University of Windsor
thinking forward

INTRUSION DETECTION SYSTEM

INTRUSION DETECTION AND PREVENTION

using SAX 2.0 and WIRESHARK

Cain & Abel 4.9.35

Supervisor Dr. Akshai Kumar Aggarwal
Director School of Computer Sciences
University of Windsor
Presented by Faisal Mahmood
Graduate Student
School of Computer Science
University of Windsor
Class Project for 30-60-564

Content

INTRODUCTION

What is Intrusion ?

- There are quite a few factors that dictate how safe the data is on your computer. In defining "safety", we can either talk about it being safe from virus attack, safe from system damage, or safe from intrusion.

- **Intrusion**, the act of someone that you don't know, who gains access to your computer without your permission, is on the rise.

- This is really a **big concern** and bad news for computer users as they always want to make it sure that their important data is safe from intruders.

INTRODUCTION

Why Intrusion is done ?

- Hackers are more interested in gaining access to your computer and using it for other purposes.

- If a hacker can gain access and use your Internet access, then they can use your machine to launch other attacks on other computers and keep themselves pretty well hidden.

- Hackers have control of thousands of machine and can use them any time for their attacks. We experience many such events almost daily. Recent one was on Twitter, yahoo mail server and also on White House official web site.

INTRODUCTION

Why intrusion is done ?

- There are certain applications that take days to months to run a series of processes on even the fastest computer. But if a hacker can gain access to 1000 computers and utilize their combined processing power, a process that would take a month on a single computer could complete the operation in less than an hour.

- Mostly intrusion is to retrieve the special data from the system or make the availability of any service difficult or completely shutdown. Big Ecommerce businesses portals suffer the most in the sense of revenue lose for those types of intrusion like amazon.com experienced recently

INTRODUCTION

Ways to minimize the intrusion

- **Updating the Operating system**

  The later operating systems have better security built into them than the earlier ones

- **Firewalls**

  Simply put, a firewall is a piece of software that stops intruders from accessing your computer. It sets up rules that allow you to access the Internet, but doesn't allow others to access your computer from the outside.

- **Intrusion by Trojans and other funky animals**

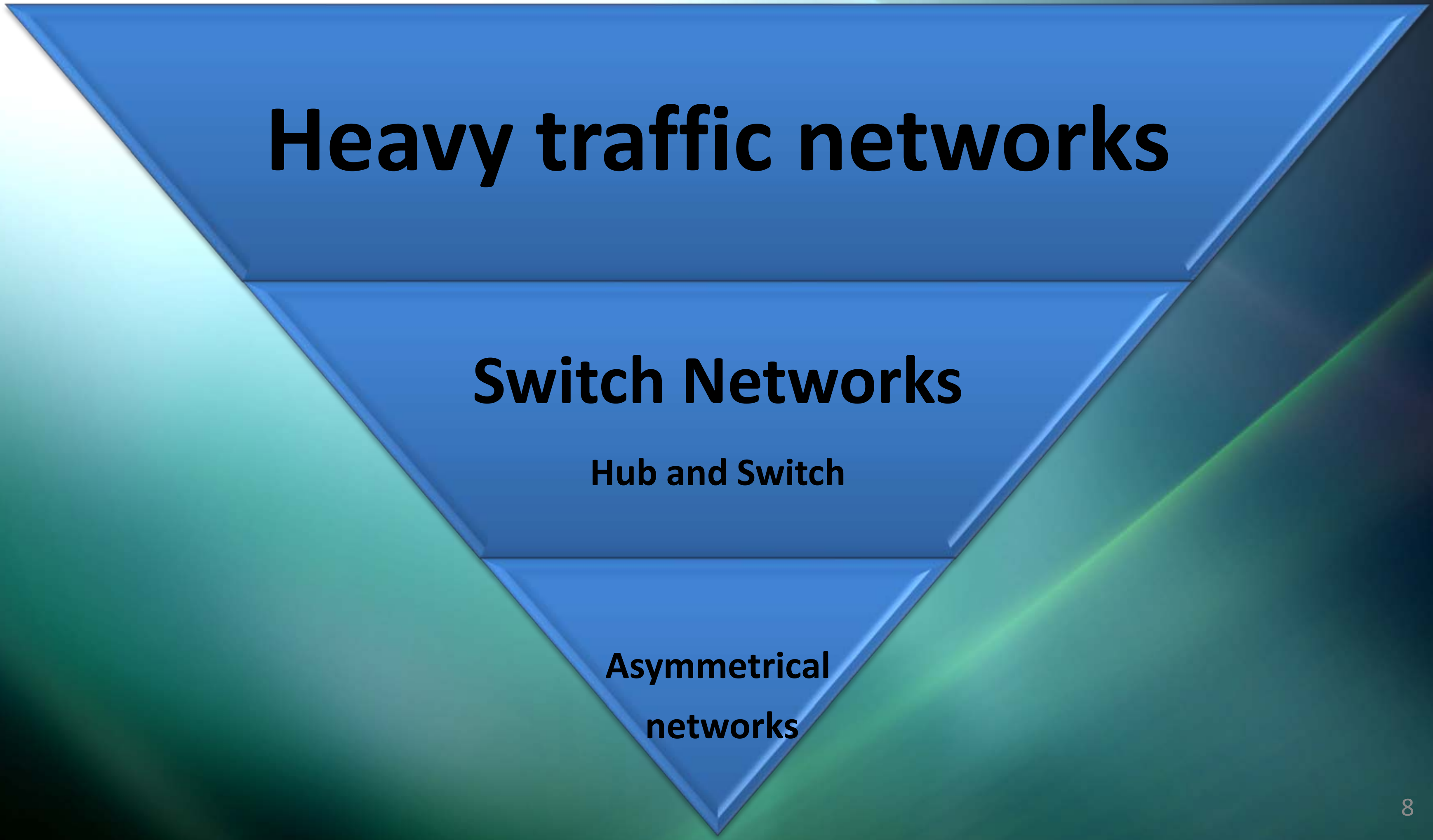
  Comes from the inside out.

INTRODUCTION

How the Intrusion detection system works ?

- An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling computer systems, mainly through a network, such as the **Internet**
- Intrusion detection can be perform by implementing some important tasks on the **host computer** and **network** itself like real time **traffic analysis** and **packet login** on the IP networks
- IDS can be composed of several components: **Sensors** which generate security events, a **Console** to monitor events and alerts and control the sensors, and a **central Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received

nIDS The environments that are especially susceptible to missed intrusions are



Heavy traffic networks

Switch Networks

Hub and Switch

Asymmetrical networks

nIDS

Heavy traffic networks

- In these environments the high amount of traffic overloads the IDS sensor and intrusion traffic is missed.

  100 % intrusion detection is a big challenge.

- There are two mainstream versions of a nIDS available on the market:

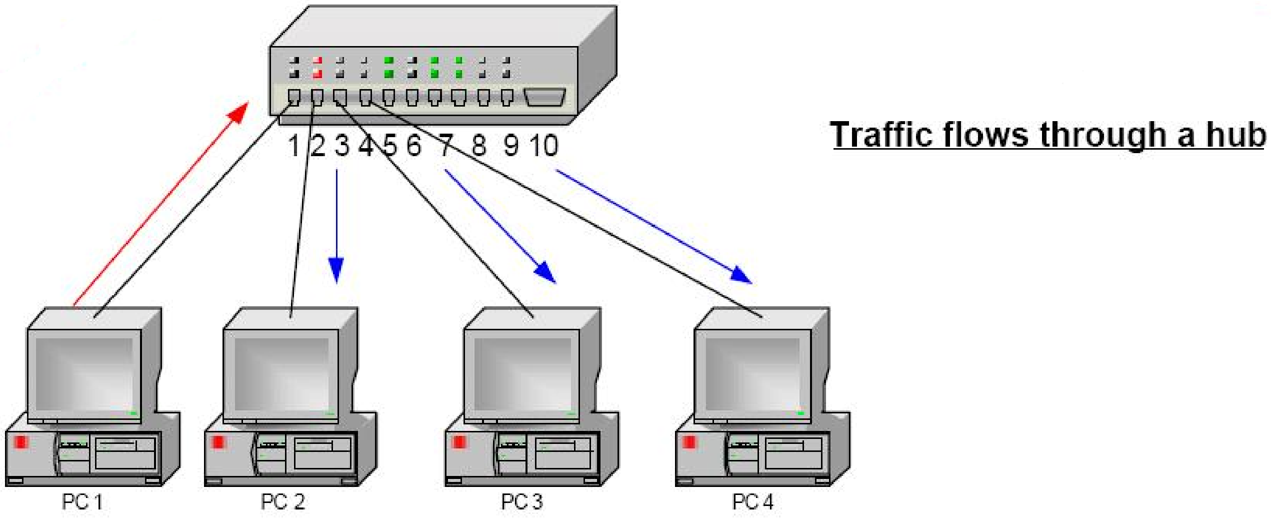
❑ **100MB sensor** (capable of monitoring up to 100MB/s)

❑ **Gigabit sensor** (capable of monitoring anywhere from 300MB to 800MB).

nIDS

Hub Networks

- A nIDS is designed to monitor individual segments, such as off a ***hub***. *H*ub is a device that uses *broadcast technology*.



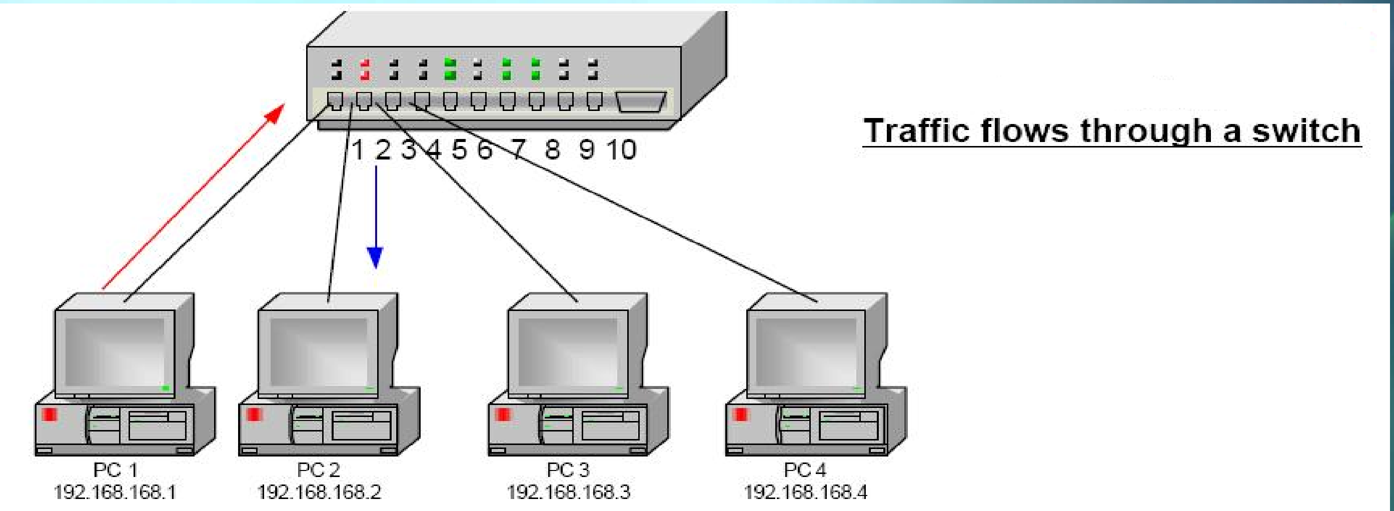
Traffic flows through a hub

PC1 wants to communicate to PC2, but the request is broadcast on all ports,
so if PC4 was used as a nIDS it would hear all communications

nIDS

Switch Networks

- A switch understands Layer 3 & 4 information, and therefore knows the IP address/s of the devices connected to it.



