



Cisco Self-Defending Network

Redes Capazes de Auto Defesa

Daniel Barossi Garcia

CISSP, CCSP, CCIE

Mar 2006

Estratégia de Otimização de Processos e Negócios: O Papel Da Rede

Cisco.com

EVOLUÇÃO DA ESTRATÉGIA DE REDES

CONECTIVIDADE



REDE
INTELIGENTE

➤ OTIMIZAÇÃO DOS PROCESSOS DE NEGÓCIOS
OTIMIZAÇÃO REQUER UMA REDE INTELIGENTE

POR QUE REDES INTELIGENTES?

- A Rede toca todas as partes do processo de negócios
- Aplicativos e serviços estão *individualmente* mais eficientes
- Aplicativos e serviços trabalham *em conjunto* para uma eficiência maior

O Novo Paradigma da Segurança - SDN

Cisco.com

Collaboration E-Mail Calendar Audio-Conferencing Web Application



SEGURANÇA
Self Defending Network



Voice and Messaging

Telephone Services

Instant Messaging

Contact Center

A Internet sempre foi “Terra de Ninguém”

Cisco.com



- A falta de regulamentação fez da Internet uma “terra de ninguém”
- Em 2004 vimos uma escalada no uso de programas destinados ao crime cibernético. Os ganhos financeiros são o principal motivador para esses crimes.

- Sete dos dez hackers mais ativos do mundo são brasileiros
- Brasil vira centro de crimes digitais, diz 'NY Times'
- Evitar vírus de computador 'estressa mais que divórcio'



Evolução das Ameaças

Cisco.com



O Verme Sapphire ou “Slammer”

Cisco.com

- Infeção dobrava a cada 8.5 segundos
- Infectou 75,000 hosts nos primeiros 11 minutos
- Causou parada de redes, cancelamento de voos e falhas em “Caixas Eletrônicos”

Minutos após o lançamento



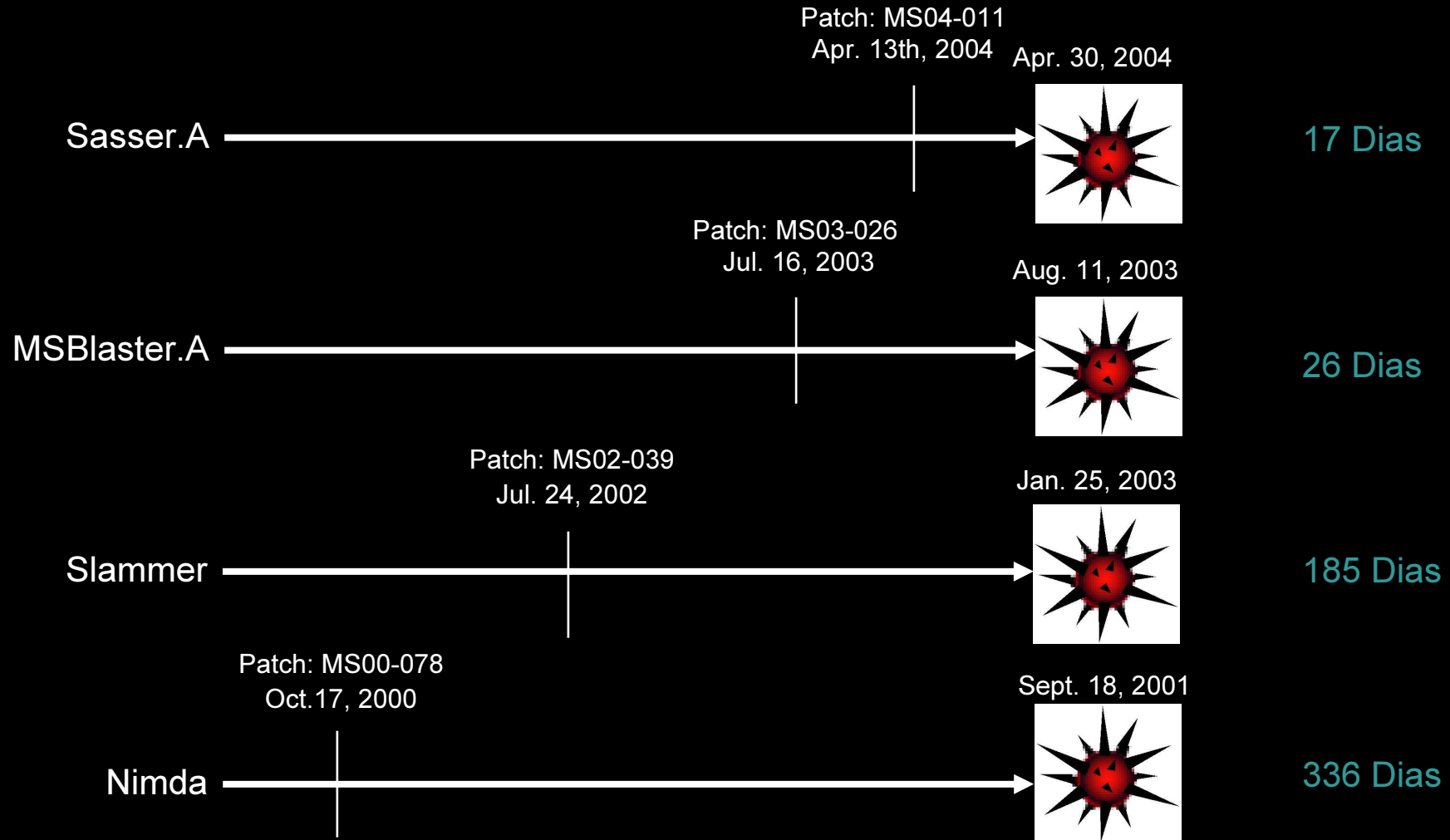
O Que Deu Errado?

Cisco.com

- **Dispositivos tradicionais de segurança NÃO conseguem evitar que vermes como o SQL Slammer executem o ataque e se espalhem**
 - Passam por firewalls permitindo tráfego**
 - Não são detectados pelos anti-virus sem uma atualização**
 - Não são detectados pela maioria dos dispositivos de IDS sem uma nova assinatura**
 - Produtos HIDS tradicionais não protegeram adequadamente os servidores sem uma atualização das assinaturas**
- **Dispositivos tradicionais de segurança NÃO conseguem evitar que vermes como o Slammer afetem a rede**
 - Produtos pontuais não evitam Denial of Service**
 - Produtos pontuais não evitam a propagação entre servidores**
 - Produtos pontuais não previnem ataques cgi-bin, buffer overflows, fragmented attacks, Unicode attacks, SQL, etc.**

Tempo entre a disponibilidade do patch e das ferramentas para explorar as vulnerabilidades diminui

Cisco.com



Como Você Quer a Sua Segurança?

Cisco.com



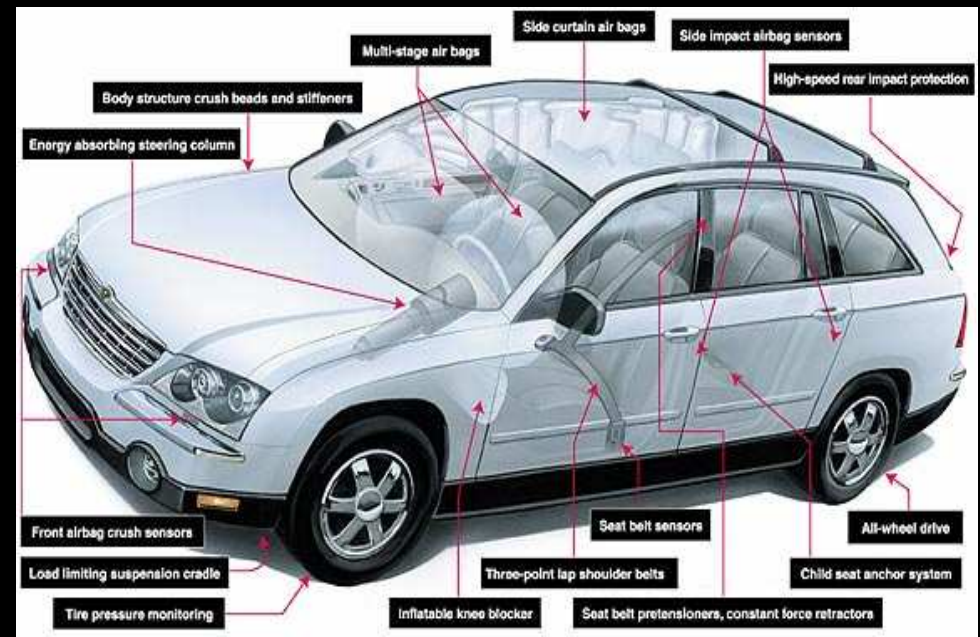
Segurança como uma opção

Segurança como um aditivo

Integração extremamente complicada

Não é economicamente viável

Não pode focar na principal prioridade



Segurança como parte do sistema

Segurança Embutia à rede

Colaboração inteligente

Segurança apropriada

Foco direto na principal prioridade

Firewall é Apenas Parte da Solução...

