Övningar – Nätverksteknik ARP

Ett par instuderingsuppgifter som handlar om Nätverksteknik ARP.

1. Vad står förkortningen **ARP** för?

2. Vad används ARP till?

3. Hur många av enheterna på det lokala nätverket ser typiskt en så kallad ARP-query från någon annan?

4. Hur många på det lokala nätverket ser typiskt svaret som kommer på en ARP-fråga?

5. Om vi antar att vi känner till en viss MAC-adress som hör till en viss dator som befinner sig på ett annat nätverk än vi, har vi någon nytta av denna information?

6. Om inte, varför?

7. **Praktisk övning:** Starta CMD (kommandotolken), Powershell eller Windows terminalen och kör kommandot **ARP -a**. Vad ser vi?

8. **Fördjupningsuppgift**: Vad innebär en ARP-poisoning attack?

ARP Laboration

1. Starta Wireshark och starta en inspelning tillsammans med filtret ”**arp or icmp**”. Låt sedan programmet vara igång i inspelningsläge.

2. Öppna en kommandoprompt i administrativt läge och notera vilken IP-adress datorn använder:
   a. _____

   Notera vilken adress som är default gateway:
   b. _____

   Om du har en annan enhet på det lokala nätverket notera den enhetens IP-adress (skrivare, TV, mobil, annan dator etc)
   c. _____

3. Rensa det aktuella innehållet i ARP-cachen. (**arp -d ***)

4. Kör en ”ping” mot adressen noterad ovan i punkt c.

5. Kontrollera att du får svar. Kontrollera i ARP-cache, syns koppling mellan IP och MAC?
   _____

   Notera MAC-adress till denna IP här:
   _____

6. Växla till Wireshark och pausa inspelning. Leta efter ARP-fråga efter aktuell IP-adress och markera denna.

   Titta först i Ethernet-del av denna frame. Vilken är destinations-adress?
   _____

   Varför används denna adress?
   _____
   _____

   Vilken ethertype har denna frame? _____

7. Titta nu i själva ARP-delen.

   Vilken ”opcode” används? _____

   Studera de fyra fälten Sender respektive Target MAC och IP. Vilken information är det som ”saknas” (d.v.s. där fältet är blankt)?
   _____

8. Hitta sedan det ARP-svar som följer denna fråga. Notera först i Ethernet-header om det är någon skillnad i destinations-MAC-adress. Vad är det som gör denna ”olikhet” jämfört med frågan?

   _____
   _____

9. Notera i ARP-del vilken OP-code som används? _____

   Studera Sender och Target MAC och IP-fältet, finns all information nu?

   _____

10. Hitta det första ICMP-meddelande från din dator till sökt maskin. Öppna detta paket och studera Ethernet-header och destinations-MAC, är detta samma MAC som noterades i punkt 12? _____

11. Starta en ny inspelning i Wireshark, (spara inte).
    Rensa innehållet i ARP-cachen.
    Pinga nu en adress på internet, t ex **www.sunet.se.**

    Kontrollera i kommandoprompt hur innehållet i ARP-cache ser ut. Syns någon koppling till adressen på sunet? Om inte, varför?

    _____
    _____

12. Titta i Wireshark, se vilken ARP-fråga som ställdes av *din* dator (observera att andra ARP-frågor kan synas). Varför efterfrågades denna adress av din maskin?

    _____
    _____

    Titta i ARP-cache vilken MAC-adress som tillhör default gateway:

    _____

13. I Wireshark, hitta det första ICMP-meddelande som gick från din dator mot maskin på Internet. Markera detta paket och titta i Ethernet-header. Vilken är destinations-MAC-adress och varför syns denna?

    _____
    _____
    _____