Yersinia is a network tool designed to take advantage of some weakness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

It consists of various layer-2 attacks exploiting the weaknesses of different layer-2 protocols. Thus a pentester can identify the vulnerabilities in the deep layer 2 of the network. During pentests, yersinia is used to initiate attacks on layer-2 devices like switches, dhcp servers spanning tree protocols etc. Currently yersinia supports :

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Yersinia Homepage: http://www.yersinia.net/

WARNING !!! Some of the modes in Yersinia creates a Denial Of Service(DOS). Be Careful ! Use only on a test network or with a prior permission.

Options

-h,help	Help screen.
-V,Version	Program version.
-G	Start a graphical GTK session.
-I,interactive	Start an interactive ncurses session.
-D,daemon	Start the network listener for remote
admin (Cisco CLI em	ulation).
-d	Enable debug messages.
-l logfile	Save the current session to the file logfile. If
logfile exists, the da	ta will be appended at the end.
-c conffile	Read/write configuration variables from/to conffile.
-М	Disable MAC spoofing.
GTK GUI	
The GTK GUI (-G) is a GTK graphical interface with all of the
yersinia powerful feat	ures and a professional 'look and feel'.
NCURSES GUI	
The ncurses GUI	(-I) is a ncurses (or curses) based
console where the use	er can take advantage of yersinia powerful features.
Press 'h' to display	the Help Screen and enjoy your session :)
NETWORK DAEMON	
The Network Da	emon (-D) is a telnet based server (ala Cisco mode)
that listens by defaul	t in port 12000/tcp waiting for
incoming telnet conne	ections. It supports a CLI similar to a Cisco
device where the user	(once authenticated) can display different settings
and can launch atta	cks without having yersinia running in her own
machine (especially use	eful Windows users).

Yersinia Home page : <u>http://www.yersinia.net/</u>

Lab 1 : DHCP Salvation using Yersinia NCurses mode

In this lab we flood the dhcp server with dhcp discover packets with spoofed mac address. So the dhcp server grants different ip addresses to all requests and fills up the dhcp pool. There after a new legitimate client requesting an ip address will not receive it. This is known as DHCP Salvation.

For this demo we have a kali linux machine(attacker) and a backtrack machine(target) on a network range 192.168.2.0/24. The dhcp server is running at 192.168.2.1 and has a pool of 254 ips form 192.168.2.1-254.

Command	d: yers	inia -I				
				root@kali: ~		_ = ×
File Edit	View Se	arch Termir	al Help			
yersi	inia 0.7. RootId	3 by Slay	& tomac - STP BridgeId	mode ————— Port	Iface Last see	[18:28:33] n
			- Notification Warning: inte t one - Press any ke	window	ed as the defaul	
You've ç	Total	Packets:	0	STP Packets: 0 -	MAC Spoofin	9 [X]
	Sourc Id 00 Bridg	e MAC GA:2 GO Ver GO eId CBG9.E	23:16:02:FF:08 Type 00 Flags 7CD90117CAA P	Destination MAC 00 RootId 5080.7 ort 8002 Age 0000	01:80:C2:00:00:00 60F0E14AC58 Pathcost 00000 Max 0014 Hello 0002 Fwd 0	9090 909F

<u>Step 1</u> : Launch yersinia in interactive mode.

Yersinia NCurses mode

<u>Step 2</u>: Press h for help. Then change interface to eth0(or your default interface)

Yersinia Options

Press "i" to select the edit interfaces option



Selecting Interface

Step 3: Select DHCP mode by pressing F2 key.

