

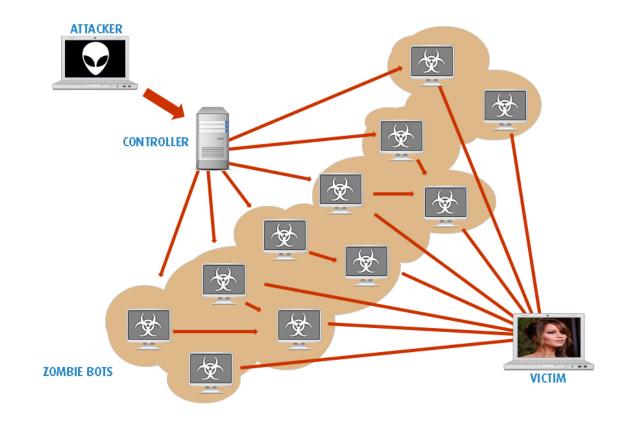
DDoS Testing with ValkyrieManager

Step by Step Guide



Distributed **D**enial **o**f **S**ervice (DDoS)

Multiple compromised systems – usually infected with a Trojan – are used to target a single system causing a Denial of Service (DoS) attack.



DDoS – THE RISKS

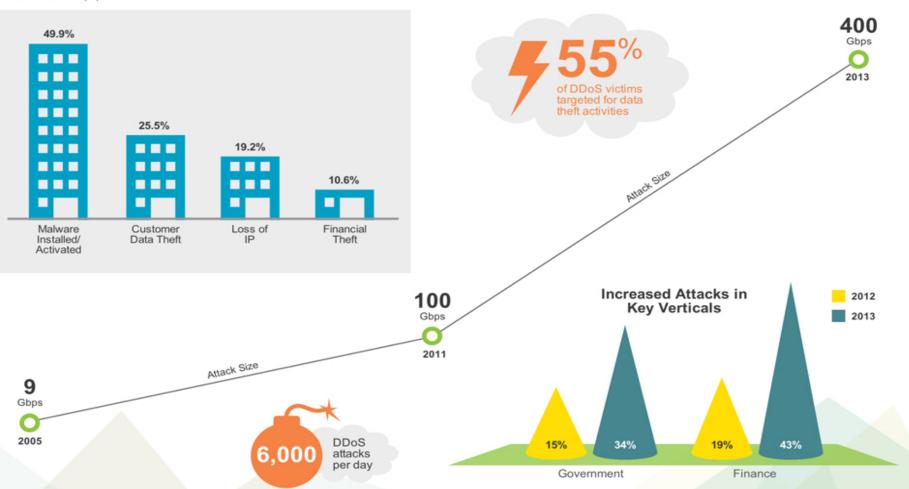
DDoS Threat Landscape

FROST & SULLIVAN 🗚



Rise in Use of DDoS as Diversionary Tactic

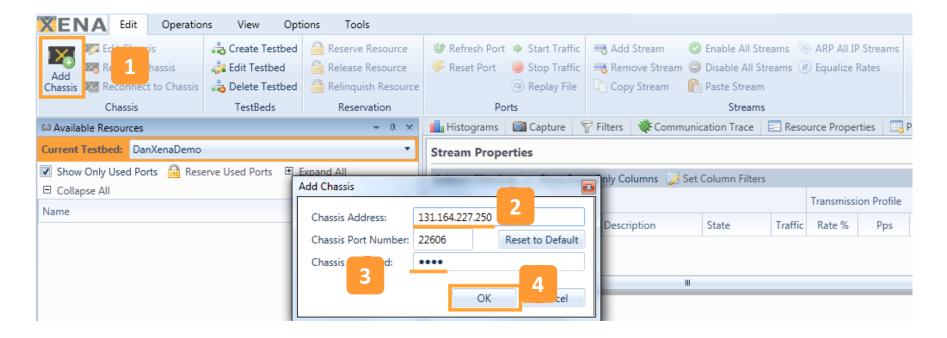
Business Affected (%)





Click "Add Chassis"

- Insert Xena Management Port IP address
- Insert password (Default = "xena")
- 4 Click "OK"





- 1 Choose port to be used for the attack.
- 2 Click "Reserve Used Ports" to reserve the selected "Used" port.
- 3 Eliminate the view of other ports by checking "Show Only Used Ports"

🛍 Available Resources			- ú
Current Testbed:			
Testbed Name	Select	Port #	Logging?
	۲	15	No
Show Only Used Ports 🗟 Reserve Used Ports	🏸 Re	set Use	d Ports 📮
Cherrie Cherrie IP Address Expand		Collap	se All
Na 2 Us	ed	Owr	ner
Chassis 5 'L23 Live Demo' (192.168.1.	1		
▲ Module 6 'Odin-1G-3S-6P'			
🛍 Port 0 'SFP-E 10/100/1000M'	•		



The following DDoS attacks will be covered in this guide:

- SYN Flood
- UDP Flood
- Teardrop Attack
- Smurf Attack
- Ping of Death
- Ping Flood
- ARP Spoofing
- TCP Attack



SYN Flood

A classic DDoS attack that sends rapid amounts of packets to a machine in an attempt to keep connections from being closed.

10040

The sending machine does not close the connection, and eventually that connection times out.

If the attack is strong enough it will consume all resources on the server and send the website offline.

- 1 Right-click on Attacking port.
- 2 Click "Add Stream"

📫 Available Resources						- û
Current Testbed:						
Testbed Name				Select	Port #	Logging?
				۲	15	No
Show Only Used Ports	🔒 Reserv	e Used P	orts	🔑 Re	set Use	d Ports 💂
Chassis Sort Order: IP A	ddress 🔹	🗄 Exp	and	AII 🗆	Collap	se All
Name			Us	ed	Owr	her
🔺 🐹 Chassis 5 'L23 Liv	e Demo' (19	92.168.1.				
▲ 📑 Module 6 'Odir						
1 Port 0 'SFP-E	E 10/100/10	M000	1	•	user	r1
			Ad	d Strear	m	2
			Ad	d Multi	ple Stre	ams
			Str	eam He	aders fr	om PCAP
		G	Rel	ease Po	ort	
			Un	-use Po	rt	
			Loa	ad Port	Configu	iration
			Sav	/e Port (Configu	ration
		G	Ref	fresh Po	ort	
		4	Res	set Port		

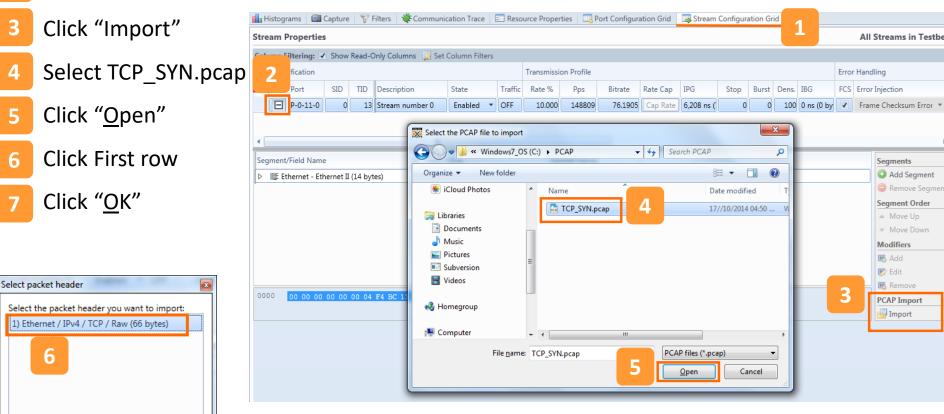


- Go to "Stream Configuration Grid" tab.
- 2 Click "+".

7

<u>0</u>K

Cancel





Configure D.MAC by either

- 1. Manually writing the Address
- 2. Click the ARP button to ARP the GW configured for the port.

⊿ ∥≣ Ethernet - Ethernet II (14 bytes)

🔤 DMAC Address (48 bit)	04 F4 BC 11 49 21	XB live demo/11/1	•
MAC Address (48 bit)	04 F4 BC 11 49 20	XB live demo/11/0	•

Stream Properties

1

All Streams in Testber

Colu	umn F	iltering: 🔽	Show	Read-C	nly C	olumns 🛛 📝 Set Column Filte	ers									
	Iden	tification			Pack	et Content	Protocol Segment	Connectivity	Check							
	Port SID TID Payload Pattern					Payload Pattern	Summary	DMAC	SMAC	VLAN	IPv4 SrcAddr	IPv4 DstAddr	IPv6 SrcAddr	IPv6 DstAddr	Resolve	Check
	Ξ	□ P-0-11-0 0 • 00 00 00 00 00 00 00 00 00 00 00 0			Ethernet/IPv4/TCI	04 F4 BC 11 49 21	04 F4 BC 11 49 20		10.0.0.11	157.166.226.2			Send ARP	Send PING		



- 12B Raw header = TCP options and may be removed to generate smaller SYN Packets. (Note that some devices might see that as an illegal TCP Packet)
- 2 TID(20B) may be removed for the same reason and since Packet Loss/Latency/Jitter... are not important in this test case scenario.

Segment/Field Name	M Field Value	Nam	■ Options: (12 bytes), Maximum segment size,	No-Operat	ion (NOP), Wind	dow scale, No-Operatio	n (NOP), No-Operat
▷ IIE Ethernet - Ethernet II (14 bytes)			Maximum segment size: 1460 bytes Kind: Maximum Segment Size (2)				
			Length: 4				
IF IPv4 - Internet Protocol v4 (20 bytes)			MSS Value: 1460				
▷ II를 TCP - Transmission Control Protocol (2)			No-Operation (NOP)				
◢ 📲 Raw - Data Segment (12 bytes)			□ Type: 1 0 = Copy on fragmentation: No				
HEX Data Value (96 bit)	02 04 05 B4 01 03 03 02 01 01 04 02		.00 = Class: Control (0)	, ,			
			0 0001 = Number: No-Operation (NOP) (1)			
			Window scale: 2 (multiply by 4)				
			Kind: Window Scale (3) Length: 3				
			shift count: 2				
			[Multiplier: 4]				
			NO-Operation (NOP)				
			🖻 Туре: 1				
			0 = Copy on fragmentation: No)			
			.00 = Class: Control (0) 0 0001 = Number: No-Operation (NOP	0. (1)			
			\square No-Operation (NOP)				
			□ Type: 1				
			0 = Copy on fragmentation: No)			
			.00 = Class: Control (0)				
			0 0001 = Number: No-Operation (NOP	?) (1)			
			TCP SACK Permitted Option: True Kind: SACK Permitted (4)				
			Length: 2				
		200		0.45.00	hu e e	-	
		00	00 00 1d d4 62 57 e1 74 e5 0b cc fc 50 08 0 10 00 34 49 0d 40 00 80 06 27 ec 0a 00 00 0	04500 b9da6	bW.tP. .4I.@ '	E.	
		002	20 e2 19 c8 b8 00 50 0d f4 75 d4 00 00 00 0	0 80 02	P u		
			30 20 00 78 7a 00 00 <mark>02 04 05 b4 01 03 03 0</mark> 40 04 02	02 01 01	. XZ		
		201					



1 Select Rate – Pps recommended.

Rate can be configured as Bursty as well.

