BSM 471-AĞ GÜVENLİĞİ

Hafta5: Katman 3 Saldırıları ve Önleme Teknikleri

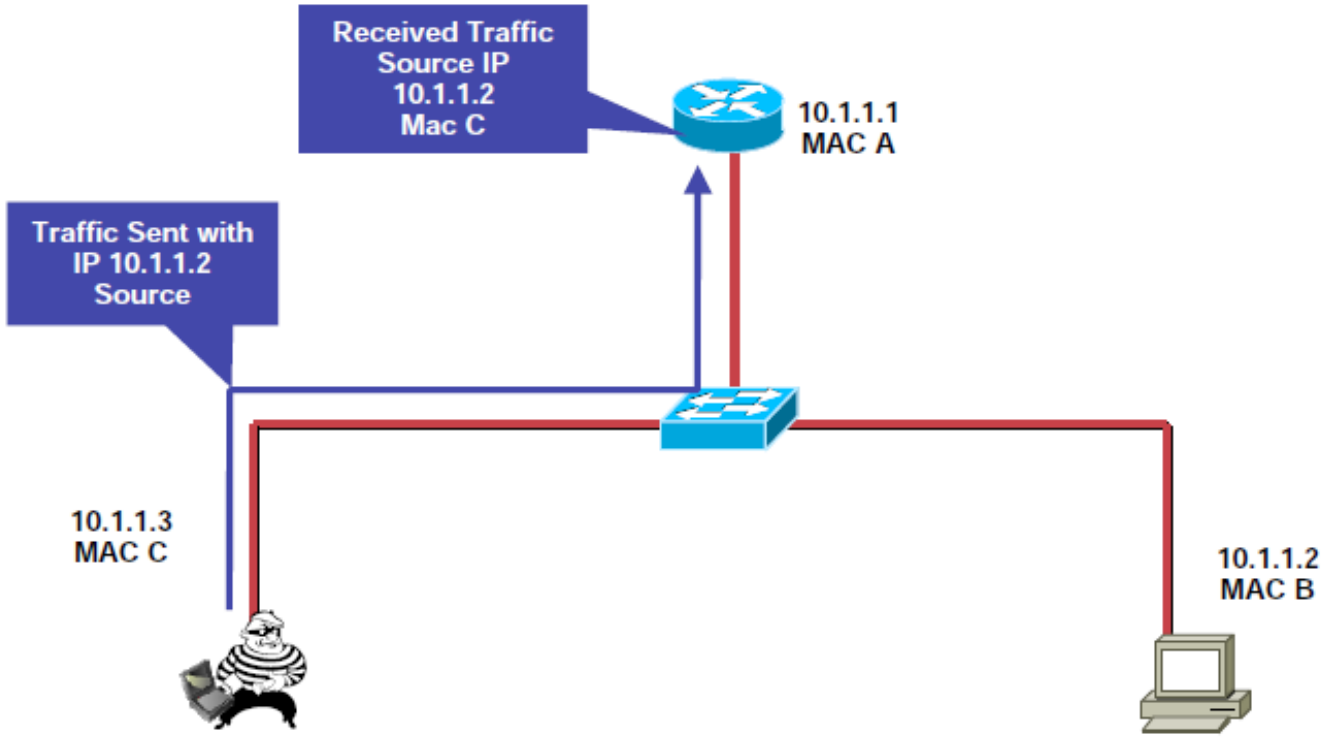
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

