KARADENİZ TEKNİK ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
SİBER GÜVENLİK LABORATUVARI

Raw Paket Programlama

IP spoofing, MAC spoofing, ping flood ve SYN flood gibi ağ saldırıları, hedef sistemlerin kimlik bilgilerini veya iletişim kaynaklarını taklit ederek ağ hizmetlerini bozmayı veya yetkisiz erişim elde etmeyi amaçlayan yaygın tehditlerdir. Bu saldırılar hem bireysel makineler hem de kurumsal ağlar için hizmet kesintisi, veri kaybı ve izinsiz erişim riski taşır; saldırganlar genellikle tespit edilmemek için kaynak adreslerini gizler veya trafiği aşırı yükleyerek hedefi etkisizleştirir. Bu tür tehditlere karşı savunma, olay öncesi hazırlık (ağ tasarımı, segmentasyon, erişim kontrolü) ve olay anında hızlı tespit ile müdahaleyi içerir. Tespit yöntemleri arasında anomali tabanlı ağ trafiği analizleri, IPS/IDS uyarıları, bağlantı ve oturum istatistiklerinde olağan dışı artışların izlenmesi yer alır; ayrıca sistem günlükleri ve ağ akış (flow) verileri kritik ipuçları sağlar. Ağ seviyesinde filtreleme (ingress/egress filtering), anti-spoofing politikaları ve ARP/port güvenlik önlemleri spoofing riskini azaltır; bağlantı sınırlandırma ve SYN cookie benzeri mekanizmalar ise taşma saldırılarını hafifletir. Etkin bir savunma kuşağı, gerçek zamanlı izleme, otomatik throttling, siyah liste/karantina uygulamaları ve saldırı kaynağına ilişkin istihbarat entegrasyonunu kapsar. Ayrıca saldırı tespitinde adli izlerin korunması, log merkezileştirme ve olay müdahale planları kritik öneme sahiptir; hukuki ve etik çerçevede hareket etmek, saldırıların amaçlandığı ortamda yetkisiz testlerden kaçınmayı gerektirir.

IP Spoofing

IP Spoofing (IP sahteciliği), bilgisayar ağlarında kullanılan bir saldırı tekniğidir ve temel olarak ağ paketlerinin kaynak IP adresini değiştirerek, paketin sanki farklı bir cihazdan gönderilmiş gibi görünmesini sağlar. Normalde bir cihazdan çıkan paket, o cihazın gerçek IP adresini taşır; ancak saldırganlar özel araçlar veya yazılımlar kullanarak bu alanı sahte bir IP adresiyle değiştirir. Böylece hedef sistem, paketin aslında saldırgandan değil, güvenilir veya tanıdık bir kaynaktan geldiğini zanneder. Bu yöntem genellikle kimlik gizleme, güvenlik duvarlarını veya IP tabanlı erişim kontrollerini atlatma, dağıtık hizmet engelleme (DDoS) saldırılarında kurban sistemleri yanıltma gibi amaçlarla kullanılır. IP spoofing tekniği doğrudan saldırgana geri dönüş cevabı sağlamadığı için, çoğu zaman tek başına değil, SYN flood gibi başka saldırı yöntemleriyle birlikte uygulanır. Bu nedenle IP spoofing, hem ağ güvenliği açısından kritik bir tehdit oluşturur hem de saldırı tespit sistemleri tarafından yakalanması zor bir yöntemdir.

Uygulama Aşaması

- sudo dhclient eth0

Saldırgan hedef makineye

- ping -c 100 192.168.56.103

Komutu kullanarak 100 adet ping atabilir.

Sniffer saldırgan ile hedef makine arasındaki trafiği

- sudo tcpdump -i enp0s3 -n icmp

komutu kullanarak dinleyebilir veya

- sudo tcpdump -i enp0s3 -n icmp -w test.pcap

komutu ile trafiği kaydedebilir.

hping3 ile

- `sudo hping3 -a 192.168.56.50 -S -p 80 192.168.56.103`

`-a 192.168.1.50` → sahte kaynak IP

`-S` → TCP SYN bayrağı gönder

`-p 80` → hedefin 80. portuna (HTTP) gönder

Bu komutla hedef, paketi 192.168.1.50'den gelmiş gibi görür.