Cisco.com



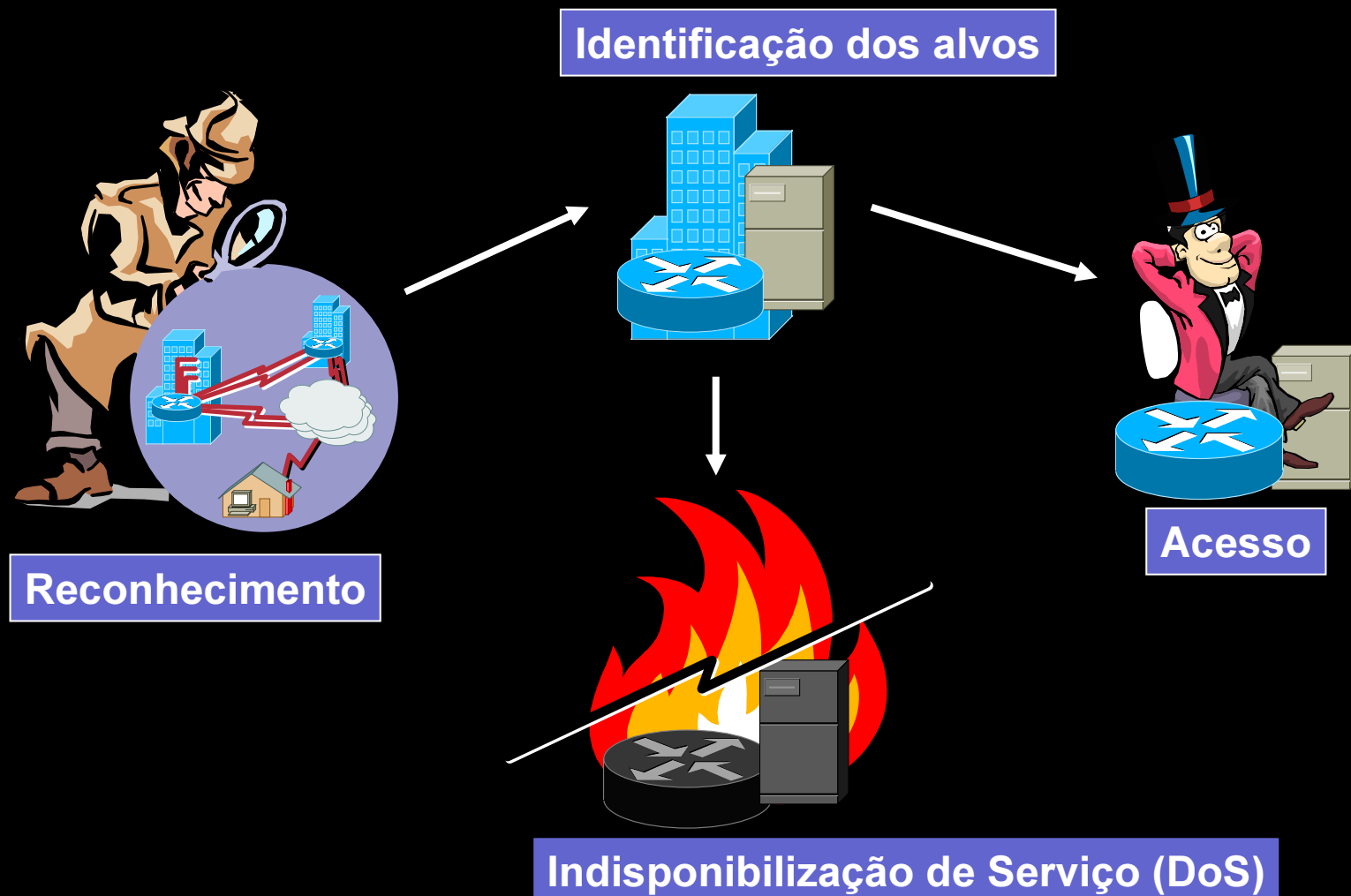
Existem Ferramentas Mais Apropriadas...

Cisco.com



Passos típicos de um ataque

Cisco.com



Exemplo de Scanner : NMAP

Cisco.com

- **Sweep options**

 - Fast and slow scans

 - Port ranges (for services)

- **Device detection (some of the tests):**

 - UDP, TCP connect, TCP SYN, ftp proxy (bounce), reverse-ident, ICMP ping sweep, FIN, ACK Sweep, Idlescan (IPID-based)

- **OS detection (some of the tests):**

 - FIN probe RESET or ignored?

 - TCP ISN sampling

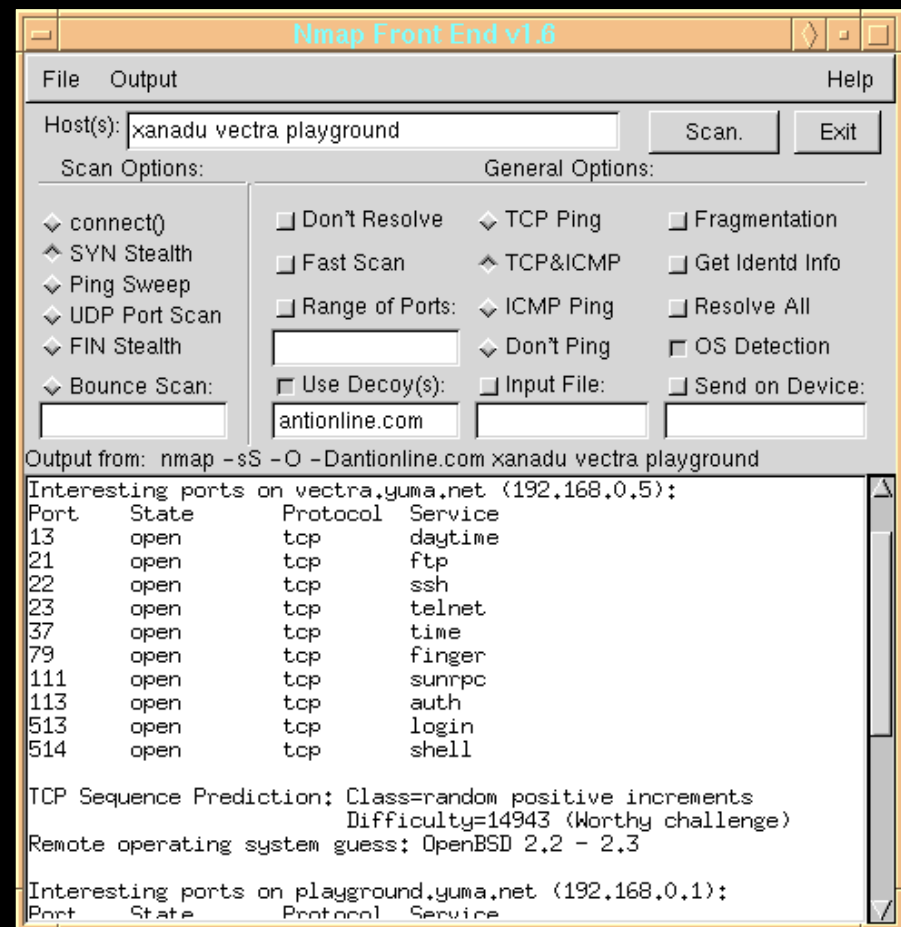
 - IPID sampling

 - Don't frag set?

