Fundamentos de Segurança de Redes

Prof. Fred Sauer, D.Sc.
Elaborado por Túlio Alvarez

Aula 2 – Tipos de Ataques

Aula 2 - Tipos de Ataques

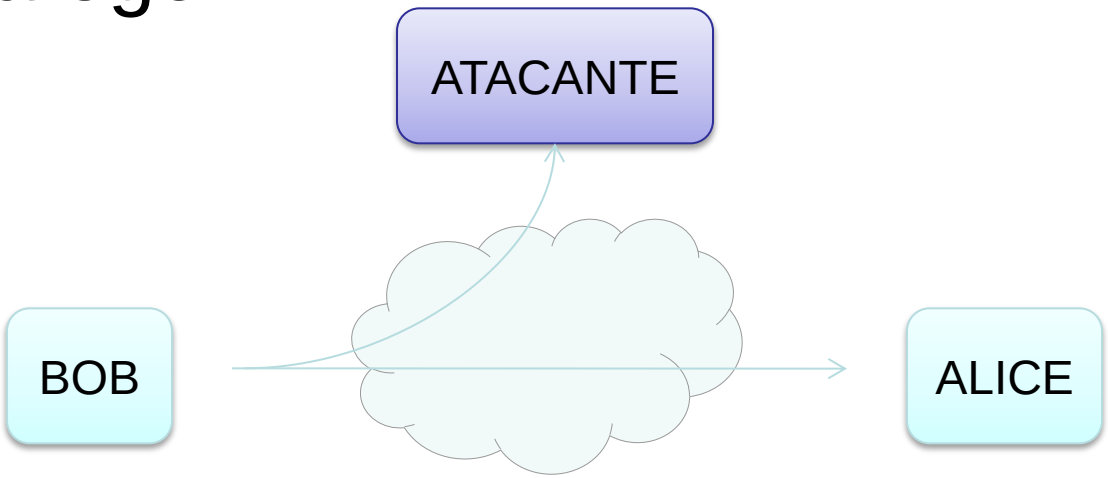
- Sniffers
- Fraudes com uso do EMAIL
  - Phishing
  - SPAM
- Varredura de portas
- Varredura de vulnerabilidades
- Spoofing
- Poisoning
- Man-in-the-middle
- DoS/DDoS
  - Buffer overflow1
  - SYN FLOOD
  - SMURF
  - FRAGGLE
  - Fragmentação
  - LAND
- Web attacks:
  - SQL *injection*
  - *Cross-site scripting*
  - *defacement* (pichação)

Revisão

- Tipos de Ataque
  - Passivos (monitoração)
  - Ativos (modificação, criação, negação de serviços, etc)

Revisão

- Passivos: objetivo de obter informações que estão sendo transmitidas. Ex.: análise de tráfego.

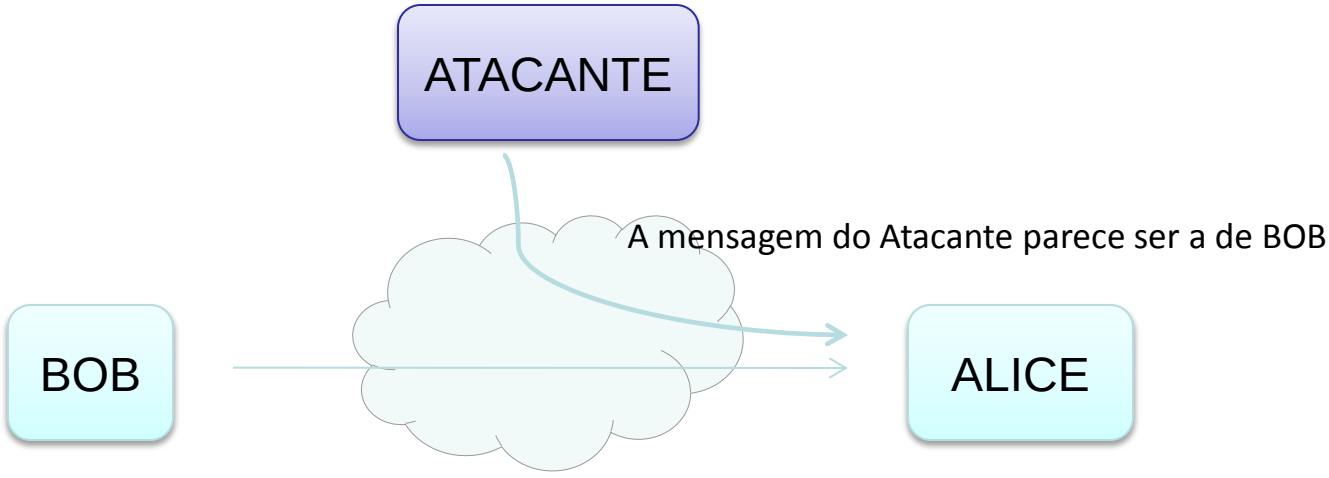


ANÁLISE DE TRÁFEGO

4

Revisão

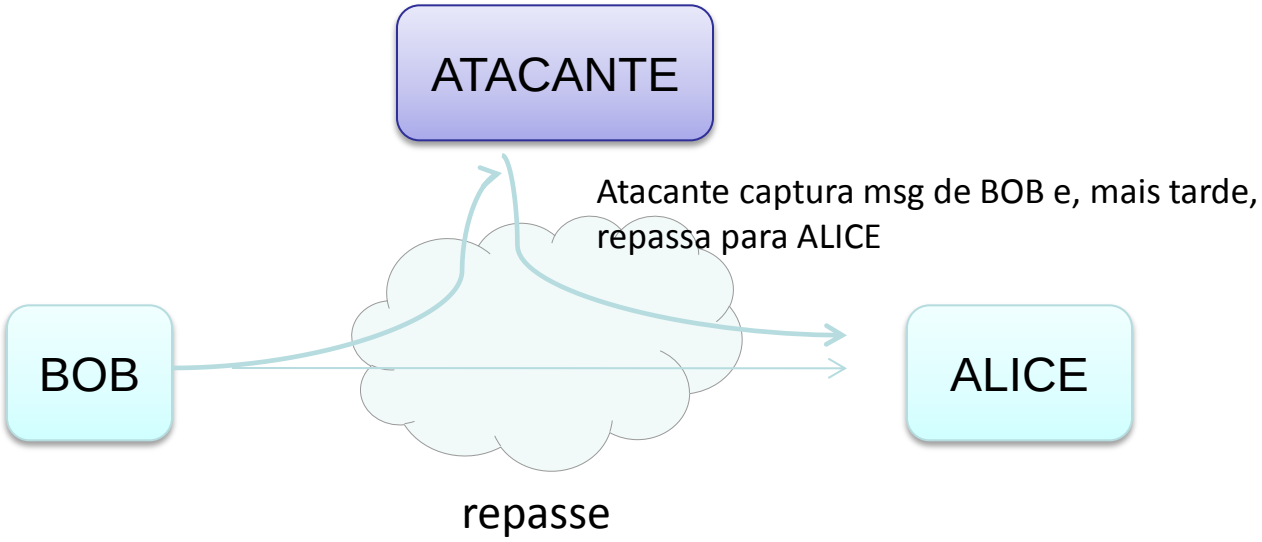
- Ativos: envolvem modificação do fluxo ou criação/simulação do mesmo. Ex.:
  - Disfarce: ATACANTE finge ser BOB para se comunicar com ALICE



Disfarce

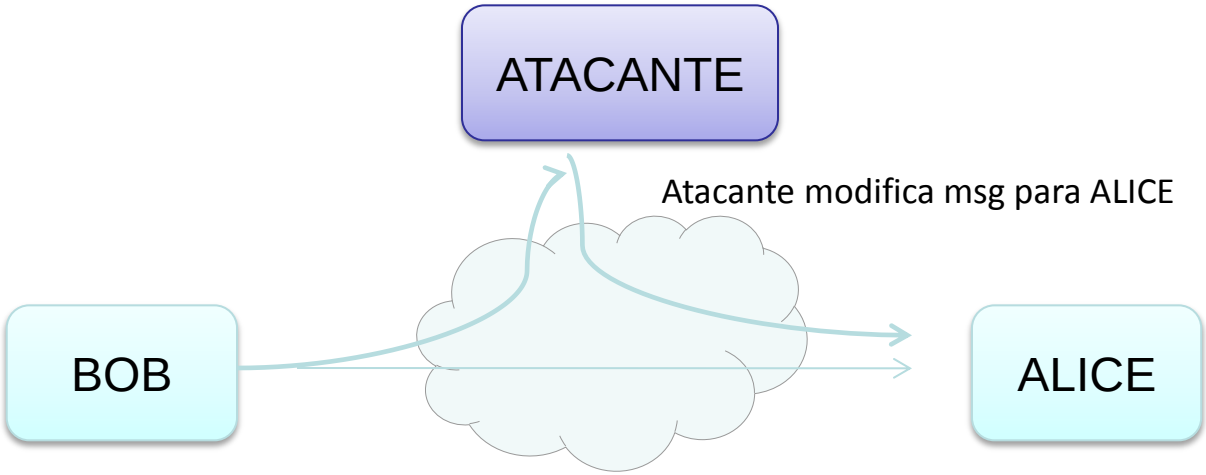
Revisão

- Ativos
  - Repetição (replay) : envolve captura passiva de determinados dados e sua retransmissão para tentar acesso ou efeito não autorizado.



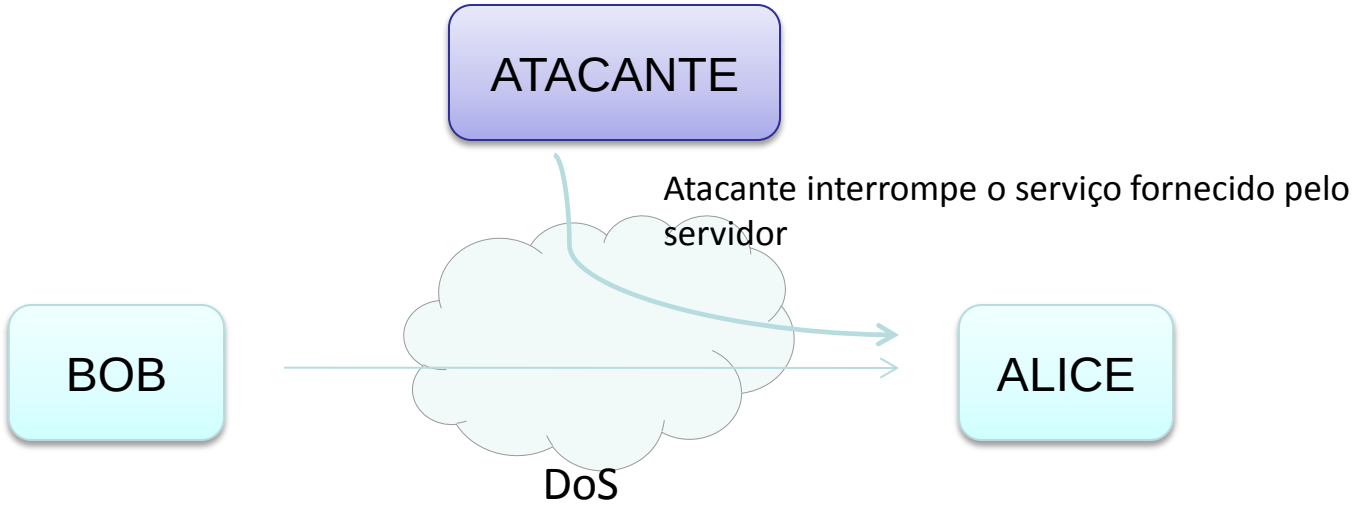
Revisão

- Ativos
  - Modificação: alterar alguma parte da msg para produzir efeito não autorizado.



