PEN TEST
Afinal, o que é?

Paulo Renato
Security Specialist & GNU/Linux
LPIC – 1 | LPIC – 2 | NCLA | DCTS| VSP-4 | VSTP-4

Apresentação

Paulo Renato Lopes Seixas

- Especialista em projetos de redes corporativas e ambientes para consolidação da virtualização;

- Graduado em Sistemas de Informação pela Universidade Estadual de Goiás;

- Implementação de soluções para reduções de custos em TI, projetos de Redes e Treinamentos especializados utilizando Software Livre, tais como GNU/Linux para Segurança de Redes como Firewall, Pen-Test e Segurança de redes baseado na norma ISO 27002 (antiga ISO/IEC 17799);

- Gerente de Outsourcing;

- Certificado LPIC-2 (Linux Professional Institute Nível 2);

- Certificado VSP-4 | VTSP-4 | NCLA | DCTS

PEN TEST
A ARTE DA INSTRUSÃO

Alguns termos

- Hacker – Pessoa com grande habilidade técnica
- Cracker – Invasor de sistemas
- White Hat – Hacker do bem
- Black Hat – Hacker do mal

Afinal, existe hacker do bem ou do mal ?????

Segurança da Informação

Segurança da Informação

- Segundo a norma ISO/IEC 27001, **é a proteção contra** um grande número de **ameaças** às **informações**, de forma a assegurar a continuidade do negócio, **minimizando danos** comerciais e maximizando o retorno de possibilidades e investimentos.
- o conceito não está restrito somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. **Se aplica a todos os aspectos de proteção de informações**.

Segurança da Informação

A Tríade da Segurança da Informação

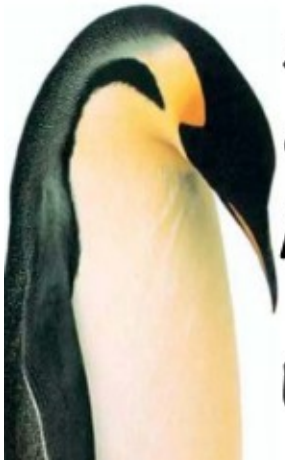
- Confidencialidade
  - Nós podemos ou conseguimos manter segredo ?
- Integridade
  - O que é ou Quem é você ?
  - Sua mensagem foi alterada ?
- Disponibilidade
  - Eu consigo acessar as bases de informações sempre que desejo ?

INTRODUÇÃO
TESTE DE INTRUSÃO

NTAMonitor (09/2007):

"Cerca de 90% dos websites organizacionais contêm pelo menos uma falha que permita a utilizadores clandestinos ganhar acesso ao sistema ou comprometer a sua disponibilidade!"

INTRODUÇÃO
TESTE DE INTRUSÃO



"Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas..."

Extraído da obra: "A Arte da Guerra"

O que é PEN TEST ?

E a abreviação da palavra inglesa “Penetration Test”, que em português significa “Teste de Penetração”.

- **é o processo de identificar e explorar vulnerabilidades**, tentando utilizar dos mais diversificados métodos que um atacante pode utilizar, tais como ataques lógicos, físicos e engenharia social.

- é uma parte fundamental da segurança da informação, que permite de forma rápida identificar vulnerabilidades e o seu devido risco.

Pen Test != Análise de Vulnerabilidade

- A análise de vulnerabilidade por não explorar as possíveis falhas, muitas vezes tende a gerar relatórios com um número alto de falsos positivos.

- Os dados utilizados são superficiais, o que provoca a idealização de possíveis vulnerabilidades.

- Devido a esses fatores, fica impossível relacionar o risco que uma vulnerabilidade explorável pode causar.

- Pen Test é uma forma eficaz de determinar o risco real das vulnerabilidades, e conseqüentemente prioriza-las de forma correta.

PEN TEST
Aspectos importantes

- **Contrato com valor jurídico** especificando de forma clara os alvos, objetivos, tipos de ataques que podem ser realizados, prazos, limites, confidencialidade e **autorização da organização.**

- A equipe de segurança **não deve estar ciente** da contratação do Pen Tester por uma equipe externa, caso contrário provavelmente medidas complementares e monitoramento mais severo serão utilizados durante o Pen Test, dessa forma não simulando um ataque em condições reais.

Porque realizar um PEN TEST ?

- Simulação real de ataque, que poderia ser um cracker, funcionário insatisfeito, espionagem industrial, etc.

- O mundo atual gira em torno do dinheiro. Qual é um dos bens mais preciosos para gerar capital ?

A informação!

Protegendo as suas informações você estará livre da concorrência desleal.

