Assignment 02

RISHI KUMAR SONI 1001774020

QUESTION	ANSWERS
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 alice11
19	whoami
20	mkdir prelab2
21	pwd
22	touch testfile
23	chown user2 testfile
24	chmod 764 testfile
25	rm -rf prelab2 testfile
26	unmask 022

27 unmask 077

28 void and void

29 setreuid

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

30 Saves the uid, euid, and (mostly critically and specified in the website) sets the euid back to the uid for safety.

31 Just one:

```
stream=fopen(SCORES_FILE,"a");
```

32 a

33 d

34 Yes because it is 6 characters which is before the "exponential wall" takes off

35 Since the hashed values are salted, he will have to try every hash with every salt which would take a long time. Pre-computation is out since he can't store all hashes with all salts. However, for each indivdual password of interest, there is only one salt and SHA-1 is fast, enabling him to crack any medium strength or weaker passwords.

36 .

A) K)j9h8g7

B) !234QwerAsdfZxcv

C) wingardiumleviosa = 149270665.544 seconds

Wi*ngardiumleviosa = 4950714077204901.56 seconds

D) pseudopseudohypoparathyroidism

E) 123456789aA*

f) infosec-5380-001

37 . B

38 . D

39 . log tcp any any - > 156.118.76.54.23 (msg : tftelnet packettf)

40. !

41 . nmap -o < ip address of target host > OR nmap -A < ip address of target host >

42 . C

43. Netwoek-based(NIPS), Wireless (WIPS) , Network behavior analysis(NBA), Host-based(HIPS)

44.C

45. B

46. E

47

a. ps -U root

b. kill 1234 or Kill- 9

c lsof -I tcp

netsat –inet –tcp OR netstat -at

d. And / -perms -2000 print

e. kill -HUP <pid>

f . /etc/init.d/xintetd restart or kill -HUP<pid of xinetd>

48. $ PATH is set to a list of directories where commands (binaries) can be found and is searched each Bme a command is executed.

tf/usr/bin:/usr/sbin:/usr/local/bintf

49. c

50 . A or B

51 .B

52. D

53. in /etc/hosts.deny:

ALL:ALL

In/etc/hosts.allow:

telnet : 192.168.1.10

sshd : 192.168.12.1, 192.168.1.10

54. A

55.

Int_if=tfxl0tf

Tcp_services=tf{22,113}tf

Icmp_types=tfechoreqtf

Comp3=tf192.168.0.3tf

objecBve:Helps with Make the ruleset as simply and easy to maintain as possible.

Rule : set block-policy return

ObjecBve:None. This sets the block policy to return.

Rule : set logininterface egress

objecBve: Log Qlter staBscBcs on the external interface

Rule : set skip on lo

objecBve: None, but it is a best pracBce to not Qlter on the loopback interface.

Rule : anchor tfWp-proxy/*tf

objecBve: Helps with the make the ruleset as simple and easy to maintain as possible.

Dynamically insert rules.

Rule : pass in quick on $int_if net proto tcp to any port Wp divert-to 127.0.0.1 port 8021

objecBve: None . Diverts FTP connecBons to the FTP proxy on this host, post port 8021.

Rule: match out on egress inet from !(egress:network) to any nat-to(egress:0)

obecBve:None. Its sets up the NAT.

Rule : block in log

objecBve: Use a tfdefault denytf Qlter ruleset, and Log Qlter staBsBcs on the external interface.

Rule : pass out quick

objecBve : Helps with make the ruleset as simple and easy to maintain as possible.

Egress traXc is allowed out without further rules.

Rule : anBspoof quick for { lo $int_if}

objecBve: None. Blocks spoofed Ips(loopback and internal Ips from the external interface).

objecBve: Log Qlter staBscBcs on the external interface

Rule : pass in on egress inet proto tcp from any to egree prot $ tcp_services

objecBve: Allow the following income traXc to the Qrewall from the internet:

SSH(TCP port 22): this will be used for external maintenance of the Qrewall machine.

Auth/Ident (TCP port 113) : used by some services such as SMTP and IRC.

Rule : pass in on egress inet proto tcp to(egress) port 80 rdr-to $comp3

objecBve: Redirect TCP port 80 connecBon aYempts which are aYempts to access a web server to computer COMP3. Also, permit TCP port 80 traXc desBned for COMP3 throught the Qrewall.

Rule : pass in inet proto icmp all icmp-type $icmp_types

objecBve: Allow the following incoming traXc to the Qrewall from the internet:

ICMP Echo Requests:the ICMP packet type used by ping(8).

Rule : pass in on $int_if

objecBve: None. Passes internal traXc without restricBons.