Introduction

The **Network Vulnerabilities** module provides you with the instruction and Server hardware to develop your hands on skills in the defined topics. This module includes the following exercises:

- 1) Network Footprinting
- 2) Packet Sniffing
- 3) MitM with ARP Spoofing
- 4) Denial of Service

Lab Diagram

During your session you will have access to the following lab configuration.



Connecting to your lab

In this module you will be working on the following equipment to carry out the steps defined in each exercise.

- SERVER1 (Domain Controller)
- CLIENT1 (XP Workstation)

Each exercise will detail which console you are required to work on to carry out the steps.

To start simply click on the named Server from the device list (located on the left hand side of the screen) and click the **Power on** from the in tools bar. In some cases the devices may power on automatically.

During the boot up process an activity indicator will be displayed in the name tab:

Black - Powered Off

- Orange Working on your request
- Green Ready to access

If the remote console is not displayed automatically in the main window (or popup) click the **Connect** icon located in the tools bar to start your session.

If the remote console does not appear please try the following option:

• Switch between the HTML 5 and Java client versions in the tools bar.

In the event this does not resolve your connectivity problems please visit our Help / Support pages for additional resolution options.

Copyright Notice

This document and its content is copyright of Practice-IT - © Practice-IT 2013. All rights reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following:

1) You may print or download to a local hard disk extracts for your personal and non-commercial use only.

2) You may copy the content to individual third parties for their personal use, but only if you acknowledge the website as the source of the material. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system.

Exercise 1 - Network Footprinting

In this lab, you will practise attack strategies such as footprinting, spoofing, and Denial of Service.

A network scan is usually the first step in an attempt to penetrate security (or indeed to establish what needs defending). Footprinting establishes the topology and protocols deployed on the network while fingerprinting determines the services and other configuration details of a target host.

One of the most popular scanning tools in nmap. This is a command-line program operated using scripts. A GUI version (Zenmap) can perform several very useful pre-configured scans though.

From the Practice-Lab application power on the Server, and Client devices.

Select the "Connect" button when it becomes available to logon to Server.

Once you have logged in double click on the VMware Player icon located on the desktop.



Double click the **BackTrack** icon to start the server.



Click in the Black window and Press **Enter** to select the default graphics mode (or use the **Arrow** key to select 800x600 if you have a low resolution display).



When Backtrack has booted, type the following at the # prompt

startx

Press Enter to load the GUI.



Right-click the flag icon on the taskbar to select the appropriate regional keyboard layout and settings.

Click the Konsole icon to open a command shell.



To connect the BackTrack Server to the same network as the CLIENT machine (using the DHCP server on SERVER), enter the following command:

dhclient



The DEVICE should receive an address in the 192.168.0.0 - 100 range. (Normally 192.168.0.10)

Use the K(onqueror) menu to open **Backtrack > Network Mapping > Portscanning > Zenmap**.



Enter 192.168.0.0/29 into the "Target" box. Click Scan.



The scan will take a few minutes to complete and should finish with an "Nmap done" status message.

Click the **Topology** tab - this shows the hosts found via the scan, in this case restricted to the local subnet. You should be able to see all three DEVICEs.



Click the **Host Details** tab. This shows the scan's attempt to identify the OS. Click the different hosts in the left-hand panel to view them. Note that the bomb icon shown on the SERVER DEVICE indicates lots of open ports.

Note: Zenmap provides a GUI to the port scanning tool nmap



Click the **Ports / Hosts** tab. This shows precisely which ports are open on each host and in some cases the model and version of the server hosting them.

🥝 Server - Windows Internet Explorer	
# https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO-3phost.htm	₽ 22
🙀 BackTrack - YMware Player (Non-commercial use only)	_ 8 ×
Player 👻 🔡 💌 🔚 🧱	« 🗐
Scan Tools Profile Help	
Command: [nmap -14 - A - V 192.168.0.0/29	
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans	
OS 4 Host - Port 4 Protocol 4 State 4 Service 4 Version	
192,168.0.1 🥯 53 tcp open domain Microsoft DNS 6.	
🚽 192.168.0.2 🛛 😑 80 tcp open http Microsoft IIS http	
🚽 192.168.0.3 🥚 88 tcp open kerberos-sec Microsoft Window	
😑 135 tcp open msrpc Microsoft Window	
😑 139 tcp open netbios-ssn	
😑 389 tcp open Idap	
🥮 445 tcp open netbios-ssn	
🥮 464 tcp open kpasswd5	
😑 593 tcp open ncacn_http Microsoft Window	
😑 636 tcp open Idap	
🥚 902 tcp open vmware-auth VMware Authent 🗌 🔒	
😑 912 tcp open vmware-auth VMware Authent	
😑 3268 tcp open Idap	
😑 3269 tcp open Idap	
🥚 3389 tcp open microsoft-rdp Microsoft Termin 🔽	
Filter Hosts	
🍡 🐏 📰 🥹 🜌 🐖 💥 🚽 🐨 root@bt: ~ - 5 🗙 Zenmap 🛛 🔯 🖓 1 2 🚦 😭 >	
Astart 🕹 🖉 🥞 🥙 EN	* 🏱 🔁 😘 📼
	🔍 100% 🔻 🚽

Finally, click the **Services** tab - this sorts the display by service rather than host. For any service you are interested in attacking (or defending) you can see which host(s) are running it.

