## Firewall Laboratory – Module 11 Firewalls

**Background**: This Lab reinforces the concepts of firewalls by requiring the student to complete the configuration of a host-based firewall.

## **Requirements/assumptions**:

- Windows NT 4.0/2000
- Internet access
- Local administrative privileges

<u>Scenario</u>: Some of the current IT staffers from RHS saw postings in an Internet chat room from an alias that the terminated employee used. The postings were bragging about the prospects of the conquest of a newly merged company's infrastructure by Trojans he had put in place prior to leaving the company. It is believed that this former employee made these posts, and that he has in fact placed some malicious software somewhere on the network. It is also believed, based on a complete scrub of the former employee's system, that this staff member may have had knowledge and experience with the following Trojans: SubSeven, WinCrash, and BackOrifice. In addition, there is concern that there should be steps taken to reduce the ability to footprint the entire network through ping sweeps, both to internal and external hosts. Only the management network, which resides in the 192.168.30.240 - 192.168.39.254 range, should be allowed to ping the hosts on the network. All other ping requests should be dropped.

Given the short time frame for integration of the infrastructures, the CIO has made a decision to press ahead as soon as possible with the integration work. However, to preserve security, he has directed that host-based firewalls be installed on systems that would cause the most damage to the organization if they were compromised. Also, given the tight budget for the current fiscal year and the large number of servers that will have to be protected against the potential malicious software, you have decided that a free software tool is the only answer. You have researched the known freeware host-based firewalls and determined that Tiny Personal Firewall is the best solution for your needs.

## Download and Install Tiny Personal Firewall

- 1. Open the InfoSec Course Shared\Tools folder located on your Desktop
- 2. Double Click the Tiny Personal Firewall Setup file: [pf2.exe].
- 3. The Tiny Personal Firewall Setup Wizard starts, click the following buttons

iny Personal Firewall Setup					×
	Welcome to Personal Fire The InstallShie your computer.	the InstallShiel swall Id® Wizard will in To continue, clic	<b>t Wizard for</b> stall Tiny Pers k Next.	Tiny onal Firewall c	'n
		< Back	Next >	Cance	el
Tiny Personal Firewall Setup					×
Choose Destination Location Select folder where Setup will ins	all files.				
Satur will install Timy Porcanal F	irowell in the foll	owing foldor			
Destination Folder				Province	. 1
C\Program Files\Tiny Person	al Firewall			DIOWSE	····
InstallShield		< Back	Next >		ancel
Tiny Personal Firewall Setup					
Please select a program folder.					
Setup will add program icons to t or select one from the existing fol	he Program Fol ders list. Click↑	der listed below. Vext to continue.	You may type	e a new folder	name,
Program Folders: Tiny Personal Firewall					
Existing Folders:					
Accessories Administrative Tools Aladdin Expander 5.0 Jasc Software LANguard File Integrity Checker LANguard Network Scanner LC3 MD5					
Microsoft Office Tools Norton AntiVirus Corporate Editi	on				-
InstallShield		< Back	Next >		Cancel

Tiny Personal Firewall Setup		×
Start Copying Files		
Review settings before copying files.		
Setup has enough information to start copying the settings, click Back. If you are satisfied with the se	program files. If you want to revie ttings, click Next to begin copying	w or change any files.
Current Settings:		
Configuration: Typical		<u></u>
Destination Directory. C:\Program Files\Tiny Personal Firewa	all	
Program Group (Start Menu): Tiny Personal Firewall		<b>*</b>
₹		•
InstallShield		
	< Back Next	Cancel

Tiny Personal Firewall Setup	
	InstallShield Wizard Complete The InstallShield Wizard has successfully installed Tiny Personal Firewall. Before you can use the program, you must restart your computer. • Yes, I want to restart my computer now. • No, I will restart my computer later. Remove any disks from their drives, and then click Finish to complete setup.
	< Back Finig Cancel

- 4. When the computer reboots, Tiny Personal Firewall will be running. As various programs attempt to make connections either into or out from your system, Tiny will prompt you for input. These may include programs such as Norton Antivirus, Internet Explorer or Netscape Navigator, etc. Each new connection will result in a prompt that you must either permit or deny. Ensure that you read each prompt carefully, and click the checkbox
- 5. After you have gone through all of the initial installation steps and gone through the connections which your computer is attempting to make and either permitted or denied them, it is time to customize our rules.
- 6. Double click on the Tiny Personal Firewall icon () in the system tray.
- 7. Click on the 'Advanced' button.