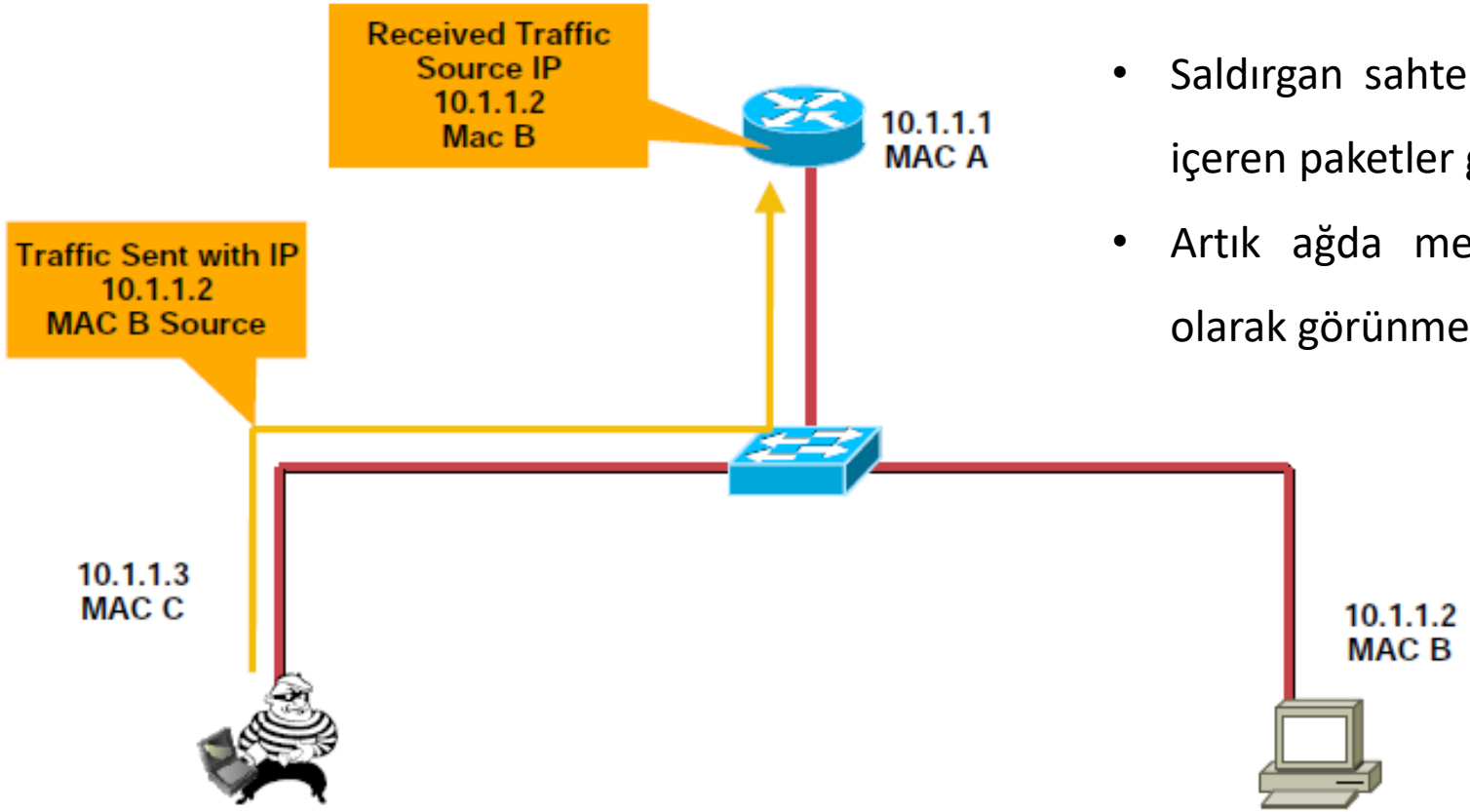
- ***Katman 3 Saldırıları;***
  - IP Spoofing
  - DDoS Kavramı ve ICMP Saldırıları
  - Yönlendirme Protokolleri Saldırıları

IP Aldatmaca (Spoofing) Saldırıları

- Saldırgan, gönderenin kimliğini gizlemek veya başka bir bilgisayar sisteminin kimliğine bürünmek için sahte bir kaynak IP adresiyle IP paketleri oluşturur.
- IP aldatma saldırısının temel amacı, saldırganın ana bilgisayara kök erişimi elde etmesine ve hedef sisteme bir arka kapı giriş yolu oluşturmasına olanak tanıyan bir bağlantı kurmaktır.
- Spoofing, bazen üstbilgi sahteciliğine atıfta bulunmak için de kullanılır, çünkü saldırgan paketlerin üstbilgisini sahte bilgilerle oluşturur.

