Ataques de Negação de Serviços (DoS)

George Lucas
Breno G. de Oliveira

Negação de Serviços >> Definição

Investida contra serviços e recursos digitais

- Desempenho extremamente baixo
- Indisponibilidade completa (ativa ou passiva)

Negação de Serviços >> Motivação

Vandalismo

http://www.zone-h.org

DNS Attack Downs Internet in Parts of China

http://www.pcworld.com/businesscenter/article/165319/dns_attack_downs_internet_in_parts_of_china.html

Negação de Serviços >> Motivação

Chantagem

“Botnets can be used to blackmail targeted sites”
http://www.usatoday.com/tech/news/computersecurity/2008-03-16-bot-side_N.htm

“Online Russian blackmail gang jailed
for extorting $4m from gambling websites”
http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html

Negação de Serviços >> Motivação

“Ativismo” (Ciber-terrorismo)

Activists Launch Hack Attacks on Tehran Regime
http://www.wired.com/dangerroom/2009/06/activists-launch-hack-attacks-on-tehran-regime/

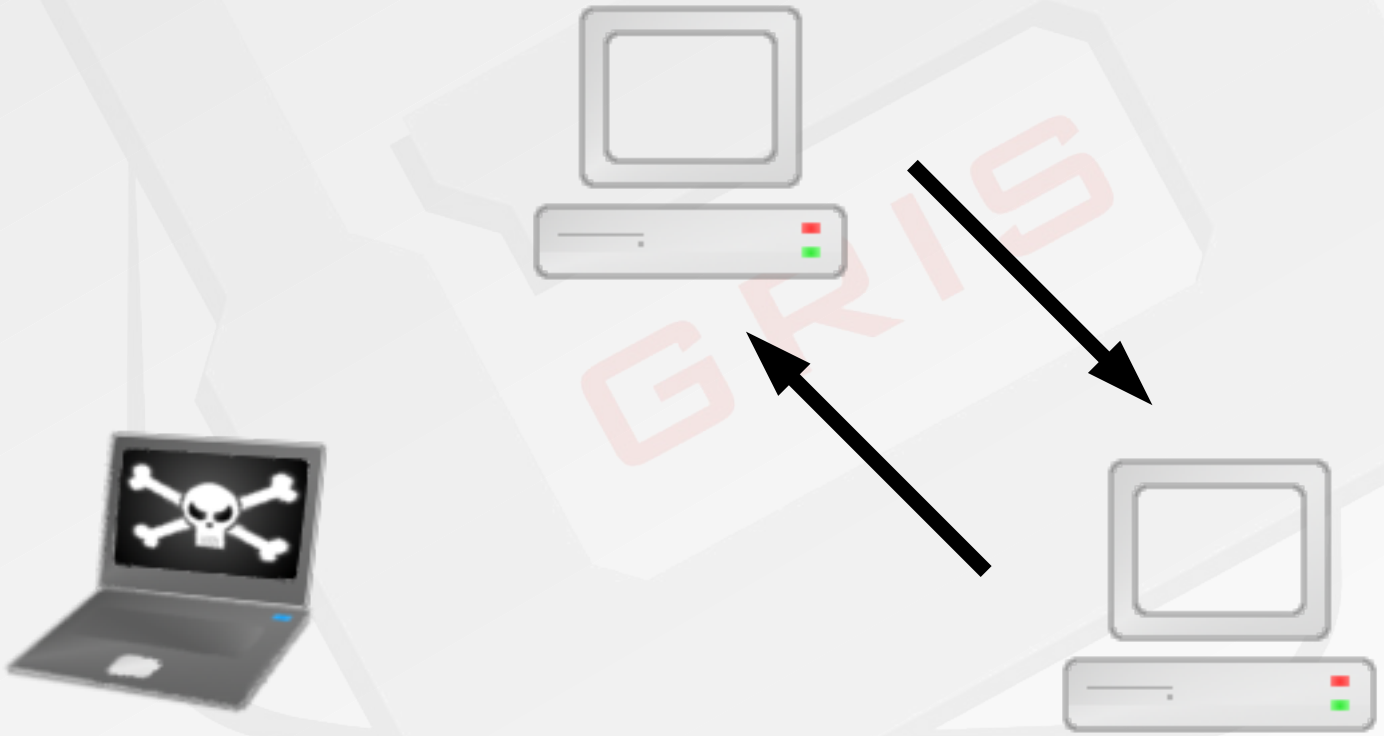
“DDoS attack boots Kyrgyzstan from net”
http://www.theregister.co.uk/2009/01/28/kyrgyzstan_knocked_offline/

