[illegible] CEH [illegible] 32 –

[illegible] CEH ([illegible]): [illegible] ARP [illegible] MAC [illegible]

[illegible] ARP [illegible] ARP [illegible]. [illegible] ARP [illegible]. [illegible] Bogus ARP [illegible]. [illegible] ARP [illegible]. [illegible].

[illegible] CEH [illegible].

[illegible]

[illegible]. [illegible] (collision domain) [illegible]. [illegible]. [illegible]

[illegible] SSL [illegible] SSH [illegible]. [illegible] HTTP [illegible] FTP [illegible].

[illegible]

[illegible]. [illegible]. [illegible]. [illegible]:

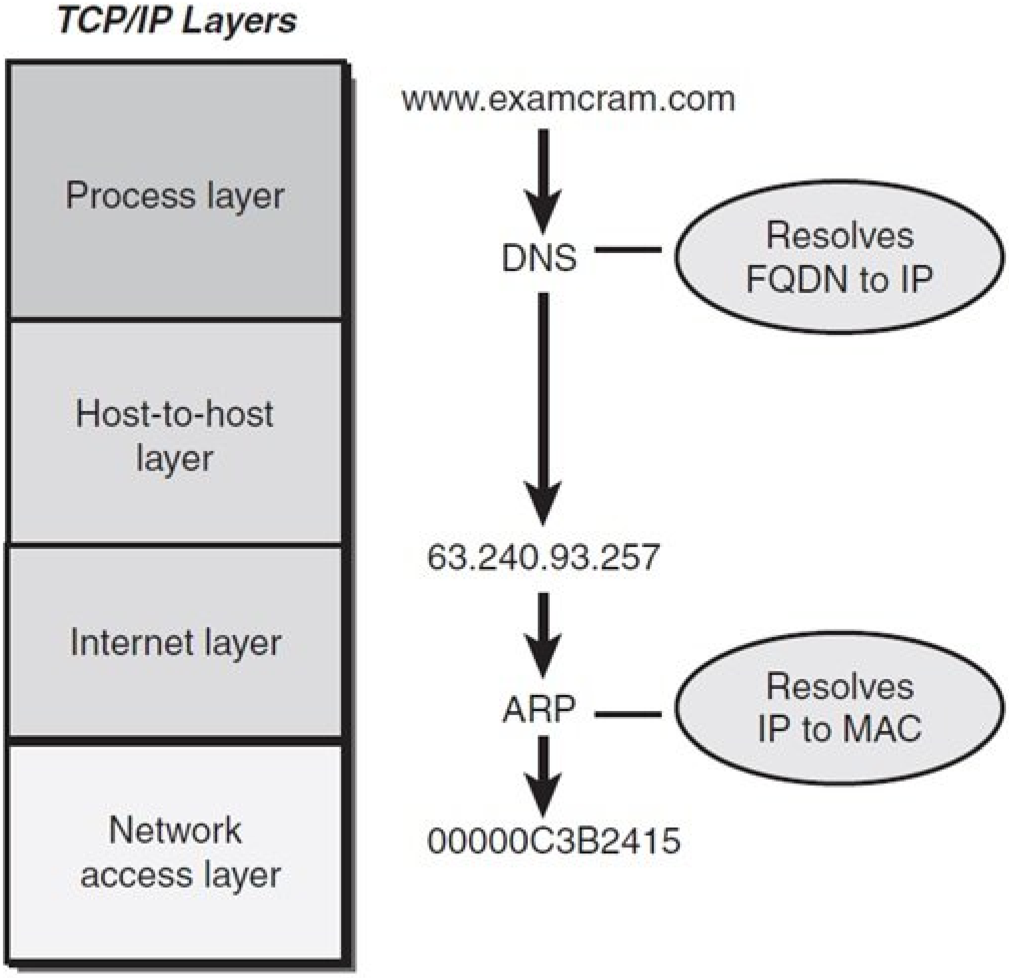
- Address Resolution Protocol (ARP) poisoning
- Media Access Control (MAC) flooding
- Rogue DHCP servers
- Spoofing
- DNS poisoning

[illegible] ARP [illegible] ARP [illegible].

[illegible]: [illegible] CEH [illegible] (promiscuous mode) [illegible].

Address Resolution Protocol

ARP [illegible] (DNS) [illegible]. DNS [illegible] ARP [illegible]. ARP [illegible]. DNS [illegible] ARP [illegible]. [illegible] TCP / IP [illegible].