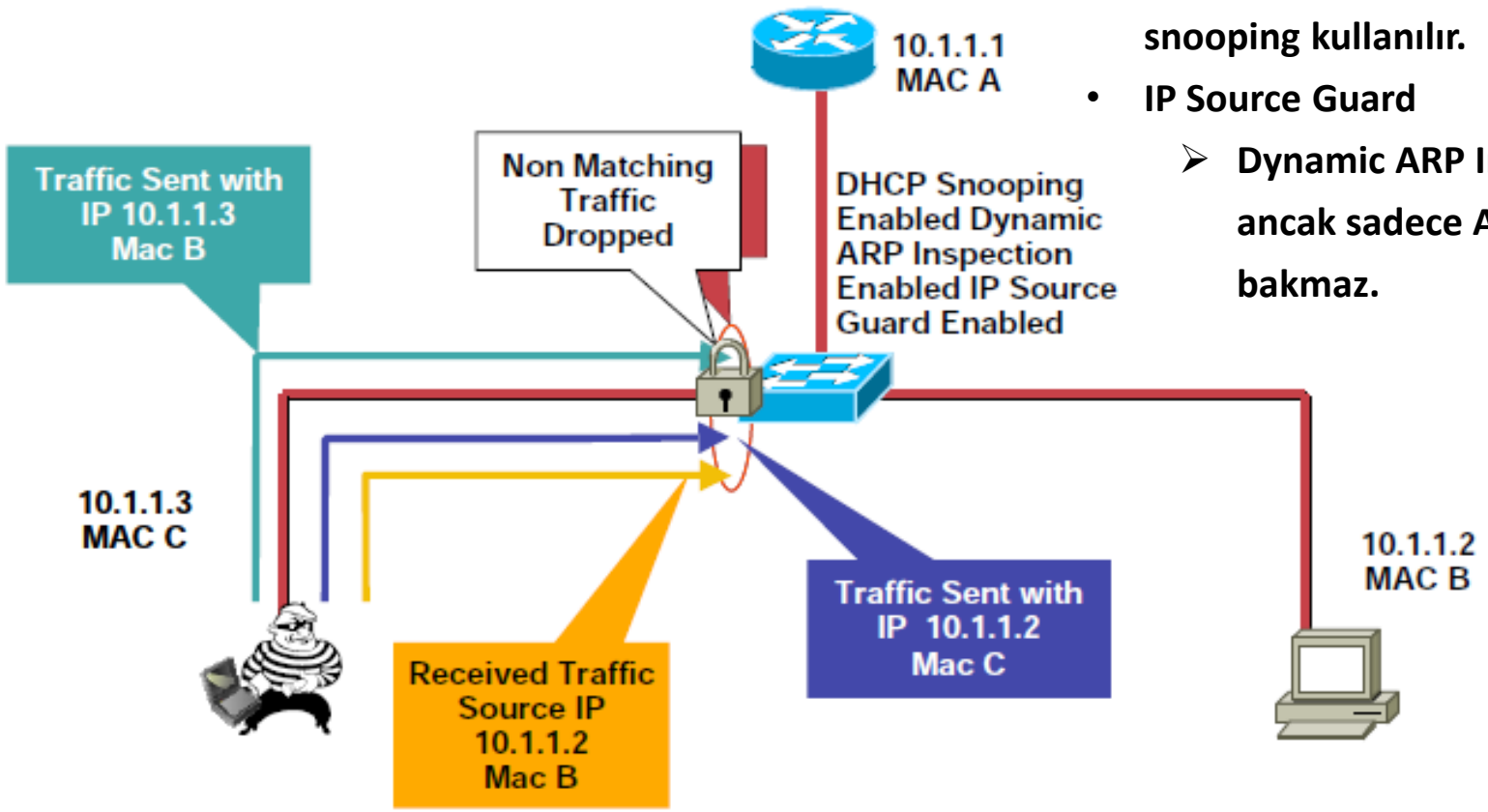


IP/MAC Aldatmaca (Spoofing) Saldırıları



- Saldırgan sahte IP ve MAC adresler içeren paketler gönderir.
- Artık ağda mevcut bir uç düğüm olarak görünmektedir.

Aldatma Saldırıları için Güvenlik Çözümleri



- **Tablo bilgisi oluşturabilmek için DHCP snooping kullanılır.**
- **IP Source Guard**
  - **Dynamic ARP Inspection'a benzer ancak sadece ARP mesajlarına bakmaz.**

IP Source Guard Configuration
IP/MAC Checking Only (Opt 82)