	root@kali: ~											- • ×
File	Edit	View	Search	Termir	al Help							
	yersi	nia 0. SIP 192 192 192 192 192 192	7.3 by 168.2.1 168.2.1 168.2.1 168.2.1 168.2.1 168.2.1 168.2.1	Slay 254 4 254 3 254	& tomac - DIP 192.168.2 192.168.2 192.168.2 192.168.2 192.168.2 192.168.2	DHCP 2.254 2.254 2.4 2.254 2.3	mode MessageType REQUEST ACK REQUEST ACK REQUEST ACK		Iface eth0 eth0 eth0 eth0 eth0 eth0	Last s 21 Oct 21 Oct 21 Oct 21 Oct 21 Oct 21 Oct	een 18:30:53 18:32:17 18:32:17 18:33:27 18:33:27 18:33:27	18:34:24]-
L		Tot	tal Paci	kets:	6	D	HCP Packets:	6	MAG	Spoof	ing [X] —	'
	DHCP I	Fields Sou SIF Op CI CH	9 000.00 01 Hty 000.00 02:48:	C 02:4 30.000 0e 01 3.000. 33:66:	8:33:66:0 .000 DIP HLEN 06 H 000 YI 00 02:51 Ext	2:51 D 255.25 ops 00 00.000. ra)estination MA 55.255.255 SPo) Xid 643C9869 .000.000 SI 00	C FF:FF:FF:FF rt 00068 DPor Secs 0000 Fl 0.000.000.000	:FF:Ff t 0006 ags 80) GI 00	= 57 300 30.000.	000.000	

Yersinia in DHCP Mode

<u>Step 4</u>: Execute Attack by pressing x key and then selecting corresponding sub-attack.

							n	oot@kali: ~				_ 🗆 ×
File B	Edit	View	Search	Termir	nal H	elp						
yersin		ia 0. SIP 192. 192. 192. 192. 192.	.7.3 by .168.2.1 .168.2.1 .168.2.1 .168.2.1 .168.2.1	Slay 2 254 4 254 3 m	<pre>/ & tomac - DHCI DIP 192.168.2.254 192.168.2.2 192.168.2.254 192.168.2.4</pre>			mode MessageType REQUEST ACK REQUEST ACK ATLACK Papel		Iface Last seen eth0 21 Oct 18:30:5 eth0 21 Oct 18:30:5 eth0 21 Oct 18:32:1 eth0 21 Oct 18:32:1 1 Oct 18:32:2	[2 een 18:30:53 18:32:17 18:32:17 18:32:17 18:33:27	18:35:49]
		192.		254	No 0 1 2 3	DoS X X	Desc send send c rea send	ription Hing RAW packet Hing DISCOVER packet ating DHCP rogue ser Hing RELEASE packet	ver	1 Oct	18:33:27	
Those	e str	- Tot range	al Pack	kets						Spoof	ing [X]	
			000.00 01 Hty 000.00 02:48:	C 02:4 00.000 pe 01 0.000 33:66	48:33 9.000 HLEN .000 .02:5	:66:02 DIP 2 06 Ho YI 000 1 Extr	:51 D 55.25 ps 00 .000. a	Destination MAC FF:F4 55.255.255 SPort 0004 3 Xid 643C9869 Secs (0000.000 SI 000.000.0	F:FF:FF:FF 68 DPort 00 0000 Flags 000.000 GI	:FF 9067 8000 000.000.	000.000	

Selecting the type of DHCP attack

Now press 1 key to launch DHCP Discover attack.

						re	oot@kali: ~					- 🗆 X
File	Edit	View	Search	Termin	al Hel	þ						
,	rersi	nia 6 SIP 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	.7.3 by .0.0 .0.0 .0.0 .0.0 .0.0 .0.0 .0.0 .0	Slay	toma DIP 255.25 255.25 255.25 255.25 255.25 255.25 255.25 255.25 255.25 255.25 255.25 255.25 255.25	c - DHCP 5.255.255 5.255.255 5.255.255 5.255.255	mode MessageType DISCOVER DISCOVER DISCOVER DISCOVER DISCOVER DISCOVER DISCOVER DISCOVER DISCOVER DISCOVER		Iface eth0 eth0 eth0 eth0 eth0 eth0 eth0 eth	Last s 21 Oct 21 Oct	een 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20 18:37:20	[18:37:20]-
L		To	tal Pac	kets:	111447	D	HCP Packets:	111447	HA(C Spoof	ing [X] —	
			s urce MA0 P 000.00 01 Htyp 000.000 02:48:	02:4 30.000 0e 01 3.000. 33:66:	8:33:6 .000 D HLEN 0 000 YI 02:51	6:02:51 D IP 255.25 6 Hops 00 000.000. Extra	estination M 5.255.255 SP Xid 643C986 000.000 SI 0	AC FF:FF:FF:FF ort 00068 DPor 9 Secs 0000 Fl 00.000.000.000	:FF:FF t 0000 ags 80 0 GI 00	= 57 300 30.000.	000.000	

Numerous DHCP Discover Packets being sent.