A switch understands Layer 3 or 4 information (i.e. IP address), so when PC 1 sends a request to PC 2, the switch knows that the packets are deemed for 192.168.168.2 and only sends it there. A nIDS seated on PC 4 would not be able to "hear" the conversation, so not be able to monitor for attacks

nIDS

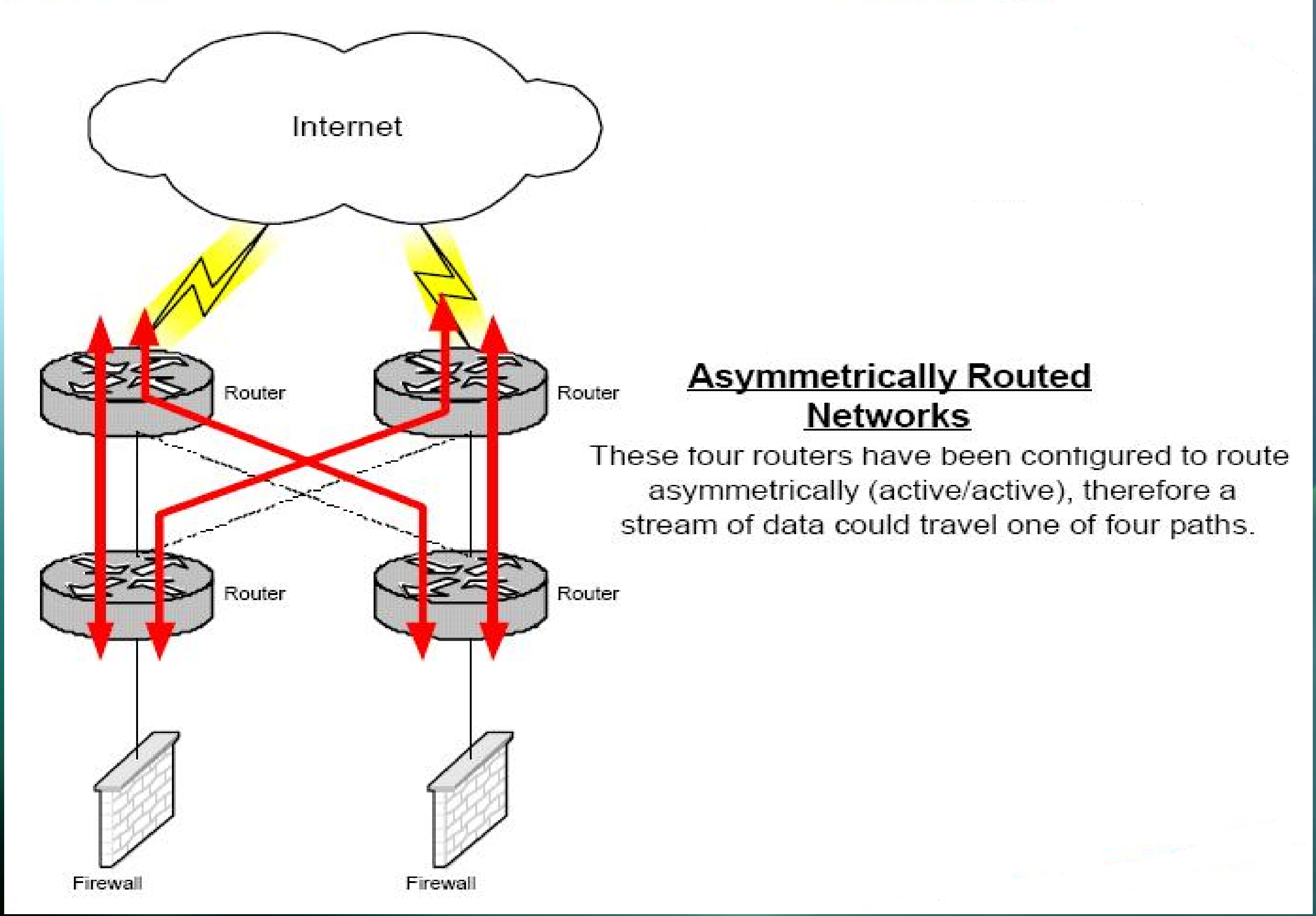
nIDS Solution for Switch and Hub network

- The issue is how to connect a nIDS so that it can listen to all the communication on the switch.

  The answer lies in what Cisco calls *SPAN ports (www.cisco.com\warp\public\473/41.html) or* what other vendors also call *Mirror Ports. The principal is the same in both. You set one port, on* the switch, to take copies of the other traffic from other ports.

nIDS

Asymmetrically Routed Networks



Asymmetrically Routed Networks

These four routers have been configured to route asymmetrically (active/active), therefore a stream of data could travel one of four paths.

nIDS

A nIDS can only work properly if it sees all the packets in a stream of data.

look at a simple CGI bin exploit on a web server, a hacker could enter in:

http://www.target.com/cgi-bin/test-cgi?* to get a list of all the files and directories in the scripts directory.

This stream could be split into 5 packets

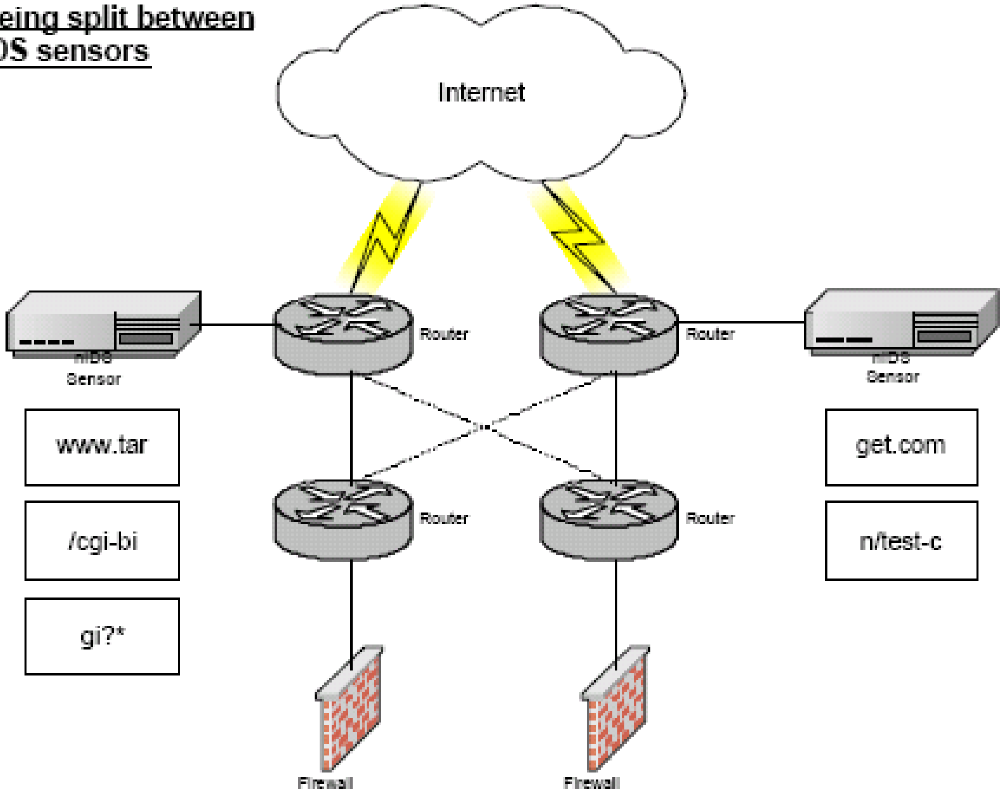
www.tar get.com **/cgi-bi** n/test-c **gi?***

Within an asymmetrically routed network, this stream of data could be sent any one of 4 ways --even if one has connected a nIDS to a SPAN port on each of the *front routers, (see Diagram on next slide)* and the data was distributed equally to each of these routers, half the packets would go to one nIDS and half to the other - so neither would pick up the attack.

nIDS

Asymmetrically Routed Networks

Packets being split between nIDS sensors



A nIDS Sensor has been connected to each router, if the stream of data was exactly split 50/50 between routers, then each nIDS will only see half the conversation.

PROJECT

Description of the Project

- Detect the Intrusion on the Network.
- Generate the attack on one computer and detect the intrusion on the other computer.
- Protecting the personal computer system using the host based intrusion detection system.

Issues to be Identified and Discussed

- The main issue for this project is to check the host network for vulnerabilities and signs of hacker activity.
- The host machine will be connected to the internet and represents the typical home user machine.
- Monitoring network traffic coming into the host machine and keep of all the traffic the host machine has received.

PROJECT

Project Focus

- Baseline of the project is to monitored packet traffic before taking any preventive action. Then after the preventive steps, monitoring packet traffic to see if Sax2 is catching suspicious behavior like it is suppose to.

