

# ATAQUES

DoS, DDoS, Smurf e Ping of Death



**Alunos:**

Clauzio Cristiano Perpétuo

Cleber Franco Madureira

Hugo Azevedo de Jesus

# SUMÁRIO

- Introdução;
- ICMP, Ping of Death e Smurf;
- TCP, DoS e DDoS;
- Implementação;
- Técnicas de Defesa;
- Conclusão;
- Referências Bibliográficas.

# INTRODUÇÃO

- Patrimônio hoje em dia;
- Informação;
- Ter disponibilidade;
- Mercado competitivo, rápido e dinâmico;
- Administradores e batalhas virtuais;
- Técnicas de Ataque como DoS, DDoS, etc;
- Propósito da Apresentação.

# ICMP

Teoria Básica

# ICMP

- O ICMP – Internet Control Message Protocol – é um protocolo que faz parte da pilha TCP/IP, enquadrando-se na camada de rede (nível 3), a mesma camada do protocolo IP – Internet Protocol;
- O seu uso mais comum é feito pelo utilitários ping;
- O ping envia pacotes ICMP para verificar se um determinado host está disponível na rede. Também serve para medir o desempenho da rede;

# ICMP

## Ping

```
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
```

```
cleber:/mnt/pendrive# ping 10.5.12.18
```

```
PING 10.5.12.18 (10.5.12.18) 56(84) bytes of data.
```

```
64 bytes from 10.5.12.18: icmp_seq=1 ttl=128 time=0.615 ms
```

```
64 bytes from 10.5.12.18: icmp_seq=2 ttl=128 time=0.594 ms
```

```
64 bytes from 10.5.12.18: icmp_seq=3 ttl=128 time=0.529 ms
```

```
64 bytes from 10.5.12.18: icmp_seq=4 ttl=128 time=0.616 ms
```

```
--- 10.5.12.18 ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
```

```
rtt min/avg/max/mdev = 0.529/0.588/0.616/0.042 ms
```

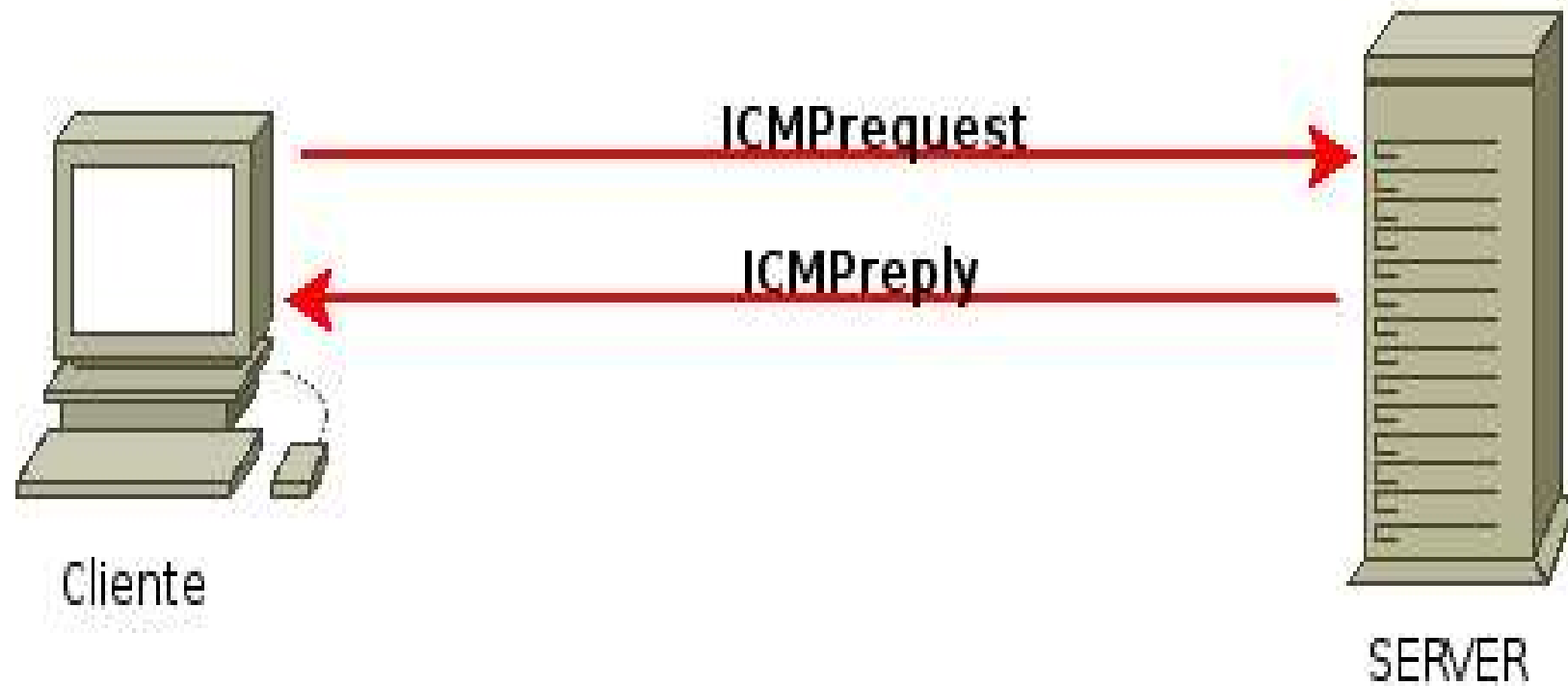
```
cleber:/mnt/pendrive#
```

# ICMP

```
Terminal
Arquivo Editar Ver Terminal Abas Ajuda
cleber:~# tcpdump -v icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:48:29.005372 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], length: 84) cleber > 10.5.12.18: icmp 64: echo request seq 1
15:48:29.005934 IP (tos 0x0, ttl 128, id 104, offset 0, flags [DF], length: 84) 10.5.12.18 > cleber: icmp 64: echo reply seq 1
15:48:30.014640 IP (tos 0x0, ttl 64, id 1, offset 0, flags [DF], length: 84) cleber > 10.5.12.18: icmp 64: echo request seq 2
15:48:30.015482 IP (tos 0x0, ttl 128, id 105, offset 0, flags [DF], length: 84) 10.5.12.18 > cleber: icmp 64: echo reply seq 2
15:48:31.024743 IP (tos 0x0, ttl 64, id 2, offset 0, flags [DF], length: 84) cleber > 10.5.12.18: icmp 64: echo request seq 3
15:48:31.025339 IP (tos 0x0, ttl 128, id 106, offset 0, flags [DF], length: 84) 10.5.12.18 > cleber: icmp 64: echo reply seq 3
15:48:32.024662 IP (tos 0x0, ttl 64, id 3, offset 0, flags [DF], length: 84) cleber > 10.5.12.18: icmp 64: echo request seq 4
15:48:32.025245 IP (tos 0x0, ttl 128, id 107, offset 0, flags [DF], length: 84) 10.5.12.18 > cleber: icmp 64: echo reply seq 4
15:48:33.024666 IP (tos 0x0, ttl 64, id 4, offset 0, flags [DF], length: 84) cleber > 10.5.12.18: icmp 64: echo request seq 5
15:48:33.026664 IP (tos 0x0, ttl 128, id 108, offset 0, flags [DF], length: 84) 10.5.12.18 > cleber: icmp 64: echo reply seq 5

10 packets captured
10 packets received by filter
0 packets dropped by kernel
cleber:~#
```

# ICMP



# Ping da Morte

- O tamanho máximo de um pacote IPv4 é de 64Kbytes;
- Um antiga vulnerabilidade explorada em relação a este limite de tamanho e o processo de fragmentação e remontagem de datagramas é conhecida como Ping da Morte;
- Esta vulnerabilidade consiste em causar um estouro de buffer no host destino, enviando-se vários datagramas fragmentados, cujo tamanho total exceda 64 Kbytes;

# Ping da Morte

- Este bug não estava limitado apenas ao Unix e Windows, aparecia em um varios sistemas que utilizasse IPv4;
- Mas o recordista na correção do bug foi o GNU/Linux que em duas horas de meia depois do anuncio na internet, já estava oferecendo um patch para resolver o problema;

