----------8----------
Udaljeno otkrivanje aplikacija --> skeniranje pristupa, otvoren pristup znaci prisutnost aplikacije
TCP skeniranje -SYN skeniranje(salje se SYN i ceka se odgovor, ako nema odgovora ne znamo kakava je situacija), TCP connect (ako nije ukljucen filter)
- FIN skeniranje (sigurno se moze znati da nema nicega, vraca se RST inace ignore), skeniranje framgentacijom (izbjegavanje detekcije)

Prikrivanje izvora skeniranja - idlescan (nacin skeniranja koristenjem 3. strane, zombi (mala kolicina, predvidljivi IP))
- ideja (nadi ID koji zombi koristi, salji paket gdje je izvorisna adresa zombijeva)

UDP skeniranje
-slanje praznog udp datagrama
-za zatvoren pristup pristizu poruke "icmp port unreachable"

Problemi skeniranja
-spora tehnika skeniranja, problemi (udp je nepouzdan pa
moramo nekoliko puta pokusati da budemo sigurni)
-sporije nego TCP, ako je subnet 24 znaci 254 racunala za skenirat
-filter onemogucava provjeru otvorenosti porta
-ne dolaze poruke to ne znaci da je port otvoren

Poteskoce sa skeniranjem
- velik broj pristupa i skeniranja cvoru
- zbog filtera nije moguce je li port otvoren ili ne
- otvoren port ne znaci da je tamo aplikacija

----------7----------
Zastita DNS-a : TSIG: dinamicka osvjezavanja zone i prijenos na sekundarne polozaje

Zastita DNSa: DNSSEC
--> dokaz ispravnosti podataka, klijent pomocu resolvera dobiva sigurne podatke
--> podaci na RRu se potpisuju privatnim kljucem, potpis osigurava valjanost s kraja na kraj
--> novi zapisi (dnskey, ds, nsec), novi flagovi (cd, ad), novi bitovi(do)

Problemi <--ne osigurava povjerljivost, ne stiti od DDoS napada
Zloupotrebe DNSa --> autorizacija i autentifikacija na temelju domene, raspodjela osjetljivih podataka