Python + Scapy ile

```
from scapy.all import *
dst_ip  = "192.168.56.103"
spoof_ip = "192.168.56.50"
iface   = "eth0"
dst_mac = getmacbyip(dst_ip)
pkt = Ether(dst=dst_mac) / IP(src=spoof_ip, dst=dst_ip) / TCP(sport=12345, dport=80, flags="S", seq=1000)
sendp(pkt, count=5, iface=iface, verbose=1)
```

Bu script hedefe 5 tane sahte SYN paketi yollar.

Tespit Yöntemleri

Sniffer makinede

Wireshark / tcpdump ile inceleme

- sudo tcpdump -i enp0s3 -n "host 192.168.56.103 and tcp[tcpflags] & tcp-syn != 0"

Gelen paketlerin kaynak IP'si ile MAC adresi uyuşmuyor olabilir.

ARP tablosu ile karşılaştırma yaparak sahteciliği fark edebilirsin.

ARP Kontrolü

Hedef makinede:

- `arp -a`

Eğer `192.168.1.50` IP'si için MAC adresi görünmüyorsa, ama o IP'den paket geliyorsa spoof var.

Özet

IP spoofing, sahte IP adresiyle paket göndermektir.

Deney ortamında `hping3` veya Scapy ile kolayca yapılabilir.

Tespit için:

Kaynak IP ↔ MAC eşleşmesi kontrol edilmeli.

ARP tabloları izlenmeli.

IDS/IPS sistemleri (Snort, Suricata) kullanılmalı.

MAC Spoofing

MAC Spoofing (MAC sahteciliği), bilgisayarın ağ kartına üretici tarafından verilen ve normalde değiştirilemez gibi görünen benzersiz MAC adresinin yazılımsal olarak değiştirilmesi işlemidir. Bu yöntemle bir cihaz, ağ üzerinde farklı bir donanım kimliğine bürünerek başka bir cihazmış gibi davranabilir. Genellikle ağ erişim kısıtlamalarını atlatmak (örneğin, sadece belirli MAC adreslerine izin veren Wi-Fi ağlarına bağlanmak), kimliğini gizlemek, ya da başka bir cihazın yerine geçip veri trafiğini dinlemek için kullanılır. MAC spoofing kolayca yapılabilse de, yönetilebilir switch'lerin "port security" özelliği, ARP tablosu kontrolü veya IDS/IPS sistemleri sayesinde tespit edilebilir. Bu nedenle, özellikle kurumsal ağlarda ciddi bir güvenlik açığı olarak değerlendirilir.

Uygulama Aşaması

Linux Üzerinde (ifconfig / ip link)

Ağ kartını kapat
- sudo ifconfig eth0 down

Yeni sahte MAC adresi ata
- sudo ifconfig eth0 hw ether 00:11:22:33:44:55

Ağ kartını tekrar aç

- sudo ifconfig eth0 up

Bu sayede ağda cihaz, artık sahte MAC ile görünecektir.

- sudo tcpdump -i eth0 -e -vv 'arp or icmp'
- ping -c 4 192.168.56.103

Tespit Yöntemleri

1. Sniffer makinede
- sudo tcpdump -i enp0s3 -n icmp -w mac_spoof.pcap
2. Hedef makinede
- arp -a

3. Switch Port Security
    a. Cisco/HP gibi yönetilebilir switch'lerde "port security" açılır.
    b. Belirli bir porta sadece belirli MAC adresleri izin verilir.
4. ARP Tablosu Kontrolü
    a. Bir IP için farklı MAC adresleri görünüyorsa sahtecilik vardır.
5. Wireshark / IDS
    a. Aynı porttan veya IP'den birden fazla farklı MAC adresi geliyorsa anormaldir.
    b. Örneğin Wireshark'ta "Duplicate Address Detection" uyarısı çıkabilir.
6. Log Analizi
    a. DHCP sunucusunda aynı IP'ye farklı MAC'ler talepte bulunursa şüpheli.

