ETHICAL HACKING LAB SERIES

Lab 19: Using Certificates to Encrypt Email

Certified Ethical Hacking Domain: Cryptography

Document Version: 2015-08-14

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

In this lab, students will view unencrypted and encrypted email messages.

This lab includes the following tasks:

1. Capturing Plain Text Email Traffic with tcpdump
2. Analyzing Plain Text Email Traffic
3. Capturing Encrypted Email Traffic with tcpdump
4. Analyzing Encrypted Email Traffic

Domain: Cryptography

If email is sent over a network without using encryption, then passwords and messages can be viewed by anyone who is able to capture the email messages while they are being transmitted. If encryption is used when email is sent, the message will be unreadable.

Certificate Authority – Known as the root CA, or Certificate Authority, is the certificate server that is the authority for all certificates requested within a Public Key Infrastructure, or PKI. The Enterprise Editions of Windows Server can act as a CA.

Symmetric Encryption – This is a form of encryption in which the same key is used to encrypt and decrypt data. Examples of Symmetrical Encryption algorithms include Advanced Encryption Standard (AES) algorithm and DES (Data Encryption Standard).

Asymmetric Encryption – This is a form of encryption in which a different key is used to encrypt and decrypt data. Examples of Symmetrical Encryption algorithms include RSA, which stands for Rivest, Shamir, and Adleman, the 3 original authors.

Public Key – The Public Key is used to encrypt messages. The user can send their Public Key to another user by digitally signing an email message. The user will then use the public key provided to them by the sender to encrypt messages sent to that sender.

Private Key – The Private Key is not distributed to other users. It is kept private and used to decrypt email messages that were encrypted with the user's public key.

Pod Topology

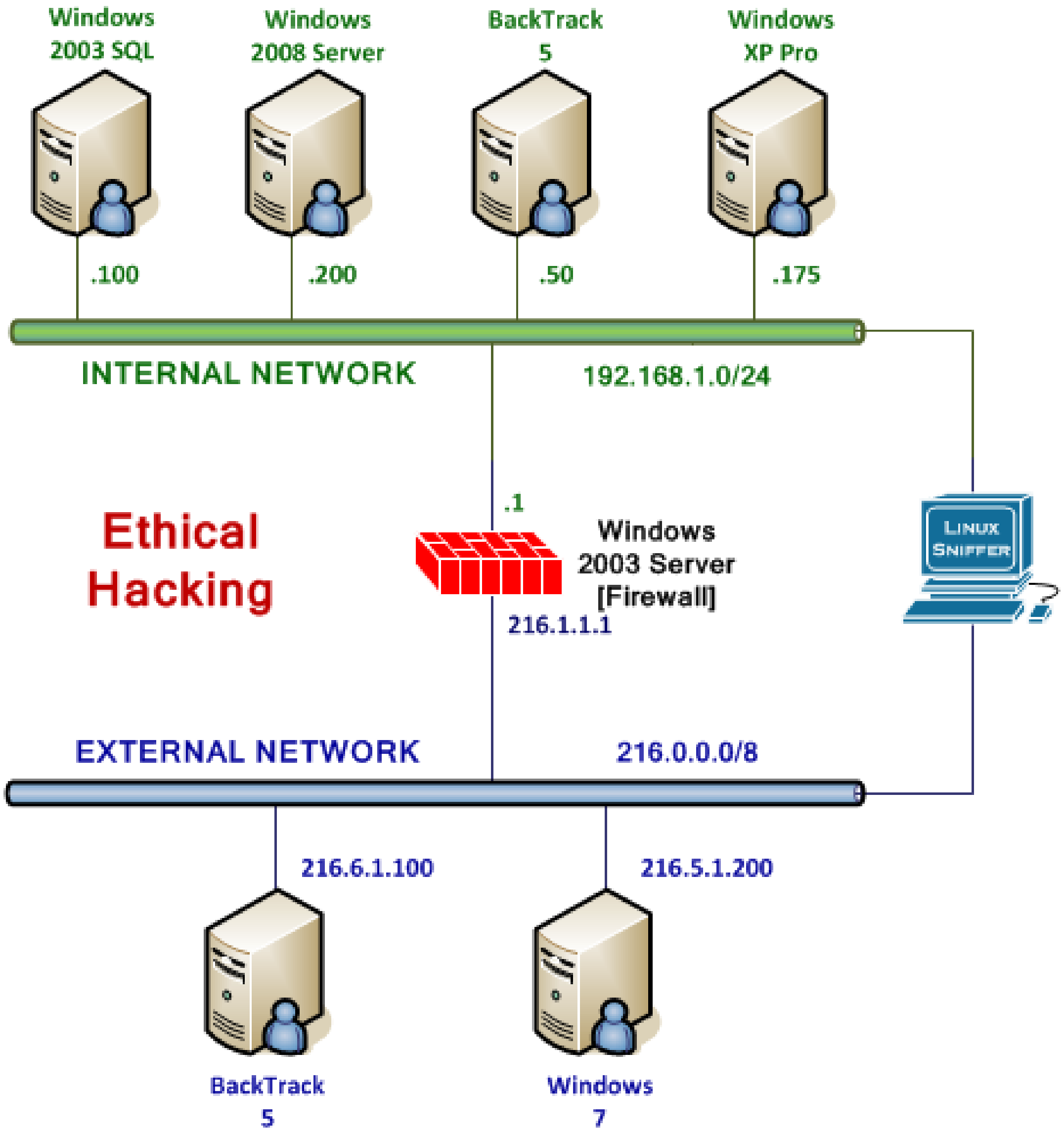


Figure 1: Lab Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

This lab requires the use of the Windows XP, Windows 7, Windows Server 2003 SQL, and Linux Sniffer machines.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows 2003 SQL	192.168.1.100	sperkins	northcarolina
Windows XP Pro	192.168.1.175	Administrator	Ethicalhackin&
Windows 7	216.5.1.200	student	password
Linux Sniffer	NO IP ADDRESS	root	toor

1 Plain Text Email Traffic - tcpdump

Part of a network administrator's job can be to capture and analyze network traffic. This is done for a variety of reasons, including the identification of the cause of bottlenecks, determining who is responsible for certain download activity, or analyzing an intrusion. There are also some ethical issues to consider as a network administrator can view email messages and credentials. For this reason, email encryption is important.

1.1 Capturing Plain Text Email Traffic with tcpdump

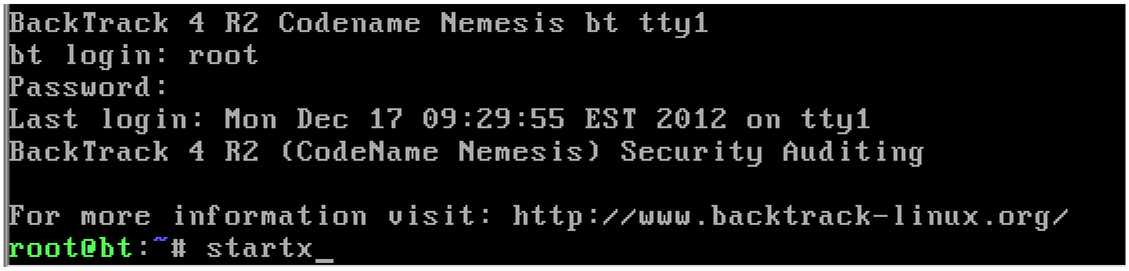
The Linux distribution BackTrack is installed on the sniffer machine. BackTrack is a distribution used by security professionals for pentration testing and forensics.

Log on to the sniffer

1. Log into the **Linux Sniffer** with the *username* of **root** with the *password* of **toor**.

   For security purposes, the password will not be displayed.

2. Type the following command to initialize the GUI, Graphical User Environment:
   root@bt:~# **startx**



```
BackTrack 4 R2 Codename Nemesis bt tty1
bt login: root
Password:
Last login: Mon Dec 17 09:29:55 EST 2012 on tty1
BackTrack 4 R2 (CodeName Nemesis) Security Auditing

For more information visit: http://www.backtrack-linux.org/
root@bt:~# startx_
```

Figure 2: Logging on to the Sniffer

3. Open a terminal on the Linux system by clicking on the picture to the right of Firefox in the task bar, located at the bottom of the screen in BackTrack.

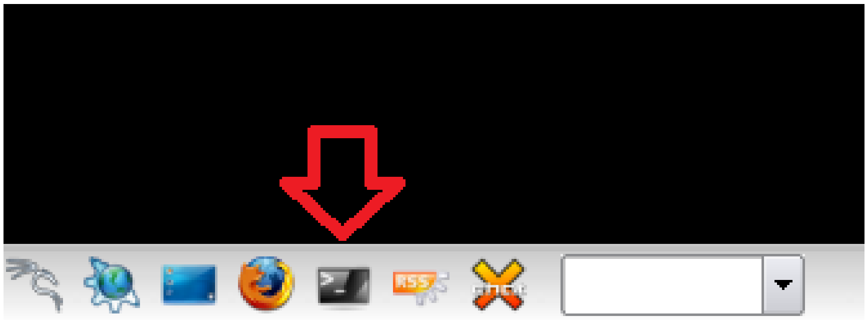
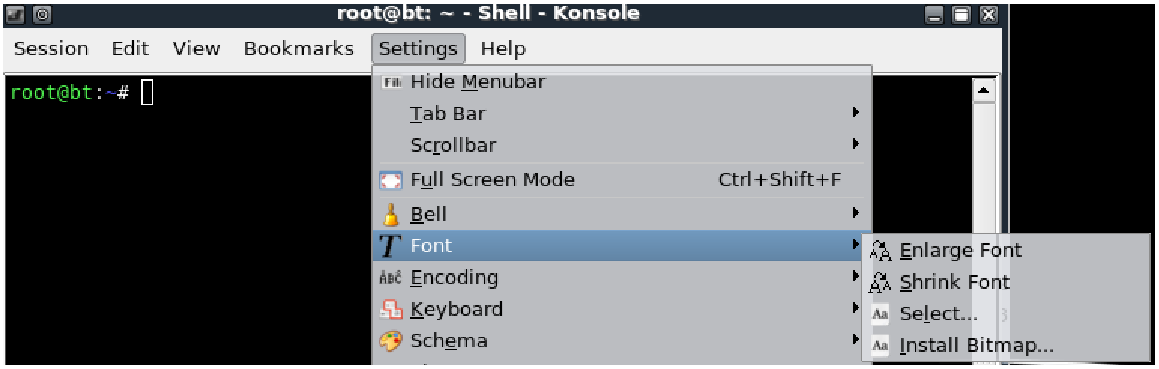


Figure 3: The Terminal Windows within BackTrack

After opening the terminal, you may want to consider adjusting the size of the font.

4. To increase the font size within the terminal, click **Settings** from the Terminal menu bar, select **Font**, then select **Enlarge Font**. Repeat this step if necessary.

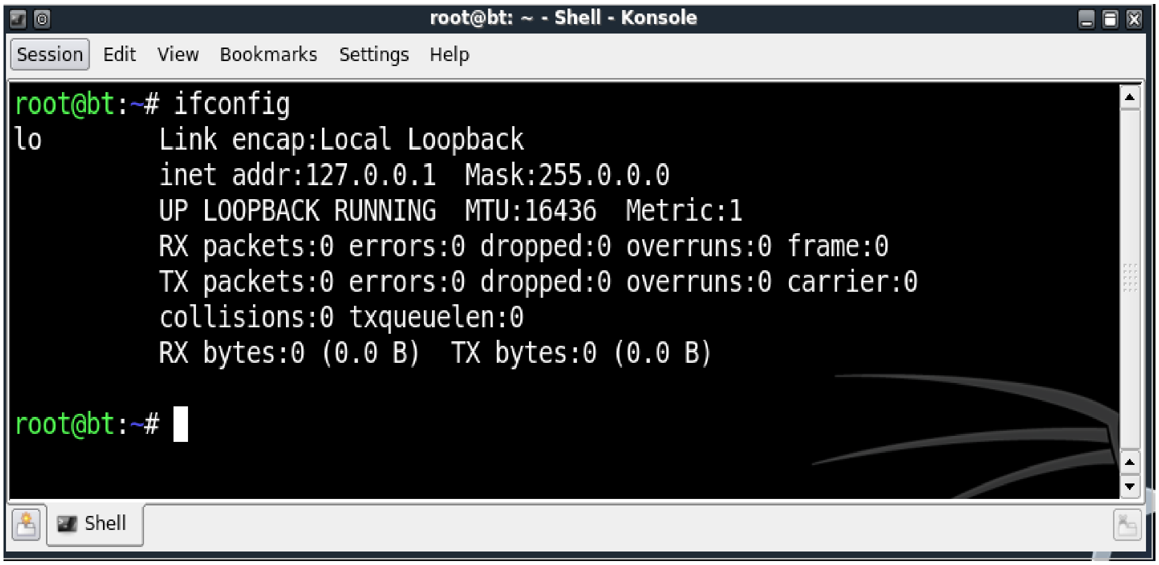


```
root@bt:~#
```

Figure 4: Increase the Font Size of the Terminal Windows

One of the nice features about some versions of BackTrack is they are not automatically assigned IP addresses through the use of DHCP, or Dynamic Host Configuration Protocol. The idea is to come on the network quietly, without being detected.

