Yersinia

Framework for layer 2 attacks
Why Yersinia?

No other bacteria, perhaps organism, had so much of an effect on human history as Yersinia pestis, the bacteria that causes plague.

Many outbreaks of plague have caused death and population reduction throughout history. The most famous, however, was the notorious Black Death of medieval times that killed one third of the population of 14th century Europe. People watched their family and friends die with sickly buboes (swollen lymph nodes) on their necks and a color near black all over their bodies, caused by respiratory failure. People who contracted the disease and were unable to fight it off died within three to five days.

(taken from http://members.aol.com/omaryak/plague/)
Who we are

- Colleagues working in the Information Security Field from Spain.
- Company: S21sec (http://www.s21sec.com)
- Interested in network protocols and how to assess customer networks (or how to protect your networks from the bad guys)
- Open to help the IS community.
Overview

Reasons

- We were tired of doing always the same Layer 2 attacks (ARP Poisoning, CAM Flooding, ...)
- We were tired of watching the same interesting packets flowing in our customers networks and not being able to play with them.
- We were tired of check that, very often, routers and switches configuration are poorly set up and rarely hardened.
- We were tired of seeing theorical attacks against these protocols but without any public information.
- So, it was time for a change 😊
Overview

- Architecture

  - Ncurses GUI
  - Network clients
  - Command line
  - Protocols
  - Yersinia CORE
  - Launched Attacks
  - PCAP Listener
Overview

Features.

- 100% written in C. It uses libpcap, libnet and ncurses.
- Runs in Linux, *BSD and Solaris
- Multithreaded: it supports multiple users and multiple attacks per user.
- Examine, analyze and watch your packets
- Edit each protocol’s fields
- Capture your network data in pcap format.
- **Current protocols enabled**: STP, CDP, DTP, DHCP, HSRP, 802.1Q and VTP.
- Customize your preferences in a configuration file.
- Learn packets from the network and replay them with your modifications.
- Listens to your network!!
- Three main modes: command line, network client and ncurses GUI.
Command line client

Usage

Usage: yersinia [-hVID] [-l logfile] protocol
[protocol_options]
  -V   Program version.
  -h   This help screen.
  -I   Interactive mode (ncurses).
  -D   Daemon mode.
  -l logfile Select logfile.
  -c conffile Select config file.
  protocol Can be one of the following: cdp, dhcp, dot1q,
            dtp, hsrp, stp, vtp.

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers
<yersinia *AT* wasahero.org>
Command line client

Features

- Easy, fast to run
- Friendly shell script integration (pen-testing stuff)
- No fancy $TERM needed, just the command line.
Network client

Usage.

yersinia -D

(-D stands for Daemon)

Features

- Listens to default port 12000/tcp
- Authentication (login & enable)
- CLI similar to Cisco one (with some addons!!!)
- Allows to set up a Yersinia server in each network segment so that the network administrators can assess their networks
- Easy to manage if you have Cisco administration experience
- Help MS Windows users to run Yersinia!! 😊
Ncurses GUI

Usage

yersinia -I

(-I stands for Interactive)

Features

- Fancy, visual, and powerful GUI
- Ncurses compatible with Linux, *BSD and Solaris (curses)
- Examine and analyze your interesting network packets, and learn how to take advantage of the misconfigurations.
- Watch Yersinia’s wonderful features in a glance!
- Beautiful colours 😊
SECOND ACT

Protocols and attacks

Hands on keyboard!
(Rapid) Spanning Tree

Overview.

- Takes care of your network loops
- Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) support
- Two different BPDU formats: Configuration BPDU and TCN BPDU
- No authentication
- Widely implemented in medium/big companies
- Easy to play with
Attacks implemented

- Send a RAW configuration BPDU
- Send a RAW TCN BPDU
- DoS generated by sending different configuration BPDU
- DoS generated by sending different TCN BPDU
- Becoming the Root Role in the Spanning Tree
- Becoming other active switch in the Spanning Tree
- Becoming the Root Role with a MiTM attack
(Rapid) Spanning Tree

STP under Multihomed attack!!

Users

Switch ZIP1

Switch ZAPE

Attacker

Users
(Rapid) Spanning Tree

Mitigations (Cisco only)

- Use **port security and disable STP** in those ports that don't require STP. For information about port security, please check the following url:

- If you are using the portfast feature in your STP configuration, enable also the **BPDU guard** for avoiding these attacks when the port automatically enters the forwarding state:

- Use the **root guard** feature for avoiding rogue devices to become root:
Cisco Discovery Protocol

Overview

- Cisco Proprietary Protocol
- Cisco devices use it for communicating to each other
- It carries some interesting data (IOS Version, Platform, VLAN Domain, ...)

Black Hat Briefings
Cisco Discovery Protocol

- Attacks implemented
  - Sends a RAW CDP packet
  - DoS flooding CDP table (first implemented by FX from Phoenolit)
  - Sets up a virtual device (useless, but can annoy network administrators)
Cisco Discovery Protocol

Thousands of neighbours!!