- Sax2 allows for customizable security policies and gives network traffic statistics. These capabilities along with computer generated audits provided me real-time response and accurate information of network activity

TOOLS / SOFTWARE cont..1

Available Tools for Intrusion Detection System

- **SNORT** every one’s favorite open source ID’s
- **OSSEC HIDS** An Open Source Host-based Intrusion Detection System
- **BASE** The Basic Analysis and Security Engine
- **Sguil** The Analyst Console for Network Security Monitoring
- **Netcat** The network Swiss army knife
- **Metasploit Framwork** : Hack the Planet
- **Kismet** : A powerful wireless sniffer
- **Hping2** : A network probing utility like ping on steroids
- **Tcpdump** : The classic sniffer for network monitoring and data acquisition
- **Sax2 Intrusion detection** and prevention system (IDS)
- **Wireshark** fantastic open source network protocol analyzer for Unix and Windows
- (Selected tools for the Project1)

TOOLS / SOFTWARE cont..2

Introduction to the selected tool

Intrusion Detection System – ***Sax2*** *Main features*

1. Intrusion Detection and Prevention
2. Conduct of Audits
3. Traffic Statistics and analysis
4. Customize Security Policy
5. Logs and events
6. Support multiple adapters

7.Conversation and packet streaming

8. Real-time Alert and Response
9. Network Based IDS

TOOLS / SOFTWARE cont..3

System requirements and tool installation

Sax2.0

- Sax2 is freeware and can be downloaded from various sites offering free downloads. Some well known sites are

http://wareseeker.com

http://www.freedownloadscenter.com/

http://3d2f.com/

http://sax2-intrusion-detection-system-free-.smartcode.com

http://www.ids-sax2.com/

Operating Systems

Win 2000/NT, Windows XP, Win 2003, Windows Vista

Size 5.52 MB

TOOLS / SOFTWARE cont ..4

Installing the tool and System requirements

Size 5.52 MB

System Requirements

The following minimum requirements are the base line to install and run Ax3soft Sax2ly.

It would be better if your system has a higher configuration, especially in a busy or big network.

a). **Minimum requirements**: P4 1.2G CPU, 512 MB RAM, Internet Explorer 5.5 or higher

b). **Recommended requirements**: P4 3.0G CPU, 1 GB RAM or more, Internet Explorer 6.0 or higher

c). **Supported Windows Platforms**: Windows 2000 (SP 4 or later) Windows XP (SP 1 or later) and x64 Edition, Windows Server 2003 (SP 2 or later) and x64 Edition, Windows Vista and x64 Edition

TOOLS / SOFTWARE cont ..5

Installing the tool and System requirements

WIRESHARK

The world’s foremost network protocol analyzer

http://www.wireshark.org/docs/

CAIN ABEL

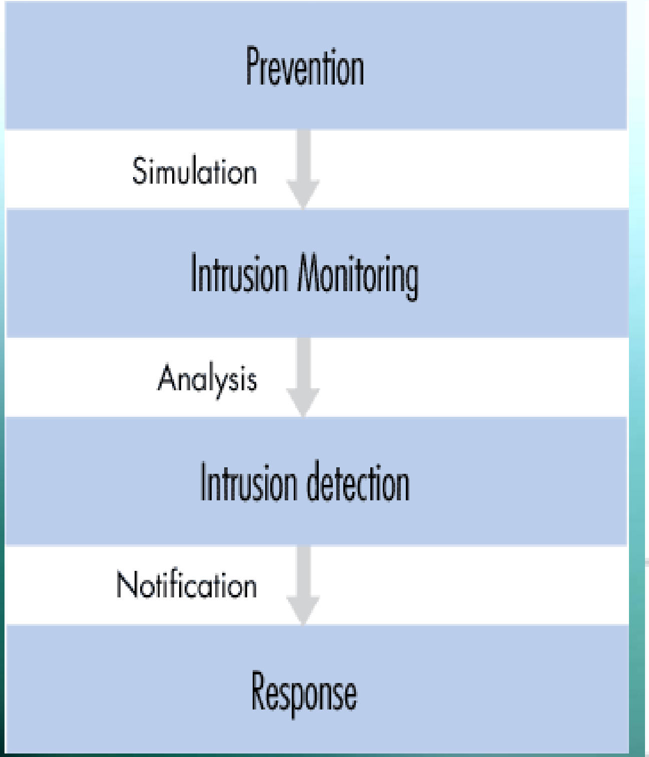
Cain & Abel is a password recovery tool for Microsoft Operating Systems

WINPCAP (automatically install with CAIN & ABEL

http://www.oxid.it/cain.html

PROJECT EXECUTION

Intrusion detection system activities



Prevention

Simulation

Intrusion Monitoring

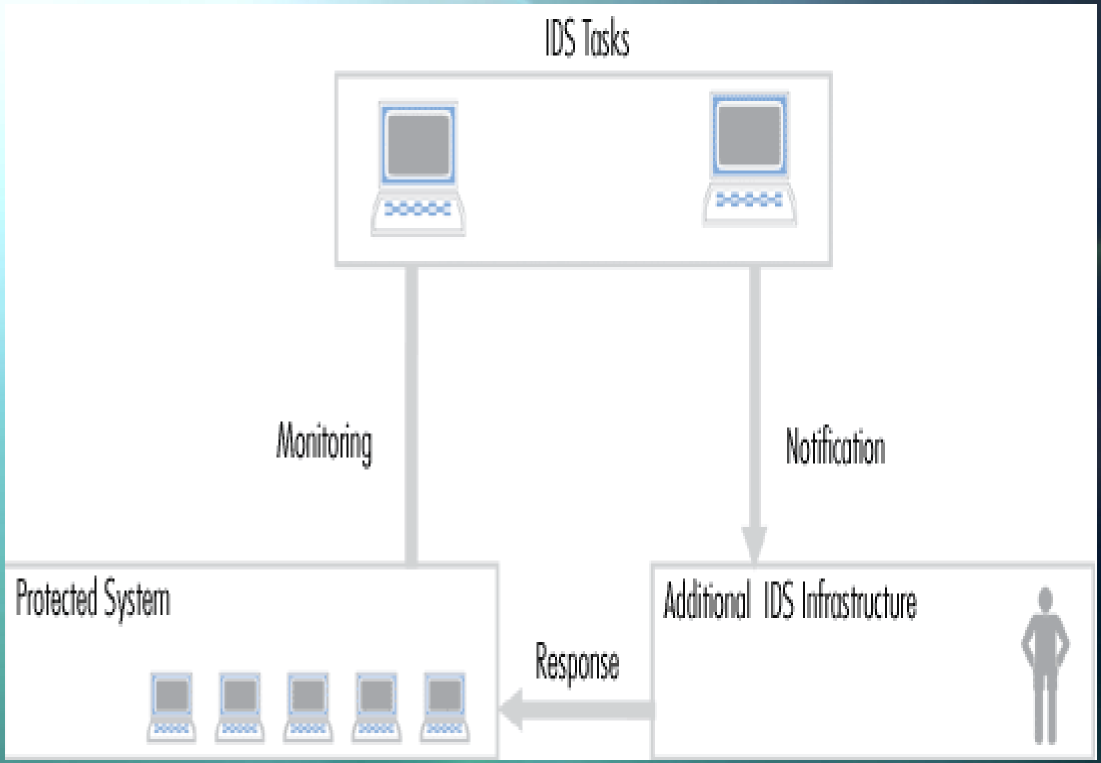
Analysis

Intrusion detection

Notification

Response

Intrusion detection system Infrastructure



IDS Tasks

Monitoring

Notification

Protected System

Response

Additional IDS Infrastructure

PROJECT EXECUTION

System specification of VICTIM and ATTACKER

ATTACKER

LAPTOP

- **Windows VISTA**
- **CAIN & ABEL**
- **WIRESHARK**
- **IP ADDRESS 192.168.1.101**
- **Subnet Mask 255.255.255.0**
- **Default Gateway 192.168.1.1**

VICTIM

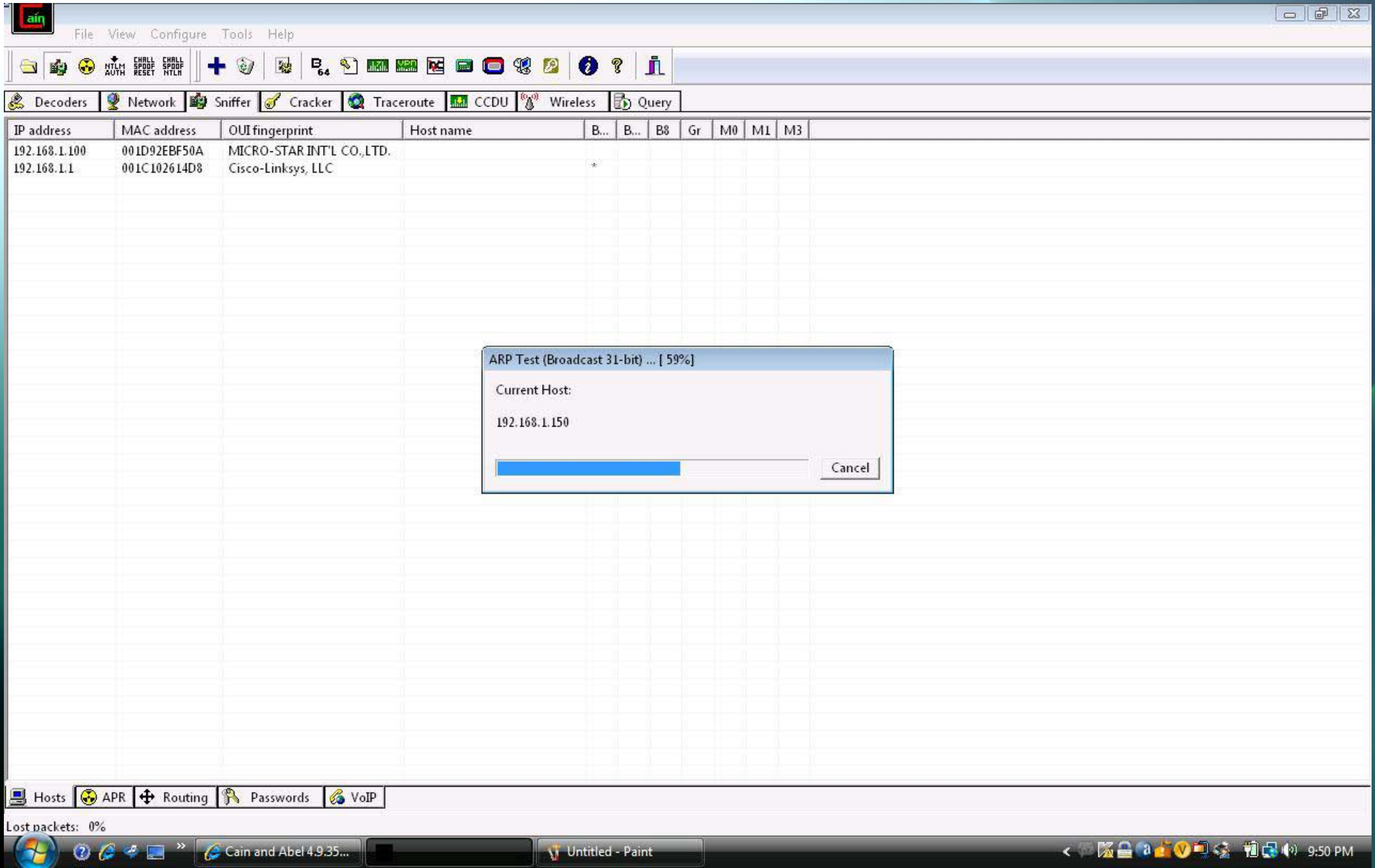
Desktop

- **Windows XP**
- **IP ADDRESS 192.168.1.100**
- **Subnet Mask 255.255.255.0**
- **Default Gateway 192.168.1.1**