“O maior cyberataque do Planeta”
http://olhardigital.uol.com.br/central_de_videos/video_wide.php?id_conteudo=8514

Negação de Serviços >> Motivação

Ataques elaborados

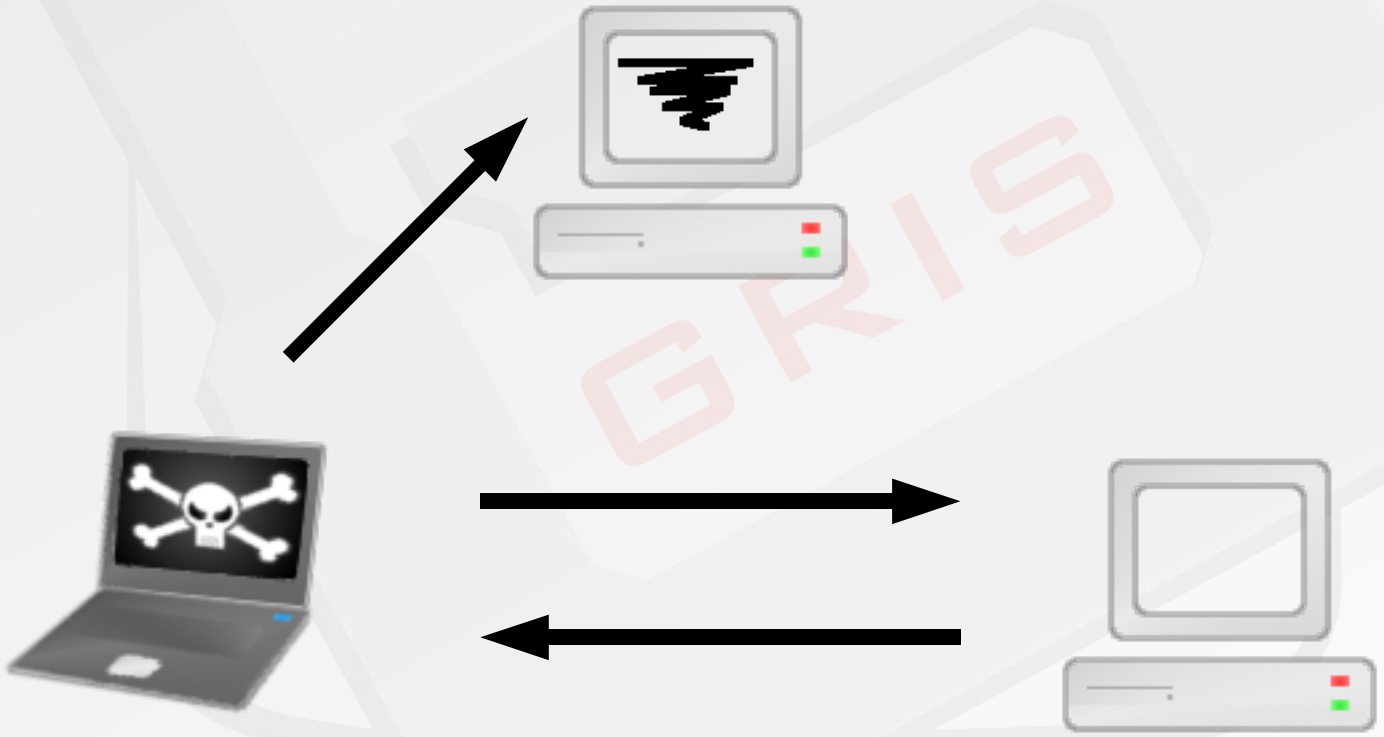
(geralmente envolvendo “spoofing”)



Negação de Serviços >> Motivação

Ataques elaborados

(geralmente envolvendo “spoofing”)

