Jerry Olds

1001533643

CSE-4380-001

3/2/2020

Pre-Lab 2

1) b
2) b
3) d
4) a
5) a
6) d
7) d
8) c
9) a
10) c
11) c
12) b
13) b
14) d
15) a
16) useradd alice
17) id alice
18) su alice1
19) whoami
20) mkdir prelab2
21) pwd
22) touch testfile
23) chown user2 testfile
24) chmod 764 testfile
25) rm testfile rmdir prelab2
26) unmask 022
27) umask 077
28) getuid() and geteuid() do not accept any parameters

29) We use setreuid if _POSIX_SAVED_IDS is not defined

```
   void
do_setuid (void)
{   int
status;
#ifdef
_POSIX_SAVED_
IDS   status
= seteuid
(euid);
#else
  status = setreuid (ruid, euid);
#endif   if (status
< 0) {
    fprintf (stderr, "Couldn't set uid.\n");
exit (status);
    }
}
```

30)Remembers the real and effective user IDs

31) 1

32) a

33) d

34)Yes, he could crack the password within 24 hours. Anything 6 characters or less can be cracked within 24 days with a Radeon 6970 processor

35)Because MyMav uses a salt, it would take a very long time to try each hashed password with each salt. If Mallory only wanted a few targeted passwords, he would be able to get them in a more reasonable amount of time.

36)

a. 9#*d(38j

b. @Thisisapassword5

c. @Thisisapassword5, Thisisapassword5

d. candlebottleremotecupglassespicture

e. _Passwordpassword1

f. JerryDuaneOldsTheThird, if someone was targeting me and knew my name, my name as a password would not take centuries to crack

37)

a.

password: password
entropy: 0
crack time: instant

password: password151564
entropy: 15.688
crack time: 2.64s

password: thisisapassword57
entropy: 21.595
crack time: 158.4s

b.

i. it took 33 seconds to crack the three passwords using Jack the Ripper

ii. 33 seconds to crack all three passwords for Jack the Ripper, 161.08 seconds to crack all three passwords for zxcvbn

iii. john --wordlist=password.lst --rules password.txt

iv. Using a wordlist and a salt will increase the time of cracking a password, but using only a salt in default mode will usually decrease the time it takes to crack passwords

38)b

39)d

40) ./snort -dev -l ./log -h 156.118.76.54/23

41) !

42) -O

43)b

44) Network-based, Wireless, Network behavior, Host-based

45)d

46)b

47)e

48)

a. ps -elf|grep root

b. kill -9 1234

c. ss -lntu

d. find / -perm +2000

e. inetconv

f. xinetconv

49) ~/, $PATH=/usr/bin:/usr/sbin:/usr/local/bin

50)c

51)b

52)c

53)d

54)

a. in the hosts.deny file enter the line sshd,vsftpd : ALL and ALL : ALL

b. in the hosts.allow file enter the line in.telnetd: 192.168.10.0/24

c. in the hosts allow file enter the line sshd: 192.168.12.1 192.168.10.0/24

55)a

56)

Rule: block in log

Objective: Use a "default deny" filter ruleset

Rule: pass in on egress inet proto tcp from any to (egress) \
port $tcp_services
pass in inet proto icmp all icmp-type $icmp_types
Objective: Allow the following incoming traffic to the firewall from the Internet:

- SSH (TCP port 22)
- Auth/Ident (TCP port 113)
- ICMP Echo Requests

Rule: in on egress inet proto tcp to (egress) port 80 rdr-to $comp3
Objective: Redirect TCP port 80 connection attempts (which are attempts to access a web server) to computer COMP3

Rule: set loginterface egresss
Objective: Log filter statistics on the external interface

Rule: set block-policy return
Objective: By default, reply with a TCP RST or ICMP Unreachable for blocked packets.

Rule: Macros
Objective: Make the ruleset as simple and easy to maintain as possible.

57) I have no clue how to do this