THE BRIDGE

CYBER SECURITY

Ataques Man in the Middle

MITM

- **Ejecución ARP Spoofing/ARP Poisoning:**
  - Herramientas:
    - **Ettercap**
      - Ettercap es una suite integral para ataques MITM.
      - https://www.ettercap-project.org/index.html
    - **Wireshark**
      - El analizador de protocolos de red más popular del mundo
      - https://www.wireshark.org/

MITM

Start LIVE DEMO

Wireshark Cheat Sheet

comparitech

Default columns in a packet capture output

No.	Frame number from the beginning of the packet capture
Time	Seconds from the first frame
Source (src)	Source address, commonly an IPv4, IPv6 or Ethernet address
Destination (dst)	Destination address
Protocol	Protocol used in the Ethernet frame, IP packet, or TCP segment
Length	Length of the frame in bytes

Logical Operators

Operator	Description	Example
and or &&	Logical AND	All the conditions should match
or or ||	Logical OR	Either all or one of the condition should match
xor or ^^	Logical XOR	exclusive alternation - Only one of the two conditions should match not both
not or !	NOT(Negation)	Not equal to
[n] [...]	Substring operator	Filter a specific word or text

Filtering packets (Display Filters)

Operator	Description	Example
eq or ==	Equal	ip.dest == 192.168.1.1
ne or !=	Not Equal	ip.dest != 192.168.1.1
gt or >	Greater than	frame.len > 10
lt or <	Less than	frame.len <10
ge or >=	Greater than or Equal	frame.len >= 10
le or <=	Less than or Equal	frame.len<=10

Filter Types

Capture filter	Filter packets during capture
Display Filter	Hide Packets from a capture display

Wireshark Capturing Modes

Promiscuous mode	Sets interface to capture all packets on a network segment to which it is associated to
Monitor mode	setup the Wireless interface to capture all traffic it can receive (Unix/Linux only)

Miscellaneous

Slice Operator	[...] - Range of values
Membership Operator	{} - In
CTRL+E	- Start/Stop Capturing

Capture Filter Syntax

Syntax	protocol	direction	hosts	value	Logical operator	Expressions
Example	tcp	src	192.168.1.1	80	and	tcp dst 202.164.30.1

Display Filter Syntax

Syntax	protocol	String 1	String 2	Comparison Operator	value	logical operator	Expressions
Example	http	dest	ip	==	192.168.1.1	and	tcp port

Keyboard Shortcuts - main display window

Accelerator	Description	Accelerator	Description
Tab or Shift+Tab	Move between screen elements, e.g. from the toolbars to the packet list to the packet detail.	Alt+⟶ or Option+⟶	Move to the next packet in the selection history.
↓	Move to the next packet or detail item.	⟶	In the packet detail, opens the selected tree item.
↑	Move to the previous packet or detail item.	Shift+⟶	In the packet detail, opens the selected tree item and all of its subtrees.
Ctrl+ ↓ or F8	Move to the next packet, even if the packet list isn't focused.	Ctrl+⟶	In the packet detail, opens all tree items.
Ctrl+ ↑ or F7	Move to the previous packet, even if the packet list isn't focused.	Ctrl+⟵	In the packet detail, closes all tree items.
Ctrl+.	Move to the next packet of the conversation (TCP, UDP or IP).	Backspace	In the packet detail, jumps to the parent node.
Ctrl+,	Move to the previous packet of the conversation (TCP, UDP or IP).	Return or Enter	In the packet detail, toggles the selected tree item.

