



Ethical Hacking Lab Series

Lab 19: Using Certificates to Encrypt Email

Certified Ethical Hacking Domain:
Cryptography

Document Version: **2013-07-02 (Beta)**

Organization: Moraine Valley Community College
Author: Jesse Varsalone

Copyright © National Information Security, Geospatial Technologies Consortium (NISGTC)

The development of this document is 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 work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.



The Center for Systems Security and Information Assurance (CSSIA), in partnership with the Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction	3
Domain: Cryptography.....	3
Pod Topology	4
Lab Settings.....	5
1 Plain Text Email Traffic - tcpdump.....	6
1.1 Capturing Plain Text Email Traffic with tcpdump.....	6
1.2 Conclusion	18
1.3 Discussion Questions.....	18
2 Plain Text Email Traffic - Wireshark.....	19
2.1 Analyze Plain Text Email Traffic Using Wireshark	19
2.2 Conclusion	22
2.3 Discussion Questions.....	22
3 Encrypted Email Traffic - tcpdump	23
3.1 Capturing Encrypted Email Traffic with tcpdump	23
3.2 Conclusion	30
3.3 Discussion Questions.....	30
4 Encrypted Text Email Traffic - Wireshark	31
4.1 Analyzing Encrypted Text Email Traffic Using Wireshark	31
4.2 Conclusion	33
4.3 Discussion Questions.....	33
References	34

Introduction

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

By the end of this lab, students will be able to hide digital information as well as reveal hidden data within pictures by using S-Tools . S-Tools is a steganography tool that can be utilized to hide pictures or WAV files. Only users who know the password and encryption algorithm used in order to reveal the hidden picture or the hidden WAV file.

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

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.

Symmetrical 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).

Asymmetrical 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

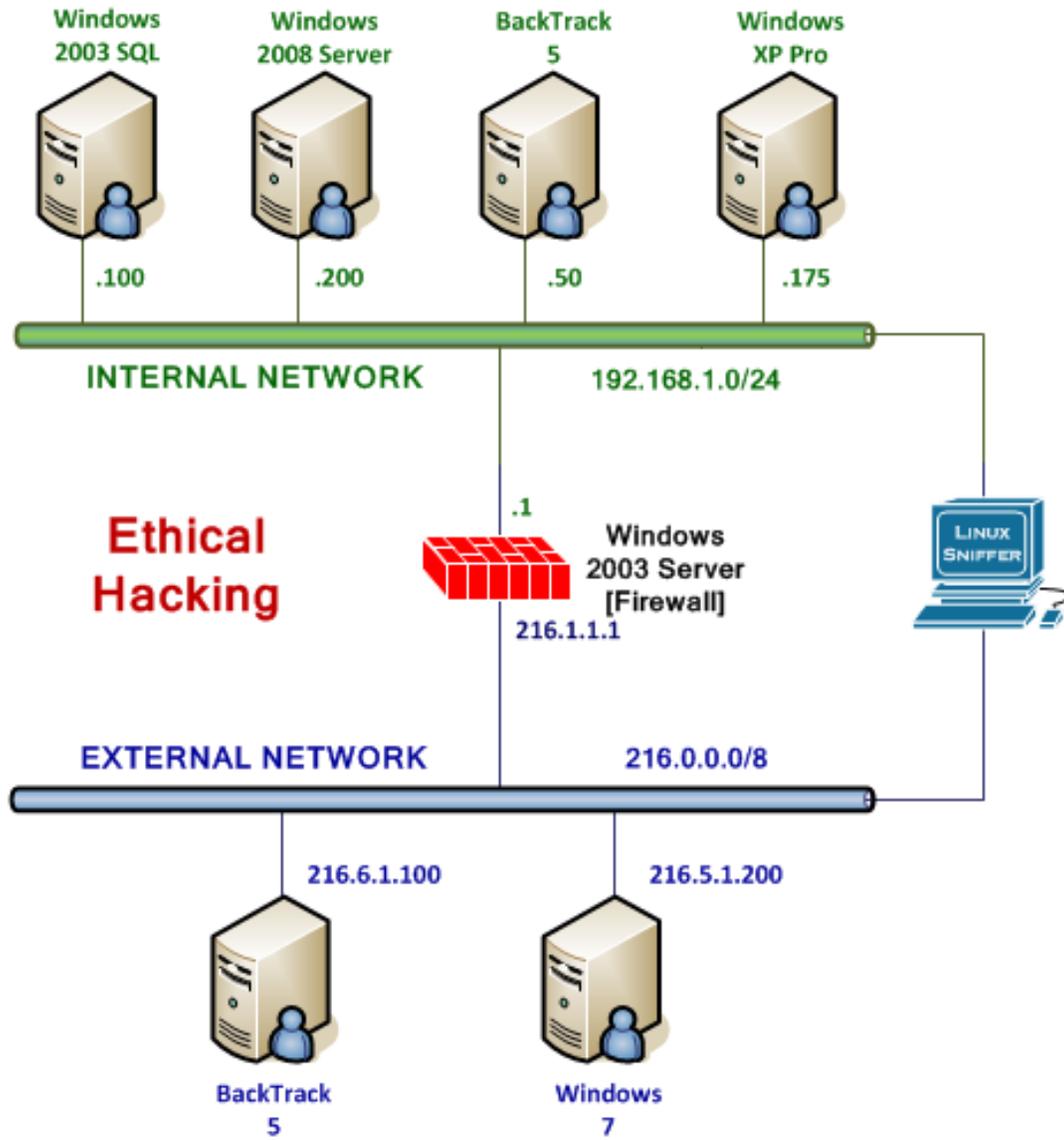


Figure 1: Lab Topology

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 Internal attack machine running Windows 7.

Windows XP Pro	192.168.1.175
Windows XP Pro Administrator password	Ethicalhackin&
Linux Sniffer	No IP Addresses
Linux Sniffer root password	toor
Windows 2003 SQL	192.168.1.100
Windows 2003 SQL Administrator password	P@ssw0rd

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 penetration 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.

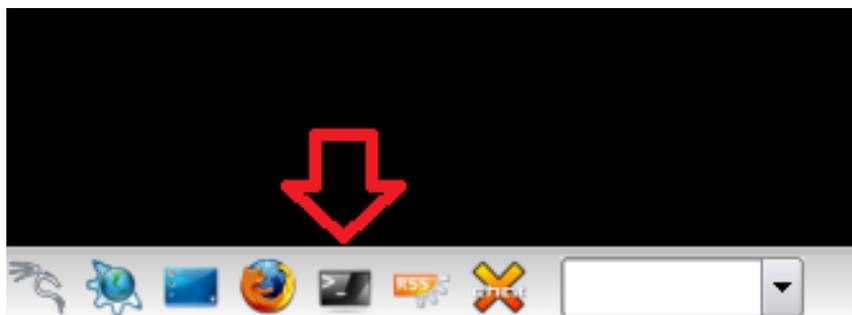


Figure 3: The Terminal Windows within BackTrack

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.