# Ping da Morte

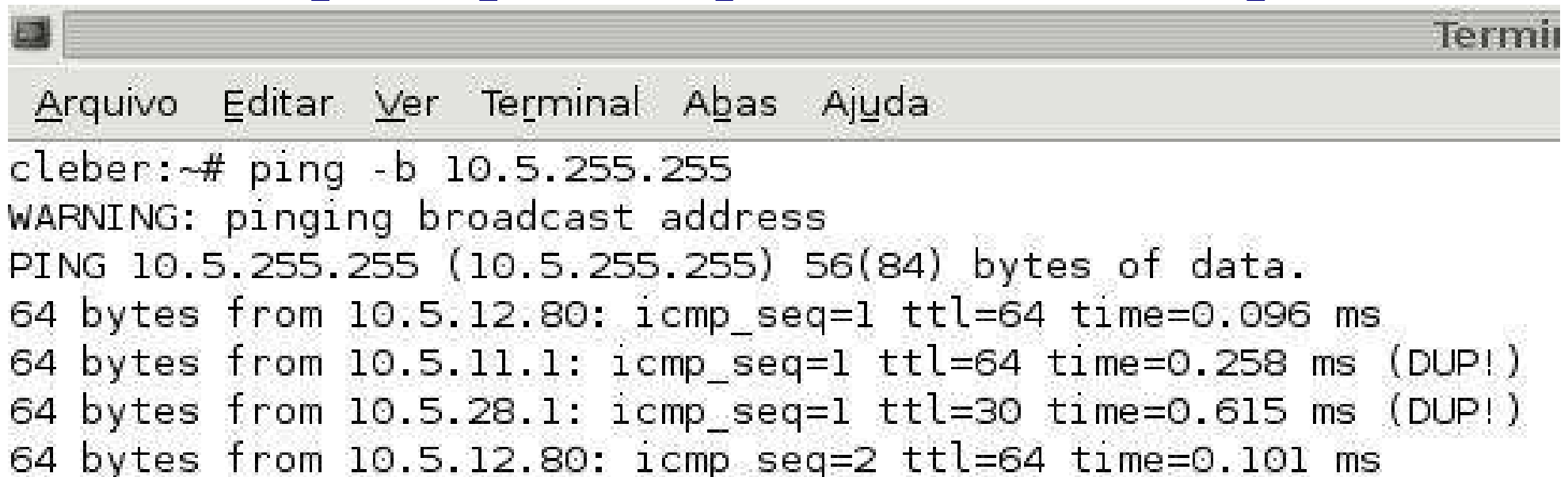
- Nos sistemas atuais não acontece mais esse problema pois não recebe nem envia pacotes maiores do que 64kbytes;

```
Terminal
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
cleber:/mnt/pendrive# ping -s 65999 10.5.12.18
Error: packet size 65999 is too large. Maximum is 65507
cleber:/mnt/pendrive# ping -s 65507 10.5.12.18
PING 10.5.12.18 (10.5.12.18) 65507(65535) bytes of data.
From 10.5.12.18 icmp_seq=1 Frag reassembly time exceeded
From 10.5.12.18 icmp_seq=2 Frag reassembly time exceeded
From 10.5.12.18 icmp_seq=3 Frag reassembly time exceeded
From 10.5.12.18 icmp_seq=4 Frag reassembly time exceeded
From 10.5.12.18 icmp_seq=5 Frag reassembly time exceeded
From 10.5.12.18 icmp_seq=6 Frag reassembly time exceeded

--- 10.5.12.18 ping statistics ---
70 packets transmitted, 0 received, +6 errors, 100% packet loss, time 69566ms
, pipe 65
cleber:/mnt/pendrive#
```

# Smurf Attack

- Smurf é um simples ataque baseado em IP spoofing e Broadcast;
- Um pacote (ICMP) é enviado para um endereço de broadcast, todos os hosts que fazem parte para daquela rede irão responder;



```
Terminal
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
cleber:~# ping -b 10.5.255.255
WARNING: pinging broadcast address
PING 10.5.255.255 (10.5.255.255) 56(84) bytes of data.
64 bytes from 10.5.12.80: icmp_seq=1 ttl=64 time=0.096 ms
64 bytes from 10.5.11.1: icmp_seq=1 ttl=64 time=0.258 ms (DUP!)
64 bytes from 10.5.28.1: icmp_seq=1 ttl=30 time=0.615 ms (DUP!)
64 bytes from 10.5.12.80: icmp_seq=2 ttl=64 time=0.101 ms
```