TESTE DE INTRUSÃO

Anatomia dos Ataques

- **Footprint**

  Visa a obtenção de informações iniciais e relevantes do sistema alvo, uso de ES.
  É a parte mais demorada, é a fase do planejamento do ataque.

- **Fingerprint**

  Identificar o Sistema operacional da vítima.

TESTE DE INTRUSÃO

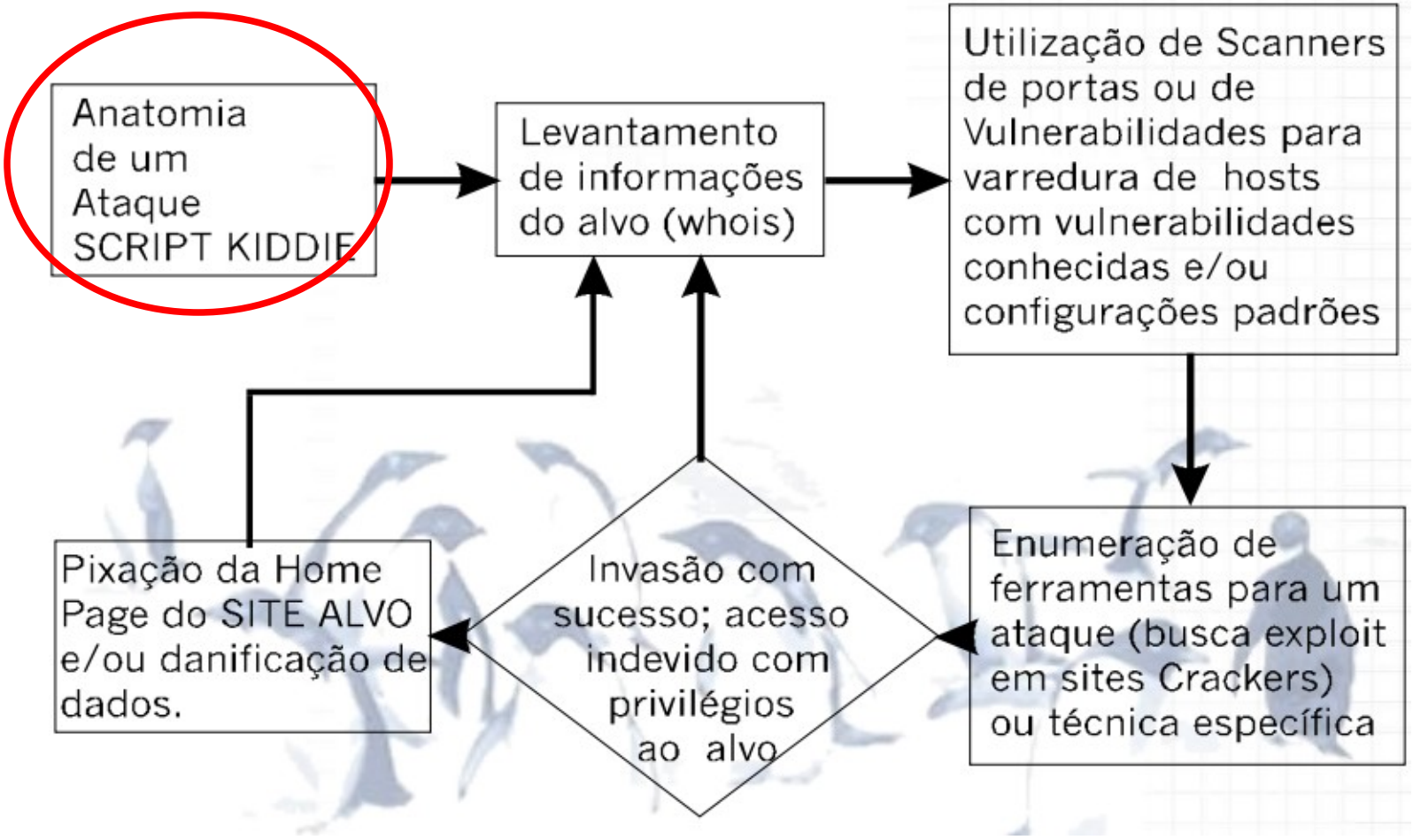
Anatomia de um Ataque

- **Enumeração**

  Fase de scaneamento de portas e serviços, objetivando a enumeração do alvo.