PROJECT EXECUTION

Screen shoots for CAIN

Looking for the poisoning route



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.1.100	001D92EBF50A	MICRO-STAR INT'L CO.,LTD.								
192.168.1.1	001C102614D8	Cisco-Linksys, LLC		*						

ARP Test (Broadcast 31-bit) ... [59%]

Current Host:

192.168.1.150

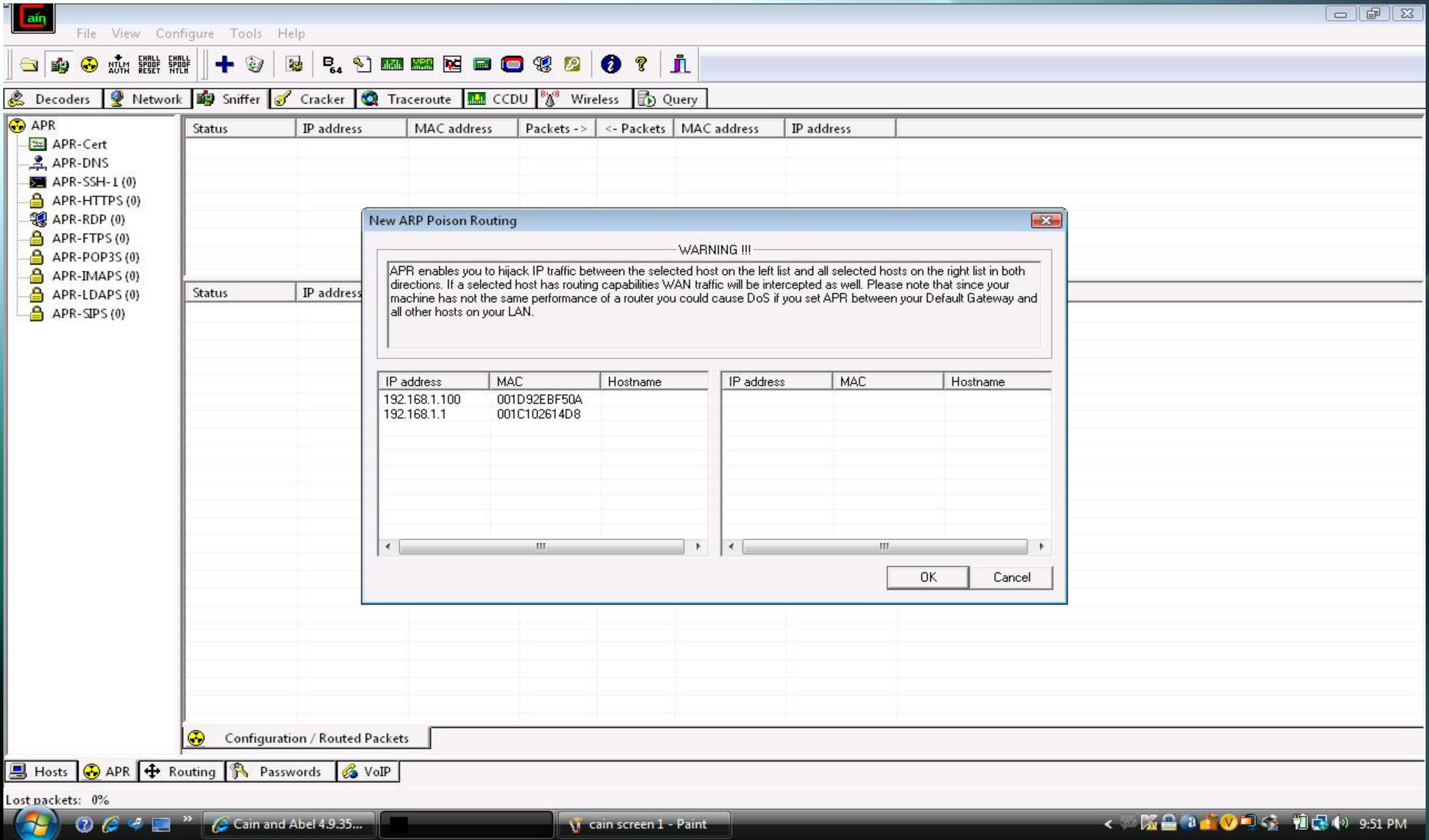
Cancel

Lost packets: 0%

PROJECT EXECUTION

Screen shoots for CAIN

New ARP poisoning route



New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.1.100	001D92EBF50A	
192.168.1.1	001C102614D8	