5. Only the loopback address, 127.0.0.1, is displayed when you type:
   root@bt:~# **ifconfig**

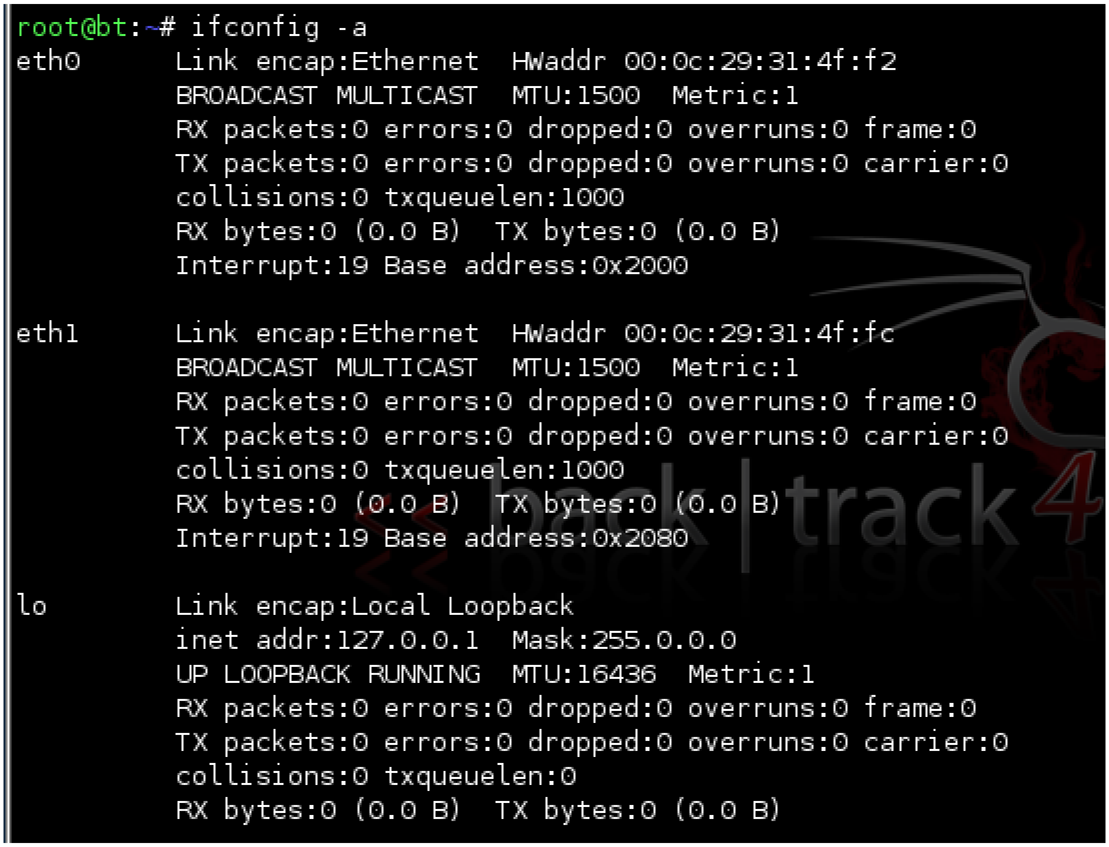

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
root@bt:~# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~#
```

Figure 5: No IP address, other than the Loopback Address of 127.0.0.1, are Displayed

6. Type the following command to view all available interfaces on the system:
   root@bt:~# **ifconfig -a**



```
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:f2
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:fc
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figure 6: All Available Interfaces on the System

A sniffer should be operating in promiscuous mode so it can see all network traffic.

Two ways to ensure that a sniffer will capture all traffic on a network segment are:

- Connect the Sniffer and other devices on the Network to a Hub
- Connect the Sniffer to a switch’s SPAN (Switched Port Analyzer Network) port.

In this lab, we will only be capturing traffic on the internal network (Network # 1 in the figure below), so only interface eth0 will be used to capture traffic. It will not be necessary to capture traffic on the external network (Network # 2) with the eth1 interface.

Neither of the interfaces, eth0 or eth1, are assigned IP addresses on their respective networks. The reason the sniffer has two interfaces is that it is located on two networks.

The Windows Firewall also has 2 interfaces and is connected to both networks.

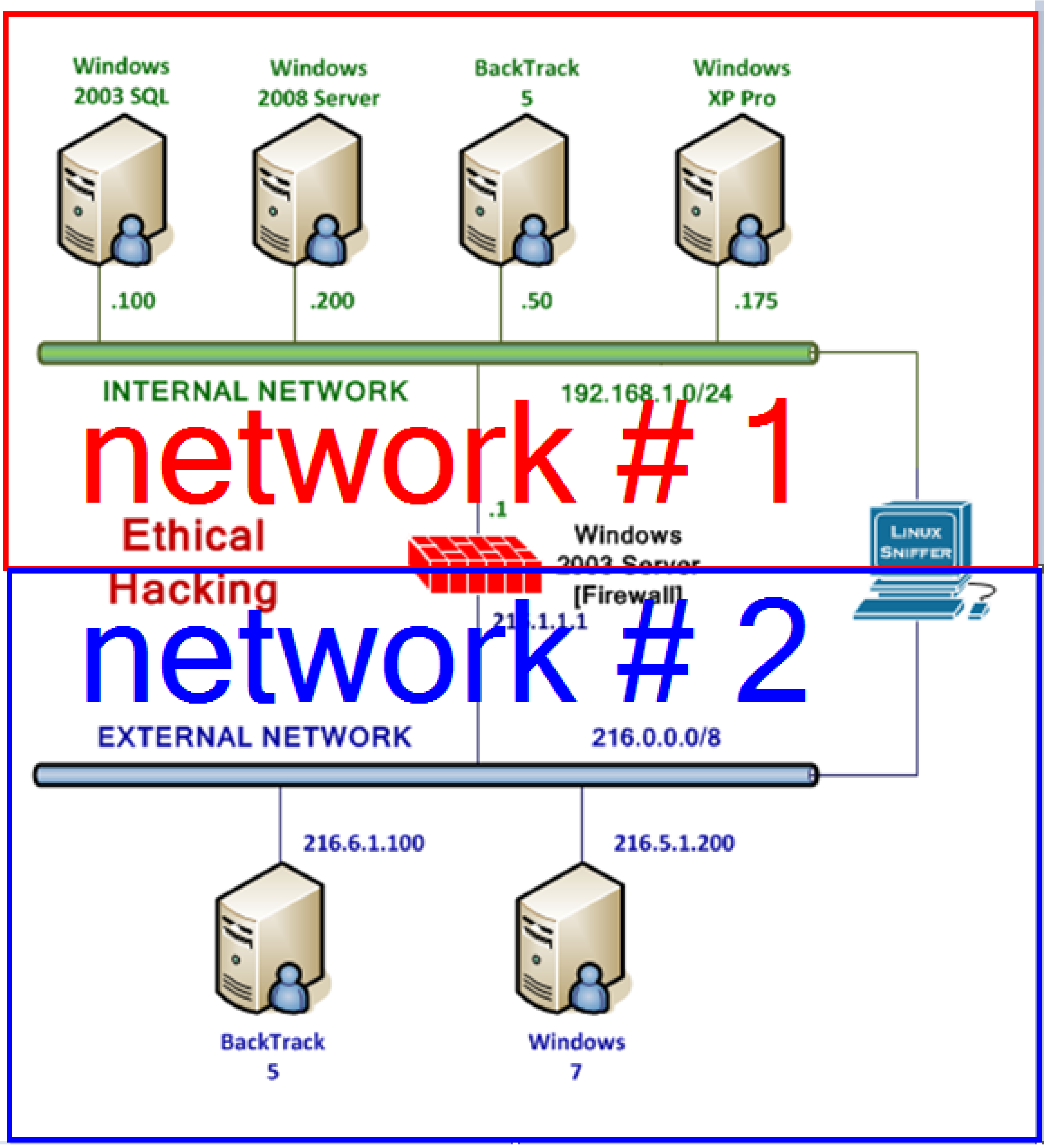
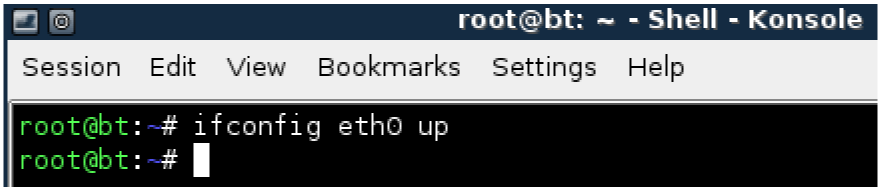


Figure 7: The Sniffer is Connected to Two Networks

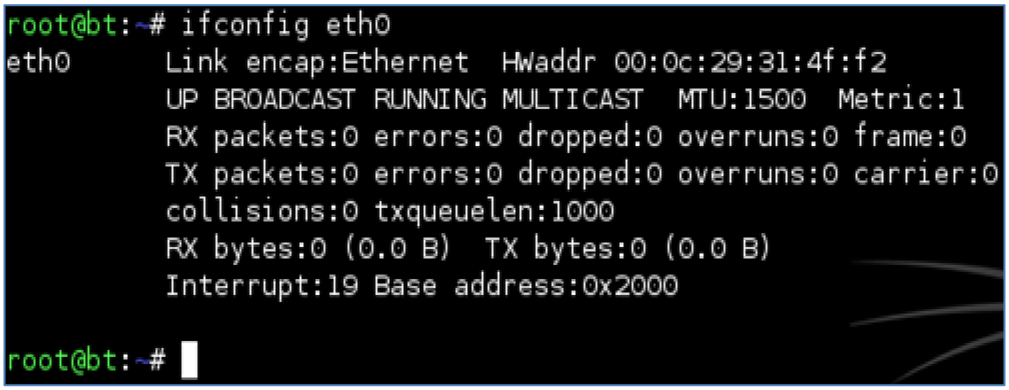
7. To activate the first interface, type the following command:
   root@bt:~# **ifconfig eth0 up**


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
root@bt:~# ifconfig eth0 up
root@bt:~# █
```

Figure 8: Activating the First Interface

8. To verify the first interface, type the following command:
   root@bt:~# **ifconfig eth0**



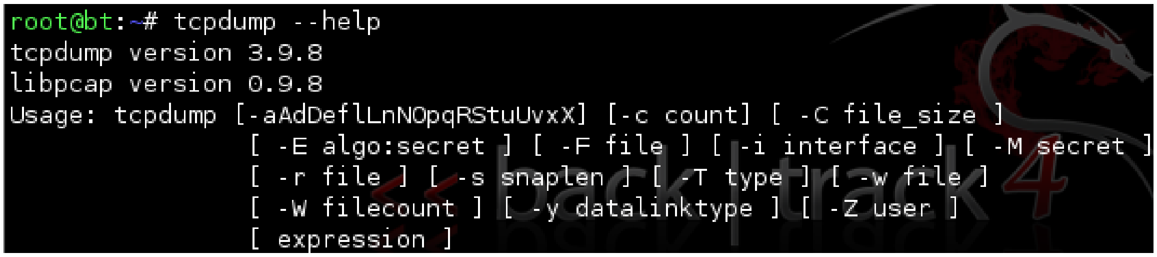
```
root@bt:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:f2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

root@bt:~#
```

Figure 9: The Interface is activated without an IP address

The Linux/UNIX utility tcpdump is commonly used by network administrators to capture network traffic on a sniffer. Many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark or Network Miner is not possible. Another benefit to using tcpdump is it handles very large capture files with no problem.

9. Type the following command to view several available switches for tcpdump:
   root@bt:~# **tcpdump --help**

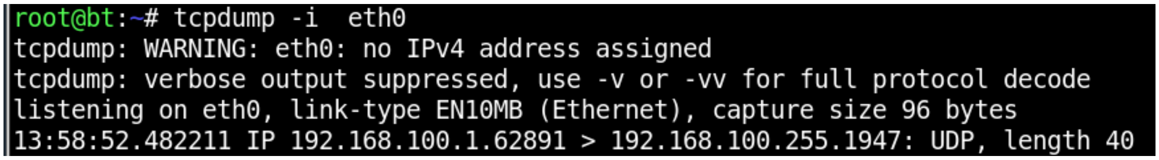


```
root@bt:~# tcpdump --help
tcpdump version 3.9.8
libpcap version 0.9.8
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
               [ -E algo:secret ] [ -F file ] [ -i interface ] [ -M secret ]
               [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ] [ -y datalinktype ] [ -Z user ]
               [ expression ]
```

Figure 10: The Available Options for tcpdump

10. To run tcpdump on the network segment interface eth0 is connected to, type:
    root@bt:~# **tcpdump -i eth0**

Wait until at least one packet is displayed before stopping the capture.

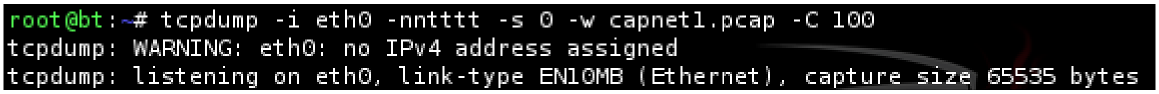


```
root@bt:~# tcpdump -i  eth0
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:58:52.482211 IP 192.168.100.1.62891 > 192.168.100.255.1947: UDP, length 40
```

Figure 11: The output of tcpdump on the network segment interface eth0 is connected

After a packet or more is displayed, hit CTRL+C to stop the network capture.
If the network 192.168.1.0/24 is displayed, eth0 is located on the first network.
If the network 216.0.0.0/8 is displayed, eth0 is located on the second network.
Also, notice that the default for tcpdump is to only capture the first 96 bytes.

11. To capture traffic on the 192.168.1.0/24 network and send it to a file, type:
    root@bt:~# **tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100**

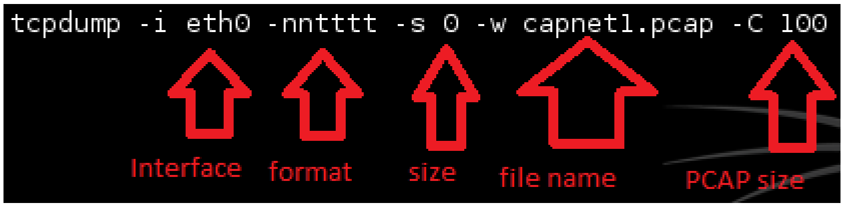


```
root@bt:~# tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

Figure 12: tcpdump syntax

The following details the switches used with the tcpdump command:

Switch	Purpose
-i eth0	Use Interface Zero
-nntttt	Disable DNS Resolution, Date and Time Format
-s 0	Disables Default Packet Size of 96 bytes, full packet size
-w	Write to a capture file, instead of displaying to the screen
-C	Split the captures into files of this size



```
tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
```