ARP [illegible]. ARP [illegible]. ARP [illegible]:

1. [illegible] :ARP [illegible] A [illegible] "[illegible]"

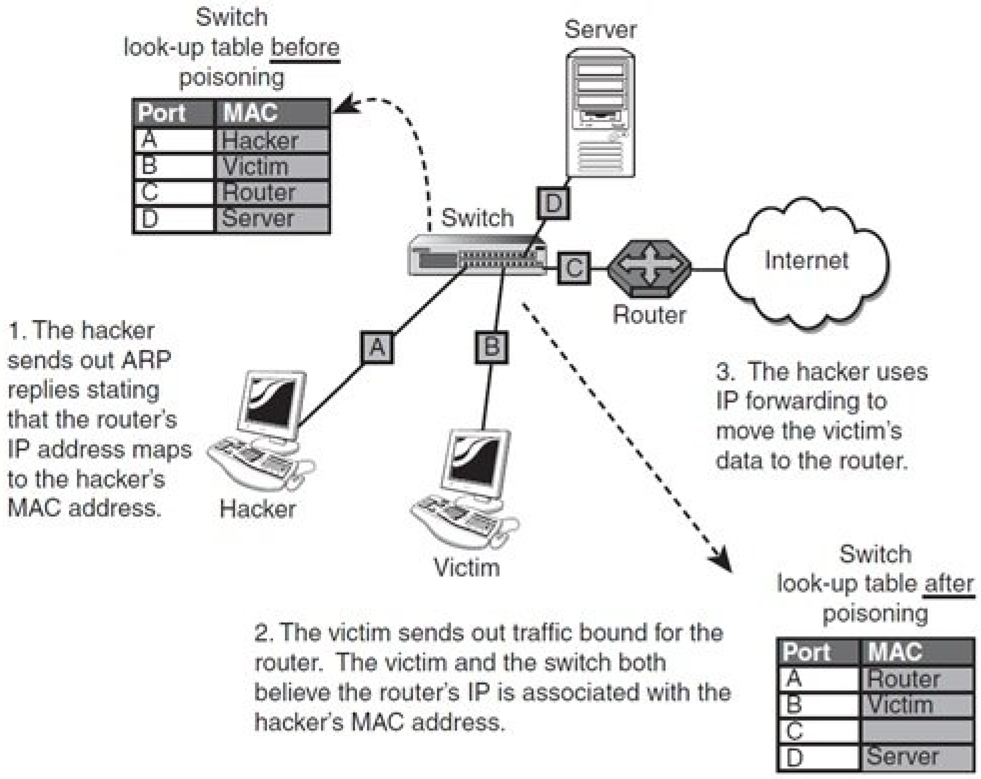
2. [illegible] :ARP [illegible] B [illegible] A [illegible]: "[illegible]. XYZ [illegible]."

[illegible] ARP [illegible] ARP [illegible] ARP [illegible] ARP [illegible] ARP [illegible] ARP [illegible] ARP [illegible] 2 [illegible] 15 [illegible] arp -a [illegible] ARP [illegible].

