

Akademiija tehničko vaspitačkih nauka Komunikacione tehnologije Zaštita podataka u komunikacionim mrežama

# LABORATORIJSKA VEŽBA BR. 10

# Mrežne barijere

Programski paket Comodo Personal Firewall

### POTREBNA OPREMA

- Računar sa instaliranim Windows operativnim sistemom
- Instalirani programski paket Comodo Personal Firewall

## **TEORIJSKE OSNOVE**

#### **Comodo Personal Firewall**

Comodo Internet Security Kombinuje tehnike Antivirusne zaštite i naprednih tehnika filtriranja paketa i HIP sistem (engl.: *Host Intrusion Prevention*) kako bi zaštitio računar od internih i eksternih pretnji. Comodo u svom paketu sadrži Antivirusnu proaktivnu zaštitu, Mrežnu barijeru koja neprekidno pruža zaštitu filtriranjem paketa, Defence + koji sadrži napredne tehnike postavljanja pravila baziranim na IPS-u, (engl.: *Intrusion Prevention System*), koja pružaju zaštitu sistemskih datoteka od malicioznih (zlonamernih) procesa i blokira nepoznati malware pre nego što dobije priliku da se instalira na sistem. Sadrži još dva paketa koji su dostupni u **Profesional** verzijama, što znači da se ova dva paketa dodatno naplaćuju. To su **Live PC Support** što podrazumeva sve tipove online zaštite I **Secure Wireless Internet Conectivity** paket koji pruža bezbedno konektovanje na internet preko bilo koje javne bežične mreže (lokacije).

#### Demonstracija na Virtual Box-u

Sada ćete pokrenuti Comodo čija se startup ikonica nalazi na Desktopu. Na prvom prozoru imate listu svih dešavanja u saobraćaju (Sumary), Imate **Network Defence** i **Defence** +. Nas će danas interesovati samo Network Defence i način na koji ćete postaviti određena pravila za filtriranje paketa, restrikciju pristupa nekim programima kao i dozvolu pokretanja.

Kliknite na ikonicu **Firewall**, i otvoriće vam se područje Comodo-a gde ćete unositi pravila filtriranja:





Klikom na **Define a New Trusted Application** otvarate prozor za definisanje polise na određenu aplikaciju. Tako u ovom slučaju definišete aplikaciju od poverenja na sledeći način:



Otvara se prozor za definisanje aplikacije od poverenja i nju nalazite tako što ćete klikom na **Select** i **Browse** naći putanju do aplikacije kojoj želite da dozvolite pokretanje, (Za ovaj primer, ja sam uzeo TC PowerPack):

😻 Define a New Trusted Application	X	
	Select 💌	File Groups
What do these settings do?	Apply Cancel	Browse.

Potvrdite izbor aplikacije klikom Apply.

Define a New Trusted Application	<b>□</b>
C:\Program Files\TC PowerPack\TCPowerPack.exe	Select -
What do these settings do?	Apply Cancel

Sada klikom na Advanced dugme koje se nalazi na levoj strani aplikacije otvarate područje za napredno podešavanje polisa (pravila), zatim klik na **Network Security Policy** otvarate prozor za editovanje svih pravil koja su aktivna:

Network Security Policy Define and configure And the security Policy Experienced firewall users may use this section to create, or modify packet filtering rule Network Security Policy of the packet filtering engine in the firewall.
---

😻 Network Security Policy		
Application Rules Global Rules		
Application name Treat as	-	Add
Custom     Custom		
🖵 🥪 Allow All Requests		Edit
🖃 🕵 C:\Program Files\CrypTool\CrypTool.exe Custom	=	Demove
Allow All Requests		Kelliove
C:\Program Files\GNU\GnuPG\gpg2.exe Custom		Move Up
Allow IP Out From IP Any To IP Any Where Protocol Is Any		
C:\Program Files\GNU\GnuPG\bin\kbuildsycoca4.exe Custom		Move Down
Allow IP Out From IP Any To IP Any Where Protocol Is Any		
C:\Program Files\GNU\GnuPG\bin\kleopatra.exe     Custom		Purge
Allow IP Out From IP Any To IP Any Where Protocol Is Any		
C:\Program Files\GNU\GnuPG\bin\dbus-daemon.exe Custom		
Allow IP Out From IP Any To IP Any Where Protocol Is Any		
□ C:\Program Files\Avira\AntiVir Desktop\update.exe Custom		
Allow IP Out From IP Any To IP Any Where Protocol Is Any	-	
Concerned i en		
What do these settings do?	ОК	Cancel

