

# Penetrating Firewalls

*Presented by*

Sheetal Joseph

# Road Map

- Public information leakage (passive recon).
- Fingerprinting a firewall type (active recon)
- Firewalk
- Paratrace
- Loki attack
- Reverse www shell

# Public Information Leakage

Company name: BankofMumbai

Location: xyz, Mumbai

Job Category: Network Administrator

Skills: Working knowledge of Microsoft NT Server, Windows XP, Microsoft ISA.proxy and HP Openview

Cisco PIX, Juniper SSL VPN, Juniper Netscreen, 802.11 wireless devices

# Public Information Leakage

```
From: "Rob Y." <rcbert.yung@1-3com.com>
Newsgroups: comp.security.firewalls
Subject: Symantec Firewall + RSA/ACE
Date: Sun, 20 Mar 2005 15:35:39 -0500
Organization: Aioe.org NNTP Server
Lines: 39
Message-ID: <d1kmqt$a1f$1@domitilla.aioe.org>
NNTP-Posting-Host: /3tD4wGQ1UxhR/fNpDZbmA.domitilla.aioe.org
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit
X-Complaints-To: abuse@aioe.org
NNTP-Posting-Date: Sun, 20 Mar 2005 20:35:42 +0000 (UTC)
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.2) .
```

Hi,

I have a server in a DMZ off of my Symantec Enterprise Firewall v7.04. On this server I've installed the new RSA/Agent for Windows v6.0. My RSA/Ace 6.0 server is behind the private interface of my firewall in a different subnet. When I do the "direct authentication test" via the RSA test tool on the DMZ server, I can contact the ACE server fine, however the authentication keeps failing with "Invalid passcode" (ACE log). Some background:

# Fingerprinting Using Default Ports

- Checkpoint FW-1
  - tcp/256, tcp/264, tcp/18264
- Symantec v8.0, SGS 5400)
  - tcp/2456
- Smoothwall
  - tcp/81, tcp/441



# Traceroute, tracert

Tracing route to visualroute.com [192.41.43.189]  
over a maximum of 30 hops:

```
 1  89 ms  87 ms  87 ms  199.70.3.58
 2  90 ms  95 ms  90 ms  199.70.3.49
 3 100 ms  90 ms  90 ms  gbr5-p21.n54ny.ip.att.net [12.122.253.245]
 4  90 ms  90 ms  90 ms  gbr3-p90.n54ny.ip.att.net [12.122.5.114]
 5  90 ms  90 ms  95 ms  ggr1-p370.n54ny.ip.att.net [12.123.1.125]
 6 110 ms 110 ms 115 ms  att-gw.ny.verio.net [192.205.32.174]
 7 115 ms 110 ms 115 ms  p4-1-3-0.r01.chcgil01.us.bb.verio.net [129.250.2.14]
 8 125 ms 110 ms 110 ms  p4-6-0.r00.chcgil01.us.bb.verio.net [129.250.2.253]
 9 135 ms 140 ms 135 ms  p4-4-0.r00.dllstx01.us.bb.verio.net [129.250.4.89]
10 140 ms 140 ms 165 ms  p4-1-0-0.r01.dllstx01.us.bb.verio.net [129.250.3.74]
11 200 ms 200 ms 200 ms  p1-0-0-0.r01.oremut01.us.bb.verio.net [129.250.2.41]
12 204 ms 200 ms 200 ms  pvu1.vwhpvu1.verio.net [129.250.29.202]
13 200 ms 195 ms 200 ms  visualroute.com [192.41.43.189]
```

Trace complete.

# Firewalk

- Finds the *open ports* on a Firewall.
- Sends TCP or UDP packets with an IP TTL evaluated to expire just one hop past the firewall.
- If the firewall allows the traffic in, then it will send the packets to target where the TTL will get zero and the target will elicit a TTL exceeded on transit back to attacker.
- If the firewall does not allow the traffic in, then we will not see any packet back which means the port is closed.

# Paratrace

- Paratrace can identify routing devices behind a stateful packet firewall, even if they have been network address translated.
- Utilises the way routers work on the Internet and therefore is not an actual coding error on the vendor's behalf, but a general weakness in the design of IPv4.
- The systems affected by this are any routing devices that comply with the IPv4 RFC's.
- The protocols utilised in the exploit are TCP and ICMP.

