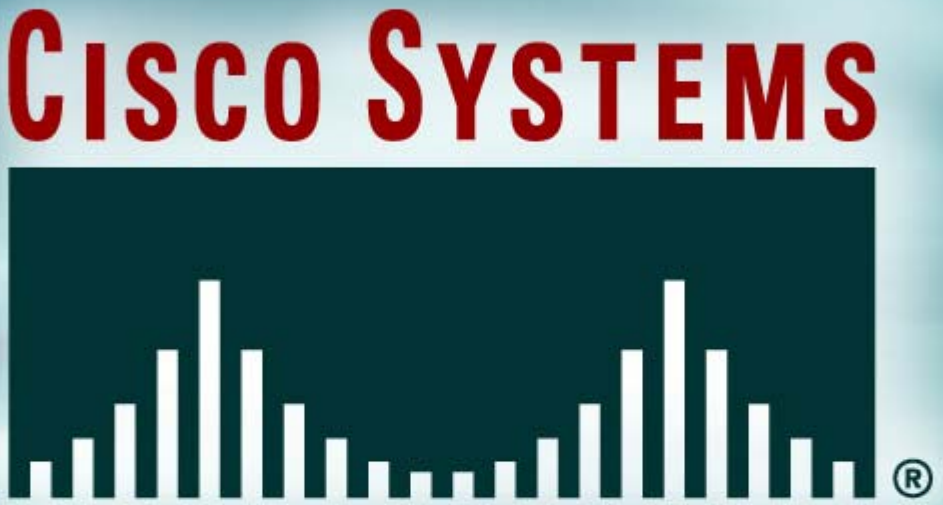


Network Security: Risk and Threat Model

Session SEC-200

Disclaimer

"This presentation provides a tit for tat description of a fictional electronic war between a determined cracker and an overworked, but well funded, IT staff.

Cisco does not recommend such reactionary security design. Rather we suggest you attend the second session in this series for a systematic approach to network security."

Agenda

- Initially weak or no security on Enterprise web presence
- Exploits mounted by disgruntled ex-employee
- Incremental steps undertaken by Enterprise to protect against more and more determined attack types……..

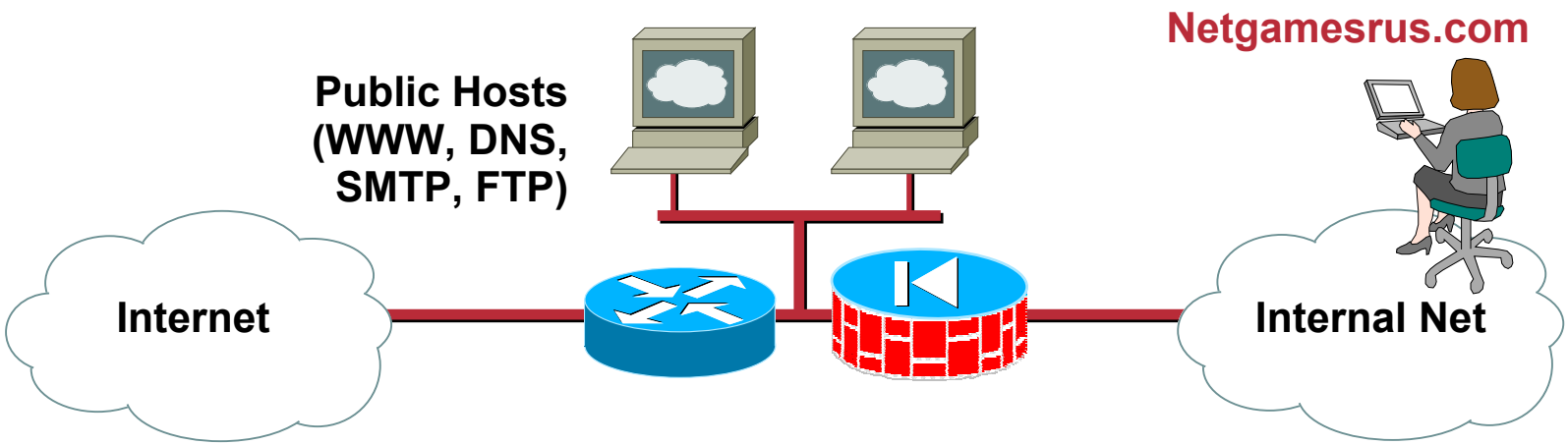
The Attacker

- **Netslayer (aka n3T51ay3r)**
  - **Disgruntled ex-employee**
  - **Seeks revenge**
  - **Unlimited time to mount exploits**

The Defenders

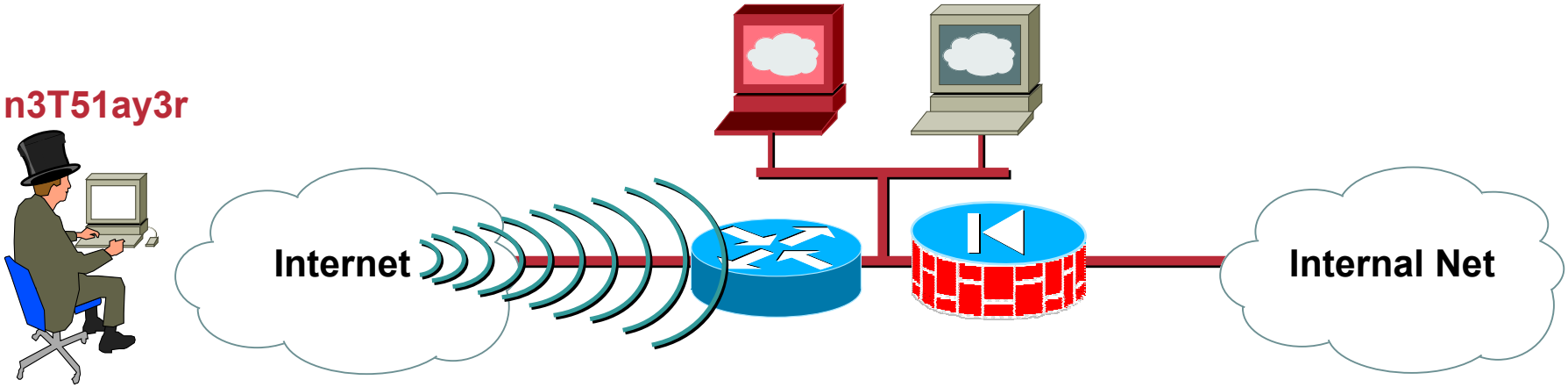
- **Netgamesrus.com**
  - **Web-based gaming company**
  - **Experienced dramatic growth, priority was connectivity over security**
  - **Lean but enthusiastic IT team**
  - **Time to market key for new web apps**

Initial Connectivity



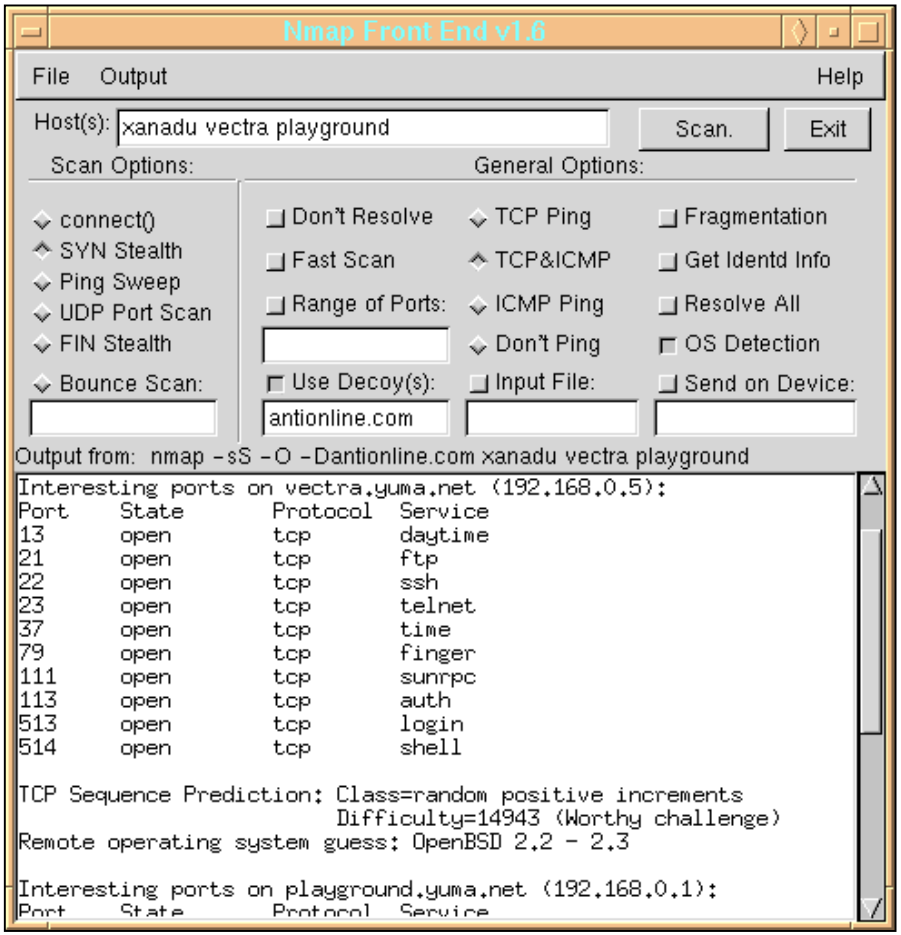
- Router only provides WAN connectivity
- FW is concerned with internal net

Easy initial exploits

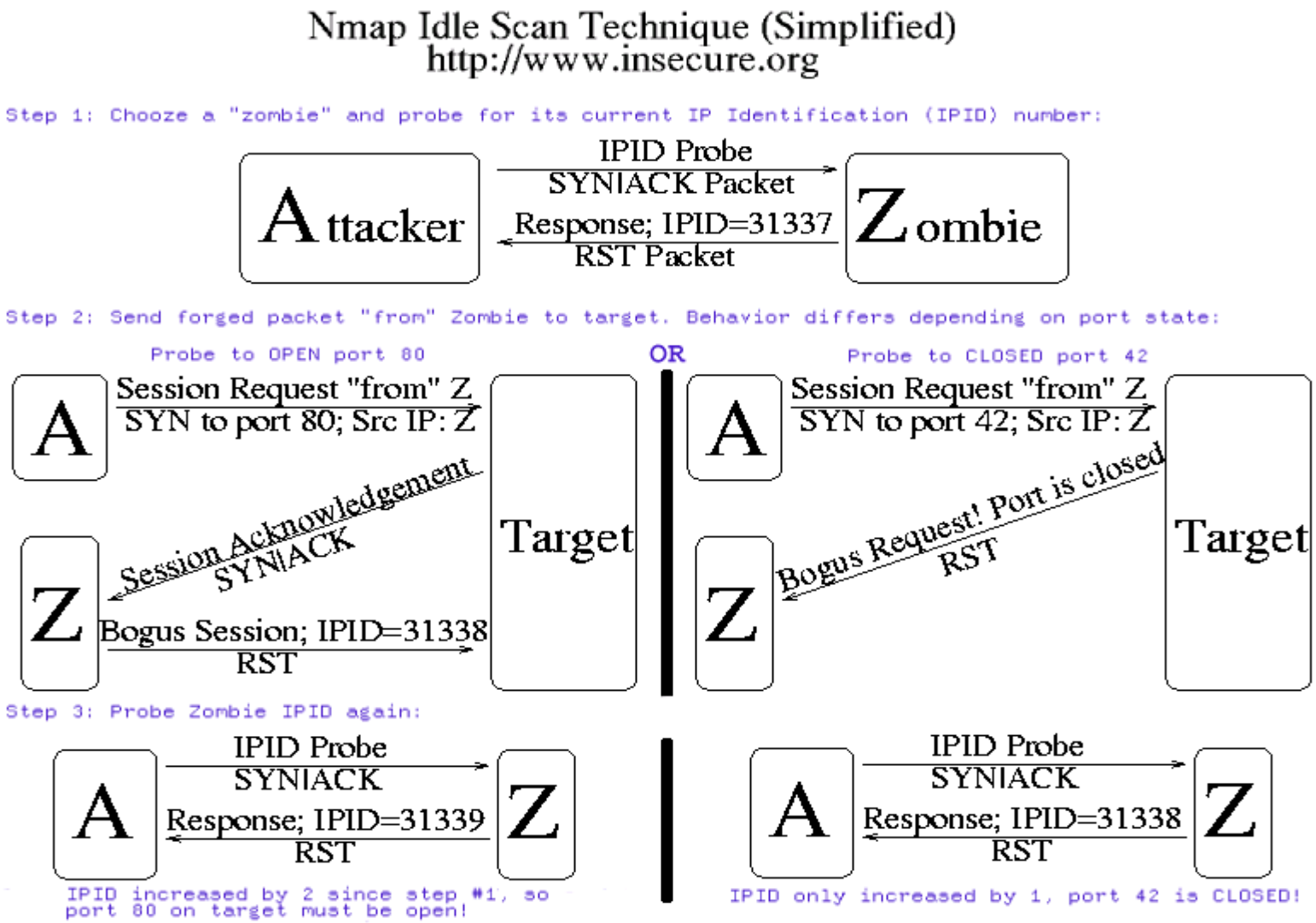


- Scan ports and vulnerabilities to find target
- Outdated bind discovered on web server
- Root privilege obtained, logs cleaned, and root kit installed

Scanning Tools



Idlescan



BIND Vulnerabilities

CERT Advisory CA-1999-14 Multiple Vulnerabilities in BIND - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: http://www.cert.org/advisories/CA-1999-14.html

Charles Schwab | Instant Message | CEC | Cisco Dashboard | Common Tools | Internal Suppt | Fiscal Year 200 | UK cinema guide | BBC Online - Sc | Bookmarks

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

Options

Advisories

Vulnerability Notes Database

Incident Notes

Current Activity

Related

Summaries

Tech Tips

AirCERT

Employment Opportunities

more links

CERT Statistics

Vulnerability Disclosure Policy

CERT Knowledgebase

System Administrator courses

CSIRT courses

Other Sources of

CERT® Advisory CA-1999-14 Multiple Vulnerabilities in BIND

Original release date: November 10, 1999
Last revised: April 25, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running various versions of BIND

I. Description

Six vulnerabilities have been found in BIND, the popular domain name server from the Internet Software Consortium (ISC). One of these vulnerabilities may allow remote intruders to gain privileged access to name servers.

Vulnerability #1: the "nxt bug"

Some versions of BIND fail to properly validate NXT records. This improper validation could allow an intruder to overflow a buffer and execute arbitrary code with the privileges of the name server.

NXT record support was introduced in BIND version 8.2. Prior versions of BIND, including 4.x, are not vulnerable to this problem. The ISC-supplied version of BIND corrected this problem in version 8.2.2.

Document: Done

Start 00:21

BIND (cont)

- CERT alerts on BIND

  Most vulnerabilities could result in named crash

  One allows buffer overflow exploit…

  …. Arbitrary code execution

  - with root privileges !

SANS UNIX #3: BIND

Cisco.com

U3 - Bind Weaknesses

U3.1 Description:

The Berkeley Internet Name Domain (BIND) package is the most widely used implementation of Domain Name Service (DNS) -- the critical means by which we all locate systems on the Internet by name (e.g., www.sans.org) without having to know specific IP addresses -- and this makes it a favorite target for attack. Sadly, according to a mid-1999 survey, as many as 50% of all DNS servers connected to the Internet are running vulnerable versions of BIND. In a typical example of a BIND attack, intruders erased the system logs and installed tools to gain administrative access. They then compiled and installed IRC utilities and network scanning tools, which they used to scan more than a dozen class-B networks in their search for additional systems running vulnerable versions of BIND. In a matter of minutes, they had used the compromised system to attack hundreds of remote systems, resulting in many additional successful compromises. This example illustrates the chaos that can result from a single vulnerability in the software for ubiquitous Internet services such as DNS. Outdated versions of Bind also include buffer overflow exploits that attackers can use to get unauthorized access.

U3.2 Systems impacted:

Multiple UNIX and Linux systems

U3.3 CVE entries:

CVE-1999-0024, CVE-1999-0184, CVE-1999-0833, CVE-1999-0009, CVE-1999-0835, CVE-1999-0848, CVE-1999-0849, CVE-1999-0851, CVE-2001-0010, CVE-2001-0011, CVE-2001-0013

U3.4 How to determine if you are vulnerable:

Run a vulnerability scanner, check the version of BIND, or manually check the files to see if they are vulnerable. If in doubt, err on the side of caution, and upgrade the system.

U3.5 How to protect against it:

The following steps should be taken to defend against the BIND vulnerabilities:

SANS#1 Vulnerability: Default Installs

Cisco.com

Top Vulnerabilities That Affect All Systems (G)

G1 - Default installs of operating systems and applications

G1.1 Description:

Most software, including operating systems and applications, comes with installation scripts or installation programs. The goal of these installation programs is to get the systems installed as quickly as possible, with the most useful functions enabled, with the least amount of work being performed by the administrator. To accomplish this goal, the scripts typically install more components than most users need. The vendor philosophy is that it is better to enable functions that are not needed, than to make the user install additional functions when they are needed. This approach, although convenient for the user, creates many of the most dangerous security vulnerabilities because users do not actively maintain and patch software components they don't use. Furthermore, many users fail to realize what is actually installed, leaving dangerous samples on a system simply because users do not know they are there.

Those unpatched services provide paths for attackers to take over computers.

For operating systems, default installations nearly always include extraneous services and corresponding open ports. Attackers break into systems via these ports. In most cases the fewer ports you have open, the fewer avenues an attacker can use to compromise your network. For applications, default installations usually include unneeded sample programs or scripts. One of the most serious vulnerabilities with web servers is sample scripts; attackers use these scripts to compromise the system or gain information about it. In most cases, the system administrator whose system is compromised did not realize that the sample scripts were installed. Sample scripts are a problem because they usually do not go through the same quality control process as other software. In fact they are shockingly poorly written in many cases. Error checking is often forgotten and the sample scripts offer a fertile ground for buffer overflow attacks.

G1.2 Systems impacted:

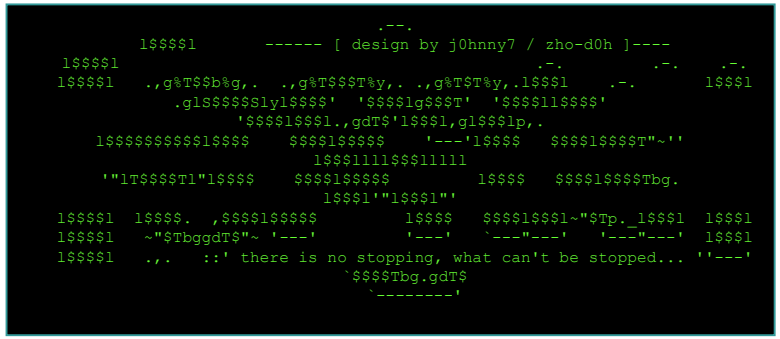
Most operating systems and applications. Keep in mind that almost all third-party web server extensions come with sample files, many of which are extremely dangerous.

G1.3 CVE entries:

(Note: This list is not complete or all-inclusive. It is a sample of some of the vulnerabilities covered by this

Root Kit installed —t0rnkit

- Been around for about 2 years and has spawned many variations and updates;
- Some Standard t0rnkit operations:
  1. Kill syslogd
  2. Store intruder password for trojan horse programs in /etc/ttyhash
  3. Install a trojanized version of sshd configured to listen on an intruder-supplied port number
  4. Hides rootkit file names, process names, etc.
  5. Replace the following system binaries with trojanized copies: /bin/login, /sbin/ifconfig, /bin/ps, /usr/bin/du, /bin/ls, /bin/netstat, /usr/sbin/in.fingerd, /usr/bin/find, /usr/bin/top
  6. Installing a password sniffer, sniffer logfile parser, and system logfile cleaning tool
  7. Attempts to enable telnet, shell, and finger in /etc/inetd.conf by removing any leading '#' comment characters
  8. Restarting /usr/sbin/inetd
  9. Starting syslogd

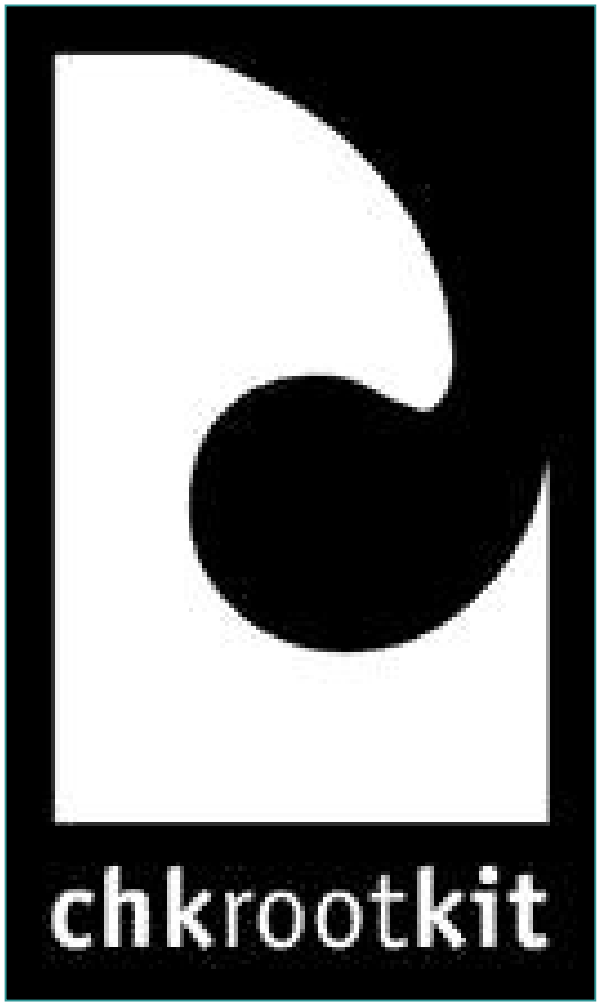


Can Be Propagated by Worms!
Lion Worm in 2001

http://www.cert.org/incident_notes/IN-2000-10.html

Root Kit Detection

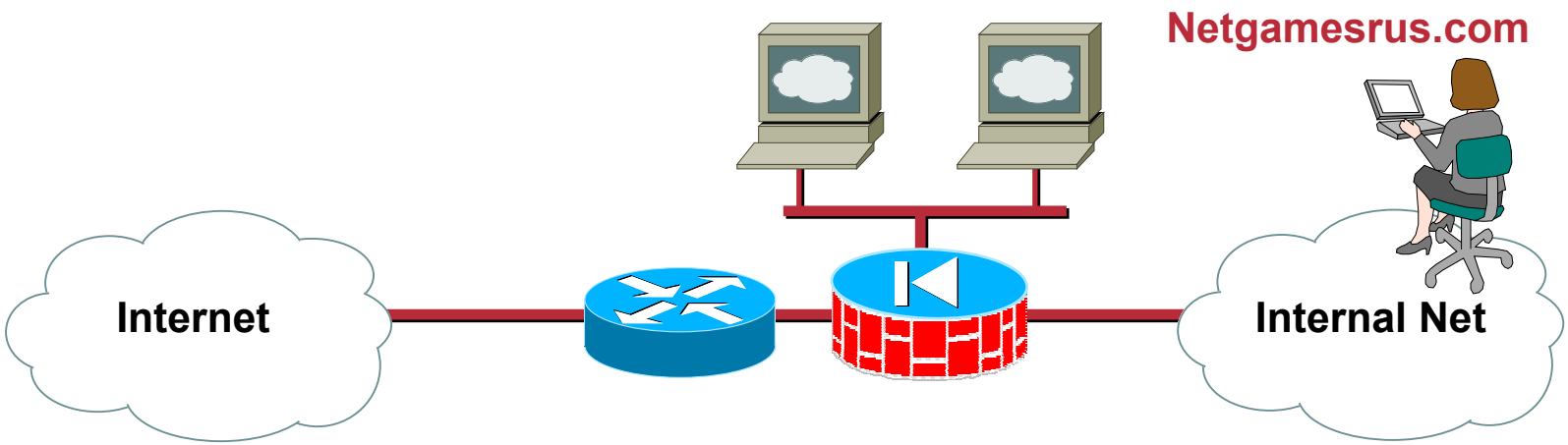
Detects: lrk3, lrk4, lrk5, lrk6 (and some variants); Solaris rootkit; FreeBSD rootkit; t0rn (including some variants and t0rn v8); Ambient's Rootkit for Linux (ARK); Ramen Worm; rh[67]-shaper; RSHA; Romanian rootkit; RK17; Lion Worm; Adore Worm; LPD Worm; kenny-rk; Adore LKM;
ShitC Worm; Omega Worm; Wormkit Worm; Maniac-RK; dsc-rootkit; Ducoci rootkit; x.c Worm;
RST.b trojan; duarawkz; knark LKM; Monkit; Hidrootkit; Bobkit; Pizdakit.