Figure 13: Detailed tcpdump Syntax Explained

12. Log on as *Administrator* to the **Windows XP Pro** with the password of **Ethicalhackin&**

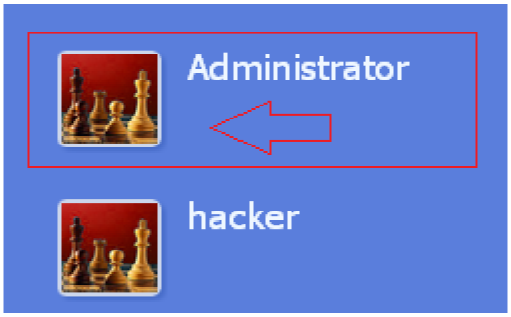


Figure 14: Logging in as Administrator

13. Click on the **Start** button on XP and then select **E-mail** from the Start Menu.

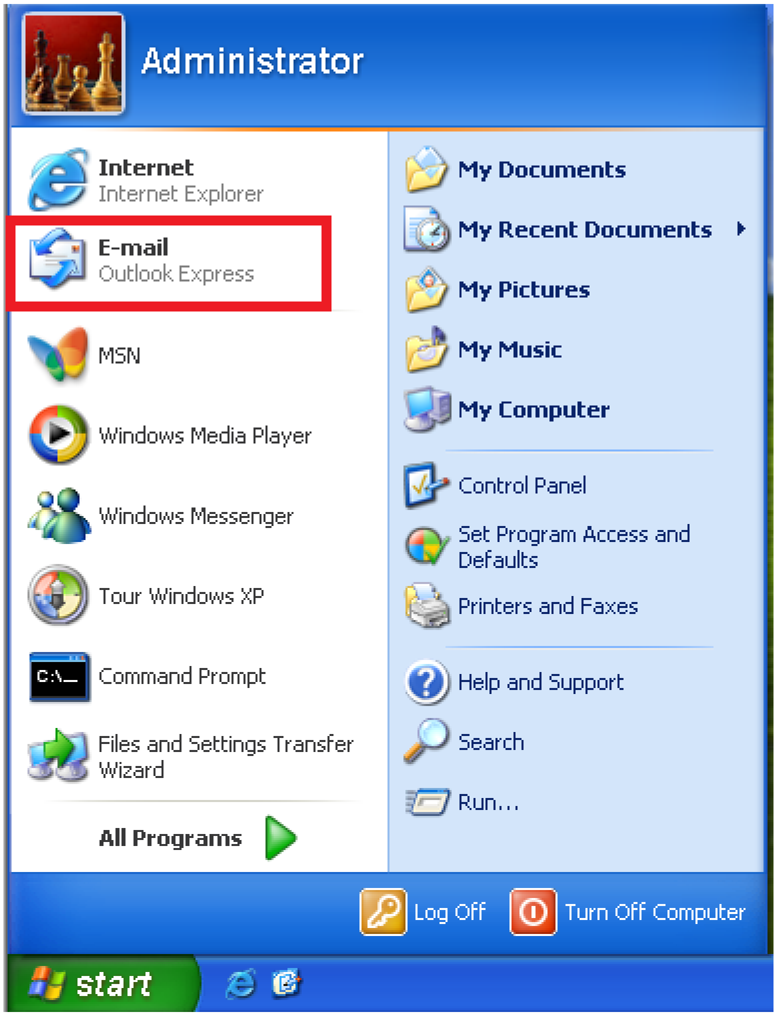


Figure 15: Opening Outlook Express

14. Click **Create Mail** to create an email message. The *New Message* box will open.

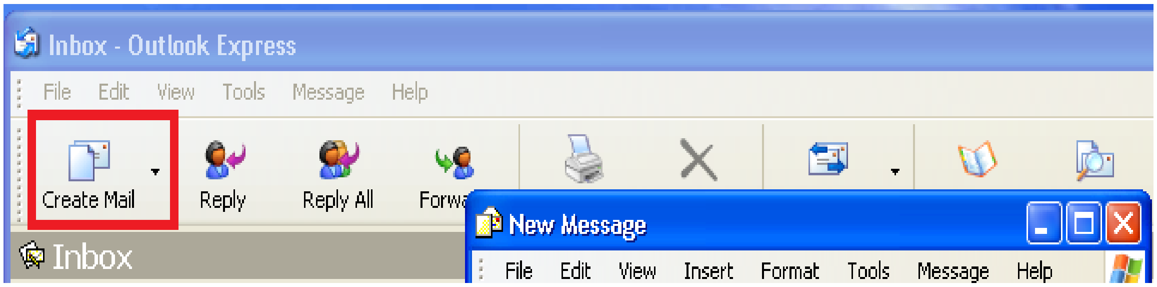

Inbox - Outlook Express
File Edit View Tools Message Help
Create Mail
Reply
Reply All
Forwa
Inbox
New Message
File Edit View Insert Format Tools Message Help

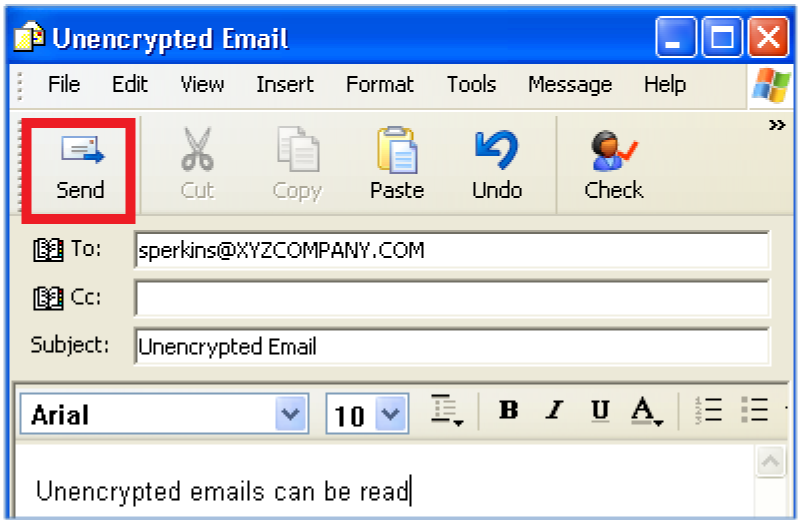
Figure 16: Creating a New Email Message

15. Follow the steps below to successfully send the email to sperkins.

- In the **To** box, type sperkins@XYZCOMPANY.COM
- In the **Subject** type, **Unencrypted Email**
- In the **message** area, type:

  Unencrypted emails can be read

After completing the three above steps, click **Send** to send the email.



To: sperkins@XYZCOMPANY.COM

Cc:

Subject: Unencrypted Email

Unencrypted emails can be read

Figure 17: Sending the Email Message

16. Click the **Send/Receive** button to ensure that the email is sent.

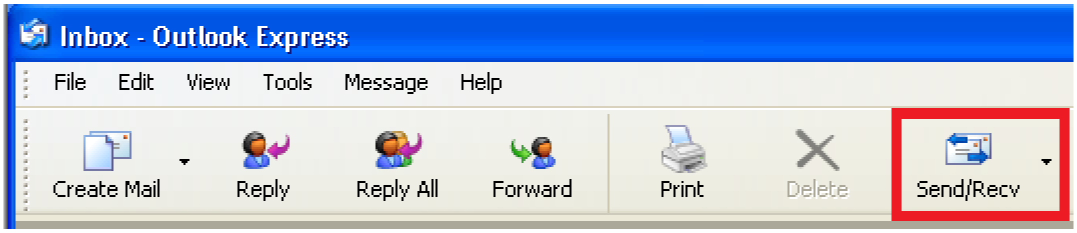
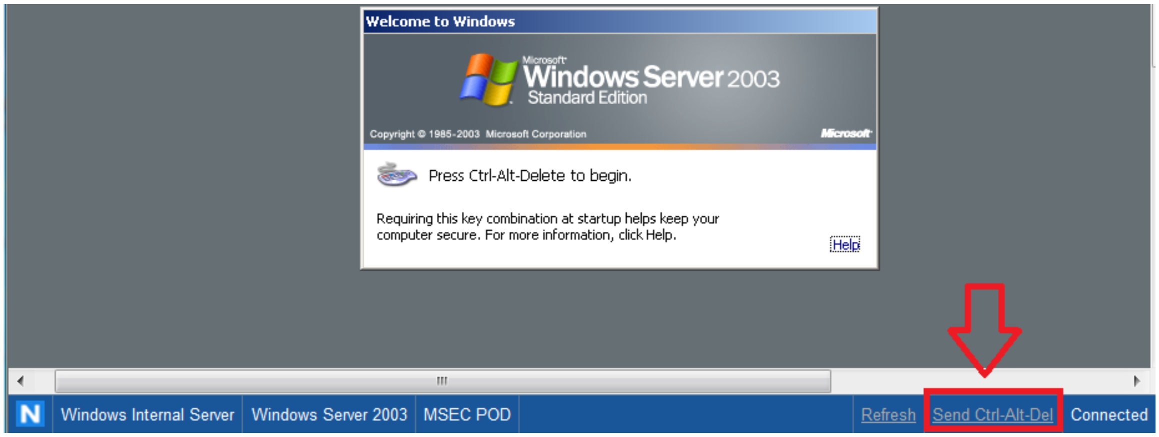


Figure 18: Sending the Email Message

If you receive an error message, it would mean that the email address was typed incorrectly. The only way to fix this issue is to delete the message from the Outbox.

17. Log on to the **Windows 2003 SQL** Server. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on to the 2003 server with the username of **sperkins** and the password of **northcarolina**.



Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 19: Send Ctrl-Alt-Del to the Windows 2003 Server

18. Click on **Start** on 2003 and select **Outlook Express** from the Start Menu.

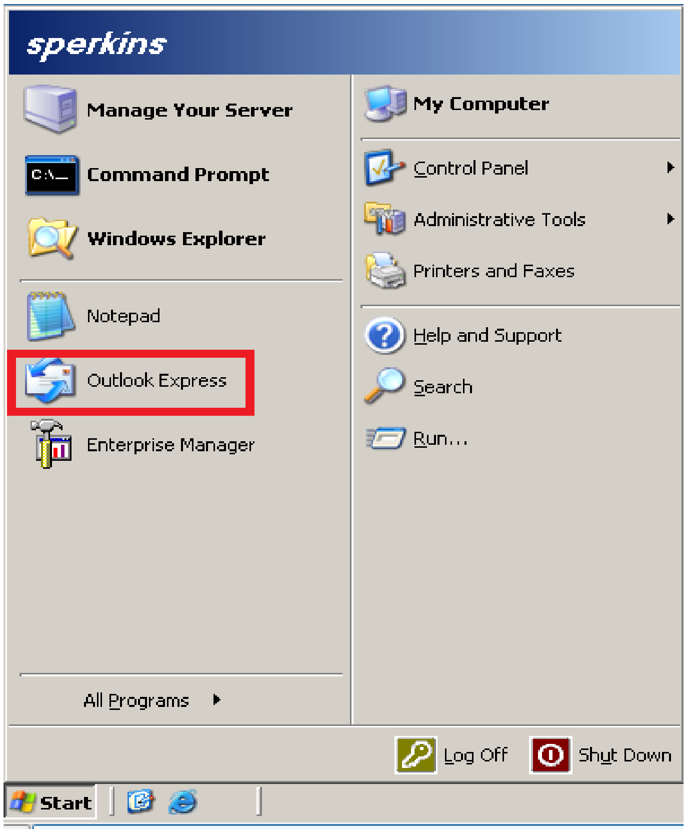


Figure 20: Opening Outlook Express

19. Click the **Send/Receive** button to receive rmiller's email.

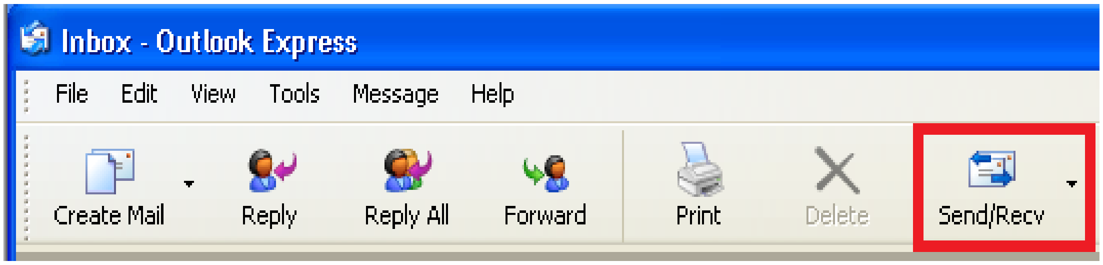
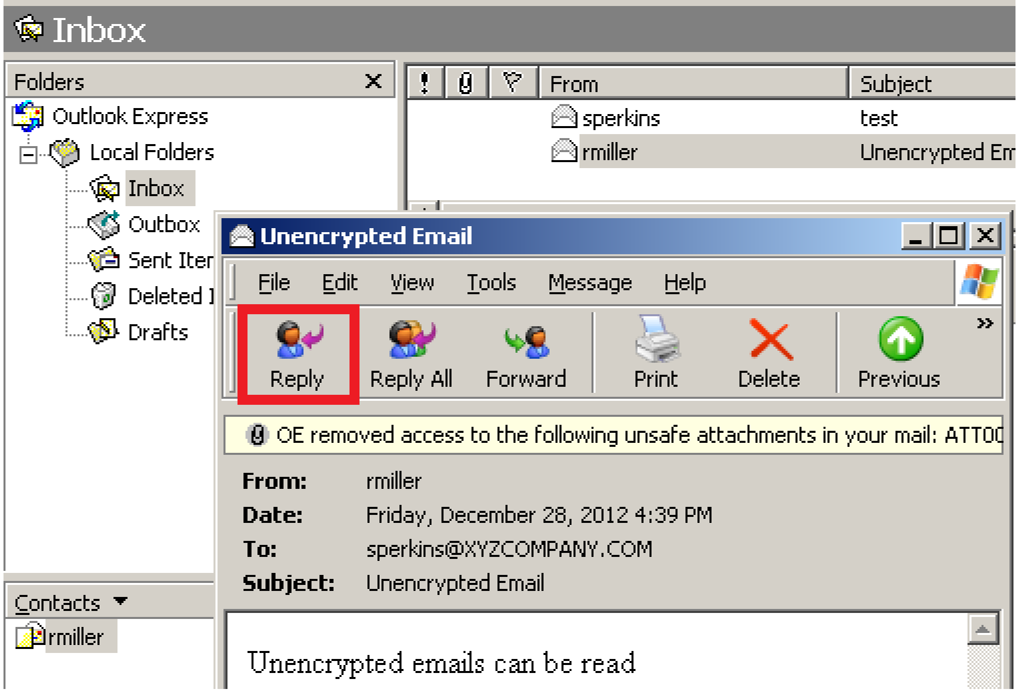


Figure 21: Sending the Email Message

20. The email from rmiller should appear in the Inbox with the subject and message. Click the **Reply** button to reply to the email message from sperkins.