 - TCP initial window

 - ICMP error messaging integrity

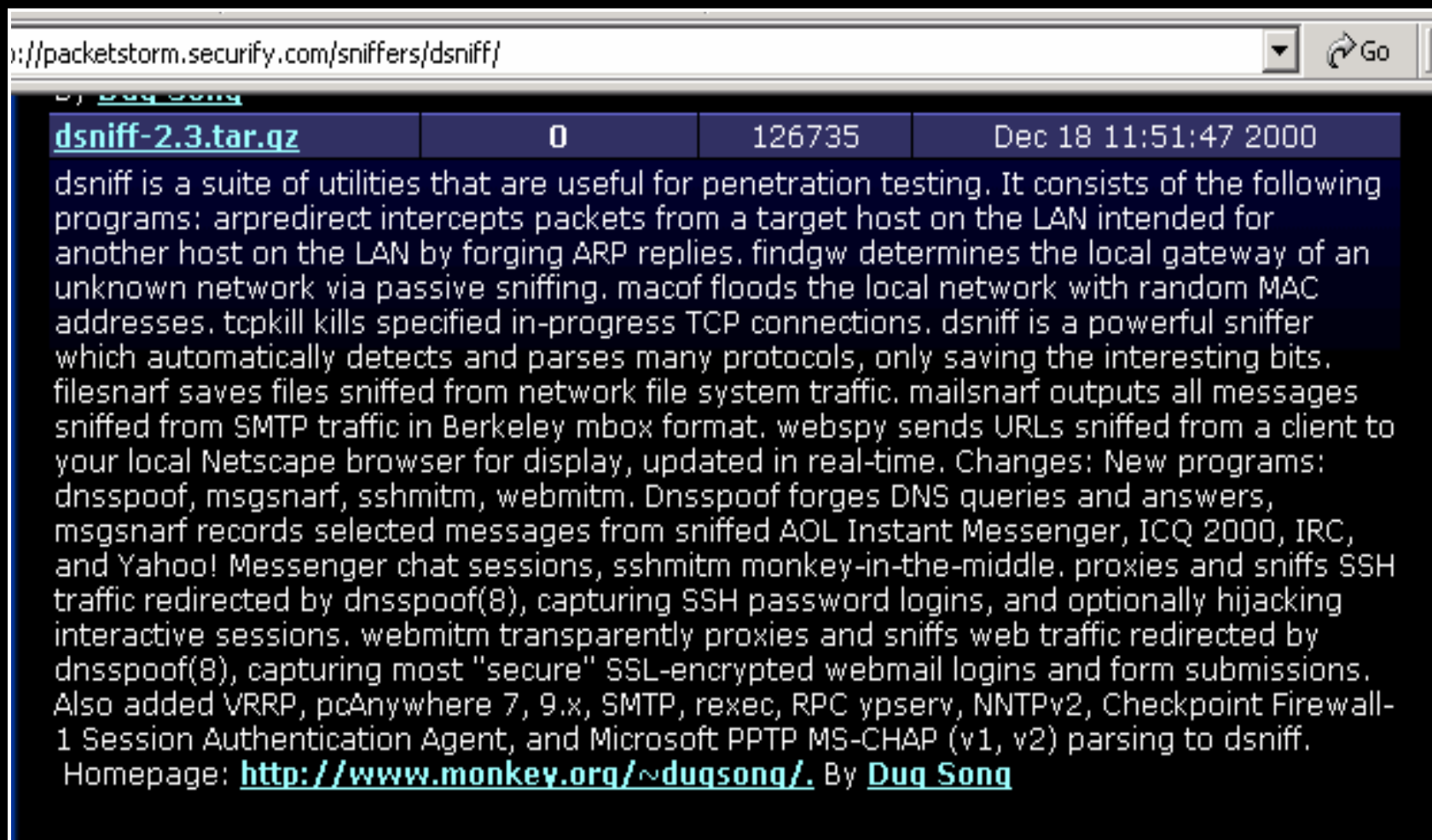
 - TCP options responses



Após o Reconhecimento: Pesquisar vulnerabilidades

Novas técnicas e ferramentas disponíveis na WEB

Cisco.com



http://packetstorm.securify.com/sniffers/dsniff/

| | | | |
|-----------------------------------|---|--------|----------------------|
| dsniff-2.3.tar.gz | 0 | 126735 | Dec 18 11:51:47 2000 |
|-----------------------------------|---|--------|----------------------|

dsniff is a suite of utilities that are useful for penetration testing. It consists of the following programs: arpredirect intercepts packets from a target host on the LAN intended for another host on the LAN by forging ARP replies. findgw determines the local gateway of an unknown network via passive sniffing. macof floods the local network with random MAC addresses. tcpkill kills specified in-progress TCP connections. dsniff is a powerful sniffer which automatically detects and parses many protocols, only saving the interesting bits. filesnarf saves files sniffed from network file system traffic. mailsnarf outputs all messages sniffed from SMTP traffic in Berkeley mbox format. webspys sends URLs sniffed from a client to your local Netscape browser for display, updated in real-time. Changes: New programs: dnsspoof, msgsnarf, sshmitm, webmitm. Dnsspoof forges DNS queries and answers, msgsnarf records selected messages from sniffed AOL Instant Messenger, ICQ 2000, IRC, and Yahoo! Messenger chat sessions, sshmitm monkey-in-the-middle. proxies and sniffs SSH traffic redirected by dnsspoof(8), capturing SSH password logins, and optionally hijacking interactive sessions. webmitm transparently proxies and sniffs web traffic redirected by dnsspoof(8), capturing most "secure" SSL-encrypted webmail logins and form submissions. Also added VRRP, pcAnywhere 7, 9.x, SMTP, rexec, RPC ypserv, NNTPv2, Checkpoint Firewall-1 Session Authentication Agent, and Microsoft PPTP MS-CHAP (v1, v2) parsing to dsniff. Homepage: <http://www.monkey.org/~duqsong/>. By [Dug Song](#)

SANS: Windows Top10 Vulnerabilities

Cisco.com

W8 LSAS Exposures

W8.1 Description

The Windows Local Security Authority Subsystem Service on Windows 2000, Server 2003 and Server 2003 64 Bit, XP and XP 64 Bit editions contains a critical buffer overflow that if exploited can lead to full system compromise. This overflow is outlined in the Microsoft Security Bulletin MS04-011. This attack can be accomplished remotely and anonymously over RPC on un-patched Windows 2000 and XP systems but requires administrative privileges to be effective.

While Windows Server 2003 and Windows XP 64 bit 2003 Edition products did contain the vulnerability, the /GS overflow protection that's was added to certain parts of the OS prevented Sasser from doing any **significant damage** or a full system compromise.

The Local Security Authority Subsystem Service (LSASS) plays an important role in system authentication and Active Directory functionality. It is here in the interface process with Active Directory that the logging function of the LSASRV.dll can be overflowed with an inordinately long string. Potentially this vulnerability can lead to full system compromise.

The gravity of the fact that this vulnerability can be easily exploited remotely is demonstrated by the recent propagation of the LSASS based Sasser and Korgo worms. Also known as W32.Sasser (<http://www.cert.org/current/archive/2004/07/12/archive.html#sasser>, <http://www.microsoft.com/security/incident/sasser.msp>) and W32.Korgo (<http://www.cert.org/current/archive/2004/07/12/archive.html#korgo>). Many recent malicious "bot" worms use this vulnerability for infection as well and their importance as a developing security issue is growing daily and often overlooked.

The vulnerability has been assigned CVE number CAN-2003-0533. It is strongly encouraged that network administrators not only patch their systems against this vulnerability but implement all necessary access controls at network ingress points to stop Windows RPC based abuses from entering vulnerable environments.

W8.2 Operating Systems Affected

Windows 2000, Windows XP and Professional, Windows XP 64-Bit Edition, Windows 2003

W8.3 CVE/CAN Entries

[CVE-1999-0227](#)

[CAN-2003-0507](#), [CAN-2003-0533](#), [CAN-2003-0663](#), [CAN-2003-0818](#)

W8.4 How to Determine if You Are Vulnerable:

This vulnerability can either be checked across the network or locally on the system itself. A network check is best-suited to security and network administrators who need to detect vulnerable machines within a network or an IP range. A localized check suits end-users who need

SANS UNIX U1: BIND (ainda o BIND...)

Cisco.com

U9 BIND/DNS

U9.1 Description

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of the Domain Name Service (DNS), the system that allows one to locate a server on the Internet (or a local network) by using its name (e.g., www.sans.org) without having to know its specific IP address. The ubiquity of BIND has made it a frequent target of attack. While BIND developers have historically been quick to repair vulnerabilities, an inordinate number of outdated or misconfigured servers remain

A number of factors contribute to the risk a vulnerable machine may provide a platform for denial of service, discussed in [Advisory CA-2002-19](#), in which specific DNS packets to force cause the BIND daemon to crash. By sending malicious execute arbitrary code or ev

In addition to the risk a vulnerable machine may provide a platform for denial of service, discussed in [Advisory CA-2002-19](#), in which specific DNS packets to force cause the BIND daemon to crash. By sending malicious execute arbitrary code or ev

Nearly all Unix and Linux systems have BIND enabled. Binary versions of BIND are available for a wide variety of operating systems.