TESTE DE INTRUSÃO

Estágios dos Ataques



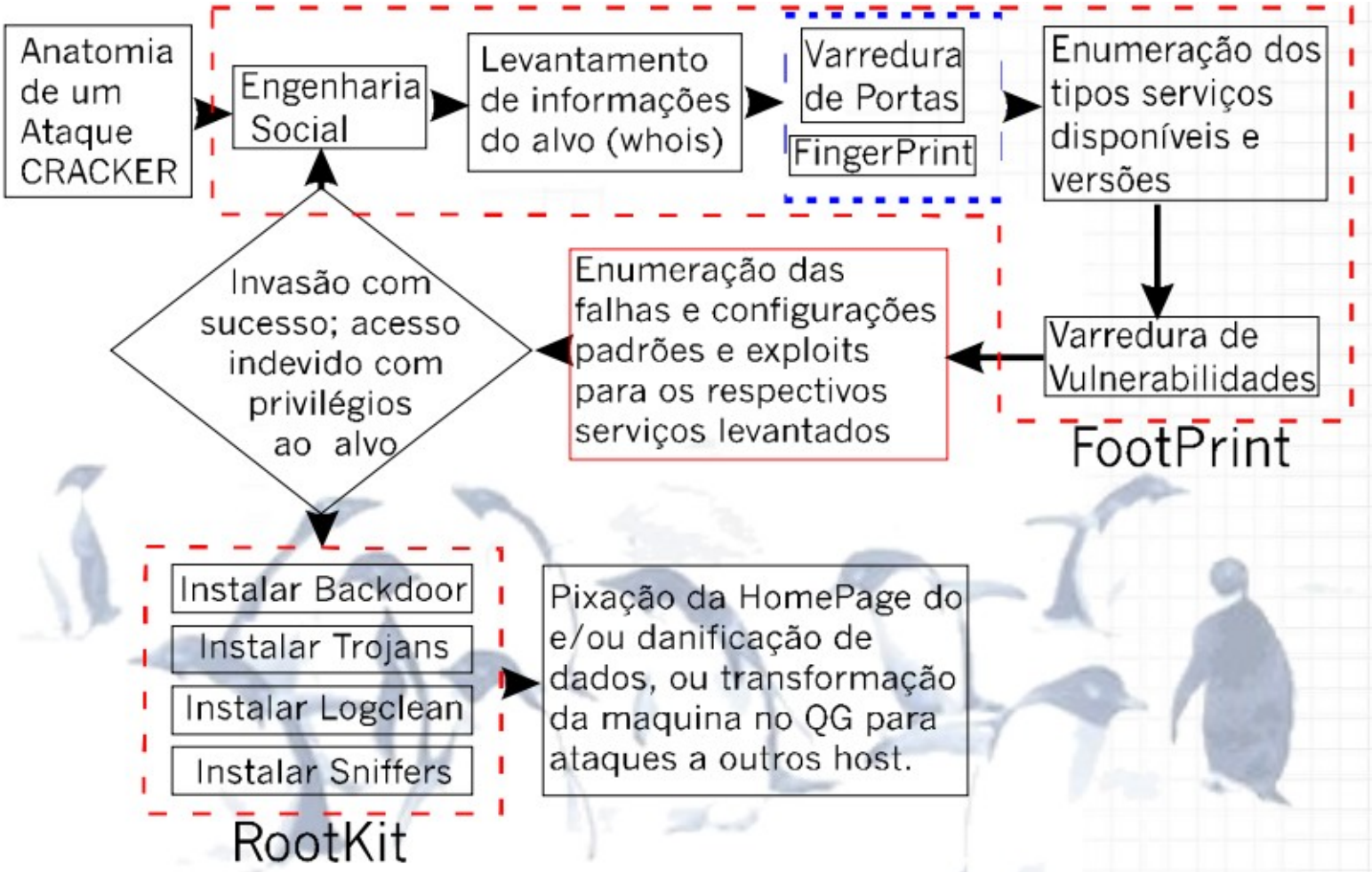
TESTE DE INTRUSÃO

Ataque do Script kiddie

* http://www.rnp.br/newsgen/9905/kiddie.html

TESTE DE INTRUSÃO

Estágios dos Ataques



TESTE DE INTRUSÃO

Tipos de Pent-Test

- White Box: Conheçe pouco (IP,HOST)

- Black Box: Caixa fechada - sem know

- Gray Box : Mistura do White e Black

TESTE DE INTRUSÃO

Tipos de Pent-Test

- **Blind:**

  Nessa modalidade o atacante não conhece nada do ambiente, porém a vítima sabe que o ataque será feito e o que será feito.

TESTE DE INTRUSÃO

Tipos de Pent-Test

- **Double Blind:**

  Nessa modalidade o atacante não conhece nada do ambiente, e a vítima não sabe que o ataque será feito e o que será feito.