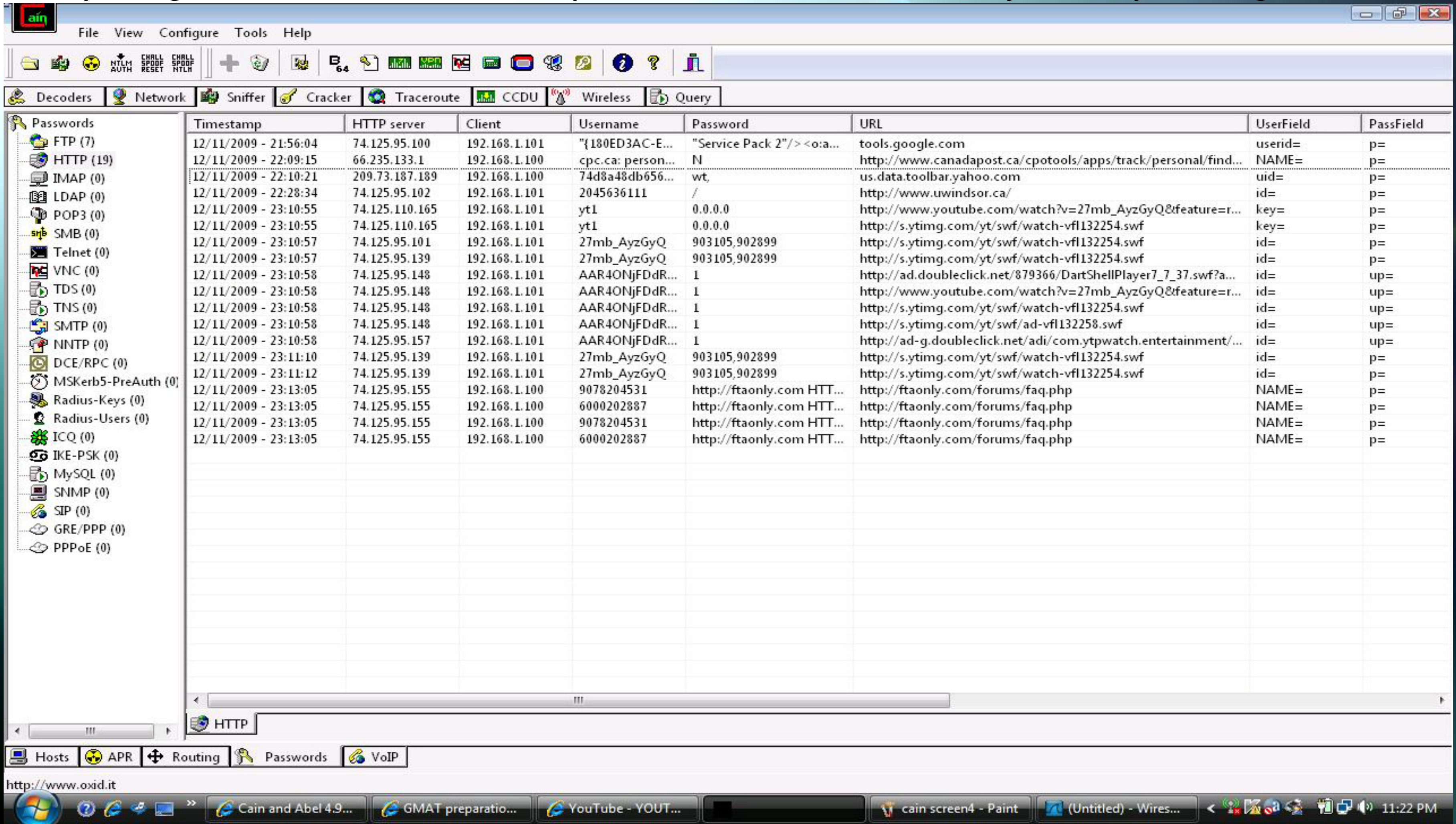
IP address	MAC	Hostname

OK Cancel

PROJECT EXECUTION

Screen shoots for CAIN

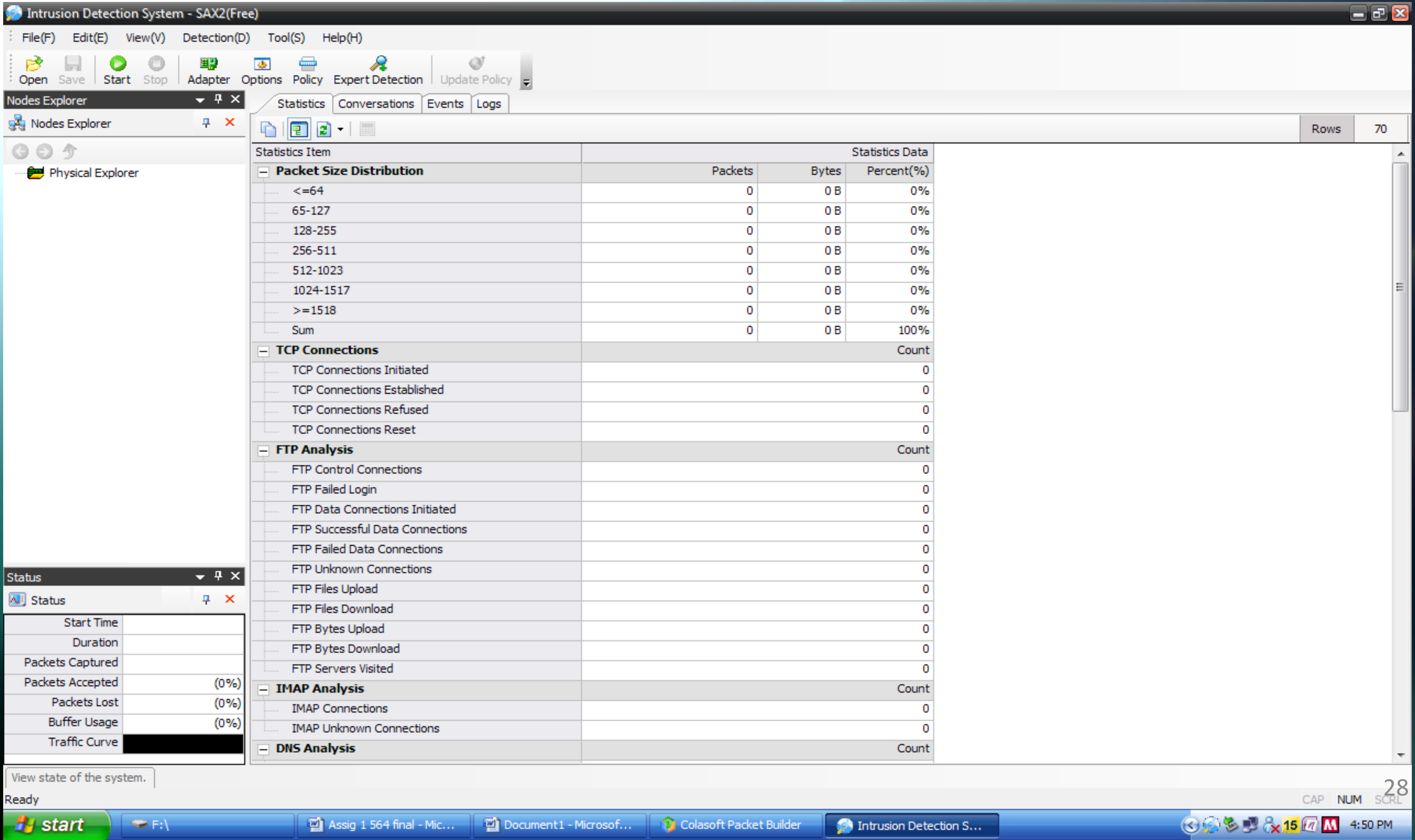
ARP poising result on the Victim desktop. All visited URL's are shown after ARP poisoning



Timestamp	HTTP server	Client	Username	Password	URL	UserField	PassField
12/11/2009 - 21:56:04	74.125.95.100	192.168.1.101	"{180ED3AC-E...	"Service Pack 2"/><o:a...	tools.google.com	userid=	p=
12/11/2009 - 22:09:15	66.235.133.1	192.168.1.100	cpc.ca: person...	N	http://www.canadapost.ca/cpotools/apps/track/personal/find...	NAME=	p=
12/11/2009 - 22:10:21	209.73.187.189	192.168.1.100	74d8a48db656...	wt,	us.data.toolbar.yahoo.com	uid=	p=
12/11/2009 - 22:28:34	74.125.95.102	192.168.1.101	2045636111	/	http://www.uwindsor.ca/	id=	p=
12/11/2009 - 23:10:55	74.125.110.165	192.168.1.101	yt1	0.0.0.0	http://www.youtube.com/watch?v=27mb_AyzGyQ&feature=r...	key=	p=
12/11/2009 - 23:10:55	74.125.110.165	192.168.1.101	yt1	0.0.0.0	http://s.ytimg.com/yt/swf/watch-vfl132254.swf	key=	p=
12/11/2009 - 23:10:57	74.125.95.101	192.168.1.101	27mb_AyzGyQ	903105,902899	http://s.ytimg.com/yt/swf/watch-vfl132254.swf	id=	p=
12/11/2009 - 23:10:57	74.125.95.139	192.168.1.101	27mb_AyzGyQ	903105,902899	http://s.ytimg.com/yt/swf/watch-vfl132254.swf	id=	p=
12/11/2009 - 23:10:58	74.125.95.148	192.168.1.101	AAR4ONjFDdR...	1	http://ad.doubleclick.net/879366/DartShellPlayer7_7_37.swf?a...	id=	up=
12/11/2009 - 23:10:58	74.125.95.148	192.168.1.101	AAR4ONjFDdR...	1	http://www.youtube.com/watch?v=27mb_AyzGyQ&feature=r...	id=	up=
12/11/2009 - 23:10:58	74.125.95.148	192.168.1.101	AAR4ONjFDdR...	1	http://s.ytimg.com/yt/swf/watch-vfl132254.swf	id=	up=
12/11/2009 - 23:10:58	74.125.95.148	192.168.1.101	AAR4ONjFDdR...	1	http://s.ytimg.com/yt/swf/ad-vfl132258.swf	id=	up=
12/11/2009 - 23:10:58	74.125.95.157	192.168.1.101	AAR4ONjFDdR...	1	http://ad-g.doubleclick.net/adi/com.ytpwatch.entertainment/...	id=	up=
12/11/2009 - 23:11:10	74.125.95.139	192.168.1.101	27mb_AyzGyQ	903105,902899	http://s.ytimg.com/yt/swf/watch-vfl132254.swf	id=	p=
12/11/2009 - 23:11:12	74.125.95.139	192.168.1.101	27mb_AyzGyQ	903105,902899	http://s.ytimg.com/yt/swf/watch-vfl132254.swf	id=	p=
12/11/2009 - 23:13:05	74.125.95.155	192.168.1.100	9078204531	http://ftaonly.com HTT...	http://ftaonly.com/forums/faq.php	NAME=	p=
12/11/2009 - 23:13:05	74.125.95.155	192.168.1.100	6000202887	http://ftaonly.com HTT...	http://ftaonly.com/forums/faq.php	NAME=	p=
12/11/2009 - 23:13:05	74.125.95.155	192.168.1.100	9078204531	http://ftaonly.com HTT...	http://ftaonly.com/forums/faq.php	NAME=	p=
12/11/2009 - 23:13:05	74.125.95.155	192.168.1.100	6000202887	http://ftaonly.com HTT...	http://ftaonly.com/forums/faq.php	NAME=	p=

PROJECT EXECUTION

Sax2 Screen 1** before starting Intrusion Detection System **capturing live packets

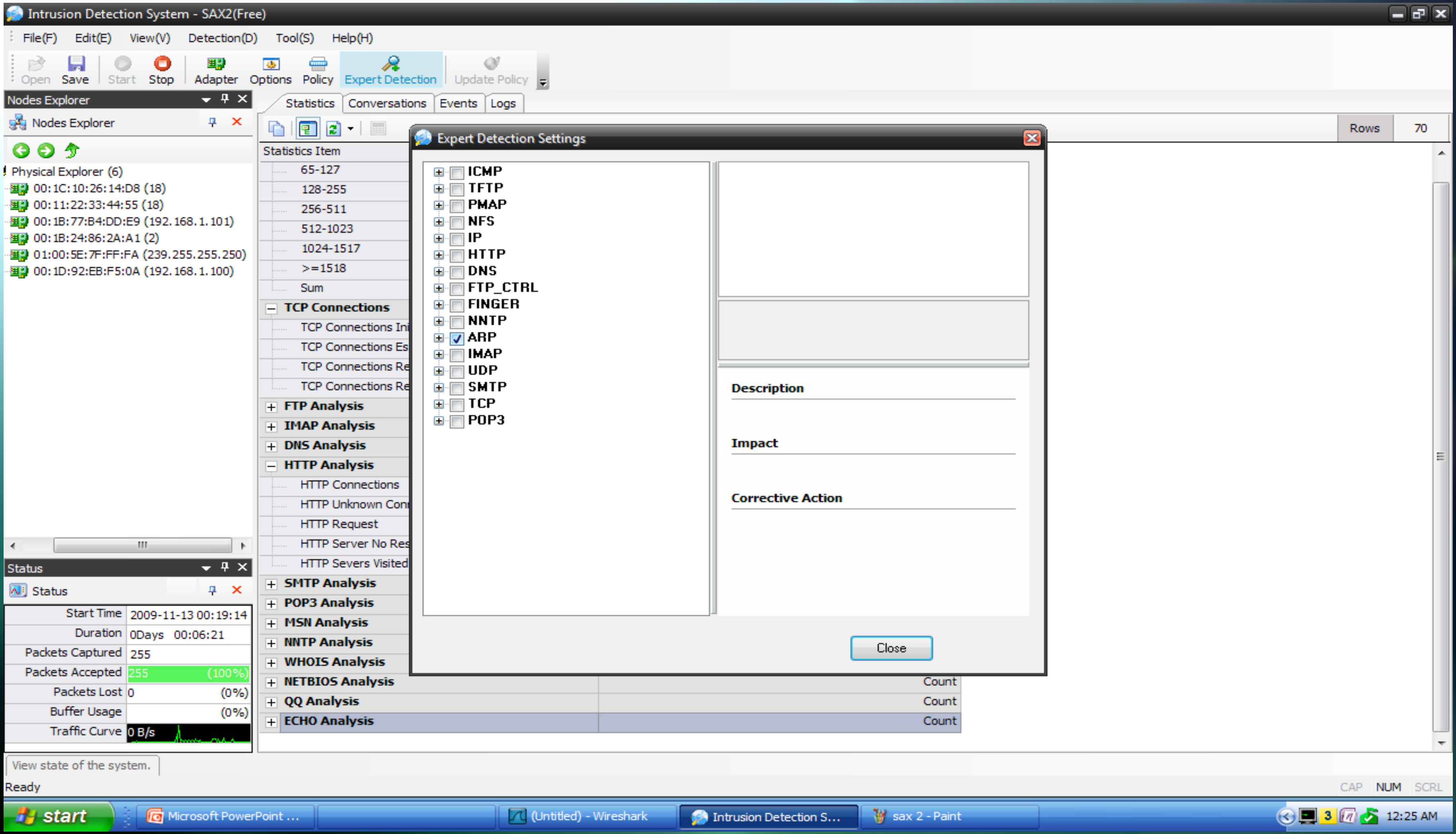


Statistics Item	Statistics Data		
Packet Size Distribution	Packets	Bytes	Percent(%)
<=64	0	0 B	0%
65-127	0	0 B	0%
128-255	0	0 B	0%
256-511	0	0 B	0%
512-1023	0	0 B	0%
1024-1517	0	0 B	0%
>=1518	0	0 B	0%
Sum	0	0 B	100%
TCP Connections			Count
TCP Connections Initiated			0
TCP Connections Established			0
TCP Connections Refused			0
TCP Connections Reset			0
FTP Analysis			Count
FTP Control Connections			0
FTP Failed Login			0
FTP Data Connections Initiated			0
FTP Successful Data Connections			0
FTP Failed Data Connections			0
FTP Unknown Connections			0
FTP Files Upload			0
FTP Files Download			0
FTP Bytes Upload			0
FTP Bytes Download			0
FTP Servers Visited			0
IMAP Analysis			Count
IMAP Connections			0
IMAP Unknown Connections			0
DNS Analysis			Count

Start Time	
Duration	
Packets Captured	
Packets Accepted	(0%)
Packets Lost	(0%)
Buffer Usage	(0%)
Traffic Curve	

PROJECT EXECUTION

Expert detection setting. Selecting ARP for detecting ARP poisoning in IDS SAX 2.0



Nodes Explorer

Physical Explorer (6)
- 00:1C:10:26:14:D8 (18)
- 00:11:22:33:44:55 (18)
- 00:1B:77:B4:DD:E9 (192.168.1.101)
- 00:1B:24:86:2A:A1 (2)
- 01:00:5E:7F:FF:FA (239.255.255.250)
- 00:1D:92:EB:F5:0A (192.168.1.100)

Status

Start Time	2009-11-13 00:19:14
Duration	0Days 00:06:21
Packets Captured	255
Packets Accepted	255 (100%)
Packets Lost	0 (0%)
Buffer Usage	(0%)
Traffic Curve	0 B/s

View state of the system.

