

# (In)Segurança Virtual

## Técnicas de Ataque e Defesa

Expotec 2009 – IFRN- Campus Mossoró

Nícolas André - [nicholasandreoliveira9@gmail.com](mailto:nicholasandreoliveira9@gmail.com)

[www.iotecnologia.com.br](http://www.iotecnologia.com.br)

Mossoró-RN  
Setembro-2009

# O que é preciso!

- Engenharia Social
- Pensamento Hacker
- Anonimato
- Conhecimentos básicos : redes, programação, arquitetura de sistemas operacionais

# O que é preciso!

- Engenharia Social e Segurança são termos intimamente ligados.
- Ataque indireto:
  - Utilização de ferramentas de invasão.
- Ataque direto:
  - Contato pessoal.
- Suas armas: Pesquisa e impostura.
- É preciso ser quem você não é.
- Os proxy são seus amigos!



# O caminho da informação

- Funcionários descontentes
- Apelo Sentimental
- Programação neurolinguística
  - acompanha-acompanha-acompanha-comanda
- A internet é sua amiga
  - O Google está aí para ser usado.

# Vulnerabilidades

- É preciso saber como se aproveitar delas!
- Sistema Alvo: Windows ou \*Unix(Linux, BSD etc)?
- O que é preciso para se aproveitar dela?
- Três tipos de Vulnerabilidades:
  - Falhas que afetam a disponibilidade da máquina.
  - Falhas que permitem o acesso limitado ao sistema.
  - Falhas que permitem a execução de código arbitrário na máquina.

# Buscando Vulnerabilidades

- Scanner de portas
  - Nmap
- Scanner de Vulnerabilidades
  - Nessus
  - Nikto
  - Vetescan
- Scanner de SO
  - Queso
  - Cheops



# Requisitos para um ataque e defesa bem sucedido

PLANEJAMENTO + CONHECIMENTO = INVASÃO

PLANEJAMENTO + CONHECIMENTO = DEFESA

# Partes de um Ataque

- Observação
- Busca
- Invasão
- Manutenção
- Evasão



# Como se defender

- Firewall bem configurado, com políticas de segurança bem definidas.
- Serviços que não são usados deverão ser desligados.
- Mudar a porta padrão dos serviços utilizados no servidor.
  - Servidor FTP(porta 21) – porta 4456
- Sistemas de IDS
- Honeypots

# Honeypots e IDS

- Honeypots:
  - Sistemas que simulam um ambiente vulnerável.
  - Uma cilada para o Hacker.
- IDS:
  - Sistema de detecção de intrusos.
  - Roda em em segundo plano em tempo real, tentando detectar uma possível intrusão.

# Dentro do sistema, o que fazer?

- Qual seu objetivo?
- Qual seu nível de acesso?
- Olhe seu planejamento!
- Não demore!
- Não execute comandos desnecessários!



# Saindo da Teoria!

- Técnicas de Ataque

# Antes de tudo!

- Se torne Anônimo!
  - <http://proxy.org/>
  - <http://anonymouse.org/anonwww.html>
  - <http://www.proxy4free.com/page1.html>
  - JAP - [http://anon.inf.tu-dresden.de/index\\_en.html](http://anon.inf.tu-dresden.de/index_en.html)
- Emails anônimos:
  - MixMaster -  
<http://sourceforge.net/projects/mixmaster/files/Mixmaster/3.0/mixmaster-3.0.tar.gz/download>

# Primeira etapa: Observação

- Observe seu alvo!
- Use técnicas de Engenharia Social.
- Obtenha informações por meios legais.
  - Sites de buscas
  - [www.registro.br](http://www.registro.br)
  - Whois
  - \$dig @ns1.mgxtelecom.com.br bf2brasil.com.br AXFR



# Segunda etapa: busca

- Definindo o Alvo!
  - Scaneando várias faixas de endereços ip.
  - Fazendo scan completos em certos ips.
- Scaneando o alvo.
  - Scanner de portas(redes) - nmap
  - Scanners de Vulnerabilidades - Nessus
  - Scanners de SO

# Buscando o alvo

- Verificando se ele está on:
  - Ping ip\_alvo
- Tentando obter um simples esquema da rede:
  - Traceroute ip\_alvo
- Obtendo um esquema mais completo:
  - Cheops
- Descobrendo o Sistema Operacional:
  - Cheops
  - Nessus
  - Nmap



# Buscando portas abertas

- Nmap:
  - Simple scan: `nmap 192.168.0.102`
  - Obtendo informações sobre portas abertas: `nmap -sV 192.168.0.102`
  - Tentando identificar o SO: `nmap -O 192.168.0.102`
  - Half-Open Scan: `nmap -sS 192.168.0.102`
  - Scan UDP: `nmap -sU 192.168.0.102`
  - Scan completo de portas: `nmap -sS -p 0-65535 192.168.0.102`



# Buscando Vulnerabilidades

- Nessus
  - Open Source – Considerado uns dos melhores scanners de vulnerabilidades
  - Utiliza das informações do nmap
- Languard
  - Um scanner pago para windows
  - Didático e fácil de utilizar

# A terceira etapa: O ataque

- Como eu chego ao meu objetivo?
  - SQL Injection
  - Sniffing
  - Spoofing
  - Exploits
  - Dos
  - Quebra de Senhas

# Exploits

- São scripts e programas designados para exploração de vulnerabilidades em um sistema.
  - Detectada a vulnerabilidades → Aplicação de um exploit
- Exemplo prático:
  - Descobre-se no endereço fictício um sistema Unix rodando uma versão antiga do BIND(um servidor DNS), usa-se um exploit para essa versão chamado bindxplt.



