**Network Security MINI PROJECT:**

**Allan F Makwembere 2108418**

**Elian-Roy 2115470**

**Zahran Mahmood 2100516**

**FIREWALL Configurations**

Firewall#sh run

Building configuration...

Current configuration : 3979 bytes

!

! Last configuration change at 10:01:05 UTC Wed Apr 26 2023 by user01

!

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname Firewall

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 5 $1$3G/8$YPv6TgBEbVMEHjnGBlzvA0

!

no aaa new-model

ethernet lmi ce

!

!

!

!

!

!

!

!

!

!

!

!

ip domain name networksecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

license udi pid CISCO1921/K9 sn FCZ202270G9

license boot module c1900 technology-package securityk9

!

!

username user01 secret 5 $1$f5Xv$r6YArkZJfPsB7tAOd8QQh.

username admin privilege 15 secret 5 $1$9ru0$4GVbn09bjS3IeFGmOCAyV.

!

redundancy

!

!

!

!

!

!

class-map type inspect match-any dmz-to-isp

match protocol http

match protocol https

match protocol icmp

match protocol dns

class-map type inspect match-any internaluser-to-internalserver

match protocol tcp

match protocol udp

match protocol icmp

class-map type inspect match-any internaluser-to-isp

match protocol icmp

match protocol https

match protocol http

match protocol dns

class-map type inspect match-any internaluser-to-dmz

match protocol http

match protocol https

match protocol icmp

match protocol dns

!

policy-map type inspect dmz-to-internaluser

class type inspect internaluser-to-dmz

inspect

class class-default

drop

policy-map type inspect dmz-to-isp

class type inspect dmz-to-isp

inspect

class class-default

drop

policy-map type inspect internaluser-to-dmz

class type inspect internaluser-to-dmz

inspect

class class-default

drop

policy-map type inspect internaluser-to-internalserver

class type inspect internaluser-to-internalserver

inspect

class class-default

drop

policy-map type inspect internaluser-to-isp

class type inspect internaluser-to-isp

inspect

class class-default

drop

!

zone security internalserver

zone security internaluser

zone security dmz

zone security isp

zone-pair security dmz-to-isp source dmz destination isp

service-policy type inspect dmz-to-isp

zone-pair security isp-to-dmz source isp destination dmz

service-policy type inspect dmz-to-isp

zone-pair security internaluser-to-dmz source internaluser destination dmz

service-policy type inspect internaluser-to-dmz

zone-pair security internaluser-to-internalserver source internaluser destination internalserver

service-policy type inspect internaluser-to-internalserver

zone-pair security dmz-to-internaluser source dmz destination internaluser

service-policy type inspect dmz-to-internaluser

zone-pair security internaluser-to-isp source internaluser destination isp

service-policy type inspect internaluser-to-isp

!

!

!

!

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

zone-member security internalserver

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.0.2 255.255.255.0

zone-member security internaluser

duplex auto

speed auto

!

interface Serial0/0/0

ip address 209.165.202.1 255.255.255.252

zone-member security isp

!

interface Serial0/0/1

ip address 209.165.201.1 255.255.255.252

zone-member security dmz

!

router rip

network 192.168.0.0

network 192.168.1.0

network 209.165.201.0

network 209.165.202.0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

!

!

!

control-plane

!

!

banner motd ^CCOnly zahran permitted!^C

!

line con 0

exec-timeout 5 0

password 7 083B4D461B180B46405858517C

logging synchronous

login local

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

exec-timeout 5 0

privilege level 15

password 7 001E120E165A05575D72181B5F

login local

transport input ssh

!

scheduler allocate 20000 1000

!

end

**DMZ CONFIGURATION**

no ip address

 shutdown

!

interface GigabitEthernet0/0

 ip address 209.165.200.1 255.255.255.0

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 no ip address

 duplex auto

 speed auto

!

interface Serial0/0/0

 no ip address

 clock rate 2000000

!

interface Serial0/0/1

 ip address 209.165.201.2 255.255.255.252

 clock rate 2000000

!

router rip

 network 209.165.200.0

 network 209.165.201.0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

!

!

!

control-plane

!

!

banner motd ^CCOnly Allan permited!^C

!

line con 0

 exec-timeout 5 0

 password 7 13213A285A5E577E7E717F

 logging synchronous

 login local

line aux 0

line 2

 no activation-character

 no exec

 transport preferred none

 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

 stopbits 1

line vty 0 4

 exec-timeout 5 0

 privilege level 15

 password 7 112D343F46405858517C7C

 login local

 transport input ssh

!

scheduler allocate 20000 1000

!

end

DMZ#

DMZ#show run

Building configuration...

Current configuration : 1812 bytes

!

! Last configuration change at 13:17:09 UTC Tue Apr 25 2023 by admin

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname DMZ

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 5 $1$fvIl$CsqiVYujlX4EihCc.VVUr/

!

no aaa new-model

!

!

!

!

!

!

!

!

!

!

!

!

!

!

ip domain name networksecurity.com

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

cts logging verbose

!

!

license udi pid CISCO1921/K9 sn FCZ1927C0XK

license boot module c1900 technology-package securityk9

!

!

username Allan1 secret 5 $1$nU96$4QbmxKF6CJNBwHt7AoD9U.

username admin privilege 15 secret 5 $1$K9Aa$XQCh6jp2xWRqLn621hk9g0

!

redundancy

!

!

!

!

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

!

!

!

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

 no ip address

 shutdown

!

interface GigabitEthernet0/0

 ip address 209.165.200.1 255.255.255.0

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 no ip address

 duplex auto

 speed auto

!

interface Serial0/0/0

 no ip address

 clock rate 2000000

!

interface Serial0/0/1

 ip address 209.165.201.2 255.255.255.252

 clock rate 2000000

!

router rip

 network 209.165.200.0

 network 209.165.201.0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

!

!

!

!

control-plane

!

!

banner motd ^CCOnly Allan permited!^C

!

line con 0

 exec-timeout 5 0

 password 7 13213A285A5E577E7E717F

 logging synchronous

 login local

line aux 0

line 2

 no activation-character

 no exec

 transport preferred none

 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

 stopbits 1

line vty 0 4

 exec-timeout 5 0

 privilege level 15

 password 7 112D343F46405858517C7C

 login local

 transport input ssh

!

scheduler allocate 20000 1000

!

end

**ISPROUTER**

ISPRouter#sh run

Building configuration...

Current configuration : 1962 bytes

!

! Last configuration change at 14:35:46 UTC Tue Apr 25 2023 by user1

!

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname ISPRouter

!

boot-start-marker

boot-end-marker

!

!

security passwords min-length 10

enable secret 5 $1$HmDy$j87ngBjQDux0dT6khjTua.

!

no aaa new-model

!

!

!

!

!

!

!

!

!

!

!

!

!

!

ip domain name networksecurity.com

ip cef

no ipv6 cef

multilink bundle-name authenticated

!

cts logging verbose

!

!

license udi pid CISCO1921/K9 sn FGL202525DK

!

!

username user1 secret 5 $1$Bx7I$T6TJ36ik8xld.ItPCIfnN/

username admin privilege 15 secret 5 $1$0ei5$upDrfsceNC9XuOJfUsv/t0

!

redundancy

!

!

ip ssh time-out 90

ip ssh authentication-retries 2

ip ssh version 2

!

!

!

!

interface Embedded-Service-Engine0/0

 no ip address

 shutdown

!

interface GigabitEthernet0/0

 ip address 198.51.100.1 255.255.255.0

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 no ip address

 duplex auto

 speed auto

!

interface Serial0/0/0

 ip address 209.165.202.2 255.255.255.252

 clock rate 64000

!

interface Serial0/0/1

 ip address 209.165.202.2 255.255.255.252

 clock rate 64000

!

router rip

 network 192.168.0.0

 network 192.168.1.0

 network 198.51.100.0

 network 209.165.202.0

 network 209.168.202.0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 192.168.0.0 255.255.255.0 209.165.202.1

ip route 192.168.1.0 255.255.255.0 209.165.202.1

ip route 209.165.200.0 255.255.255.0 209.165.201.1

!

!

!

!

control-plane

!

!

banner motd ^CCELIAN-ROY!^C

!

line con 0

 exec-timeout 5 0

 password 7 143E213B3E0B3F3F213A62

 logging synchronous

 login local

line aux 0

line 2

 no activation-character

 no exec

 transport preferred none

 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

 stopbits 1

line vty 0 4

 exec-timeout 5 0

 privilege level 15

 password 7 013A35346904131B245E1F

 login local

 transport input ssh

!

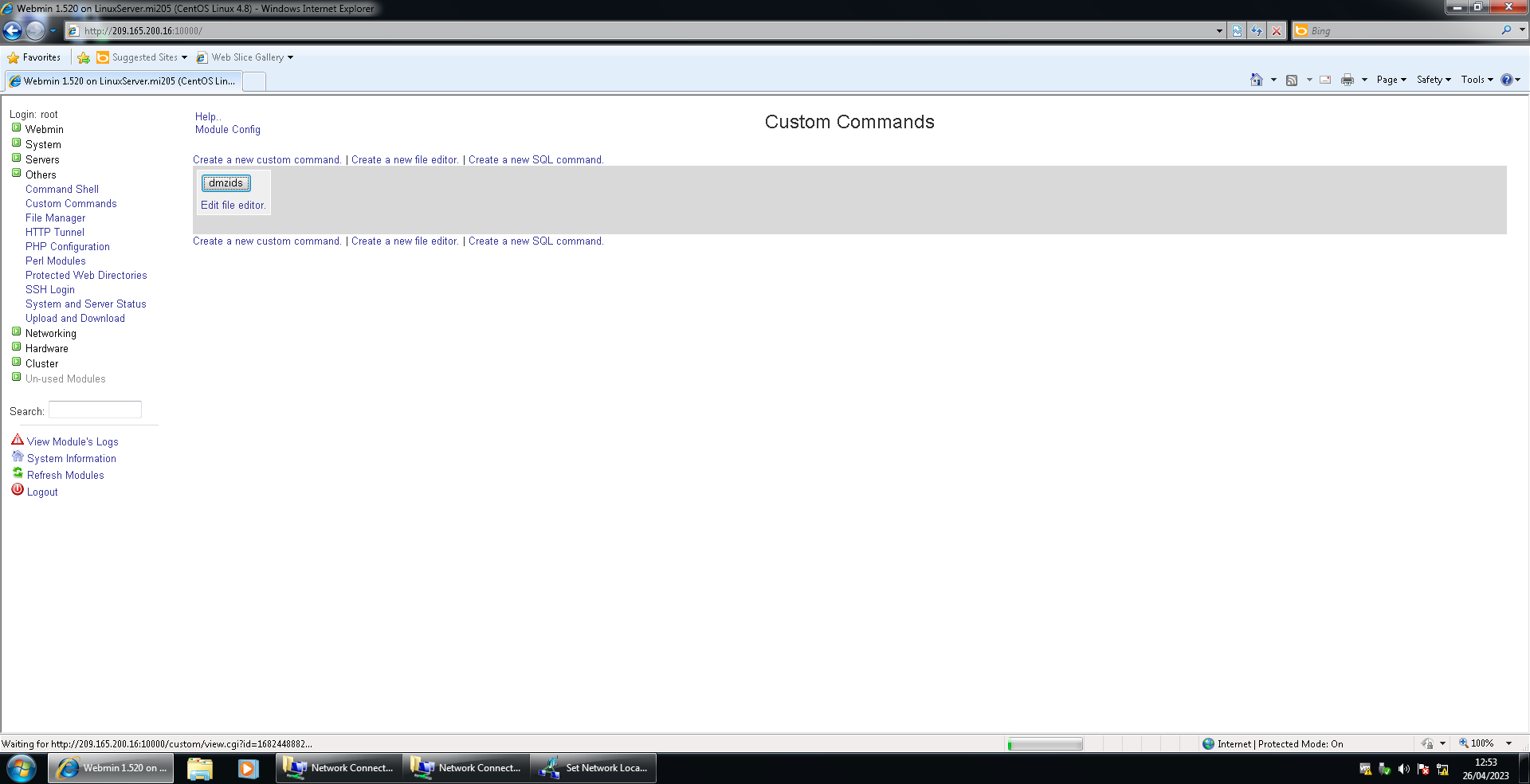
scheduler allocate 20000 1000

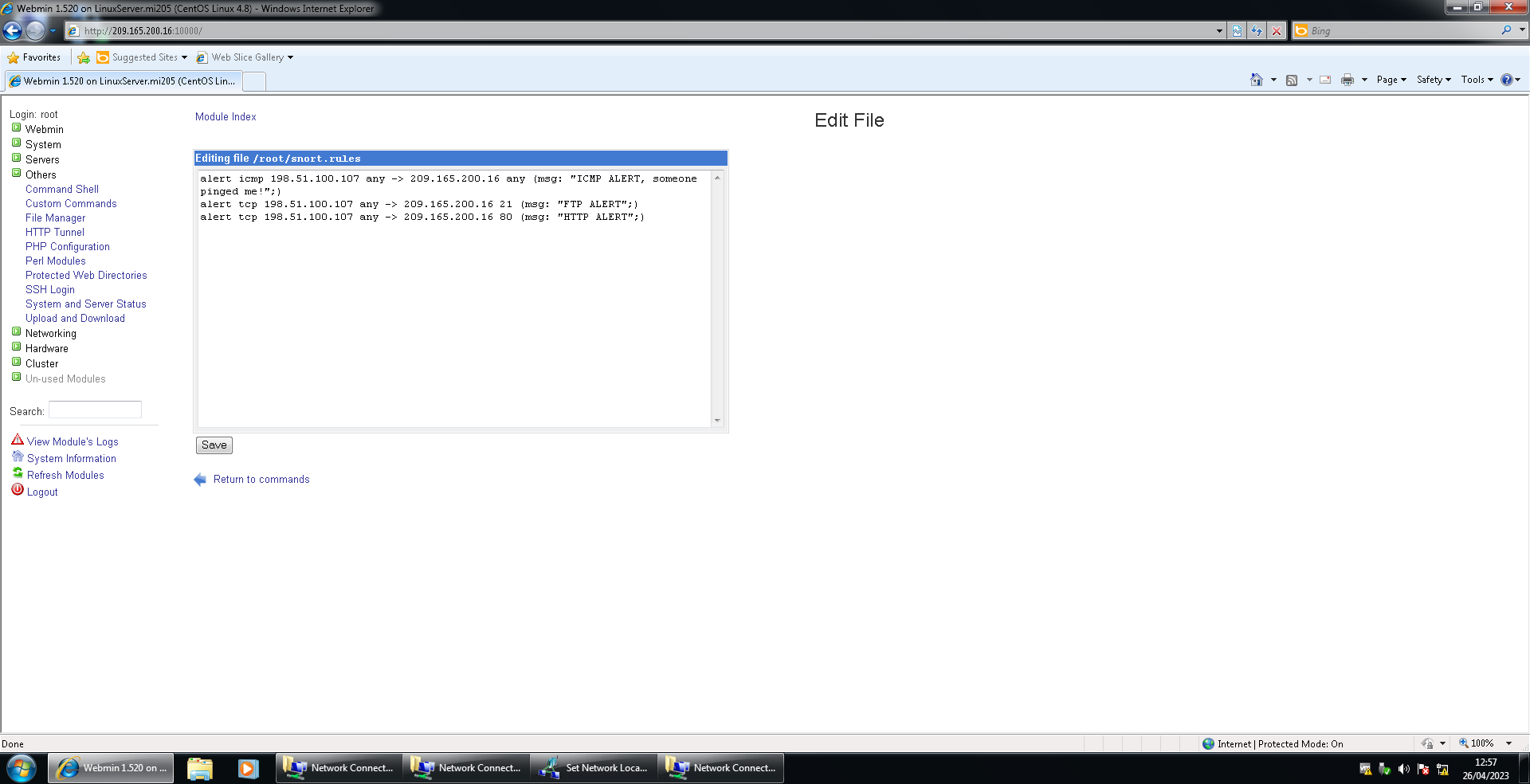
!

