Lecture 21: Buffer Overflow Attack

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

April 4, 2017

11:02am

Goals:

- Services and ports
- A case study on buffer overflow vulnerabilities: The `telnet` service
- Buffer Overflow Attack: Understanding the call stack
- Overrunning the allocated memory in a call stack
- Demonstration of Program Misbehavior Because of Buffer Overflow
- **Using `gdb` to craft program inputs for exploiting buffer-overflow vulnerability**

CONTENTS

21.1: Services and Ports

- Since buffer overflow attacks are typically targeted at specific services running on certain designated ports, let's start by reviewing the service/port pairings for some of the standard services in the internet.

- Every service on a machine is assigned a port. On a Unix/Linux machine, the ports assigned to standard services are listed in the file `/etc/services`. [The pathname to the same sort of a file in a Windows machine is `C:Windows\System32\Drivers\etc\services` . If you want to teach this file through Cygwin, the pathname is `/cygdrive/c/windows/System32/drivers/etc/services`] Here is a very small sampling from this list from my Linux laptop:

```
# The latest IANA port assignments for network services can be obtained
# from:
#        http://www.iana.org/assignments/port-numbers
#
# The Well Known Ports are those from 0 through 1023.  The Registered
# Ports are those from 1024 through 49151. The Dynamic and/or Private
# Ports are those from 49152 through 65535

# Each line describes one service, and is of the form:
#
#    service-name  port/protocol  [aliases ...]    [# comment]

echo 7/tcp
echo 7/udp
daytime 13/tcp
daytime 13/udp
ftp-data 20/tcp
ftp 21/tcp
ssh 22/tcp # SSH Remote Login Protocol
telnet 23/tcp
smtp 25/tcp mail
time 37/tcp timserver
domain  53/udp
domain 53/tcp
tftp 69/tcp
finger 79/tcp
http 80/tcp www www-http # WorldWideWeb HTTP
kerberos 88/tcp kerberos5 krb5 # Kerberos v5
hostname 101/tcp hostnames # usually from sri-nic
pop3 110/tcp pop-3 # POP version 3
sunrpc 111/tcp portmapper # RPC 4.0 portmapper TCP
sunrpc 111/udp portmapper # RPC 4.0 portmapper UDP
auth 113/tcp authentication tap ident
auth 113/udp authentication tap ident
sftp 115/tcp
sftp 115/udp
uucp-path 117/tcp
nntp 119/tcp readnews untp # USENET News Transfer Protocol
ntp 123/tcp
netbios-ns 137/tcp # NETBIOS Name Service
imap2  143/tcp imap  # Internet Mail Access Protocol
imap2  143/udp imap
ipp 631/tcp # Internet Printing Protocol
rsync 873/tcp # rsync
imaps   993/tcp # IMAP over SSL
pop3s 995/tcp # POP-3 over SSL
biff 512/udp comsat
login 513/tcp
who 513/udp whod
shell 514/tcp cmd # no passwords used
printer 515/tcp spooler # line printer spooler
printer 515/udp spooler # line printer spooler
talk 517/udp
router 520/udp route routed # RIP
uucp 540/tcp uucpd # uucp daemon
netstat 15/tcp # (was once asssigned, no more)
...
```

```
...
and many many more, see /etc/services for the complete list.
```

- It is important to note that when we talk about a network service on a machine, it does not imply that the service is only meant for human users in a network. In fact, many of the services running on your computer are for the benefit of other computers (and other devices such as printers, routers, etc.).

- A continuously running computer program that provides a service to others in a network is frequently called a **daemon server** or just **daemon**.