P1)

Connections

Ospf code

1)en

2)conf t

3)router ospf 1

4)network 192.168.10.0 0.0.255.255 area 1

5)network 10.0.0.0 0.255.255.255 area 1

Same steps for all 3 routers

i)OSPF MD5 Authentication

code

Router 1

1. en
2. conf t
3. router ospf 1
4. area 1 authentication message-digest
5. exit
6. interface s0/1/0
7. ip ospf message-digest-key 1 md5 mdpass
8. exit
9. show ospf interface(to check authentication is applied or not) and then apply in all 3 routers

ii)NTP

go to

server service NTP enable Key-1 password ntppass change to current time if required

Routers(All routers)

Code

1. en
2. show clock

3. conf t
4. ntp server 192.168.10.2(what is your ip address)
5. ntp update-calendar
6. exit
7. show clock
8. conf t(if we have exitted)
9. ntp authenticate
10. ntp trusted-key 1
11. ntp authentication-key 1md5 ntppass

iii)Syslog
continue if ntp is asked otherwise start with en
code

1. conf t
2. service timestamp log datetime msec(do not exit)
3. logging host 192.168.10.3(what we have taken ip)
4. exit
5. en
6. show logging

perform in all three routers

iv)SSH connection
for any one router
router3 in CLI
Code

1. ip domain-name cybernet.com
2. username SSHadmin privilege 15 secret sshpass
3. line vty 0 4
4. login local
5. transport input ssh
6. exit
7. hostname R3

8. crypto key generate rsa
9. 1024
10. Exit

Check remote connection on the pc

Go to pc Desktop cmd type ssh-l SSHAdmin 192.168.10.2(deny)

Ssh-l SSHAdmin 192.168.20.1 password sshpass(alow)

P2) Configure AAA

a)Configure a local user account on Router and vtg lines using localAAA

code router 0

1. en
2. conf t
3. username Admin1 secret admin1pass
4. aaa new-model
5. aaa authentication login default local
6. line console 0
7. login authentication default
8. end
9. conf t
10. ip domain-name cybernet.com
11. hostname R1
12. crypto key generate rsa
13. line vty 0 4
14. login authentication default
15. transport input ssh
16. end
17. exit

router 1

code

1. en

2. conf t
3. username Admin2 secret admin2pass
4. aaa new model
5. aaa authentication login default group tacacs+ local
6. tacacs-server host 192.168.2.2 (tacas server ip)
7. tacacs-server key tacacspass
8. line console 0
9. login authentication default
10. end
11. exit

Router2
Code

1. en
2. conf t
3. username Admin3 secret admin3pass
4. aaa new model
5. aaa authentication login default group radius local
6. radius-server host 192.168.3.2
7. radius-server key radiuspass
8. line console 0
9. login authentication default
10. end
11. exit

P3)Configuring extended ACL

Number Acl(FTP access)
Code

1. en
2. conf t
3. hostname maaz

4. access-list 100 permit tcp 172.22.34.224 0.0.0.31(FTP PC-Address) host 172.22.34.194 (server address) eq ftp
5. interface gi0/0
6. ip access-group 100 in
7. exit

Name ACL(HTTP access)
1)en
2)conf t
3)ip access-list extended HTTP_ONLY
4)permit tcp 172.22.34.240 0.0.0.15 host 172.22.34.194 (server address) eq www
 4)interface gi0/1
5)ip access-group HTTP_ONLY in
6)exit

PRAC4) IP ACLs TO MITIGATE ATTACKS

STEP1: Loop back address in Router2

1) interface Lo0
2) ip address 192.168.2.1 255.255.255.0

STEP2: Ospf routing in all 3 routers

STEP3: Verify in SSH connection from PC-A

For PC-A in Router2
1) en
2) conf t
3) logging host 192.168.1.2

4) ip domain-name cybernet.com
5) username SSHadmin privilege 15 secret sshpass
6) line vty 0 4
7) login local
8) transport input ssh
9) crypto key generate rsa

For PC-C in Router2

1) en
2) conf t
3) logging host 192.168.3.2
4) ip domain-name cybernet.com
5) username SSHadmin privilege 15 secret sshpass
6) line vty 0 4
7) login local
8) transport input ssh
9) crypto key generate rsa
10)exit

STEP4:

R1:

1) access-list 10 permit host 192.168.3.2
2) line vty 0 4
3) access-class 10 in

R2:

1) access-list 10 permit host 192.168.3.2
2) line vty 0 4
3) access-class 10 in

R1:

1) access-list 10 permit host 192.168.3.2
2) line vty 0 4
3) access-class 10 in

STEP5: PC-A(server)

Code

1) access-list 120 permit udp any host 192.168.1.2 eq domain
2) access-list 120 permit tcp any host 192.168.1.2 eq smtp
3) access-list 120 permit tcp any host 192.168.1.2 eq ftp
4) access-list 120 deny tcp any host 192.168.1.2 eq 443
5) access-list 120 permit tcp host 192.168.3.2 host 192.168.1.2 eq 22
6) interface s0/1/0
7) ip access-group 120 in
8) exit

PRAC5)Configuring a zone-based policy firewall

STEP1: Ospf routing in all 3 routers

STEP2: Establish a SSH connection for routers from pc and server

STEP3:check version of router3 and enable security feature

code

1) en
2) conf t
3) licence boot module C1900 technology-package security
4) exit
5) copy run start
6) reload
7) exit

STEP4:ACL and class map

code

1) access-list 101 permit ip 192.168.30.0 0.0.0.255 any
2) class-map type inspect match-all IN-NET CLASS-MAP
3) match access-group 101
4) exit

STEP5:Policy map

1) policy-map type inspect IN-2-OUT-MAP
2) class type inpect IN-NET-CLASS-MAP
3) inspect
4) exit

STEP6:Create a Zone

Code

1) Zone Security IN-ZONE
2) Exit
3) Zone Security OUT-ZONE
4) Exit
5) Zone-pair security IN-2-OUT-ZAIR Source IN-ZONE destination OUT-ZONE
6) Service-policy type inspect IN-2-OUT-PMAP
7) Zone-member Security IN-ZONE
8) Exit
9) Int Se 0/1/0
10) Zone-member security OUT-ZONE
11) Exit

***Command for output-(PC-C)**

ping 192.168.10.2
ssh-l SSHAdmin 20.0.0.2
Show policy-map type inspect zone-pair session(R3’S CLI)
(PC-A)
ping 192.168.30.2

Pracrical6:Configure IOS (IPS)using CLI

Code(R1)

1) en
2) conf t
3) licences boot module C1900 technology-package security
4) yes
5) exit
6) copy run start
7) reload yes
8) exit

(configure IOS (IPS))

9) en
10) mkdir dirips
11) enter
12) conf t
13) ip ips config location flash:dirips
14) ip ips name iosips
15) ip ips notify log
16) Service timestamp log datetime msec
17) logging host 192.168.10.3(SYSLOG SERVER)
18) ip ips signature-category
19) category all
20) retired true
21) exit
22) category ios-ips basic
23) retired false
24) exit
25) exit
26) enter

27) int g0/0
28) ip ips iosips out
29) exit
30) conf t
31) ip ips signature definature
32) Signature 2004 0
33) Status
34) retired false
35) retired true
36) exit
37) Engine
38) event-action deny
39) event-action produce-alert
40) exit(*3times)
41) Enter
42) Exit
43) Show ip ips all