IP Spoof vs MAC Spoof Karşılaştırma

- IP Spoof: Ağ katmanında (Layer 3), IP adresi sahte.
- MAC Spoof: Veri bağlantı katmanında (Layer 2), donanım kimliği sahte.
- IP spoof genellikle internete çıkışta (kaynak gizleme) kullanılır,
- MAC spoof ise genellikle LAN/Wi-Fi üzerinde (erişim atlatma) kullanılır.

Özet:
MAC Spoofing, ağ kartının MAC adresini yazılımsal olarak değiştirerek başka bir cihaz gibi görünme tekniğidir. Linux'ta `ifconfig`, `ip link`, `macchanger` gibi araçlarla yapılabilir. Tespiti için ARP tabloları, switch port security, IDS/IPS sistemleri ve DHCP logları kullanılabilir.

Ping Flood

Ping Flood (Ping Taşkını), bir tür Denial of Service (DoS) saldırısıdır ve hedef sistemin ağını veya işlem gücünü tüketmek amacıyla çok sayıda ICMP Echo Request (ping) paketi göndermeye dayanır. Normalde ping, bir cihazın ağda erişilebilir olup olmadığını kontrol etmek için küçük ICMP paketleri yollar ve karşı taraf Echo Reply döner. Ancak ping flood saldırısında saldırgan, hedefe sürekli ve yüksek hacimde ping paketi gönderir; hedef ise bunlara cevap vermek zorunda kaldığından işlemci, bellek ve bant genişliği hızla tükenir. Bunun sonucunda hedef sistem yavaşlar, ağ bağlantısı kesintiye uğrar veya tamamen erişilemez hale gelebilir. Bu saldırı genellikle hping3, ping -f gibi araçlarla yapılabilir ve tek bir makineden başlatılabileceği

gibi çok sayıda makineden eşzamanlı gönderilirse DDoS (Distributed DoS) halini alır. Ping flood'un tespiti, genellikle ağ trafiğinde olağandışı yoğun ICMP paketlerinin gözlemlenmesiyle, engellenmesi ise güvenlik duvarlarında ICMP trafiğini sınırlayarak ya da rate limiting uygulanarak sağlanır.

Uygulama Aşamaları

Linux ping komutu ile

- sudo ping -f -s 1000 -i 0.002 192.168.56.103

-f → flood modu (çok hızlı paket gönderir)
-s 1000 → 1000 byte'lık paket boyutu
-i 0.002: 2 milisaniye aralıkla paket gönderir.

Bu komut root yetkisi ile çalışır ve hedefi ICMP paketlerine boğar.

hping3 ile

- sudo hping3 -1 --flood -d 120 192.168.56.103

-1 → ICMP (ping) modu
--flood → durmaksızın paket gönder
-d 1200 → 1200 byte boyutunda paket

Bu yöntemle hedefin CPU'su ve ağı kısa sürede aşırı yüklenir.

Tespit Yöntemleri

Analiz — pcap / tshark komutları

ICMP paket sayısı / saniye:

- `tshark -r ping.pcap  -Y icmp -q -z io,stat,0,"COUNT(icmp)"`

Kaynak başına paket sayısı:

- tshark -r ping.pcap -T fields -e ip.src | sort | uniq -c | sort -nr | head

Wireshark ile

Normalde saniyede birkaç ICMP paketi görülürken, flood sırasında binlerce paket görünür.

Grafiklerde (Statistics → IO Graphs) ani trafik patlaması izlenebilir.

Sistem Kaynakları ile

Hedef makinede:

- `top`

veya

- `sar -n DEV 1`

CPU yükselir, ağ arayüzünde (eth0) aşırı RX (receive) trafiği görülür.

