

# Ataques

## Parte II

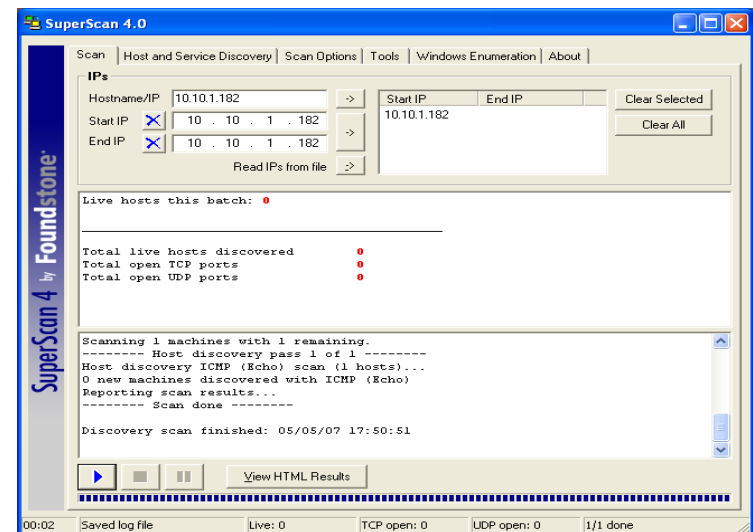
**Prof. Harley de Faria Rios**

# Varredura em redes (*Scan*)

- A varredura em redes e a exploração de vulnerabilidades associadas podem ser usadas de forma:
  - **Legítima:** por pessoas devidamente autorizadas, para verificar a segurança de computadores e redes e, assim, tomar medidas corretivas e preventivas.
  - **Maliciosa:** por atacantes, para explorar as vulnerabilidades encontradas nos serviços disponibilizados e nos programas instalados para a execução de atividades maliciosas.
    - Os atacantes também podem utilizar os computadores ativos detectados como potenciais alvos no processo de propagação automática de códigos maliciosos

# Port scan (varredura de portas)

- Atividade maliciosa de reconhecimento que descobre serviços ativos na máquina
  - Primeira medida para descobrir vulnerabilidades em serviços;
  - Passo inicial de muitos ataques;
  - Verificação das respostas com endereço de retorno necessário permitindo rastrear origem;
  - Detectável via *logs*: servidor, *firewall*, IDS.



