Counter Hack Notes

Gautam Batra

January 10, 2021

1 Important Commands

Command	Use
netstat -na	show port status, n=numerical form, a=all
chkconfig	list the names of services started by init, and those started by inetd/xinetd
lsof	list open files: lists the files opened for each process lsof|grep [prog_name]: to see files specific to a program lsof -p [pid]: lists files opened by the process denoted by the PID lsof -i: lists the tcp and udp usage
/etc/passwd	Contains information about each user (one user per line). If (encrypted) passwords not mentioned, * or x will be displayed. Passwords will be stored in the shadow password file: /etc/shadow or /etc/secure
s/etc/group	contains information about the groups
find / -uid 0 -perm -4000 -print	find all SetUID programs
rsh, rlogin, rcp	remote shell/login/copy. unsecured (clear text). dont use.

2 Notes

- TCP Control bits: **U**nskilled **A**ttackers **P**ester **R**eal **S**ecurity **F**olks
- Find all SYN packets tcpdump 'tcp[13] & 2 != 0'
- IP Tables: Blocking an IP:
  iptables -A INPUT -s 192.168.1.5 -j DROP
- A port with a listening service is known as an open port, whereas a port where nothing is listening is closed.
- inetd: internet daemon
- /etc/services: contains list of all network services and port numbers
- /etc/inetd.conf: for configuring individual network services
  wait status: wait = one process for all requests of a service
  nowait = inetd creates one process per request
- chkconfig --list: display a list of all services configured to start up at system boot and by xinetd

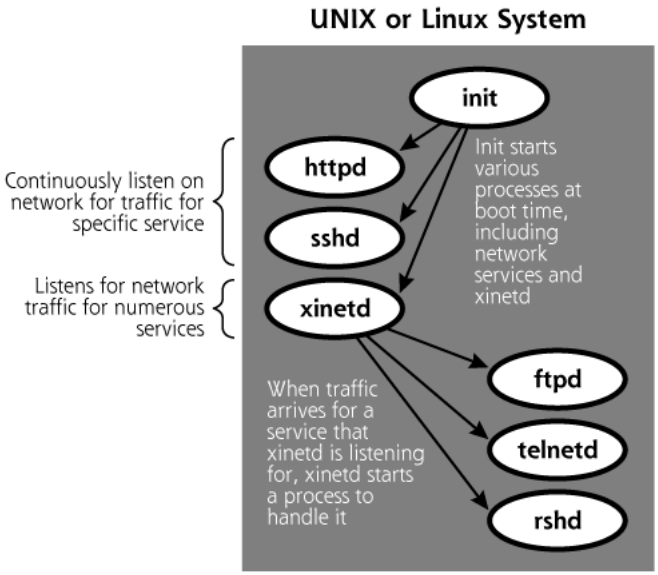

Figure 1: Relationship between init, xinetd, and various network services