Buffer Overflow SLMail-5.5.0 Service and Gain Root Shell

Devin Trejo
devin.trejo@temple.edu

April 8, 2016

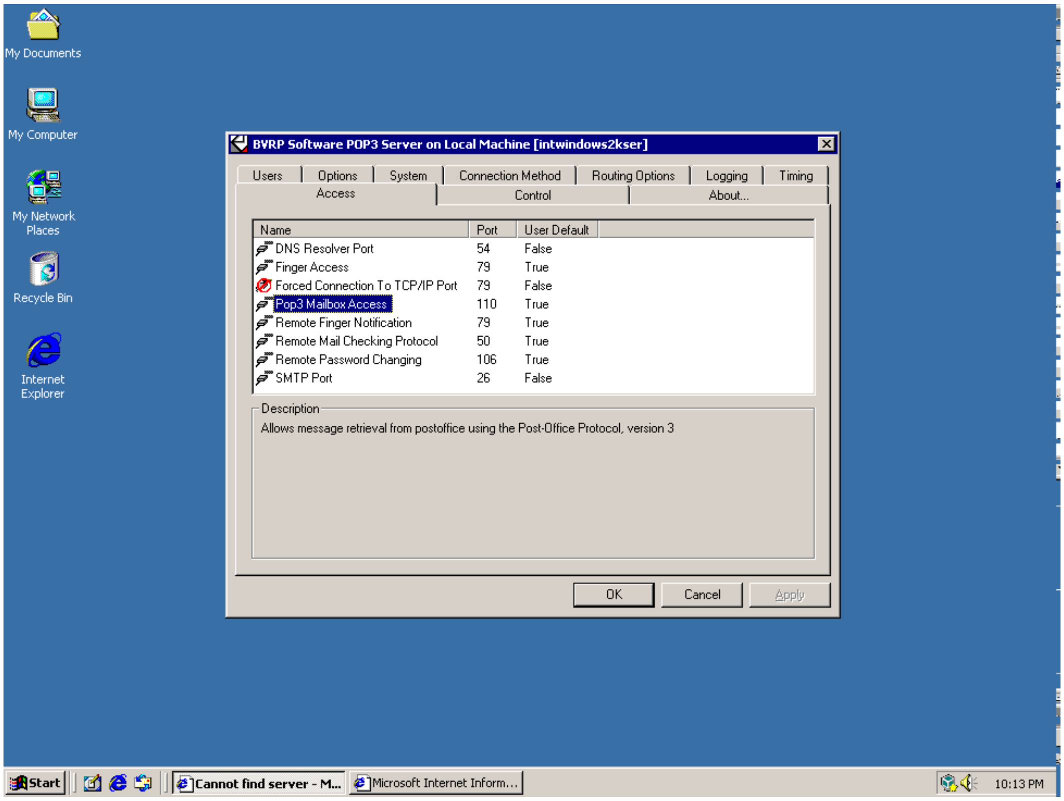
1 Summary

2 Introduction

2.1 Background SLMail5.5.0

SLMail is a message management tool that was advertised towards small to medium sized businesses published by SeatleLabs. The software was popular around the year 2001 for its ease of use and "security" of its email service [1]. The service was also scalable for an unlimited number of users to use. The software boast a number of security features including "Limitting Viruses by identify specific files or types not permitted to enter/leave the server, Reject emails containing unwanted words, Avoid external use of network as relay for spam, reduce flow of junk mail (anti-spam filter), and authenticate users before they send mail" [1]. The last "security" feature was instead a security flaw as the password authentication had a server buffer overflow vulnerability. The service is no longer continue if one were to search for it on SeattleLabs current website.

The SLMail service is an external program outside a standard Windows Server environment, that is bought and downloaded direct from SeattleLabs's website. The default configuration options after a succesfull installation of SLMail can be seen in figure 1. The specific version we concern ourselves for this project will by **SLMail5.5.0** which has a known buffer overflow exploit inside the user authentication prompt. When logging in over POP3, an application standard protocol for retrieving emails from a remote server, SLMail will prompt for a user-name and password combination associated with the desired email. If we write our user-name as any string and password containing a shell program we can setup and execute a script on the remote mail server. The shell script written will be specially crafted to open a port on the remote server, that gives us access to a shell that contains administrative privileges.