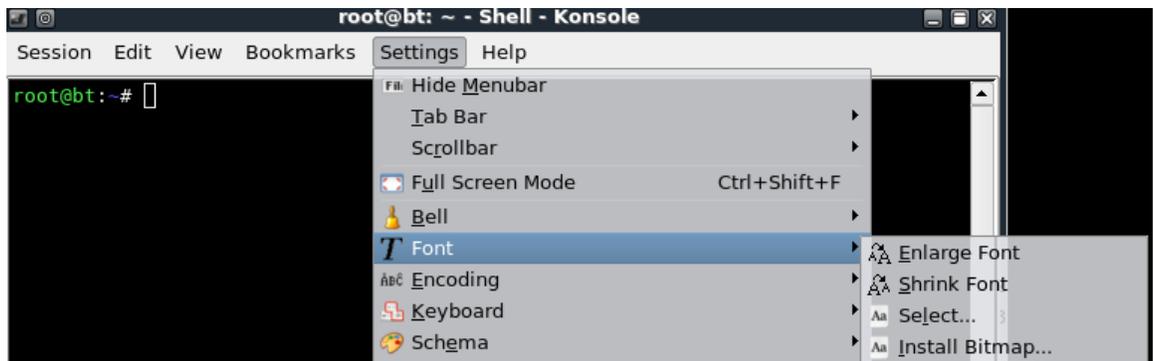


Figure 4: Increase the Font Size of the Terminal Windows

One of the nice features about some versions of BackTrack is they are not automatically assigned IP addresses though 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`

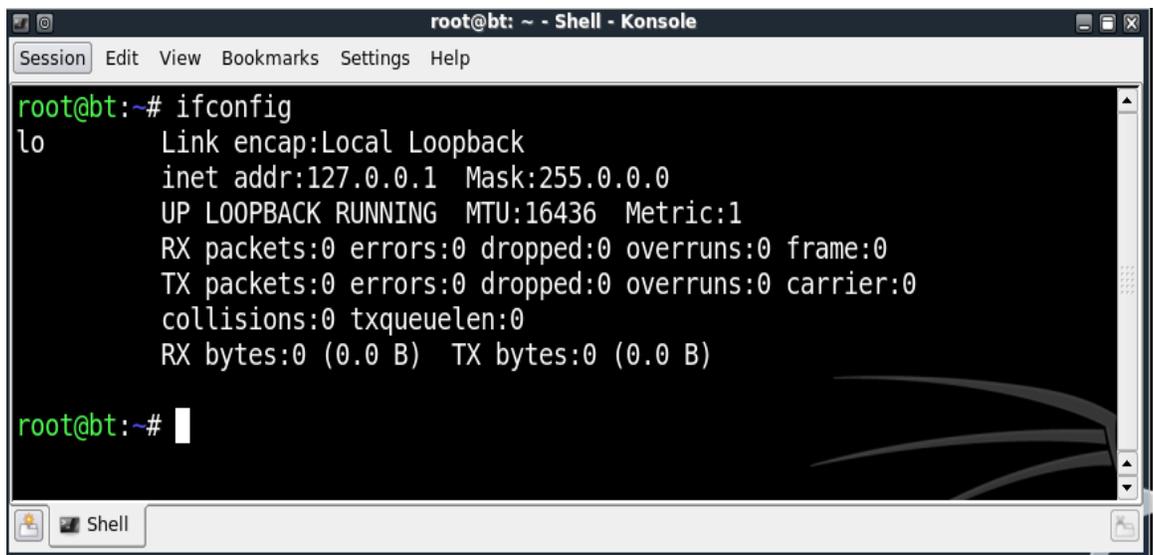


Figure 5: No IP address, other than the Loopback Address of 127.0.0.1, are Displayed

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.

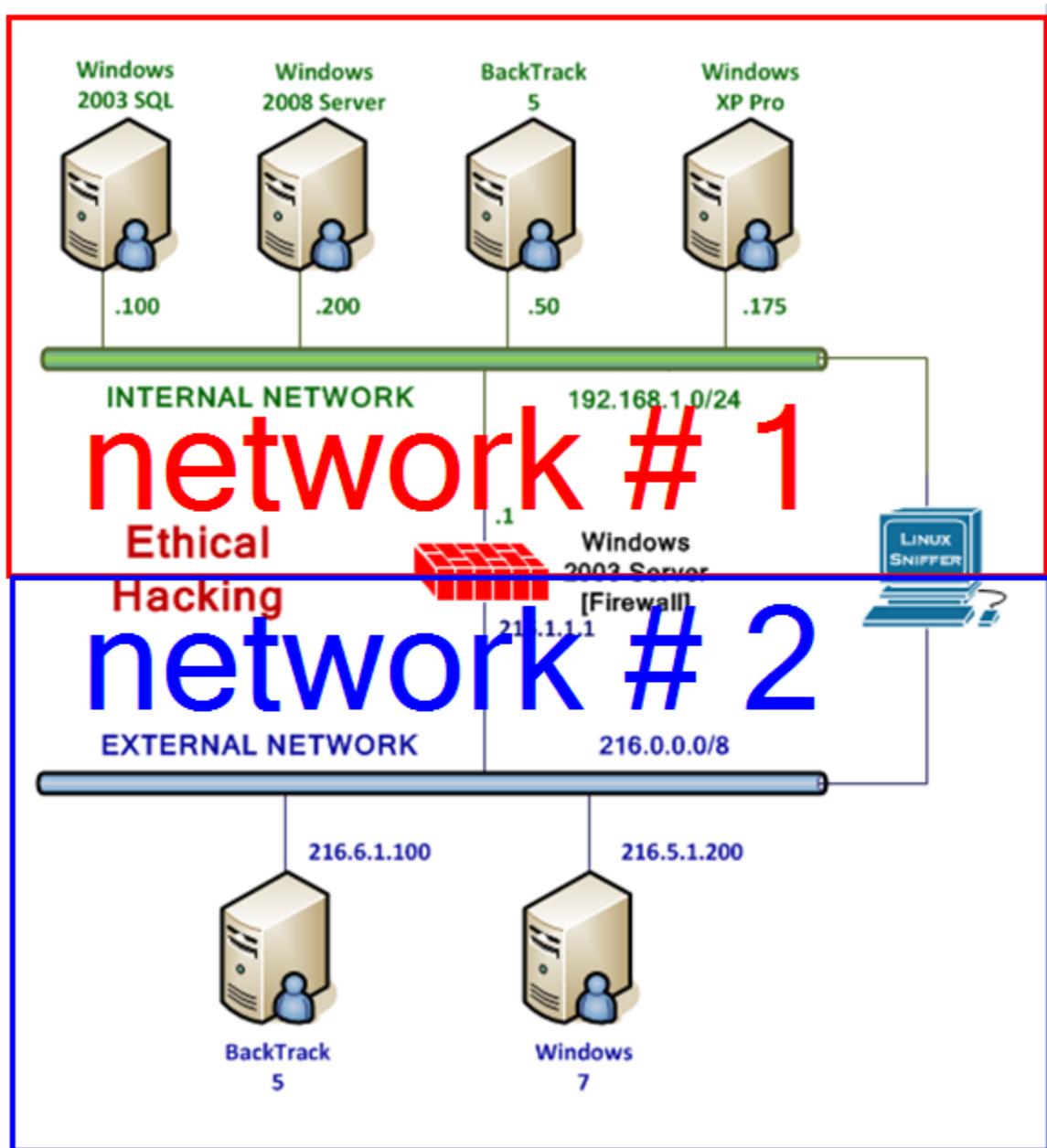


Figure 7: The Sniffer is Connected to Two Networks

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 [-aAdDefllLnNOPqRStuUvxxX] [-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 datainktype ] [ -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