Revisão

- Ativos
  - Negação de Serviço: impedir ou inibir o funcionamento e gerenciamento de uma entidade, causando sua interrupção, seja por sobrecarga ou desativação.



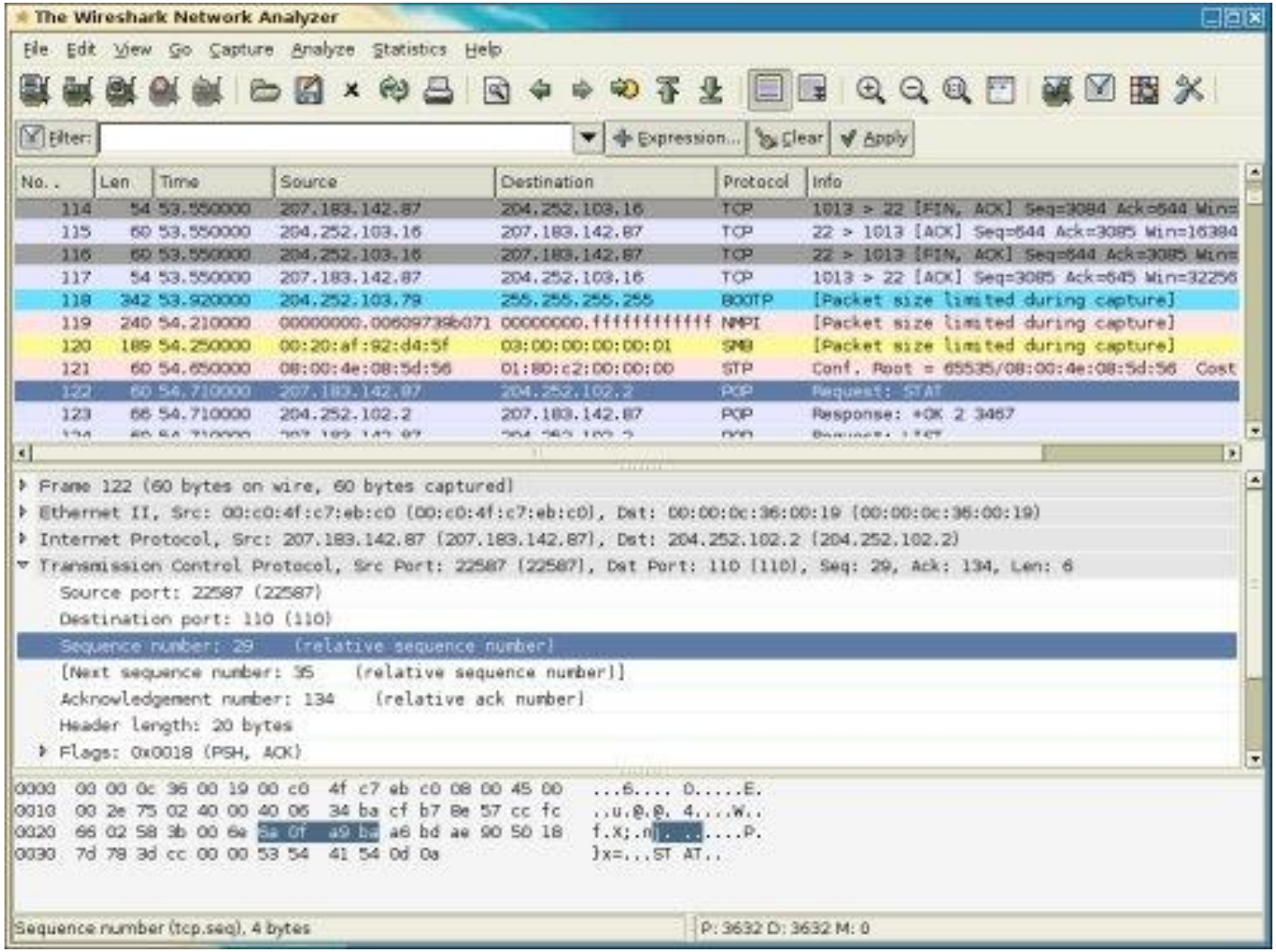
Sniffers

- Programa para interceptar e registrar o tráfego de dados de uma rede
- Cada pacote é capturado e pode ser analisado bit a bit
- Senhas e dados em claro podem ser capturados (telnet, login em sites sem criptografia, email, conversas em chat, etc)
  - Ethereal/Wireshark
  - TCPDUMP, WINDUMP
  - Carnivore (FBI), ECHELON (NSA)

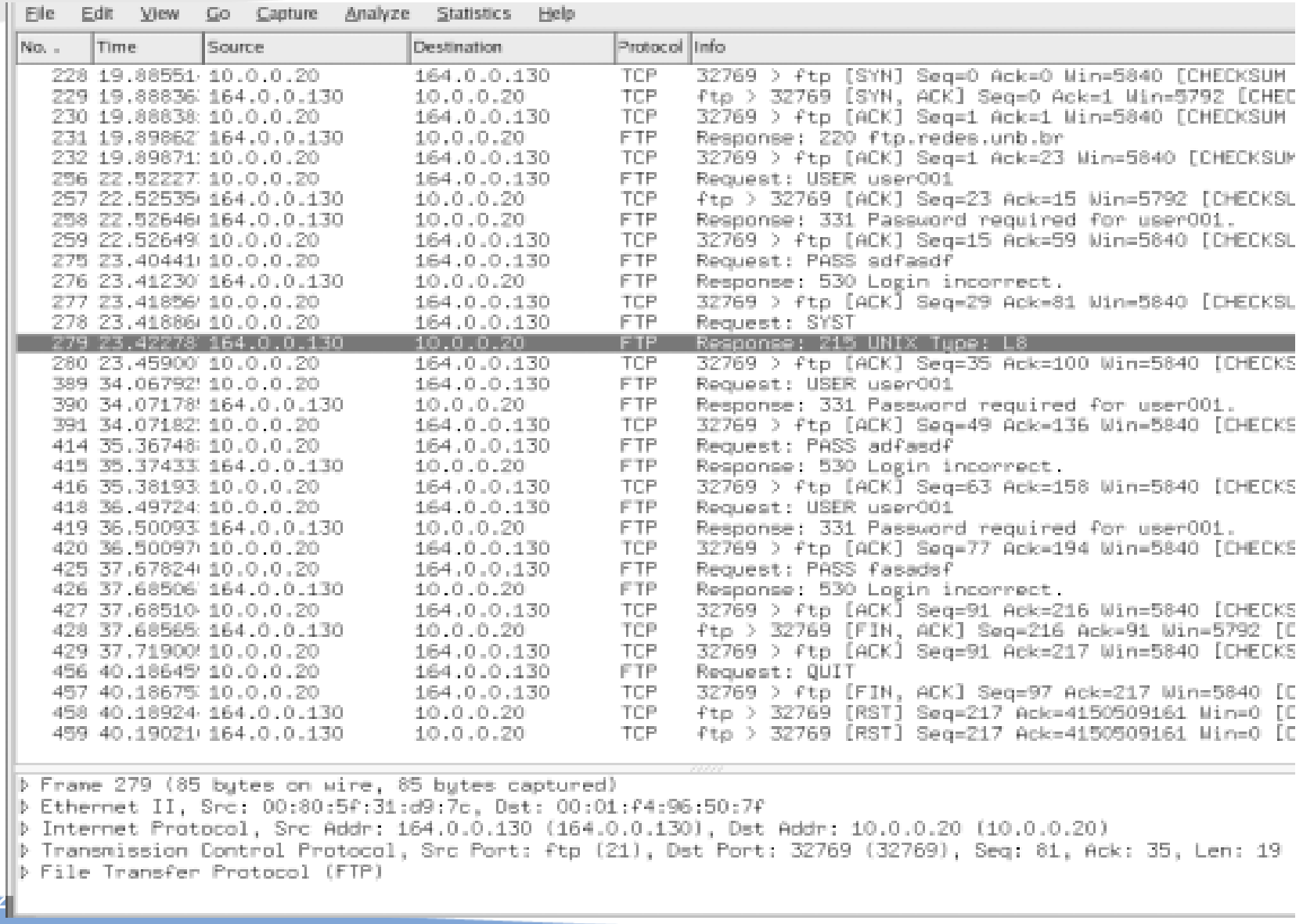
Sniffers

- Placa opera em modo promíscuo para capturar todos os dados do segmento de rede
- Difícil de ser detectado, porém há técnicas para detectar sniffer – exemplos:
  - ARP (resposta da máquina que contém o sniffer)
  - PING (lentidão na resposta e resposta com MAC errado)

Sniffers - Wireshark



Sniffers - Ethereal



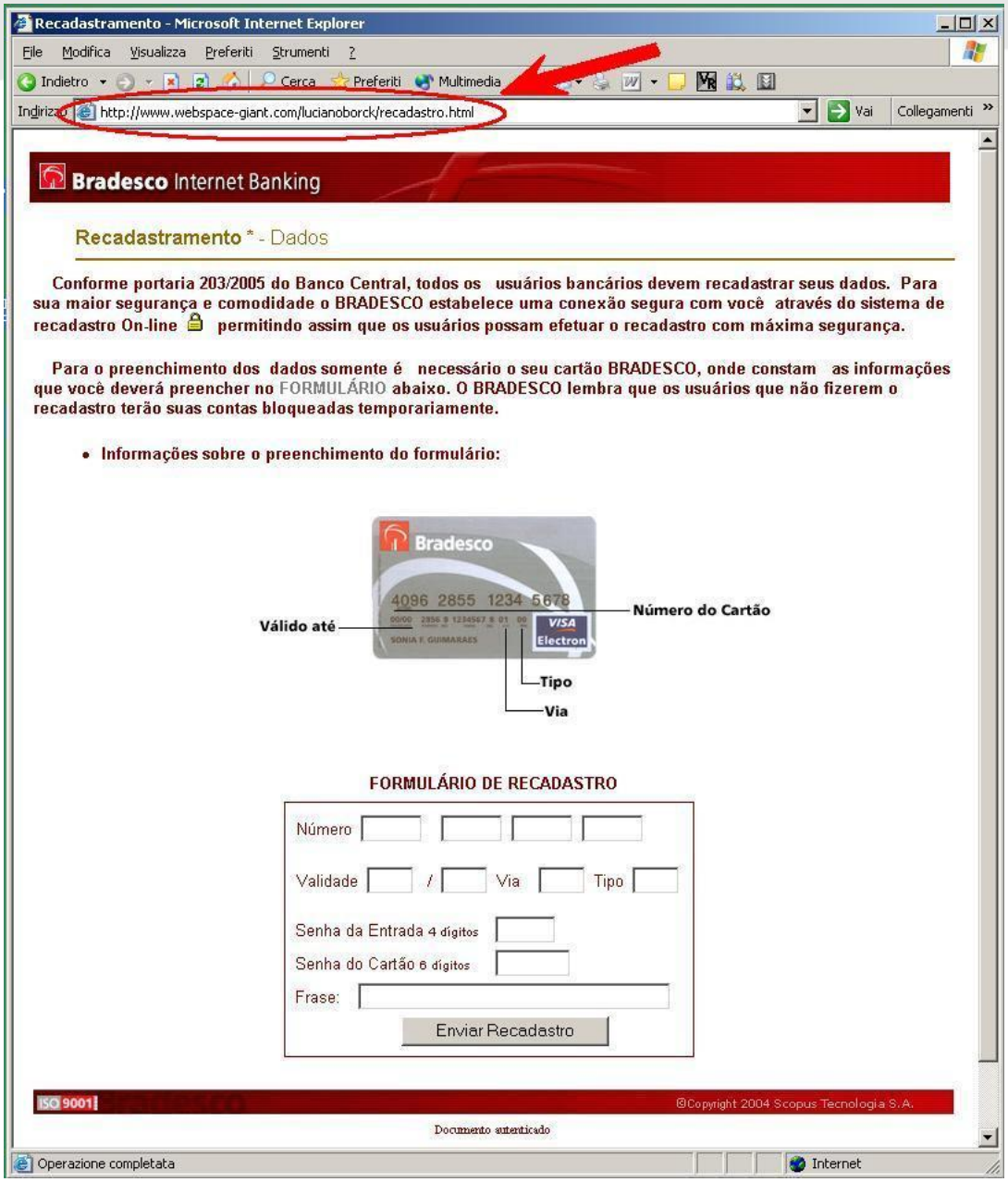
Fraude com uso do EMAIL

- Spam
- Phishing Scam (Phishing)

Phishing

- Tipo de engenharia social
- Envio de msg não solicitada com objetivos maliciosos
  - mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
  - mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários
  - Outras variantes.