http://www.chkrootkit.org

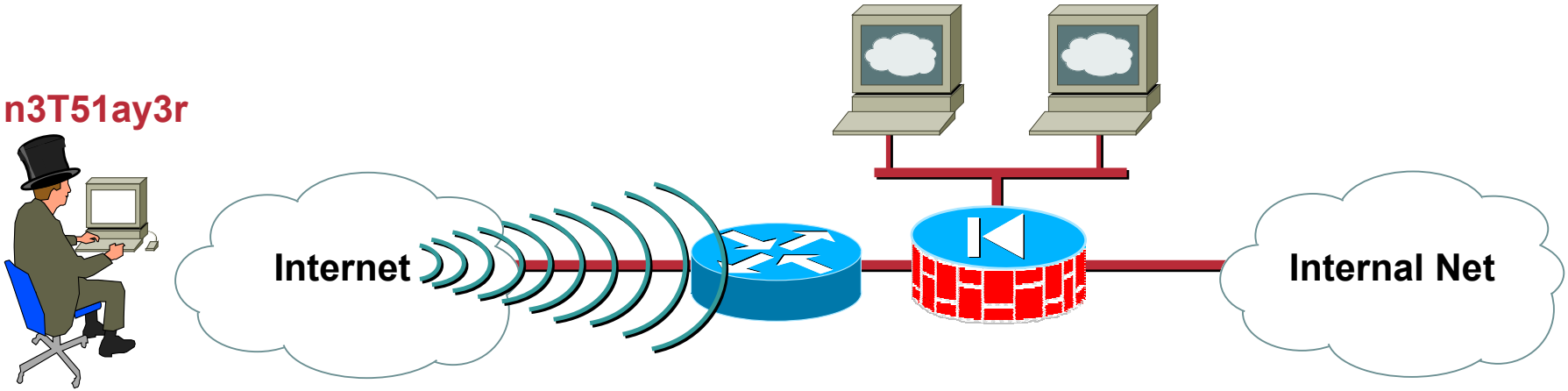
http://rr.sans.org/malicious/chkrootkit.php

Fixes applied



- A player with scanning software happens to find your host is compromised and tattles
- Rebuild (due to rootkit) and patch hosts
- Turn off unwanted services
- Move public services to third interface of firewall for service isolation

What does this mean to Netslayer



- **Games services still online**
- **Rescan**
  - **There are less services available**
  - **Services are patched**
- **Wait for “new” vulnerability posting on net …**

It's Only a Matter of Time

Cisco.com

Sign In | My Account | About Us | Advertise | Contact

SecurityFocus ONLINE — ARIS analyzer (Attack Registry & Intelligence Service) — Manage Incidents

Home | SFOnline | The Basics | Microsoft | Unix | IDS | Incidents | Virus

Bugtraq | Mailing Lists | Library

VULNERABILITIES

by vendor | by title | by keyword | by bugtraq id | by cve id

Vendor: OpenBSD
Title: Select One
Version: Any

- 2002-03-18: BSD TCP/IP Broadcast Connection Check Vulnerability

Vendor: Microsoft
Title: Select One
Version: Any

- 2002-03-19: Multiple Vendor Java Virtual Machine Bytecode Verifier Vulnerability
- 2002-03-19: Microsoft MSN Messenger Message Spoofing Vulnerability
- 2002-03-13: Microsoft Windows 2000 / NT 4.0 Process Handle Local Privilege Elevation Vulnerability
- 2002-03-08: Microsoft Windows 2000 Password Policy Bypass Vulnerability
- 2002-03-07: Microsoft Windows User Shell Buffer Overflow Vulnerability
- 2002-03-06: Microsoft Windows NT Security Policy Bypass Vulnerability
- 2002-03-05: Microsoft SQL Server Multiple Extended Stored Procedure Buffer Overflow Vulnerabilities
- 2002-03-05: Microsoft IIS Authentication Method Disclosure Vulnerability
- 2002-03-04: Multiple Vendor Java Virtual Machine Session Hijacking Vulnerability
- 2002-02-27: Multiple Vendor MacOS Browser Arbitrary Program Download Vulnerability
- 2002-02-27: Microsoft SMTP Service Malformed Command Denial of Service Vulnerability
- 2002-02-27: Microsoft Windows SMTP Service Authorization Bypass Vulnerability
- 2002-02-21: Microsoft Commerce Server 2000 ISAPI Buffer Overflow Vulnerability
- 2002-02-21: Microsoft VBScript Same Origin Policy Violation Vulnerability
- 2002-02-19: Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability
- 2002-02-19: Microsoft SQL Server OLE DB Provider Name Buffer Overflow Vulnerability
- 2002-02-14: Microsoft Visual C++ 7/Visual C++.Net Buffer Overflow Protection Weakness
- 2002-02-13: Outlook Express Attachment Carriage Return/Linefeed Encapsulation Filtering Bypass Vulnerability
- 2002-02-12: Microsoft IIS 5.1 Frontpage Server Extensions File Source Disclosure Vulnerability
- 2002-02-12: Multiple Vendor SNMP Trap Handling Vulnerabilities
- 2002-02-12:
- 2002-02-11:
- 2002-02-11:
- 2002-02-11:
- 2002-02-11:
- 2002-02-11:
- 2002-02-11:
- 2002-02-07:
- 2002-02-07:

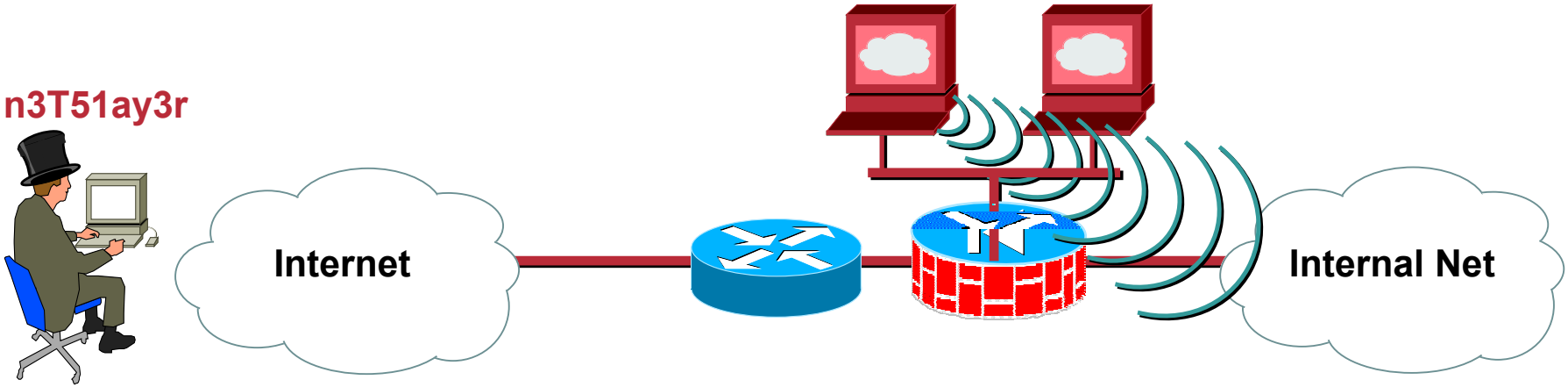
Vendor: Cisco
Title: Select One
Version: Any

- 2002-02-27: Cisco IOS Cisco Express Forwarding Session Information Leakage Vulnerability
- 2002-02-12: Cisco IOS Malformed SNMP Message Denial of Service Vulnerabilities
- 2002-02-07: Cisco Secure ACS NDS Expired/Disabled User Authentication Vulnerability
- 2002-01-31: Cisco Tac_Plus Accounting Directive Insecure File Creation Vulnerability
- 2002-01-16: Cisco Media Gateway Controller Solaris Vulnerability Exposure Vulnerability
- 2002-01-09: Cisco SN 5420 Storage Router Information Disclosure Vulnerability
- 2002-01-09: Cisco SN 5420 Storage Router Fragmented Packet DoS Vulnerability
- 2002-01-09: Cisco SN 5420 Storage Router Large Header DoS Vulnerability
- 2001-12-31: Cisco Cable Access Router MIB Community Default Passwords Vulnerability
- 2001-11-28: Cisco Context Based Access Control Protocol Check Bypassing Vulnerability
- 2001-11-15: Cisco Local Interface ARP Denial of Service Vulnerability
- 2001-11-14: Cisco 12000 Series Internet Router Denial Of Service Vulnerability
- 2001-11-14: Cisco Access Control List Fragment Non-blocking Vulnerability
- 2001-11-14: Cisco 12000 Series Internet Router ACL Failure To Drop Packets Vulnerability
- 2001-11-14: Cisco Outbound Access Control List Bypass Vulnerability
- 2001-11-14: Cisco 12000 Outgoing ACL Fragmented Packet Vulnerability
- 2001-11-14: Cisco Fragment Keyword Outgoing Access Control Vulnerability
- 2001-11-14: Cisco 12000 Series Turbo ACL Fragment Bypass Vulnerability
- 2001-11-14: Cisco Access Control List Fragment Keyword Ignored Vulnerability
- 2001-10-10: Cisco PIX Firewall Manager Plaintext Password Vulnerability
- 2001-10-09: Cisco Discovery Protocol Neighbor Announcment Denial of Service Vulnerability
- 2001-09-26: Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability Re-Introduction
- 2001-09-12: RSA BSAFE SSL-J Authentication Bypass Vulnerability
- 2001-09-05: Multiple IDS Vendor Encoded IIS Attack Detection Evasion Vulnerability
- 2001-08-23: Cisco CBOS Multiple TCP Connection Denial of Service Vulnerability
- 2001-08-01: Cisco SN Storage Router Developer Shell Unauthorized Access Vulnerability
- 2001-07-25: Cisco IOS UDP Denial of Service Vulnerability
- 2001-07-18: Multiple Vendor Telnetd Buffer Overflow Vulnerability
- 2001-07-12: Cisco IOS Malformed PPTP Packet Denial of Service Vulnerability

Vendor: Apache Group
Title: Apache
Version: Any

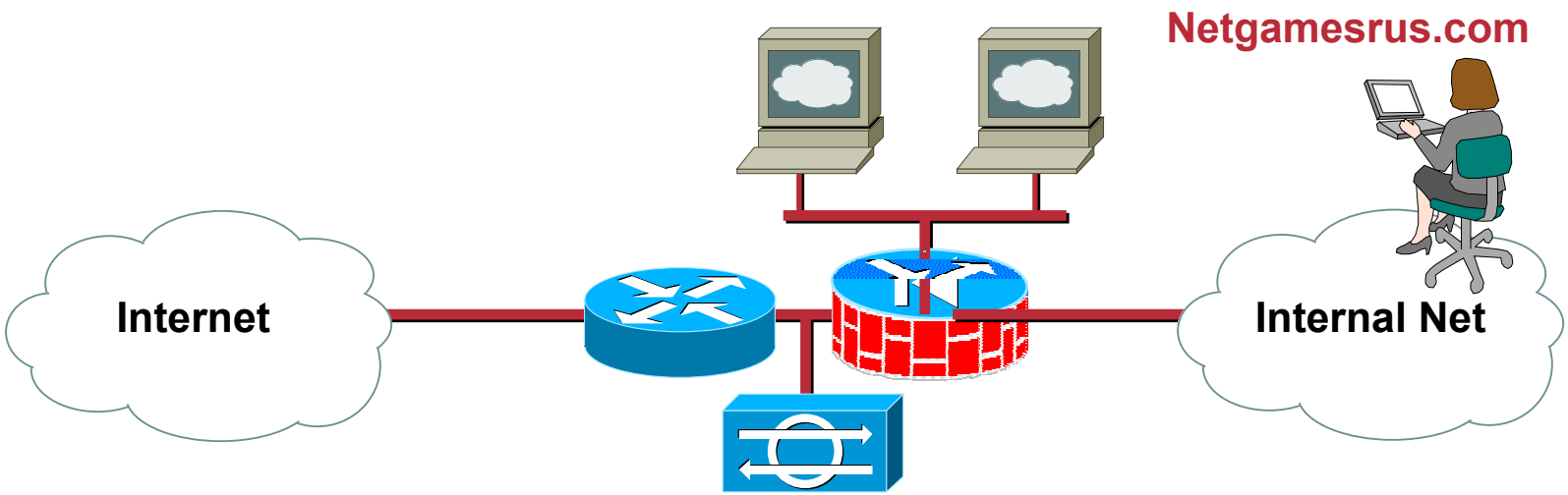
- 2002-02-07: Apache 2 for Windows php.exe Path Disclosure Vulnerability
- 2002-02-07: Apache 2 for Windows OPTIONS request Path Disclosure Vulnerability
- 2002-01-06: Apache Non-Existent Log Directory Denial Of Service Vulnerability
- 2002-01-04: Apache Win32 PHP.EXE Remote File Disclosure Vulnerability
- 2002-01-04: Apache HTTP Request Unexpected Behavior Vulnerability
- 2001-11-28: Apache Split-Logfile File Append Vulnerability
- 2001-11-08: Apache mod_usertrack Predictable ID Generation Vulnerability
- 2001-09-10: MacOS X Client Apache Directory Contents Disclosure Vulnerability
- 2001-08-12: Apache Mod ReWrite Rules Bypassing Image Linking Vulnerability
- 2001-08-09: Apache Server Address Disclosure Vulnerability
- 2001-07-10: Apache Possible Directory Index Disclosure Vulnerability
- 2001-06-10: MacOS X Client Apache File Protection Bypass Vulnerability
- 2001-04-12: Apache Web Server HTTP Request Denial of Service Vulnerability
- 2001-03-13: Apache Artificially Long Slash Path Directory Listing Vulnerability
- 2000-12-06: Apache Web Server with Php 3 File Disclosure Vulnerability
- 2000-09-29: Apache Rewrite Module Arbitrary File Disclosure Vulnerability
- 2000-09-07: SuSE Apache WebDAV Directory Listings Vulnerability
- 2000-05-31: Apache HTTP Server (win32) Root Directory Access Vulnerability
- 1999-09-25: NCSA/Apache httpd ScriptAlias Source Retrieval Vulnerability
- 1998-09-03: Multiple Vendor MIME Header DoS Vulnerability
- 1998-01-06: Apache Web Server DoS Vulnerability
- 1997-01-12: Apache mod_cookies Buffer Overflow Vulnerability
- 1996-12-10: Multiple Vendor nph-test-cgi Vulnerability
- 1996-04-01: Multiple Vendor test-cgi Directory Listing Vulnerability
- 1996-03-20: phf Remote Command Execution Vulnerability

In the hackers favour



- Exploit latest vulnerability (a race)
- Reinstall rootkit, clean logs
- Download additional attack tools
- Scan isolated service network and internal net
- Own more public hosts

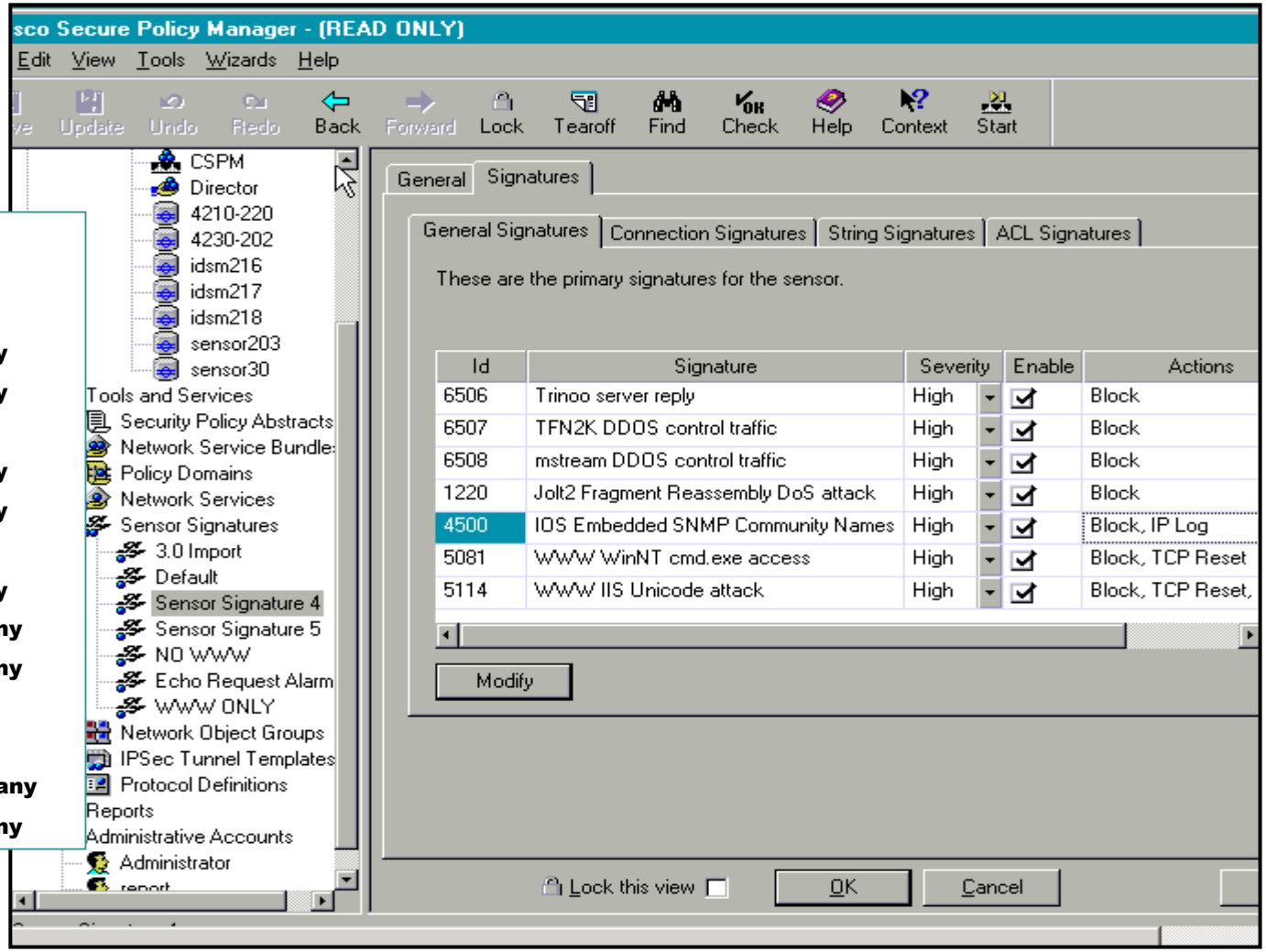
Raise the Bar



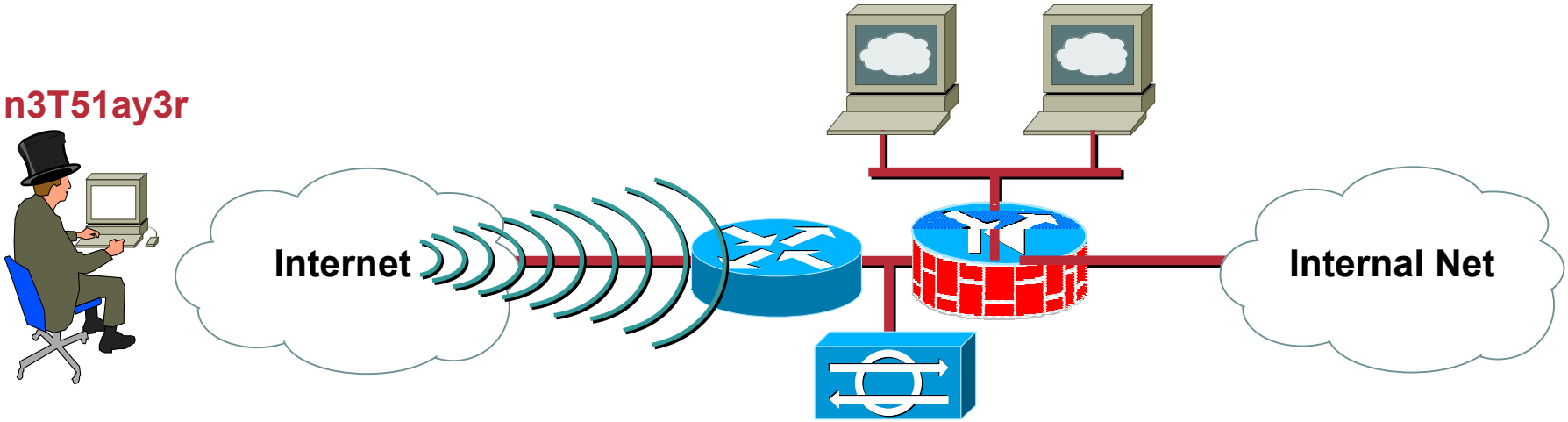
- Internal scan finds compromised hosts
- Fix and rebuild hosts
- Install network IDS
- Enable shunning and TCP resets
  - Most signatures
  - Reconfigure ACLs on the router

NIDS Response


```
7100he#show access-list
Extended IP access list 197
    permit ip host 10.1.1.20 any
    deny ip host 112.70.126.43 any
    deny ip host 96.193.155.79 any
    deny ip host 40.232.39.97 any
    deny ip host 220.64.150.28 any
    deny ip host 50.19.117.109 any
    deny ip host 176.82.33.85 any
    deny ip host 196.161.217.4 any
    deny ip host 111.100.101.15 any
    deny ip host 130.234.112.89 any
    deny ip host 243.68.1.8 any
    deny ip host 59.93.177.47 any
    deny ip host 239.213.208.158 any
    deny ip host 204.170.43.113 any
```

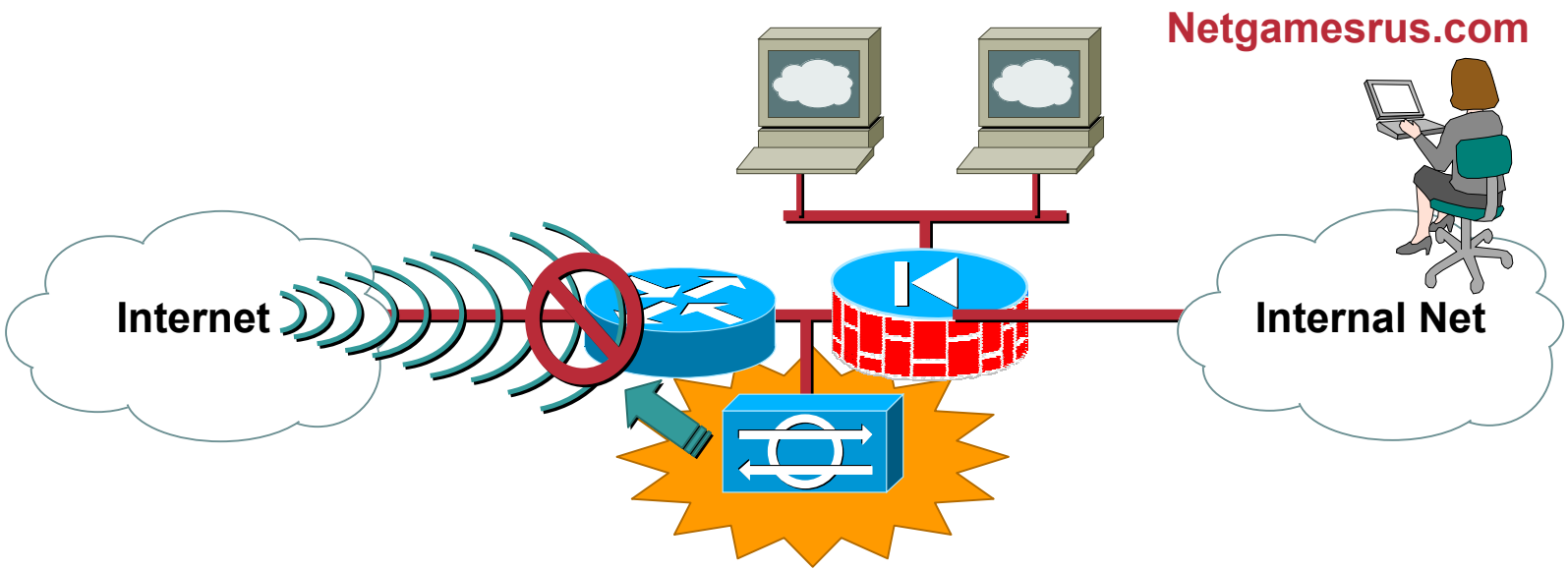


What does the hacker see?



