HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

KOKLAYICILAR:

Sniffing Nedir?

Sniffing türkçe anlamı ile koklama bilgi güvenliğinde giden gelen veriyi araya girerek ele geçirmektir.Sniffing'in genel amacı hassas veri elde etmektir.

Network Sniffing Nedir?

Network sniffing

Sniffing Tehditleri:

Saldırgan promiscius modda bütün ağı dinleyebilir.Analiz etmek üzere kaydedebilir

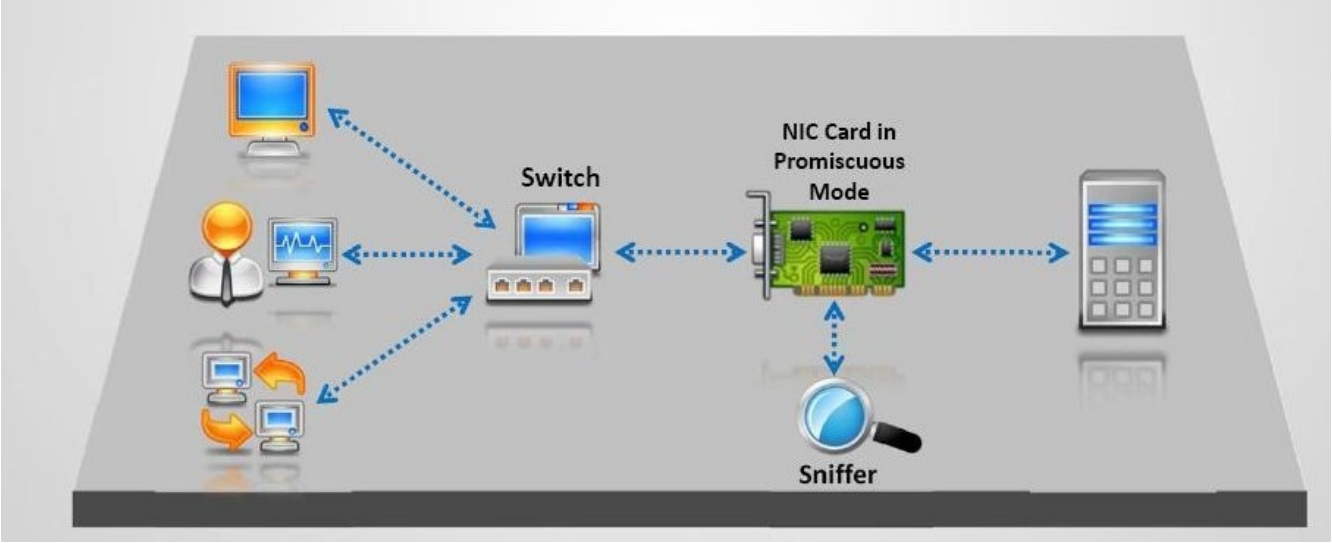
Elde edebileceği bilgiler şifresiz olarak gönderilen http web login bilgileri,girilen siteler irc logları,gelen giden epostalar, ftp şifreleri olmak üzere genişletilebilir.

Koklayıcı sadece yer aldığı ağdaki bilgileri elde edebilir.

Havaalanları halka açık internet hizmetinin aktif olarak kullanıldığı yerlerde ağa bağlı olan kötü niyetli bir kullanıcı aynı ağda yer aldığı kişilerin hangi sitelere girdiğini, şifrelerini ve hassas verilerini elde edebilir.

Koklayıcı nasıl çalışır?