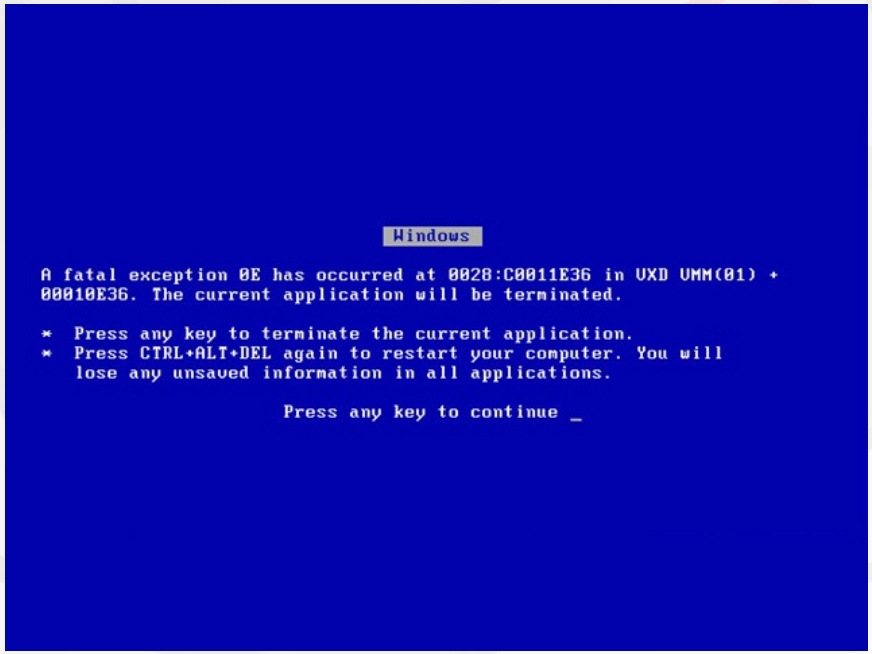


Negação de Serviços >> Tipos

- Consumo de recursos computacionais como banda, espaço em disco ou tempo de CPU
- Quebra de arquivos de configuração
- Quebra de informação de estados
- Quebra de componentes físicos
- Obstrução de canais de comunicação

Negação de Serviços >> Ataques Locais

- Exploram erros em aplicações...
- ...ou entopem algum recurso (CPU, Memória, disco, etc)



Negação de Serviços >> Ataques Locais

```
$ dd if=/dev/zero  of=/var/spool/mail/MEU_USUARIO


$ :(){ :|:& };:


$ perl -e 'while(1) { fork();
          open $fh, “</proc/meminfo”;
          open $hf, “>/tmp/bla”; }'
```

Negação de Serviços >> Ataques em Rede

- Ataques Remotos Simples (DoS remoto)
- Ataques Distribuídos (DDoS)
- Ataques Distribuídos Refletidos (DRDoS)
- Ataques de Amplificação
- Ataques Permanentes (PDoS)

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples
(DoS remoto)

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples (DoS remoto)

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples
(DoS remoto)

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples (DoS remoto)

Alvos podem ser servidores...

- SSH, SSL/TLS, HTTP, VoIP

Ou clientes!

- Navegadores, Plugins, Sistemas Operacionais

Negação de Serviços >> Ataques a HTTP

Slow Loris

- Identifica janela de timeout de servidores HTTP/HTTPS (incluindo vhosts) ou Proxies
- Realiza ataques DoS eficientes sem aumentar a carga do sistema alvo (ou exigir mais de um atacante)
- Consegue contornar proteção HTTPReady
- Consegue evitar Cache (experimental)

```
# ./slowloris.pl -dns www.example.com -port 80
  -timeout 2000 -num 500 -tcpto 5
```

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples (Obstrução de Canais)

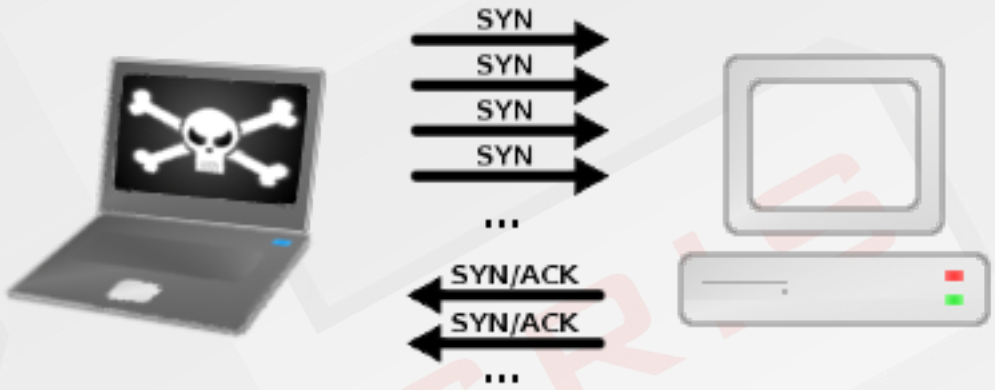
金盾工程

```
# tcpnice -i eth0 EXPRESSAO_FILTRO

# tcpkill -i eth0 -[1..9] EXPRESSAO_FILTRO
```