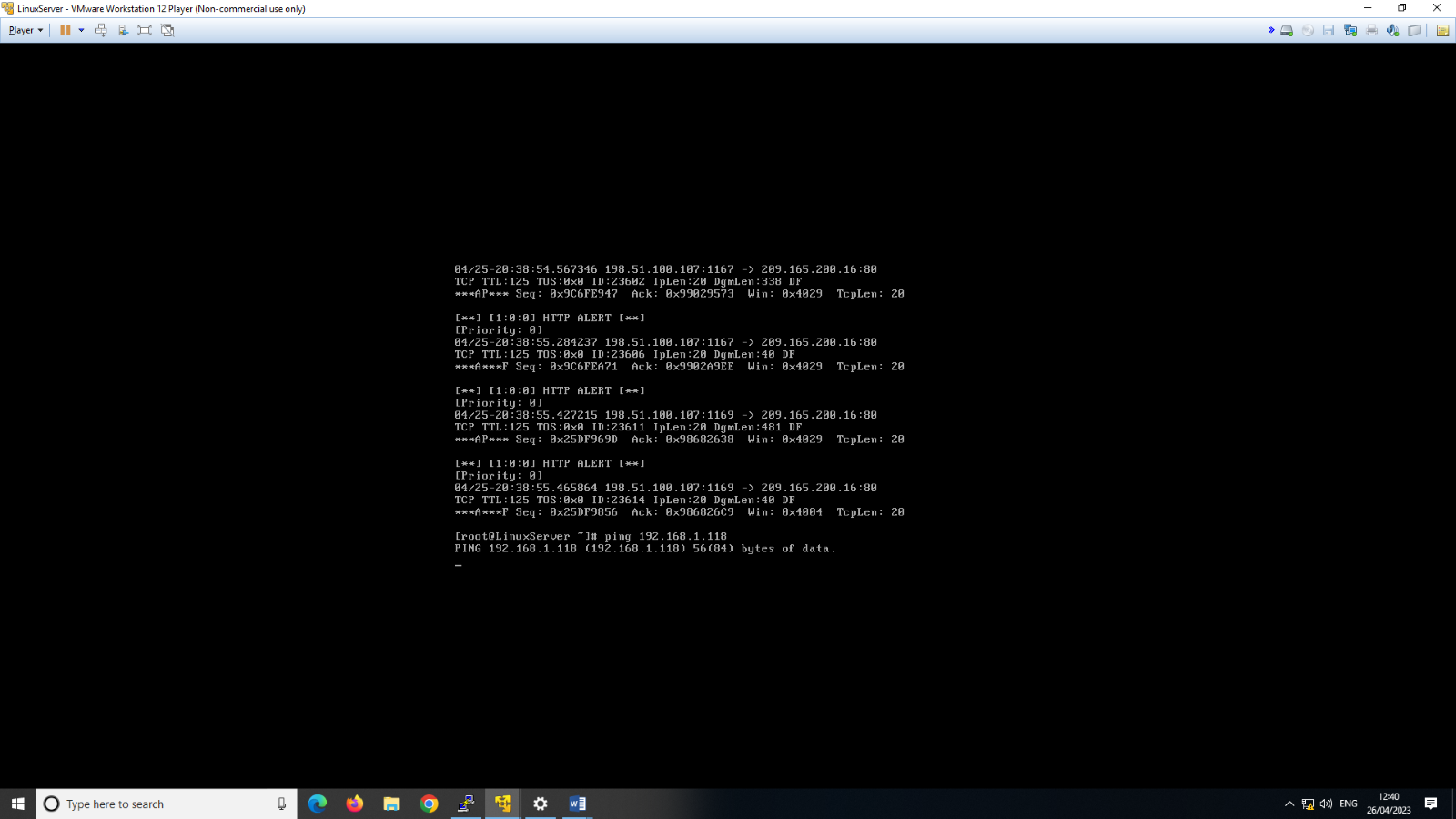
end

**TASK 4: IDS CONFIGURATIONS:**

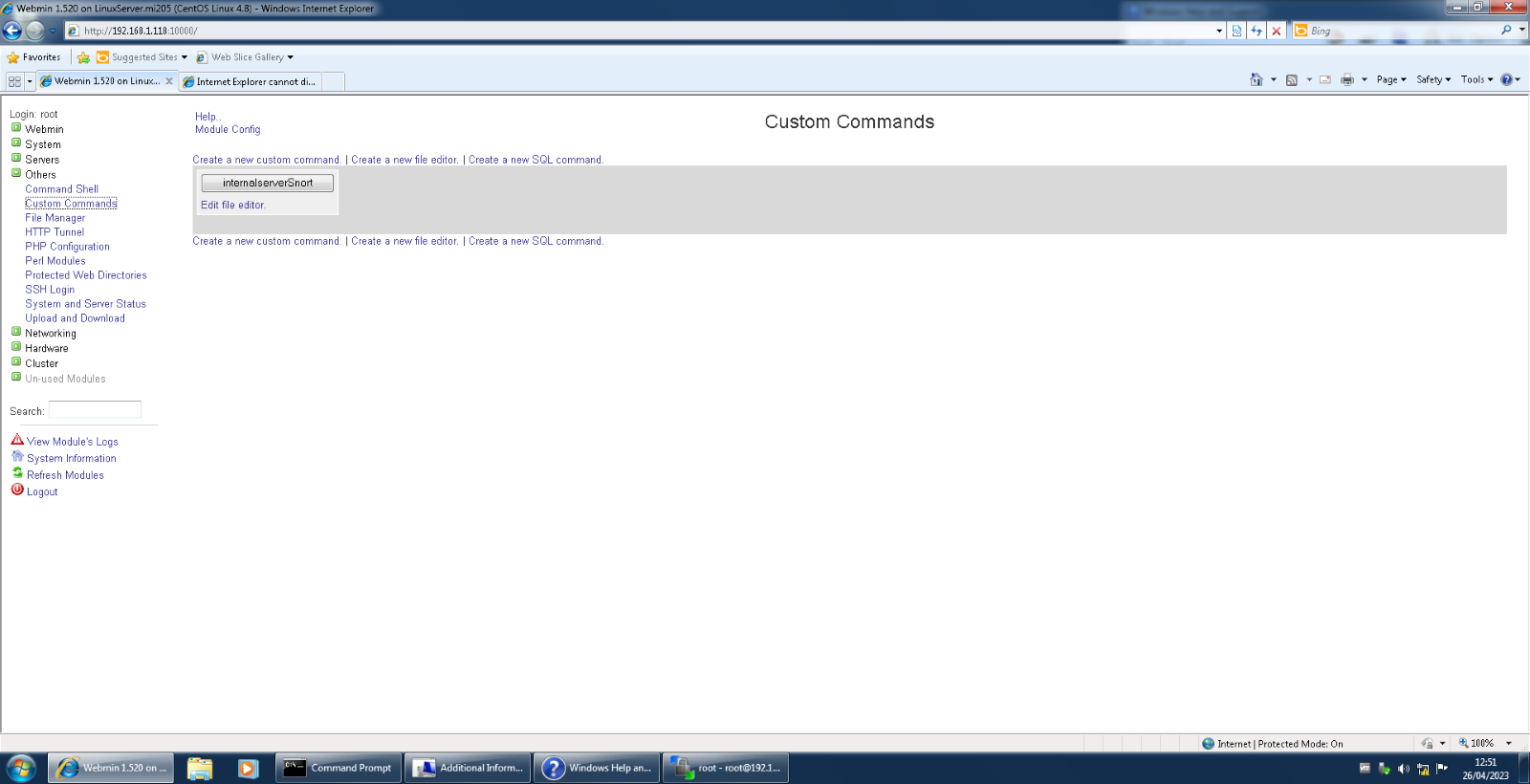
**DMZ SNORT**







**INTERNALSERVER SNORT**

****