From	Subject
sperkins	test
rmiller	Unencrypted Em

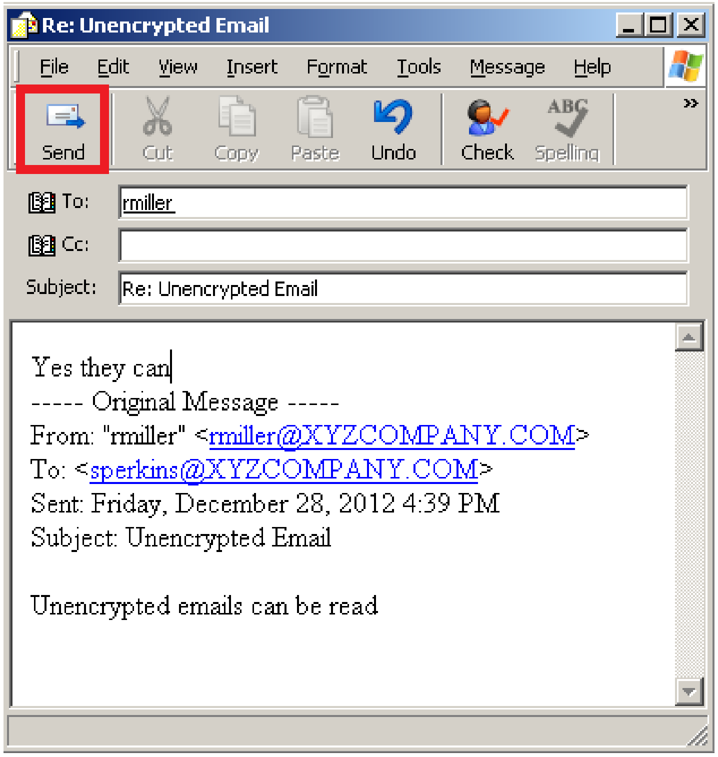
OE removed access to the following unsafe attachments in your mail: ATT00

From: rmiller
Date: Friday, December 28, 2012 4:39 PM
To: sperkins@XYZCOMPANY.COM
Subject: Unencrypted Email

Unencrypted emails can be read

Figure 22: Replying to the Email Message

21. In the message area, type **Yes they can**. Click **Send** to send the email message.



To: rmiller
Cc:
Subject: Re: Unencrypted Email

Yes they can
----- Original Message -----
From: "rmiller" <rmiller@XYZCOMPANY.COM>
To: <sperkins@XYZCOMPANY.COM>
Sent: Friday, December 28, 2012 4:39 PM
Subject: Unencrypted Email

Unencrypted emails can be read

Figure 23: Sending the Reply

22. Click the **Send/Receive** button to send the reply to rmiller.

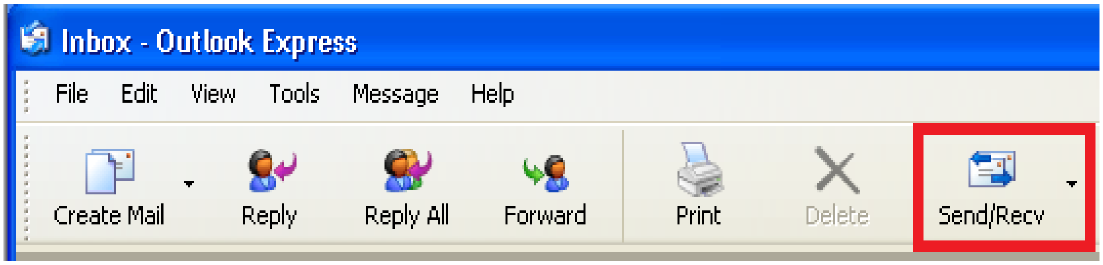
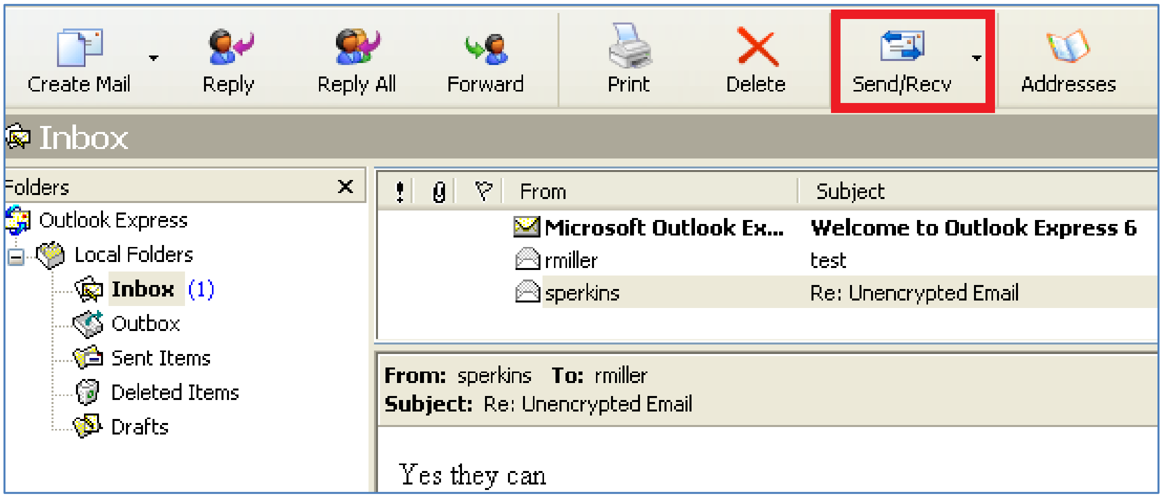


Figure 24: Sending the Email Message

23. On **Windows XP Pro**, Click the **Send/Receive** button to ensure that the reply is received.



From	Subject
Microsoft Outlook Ex...	**Welcome to Outlook Express 6**
rmiller	test
sperkins	Re: Unencrypted Email

From: sperkins **To:** rmiller
Subject: Re: Unencrypted Email

Yes they can

Figure 25: Clicking Send/Receive

1.2 Conclusion

The tcpdump command is built into the Linux and Unix operating systems. It can be used to capture network traffic. The benefits of using tcpdump include the fact that many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark is not possible. Another benefit to using tcpdump is it handles very large capture files with no problem, and it allows you to filter for specific traffic. In the next task, you will be able to view plain text emails and passwords within the pcap file.

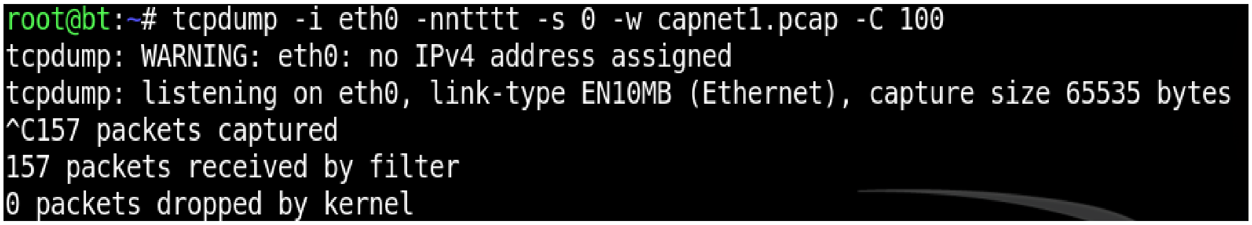
2 Plain Text Email Traffic - Wireshark

Wireshark is a GUI, or Graphical User Interface, tool that will allow you to capture and analyze network traffic. Wireshark runs on Windows, Linux, and on Mac OS X. Wireshark can be downloaded from the following link: http://www.wireshark.org/download.html.

2.1 Analyze Plain Text Email Traffic Using Wireshark

1. After sending the plain text emails between rmiller and sperkins, we can stop the capture. Press **CTRL+C** to stop tcpdump from running and capturing network traffic. You should receive a message about the number of packets that were captured by tcpdump.

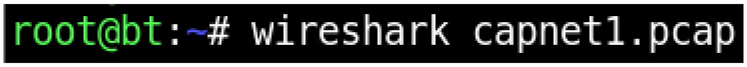
The number of packets captured will vary.



```
root@bt:~# tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C157 packets captured
157 packets received by filter
0 packets dropped by kernel
```

Figure 26: Opening the tcpdump capture with Wireshark

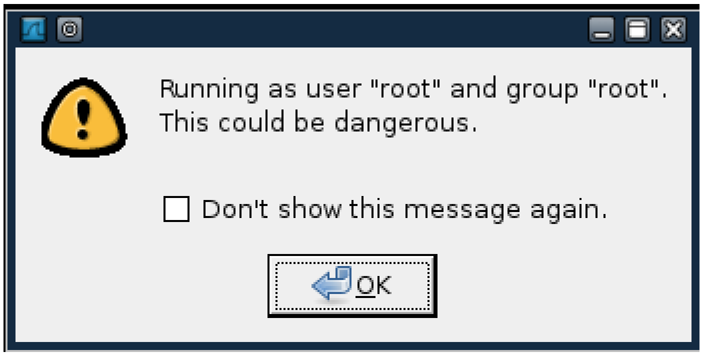
2. To view the capture file, type the following command at the Linux Sniffer terminal:
   root@bt:~# **wireshark capnet1.pcap**



```
root@bt:~# wireshark capnet1.pcap
```

Figure 27: Opening the tcpdump capture with Wireshark

3. Check the **Don't show the message again** box and click the **OK** button.



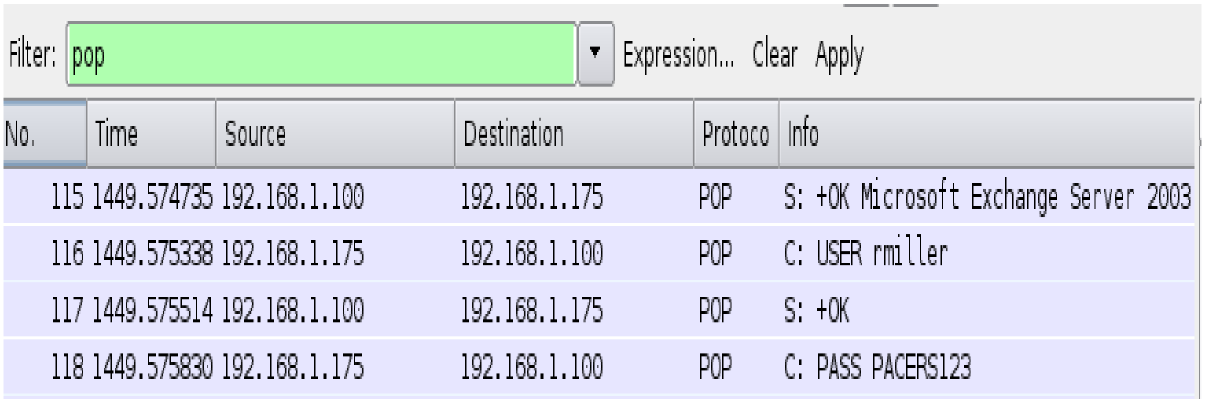
Running as user "root" and group "root". This could be dangerous.

□ Don't show this message again.

Figure 28: Opening the tcpdump capture with Wireshark

Email is often received by using the POP3, or Post Office Protocol version 3, protocol. By default, most POP traffic is transmitted in clear text. Many organizations still use POP.

4. Type **pop** in the Wireshark filter pane and click **Apply** to view the traffic.



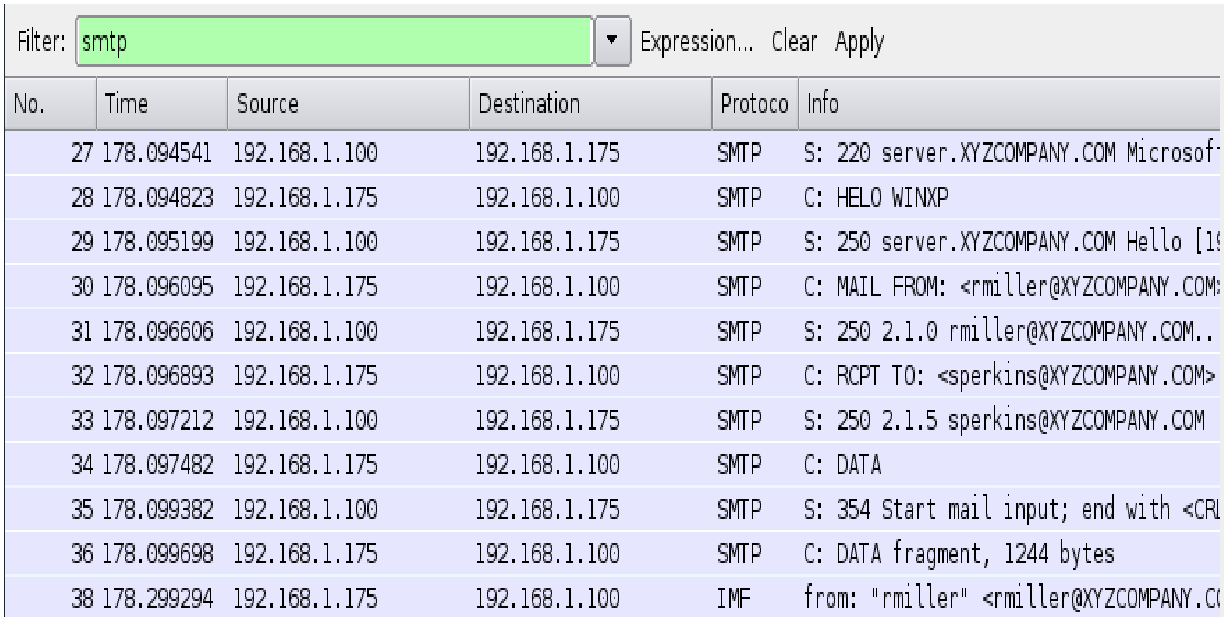
Filter: pop

No.	Time	Source	Destination	Protoco	Info
115	1449.574735	192.168.1.100	192.168.1.175	POP	S: +OK Microsoft Exchange Server 2003
116	1449.575338	192.168.1.175	192.168.1.100	POP	C: USER rmiller
117	1449.575514	192.168.1.100	192.168.1.175	POP	S: +OK
118	1449.575830	192.168.1.175	192.168.1.100	POP	C: PASS PACERS123

Figure 29: POP Traffic within Wireshark

Email is often sent by using the SMTP, or Simple Mail Transfer Protocol. By default, most SMTP traffic is transmitted in clear text. Many organizations use SMTP, and many SMTP servers do not require authentication, which can make them a target of spammers.