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples (SYN Flood)

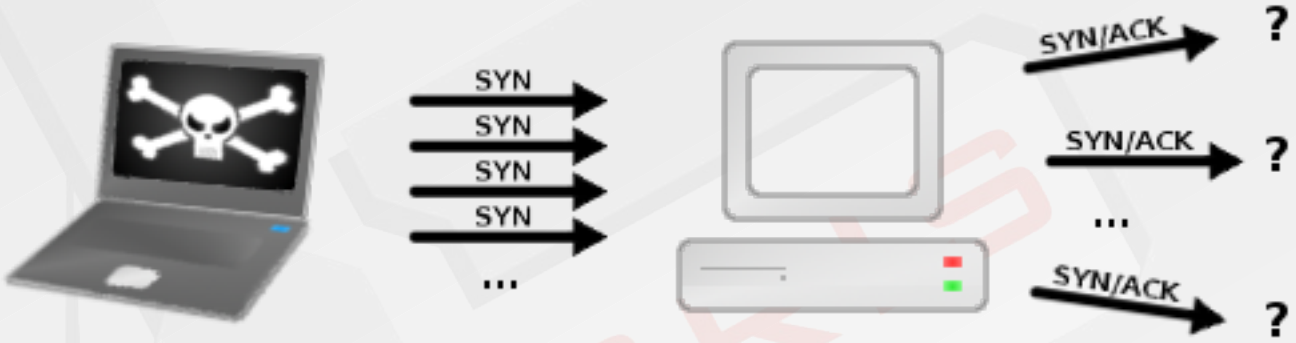



```
# hping3 --flood --interface eth0 -S -p PORTA_ALVO IP_ALVO
```

SYN Flood tradicional (1 x 1)

Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples (SYN Flood)




```
# hping3 --flood --spoof IP_ORIGEM (ou –rand_source)
  -S -p PORTA_ALVO IP_ALVO
```

SYN Flood tradicional (1 x 1) com *spoofing* de origem

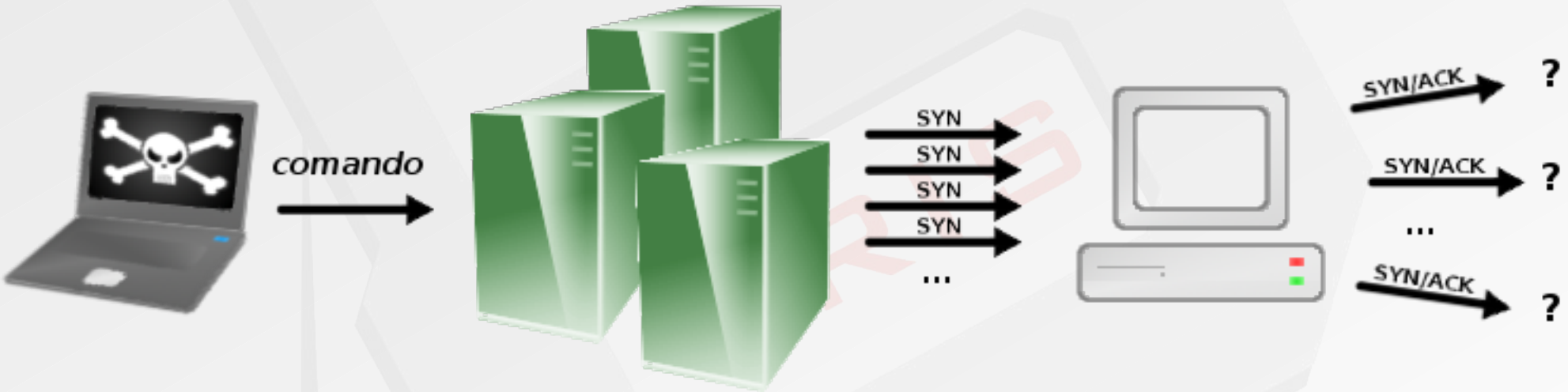
Negação de Serviços >> Ataques em Rede

Ataques Remotos Simples (SYN Flood)