Exemplos de Phishing

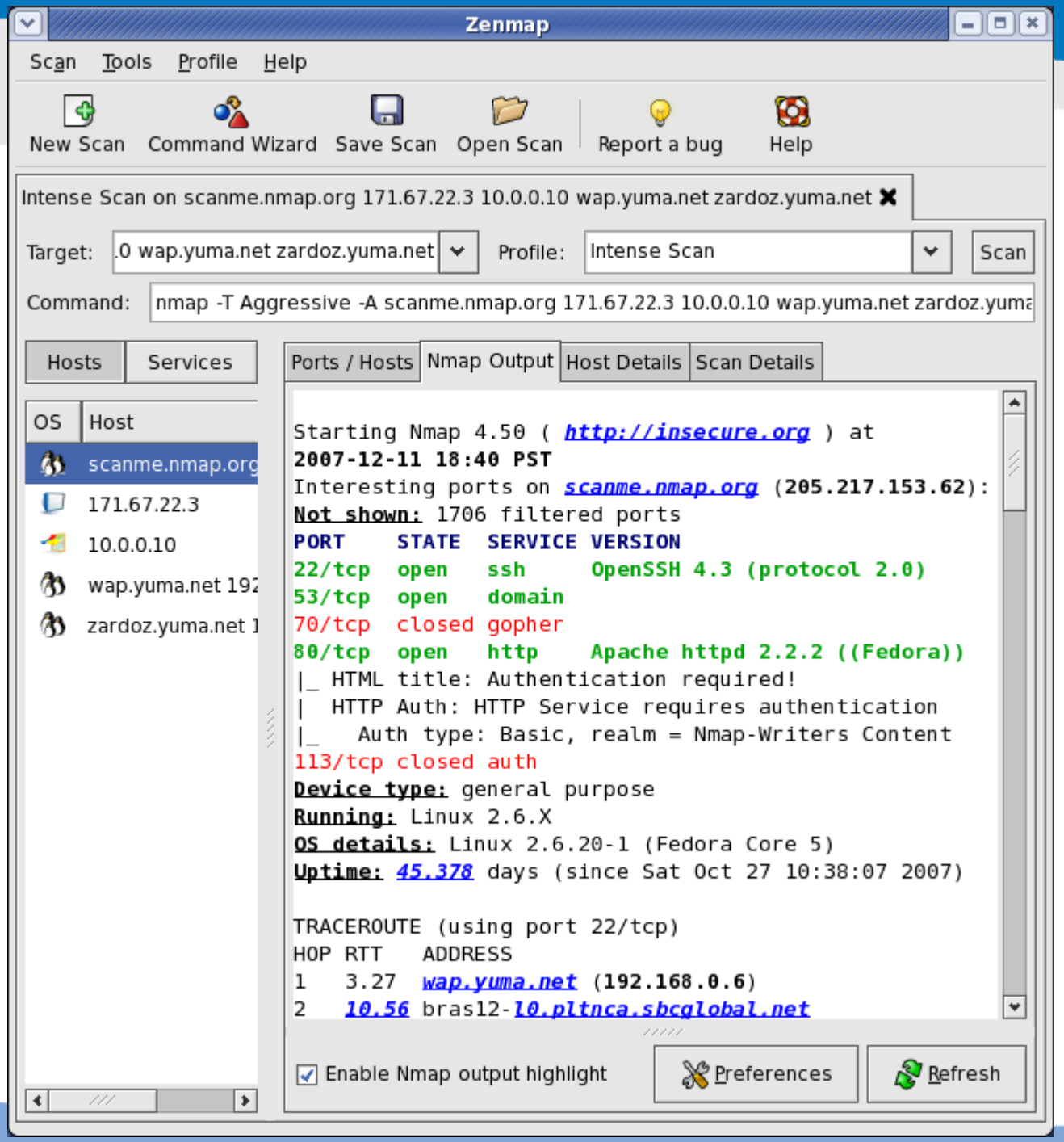


Exemplos de Phishing

Varredura de Portas

- Uso de um Software desenhado para buscar informação sobre hosts/portas utilizando a pilha TCP/IP.
  - Verificar tipos e versões de serviços no host
  - Portas padronizadas (1-1024)
  - Realizar auditorias
- Ex: Nmap

NMAP


Zenmap
Scan Tools Profile Help
New Scan
Command Wizard
Save Scan
Open Scan
Report a bug
Help
Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net
Target: .0 wap.yuma.net zardoz.yuma.net
Profile: Intense Scan
Scan
Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma
Hosts
Services
OS
Host
scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1
Ports / Hosts
Nmap Output
Host Details
Scan Details
Starting Nmap 4.50 (http://insecure.org) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 4.3 (protocol 2.0)
53/tcp open domain
70/tcp closed gopher
80/tcp open http Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
| HTTP Auth: HTTP Service requires authentication
|_ Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)
TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
1 3.27 wap.yuma.net (192.168.0.6)
2 10.56 bras12-l0.pltnca.sbcglobal.net
Enable Nmap output highlight
Preferences
Refresh

Varredura de Portas

- Vários tipos de varreduras:
  - TCP connect ()
    - Conexão estabelecida se porta aberta,
  - TCP SYN (half open)
    - Receber SYN/ACK - porta aberta – Receber RST - fechada
    - Conexão não é estabelecida porque scanner manda RST
  - TCP ACK → sempre respondido com RST se fechada
  - UDP vazio
    - ICMP port unreachable – porta fechada
  - ICMP (ping sweep – “varredura”)
    - Após um ICMP ECHO REQUEST não respondido, envia TCP SYN ou ACK porta 80*
      - Porque Firewalls podem bloquear ICMP ECHO
    - Se receber RST ou SYN/ACK o alvo está alive e há bloqueio de ICMP ECHO

*Obs.: porta omissiva 80

Varredura de Portas

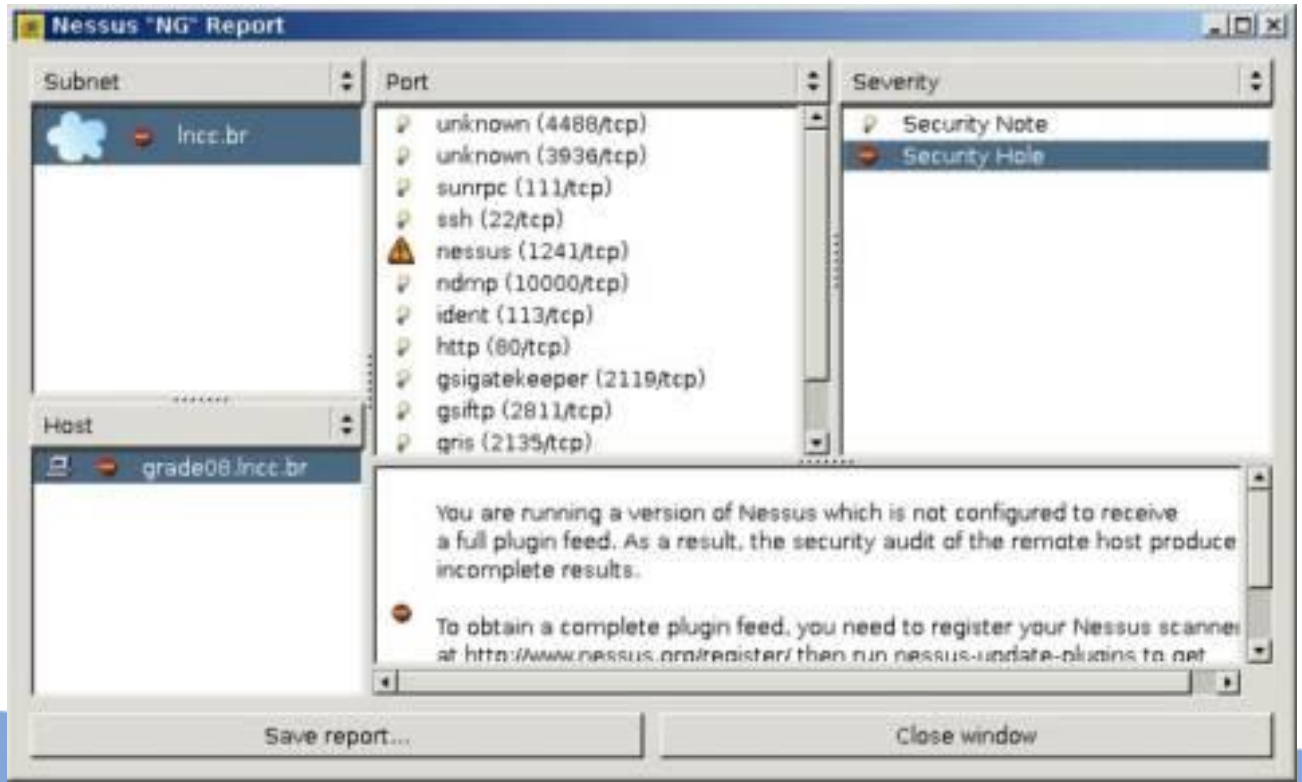
- IDS procuram por SYN SCANS, então são usados (modo stealth):
  - FIN (Flag TCP)
    - Resposta for RST – porta fechada; se não responde - aberta
  - Xmas Tree
    - Envio de pacotes com flags FIN, URG e PUSH também geram RST se porta fechada e nada se porta aberta
  - Null Scan
    - Nenhum flag - Portas fechadas respondem RST a pacotes que não sejam SYN e nada se abertas
  - Comportamento previsto na RFC 793 – FIN scan, XMAS e NULL scan não funcionam com windows
- RPC Scan – comandos NULL SunRPC provocam respostas se a porta estiver aberta, mas abre sessões gerando log

