UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

Institute of IT-Security and Security Law

3rd IT Security Summer School Madagascar 2020

Email Security

November 18, 2020
Prof. Dieter Gollmann, Johannes Köstler

Objectives

- Learn how to detect spam and phishing emails.
- Learn about email authentication.
- Set up a mail server that authenticates outgoing email.
- Send signed and enrypted emails.

Report

- Report all actions that you take precise and clear.

Introduction

In some exercises of this lab you are going to setup a secure mail server. Therefore you need to configure your remote server according to the configuration your group received.

```
Group Name: <group>
Domain: <group>.itsec-madagascar.de
Server IP: <ip>
Host Name: hermes
Fully Qualified Host Name: hermes.<group>.itsec-madagascar.de
Password: <password>
```

Listing 1: Group Configuration

1. Login to the remote machine by establishing a SSH session to the remote host with user `root` and the supplied password.

   ```
   ssh root@<ip>
   ```

2. During the first login it is a good idea to update the installed packages via the package manager.

   ```
   apt update && apt upgrade
   ```

3. In the next step you need to change the host and domain name. Add the host name (e.g. `hermes`) and your domain name to the appropriate files.

   ```
   <host>
   ```

   Listing 2: /etc/hostname

   ```
   <host>.<domain>
   ```

   Listing 3: /etc/mailname

   ```
   127.0.0.1       localhost
   ::1             localhost ip6-localhost ip6-loopback
   ff02::1         ip6-allnodes
   ff02::2         ip6-allrouters

   # Auto-generated hostname. Please do not remove this comment.
   <ip> <host>.<domain> <host>
   ```

   Listing 4: /etc/hosts

   ```
   search <domain>
   ```

   Listing 5: /etc/resolvconf/resolv.conf.d/tail

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 62.141.32.5
nameserver 62.141.32.4
nameserver 62.141.32.3
search vs.webtropia.com
search <domain>
```

Listing 6: /etc/resolv.conf

Reboot the host to apply all changes.

```
reboot
```

4. You then need to setup a DNS server. Install the required packages.

```
apt install bind9 bind9utils
```

You can check if the BIND server is running by running the following commands.

```
systemctl enable bind9
systemctl status bind9
named -V
```

Define the privileged nodes in an access control list named `trusted` as well as a list of forwarding servers. Apart from that, add the following configuration directives in the options section of the main configuration file to disable zone transfers and enable recursive queries as well as the query log.

```
acl "trusted" {
  localhost;
  localnets;
};


options {
  directory "/var/cache/bind";

  forwarders {
    8.8.8.8;
    8.8.4.4;
  };


  // enable recursive queries
  recursion yes;

  // enable the query log
  querylog yes;

  // disallow zone transfer
  allow-transfer { none; };

  // allow queries for trusted clients
  allow-query { trusted; };
  allow-recursion { trusted; };
  allow-query-cache { trusted; };
};
```

Listing 7: /etc/bind/named.conf.options

In the next step you need to set up a zone file for your domain. Add the zone entry to your local configuration.

```
zone "<domain>" {
  type master;
  file "/etc/bind/db.<domain>";
  allow-query { any; };
};
```

Listing 8: /etc/bind/named.conf.local

Create a copy of the empty zone template file.

```
cp /etc/bind/db.empty /etc/bind/db.<domain>
```

And edit the file

```
$TTL    60
@       IN      SOA     ns1.<domain>. admin.<domain>. (
              2         ; Serial
              604800    ; Refresh
              86400     ; Retry
              2419200   ; Expire
              86400 )   ; Negative Cache TTL
;
@       IN      NS      ns1.<domain>.

@       IN      A       <ip>
ns1     IN      A       <ip>
hermes  IN      A       <ip>
mail    IN      A       <ip>

<domain>.      IN      MX      10      mail.<domain>.

www     IN      CNAME   hermes.<domain>.
```

Listing 9: /etc/bind/db.⟨domain⟩

You can check your configs for errors with the `named` utilities and restart the `bind9` service if no errors or warnings were shown.

```
named-checkzone <domain> /etc/bind/db.<domain>
named-checkconf
systemctl restart bind9
```

The final step is to configure the host to use the newly set-up DNS server on `localhost`. In our very special setting we cannot add this to the `base` part of the resolver configuration as it would be overwritten after each reboot.

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by
    resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 127.0.0.1
```

Listing 10: /etc/resolvconf/resolv.conf.d/head

5. To check if the DNS entries are working, you can try to reach the web server that is running on your remote host with your local browser.

Exercise 1 Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) allows the exchange of electronic mails.