Sada klikom na **Edit** možete promeniti pravila po kojima se aplikacijama dozvoljava ili zabranjuje aktivnost u prozoru **Application Network Access Control**:

😻 Application Network Access	: Control		X
Application Path:			
C:\Program Files\TC PowerPack\TCP	owerPack.exe		Select 🔹
Network Access Rules			
OUse a Predefined Policy	Blocked Application	-	
Use a Custom Policy	Copy From		
Allow All Requests			
	Remove	Move Up	Move Down
What do these settings do?		Apply	Cancel

Klikom na dugme Edit menjate trenutno važeću polisu za ovu aplikaciju tako da Source Address postavite na određenu adresu: **192.168.0.66** a Destination Addresss postavite na **192.168.0.99**:

General		
Action:	Allow 🔽	Log as a firewall event if this rule is fired
Protocol:	IP 🔽	
Direction:	In/Out 🗾	
Description:	Allow All Requests	
ource Address	Destination Address	IP Details w)
ource Address	Destination Address	IP Details
Exclude (i.e Any Single IP	Destination Address NOT the choice belo IP:	IP Details w/) 192 . 168 . 0 . 66
Exclude (i.e     Any     Single IP     IP Range	Destination Address NOT the choice belo IP:	IP Details w) 192 . 168 . 0 . 66
Exclude (i.e     Any     Single IP     IP Range     IP Mask     Zone	Destination Address NOT the choice belo IP:	IP Details w) 192 . 168 . 0 . 66
Exclude (i.e     Any     Single IP     IP Range     IP Mask     Zone     Host Name	Destination Address	IP Details w) 192 . 168 . 0 . 66

😻 Network Control	l Rule		
General			$\neg$
Action: Al	low 🔽	Log as a firewall event if this rule is fired	
Protocol: IP	, 🔽		
Direction: In	i/Out 🗾		
Description: A	llow All Requests		
Source Address Des	stination Address	IP Details	
🔲 Exclude (i.e. NC	OT the choice below	)	
O Any	IP:	192 . 168 . 0 . 99	
Single IP			
IP Range			
🔘 IP Mask			
🔘 Zone			
Host Name			
MAC Address			
What do these sett	tings do?	Apply Cance	

Sada ćete dodati aplikaciju u listu aplikacija kojima ne verujete. Klikom na **Define a New Blocked Application** otvarate prozor za definisanje te aplikacije:

	-0	Define a New Blow This shortcut repress create an automatic you do not trust.	ser Define	<b>lication</b> <u>a New Block</u> for applica	<mark>ked Applica</mark> ations that	ation	
😻 Define a Nev	w Blocke	d Application			<b>X</b>	5)	
					Select 💌	File Groups Running Pro	•
What do thes	e settings (	do?		Apply	Cancel	Browse	- <b>k</b> a

Ja sam za ovaj primer izabrao da zabranim aktivnost Messenger-a:

Define a New Blocked Application	x
C:\Program Files\Messenger\msmsgs.exe	Select 💌
What do these settings do?	Apply Cancel

Klikom na Network Security Policy otvarate prozor za izmenu polisi:

U zavisnosti od toga koliko ne verujete datoj aplikaciji, postavićete zabranu u toj težini. Možete ostaviti predefinisanu polisu za zabranu koja će zabraniti pokretanje ove aplikacije sa bilo koje adrese i praviće Log datoteke ua svaki pokušaj pokretanja.