5. Type **smtp** in the Wireshark filter pane and click **Apply** to view the traffic.

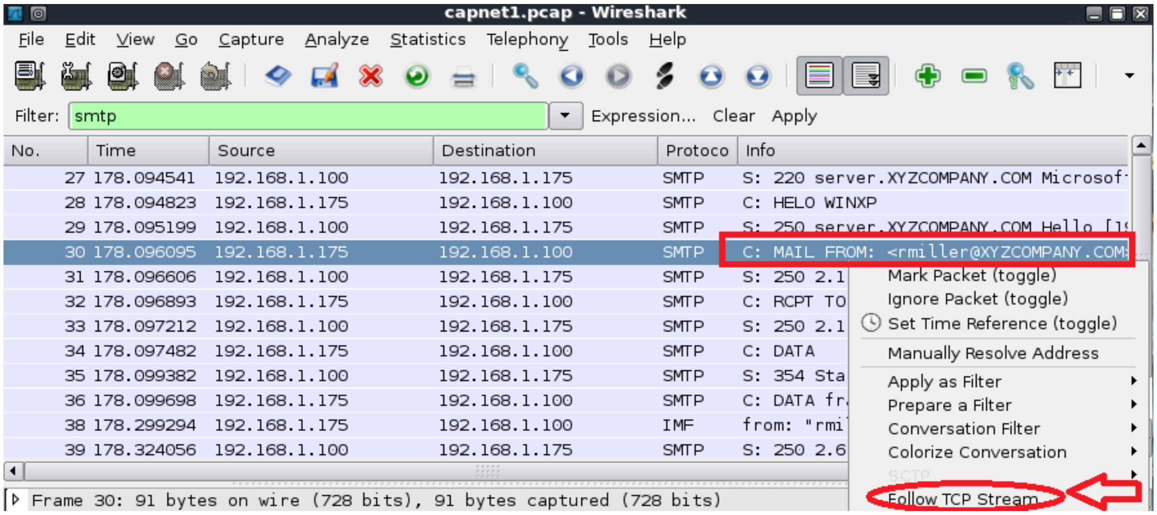


Filter: smtp

No.	Time	Source	Destination	Protoco	Info
27	178.094541	192.168.1.100	192.168.1.175	SMTP	S: 220 server.XYZCOMPANY.COM Microsof
28	178.094823	192.168.1.175	192.168.1.100	SMTP	C: HELO WINXP
29	178.095199	192.168.1.100	192.168.1.175	SMTP	S: 250 server.XYZCOMPANY.COM Hello [1
30	178.096095	192.168.1.175	192.168.1.100	SMTP	C: MAIL FROM: <rmiller@XYZCOMPANY.COM
31	178.096606	192.168.1.100	192.168.1.175	SMTP	S: 250 2.1.0 rmiller@XYZCOMPANY.COM..
32	178.096893	192.168.1.175	192.168.1.100	SMTP	C: RCPT TO: <sperkins@XYZCOMPANY.COM>
33	178.097212	192.168.1.100	192.168.1.175	SMTP	S: 250 2.1.5 sperkins@XYZCOMPANY.COM
34	178.097482	192.168.1.175	192.168.1.100	SMTP	C: DATA
35	178.099382	192.168.1.100	192.168.1.175	SMTP	S: 354 Start mail input; end with <CR
36	178.099698	192.168.1.175	192.168.1.100	SMTP	C: DATA fragment, 1244 bytes
38	178.299294	192.168.1.175	192.168.1.100	IMF	from: "rmiller" <rmiller@XYZCOMPANY.C

Figure 30: SMTP Traffic within Wireshark

6. Right-click on the packet that says **MAIL FROM:** *and select* **Follow TCP stream**.

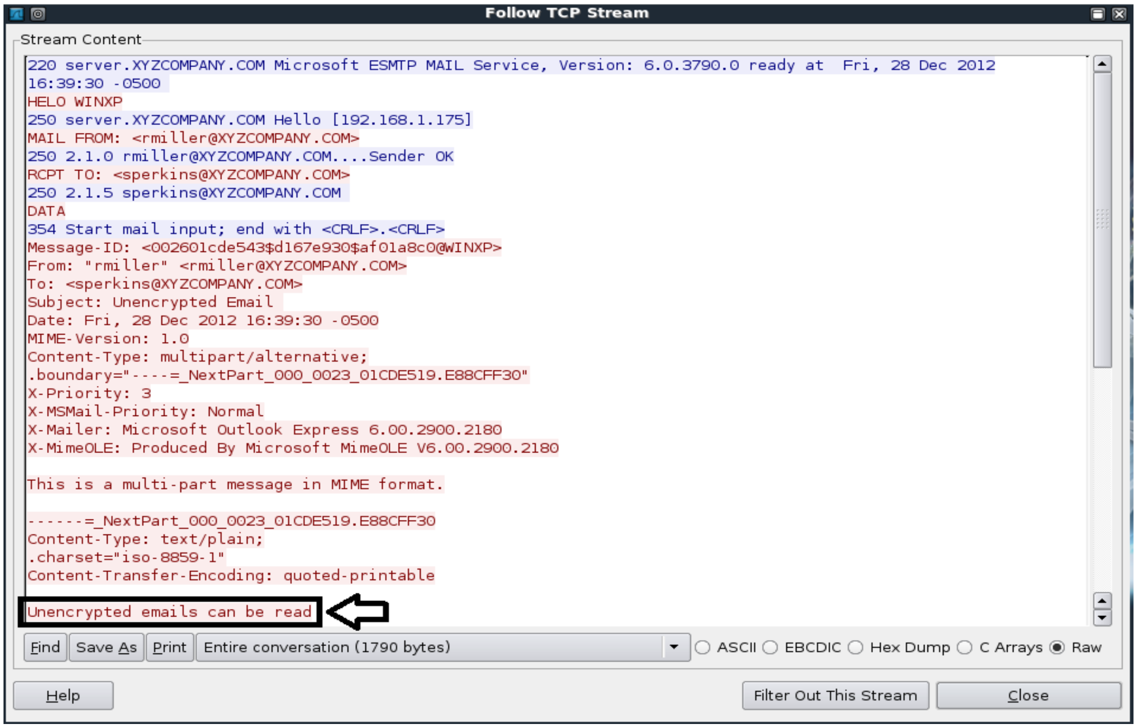


```
No.  Time        Source         Destination    Protoco Info
  27 178.094541  192.168.1.100  192.168.1.175  SMTP    S: 220 server.XYZCOMPANY.COM Microsof
  28 178.094823  192.168.1.175  192.168.1.100  SMTP    C: HELO WINXP
  29 178.095199  192.168.1.100  192.168.1.175  SMTP    S: 250 server.XYZCOMPANY.COM Hello [1
  30 178.096095  192.168.1.175  192.168.1.100  SMTP    C: MAIL FROM: <rmiller@XYZCOMPANY.COM>
  31 178.096606  192.168.1.100  192.168.1.175  SMTP    S: 250 2.1
  32 178.096893  192.168.1.175  192.168.1.100  SMTP    C: RCPT TO
  33 178.097212  192.168.1.100  192.168.1.175  SMTP    S: 250 2.1
  34 178.097482  192.168.1.175  192.168.1.100  SMTP    C: DATA
  35 178.099382  192.168.1.100  192.168.1.175  SMTP    S: 354 Sta
  36 178.099698  192.168.1.175  192.168.1.100  SMTP    C: DATA fr
  38 178.299294  192.168.1.175  192.168.1.100  IMF     from: "rmi
  39 178.324056  192.168.1.100  192.168.1.175  SMTP    S: 250 2.6

Frame 30: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
```

Figure 31: Opening the tcpdump capture with Wireshark

Within the TCP stream, you will be able to view the unencrypted email within Wireshark. After viewing the plain text message SMTP stream, click the **Close** button.



```
220 server.XYZCOMPANY.COM Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at  Fri, 28 Dec 2012
16:39:30 -0500
HELO WINXP
250 server.XYZCOMPANY.COM Hello [192.168.1.175]
MAIL FROM: <rmiller@XYZCOMPANY.COM>
250 2.1.0 rmiller@XYZCOMPANY.COM....Sender OK
RCPT TO: <sperkins@XYZCOMPANY.COM>
250 2.1.5 sperkins@XYZCOMPANY.COM
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Message-ID: <002601cde543$d167e930$af01a8c0@WINXP>
From: "rmiller" <rmiller@XYZCOMPANY.COM>
To: <sperkins@XYZCOMPANY.COM>
Subject: Unencrypted Email
Date: Fri, 28 Dec 2012 16:39:30 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
.boundary="----=_NextPart_000_0023_01CDE519.E88CFF30"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

------=_NextPart_000_0023_01CDE519.E88CFF30
Content-Type: text/plain;
.charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Unencrypted emails can be read
```

Figure 32: The Plain Text Email Message is displayed within Wireshark

7. Close Wireshark by selecting **File** from the menu bar and selecting **Quit**.

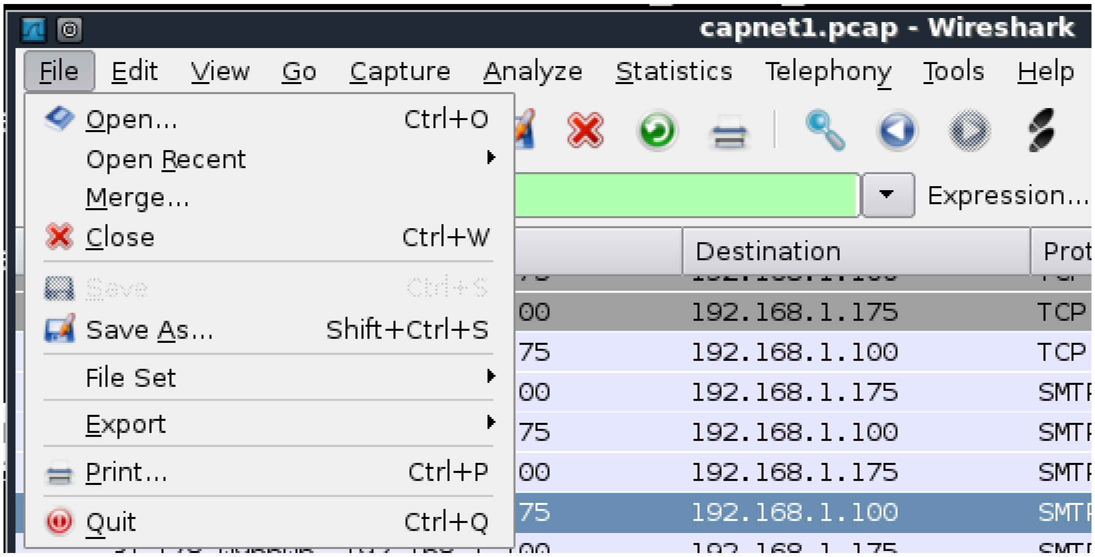


Figure 33: Closing the Wireshark Program

2.2 Conclusion

Wireshark is a GUI, or Graphical User Interface, tool that will allow you to analyze as well as capture network traffic. Wireshark runs on Windows, Linux, and Mac OS X. The Wireshark filter pane can be used to filter for various types of traffic, including pop and smtp. In this exercise, we used Wireshark to display plain text usernames, passwords, and email messages. By default, SMTP and POP traffic are transmitted in clear text.

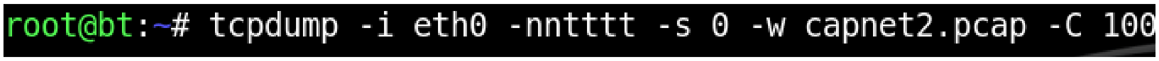
3 Encrypted Email Traffic - tcpdump

In this task, we will once again use the Linux tcpdump program on the sniffer. This time we should not be able to read the email message, which will be encrypted.

3.1 Capturing Encrypted Email Traffic with tcpdump

In this step, we will start the sniffer again using tcpdump with a different filename.

1. Open the **Linux Sniffer** machine again. To capture traffic on the 192.168.1.0/24 network and send it to a file, type:
   root@bt:~# **tcpdump -i eth0 -nntttt -s 0 -w capnet2.pcap -C 100**



```
root@bt:~# tcpdump -i eth0 -nntttt -s 0 -w capnet2.pcap -C 100
```

Figure 34: Running tcpdump with appropriate switches

2. Log back on to **Windows XP Pro** as **Administrator** with the password of **Ethicalhackin&**

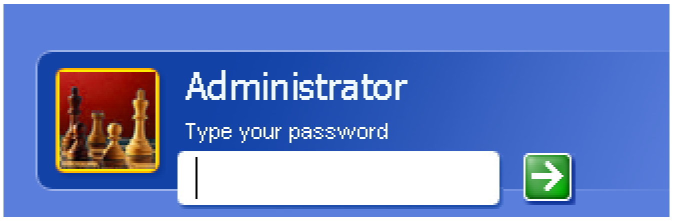


Figure 35: Log back in as Administrator

3. Open Outlook Express and click **Create Mail** to create an email message. The New Message box will open.

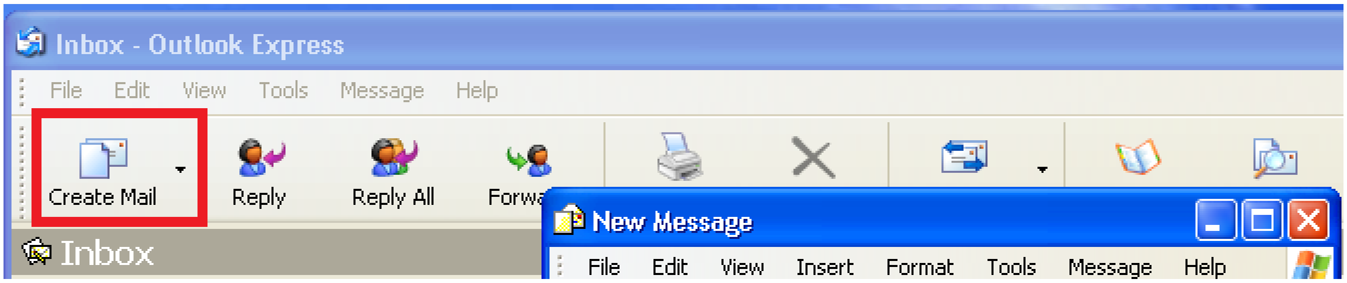


Figure 36: Creating a New Email Message

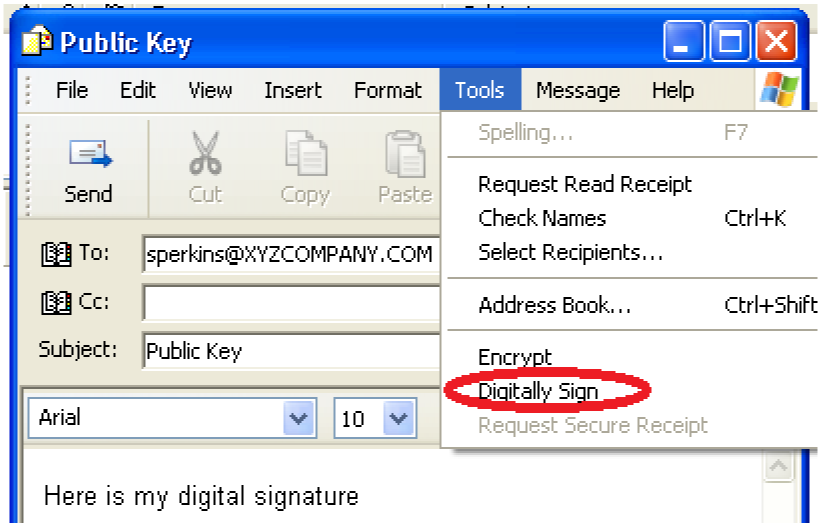
A Public Key is used to encrypt messages. A user can send their Public Key to another user by digitally signing an email message. The user will then use the public key provided to them by the sender to encrypt messages sent to that sender. Rmiller can send out his public key by digitally signing the email message he is sending to sperkins.