Programa de port scan

# NMAP

```
C:\WINDOWS\system32\cmd.exe
C:\net\nmap>nmap -sUC -O -T4 scanme.nmap.org

Starting Nmap 4.68 ( http://nmap.org ) at 2008-07-13 23:23 Pacific Daylight Time

Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1709 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
25/tcp    closed smtp
53/tcp    open  domain   ISC BIND 9.3.4
70/tcp    closed gopher
80/tcp    open  http      Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 11.487 days (since Wed Jul 02 11:42:43 2008)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 27.516 seconds

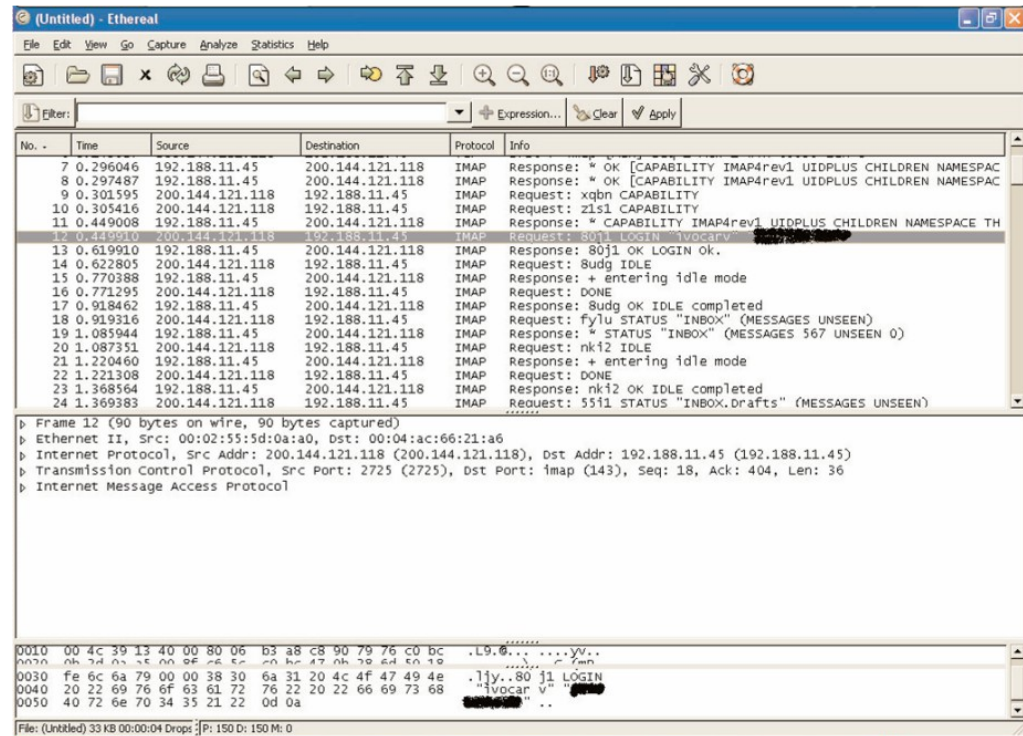
C:\net\nmap>
```

## Interceptação de tráfego (*Sniffing*)

- Uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*. Esta técnica pode ser utilizada de forma:
  - **Legítima:** por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.
  - **Maliciosa:** por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

# Interceptação de tráfego (*Sniffing*)

- Programa que “escuta” a rede em busca de informações importantes
- ▲ Detecção: Uso da placa Ethernet  
*Hub*: alvo fácil de um *sniffer*



The screenshot displays the Wireshark interface with a packet capture of an IMAP session. The packet list on the left shows 24 packets, with packet 12 selected. The packet details pane on the right shows the structure of the selected packet, which is an IMAP response (8011 OK LOGIN 'lvocarv'). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
7	0.296046	192.188.11.45	200.144.121.118	IMAP	Response: * OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE]
8	0.297487	192.188.11.45	200.144.121.118	IMAP	Response: * OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE]
9	0.301595	200.144.121.118	192.188.11.45	IMAP	Request: xqbn CAPABILITY
10	0.305416	200.144.121.118	192.188.11.45	IMAP	Request: 21s1 CAPABILITY
11	0.449008	192.188.11.45	200.144.121.118	IMAP	Response: * CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE TH
12	0.449910	200.144.121.118	192.188.11.45	IMAP	Request: 8011 LOGIN 'lvocarv'
13	0.619910	192.188.11.45	200.144.121.118	IMAP	Response: 8011 OK LOGIN Ok.
14	0.622805	200.144.121.118	192.188.11.45	IMAP	Request: 8udg IDLE
15	0.770388	192.188.11.45	200.144.121.118	IMAP	Response: + entering idle mode
16	0.771295	200.144.121.118	192.188.11.45	IMAP	Request: DONE
17	0.918462	192.188.11.45	200.144.121.118	IMAP	Response: 8udg OK IDLE completed
18	0.919316	200.144.121.118	192.188.11.45	IMAP	Request: fyly STATUS "INBOX" (MESSAGES UNSEEN)
19	1.085944	192.188.11.45	200.144.121.118	IMAP	Response: * STATUS "INBOX" (MESSAGES 567 UNSEEN 0)
20	1.087351	200.144.121.118	192.188.11.45	IMAP	Request: nk12 IDLE
21	1.220460	192.188.11.45	200.144.121.118	IMAP	Response: + entering idle mode
22	1.221308	200.144.121.118	192.188.11.45	IMAP	Request: DONE
23	1.368564	192.188.11.45	200.144.121.118	IMAP	Response: nk12 OK IDLE completed
24	1.369383	200.144.121.118	192.188.11.45	IMAP	Request: 5511 STATUS "INBOX.drafts" (MESSAGES UNSEEN)