# DOD Standard – Transmission Control Protocol

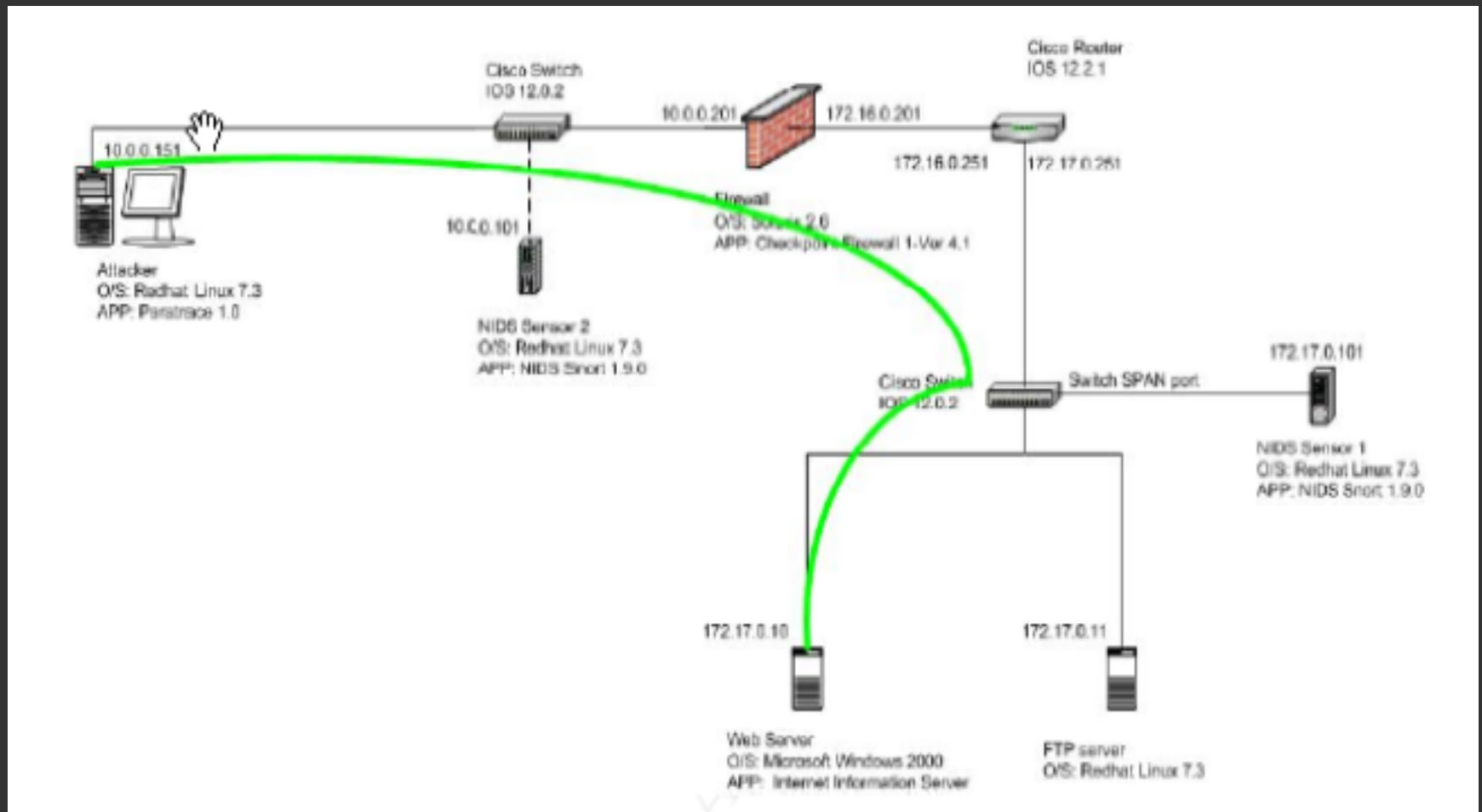
## 2.6. Reliable Communication

When the TCP transmits a segment, it puts a copy on a retransmission queue and starts a timer; when the acknowledgement for that data is received, the segment is deleted from the queue. If the acknowledgement is not received before the timer runs out, the segment is retransmitted (DOD Standard TCP, Section 2.6)

