

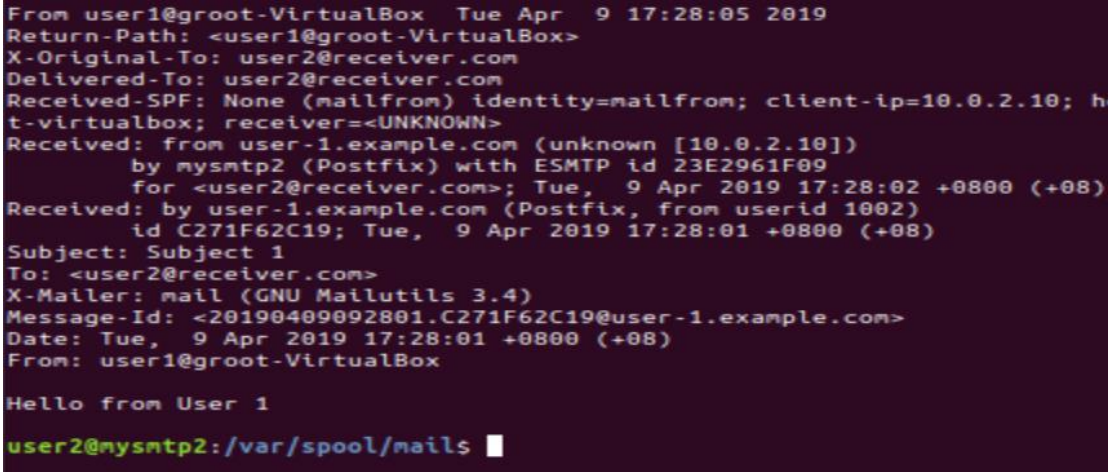
# Assignment 9 - Email Security with SPF, DKIM

## Security Tools Lab 2

Hand out : 9-Apr-2019

Hand in : 17-Apr-2019

1.	<p><b>Objectives</b></p> <p>By the end of this lab, you should be able to:</p> <ul style="list-style-type: none"><li>• Email security implementations to<ul style="list-style-type: none"><li>◦ Verify sender through SPF</li><li>◦ Verify message through DKIM</li></ul></li></ul> <p><b>System</b></p> <ul style="list-style-type: none"><li>• Sender VM (user1 : password1) + Clone (Spoofed Sender)</li><li>• Receiver VM (user2 : password2)</li></ul> <p><b>Notes</b></p> <p>Use NAT Network in VirtualBox</p>
2.	<p>Start both VMs in NAT Network in Virtual Box and login with the respective usernames/passwords. Both users are in sudoers file so you can escalate your privileges to sudo.</p> <p>Find out the IP addresses of the 2 servers. Navigate to /var/cache/bind/ on both machines. These IP addresses must be added to the local DNS entries in their zone files. Configure db.example.com and db.receiver.com on both User1 and User2 machines to reflect the correct IP.</p> <p>After changes you must restart the 'bind' service for changes to take effect</p> <ul style="list-style-type: none"><li>➤ sudo service bind9 restart</li><li>➤ sudo service postfix restart</li></ul> <p>Verify your changes through ping and dig commands</p> <ul style="list-style-type: none"><li>➤ ping example.com</li><li>➤ ping receiver.com</li><li>➤ dig example.com any</li><li>➤ dig receiver.com any</li></ul>
3.	<p>Now that your sender and receiver is properly configured, you can proceed to send emails and verify. On the sender side open a terminal to point to the log files to verify any issue in transmission</p> <ul style="list-style-type: none"><li>➤ cd /var/log</li><li>➤ sudo tail -n50 syslog</li></ul>