U9.3 CVE Entries

[CVE-1999-0009](#), [CVE-1999-0024](#), [CVE-2001-0001](#), [CAN-2002-0400](#)

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

Home Site Index Search Contact FAQ
vulnerabilities, incidents & fixes security practices & evaluations survivability research & analysis training & education

CERT® Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries

Original release date: June 28, 2002
Last revised: September 9, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Applications using vulnerable implementations of the Domain Name System (DNS) resolver libraries, which include, but are not limited to

- Internet Software Consortium (ISC) Berkeley Internet Name Domain (BIND) DNS resolver library (libbind)
- Berkeley Software Distribution (BSD) DNS resolver library (libc)
- GNU DNS resolver library (glibc)

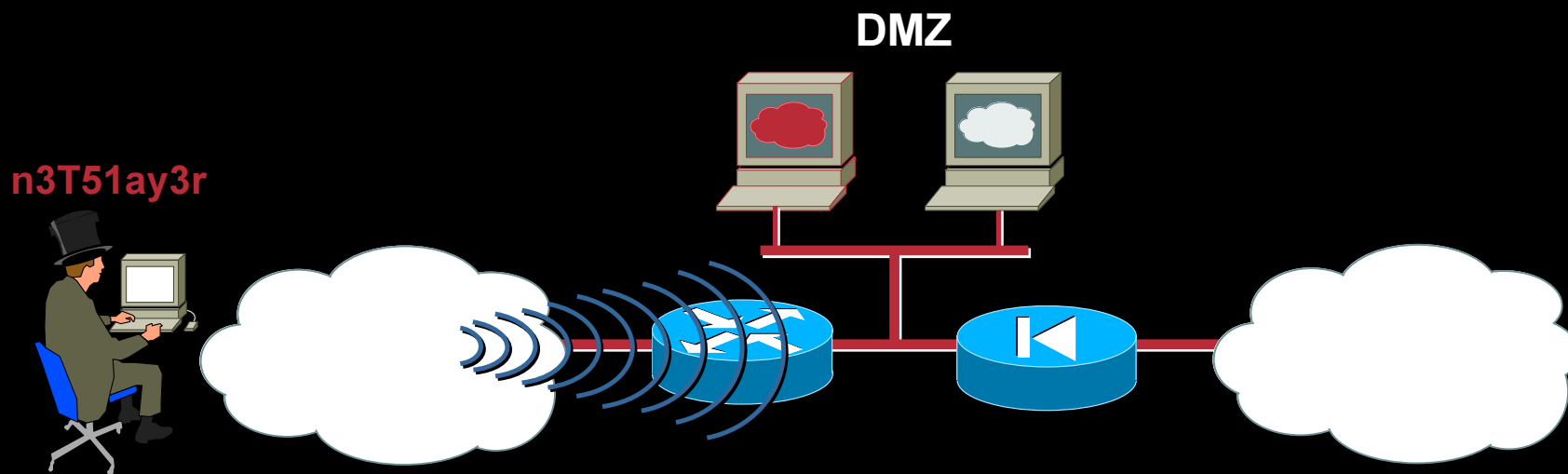
Overview

Buffer overflow vulnerabilities exist in multiple implementations of DNS resolver libraries. Operating systems and applications that utilize vulnerable DNS resolver libraries may be affected. A remote attacker who is able to send malicious DNS responses could potentially exploit these vulnerabilities to execute arbitrary code or cause a denial of service on a vulnerable system.

Options
Advisories
Vulnerability Notes Database
Incident Notes
Current Activity
Related Summaries
Tech Tips
ArCERT
Employment Opportunities
more links
CERT Statistics
Vulnerability Disclosure Policy
CERT Knowledgebase
System Administrator courses

Ao ataque !

Cisco.com



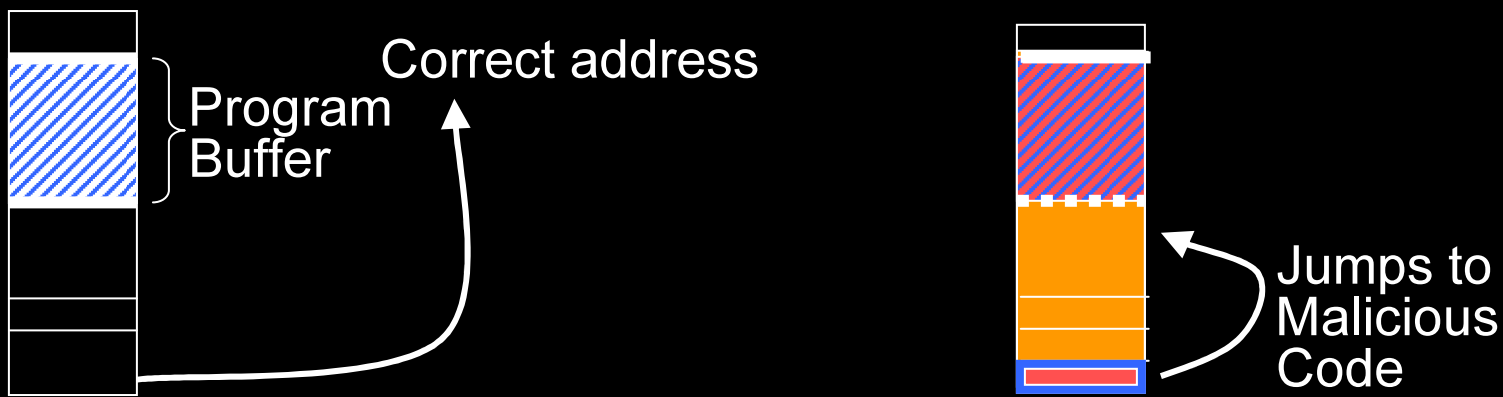
- Reconhecimento, pesquisa de vulnerabilidades...
- Versão antiga (e vulnerável) do BIND descoberta em um servidor
- Acesso “root” obtido, logs apagados e “rootkit” instalado
- (Só o começo da brincadeira...)

Um problema cada vez mais comum: Buffer Overflow

Cisco.com

Exemplo: SNMP

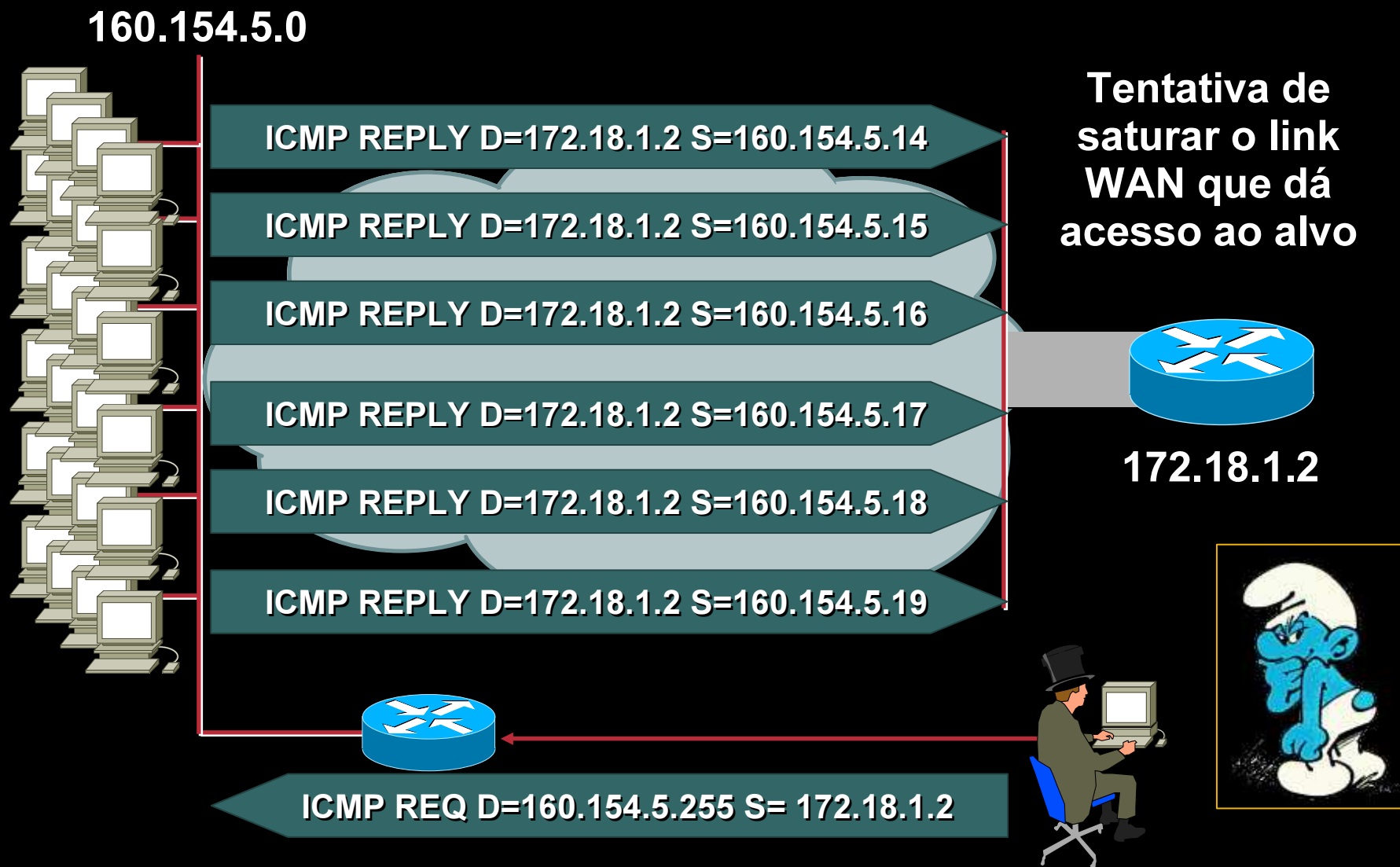
Se alguns parâmetros de pacotes em versões vulneráveis do protocolo SNMP forem muito grandes, eles poderão causar um “buffer overflow”



Bad address to jump to when the current function ends

Smurf Attack: um exemplo de “Denial of Service”

Cisco.com



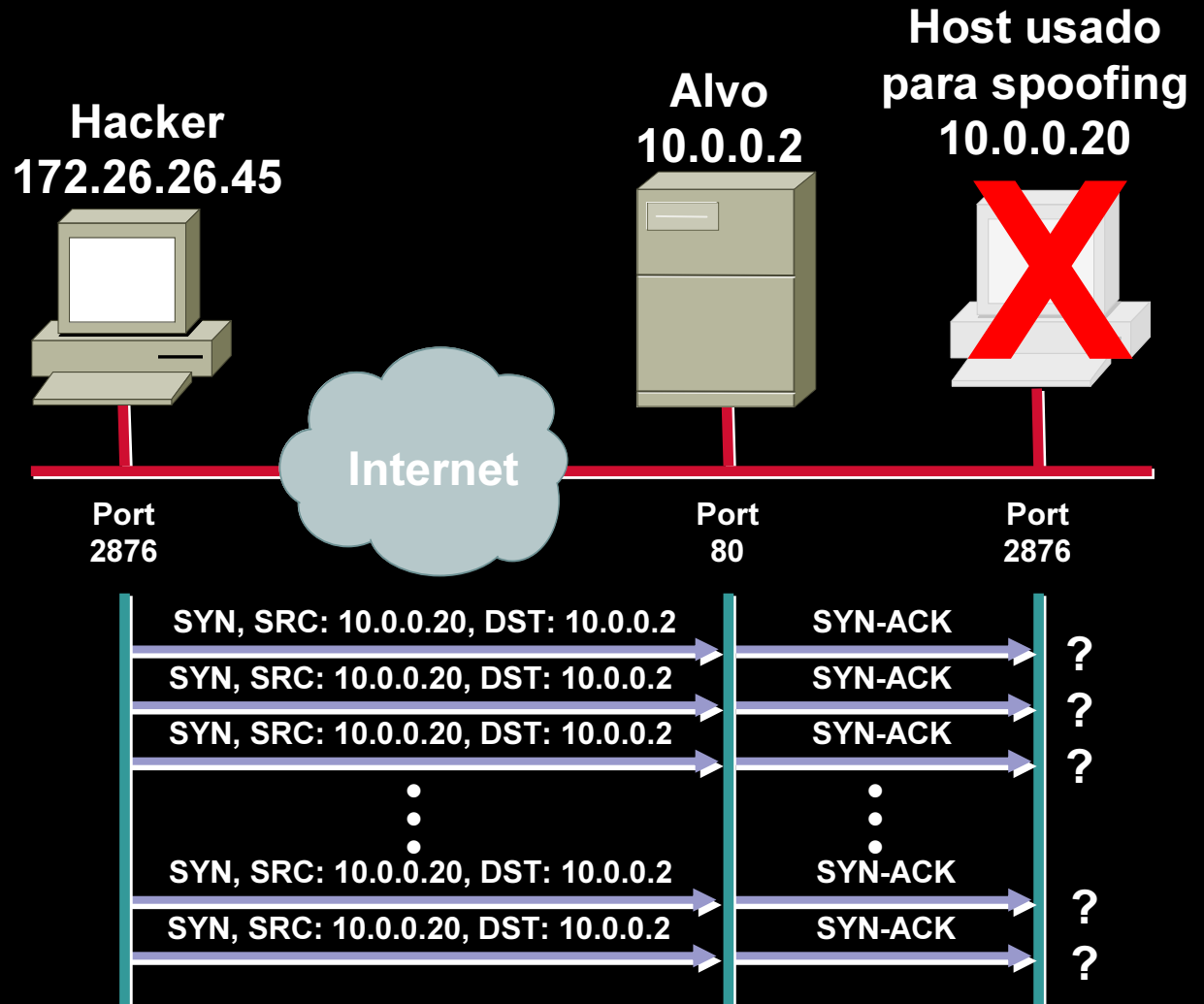
SYN Flood: mais um clássico “Denial of Service”

Cisco.com

O hacker forja o endereço IP de origem, usando um endereço não existente.

O alvo responde aos pacotes SYN enviando pacotes SYN/ACK para o suposto host (endereço forjado)

O alvo satura seus buffers com conexões TCP incompletas (pois nunca receberá resposta do host não existente) e para de responder às requisições legítimas.



Distributed Denial of Service

Cisco.com

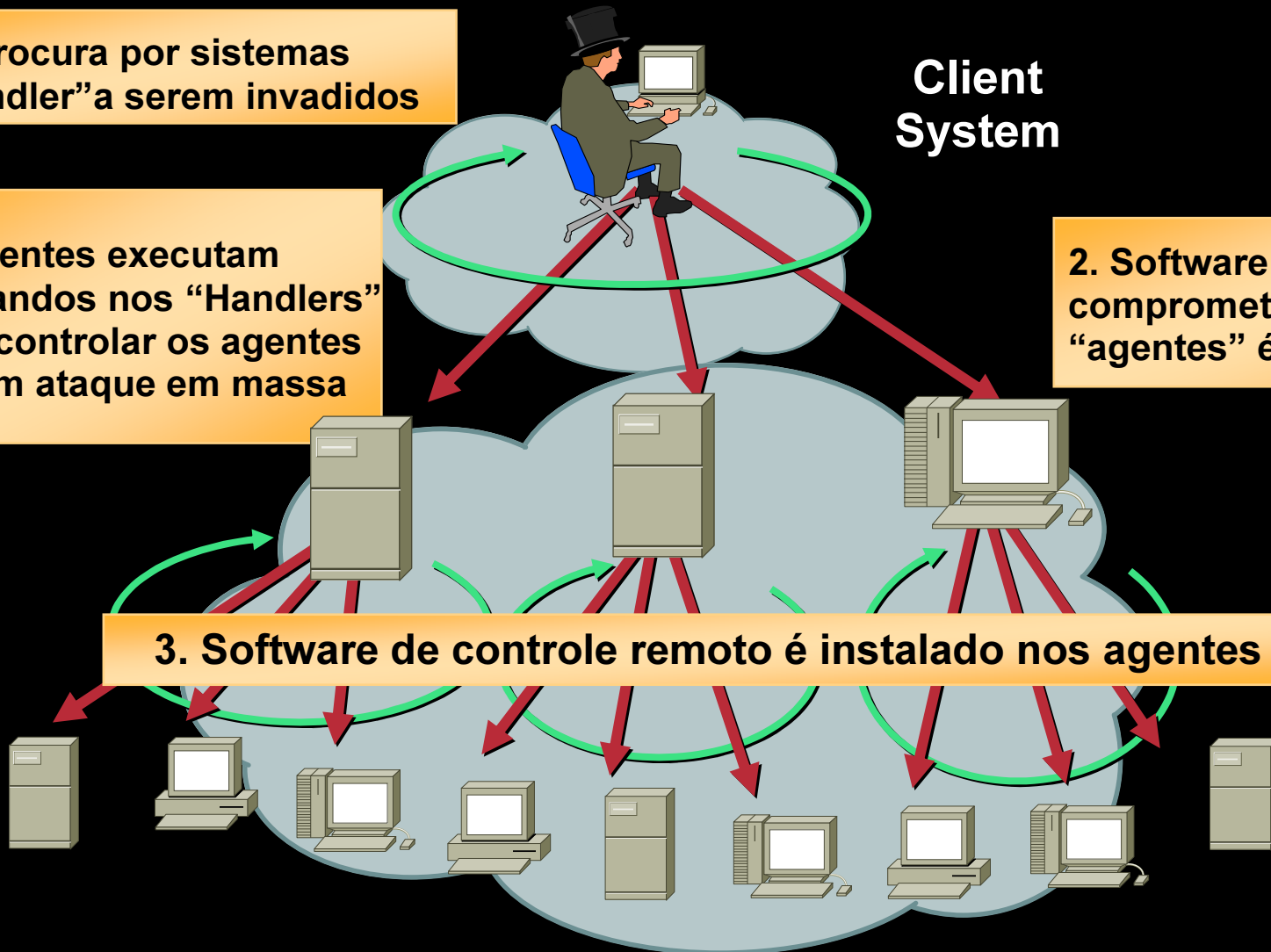
1. Procura por sistemas "handler" a serem invadidos

Client System

4. Clientes executam Comandos nos "Handlers" para controlar os agentes em um ataque em massa

2. Software para encontrar, comprometer e infectar "agentes" é instalado

3. Software de controle remoto é instalado nos agentes



War Dialers: o acesso remoto pode ser o ponto fraco

Cisco.com

Address <http://packetstorm.securify.com/wardialers/indexdl.shtml>

Archives Forums search Recent Files go

packet storm

about us
forums
assessment
defense
papers
magazines
misc
links
careers

Welcome to the War Dialers Section.

To Change Sort Order, Click On A Category.
Sorted By: Downloads.

| File Name | Downloads | File Size | Last Modified |
|---|-----------|-----------|----------------------|
| mhunter2.zip modem hunter. | 3300 | 47962 | Aug 16 17:14:20 1999 |
| bbp10src.zip BlueBeep war dialer. | 2669 | 344375 | Aug 16 17:14:20 1999 |
| phonetaq13.zip Sorry, a description is unavailable. | 2202 | | |
| tl110.zip Tone Loc | 2067 | | |
| ShokDial4-1.tgz ShokDial 4.1, an excellent war dialer for linux. Another | 2044 | | |
| phonetaq.zip Sorry, a description is unavailable. | 2042 | | |
| zhack410.zip Sorry, a description is unavailable. | 1995 | | |
| pbx_scan.zip PBX Scanner v5.0. | 1937 | | |
| toneutil.zip Tone Loc utilities. | 1923 | | |
| auto-dial.zip | 1823 | 27846 | Aug 16 17:14:19 1999 |

ToneLoc 1.10 by Minor Threat & Mucho Maas (Sep 29 1994)

ToneLoc is a dual purpose wardialer. It dials phone numbers using a mask that you give it. It can look for either dialtones or modem carriers. It is useful for finding PBX's, Loops, LD carriers, and other modems. It works well with the USRobotics series of modems, and most hayes-compatible modems.

USAGE:
ToneLoc [DataFile] /M:[Mask] /R:[Range] /X:[ExMask] /D:[ExRange] /C:[Config] /#:[Number] /S:[StartTime] /E:[EndTime] /H:[Hours] /T /K

| | | |
|-------------|--|----------------------------|
| [DataFile] | - File to store data in, may also be a mask | Required |
| [Mask] | - To use for phone numbers | Format: 555-XXXX Optional |
| [Range] | - Range of numbers to dial | Format: 5000-6999 Optional |
| [ExMask] | - Mask to exclude from scan | Format: 1XXX Optional |
| [ExRange] | - Range to exclude from scan | Format: 2500-2699 Optional |
| [Config] | - Configuration file to use | Optional |
| [Number] | - Number of dials to make | Format: 250 Optional |
| [StartTime] | - Time to begin scanning | Format: 9:30p Optional |
| [EndTime] | - Time to end scanning | Format: 6:45a Optional |
| [Hours] | - Max # of hours to scan | Format: 5:30 Optional |
| | Overrides [EndTime] | |
| /T | = Tones, /K = Carriers (Override config file, '-' inverts) | Optional |

“Drive-By Hacking”

Cisco.com

...Is Possible as It Has Been Proven by “

- Cruising with a car + laptop + WLAN card
- + GPS scanning for (unprotected) 802.11 wireless networks
- + Perl script to log the SSID, AP's MAC address, best S/N ratio and location (GPS)



www.personalteleco.net/index.cgi/WarDriving

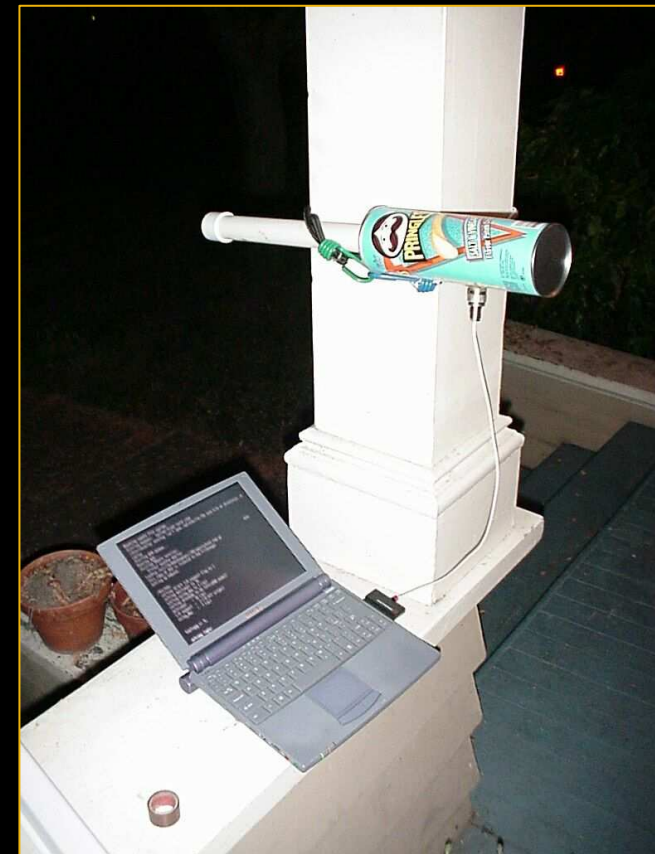
Hacking a grandes distâncias

Cisco.com

“Over a clear line of sight, with short antenna cable runs, a 12db to 12db can-to-can shot should be able to carry an 11Mbps link well over ten miles.”

Rob Flickenger, O'Reilly Systems Administrator

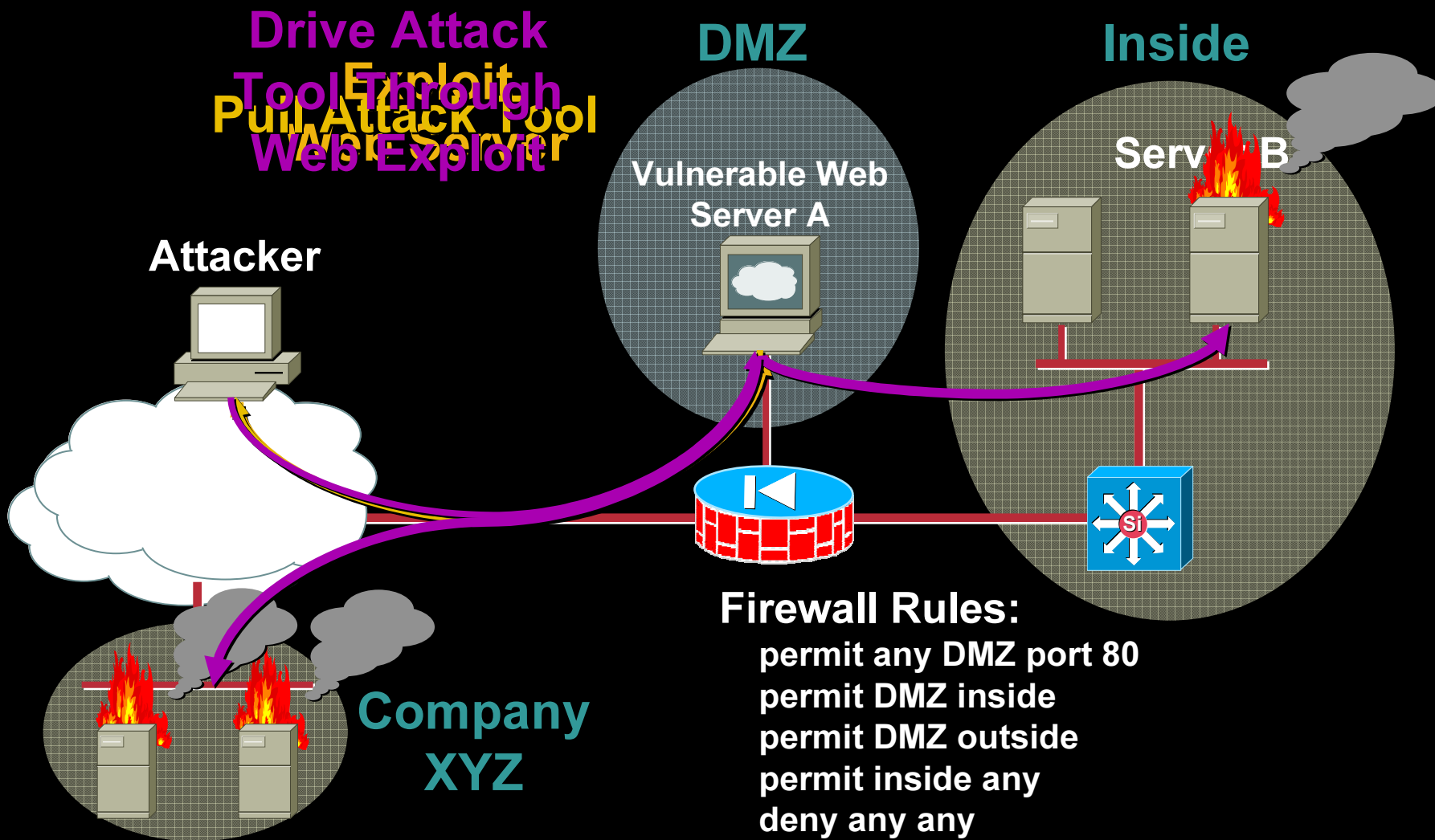
- “Pringles” YAGI Antenna
Custo: US\$10
Alcance: 10 Milhas
Já foi possível atacar alvo em lado oposto do Rio Hudson (separando New Jersey e New York)



Moral: Não confie tanto em distância!

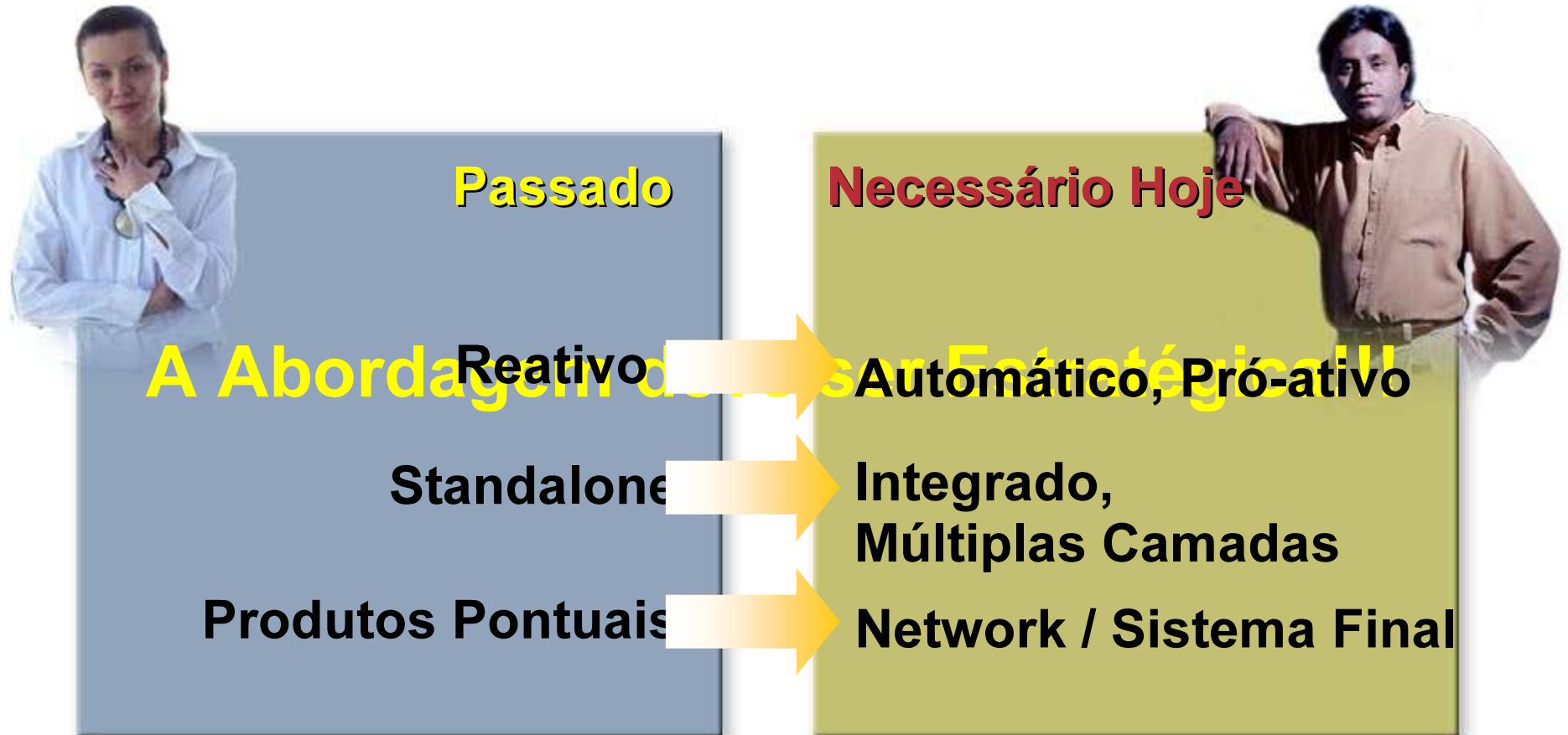
<http://www.oreillynet.com/cs/weblog/view/wlg/448>

Atacando através do Firewall



Precisamos mudar a abordagem de segurança

Cisco.com





Estratégia Self-Defending Networks

Cisco.com

SELF-DEFENDING NETWORK

Estratégia da Cisco para
aumentar drasticamente a
capacidade das redes em
**identificar, prevenir e se
adaptar** contra ameaças

**Segurança
Integrada**

**Sistema de
Segurança
Colaborativo**

**Sistema de
defesa pró-
ativo
(ATD)**

Evolução da Estratégia de Segurança Cisco

Cisco.com

SDN Fase III “Defesa Adaptável contra ameaças”

- Reconhecimento mútuo entre Serviços de Segurança & inteligência de Rede & aplicativos
- Aumenta a eficiência da Segurança, permite respostas pró-ativas.
- Consolidação de serviços, aumento da eficiência operacional
- Reconhecimento e inspeção de aplicativos para garantir a otimização dos serviços.

SDN Fase II “Sistema de Segurança Colaborativo”

- Segurança se torna um Sistema: Endpoints + Rede + Políticas
- Múltiplos serviços e dispositivos trabalhando de forma coordenada para evitar ataques. Gerenciamento ativo
- NAC, IBNS, SWAN

SDN Fase I “Segurança Integrada”

- Transforma cada elemento de rede em um ponto de defesa Roteadores, Switches, dispositivos. Endpoints
- Conectividade Segura (V3PN, DMVPN), Defesa contra ameaças, Identidade e confiabilidade
- Proteção à Rede em si