Select Burst size and density - the Transmission Rate will become the Average rate)

2 Select Packet Size Type.

Packet size range 60 B -16,383 B.

3 Select the Payload Type. Random recommended.

Iden	tification						Transmissio	n Profile							Packet Content				
	Port	SID	TID	Description	State	Traffic	Rate %	Pps	Bitrate	Rate Cap	IPG	Stop	Burst	Dens.	IBG	Size Type	Min	Max	PL Type
÷	P-0-11-0	0		TCP Syn DDoS	Enabled 🔹	OFF	6.400	100000	48.0000	Cap Rate	9,520 ns (:	0	0	100	0 ns (0 by	Fixed Size 🔹	60	1518	Random 🔻



- 1 Right click on "Src IP Addr"
- 2 Click "Add Modifier"
- 3 Select #of Src Ip`s
- <u>4</u> Select Address Action (Random Recommended)
- 5 Click "<u>O</u>K".

				CHECK II II	the second s	CHOILING .
🗹 Show Only Used Ports 🔒 Reserve Used Ports 🖐 Reset Used Ports 🍃	Inte	r Packet Gap: 0 bytes				
Chassis Sort Order: IP Address ▼	Inte	r Burst Gap: 0 bytes				
Name Used Owner	Inte	r Burst Gap: 0 ns (0 bytes)				
▲ 📉 Chassis 5 'L23 Live Demo' (192.168.1.	Burs	st Signature:				
▲ Module 6 'Odin-1G-3S-6P'		Packet Header Definitions (Total Heade	r Siz	e: 34 bytes)		
▲ Port 0 'SFP-E 10/100/1000M'						
	Seg	ment/Field Name	М	Field Value	Named Values	
Add New Modifier	X	l Ethernet - Ethernet II (14 bytes)				
IP Modifier Settings		I≣ IPv4 - Internet Protocol v4 (20 bytes)				
4		DEC Version (4 bit)		4		
Resulting Pattern: xxxxxxx.0.11		📧 Header Length (4 bit)		5		
Min Value: 0.0 Action: Random	•	IN DSCP (6 bit)		000000	Best effort	•
Step Value: 1 Address Offset: 26		ECN (2 bit)		00]	
Count: 50000 Address Mask: 255.255		DEC Total Length (16 bit)		46		
Repeat Count: 1 Type: Standard (16 bit)) -	HEX Identification (16 bit)		00 00		
3 <u>OK</u> <u>Canc</u>	- al	IN Flags (3 bit)		000		
	lei	Dec Fragment Offset (13 bit)		0		
		DEC TTL (8 bit)		127		
4		DEC Protocol (8 bit)		255	<special></special>	•
		HEX Header Checksum (16 bit)		B1 06		
	1	IP⊒ Src IP Addr (32 bit)		10.0.0.11		2
		IP4 Dest IP Addr (32 bit)		157.166.226.25	R Add Modif	ier
	000 001 002	0 00 2E 00 00 00 00 7F FF B1 06 07				



1 To achieve 65K*4096 (~268.3M) addresses, add additional Modifier configured as follows:

P Modifier Setti			
esulting Pattern:	XXX.XXX.U.11		
Start Value:	0	Action:	Increment •
Step Value:	1	Address Offset:	26
Count:	65535	Address Mask:	255.255
Repeat Count:	1		

Resulting Pattern:	10.0.xxx.xxx		
Start Value:	0	Action:	Increment •
Step Value:	1	Address Offset:	28
Count:	65535	Address Mask:	255.255
Repeat Count:	4096		



UDP Flood

A DoS attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.

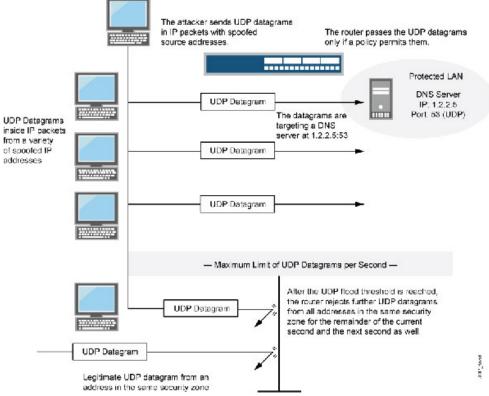
A UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host.

The victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients.



UDP Flood (Attached IPv6 DNS Query)

A User Datagram Protocol Flood works by flooding ports on a target machine with packets that make the machine listen for applications on those ports and send back an ICMP packet.





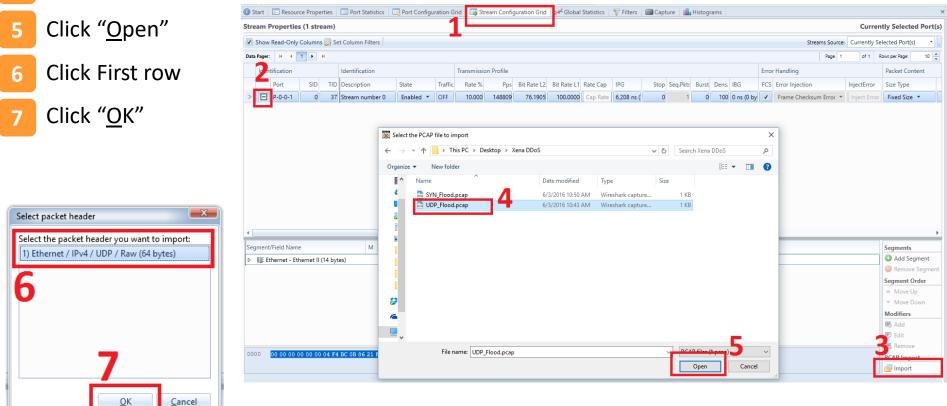
1 Right-click on Attacking port.

2 Click "Add Stream"

🛍 Available Resour	ces					-	ņ
Current Testbed:							
Testbed Name				Select	Port #	Loggin	ng?
				۲	15	No	
Show Only Used	Ports 🔒 Reserv	e Used F	orts	🔑 Re	set Use	d Ports	Ę
Chassis Sort Order:	IP Address 🔹	🗄 Exp	and	AII 🗆	Collap	se All	
Name			Us	ed	Owr	ner	
🔺 📉 Chassis 5 'L	23 Live Demo' (19	92.168.1.					
	'Odin-1G-3S-6P'	_					_
Port 0	SFP-E 10/100/10	M000	1			r1	
			Ad	d Strear	m	2	
			Ad	d Multi	ple Stre	ams	
			Str	eam He	aders fr	om PCA	٩P
		G	Rel	ease Po	ort		
			Un	-use Po	rt		
			Loa	ad Port	Configu	iration	
			Sa	/e Port (Configu	ration	
		G	Ref	fresh Po	ort		
		4	Res	set Port			



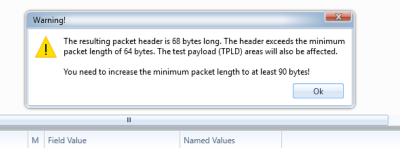
- Go to "Stream Configuration Grid" tab.
- 2 Click "+".
- 3 Click "Import"
- 4 Select UDP_Flood.Pcap





1

You may see the alert telling you to increase the minimum packet length. Change the minimum size to 90 bytes.



am P	roperties	s (1 stre	2am)															Cur	ently Selecte	ed Port(s)
how	Read-Only /	Column	s 📝 Se	t Colum	n Filters												Streams Source:	Currentl	y Selected Port(s	s) • -
/ager:	- H	1.	H.														Page 1	of 1	Rows per Page:	10 🔹
Ident	tification			Transmi	ssion Pr	ofile			Errc	or Handling		Packet Content	1							
	Port	SID	TID		Stop	Seq.Pkts	Burst	Dens. IBG	FCS	Error Injection	InjectError	Size Type			Max	PL Type	Payload Pattern			Ext. Payloa
E	P-0-0-0	0	37	18 ns (0	1	0	100 0 ns (/	by 🗸	Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻		90	1518	Incrementing 💌	00 00 00 00 00 00 00 00 00 00 00 0	0 00 00 0	0 00 00 00 00	
Sh Pa	how F ager: Identi	ager: H 4 1 Identification	how Read-Only Columns ager: H I F Identification Port SID	ager: H I H Identification Port SID TID	how Read-Only Columns Set Column ager: H 1 H Identification Transmiss Port SID TID	how Read-Only Columns Set Column Filters ager: H 4 1 H Identification Transmission Pro- Port SID TID Stop S	how Read-Only Columns Set Column Filters ager: H I H Identification Port SID TID Stop Seq.Pkts	how Read-Only Columns Set Column Filters ager: H I I I I I I I I I I I I I I I I I I	how Read-Only Columns 💭 Set Column Filters ager: H 4 1 H Identification Port SID TID Stop Seq.Pkts Burst Dens. IBG	how Read-Only Columns 💭 Set Column Filters ager: H I H Identification Transmission Profile Error Port SID TID Stop Seq.Pkts Burst Dens. IBG FCS	how Read-Only Columns Set Column Filters ager: H I I H Identification Transmission Profile Error Handling Port SID TID Stop Seq.Pkts Burst Dens. IBG FCS Error Injection	how Read-Only Columns Set Column Filters	how Read-Only Columns Set Column Filters ager: H I I H Identification Transmission Profile Error Handling Packet Content Port SID TID Stop Seq.Pkts Burst Dens. IBG FCS Error Injection InjectError Size Type	how Read-Only Columns Set Column Filters	how Read-Only Columns S Set Column Filters	how Read-Only Columns Set Column Filters	how Read-Only Columns Set Column Filters	how Read-Only Column Filters Streams Source:	how Read-Only Columns is set Column Filters Source: Currently age: H I I H Identification Transmission Profile Error Handling Packet Content Port SID TID Stop Seq.Pkts Burst Dens IBG FCS Error Injection InjectError Size Type Min Max ¹ / ₂ L Type Payload Pattern	how Read-Only Column Rivers Source: Currently Selected Ports age: H 1 H Page 1 of 1 Rows per Page: Identification Transmission Profile Error Handling Packet Content 1 H

1



Configure D.MAC by either

- 1. Manually writing the Address
- 2. Click the ARP button to ARP the GW configured for the port.