	<p>On the receiver side open a terminal to access emails received on 'user2'</p> <ul style="list-style-type: none"> <li>➤ <code>cd /var/spool/mail</code></li> <li>➤ <code>tail -n50 user2</code></li> </ul> <p>On the sender side, send an email (we're using 'postfix') to the receiver.</p> <ul style="list-style-type: none"> <li>➤ <code>echo "Hello from User 1"   mail -s "Subject 1" -a "From:user1@example.com" user2@receiver.com</code></li> </ul> <p>Now check on the receiver side email terminal whether the email has been received</p>  <p>Back up the email by copying it and pasting in an email file (eg ~/Plain.eml)</p>
4.	<p>Clone you sender's VM (Spoofed sender) and start it in the same NAT network but ensure it has a different IP from the original sender VM.</p> <ul style="list-style-type: none"> <li>➤ <code>echo "Spoofed sender"   mail -s "Spoof" -a "From: user1@example.com" user2@receiver.com</code></li> </ul> <p>Observe the email at the receiver end. Back it up in an email file (eg ~/Spoofed.eml)</p> <p>Now enable SPF in the DNS zone file at the receiver DNS. Edit file /var/cache/bind/db.example.com to include to include an appropriate entry for SPF. You can refer to dig entries of any well-known site, for example 'sutd.edu.sg'. You can also refer to <a href="https://www.linuxbabe.com/mail-server/setting-up-dkim-and-spf">https://www.linuxbabe.com/mail-server/setting-up-dkim-and-spf</a>.</p> <p>Based on DIG TXT for SUTD, how many IP addresses are permitted to send email on behalf of sutd.edu.sg?</p> <p>Make sure you restart 'bind9' &amp; 'postfix'. Verify with DIG TXT command (attach screenshot).</p> <p>What is the new entry you need to add to the zone file?</p> <p>Send an email from original sender VM with 'From' as 'user1@example.com' and notice the difference at the receiver side. SPF test should now pass.</p>

```
From: user1@example.com Tue Apr 12 10:10:10 UTC 2022
Return-Path: <user1@example.com>
X-Original-To: user2@receiver.example.com
Delivered-To: user2@receiver.example.com
Received-SPF: Pass (mailfrom=example.com)
Received: from example.com (192.0.2.1) by receiver.example.com (192.0.2.2)
  id 1234567890; Tue, 12 Apr 2022 10:10:10 UTC
```

Back it up in an email file and attach a screenshot of it in your report.

On the Spoofed Sender VM, repeat the same command at the beginning of this section. Does it pass the test? Back up the email and attach a screenshot in your report.

- At the sender machine, we have already created the signing table (/etc/opendkim/signing.table) and key table (/etc/opendkim/key.table) specifying the name of the key and location of the key used for signing the domain (i.e., /etc/opendkim/keys/example.com/default.private). Observe the files.

At the sender VM, display the generated public key:

```
$ sudo cat /etc/opendkim/keys/example.com/default.txt
```

You'll need to copy and paste it into DNS zone file `/var/cache/bind/db.example.com` of receiver VM in a TXT entry. You can now refer to well-known sites to understand the entry. You can also refer to <https://www.linuxbabe.com/mail-server/setting-up-dkim-and-spf>.

Make sure you restart 'bind9', 'postfix' & 'opendkim'. Verify with DIG TXT command (attach screenshot).

What is the new entry you need to add to the zone file? Can you explain the significance of all the tags in your DKIM entry (v,a,c,d,s,t,bh,h,b)

Send an email now from Original Sender VM. Do you see any difference? If you've configured it properly you should be able to see the DKIM signature.

```
Received: by user-1.example.com (Postfix, from userid 1002)  
id 6376F62C19; Tue, 9 Apr 2019 17:32:09 +0800 (+08)  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.com;  
s=default; t=1554802329;  
bh=ShddNa5Iek34WryBN2twMkLxv7o90PNk4Uuh5YurPE=;  
h=Subject:From:To:Date:From;  
b=mNsRZ00B2uOdb4fM5t+r1E8bID/jk5ssHLu3ZkUSq00+PcwbWaHcUV+n03wDYJjWN  
V5hR2bQLDHheUN3MvktLTfZ4i+z37PnldSCzr30MuQZ7WpmGpt+F0odT61+dNeXpmN  
wINFDQg92/0r2lUCtHjBHBHppBR0PAe+iNmGdvI=
```

Back up the received email (eg ~/dkim\_verified.eml) in an email file and attach a screenshot of it in your report.

To ensure that DKIM queries are sent to receiver's local DNS that contains public key, run the following command using backed up email:

```
$ dkimverify < ~/dkim verified.eml
```

It should say 'signature ok'

signature ok

	Include the screenshot in your report.
6.	<p>Now, modify the public key in the DNS entry (file <code>/var/cache/bind/db.example.com</code>) of receiver's VM by replacing a single letter of it (anywhere in the middle of the key string), and thus in turn making the private key of sender invalid. Restart all services ('bind9', 'postfix', 'opendkim' and try to resent the email from sender again. Save the email into file <code>~/dkim_invalid.eml</code>.</p> <p>Verify whether the signature of exported email file is incorrect by using the <code>dkimverify</code> command.</p>
7.	<p><b>Submission</b></p> <p>Please submit a report of all the steps and screenshots in order to implement and test both SPF and DKIM. Answer all questions posed. Attach all the backed-up email (*.eml) and name them accordingly.</p>