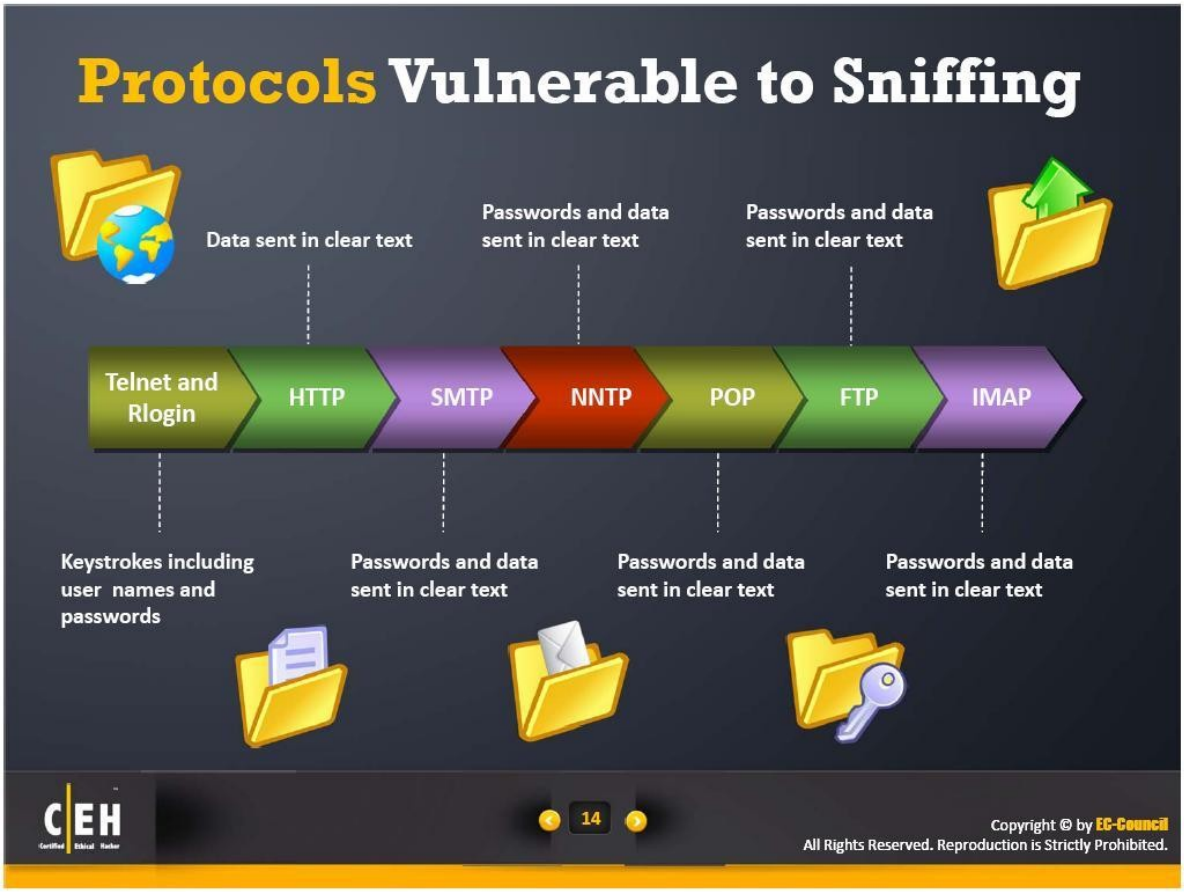
Koklayıcı promisc mod ile çalıştırıldığı netwok kartında LAN(yerel alan ağı) üzerinde iletilen her veri paketi koklayıcı tarafından alınır, okunur ve kaydedilerek analiz edilebilir.



Promiscious Mode Nedir?

Promisc mod kablolu NIC(Network Interface Controller) kartlarının bir modudur. Aynı subnetde yer alan tüm paketlerin bir kopyasını kendi üzerine alır. Promisciuous modda çalışabilmek için yönetici hakları gerekmektedir.

Kaynak:http://searchsecurity.techtarget.com/definition/promiscuous-mode



Sniffing'e karşı etkisiz kalan protokoller.