ENGENHARIA SOCIAL

ENGENHARIA SOCIAL

O QUE É?

São as práticas utilizadas para **obter acesso a informações importantes ou sigilosas** em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas.

TESTE DE INTRUSÃO

Engenharia Social

- Podemos considerar a engenharia social como a arte de enganar pessoas para conseguir informações, as quais não deveriam ter acesso.

“Não existe patch para a burrice humana”

ENGENHARIA SOCIAL

Tipos de ES

* **Phishing;**
* **Vishing;**
* **Trojan house;**
* **Shoulder surfing** (Aeroporto);
* **Rush Authentication;**
* **Dumpster Diving;**

TESTE DE INTRUSÃO

Engenharia Social

- **Dumpster Diving**

- É o ato de vasculhar lixeira para encontrar informações, que aparentemente "não tem valor" para a organização.

ENGENHARIA SOCIAL

Phishing

* http://www.rnp.br/cais/fraudes.php

ENGENHARIA SOCIAL

Phishing - Fatos atuais

IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/

Receita Federal. - www.receita.fazenda.gov.br

Receita Federal

Prezado, casteffen@terra.com.br

Consta em nosso sistema, que o CPF cadastrado para este e-mail (casteffen@terra.com.br) possue pendências em nossos sistemas (SPC E SERASA), nas quais não foram quitadas em suas respectivas datas de vencimento.

Pedimos a vossa atenção a este comunicado, pois, medidas legais serão adotadas, tais como Bloqueio no Cadastro Nacional de Pessoa Física, bem como no Cadastro Nacional de Pessoa Jurídica.

Você tem o prazo de 30 dias para imprimir o boleto e pagar em qualquer casa lotérica ou agência bancária.

Visualize o extrato do IRPF para maiores esclarecimentos.

Clique no botão abaixo para visualizar o extrato do IRPF.

IRPF

EXTRATO

Receita Federal. - www.receita.fazenda.gov.br

ENGENHARIA SOCIAL

Phishing - Fatos atuais

ENGENHARIA SOCIAL

Phishing - Fatos atuais

Big Brother Brasil

Fique de olho nas emoções do jogo!

Concorra agora mesmo a um Fiat Punto T-JET 2010 para esse próximo paredão clique aqui!

Lembre a trajetória de Anamara
Baiana de Juazeiro, Anamara entrou na casa mais vigiada do Brasil alertando: "Se não gosto de alguém, falo na cara". E ela cumpriu a promessa. "Até o final eu voto em você", disse a Dourado, após ser chamada de "falsa" e "cínica" pelo gaúcho. "Você é lunática, complexada", disparou para Elenita numa discussão durante o Mercadinho. Já com Alex e Eliéser, o desentendimento foi por economia de óleo de cozinha. Anamara também se estranhou com Sérgio, que a eliminou da Prova do Líder antes que ela conseguisse ouvir uma mensagem gravada pela mãe. A baiana falou tanto na casa que chegou a incomodar alguns brothers. "Ela fala demais", afirmou Cláudia certa vez. "Quem fala muito, se contradiz", opinou Eliéser sobre a baiana.

Baixe para assistir ao vivo o BBB 10 na internet e cadastre-se para concorrer o Fiat Punto, Clique aqui.

Compromisso com o Brasil, pioneirismo e inovação como características marcantes, produtos de alta qualidade e tecnologia, design admirado, respeito ao consumidor e responsabilidade social. Estes atributos compõem o perfil da Fiat Automóveis, uma das empresas automobilísticas com maior crescimento no mercado brasileiro e líder de vendas no setor.

FIAT

ENGENHARIA SOCIAL

Engenharia Reversa

* A vitima pedindo ajuda ao atacante;

