

# Cyber Security Essentials

## Lab 6 – Packet builder, IP Spoofing and DOS/DDOS attacks

### Task 1: Analyse pcap/pcapng file

Import pcap/pcapng file provided as part of lab 5 using Colasoft packet builder tool and show how to spoof IP address.

The screenshot shows the Colasoft Packet Builder interface. On the left, the 'Packet Details' pane shows a selected packet with the following fields:

- More fragment: ☐
- Fragment Offset: 0
- Time to Live: 6
- Protocol: TCP
- Checksum: 0x6b6c (correct)
- Source Address: 52.216.131.91
- Destination Address: 192.168.31.78
- TCP - Transmission Control Protocol: 443
- Source port: 232

On the right, the 'Packet List' pane shows a list of packets. The selected packet is highlighted in blue:

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Flags	Window	Checksum	Sequence
14314	0.00000075...	192.168.31.78	192.168.31.81	UDP	214	Source Port=8000...	12118				
14315	0.00000076...	192.168.31.81	192.168.31.78	UDP	214	Source Port=12118...	8000				
14316	0.00000036...	52.216.131.91	192.168.31.78	TCP	1486	JACKSeqNumber=...	1486				
14317	0.00000011...	52.216.131.91	192.168.31.78	TCP	1486	JACKSeqNumber=...	1486				
14318	0.00000000...	52.216.131.91	192.168.31.78	TCP	1486	JACKSeqNumber=...	1486				
14319	0.00000000...	192.168.31.78	52.216.131.91	TCP	54	JACKSeqNumber=...	1486				
14320	0.00000038...	52.216.131.91	192.168.31.78	TCP	1486	JACKSeqNumber=...	1486				

### Task 2: DOS attack

Show how can you launch DOS attack using multiple packets at a time. Also create a TCP packet, spoof source IP and show how to launch DOS attack using only 1 packet. (Hint: you need to send 1 packet multiple times continuously).

### DOS Attack

The screenshot shows the 'Send Selected Packets' dialog box. The 'Options' section is expanded, showing the following settings:

- Adapter: VMware Virtual Ethernet Adapter
- Burst Mode (no delay between packets): ☐
- Loop Sending: ☒ (500 loops)
- Delay Between Loops: 100 milliseconds

The 'Sending Information' section shows:

- Total Packets: 1 \* 500 = 500
- Packets Sent: 0
- Progress:

At the bottom, there are buttons for 'Start', 'Stop', 'Close', and 'Help'.

Send Selected Packets

Options

Adapter: VMware Virtual Ethernet Adapter

Select...

☐ Burst Mode (no delay between packets)

☒ Loop Sending:
 

500

loops (zero for infinite)

Delay Between Loops: 100

milliseconds

Sending Information

Total Packets: 1 \* 500 = 500

Packets Sent: 500

Progress:

Start

Stop

Close

Help

## DDOS Attack

14308	0.0000010...	52.216.131.91:443	192.168.31.78:21407	TCP	1,486	[ACK]SeqNumber=...
14309	0.0000000...	52.216.131.90:443	192.168.31.78:21407	TCP	1,486	[ACK, PSH]SeqNu...
14310	0.0000000...	52.216.131.89:443	192.168.31.78:21407	TCP	1,486	[ACK]SeqNumber=...

Send Selected Packets

Options

Adapter: VMware Virtual Ethernet Adapter

Select...

☒ Burst Mode (no delay between packets)

☐ Loop Sending:
 

500

loops (zero for infinite)

Delay Between Loops: 10

milliseconds

Sending Information

Total Packets: 3

Packets Sent: 3

Progress:

Start

Stop

Close

Help

### Task 3: Adding message to packet

Add message “Hi, My name is <Your Name>” to the packet you have created.