Frame 12 (90 bytes on wire, 90 bytes captured)  
Ethernet II, Src: 00:02:55:5d:0a:10, Dst: 00:04:ac:66:21:a6  
Internet Protocol, Src Addr: 200.144.121.118 (200.144.121.118), Dst Addr: 192.188.11.45 (192.188.11.45)  
Transmission Control Protocol, Src Port: 2725 (2725), Dst Port: 143, Seq: 18, Ack: 404, Len: 36  
Internet Message Access Protocol

0010 00 4c 39 13 40 00 80 06 b3 a8 c8 90 79 76 c0 bc .L9.8...yvv..  
0020 00 7d 00 5c 00 0f 26 0c 20 4c 4f 47 49 4e .jly.80 j1 LOGIN..  
0030 fe 6c 6a 79 00 00 38 30 6a 31 20 4c 4f 47 49 4e ..lvocarv..  
0040 20 22 69 76 6f 63 61 72 76 22 20 22 66 69 73 68 ..  
0050 40 72 6e 70 34 35 21 22 0d 0a

File: (Untitled) 33 KB 00:00:04 Drops: 0 P: 150 D: 150 M: 0

## Força bruta (*Brute force*)

- Adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar *sites*, computadores e serviços em nome e com os mesmos privilégios deste usuário.
- Qualquer computador, equipamento de rede ou serviço que seja acessível via Internet, com um nome de usuário e uma senha, pode ser alvo de um ataque de força bruta.
- As tentativas de adivinhação costumam ser baseadas em:



## Força bruta (*Brute force*)

- Dicionários de diferentes idiomas e que podem ser facilmente obtidos na Internet;
- listas de palavras comumente usadas, como personagens de filmes e nomes de times de futebol;
- substituições óbvias de caracteres, como trocar "a" por "@" e "o" por "0";
- sequências numéricas e de teclado, como "123456", "qwert" e "1qaz2wsx"



## Falsificação de e-mail (*E-mail spoofing*)

- Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.
- Esta técnica é possível devido a características do protocolo SMTP (*Simple Mail Transfer Protocol*) que permitem que campos do cabeçalho, como:
  - "From:" (endereço de quem enviou a mensagem),
  - "Reply-To" (endereço de resposta da mensagem) e
  - "Return-Path" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

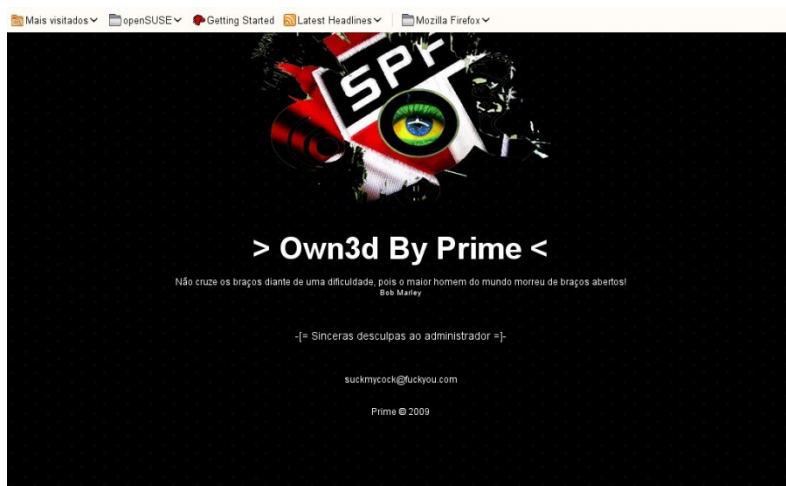
## Falsificação de *e-mail* (*E-mail spoofing*)

