Lab 5: SMTP, POP-3 and IMAP

Aim:

To provide a foundation in understanding of email with a focus on SMTP, POP-3 and IMAP.

Time to complete: Up to 45 minutes.

Activities:

- **Complete Lab 5**: SMTP, POP-3 and IMAP.
- **Complete Test 5**.

Leaning Activities:

At the end of these activities, you should understand:

- How to determine key details related to SMTP, POP-3 and IMAP.
- Understand email is sent and read.
- Capture traffic for traces.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- Which is the main core weaknesses of the SMTP, POP-3 and IMAP protocols?

- Which ports are likely to be open on the firewall for SMTP, POP-3 and IMAP?

Lab 5: SMTP, POP-3 and IMAP

1 Details

Aim: To provide a foundation in understanding SNMP, POP-3 and IMAP.

The demo of this lab is at: http://youtu.be/3RHrq3EehsE

2 Activities

L1.1 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/smtp.zip

Determine the following:

The IP address and TCP port used by the host which is sending the email:

The IP address and the TCP port used by the SMTP server:

Who is sending the email:

Who is receiving the email:

When was the email sent:

When was the email client used to send the email:

What was the message, and what was the subject of the email:

With SMTP, which character sequence is used to end the message:

L1.2 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/pop3.zip

Determine the following:

The IP address and TCP port used by the host which is sending the email:

The IP address and the TCP port used by the POP-3 server:

Whose mail box is being accessed:

How many email messages are in the Inbox:

The messages are listed as:

1 5565
2 8412
3 xxxx

Which is the ID for message 3:

For Message 1, who sent the message and what is the subject and outline the content of the message:

For Message 2, who sent the message and what is the subject and outline the content of the message:

For Message 3, who sent the message and what is the subject and outline the content of the message:

Which command does POP-3 use to get a specific message:

L1.3 Download the following file, and open it up in Wireshark:

http://asecuritysite.com/log/imap.zip

Determine the following:

The IP address and TCP port used by the host which is sending the email:

The IP address(es) and the TCP ports used by the SMTP and the IMAP server:

Whose mail box is being accessed:

How many email messages are in the Inbox:

Trace the email message that has been sent for its basic details:

Outline the details of email which are in the Inbox:

L1.4 Start the Windows 2003 virtual machine. From the console on your host enter the command:

```
telnet w.x.y.z 25
```

Next enter the commands in bold:

```
220 napier Microsoft ESMTP MAIL Service, Version: 6.0.3790.3959 ready
    at  Sun,
0 Dec 2009 21:56:01 +0000
help
214-This server supports the following commands:
214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN
    BDAT VRFY
helo me
250 napier Hello [192.168.75.1]
mail from: email@domain.com
250 2.1.0 email@domain.com....Sender OK
rcpt to: fred@mydomain.com
250 2.1.5 fred@mydomain.com
Data
354 Start mail input; end with <CRLF>.<CRLF>
From: Bob <bob@test.org>
To: Alice <alice@ test.org >
Date: Sun, 20 Dec 2009
Subject: Test message

Hello Alice.
This is an email to say hello
.
250  2.6.0  <NAPIERMp7lzvxrMVHFb00000001@napier>  Queued  mail  for
    delivery
```

L1.5 On the Windows 2003 virtual machine, go into the `C:\inetpub\mailroot\queue` folder, and view the queued email message.

- ☞ Was the mail successfully queued? If not, which mail folder has the file in?
- ☞ Outline the format of the EML file?