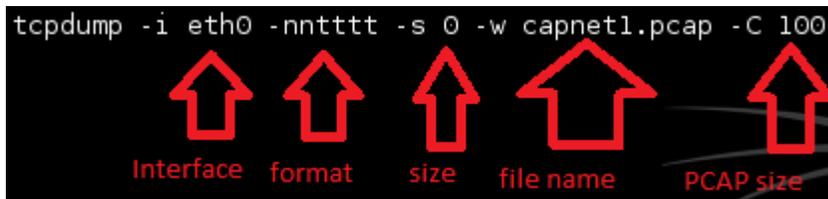


Figure 13: Detailed tcpdump Syntax Explained

12. Log on as **Administrator** to **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.

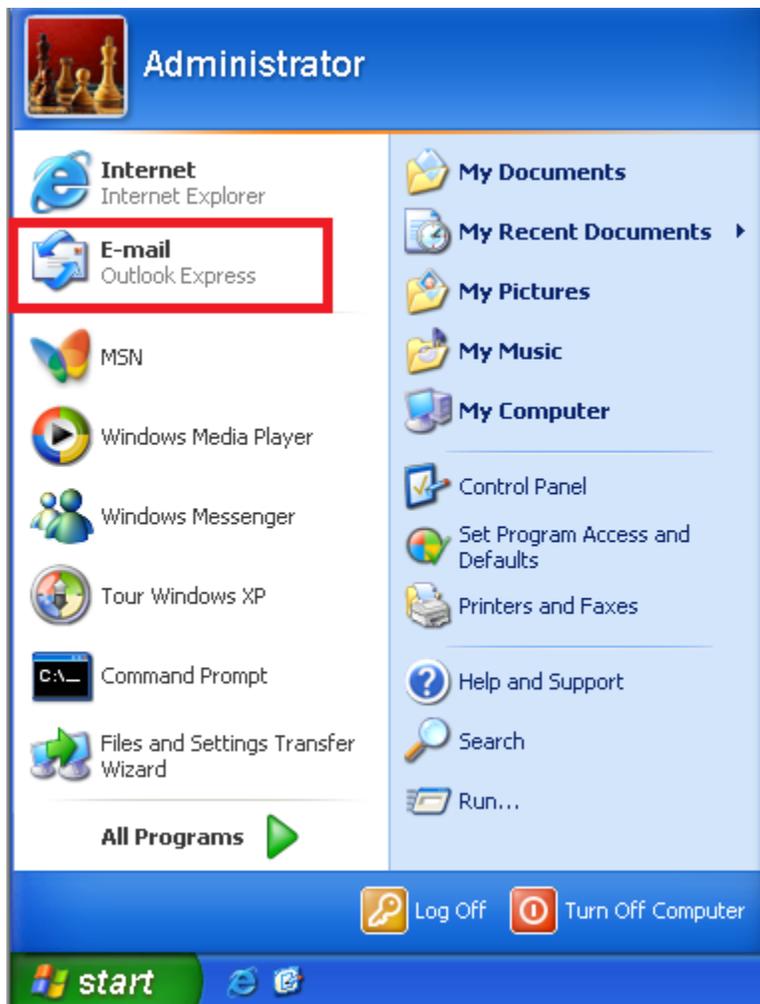


Figure 15: Opening Outlook Express

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

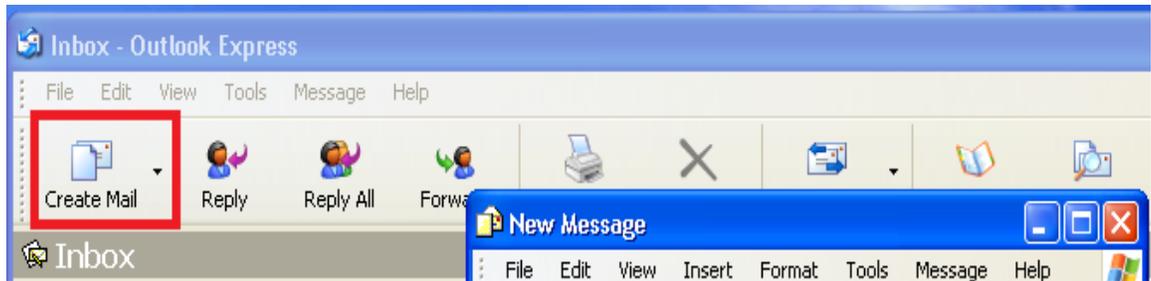


Figure 16: Creating a New Email Message

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.

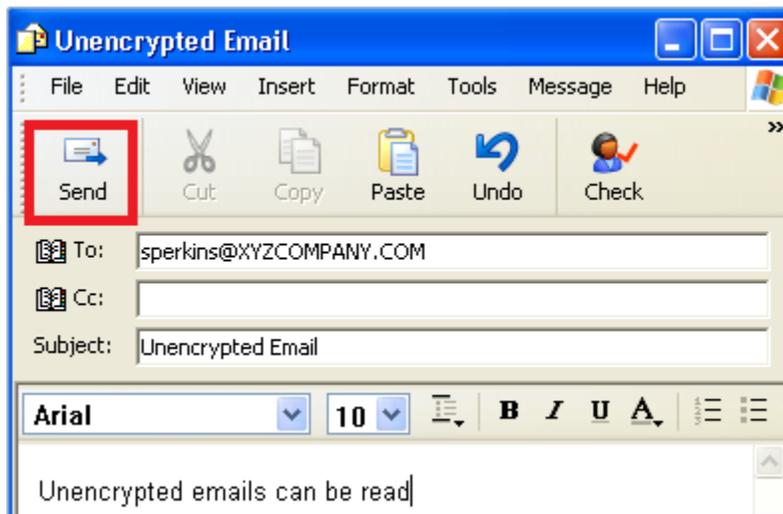


Figure 17: Sending the Email Message

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**.



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.