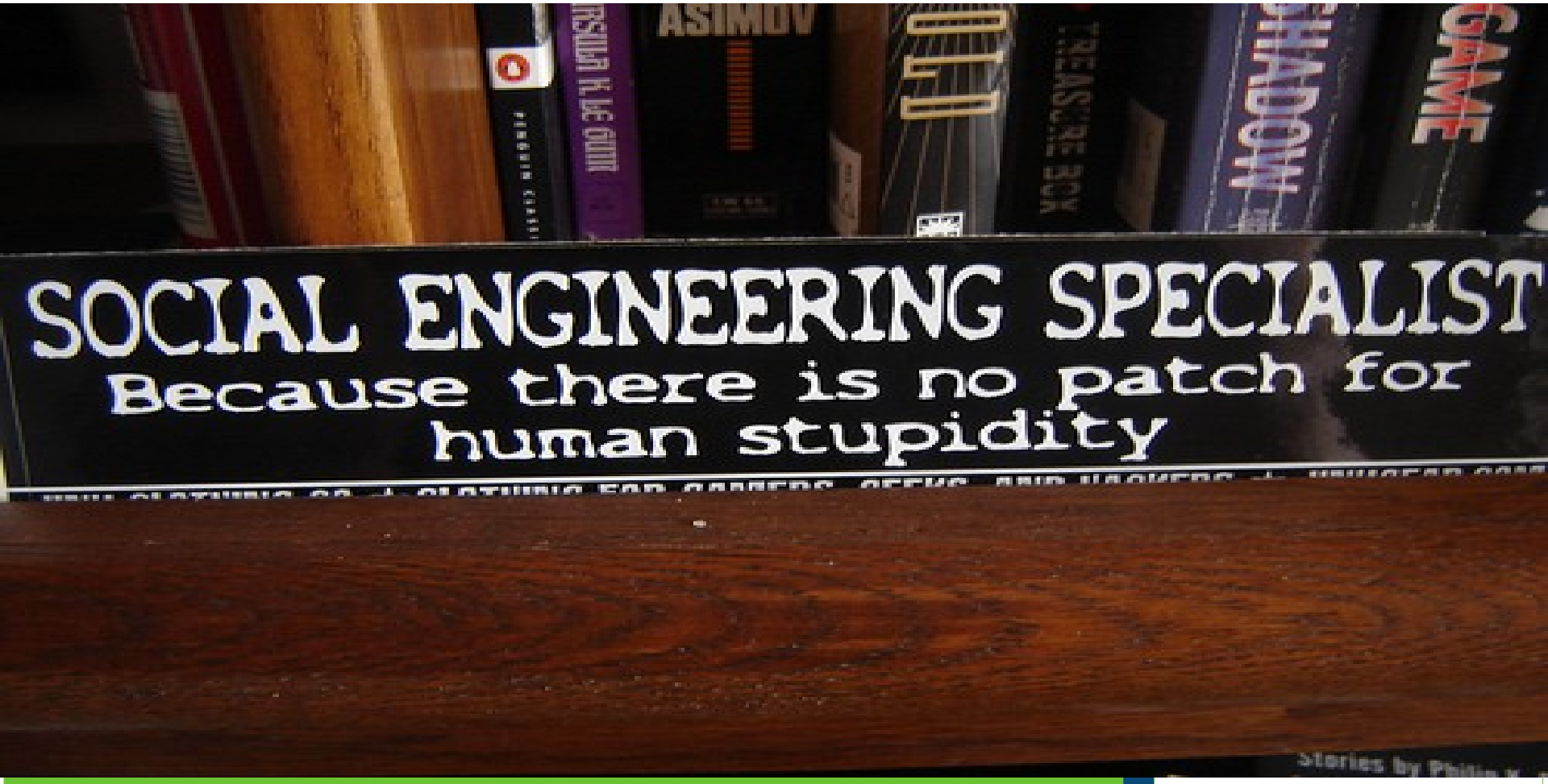
ENGENHARIA SOCIAL

Exemplo

- Obtendo uma pizza gratuita(inglês)

http://www.youtube.com/watch?v=z68gZJwdAAg

Porque a engenharia social é um sucesso?



ENGENHARIA SOCIAL
CONTRAMEDIDAS

- Implementar uma **política de segurança** que proíbe a divulgação dos números internos de funcionários, contratados, consultores e temporários, que proíbe copias de documentos e/ou qualquer outro tipo de documento pessoal do funcionário para pessoas que não são da empresa ou departamento que não compete ter estas informações. Mas como identificar uma pessoa que não é funcionário da empresa?

- Todo empregado deve ser treinado para verificar não apenas a identidade do solicitante, como também a necessidade que o requisitante tem de saber;

- Todos da Organização devem ser **treinados para ter um grau apropriado de suspeita e cuidado ao serem contactados por alguém que não conhecem pessoalmente**, sobretudo quando alguém solicitar algum tipo de acesso a um computador ou rede de dados;

- Nunca compartilhe suas senhas;

- Não discuta informações confidencias em ambientes públicos;

- Nunca clique em links que desconhece, principalmente oriundo de email suspeitos;

- Sempre **CONFIE, DESCONFIANDO.**

- Portanto, a segurança da sua empresa depende da sua **EDUCAÇÃO** .

LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

É o processo de **acumular dados relacionados a um ambiente de rede** específico, normalmente com o objetivo de encontrar formas de invadir esse ambiente..

LEVANTAMENTO DE INFORMAÇÕES

Por onde começar?

Inicie visitando o site do seu alvo.