4. Follow the steps below to successfully send the email to sperkins.

- In the **To** box, type sperkins@XYZCOMPANY.COM
- In the **Subjec**t type, Public Key
- In the **message** area, type:

  Here is my digital signature

- From the **Tools** menu, select **Digitally Sign**.



To: sperkins@XYZCOMPANY.COM

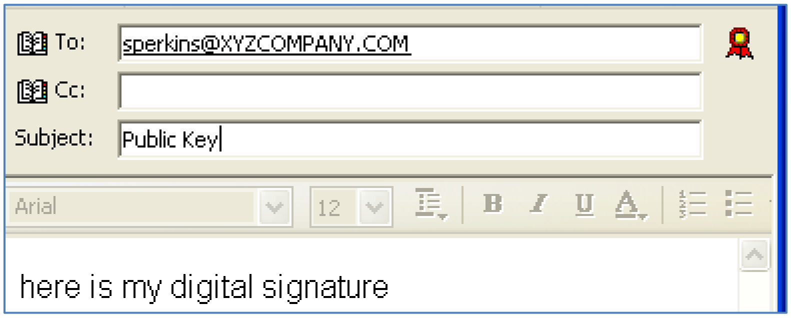
Subject: Public Key

Here is my digital signature

Figure 37: Digitally Signing the Email Message

5. Verify the email address is correct and click **Send** to send the email.

There should be a red ribbon to the right of the user's email address.



To: sperkins@XYZCOMPANY.COM

Subject: Public Key

here is my digital signature

Figure 38: Sending the Email Message

6. Click the **Send/Receive** button to ensure that the email is sent.

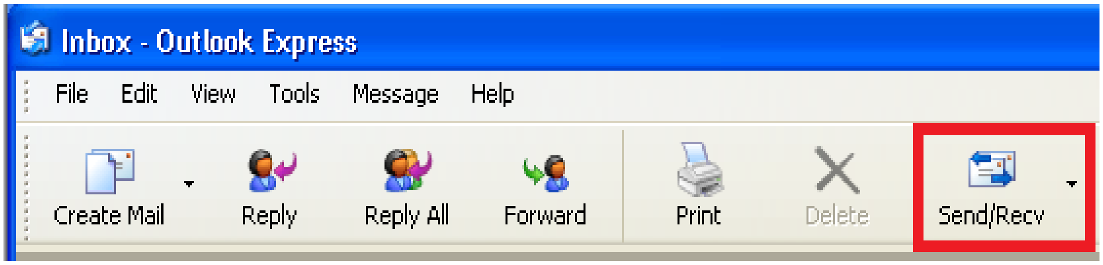
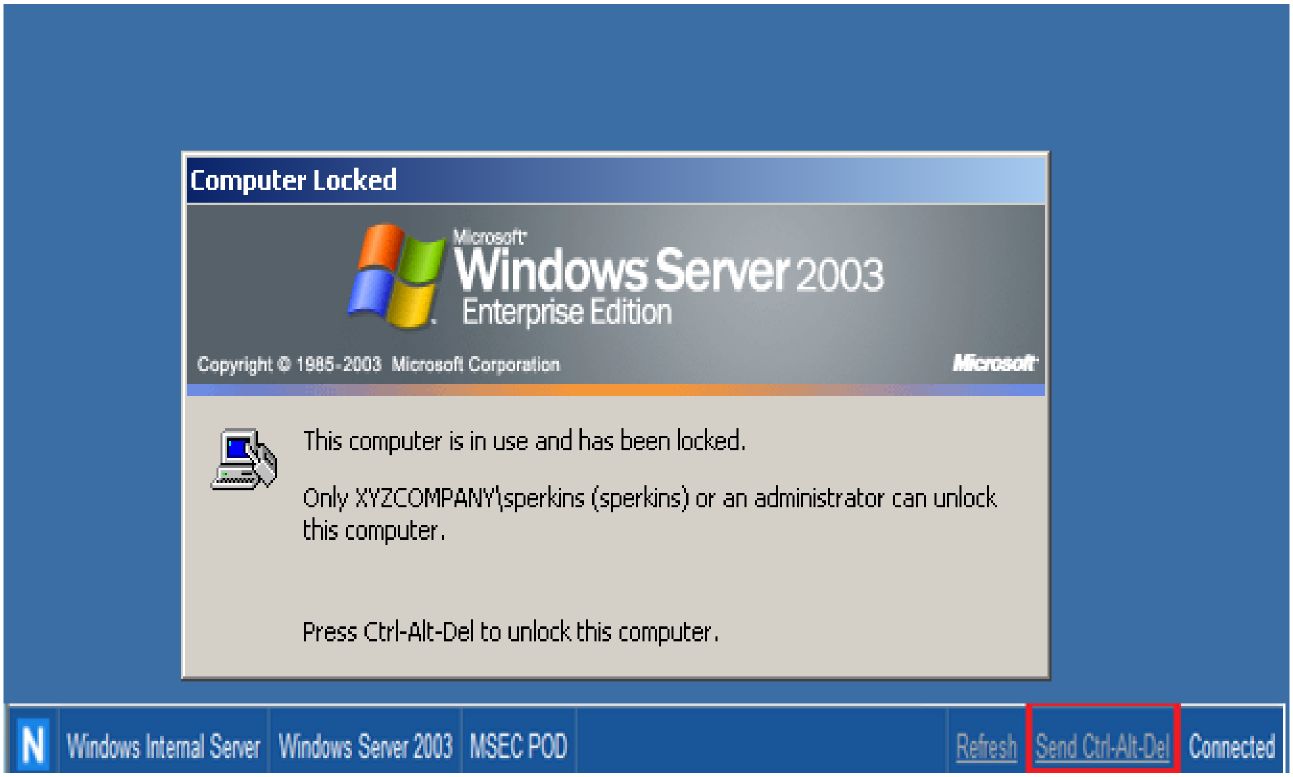


Figure 39: Ensuring that the Email is sent

If you receive an error message, it would mean that the email address was typed incorrectly. The only way to fix this issue is to delete the message from the Outbox.

7. Log on to the **Windows 2003 SQL** Server. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log back on to the 2003 server with as **sperkins** and the password of **northcarolina**.


Computer Locked
Microsoft Windows Server 2003 Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft

This computer is in use and has been locked.

Only XYZCOMPANY\sperkins (sperkins) or an administrator can unlock this computer.

Press Ctrl-Alt-Del to unlock this computer.

Figure 40: Send Ctrl-Alt-Del to the Windows 2003 Server

8. On **Windows 2003 SQL**, click the **Send/Receive** button to receive sperkins's email.

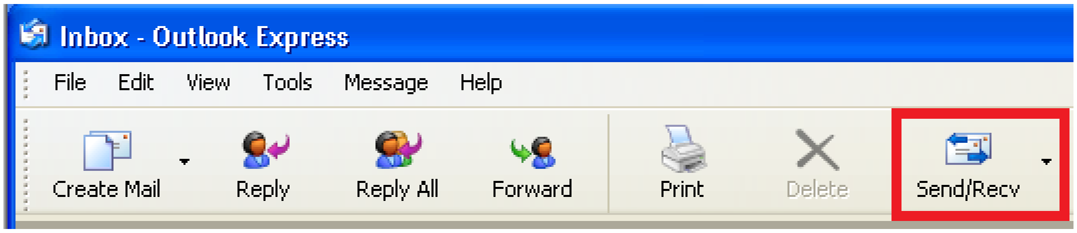
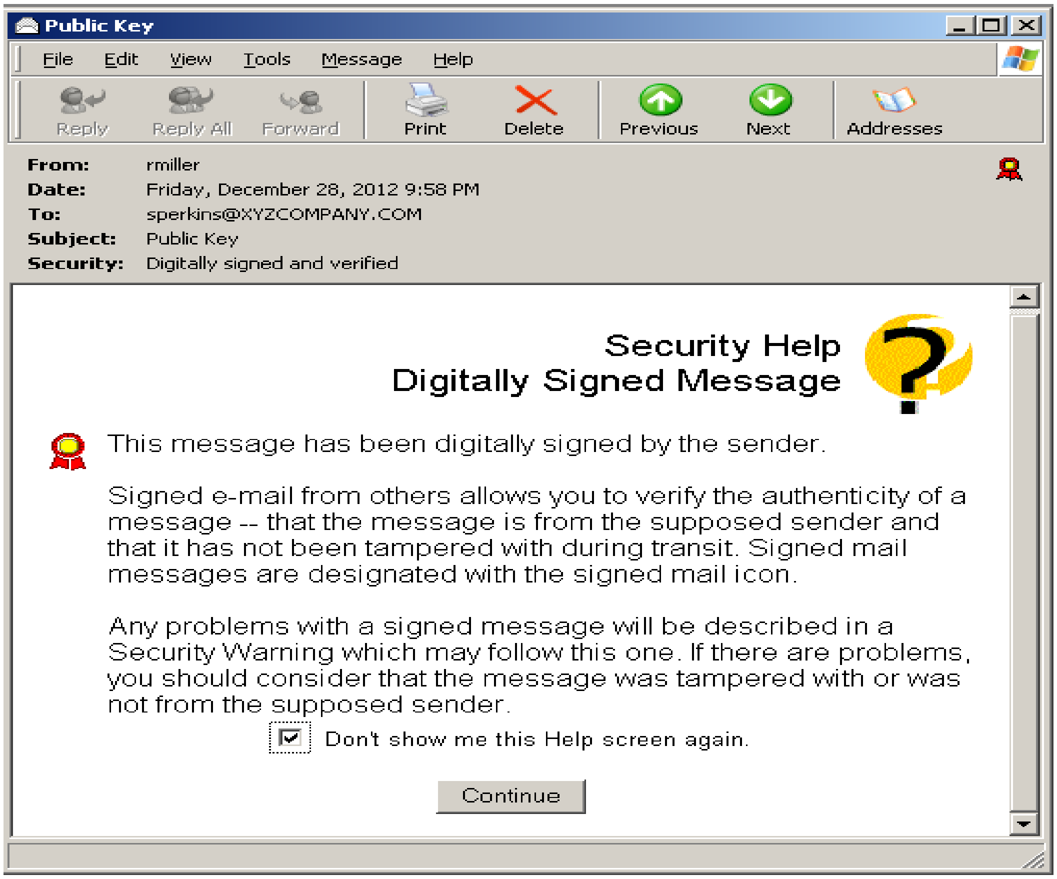


Figure 41: Sending the Email Message

9. The email from rmiller should appear. When you attempt to open the email, you will receive a message about a digital signature. Check the box that says **Don't show me this Help screen** again and click the **Continue** button.



From: rmiller
Date: Friday, December 28, 2012 9:58 PM
To: sperkins@XYZCOMPANY.COM
Subject: Public Key
Security: Digitally signed and verified

Security Help
Digitally Signed Message

This message has been digitally signed by the sender.

Signed e-mail from others allows you to verify the authenticity of a message -- that the message is from the supposed sender and that it has not been tampered with during transit. Signed mail messages are designated with the signed mail icon.

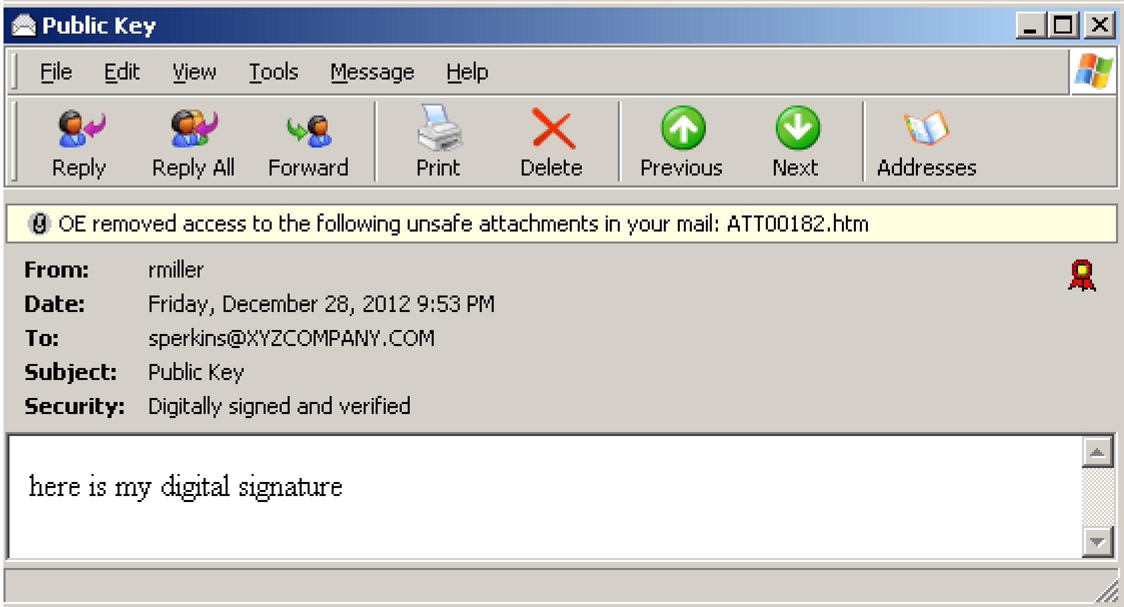
Any problems with a signed message will be described in a Security Warning which may follow this one. If there are problems, you should consider that the message was tampered with or was not from the supposed sender.