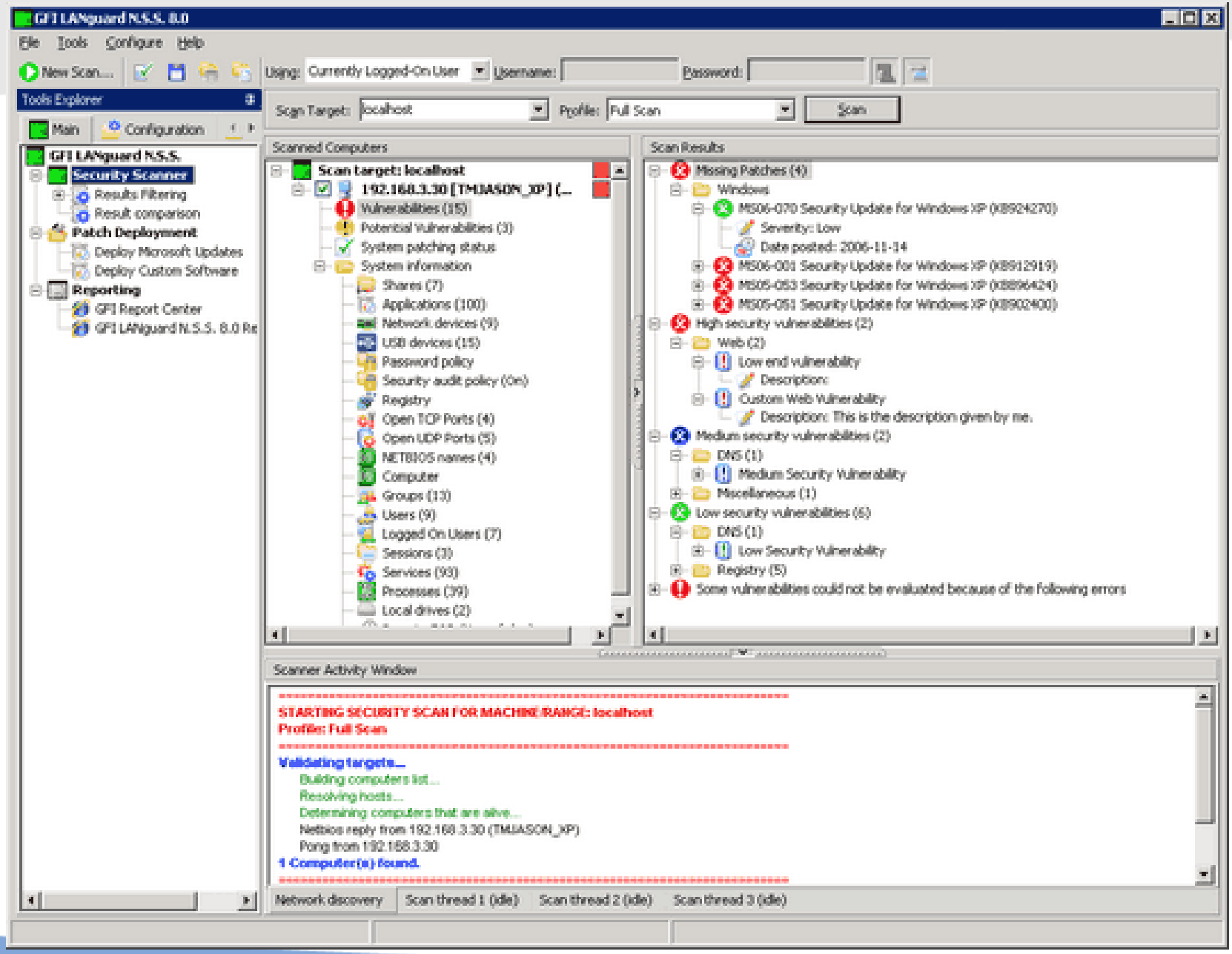
Varredura de Vulnerabilidades

- Busca de vulnerabilidades específicas para cada tipo de serviço
- Os softwares realizam testes na rede à procura de falhas de segurança seja em protocolos, serviços, aplicativos ou sistemas operacionais
  - Ex.: NESSUS, RETINA, LANGUARD, SAINT, MBSA, Core Impact, etc.
- Importante manter os plugins atualizados

Varredura de Vulnerabilidades

- Utilizados em auditorias e pentests (testes de ataques)
- A descoberta das vulnerabilidades é fundamental para evitar um ataque




GFI LANguard N.S.S. 8.0
File Tools Configure Help
New Scan...
Using: Currently Logged-On User
Username:
Password:
Tools Explorer
Main
Configuration
GFI LANguard N.S.S.
Security Scanner
Results Filtering
Result comparison
Patch Deployment
Deploy Microsoft Updates
Deploy Custom Software
Reporting
GFI Report Center
GFI LANguard N.S.S. 8.0 Re
Scan Target: localhost
Profile: Full Scan
Scan
Scanned Computers
Scan target: localhost
192.168.3.30 [TMJASON_XP] (...
Vulnerabilities (15)
Potential Vulnerabilities (3)
System patching status
System information
Shares (7)
Applications (100)
Network devices (9)
USB devices (15)
Password policy
Security audit policy (On)
Registry
Open TCP Ports (4)
Open UDP Ports (5)
NETBIOS names (4)
Computer
Groups (13)
Users (9)
Logged On Users (7)
Sessions (3)
Services (93)
Processes (39)
Local drives (2)
Scan Results
Missing Patches (4)
Windows
MS06-070 Security Update for Windows XP (KB924270)
Severity: Low
Date posted: 2006-11-14
MS06-001 Security Update for Windows XP (KB912919)
MS05-053 Security Update for Windows XP (KB896424)
MS05-051 Security Update for Windows XP (KB902400)
High security vulnerabilities (2)
Web (2)
Low end vulnerability
Description:
Custom Web Vulnerability
Description: This is the description given by me.
Medium security vulnerabilities (2)
DNS (1)
Medium Security Vulnerability
Miscellaneous (1)
Low security vulnerabilities (6)
DNS (1)
Low Security Vulnerability
Registry (5)
Some vulnerabilities could not be evaluated because of the following errors
Scanner Activity Window
STARTING SECURITY SCAN FOR MACHINE/RANGE: localhost
Profile: Full Scan
Validating targets...
Building computers list...
Resolving hosts...
Determining computers that are alive...
Netbios reply from 192.168.3.30 (TMJASON_XP)
Pong from 192.168.3.30
1 Computer(s) found.
Network discovery
Scan thread 1 (idle)
Scan thread 2 (idle)
Scan thread 3 (idle)

Spoofing e Poisoning

- Spoofing:
  - Spoofing = falsificação
  - Mascarar IP de origem utilizando endereços falsos
  - Utilizado principalmente em ataques DoS, para burlar regras de firewall
    - Ex.: IP Spoofing, Email Spoofing, MAC Spoofing, etc

Spoofing e Poisoning

- Poisoning
  - Técnica de envenenamento/alteração de dados de tabelas
  - Ex.: DNS Poisoning
    - Servidores DNS não fazem autenticação quando trocam informações com outros servidores de nomes
    - Atacante pode inserir informações erradas com intenção de desviar usuários para hosts pré-definidos

Man-in-the-middle (MITM)

- Ataque ativo
  - Com sequestro de conexões (session hijacking)
- Difícil de ser realizado
- Tem como base a exploração do estado de dessincronização dos dois lados da conexão TCP
  - Um terceiro pode entrar no meio dos hosts e enviar pacotes válidos para ambos.
  - Ex.: CAIN, DSNIFF, Ettercap, etc
- Redes sem fio são vulneráveis

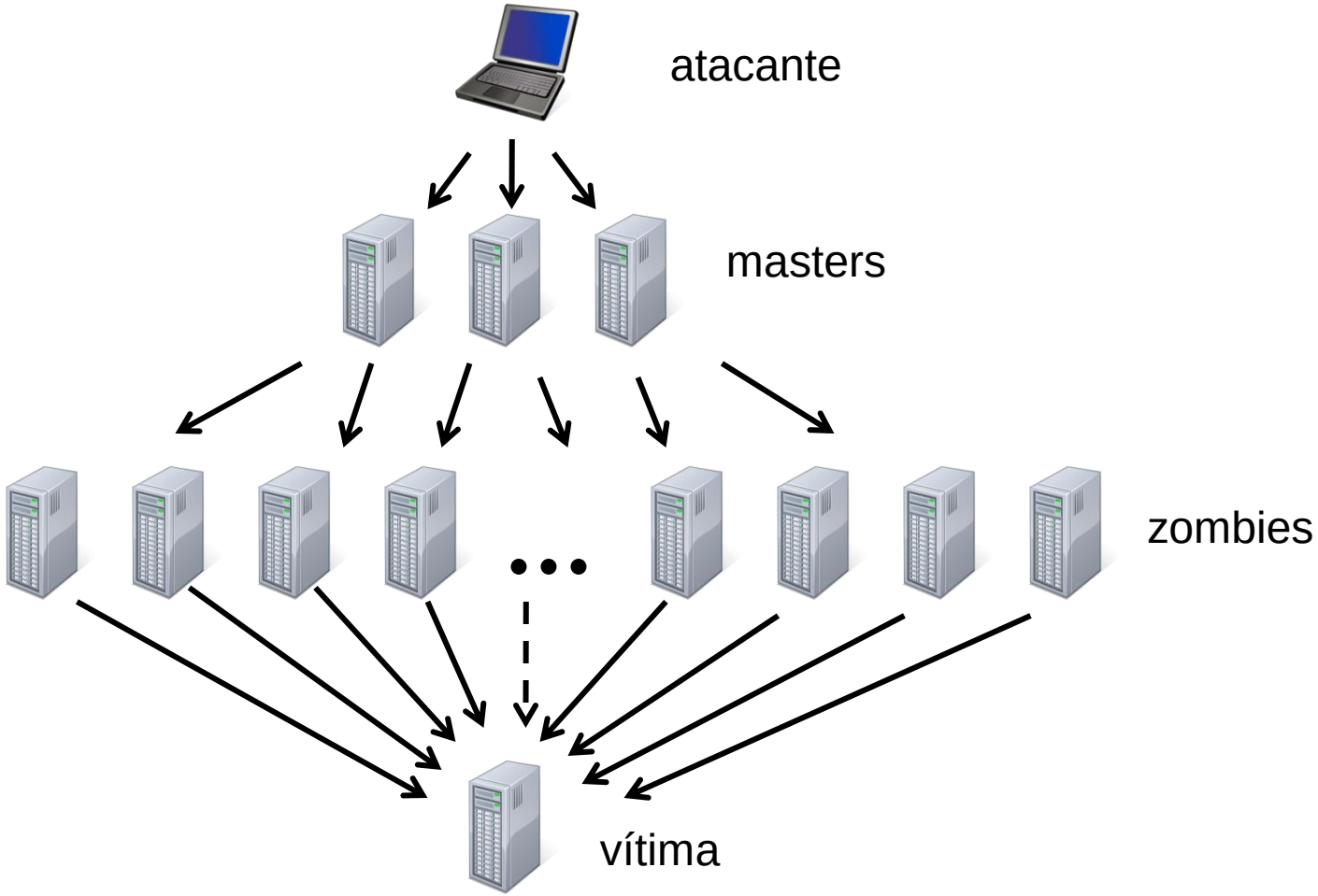
Denial-of-Service - DoS

- Ataca os recursos do sistema
- Usuários legítimos ficam impossibilitados de utilizar sistema
- Várias técnicas:
  - Ataque distribuído (DDoS)
  - Buffer Overflow
  - Flooding – inundação. Várias requisições simultâneas
  - Transferência de arquivos muito grandes para o servidor com a finalidade de lotar a capacidade