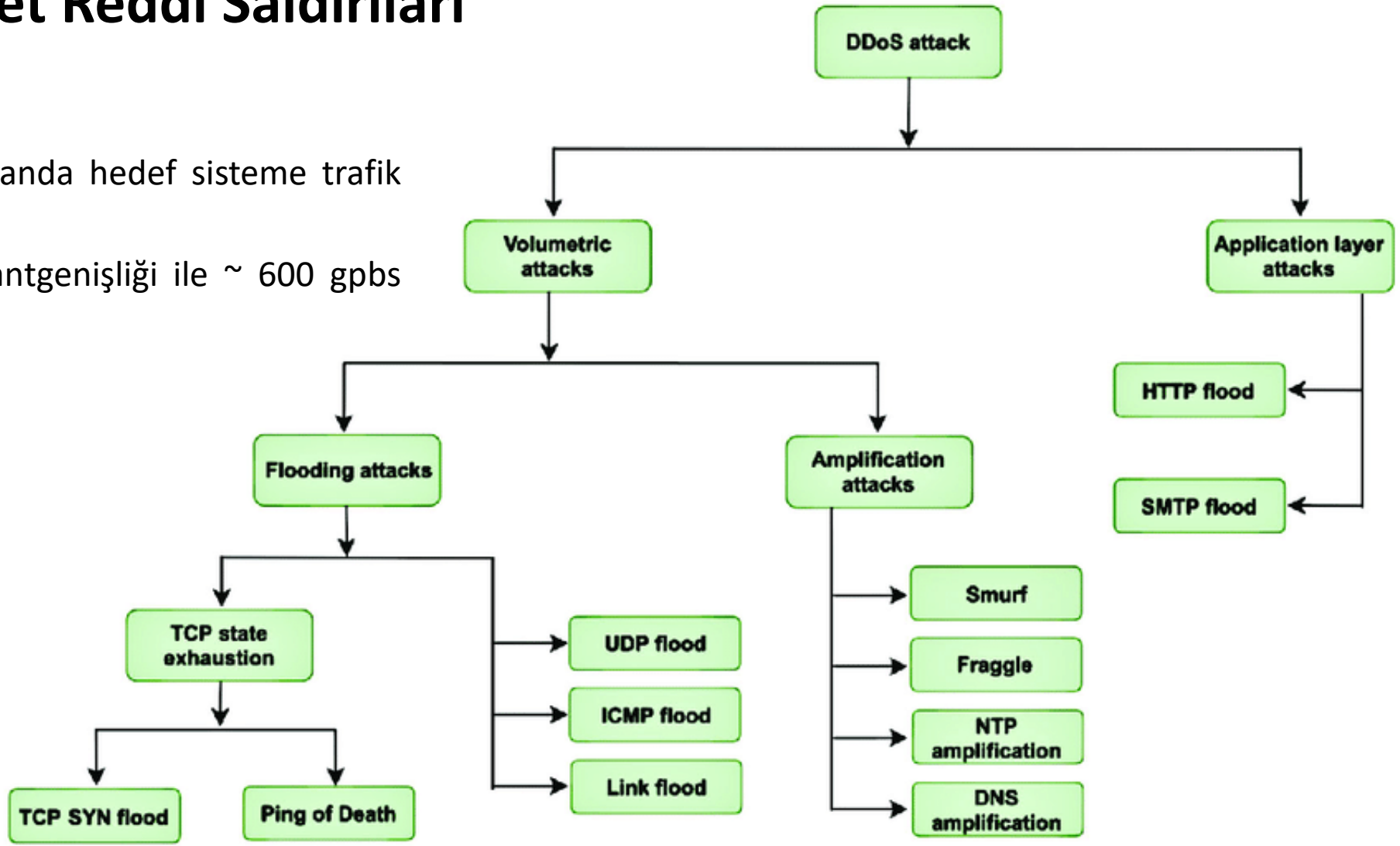
IOS
Global Commands
ip dhcp snooping vlan 4,104
ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping
port-security

IP Source Guard Configuration
IP Checking Only (no Opt 82)

IOS
Global Commands
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
Interface Commands
ip verify source vlan dhcp-snooping

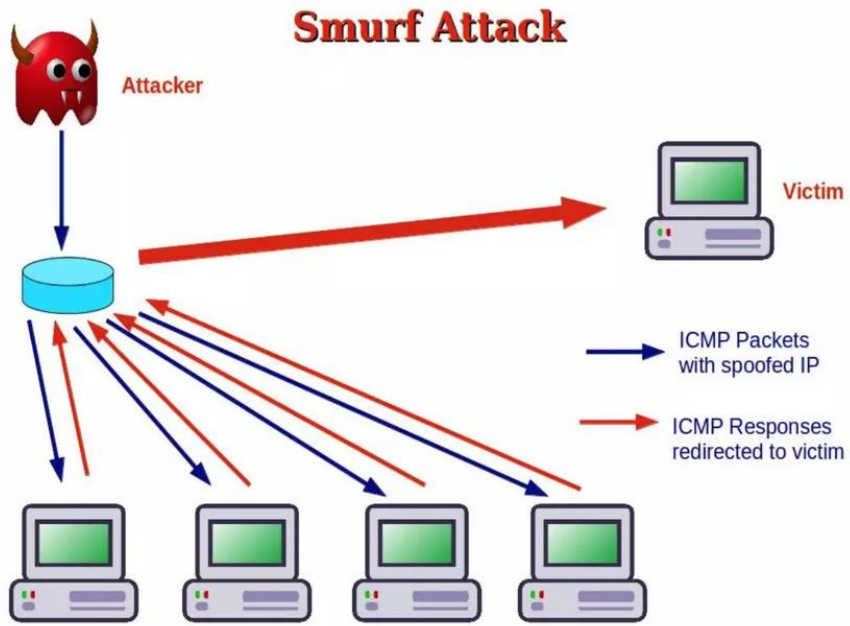
Dağıtılmış Hizmet Reddi Saldırıları

- Bir çok kaynaktan aynı anda hedef sisteme trafik üretme
- Teorik olarak 1 gbps bantgenişliği ile ~ 600 gpbs trafik
- Hping, scapy araçları