SYN Flood tradicional (1 x 1) com intermediário

Negação de Serviços >> Ataques em Rede

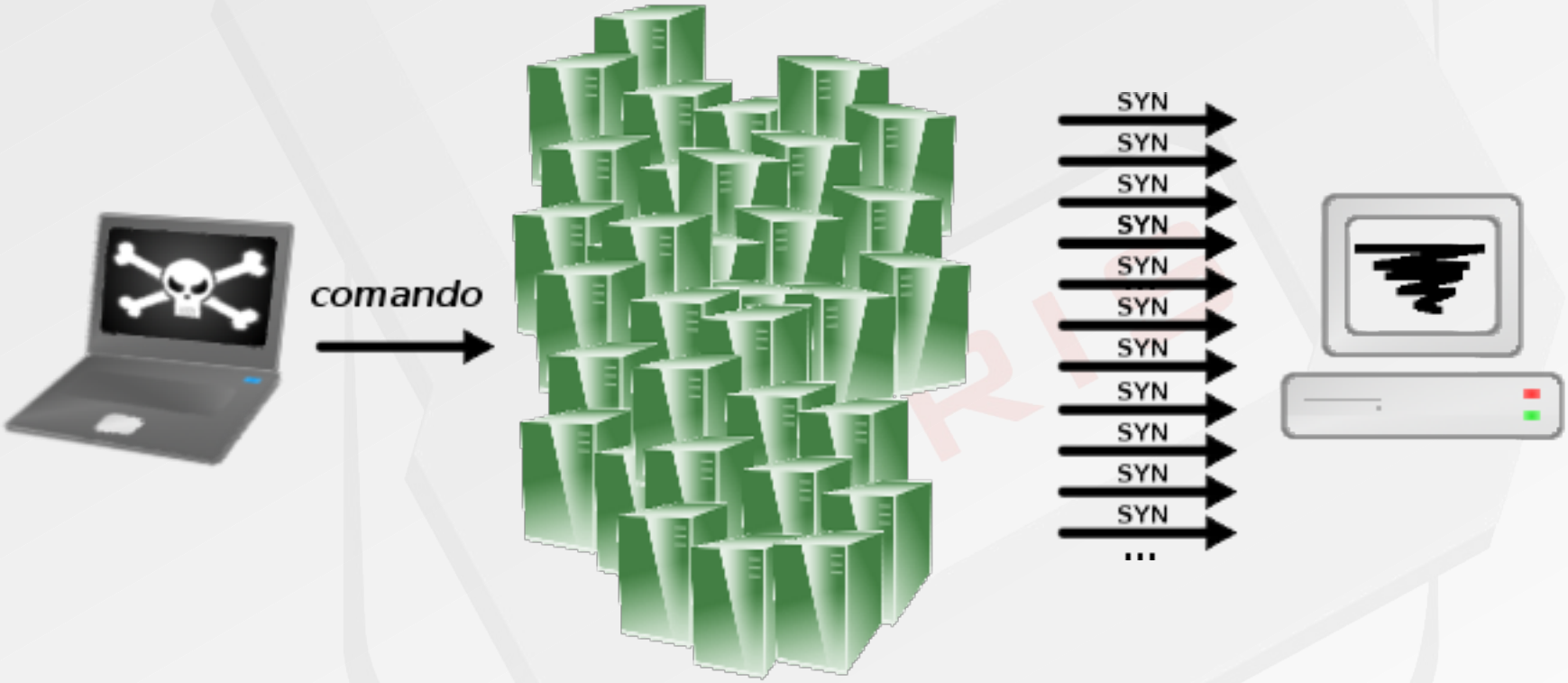
Ataques Distribuídos (DDoS)



SYN Flood Distribuído (3 x 1)

Negação de Serviços >> Ataques em Rede

Ataques Distribuídos (DDoS)

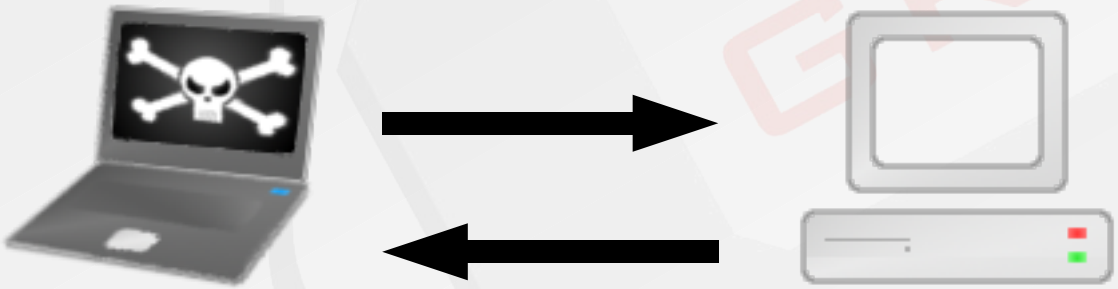


SYN Flood Distribuído (N x 1)