Distributed Denial-of-Service - DDoS

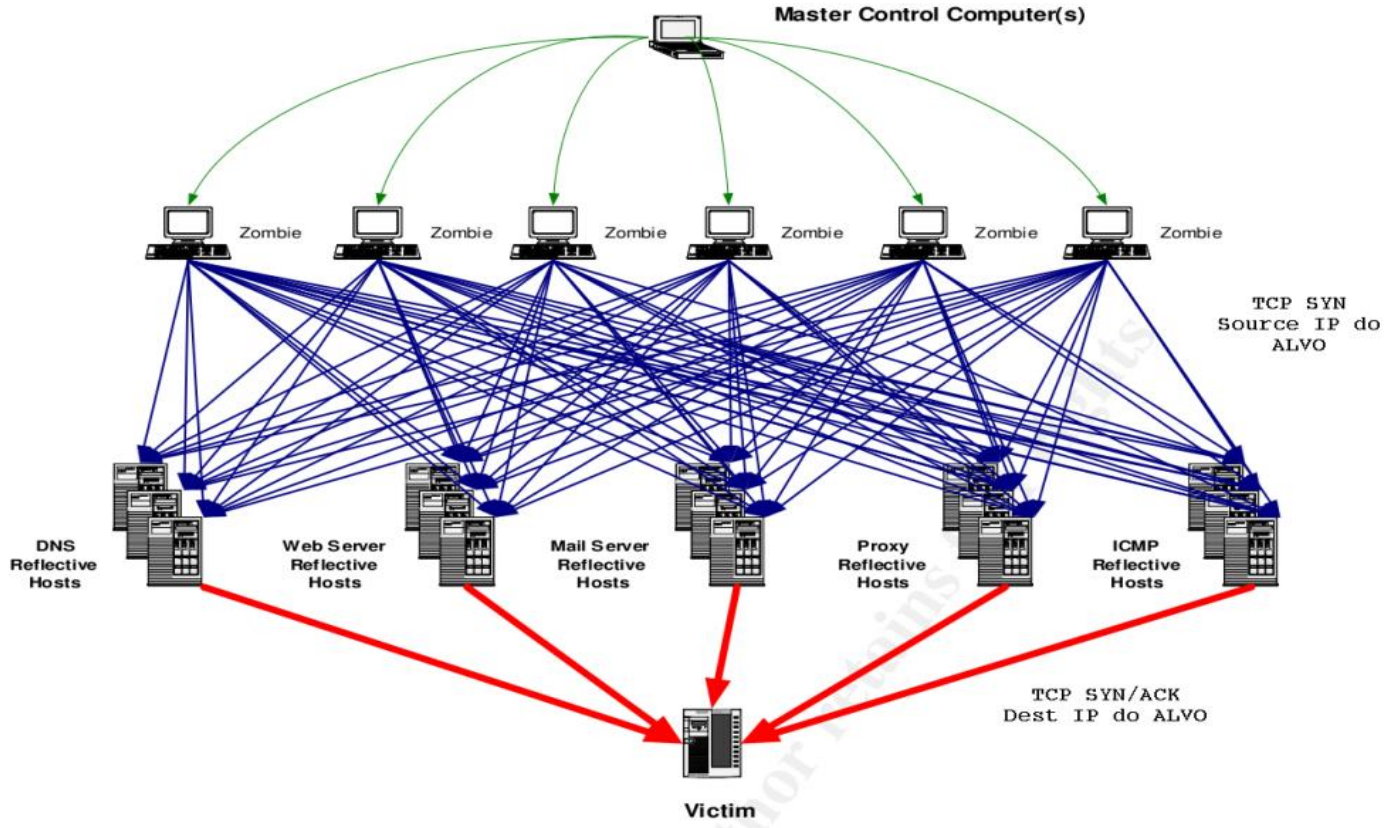
- Extensão lógica do DoS, quando muitos computadores estão envolvidos no ataque
- Vários computadores realizando requisições ou enviando pacotes mal formados a um sistema
  - Podem estar cientes ou não (zombies)
  - Ex.: ataque de uma botnet a um determinado site

Distributed Denial-of-Service - DDoS



DrDoS

- Distributed Reflexive DoS
- Mais difícil de detectar que o DoS, porque usa uma camada de servidores legítimos



Buffer Overflow

- “Estouro da pilha” de memória
- Método de ataque mais empregado – vários exploits
  - Um exploit para cada SO x hardware.
- Ocorre onde o controle do buffer (memória temporária para armazenamento de dados) não é feito adequadamente
  - Processo recebe mais dados que pode suportar

Buffer Overflow

- Possibilidade de execução de códigos arbitrários
- Pode resultar:
  - na perda ou modificação de dados
  - perda do controle do fluxo de execução do sistema, ou
  - paralisação do sistema.
- Diversos métodos:
  - Stack mashing, off-by-one ou frame pointer overwrite buffer overflow, return-into-libc e heap overflow.

Buffer Overflow

- “Estouro da pilha”
  - Descobrir uma variável do tipo buffer que esteja vulnerável
  - Verificar, no código fonte ou por tentativa ou erro, os endereços onde as chamadas de função estão, bem como o endereço que marca o início do buffer da variável
  - Fabricar um exploit que insira códigos de máquina no buffer, contendo instruções para nos dar um shell, e depois estufe a pilha até atingir a posição do ponteiro de retorno, lá colocando o endereço de início do buffer.

Buffer Overflow

Pilha Original

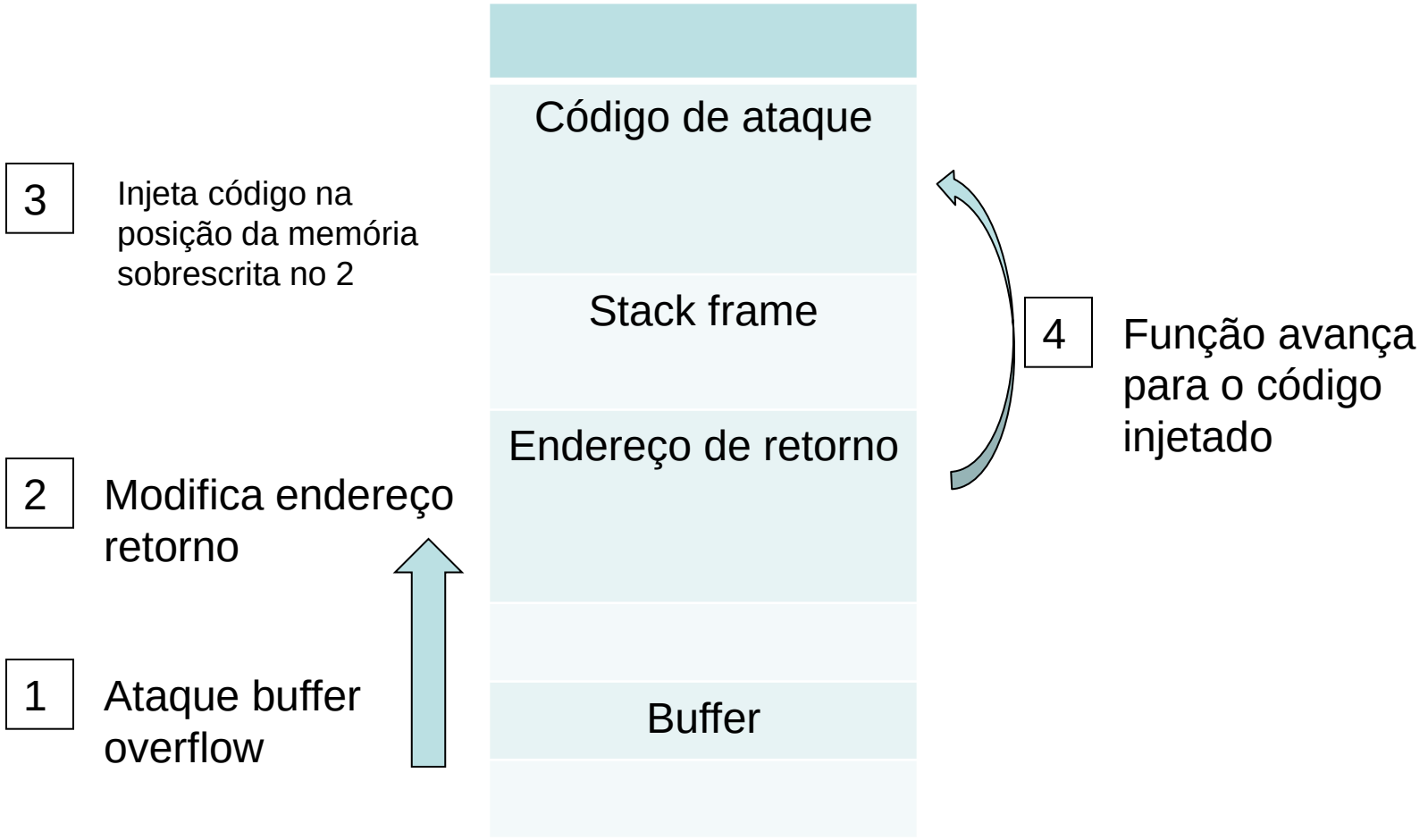
0xbffffd4	ESP
0xbffffd8	nome4 (arg)
0xbffffdc	nome4 (arg)
0xbffffe0	nome4 (arg)
0xbffffe4	nome3
0xbffffe8	nome2
0xbffffec	nome1
0xbffffff0	EBP
0xbffffff4	0x00400008 (EIP retorno)
0xbffffff8	arg[1] (parâmetro)

Pilha do Exploit

0xbffffd4	ESP
0xbffffd8	NOP (0x90)
0xbffffdc	NOP (0x90)
0xbffffe0	NOP (0x90)
0xbffffe4	NOP (0x90)
0xbffffe8	NOP (0x90)
0xbffffec	NOP (0x90)
0xbffffff0	execute /bin/sh
0xbffffff4	0xbffffd8
0xbffffff8	arg[1] (parâmetro)

www.crimesciberneticos.com

Buffer Overflow



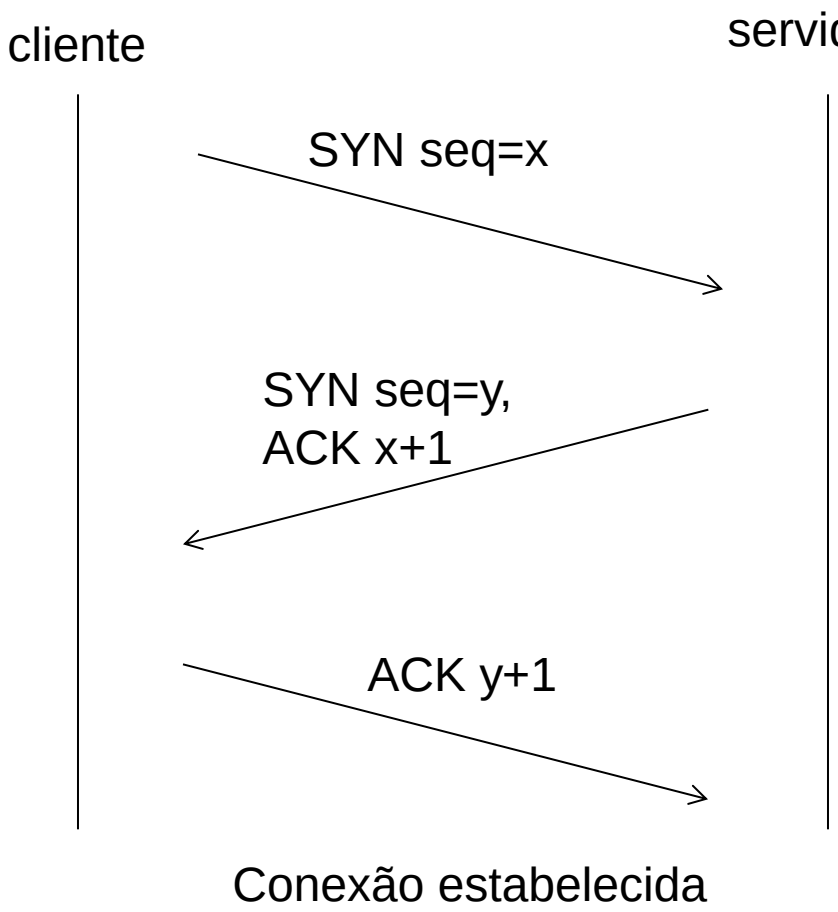
Buffer Overflow

- Difíceis de serem detectados
- Deve-se manter sistemas atualizados
- Utilização de IPS