ICMP Smurf Saldırıları

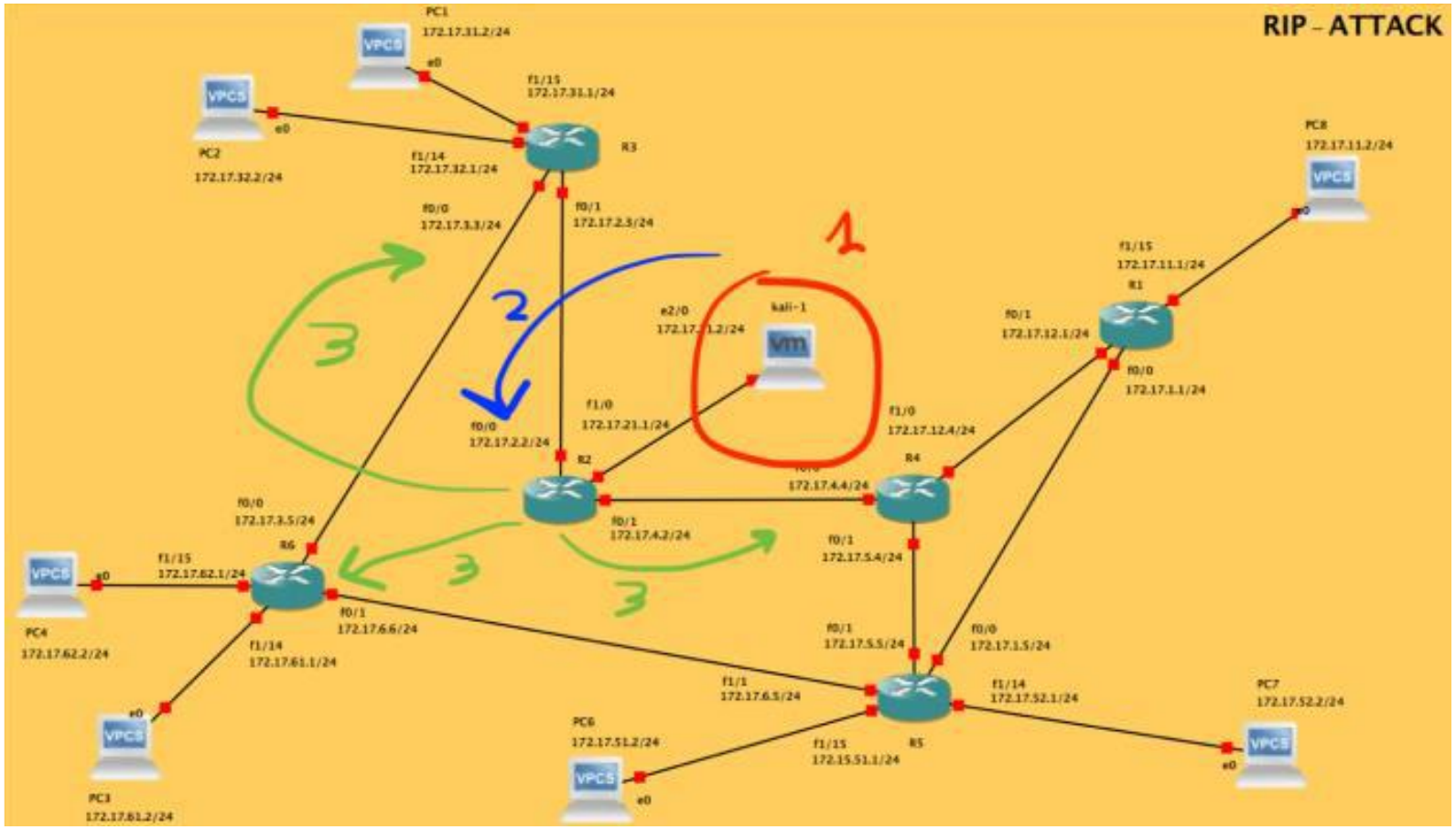
- Bir Smurf saldırısı, bilgisayar ağlarını çalışmaz hale getiren bir tür dağıtılmış hizmet reddi (DDoS) saldırısıdır. Smurf programı bunu İnternet Protokolü (IP) ve İnternet Denetim İletisi Protokolü (ICMP) güvenlik açıklarından faydalanarak yapar.
- Bir Smurf saldırısının adımları şunlardır:
  - Öncelikle kötü amaçlı yazılım sahte IP adresine ekli bir ağ paketi oluşturur. Bu teknik, "zehirlenme" olarak bilinir.
  - Paketin içinde bulunan bir ICMP ping mesajı, paketi alan ağ düğümlerinin yanıt göndermesini ister.
  - Ardından bu yanıtlar veya "yankılar" tekrar ağ IP adreslerine gönderilerek sonsuz bir döngü oluşturulur.
- **Alınabilecek Önlem;**
  - Ağa gelen yönlendirilmiş yayın trafiğini engellemek
  - Ana makineleri ve yönlendiricileri ICMP yankı isteklerine yanıt vermeyecek şekilde yapılandırmak