Switch
ZAPE

Attacker
Cisco Discovery Protocol

- Mitigations
  - Disable CDP 😊
Dynamic Host Configuration Protocol

Overview

- Client / Server model
- Assigns IP Addresses and other network information (DNS servers, gateway, WINS servers, netmask, ...)
- Widely spread
- No authentication
- Can cause a severe damage to an organization
- Uses UDP protocol (port 68/udp and 67/udp)
Dynamic Host Configuration Protocol

- Attacks implemented
  - Sends a RAW packet
  - Sends a DISCOVER
  - Sends an OFFER packet
  - Sends a REQUEST packet
  - Sends a RELEASE packet
  - Sends a DECLINE packet
  - Sends an INFORM packet
  - DoS exhausting available ip address from the DHCP pool
  - Sets up a rogue DHCP Server to configure clients with nasty IP settings (can be used for MiTM attacks or for creating chaos)
Dynamic Host Configuration Protocol

Rogue DHCP Server!!

DHCP Clients

Switch
ZAPE

Attacker

DHCP server
Dynamic Host Configuration Protocol

Mitigations

- Use Port Security (again!)
- DHCP Snooping: set up which interfaces can answer for DHCP requests (trusted/untrusted) For more information, please visit http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a008011c8ac.html
Hot Standby Router Protocol

Overview

- HA model (Active/Passive)
- Plain text authentication (default: cisco)
- Sends datagrams to multicast
- Uses UDP Protocol (port 1985/udp)
Hot Standby Router Protocol

- Attacks implemented
  - Sends a raw HSRP packet
  - Becomes the ACTIVE element with a fake IP address
  - Becomes the ACTIVE element with your real IP address (MiTM)
Hot Standby Router Protocol

New Active Router!!

Switch
ZAPE

Attacker
Hot Standby Router Protocol

Mitigations

- Use MD5 authentication (available from 12.3(2)T)
- IPSEC
Dynamic Trunking Protocol

Overview

- Cisco Proprietary Protocol
- Sets up trunking between switches
- By default, trunking is NEGOTIABLE
Dynamic Trunking Protocol

- Attacks implemented
  - Sends a RAW DTP packet
  - Enables trunking
Dynamic Trunking Protocol

Enabling Trunking!!

Switch
ZAPE

VLAN Servers

Atta
Courier

VLAN Office

Attacker
Dynamic Trunking Protocol

- Mitigations
  - Set all ports to DTP off (no more auto!!)
VLAN Trunking Protocol

Overview

- Cisco Proprietary Protocol
- Allows adding/deleting VLANs from a centralized point
VLAN Trunking Protocol

- Attacks implemented
  - Sends a RAW VTP packet
  - Deletes all VTP vlans
  - Deleting one vlan
  - Adds one vlan
Adding/deleting VLANs!!

Switch
ZAPE

Trunked!!

Attacker
VLAN Office

New VLANs

VLAN Servers

VLAN Trunking Protocol
VLAN Trunking Protocol

Mitigations

- Use a password!!! (we are still trying to find out how the MD5 field works with a password enabled)
- Disable it if not needed
IEEE 802.1Q

Overview

- Needed for passing frames between switches (trunking)
- Adds an extra layer (802.1Q)
- Tags packets with their VLAN Information
IEEE 802.1Q

- Attacks implemented
  - Sends a RAW 802.1Q packet
  - Sends a RAW 802.1Q double encapsulated packet
  - THE VLAN attack, or how to become the VLANs Master!!
IEEE 802.1Q

Sending 802.1Q packets!!

Switch
ZAPE

VLAN Servers

Trunked!!

Attacker

VLAN Office
IEEE 802.1Q

- Mitigations
  - Same as DTP
THIRD ACT

Next steps

One step beyond!
Next steps

- Addition of new layer 2 protocols: ISMP, ISL, VQP/VMS
- Once the framework is totally finished, is time for the research
- Play with more complex network devices and different vendors (currently we are mostly focused on Cisco, since it is easy to get one in Ebay!!!)
- Authors expectations
- We need your help!! (it is becoming such a huge project!)
References / Further Reading

- CDP vulnerability by FX: [http://www.phenoelit.de/stuff/CiscoCDP.txt](http://www.phenoelit.de/stuff/CiscoCDP.txt)
- Vlan gsec paper
References / Further Reading

- Configuring VLAN Trunks:
  [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_2/configide/e_trunk.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_2/configide/e_trunk.htm)

- Cisco frames format:

- Tcpdump. [http://www.tcpdump.org](http://www.tcpdump.org)

- Ethereal: [http://www.ethereal.com](http://www.ethereal.com)

- 802.1q: IEEE standard for local and metropolitan area networks: Virtual Bridged Local Area Networks.

Many thanks for your attention

Alfredo Andres
<slay@wasahero.org>

David Barroso
<tomac@wasahero.org>