In this you can see all dhcp discover packets being sent from our attacker system. Also check the same on wireshark.

0	apturing from eth0 [W	ireshark 1.10.2 (SVN Rev	51934 from /trunk	-1.10)]	- ×
File Edit View Go	Capture Analyze Stati	istics Telephony Tools	Internals Help		
• • 🖌 🗖 🧟	(🖴 🗎 🗶 C	9. 🗢 🗢 🛧 🗄		o A 🕾 😹 🕅 👯	· ·
Filter:		✓ Expression	n Clear Apply S	Save	
No. Time	Source	Destination	Protocol Lengtl	Info	
108922 14.14466000	0.0.0.0	255.255.255.255	DHCP 286 0	OHCP Discover - Transaction	n ID 0x643
108923 14.14490300	0.0.0.0	255.255.255.255	DHCP 286 0	OHCP Discover - Transaction	n ID 0x643
108924 14.14496700	0.0.0.0	255.255.255.255	DHCP 286 0	OHCP Discover - Transaction	n ID 0x643
108925 14.14505800	0.0.0.0	255.255.255.255	DHCP 286 0	CHCP Discover - Transaction	n ID 0x643
108926 14.14519700	0.0.0.0	255.255.255.255	DHCP 286 0	OHCP Discover - Transaction	n ID Ox643
108927 14.14544900	0.0.0.0	255.255.255.255	DHCP 286 0	OHCP Discover - Transaction	n ID 0x643
108928 14.14551300	0.0.0.0	255.255.255.255	DHCP 286 0	OHCP Discover - Transaction	n ID 0x643
108929 14.14567100	0.0.0.0	255.255.255.255	DHCP 286 [OHCP Discover - Transaction	n ID Ox643
· · · · · · · · · · · · · · · · · · ·	hater and a longe h		1 (0000 bits)	interactions of	
+ Frame 108929: 286	bytes on wire (2288 b)	its), 285 bytes capture	d (2288 bits) on :	interface U	
Ethernet II, Src: Teternet Desternel	9T:TZ:40:3a:ca:8T (9T	:T2:40:3a:ca:8T), UST:	Broadcast (TT:TT:		_
Internet Protocol	teeel Cre Dest, bests	.0 (0.0.0.0), Dst: 200.	.200.200.200 (200.	200,200,200)	
User Datagram Pro Destetras	tocol, Src Port: Dootp	c (68), DSt Port: Dootp	is (67)		
Buutstrap Protoco					
0000 ff f	ff 9f f2 4e 3a ca 8f 0 00 10 11 a9 ce 00 00 0 43 00 fc 9c 25 01 01 0 00 00	08 00 45 10	N:E. .%d< N:5		
😑 赵 eth0: <live captur<="" td=""><td>e in progress> Fil Packe</td><td>ts: 164869 · Displayed: 164</td><td>4869 (100.0%)</td><td>Profile: Default</td><td></td></live>	e in progress> Fil Packe	ts: 164869 · Displayed: 164	4869 (100.0%)	Profile: Default	

DHCP Discover requests being sent seen in Wireshark.

Now wait for 1 minute and try to connect a new client to the network(here a backtrack machine). Any machine (VM or Real) connected to the same network as in that of the attacker machine's selected interface of attack is in(here Kali linux machine with eth0 interface), will do.

t@bt:~# ip a 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000 link/ether 00:0c:29:ef:62:58 brd ff:ff:ff:ff:ff:ff inet6 fe80::20c:29ff:feef:6258/64 scope link valid_lft forever preferred_lft forever oot@bt:~# dhclient eth0 Internet Systems Consortium DHCP Client V3.1.3 Copyright 2004-2009 Internet Systems Consortium. All rights reserved. For info, please visit https://www.isc.org/software/dhcp/ Listening on LPF/eth0/00:0c:29:ef:62:58 LPF/eth0/00:0c:29:ef:62:58 Socket/fallback Sending on Sending on DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8 DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14 DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 21 DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 15 DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3 No DHCPOFFERS received. No working leases in persistent database - sleeping. root@bt: "#

Client Machines denied of IP address.

Here you can see that no default ip was there. Then dhclient(tool for getting ip from DHCP server) was run, but no lease was found. Meaning all ips in the dhcp pool are filled up