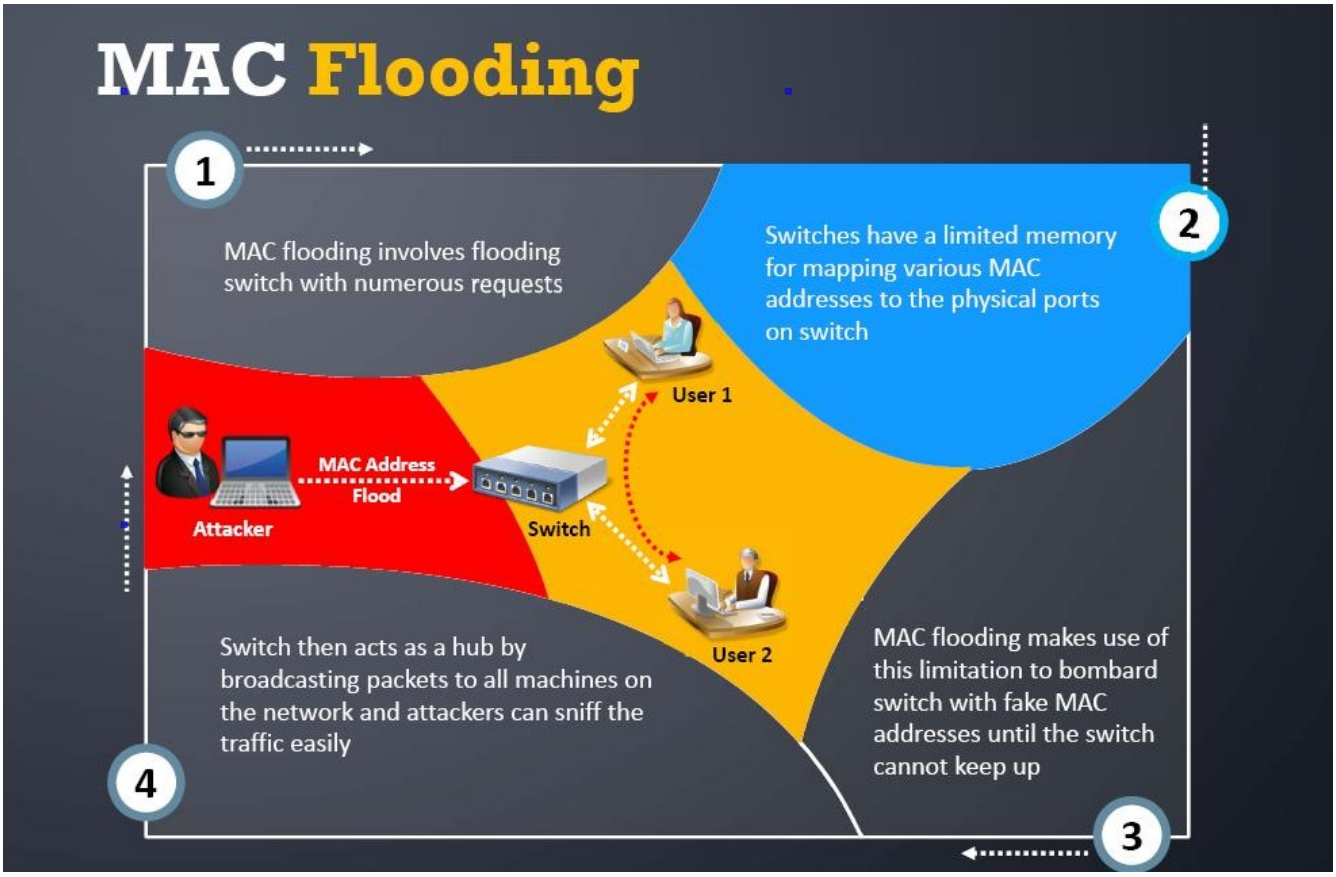
Snifferlar data link katmanında çalışırlar.Data Link katmanı güvenliksiz şekilde bırakılırsa diğer bütün katmanlar otomatik olarak dinlenebilmektedir.