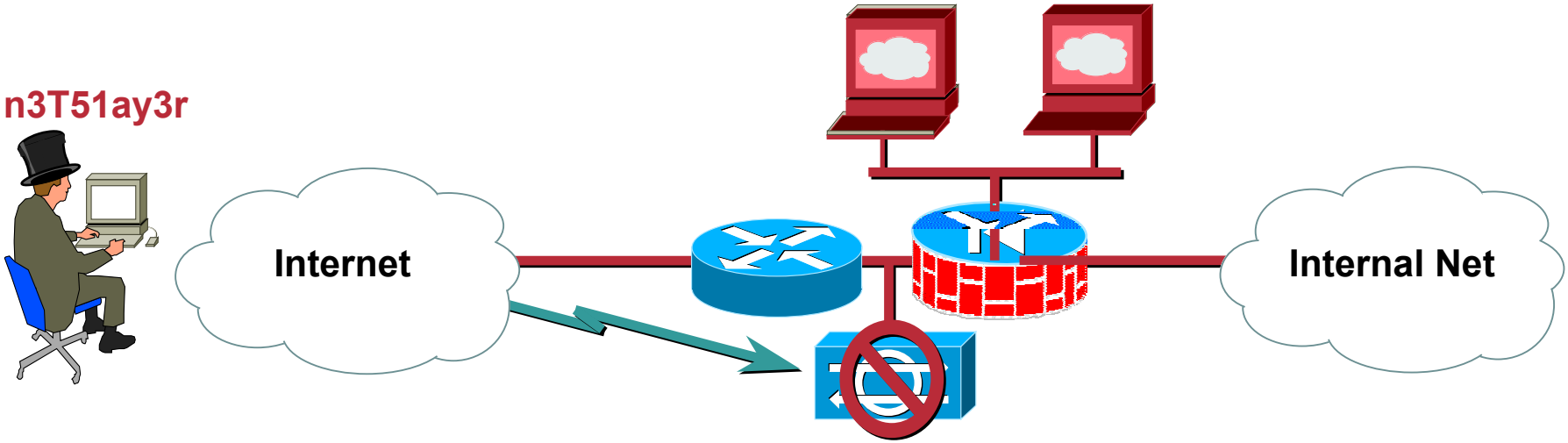
- Services found, though patched again
- Run vulnerability scans but inconsistent response
- Pings also blocked
- Other hackers observe the same result

IT Success!



- Scan and exploit attempts captured
- Shunning worked

Stick IDS



- Researched behavior, NIDS and shunning assumed
- Find method to defeat NIDS shunning—Stick
  - http://www.eurocompton.net/stick/
  - Overwhelms shunning capability
- Launch stick, re-exploit hosts, install toys
- Other available tools: Snot and Fragroute
  - http://www.monkey.org/~dugsong/fragroute/

Stick Tool

Cisco.com

Address http://www.eurocompton.net/stick/ Go Links

Fun with Packets:

Designing a Stick

By Coretez Giovanni

This paper outlines a denial-of-service attack against not the computer network, but the human processes that support intrusion detection. This attack is a resource exhaustion attack as outlined in the previous paper "Topology of denial of service".
It is informally written to express my opinion by which the tool "stick" was written to exploit. Hopefully this tool clearly shows some IDS flaws that will soon be remedied by better IDS products. Arthur Money spoke at Blackhat '00 about quality. Too bad there must not have been any software developers there to listen.
I use Stick and other self-developed tools for evaluating stress capability of IDS and firewalls. At this time I do not have comprehensive listing of IDS that are unaffected by the preceding method
I am not endorsing any products in t
before payload alarm which is esser
good deal of other attacks.
If my home lab ever gets big enough
and testing (as you always should d

Designing of the Attack

People are the essential element in i
reviewed and summarized for respo
Therefore, when a high number of fa
spoofed attacks. When a high numb
status of the network. This is a form
The key of course is to create a high

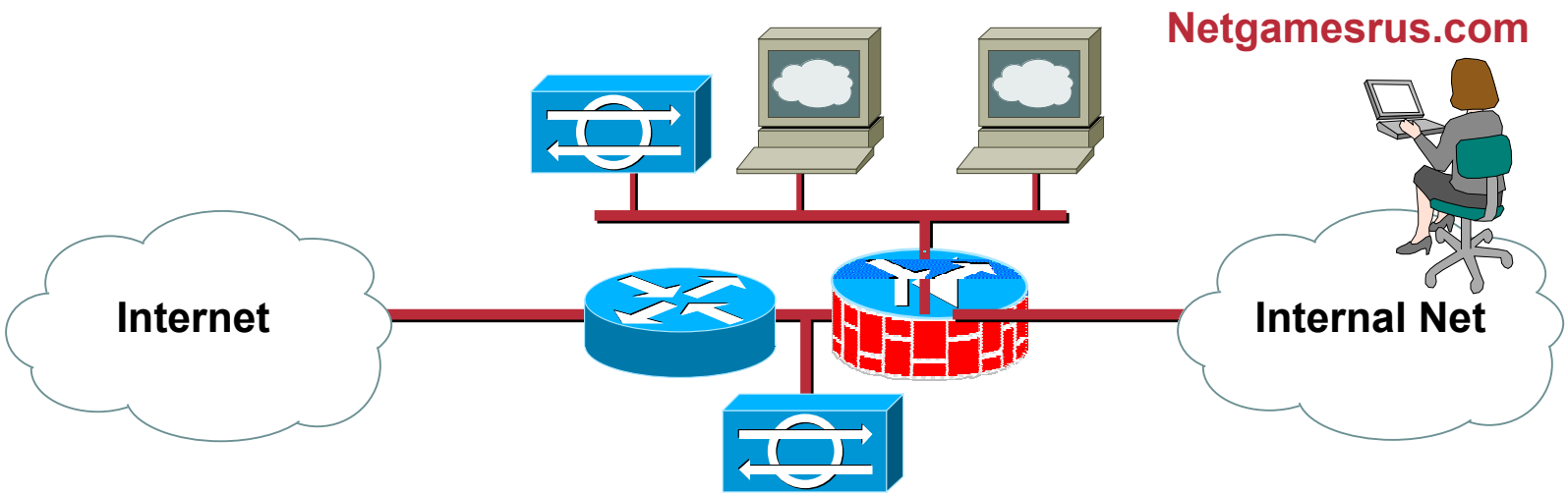
Create An Alarm

```
[root@sconvery-lnx stick]# ./stick -h

Usage: stick [sH ip_source] [sC ip_class_C_spoof] [sR start_spoof_ip end_spoof_ip]
          [dH ip_target] [dC ip_class_C_target] [dR starttargetip end_target_ip]
 ---------------------------------------------------------------------------
 defaults destination to 10.0.0.1 and source default is 0.0.0.0-255.255.255.255
 Software Design for limitted Stress Test capablity.

[root@sconvery-lnx stick]# ./stick dH 12.1.1.1
Destination target value of: 101010c
Stress Test - Source target is set to all 2^32 possiblities
 sending rule 496
 sending rule 979
 sending rule 896
 sending rule 554
 sending rule 735
 sending rule 428
```

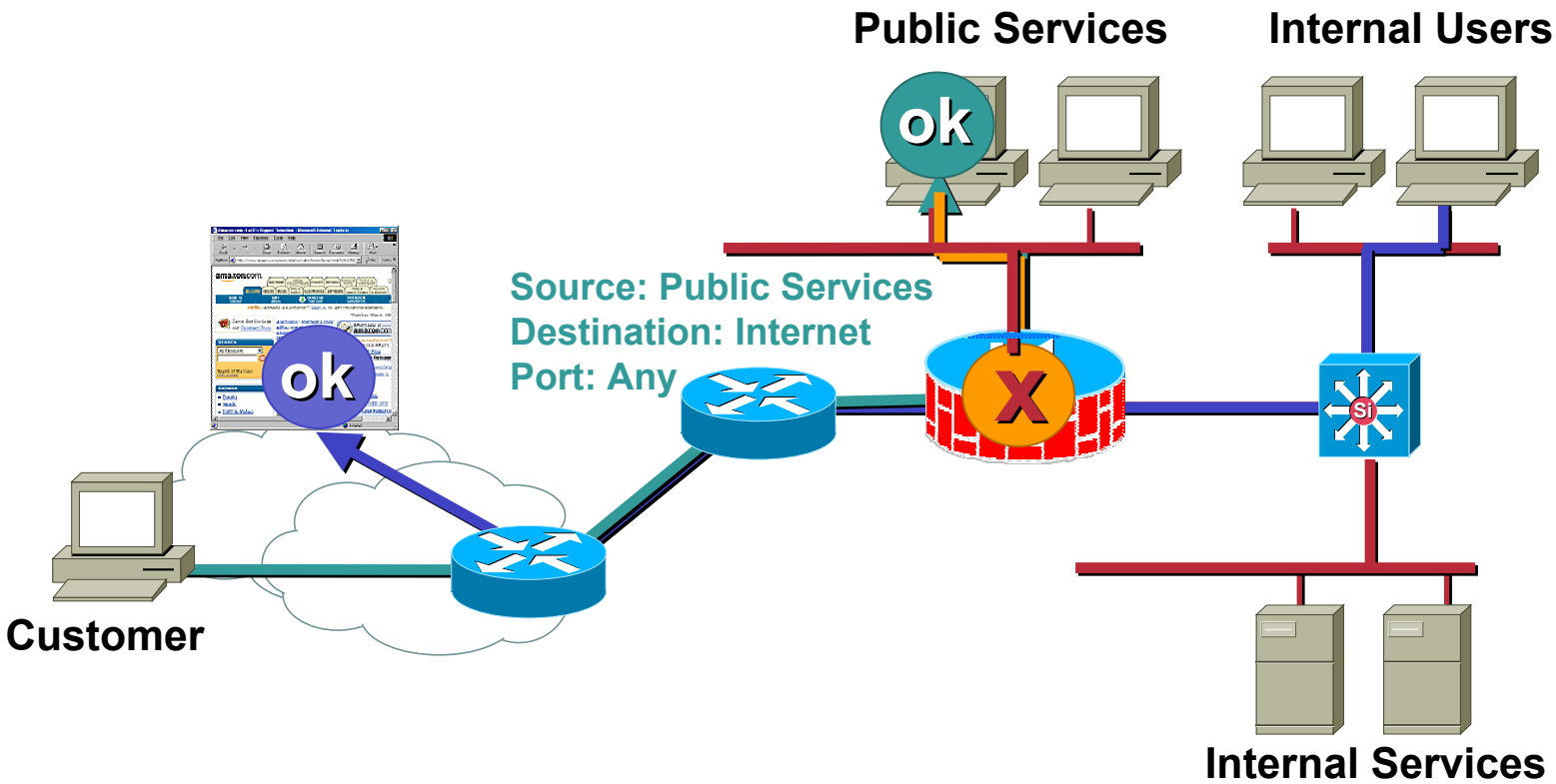
New Management



- **Two observations**
  - **NIDS shunning pre-FW may be overflowed so turn off shunning**
  - **Firewall logs show download of tools on hosts**
- **Install NIDS in public segment and liberally shun on FW**
- **FW ACLs to prevent public services segment outbound sessions**
- **Rebuild hosts using Ghost ☺ and patch**

Specific Filtering

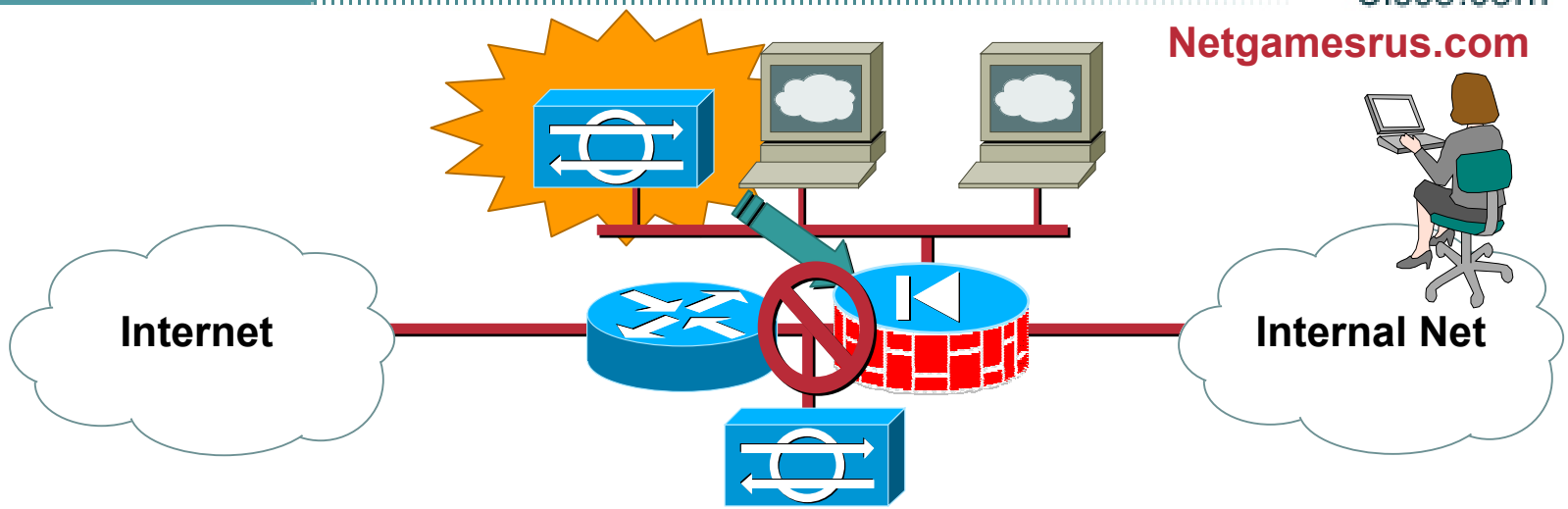
- No outbound for Web servers
- Be specific on other access



Lessons Learned: n3T51ay3r vs. Netgamesrus.com

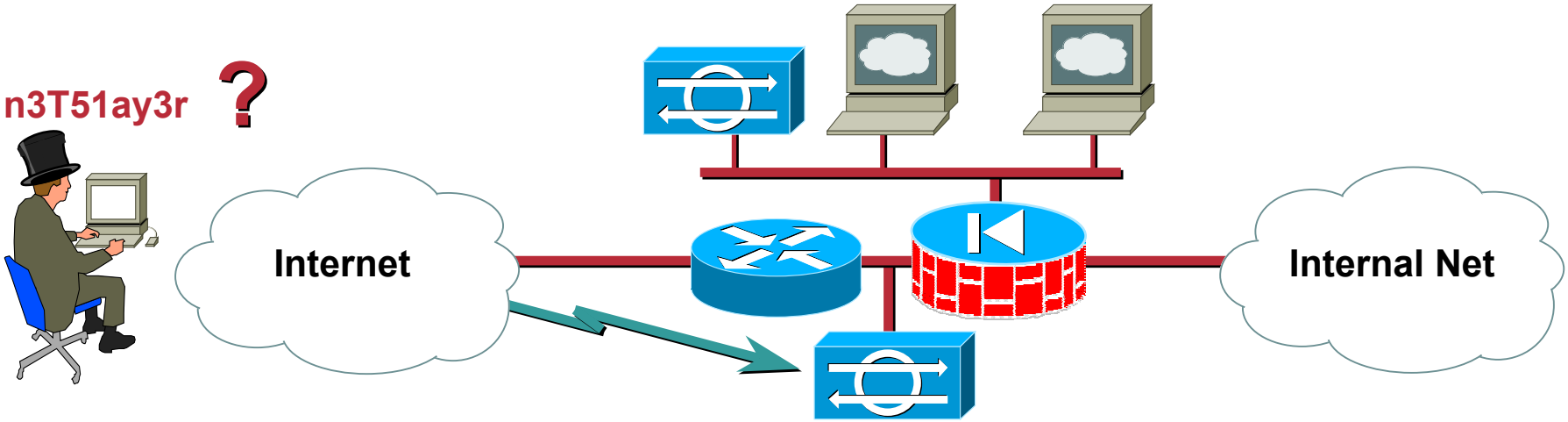
- Bind hack—Mitigated by patches and NIDS
- Root kit—Found by scan, manually removed
- New vulnerability—Found by FW logs, mitigated by patches
- Attack tool download—Mitigated by outbound filtering on FW
- IDS shun DoS—Stick—No shunning on NIDS in front of FW

Additional NIDS tier applied



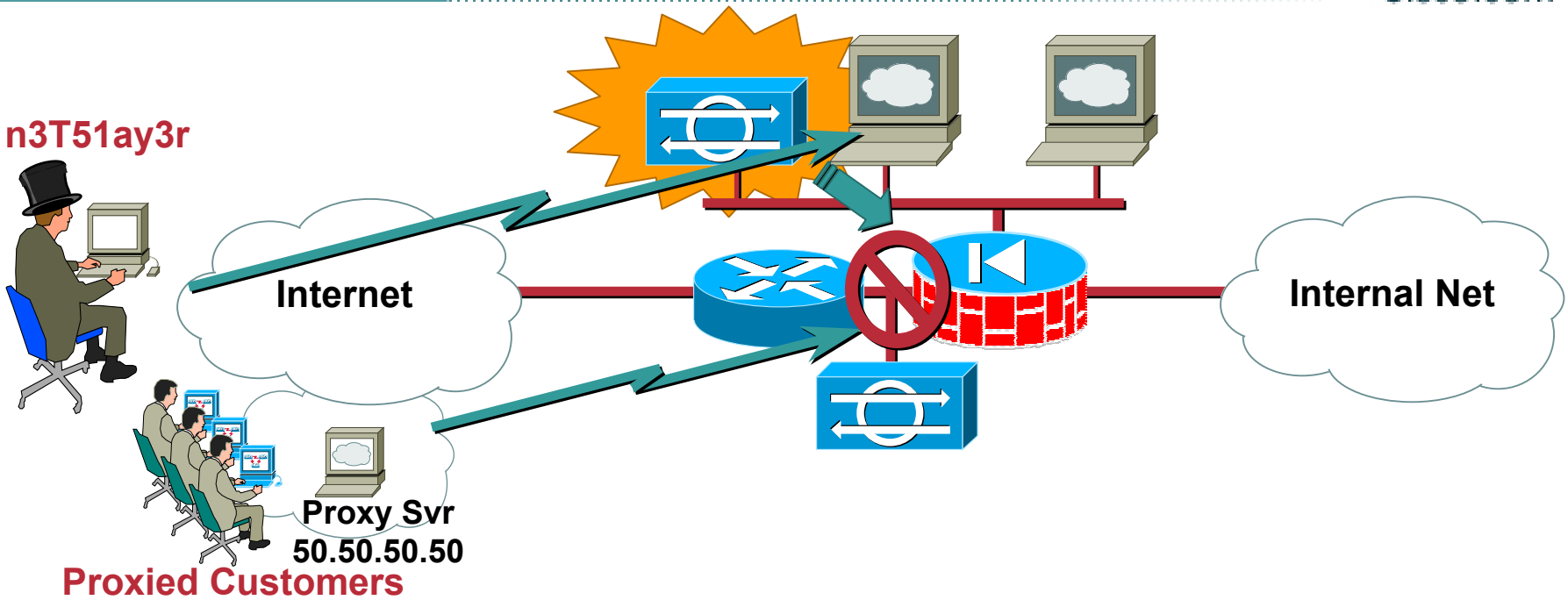
- NIDS alarming tracks cracker activities
- Shunning on FW working
- FW mitigates stick effects on NIDS in public services segment

This is getting tough for the hacker



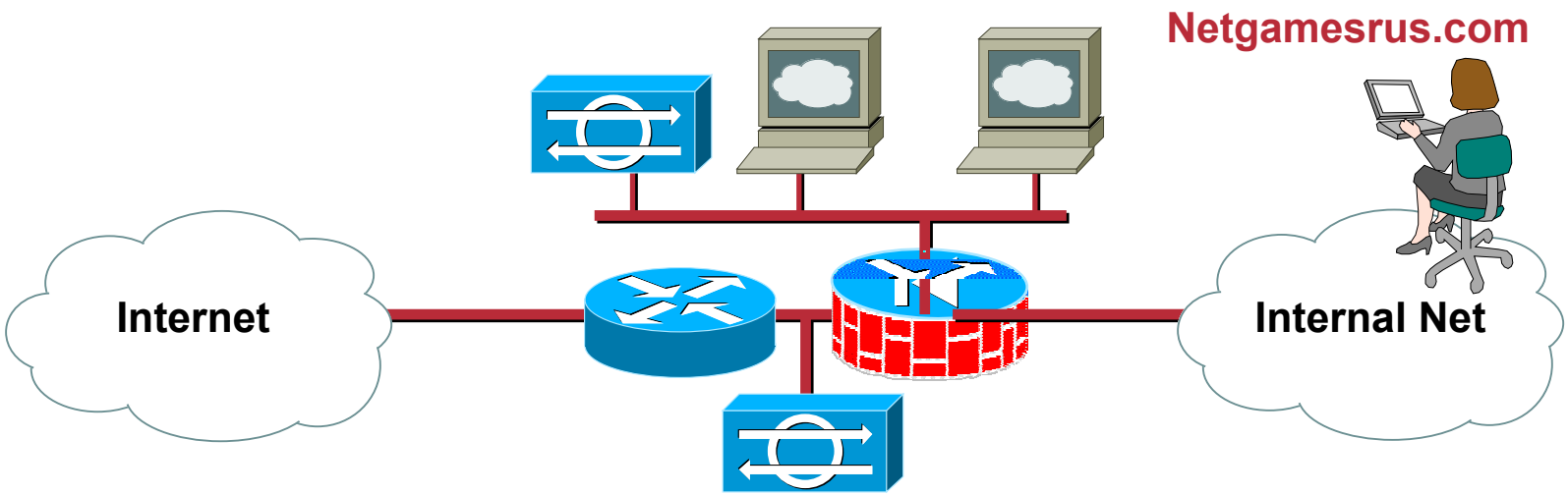
- Must still be shunning
- Use stick again
- Still no success

The Empire Strikes Back



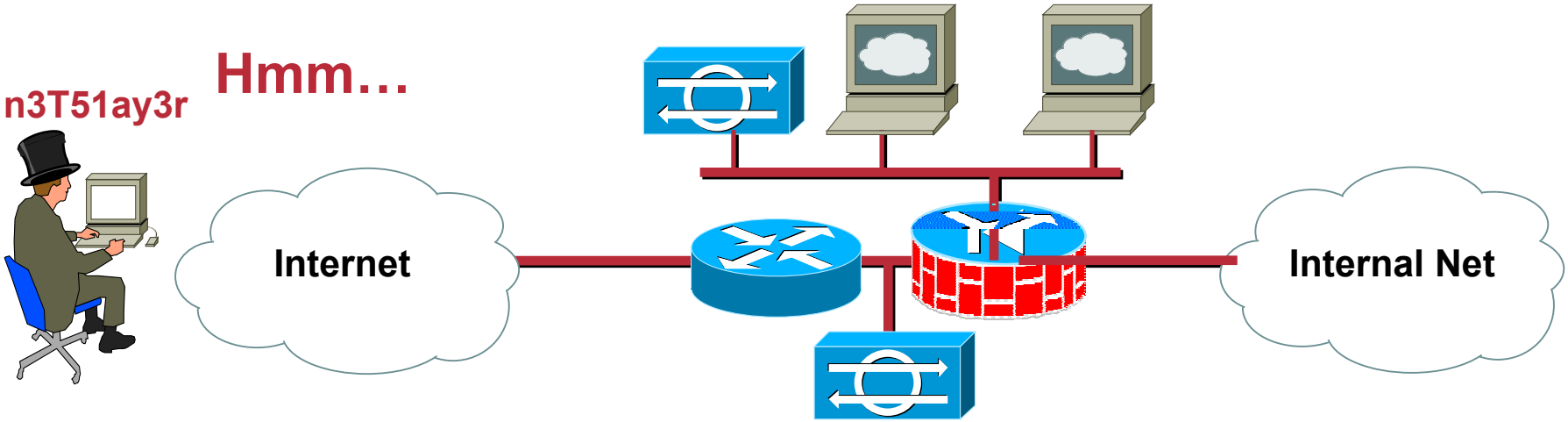
- **What is being shunned?**
  - Looks like composite and atomic attacks are shunned
- **Exploit poorly deployed shunning:**
  - Launch spoofed atomic attacks from proxy servers of large ISPs
- **Now legitimate customers can't get in!**

To Shun or Not to Shun



- **Public exposure (due to shun problem) creates job uncertainties among the IT staff**
- **Perhaps shunning everything is a bad idea?**
  - **Set shun posture to only critical multi-packet TCP attacks**
  - **Consider TCP handshake monitoring on IDS**
  - **Tune IDS (shun length, false positives, alarm levels, hire staff to monitor IDS 24x7)**

Try, Try Again



- Looks like they've got their act together

Trying the ISP DoS again doesn't work

Shunning must have been tuned

- Change approach consider host attacks again

What CGI scripts are running on the box?