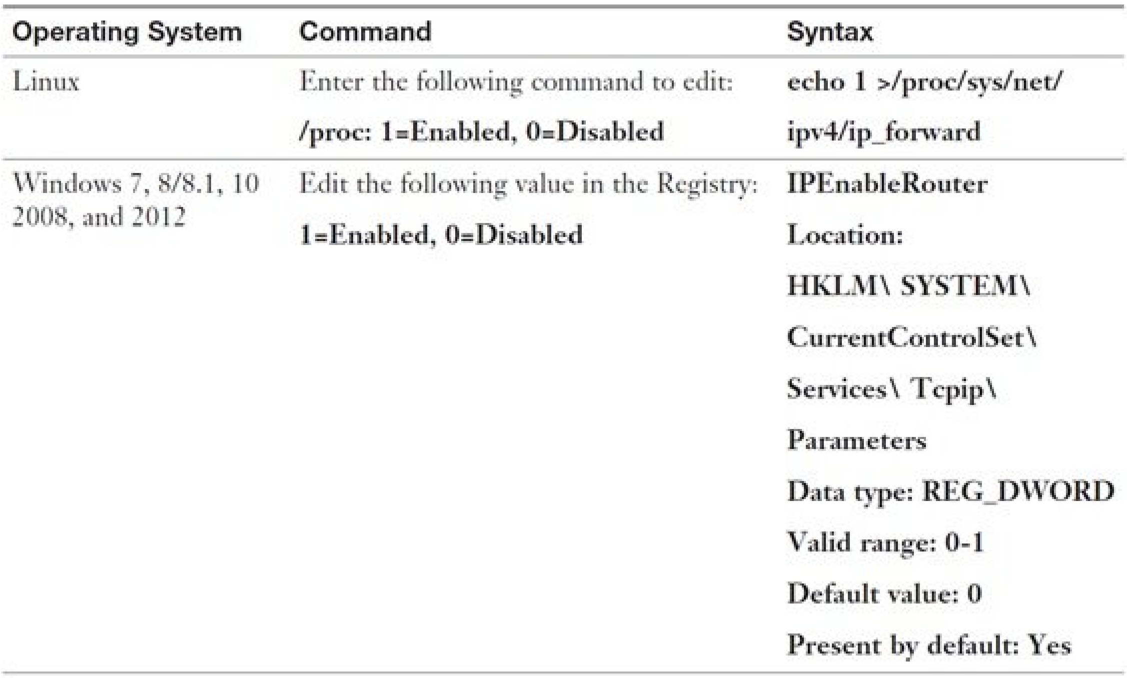
[illegible] ARP [illegible] MAC

[illegible] ARP [illegible] ARP [illegible] ARP [illegible] Bogus ARP [illegible] ARP [illegible].

[illegible] ARP [illegible]:


Switch
look-up table before
poisoning
Port | MAC
A | Hacker
B | Victim
C | Router
D | Server
Server
Switch
D
C
A
B
Router
Internet
1. The hacker sends out ARP replies stating that the router's IP address maps to the hacker's MAC address.
Hacker
Victim
3. The hacker uses IP forwarding to move the victim's data to the router.
2. The victim sends out traffic bound for the router. The victim and the switch both believe the router's IP is associated with the hacker's MAC address.
Switch
look-up table after
poisoning
Port | MAC
A | Router
B | Victim
C |
D | Server

[illegible] IP [illegible].



Operating System	Command	Syntax