Ready

Statistics Item
- 65-127
- 128-255
- 256-511
- 512-1023
- 1024-1517
- >=1518
- Sum
- TCP Connections
  - TCP Connections Ini
  - TCP Connections Es
  - TCP Connections Re
  - TCP Connections Re
- FTP Analysis
- IMAP Analysis
- DNS Analysis
- HTTP Analysis
  - HTTP Connections
  - HTTP Unknown Con
  - HTTP Request
  - HTTP Server No Res
  - HTTP Severs Visited
- SMTP Analysis
- POP3 Analysis
- MSN Analysis
- NNTP Analysis
- WHOIS Analysis
- NETBIOS Analysis — Count
- QQ Analysis — Count
- ECHO Analysis — Count

Expert Detection Settings

- □ ICMP
- □ TFTP
- □ PMAP
- □ NFS
- □ IP
- □ HTTP
- □ DNS
- □ FTP_CTRL
- □ FINGER
- □ NNTP
- ☑ ARP
- □ IMAP
- □ UDP
- □ SMTP
- □ TCP
- □ POP3

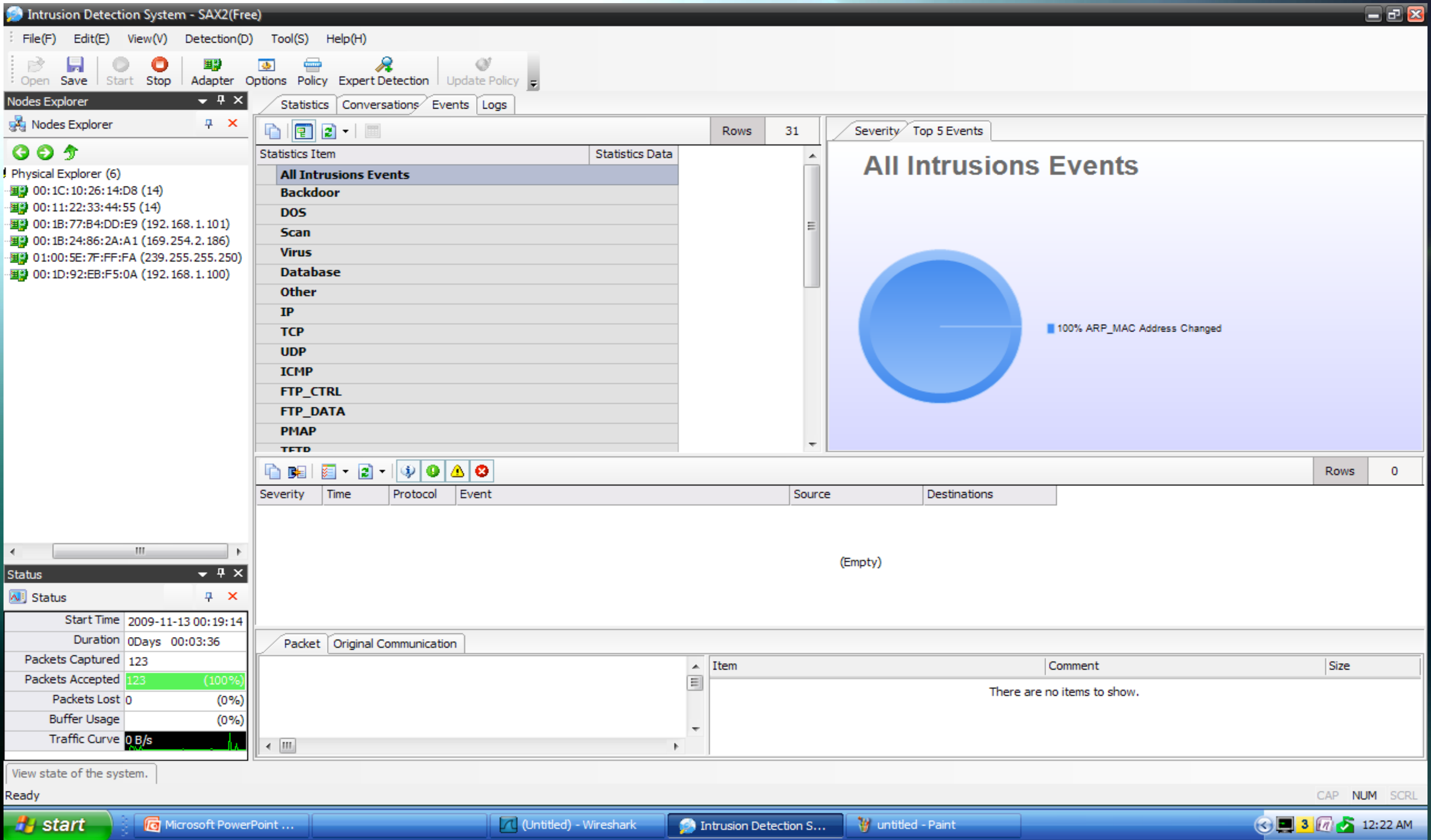
Description

Impact

Corrective Action

PROJECT EXECUTION

All Intrusions events detected by SAX 2.0



Physical Explorer (6)
- 00:1C:10:26:14:D8 (14)
- 00:11:22:33:44:55 (14)
- 00:1B:77:B4:DD:E9 (192.168.1.101)
- 00:1B:24:86:2A:A1 (169.254.2.186)
- 01:00:5E:7F:FF:FA (239.255.255.250)
- 00:1D:92:EB:F5:0A (192.168.1.100)

Rows 31

Statistics Item	Statistics Data
All Intrusions Events	
Backdoor	
DOS	
Scan	
Virus	
Database	
Other	
IP	
TCP	
UDP	
ICMP	
FTP_CTRL	
FTP_DATA	
PMAP	
TFTP	

All Intrusions Events

🟦 100% ARP_MAC Address Changed

Rows 0

Severity	Time	Protocol	Event	Source	Destinations

(Empty)

Item	Comment	Size

There are no items to show.

Status

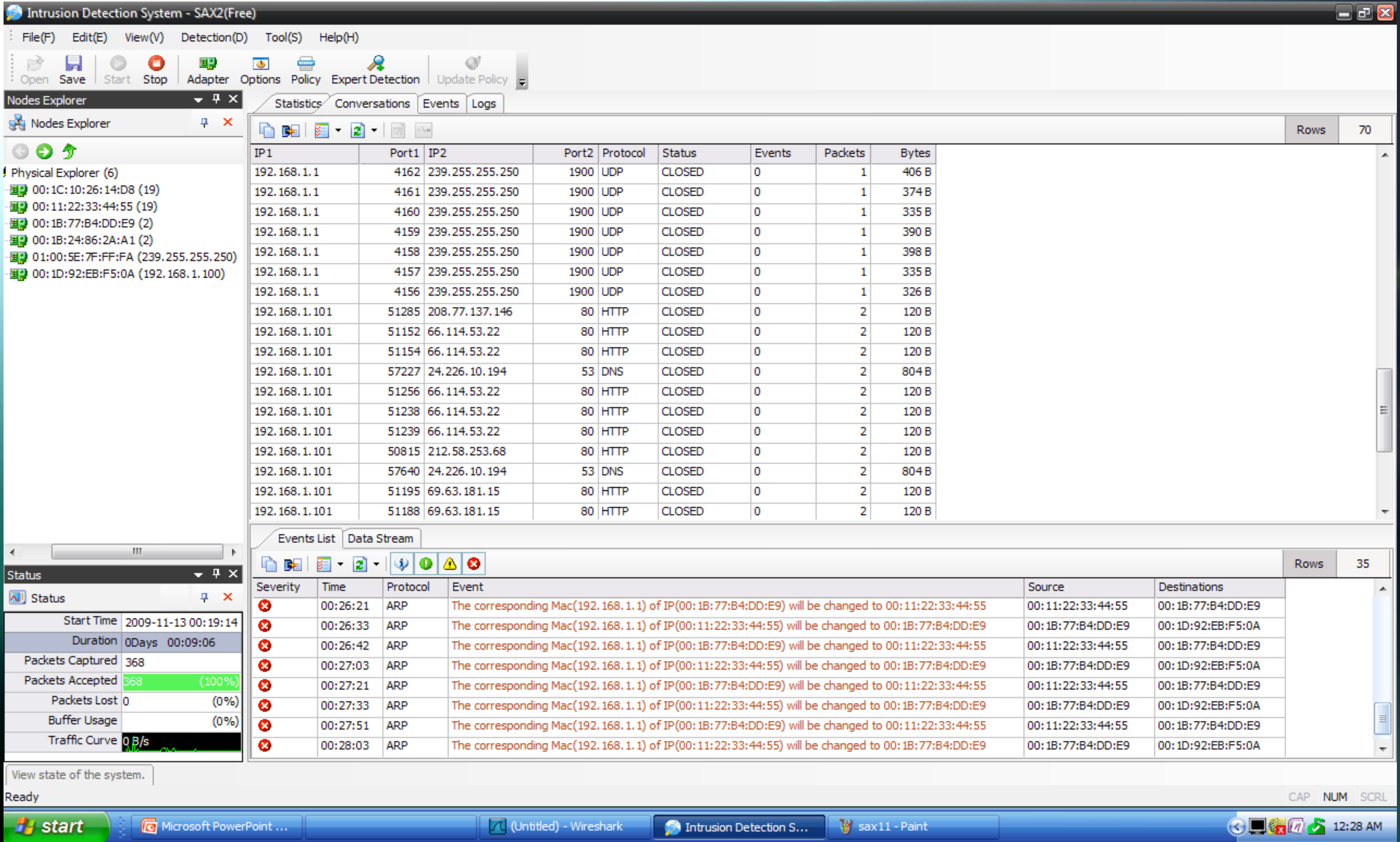
Start Time	2009-11-13 00:19:14
Duration	0Days 00:03:36
Packets Captured	123
Packets Accepted	123 (100%)
Packets Lost	0 (0%)
Buffer Usage	(0%)
Traffic Curve	0 B/s

View state of the system.