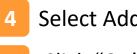
Identification Packet Co Protocol Segments Connectivity Check Port SID TID Payloa 35 Summary DMAC SMAC V AN DSCP IPV6 Stackaddr IPV6 Gateway Address IPV6 Gateway Address Resolve Check Check Resolve Check Resolve Check Check Resolve Resolve Resolve Check Resolve Resolve Resolve Resolve Resolve Resolve Resolve Resolve Resolve																				
> □ P-0-0-0 0 37 Ethernet/IPv4/UD 00 02 02 02 02 13 00 01 01 01 12 0 192.168.1.18 192.168.7.138 0.0.0.0 :: Send ARP Send PIN * * * * * * * * * * Send ARP Send Add Send Address (Address (Address (Address (Address		Iden	tification			Packet C	ò I	Protocol Segment	s								Connectivity Check			
Segment/Field Name M Field Value Named Values Image: Ethernet - Ethernet II (14 bytes) Image: Ethernet - Ethernet II (10 011 0 01 12 Image: Ethernet Protocol v4 (20 bytes) Image: II (14 - Internet Protocol v4 (20 bytes) Image: II (14 - Internet Protocol v4 (20 bytes) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (20 bytes)) Image: II (14 - Internet Protocol v4 (2			Port	SID	TID	. Payload	S :	Summary	DMAC	SMAC	V AN	DSCP	IPv4 SrcAddr	IPv4 DstAddr	IPv6 SrcAddr	IPv6 DstAddr	IPv4 Gateway Address	IPv6 Gateway Addres	Resolve	Che(k
▲ IF Ethernet - Ethernet II (14 bytes)	>	Ξ	P-0-0-0	0	37		I	Ethernet/IPv4/UD	00 02 02 02 02 13	00 01 01 01 01 12		0	192.168.1.18	192.168.7.138			0.0.0.0	::	Send ARP	Send PIN
▲ IIE Ethernet - Ethernet II (14 bytes) IIE Ethernet - Ethernet II (14 bytes) IIE Ethernet - Ethernet II (14 bytes) Image DMAC Address (48 bit) 00 02 02 02 02 13 <unknown> Image DMAC Address (48 bit) 00 01 01 01 01 12 <unknown> Image Ethernype (10 bit) 00 00 00 01 01 01 01 12 <unknown> Image Ethernype (10 bit) 00 00 00 IP Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) <</unknown></unknown></unknown>																				
▲ IIE Ethernet - Ethernet II (14 bytes) IIE Ethernet - Ethernet II (14 bytes) IIE Ethernet - Ethernet II (14 bytes) Image DMAC Address (48 bit) 00 02 02 02 02 13 <unknown> Image DMAC Address (48 bit) 00 01 01 01 01 12 <unknown> Image Ethernype (10 bit) 00 00 00 01 01 01 01 12 <unknown> Image Ethernype (10 bit) 00 00 00 IP Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) Image I IPv4 - Internet Protocol v4 (20 bytes) <</unknown></unknown></unknown>	•																Ш			•
Image: Contract Content of Control (COS) (COS) Image: Contract Content of Control (COS) (COS) Image: Contract Contract Contrel Contract Contract Contract Contract Contract Contract Contract	Seg	iment,	/Field Name				N	I Field Value		Named Values									Segments	
Image: Divide Address (48 bit) 00 00 02 02 02 02 02 10 Curknown> Image: Divide Address (48 bit) Image: Divide Address (48 bit) 00 01 01 01 01 12 <unknown> Image: Divide Address (48 bit) Image: Divide Address (48 bit) 00 01 01 01 01 12 <unknown> Image: Divide Address (48 bit) Image: Divide Address (48 bit) 00 01 01 01 01 12 <unknown> Image: Divide Address (48 bit) Image: Divide Address (48 bit) 00 01 01 01 01 12 <unknown> Image: Divide Address (48 bit) Image: Divide Address (48 bit) 00 01 01 01 01 12 <unknown> Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) Image: Divide Address (48 bit) <td< td=""><td>4</td><td>I≣ Et</td><td>hernet - Ethe</td><td>rnet II (</td><td>14 byt</td><td>es)</td><td></td><td>-</td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>🗿 Add Se</td><td>gment</td></td<></unknown></unknown></unknown></unknown></unknown>	4	I≣ Et	hernet - Ethe	rnet II (14 byt	es)		-		1									🗿 Add Se	gment
Image: Ether type (10 bit) 00 01 01 01 01 12 <unknown> Image: Ether type (10 bit) 00 00 IP Image: Ether type (10 bit) 00 00 IP Image: Ether type (10 bit) 00 00 IP Image: Ether type (10 bit) 00 00 IP Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit) Image: Item type (10 bit)</unknown>		MAG	DMAC Addre	ss (48 b	oit)			00 02 02 02	02 13	<unknown></unknown>	•								🔘 Remov	e Segment
Ether type (10 bit) 05 00 IP ▷ IIE IP		MAG	SMAC Addre	ss (48 b	it)			00 01 01 01	01 12	<unknown></unknown>	-								Segment (Order
 > IlĒ IPv4 - Internet Protocol v4 (20 bytes) > IlĒ UDP - User Datagram Protocol (8 bytes) □ Add 		(DEA)	Etheriype (10	D DIT)				08 00		IP										
▷ IIIF UDP - User Datagram Protocol (8 byte:	⊳				sl v4 (2	() hytes)													Move I	Down
ad Ad	ŕ																		Modifiers	
Raw - Data Segment (22 bytes)	⊳	I≣ U	DP - User Dat	tagram	Protoc	ol (8 byte:	2:												🔣 Add	
	\triangleright	l≣ Ra	aw - Data Seg	gment (2	22 byte	es)													No. Edit	



Randomize Source IP Address

- 1 Right click on "Src IP Addr"
- 2 Click "Add Modifier"

3 Select #of Src Ip`s



5

Select Address Action (Random Recommended)

Click "<u>O</u>K".

🛍 Available Resources 👻 🕫 🕕 🕕 St	art 🛛 🔲 Port Statistics 🛛 🔜 Port Configuration	Grid 🛛 🕞 Stream Configuration Grid	🖞 💅 Global Statistics 🛛 🍞 Filters 🛛 🛍 Capture
Current Testbed: Main	Stream Config		
Testbed Name Select Port # Logging? Stree	am Properties		
🖷 💿 15 No	st Size: 0 packets	Resolve Peer	Address: Send ARP
Bu	st Density: 100 percent	Check IP Pee	
🗹 Show Only Used Ports 🔒 Reserve Used Ports 🖐 Reset Used Ports 📮 🛛 Int	er Packet Gap: 0 bytes	Check in ree	Send Pivo
Chassis Sort Order: IP Address 🔹 🗄 Expand All 🖃 Collapse All	er Burst Gap: 0 bytes		
Name Used Owner	er Burst Gap: 0 ns (0 bytes)		
▲ 🗶 Chassis 5 'L23 Live Demo' (192.168.1.	st Signature:		
▲ GEE Module 6 'Odin-1G-3S-6P'	Packet Header Definitions (Total Header Size	: 34 bytes)	
▲ the Port 0 'SFP-E 10/100/1000M' • user1 • Stream number 0 (0/20)	ment/Field Name M	Field Value	Named Values
	Ethernet - Ethernet II (14 bytes)		Hanica Valacs
	E IPv4 - Internet Protocol v4 (20 bytes)		
IP Modifier Settings	, ,		
Resulting Pattern: xxx.xxx.1.18	DEC Version (4 bit)	4	
	📧 Header Length (4 bit)	5	
Min Value: 0.0 Action: Random	BIN DSCP (6 bit)	000000	Best effort 🔹
Step Value: 1 Address Offset: 20	■N ECN (2 bit)	00	
Count: 65536 Address Mask: 255.255	DEC Total Length (16 bit)	46	
Repeat Count: 1 Type: Standard (16 bit)	📧 Identification (16 bit)	00 00	
3 OK Cancel	■N Flags (3 bit)	000	
	📧 Fragment Offset (13 bit)	0	
	DEC TTL (8 bit)	127	
5	DEC Protocol (8 bit)	255	<special></special>
	Header Checksum (16 bit)	OF E4	
1	□P4 Src IP Addr (32 bit)	192.168.1.18	Add Modifier 2
	IP4 Dest IP Addr (32 bit)	192.168.168.138	Add Modifier



Randomize Dest Port Number (optional)