RIP Protokolü Zafiyet Analizi

- RIP v1 **255.255.255.255** adresine broadcast olarak, RIP v2 **244.0.0.9** adresine ve RIP v3 **FF02::9** adresine multicast olarak yayın yapmaktadır. Bu durum protokolde zafiyete neden olan en önemli noktadır.
- RIP, UDP tabanlı bir protokoldür. RIP kullanan her yönlendiricinin, RIP-1/RIP-2 bağlantı noktası olan **520** numaralı UDP bağlantı noktası üzerinde datagram gönderen ve alan bir yönlendirme işlemi vardır. Başka bir yönlendiricinin RIP işlemine yönelik tüm iletişimler, RIP bağlantı noktasına gönderilir. Tüm yönlendirme güncelleme mesajları, RIP bağlantı noktasından gönderilir. İstenmeyen yönlendirme güncelleme mesajlarının hem kaynak hem de hedef bağlantı noktası, RIP bağlantı noktasına eşittir. Bir isteğe yanıt olarak gönderilen güncelleme mesajları, isteğin geldiği bağlantı noktasına gönderilir. RIP bağlantı noktası dışındaki bağlantı noktalarından belirli sorgular gönderilebilir, ancak bunların hedef makinedeki RIP bağlantı noktasına yönlendirilmesi gerekir. Bu zafiyetten yararlanmak için sahte RIP paketleri oluşturmak ve PCAP yardımıyla hedef routera göndermek yeterlidir.
- **Alınabilecek Önlem;**
- RIP zafiyetinden korunmak için özellikle RIP v2 ve v3 versiyonlarında mevcut olan **Authentication** desteğini etkinleştirmek gerekmektedir. Authentication desteği etkinleştiği zaman ağda bulunan bir router kendisine gelen RIP paketlerini kabul etmeden önce göndericinin kimliğini doğrulama işlemi yapar.