SPAN (Switched Port Analyzer):

Span Port switch'den geçen her paketin bir kopyasını kendi üzerine analiz etmek üzere alan port mirroring ya da port monitoring için kullanılan switch portudur.

Aktif Sniffing Çeşitleri:

Mac Flooding Nedir? Nasıl yapılır?



1.Mac flooding ya da DoS switchlerin mac adres tablosunu doldurarak sürekli istek göndererek meşgul bırakarak cevap veremez hale getirmektir.
2.Switchler sınırlı sayıda MAC adres tablosuna sahiptir.
3.Mac adres tablosu dolar.Böylece tabloya eklenmek istiyen hostlar tabloya dahil olamaz.Bu durumda switch hub gibi davranmaya başlar.
4.Mac flooding sayesinde switch ağda yer alan bütün bilgisayarlara broadcast yapar.Sonucunda ise sniffing işlemi yapılabilir hale gelir.

Önlem(Cisco için):

Portlarda default olarak port security kapalı durumdadır.

Switch(config-if)#switchport port-security

Komutuyla aktif hale getirilir.

Switch (config-if)#switchport port-security maximum

Arp Spoofing

Address resolution protokolü manipüle ederek kullanılan saldırı çeşidi.

ARP Spoofing adımları:

cat /proc/sys/net/ipv4/ip_forward

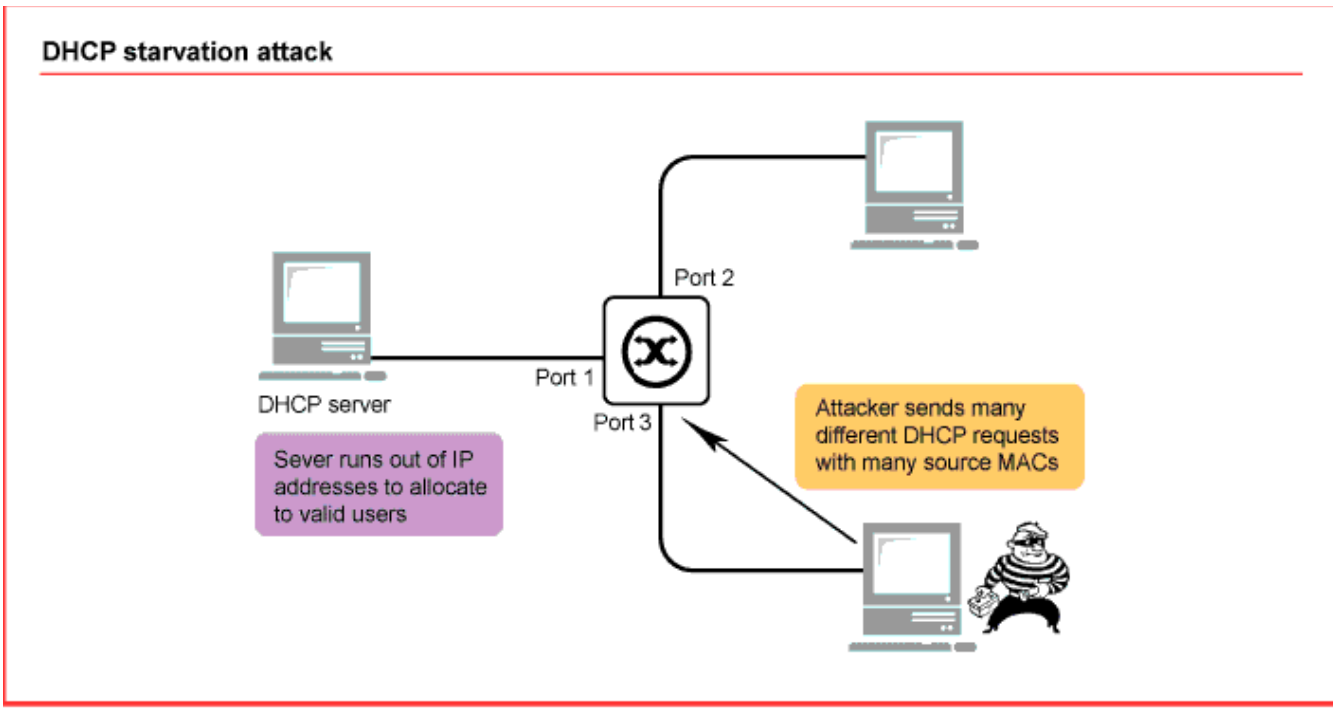
echo 1 >> /proc/sys/net/ipv4/ip_forward

arp -i eth0 -t hedef gateway
arp -i eth0 -t gateway hedef