☑ Don't show me this Help screen again.

Continue

Figure 42: Message about Digital Signatures

10. Read the email message, which has been digitally signed and verified.



OE removed access to the following unsafe attachments in your mail: ATT00182.htm

From: rmiller
Date: Friday, December 28, 2012 9:53 PM
To: sperkins@XYZCOMPANY.COM
Subject: Public Key
Security: Digitally signed and verified

here is my digital signature

Figure 43: Message from rmiller including Digital Signature

11. In the contacts area in the left corner, right-click on *rmiller* and select **Send Email**

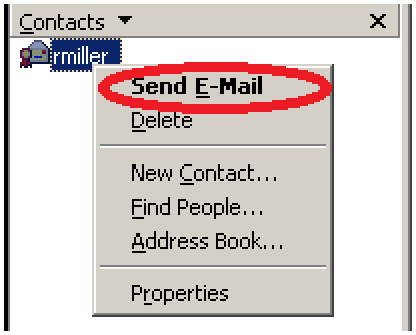


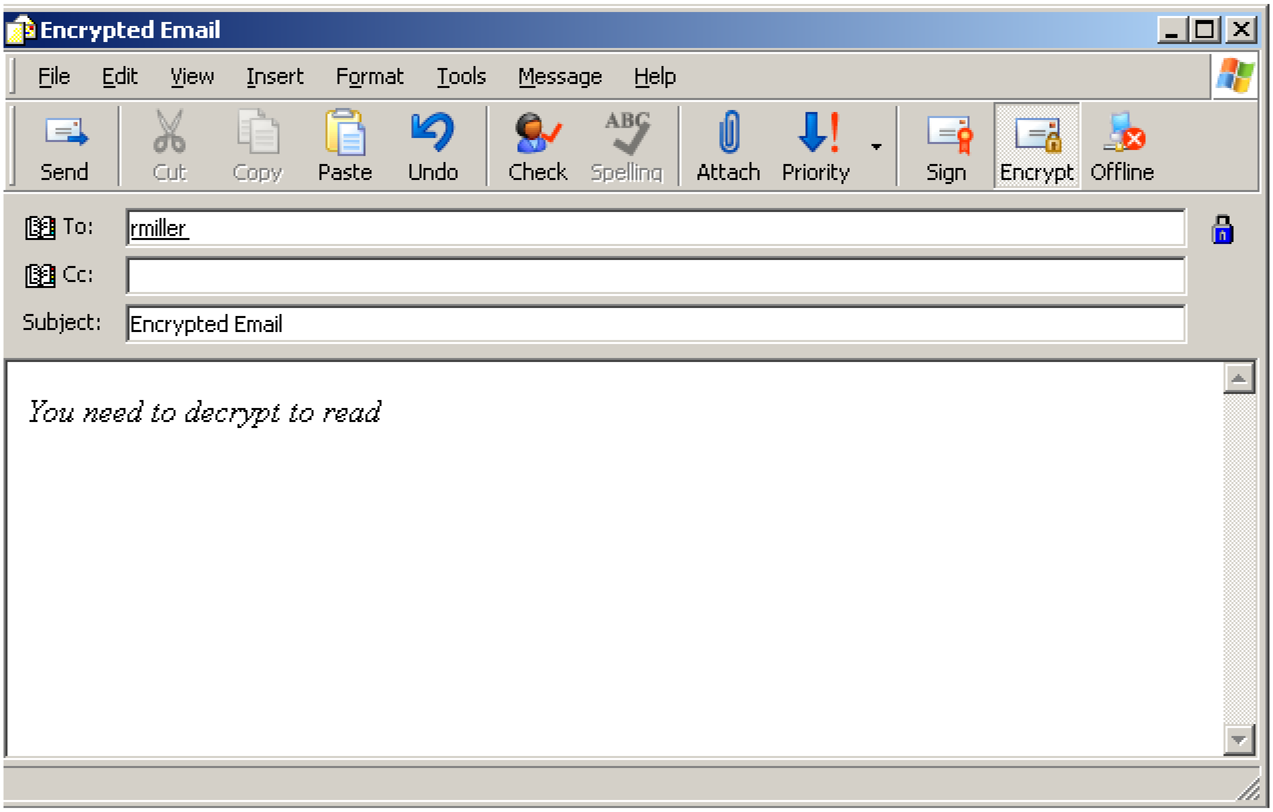
Figure 44: Sending the Reply

12. Follow the steps below to encrypt the email to rmiller.

- In the **Subject** type, **Encrypted Email**
- In the **message** area, type:

  You need to decrypt to read

- From the **Tools** menu, select **Encrypt**.
- You will see a blue lock appear to the right of rmiller’s name.
- Click **Send**.



To: rmiller

Cc:

Subject: Encrypted Email

You need to decrypt to read

Figure 44: Sending the Encrypted Email Message

13. On **Windows 2003 SQL**, click the **Send/Receive** button to send the encrypted email to rmiller.

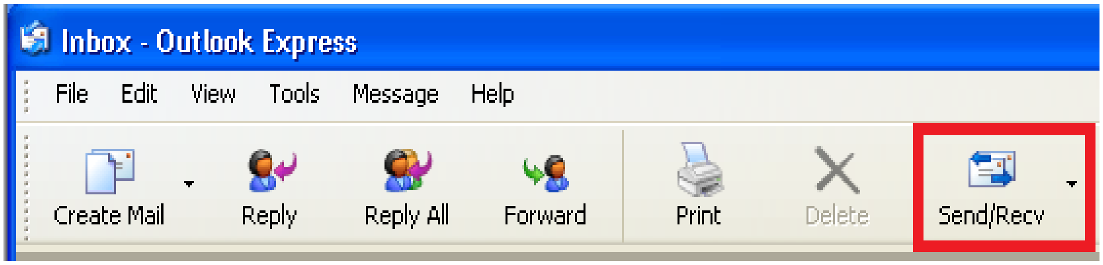
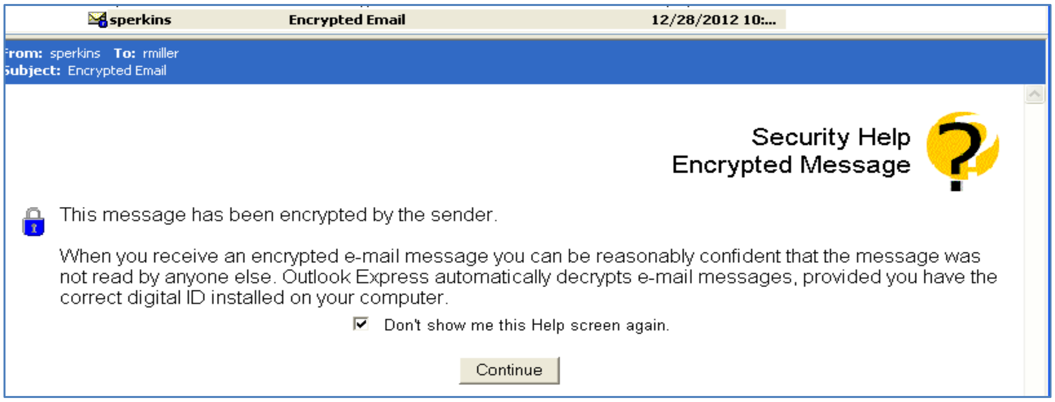


Figure 45: Ensuring the Encrypted Email is Sent

14. On **Windows XP Pro**, Click the **Send/Receive** button to ensure the message is received. Open the email and read the statement that *the message has been encrypted by the sender*. Check the *Don’t show me this help screen again* box and click **Continue**.



sperkins Encrypted Email 12/28/2012 10:...

From: sperkins To: rmiller
Subject: Encrypted Email

Security Help
Encrypted Message

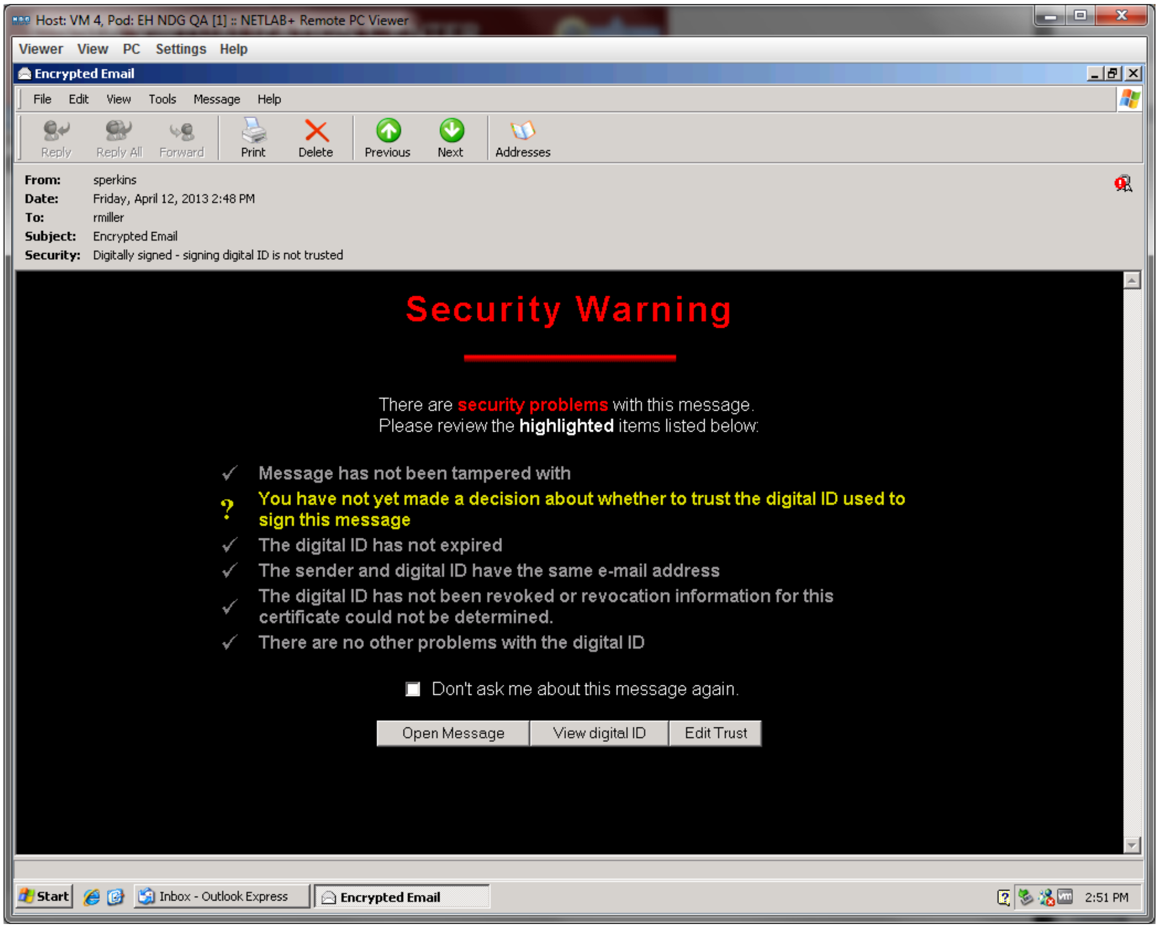
This message has been encrypted by the sender.

When you receive an encrypted e-mail message you can be reasonably confident that the message was not read by anyone else. Outlook Express automatically decrypts e-mail messages, provided you have the correct digital ID installed on your computer.

☑ Don't show me this Help screen again.

Figure 46: A message about the Encrypted Email

If you receive the Security Warning below, click the checkbox next to “Don’t ask me about this message again” and then click **Open Message.**



Host: VM 4, Pod: EH NDG QA [1] :: NETLAB+ Remote PC Viewer
Viewer View PC Settings Help
Encrypted Email
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: sperkins
Date: Friday, April 12, 2013 2:48 PM
To: rmiller
Subject: Encrypted Email
Security: Digitally signed - signing digital ID is not trusted

Security Warning

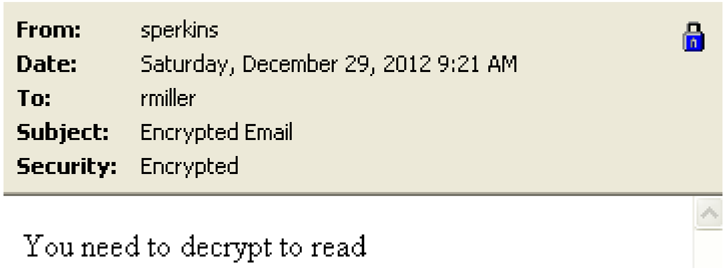
There are security problems with this message.
Please review the highlighted items listed below:

✓ Message has not been tampered with
? You have not yet made a decision about whether to trust the digital ID used to sign this message
✓ The digital ID has not expired
✓ The sender and digital ID have the same e-mail address
✓ The digital ID has not been revoked or revocation information for this certificate could not be determined.
✓ There are no other problems with the digital ID

□ Don't ask me about this message again.

Figure 47: Security Warning

Now, you should be able to read the email in clear text.



From: sperkins
Date: Saturday, December 29, 2012 9:21 AM
To: rmiller
Subject: Encrypted Email
Security: Encrypted

You need to decrypt to read

Figure 48: The decrypted Email message

3.2 Conclusion

Since both SMTP and POP are transmitted in clear test by default, messages that are not encrypted could be read by an attacker with access to the internal network. To prevent this, we included a public key when digitally signing an email, which then allowed us to encrypt future messages sent to that user.