Negação de Serviços >> Ataques em Rede

Ataques Distribuídos Refletidos (DRDoS)

Refletor: *qualquer host que retorne um pacote ao receber um pacote*



Negação de Serviços >> Ataques em Rede

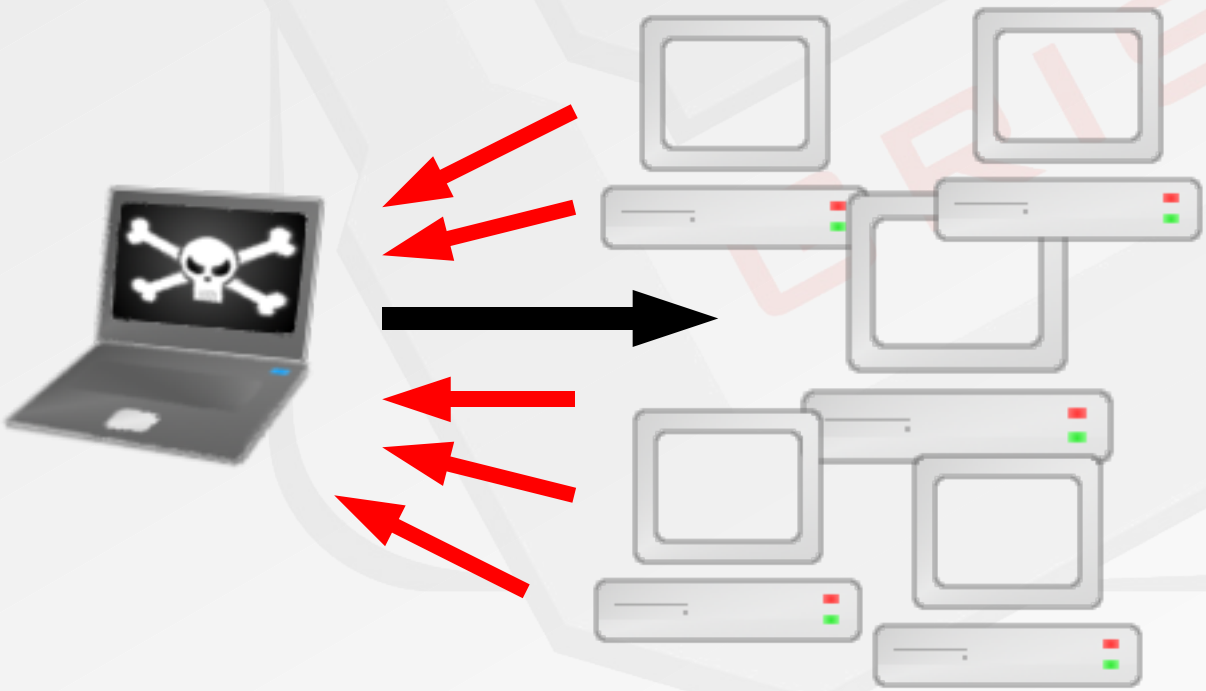
Ataques Distribuídos Refletidos (DRDoS)

Refletor: *qualquer host que retorne um pacote ao receber um pacote*

Negação de Serviços >> Ataques em Rede

Ataques Distribuídos Refletidos (DRDoS)