RIP Protokolü Zafiyet Analizi-devam

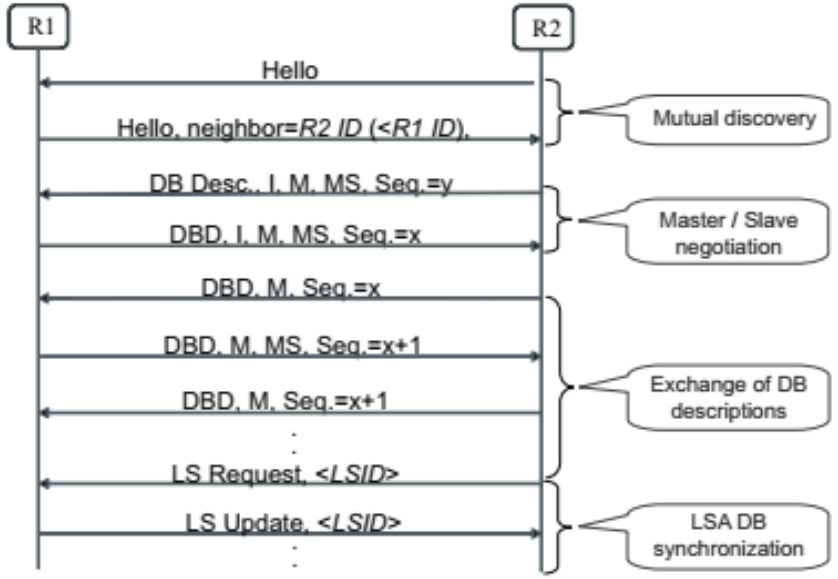


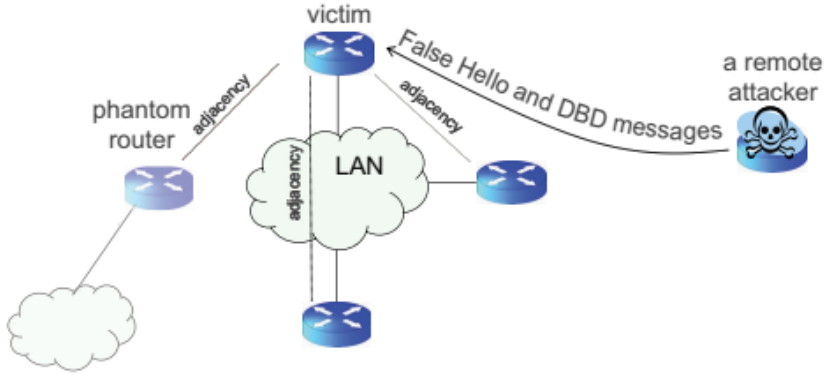
OSPF Protokolü Zafiyet Analizi

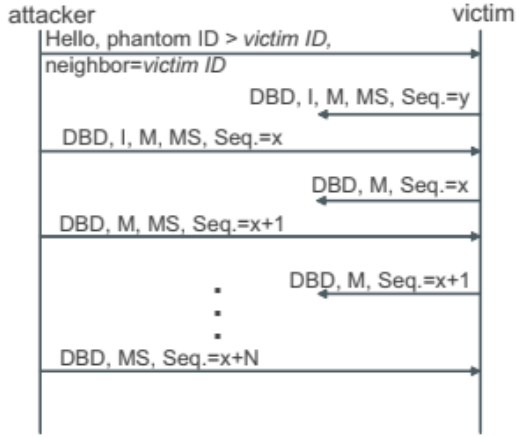
- OSPF yapılandırmasına sahip yönlendirici varsayılan olarak her 30 saniyede bir **225.0.0.5** adresine ortamda başka OSPF yönlendirici olup olmadığını anlamak için **Hello** paketi gönderir. Bu mesajı alan OSPF yönlendirici buna cevap vererek komşuluk ilişkisi kurulur. OSPF saldırılarında da temel güvenlik zafiyeti burada oluşmaktadır.
- Saldırı yapmak için yönlendirici gibi davranan bir bilgisayar sahte OSPF Hello mesajları oluşturur ve gönderir. Bunu alan OSPF yönlendirici komşuluk ilişkisi kurmak için kendi ID'si içeren bir cevap mesajı gönderir. Bu noktada OSPF yönlendiricilerden birisi DR (designated router) seçilir. DR seçimi yönlendirici ID'si en yüksek olan seçilir. Saldırgan oluşturduğu sahte OSPF paketindeki ID bilgisini kurbandan yüksek yapar ve önce kendi üzerinde bulunan sahte OSPF yönlendirme tablosunu kurban yönlendirici ile paylaşır. Kurban yönlendirici de kendi üzerindeki yönlendirme tablosunu saldırgan ile paylaşır.
- **Alınabilecek Önlem;**
- OSPF yapılandırmasında zafiyetten korunmak için öncelikle **authentication** mutlaka etkinleştirilmelidir. Ayrıca authentication işleminde oturum bilgileri düz metin olarak değil **MD5** şifreli olarak seçilmelidir.

OSPF Protokolü Zafiyet Analizi-devam

- OSPF protokolünün authentication desteği olması authentication işlemi sırasında şifre-kullanıcı adı bilgilerinin MD5 şifreleme kullanılarak iletilmesi RIP protokolüne göre bu sahte mesaj oluşturma işlemini zorlaştırmaktadır. Ancak MD5 şifreleme de günümüz bilgisayar sistemlerinde kaba kuvvet saldırıları ile devre dışı bırakılabilmektedir.







BGP Protokolü Zafiyet Analizi

- BGP'de, yönlendirme tablolarının paylaşımında **MD5 temelli authentication** işlemi yapılmakta ve iletişim TCP 179 nolu porttan yapılmaktadır. Ancak ortadaki adam saldırılarında sıkça görülen TCP oturumlarının çalınması durumu yaşanabilmektedir. Bu durumda ağ trafiği saldırgan tarafından dinlenebilmekte veya saldırgan tarafından oluşturulan sahte bir rotanın yönlendirme tablosuna eklenmesi yapılabilmektedir.
- BGP protokolünde sorun olan bir diğer zafiyet ise saldırgan tarafından ele geçirilmiş veya yetkili kullanıcı tarafında yanlış yapılandırılmış bir yönlendiricinin **yanlış rota bilgilerini** sisteme enjekte etmesidir. Bu durumda iletişim kopabilmekte veya ağ trafiğinin verilen yanlış rota üzerinden akmasına neden olabilmektedir.
- **Alınabilecek Önlem;**
- BGP internet ağındaki veri trafiğini yönettiği için internette yapılan her türlü veri transferinin şifreli olarak yapılmalıdır. Bir otonom sistem internete çıkış yapacak ise servis sağlayıcılar tarafından yönlendirici yapılandırması çok dikkatli olarak yapılmalıdır.