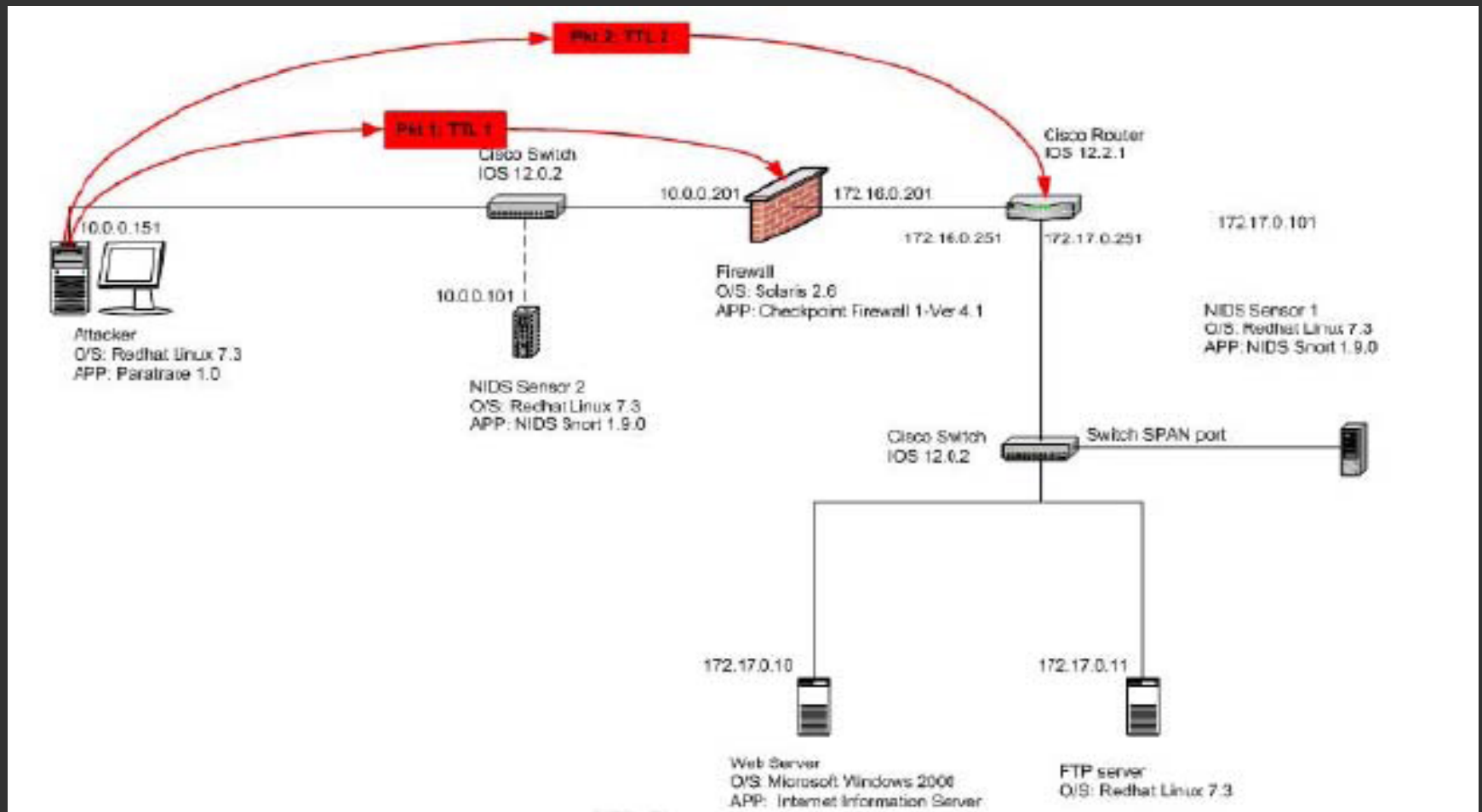
# Summary of attack

1. Attacker runs Paratrace program with the target of the web server
2. Attacker then connects to web server
3. The Paratrace program creates duplicates of the TCP packets and sends them onto the target network. These packets have low TTL values.
4. Routing devices that see the TCP packets with TTL 1, decrement the value to 0, drop the packet and send an ICMP "Time Exceeded" message back to the originator of the TCP packets, the attacker.
5. Attacker receives the ICMP messages and creates a map of the internal network.

# Step 1 – Establish Connection with Web Server



# Step 2 - Paratrace Goes Active



# Tcpdump Trace

20:43:16.001112 172.17.0.10.80 > 10.0.0.151.1084: . ack 9 win 10136 (DF)  
(ttl 247, id 21699, len 52)

20:43:16.001674 172.17.0.10.80 > 10.0.0.151.1084: P 43:73(30) ack 9 win  
10136 (DF) (ttl 247, id 21700, len 82)

20:43:16.002595 10.0.0.151.1084 > 172.17.0.10.80: . ack 73 win 5840 (DF)  
(ttl 64, id 50294, len 52)

