AĞ GÜVENLİĞİ VE SIZMA TESTİ

~ cat network_Security/introduction.txt

*MITM
- → ARP Poinsoning
- → ICMP Redirect
- → DHCP Spoofing & Starving
- → DNS Cache Poisoning

*Service Blocking
- → DOS
- → DDOS
- → DRDOS (Amplification)

~ cat network_Security/ARP.txt

Address Resolution Protocol

* IP → MAC
    ** Communication between layer2 devices

1- Arp Request
    **Who is 192.168.1.1? Tell 192.168.1.11
    ** Broadcast
2-Arp Response
    ** 192.168.1.1 is at AA:BB:CC:DD:EE:FF

~ cat network_Security/ARP_Poison.txt

ARP Request

→ ARP Tablosuna ekleme yap veya değiştir

ARP Response

→ ARP Tablosundaki girdiyi değiştir

~ cat network_Security/ICMP.txt

Internet Control Message Protocol

→ IP protokolünde çıkabilecek hataları raporlamak

→ Bağlantı kontrolü (Ping)

ICMP types

Type 8 – Echo Request

Type 0 – Echo Reply

Type 5 – Redirect

...

ICMP Codes

Type 5 Code 1 – Redirect For Host

...

~ cat network_Security/ICMP_Redirect.txt

IP Header (Source:Router, Destination=Victim)
ICMP Header(Type=5, Code=1, Gateway=Attacker)
IP Header(Source:Victim, Destination=Target)
Random UDP/TCP header

*1 PAKET ALINDI

~ cat network_Security/DHCP.txt

Dynamic Host Configuration Protocol

→ IP adresi atama
→ Ağ bilgilerini paylaşma
  → Subnet Mask
  → Default Gateway
  → Default DNS
  → ...

~ cat network_Security/DHCP_Attacks.txt

DHCP Starving

→ DHCP sunucusuna karşı yapılır

→ Sunucunun elindeki bütün ipleri alarak başka kullanıcıların Ağa bağlanması engellenir

DHCP Poisoning/Spoofing

→ Kullanıcılara yapılır

→ DHCPden ip isteyen kullanıcıya yanlış bilgiler gönderilir.

~ cat network_Security/DNS.txt

Domain Name System

→ Ip adreslerinin isimlendirilmesine yarar

** 80.251.40.153 → ankara.edu.tr

→ Domainler ile ilgili bilgi verir

** A, AAA,NS, CNAME, MX, SRV, TXT

~ cat network_Security/DNS_Cache_Poisoning.txt

DNS Sunucusu

** 80.251.40.153 → ankara.edu.tr

Dönmesi gerekirken

** 13.37.13.37 → ankara.edu.tr

Dönerse, bir saldırgan tarafından ele geçirilmiştir.
Ankara.edu.tr ye girmek istediğinizde saldırganın
Yönlendirdiği sunucuya bağlanırsın.

~ cat network_Security/DOS-DDOS-DRDOS

Denial Of Service

**Bir sunucuya bir makineden çok istek gönderip servis vermesini engellemek.

Distributed Denial Of Service

**Bir sunucuya birden çok makineden (Zombi) istek gönderilip servis vermesini engellemek.

Distributed Reflective Denial Of Service

**UDP üzerinden çalışan protokolleri kullanarak ağ trafiğini yükseltip, sunucunun servis vermesini engellemek.