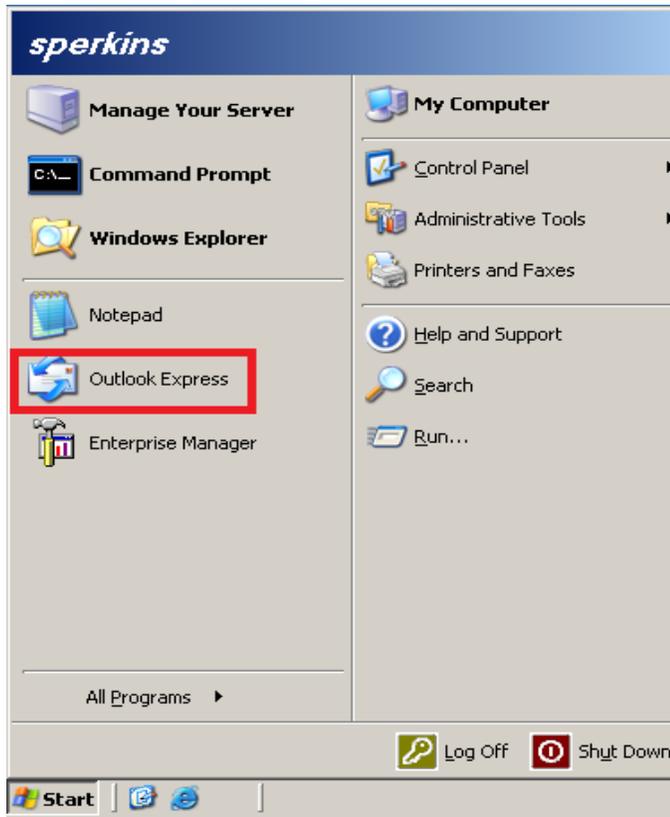


Figure 20: Opening Outlook Express

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

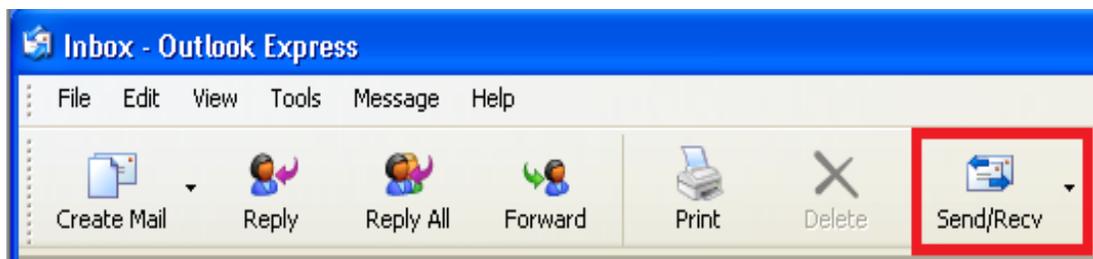


Figure 21: Sending the Email Message

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

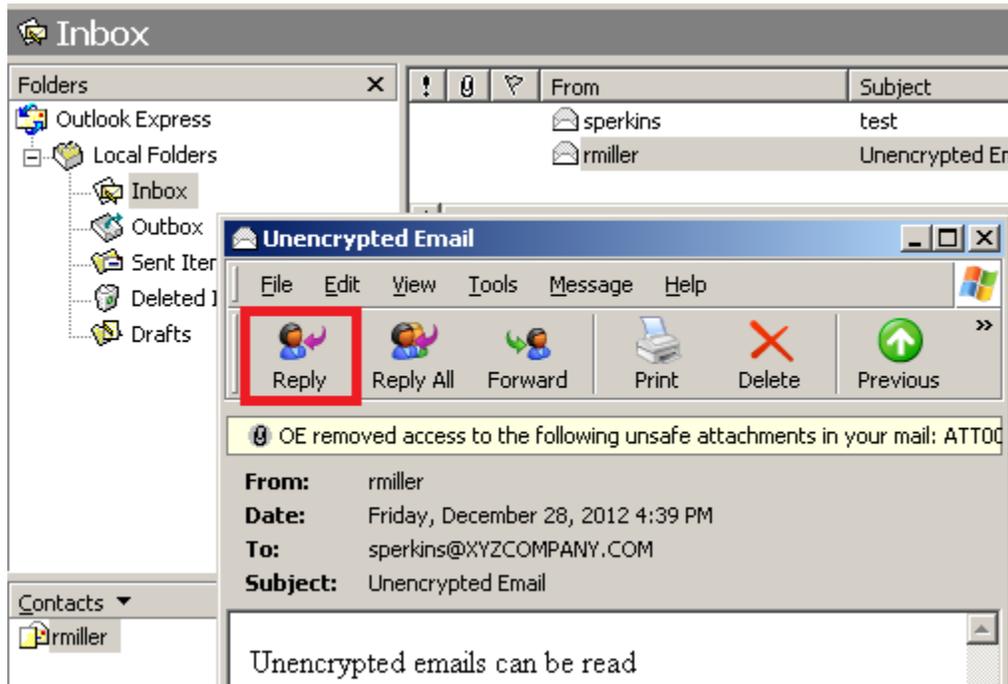


Figure 22: Replying to the Email Message

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

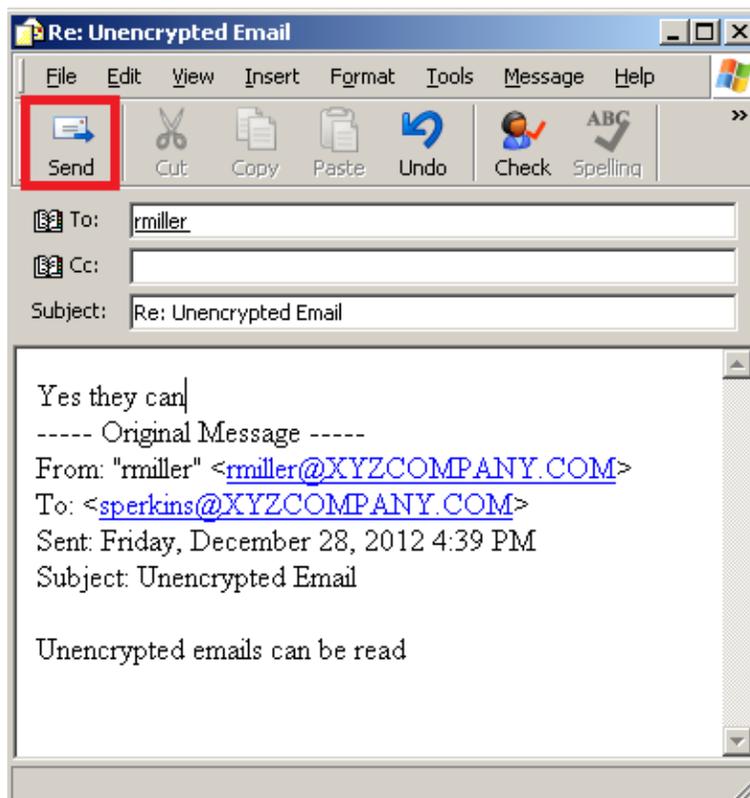


Figure 23: Sending the Reply

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

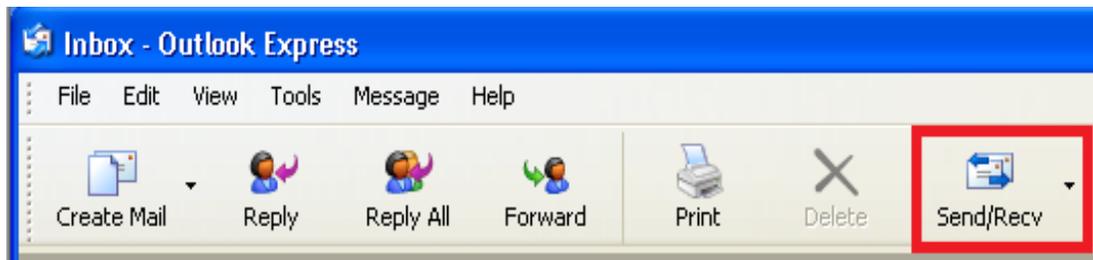


Figure 24: Sending the Email Message

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

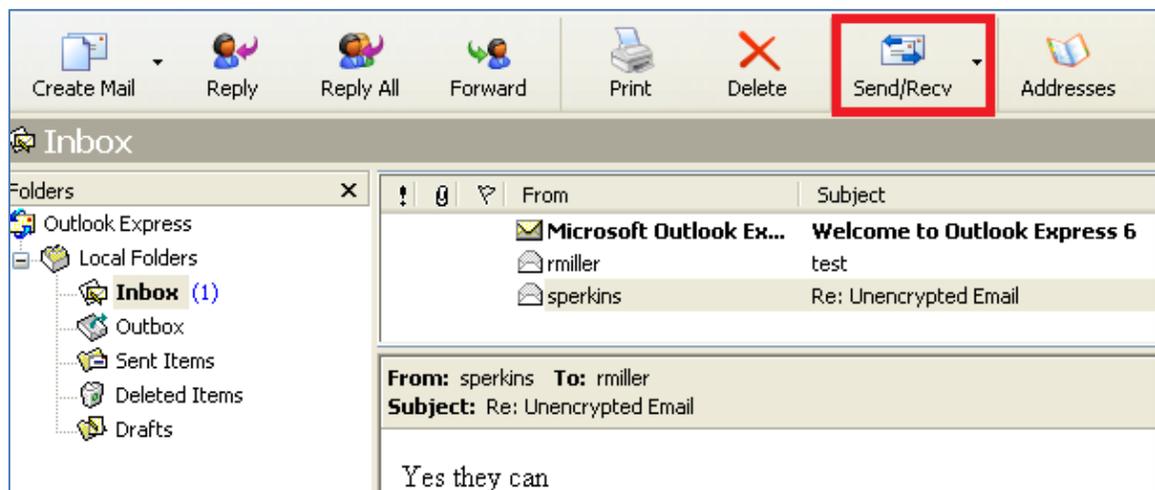


Figure 25: Clicking Send/Receive

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.

1.3 Discussion Questions

1. Does a network interface on a Sniffer machine require an IP address?
2. In what mode does a Sniffer's network interface operate?
3. How do you determine available switches for tcpdump?
4. How can you display all of the network interfaces in Linux?

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 BackTrack 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.



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.

The image shows a Wireshark capture window with the filter 'pop' applied. The packet list pane displays four packets related to POP traffic between 192.168.1.100 and 192.168.1.175.

No.	Time	Source	Destination	Protocol	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.

The image shows a Wireshark capture window with the filter 'smtp' applied. The packet list pane displays ten packets related to SMTP traffic between 192.168.1.100 and 192.168.1.175.

No.	Time	Source	Destination	Protocol	Info
27	178.094541	192.168.1.100	192.168.1.175	SMTP	S: 220 server.XYZCOMPANY.COM Microsoft
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**.

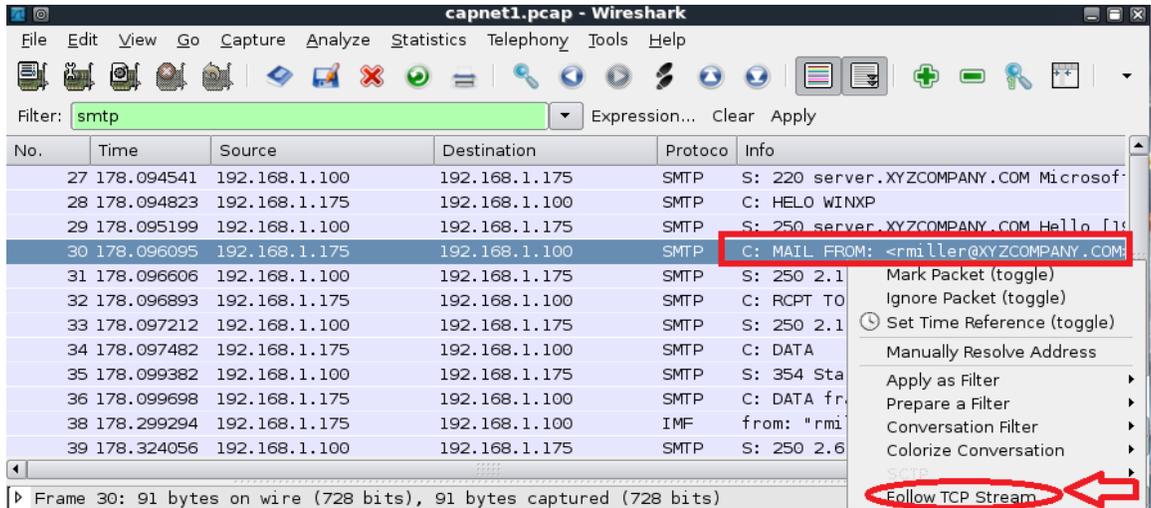


Figure 31: Opening the tcpdump capture with Wireshark

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.

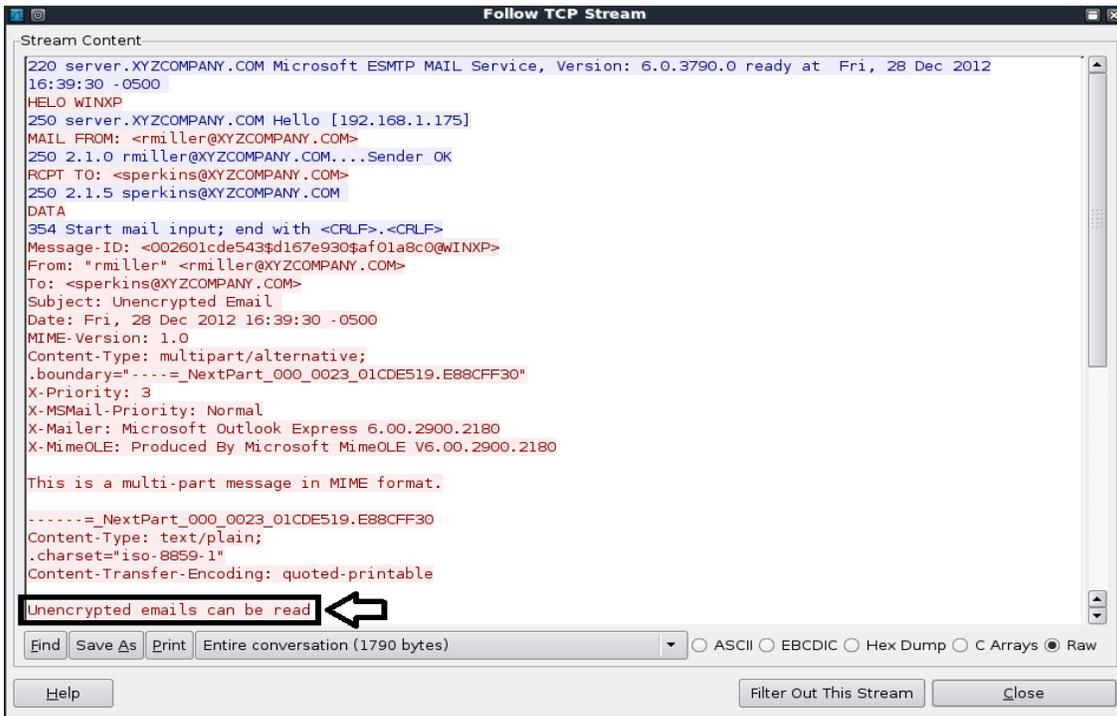


Figure 32: The Plain Text Email Message is displayed within Wireshark

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

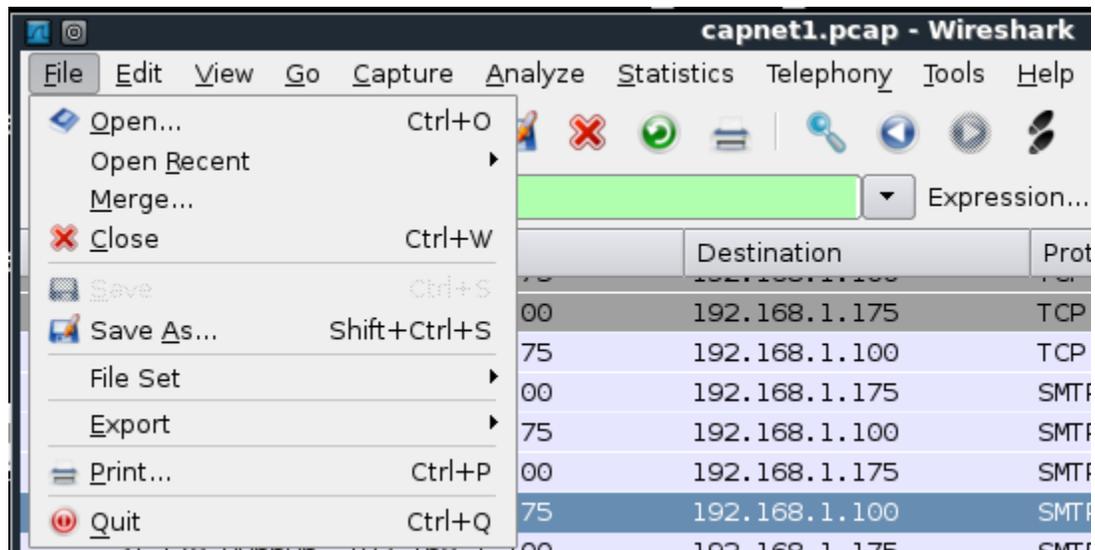


Figure 33: Closing the Wireshark Program

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.

2.3 Discussion Questions

1. How do you filter for Simple Mail Transfer Protocol traffic within Wireshark?
2. How do you filter for Post Office Protocol traffic within Wireshark?
3. Do POP usernames and passwords appear in clear text by default?
4. How do you open the Wireshark program from the terminal in Linux?

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 **WindowsXP Pro** as **Administrator** with the password of **Ethicalhackin&** .

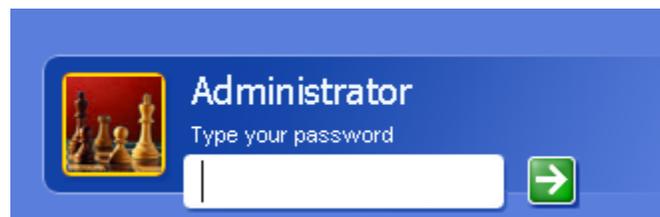


Figure 35: Log back in as Administrator

3. 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 **Subject** type, Public Key
- In the **message** area, type:

Here is my digital signature

- From the Tools menu, select digitally sign.

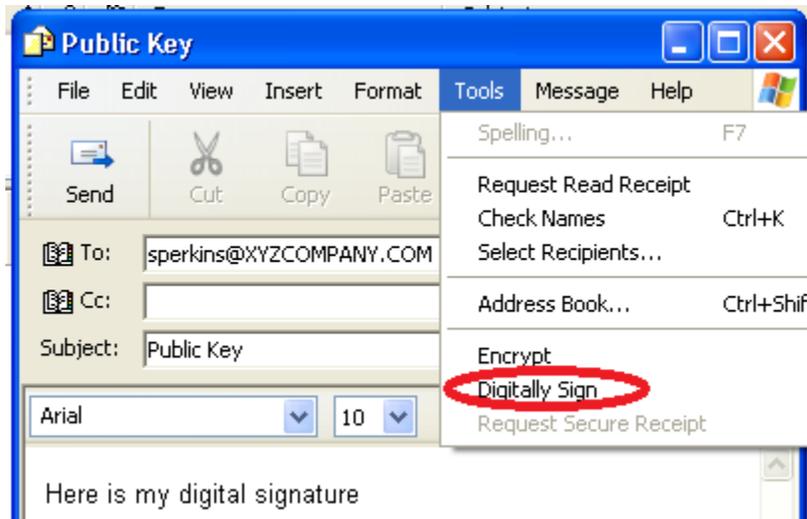


Figure 37: Digitally Signing the Email Message

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.



Figure 38: Sending the Email Message

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

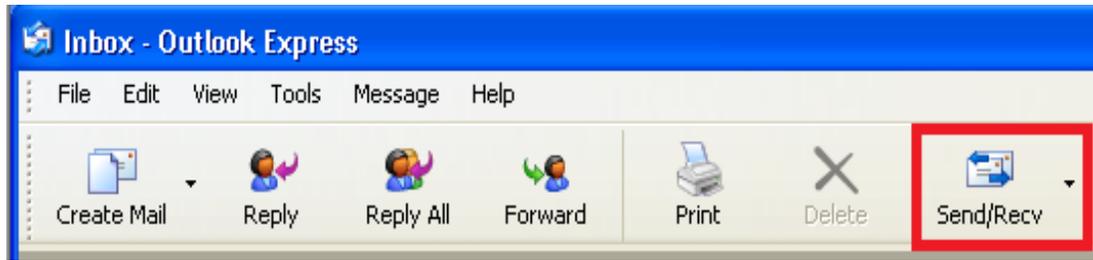


Figure 39: Ensuring that the Email is sent

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**.



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.

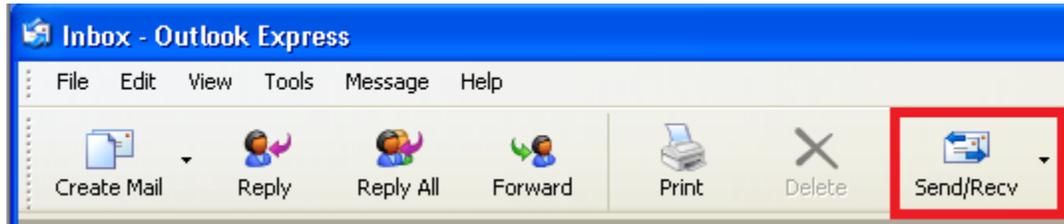


Figure 41: Sending the Email Message

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.