1. Discuss the main problem with the plain SMTP protocol, which enables a lot of downstream problems like spam and phishing?

2. Explain the differences between the three originator fields in the MIME header.

3. Decide which of the emails shown in the appendix are legitimate and explain which indicators led you to this decision. Can you share examples of unsolicited emails from your account?

4. Explain the main concepts behind SPF, Sender ID, DKIM, and DMARC.

Exercise 2 Mail Server Setup

In this exercise you are going to set up a mail server on your remote host.

1. Install the `postfix` package with the mail configuration type `Internet Site` and your `<domain>` as the system mail name.

2. You can test your SMTP setup with the `mail` utility on your command line to send a test mail to your private email address.

   ```
   echo "This is a test!" | mail -s Test <email>
   ```

   Use your mail server only for testing purposes and do not send unsolicited mail to any recipients!

3. Setup some basic IMAP mailboxes with `dovecot`. Usually the `dovecot` server would be configured with a database, spam filters and signed certificates, but for our experiment a file system based and self signed setup will be sufficient. You

   Install the `dovecot` with IMAP support via the package manager.

   ```
   apt install dovecot-imapd mutt mailutils
   ```

   Enable the plaintext authentication in the authentication configuration file. You should not us plaintext authentication in a production environment as the passwords could be easily sniffed from the network!

   ```
   disable_plaintext_auth = no
   auth_mechanisms = plain login
   ```

   Listing 11: /etc/dovecot/conf.d/10-auth.conf

   The next step is to configure the mailbox directory. Adapt the mailbox configuration file as shown below, so that every local user will have the `Maildir` directory as a mailbox inside its home directory.

```
mail_location = maildir:~/Maildir
```

Listing 12: /etc/dovecot/conf.d/10-mail.conf

After that the internal authentication with `postfix` needs to configured.

```
unix_listener /var/spool/postfix/private/auth {
  mode = 0666
  user = postfix
  group = postfix
}
```

Listing 13: /etc/dovecot/conf.d/10-master.conf

For the configurations to become effective you need to restart the dovecot service.

```
systemctl restart dovecot
systemctl status dovecot
```

You can then add local users with the `useradd` command line tool.

```
useradd -p <password> -s /bin/bash -m <user>
```

And test the mailbox with the `mutt` email client.

```
mutt -f imaps://<user>@localhost
```

4. Optional: Try to use `thunderbird` on your local machine and setup a mail account that uses SMTP and IMAP to connect to your remote server.

Exercise 3 Mail Authenticity

Email authentication can prove that an email really originates from the legitimate sender and prevent the transmission of unsolicited messages.

1. Add a SPF record to your DNS zone file, which authorizes your server to send mails from your domain. Explain how you could include further mail servers with a specific ip or from a certain domain. What actions are taken if the policy applies to a certain sender?

2. Install a DKIM policy for your domain by integrating `opendkim` into your `postfix` server and adding the public key to your DNS zone. Test your configuration by sending an email to check-auth@verifier.port25.com. You should see a `DKIM check: pass` information in your reply.

3. Extract the `DKIM-Signature` from an email sent by your server and explain its tag values. Also sketch the verification procedure performed by the receiving mail server.

4. Add a DMARC policy that rejects emails that do not pass the SPF and DKIM policies from above and notifies the domain owner (`postmaster@<domain>`) about all rejections.

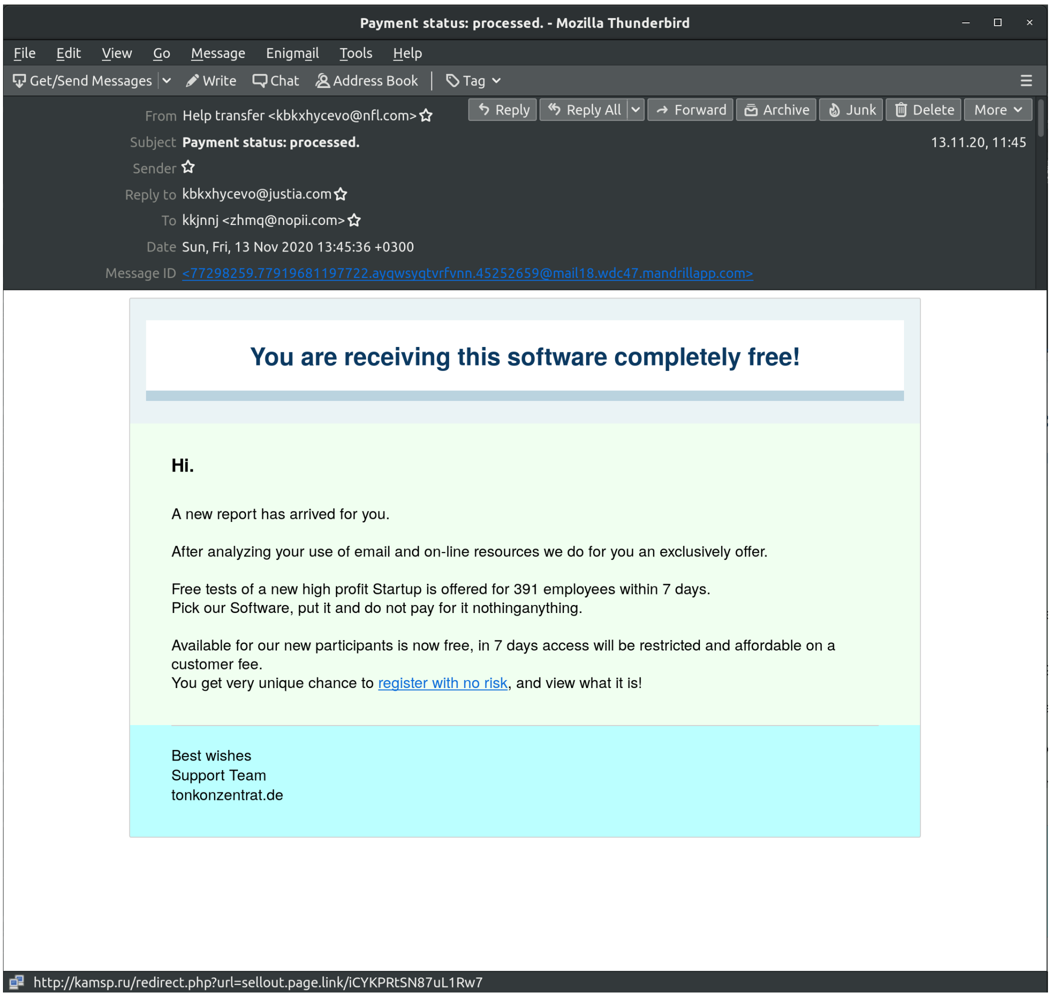
5. Allow a different group to send emails originating from your domain on your behalf.

Exercise 4 Mail Confidentiality

In this exercise you are going to exchange encrypted and signed emails with other groups. If your web server is up and running you can use that email, otherwise you can also use Thunderbird with your private email for this exercise.

1. Install OpenPGP on your local machine and integrate it in Thunderbird. Thunderbird version before 78 need the Enigmail extension. Create an OpenPGP key pair and upload your public key to a key server. Send an encrypted and signed message to other groups. Ensure that you can verify and decrypt messages that you received from other groups.
2. Use OpenSSL to set up your own Certificate Authority. Generate a X.509 certificate derived from a RSA key pair signed by your Certificate Authority and store it in a PKCS12 conform file. Import this certificate into Thunderbird and use it to exchange signed messages with other groups.

Appendix

1. 

From Help transfer <kbkxhycevo@nfl.com>

Subject **Payment status: processed.**

13.11.20, 11:45

Sender

Reply to kbkxhycevo@justia.com

To kkjnnj <zhmq@nopii.com>

Date Sun, Fri, 13 Nov 2020 13:45:36 +0300

Message ID <77298259.77919681197722.ayqwsyqtvrfvnn.45252659@mail18.wdc47.mandrillapp.com>

You are receiving this software completely free!

Hi.

A new report has arrived for you.

After analyzing your use of email and on-line resources we do for you an exclusively offer.