# Smurf Attack

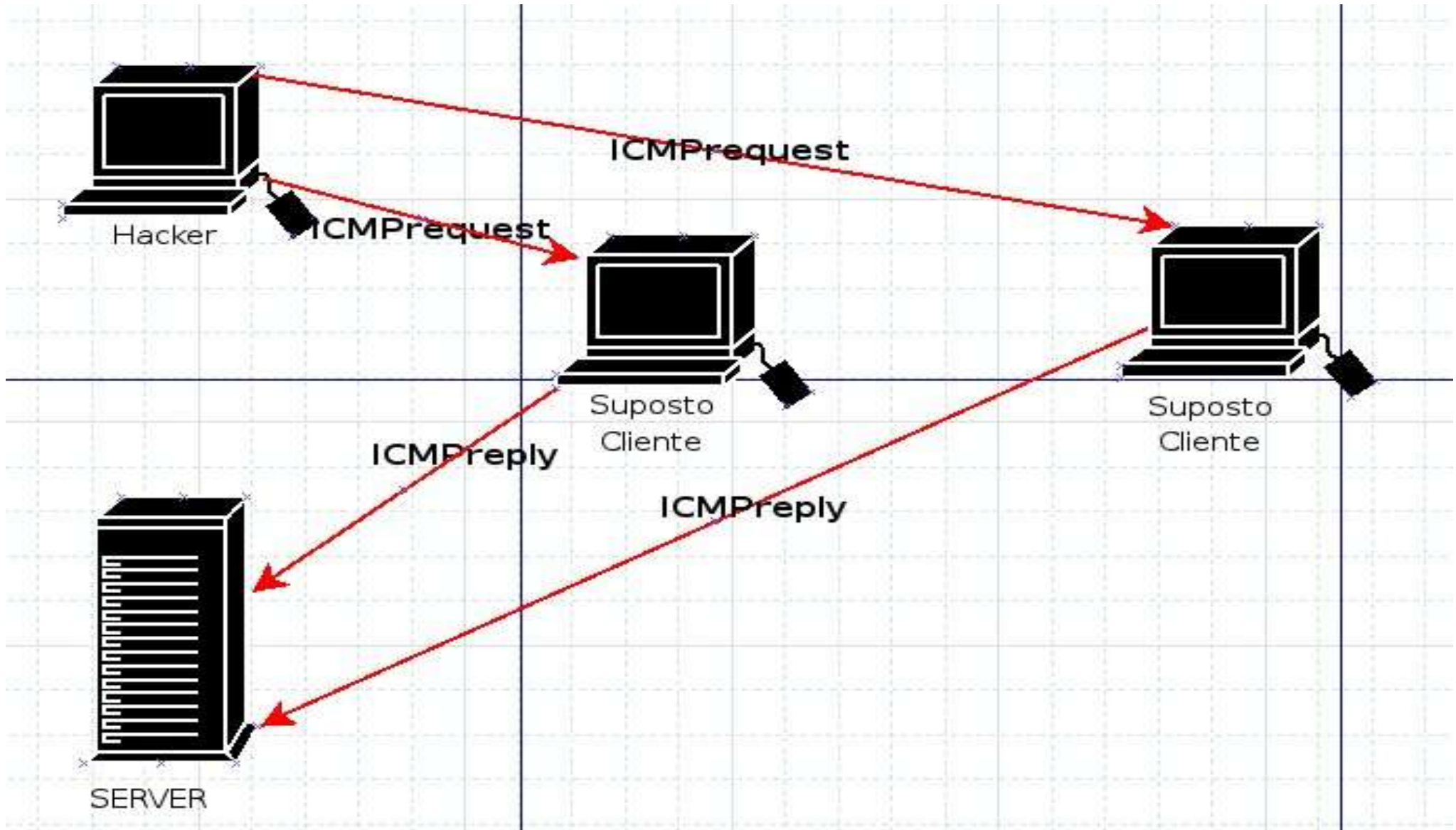
```
Terminal
Arquivo Editar Ver Terminal Abas Ajuda
cleber:~# tcpdump -v icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
17:08:23.055685 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], length: 84) cleber > 10.5.255.255: icmp 64: echo request seq
1
17:08:23.055869 IP (tos 0x0, ttl 64, id 24523, offset 0, flags [none], length: 84) 10.5.11.1 > cleber: icmp 64: echo reply se
q 1
17:08:23.056195 IP (tos 0x0, ttl 30, id 63512, offset 0, flags [none], length: 84) 10.5.28.1 > cleber: icmp 64: echo reply se
q 1

3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

# Smurf Attack

- Neste caso os IP's serão trocados (técnica spoofing) pelo endereço IP da vítima(Servidor) escolhida pelo \*hacker;
- Na técnica de Spoofing os pacotes IP possuem um endereço destino e um endereço origem. Normalmente o endereço origem reflete a realidade, mas nada impede que um hacker altere este pacote para que ele pareça ter vindo de outro lugar;
- Dessa maneira quando os computadores que receberem o broadcast, responderão com ICMP Echo Reply para o endereço IP (spoofed) contido naquele broadcast;

# Smurf Attack



# Smurf Attack

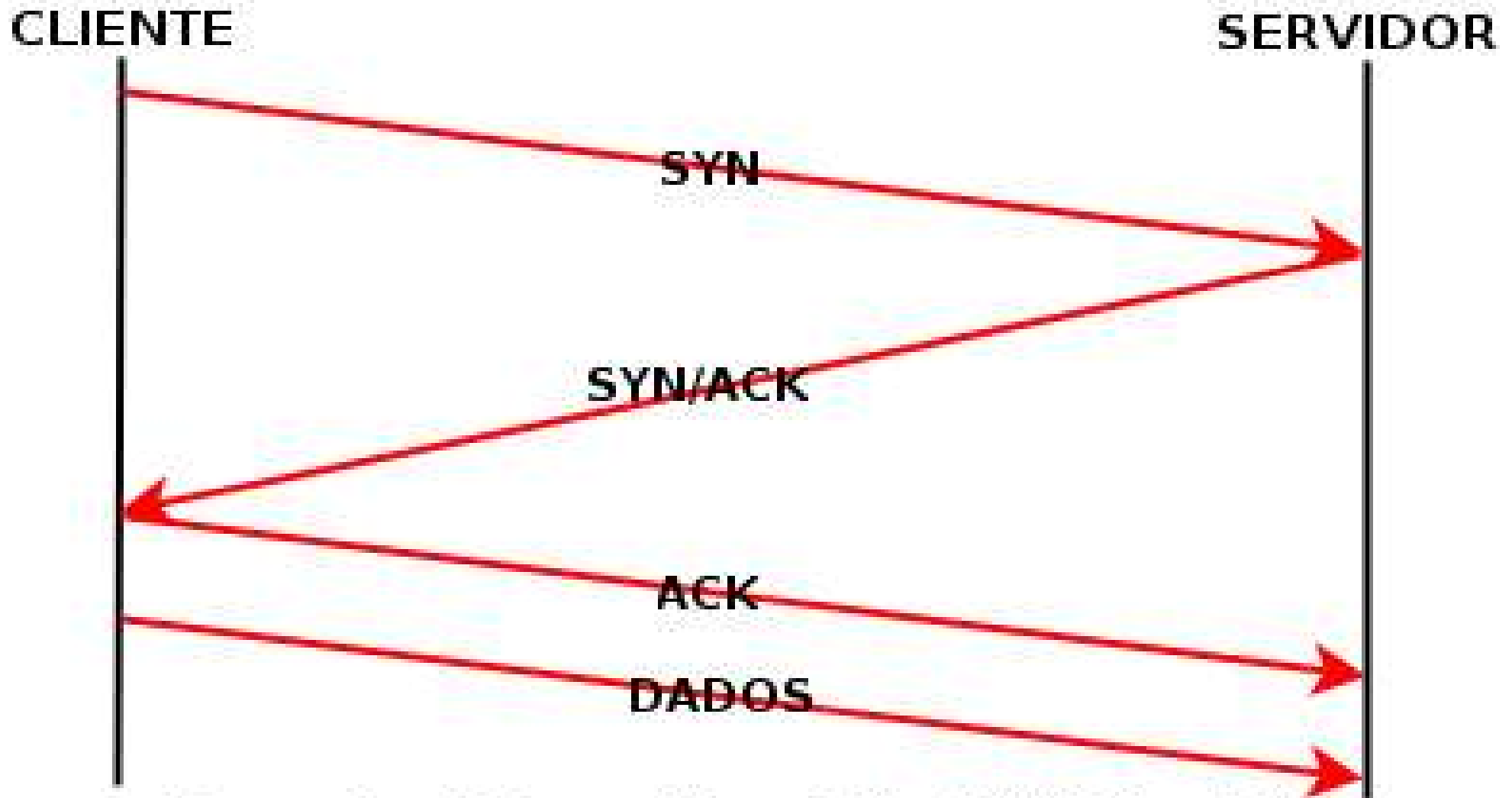
- Dependendo do numero de computadores naquela sub rede dezenas, centenas ou ate milhares de pacotes ICMP Echo Reply serão enviados para o endereço IP da vitima fazendo com que a conexão seja bloqueada ou simplesmente tornando a conexão lenta demais;
- Esse técnica pode ser aplicada em conjunto com vários outros \*hackers para que o efeito seja ainda maior e duradouro. Para a vítima na ha muito o que fazer a não ser contatar o responsável pela sub rede que esta servido de amplificador de Smurf ( Smurf Amplifier);