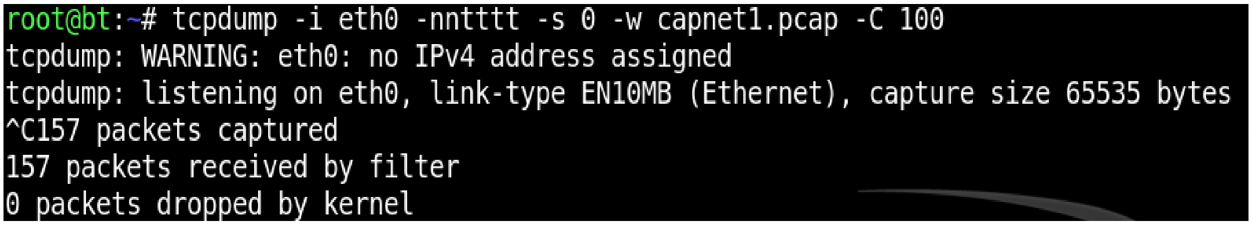
4 Encrypted Text Email Traffic - Wireshark

In this exercise, we will view the cipher text used to encrypt the email message sent from sperkins to rmiller. Sperkins used the rmiller's public key to encrypt the email message.

4.1 Analyzing Encrypted Text Email Traffic Using Wireshark

1. After sending the cipher text emails between rmiller and sperkins, we can stop the capture on the **Linux Sniffer** machine. Press CTRL+C to stop tcpdump from running and capturing network traffic. You should receive a message about the number of packets that were captured by tcpdump.

The number of packets captured can vary.



```
root@bt:~# tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
^C157 packets captured
157 packets received by filter
0 packets dropped by kernel
```

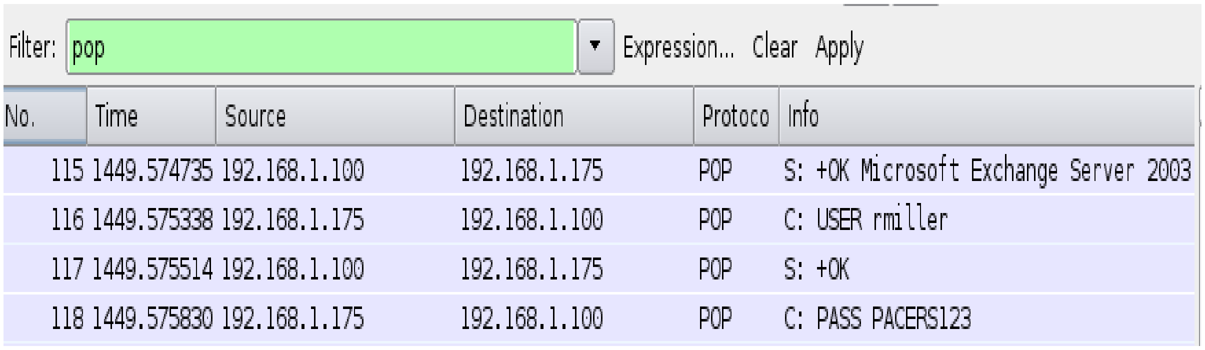
Figure 49: Stopping the tcpdump capture

2. To view the capture file, type the following command at the BackTrack terminal: root@bt:~# **wireshark capnet2.pcap**

```
root@bt:~# wireshark capnet2.pcap
```

Figure 50: Opening the tcpdump capture with Wireshark

3. Type **pop** in the Wireshark filter pane and click **Apply** to view the traffic.



Filter: pop

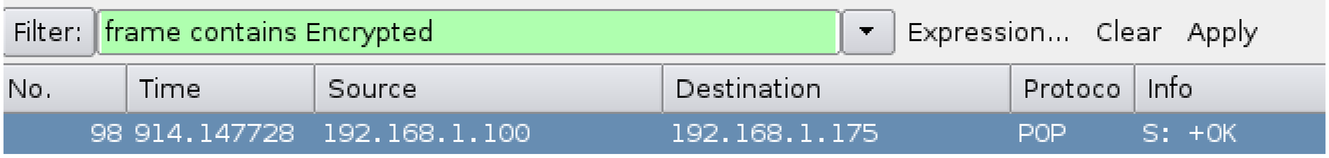
No.	Time	Source	Destination	Protoco	Info
115	1449.574735	192.168.1.100	192.168.1.175	POP	S: +OK Microsoft Exchange Server 2003
116	1449.575338	192.168.1.175	192.168.1.100	POP	C: USER rmiller
117	1449.575514	192.168.1.100	192.168.1.175	POP	S: +OK
118	1449.575830	192.168.1.175	192.168.1.100	POP	C: PASS PACERS123

Figure 51: POP Traffic within Wireshark

Although the email message itself was encrypted, the authentication is still in plain text.

4. Type **frame contains Encrypted** in the Wireshark filter pane and click **Apply**.

The case must match what you used in the subject of the encrypted email.

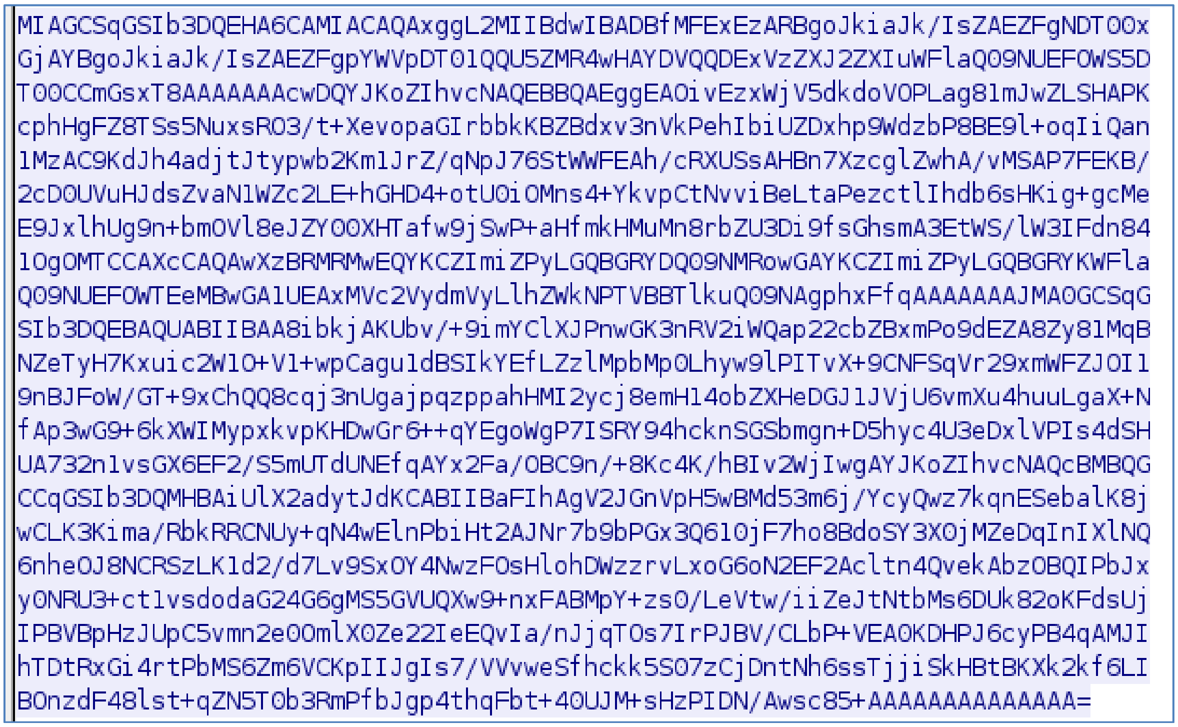


```
No.     Time         Source          Destination     Protoco  Info
     98 914.147728   192.168.1.100   192.168.1.175   POP      S: +OK
```

Figure 52: SMTP Traffic within Wireshark

Even though the email message is encrypted, the subject is not. Keeping the subject in plain text will help email server software determine if an email message is spam.

5. Right-click on the packet and **select Follow TCP stream**. The email is encrypted.



```
MIAGCSqGSIb3DQEHA6CAMIACAQAxggL2MIIBdwIBADBfMFExEzARBgoJkiaJk/IsZAEZFgNDT00x
GjAYBgoJkiaJk/IsZAEZFgpYWVpDT01QQU5ZMR4wHAYDVQQDExVzZXJ2ZXIuWFlaQ09NUEFOWS5D
T00CCmGsxT8AAAAAAAcwDQYJKoZIhvcNAQEBBQAEggEAOivEzxWjV5dkdoVOPLag81mJwZLSHAPK
cphHgFZ8TSs5NuxsRO3/t+XevopaGIrbbkKBZBdxv3nVkPehIbiUZDxhp9WdzbP8BE9l+oqIiQan
1MzAC9KdJh4adjtJtypwb2Km1JrZ/qNpJ76StWWFEAh/cRXUSsAHBn7XzcglZwhA/vMSAP7FEKB/
2cD0UVuHJdsZvaN1WZc2LE+hGHD4+otU0iOMns4+YkvpCtNvviBeLtaPezctlIhdb6sHKig+gcMe
E9JxlhUg9n+bmOVl8eJZY0OXHTafw9jSwP+aHfmkHMuMn8rbZU3Di9fsGhsmA3EtWS/lW3IFdn84
1OgOMTCCAXcCAQAwXzBRMRMwEQYKCZImiZPyLGQBGRYDQ09NMRowGAYKCZImiZPyLGQBGRYKWFla
Q09NUEFOWTEeMBwGA1UEAxMVc2VydmVyLlhZWkNPTVBBTlkuQ09NAgphxFfqAAAAAAJMA0GCSqG
SIb3DQEBAQUABIIBAA8ibkjAKUbv/+9imYClXJPnwGK3nRV2iWQap22cbZBxmPo9dEZA8Zy81MqB
NZeTyH7Kxuic2W1O+V1+wpCagu1dBSIkYEfLZzlMpbMp0Lhyw9lPITvX+9CNFSqVr29xmWFZJOI1
9nBJFoW/GT+9xChQQ8cqj3nUgajpqzppahHMI2ycj8emH14obZXHeDGJ1JVjU6vmXu4huuLgaX+N
fAp3wG9+6kXWIMypxkvpKHDwGr6++qYEgoWgP7ISRY94hcknSGSbmgn+D5hyc4U3eDxlVPIs4dSH
UA732n1vsGX6EF2/S5mUTdUNEfqAYx2Fa/OBC9n/+8Kc4K/hBIv2WjIwgAYJKoZIhvcNAQcBMBQG
CCqGSIb3DQMHBAiUlX2adytJdKCABIIBaFIhAgV2JGnVpH5wBMd53m6j/YcyQwz7kqnESebalK8j
wCLK3Kima/RbkRRCNUy+qN4wElnPbiHt2AJNr7b9bPGx3Q61OjF7ho8BdoSY3X0jMZeDqInIXlNQ
6nheOJ8NCRSzLK1d2/d7Lv9SxOY4NwzFOsHlohDWzzrvLxoG6oN2EF2Acltn4QvekAbzOBQIPbJx
y0NRU3+ctlvsdodaG24G6gMS5GVUQXw9+nxFABMpY+zs0/LeVtw/iiZeJtNtbMs6DUk82oKFdsUj
IPBVBpHzJUpC5vmn2e0OmlX0Ze22IeEQvIa/nJjqTOs7IrPJBV/CLbP+VEA0KDHPJ6cyPB4qAMJI
hTDtRxGi4rtPbMS6Zm6VCKpIIJgIs7/VVvweSfhckk5S07zCjDntNh6ssTjjiSkHBtBKXk2kf6LI
BOnzdF48lst+qZN5T0b3RmPfbJgp4thqFbt+40UJM+sHzPIDN/Awsc85+AAAAAAAAAAAAA=
```

Figure 53: The Encrypted Email Message

6. Click **Close** when done viewing Follow TCP Stream.

7. Close Wireshark by selecting **File** from the menu bar and selecting **Quit**.

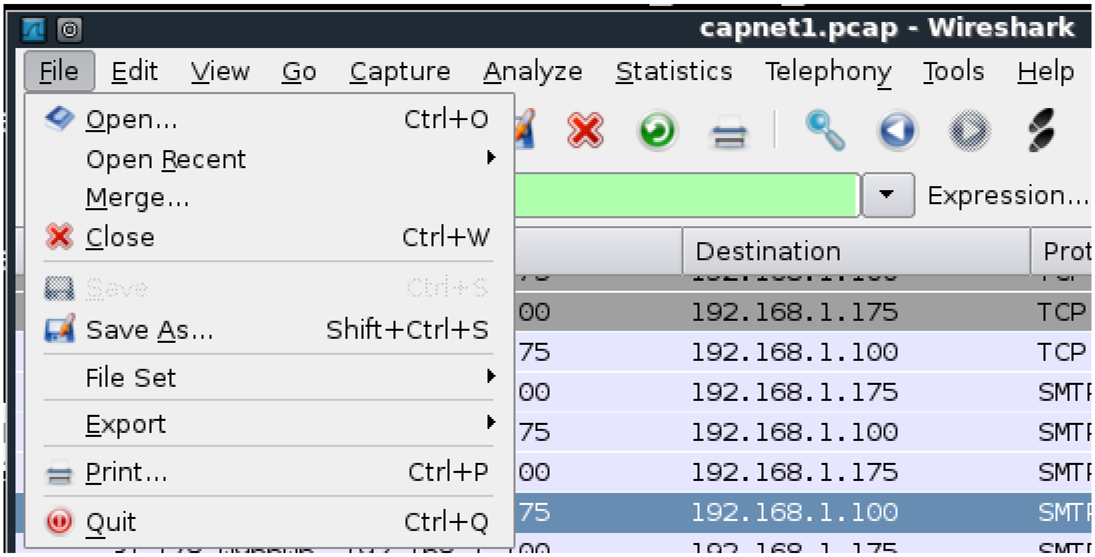


Figure 54: Closing the Wireshark Program

4.2 Conclusion

By default, SMTP and POP traffic are transmitted in clear text. A PKI infrastructure can be used to encrypt email messages so they are not compromised when they are in transit.

References

1. Wireshark:
   http://www.wireshark.org/

2. tcpdump:
   http://www.tcpdump.org/