Önleme Yöntemleri

- Rate Limiting: ICMP paketlerini saniyede sınırlamak.
- sudo iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 5/s -j ACCEPT
- sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
- Firewall / Router ayarları: ICMP flood'a karşı otomatik koruma.
- IDS/IPS sistemleri: Şüpheli yoğun ICMP trafiğini engeller.

Özet:
Ping Flood, hedefi ICMP paketleriyle aşırı yükleyerek hizmet veremez hale getiren bir DoS saldırısıdır. Laboratuvar ortamında ping -f veya hping3 --flood ile uygulanabilir. Tespiti tcpdump/Wireshark/IDS ile, engellemesi firewall + rate limiting ile yapılır.

SYN flood

SYN flood, bir tür Hizmet Engelleme (DoS) saldırısıdır ve TCP bağlantı sürecindeki 3'lü el sıkışma (three-way handshake) mekanizmasını hedef alır. Normalde istemci bir sunucuya bağlanırken SYN paketi gönderir, sunucu SYN-ACK ile yanıtlar, ardından istemci ACK göndererek bağlantıyı tamamlar. SYN flood saldırısında ise saldırgan çok sayıda sahte veya yarım kalmış SYN paketi yollar, fakat son ACK adımını gerçekleştirmez. Bu durumda sunucu her isteği beklemede tutarak kaynaklarını (hafıza ve bağlantı tabloları) tüketir. Kaynaklar dolduğunda meşru kullanıcıların bağlantı kurması engellenir ve hedef sistem hizmet veremez hale gelir. Bu yüzden SYN flood saldırıları, özellikle yüksek hacimli olduğunda, sistemleri ciddi şekilde yavaşlatabilir veya tamamen devre dışı bırakabilir.

• Saldırı mantığı

- Saldırgan, hedef sunucuya binlerce sahte SYN paketi yollar.
- Bu paketlerde genellikle sahte IP adresleri (spoofed IP) kullanılır ki sunucunun gerçek istemciye yanıt göndermesi mümkün olmasın.
- Sunucu her bağlantı isteği için `SYN-ACK` gönderir ve `ACK` yanıtını bekler.
- Yanıt gelmeyince bağlantı yarım kalır (half-open connection) ve sunucu kaynak tüketmeye devam eder.

Uygulama Aşamaları

hping3**,** nping**,** scapy (Python kütüphanesi) gibi araçlarla SYN flood yapılabilir.

hping3 ile

- sudo hping3 -S -p 80 --flood 192.168.56.103

-S → SYN bayrağı gönder

-p 80 → hedef port (ör: web sunucusu)

--flood → çok hızlı paket gönder

Hedef sunucu TCP bağlantı tablosunu doldurur, cevap veremez hale gelir.

Önleme Yöntemleri

1. TCP SYN Cookies

    - Modern işletim sistemlerinde kullanılan bir yöntemdir.
    - Sunucu, yarım bağlantı için kaynak ayırmaz; `ACK` gelirse bağlantıyı gerçek kabul eder.

2. Firewall / IDS / IPS Kullanımı
    - iptables veya pf gibi firewall'larda SYN flood filtreleri konulabilir.
    - Örnek iptables kuralı:

    - ```
      iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
      ```
    - ```
      iptables -A INPUT -p tcp --syn -m limit --limit 10/s -j ACCEPT
      ```
    - ```
      iptables -A INPUT -p tcp --syn -j DROP
      ```

      Bu kurallar, saniyede 10 SYN paketini kabul eder, fazlasını engeller.

3. Rate Limiting (Hız sınırlama)

    - Router veya firewall üzerinde, belirli bir IP'den gelen bağlantı isteği sayısı sınırlandırılır.

4. Saldırı Tespiti (Snort, Suricata, Zeek)

    - Anormal miktarda SYN isteği geldiğinde alarm üretir veya otomatik engeller.

5. Load Balancer / Reverse Proxy

    - Büyük sistemlerde saldırıyı doğrudan hedef sunucuya ulaştırmadan önce yük dengeleyici cihaz filtreler.

