

The image shows a Kali Linux desktop environment with two virtual machines (VMs) running. The top VM is running Wireshark, displaying a packet capture of an ICMP Echo (ping) request from 192.168.1.10 to 192.168.1.1. The bottom VM is running a terminal with a netstat command output showing active connections to 192.168.1.1.

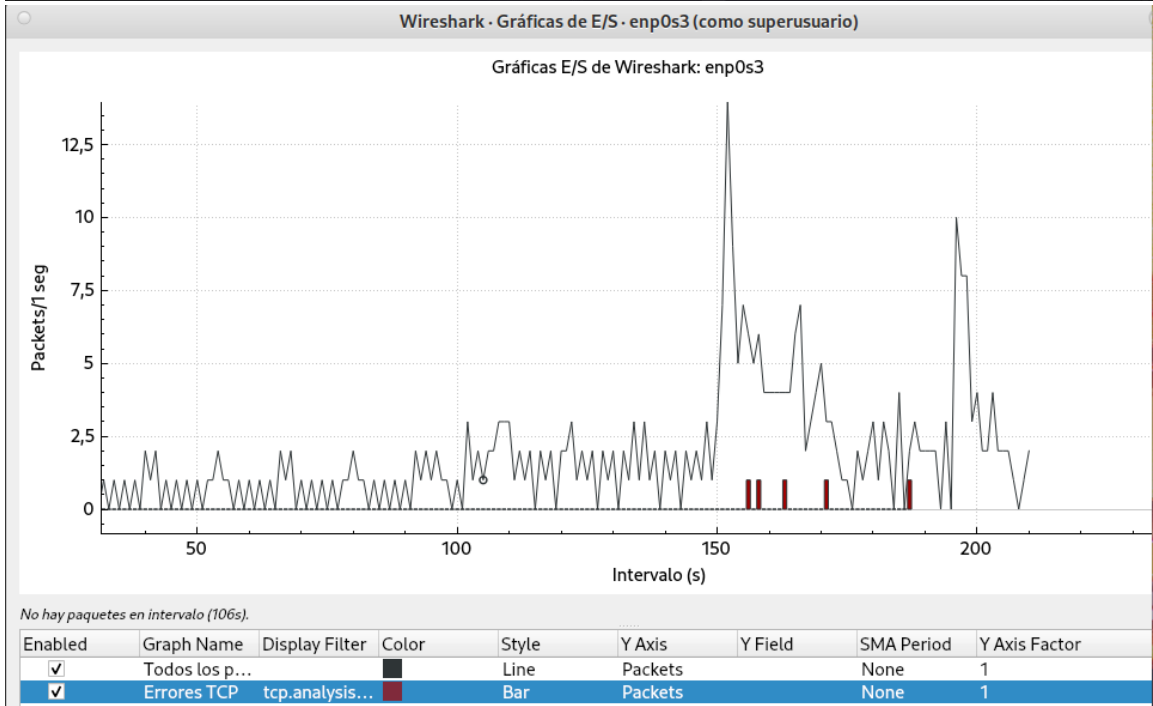
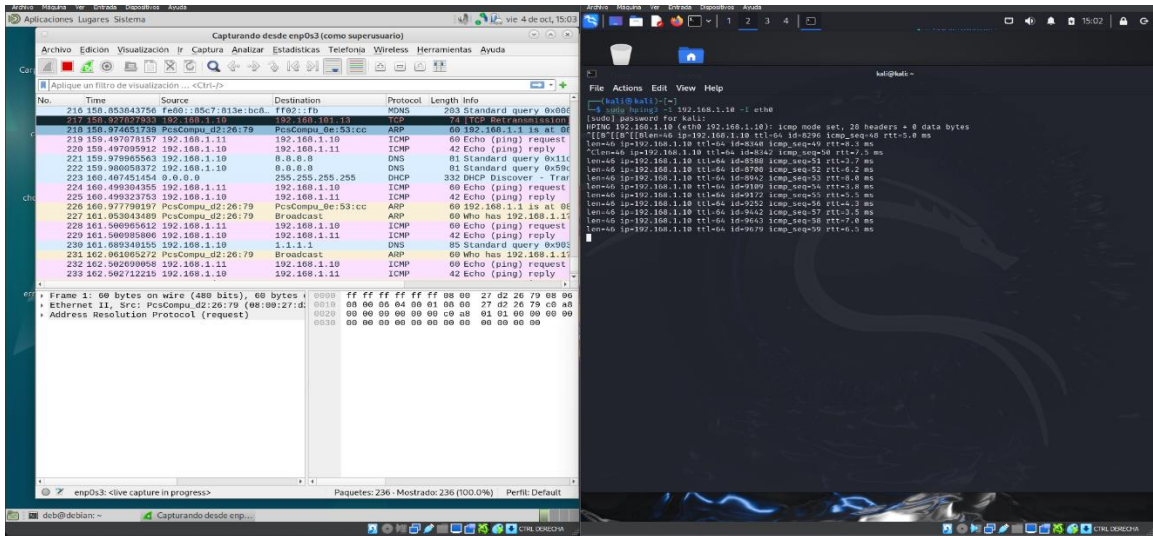
**Top VM (Wireshark):**