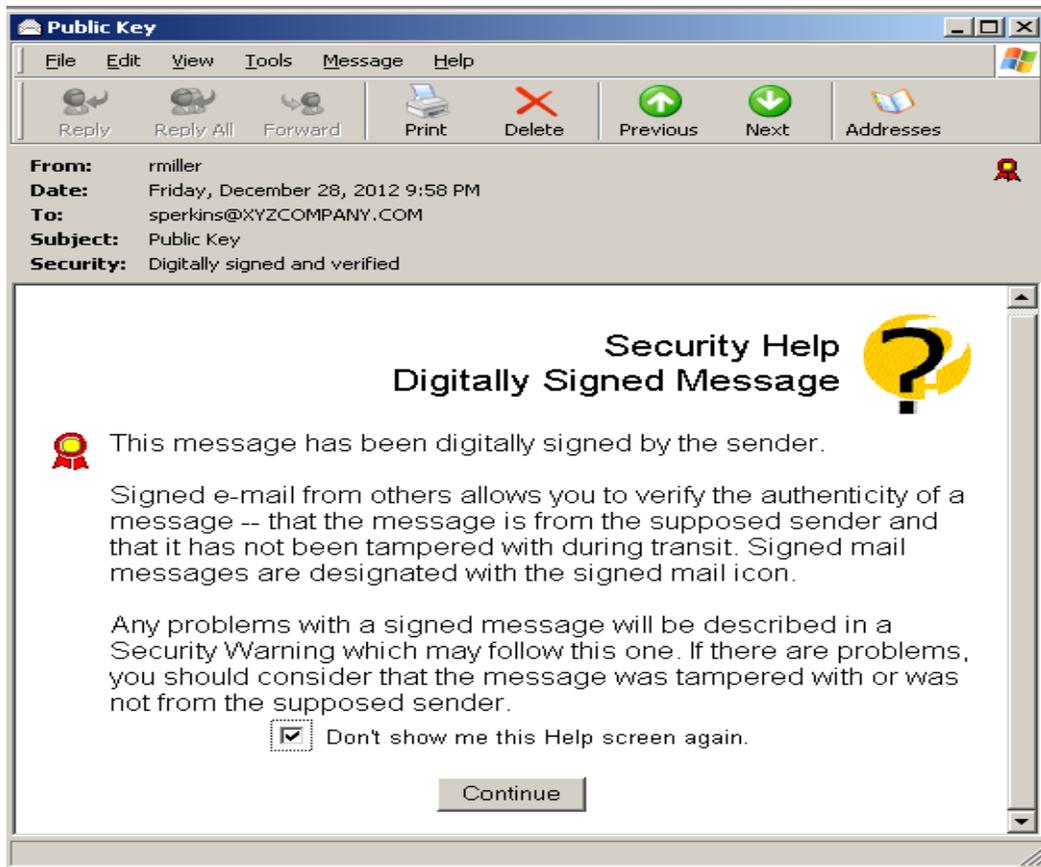


Figure 42: Message about Digital Signatures

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

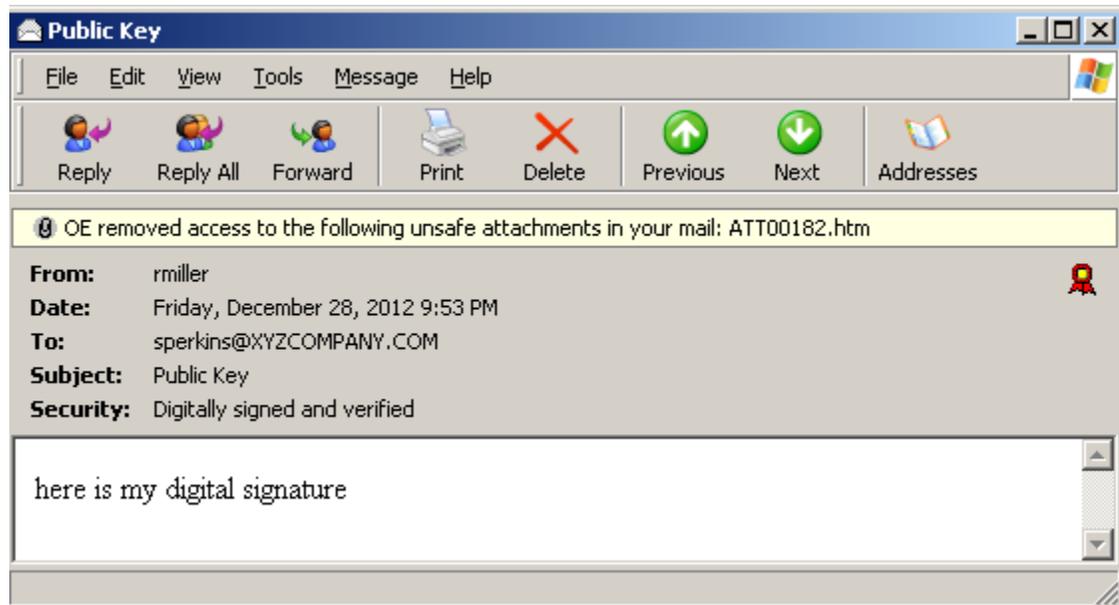


Figure 43: Message from rmiller including Digital Signature

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

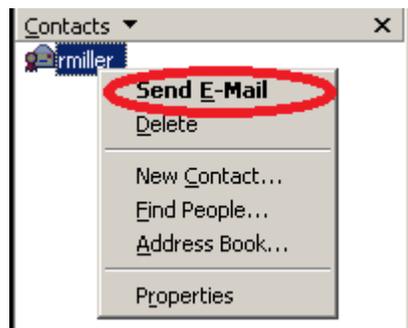


Figure 44: Sending the Reply

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 digitally sign.
- You will see a blue key appear to the right of rmiller's name.

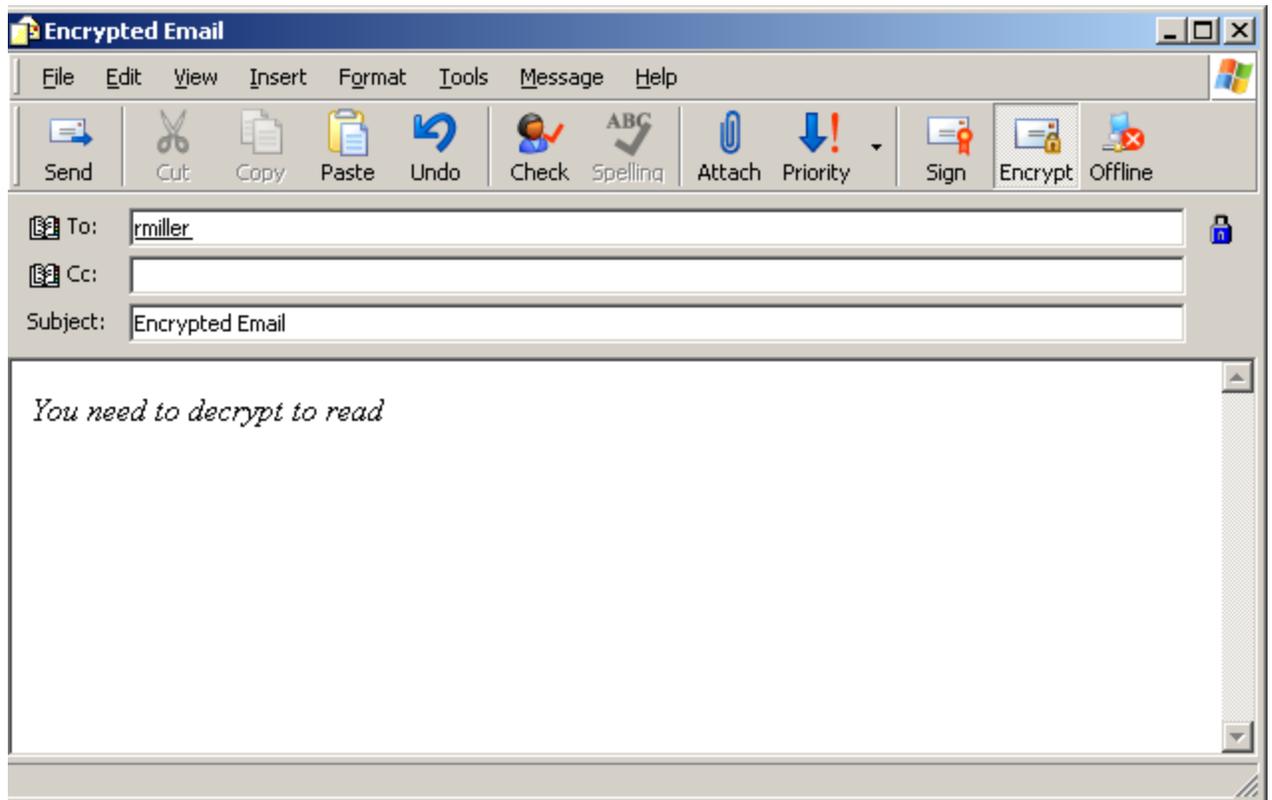


Figure 44: Sending the Encrypted Email Message

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

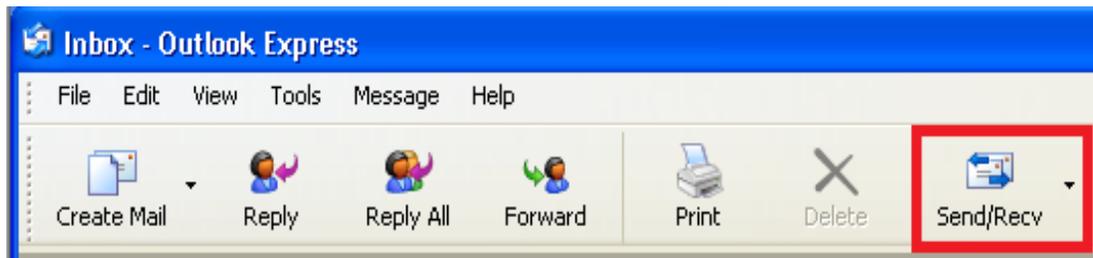


Figure 45: Ensuring the Encrypted Email is Sent

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.

