A. 08:00:27:11:cf:53
B. 10.0.2.15
C. 08:00:27:1a:45:12
D. 10.0.2.4
E.
```
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt If
ace
default         10.0.2.1        0.0.0.0         UG        0 0          0 et
h0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 et
h0
```
F.
```
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask
Iface
10.0.2.2                 ether   52:54:00:12:35:00   C
eth0
10.0.2.1                 ether   52:54:00:12:35:00   C
eth0
10.0.2.3                 ether   08:00:27:f1:23:27   C
eth0
10.0.2.4                 ether   08:00:27:1a:45:12   C
```
G.
```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
```
H.
```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   08:00:27:11:CF:53   C                     eth0
10.0.2.15                ether   08:00:27:11:CF:53   C                     eth0
```
I. 52:54:00:12:35:00, because it corresponds to the gateway of default destination.
J. I saw http response from the website on metasploitable, but no packet captured on Kali.
K.
L. Different ip addresses are paired with the same MAC address, indicating that arp poisoning has taken place.
```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   08:00:27:11:CF:53   C                     eth0
10.0.2.15                ether   08:00:27:11:CF:53   C                     eth0
10.0.2.1                 ether   08:00:27:11:CF:53   C                     eth0
```
M. 08:00:27:11:CF:53. It is the new MAC address associated with the default destination 10.0.2.1.
N.
O. Yes, I saw HTTP response, and I saw captured packets on Wireshark. I can tell get response is from Kali, and OK response is from the website.
P. The attacker produced fake responses that changed paired some ip addresses with wrong MAC addresses, sent to Metasploitable, and thus updated its arp cache.
Q. Let it check if an incoming response contains conflicting ip-MAC addresses pairs with what is in the arp cache. It will generate false positives if an ip address has indeed been associated with a new MAC address.