- File: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
- Ethernet II, Src: PcsCompu\_de:53:cc, Dst: 192.168.1.1
- Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
- ICMP Echo (ping) request, Seq=0

**Bottom VM (Terminal):**

```

root@kali:~# netstat -tlnp
Active Internet connections (only TCP)
tcp        0 0 0.0.0.0:22        0.0.0.0:22        LISTENING   *
tcp        0 0 192.168.1.1:22   192.168.1.1:22    LISTENING   sshd: root@
tcp        0 0 192.168.1.1:80   192.168.1.1:80    LISTENING   *:
tcp        0 0 192.168.1.1:443  192.168.1.1:443   LISTENING   *:
tcp        0 0 192.168.1.1:555  192.168.1.1:555   LISTENING   *:
tcp        0 0 192.168.1.1:556  192.168.1.1:556   LISTENING   *:
tcp        0 0 192.168.1.1:557  192.168.1.1:557   LISTENING   *:
tcp        0 0 192.168.1.1:558  192.168.1.1:558   LISTENING   *:
tcp        0 0 192.168.1.1:559  192.168.1.1:559   LISTENING   *:
tcp        0 0 192.168.1.1:560  192.168.1.1:560   LISTENING   *:
tcp        0 0 192.168.1.1:561  192.168.1.1:561   LISTENING   *:
tcp        0 0 192.168.1.1:562  192.168.1.1:562   LISTENING   *:
tcp        0 0 192.168.1.1:563  192.168.1.1:563   LISTENING   *:
tcp        0 0 192.168.1.1:564  192.168.1.1:564   LISTENING   *:
tcp        0 0 192.168.1.1:565  192.168.1.1:565   LISTENING   *:
tcp        0 0 192.168.1.1:566  192.168.1.1:566   LISTENING   *:
tcp        0 0 192.168.1.1:567  192.168.1.1:567   LISTENING   *:
tcp        0 0 192.168.1.1:568  192.168.1.1:568   LISTENING   *:
tcp        0 0 192.168.1.1:569  192.168.1.1:569   LISTENING   *:
tcp        0 0 192.168.1.1:570  192.168.1.1:570   LISTENING   *:
tcp        0 0 192.168.1.1:571  192.168.1.1:571   LISTENING   *:
tcp        0 0 192.168.1.1:572  192.168.1.1:572   LISTENING   *:
tcp        0 0 192.168.1.1:573  192.168.1.1:573   LISTENING   *:
tcp        0 0 192.168.1.1:574  192.168.1.1:574   LISTENING   *:
tcp        0 0 192.168.1.1:575  192.168.1.1:575   LISTENING   *:
tcp        0 0 192.168.1.1:576  192.168.1.1:576   LISTENING   *:
tcp        0 0 192.168.1.1:577  192.168.1.1:577   LISTENING   *:
tcp        0 0 192.168.1.1:578  192.168.1.1:578   LISTENING   *:
tcp        0 0 192.168.1.1:579  192.168.1.1:579   LISTENING   *:
tcp        0 0 192.168.1.1:580  192.168.1.1:580   LISTENING   *:
tcp        0 0 192.168.1.1:581  192.168.1.1:581   LISTENING   *:
tcp        0 0 192.168.1.1:582  192.168.1.1:582   LISTENING   *:
tcp        0 0 192.168.1.1:583  192.168.1.1:583   LISTENING   *:
tcp        0 0 192.168.1.1:584  192.168.1.1:584   LISTENING   *:
tcp        0 0 192.168.1.1:585  192.168.1.1:585   LISTENING   *:
tcp        0 0 192.168.1.1:586  192.168.1.1:586   LISTENING   *:
tcp        0 0 192.168.1.1:587  192.168.1.1:587   LISTENING   *:
tcp        0 0 192.168.1.1:588  192.168.1.1:588   LISTENING   *:
tcp        0 0 192.168.1.1:589  192.168.1.1:589   LISTENING   *:
tcp        0 0 192.168.1.1:590  192.168.1.1:590   LISTENING   *:
tcp        0 0 192.168.1.1:591  192.168.1.1:591   LISTENING   *:
tcp        0 0 192.168.1.1:592  192.168.1.1:592   LISTENING   *:
tcp        0 0 192.168.1.1:593  192.168.1.1:593   LISTENING   *:
tcp        0 0 192.168.1.1:594  192.168.1.1:594   LISTENING   *:
tcp        0 0 192.168.1.1:595  192.168.1.1:595   LISTENING   *:
tcp        0 0 192.168.1.1:596  192.168.1.1:596   LISTENING   *:
tcp        0 0 192.168.1.1:597  192.168.1.1:597   LISTENING   *:
tcp        0 0 192.168.1.1:598  192.168.1.1:598   LISTENING   *:
tcp        0 0 192.168.1.1:599  192.168.1.1:599   LISTENING   *:
tcp        0 0 192.168.1.1:600  192.168.1.1:600   LISTENING   *:
tcp        0 0 192.168.1.1:601  192.168.1.1:601   LISTENING   *:
tcp        0 0 192.168.1.1:602  192.168.1.1:602   LISTENING   *:
tcp        0 0 192.168.1.1:603  192.168.1.1:603   LISTENING   *:
tcp        0 0 192.168.1.1:604  192.168.1.1:604   LISTENING   *:
tcp        0 0 192.168.1.1:605  192.168.1.1:605   LISTENING   *:
tcp        0 0 192.168.1.1:606  192.168.1.1:606   LISTENING   *:
tcp        0 0 192.168.1.1:607  192.168.1.1:607   LISTENING   *:
tcp        0 0 192.168.1.1:608  192.168.1.1:608   LISTENING   *:
tcp        0 0 192.168.1.1:609  192.168.1.1:609   LISTENING   *:
tcp        0 0 192.168.1.1:610  192.168.1.1:610   LISTENING   *:
tcp        0 0 192.168.1.1:611  192.168.1.1:611   LISTENING   *:
tcp        0 0 192.168.1.1:612  192.168.1.1:612   LISTENING   *:
tcp        0 0 192.168.1.1:613  192.168.1.1:613   LISTENING   *:
tcp        0 0 192.168.1.1:614  192.168.1.1:614   LISTENING   *:
tcp        0 0 192.168.1.1:615  192.168.1.1:615   LISTENING   *:
tcp        0 0 192.168.1.1:616  192.168.1.1:616   LISTENING   *:
tcp        0 0 192.168.1.1:617  192.168.1.1:617   LISTENING   *:
tcp        0 0 192.168.1.1:618  192.168.1.1:618   LISTENING   *:
tcp        0 0 192.168.1.1:619  192.168.1.1:619   LISTENING   *:
tcp        0 0 192.168.1.1:620  192.168.1.1:620   LISTENING   *:
tcp        0 0 192.168.1.1:621  192.168.1.1:621   LISTENING   *:
tcp        0 0 192.168.1.1:622  192.168.1.1:622   LISTENING   *:
tcp        0 0 192.168.1.1:623  192.168.1.1:623   LISTENING   *:
tcp        0 0 192.168.1.1:624  192.168.1.1:624   LISTENING   *:
tcp        0 0 192.168.1.1:625  192.168.1.1:625   LISTENING   *:
tcp        0 0 192.168.1.1:626  192.168.1.1:626   LISTENING   *:
tcp        0 0 192.168.1.1:627  192.168.1.1:627   LISTENING   *:
tcp        0 0 192.168.1.1:628  192.168.1.1:628   LISTENING   *:
tcp        0 0 192.168.1.1:629  192.168.1.1:629   LISTENING   *:
tcp        0 0 192.168.1.1:630  192.168.1.1:630   LISTENING   *:
tcp        0 
```



```
deb@debian:~/Escritorio$ cat detalles\wireshark
# This file was created by Wireshark. Edit with care.
#@Bad TCP@tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack@[4626,10023,11822][63479,34695,34695]
#@SRP State Change@srp.state != 0 && hsrp.state != 168@[4626,10023,11822][65535,64764,40092]
#@Spanning Tree Topology Change@stp.type == 0x00@[4626,10023,11822][65535,64764,40092]
#@OSPF State Change@ospf.msg != 1@[4626,10023,11822][65535,64764,40092]
#@ICMP errors@icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }@[4626,10023,11822][47031,63479,29812]
#@ARP@arp@[64250,61680,55255][4626,10023,11822]
#@ICMP@icmp || icmpv6@[64764,57568,65535][4626,10023,11822]
#@TCP RST@tcp.flags.reset eq 1@[42148,0,0][65535,64764,40092]
#@SCTP ABORT@sctp.chunk_type eq ABORT@[42148,0,0][65535,64764,40092]
#@TTL low or unexpected@ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !{vrrp || carp})@[42148,0,0][60652,61680,60395]
#@Checksum Errors@eth.fc.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" || mstp.checksum.status=="Bad" || cdp.checksum.status=="Bad" || edp.checksum.status=="Bad" || wlan.fc.status=="Bad" || stt.checksum.status=="Bad"@[4626,10023,11822][63479,34695,34695]
#@SMB@smb || nbss || nbns || netbios@[65278,65535,53456][4626,10023,11822]
#@HTTP@http || tcp.port == 80 || http2@[58596,65535,51143][4626,10023,11822]
#@DCERPC@dcercp@[51143,38807,65535][4626,10023,11822]
#@Routing@hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp@[65535,62451,54998][4626,10023,11822]
#@TCP SYN/FIN@tcp.flags & 0x02 || tcp.flags.fin == 1@[41120,41120,41120][4626,10023,11822]
#@TCP@tcp@[59367,59110,65535][4626,10023,11822]
#@UDP@udp@[56026,61166,65535][4626,10023,11822]
#@Broadcast@eth[0] & 1@[65535,65535,65535][47802,48573,46774]
#@System Events@systemd_journal || sysdlog@[59110,59110,59110][11565,28527,39578]
```