Protocols - Values

ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp

MITM

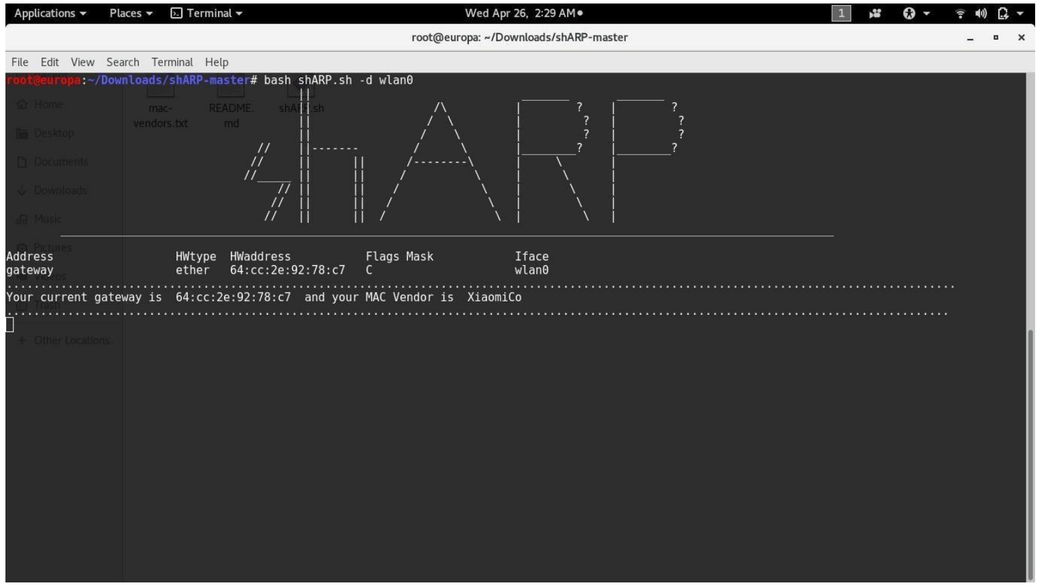
Common Filtering commands			
Usage	**Filter syntax**	**Usage**	**Filter syntax**
Wireshark Filter by IP	ip.addr == 10.10.50.1	Filter by URL	http.host == “host name”
Filter by Destination IP	ip.dest == 10.10.50.1	Filter by time stamp	frame.time >= “June 02, 2019 18:04:00”
Filter by Source IP	ip.src == 10.10.50.1	Filter SYN flag	tcp.flags.syn == 1
Filter by IP range	ip.addr >= 10.10.50.1 and ip.addr <= 10.10.50.100		tcp.flags.syn == 1 and tcp.flags.ack == 0
Filter by Multiple Ips	ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100	Wireshark Beacon Filter	wlan.fc.type_subtype = 0x08
Filter out IP address	!(ip.addr == 10.10.50.1)	Wireshark broadcast filter	eth.dst == ff:ff:ff:ff:ff:ff
Filter subnet	ip.addr == 10.10.50.1/24	Wireshark multicast filter	(eth.dst[0] & 1)
Filter by port	tcp.port == 25	Host name filter	ip.host = hostname
Filter by destination port	tcp.dstport == 23	MAC address filter	eth.addr == 00:70:f4:23:18:c4
Filter by ip address and port	ip.addr == 10.10.50.1 and Tcp.port == 25	RST flag filter	tcp.flags.reset == 1

Main toolbar items							
Toolbar Icon	**Toolbar Item**	**Menu Item**	**Description**	**Toolbar Icon**	**Toolbar Item**	**Menu Item**	**Description**
	Start	Capture → Start	Uses the same packet capturing options as the previous session, or uses defaults if no options were set		**Go Forward**	Go → Go Forward	Jump forward in the packet history
	Stop	Capture → Stop	Stops currently active capture		**Go to Packet...**	Go → Go to Packet...	Go to specific packet
	Restart	Capture → Restart	Restarts active capture session		**Go To First Packet**	Go → First Packet	Jump to first packet of the capture file
	Options...	Capture → Options...	Opens “Capture Options” dialog box		**Go To Last Packet**	Go → Last Packet	Jump to last packet of the capture file
	Open...	File → Open...	Opens "File open" dialog box to load a capture for viewing		**Auto Scroll in Live Capture**	View → Auto Scroll in Live Capture	Auto scroll packet list during live capture
	Save As...	File → Save As...	Save current capture file		**Colorize**	View → Colorize	Colorize the packet list (or not)
	Close	File → Close	Close current capture file		**Zoom In**	View → Zoom In	Zoom into the packet data (increase the font size)
	Reload	View → Reload	Reloads current capture file		**Zoom Out**	View → Zoom Out	Zoom out of the packet data (decrease the font size)
	Find Packet...	Edit → Find Packet...	Find packet based on different criteria		**Normal Size**	View → Normal Size	Set zoom level back to 100%
	Go Back	Go → Go Back	Jump back in the packet history		**Resize Columns**	View → Resize Columns	Resize columns, so the content fits to the width

Resource: Wireshark Docs https://www.wireshark.org/docs/wsug_html_chunked/

MITM

- **Herramienta para defendernos de un Man In the Middle**
  - **Anti ARP Spoofing/ARP Poisoning**
    - **Software anti ARP Spoofing/ARP Poisoning:**
      - https://github.com/europa502/shARP
    - **shARP es capaz de detectar la presencia de un tercero en una red privada de manera activa.**
    - **Este escrito en bash, por lo que es compatible con muchos sistemas operativos.**
    - **Modos de funcionamiento:**
      - El **modo defensivo,** proteger al usuario final del ataque, desconectando de la red al propio usuario, y alertarle a través de los altavoces del sistema. Alerta de que alguien está realizando un ataque en la red, y se desconectara para protegernos
      - El **modo ofensivo** lo que hace es desconectar el sistema del usuario de la red, y envía paquetes de des autenticación al atacante, lo que le impide realizar otros ataques hasta que paremos el propio programa



https://null-byte.wonderhowto.com/forum/prevent-your-network-from-being-arp-spoofed-with-sharp-0181104/


THE
BRIDGE