Application Layer Attacks

.oO Phrack 49 Oo.

Volume Seven, Issue Forty-Nine

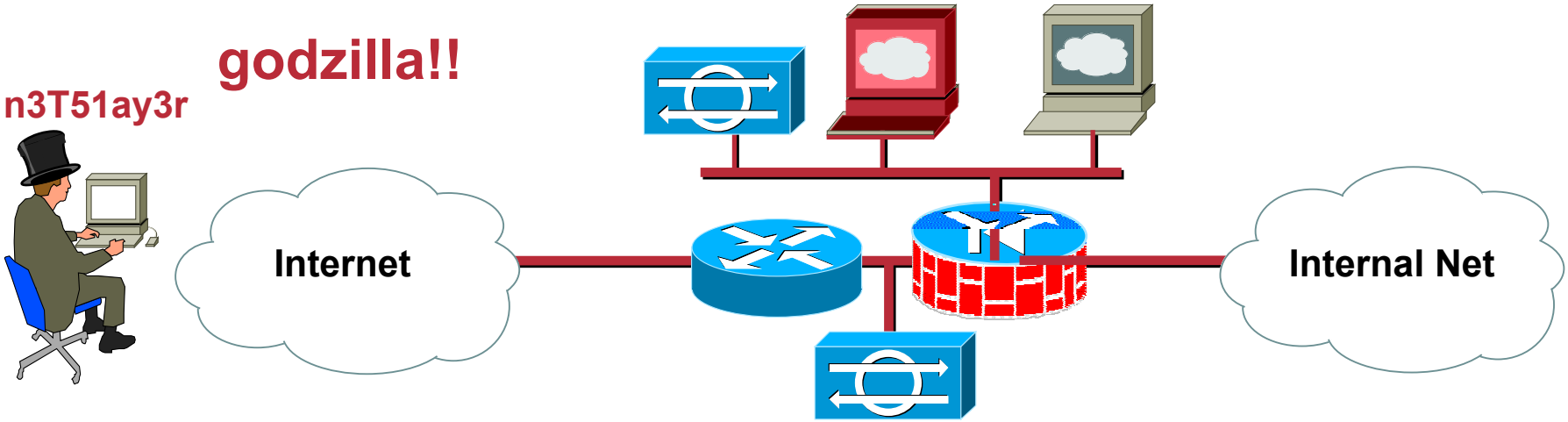
File 14 of 16

BugTraq, r00t, and Underground.Org
bring you

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Smashing The Stack For Fun And Profit
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

by Aleph One
aleph1@underground.org

godzilla.d



- Found a public domain CGI in use (SANS General #7)
- Examine source code and run tools to find an unpublished vulnerability
- After substantial research, success
- Compromise web server with new toy (godzilla.d)

SANS General #7: CGI Vulnerabilities

Cisco.com

G7 - Vulnerable CGI Programs

G7.1 Description:

Most web servers, including Microsoft's IIS and Apache, support Common Gateway Interface (CGI) programs to provide interactivity in web pages enabling functions such as data collection and verification. In fact, most web servers are delivered (and installed) with sample CGI programs. Unfortunately, too many CGI programmers fail to consider that their programs provide a direct link from any user anywhere on the Internet directly to the operating system of the computer running the web server. Vulnerable CGI programs present a particularly attractive target to intruders because they are relatively easy to locate and operate with the privileges and power of the web server software itself. Intruders are known to have exploited vulnerable CGI programs to vandalize web pages, steal credit card information, and set up back doors to enable future intrusions. When the Department of Justice web site was vandalized, an in-depth assessment concluded that a CGI hole was the most probable avenue of compromise. Web server applications are similarly vulnerable to threats created by uneducated or careless programmers. As a general rule, sample programs should always be removed from production systems.

G7.2 Systems impacted:

All web servers.

G7.3 CVE entries:

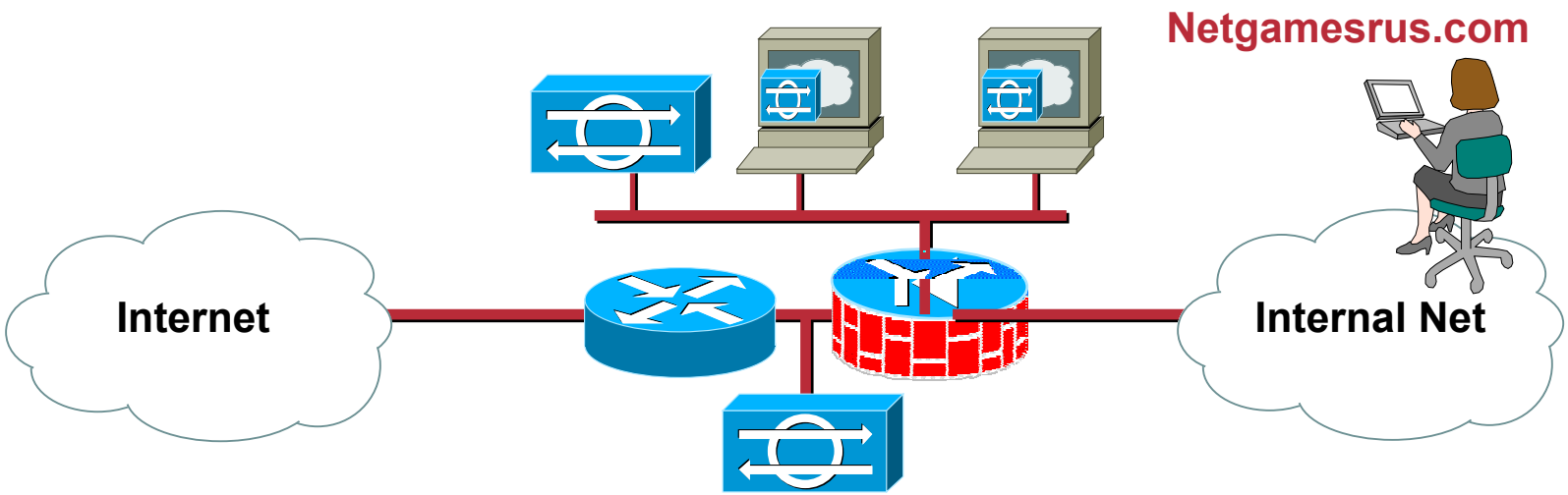
(Note: This list is not complete or all-inclusive. It is a sample of some of the vulnerabilities covered by this category.)

CVE-1999-0067, CVE-1999-0346, CVE-2000-0207, CVE-1999-0467, CAN-1999-0509, CVE-1999-0021, CVE-1999-0039, CVE-1999-0058, CVE-2000-0012, CVE-2000-0039, CVE-2000-0208, CAN-1999-0455, CAN-1999-0477

G7.4 How to determine if you are vulnerable:

If you have any sample code on your web server, you are vulnerable. If you have legitimate CGI programs, ensure you are running the latest version, and then run a vulnerability scanning tool against your site. By simulating what an attacker would do, you will be prepared to protect your systems. To find vulnerable CGI scripts, you may use a CGI scanner called whisker that can be found at:

Why us?



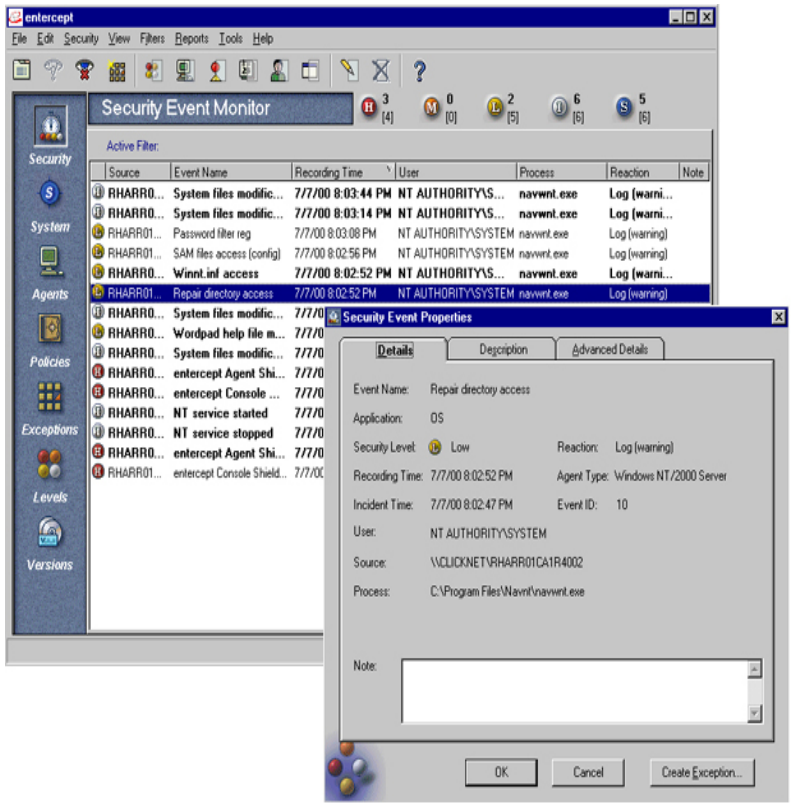
- Find, Ghost, and patch hosts
- Fix CGI script (with outside help)
- Post to Bugtraq (or not)

Do we really want more visibility?

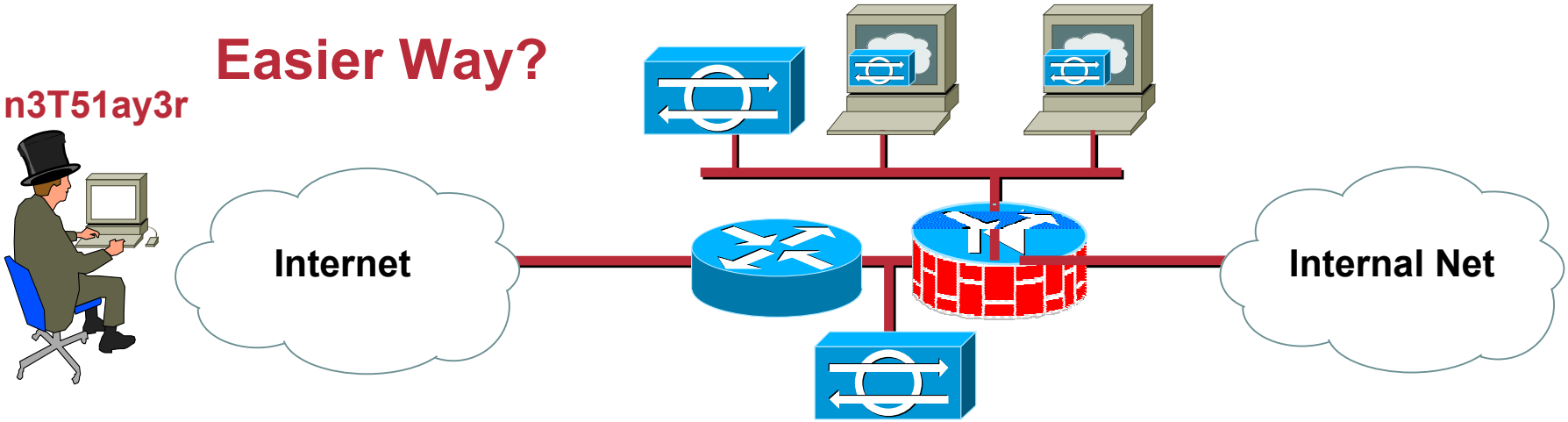
- Install host IDS on appropriate hosts

Host Intrusion Detection

- Host IDS is best installed on key servers
- Features vary per product, including watching for:
  - File system
  - Process table
  - I/O
  - System resource usage
  - Memory allocation
- Actions include alarm and sometimes prevent
- Financially and operationally impractical to install on all hosts



Alternate Route Needed



- Their Internet access seems pretty locked-down
- Try war driving

Drive by hacking

- Identifies WLAN details (SSID, AP MAC, use of WEP)
- Links directly to GPS to give AP location
- Can convert into Streetmap.co.uk format using: http://www.interrorem.com/software/stumbler.php3

Long Distance Hacking

"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

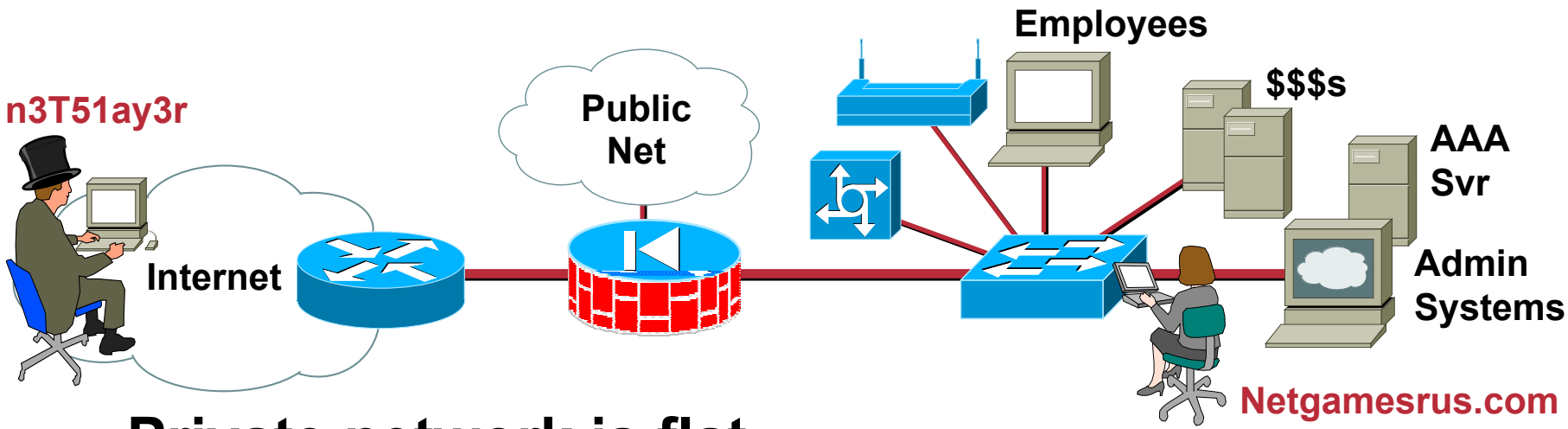
- "Pringles" YAGI Antenna
  - Cost: $10
  - Range: 10 Miles

Friday, 8 March, 2002, 09:23 GMT

Hacking with a Pringles tube

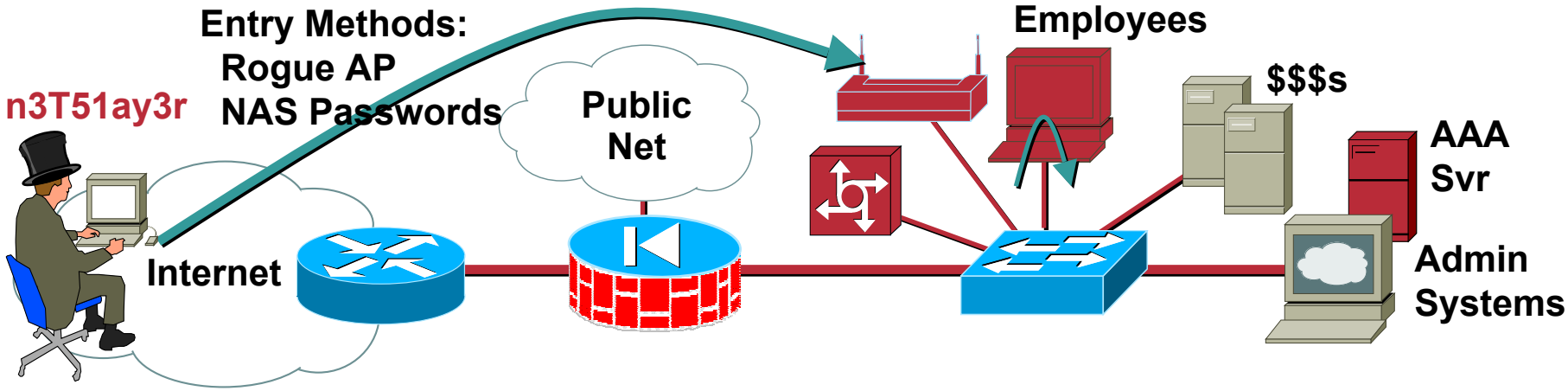
A crisp can is an effective tool for curious hackers

Private Network Disclosed



- **Private network is flat**
- **Management communications is:**
  - **In-band (over the company's user network)**
  - **In the clear (telnet, tftp, syslog, SNMP)**
- **Dial-in access available (reusable passwords)**
- **WLAN access available via rogue AP (default SSID, standard WEP)**

Breach Private Network



- War driving finds poorly secured WLAN Access Point (AP); after a bit of packet analysis, the WEP key is mine

- Setup jump host on an employee machine, install rootkit and attack tools, hack comfortably from my car
- Use sniffers to map network and grab passwords
  - Learn addressing and server devices
  - Observe mgmt channels
  - Obtain passwords via sniffing and password cracking (rootkits, dsniff, LC4)

802.11b Is Insecure

- **WEP has "Issues"**

  Security of the WEP Algorithm:
  http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

  Your 802.11 Wireless Network has No Clothes:
  http://www.cs.umd.edu/~waa/wireless.pdf

  Weaknesses in the Key Scheduling Algorithm of RC4:
  http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps

  Using the Fluhrer, Mantin, and Shamir Attack to Break WEP:
  http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

  Practical implementations of the attacks

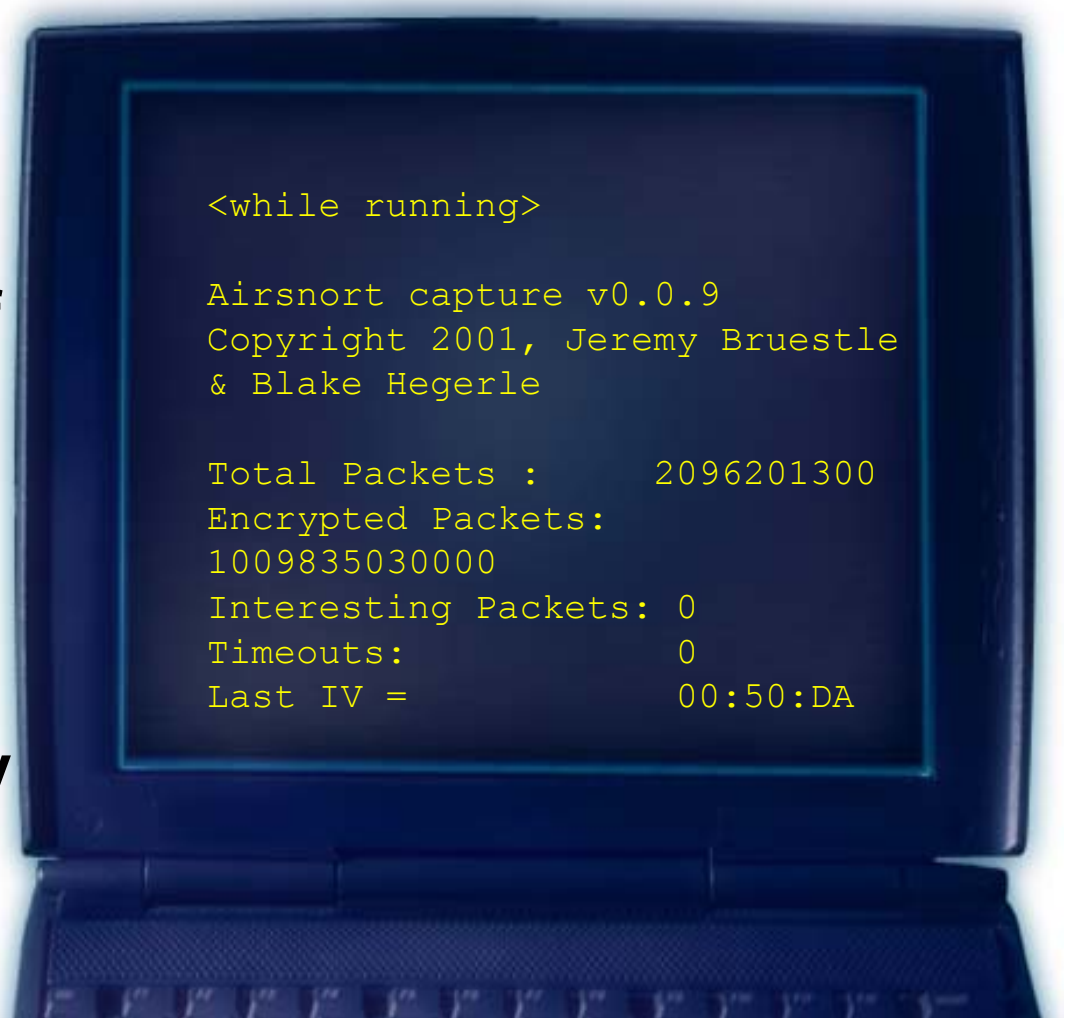
    http://airsnort.sourceforge.net/

    http://wepcrack.sourceforge.net/

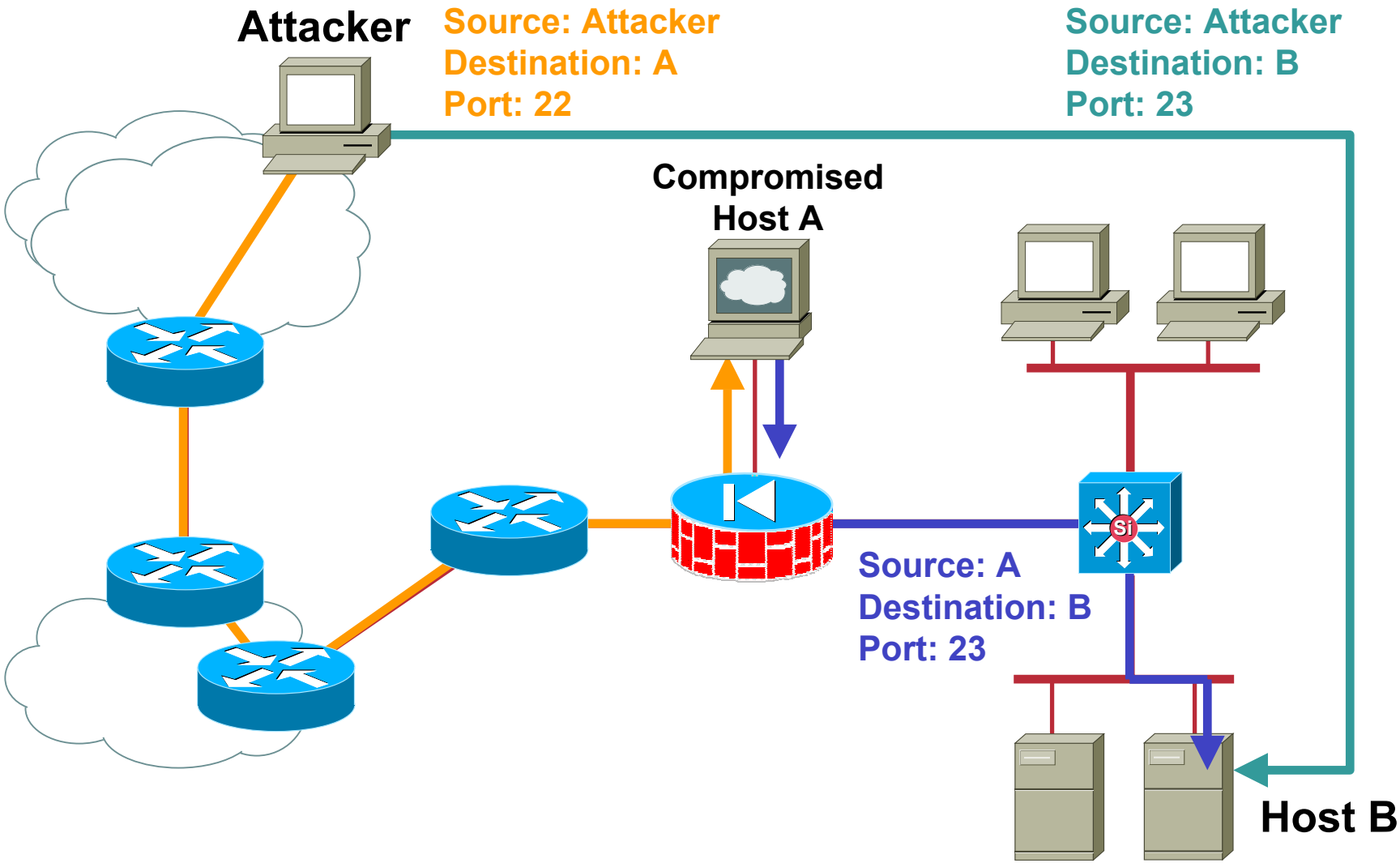
- **Even if WEP were secure (which it's not), the standard makes no provisions for key distribution or management**

Airsnort

- Easy to use exploit of the “Fluhrer” defined weakness
- Requires 5-10 million WEP encrypted packets
- Guesses the WEP key in under a second



Jump Hosts (Port Redirection)



Dsniff

- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH / SSL Interception
- Switches can be sniffed without SPAN
- ARP has no security

SANS W6: Weak Password Hashing

Cisco.com

W6 - Weak hashing in SAM (LM hash)

W6.1 Description:

Though most Windows users have no need for LAN Manager support, Microsoft stores LAN Manager password hashes, by default, on Windows NT and 2000 systems. Since LAN Manager uses a much weaker encryption scheme than do the more current Microsoft approaches, LAN Manager passwords can be broken in a very short period of time. Even strong password hashes can be cracked in under a month. The major weaknesses of LAN Manager hashes is the following:

- password truncated to 14 characters
- password padded with spaces to become 14 characters
- password converted to all upper case characters
- password split into two seven character pieces

This means that a password cracking program has to crack only two seven-character passwords without even testing lower case letters. In addition, LAN Manager is vulnerable to eavesdropping of the password hashes. Eavesdropping can provide attackers with user passwords.

W6.2 Systems impacted:

Microsoft Windows NT and 2000 computers

W6.3 CVE entries:

N/A

W6.4 How to determine if you are vulnerable:

If you are running a default installation of NT or 2000, you are vulnerable since LAN Manager hashes are created by default. You may (if you have specific written permission from your employer) test the ease of password cracking on your own systems using an automated password cracking tool like LC3 (l0phtcrack version 3) available from: http://www.atstake.com/research/lc3/download.html

W6.5 How to protect against it:

LC4 (aka l0phtcrack)

LC3 - [Untitled1]

File View Import Session Help

User Name	LM Password	<8	NTLM Password	Audit Time
Administrator		x		
boone.speed	DRAMATIC1!		dramatic1!	0d 0h 0m 57s
chris.sharma	AGE18	x	age18	0d 0h 1m 8s
dale.goddard	UNCRACK???????			
dave.graham	CARTILAGINOUS		cartilaginous	0d 0h 0m 2s
Guest	AUTHORITARIAN			0d 0h 0m 1s
jerry.moffat				
klem.loscot				
lynn.hill				
patrick.edlinger				
scott.franklin				
yuji.hirajama				

Ready

Auditing Options For This Session

Dictionary Crack

☑ Enabled — Word file: C:\Program Files\Security Software T — Browse...

The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

Dictionary/Brute Hybrid Crack

☑ Enabled — 2 Characters to vary (more is slower)

The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.

Brute Force Crack

☑ Enabled — Character Set: A - Z and 0 - 9

☑ Distributed — Custom Character Set (list each character): TOUGHON3

Part 1 Of 2

The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3plt6s" or "vC5%69+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.

Dictionary Status

words total 16180
words done 235007
% done 6.885%

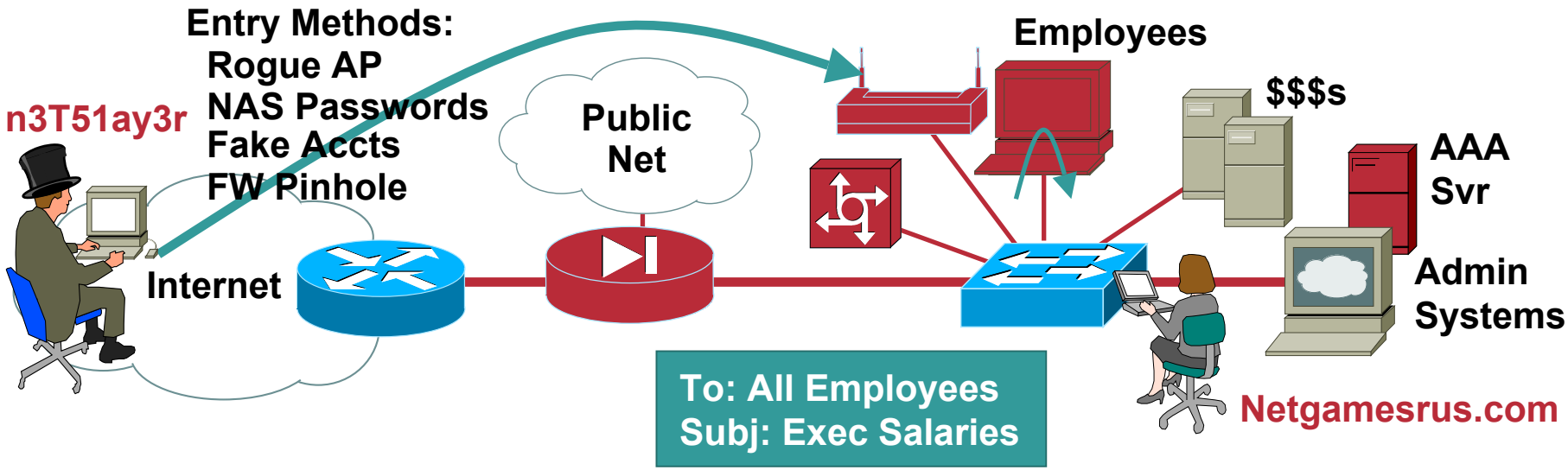
Brute Force

time elapsed 0d 0h 0m 0s
time left
% done
current test
keyrate

☑ User Info Check
☑ Dictionary
☐ Hybrid
☐ Brute Force

LC3
Security Software Technologies, Inc.
securitysoftwaretech.com

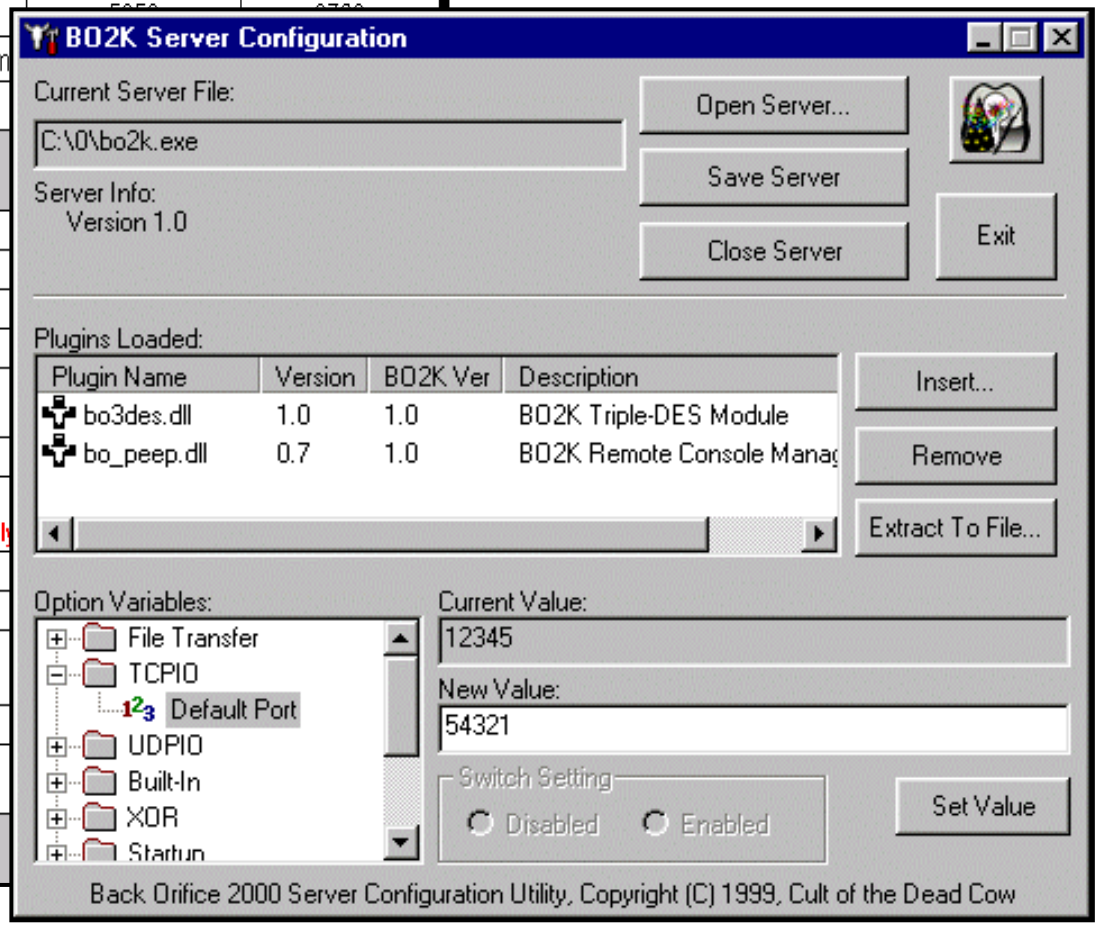
Own Internal Devices



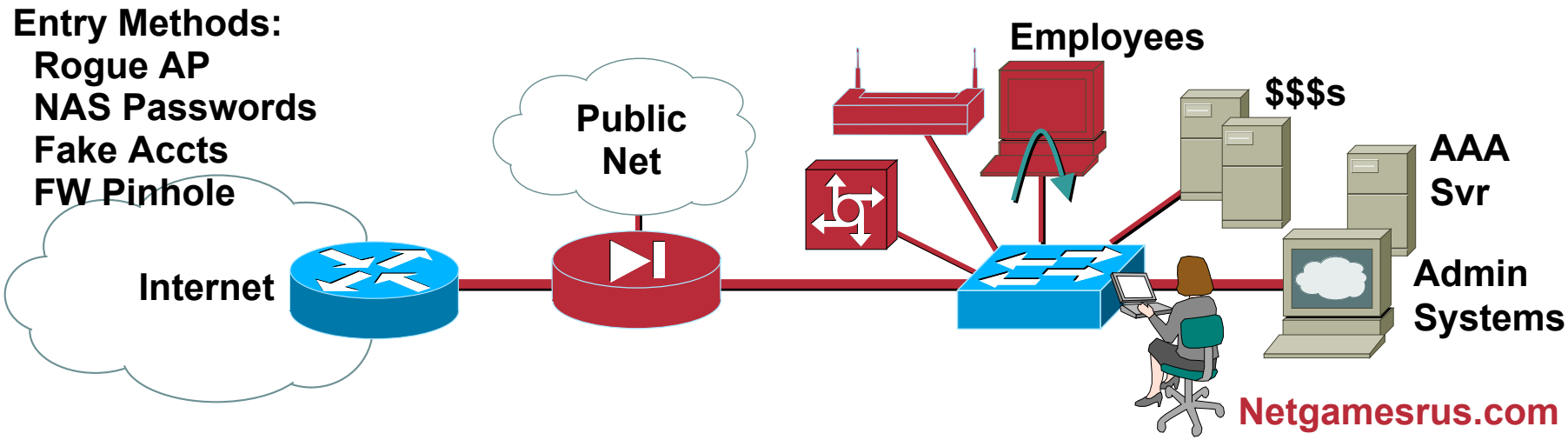
- Create backdoor logins (for use later!)
- Create a "pinhole" on the FW by modifying ACLs and NAT
  - Useful for "friendly" access
- Review company confidential data on servers
- Send salary info to company-wide mail list
- Install BO2k server on several systems

Back Orifice 2000

	Back Orifice 2000	pcAnywhere 9.0	Carbon Copy 32 5.0	CoSession Remote 32 V8
Contact Information:	Cult of the Dead Cow (www.cultdeadcow.com)	Symantec 541-334-6054 or 800-441-7234	Compaq 281-370-0670 or 800-888-	Artisoft 520-670-7100 or 800-846-
Website URL:	www.bo2k.com	www.symantec.com		
Price:	FREE	$169.95		
Remote Control Features:				
Keystroke Logging	✓	✗		
Remote Reboot	✓	✗		
Print redirection	✗	✓		
Registry Editing	✓	✗		
Multiple host/guest sessions	✓ ✓	✓ ✓		
Data encryption	✓	✓		
Strong encryption	✓	✓ MS Crypto API Only		
Color scaling	✓	✓		
Remote Install	✓	✓		
Remote Update	✓	✓ Only with LiveUpdate		
Remote Uninstall	✓	✗		
Host keyboard/mouse lock	✓ ✓	✓ ✓		
File-Transfer Features:				



There's Movement All over the Place!



- Email got noticed, "originated" from innocent employee
- Host-based virus scanning detects and removes BO2k on several workstations and servers
- Install NIDS and watch traffic on key servers
- Install ACLs on FW to prevent outbound access for key servers

BO2k Detection

sco Secure Policy Manager - (READ ONLY)

Edit View Tools Wizards Help

Update Undo Redo Back Forward Lock Tearoff Find Check Help Context Start

- CSPM
- Director
- 4210-220
- 4230-202
- idsm216
- idsm217
- idsm218
- sensor203
- sensor30
- Tools and Services
  - Security Policy Abstracts
  - Network Service Bundle
  - Policy Domains
  - Network Services
  - Sensor Signatures
    - 3.0 Import
    - Default
    - Sensor Signature 4
    - Sensor Signature 5

General | Signatures

General Signatures | Connection Signatures | String Signatures | ACL Signatures

These are the primary signatures for the sensor.

Signature	Severity	Enable	Actions
Auth failure Telnet	Low	☑	None
Back Orifice	High	☑	None
BackOrifice BO2K TCP Non Stealth	High	☑	Block, TCP Reset
BackOrifice BO2K TCP Stealth 1	High	☑	Block, TCP Reset
BackOrifice BO2K TCP Stealth 2	High	☑	Block, TCP Reset
BackOrifice BO2K UDP	High	☑	Block
BIND improper SIG validation DoS	High	☑	None
BIND NXT overflow	High	☑	None

Event Viewer - Database Events - CSIDS Alarms

File Edit View Actions Tools

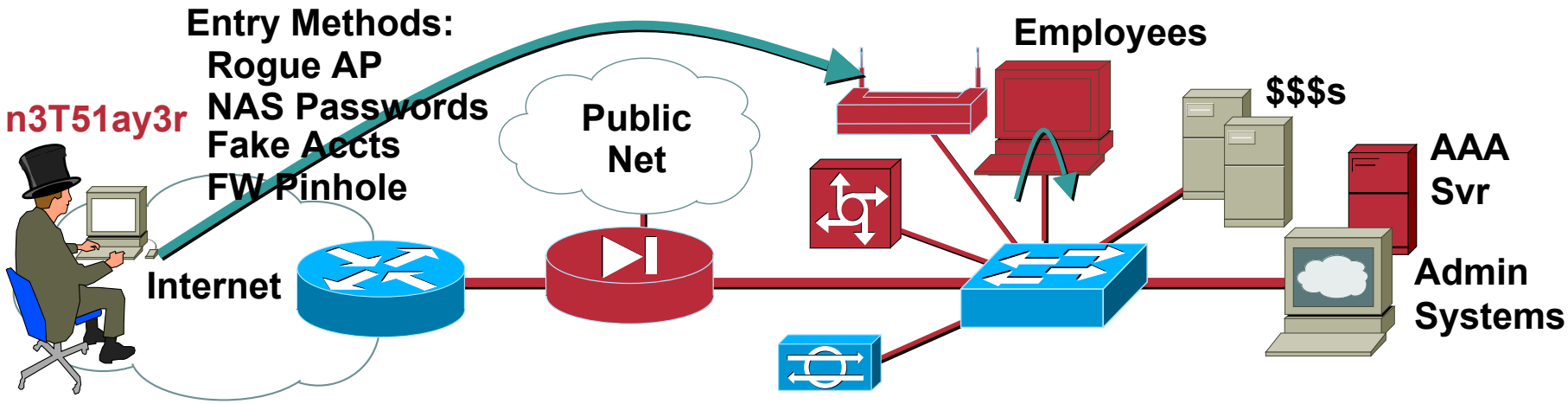
- NRD-SANS
- NRS-Outside
- NRS-Inside
- idsm
- idsm2
- NRS-minime
- IDNetSensor30

Count	Name	Source Address	Dest Address	Details	Source Loc	Dest Loc	Severity
2	BackOrifice BO2K TCP Non Stealth	15.1.1.26	15.1.1.27	<none>	OUT	OUT	High
14		15.1.1.27	15.1.1.26	<none>	OUT	OUT	High
72	DNS Version Request	10.1.2.2	+				
106	ICMP echo reply	+					
23	ICMP flood	10.1.1.123	10.1.1.166	<none>	+		

NIDS in High Load Environments

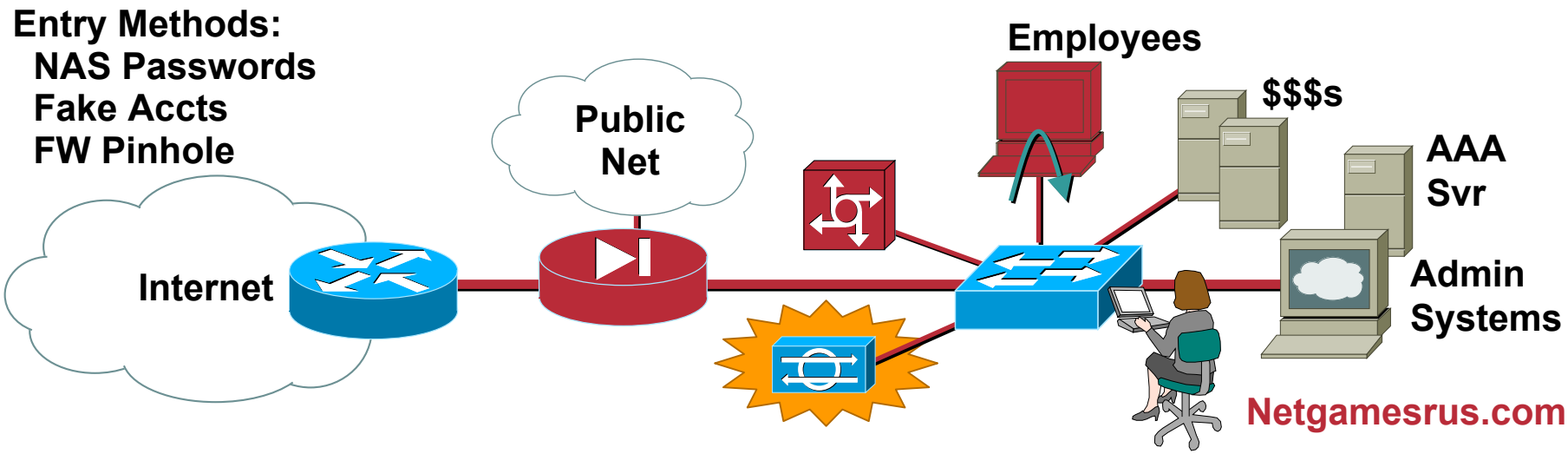
- NIDS value reduced when packet rate too high due to data loss (NIDS fails open)
- Tricks for reducing load include:
  - Load balancing multiple NIDS devices
  - Layer 3 and 4 pre-screening of data
  - Unidirectional, not bi-directional, examination (some signatures do not fire properly)
- Beware overly sensitive alarming, don't be overwhelmed

AP Access Again



- Access network again via AP
- Where's my BO2k servers?
- Reinstall and run BO2k
- Client access to BO2k server keeps failing???
- Run away!