Ad Notice Otherwise Benove Chassis Disconnect from Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chassis State Chassis State Chassis State Chassis State Chassis State Chassis State Port State Chassis State Port State Chassis State Port State <tr< th=""><th>nmended)</th><th>rt Action (Random R</th><th>3 Select P</th><th>1 Right click on "Dest Port"</th></tr<>	nmended)	rt Action (Random R	3 Select P	1 Right click on "Dest Port"
Stat Chassis Create Testber Consist Create Testber Chassis Consorted from Chassis Chassis Chas	inager v1.62 r79.3	(''. test.vmcfg	4 Click " <u>C</u>	
✓ Show Only Used Ports Beserve Used Ports Chassis Sort Order: P Address Destis 5 'L22 Live Demo' (192:168.1.18 Demo' (192:168.1.18 Dest IP Add (12 bit) Dest IP Add (22 bit) Dest I	Remove Stream Disable All Streams & Equalize Rates Copy Stream Paste Stream Streams	d Release Resource Reservation Ports Port Statistics Port Configuration Grid States Reservation Ports Port Statistics Reservation Grid Reservation Grid Reservation Grid Resource Ports Port Statistics Reservation Grid	Reconnect to Chassis Disconnect from Chassis Keep Disconnected Create T Edit Test Delete T TestBe Create T Delete T Main S	Add Discover Chassis Discover Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chassis Chassis
▲ Image: Chassis 5 1/23 Live Demo' (192.168.1. 4 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.1 6 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.18 5 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.18 6 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.18 6 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.18 6 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.18 6 ▲ Image: Chassis 5 1/23 Live Demo' (192.168.1.18 0 Add New Modiffer 6 General Modiffer Settings 3 Min Value: Action: Random Step Value: Position: Add New Modiffer Position: Add New Modiffer FFFFF Repeat Count: 1 Type: Standard (16 bit) QK Cancel Q 10 Max Value: 65535 Mask: FFFFF QK Cancel QK Cancel QK Cancel QK Cancel QK Cancel QK Cancel QK Cancel <t< th=""><th>Named Values</th><th>ket Header Definitions (Total Header Size: 42 bytes) ht/Field Name M Field Value Ethernet - Ethernet II (14 bytes)</th><th>ed Ports</th><th>Image: Show Only Used Ports Image: Reserve Used Ports Chassis Sort Order: IP Address The Expansion of th</th></t<>	Named Values	ket Header Definitions (Total Header Size: 42 bytes) ht/Field Name M Field Value Ethernet - Ethernet II (14 bytes)	ed Ports	Image: Show Only Used Ports Image: Reserve Used Ports Chassis Sort Order: IP Address The Expansion of th
Win Value: O Action: Random Step Value: Position: 36 Max Value: 65535 Mask: FFFF Repeat Count: Type: Standard (16 bit) OK Cancel 4 If UDP - User Datagram Protocol (8 byte)	Best effort 🔹	I Version (4 bit) 4 I Header Length (4 bit) 5 I DSCP (6 bit) 000000	8.1.	▲ DFF Module 6 'Odin-1G-3S-6P' ▲ Dort 0 'SFP-E 10/100/1000M' Stream number 0 (0/20)
Repeat Count: 1 OK Cancel Image: Count: Image: Count: <th></th> <th>Identification (16 bit) 00 00 Islags (3 bit) 000 Islags Fragment Offset (13 bit) 0</th> <th>n: Random 🔻</th> <th>Min Value: 0 Action: Ra Step Value: 1 Position:</th>		Identification (16 bit) 00 00 Islags (3 bit) 000 Islags Fragment Offset (13 bit) 0	n: Random 🔻	Min Value: 0 Action: Ra Step Value: 1 Position:
	UDP -	Image: Protocol (8 bit) 17 Image: Protocol (8 bit) 10 D2 Image: Protocol (8 bit) 192.168.1.18 Image: Protocol (8 bit) 192.168.1.18	OK Cancel	ОК
Dest Port (16 bit) 0 None	None Contraction C	Image: Signal		

DDoS – TEARDROP ATTACK



Teardrop (IP Fragment Overlap) Attack

When two fragments contained within the same IP datagram have offsets that indicate that they overlap each other in positioning within the datagram.

Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments.



Teardrop Attack

A legitimate host has no reason of producing overlapping fragments.

A receiver has no reason to accept them.

RFC5722 recommends that overlapping fragments should be totally disallowed:

 ...the entire datagram (as well as any constituent fragments, including those not yet received) must be silently discarded. If fragmentation overlapping is handled differently by different OS, if manipulated properly can lead to:

- OS Fingerprinting
- IDS Insertion / Evasion
- Firewall Evasion
- DoS due to consumption of the resources.
- DoS due to ...kernel crashes.
- Even ...remote code execution

1 0.000000	192.0.2.1	192.0.2.2	ICMP	98 Echo (ping) request id=0x8c13, seg=0/0, ttl=64 (no response found!)
2 0.835102	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=16120, ID=00f2)
3 0.835127	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=47016, ID=00f2)
4 0.835190	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=6104, ID=00f2)
5 0.835200	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=27528, ID=00f2)
6 0.835210	192.0.2.1	192.0.2.2	IPV4	74 Fragmented IP protocol (proto=UDP 17, off=40632, ID=00f2)
7 0.835220	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=32104, ID=00f2)
8 0.835229	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=45976, ID=00f2)
9 0.835265	192.0.2.1	192.0.2.2	IPV4	74 Fragmented IP protocol (proto=UDP 17, off=52552, ID=00f2)
10 0.835275	192.0.2.1	192.0.2.2	IPv4	74 Fragmented IP protocol (proto=UDP 17, off=13944, ID=00f2)
10 0.835275	192.0.2.1	192.0.2.2	IPV4	74 Fraqmented IP protocol (proto=UDP 17, off=13944, ID=00f2)
	192.0.2.1	192.0.2.2	IPV4	74 Fragmented IP protocol (proto=UDP 17, off=52552, ID=00f2)

DDoS – TEARDROP ATTACK



Teardrop Attack

Load configuration file Teardrop_Attack.xpc It will add Streams with no T and set port Tx Mode to: Sequential

	🛍 Available Resou	rces				-	ņ
	Current Testbed:						
	Testbed Name			Select	Port #	Loggin	g?
file				۲	15	No	
lie							
	Show Only Used	l Ports 🔒 Reserve	e Used Ports	🖐 Re	set Used	Ports	Ţ
с.хрс	Chassis Sort Order:	IP Address 🔹	Expand	AII 🗉	Collaps	e All	
	Name			Jsed	Ow	ner	
with no TID	▲ 📉 Chassis 5 'l	.23 Live Demo' (19	2.168.1.17				
		5 'Odin-1G-3S-6P' 'SFP-E 10/100/10	000	✓ •	0 use	1	
_		et number 1 (1 (n		¥ •	 use 	:r i	
le to:	🚥 Pack	et number 2 (2 (n	o TID))				
	🚥 Pack	et number 3 (3 (n	o TID))				
		et number 4 (4 (n					
		et number 5 (5 (n et number 6 (6 (n					
		et number 0 (0 (n et number 7 (7 (n					
		et number 7 (7 (n et number 8 (8 (n					
	🚥 Pack	et number 9 (9 (n	o TID))				
	📑 Strea	m number 10 (10) (no TID)				

ain Port Config Tran	sceiver Features Impairments Config	
ort Properties		
 Main Properties 	占 Load Streams 🔚 Sav	e Streams
Identification		La
Name:	P-5-6-0	Po
Description:	IPv4	M
Loaded From:	Teardrop_Attack.xpc	S
Interface Type:	SFP-E 10/100/1000M	Ci
Reserved By:	user1	Ef
TX Control		A
Sync Status:	 IN SYNC 	M
Traffic Status:	 OFF 	St
Traffic Control:	🍁 Start	т
Include in Global Cont	trol: 🗹	0
Enable TX Output:		La
TX Time Limit:	00:00:00	M
TX Time Elapsed:	00:00:00	
Stop After:	0 packets	м
TX Profile		Re
	Sequential 💌	G
Port TX Mode:	Sequentiar	
Rate Fraction:	0.01 percent	G
Packet Rate:	100 packets/second	Pa
Bit Rate:	0.064 Mbit/sec (L2)	Pa



Smurf Attack

A DDos attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network.

Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

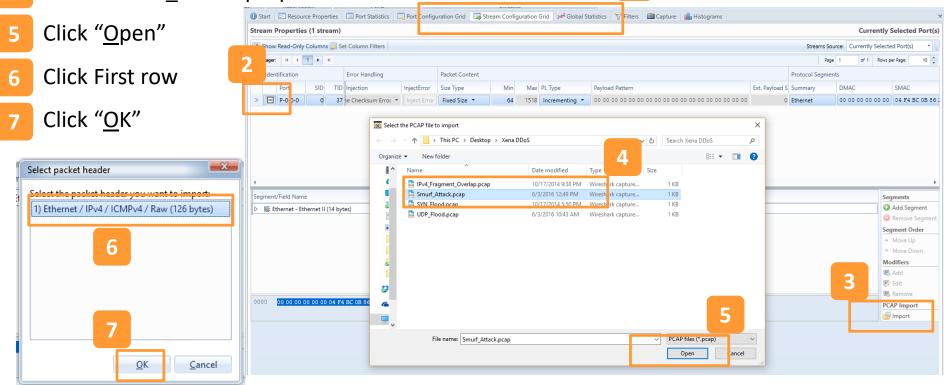


- 1 Right-click on Attacking port.
- 2 Click "Add Stream"

🛍 Available Resour	ces					-	ů.
Current Testbed:							
Testbed Name			1	Select	Port #	Loggin	ıg?
				۲	15	No	
Show Only Used	Ports 🔒 Reserv	e Used P	orts	 FRe	set Use	d Ports	÷
Chassis Sort Order:	IP Address 🔹	🕀 Exp	and /	AII 🗆	Collap	se All	
Name			Use	d	Owr	ner	
🔺 🐹 Chassis 5 'L	23 Live Demo' (19	2.168.1.					
	'Odin-1G-3S-6P'	_					
1 Port 0	SFP-E 10/100/10	000M	1	•	user	r1	
			Add	Strear	n	2	
			Add	Multip	ple Stre		
			Strea	am He	aders fr	om PCA	λP
		6	Rele	ase Po	ort		
			Un-ı	use Po	rt		
		e	Load	d Port	Configu	iration	
			Save	e Port (Configu	ration	
		٢	Refr	esh Po	rt		
		4	Rese	et Port			



- Go to "Stream Configuration Grid" tab.
- 2 Click "+".
- 3 Click "Import"
- 4 Select Smurf_Attack.pcap





1

You may see the alert telling you to increase the minimum packet length. Change the minimum size to 152 bytes.

					tification		Error Handling		Packet Conte	nt			_	
					Port SID	TID	Injection	InjectError	Size Type		Min	Max	L Type	Payload Pattern
					P-0-0-0 0	37	ne Checksum Error 🔻	Inject Error	Fixed Size	-	64	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00
		Packet Content			(Field Name hernet - Ethernet II (v4 - Internet Protoco	ol 14 (2	20 bytes)	:ket length of	64 bytes. The t	num p	yload (TPLE acket length) areas w	exceeds the minim vill also be affected.	X um
	InjectError	Size Type	Min	Max	PL Type		Payload Pa	ttern						
or 🔻	Inject Error	Fixed Size 🔻	152	518	Incrementing	-	00 00 00	0 0 0 0	0 0 0 0 0	00	00 00	00		