Not:interface kablosuz ise wlan0 ya da seçili olarak gelen olur.

ettercap vb. Araçlar kullanılabilir.

DHCP Starvation



Resimde yer alan dhcp starvation saldırısında saldırgan dhcp sunucusuna farklı kaynaklı mac adreslerinden ardı ardına istek gönderir.DHCP sunucusu istekler karşısında ip ataması gerçekleştiremez.Ağa bağlı kullanıcılar yeni ip alamaz ve internet bağlantıları işlemez hale gelir.

DHCP starvation ataktan korunmak için mac istek sınırlandırması önlemi varsa alınmalı aksi durumda ise dhcp sunucusu kapatılarak manuel olarak yerel ağda fazla bilgisayar olmadığı durumda statik ip ataması yapılmalıdır.

Pasif Sniffing:

Hublar aracılığıyla broadcast'i diğer bilgisayarlar yapar. Günümüzde switch kullanımının artmasıyla popülaritesini yitirmiştir.

Sniffing Tespit:

PromqryUI

PromiScan vb. Araçlar kullanılabilir.Snort, suricata gibi IDS programları ile güvenlik ihlalleri tespit edilebilir.

WİRESHARK:

Wireshark birçok protokolü destekleyen promiscious modda çalıştırıldığı takdir de ağın dinlenmesine olanak sağlayan gelişmiş açık kaynak bir sniffing aracıdır.

Wireshark ile istenilen protokoller gerekli filtreler girildiği takdir de dinlenebilir.

Wireshark kullanımını kolaylaştıran display filters listesi için adres:

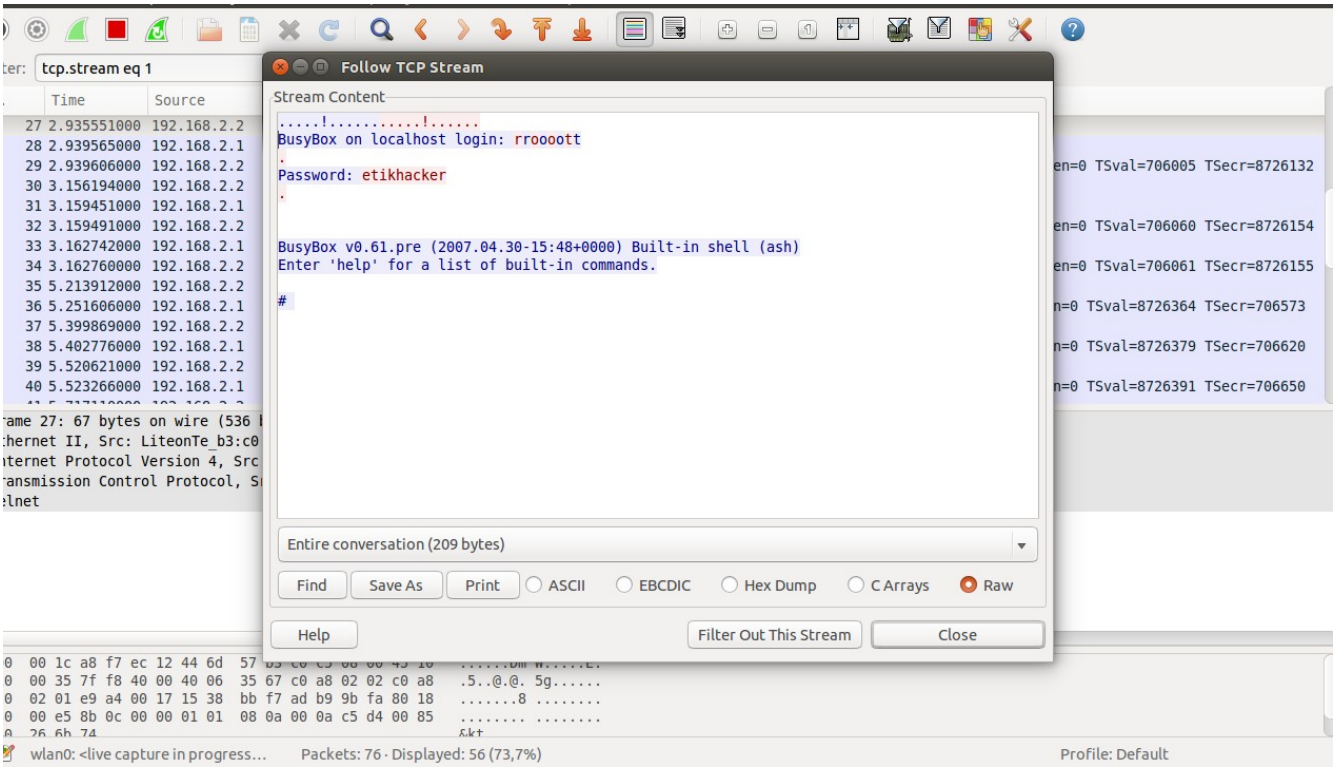
http://wiki.wireshark.org/DisplayFilters

Display filter örnekleri:

hedef domainin ipsini çözdükten sonra sadece o ip numarasındaki paketleri izlemek için:

Port isteklerini görme:
Aşağıdaki istek telnet trafiğini görüntüler.
tcp.port==23

Resimde “follow tcp stream” denildikten sonra telnet ile gönderilen şifre görülmektedir.



ip.dst == 192.241.86.68

kaynak yerel ip için:

ip.src == 192.168.2.2

http istekleri için:

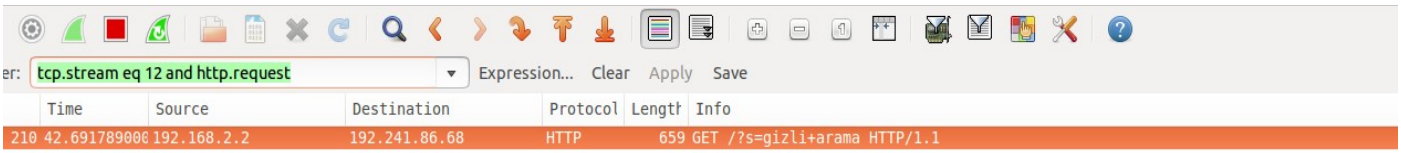
http.request
http.response

Derste yapılan uygulamada http paketlerinden POST edilenler “follow tcp stream” tıklandığı zaman şifreler elde edilebilmektedir.Çünkü http protokolü şifresiz çalışmaktadır.

içinde “password” geçen tcp paketleri için:

tcp contains password

Aşağıdaki “display filter” web sitesinde yapılan aramayı göstermektedir.



Alınabilecek Önlemler:

Şifrelemeli bağlantı kullanılmalıdır.VPN vb.
Ağgeçidinin MAC adresi ARP önbelleğine eklenmelidir.
Statik IP adresleri ve static arp tabloları kullanılarak saldırganların sahte arp girdileri eklemeleri engellenir.
Mac adresi filtrelemesi yapılmalıdır.
Telnet ftp yerine ssh gibi dosya transfer araçları kullanılmalıdır.