SYN Flooding

- Usa propriedades do TCP (three-way-handshake)
- Grande número de requisições SYN é enviado
- O servidor não é capaz de responder a todas
- A pilha de memória sofre um overflow
- Requisições de usuários legítimos-desprezadas

SYN Flooding



Vários pacotes
SYN :
Fila das conexões
no servidor cheia
- SYN Flooding

SYN Flooding

- Pode ser evitado/minimizado:
  - Comparando taxas de requisições de novas conexões com o número de conexões em aberto – msg de alerta e ações preconfiguradas quando taxa chegar a um det. valor
  - Em conexões de baixa velocidade - Utilização de time-out e taxa máxima de conexões semi-abertas
  - Em conexões de alta velocidade – desabilitar ou bloquear temporariamente todos os pacotes SYN do host após determinada taxa de conexão

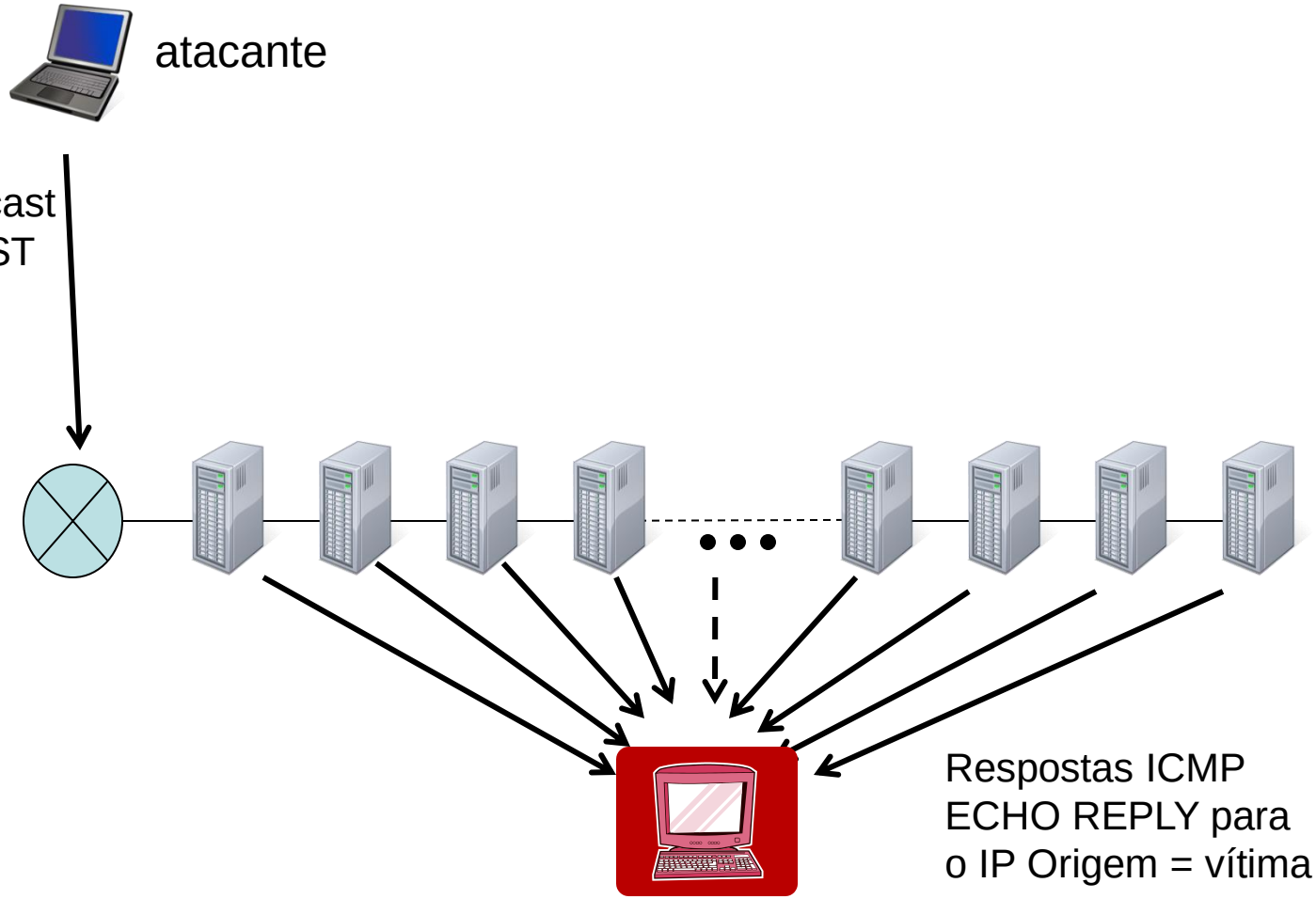
SYN Flooding

- Pode ser evitado/minimizado:
  - Utilizando FIREWALL configurado para evitar este tipo de ataque
  - IDS – para alertar quando da ocorrência do ataque
  - Instalar patches de correção que evitam o SYN attack

SMURF Attack

- Ataque nível de rede
- Grande tráfego de pacotes ICMP ECHO REQUEST é enviado para IP Broadcast da Rede com o endereço origem o da vítima
- Cada host da rede recebe a requisição ICMP e responde para o origem (ECHO REPLY)
- Vítima recebe um ataque DoS

SMURF Attack



SMURF Attack

- Prevenção:
  - Roteador – não receber ou deixar passar pacotes para endereços de broadcast por meio de suas interfaces de rede
    - Elimina PSB de ICMP ECHO para diagnóstico de rede
  - HOST configurados para não responder ICMP ECHO para o endereço Broadcast
  - Filtrar ataques com IP Falsos – spoffing (técnica egress filtering)
  - Utilização de IDS/IPS

SMURF Attack

Smurf Attack

Denial of Service

Sniffer data trace excerpts:

```
00:00:05.327 spoofed.target.com > 192.168.15.255: icmp: echo request
00:00:05.342 spoofed.target.com > 192.168.1.255:  icmp: echo request
00:00:14.154 spoofed.target.com > 192.168.15.255: icmp: echo request
00:00:14.171 spoofed.target.com > 192.168.1.255:  icmp: echo request
00:00:19.055 spoofed.target.com > 192.168.15.255: icmp: echo request
00:00:19.073 spoofed.target.com > 192.168.1.255:  icmp: echo request
00:00:23.873 spoofed.target.com > 192.168.15.255: icmp: echo request ...

05:20:48.261 spoofed.target.com > 192.168.0.0:       icmp: echo request
05:20:48.263 spoofed.target.com > 255.255.255.255:   icmp: echo request
05:21:35.792 spoofed.target.com > 192.168.0.0:       icmp: echo request
05:21:35.819 spoofed.target.com > 255.255.255.255:   icmp: echo request
05:22:16.909 spoofed.target.com > 192.168.0.0:       icmp: echo request
05:22:16.927 spoofed.target.com > 255.255.255.255:   icmp: echo request
05:22:58.046 spoofed.target.com > 192.168.0.0:       icmp: echo request
05:22:58.061 spoofed.target.com > 255.255.255.255:   icmp: echo request ...
```

FRAGGLE Attack

- Mesmo tipo de ataque, porém utiliza protocolo UDP
- UDP ECHO (porta 7) ou UDP CHARGEN (porta 19)
  - ECHO – repete os bytes recebidos
  - CHARGEN – responde com 0 a 512 caracteres randomicos

FRAGGLE Attack

- Prevenção
  - Similar ao estipulado para SMURF, porém deve-se observar que o protocolo é UDP

Fragmentação de Pacotes IP

- Relacionada com o MTU (*Maximum Transmission Unit*), que é a quantidade máxima de dados que podem passar em um pacote por um meio físico da rede
  - Ex.: ethernet: MTU = 1500 bytes (octetos).
  - Ex.: FDDI: MTU= 4470 bytes
- Fragmentação e desfragmentação são necessárias para a comunicação inter-redes
- Host de destino que remonta o pacote

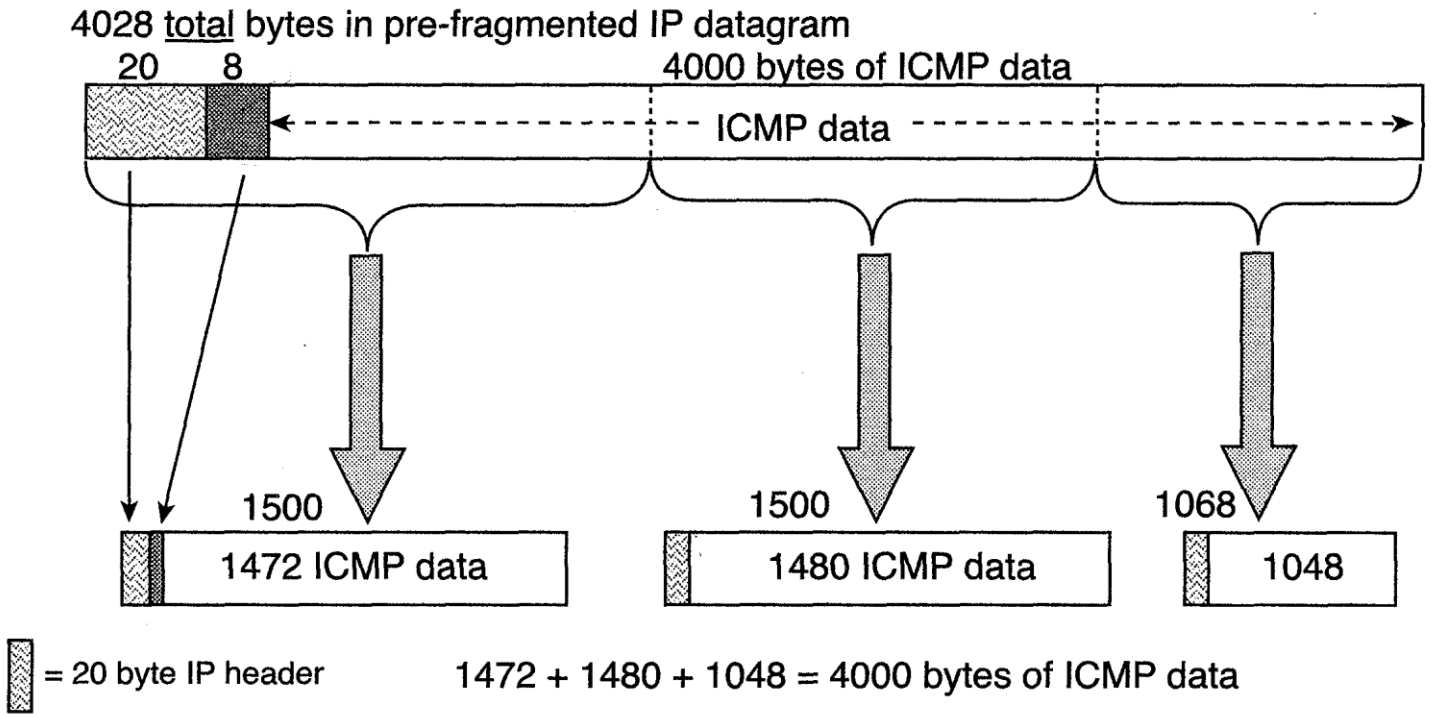
Fragmentação de Pacotes IP

- Possibilidade de ataque devido ao modo de como é implementada a fragmentação e reagrupamento
- O sistema não tenta processar o pacote até que todos os fragmentos sejam recebidos e reagrupados
- Pode ocorrer overflow na pilha TCP quando há reagrupamento de pacotes maiores que o tolerado

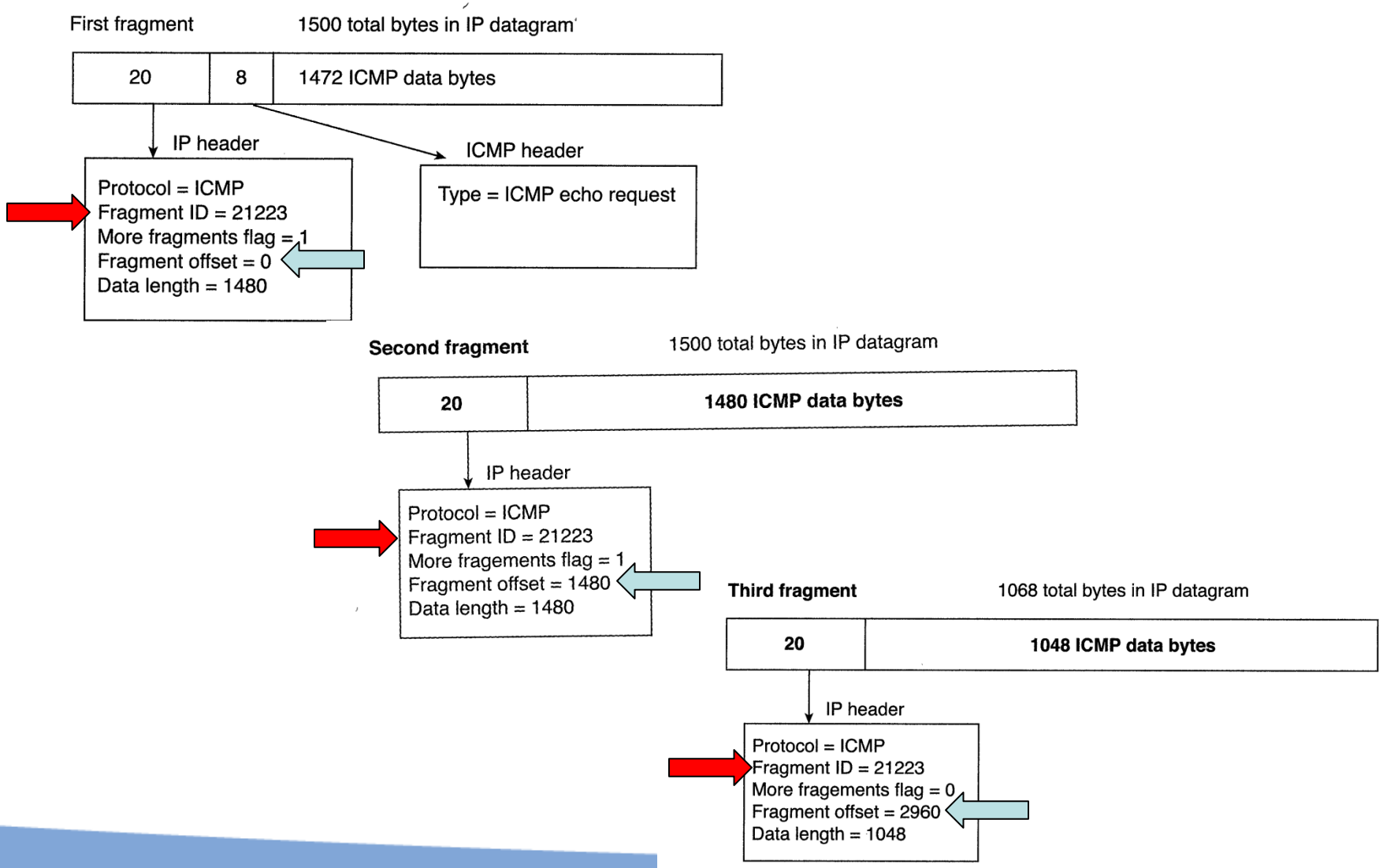
Fragmentação de Pacotes IP

- Ex.: Ping of Death (1996)
  - Envio de pacotes ICMP ECHO REQUEST com tamanho de 65535 bytes
    - Impossível reagrupar pacote tão grande
    - Corrigido com atualizações de SO
- Ataques de fragmentação não podem ser evitados com filtro de pacotes
  - Somente os primeiros pacotes possuem as informações (cabeçalhos) TCP, UDP ou ICMP

Fragmentação de Pacotes IP



Fragmentação de Pacotes IP

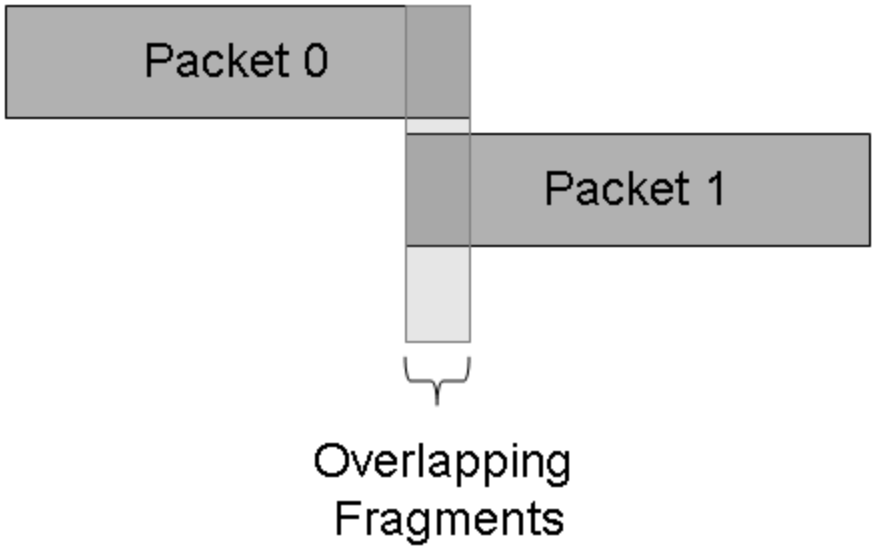


Fragmentação de Pacotes IP

- TEARDROP
  - Ferramenta utilizada para explorar problemas de fragmentação IP nas implementações TCP/IP
  - Envio de vários pacotes com fragmentos que podem causar travamento ou reinicialização do sistema alvo no ato da remontagem.
    - Pacotes fragmentados se sobrepõe quando reagrupados causando pane no sistema
  - Para evitar:
    - Manter atualizados os sistemas operacionais
    - Não permitir pacotes com fragmentos mal formados

Fragmentação de Pacotes IP

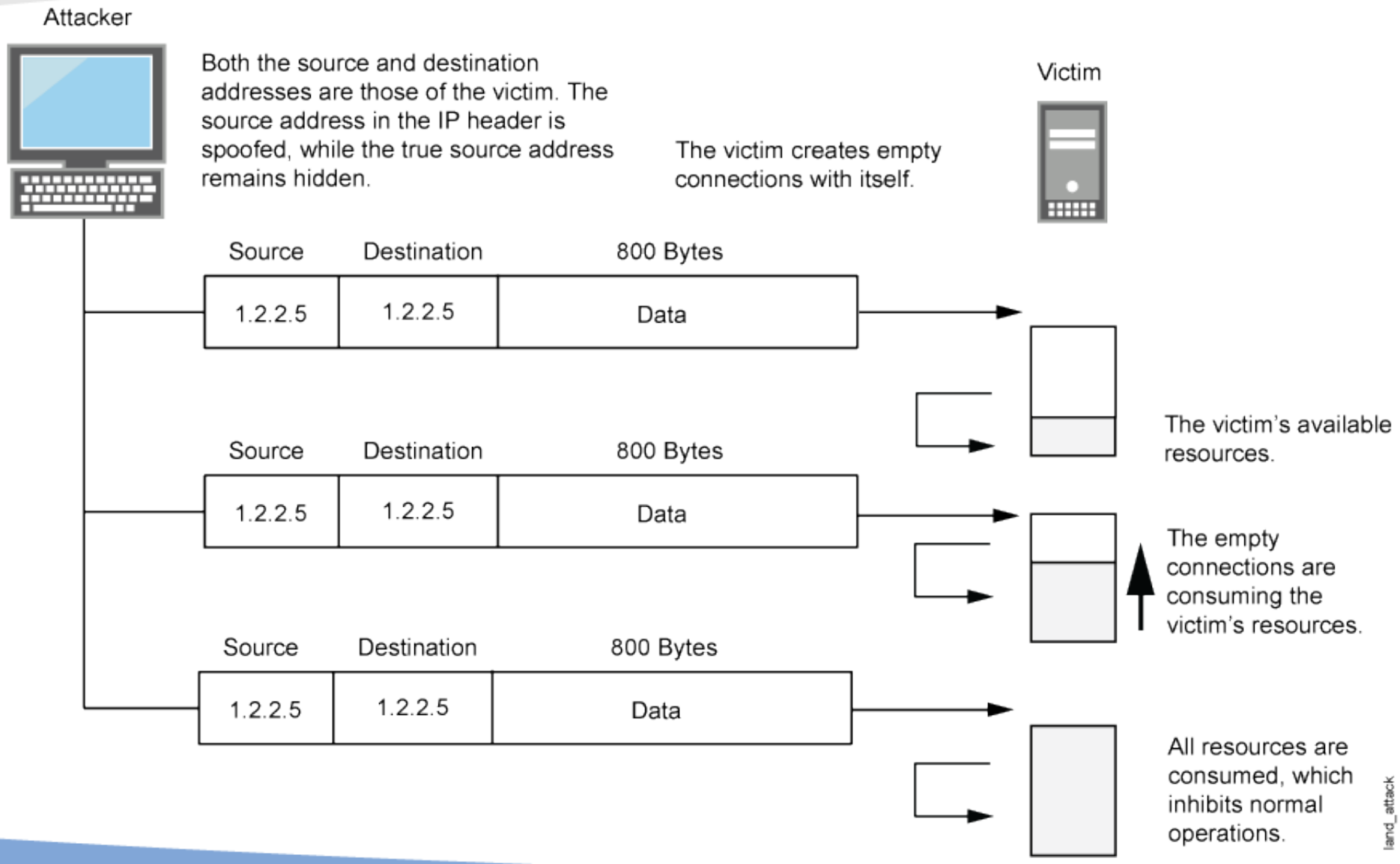
- TEARDROP



LAND Attack

- Variação do SYN Flooding
- Pode fazer com que implementações TCPIP não protegidas realizem loop de estabelecimento de conexão
- Um pacote TCP com SYN setado é montado com endereço de origem e destino sendo o IP do servidor alvo
  - IP origem = IP destino
  - Porta origem = porta destino
- Obj: travar a máquina alvo

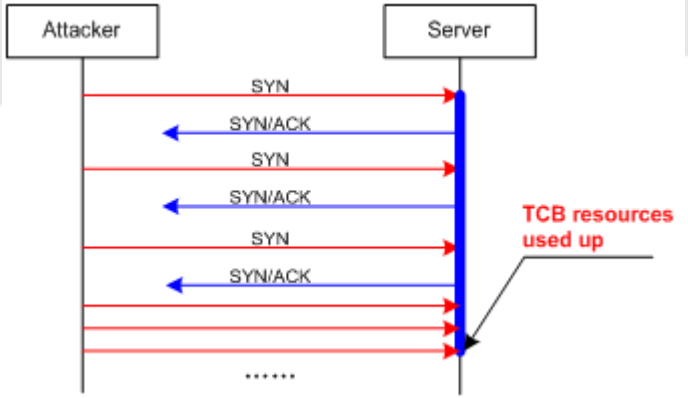
Land Attack


Attacker
Both the source and destination addresses are those of the victim. The source address in the IP header is spoofed, while the true source address remains hidden.
Victim
The victim creates empty connections with itself.
Source
Destination
800 Bytes
1.2.2.5
1.2.2.5
Data
Source
Destination
800 Bytes
1.2.2.5
1.2.2.5
Data
Source
Destination
800 Bytes
1.2.2.5
1.2.2.5
Data
The victim's available resources.
The empty connections are consuming the victim's resources.
All resources are consumed, which inhibits normal operations.
land_attack

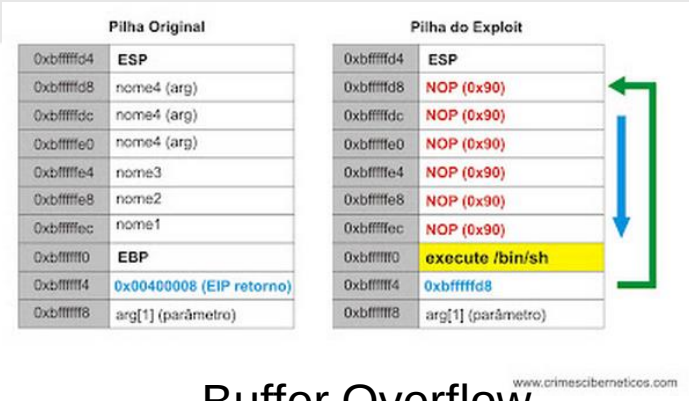
LAND Attack

- Ao receber o pacote o servidor responde para ele mesmo e estabelece uma conexão vazia.
- Cada conexão fica assim até que cancele por inatividade
- Para se proteger:
  - Patches de correção
  - Firewall configurado para não aceitar endereço de origem interno na placa de rede externa
  - Endereços devem ser filtrados:
    - Domínios: 10 , 127 , 192.168 , 172.16 a 172.31

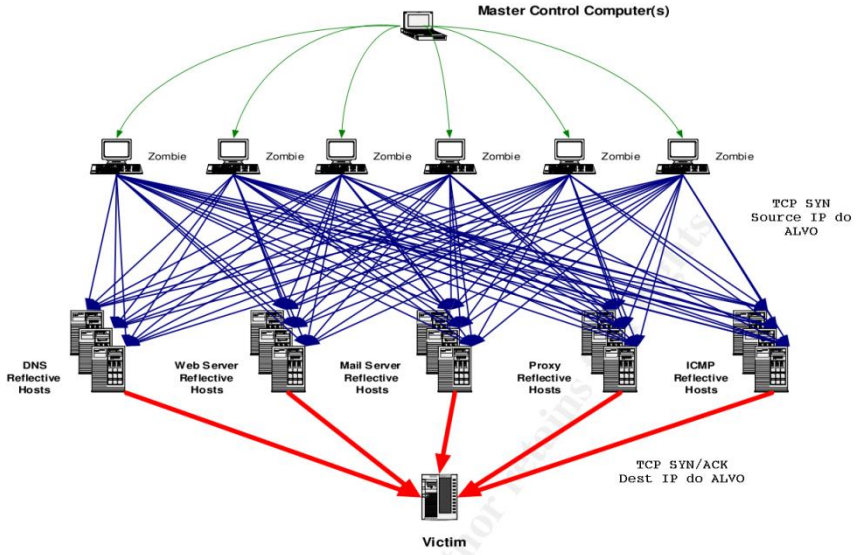
DoS - Resumo

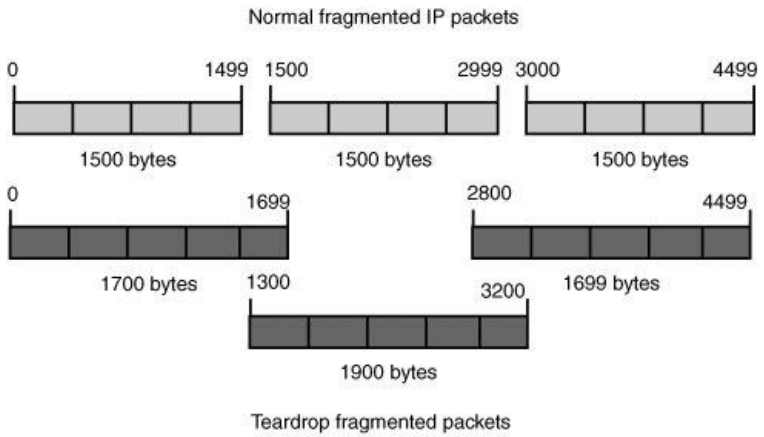


SYN Flooding



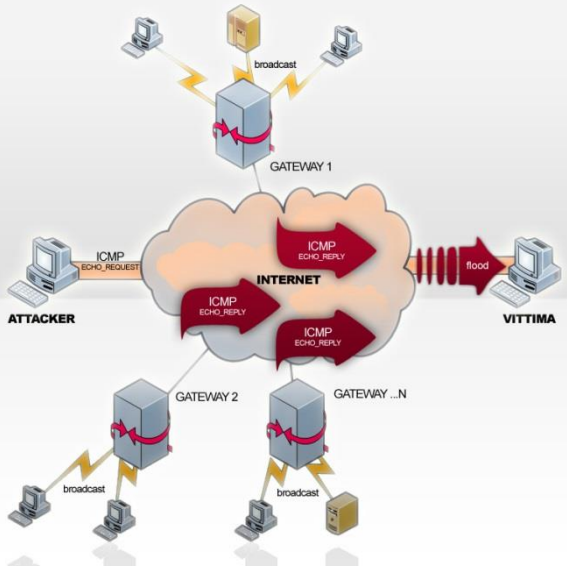
Buffer Overflow





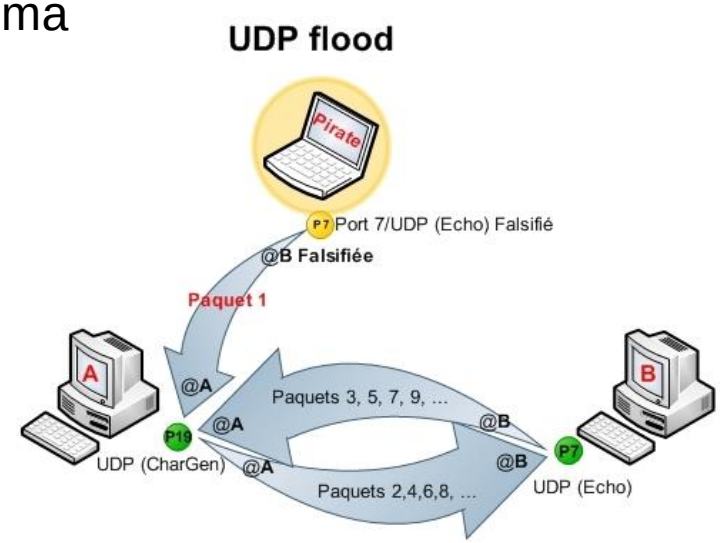
Teardrop

DRDos (SYN/ACK Attack) ⇨ Diferença para o DDoS – não há a camada de servidores reflexivos

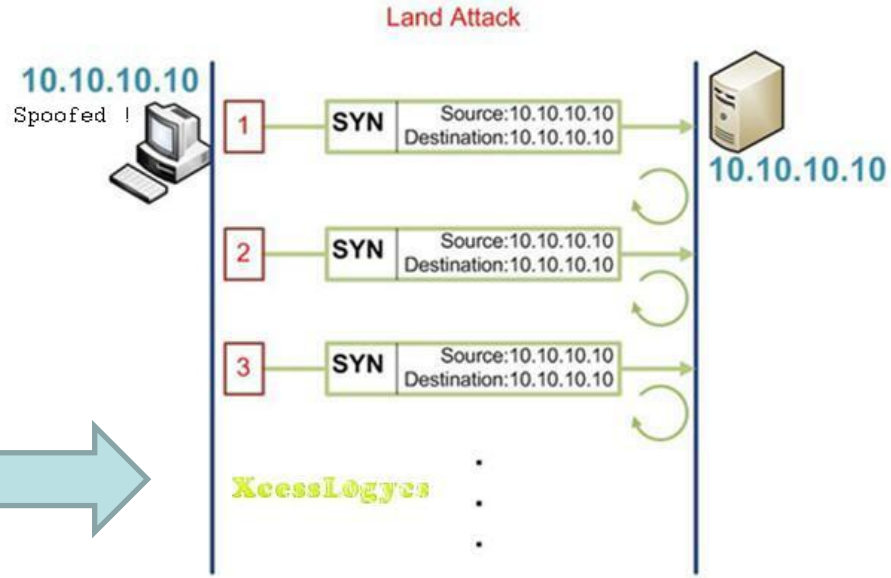


Smurf

SMURF: O atacante envia para o broadcast de redes mensagens ICMP echo com o IP de origem da vítima



FRAGGLE: O atacante envia mensagens UDP para um servidor UDP ECHO (porta 7) ou UDP CHARGEN (porta 19) com endereço de origem da vítima



LAND: O atacante envia para a vítima requisições de conexão TCP com o endereço de origem da própria vítima, provocando loop

Web Attacks

- Sql injection
  - Método que consiste em enganar as rotinas de login
  - Inserir comandos de linguagem SQL nos campos de login e senha para mapear o banco de dados
  - Pode ser adaptado para qualquer linguagem de scripting ou CGI, como PHP ou Perl
  - Ex.:

` OR 1=1--

`` or 1=1--

or 1=1--

Usuário loga como o 1º da tabela USERS ou como um usuário pré-definido. Ex.: www.VULN.com/login.php?USER=admin&pass=´OR 1=1--

`or `x´=´x

`) or (`x´=´x

Sempre verdadeiro. Vai listar todos os usuários da tabela USERS

Web Attacks

- Cross-Site Scripting (XSS)
  - Tipo de vulnerabilidade típica de aplicações web que permite injeção de código malicioso na página bypassando o controle de acesso
  - Chamado de “cross” porque é feito através de um 3º malicioso, onde o usuário clica em um link que apresenta (por exemplo) o cookie da sessão do usuário legítimo
  - Ex.: execução de códigos javascript para permitir o seqüestro de sessão (roubo de cookie)
    - http://[target]/index.php?act=´><script>alert(document.cookie)</script>

Defacements

- Alteração de páginas da internet
- Cunho pessoal ou político
- Conhecido como pichação de páginas

Defacement (Pichação)