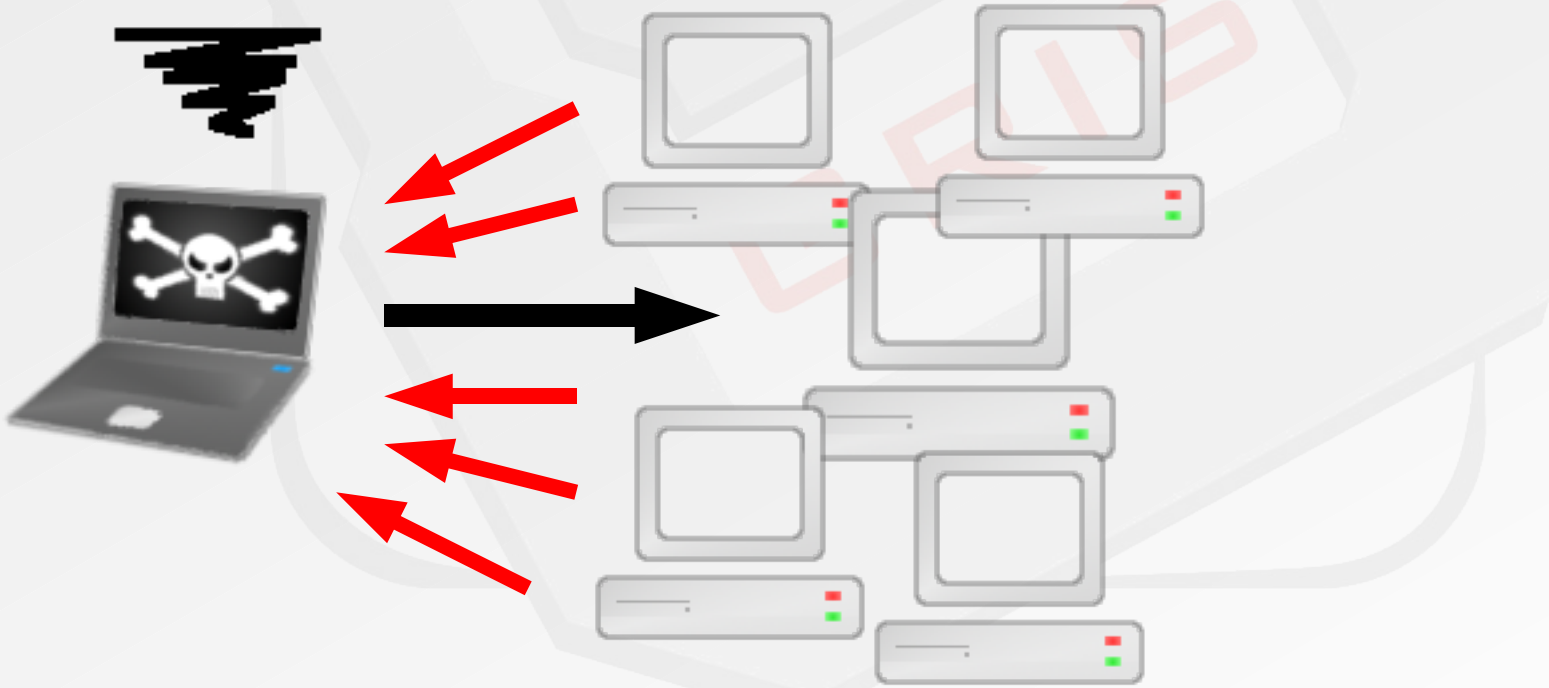
Refletores Especiais: Acesse um host, receba resposta de vários hosts (*"broadcast"*)



Negação de Serviços >> Ataques em Rede

Ataques Distribuídos Refletidos (DRDoS)

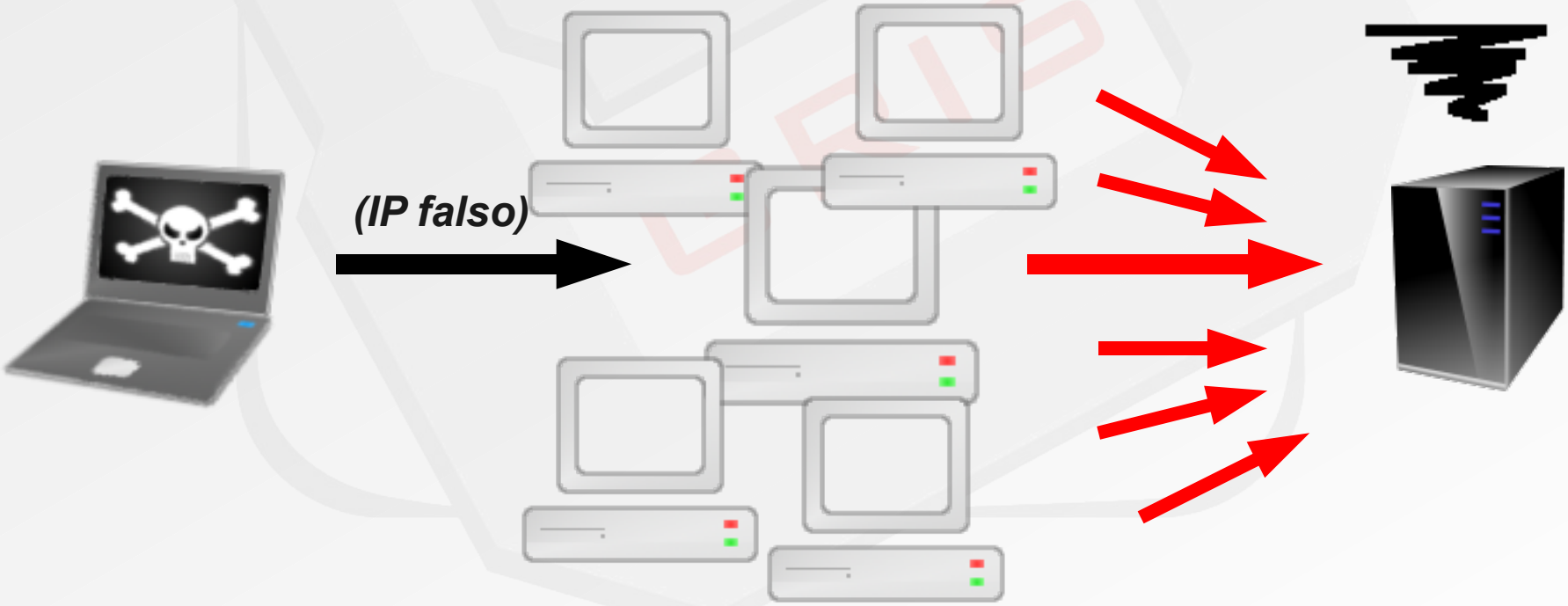
Refletores Especiais: Acesse um host, receba resposta de vários hosts (*"broadcast"*)