# SQL injection

- Através de códigos inseridos nos campos login e senha é possível obter informações valiosas sobre o banco de dados de usuários de determinado site.

| ID | Nome    | Login      | Senha | Admin |
|----|---------|------------|-------|-------|
| 1  | Nícolas | blink182br | 123   | s     |
| 2  | Daniel  | duda       | 321   | n     |
| 3  | José    | jups       | 456   | n     |

# Quebra de Senhas

- Quebradores de senhas
  - Jonh The Ripper
  - L0phtCrack
- Roubando as senhas no windows:
  - HKEY\_LOCAL\_MACHINE\SECURITY\SAM\Domains\Account\Users – pwdump
- No Linux:
  - /etc/passwd
  - /etc/shadow

# Snifers

- São “farejadores” - escutam o que está trafegando na rede.
  - Hunt
  - Wireshark
  - IPtraft

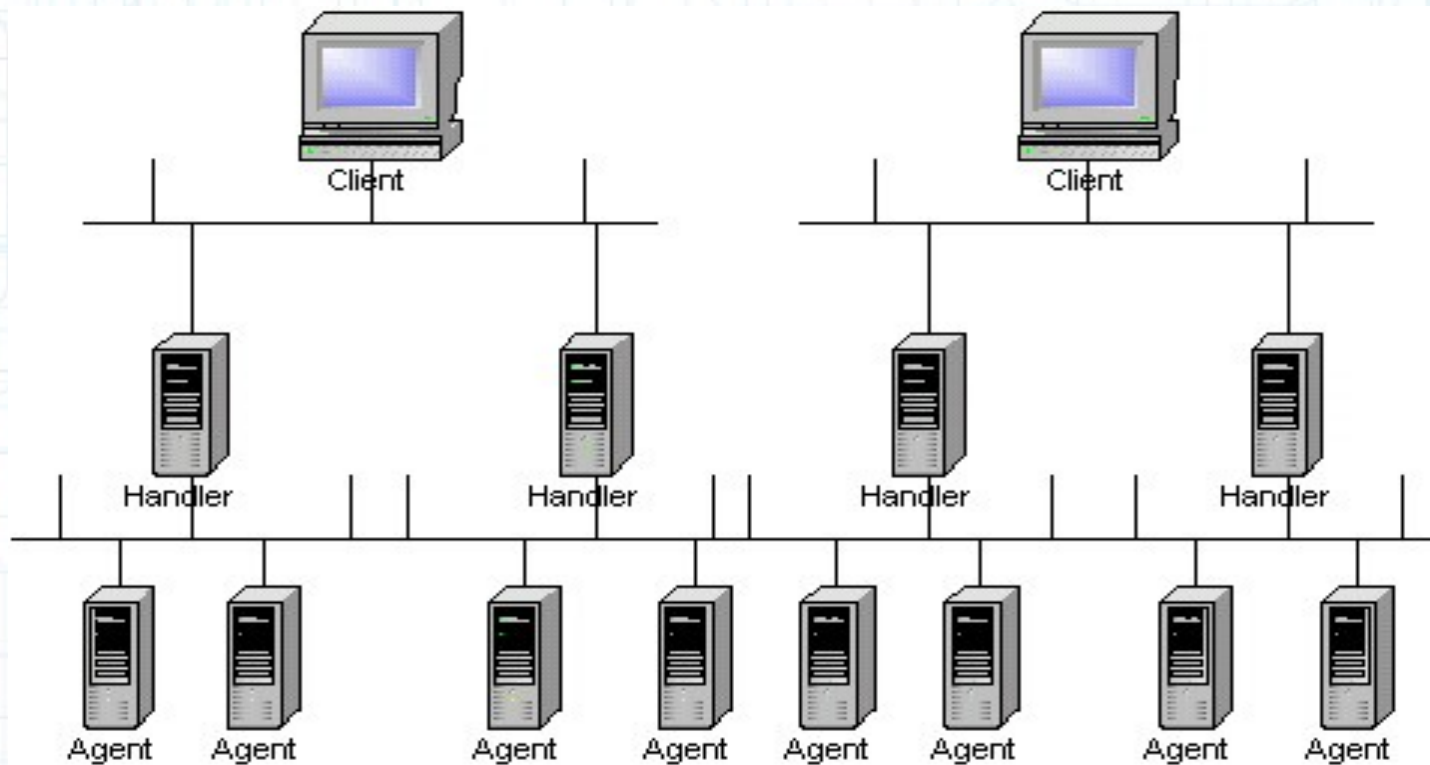


# DoS

- O famoso ataque de negação de serviço
- Consistem em enviar dados que o alvo não consegue suportar, derrubando o alvo.
  - DoS Local
  - Ataque Smurf
  - UDP Flood

# DDoS

- Ataques DdoS se utilizam de várias máquinas para derrubar um alvo.



# “O outro lado da moeda”

- Como se defender



# Identificando Tentativas de Scan

- É possível usar de sistema IDS, para identificar tentativas de scan e confundir o scan.
  - Snort
  - PortSentry
- Exemplo com nmap e PortSentry
  - O PortSentry envia respostas falsas e envia mensagens para `/var/log/messages`

# Medidas de Segurança

- Configurar bem seu Firewall
- Manter seu sistema atualizado
- Bloquear alta quantidades de pacotes para evitar ataque DoS
- Instalar sistemas IDS para identificar Snifers, e possíveis scan

# FIM!

- Obrigado por assistirem este minicurso!
  - Lembre-se, Com grandes poderes existem grande responsabilidades!
- Perguntas?