## Firewall Lab – Module 11 Firewalls

8. A window similar to this one will then open:

Fire	ewall C	Configuration			nal				×
	niter Au	ILES   MICROSOft Networking   MIS	scellaneous   Apj	olication's M	D5				_
		Rule Description	Protocol	Local	Remote	Application			
		" 🔁 Loopback	UDP/TCP (B	[Any port]	[127.0.0.1]:[Any port]	Any application			
		₩₩ DNS	UDP (Both)	[Any port]	[Any address]:[53]	Any application			
		Cutgoing ICMP Echo R	ICMP (Out)	[Any]	[Any address]	Any application			
		T Incoming ICMP Echo R	ICMP (In)	[Any] [Any port]	[Any address] [Any address]:[88]	Any application		Æ	
		□⇒ Local Security Authority	TCP (Out)	[Any port]	[Any address].[00]	CIWINNTISYST	EM32\ESASSIE/	KE .	
		■ → Windows Logon Applic	TCP (Out)	[Any port]	[Any address]:[389]	C:\WINNT\SYSTI	EM32\WINLOGO	DN.E	
		€ → Internet Explorer	TCP (Out)	[Any port]	[Any address]:[Any	C:\PROGRAM FIL	ES\INTERNET	EXF	
					N				
					43				
								•	
			[ [	<b></b>	Ask for a	ction when no rule i	s found	_	
Add Insert Edit Delete									
						ок	Cancel	Apply	
					l				

- 9. To add the rules to block the ports, click on the 'Add' button.
- 10. The following window opens up:

ter rule		<u>?</u> ×
Description:	<b>[</b>	
Protocol:	Any 🔻	
Direction:		
- Local endpoint-	- Application	
− Remote endpoi Address type:	nt Any address	
Rule valid		
<ul> <li>Action</li> <li></li></ul>	Log when this rule match	
	OK	

- 11. You will want to configure the firewall to block the following TCP ports: 6711, 6712, 6776, 7000, 16660, 31337, 31338. To accomplish this, perform the following steps:
  - a. First, give the rule a name (i.e. subseven)
  - b. Select from the drop down menu the protocol which this rule will apply to (i.e. TCP for subseven)
  - c. Select the direction from the drop down menu for the rule (Incoming)
  - d. Select the Port Type from the drop down menu (List of ports for subseven)
  - e. In the 'List of Ports' box, fill in those ports associated with Subseven (6711, 6712, 6776, 7000)
  - f. Select the appropriate action for this rule (Deny)
  - g. Since we're concerned about insiders on the network, it is advisable to log when this rule is enforced (for tracking purposes and to possibly find any impropriety. When we are through with the filter rule configuration, it should look like this:

Filter rule	?   ×
Description: SubSeven	
Protocol: TCP	
Direction: Incoming	
Local endpoint	
Port type: List of ports  Any	
List of Ports: 6711 6712 6776 7000	
Remote endpoint Address type: Any address 💽 Port type: Any port 💌	
Rule valid	
Always	
Action C Permit Deny Log when this rule match Display alert box when this rule match	
OK Cancel	

- 12. Now you will want to configure the firewall rules to include blocking the TCP ports for WinCrash (2583, 3024, 4092, 5742) and Back Orifice (31337-31338). Follow the same steps above and deny all incoming traffic on those ports.
- 13. To disable echo replies to all but the management network, start by creating a new Filter Rule (click Add... in the Firewall Configuration window)
- 14. Enter 'Allow Echo Request from Mgt Network' for the description.

- 15. Set Protocol to 'ICMP'
- 16. Set Direction to 'Incoming'
- 17. Ensure 'Echo Request' is in the box next to 'Set ICMP'
- 18. Set the remote endpoint to 'Network/Range'
- 19. Enter the network range (192.168.30.240 to 254)
- 20. Click 'OK'
- 21. Click 'Add...'
- 22. Enter 'Allow Echo Reply to Mgt Network' for the description.
- 23. Set 'ICMP' as the protocol
- 24. Change direction to 'Outgoing'
- 25. Click the 'Set ICMP' box
- 26. Check the box for '[0] Echo Reply'
- 27. Uncheck the box for '[8] Echo Request'
- 28. Click OK
- 29. Change Remote endpoint to 'Network/Range' and enter the range again
- 30. Click OK
- 31. Test your firewall by pinging your partner's IP address. You should not get a response. Then the instructor will ping all systems from a computer in the management network. These packets should traverse the network unobstructed.