## 1. Monitoreo del tráfico de red con Wireshark (Máquina Debian)

- a) En **Wireshark**, se están capturando paquetes ARP y ICMP (peticiones y respuestas de ping). El análisis está orientado a observar la resolución de direcciones (ARP) y la respuesta de las máquinas a peticiones ICMP (ping).
- b) La gráfica de **Wireshark** muestra un análisis de tráfico TCP en términos de paquetes por segundo y errores detectados.
- c) Esta herramienta es útil para monitorear cómo se comporta una red bajo un ataque ARP spoofing o DoS, ya que permite detectar flujos anormales de paquetes o intentos de suplantación de identidad en la red.

## 2. Ataque de ARP Spoofing con Kali Linux

- En la terminal de **Kali Linux**, se está utilizando la herramienta **arpsoof** para generar tráfico ARP falso en la red. Estás haciendo que las máquinas dentro de la red crean que el atacante (Kali Linux) es en realidad el router o el destino legítimo (192.168.1.1).

## 3. Discusión sobre Estrategias de Mitigación

- a) El uso de **Wireshark** y **ARP spoof** es excelente para aprender a detectar y mitigar ataques en redes locales.
- b) Para un servidor de **WordPress** u otros servicios, las siguientes medidas podrían ser efectivas contra ataques ARP Spoofing y DoS:
  - **Firewalls de red:** Configurar reglas de filtrado de tráfico en el firewall para limitar el tráfico anormal y bloquear intentos de spoofing.
  - **ARP Inspection:** Implementar técnicas como **Dynamic ARP Inspection (DAI)** para validar las respuestas ARP y evitar ataques de suplantación.
  - **Limitar la tasa de paquetes ICMP:** Configurar firewalls o herramientas de mitigación para limitar las tasas de paquetes ICMP para evitar que se utilicen en ataques de denegación de servicio.
  - **IDS/IPS:** Un sistema de detección o prevención de intrusos (IDS/IPS) puede ayudar a identificar y bloquear intentos de ataques ARP Spoofing.

## 4. Conclusión: Buenas Prácticas para Proteger WordPress

- Mantener actualizado el software del servidor y del sitio WordPress.
- Implementar **WAF (Web Application Firewall)** y filtros contra ataques DoS.
- Configurar correctamente las reglas de firewall para bloquear tráfico malicioso y conexiones anormales.