# TCP

Teoria Básica

# TCP

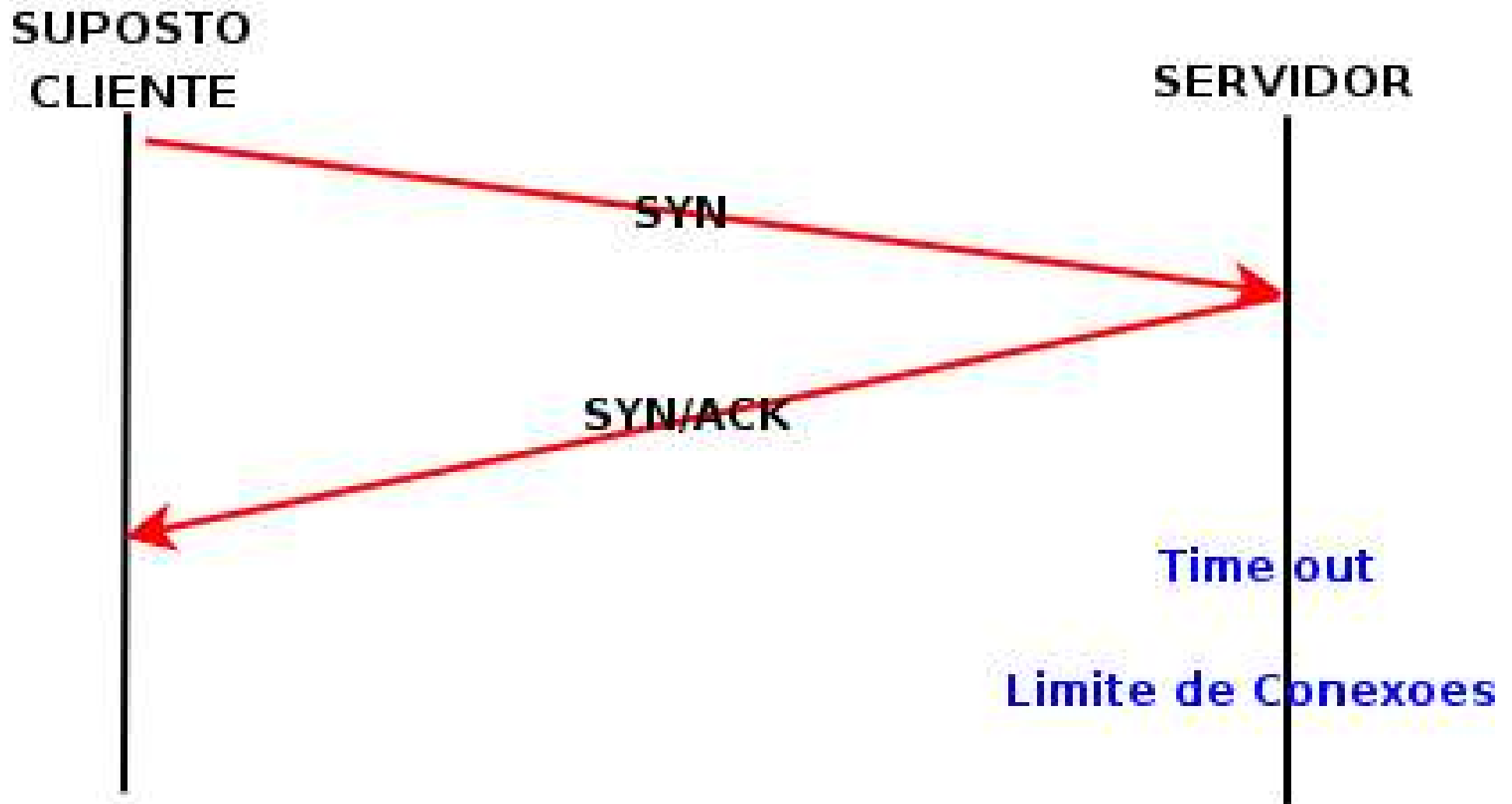
## Estabelecimento de Conexão



\*Segmentos TCP com Flags SYN, SYN/ACK e ACK

# TCP

## Estabelecimento Parcial de Conexão



\*Milhares de Segmentos TCP com a Flag SYN

# DoS/DDoS

## Introdução

“Os ataques conhecidos como *denial-of-service* (DoS) são caracterizados por uma tentativa explícita do atacante de impedir que um usuário legítimo utilize determinado serviço.”

# DoS/DDoS

## Estratégias

- Inundar uma rede visando impedir que usuários legítimos façam uso dela;
- Impedir ou romper a conexão entre duas máquinas visando impedir o acesso a um serviço;
- Impedir o acesso de um determinado serviço ou *site*;
- Impedir ou negar um serviço a um sistema ou pessoa específicos;

# DoS/DDoS

## Característica

- Exploram falhas em serviços e SOs utilizando técnicas de IP *Spoofing*:
  - *Ping-of-dead*;
  - *SYN Flooding*;
  - *UPD packet storm*;
  - *smurf*;

# DoS/DDoS

## Forma básica de ataque

- Exploração de vulnerabilidade já conhecidas em SOs e serviços;
- Obtenção de acesso privilegiado a qualquer máquina na *Internet* com *scripts* automatizados na maioria das vezes;
- Geração de uma lista de endereços IPs das máquinas exploradas que formam a rede de ataque. (Fapi, Blitznet, Trin00, TFN, Stacheldraht, Shaft, TFN2K, Trank...);

# DoS/DDoS

## Rede de ataque típica

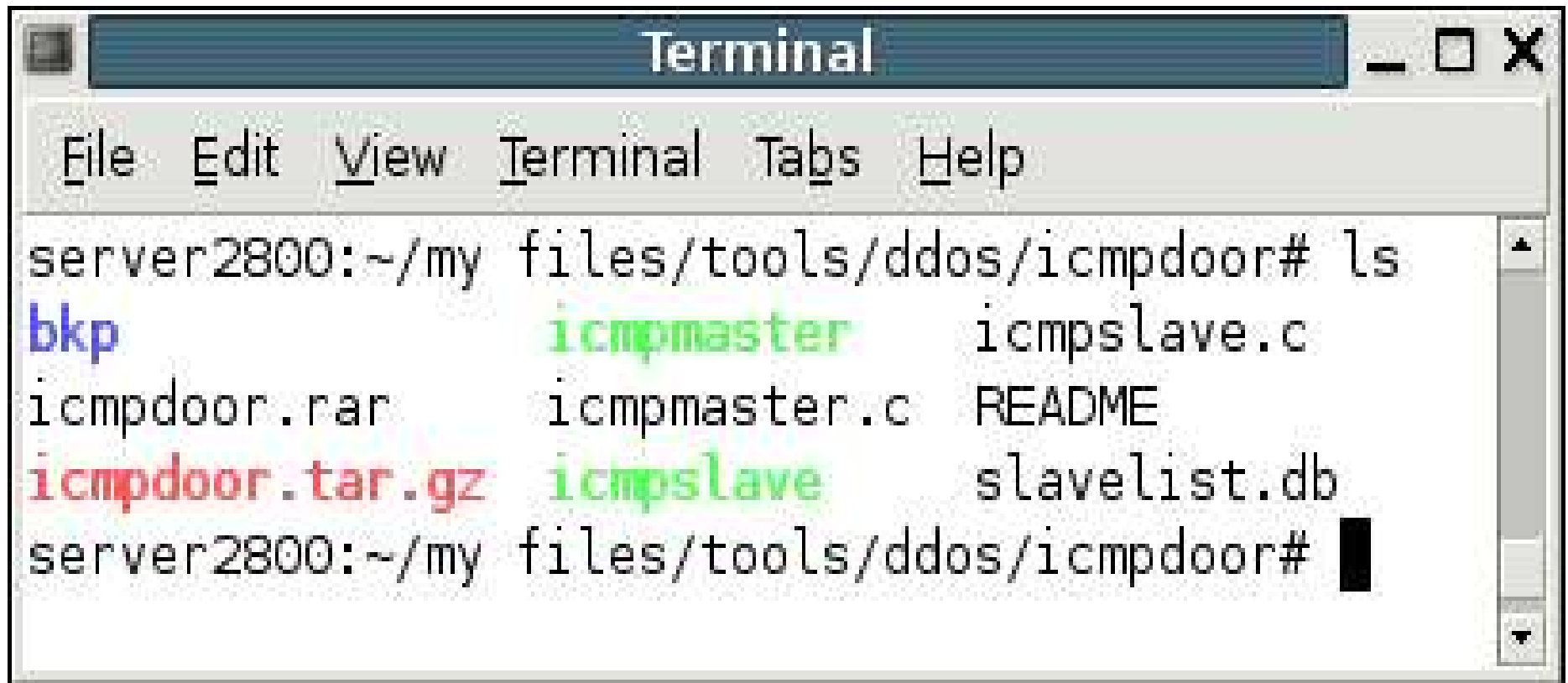
 <file:///root/my%20files/my%20documents/InstitutoFatima/ddos.png>

# IMPLEMENTAÇÃO NO GNU/LINUX

ICMPDOOR

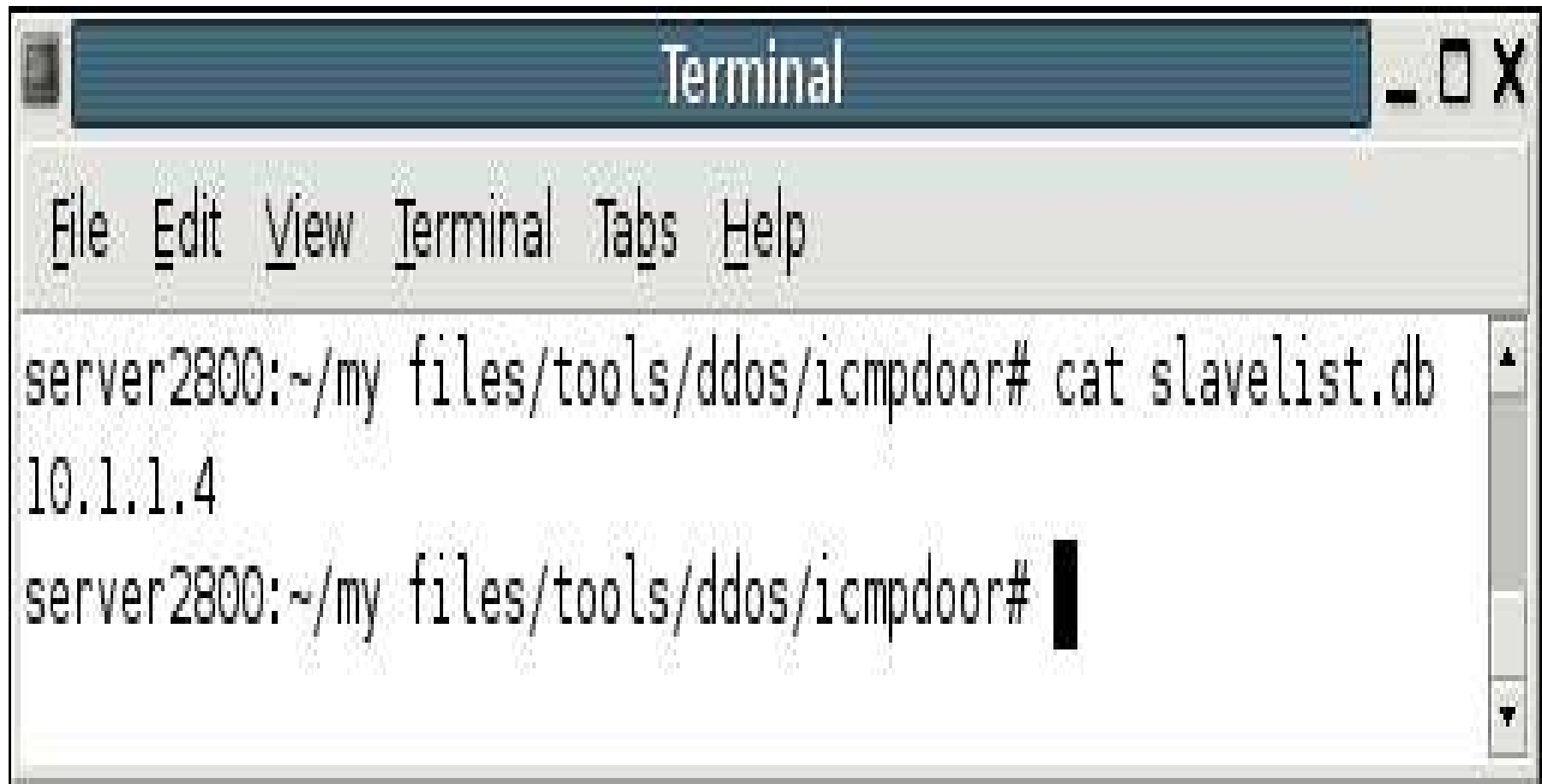
# ICMPDOOR

- DDoS (master e vários slaves);
- IP e TCP Spoofing;