🦪 Server - Windows Internet Explorer	
Shttps://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO-3phost.htm	A 22
🔁 BackTrack - VMware Player (Non-commercial use only)	_ 8 ×
Player 👻 🔐 😴 🔚 🥫	« 🥁
Scan Tools Profile Help	
larget: 192.108.0.0/29 Profile: intense scan Scan Cancer	
Command: [nmap -T4 -A -v 192.168.0.0/29	
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans	
Service 4 Port 4 Protocol 4 State 4 Service 4 Version	
domain 🥚 53 tcp open domain Microsoft DNS 6.	
http 🛛 😑 80 tcp open http Microsoft IIS http	
kerberos-sec 🥚 88 tcp open kerberos-sec Microsoft Window	
msrpc 🥚 135 tcp open msrpc Microsoft Window	
ncacn_http 🥘 139 tcp open netbios-ssn	
netbios-ssn 😑 389 tcp open Idap	
microsoft-rdp 😑 445 tcp open netbios-ssn	
ldap 😑 464 tcp open kpasswd5	
vmware-auth 🤤 593 tcp open ncacn_http Microsoft Window	
kpasswd5 😑 636 tcp open Idap	
902 tcp open vmware-auth VMware Authent	
🥚 912 tcp open vmware-auth VMware Authent	
😑 3268 tcp open Idap	
😔 3269 tcp open Idap 💽	
3389 tcp open microsoft-rdp Microsoft Termin:	
Filter Hosts	
🏷 👾 🔜 🥹 🜌 🖙 💥 🔄 🔽 root@bt: ~ - 5 🗙 Zenmap 🛛 🕅 🔊 🆓 1 2 🛛 { { ; ; 54 >	
Arstart 🔜 🔁 😭 🗞 EN 🕿	P 19 👍 📰
	€ 100% ▼

Close Zenmap, discarding any changes.

Continue to the next exercise to discover more network vulnerability tools.

Exercise 2 - Packet Sniffing

Another critical information gathering tool is a protocol analyzer. This tool captures unicast packets sent to the host and broadcast packets on the same subnet. The most widely used is Wireshark, which is bundled with Backtrack.

From the console, type wireshark and press Enter.



Click OK to the warning.

Maximize the window.

Click the Capture Options button.



In the "Capture Filter" box, type:

host 192.168.0.10

(A capture filter is used to restrict the type of packets processed by Wireshark)

Click Start.

Server - Windows Internet Explorer	
e https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO	I-3phost.htm
🙀 BackTrack - VMware Player (Non-commercial use only)	
Player 👻 🛄 😴 🧱 🧃	« 🔄
Wiresbark: Canture Ontions	
-Capture	
Interface: ath0	
IP address: 192 168.0 10	
Link-laver header type: Ethernet 💌	
Capture packets in promiscuous mode	abuto(s)
Capture packets in monitor mode	ocol Analyze
Capture packets in pcap-ng format (experimental)	
Limit each packet to 💷 🗘 bytes	
Capture Filter: host 192.168.0.10	
Capture File(s)Display Options	
File: Browse	real time lile
Use <u>m</u> ultiple files	
🔣 Next file every 🚺 🗘 megabyte(s) 👻 Automatic scrolling in live	capture
Next file every	es
Ring buffer with 2 files	e capture files on the wi
Stop capture after 1 the(s)	
Stop Capture	tion
after 1 \$ packet(s)	
I after I \$ megabyte(s) • I	Sidion
🔲 after 🗍 🛟 minute(s) 🗸 🛛 🔀 Enable transport name re	esolution
<u>H</u> elp	Start efault
💐 🥘 📰 🧐 🜌 🚥 💥 💿 🐨 🐨 🖬 root@bt: ~ - 5 📶 The Wiresha	1 2 22.23
Arstart 🛃 🔀 🚞 💐	🛛 EN 🖹 🎗 🍽 🏗 🗤 🛌
	🗮 100% 🔻

Connect to the **CLIENT** device using the Practice-Labs application.



Open a command prompt and ping the IP address of BackTrack (192.168.0.10).



Switch back to Backtrack and stop the capture and note what has been captured.