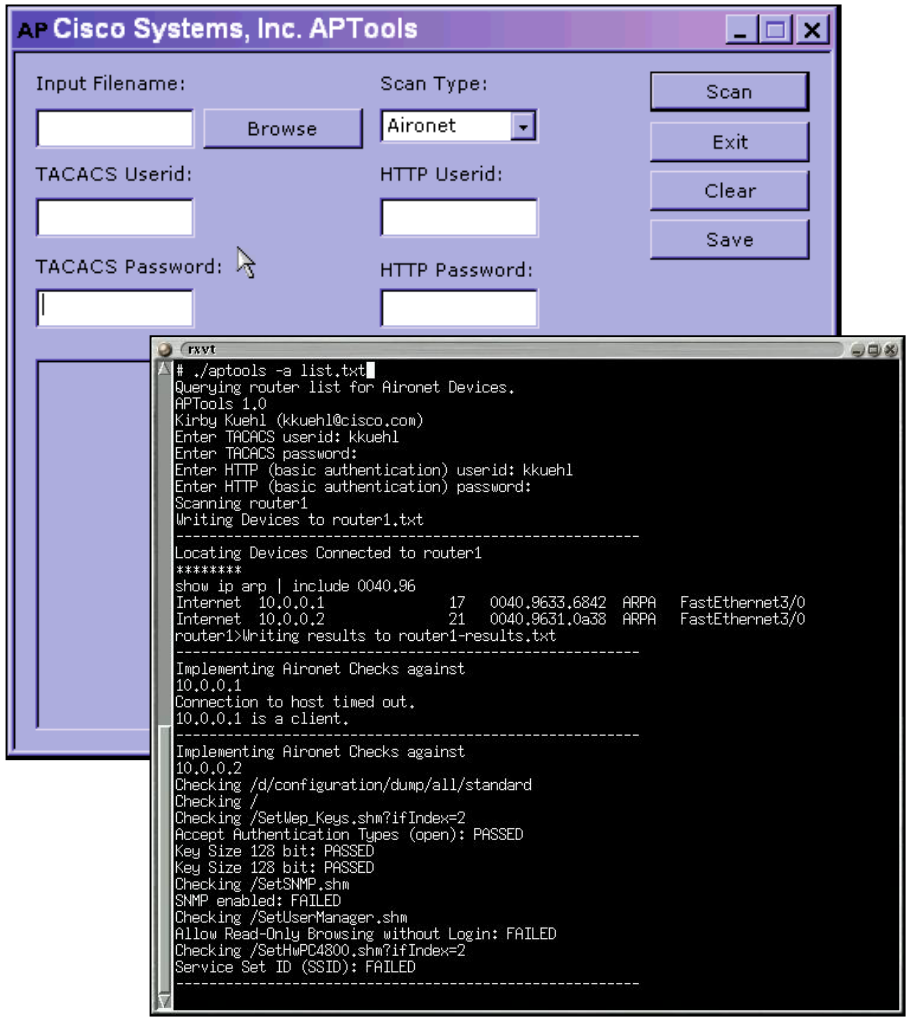
Caught in the Act



- Sysadmin sees the BO2k reset on the NIDS box and traces it back to the rogue AP
- Rogue AP removed, IT supported WLAN project begins (“remind” employees of the corporate security policy)
- Remove BO2k from internal systems (again)

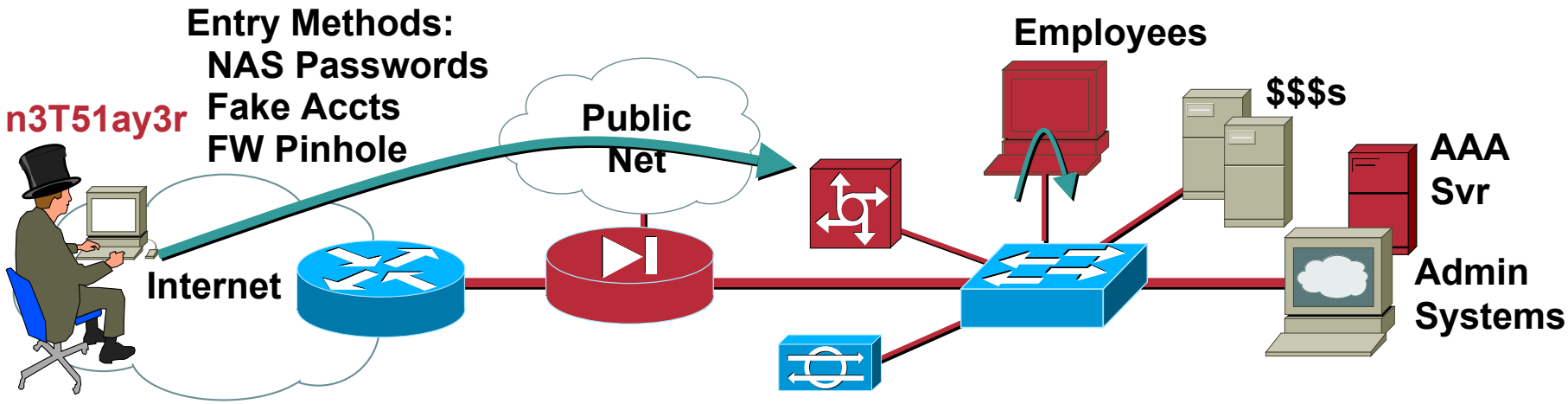
Rogue AP Detection

- **802.11b Detection Methods:**
  - **TCP Fingerprinting (NMAP)**
  - **802.11b Analyzer (War Driving)**
  - **SNMP**
  - **APTools (Query Network)**
- **APTools:**
  - **Query routers and switches ARP tables, also NMAP input**
  - **Identifies APs through IEEE OUI and Company_id Assignments**
  - **Audit APs settings**
  - **HTTP Basic Authentication Support**
  - **Developed and tested on Cisco products: Cisco Aironet Access Points, Cisco routers, and Cisco switches; your mileage may vary**



Beta Version Available at aptools.sourceforge.net

Still Have Other Ways In



- After a while, try to gain entry again
- Can't break into AP, so access network via NAS with newly created account (leave the pinhole for last resort)
- Where's BO2k?
- Reinstall BO2k with crypto and stealth updates, run it
- Seems to work

Back Orifice 2000 Plug-ins

Address http://www.roe.ch/bo2k/

WWW.ROE.CH

[roe.ch]
Home
Who I am
Support Me

[Coding]
Cryptography
BO2K Plugins
Other Projects

[Networking]
Linux
Security

[PBM and RPG]
Eidolon Arinot
Kartograph. Allianz
Battles of Europe II
Roleplay

[site under heavy reconstruction]

Plugins for Back Orifice 2000

«The strongest encryption available for BO2K. Great!»
--- DilDog, author of BO2K, member of cDc and The L0phT

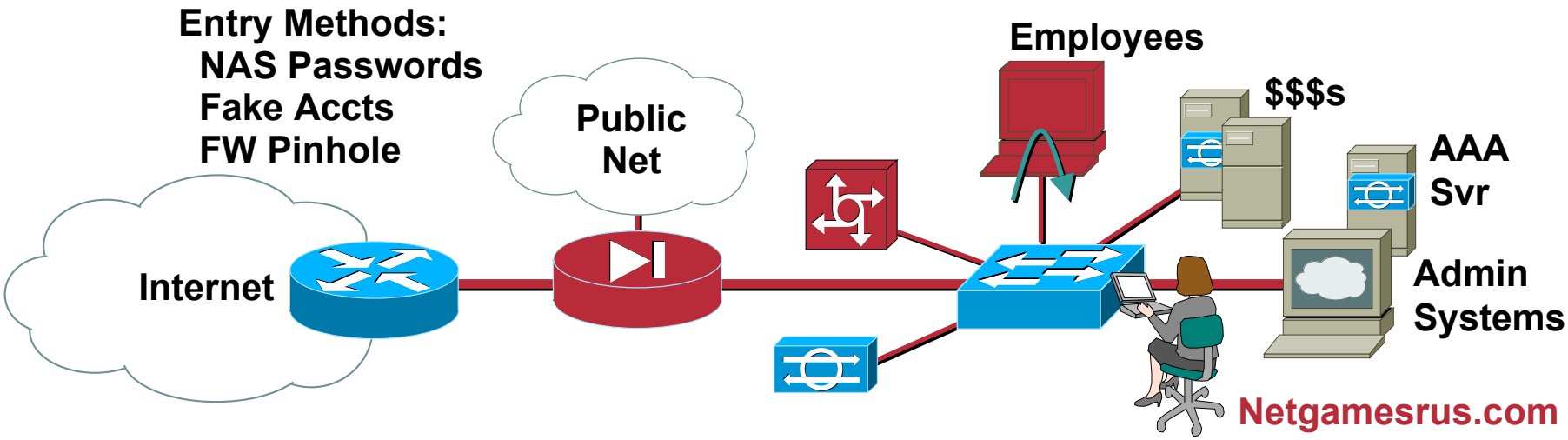
«Thanks for solving this problem, Roe.
I have been reading in firewall mailing lists and newsgroups about this very thing.»
--- the Pull, security geek, about STCPIO

«Your encryption plugins are good.»
--- Maw~, author of the IDEA and RC6 plugins

«Sweet Plugins! Now I have awesome encryption. Thanks for creating them.»
--- Christopher Witter, MCSE, MCP +Internet, ICIS, IIAE

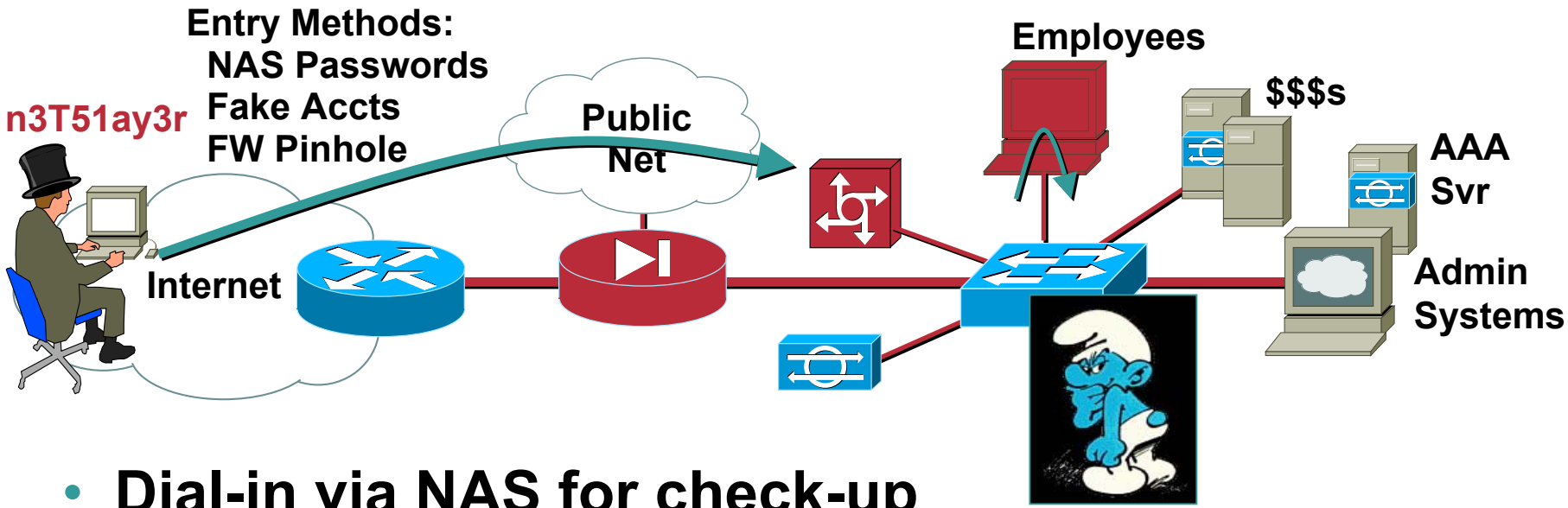
«I'll buy you a beer.»
--- Reid Fleming, member of cDc

Deja Vu



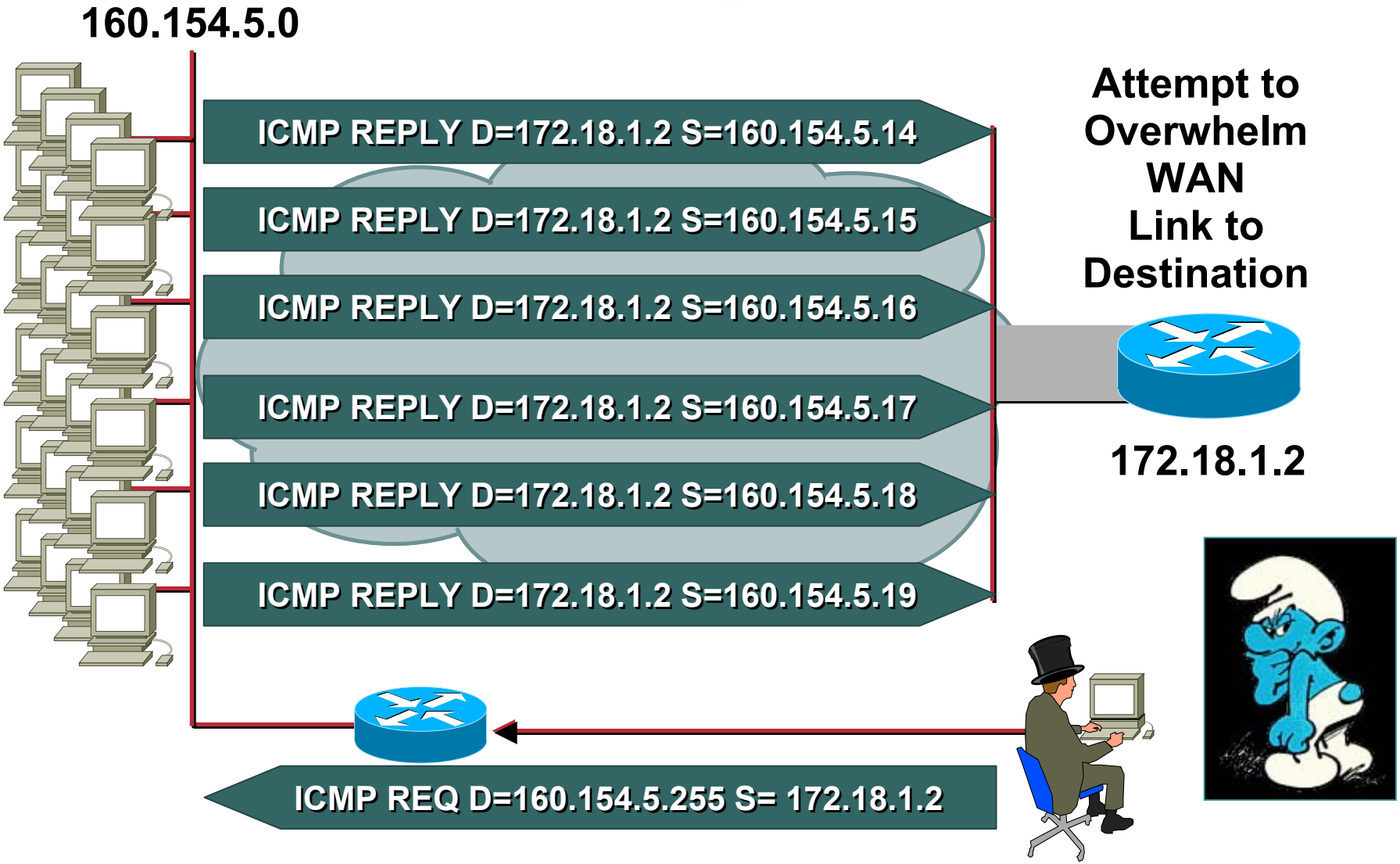
- Regular security virus scan catches BO2k
- Remove BO2k and install HIDS on key servers
- Start an audit to find out source of attack

Low Tech Attack

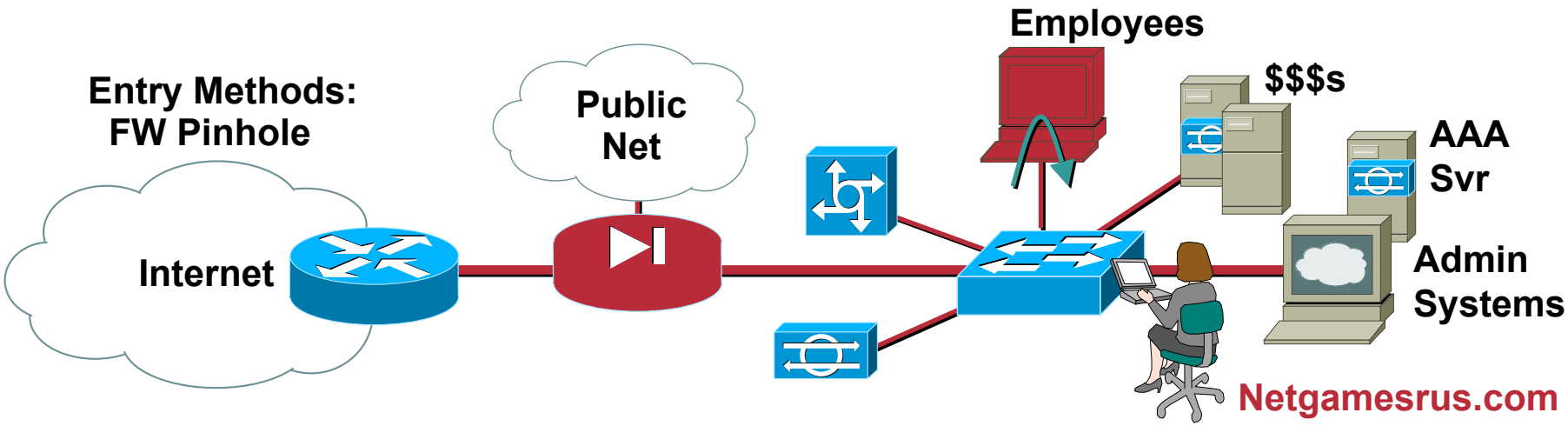


- Dial-in via NAS for check-up
- BO2k gone again?
- Feeling vindictive, launch smurf attack against public web server
- Smirk and logout

Smurf Attack



DoS Clean Up

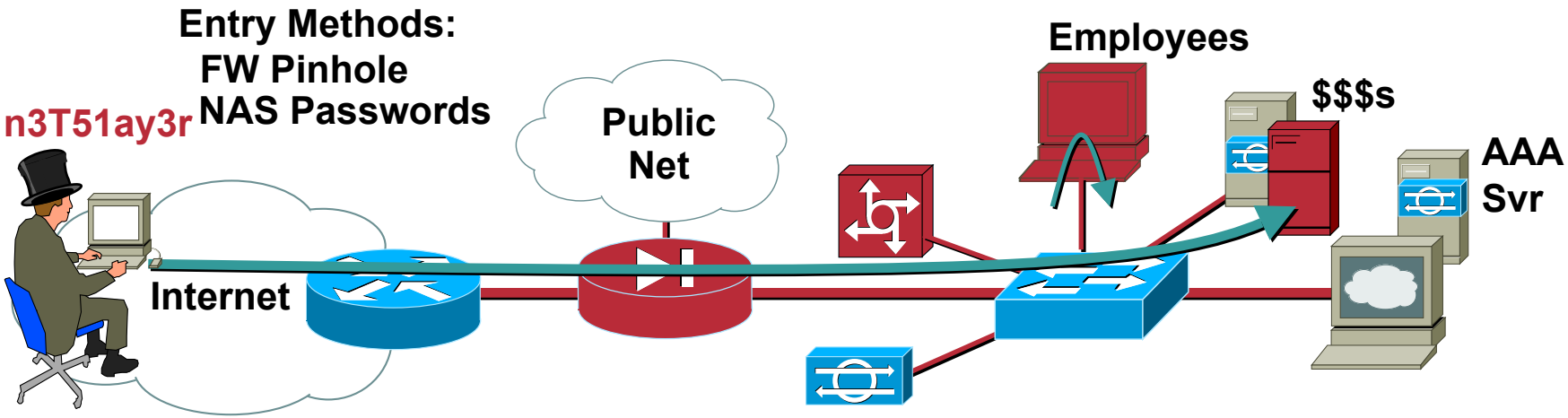


- Find and stop system generating broadcast echos
- Upgrade systems to prevent smurf attacks
- Host audit logs show bogus account in-use
- Purge bogus accounts from all systems (including AAA server) and expire all passwords

Lessons Learned: n3T51ay3r vs. Netgamesrus.com

- Bind hack—Mitigated by patches, NIDS, and HIDS
- New vulnerability—Mitigated by HIDS or sysadmin!
- Root kit—Mitigated by HIDS
- Attack tool download—Mitigated by outbound filtering on firewall
- IDS shun DoS—Stick—No shunning on NIDS in front of FW
- CGI script vulnerability—Mitigated by HIDS, patch practices, code reviews, and NIDS
- LC4 password crack
- BO2k—Mitigated by host virus scanning, HIDS & NIDS
- Rogue AP— Detected by AP tools and physical scan
- Internal smurf attack-mitigated by router and host modifications, NIDS can detect

Through the Firewall



- Bogus accounts inactive and passwords changed
- Using existing pinhole, compromise internal sales report Web server using NT IIS RDS vulnerability (SANS #4)
- Use sniffers to re-learn passwords
- Compromised sales server has access to customer database, with credit card info, via a SQL access script with auth credentials stored in the clear
- Obtain, post, and use credit cards via bogus SQL script using obtained authentication credentials (call it “fetchmydata”)

SANS W3: IIS RDS

W3 - IIS RDS exploit (Microsoft Remote Data Services)

W3.1 Description:

Microsoft's Internet Information Server (IIS) is the web server software found on most web sites deployed on Microsoft Windows NT 4.0. Malicious users exploit programming flaws in IIS's Remote Data Services (RDS) to run remote commands with administrator privileges.

W3.2 Systems impacted:

Microsoft Windows NT 4.0 systems running Internet Information Server have the /msadc virtual directory mapped are most likely vulnerable.

W3.3 CVE entries:

CVE-1999-1011

W3.4 How to determine if you are vulnerable:

If you are running an un-patched system, you are vulnerable.

An excellent guide to the RDS weakness and how to correct it may be found at:
http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2

W3.5 How to protect against it:

This is not fixable via a patch. To protect against this issue, follow the directions in the security bulletins:

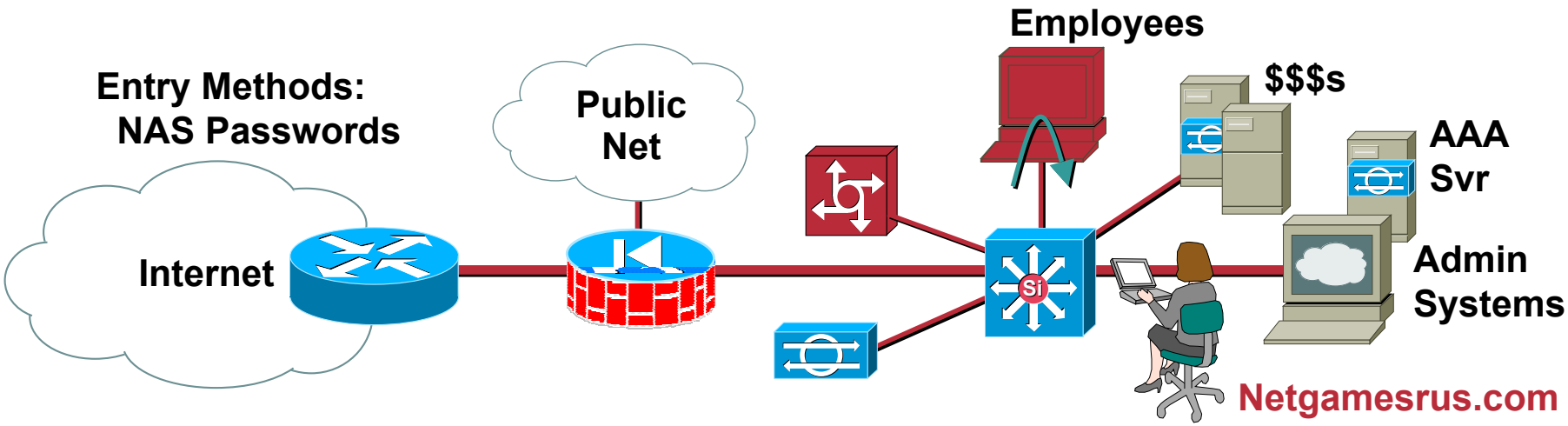
- http://support.microsoft.com/support/kb/articles/q184/3/75.asp
- http://www.microsoft.com/technet/security/bulletin/ms98-004.asp
- http://www.microsoft.com/technet/security/bulletin/ms99-025.asp

Beware Where You Store Credentials

Cisco.com

```
…
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
</head>
<body background="_themes/auto/autobkgd.gif" bgcolor="#666666" text="#FFFFFF"
link="#FFCC33" vlink="#CCCC99" alink="#CCCCCC"><!--mstheme--><font face="Arial,
Arial, Helvetica">
<p><img border="0" src="images/pod<%Response.Write
Application("sevt_podnumber")%>.gif" width="640" height="66"></p>
<p>
<%
On Error resume Next
openstr = "DRIVER={SQL Server}; server=192.168.0.10;
database=pubs;UID=pubs;PWD=password"
Set cn = Server.CreateObject("ADODB.Connection")
cn.Open openstr
sql = "SELECT sum(qty) FROM buys; "
…
```

Customers Upset = Big Reaction



- Customers unhappy with credit card posting and charges
- Audit of FW rules coincidentally removes pinhole
- Exhaustively patch internal servers and sprinkle more HIDS
- Partition internal network, upgrading to L3 switch, and setup ACLs to block access
- Add custom string in NIDS for calls to “fetchmydata”, the script that was used in attack

Layer 4 ACLs in Switches

- L4 access control in switches (e.g. CAT6k)
- ASIC/HW support important for Gig environments
- Logging, when available, is unwise at high data rates
  - On a CAT6k performance drops an order of magnitude
- Note access control is stateless
  - Ideal for L3 use
  - L4 multi-channel protocol filtering is hard and insecure (no state tracking)
- Stateful firewalls in switches are now available

The Needle in the Haystack

Cisco.com

```
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out permit icmp any any echo-reply
access-list out permit tcp any host 172.16.225.52 eq www
access-list out permit tcp any host 172.16.225.52 eq ftp
access-list out permit tcp any host 172.16.225.50 eq smtp
access-list out permit tcp any host 172.16.225.55 eq 22
access-list out permit udp any host 172.16.225.51 eq domain
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in permit icmp any any echo
access-list in permit udp host 10.1.11.50 host 172.16.225.51 eq domain
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.1.103.50 eq 15871
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq smtp
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq 20389
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq ftp
access-list in deny ip any 172.16.225.0 255.255.255.0
access-list in permit ip 10.0.0.0 255.0.0.0 any
```

Pinhole

Custom SQL NIDS String

Forward Lock Tearoff Find Check Help Context Start

General | Signatures

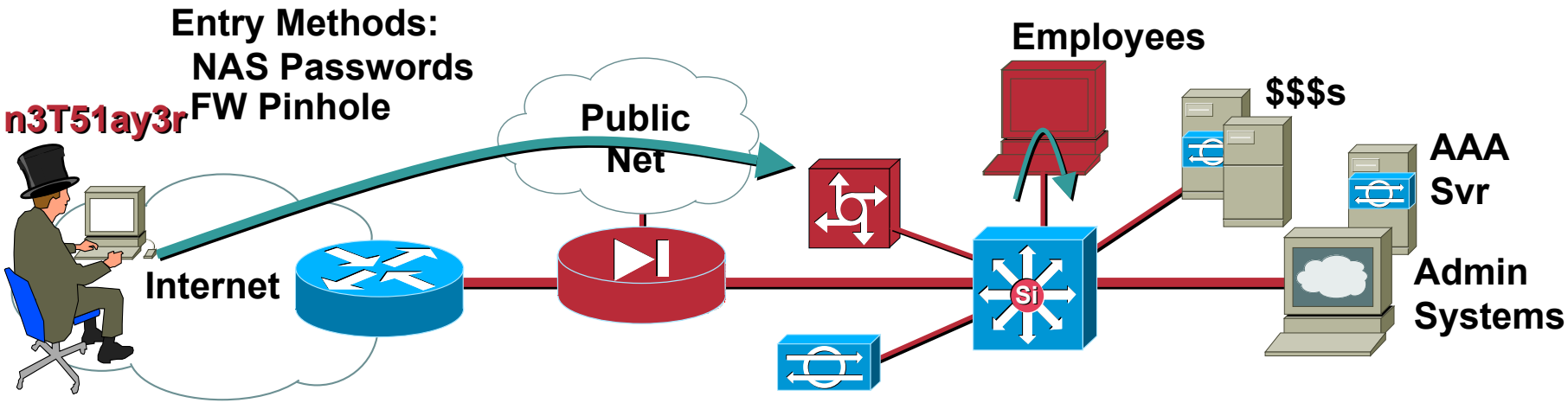
General Signatures | Connection Signatures | String Signatures | ACL Signatures

These are the String sub-signatures for the sensor.

String	Port	Direction	urrer	Severity	Enable	Actions
[+][ ]+[+]	23	To	1	Low	✓	None
[/]etc[/]shadow	23	To	1	High	✓	None
[+][ ]+[+]	513	To &	1	High	✓	None
[+][ ]+[+]	513	To	1	High	✓	None
[+][ ]+[+]	513	From	1	Low	✓	None
GET.*[.]printer[\x00-\xff]*[\n][Hh][C	80	To	1	High	✓	None
fetchmydata	80	To	1	High	✓	Block, TCP Reset,

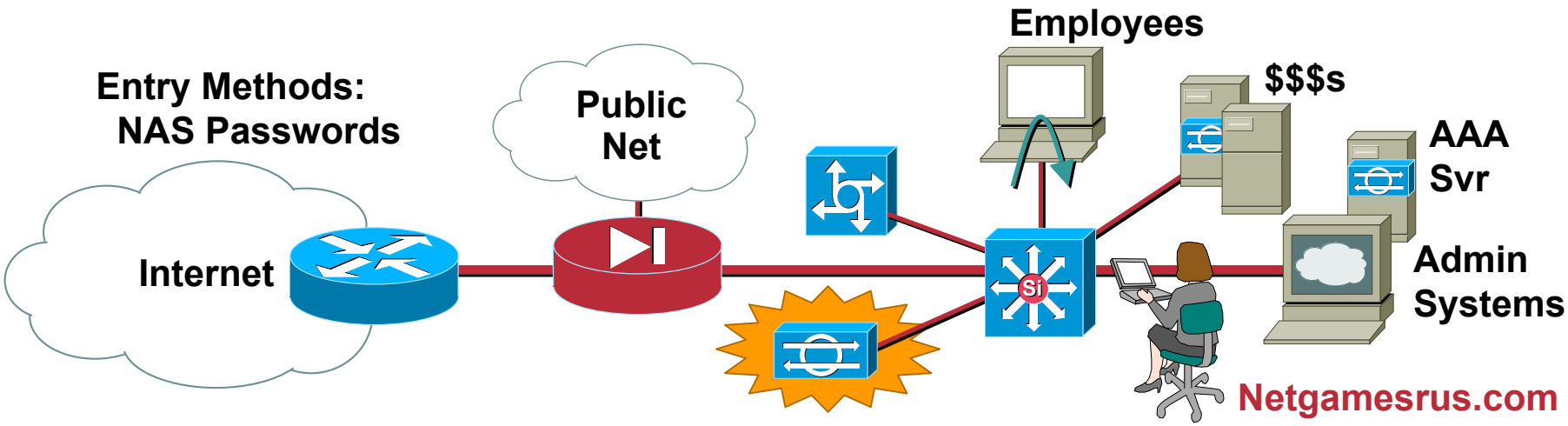
Add | Delete | Modify

Another Regular Check-Up



- Firewall pinhole is plugged
- Dial-in via NAS with cracked password
- Use sniffers to learn admin password, add back pinhole
- Start poking around the databases again, access script on internal server…where did it go?
- Ping several servers—some respond, others do not
- Start SLOW network mapping script to stay below NIDS's scan match signature timing then leave

We've Got a Live One!



- NIDS triggers on "fetchmydata" bogus script call (alarms ensue)
- Backtrack through access logs to determine who had the specific NAS IP at that time, initiate traceback
- *Sigh* another compromised password, time for OTP
- Jump host finally discovered via NIDS logs!
- Scripts, sniffers, and dsniff found, system taken out of service
- Add NIDS custom string for traffic destined to the old jump host IP
- Research dsniff, cry, then deploy SSH / SSL for management and improve L2 security

One Time Passwords (OTP)

- Commonly used for NAS, device mgmt, and remote access VPNs (don't rely solely on HW authentication)
- Mitigate eavesdropping and replay attacks
- Each password only useful once
- Synchronization between authentication server and client
- Agreement may be based on time, sequence, and a PIN
- Software and hardware-based

L2 Security

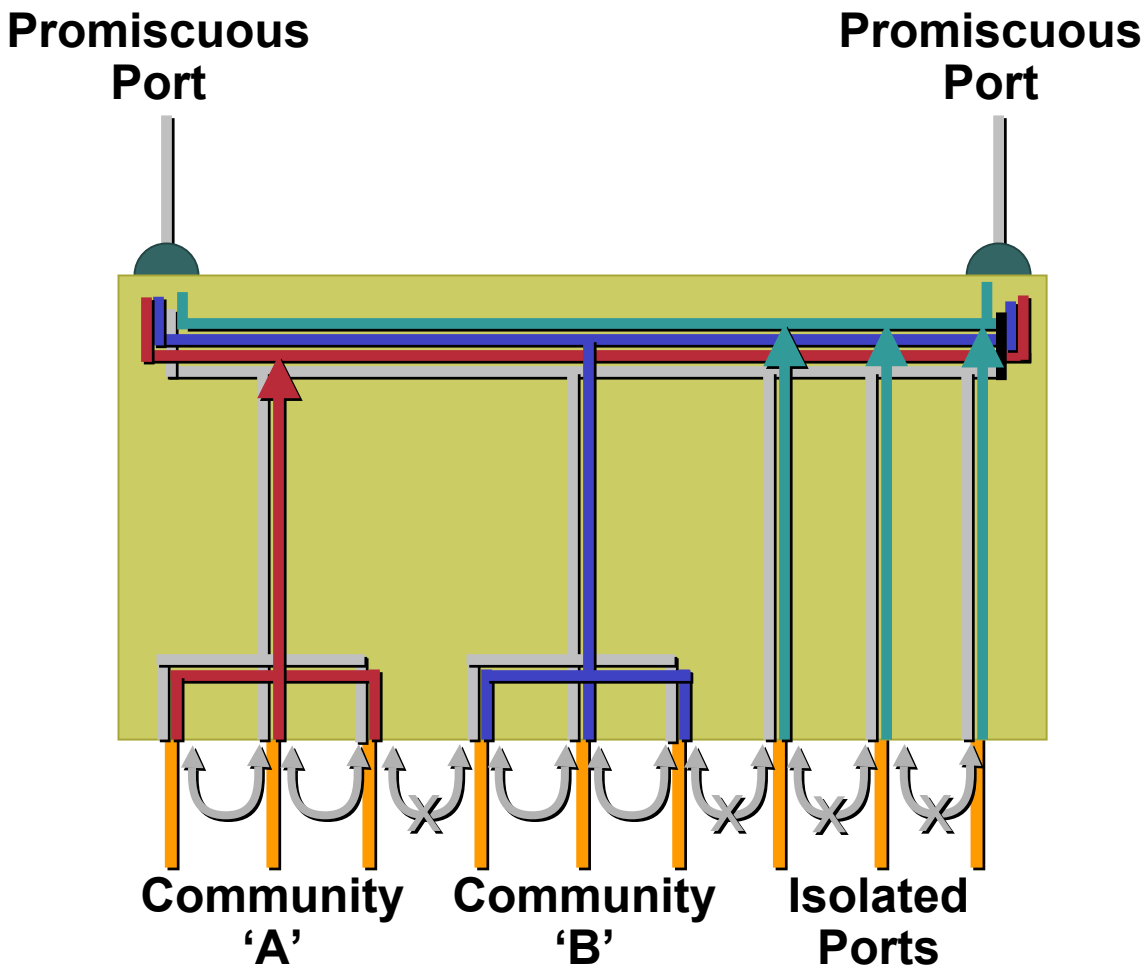
- Port security
- Static ARP
- ARPwatch
- Private VLANs
- 802.1X

Private VLANs

Cisco.com

Only One Subnet!

- Primary VLAN
- Community VLAN
- Community VLAN
- Isolated VLAN



Management Channel Security

- In-band in the clear
  - Optionally with strong authentication
- In-band secured
  - Application layer encryption (SSH, SSL)
  - Network layer encryption (IPSec)
    - Good for non config protocols
      - Syslog, TFTP, SNMP
- Out-of-band management
  - Strongest security
  - Beware topo sensitive NMS

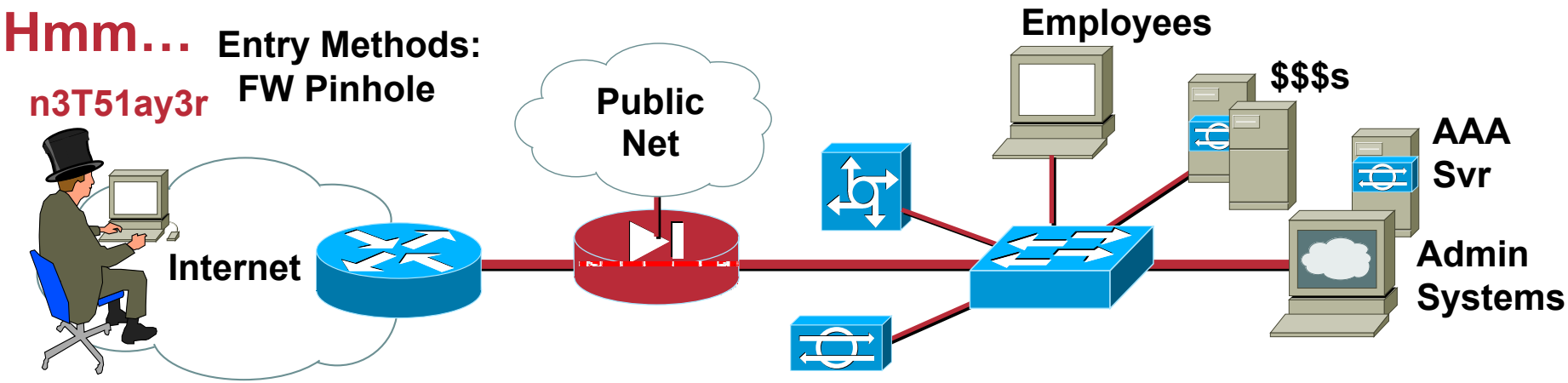
More Dsniff

p://packetstorm.securify.com/sniffers/dsniff/ Go

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

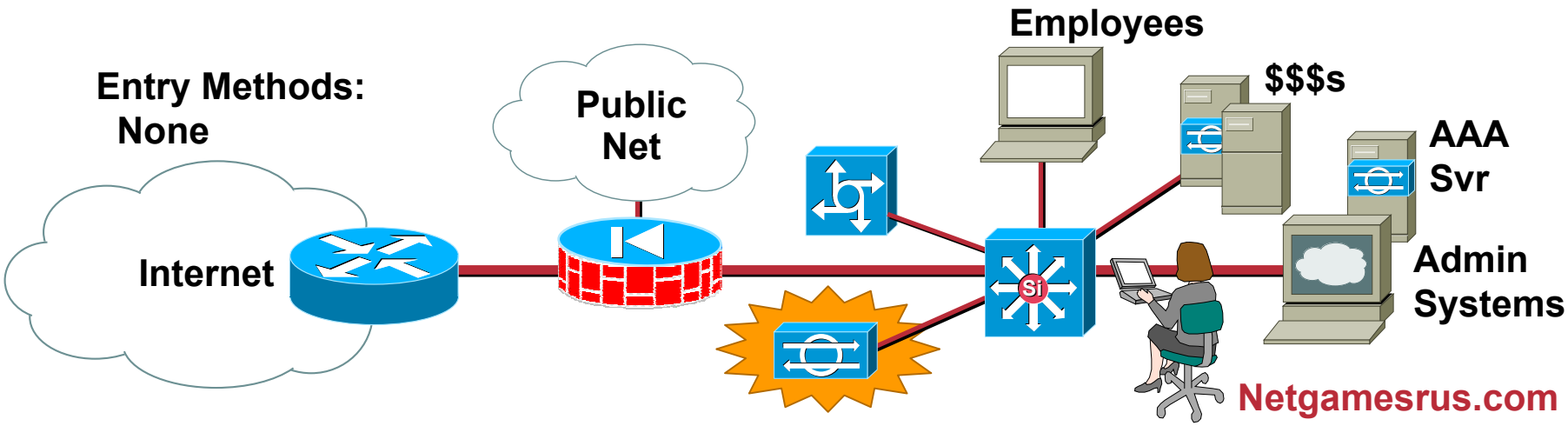
dsniff is a suite of utilities that are useful for penetration testing. It consists of the following programs: arpredirect intercepts packets from a target host on the LAN intended for another host on the LAN by forging ARP replies. findgw determines the local gateway of an unknown network via passive 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. webspy 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/~dugsong/. By Dug Song

Time to Check on Scan



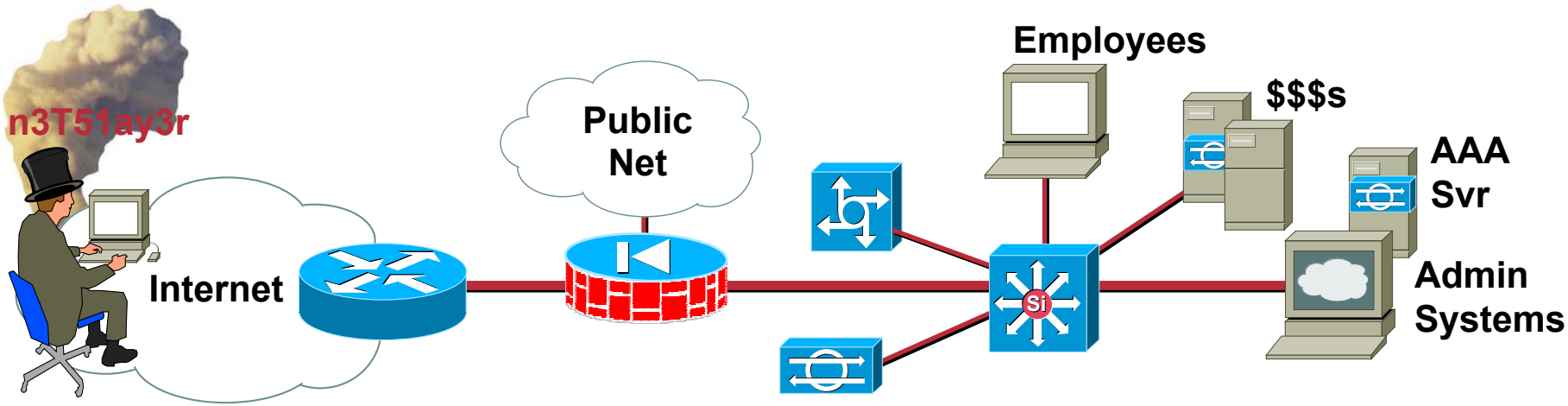
- After a period of time, try to gain access again
- Try NAS, prompted for PASSCODE??? Damn!
- Use pinhole to jump host, no response

They're Here!



- NIDS triggers on custom rule for jump host IP access
- IP was outside our range
- Check firewall rules, discover additional pinhole
- Fix firewall
- Start trace back to attacking IP—now we've got you!

Vengeance



- Detect trace back on launch-site firewall
- Queries from my target? School is now in session
- Since I don't have any way to get in

  "I say we take off, nuke the site from orbit. It's the only way to be sure."
- Launch DDoS

DDoS Reflection Attacks

Cisco.com

- Newer DDoS technique using TCP basics
- Similar to DNS reflection attack on register.com
- No requirement to compromise hosts
- Traffic looks normal
- Attack sources are legitimate and spread over the entire Internet
- Sites acting as reflector will likely not notice performance degradation
- No easy attack mitigation options
- RFC2827 PLEASE!!!!!

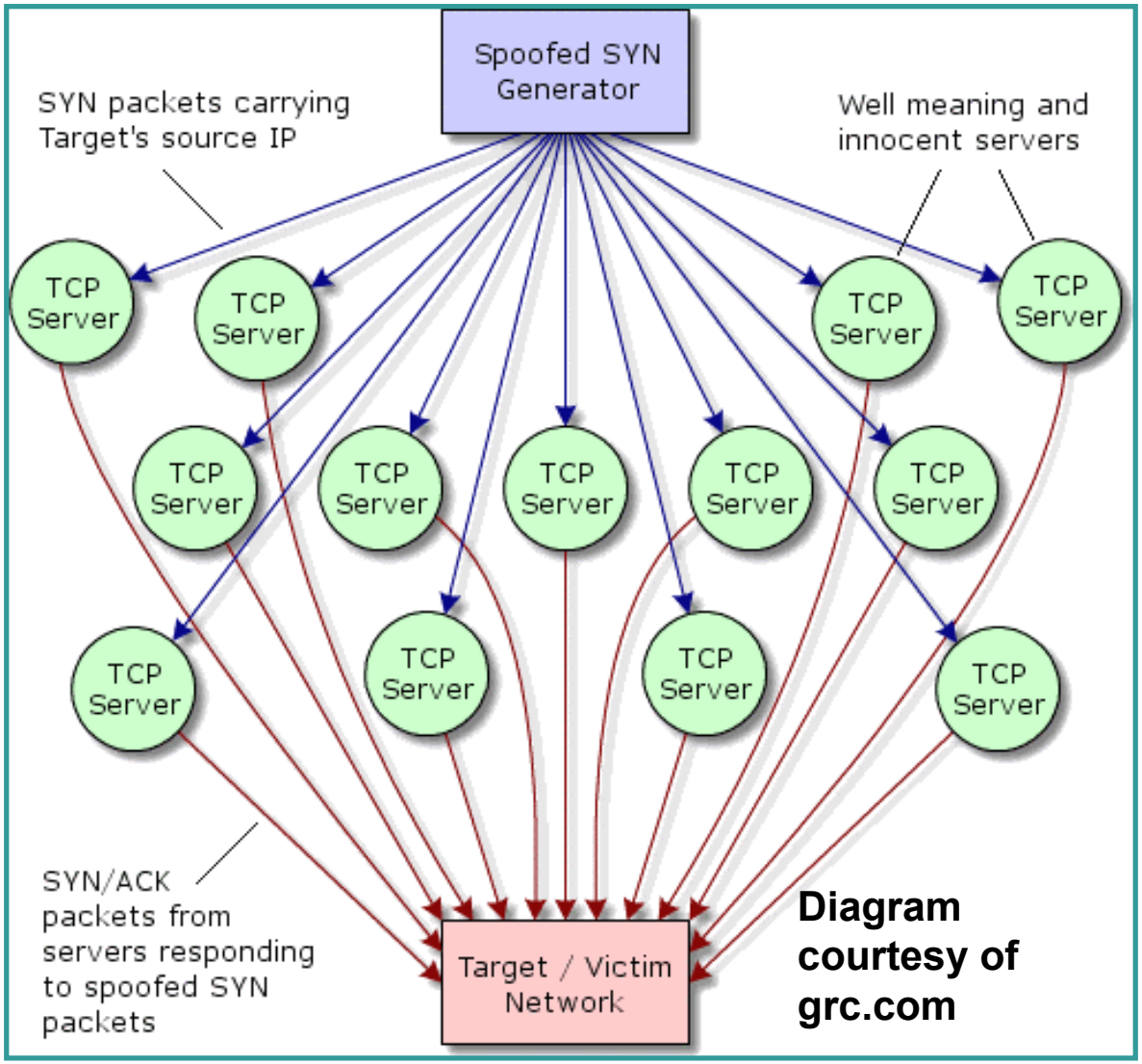
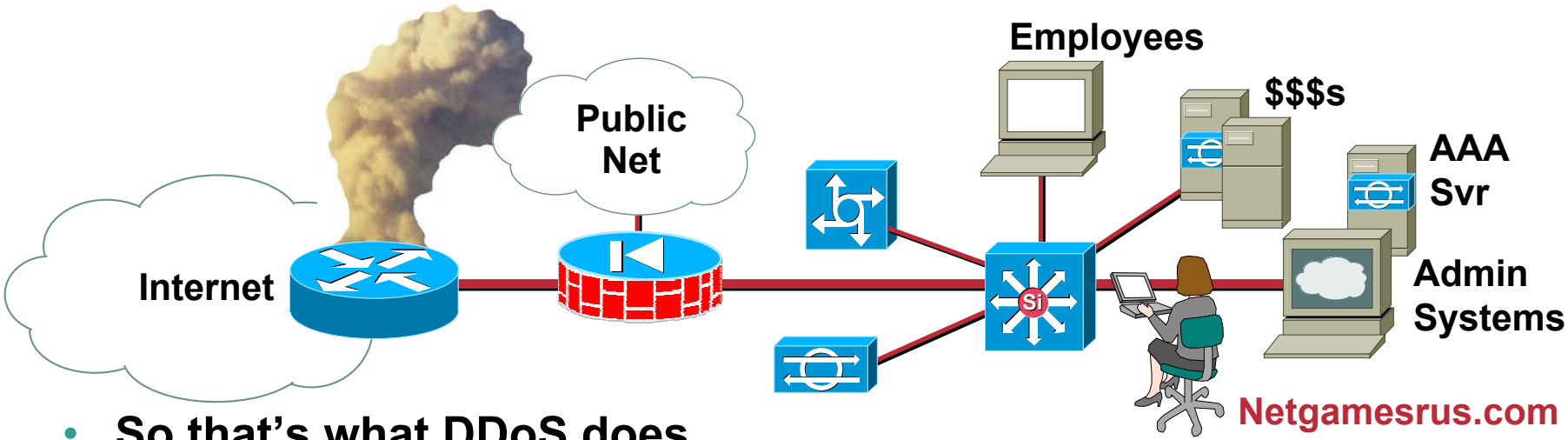


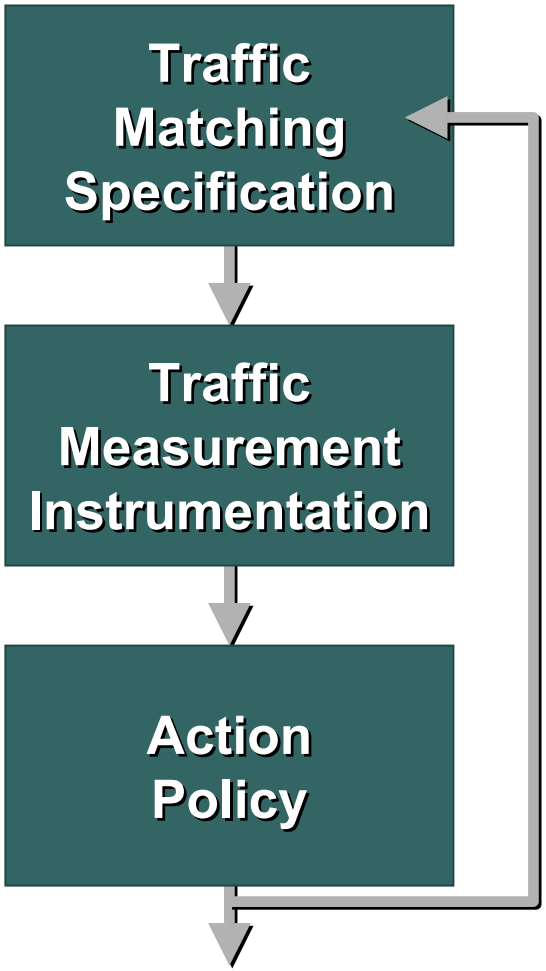
Diagram courtesy of grc.com

Oh My Goodness!



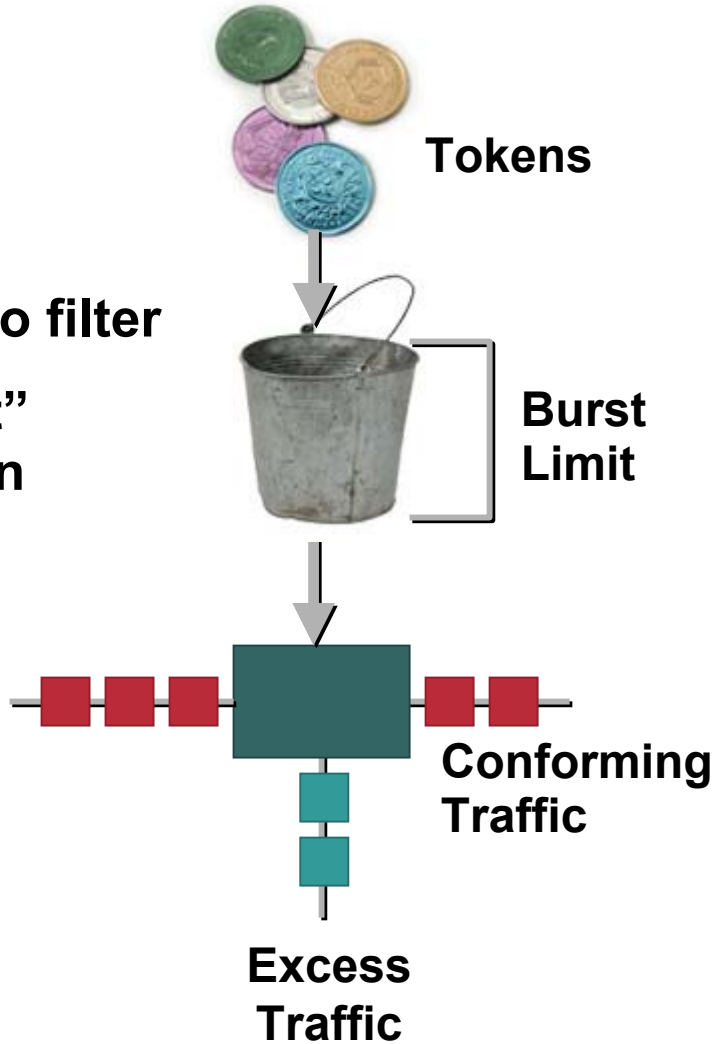
- So that's what DDoS does
- Research problem and call ISP
- Begin painfully long traceback process
- Request that ISP implement CAR (useful for some DDoS attacks)
- Reconsider edge architecture: Should we move our e-commerce elsewhere?
- Implement RFC 1918 and 2827 filtering
- Find and read SAFE White Papers plus attend SEC-201

Committed Access Rate



- Rate limiting
- Several ways to filter
- "Token bucket" implementation

Next Policy



CAR Rate Limiting

- **Limit outbound ping to 256 Kbps**

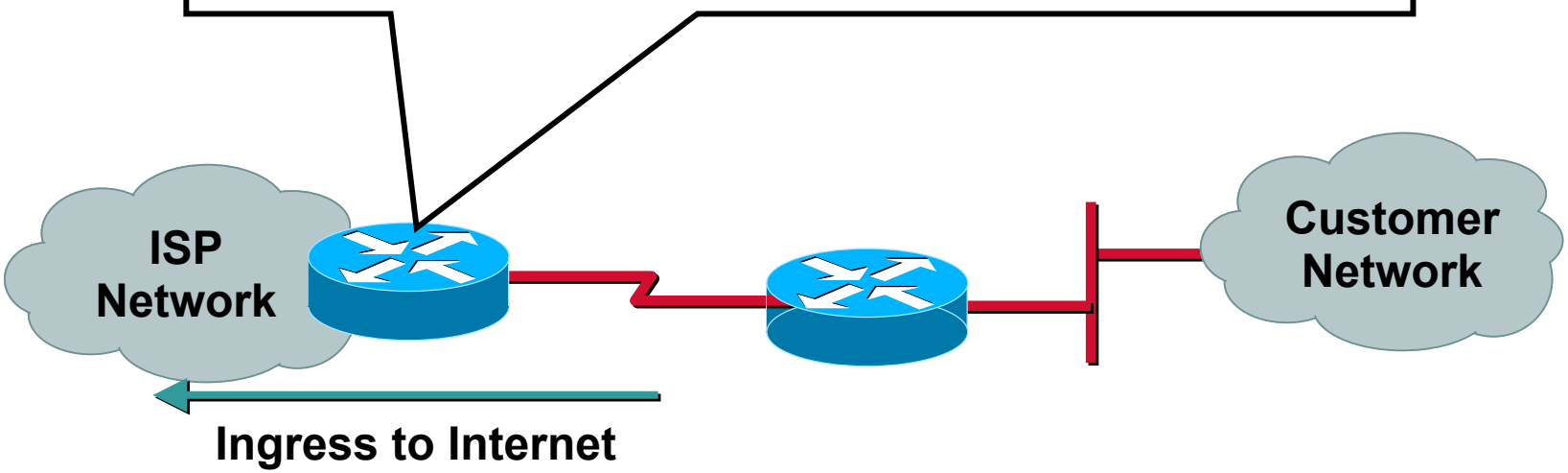
```
interface xy
    rate-limit output access-group 102 256000 8000 8000
        conform-action transmit exceed-action drop
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

- **Limit inbound TCP SYN packets to 8 Kbps**

```
interface xy
    rate-limit input access-group 103 8000  8000 8000
        conform-action transmit exceed-action drop
!
access-list 103 deny tcp any host 142.142.42.1 established
access-list 103 permit tcp any host 142.142.42.1
```

RFC 1918 Filtering

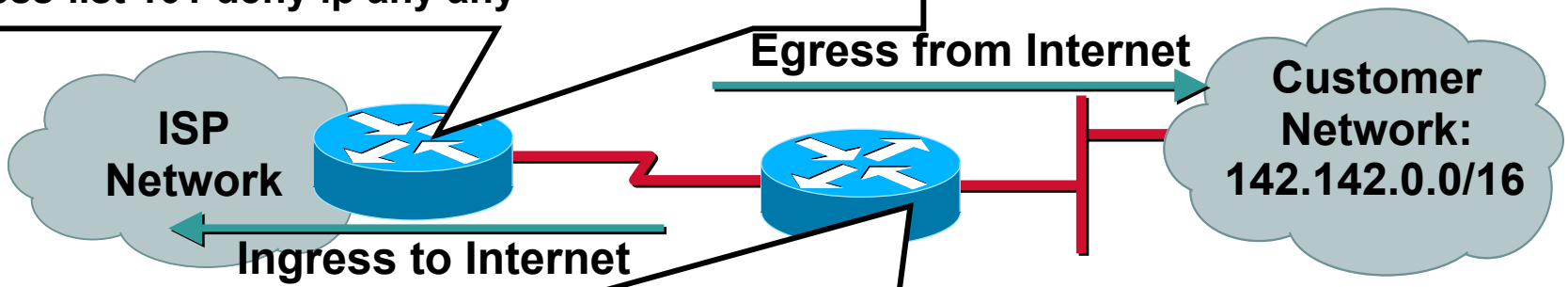

```
interface Serial n
  ip access-group 101 in
!
access-list 101 deny ip 10.0.0.0    0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0  0.15.255.255 any
access-list 101 permit ip any any
```



RFC 2827 Filtering


```
interface Serial n
  ip access-group 101 in
!
access-list 101 permit 142.142.0.0  0.0.255.255 any
access-list 101 deny ip any any
```

- Ingress packets must be from customer addresses




```
interface Serial n
  ip access-group 120 in
  ip access-group 130 out
!
access-list 120 deny ip 142.142.0.0  0.0.255.255 any
access-list 120 permit ip any any
!
access-list 130 permit 142.142.0.0  0.0.255.255 any
access-list 130 deny ip any any
```

- Egress packets cannot be from and to customer
- Ensure ingress packets are valid

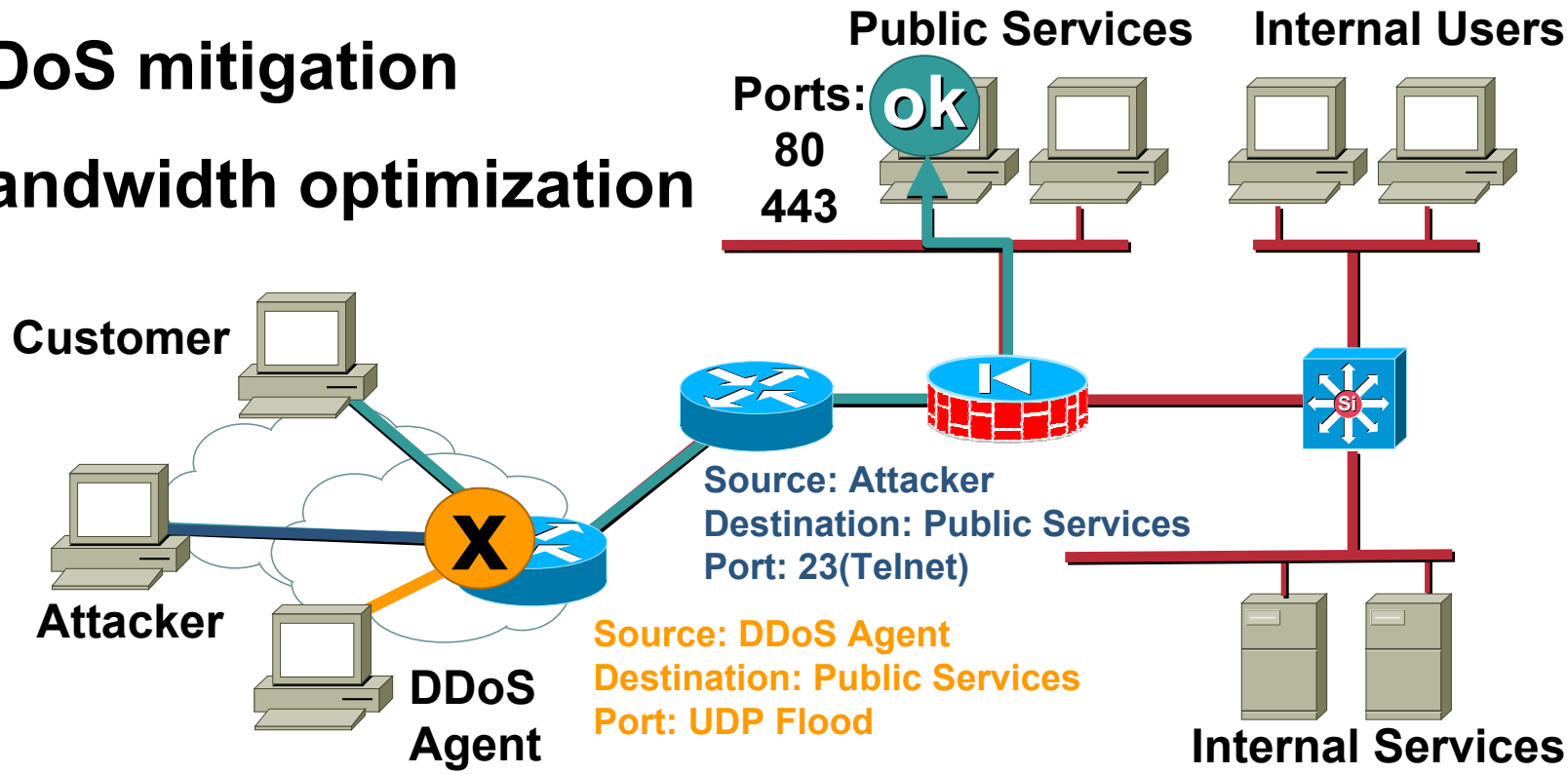
Verify Unicast Reverse-Path

- Mitigates source address spoofing by checking that a packets' return path uses the same interface it arrives on
- Best Implemented at your ISP
- Requires CEF
- Not appropriate where asymmetric paths exist

```
ip cef distributed
!
interface Serial n
  ip verify unicast reverse-path
```

Service Provider Filtering

- Best in e-commerce environments
- DDoS mitigation
- Bandwidth optimization



Lessons Learned: n3T51ay3r vs. Netgamesrus.com

- Bind hack—Mitigated by patches, NIDS, and HIDS
- New vulnerability—Mitigated by HIDS or VERY good sysadmins
- Root kit—Mitigated by HIDS
- Attack tool download—Mitigated by outbound filtering on firewall
- IDS shun DoS—Stick—No shunning on NIDS in front of FW
- CGI script vulnerability—Mitigated by HIDS, good patch practices,
  code reviews, and NIDS
- War dialing—Mitigated by one time passwords
- Internal jump host—Mitigated by local private VLANs

Lessons Learned: n3T51ay3r vs. Netgamesrus.com

- Dsniff/SMBRelay—Mitigated by L2 security practices and L3 filtering
- LC4 password crack—Assuming he gets the hashes somehow, its only a matter of time
- Internal mgmt access—Mitigated by OOB and encrypted management
- BO2k—Mitigated by host virus scanning, host IDS, NIDS, and private VLANs
- Rogue AP—Detected by AP Tools and Physical scans
- Internal smurf attack—Mitigated by router and host modifications, Private VLANs and L3 filtering, NIDS can detect
- NT IIS RDS vulnerability—Mitigated by HIDS and good patch practices
- SQL clear text auth problem—Mitigated by smart app developers
- DDoS—may be Mitigated by CAR and RFC 2827 & 1918 filtering, NIDS can detect

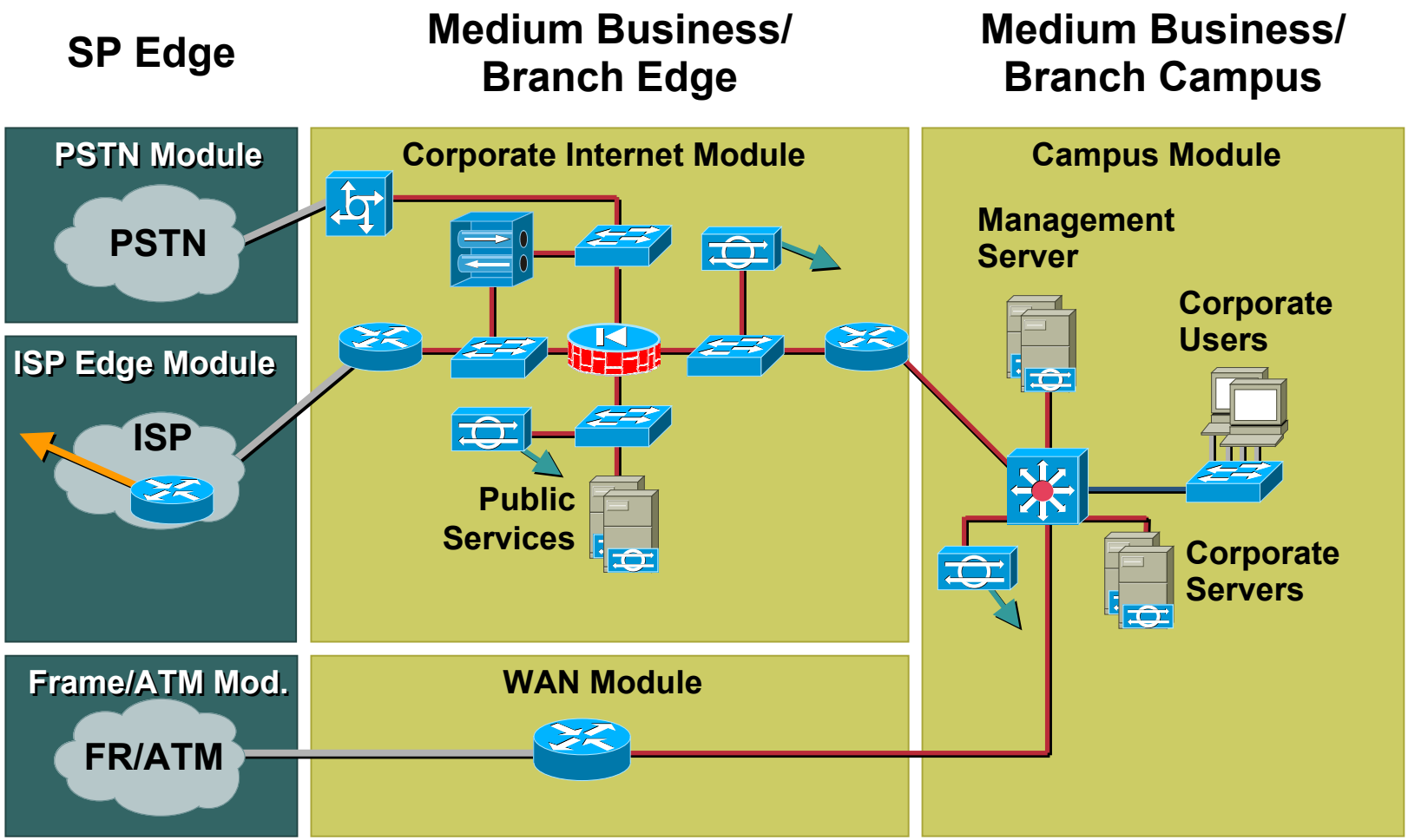
At the End of the Day

- **n3t51ay3r:**
  - Used several ISPs
  - Several favours
  - And lots of risk
- **Netgamesrus.com:**
  - Several admins and managers
  - $200K of equipment and software
  - Countless patching, re-imaging, password refreshes
  - Downtime and unhappy customers
  - PR nightmare

Is There a Better Way?

- **Comprehensive security architecture**
  - Have a security policy
  - Technologies work together as a system
  - No single point of failure
  - Overwhelming defense (barriers, trip-wires, reactions)
- **Skilled staff**
  - Prudent deployment and tuning of products
  - Limit how much is learned the hard way
- **Know the threat and your weaknesses**
  - Track threat tools and security technologies
  - Proactive approach to mitigation
  - Audit posture regularly
- **Cheaper to pay upfront than after the fact**
  - Stay employed and in business!

SEC 201: Teaser



Other Sessions of Interest – 1 of 2

- Design and Attack Mitigation, SEC-201
- Advanced Concepts in Security Threats, SEC-400
- Advanced Security Services for MPLS VPN, SEC-306
- Deploying IPSec with a PKI, SEC-302
- Deploying IPSec with QoS, SEC-303
- Deploying NAT, NSC-271
- Deploying Telecommuter IPSec VPNs, SEC-215
- Designing and Deploying Site to Site IPSec VPN, SEC-210
- Introduction to IPSec, SEC-112

Other Sessions of Interest – 2 of 2

- Introduction to Network Security, SEC-100
- PIX Firewall Internals, SEC-305
- Positioning VPN Technologies, SEC-111
- Security on Ethernet Switches, SEC-307
- Security on Routers, SEC-211
- Surviving a DoS Attack, SEC-301
- The Security of MPLS VPN, SEC-214
- Understanding & Deploying IDS, SEC-204
- Understanding Firewall Architectures, SEC-205
- Understanding Identity Management, SEC-113

Further Reading

Cisco.com

- http://www.cisco.com/go/safe
  - www.cisco.com/go/security
  - www.cisco.com/go/evpn
  - www.cisco.com/go/securityassociates
- Networking Professionals Connection (forums.cisco.com)
- Improving Security on Cisco Routers
  - http://www.cisco.com/warp/public/707/21.html
- Essential IOS Features Every ISP Should Consider
  - http://www.cisco.com/warp/public/707/EssentialIOSfeatures_pdf.zip
- Increasing Security on IP Networks
  - http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2016.htm

Network Security: Risk and Threat Model

Session SEC-200

Please Complete Your Evaluation Form

Session SEC-200

CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATION