Nada contra as listas atuais mas
  - Precisamos de segmentação
  - Listas realmente abertas
  - Vou tentar resolver isto do meu jeito
- Colabore com projetos brasileiros
  - Beholder – interface gráfica, Cygwin + Windows (?)
  - OSSEC (Daniel Cid), malware.com.br
  - chkrootkit

Idéias (2)

- Sugestões
  - Wi-Fi: várias ferramentas juntas podem formar um Poor Man's Aruba
    - Beholder + Kismet IDS distribuído
  - Investigar problemas em sistemas do seu dia-a-dia
    - Muita informatização incompetente no Brasil

Idéias (3)

- Aproveite seu tempo ocioso de faculdade
  - Projetos finais de verdade
  - Procure o departamento de empreendedorismo da sua universidade
  - O modo hacker de trabalhar muitas vezes não se adapta com empresas convencionais
    - Abra a sua então

Conclusões

- Todos são importantes no ecossistema
  - Alguém precisa escrever políticas e fazer outras coisas entediantes (para você)
- Seja menos radical (todos os chapéus)
- Hackers também precisam se organizar e produzir
  - hackerspaces.org
  - Espalhe o que é ser hacker

Conclusões (2)

- Justiça com as próprias mãos? Deixe Darwin trabalhar
- Menos tradução, mais produção.
- Reputação é construída aos poucos
  - Vocês já começaram
- Pense nos sites de segurança do Brasil
  - Isso mesmo, não há quase nada.
  - A maioria aceita e aguarda o que vem de fora
- Não seja um engenheiro de obra pronta!
  - Participe da construção também

Obrigado!

Ronaldo Vasconcellos
ronaldocv at securityguys.com.br

IRC:
#securityguys @ irc.freenode.net
(6667/TCP / 8000/TCP)