```
Terminal
File Edit View Terminal Tabs Help
server2800:~/my files/tools/ddos/icmpdoor# ls
bkp          icmpmaster  icmpslave.c
icmpdoor.rar icmpmaster.c README
icmpdoor.tar.gz icmpslave  slavelist.db
server2800:~/my files/tools/ddos/icmpdoor#
```

# ENDEREÇOS DOS SLAVES

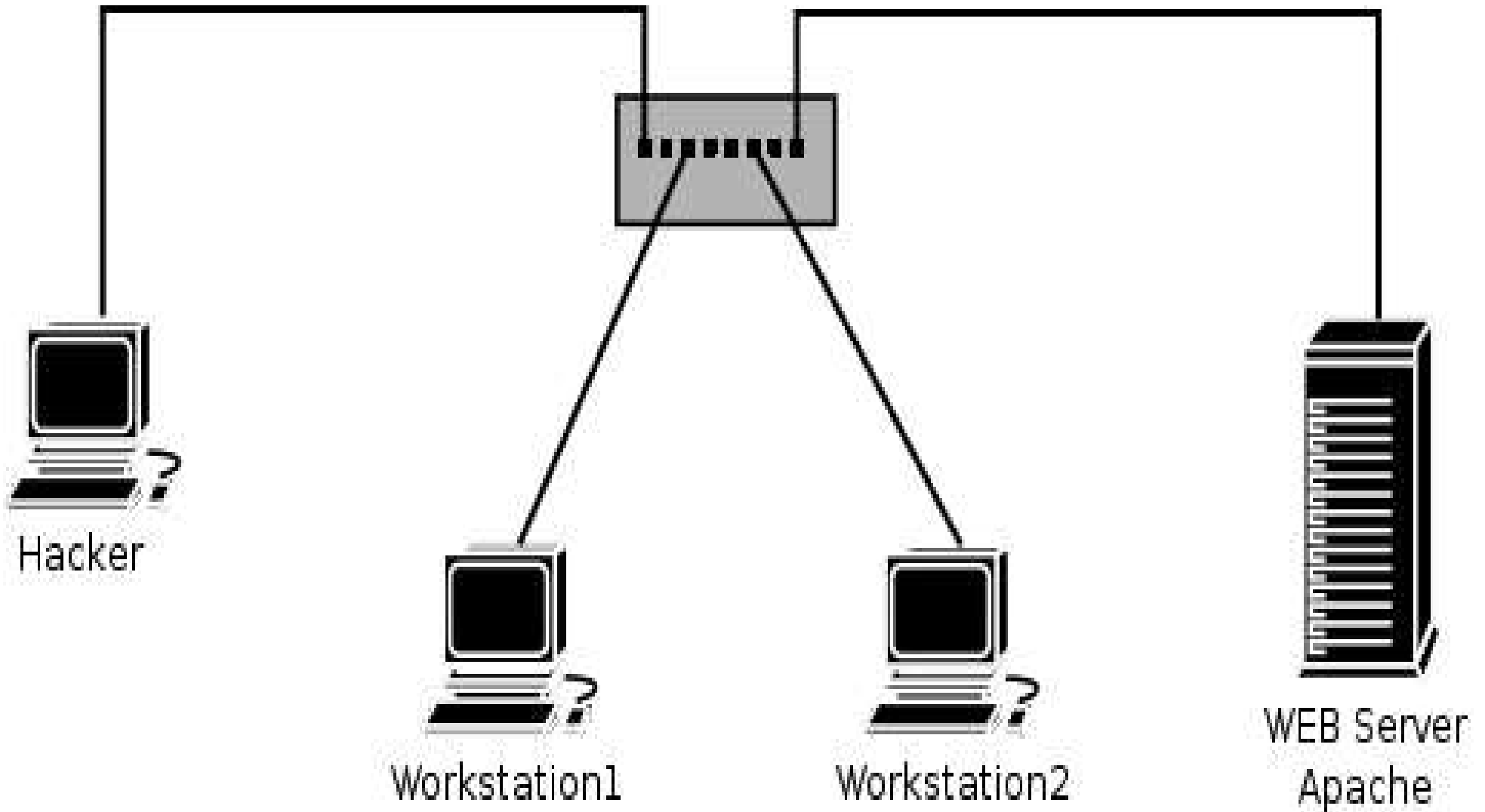


```
Terminal
```

File Edit View Terminal Tabs Help

```
server2800:~/my files/tools/ddos/icmpdoor# cat slavelist.db
10.1.1.4
server2800:~/my files/tools/ddos/icmpdoor#
```

# AMBIENTE DE TESTE



# DESCRIÇÃO DOS EQUIPAMENTOS

## **Hacker, Workstation1 e Workstation2**

(Fedora Core 4 – Kernel 2.6.11-1)

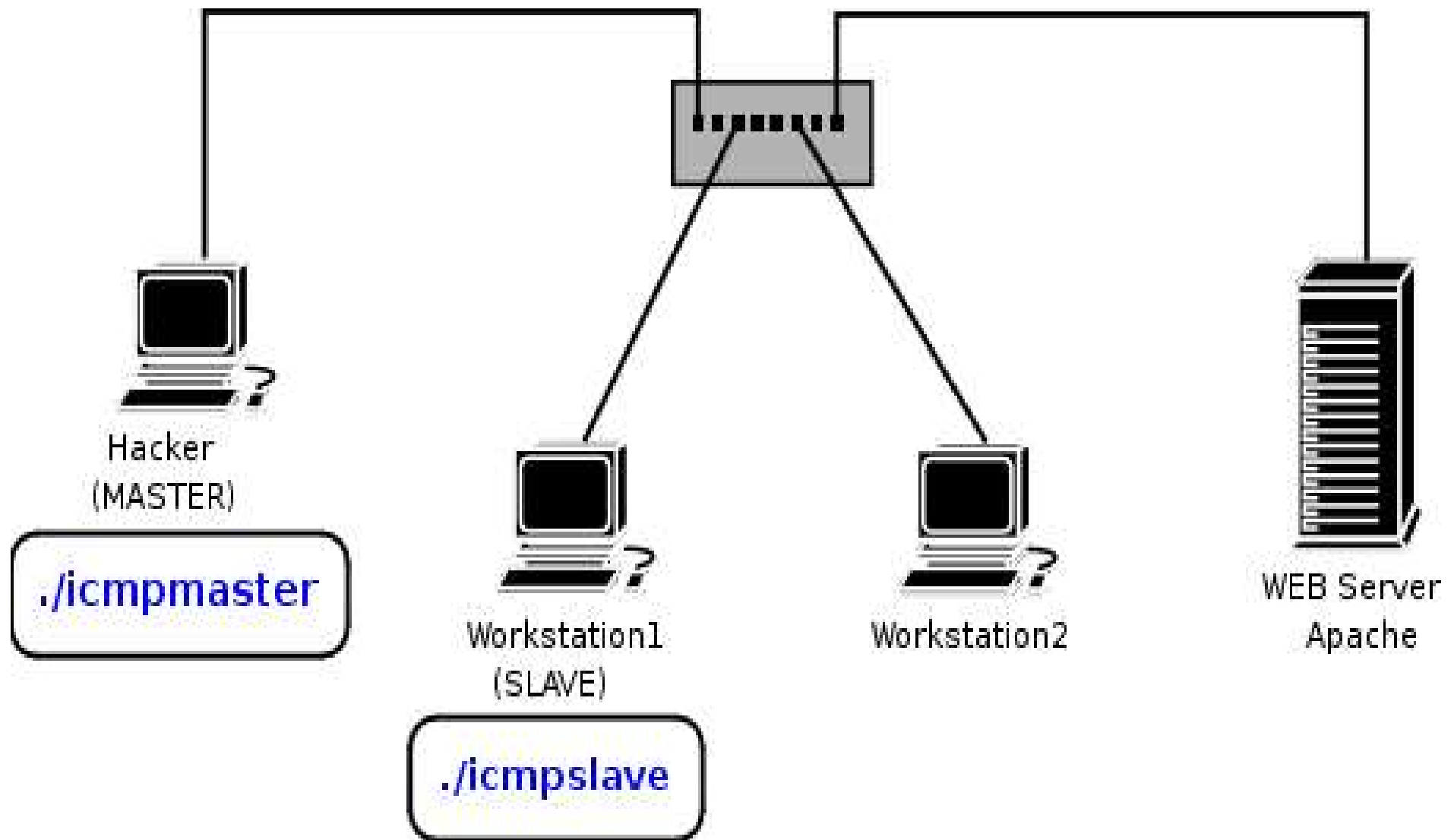
(Pentium4 2.4GHz - 512MB)

## **Apache Web Server**

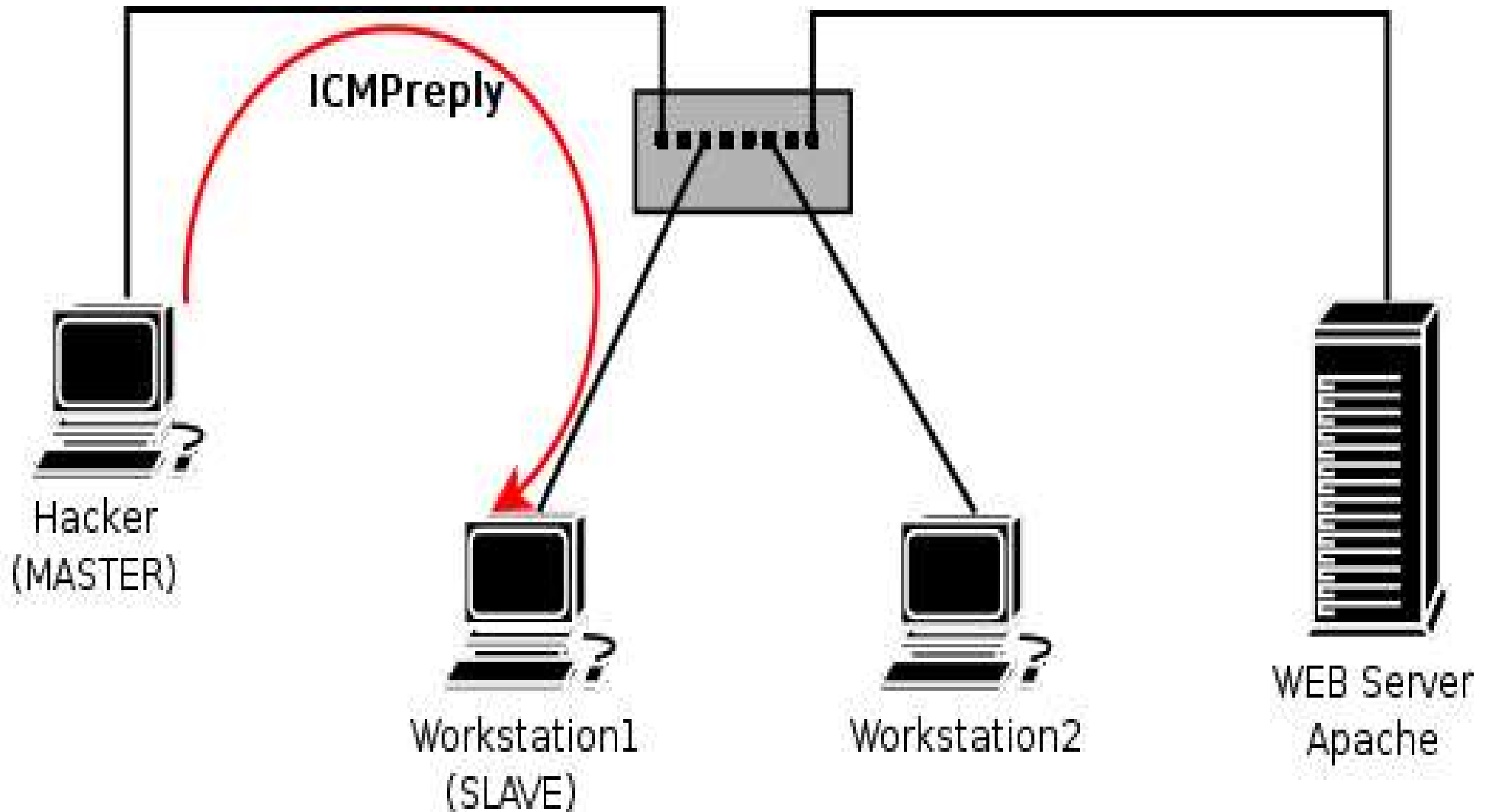
(Debian Sarge – Kernel 2.4.27-2)

(AMD 2800 – 700 MB)

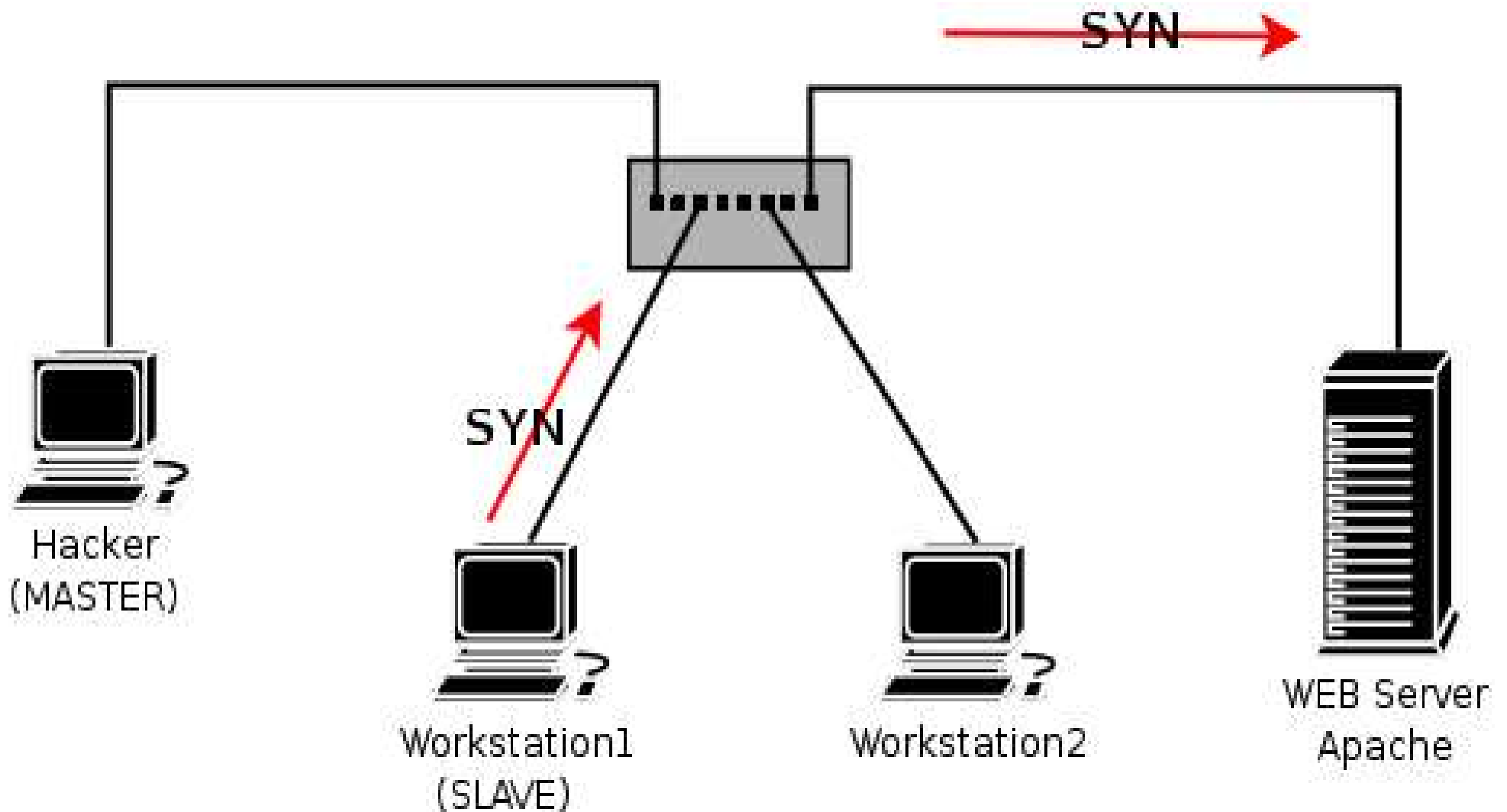
# EXECUÇÃO



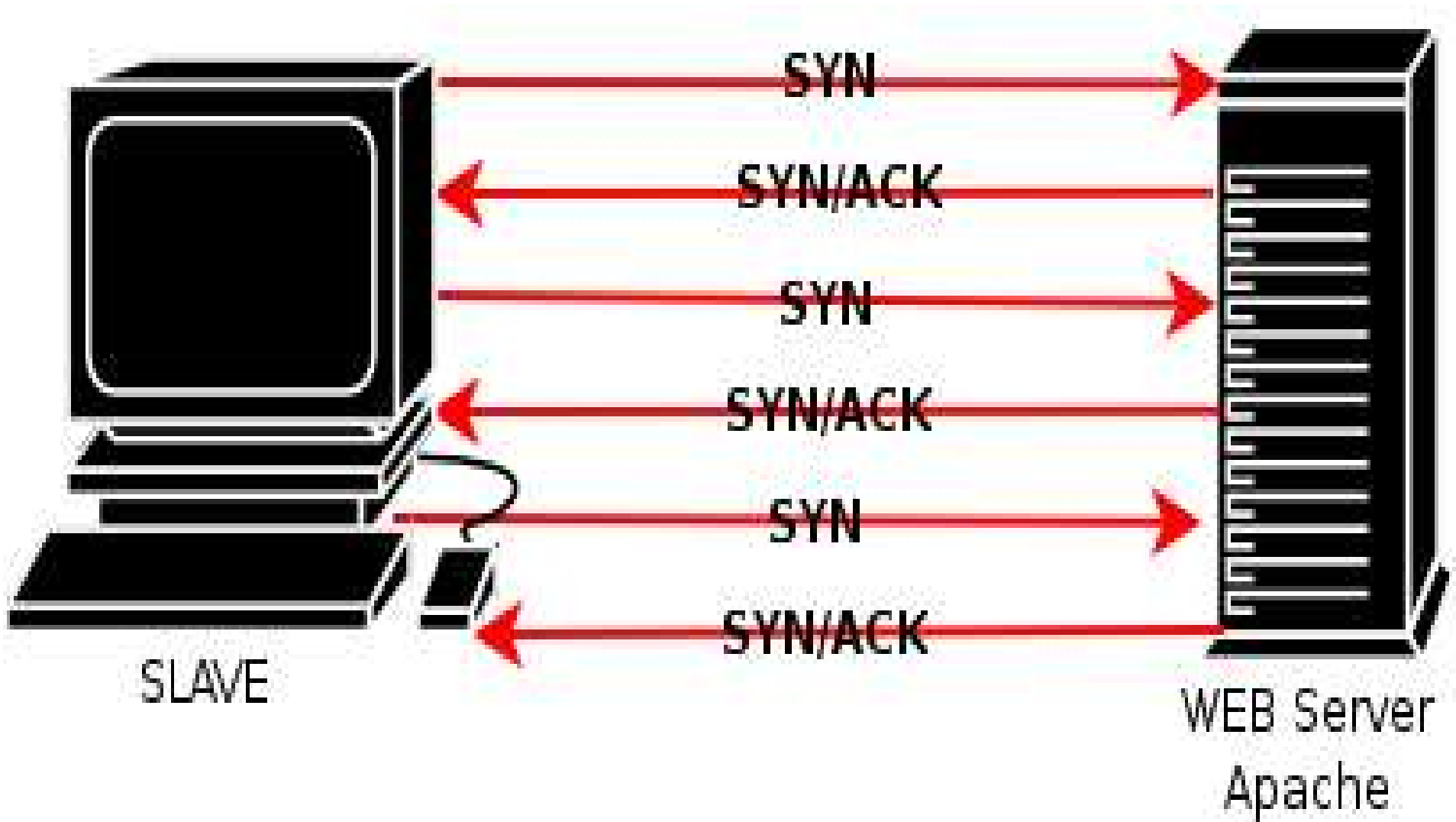
# MASTER para SLAVE



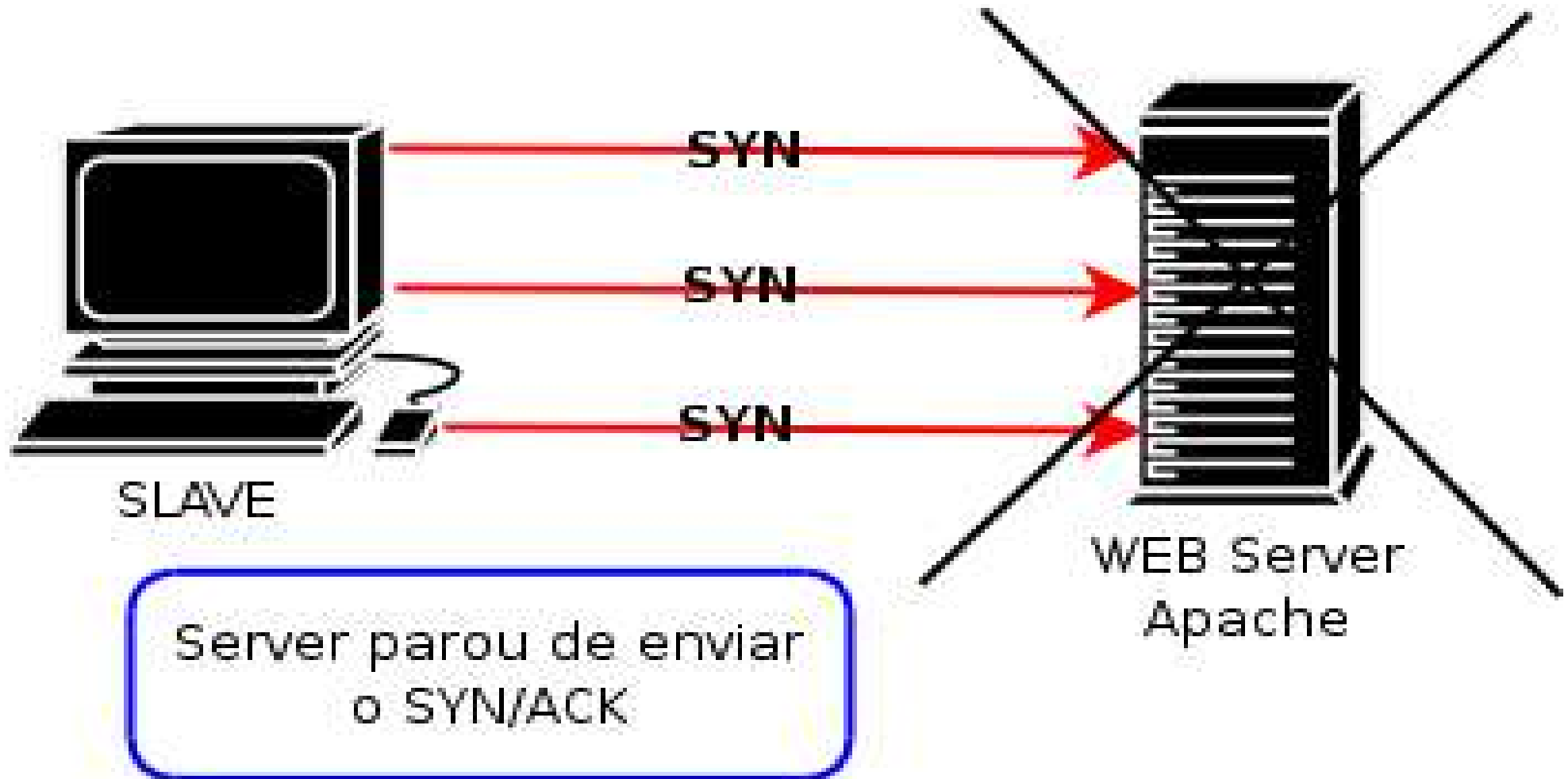
# SLAVE para VÍTIMA



# ATAQUE



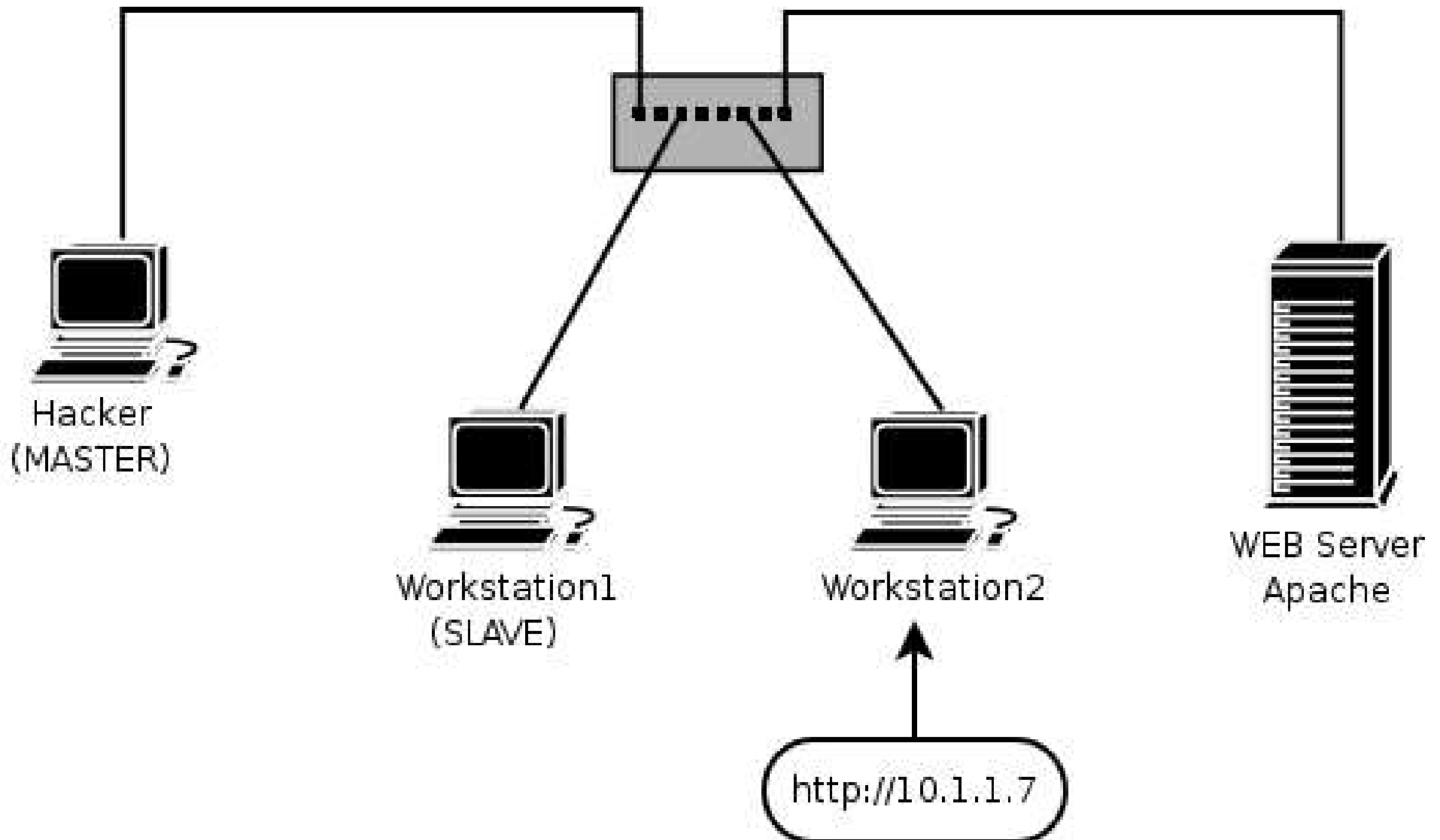
# DENIAL-OF-SERVICE




# ETHERREAL

No.	Time	Source	Destination	Protocol	Info
1123	0.0995500	10.1.1.7	67.29.100.200	TCP	www > 669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
1124	0.099688	85.142.156.36	10.1.1.7	TCP	xtel > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1125	0.099704	10.1.1.7	85.142.156.36	TCP	www > xtel [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
1126	0.099862	181.53.183.166	10.1.1.7	TCP	1593 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1127	0.099880	10.1.1.7	181.53.183.166	TCP	www > 1593 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
1128	0.100025	27.174.177.32	10.1.1.7	TCP	1991 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1129	0.100190	135.20.90.154	10.1.1.7	TCP	437 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1130	0.100354	145.200.170.91	10.1.1.7	TCP	1012 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1131	0.100516	74.48.138.42	10.1.1.7	TCP	1050 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1132	0.100681	60.15.156.193	10.1.1.7	TCP	535 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0
1133	0.100842	27.57.46.110	10.1.1.7	TCP	1657 > www [SYN] Seq=0 Ack=0 Win=2048 Len=0

# USUÁRIO LEGÍTIMO



Localização:  http://10.1.1.7/

# Hugo's Page

[Contato](#)[Ajuda](#)

## PRINCIPAL

[Página Inicial](#)[Linux](#)[Windows](#)[IPv6](#)[Trabalhos](#)[Links](#)

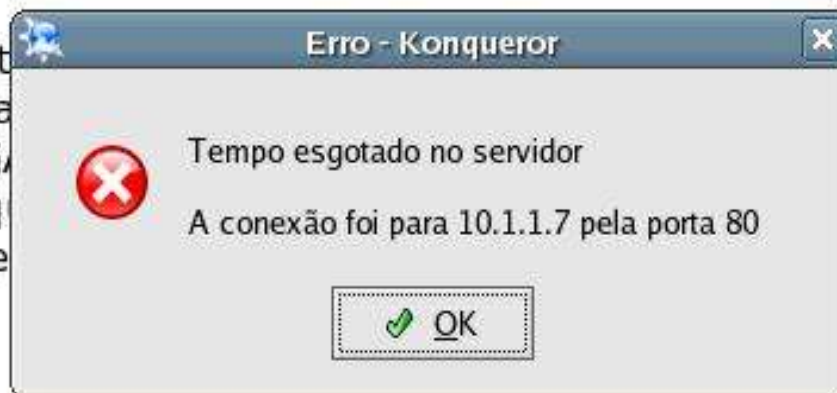
## PESSOAL

[Monografia](#)[Curriculum](#)

## VISITANTES

Esta t  
informática  
a disposiã  
trabalhos q  
autores que

da Área de  
a monografia  
"NO IPv6" e  
os de outros



# TÉCNICAS DE DEFESA

# Técnicas de defesa

## Atenção

- Excesso de tráfego;
- A existência de pacotes UDP e ICMP de tamanho acima do normal ou em excesso;
- Pacotes TCP e UDP que não fazem parte de uma conexão;

# Técnicas de defesa

## Minimizando vulnerabilidades

- Negação de *Pings* por máquinas desconhecidas;
- Regras de *Firewall* bem definidas. (*anti-Spoofing...*);
- Alteração dos parâmetros relativos às filas de sincronismo;
- Instalação de um sistema de detecção de intrusão. (SNORT...);
- Verificação periódica de *logs* e *e-mails* do sistema;

# Contra-medidas

- Ainda não existe uma solução definitiva contra os ataques de *denial-of-service* e ataques distribuídos. Algumas pesquisas estão sendo realizadas propondo soluções para o problema:
  - Identificar a origem dos pacotes forjados;
  - Inibir os amplificadores de ataques;
  - *Overlay networks*;
  - *Active Networks*;

# CONCLUSÃO

- Existem várias técnicas;
- Indisponibilizar um serviço;
- Ferramentas na Internet;
- Administradores devem estar preparados;
- Se proteger;