Kako bi se zaštitili od napada brutal napada sa mreže koji izazivaju ICMP, TCP, UDP preplavljivanje, postavićete paranoična pravila koja kažu da je za sva tri protokola dozvoljen saobraćaj sa 10 paketa u

sekundi u trajanju od 10 sekundi. Vreme za koje će sumnjivi host (računar) biti blokiran nakon pokušaja skeniranja portova, postavite na 10 minuta a vreme za koje će Firewall biti u stanju pripravnosti dok je računar žrtva DoS (engl.: *Denial of Service*) napada, postavite na 5 minuta. Ovo ćete uraditi tako što ćete kliknuti na *Advanced* dugme koje se nalazi na levoj strani aplikacije a zatim na **Attack Detection Settings**:



Zatim podesite parametre zaštite od gore navedenih napada sa odgovarajućim vrednostima:

Sada ćete definisati novu zonu od poverenja i u nju ćete ubaciti IP adresom

192.168.0.33 kao host-a koji pripada toj zoni. Kreirate i zonu kojoj ne verujete

dodeljujući IP adresu računara koji pripada toj zoni a koja je 192.168.0.13.

Klikom na **My Network Zones** otvarate prozor za definisanje mrežnih zona

kojima verujete:



ttack Detection S	Settings		X
Intrusion Detection	Miscellaneous		
TCP Flood			
Traffic Rate	10	packets / second	
Duration	10	seconds	
UDP Flood			
Traffic Rate	10	packets / second	
Duration	10	seconds	
-ICMP Flood			
Traffic Rate	10	packets / second	
Duration	10	seconds	
How long should a solution blocked after it atte	suspicious host empts a port sc	be automatically 10 minutes	
How long should th while the host is un	e firewall stay i der DOS attack	n emergency mode 300 seconds	
Protect the ARF	Cache		
Block Gratuitous	ARP Frames		
What do these se	ttings do?	OK Cancel	

Zatim dodajete novu zonu klikom na dugme Add – A New Ntework Zone:

Add 💌	A New Network Zone
	A New Address りく
Edit	
Remove	

Sada dajete ime zoni, s obzirom da je to zona od poverenja, dajete joj simbolično ime, npr.: Friend:

😻 Type name of Network Zone		
Friend		
What do these settings do?	Apply Cancel	

Sada dodajete novu IP adresu koja će pripadati ovoj zoni, odnosno IP adresu računara kome verujete. Klik na prazno polje za IP adresu ispod imena zone a zatim **Add – A New Address**:

😻 My Network Zones	
Network Zone	Add 🔹 A New Network Zone
🖃 Loopback Zone	A New Address
L IP In [127.0.0.1 / 255.0.0.0]	Edit
Friend	Remove
L (add addresses here)	

Prozor popunjavate shodno uslovima zadatka:

Exclude (i.e. NOT the select	tion below)	
O Any		
A single IP address	192 . 168 . 0 . 33	
O A range of IP addresses		
🔘 An IP address mask	I	
🔘 A host name		
O A MAC address	: : : : :	

Potvrdite novonastale promene klikom na **Apply** a zatim kreirate i zonu kojoj ne verujete tako što ćete kliknuti na **My Blocked Network Zones**:



Sada dodajete IP adresu kojoj ne verujete:

😻 My Blocked Network Zones			נ
Blocked Network Zone		Add 🛩	Network Zones 🔹 🕨
There are no item:	; to show.	Edit Remove	A New Blocked Address

Otvara vam se prozor za unos IP adrese i shodno uslovima zadatka popunjavate polja ovog prozora:

Klikom na **Apply** potvrdite sve izmene i sada ste kreirali zonu od poverenja I zonu koja sadrži IP adrese računara kojima iz nekog razloga ne želite da verujete tak oda će se shodno polisama Comodo-a primenjivati određena pravila na računare obe zone. Ove polise možete videti nakon klika na

🛿 Add a New Address		
Exclude (i.e. NOT the select	ion below)	
O Any		
A single IP address	192 . 168 . 0 . 13	
A range of IP addresses		
O An IP address mask	· · · · /	
O A host name		
A MAC address	: : : : :	
What do these settings do?		Apply Cancel