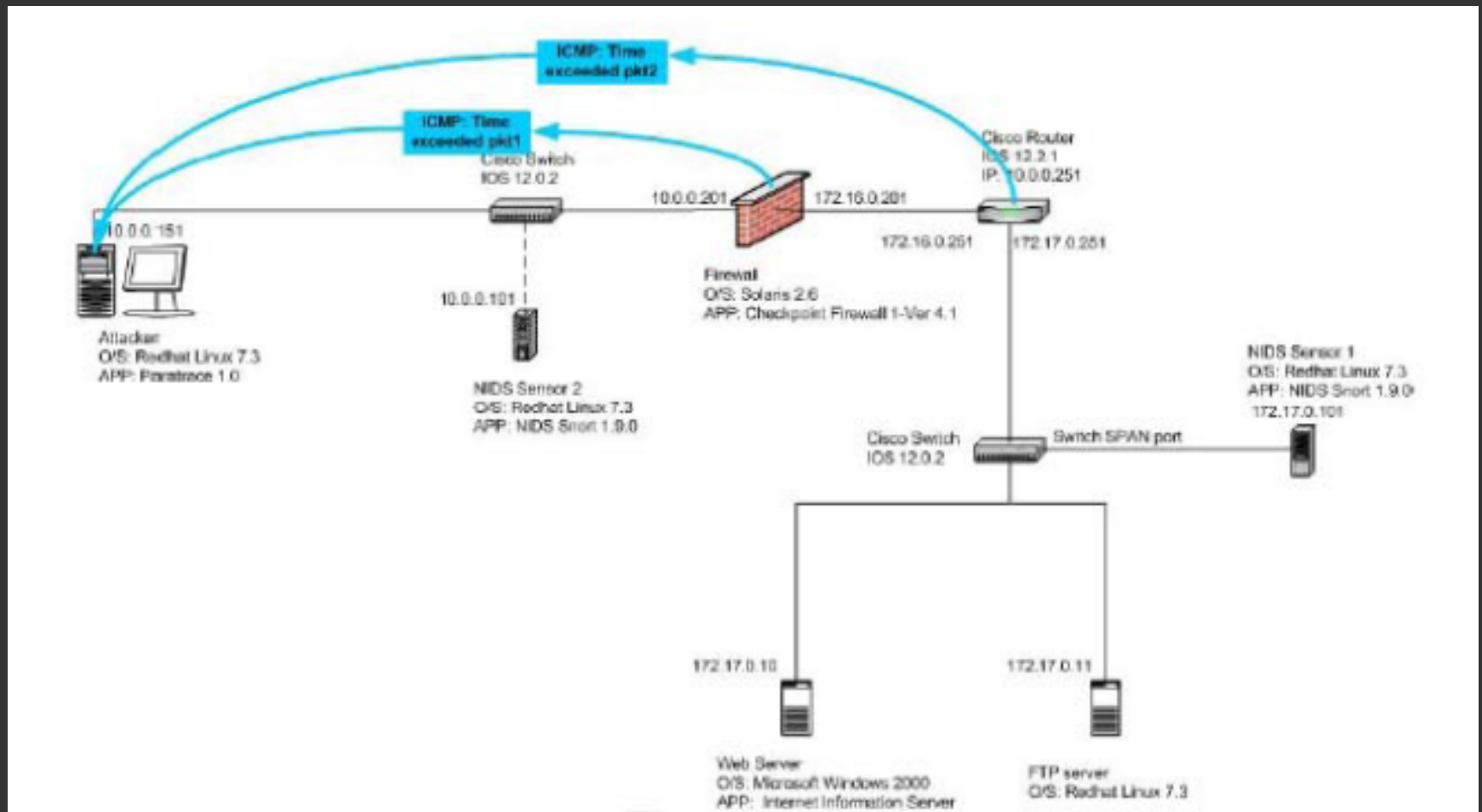
20:43:16.031099 10.0.0.151.1084 > 172.17.0.10.80: . ack 43 win 10136 (DF)  
[ttl 1] (id 1, len 52)

20:43:16.031497 10.0.0.201 > 10.0.0.151: icmp: time exceeded in-transit (ttl  
255, id 50784, len 56)

20:43:16.044021 10.0.0.151.1084 > 172.17.0.10.80: . ack 43 win 10136 (DF)  
(ttl 2, id 2, len 52)

20:43:16.044686 150.122.58.249 > 10.0.0.151: icmp: time exceeded in-transit  
(ttl 254, id 34338, len 56)

# Step 3 - Paratrace Collates ICMP Returns



# Loki

- ❑ Loki exploits the covert channel that exists inside of ICMP\_ECHO traffic.
- ❑ Arbitrary information tunneling in the data portion of ICMP\_ECHO and ICMP\_ECHOREPLY packets.
- ❑ We can encapsulate (tunnel) any information we want.

# Reverse www

- A program is run on the internal host, which spawns a child every day at a special time.
- Child executes a local shell and connects to the hacker via a http request with a ready signal
- The legitimate answer of the hacker is the commands the child would execute on its machine in the local shell

# Summary