Ready

PROJECT EXECUTION

ARP intrusion detected from the 192.168.1.101 (Attacker Laptop)


Intrusion Detection System - SAX2(Free)
File(F) Edit(E) View(V) Detection(D) Tool(S) Help(H)
Open Save Start Stop Adapter Options Policy Expert Detection Update Policy
Nodes Explorer
Statistics Conversations Events Logs
Events List Data Stream
Status
start Microsoft PowerPoint ... (Untitled) - Wireshark Intrusion Detection S... sax11 - Paint 12:28 AM
CAP NUM SCRL

Physical Explorer (6)
- 00:1C:10:26:14:D8 (19)
- 00:11:22:33:44:55 (19)
- 00:1B:77:B4:DD:E9 (2)
- 00:1B:24:86:2A:A1 (2)
- 01:00:5E:7F:FF:FA (239.255.255.250)
- 00:1D:92:EB:F5:0A (192.168.1.100)

Rows 70

IP1	Port1	IP2	Port2	Protocol	Status	Events	Packets	Bytes
192.168.1.1	4162	239.255.255.250	1900	UDP	CLOSED	0	1	406 B
192.168.1.1	4161	239.255.255.250	1900	UDP	CLOSED	0	1	374 B
192.168.1.1	4160	239.255.255.250	1900	UDP	CLOSED	0	1	335 B
192.168.1.1	4159	239.255.255.250	1900	UDP	CLOSED	0	1	390 B
192.168.1.1	4158	239.255.255.250	1900	UDP	CLOSED	0	1	398 B
192.168.1.1	4157	239.255.255.250	1900	UDP	CLOSED	0	1	335 B
192.168.1.1	4156	239.255.255.250	1900	UDP	CLOSED	0	1	326 B
192.168.1.101	51285	208.77.137.146	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	51152	66.114.53.22	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	51154	66.114.53.22	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	57227	24.226.10.194	53	DNS	CLOSED	0	2	804 B
192.168.1.101	51256	66.114.53.22	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	51238	66.114.53.22	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	51239	66.114.53.22	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	50815	212.58.253.68	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	57640	24.226.10.194	53	DNS	CLOSED	0	2	804 B
192.168.1.101	51195	69.63.181.15	80	HTTP	CLOSED	0	2	120 B
192.168.1.101	51188	69.63.181.15	80	HTTP	CLOSED	0	2	120 B

Rows 35

Severity	Time	Protocol	Event	Source	Destinations
⊗	00:26:21	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E9) will be changed to 00:11:22:33:44:55	00:11:22:33:44:55	00:1B:77:B4:DD:E9
⊗	00:26:33	ARP	The corresponding Mac(192.168.1.1) of IP(00:11:22:33:44:55) will be changed to 00:1B:77:B4:DD:E9	00:1B:77:B4:DD:E9	00:1D:92:EB:F5:0A
⊗	00:26:42	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E9) will be changed to 00:11:22:33:44:55	00:11:22:33:44:55	00:1B:77:B4:DD:E9
⊗	00:27:03	ARP	The corresponding Mac(192.168.1.1) of IP(00:11:22:33:44:55) will be changed to 00:1B:77:B4:DD:E9	00:1B:77:B4:DD:E9	00:1D:92:EB:F5:0A
⊗	00:27:21	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E9) will be changed to 00:11:22:33:44:55	00:11:22:33:44:55	00:1B:77:B4:DD:E9
⊗	00:27:33	ARP	The corresponding Mac(192.168.1.1) of IP(00:11:22:33:44:55) will be changed to 00:1B:77:B4:DD:E9	00:1B:77:B4:DD:E9	00:1D:92:EB:F5:0A
⊗	00:27:51	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E9) will be changed to 00:11:22:33:44:55	00:11:22:33:44:55	00:1B:77:B4:DD:E9
⊗	00:28:03	ARP	The corresponding Mac(192.168.1.1) of IP(00:11:22:33:44:55) will be changed to 00:1B:77:B4:DD:E9	00:1B:77:B4:DD:E9	00:1D:92:EB:F5:0A

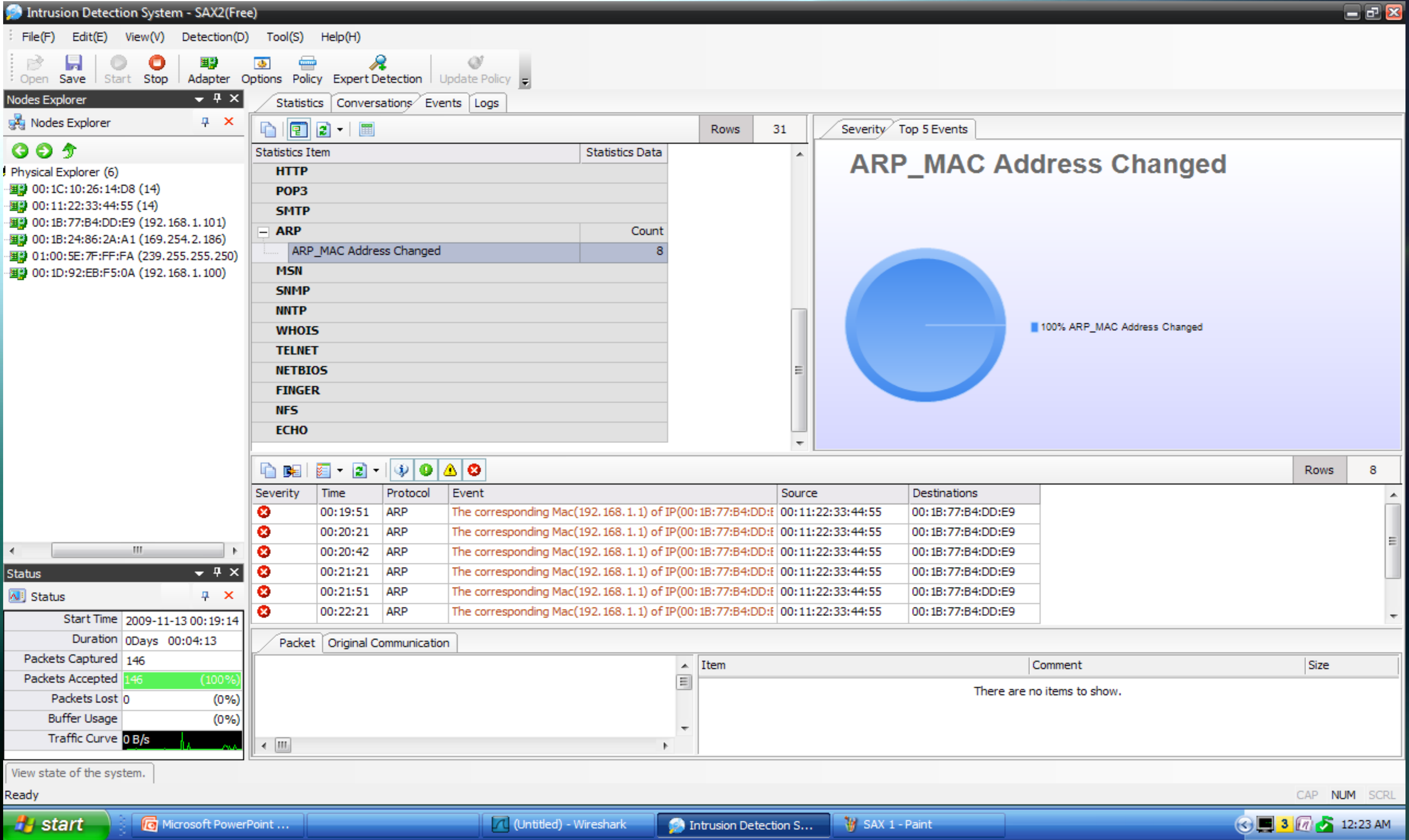
Start Time	2009-11-13 00:19:14
Duration	0Days 00:09:06
Packets Captured	368
Packets Accepted	368 (100%)
Packets Lost	0 (0%)
Buffer Usage	(0%)
Traffic Curve	0 B/s

View state of the system.

Ready

PROJECT EXECUTION

ARP intrusion detected and 100 % ARP_MAC address changed to avoid ARP poisoning



Intrusion Detection System - SAX2(Free)
File(F) Edit(E) View(V) Detection(D) Tool(S) Help(H)
Open Save Start Stop Adapter Options Policy Expert Detection Update Policy
Nodes Explorer
Statistics Conversations Events Logs
Rows 31
Severity Top 5 Events
ARP_MAC Address Changed
100% ARP_MAC Address Changed
Rows 8
Packet Original Communication
Status
View state of the system.
Ready
CAP NUM SCRL
start Microsoft PowerPoint ... (Untitled) - Wireshark Intrusion Detection S... SAX 1 - Paint 12:23 AM

Physical Explorer (6)
- 00:1C:10:26:14:D8 (14)
- 00:11:22:33:44:55 (14)
- 00:1B:77:B4:DD:E9 (192.168.1.101)
- 00:1B:24:86:2A:A1 (169.254.2.186)
- 01:00:5E:7F:FF:FA (239.255.255.250)
- 00:1D:92:EB:F5:0A (192.168.1.100)

Statistics Item	Statistics Data
HTTP	
POP3	
SMTP	
ARP	Count
ARP_MAC Address Changed	8
MSN	
SNMP	
NNTP	
WHOIS	
TELNET	
NETBIOS	
FINGER	
NFS	
ECHO	