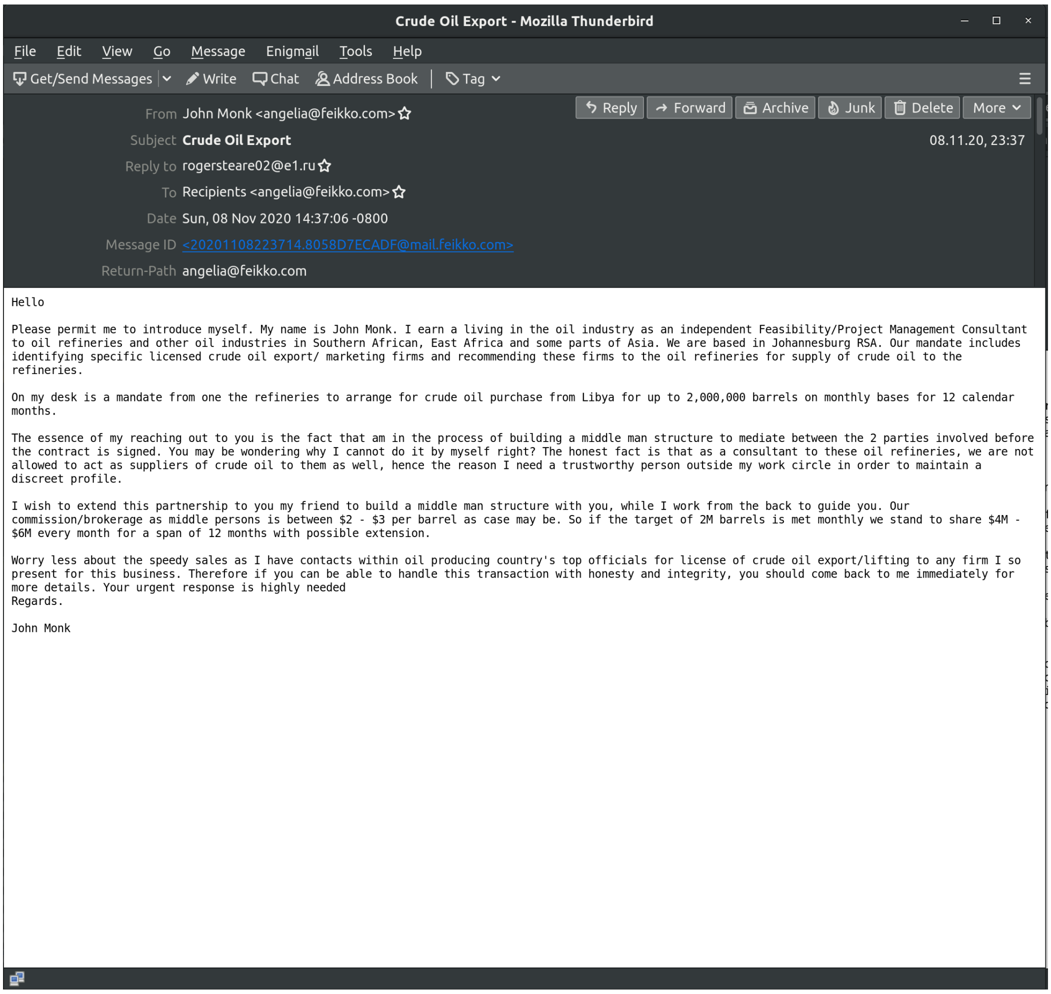
Free tests of a new high profit Startup is offered for 391 employees within 7 days.
Pick our Software, put it and do not pay for it nothinganything.

Available for our new participants is now free, in 7 days access will be restricted and affordable on a customer fee.
You get very unique chance to register with no risk, and view what it is!

Best wishes
Support Team
tonkonzentrat.de

http://kamsp.ru/redirect.php?url=sellout.page.link/iCYKPRtSN87uL1Rw7

2.


Crude Oil Export - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get/Send Messages
Write
Chat
Address Book
Tag
Reply
Forward
Archive
Junk
Delete
More

From John Monk <angelia@feikko.com>

Subject **Crude Oil Export**

08.11.20, 23:37

Reply to rogersteare02@e1.ru

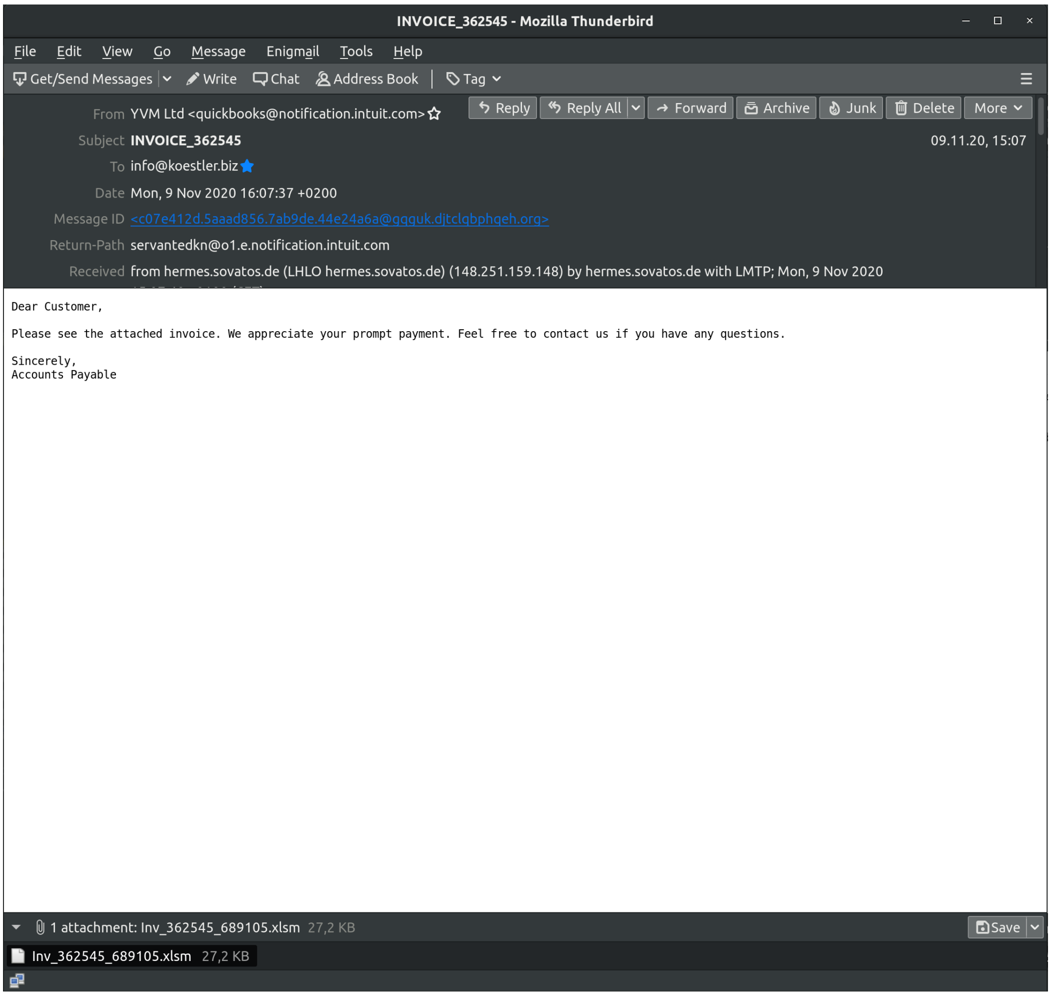
To Recipients <angelia@feikko.com>

Date Sun, 08 Nov 2020 14:37:06 -0800

Message ID <20201108223714.8058D7ECADF@mail.feikko.com>

Return-Path angelia@feikko.com

```
Hello

Please permit me to introduce myself. My name is John Monk. I earn a living in the oil industry as an independent Feasibility/Project Management Consultant
to oil refineries and other oil industries in Southern African, East Africa and some parts of Asia. We are based in Johannesburg RSA. Our mandate includes
identifying specific licensed crude oil export/ marketing firms and recommending these firms to the oil refineries for supply of crude oil to the
refineries.

On my desk is a mandate from one the refineries to arrange for crude oil purchase from Libya for up to 2,000,000 barrels on monthly bases for 12 calendar
months.

The essence of my reaching out to you is the fact that am in the process of building a middle man structure to mediate between the 2 parties involved before
the contract is signed. You may be wondering why I cannot do it by myself right? The honest fact is that as a consultant to these oil refineries, we are not
allowed to act as suppliers of crude oil to them as well, hence the reason I need a trustworthy person outside my work circle in order to maintain a
discreet profile.

I wish to extend this partnership to you my friend to build a middle man structure with you, while I work from the back to guide you. Our
commission/brokerage as middle persons is between $2 - $3 per barrel as case may be. So if the target of 2M barrels is met monthly we stand to share $4M -
$6M every month for a span of 12 months with possible extension.

Worry less about the speedy sales as I have contacts within oil producing country's top officials for license of crude oil export/lifting to any firm I so
present for this business. Therefore if you can be able to handle this transaction with honesty and integrity, you should come back to me immediately for
more details. Your urgent response is highly needed
Regards.

John Monk
```

3. 

From YVM Ltd <quickbooks@notification.intuit.com>

Subject **INVOICE_362545**

09.11.20, 15:07

To info@koestler.biz

Date Mon, 9 Nov 2020 16:07:37 +0200

Message ID <c07e412d.5aaad856.7ab9de.44e24a6a@gqguk.djtclqbphqeh.org>

Return-Path servantedkn@o1.e.notification.intuit.com

Received from hermes.sovatos.de (LHLO hermes.sovatos.de) (148.251.159.148) by hermes.sovatos.de with LMTP; Mon, 9 Nov 2020

```
Dear Customer,

Please see the attached invoice. We appreciate your prompt payment. Feel free to contact us if you have any questions.

Sincerely,
Accounts Payable
```

1 attachment: Inv_362545_689105.xlsm 27,2 KB

Inv_362545_689105.xlsm 27,2 KB