Randomize Source MAC Address

1	Right click on "SMAC A	۹ddress"									
	-	🕕 Start 🛛 🖂 Resource Pro	operties 📃 Port Stati	istics 🛛 🛄 Port Configur	ration Grid	Stream Configurati	on Grid 🛹 Global Sta	tistics 🛛 🏹 Filters 🖾 Capture 🚺	Histograms		
2	Click "Add Modifier"	Stream Properties (1 s	stream)								
)	Show Read-Only Colum	mns 📝 Set Column Filt	ters							
3	Select Action	Data Pager: H 📢 1 🕨	н								
5	Select Action	Identification	Error Handli	Packet Content						Protocol Segmen	nts
()			ID TID InjectError			PL Type	Payload Pattern		Ext. Payload S		DMAC
(R:	andom Recommended)	> 🕒 P-0-0-0	1 37 Inject Error	Fixed Size 🔻	152 1518	Incrementing 🔻	00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00	0	Ethernet/IPv4/IC1	N FF FF
4	Click " <u>O</u> K".										
		•						Ш			
		Segment/Field Name	Μ	1 Field Value		Named Values		W			
		 Segment/Field Name Ethernet - Ethernet 		1 Field Value		Named Values					_
		▲ IE Ethernet - Ethernet IMAC Address (4	et II (14 bytes) (48 bit)	FF FF FF FF FF FF		<unknown></unknown>	•	I			
Add	ew Modifier	Ethernet - Ethernet Ethernet - Ethernet MAC Address (4 MAC Address (4	et II (14 bytes) (48 bit) (48 bit)	FF FF FF FF FF FF FF		<unknown></unknown>	· · 2	III			
	New Modifier	▲ IE Ethernet - Ethernet IMAC Address (4	tt II (14 bytes) (48 bit) (48 bit) (48 bit) (t)	FF FF FF FF FF FF		<unknown></unknown>	. 2				
Gene	eral Modifier Settings 3	Illing Ethernet - Ethernet Mac Address (4 Mac SMAC Address (4 Mac SMAC Address (4 Mac EtherType (16 bit	tt II (14 bytes) (48 bit) 48 bit) t) ttocol v4 (20 bytes)	FF FF FF FF FF FF FF		<unknown></unknown>	2				
Gene		III: Ethernet - Ethernet Emeret Emeret DMAC Address (4 Initial SMAC Address (4 Initial EtherType (16 bit III: IPv4 - Internet Prot	tt II (14 bytes) (48 bit) 48 bit) tt tt tt control Message Prc	FF FF FF FF FF FF FF		<unknown></unknown>	2				
Gene Min \	eral Modifier Settings 3	III: Ethernet - Ethernet III: Ethernet III: DMAC Address (4 III: SMAC Address (4 IIII: EtherType (16 bit III: IPv4 - Internet Prot III: ICMPv4 - Internet (0	et II (14 bytes) (48 bit) 48 bit) ti totocol v4 (20 bytes) Control Message Pro ent (64 bytes)	FF FF FF FF FF FF FF		<unknown></unknown>	2				
Gene Min V Step ¹	eral Modifier Settings Value: 0 Action: Random	IIIF Ethernet - Ethernet IIIF Ethernet - Ethernet IIIF OMAC Address (4 IIIIF SMAC Address (4 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	et II (14 bytes) (48 bit) 48 bit) ti totocol v4 (20 bytes) Control Message Pro ent (64 bytes)	FF FF FF FF FF FF FF		<unknown></unknown>	2				
Gene Min V Step V	eral Modifier Settings Value: 0 Action: Random Value: 1 Position: 6	IIIF Ethernet - Ethernet IIIF Ethernet - Ethernet IIIF OMAC Address (4 IIIIF SMAC Address (4 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	et II (14 bytes) (48 bit) 48 bit) ti totocol v4 (20 bytes) Control Message Pro ent (64 bytes)	FF FF FF FF FF FF FF		<unknown></unknown>	2				

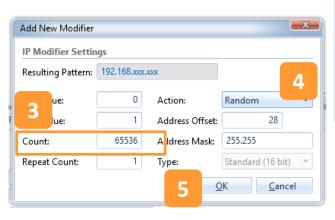


Randomize Source IP Address

- 1 Right click on "Src IP Addr"
- 2 Click "Add Modifier"
- 3 Select #of Src Ip`s
- 4 Select Address Action

(Random Recommended)

5 Click "<u>O</u>K".



0 5	start	📰 Resourr	ze Prope	rties	Port Statis	stics 📃 Port Conf	iguration Gr	rid 🗾	Stream Configurati	on Grid 🥵 Global Statistics	💎 Filters 🛛 🕅 Capture	🔒 Histograms		
Stre	eam P	Properties	(1 stre	am)										
	Show	Read-Only (Columns	, 📝 Se	et Column Filter	2rs								Stre
Data	a Pager:	: H 4 1	1.	н										
	Ident	tification			Error Handlii	Packet Content							Protocol Segment	ts
		Port	SID	TID	InjectError	Size Type	Min	Max	PL Type	Payload Pattern		Ext. Payload S	Summary	DMAC
>	Ξ	P-0-0-0	0	37	Inject Error	Fixed Size 🔻	153	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	0 0	Ethernet/IPv4/ICN	FF FF FF FF I

٠		
Segment/Field Name	M Field Value	Named Values
 IF Ethernet - Ethernet II (14 bytes) 	M	
⊿ I≣ IPv4 - Internet Protocol v4 (20 bytes)		
DEC Version (4 bit)	4	
DEC Header Length (4 bit)	5	
BIN DSCP (6 bit)	000000	Best effort 🔹
ECN (2 bit)	00	
IDEC Total Length (16 bit)	135	
HEX Identification (16 bit)	00 00	
■N Flags (3 bit)	000	
DEC Fragment Offset (13 bit)	0	
DEC TTL (8 bit)	64	
DEC Protocol (8 bit)	1	ICMP -
📧 Header Checksum (16 bit)	F0 1C	
IF4 Src IP Addr (32 bit)	192.168.1.10	
IPA Dest IP Addr (32 bit)	192.168.7.255	
▷ ■ ICMPv4 - Internet Control Message Pro		

DDoS – PING OF DEATH



Ping of Death

A type of attack on a computer system that involves sending a malformed or otherwise malicious ping to a computer.

DDoS – PING OF DEATH

- 1 Right-click on Attacking port.
- 2 Click "Add Stream"

 Show Only Used Ports Reserve Used Porto Reserve Used Ports Reserve Used Po		- ú				
Current Testbed:						
Current Testbed: Testbed Name Select Port # Image: Loggin		Logging				
				۲	15	No
Show Only Used	Ports 🔒 Reserv	e Used P	orts	🖐 Re	set Use	d Ports
Chassis Sort Order:	IP Address 🔹	🕀 Exp	and	AII 🗆	Collap	se All
Name			Us	ed	Owr	ner
	-	92.168.1.				
1 Port 0	SFP-E 10/100/10	000M				·1
			Ad	d Strear	m	2
			Ad	d Multi _l	ple Stre	ams
			Str	eam He	aders fr	om PCAP
		ŝ	Rel	ease Po	ort	
			Un	-use Po	rt	
			Loa	ad Port	Configu	ration
			Sav	/e Port (Configu	ration
		G	Ret	fresh Po	ort	
		45	Re	set Port		

DDoS – PING OF DEATH

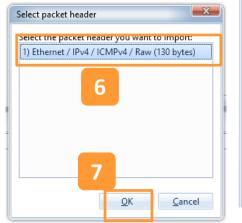


- Go to "Stream Configuration Grid" tab.
- 2 Click "+".
- 3 Click "Import"
- 4 Select Ping_Of_Death.pcap



6 Click First row



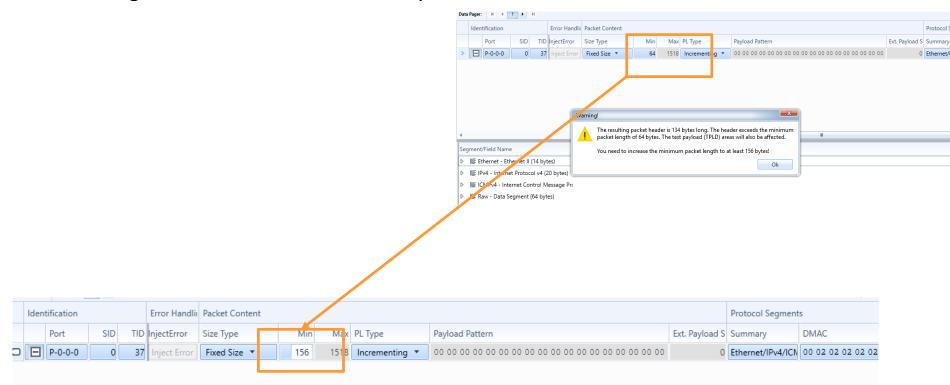


<i>"</i>	Start Res			istics 📃 P	or Configuration	n Grid 🔛	Stream Configura	tion Grid 🦟 Glob	al Statistics 🛛 🖓 Filt	ers 🛛 🕅 Capt	sure 🚺 Histog	rams			Current	ly Selected	d Port
	Show Read-O	nly Columns 👿	Set Column Fil	ters										Streams So	ource: Currently Sele	ected Port(s)	•
2	a Pager: H	{ 1 } H												Pag	ge 1 of 1 Ro	ws per Page:	10
ow 🧲	Identificatio	n	Error Handl	Packet Con	tent								Protocol Se	gments			
	Port	SID	TID InjectError	Size Type	Mi	in Max	PL Type	Payload Pattern			Ext. Pa	iyload S	Summary	DMAC	SMAC	VLAN	DSC
	> 🖃 P-D-0-	0 0	37 Inject Error	Fixed Size	• 6		Incrementing •	00 00 00 00 00	00 00 00 00 00 00 00	0 00 00 00 0	0 00 00		Ethernet	00 00 00 00 00 00	04 F4 BC 0B 86 2	0	
L					,									*	A.		
				🔀 Select the	PCAP file to imp	ort							×				
				$\leftarrow \rightarrow \vee$	↑ 🚺 > This	PC → Des	ktop → Xena DDo	S		ΰv	Search Xena DDo	S	م				
				Organize 🔻	New folder						B						
SZ D				-		^		D	4		8	•					
— ×					lame			Date modified	Туре	Size							
	•		_		IPv4_Fragmen Ping_Of_Deatl		ocap	10/17/2014 9:38 PI 6/3/2016 1:22 PM			1 KB 1 KB						
пт то ітрогт:	Segment/Field N	ame			Smurf Attack			6/3/2016 12:49 PM	Wiresh rk captur Wiresh rk captur		1 KB					Segments	
w (130 bytes)	▷ I≣ Ethernet	- Ethernet II (14	bytes)		SYN_Flood.pc	cap		10/17/2014 5:50 PI			1 KB					Add Segi	
					🔠 UDP_Flood.pc	cap		6/3/2016 10:43 AN	Wireshark captu	e	1 KB					Remove :	
																Segment Or Move Up	
																 Move Do 	
				2												Modifiers	
																🚯 Add	
				2											3	💕 Edit	
-																🚯 Remove	
	0000 00 00	00 00 00 00 04	F4 BC 0B 86	6												PCAP Impor	rt
												5				📑 Import	
				~													
					File nan	me: Ping_C)f_Death.pcap			~	PCAP lifes (.pca	ip)	~				

1



You may see the alert telling you to increase the minimum packet length. Change the minimum size to 156 bytes.



<u>0</u>K

5

<u>C</u>ancel



Increase IP Fragment Offset

1	Right click on '	"Fragment C	Offset"	1010	511,41112						
		Stream Properties (1 stream) Currently Selected Port(s Currently Sele									
2	Click "Add Modifier"		Streams Source: Currently Selecte								•
			Data Pager: H 4 1 + H						ge 1 of 1	Rows per Page:	10
			Identification Error Handlin Packet Content Protocol Segments								
3	Select Action		Port SID TID InjectEr	rror Size Type	Min Max PL Type	Payload Pattern	Ext. Payload S Sum	mmary DMAC	SMAC	VLAN	DSCP
			> P-0-0-0 0 37 Inject	Error Fixed Size 🔻	156 1518 Incrementing	00 00 00 00 00 00 00 00 00 00 00 00 00	0 Ethe	ernet/IPv4/ICN 00 02 02 02 02 02	00 01 01 01 01 01	. 01	0
(Increment Recommended)											
4 Set "Step Value" to 12.											
		(11					•	
		Segment/Field Name Image: Ethernet - Ethernet II (14 bytes)	M Field Value	Named Values					Segments Add Segment	-	
	5 Click " <u>O</u> K".		▲ IE IPv4 - Internet Protocol v4 (20 bytes)	5)						Remove Segm	ient
5			Des Version (4 bit)	4						Segment Order	
			EEE Header Length (4 bit)	5						 Move Up Move Down 	
			DSCP (6 bit)	000000	Best effort	•				Modifiers	
			ECN (2 bit)	00						🖪 Add	
			Total Length (16 bit)	46		2				📝 Edit	
			Flags (3 bit)	001		2				Remove PCAP Import	
			Fragment Offset (13 bit)	0						Import Import	_
Add New Modifier			IBET TTL (8 bit)	64		Add Modifier					
			DEC Protocol (8 bit)	1	ICMP	•					
General Modifier Settings			Header Checksum (16 bit)	D1 40							
			Src IP Addr (32 bit)	192.168.1.1							
Min V	/alue: 0 Action:	Increment 3	Dest IP Addr (32 bit)	192.168.7.61							
			L D IE ICMPv4 - Internet Control Message	Pro							
Step \	Value: 12 Position	: 20	1								
4	ue: 65535 Mask:	FFFF	-								
	at Count: 1 Type:	Standard (16 bit) 🔻									



Ping Flood (ICMP Flood)

A simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.

This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies.

If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown.



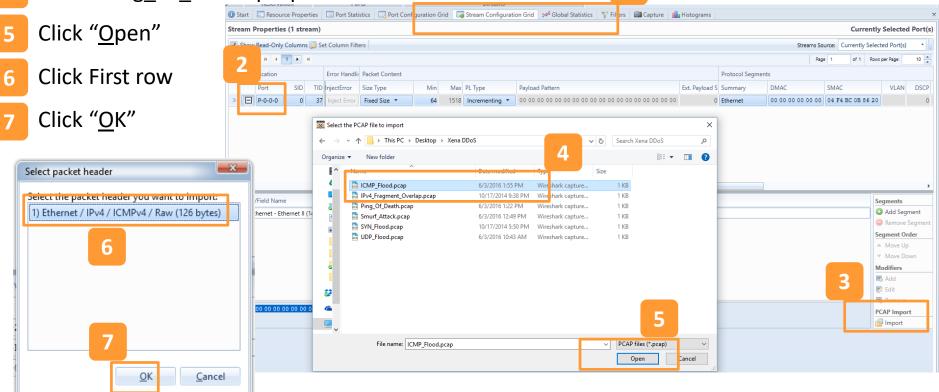
1 Right-click on Attacking port.

2 Click "Add Stream"

🛍 Available Resour	ces					-	ņ
Current Testbed:							
Testbed Name				Select	Port #	Logging	g?
				۲	15	No	
Show Only Used	Ports 🔒 Reserv	e Used P	orts	🔑 Re	set Use	d Ports	÷
Chassis Sort Order:	IP Address 🔹	🗄 Exp	and	I Ali 🗆	Collap	se All	
Name			Us	ed	Owr	ner	
🔺 🐹 Chassis 5 'L	23 Live Demo' (19	2.168.1.					
	'Odin-1G-3S-6P'	_					_
1 Port 0	SFP-E 10/100/10	M000	1			r1	
			Ad	d Strear	m	2	
			Ad	d Multi	ple Stre	ams	
			Str	eam He	aders fr	om PCA	Ρ
		Ĝ	Rel	lease Po	ort		
			Un	-use Po	rt		
			Loa	ad Port	Configu	iration	
			Sav	ve Port (Configu	ration	
		త	Ret	fresh Po	ort		
		4	Re	set Port			



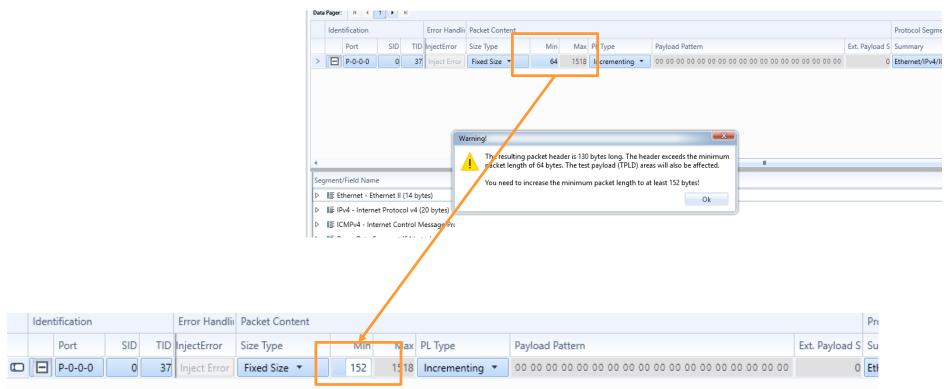
- Go to "Stream Configuration Grid" tab.
- 2 Click "+".
- 3 Click "Import"
- 4 Select Ping_Of_Death.pcap





1

You may see the alert telling you to increase the minimum packet length. Change the minimum size to 152 bytes.





Randomize Source MAC Address

1 Right click on "SMAC Address"

2	Click "Add Modifier"		Port	SID	TID I	njectError	Si	iize Type		Min	Max	PL Type	Payload	d Patte	ern		
		>	P-0-0-0	0	37	Inject Error	F	Fixed Size 🔻		152 1	1518	Incrementing 💌	00 00	00 00	00 00 00 00 00	00 00 00	00 00
3	Select Action																
(Ra	ndom Recommended)																
4	Click " <u>O</u> K".										_						
		•									_					Ш	
		Seg	ment/Field Nam	e		N	4	Field Value				Named Values					
		4	Ethernet - Et	hernet II ((14 byte	es)											
			MAG DMAC Add	lress (48 b	oit)			00 02 02 02 02 02 0	02			<unknown></unknown>					
			MAG SMAC Add	ress (48 b	oit)	1		00 3F D8 53 3D (65			<unknown></unknown>	2		_		
Add No	w Modifier		HEX EtherType	(16 bit)				08 00				IP	•		🚯 Add Modifie	r	
	2	⊳	📑 IPv4 - Intern	et Protoco	ol v4 (20) bytes)											
Genera Min Val		⊳	IE ICMPv4 - Int	ernet Con	trol Me	essage Pro											
Step Va		⊳	📑 Raw - Data S	egment ((64 byte	s)											
Max Va																	
Repeat	Count: 1 Type: Standard (16 bit)																
	<u>OK</u> <u>Cancel</u>																

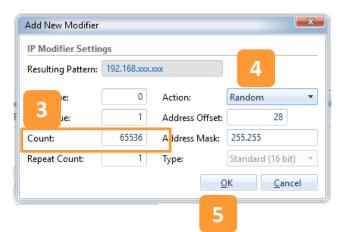


Randomize Source IP Address

- 1 Right click on "Src IP Addr"
- 2 Click "Add Modifier"
- 3 Select #of Src Ip`s
- 4 Select Address Action

(Random Recommended)

⁵ Click "<u>O</u>K".



> P-0-0-0 0 37 Inject Error Fixed Size • 152 1518 Incrementing • 00 00 00 00 00 00 00 00 00			Port	SID	TID	InjectError	Size Type	Min	Max	PL Type	Payload Pattern
	>	Ξ	P-0-0-0	0	37	Inject Error	Fixed Size 🔻	152	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00

gment/Field Name	М	Field Value	Named	Values		
I≣ Ethernet - Ethernet II (14 bytes)	K					
I≣ IPv4 - Internet Protocol v4 (20 bytes)						
DEC Version (4 bit)		4				
📧 Header Length (4 bit)		5				
BIN DSCP (6 bit)		000000	Best eff	ort 🔻		
BIN ECN (2 bit)		00				
DEC Total Length (16 bit)		46				
HEX Identification (16 bit)		00 00				
💵 Flags (3 bit)		000				
DEC Fragment Offset (13 bit)		0				
DEC TTL (8 bit)		64				
DEC Protocol (8 bit)		1	ICMP	•		
Header Checksum (16 bit)		F0 B1				
III Src IP Addr (32 bit)		192.168.1.144	2			
🏴 Dest IP Addr (32 bit)		192.168.7.61	Add Modifier			

IE ICMPv4 - Internet Control Message Pro

۰

Seg

⊳



ARP Spoofing (ARP Cache Poisoning)

A technique by which an attacker sends spoofed Address Resolution Protocol (ARP) messages onto a local area network.

Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

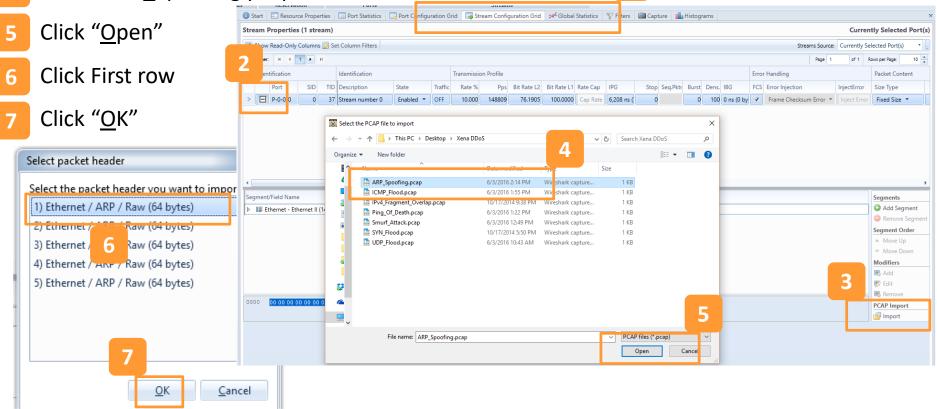


- 1 Right-click on Attacking port.
- 2 Click "Add Stream"

🛍 Available Resources	- Ú
Current Testbed:	
Testbed Name	Select Port # Logging
	I5 No
🗷 Show Only Used Ports 🔒 Reserv	e Used Ports 🖐 Reset Used Ports
Chassis Sort Order: IP Address 🔹	🗉 Expand All 🗉 Collapse All
Name	Used Owner
🔺 🐹 Chassis 5 'L23 Live Demo' (19	02.168.1.
▲ Module 6 'Odin-1G-3S-6P'	
1 Port 0 'SFP-E 10/100/10	000M 🔽 🔹 user1
	Add Stream 2
	🔒 Stream Headers from PCAP
	Release Port
	Un-use Port
	Load Port Configuration
	Save Port Configuration
	🕼 Refresh Port
	🖐 Reset Port



- Go to "Stream Configuration Grid" tab.
- 2 Click "+".
- 3 Click "Import"
- 4 Select ARP_Spoofing.pcap





1

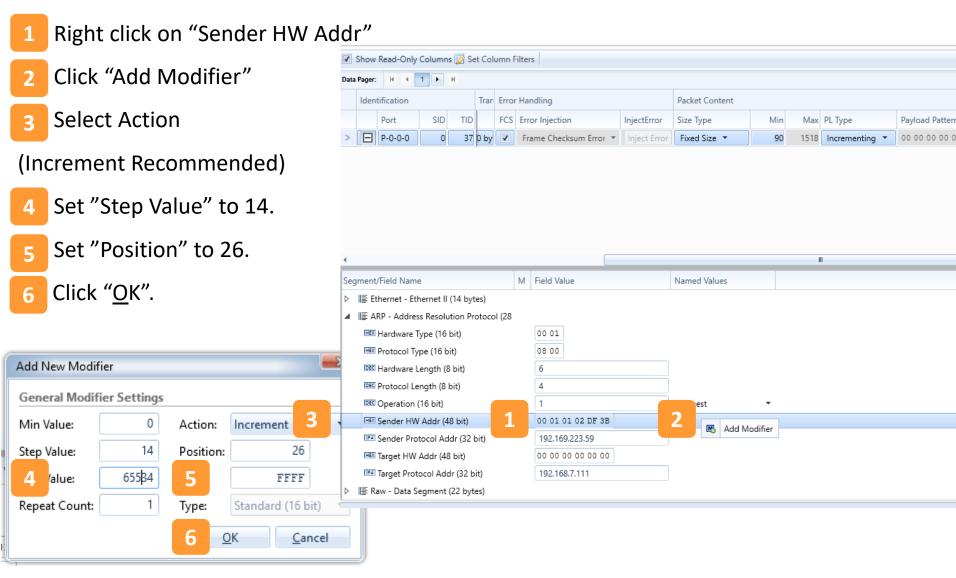
You may see the alert telling you to increase the minimum packet length. Change the minimum size to 90 bytes.

> 🖃 P-0-0-0 0 37 Stream n	umber 0 Enabled 🔻 O	FF 10.000 14880	9 76.1905	100.0000 Cap	Rate 6,208 ns (0	0	100 0 ns (0 by	 Frame Checksum Error
	Warning!			— X					
		header is 68 bytes long. T	he header evened	la tha minimum					
٠		bytes. The test payload (TP							
Segment/Field Name				hu da a l					
	You need to increase	e the minimum packet leng	gth to at least 90 l	bytes:	-				
▷ 📑 Ethernet - Ethernet II (14 bytes)				Ok					
▷ 🞼 ARP - Address Resolution Protocol (28					9				
▷ 📑 Raw - Data Segment (22 bytes)									

Stre	eam P	Properties	s (1 stre	am)										Curren	ntly Selected I	Port(s)
	Show	Read-Only (Columns	; 📝 Set	t Colum	n Filters							Streams S	iource: Currently Se	elected Port(s)	•
Data	a Pager:	н н	1	н									Pag	ge 1 of 1 F	Rows per Page:	10 🔺
	Ident	tification			Tran Er	rror Handling		Packet Content						Protocol Segment	ts	
		Port	SID	TID	FC	CS Error Injection	InjectError	Size Type	Min	Ma	C PL Type	Payload Pattern	Ext. Payload S	Summary	DMAC	5
		P-0-0-0	0	37	0 by	Frame Checksum Error 🔻	Inject Error	Fixed Size	90	151	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00		Ethernet/ARP/Ray	FF FF FF FF F	FFFC



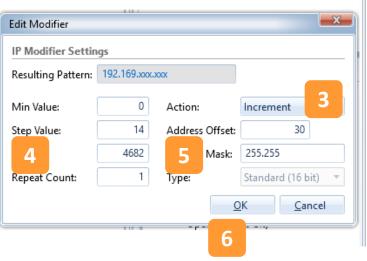
Increase Sender HW Address





Increase Sender Protocol Address

- 1 Right click on "Sender Protocol Addr"
- 2 Click "Add Modifier"
- 3 Select Action
- (Increment Recommended)
- 4 Set "Step Value" to 14.
- 5 Set "Address Offset" to 30.
- 6 Click "<u>O</u>K".



د س	ldri	E Resour	се вторе	erues		ับาน อเล	iusucs 👔 🔤 Port Conligura		🤿 Stream Coniig	guration ond	- GIOD	a statistics Training
Stre	eam F	Propertie	s (1 stre	eam)								
1	Show	Read-Only	Column	s 📝 Se	et Col	umn Fi	lters					
Data	Pager:	H 4	1	н								
	Iden	tification			Tran	Error	Handling		Packet Conte	nt		
		Port	SID	TID			Error Injection	InjectError	Size Type	Min	May	PL Type
>	Ξ	P-0-0-0	0		0 by		Frame Checksum Error 🔻	Inject Error	1			Incrementing •
/		P-0-0-0		57	о ву	•	Frame Checksum Error *	Inject Error	Fixed Size *	90	1210	incrementing *
•												11
Seg	gment	/Field Nam	e				M Field Value		Named Values	;		
⊳	I≣ Et	thernet - Et	hernet II	(14 byt	es)							
4	I≣ A	RP - Addre	ss Resolu	ition Pr	otoco	ol (28						
	HEX	Hardware 1	Гуре (16	bit)			00 01					
	HEX	Protocol Ty	/pe (16 b	it)			08 00					
	DEC	Hardware l	Length (8	3 bit)			6					
	DEC	Protocol Le	ength (8 l	bit)			4					
		Operation					1		Request	•		
4	HEX	Sender HW	/ Addr (4	8 bit)			00 01 01 02 DF 3B					
		Standard				1	P:26, FFFF, INC, R:1, [0:	65534], S:14	2			
		Sender Pro			bit)		192.169.223.59			Add Modifier		
		Target HW					00 00 00 00 00 00				1	
	IP4	Target Prot	ocol Add	dr (32 b	it)		192.168.7.111					
		aw - Data S										



1

Repeat the previous steps, you can add as many stream as you want. Remember to change the "Target Protocol Addr" to a different address.

	Show	Read-Only	Columns 📝 S	Set Col	umn F	ilters							Streams S	ource: Currer	ntly Sel
Data	Pager:	14 4	1 • H										Pa	ge 1 of	1 R
	Ident	ification		Tran	Error	Handling		Packet Content						Protocol Sec	gments
		Port	SID TI		FCS	Error Injection	InjectError	Size Type	Min	Max	PL Type	Payload Pattern	Ext. Payload S	Summary	
	Đ	P-0-0-1	0	0 by	-	Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	68	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00) 0	Ethernet/AR	P/Rav
>	Ξ	P-0-0-1	1	0 by		Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	68	1518	Incrementing 🔻	0 0 00 00 00 00 00 00 00 00 00 00 00 00	0	Ethernet/AR	P/Rav
	÷	P-0-0-1	2	0 by		Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	68	1518	Incrementing 🔻	- 00 00 00 00 00 00 00 00 00 00 00 00 00	0	Ethernet/AR	P/Rav
	÷	P-0-0-1	3	0 by		Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	68	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00	0	Ethernet/AR	P/Rav
	÷	P-0-0-1	4	0 by	1	Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	68	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00	0	Ethernet/AR	P/Rav
	÷	P-0-0-1	5	0 by	-	Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	68	1518	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00	0	Ethernet/AR	P/Rav
		Hardware T Protocol Ty	ype (16 bit) pe (16 bit)			00 01									
			ength (8 bit)			6									
	DEC	Protocol Le	ngth (8 bit)			4									
	DEC	Operation (16 bit)			1		Request	•						
4	HEX	Sender HW	Addr (48 bit)			00 01 01 02 DF 3B									
	M	Standard	(16 bit)			P:26, FFFF, INC, R:1, [2 :	65508], S:14								
	1P4	Sender Pro	tocol Addr (32	bit)		192.169.223.59									
4		Standard				P:30, FFFF, INC, R:1, [2 :	61154], S:14								
4	100 COL	larget Hvv	Adar (46 bit)			00 00 00 00 00 00									
4			ocol Addr (32			192,168,7,171									



TCP Sequence Prediction Attack

An attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets.

