TK2100

T-05

**Nettverk og internett 1**

Notater:

* Ukryptert overføring i IP nivå og kan avlyttes hele veien fra avsender til mottaker og løses stort sett på applikasjonsnivå
* 65 536 porter på pcen

1. **Hva er «MAC-spoofing»?**

Det er når man utgir seg for å ha en annen adresse

Finn ut (sniff) MAC-adressen du vil utgi deg å ha

Og deretter sett den på egen maskin

1. **Hva er «ARP-spoofing»?**

Address resolution protocol kobler nettverk og linklags- adresser

* Kringkaster forespørsler
* Casher respons
* IPV6 tar ikke i bruk denne protokollen men NDP gjør
* Spoofingen er når cache oppdaterer seg på grunnlag av alle ARP-responsmeldinger (angriper sender falske arp meldinger over et lokalt nettverk og deretter får tak i MAC adressen med IP adressen av en maskin eller en server)
* Det er ulike varianter og muligheter i ulike OS for å være mer kresen
* Det er mangelen på autentiserinsgsmekanismer som gjør det sårbar for spoofing
* Hvis hackeren får tilgang til switchen til et selskap er den kjørt

1. **Hvorfor er “ip-spoofing” ofte brukt I “DoS-angrep”?**

IP-spoofing er når man legger inn en falsk avsender adresse og er bare en endring i headeren

Denne typen spoofing er typisk brukt i ddos angrep der angriper ikke er interessert i å få svar, men bare overbelaste mottakeren. Dette kan stoppes av en router/firewall som stopper pakker som ikke har en avsender adresse som i LAN/subnet.

1. **Hva er ett «Smurf-attack» Smurfe-angrep?**

Broadcast ICMP echo pakker i nettverket med offerets spoofede ip adresse som avsender

Man sender en echo respons i et nettverk og hvis angriper sender en echo melding til 50 maskiner vil alle gå til offeret så den får 50 meldinger desto flere meldinger den får jo skadeligere blir det for offeret som kan resultere ødeleggelse av maskinen.

1. **Hva er «SYN-flod attack»?**

Dette er et typisk DOS angrep som er basert på a sende forespørsler om TCP-forbindelse raskere enn når det prosesseres av tjeneren. Angriper lager en stor mengde pakker med falske avsender adresser og setter inn SYN-flagget i disse. Tjeneren svarer med SYN-ACK og åpner en socket , men får aldri en respons. Dette ender opp med at kapasiteten på tjeneren er oppbrukt.

1. **Hva er «(D)DoS»**

Det står for distributed denial of service angrep er et angrep for å forstyrre den normale trafikken til en server eller et nettverk ved å overvelde målet eller infrastrukturen med et hav av internett trafikk.

1. **Hva mener Kripos er de typiske formene for datakriminalitet?**
2. **Kan man bruke Wireshark, nmap eller andre sikkerhets-verktøy utenfor sitt egen**

«eiendom/område» så lenge man ikke planlegger å gjøre skade?

Ferdig med oppgavene?

Husk å repetere slidene og se på sliden med «hva skal vi kunne?».

1