Server - Windows Internet Explorer				
Attps://labs.practice-labs.com/+CSCO+d07567676	533A2F2F7261747661722E63656	E70677670722D76672E70622E687	'8++/-CSCO-3phost.htm	a 2
🙀 BackTrack - ¥Mware Player (Non-commercial use	e only)			_ 8 ×
Player 👻 🔲 👻 📇 📹 📾				« i=
1	eth0 (host	192.168.0.10) - Wiresha	ark 📃 🛢 🕱	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	apture <u>A</u> nalyze <u>S</u> tatis	stics Telephony <u>T</u> ools <u>F</u>	<u>H</u> elp	
	🔷 🗖 😵 🏟			
Filter:		 Express 	sion Clear Apply	
No. Time So	ource	Destination	Protoco Info	
1 0.000000 Vm	πware_a3:2e:08	Broadcast	ARP Who has 192.168.0.10? Tel	
2 0.000014 Vm	mware_11:43:0e	Vmware_a3:2e:08	ARP 192.168.0.10 is at 00:0c:2	
3 0.000700 19	92.168.0.2	192.168.0.10	ICMP Echo (ping) request (id=C	
4 0.000724 19	92.168.0.10	192.168.0.2	ICMP Echo (ping) reply (id=C	
5 1.000949 19	92.168.0.2	192.168.0.10	ICMP Echo (ping) request (id=C	
6 1.000979 19	92.168.0.10	192.168.0.2	ICMP Echo (ping) reply (id=0	
7 2.002246 19	92.168.0.2	192.168.0.10	ICMP Echo (ping) request (id=0	
8 2.002269 19	92.168.0.10	192.168.0.2	ICMP Echo (ping) reply (id=0	
9 3.003699 19	92.168.0.2	192.168.0.10	ICMP Echo (ping) request (id=0	
10 3.003721 19	92.168.0.10	192.168.0.2	ICMP Echo (ping) reply (id=0	
11 5.010286 Vm	mware_11:43:0e	Vmware_a3:2e:08	ARP Who has 192.168.0.2? Tell	
12 5.010647 Vm	mware_a3:2e:08	Vmware_11:43:0e	ARP 192.168.0.2 is at 00:50:50	
[1]				
▶ Frame 1: 60 bytes or	n wire (480 bits), 6	0 bytes captured (480	bits)	
Ethernet II, Src: Vr	mware_a3:2e:08 (00:5	0:56:a3:2e:08), Dst: A	Broadcast (ff:ff:ff:ff:ff:ff)	
Address Resolution F	Protocol (request)			
	ff 00 50 56 22 20 00	2 02 06 00 01		
	01 00 50 56 a3 2e 08	3 c0 a8 00 02	P V	
0020 00 00 00 00 00 00 0	00 c0 a8 00 0a 00 00	00 00 00 00		
0030 00 00 00 00 00 00 0	00 00 00 00 00 00 00)		
Ph 🚵 📷 🚳 🚥 🚥	✓ □ □	root@ht:~	(host 1 1 2 1 2 1 2	
J S =	···	etio		
NStart II 🔊 😁 🎭			EN	
				🔍 100% 🔻

Continue to the next exercise to learn about Man in the middle attacks.

Exercise 3 - MitM with ARP Spoofing

As an attacker, you may be more interested in finding out what information a different host on the network is receiving and possibly to modify the transmissions between two hosts - a Man in the Middle (MitM) attack. Ettercap is one of the most widely used tools for launching MitM attacks. On a local network, one of the most powerful techniques is ARP spoofing.

Connect to SERVER Practice-Lab device.

🥥 Server - Win	ndows Internet Explorer	A CONTRACTOR OF THE OWNER.				
Attps://labs	s.practice-labs.com/+CSCO+d0	756767633A2F2F7261747661722E63656E706776707	22D76672E70622E6878++	/-CSCO-3phost.htm	r an	A 23
Recycle Bin	Labfiles Computer	 Local Disk (C:) → labfiles → 	• 2	Search labfiles	- • ×	
	Organize 🔻 🛜 Open N	lew folder			. = • 🔟 🕑	
1	🚖 Favorites	Name +	Date modified	Туре	Size	
	📃 Desktop	🔑 ftproot	13/08/2012 11:19	File folder		
wiresnark	Downloads Recent Places	📙 www.root	13/08/2012 11:19	File folder		
	A ROCOR FIGES	DCPROMO Date created: 13/08/20	08/05/2011 22:32 012 11:19	VBScript Script File	2 KB	
	詞 Libraries	FINAL Size: 320 KB	rived, overlay, private,	themes.	2 KB	
	Documents	Kaspo.0.2134_adminki Files: index, info, info_	result, news, pr01, pr02, p	r03,	45,452 KB	
	Pictures	Kav6.0.4.1424 winwksen	09/05/2011 21:36	Application	77,905 KB	
	Videos		09/05/2011 11:47	Windows Installer P	28,288 KB	
	Computer	wireshark-win32-1.4.4	07/03/2011 14:23	Application	18,978 KB	
	Network	ed Date modified: 13/08/2012 11:19				
Start	🌡 🖉 📜 🕺	<u>.</u>				11:47 12/09/2012
						🔍 100% 🔻

Open Explorer and copy the *ftproot* and *wwwroot* folders from *C:\labfiles*.

Open C:\inetpub and paste the folders, choosing to merge with the existing folders.

Browse to C:\inetpub\wwwroot

Right click the Index.htm file and open with Notepad.

*Find and delete this line: meta X50!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H**



Save and close the file.

Connect to the CLIENT device in your Practice-Lab and open a command prompt.

Type **ping 192.168.0.3** to check connectivity with the SERVER.



Open Internet Explorer and load http://webserver

Scient - Windows Internet Explorer	. 0 X
Mttps://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO-3phost.htm	₽ 🗟
Press Releases Welcome to The Book Company Website. As the holiday season approaches we are pleased to announce new discounts on all our major authors. Fancy whipping up a dish with Jamie Oliver or Nigella Lawson, then look no further than our Cookery section for their latest offerings.	
Contact Information Getting in touch with us could not be easier, you can contact us using any of the methods listed below.	
🔊 Start 🔤 C:\WINDOWS\system32 🖗 The Book Company	EN 🔍 🗞

In the command prompt, type

arp -a

This will show you a view the ARP cache. Make a note of SERVER's MAC address:



Switch to Backtrack. From the **K(onqueror)** menu, select **Internet > Ettercap**. Maximize the window.



Select Sniff > Unified Sniffing



Check that the interface "eth0 " is selected and click OK.



Select **Hosts > Scan for hosts**. This should return three results.

Once the scan has completed Select Hosts > Hosts list



This will show you a list of discovered hosts.



Select 192.168.0.3 and click **Add to Target 1** then select 192.168.0.2 (CLIENT's IP address) and click **Add to Target 2**.



Select Mitm > Arp poisoning. Click OK.

Server - Windows Internet Explorer			
https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747	661722E63656E70677670722D76672E70622E6878++/	/-CSCO-3phost.htm	8
🙀 BackTrack - VMware Player (Non-commercial use only)			_ & ×
Player 👻 🛄 👻 🧾 📷			« 🗐
a a	ettercap NG-0.7.3		
<u>S</u> tart <u>T</u> argets <u>H</u> osts <u>V</u> iew <u>M</u> itm	<u>Filters</u> Logging <u>Plugins</u> <u>H</u> elp		
Host List 🖌	poisoning		
	np redirect	n	
IP Address MAC Address Por	t stealing		
192.168.0.2 00:50:56:A3:2E	p mitm attack(s)		
192.168.0.3 00:50:56:A3:2E	· · · · · · · · · · · · · · · · · · ·		
192.168.0.250 00:1E:4A.6B.BC:/1			
Delete Host	Add to Target <u>1</u>	Add to Target <u>2</u>	
1698 tcp OS fingerprint			
2183 known services			
Randomizing 255 hosts for scanning	te		
3 hosts added to the hosts list		100	
Host 192.168.0.3 added to TARGET1			
HOST 192.108.0.2 added to IANGET2		▲ ▼	
Page 🔍 🔜 🙆 🜌 🛶 💥 🛛	👻 🜌 root@bt: ~ - 5 🗙 ettercap	NG DI NG 🔂 1 2 17:77	
Arstart 🛛 🛃 🔀 🥞 🧐		EN	* P 🖲 🍫 📰
			🔍 100% 🔻

Select OK to the displayed message



Select Start > Start sniffing.

Server - Windows Internet Explorer			X
https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747	661722E63656E70677670722D76672E70622E6878++,	/-CSCO-3phost.htm	A 22
🙀 BackTrack - ¥Mware Player (Non-commercial use only)			_ 8 ×
Player 👻 🔛 🛋 🥫			« 🧱
	ettercan NG-0 7 3		2
Start Targets Hosts View Mitm	Filters Logging Plugins Help		4
Start sniffing Ctrl+W			
Stop sniffing Ctrl+E		ſ	
Exit Ctrl+X	scription		
192.168.0.2 00:50:56:A3:4A:57			
192.168.0.3 00:50:56:A3:2E:27			
Poleto Liort	Add to Target 1	Add to Torrect 2	
Host 192.168.0.2 added to TARGET2			-
ARP poisoning victims:			
GPOLIP 1 : 192 168 0 2 00:50:56:42:2E:2	7		
GROUP 2 : 192.168.0.2 00:50:56:A3:4A:5	57		
78 🔌 🗰 🚳 💷 👾 🛀	▼ wroot@bt:~-5 ¥ ettercap	NG 1 2 1. 1 4	
Arstart 🔜 💦 🚞 🍖		EN 🕿 💬 🖗	16:14
			11/01/2013
			af 100 /0 🔺

Switch to the CLIENT workstation and ping 192.168.0.3 again.

Enter **arp** -**a** to view the ARP cache. Make a note of SERVER's MAC address:



Note that you can see BACKTRACK IP address and MAC and that the MACs for BACKTRACK and SERVER are identical. The attack we are launching is quite unsophisticated - it is possible to be a lot sneakier.

As a simple example of doing some content rewriting, we will design a filter to subvert the web server hosted on SERVER.

Switch back to the BACKTRACK SERVER and Stop the Arp poisoning and Sniffing.

Server - Windows Internet Explorer			
https://labs.practice-labs.com/+CSCO+d0756767633A2F2F72617476	61722E63656E70677670722D76672E70622E6878++/	/-CSCO-3phost.htm	8
🙀 BackTrack - VMware Player (Non-commercial use only)			_ 8 ×
Player 🗸 🔛 🚽 🔚 🥫			د 🔍 👟
	ottorcan NG-0-7-3		2
Start Targets Hosts View Mitm	Filters Logging Plugins Help		2
Start sniffing Ctrl+W			
Stop sniffing Ctrl+E			ก
Exit Ctrl+X	scription		
192.168.0.2 00:50:56:A3:2E:08			
192.168.0.3 00:50:56:A3:2E:29			
192.168.0.250 00:1E:4A:6B:BC:71			
Delete Host	Add to Target <u>1</u>	Add to Target <u>2</u>	
ARP poisoning victims:			
GROUP 1 - 192 168 0 3 00:50:56:43:25:2	Q		
GROOP 1 : 132.100.0.5 00.50.50.A5.22.2	9		
GROUP 2 : 192.168.0.2 00:50:56:A3:2E:00 Starting Unified spiffing	8		10
Starting Onlined shining			
			*
ैंद 🞘 🔤 😻 🔤 🗰 💥	▼ In root@bt: ~ - 5 🗙 ettercap	NG 📆 📉 🦓 1 2 🤁 :42	>
AStart 🛃 🕢 🚞 🏘		EN	* 🕑 🐑 🍋 🛌
			€ 100% -

Open a console and enter:

cd /usr/share/ettercap

Then edit the etter.filter file by using the nano editor.

nano etter.filter



Delete the existing code and insert the following syntax:

if (ip.proto == TCP && tcp.src == 80) {

```
replace("Book", "Bookie-Wookie");}
```



Press **Ctrl+O** then Enter to save the file then **Ctrl+X** to exit.

To compile the script (to make it usable in Ettercap), use the following command in the konsole:

etterfilter etter.filter -o etter.ef



Switch back to Ettercap and select **Filters > Load a filter**. Select the **etter.ef** file and click OK.



Start Arp poisoning and then start sniffing.



Switch back to the CLIENT workstation, open Internet Explorer, and load <u>http://webserver</u> again (or press Ctrl+F5 to refresh the page). You should see a vandalized page which has change the heading from The Book Company to The Bookie-Wookie Company.

Client - Windows Internet Explorer	X
https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO-3phost.htm	
The Bookie-Wookie Company Home - Microsoft Internet Explorer	_ 8 ×
Elle Edit View Favorites Iools Help	
🌍 Back 🔹 🕥 - 💌 😰 🏠 🔎 Search 🤺 Favorites 🕢 🍰 - 🦆 🔜 🖄	
Address 🕘 http://webserver/	💽 🛃 Go 🛛 Links 🂙
The Book Company Home Page Home The Books Press Releases The Bookie-Wookie Company	
Welcome to The Bookie-Wookie Company Website. As the holiday season approaches we are pleased to announce new discounts on all our r Fancy whipping up a dish with Jamie Oliver or Nigella Lawson, then look no further than our Cookery section for their latest offerings. Contact Information	major authors.
Getting in touch with us could not be easier, you can contact us using any of the methods listed below.	
Telephone 0207 849 9098 FAX 0207 849 9099 Postal address 111 The Strand, London WC1V 5GG Electronic mail General Information: jane@thebookcompany.co.uk Sales: sales@thebookcompany.co.uk Customer Support: support@thebookcompany.co.uk	Local intranet
Start C:\WINDOWS\system32 @ The Bookie-Wookie C	EN 19 %
	🔍 100% 🔻 💡

Switch over to BACKTRACK and in Ettercap, select **Filters > Stop filtering** then **Mitm > Stop Mitm attack(s)**.



Close Ettercap.

Switch to CLIENT and run **arp** -**a** - the ARP cache should have been restored.

Continue to the next exercise in order to learn more about Denial of service attacks.

Exercise 4 - Denial of Service

The last major class of attack is Denial of Service (DoS). There are any number of ways to prevent a server from responding to clients. We could have used Ettercap to simply discard any packets from client or server for instance.

Flood type attacks really depend on overwhelming the victim system with superior bandwidth, which itself depends on compromising thousands or even millions of "zombie" PCs in a "botnet". This exercise just illustrates how simple it is to craft the sort of malformed packets that can be used to try to flood a server.

On the SERVER, start Wireshark using the icon located on the Desktop.



Open the **Capture Options** dialog. In the "Filter options" box, enter **tcp port 80** then start the capture.

0	Server - Windows Internet Explorer			
e	https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7	261747661722E63656E70677670722D766	72E70622E6878++/-CSCO-3phost.htm	
R	Wireshark: Capture Options Capture Interface: local IP address: fe80::78e8:a8cc:53a1:bfb9, 192.168.0.1 Unklayer header type: Ethernet Capture packets in promiscuous mode Capture Filter: tcp port 80 Capture Filter: tcp port 80 Capture Filter: ture within the every Immute(s) Next file every Immute(s) Ring buffer with Stop capture after Immute(s) Immute(s) <	Connection: \Device\NPF_(253F4A Wireless Settings Remote Settings uffer size: 1 Display Options Ugdate list of packets in real time Ugdate list of packets No Packets Ugdate list of packets No Packets	Help: Expression Clear Apply ar Network Protocol Analyzer Files pen en a previously captured file nt: ample Captures wh assortment of example capture files on the wiki Profile: Default	Website Visit the proje User's C The User's G. Security Work with Wir
2	start 🛛 👪 🛛 ᇘ 💐 🗖			EN EN E E E 11:50
-				€ 100% ▼

From the CLIENT workstation, open Internet Explorer type the following url into the address bar:

http://server1

Navigate around the webpages making a mental note of how quick they are to load (there should be no noticeable delay).

Client - Windows Internet Explorer	
https://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO-3phost.htm	 ₪
🚈 The Book Company Home - Microsoft Internet Explorer	_ 8 ×
Elle Edit View Favorites Iools Help	
🔇 Back 🝷 🕥 - 🖹 😰 🐔 🔎 Search 🥋 Favorites 🚱 🎅 - 🌭 🥃 😹	
Agdress 🕘 http://server1/	💌 🛃 Go 🛛 Links 🌺
The Book Company Home Page	
Home The Books Press Releases The Book Company	
Welcome to The Book Company Website. As the holiday season approaches we are pleased to announce new discounts on all our major author whipping up a dish with Jamie Oliver or Nigella Lawson, then look no further than our Cookery section for their latest offerings.	s. Fancy
Getting in touch with us could not be easier, you can contact us using any of the methods listed below.	the state
Telephone 0207 849 9098 FAX 0207 849 9099 Postal address 111 The Strand, London WC1V 5GG Electronic mail 111 The Strand, London WC1V 5GG	
General Information: <u>jane@thebookcompany.co.uk</u> Sales: <u>sales@thebookcompany.co.uk</u> Customer Support: support@thebookcompany.co.uk	
	Local intranet
The Book Company	IN «

Close the Internet Explorer then open the Internet Options applet in Control Panel.

🥖 Client - Windows Internet Explorer											
Matthe https://labs	ttps://labs.practice-labs.com/+CSCO+d0756767633A2F2F7261747661722E63656E70677670722D76672E70622E6878++/-CSCO-3phost.htm									≅ €	
1											
Recycle Bin											
	🕵 Control P	anel									
	Eile Edit	View Favorite	s <u>I</u> ools <u>H</u>	elp							
	G Back +	🕑 · 💋	Search	Folders	15 B	× 9	<u></u> +				
	Address 🚱	Control Panel		-			1001001			💌 🔁 Go	
	\$	×.	6	-	4	P	- 1	I	1	res l	
	Accessibility Options	Add Hardware	Add or Remov	Administrative Tools	Automatic Updates	Date and Time	Display	Folder Options	Fonts	Game Controllers	
		-	5		h	4			20		
	Internet	Keyboard	Mouse	Network	Phone and	Power Options	Printers and	🐷 Regional and	Scanners and	Scheduled	
	Options			Connections	Modem		Faxes	Language	Cameras	Tasks	
		O,	2	N		<u> </u>	vm	6	200		
	Security Center	Sounds and Audio Devices	Speech	System	Taskbar and Start Menu	User Accounts	VMware Tools	Windows Firewall	Wireless Network Set		
	1										
🐮 Start 🕞 (ontrol Panel										EN 🥺 🗞
		1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 - 1999 -									€ 100% -

Under "Temporary Internet files", click **Delete Files** then click OK to both dialogs.



Switch to the SERVER and review the details in WireShark, note the **SYN > SYN/ACK > ACK** sequence in the first three packets. The remainder of the capture shows the CLIENT workstation retrieving the page using HTTP.

Server - Windows Internet Explorer							
<i> h</i>	ttps://labs.practice-	labs.com/+CSCO+d075676	7633A2F2F7261747661722E6365	6E70677670722D76672E70622E6878++/-CSCO-3phost.	itm	🔒 🗟	
	apturing from Inte	l(R) PRO/1000 MT Networ	k Connection (tcp port 80) - V	Yireshark	< l	_ 8 ×	
Eile	Edit View Go	Capture Analyze Statistic	s Telephony <u>T</u> ools <u>H</u> elp		ng	P -	
-	11 AL AL A						
			= ~ ~ ~ ~ ~ ~ ~				
Filter	r:		•	Expression Clear Apply] - 🖃 🖶 - Pa	ge 🔹 Safety 👻 Tools 👻 🔞 👻	
No.	Time	Source	Destination	Protocol Info		2	
	1 0.000000	192.168.0.1	192.168.255.10	TCP 52463 > http [SYN] Seq=0 win			
	2 0.002396	192.168.255.10	192.168.0.1	TCP http > 52463 [SYN, ACK] seq=			
	3 0.002652	192.168.0.1	192.168.255.10	TCP 52463 > http [ACK] Seq=1 Ack			
	4 0.004061	192.168.0.1	192.168.255.10	HTTP GET / HTTP/1.1			
	5 0.012636	192.168.255.10	192.168.0.1	HTTP HTTP/1.1 200 OK (text/html)			
	6 0.221161	192.168.0.1	192.168.255.10	TCP 52463 > http [ACK] Seq=279 A			
	/ 0.61/526	192.168.0.1	192.168.255.10	HITP GET /CSS/Main.CSS HITP/1.1			
	0.020200	102.108.0.1	192.108.233.10	TCP 52464 > http [SYN] Seq=0 with			
	10.0 622037	102 169 255 10	102.168.0.1	HTTP HTTP/1 1 200 OK (taxt/ccc)			
	11 0 622531	192.108.255.10	192.108.0.1	TCP http > 52464 [SVN ACK] Sed=			
	12 0.622533	192.168.0.1	192.168.255.10	TCP 52463 > http [ACK] Seg=684 A			
	13 0.622662	192.168.0.1	192.168.255.10	TCP 52464 > http [ACK] Seg=1 Ack			
	14 0.624146	192.168.0.1	192.168.255.10	HTTP GET /images/practice-labs-bl			
	15 0.629569	192.168.255.10	192.168.0.1	TCP [TCP segment of a reassemble	-1		
4			*** *** * *				
		tas an udas (FDO b	deal of history and	and (520 hine)			
	thernet IT S	res un whee (J28 c	7 (00.50.56.32.2e.07) Det: Cisco 6b.bc.71 (00.1e.4a.6b.b			
	nternet Proto	col src: 192.168	0 1 (192 168 0 1)	$s_{t} \cdot 192 168 255 10 (192 168 255 10)$	•		
E T	ransmission C	ontrol Protocol. S	rc Port: 52463 (5246)	3). Dst Port: http (80). Seq: 0. Len:	0		
4							
0000	0 00 1e 4a 6	b bc 71 00 50 56	a3 2e 07 08 00 45 00	Jk.g.P VE.	ৰ		
0010	0 00 34 45 5:	1 40 00 80 06 35 3	16 c0 a8 00 01 c0 a8	.4EQ@ 5			
0020	0 TT 0a cc e 0 20 00 17 9	T 00 50 55 5T 94	89 00 00 00 00 80 02 54 01 03 03 07 01 01	PU			
004	0 04 02	1 00 00 02 04 03	54 OI 03 03 02 OI 01				
					4		
	ntel(R) PRO/1000 MT	Network Connection: <td>Packets: 45 Displayed: 45 Marked</td> <td>Profile: Default</td> <td>h.</td> <td></td>	Packets: 45 Displayed: 45 Marked	Profile: Default	h.		
						-	
Done				Local intranet	Protected Mode: Off		
1	art 🔍	👦 😁 🎭 🛛					
						€ 100% ▼	

On the BACKTRACK, click in the console window then run the following command (remember that it is case sensitive and ignore the line break - type the whole command then press **Enter**):

hping 192.168.0.1 -p 80 -i u1000 -S -q --rand-source



hping crafts "SYN" packets from random spoofed IP addresses and sends them out at very short intervals.

Note the flood of packets captured by Wireshark on SERVER.

Server - Windows Internet Explorer				
https://labs.practice-labs.com/+CSCO+d075676	7633A2F2F7261747661722E630	8656E70677670722D76672E70622E	6878++/-CSCO-3phost.htm	
Capturing from Intel(R) PRO/1000 MT Networ	k Connection (tcp port 80) -	- Wireshark		_ 8 ×
Eile Edit View Go Capture Analyze Statistic	s Telephony <u>T</u> ools <u>H</u> elp			« j=
	 _ _ _ _ _ _			
Filter:		 Expression Clear Apply 		
No. Time Source	Destination	Protocol Info	^	
4077 1341.70066 196.6.236.129	192.168.0.2	TCP 6266 > http TCP ald > http	[SYN] Seq=0 Win=	
4079 1341, 70566 135, 55, 245, 202	192.168.0.2	TCP grd > http	[SYN] Seq=0 Win=	
4080 1341,70816 98,203,65,170	192.168.0.2	TCP grid-alt >	http [SYN] Seg=0	-4.
4081 1341.70861 112.134.152.148	192.168.0.2	TCP 6270 > http	[SYN] Seq=0 Win=	
4082 1341.71066 23.28.214.20	192.168.0.2	TCP 6271 > http	[SYN] Seq=0 Win=	State of the second sec
4083 1341.71118 8.133.178.71	192.168.0.2	TCP 6272 > http	[SYN] Seq=0 Win=	
4084 1341,71316 20.49.107.34	192.168.0.2	TCP 6273 > http	[SYN] Seq=0 Win=	
4085 1341.71566 226.223.74.226	192.168.0.2	TCP 6274 > http	[SYN] Seq=0 Win=	
4086 1341.71817.73.81.195.95	192.168.0.2	TCP 6275 > http	[SYN] Seq=0 Win=	
4087 1341.72066 210.160.222.17	192.168.0.2	TCP 6276 > http	[SYN] Seq=0 Win=	
4088 1341.72317 151.14.134.19	192.168.0.2	TCP 6277 > http	[SYN] Seq=0 whn=	
4089 1341.72304 44.29.29.102	102.108.0.2	TCP 6278 > http	[SYN] Seq=0 win=	
4090 1341,72010 102.10.107.171	192.108.0.2	TCP 6280 S http	[SYN] Seq=0 win=	
1	20012001010		Esting seed a mini-	
Ename 1: 66 but as on wine (528 b	its) 66 but os cant	upod (528 bits)		
Ethernet II Src: Whware a3.2e.0	7 (00.50.56.a3.2e.0)7) Dst. Cisco 6h.hc.	71 (00·1e·4a·6h·hc·	
F Internet Protocol. Src: 192.168.	0.1 (192.168.0.1).	Dst: 192.168.255.10 (192.168.255.10)	
Transmission Control Protocol, S S	rc Port: 52463 (524	(63), Dst Port: http (80), Seq: 0, Len: 0	
<u>1</u>				
0000 00 1e 4a 6b bc 71 00 50 56 .	a3 2e 07 08 00 45 00	0Jk.q.P VE.		
0010 00 34 45 51 40 00 80 06 35 3	16 c0 a8 00 01 c0 a8	8 .4EQ@ 5		
	59 00 00 00 00 00 80 02 h4 01 03 03 02 01 01	2PU		
0040 04 02				
Intel/P) PRO/1000 MT Network Connection: </td <td>Packets: 4091 Dicplayed: 4091</td> <td>Marked: 0 Profile: Defau</td> <td></td> <td></td>	Packets: 4091 Dicplayed: 4091	Marked: 0 Profile: Defau		
S Incolor records a connection with a	raciola, iosi pispiayoa, iosi i	The state of the s	14	
195				
Ph 🔊 📰 📦 💷 👘	- W []	V attercan NG	t@bt: ~	
→ ≫ = ⊍ = -		A ettercap No. a 100	18 DI 19	
🍂 🔊 🏹 🖓				EN 客 🕑 🛍 🔥 📰
				€ 100% -

On the CLIENT workstation, open IE and browse to the same webpage you did previously (http ://server1) you will notice it takes longer to load.

Clearly you would need a lot more bandwidth to overwhelm the server completely.

Switch to the BACKTRACK Server and halt **hping** using the **Ctrl+C** key combo.



After completing these exercises you should have a better understanding of network vulnerabilities. Go through the exercises again changing some additional parameters to view different results.

Summary

In this lab you completed the following practical tasks:

- Network Footprinting
- Packet Sniffing
- MitM with ARP Spoofing
- Denial of Service

Also Try

Using your lab infrastructure you can attempt the following topics at your own pace.