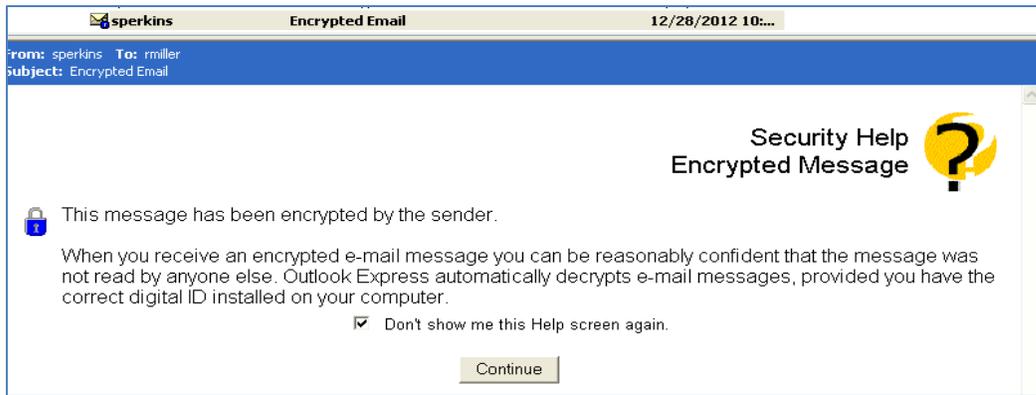


Figure 46: A message about the Encrypted Email

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

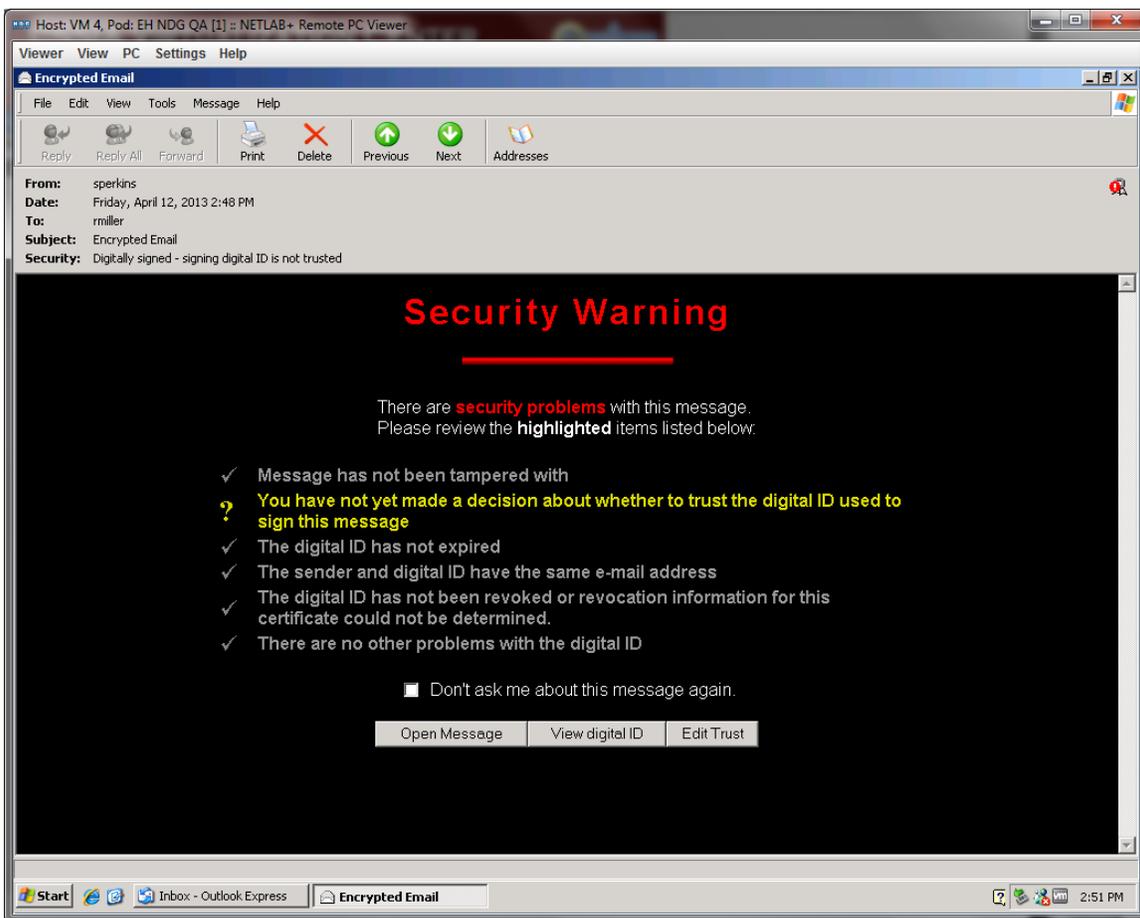


Figure 47: Security Warning

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

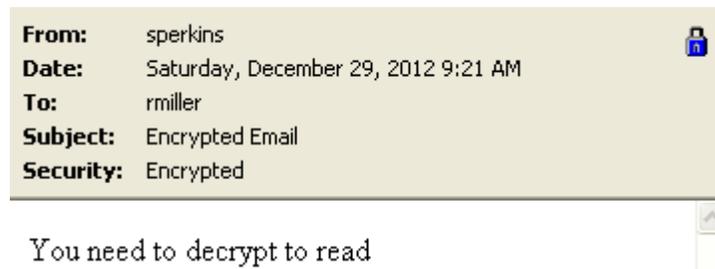


Figure 48: The decrypted Email message

3.2 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 GUIs, 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 view the cipher text used in the emails within the pcap file.

3.3 Discussion Questions

1. How do you send out your digital signature using Outlook Express?
2. How do you encrypt an email using Outlook Express?
3. How is the email message decrypted when PKI is utilized?
4. How is the email message encrypted when PKI is utilized?

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.

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.

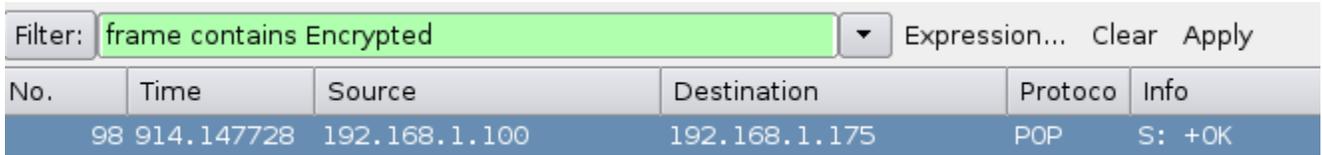


Figure 52: SMTP Traffic within Wireshark

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.



Figure 53: The Encrypted Email Message

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

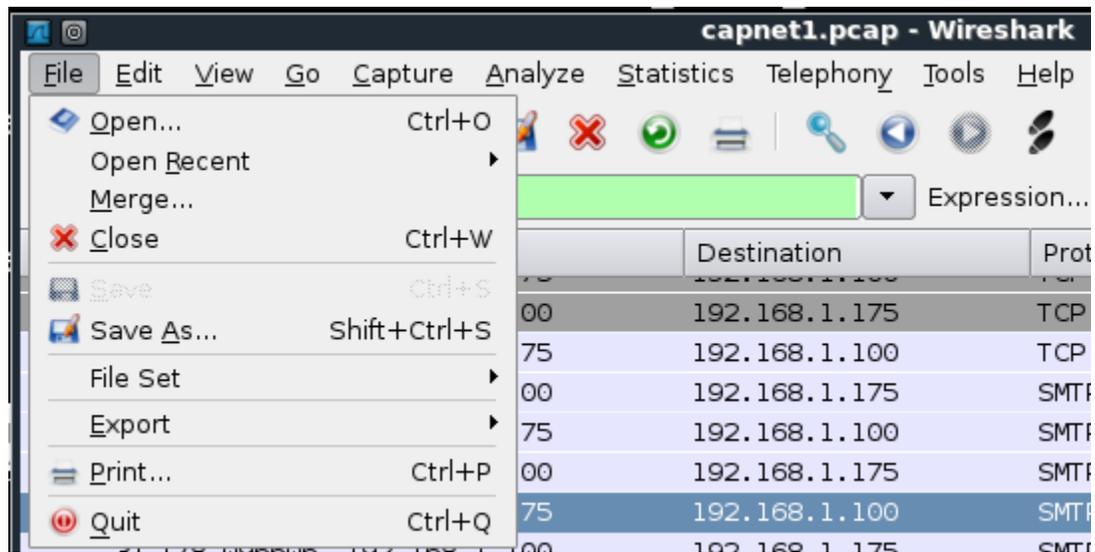


Figure 54: Closing the Wireshark Program

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.

4.3 Discussion Questions

1. What is a possible good reason not to encrypt the subject line of an email?
2. Does the use of a PKI infrastructure guarantee secure authentication?
3. Describe the term cipher text.
4. What does cipher text look like when viewed within Wireshark?

References

1. Wireshark:
<http://www.wireshark.org/>
2. tcpdump:
<http://www.tcpdump.org/>