

The screenshot shows a Linux desktop with the following elements:

- Top Bar:** Displays the title "localhost:5900 (QEMU (UbuntuDesktopGuest22.04-1)) - RealVNC Viewer" and the date/time "Feb 17 20:28".
- Activities Panel:** Located on the left, showing various application icons.
- Ettercap Application:**
 - Window Title:** "Ettercap 0.8.3.1 (EB)"
 - Host List:** A table with the following data:

IP Address	MAC Address	Description
192.168.122.1	52:54:00:AC:52:A3	
192.168.122.34	02:42:3A:E7:8B:00	
192.168.122.83	02:42:CC:7B:D9:00	
192.168.122.93	02:42:90:0D:4F:00	
192.168.122.236	0C:A3:06:D4:00:00	
192.168.122.254	02:42:48:11:EB:00	
 - Buttons:** "Delete Host", "Add to Target 1", and "Add to Target 2".
 - Status Bar:** Shows "Packets: 63 · Displayed: 63 (100.0%) · Dropped: 0 (0.0%)".

Filter "String" and input username or password in the search.

The screenshot shows the Wireshark interface with the following details:

- Filter:** http
- Packet list:** A table of captured packets on interface ens3.
- Packet details:** A hierarchical view of the selected packet (No. 31).
- Packet bytes:** A view of the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
31	17.236111626	192.168.122.236	44.228.249.3	HTTP	362	GET /login.php HTTP/1.1
36	17.284530382	44.228.249.3	192.168.122.236	HTTP	1366	HTTP/1.1 200 OK (text/html)
42	17.330574599	192.168.122.236	44.228.249.3	HTTP	413	GET /Flash/add.swf HTTP/1.1
83	17.433044930	44.228.249.3	192.168.122.236	HTTP	108	HTTP/1.1 200 OK (application/x-shockwave-flash)
139	25.867696259	192.168.122.236	44.228.249.3	HTTP	508	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
144	25.915075221	44.228.249.3	192.168.122.236	HTTP	342	HTTP/1.1 302 Found (text/html)
149	25.927049763	192.168.122.236	44.228.249.3	HTTP	409	GET /login.php HTTP/1.1
154	25.971785862	44.228.249.3	192.168.122.236	HTTP	1366	HTTP/1.1 200 OK (text/html)
161	26.026270584	192.168.122.236	44.228.249.3	HTTP	413	GET /Flash/add.swf HTTP/1.1
198	26.132061987	44.228.249.3	192.168.122.236	HTTP	108	HTTP/1.1 200 OK (application/x-shockwave-flash)

Packet details for No. 31:

- Frame 31: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface ens3, id 0
- Ethernet II, Src: 0c:a3:06:d4:00:00 (0c:a3:06:d4:00:00), Dst: 0c:19:11:73:00:00 (0c:19:11:73:00:00)
- Internet Protocol Version 4, Src: 192.168.122.236, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 51548, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
- Hypertext Transfer Protocol

Packet bytes:

```
0000 0c 19 11 73 00 00 0c a3 06 d4 00 00 08 00 45 00 ...s...E
0010 01 5c 6a 88 40 00 40 06 6d 97 c0 a8 7a ec 2c e4 ...j...m...Z...
0020 f9 03 c9 5c 00 50 d2 2e cb b4 aa dd e8 be 80 18 ...P...
0030 03 91 20 47 00 00 01 01 08 0a 00 00 a1 46 17 29 ...G...F)
0040 c0 14 47 45 54 20 2f 6c 6f 67 69 6e 2e 70 68 70 ...GET /L ogin.php
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a ...HTTP/1.1 Host:
0060 20 74 65 73 74 70 68 70 2e 76 75 6e 6e 77 65 62 ...testphp.vulnweb
0070 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 ...com Us er-Agent
0080 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 ...: Mozilla/5.0 (X
0090 31 31 3b 20 4c 69 6e 75 78 20 69 36 38 36 3b 20 ...11; Linu x i686;
00a0 72 76 3a 33 33 2e 30 29 20 47 65 63 6b 6f 2f 32 ...rv:33.0) Gecko/2
00b0 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f ...0100101 Firefox/
00c0 33 33 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 ...33.0 Ac cept: te
```

The ARP poisoning is sending ARP replies to both the Firefox VM and the NAT node. This tricks both systems into thinking they are sending packets to the "right" MAC address when they are actually being intercepted by the Ubuntu VM. In the Firefox VM, we go onto an HTTP website which is unencrypted. The Ubuntu VM is able to intercept the HTTP request which Wireshark is able to display. Through Wireshark, it is possible to see the packet details which include the username and password. This issue definitely poses a risk in enterprise settings as it is a breach in confidentiality. Credential theft can be extremely damaging, especially in the sense of admin logins. Intercepted traffic can also potentially be modified which creates a loss of data integrity as well.