Produtos Pontuais

- Múltiplos dispositivos de Segurança
- Gerenciamento separado, não integrado

Sistema Colaborativo



Controle de Admissão é Fundamental

Cisco.com

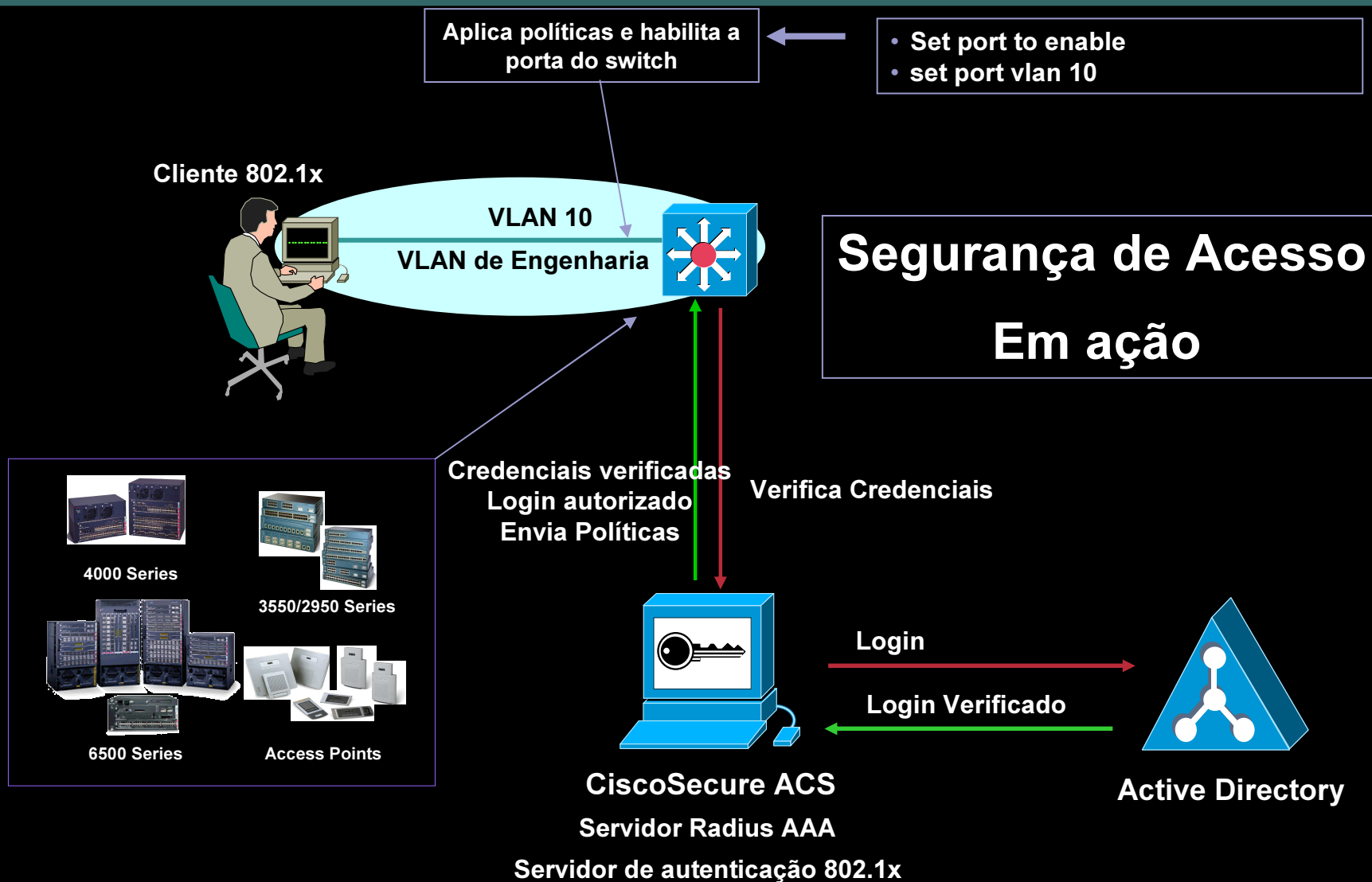
- **Muito fácil para um individuo obter acesso físico e lógico a uma Rede**
Username e password não é mais suficiente
- **Uma porta de rede pode estar habilitada ou desabilitada**
Precisamos de mais opções!
- **802.1x é parte da solução...**
- **...com Controle de Admissão à rede**
Foco em reduzir os danos causados por ameaças crescentes como os vírus e vermes



Exemplo de Self-Defending Network

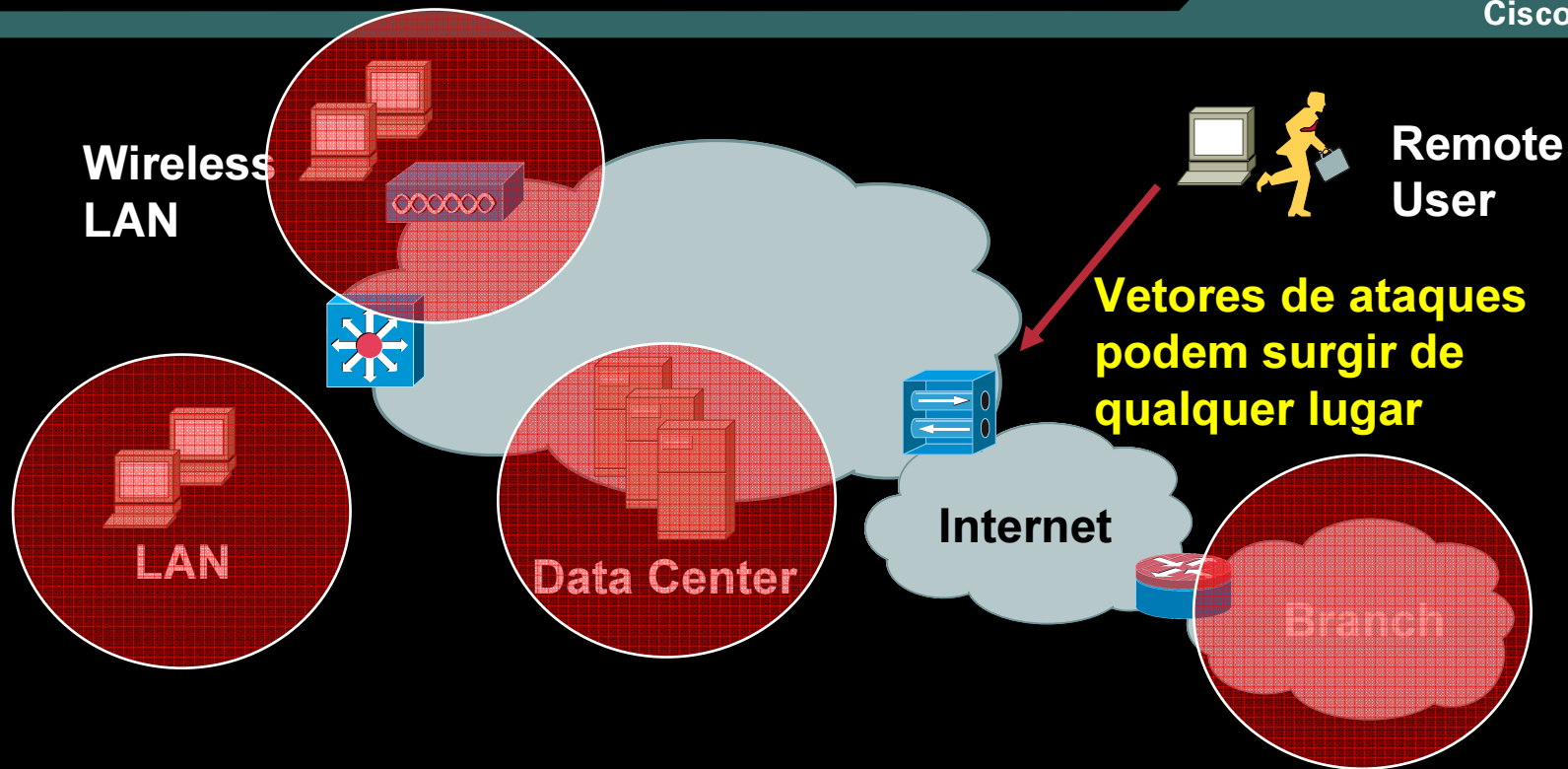
Serviços de Rede Baseado em Identidade

Cisco.com



Infecção dos Internet Worm

Cisco.com



- Os vermes se propagam e continuam a interromper os serviços, causando downtime e aplicação constante de patch
- Servidores e desktops Non-compliant são comuns
- Localizar e isolar sistemas infectados consome muito recurso e tempo
- Múltiplos tipos de usuários, métodos de acesso, e endpoints compõem um problema

Controle de Admissão na Rede Cisco: Primeira Solução de Segurança baseada em Confiança e Identidade

Cisco.com

Cliente tenta conexão

Verificação de autenticação
e políticas do cliente

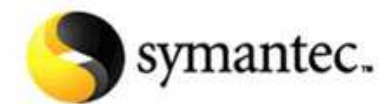


Colaboração da Indústria

Fator crítico para o sucesso

Cisco.com

Participantes do Programa Cisco Network Admission Control (NAC)



“ANYONE CAN BUILD A STOP SIGN – OR EVEN A TRAFFIC LIGHT – BUT IT TAKES A DIFFERENT MIND-SET ENTIRELY TO CONCEIVE OF A CITY-WIDE TRAFFIC CONTROL SYSTEM.”

Bruce Schneier, “Beyond Fear”

CISCO SYSTEMS