6. DDoS Mitigation Servisleri

    - Cloudflare, Akamai, AWS Shield gibi servisler SYN flood'u üstlenir, filtreler ve temiz trafiği sunucuya gönderir.

Özet:

SYN flood yapmak için özel araçlarla sürekli sahte SYN paketleri gönderilir.

Engellemek için ise SYN cookies**,** firewall kuralları**,** rate limiting**,** IDS/IPS ve büyük ölçekli sistemlerde DDoS koruma servisleri kullanılır.
      ```

Lab Ortamının Kurulumu

Deney ortamı, birbirine bağlı fakat dış ağa izole edilmiş bir sanal ağ üzerinde konumlandırılmış üç ana sanal makineden (saldırgan, hedef ve izleyici/sniffer) oluşmaktadır. Saldırı trafiğinin üretilmesi için saldırgan makinada Kali Linux; hedef makinelerle ağ trafiğini yakalamak ve analiz etmek üzere hedef ve sniffer makinelerde ise Ubuntu dağıtımları kullanılmaktadır. Sanal makineler host-only ya da internal ağ topolojisinde yapılandırılarak (örnek adresleme 192.168.56.x/24) fiziksel altyapıdan ayrı, kontrollü bir laboratuvar ağı oluşturulmuştur; bu yapı deneysel paket üretimi ve trafik gözlemi sırasında gerçek ağa olası bir sızıntıyı önlemektedir. Trafik üretimi ve saldırı senaryolarının oluşturulmasında paket düzeyinde kontrol sağlayan araçlar (Scapy, hping3 vb.) kullanılmaktadır; saldırı etkinliğinin izlenmesi ve kanıtlanması için paket yakalama ve analiz araçları (Wireshark, tcpdump) kullanılmaktadır.

Ağ bağdaştırıcılarının seçimi ve konfigürasyonu deneysel gereksinimlere göre belirlenmiştir: Host-only adaptörler, sanal makineler ile host arasında ve sanal makineler arası iletişimi sağlarken dış internet erişimini keserek deney trafiğinin izole edilmesini temin etmekte; buna karşılık, güncelleme veya dış bağımlılıkların giderilmesi gerektiğinde “karma” bir yerleşim (ör. birincil adaptörde NAT/Bridged ile kontrollü internet erişimi, ikincil adaptörde host-only ile laboratuvar trafiği) kullanılmıştır. Ağ yönetimi açısından DHCP parametreleri ve statik IP atamaları Host-Only yöneticisi veya VM yönetim konsolu aracılığıyla düzenlenmiş; paket yakalama ve pasif izleme gereksinimleri için ilgili NIC’lerin promiscuous mode desteği etkinleştirilmiştir. Ayrıca sanal ana makinede “cable connected” ve uygun sanal NIC modeli seçimi gibi temel ayarlara dikkat edilerek, VM içi ağ yapılandırmasının (IP, netmask, varsayılan gateway yalnızca NAT adaptörü için) deneysel amaçlarla tutarlı ve tekrarlanabilir olmasına önem verilmiştir.

Uygulama

Deneyin uygulama bölümünde, hem Ethernet (MAC) hem de IP katmanlarında sahteciliğin (MAC ve IP spoofing) kombine edildiği bir saldırı senaryosu yürütülecek; kontrol altında oluşturulan sahte kaynak adresleriyle ICMP ve TCP SYN trafiği üretilerek hedefin ağ davranışı, paket yakalama kayıtları ve savunma mekanizmalarının tespit etkinliği ölçülecektir.

Rapor Soruları

1. IP adres ve MAC adres nedir?
2. IP Spoofing ve MAC Spoofing nedir?
3. Ping Flood ve SYN Flood nedir?
4. IP Spoof ve MAC Spoof saldırıları bir sisteme ne tür zararlar verebilir?
5. Ping Flood ve SYN Flood saldırıları bir sisteme ne tür zararlar verebilir?
6. Deney uygulama aşamasında yazdığınız kodu detaylı bir biçimde anlatınız?