BVRP Software POP3 Server on Local Machine [intwindows2kser]

Name	Port	User Default
DNS Resolver Port	54	False
Finger Access	79	True
Forced Connection To TCP/IP Port	79	False
Pop3 Mailbox Access	110	True
Remote Finger Notification	79	True
Remote Mail Checking Protocol	50	True
Remote Password Changing	106	True
SMTP Port	26	False

Description

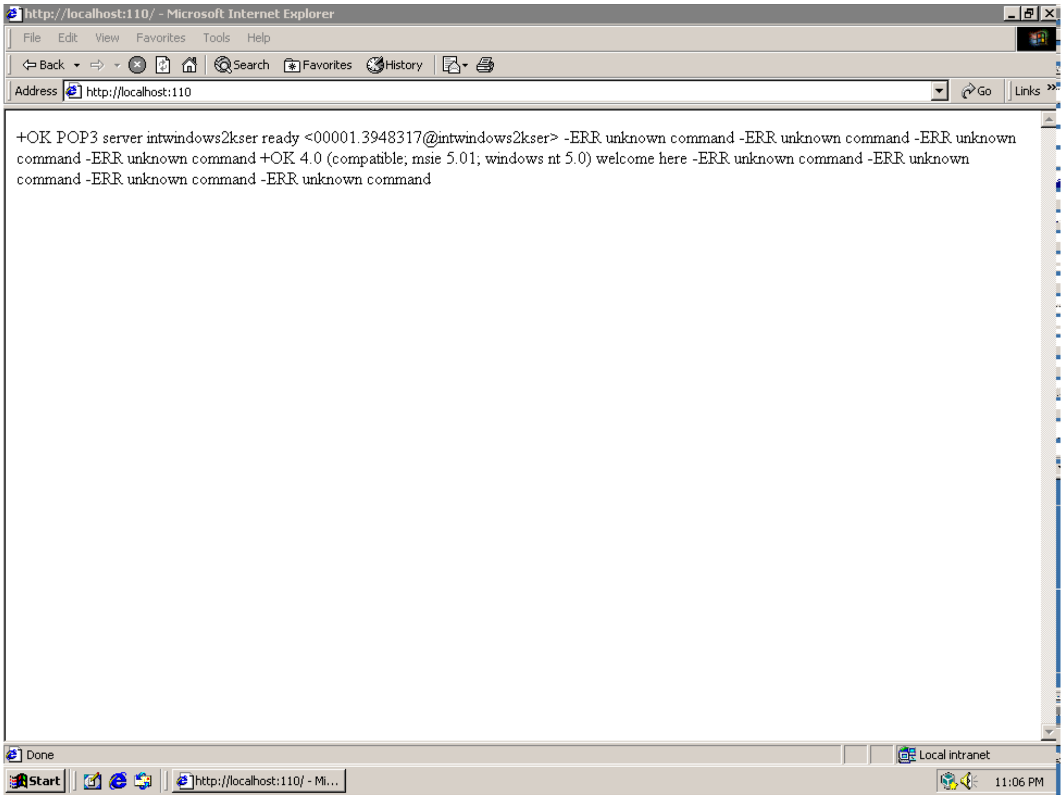
Allows message retrieval from postoffice using the Post-Office Protocol, version 3

Figure 1: Default SLMAail Port Configuration

2.2 Attack Approach: Fuzzing Attack

The first step for this attack is to gain more information of the SLMail 5.5.0 service. We will implement a technique known as **fuzzing** which will allow us to discover information such as service versions, buffer sizes, and in general the coding implementation of the remote service. To begin the fuzzing process to find the buffer size of the PASS field over the POP3 protocol, we first will write a script that loops over an array of increasing buffer sizes trying to determine the full length of the input buffer size. Since we already know there is an buffer overflow exploit for these fields we can expect at some point our input to overflow the allocated buffer and crash the program. The idea for this fuzzing processes is to overwrite the **EIP register** or the address location on the program stack containing the location in memory the program should return to after executing the USER and PASS input prompt function.

For this assignment we will examine the structure of the SLMail-5.5.0 program and gain insights on its construction. Note that connection of a direct socket connection is required. The POP3 interface seen on port 101 is not compatible with standard the standard http protocol as is demonstrated in figure 2.



http://localhost:110/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
http://localhost:110
Go
Links
Done
Local intranet
Start
http://localhost:110/ - Mi...
11:06 PM

```
+OK POP3 server intwindows2kser ready <00001.3948317@intwindows2kser> -ERR unknown command -ERR unknown command -ERR unknown
command -ERR unknown command +OK 4.0 (compatible; msie 5.01; windows nt 5.0) welcome here -ERR unknown command -ERR unknown
command -ERR unknown command -ERR unknown command
```

Figure 2: Trying to Connect to SLMail POP3 over HTTP

2.3 Test Environment

For this project we use our default test environment. We have a virtual private network consisting of our Windows 2000 SP4 Server, Kali Linux penetrating machine, and a host machine running inside Oracle Virtual Box. The server has a DHCP server running on the VM host machine. The IP/MAC addresses for each are provided in table 1.