Tente obter informações no site, como email's, nomes, contato telefônico, endereço, contatos técnicos, etc.

LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

whois - pode fornecer nomes de domínio, telefones, e-mails, redes associadas ... relacionadas a uma organização.

whois site

```
$ whois www.3way.com.br
```


LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

Obter informações de roteamento -

http://www.ripe.net/ris/index.html

Informações ASN

```
$ traceroute -A www.3way.com.br
```


LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

Looking glass

http://www.ris.ripe.net/cgi-bin/lg/index.cgi

Outras ferramentas online

$ http://www.ripe.net/tools/

LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

Sam Spade - Whois

www.samspade.org

Whois/Dig online

www.geektools.com/whois.php

www.geektools.com/digtool.php

LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

Busca gráfica

www.kartoo.com

Consultas online

www.netcraft.com

LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

Maltego (Mapeamento de hosts de forma dinâmica)

LEVANTAMENTO DE INFORMAÇÕES

FOOTPRINT

Archive.org (Páginas web antigas)

www.archive.org

Outras ferramentas:

www.sensepost.com/research_tools.html

FOOTPRINT

CONTRAMEDIDAS

- Implementar obscuridade nos serviços (banners);
- Restrição a consultas DNS;
- Utilizar as últimas versões dos softwares;
- Patches de atualização

Configuração bem feita + Obscuridade = Maior grau de Segurança

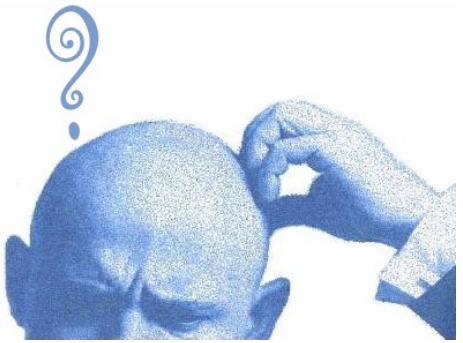
LEVANTAMENTO DE INFORMAÇÕES

FINGERPRINT

Objetiva determinar versão e tipo de sistema operacional da máquina alvo.

Qual sistema operacional?

Qual a versão?



LEVANTAMENTO DE INFORMAÇÕES

FINGERPRINT ATIVO

É o método que usa respostas enviadas a pacotes TCP ou ICMP.

Utiliza manipulação de flags no cabeçalho e compara com 'padrões' para determinar o SO.

ICMP usa menos pacotes que TCP, por isso é mais furtivo.

LEVANTAMENTO DE INFORMAÇÕES

FINGERPRINT PASSIVO

Nesse método não há envio de pacotes, mas técnicas de sniffing para analisar o tráfego normal da rede.

Utilizado em serviços publicamente disponíveis para iniciar o reconhecimento do SO.

LEVANTAMENTO DE INFORMAÇÕES

CAPTURANDO BANNER DE APP

Telnet

```
#telnet vm-vitima01 21
```

nc

```
#nc vm-vitima01 22
```

LEVANTAMENTO DE INFORMAÇÕES

CAPTURANDO BANNER DE APP

Echo + nc

```
echo -e "GET / HTTP/1.1\n" | nc  www.kernel.org 80 | egrep
   '^Server:'
```

ftp

```
#ftp vm-vitima01
```


LEVANTAMENTO DE INFORMAÇÕES

CONTRA MEDIDAS

HARDENNING

Executar procedimentos de hardenning, utilizar da técnica de obscuridade de serviços.

Verificar resposta do servidor de nomes;

Examinar informações do registro do domínio;

Encontrar proprietário do domínio;

Buscar informações em redes P2P;

Realizar testes de engenharia social;

VARREDURA DE REDES

VARREDURA DE REDES

NMAP

É um portscan que pode ser usado para verificar as portas abertas em determinado host.

nmap <opcao> <endereco>

-sS	***-sP***	***-p***	***-v***
-sT	***-sF***	***-F***	***-o***
-sU	***-O***	***-v***	***-g***

VARREDURA DE REDES

SCANNERS DE REDE

NMAP

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	`-sS`	YES	YES	NO
TCP connect() Scan	`-sT`	NO	YES	NO
FIN Scan	`-sF`	YES	YES	NO
Xmas Tree Scan	`-sX`	YES	YES	NO
Null Scan	`-sN`	YES	YES	NO
Ping Scan	`-sP`	NO	NO	NO
Version Detection	`-sV`	NO	NO	NO
UDP Scan	`-sU`	YES	NO	YES
IP Protocol Scan	`-sO`	YES	NO	NO
ACK Scan	`-sA`	YES	YES	NO
Window Scan	`-sW`	YES	YES	NO
RPC Scan	`-sR`	NO	NO	NO
List Scan	`-sL`	NO	NO	NO
Idlescan	`-sI`	YES	YES	NO
FTP Bounce Attack	`-b`	NO	YES	NO

VARREDURA DE REDES

SCANNERS DE REDE

NMAP

- Técnica 6: PING SCAN (-sP)

  - Verifica por máquinas ativas na rede.

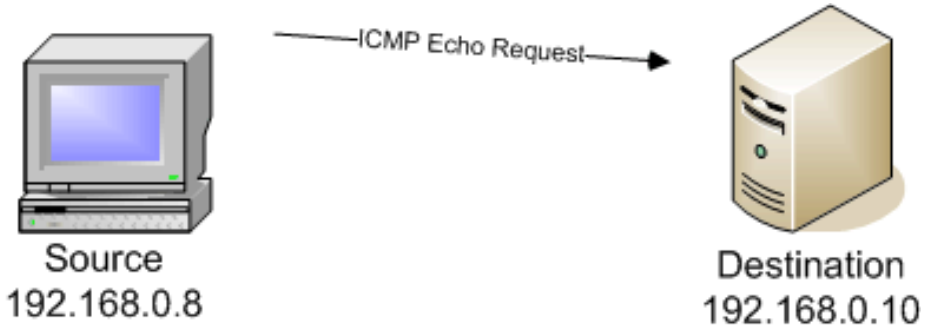
  - Utiliza do protocolo ARP para “descobrir” as máquinas ativas na rede.

VARREDURA DE REDES

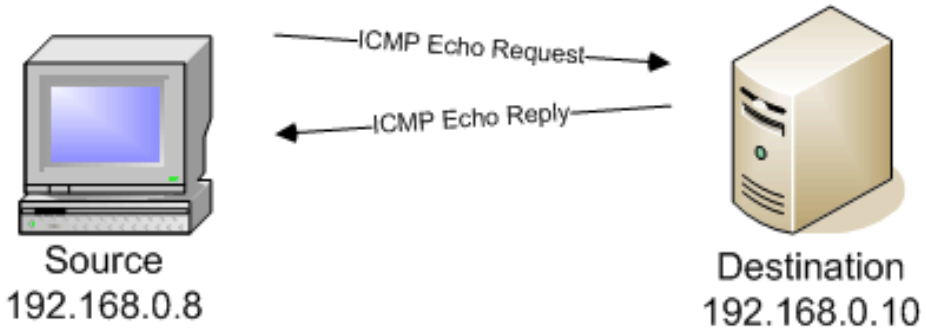
SCANNERS DE REDE

NMAP

- Técnica 6: PING SCAN (-sP)