The attacker hopes to correctly guess the sequence number to be used by the sending host. If they can do this, they will be able to send counterfeit packets to the receiving host which will seem to originate from the sending host.



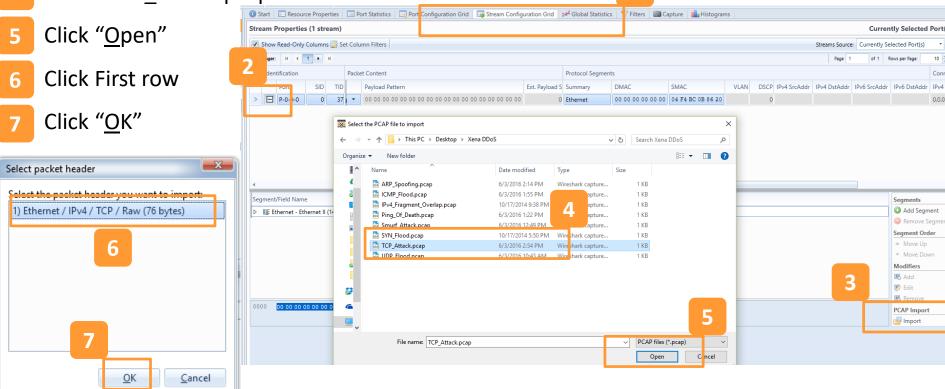
1 Right-click on Attacking port.

2 Click "Add Stream"

🛍 Available Resources			- t
Current Testbed:			
Testbed Name		Select	Port # Logging?
		۲	15 No
🗹 Show Only Used Ports 🔒 Reserve	Used Por	rts 두 Re	set Used Ports 💂
Chassis Sort Order: IP Address 🔹	🕀 Expar	nd All 🗉	Collapse All
Name	ι	Used	Owner
🔺 🐹 Chassis 5 'L23 Live Demo' (192	168.1.		
▲ Module 6 'Odin-1G-3S-6P'	_		
1 Port 0 'SFP-E 10/100/100	0M	V • (user1
		Add Strear	m 2
		Add Multi	ple Streams
	占 s	Stream He	aders from PCAP
	🔓 R	Release Po	ort
		Jn-use Po	rt
	占 L	oad Port	Configuration
	🗎 S	Save Port (Configuration
	🍪 R	Refresh Po	ort
	% R	Reset Port	

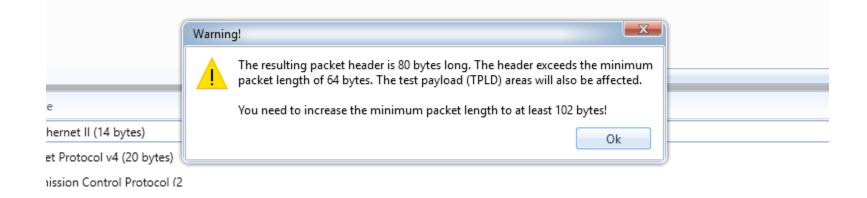


- **1** Go to "Stream Configuration Grid" tab.
- 2 Click "+".
- 3 Click "Import"
- 4 Select TCP_Attack.pcap





You may see the alert telling you to increase the minimum packet length. Change the minimum size to 102 bytes.



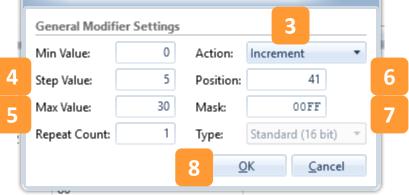
•		۶I.									
1			Transmis	Error	r Handling		Packet Content				
	SID	TID	βG	FCS	Error Injection	InjectError	Size Type	Min	Max	PL Type	Payload Pattern
C	0	37	ns (0 by		Frame Checksum Error 🔻	Inject Error	Fixed Size 🔻	102	15 18	Incrementing 🔻	00 00 00 00 00 00 00 00 00 00 00 00 00



Packet Conter Increase TCP Sequence Number Port SID TID BG InjectError Size Type Min Max PL Type Payload Pattern FCS Error Injection P-0-0-0 0 37 | ns (0 by 🛛 Fixed Size 🔻 Frame Checksum Error 🔻 Inject Error 102 1518 Incrementing T 00 00 00 00 00

- 1 Right click on "Sequence Number"
- 2 Click "Add Modifier"
- 3 Select Action
- (Increment Recommended)
- 4 Set "Step Value" to 5.
- 5 Set "Max Value" to 30.
- 6 Set "Position" to 41.
- 7 Set "Mask" to 00FF.
- 3 Click "<u>O</u>K".

			II
egment/Field Name	Μ	Field Value	Named Values
→ 🕼 Ethernet - Ethernet II (14 bytes)			
→ 🞼 IPv4 - Internet Protocol v4 (20 by	/tes)		
🛛 🞼 TCP - Transmission Control Proto	col (2		
DEC Src Port (16 bit)		1024	
Dest Port (16 bit)		80	
©EC Sequence Number (32 bit)	1	7829509	2
DEC Acknowledge Number (32 bit)		0	K Add Modifier
Deta Offset (4 bit)		5	
DEC (reserved) (3 bit)		0	
■N Flags (9 bit)		00000001	
DEC Window Size (16 bit)		8192	
HEX Checksum (16 bit)		89 82	





Inc	rease TCP ACK Number	> [E	Port	SID 0	TID 8G 37 ns (0 t		Error Inject	ion ecksum Error 🔻	InjectError	Size Type Fixed Size 🔻	Min 102		PL Type Incrementing 💌		
1	Right click on "Acknowledge Number"														
2	Click "Add Modifier"														
3	Select Action	Segment/Field Name M Field Value Named Value							med Values	III ues					
(In	crement Recommended)	 ▷ II를 Ethernet - Ethernet II (14 bytes) ▷ II를 IPv4 - Internet Protocol v4 (20 bytes) 													
4	Set "Step Value" to 5.		TCP - Transmi		ntrol Protocol	(2	1024								
5	Set "Position" to 45.	lœ Dest Port (16 bit) ◢ lœ Sequence Number (32 bit)					80 7829509								
6	Set "Mask" to 00FF.		M Standard	ge Numb	er (32 bit)	1	P:41, 00FF,	, S:5	2	B /	Add Modifier				
7	Click " <u>O</u> K".	Image: Deta Offset (4 bit) Image: Deta Offset (4 bit) Image: Deta Deta Deta Deta Deta Deta Deta Deta					5 0 00000000								
		4	Edit Mo	odifier al Modi lue: alue: alue:	6553	5 5	Action: Position: Mask:	3 Increment 45 00FF Standard (16	2 2	5					

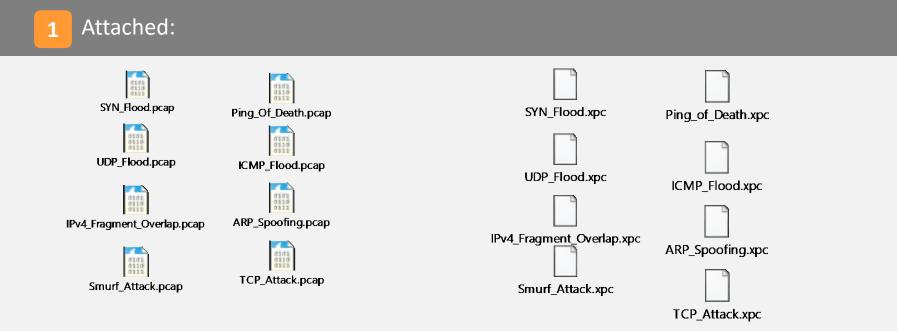


Repeat the previous steps, you can add as many stream as you want. Remember to change the "Target Protocol Addr" to a different address.

🕕 Sta	Start 🗈 Resource Properties 📄 Port Statistics 📑 Port Configuration Grid 📑 Stream Configuration Grid 💅 Global Statistics 🚏 Filters 🛍 Capture 🏭 Histograms																		
Strea	Stream Properties (2 streams) Currently Selected Port(s)																		
🗹 S	🐼 Show Read-Only Columns 🔯 Set Column Filters																		
Page H I H Page 1 I													e 10 🔺						
	Identi	ification	Packet Content Protocol Segments										Connectivity Check						
		Port	SID	TID		Ext. Payload S	Summary	DMAC	SMAC	VLAN	DSCP	IPv4 SrcAddr	IPv4 DstAddr	IPv6 SrcAddr	IPv6 DstAddr	IPv4 Gateway Address	IPv6 Gateway Address		Resolve
	÷	P-0-0-1	0		00 00	0	Ethernet/IPv4/TCI	00 02 02 02 02 02 02	04 F4 BC 0B 86 2	1	0	192.168.1.1	192.168.6.61			0.0.0.0	::	::	
	÷	P-0-0-1	1		00 00	0	Ethernet/IPv4/TCI	00 02 02 02 02 02 02	04 F4 BC 0B 86 2	1	0	192.168.1.3	192.168.6.61			0.0.0.0	:		Send ARP

2





Please also visit DDOS section of https://xenanetworks.com/other-downloads/

For additional Attacks/Malware traffic captures:

VETRESEC <u>www.netresec.com/?page=PcapFiles</u>



Visit our website:

www.xenanetworks.com

Contact us:

support@xenanetworks.com