# BIBLIOGRAFIA

- DIÓGENES, Y. **Certificação cisco**: guia de certificação para o exame 640-801. 3. ed. Rio de Janeiro: Axcel Books, 2004.
- SOARES, L. F. G.; LEMOS, G.; COLCHER, S. **Redes de computadores**: das LANS, MANS e WANS às redes ATM. 12. ed. Rio de Janeiro: Campus, 1995.
- TANENBAUM, A. S. **Redes de computadores**. 3. ed. Rio de Janeiro: Campus, 1997.

# SITES

- [http://www.cert-rs.tche.br/docs\\_html/ddos-errc-2003.pdf](http://www.cert-rs.tche.br/docs_html/ddos-errc-2003.pdf)
- [http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14\\_gci1162868,00.html](http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci1162868,00.html)
- [http://en.wikipedia.org/wiki/Active\\_Networking](http://en.wikipedia.org/wiki/Active_Networking)
- [http://en.wikipedia.org/wiki/Overlay\\_network](http://en.wikipedia.org/wiki/Overlay_network)
- [http://beginnerhacker.vilabol.uol.com.br/hacker/tutorhack/denial\\_of\\_service.htm](http://beginnerhacker.vilabol.uol.com.br/hacker/tutorhack/denial_of_service.htm)
- <http://www.ufsdump.org/papers/uuasc-november-ddos.html>
- <http://packetstormsecurity.org/distributed/>
- [http://en.wikipedia.org/wiki/Denial-of-service\\_attack](http://en.wikipedia.org/wiki/Denial-of-service_attack)
- <http://penta.ufrgs.br/Esmilda/fmtotcp.html>>. Acesso em: 9 nov. 2005
- [http://www.unicert.com.br/arquivos/sobre\\_conteudos/UBC%20705%20-%20A%20Hist%C3%B3ria%20do%20TCP-IP%20v1.0.pdf](http://www.unicert.com.br/arquivos/sobre_conteudos/UBC%20705%20-%20A%20Hist%C3%B3ria%20do%20TCP-IP%20v1.0.pdf)
- <http://magnum.ime.uerj.br/~alexsz/cursos/redes/osi/osi5.htm>>. Acesso em: 20 out. 2005.
- <http://penta.ufrgs.br/gere96/segur/ipspooof.htm>