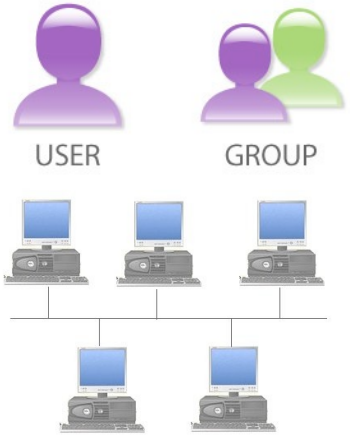


MÁQUINA DESATIVADA



MAQUINA ATIVA

ENUMERAÇÃO DE SERVIÇOS



COMPUTERS

PASSWORDS

ENUMERAÇÃO DE SERVIÇOS

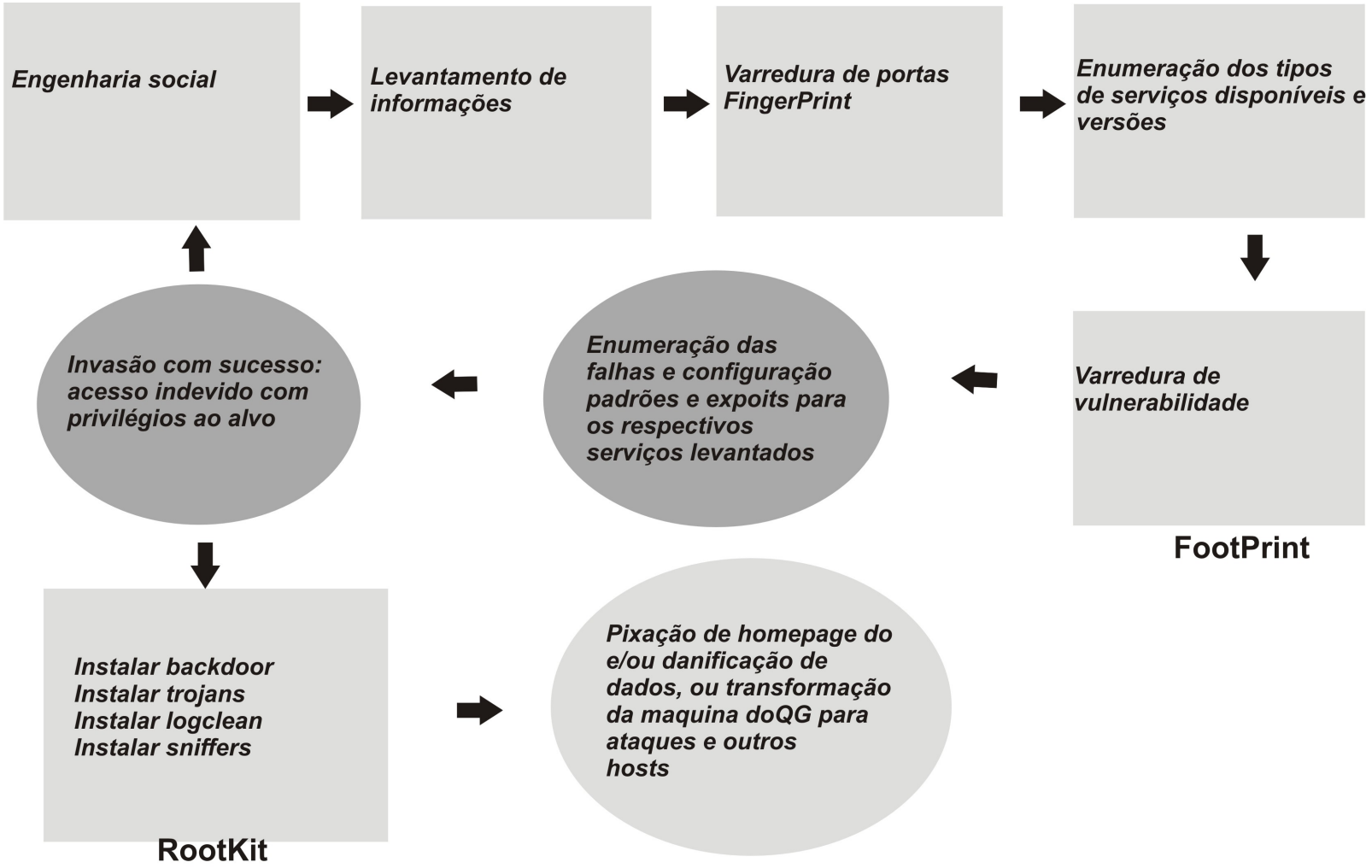
FERRAMENTAS

Na VM-ATACANTE01

```
#dig -t axfr vitimalocal.com.br @ns1.vitimalocal.com.br

#nmap -sS -v -O vitimalocal.com.br
#nc vitimalocal.com.br 22
#nc vitimalocal.com.br 79
root
```


TESTE DE INTRUSÃO



Pen Test – Passos iniciais:

- Enumeração e identificação de ativos.

- Obter o maior número possível de informações da empresa (nomes de funcionários, e-mail, funcionários que utilizam IM, empresas que prestam serviços, parceiros, clientes, etc).

- Identificar e explorar vulnerabilidades (lógicas ou físicas).

- Elevação de privilégios, para posteriormente alcançar o objetivo previamente definido pelo cliente.

PEN TEST - Benefícios

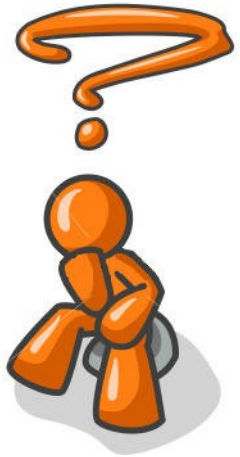
- Levantamento rápido e eficaz da situação real da segurança da empresa.

- Tomada de decisão (e posterior alocação de recursos) baseada em fatos reais.

- Recomendações de Segurança.

PEN TEST :
Afinal, o que é?

Dúvidas ???



PEN TEST
A ARTE DA INTRUSÃO

Em vez de adotar a frase:
"Já está bom", adote esta :
"O bom é inimigo do ótimo"

Não é possível ter 100% de segurança, mas devemos assegurar o máximo que pudermos !

PEN TEST
Afinal, o que é ?

Contato Profissional:
www.3way.com.br
paulorenato@3way.com.br

Obrigado !!!

Contato Pessoal
blog.netsolution.eti.br
paulorenato@netsolution.eti.br