- Atacantes utilizam-se de endereços de *e-mail* coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.
- situações onde o seu próprio endereço de *e-mail* foi indevidamente utilizado.
- você recebe respostas de *e-mails* que você nunca enviou;
- você recebe *e-mails* aparentemente enviados por você mesmo, sem que você tenha feito isto;

## Desfiguração de página (*Defacement*)

- Desfiguração de página, *defacement* ou pichação, é uma técnica que consiste em alterar o conteúdo da página *Web* de um *site*.
  - explorar erros da aplicação *Web*;
  - explorar vulnerabilidades do servidor de aplicação *Web*;
  - explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação *Web*;
  - invadir o servidor onde a aplicação *Web* está hospedada e alterar diretamente os arquivos que compõem o *site*;
  - furtar senhas de acesso à interface *Web* usada para administração remota.

# Desfiguração de página (*Defacement*)



# ***Ping da morte***

- ▲ Tipo de ataque DoS;
- ▲ Consiste no envio de pacote “ICMP *ping*” com pacote de dados maior que 64 *Kbytes*, causando travamento ou reinicialização da máquina Microsoft Windows atacada;
- ▲ Vulnerabilidade muito antiga.
- ▲ Maiores informações:
  - ▲ <http://www.cert.org/advisories/CA-1996-26.html>
- ▲ Prevenção:
  - ▲ *Upgrade* das versões dos sistemas operacionais;
  - ▲ *Firewall iptables* Linux:

```
$iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

- Ping -l- 65500 -t ip
- Ping 192.168.0.x -t -l 65000 -w 10000
- LOIC

# Pharming

- Termo atribuído ao ataque baseado na técnica *DNS cache poisoning* (**envenenamento de cache DNS**).
- consiste em corromper o DNS (**Sistema de Nomes de Domínio ou Domain Name System**) em uma rede de computadores.
- Fazendo com que a URL (**Uniform Resource Locator ou Localizador Uniforme de Recursos**) de um site passe a apontar para um servidor diferente do original.
- Ao digitar a URL (**endereço**) do site que deseja acessar, um banco por exemplo, o servidor DNS converte o endereço em um número IP, correspondente ao do servidor do banco

# Pharming

- Se o servidor DNS estiver vulnerável a um ataque de *Pharming*, o endereço poderá apontar para uma página falsa hospedada em outro servidor com outro endereço IP.



- É difícil localizar geograficamente um ip
- É possível, porém, você terá que entrar em contato com o provedor do ip, e ter algum tipo de documento que te disponibilize isso.
- Exemplo, um mandato judicial, claro que isso não é feito por qualquer pessoa ou situação.

# Um estudo de caso

- Em uma rede local existem 3 PCs que compartilham a internet (o modem é roteado). Creio que os PC's utilizam o mesmo IP externo (o que é oferecido pelo provedor ou pela velox, né) quando acessam a internet.

Bem, se um dos PC's dessa rede invadir o Banco de Dados de uma empresa, provavelmente descobrirão o IP do computador que invadiu, certo ?

A pergunta é: tem como descobrir qual computador da rede invadiu, já que todos os PC's da rede utilizam o mesmo IP externo ?

■ 2) Sim e não.

Sim - se você tiver os logs no seu roteador, pois é o único equipamento que sabe da sua rede interna e é o único local por onde \*todos\* os pacotes passam (considerando que não haja um sniffer rodando na rede, claro).

Não - para quem está fora, o IP de saída é único, não tem como saber quantos usuários têm atrás de um IP. O roteador apenas direciona o tráfego para a máquina na rede interna que fez a solicitação para fora (SYN) quando recebe a resposta (SYN+ACK). O IP da rede interna não é propagado para a internet. (seja ela rede 10.x.x.x / 192.168.x.x / 172.16-31.x.x)