Negação de Serviços >> Ataques em Rede

Ataques Distribuídos Refletidos (DRDoS)

Refletores Especiais: Acesse um host, receba resposta de vários hosts (*"broadcast"*)



Negação de Serviços >> Ataques em Rede

Ataques de Amplificação

```
> dig @nameserver ns .
;; QUESTION SECTION:
;.                IN  NS

;; ANSWER SECTION:
.           7439    IN  NS  B.ROOT-SERVERS.NET.
.           7439    IN  NS  D.ROOT-SERVERS.NET.
.           7439    IN  NS  H.ROOT-SERVERS.NET.
.           7439    IN  NS  F.ROOT-SERVERS.NET.
.           7439    IN  NS  E.ROOT-SERVERS.NET.
                        (...)
;; MSG SIZE  rcvd: 228
```

http://www.secureworks.com/research/threats/dns-amplification/?threat=dns-amplification

Negação de Serviços >> Ataques em Rede

Ataques de Amplificação

```
> dig @a.dns.br +bufsize=4096 +dnssec any br
;; QUESTION SECTION:
;br.                IN  ANY

;; ANSWER SECTION:
br.         172800 IN  NS  a.dns.br.
br.         172800 IN  NS  b.dns.br.
br.         172800 IN  NS  c.dns.br.
br.         172800 IN  NS  d.dns.br.
br.         172800 IN  NS  e.dns.br.
br.         172800 IN  NS  f.dns.br.
br.         172800 IN  RRSIG  NS 5 1 172800 20090709050001
20090702050001 12063 br. Q4IN1ZgHXbNdy9mIHAaj17G8ylyWYGHTws
(...)
;; MSG SIZE  rcvd: 1621
```

Negação de Serviços >> Ataques em Rede

Ataques Permanentes (PDoS)

- Exigem reposição do hardware após ataque (*"Bricking"*)
- Ataques a firmware
- Explorando atualização da flash (*"phlashing"*)
- PhlashDance Fuzzer

http://eusecwest.com/esw08/esw08-smith.pdf

Negação de Serviços >> Ataques Clássicos

- *Smurf Attack*
  - pedidos ICMP para endereços de broadcast com IP da vítima como origem
- *Ping flood*
  - mais pedidos ICMP echo do que a vítima pode tratar
- *Teardrop/Nuke*
  - *pacotes fragmentados e inválidos*
- *Ping of Death*
  - *pacote ping (ICMP echo) maior que 65535 bytes*

Identificando Máquinas Zumbi – O Filme

ZOMBIES
ATE MY BANDWIDTH!

ATTACK OF THE
SPACE ZOMBIE COMPUTERS
FROM HELL!

Identificando Máquinas Zumbi

- Análise de Tráfego (Manual/NIDS)
- Antivírus
- Política de Segurança

Protegendo-se de Ataques Locais

- Sistemas atualizados
- Particionamento de disco
- Cotas
- ACLs

Protegendo-se de Ataques Remotos

- Sistemas atualizados
- Topologia de rede bem estruturada
- Firewalls
- SYN Cookies
- ACLs em roteadores e switches
- Rotas e Faixas de IP alternativas

Obrigado!

Dúvidas?