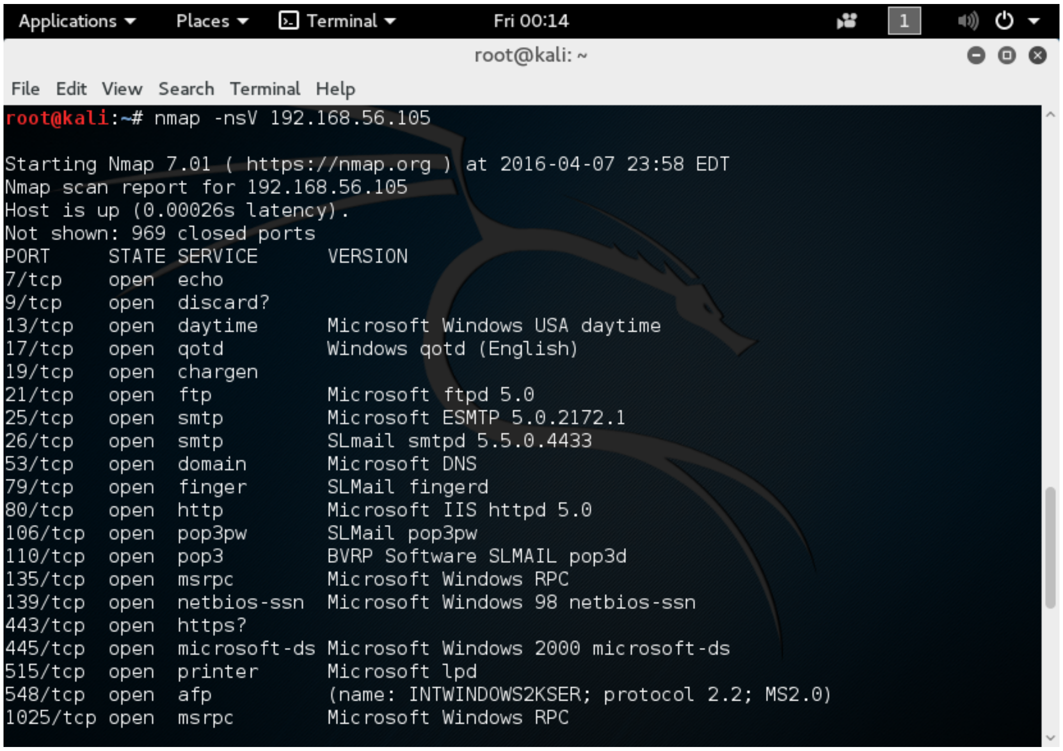
Platform	MAC ADDR	Platform IPv4 Address
Kali Linux:	08:00:27:94:5b:ba	192.168.56.102
Windows 2k Server:	08:00:27:87:29:68	192.168.56.105
VM Host Machine:	08:00:27:7c:86:0d	192.168.56.100

Table 1: IP Configuration for SLMail Pen-test Virtual Network

3 Discussion

To begin the intrusion we first have to setup our SLMail server. For this test we used default parameters as seen in figure 1. Next we conducted a NMAP scan from our Kali Linux Machine using NMAP. The scan we performed was a full version scan using the parameters seen shown below.

```
$ nmap -nsV 192.168.56.105
```



```
root@kali:~# nmap -nsV 192.168.56.105

Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-07 23:58 EDT
Nmap scan report for 192.168.56.105
Host is up (0.00026s latency).
Not shown: 969 closed ports
PORT     STATE SERVICE      VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime      Microsoft Windows USA daytime
17/tcp   open  qotd         Windows qotd (English)
19/tcp   open  chargen
21/tcp   open  ftp          Microsoft ftpd 5.0
25/tcp   open  smtp         Microsoft ESMTP 5.0.2172.1
26/tcp   open  smtp         SLmail smtpd 5.5.0.4433
53/tcp   open  domain       Microsoft DNS
79/tcp   open  finger       SLMail fingerd
80/tcp   open  http         Microsoft IIS httpd 5.0
106/tcp  open  pop3pw       SLMail pop3pw
110/tcp  open  pop3         BVRP Software SLMAIL pop3d
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows 98 netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows 2000 microsoft-ds
515/tcp  open  printer      Microsoft lpd
548/tcp  open  afp          (name: INTWINDOWS2KSER; protocol 2.2; MS2.0)
1025/tcp open  msrpc        Microsoft Windows RPC
```

Figure 3: NMAP Scan of Windows Server 2k

From the scan results seen in figure 3 we can see a multitude of open ports and the services running behind the ports. We we are interested in is port 110 which is the standard port for POP3 operations. We know from our research that after installing SLMail an open POP3 port will open that contains the known vulnerability. The NMAP scan revealed a number of other services running on our Windows 2k Server instance but for this test we will focus on port 110.

4 Conclusion

References

[1] SeattleLabs, “SLMail,” 2001. [Online]. Available: https://web.archive.org/web/20010413021016/http://www.seattlelab.com/slmail/

Appendix