Katman 3 Saldırıları Özet Tablosu

	Saldırı Türleri		Hedef Sistem	Etkisi	Araçlar
Katman 3 Saldırıları	**IP Saldırıları**	IP Aldatması	L3 Switches, Routers	IPS/IDS ve Güvenlik duvarlarını geçme	Scapy, Ostinato
	IP Paket Fragmantasyon Saldırıları	Teardrop/Syndrop/Bonk	L3/L4 Switches, Routers, Blade Sunucular	İşletim sistemi temelli DoS, kaynak tüketimi	Scapy, Targa3 DoS
		Nesta Saldırısı			
		Jolt/Dead ping saldırıları			
		Tekrarlayıcı paket sald.			
	ICMP Saldırıları	ICMP Yeniden Yönlendir	Routers, Switchler, Firewall, Son kullanıcılar	MiTM, DoS/DDoS	Scapy, Responder, StreamDivert, Packet-Flooder, Hyenae-NG, BoNeSi
		Smurf/Fraggle			
		Ping Seli (DoS,DDoS)			
	NDP Saldırıları	NDP Tablo Exhaustion	IPv6 Cihazları	Yeniden yönlendirme, DoS	Wireshark, Bettercap
		NS Aldatması			
		NUD Hatası			Scapy
	MLD Saldırıları	MLD Seli, Trafik Amplifikasyonu	Multicast Routers	Ram, CPU gibi sistem kaynakları tüketimi, DoS	Trex, WARP17
		MLD Snooping			
	Yönlendirme Protokol	RIP, OSPF, IS-IS, EIGRP kötüye kullanma	Routers, L3 Switches	DoS, Blackhole, Wormhole, MiTM	Scapy, loki, GatewayBleeding

Router Üzerindeki Sıkılaştırmalar

S.Nu	Alınacak Tedbir
1	En son üretici yazılımının kullanılıp kullanılmadığını kontrol edin.
2	Yönlendiricinin bir modeme erişimi IP adresine göre engelleyip engellemediğini kontrol edin.
3	Ağa yeni bir cihaz katıldığında yönlendirici üzerinde tanımlı Admin'in uyarı alıp almadığından emin olun.
4	LAN üzerinde UPnP'i disable edin.
5	Port yönlendirme ve IP filtrelemeyi etkinleştirin.
Yerel Yönetim	
6	Eğer cihaz destekliyorsa, HTTPs etkinleştirin.
7	HTTPs destekleniyorsa, admin erişimi sadece bu yolla sağlansın.
8	Web arabirimi için kullanılan TCP/IP bağlantı noktasının değiştirilip değiştirilemeyeceğini kontrol edin
9	Yerel admin erişimine kısıtlamak için, DHCP aralığından sadece bir IP adresi alınmasına izin verin.
10	Yönetici erişiminin yalnızca Ethernet ile sınırlandırılıp sınırlandırılamayacağını kontrol edin
11	Yönlendirici erişiminin SSID ve/veya VLAN tarafından kısıtlanıp kısıtlanamayacağını kontrol edin
12	Yönlendirici, aynı kullanıcıID'ye sahip birden fazla bilgisayarın aynı anda oturum açmasına izin vermemelidir.
13	Çok fazla başarısız denemeden sonra web arayüzüne giriş yapmak için bir tür kilitleme olup olmadığını kontrol edin

Router Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
Uzak Yönetim	
14	Varsayılan tarafından uzak yönetim ayarlarının kapalı olduğundan emin olun.
15	Bağlantı noktası numarasının uzaktan değiştirilip değiştirilemeyeceğini kontrol edin.
16	Yönlendirici oturumunu kapatmayı unutursanız, sonunda oturumunuz zaman aşımına uğramalı ve zaman sınırını ayarlayabilmelisiniz, daha kısa, daha güvenli
Router Güvenlik Duvarı	
17	**Inbound (Gelen) WAN:** Internet tarafında hangi default olarak hiçbir portun açık olmaması gerekmektedir. Sadece uzak bağlantılar için ilgili ISP tarafından atanmış bir port bulunabilir.
18	**Outbound (Giden) WAN:** Giden güvenlik duvarı kuralları ile engellenebilecek birçok saldırı türü vardır. Genel olarak, kurumsal ağlardaki yönlendiricilerin aksine, branch ofislerdeki yönlendiriciler giden güvenlik duvarı kuralları sunmazlar.