Linux	Enter the following command to edit: **/proc: 1=Enabled, 0=Disabled**	**echo 1 >/proc/sys/net/ipv4/ip_forward**
Windows 7, 8/8.1, 10 2008, and 2012	Edit the following value in the Registry: **1=Enabled, 0=Disabled**	**IPEnableRouter** **Location:** **HKLM\ SYSTEM\ CurrentControlSet\ Services\ Tcpip\ Parameters** **Data type: REG_DWORD** **Valid range: 0-1** **Default value: 0** **Present by default: Yes**

[illegible] ARP [illegible].

- Cain and Abel: [illegible] ARP [illegible]. [illegible] ARP، [illegible] ARP [illegible].

- Ufasoft Snif: [illegible].

- WinARPAttacker: [illegible].

- Ettercap: [illegible] ARP، [illegible] grabber [illegible]. [illegible] ettercap -Nzs [illegible] Ettercap [illegible] (N-) [illegible] z- [illegible] ARP [illegible] s- [illegible] WinDump [illegible] TCPdump [illegible] q [illegible] Ettercap [illegible] C- [illegible]:

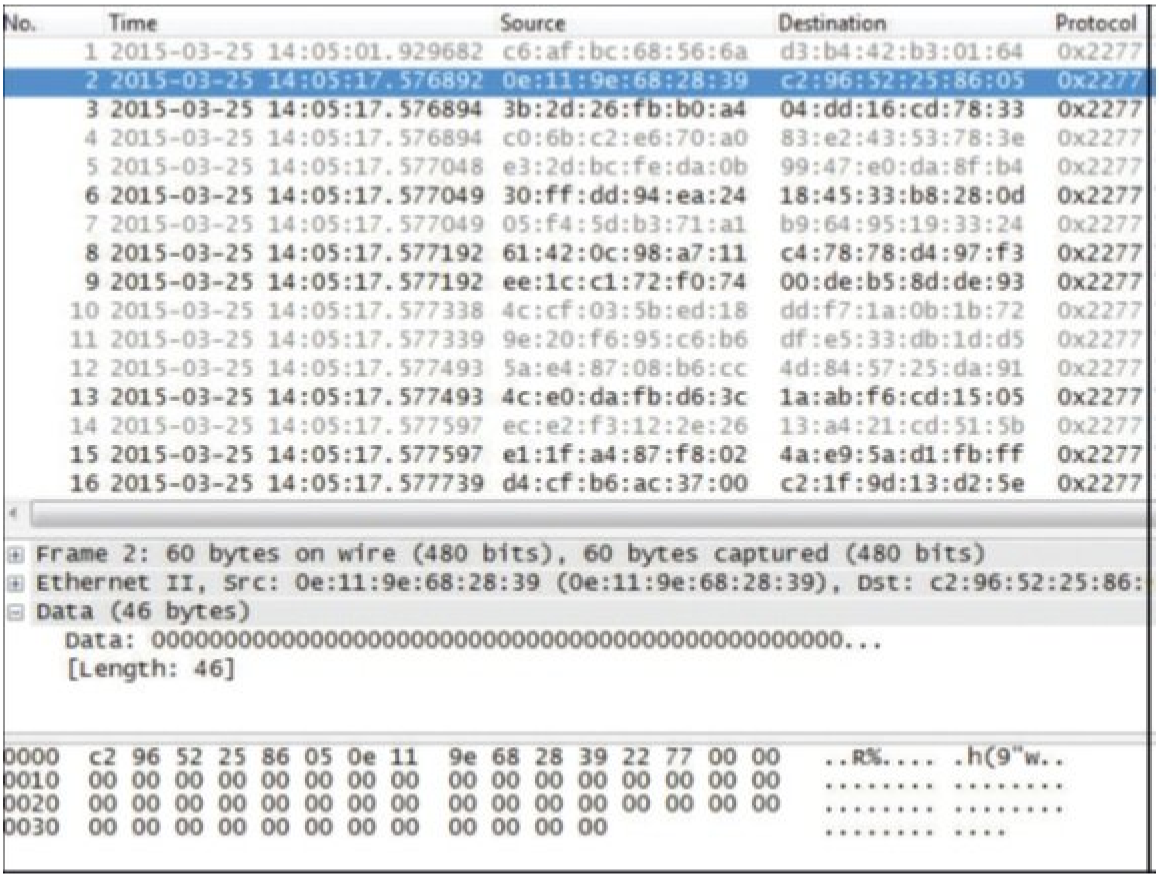
N [illegible]