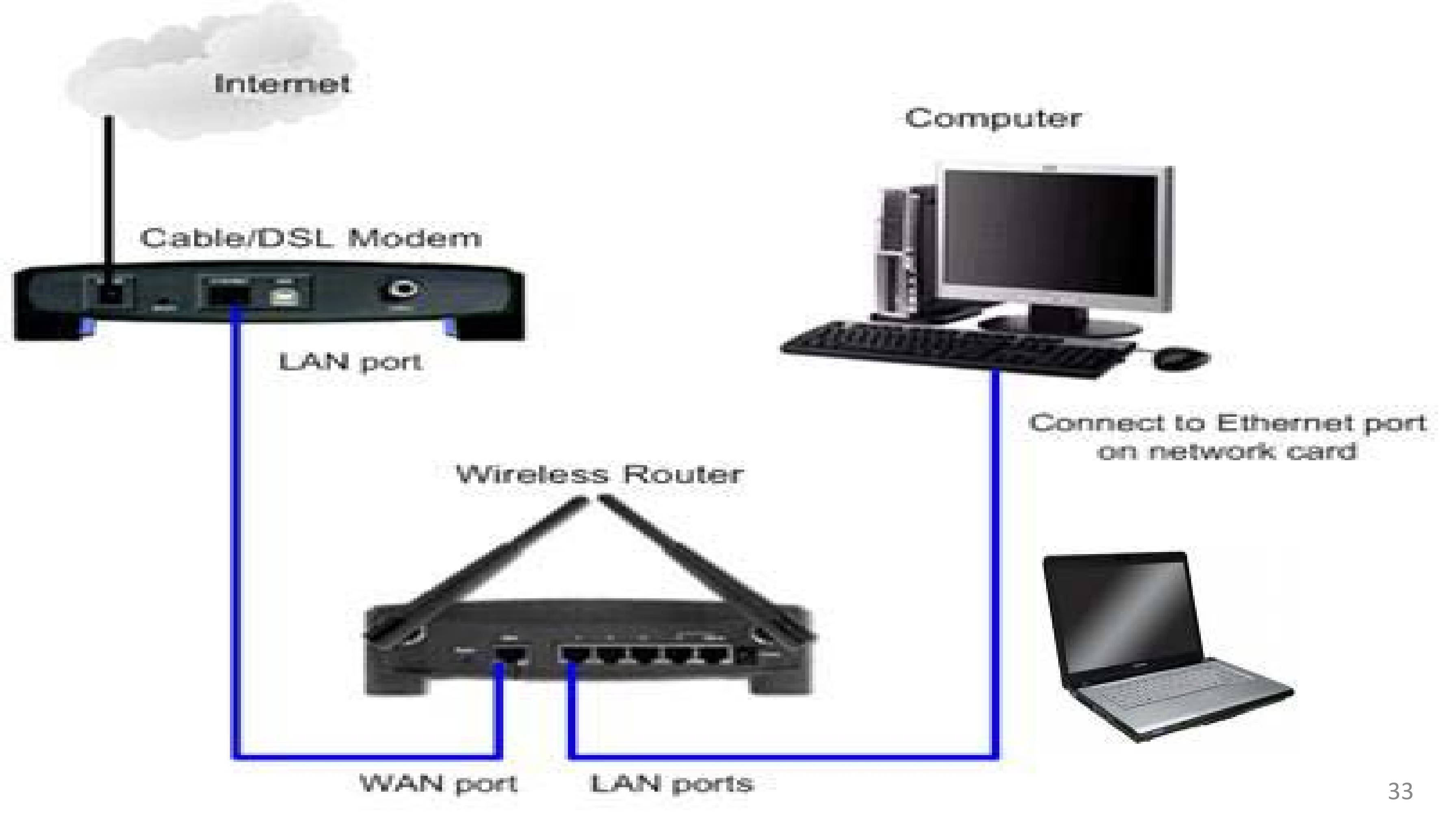
Severity	Time	Protocol	Event	Source	Destinations
☒	00:19:51	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E	00:11:22:33:44:55	00:1B:77:B4:DD:E9
☒	00:20:21	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E	00:11:22:33:44:55	00:1B:77:B4:DD:E9
☒	00:20:42	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E	00:11:22:33:44:55	00:1B:77:B4:DD:E9
☒	00:21:21	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E	00:11:22:33:44:55	00:1B:77:B4:DD:E9
☒	00:21:51	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E	00:11:22:33:44:55	00:1B:77:B4:DD:E9
☒	00:22:21	ARP	The corresponding Mac(192.168.1.1) of IP(00:1B:77:B4:DD:E	00:11:22:33:44:55	00:1B:77:B4:DD:E9

Item	Comment	Size
There are no items to show.		

Start Time	2009-11-13 00:19:14
Duration	0Days 00:04:13
Packets Captured	146
Packets Accepted	146 (100%)
Packets Lost	0 (0%)
Buffer Usage	(0%)
Traffic Curve	0 B/s

NETWORK PRESENTATION

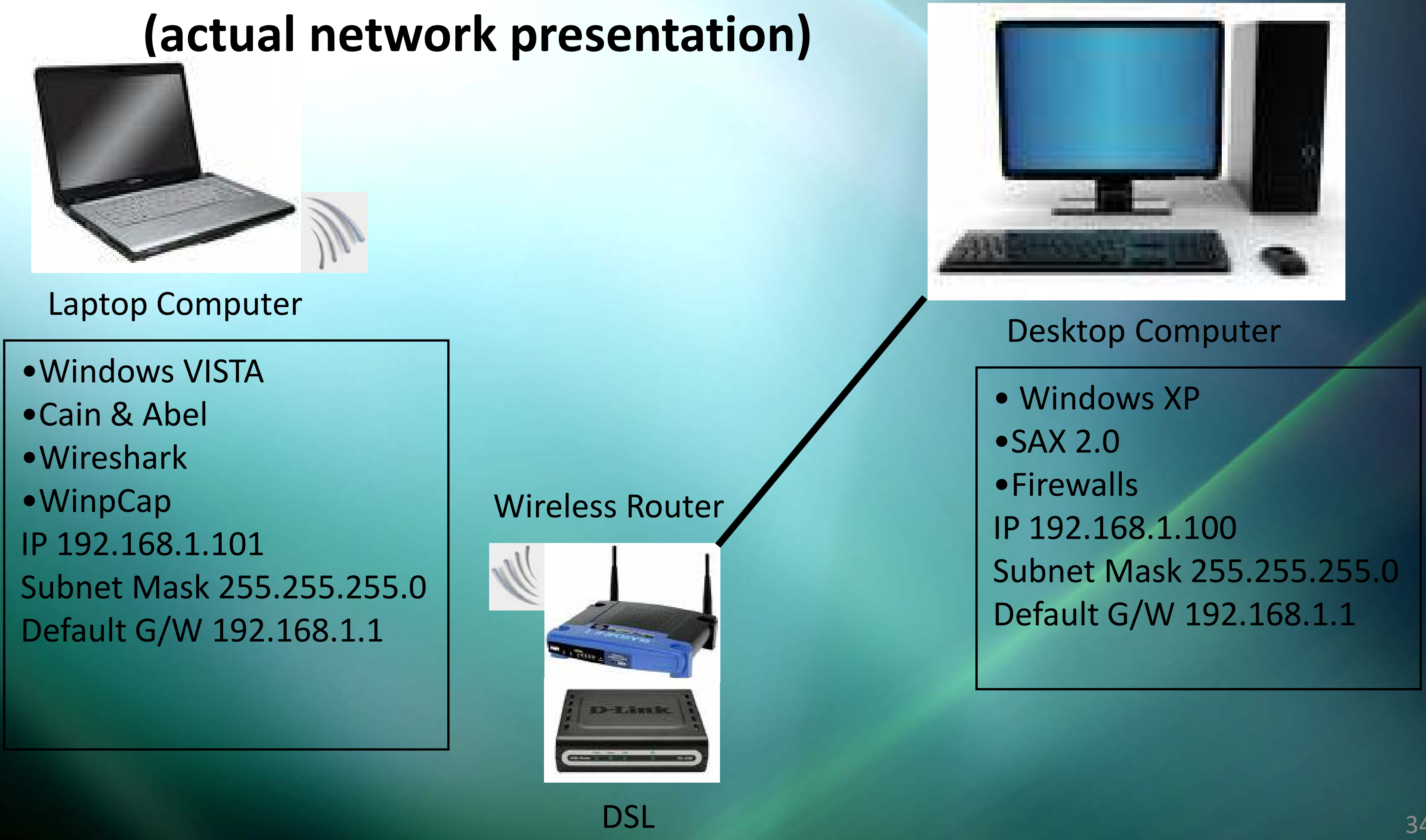
Project execution demonstration 1



NETWORK PRESENTATION

Project execution demonstration 2

(actual network presentation)



Laptop Computer

- Windows VISTA
- Cain & Abel
- Wireshark
- WinpCap

IP 192.168.1.101
Subnet Mask 255.255.255.0
Default G/W 192.168.1.1

Wireless Router

DSL

Desktop Computer

- Windows XP
- SAX 2.0
- Firewalls

IP 192.168.1.100
Subnet Mask 255.255.255.0
Default G/W 192.168.1.1

REFERENCES

[1] Book
Network Defense and Countermeasures: Principles and Practices,
Chuck Easttom. Prentice Hall, 2006.
accessed on Sept 26, 2009

[2] SAX 2.0 Features and Properties, O’Reilly.
URL: *http://docstore.mik.ua/orelly/xml/jxml/appb_01.htm*
accessed on Sept 30, 2009

[3] Class notes 0360564 Intrusion detection
URL: *http://web2.uwindsor.ca/courses/cs/aggarwal/cs60564/materials.htm*
accessed on Sept 30, 2009

[4] What is network intrusion system?
URL: *http://www.linuxsecurity.com/resource_files/intrusion_detection/network*
intrusion-detection.html#1.1
accessed on Oct 01, 2009

REFERENCES

[5] Architecture

URL: *http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#2.*

accessed on Oct 01, 2009

[6] Policy and prevention

URL : *http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#3.*

accessed on Oct 02, 2009

[7] IDS and firewalls

URL : *http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html#7.*

accessed on Oct 5, 2009

[8] Intrusion detection Systems - Wikipedia

URL : *http://en.wikipedia.org/wiki/Intrusion-detection_system*

accessed on Oct 03, 2009

REFERENCES

[9] Intrusion and intrusion detection

John McHugh, Alan Christie, and Julia Allen

Software Engineering Institute, CERT Coordination Center

URL : *http://www.cs.virginia.edu/~jones/IDS-research/Papers.html*

accessed on Oct 05, 2009

QUESTIONS ?

RESPECTABLE AUDIENCE HAS ANY QUESTION, CONCERN OR ANY DISCUSSION POINT ABOUT THE PRESENTATION, PLEASE GO A HEAD...

Thank You!