z [illegible] ARP [illegible].

a [illegible].

[illegible]: Ettercap [illegible] ARP [illegible]. [illegible] a- [illegible] s- [illegible] <ettercap -Nza <srcIP> <destIP> <srcMAC> <destMAC [illegible].

[illegible] (CAM) [illegible] content addressable memory [illegible]. [illegible] CAM [illegible].



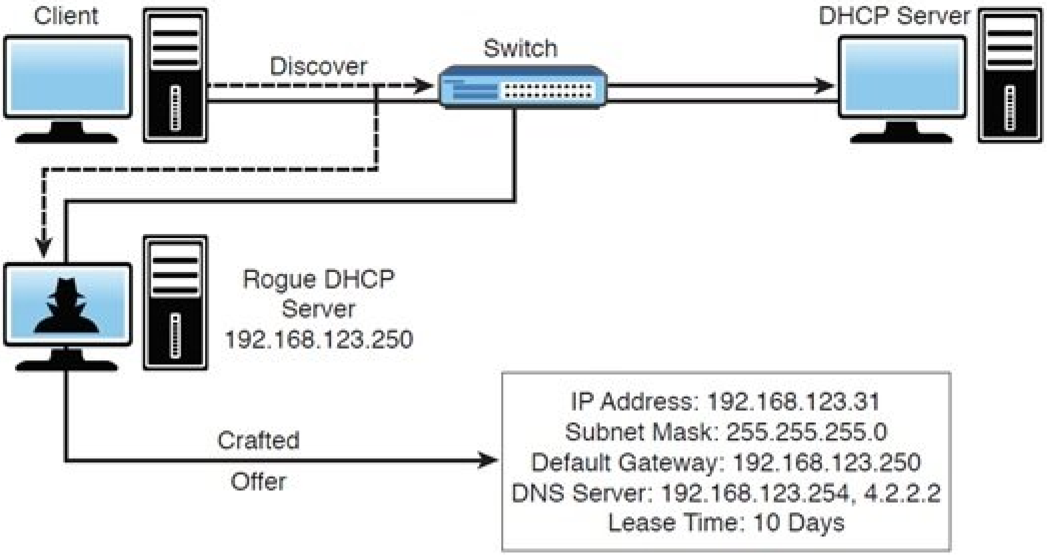
```
No.  Time                        Source             Destination        Protocol
   1 2015-03-25 14:05:01.929682 c6:af:bc:68:56:6a  d3:b4:42:b3:01:64  0x2277
   2 2015-03-25 14:05:17.576892 0e:11:9e:68:28:39  c2:96:52:25:86:05  0x2277
   3 2015-03-25 14:05:17.576894 3b:2d:26:fb:b0:a4  04:dd:16:cd:78:33  0x2277
   4 2015-03-25 14:05:17.576894 c0:6b:c2:e6:70:a0  83:e2:43:53:78:3e  0x2277
   5 2015-03-25 14:05:17.577048 e3:2d:bc:fe:da:0b  99:47:e0:da:8f:b4  0x2277
   6 2015-03-25 14:05:17.577049 30:ff:dd:94:ea:24  18:45:33:b8:28:0d  0x2277
   7 2015-03-25 14:05:17.577049 05:f4:5d:b3:71:a1  b9:64:95:19:33:24  0x2277
   8 2015-03-25 14:05:17.577192 61:42:0c:98:a7:11  c4:78:78:d4:97:f3  0x2277
   9 2015-03-25 14:05:17.577192 ee:1c:c1:72:f0:74  00:de:b5:8d:de:93  0x2277
  10 2015-03-25 14:05:17.577338 4c:cf:03:5b:ed:18  dd:f7:1a:0b:1b:72  0x2277
  11 2015-03-25 14:05:17.577339 9e:20:f6:95:c6:b6  df:e5:33:db:1d:d5  0x2277
  12 2015-03-25 14:05:17.577493 5a:e4:87:08:b6:cc  4d:84:57:25:da:91  0x2277
  13 2015-03-25 14:05:17.577493 4c:e0:da:fb:d6:3c  1a:ab:f6:cd:15:05  0x2277
  14 2015-03-25 14:05:17.577597 ec:e2:f3:12:2e:26  13:a4:21:cd:51:5b  0x2277
  15 2015-03-25 14:05:17.577597 e1:1f:a4:87:f8:02  4a:e9:5a:d1:fb:ff  0x2277
  16 2015-03-25 14:05:17.577739 d4:cf:b6:ac:37:00  c2:1f:9d:13:d2:5e  0x2277

⊞ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: 0e:11:9e:68:28:39 (0e:11:9e:68:28:39), Dst: c2:96:52:25:86:
⊟ Data (46 bytes)
    Data: 000000000000000000000000000000000000000000000000...
    [Length: 46]

0000  c2 96 52 25 86 05 0e 11  9e 68 28 39 22 77 00 00   ..R%.... .h(9"w..
0010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

[illegible]:

- EtherFlood: [illegible] EtherFlood [illegible] http://ntsecurance.nu/toolbox/etherflood [illegible].
- Macof: [illegible] http://monkey.org/~dugsong/dsniff [illegible].

[illegible] ARP [illegible]. [illegible] (DHCP) [illegible] Dynamic Host

Configuration Protocol [illegible]. [illegible] (starvation attack [illegible]. [illegible] DHCP [illegible]. [illegible] Gobbler [illegible] Yersinia [illegible]. [illegible] DHCP [illegible]. [illegible] DHCP [illegible] DHCP [illegible]. [illegible]. [illegible]. [illegible].


Client
Discover
Switch
DHCP Server
Rogue DHCP Server 192.168.123.250
Crafted Offer
IP Address: 192.168.123.31
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.123.250
DNS Server: 192.168.123.254, 4.2.2.2
Lease Time: 10 Days

[illegible] (Port-security) [illegible] DHCP [illegible]. [illegible] ([illegible]) [illegible]. [illegible]. [illegible]:

■ [illegible]: [illegible] SNMP

■ [illegible]: [illegible]

■ [illegible]: [illegible].

[illegible] DHCP [illegible]. [illegible] DHCP [illegible]:

■ [illegible].

■ [illegible].

■ [illegible] DHCP [illegible].

[illegible] DHCP [illegible] DHCP [illegible]. [illegible] 2 [illegible] DHCP [illegible].

[illegible] 2 [illegible]. [illegible] DHCP [illegible] (VLAN) [illegible]. [illegible]. [illegible].

```
Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan 30

Switch(config)# interface gigabitethernet1/0/1

Switch(config-if)# ip dhcp snooping trust
```

[illegible] DHCP snooping [illegible] VLAN 30 [illegible]. [illegible] gigabitEthernet1 / 0/1 [illegible]. DHCP Snooping [illegible] DHCP [illegible]. [illegible] DHCP snooping [illegible] DHCP [illegible] DHCP [illegible].

[illegible].

[illegible] **CEH** [illegible]:

[CEH [illegible]]()

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
13:20 - 17/03/1399
[illegible]:
[illegible] - CEH [illegible] - [illegible] - CEH [illegible] - [illegible] - CEH v10 [illegible] - [illegible] - CEH10 [illegible] - [illegible] - [illegible] - ARP [illegible] - [illegible] - [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/16924/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D9%85%D8%B3%D9%85%D9%88%D9%85%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-arp-%D9%88-%D8%AD%D9%85%D9%84%D8%A7%D8%AA-%D8%B3%DB%8C%D9%84%D8%A7%D8%A8%DB%8C-mac-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF