DHCP SERVİSİNE YENİ BİR BAKIŞ

Gökhan AKIN

İTÜ/BİDB Ağ Grubu Başkanı
ULAK-CSIRT Güvenlik Grubu Üyesi

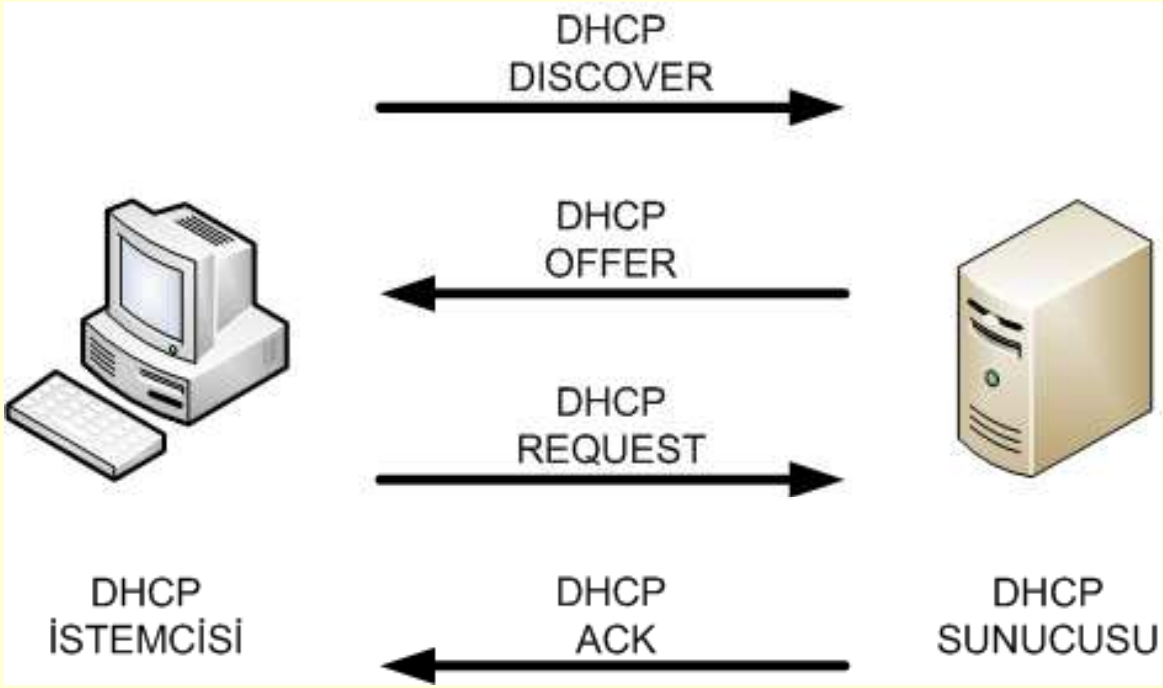
http://www2.itu.edu.tr/~akingok

DHCP Servisi

Dynamic Host Configuration Protocol", RFC 2131:

IP bazlı çalışan istemcilerin IP adresleri, alt ağ maskeleri gibi tanımlanması gereken ayarların otomatik olarak bir sunucu tarafından ayarlanmasını sağlayan protokol

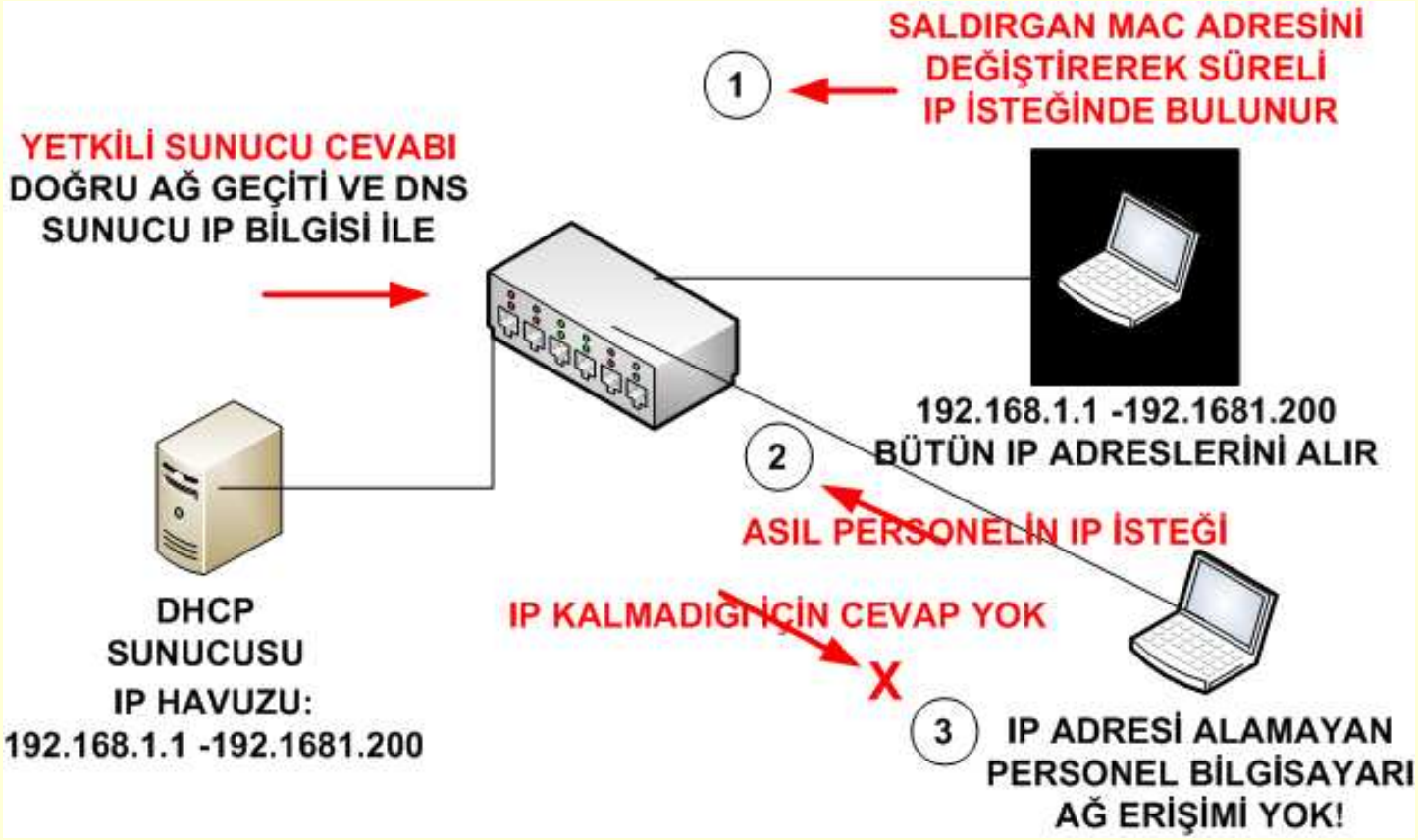
DHCP Servisi



No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
2	0.003211	192.168.1.1	192.168.1.102	DHCP	DHCP Offer
3	0.003950	0.0.0.0	255.255.255.255	DHCP	DHCP Request
4	0.007659	192.168.1.1	192.168.1.102	DHCP	DHCP ACK

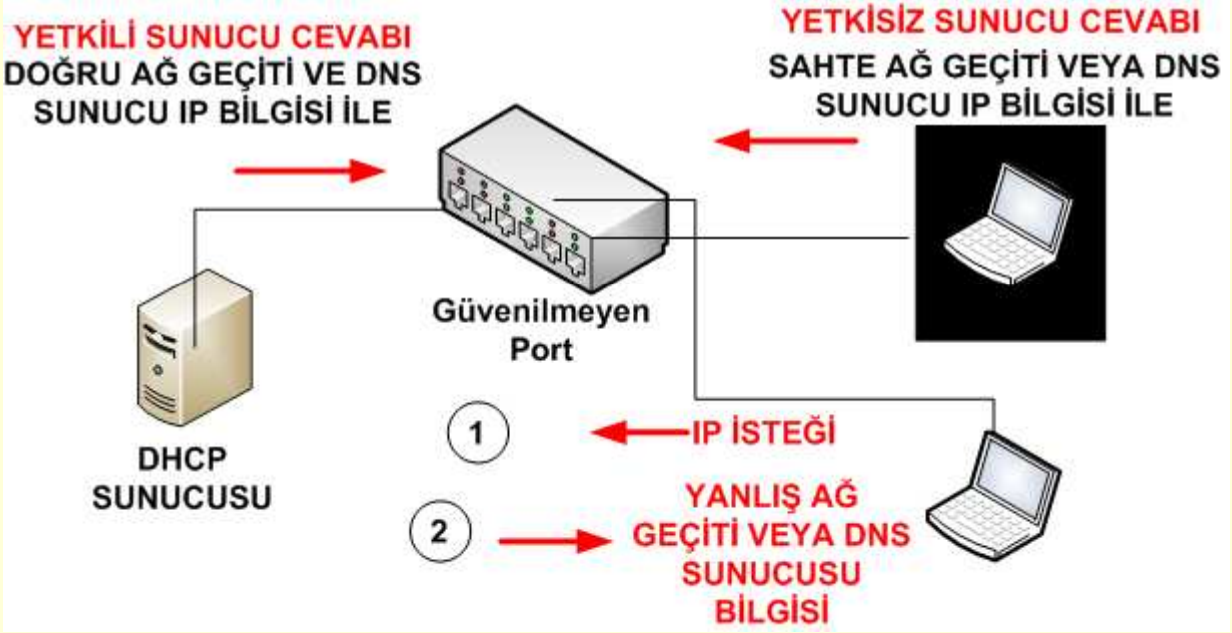
DHCP Servisinin Güvenlik Sorunları

A.DHCP Sunucusunun IP Havuzunun Boşaltılması



DHCP Servisinin Güvenlik Sorunları

B.Yetkisiz DHCP Sunucusu Kurulumu ile İstemcilere Yanlış Adreslerin Atanması



DHCP Servisinin Güvenlik Sorunları

B.Yetkisiz DHCP Sunucusu Kurulumu ile Yapılabilecekler:

1. *Kendisini ağ geçidi gösterir. IP dağıttığı herkesin trafiğini kendi üzerinden geçirir. (Aradaki adam atağı)*

Fazla sayıda bilgisayar için ağ geçidi olması durumunda ağ erişiminde yavaşlama olacaktır. Bu durum tespit edilmesini kolaylaştırır.

SSL ile güvenli şekilde erişilen siteler ile ilgili bilgilere erişim sağlanamaz.

DHCP Servisinin Güvenlik Sorunları

B.Yetkisiz DHCP Sunucusu Kurulumu ile yapılabilecekler:

2. *İstemcilere sahte DNS sunucusu IP'si dağıtabilir.*

DNS sunucusu sorunsuz çalıştığı sürece tespiti biraz süre alabilir.

Bankacılık vb sitelere ulaşılmak istendiğinde kullanıcı sahte siteye yönlendirilebilir. SSL güvenliği sahte sitenin geçerli sertifikaya sahip olmadığını uyarabilir.

DHCP Servisinin Güvenlik Sorunları

İKİ FARKI BULUN

Değişen Şartlar

Bu şekilde saldırı ihtimali hep vardı. Neden şimdi önemli?

Önceki Koşullar:

1. Aynı yerel alan ağına aynı kurumun personeli bağlanıyordu, DHCP ve benzeri atak firma içi bir personel tarafından yapılabilirdi.

2. Dial-up ve DSL gibi Internet erişimlerinde DHCP ve benzeri L2 ataklar yapılamıyordu.

Değişen Şartlar

Günümüzdeki Koşullar:

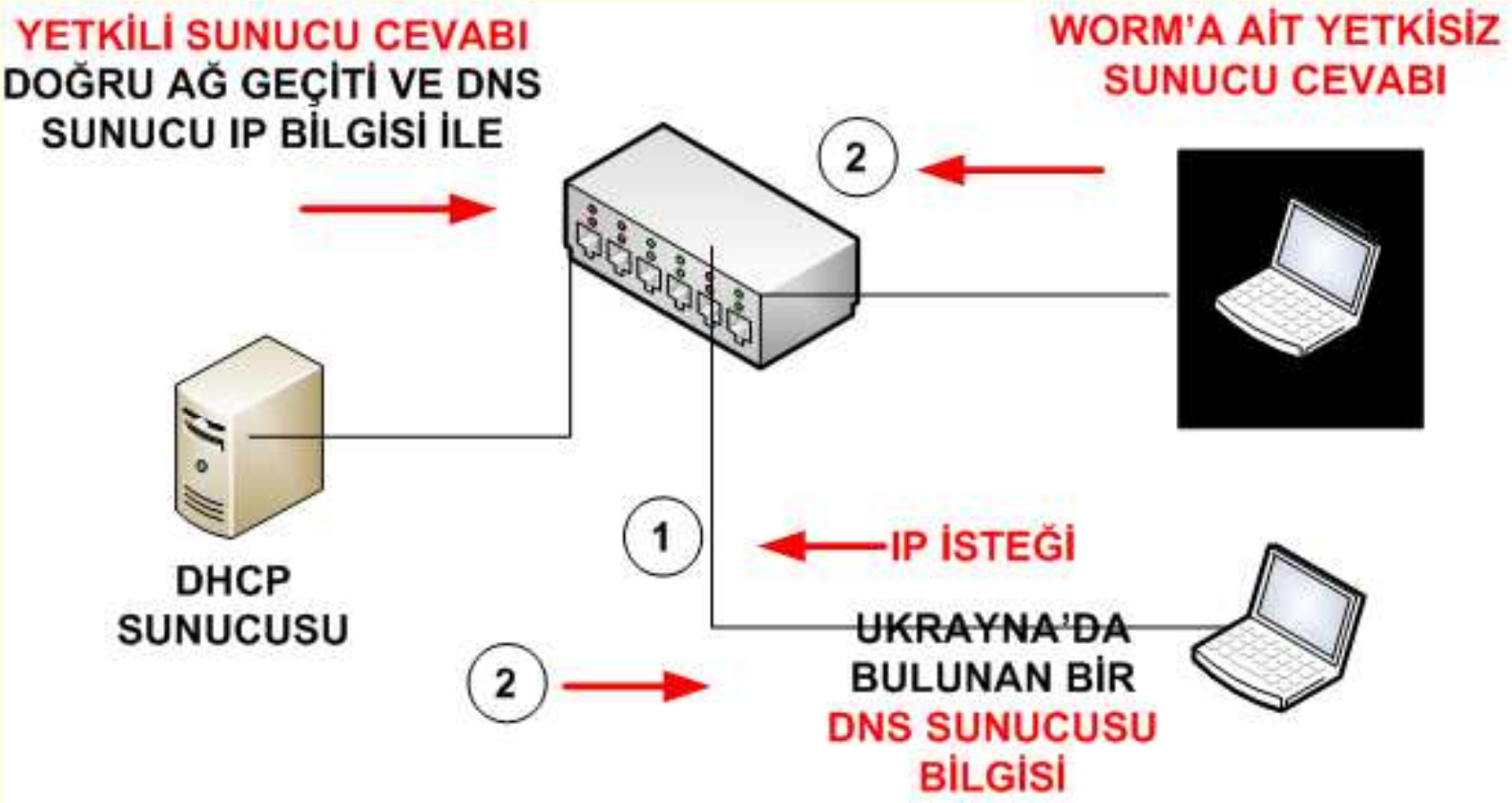
1. Aynı broadcast domain'de personel olmayan kullanıcıların kablosuz veya kablolu erişimi arttı
2. Bu gibi atakları yapabilen Worm vb zararlı yazılımların yaygın hale gelmesi

Kullanım Yerleri:

1. Otel,yurt gibi kısmen kontrol altında olan yerde Internet erişimi sağlanması

2. Geçici misafir erişimi sağlanması

İTÜ'de 2008 Sonbaharında Yaşanan Olay



İTÜ'de 2008 Sonbaharında Yaşanan Olay

SAHTE SUNUCU:

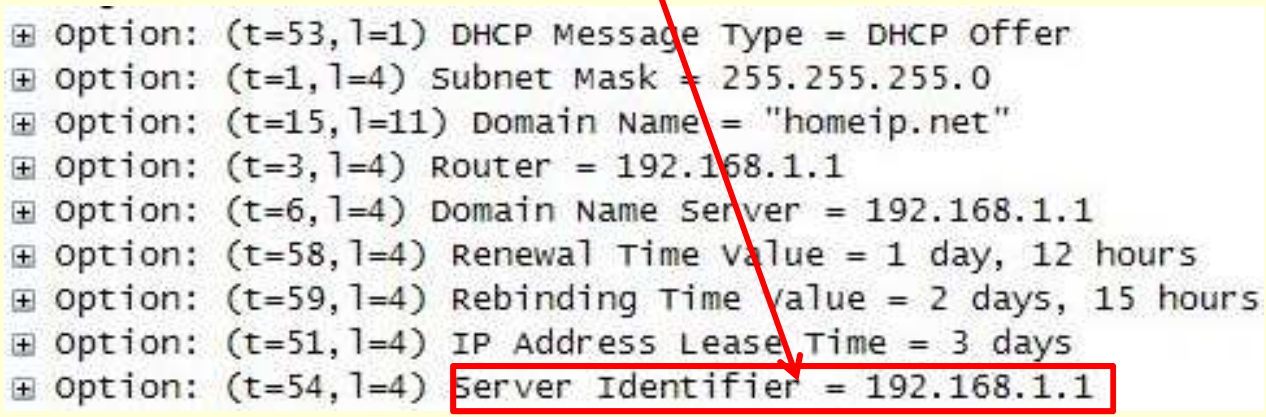
-İstemciye doğru ağ geçidi adresi,

- Doğru Altağ Maskesi

- Doğru DHCP sunucusu adresini

- Çalışan ama Ukrayna'da bulunan DNS Sunucusu

***- Tek hata** 160.75.200.0 255.255.255.0 Ağına alt ağ maskesini hesaba katmadan B Sınıfından Örneğin 160.75.143.0 gibi gelişi güzel IP vermesi.*



DHCP Servisine Yönelik Güvenlik Çözümleri

- DHCP mesajları için kimlik denetimi, RFC 3118 (yıl 2001)

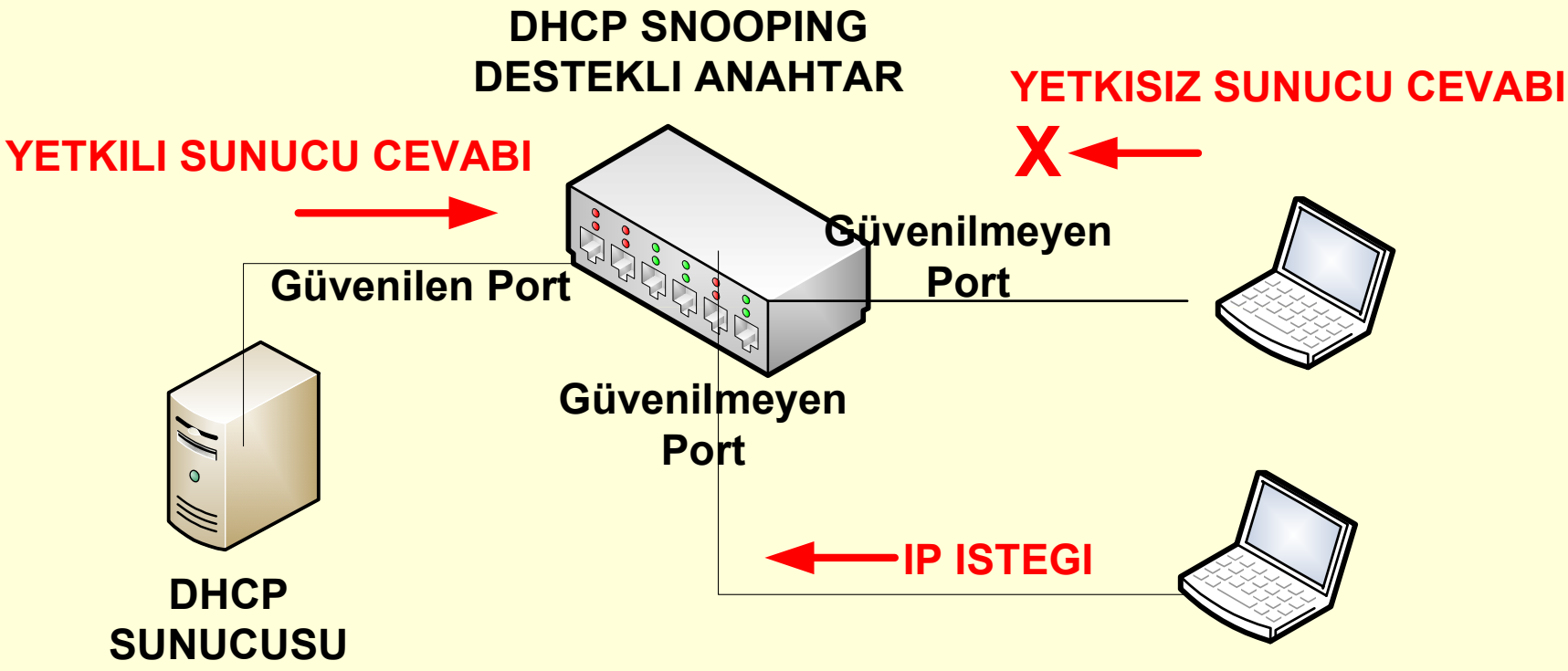
-DHCP Dinleyici programlar, istemci gibi IP adresi isteğinde bulunup cevap veren DHCP sunucularını loglayan yazılımlar kullanmak (Örnek: DHCP Probe)

-802.1X kimlik denetim sistemi kullanılması

-Yerel alan ağı 2. katman anahtarlarında DHCP Snooping özelliği ile sadece yetkili porta takılı istemcinin DHCP sunucusu olabilmesinin sağlanabilmesi

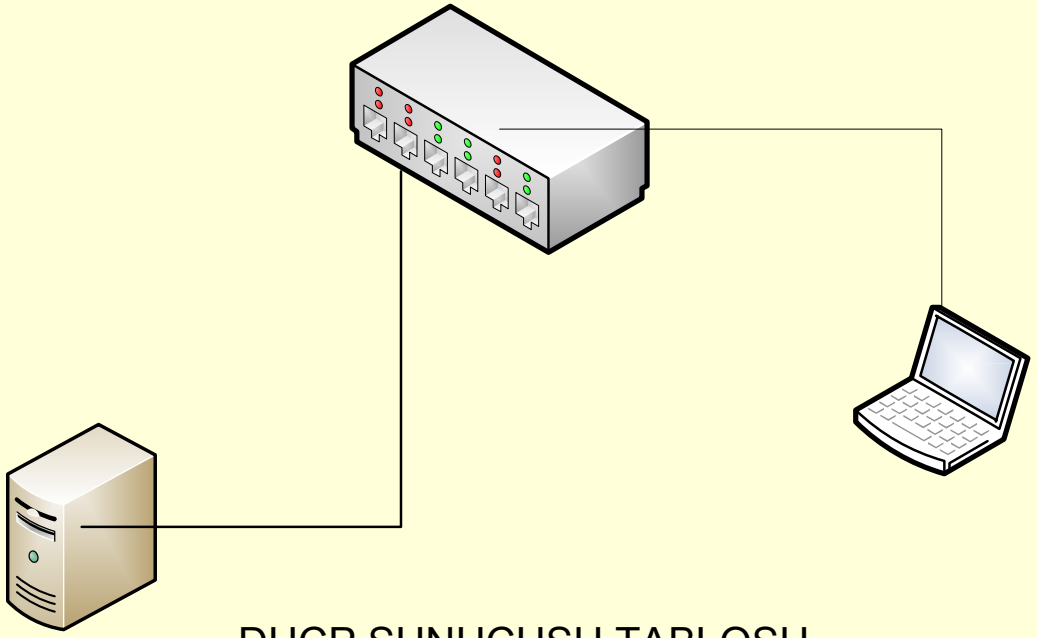
DHCP Servisine Yönelik Güvenlik Çözümleri

DHCP Snooping Çözümü



DHCP Option 82 Verisinin Değerlendirilmesi

DHCP Snooping Destekli Anahtar
MAC Adresi:00AA.AAAA.AAAA



DHCP'den IP alan
5 Numarlı Port
Bağlı İstemci

DHCP SUNUCUSU TABLOSU

IP Adresi	Donanım(MAC) Adresi	Bağlandığı anahtarın Adresi	Portu
10.0.0.100	0011.1010.1010	00AA.AAAA.AAAA	5
10.0.0.102	0011.1212.1212	00AA.AAAA.AAAA	6

Tasarlanabilecek Yeni DHCP Sunucusu

SAHİP OLUNAN ANAHTAR CİHAZ LİSTESİ

Anahtarın MAC Adresi	IP adresi	Modeli	Kampüsteki Yeri
00AA.AAAA.AAAA	10.0.0.1	ABC 24 port Ethernet Sw	Insaat Fakultesi 1.Kat
00AA.AAAA.AAAB	10.0.0.2	ABC 24 port Ethernet Sw	Insaat Fakultesi 2.Kat
00AA.AAAA.AAAC	10.0.0.3	ABC 24 port Ethernet Sw	Insaat Fakultesi 3.Kat

CİHAZLARIN PORTLARINA BAĞLANTI DETAYI

Anahtarın MAC Adresi	Port no	Priz No	Oda
00AA.AAAA.AAAA	1	11	101 nolu oda
00AA.AAAA.AAAA	2	12	101 nolu oda
00AA.AAAA.AAAA	3	13	102 nolu oda
00AA.AAAA.AAAA	4	14	102 nolu oda
00AA.AAAA.AAAA	5	15	103 nolu oda
00AA.AAAA.AAAA	6	16	103 nolu oda
00AA.AAAA.AAAA	7	17	104 nolu oda
00AA.AAAA.AAAA	8	18	104 nolu oda

OPTION 82 BİLGİSİ İLE BERABER DHCP SUNUCUSU LOGU

Anahtarın MAC Adresi	Port No	Verilen IP adresi	İstemcinin MAC Adresi	Verilme Tarihi	Verilme Saati
00AA.AAAA.AAAA	5	10.10.0.1	00BB.BBBB.BBBB	10.10.2008	10:21

Ayrıca port bazlı DHCP Rezervasyonu da yapılabilir.

Statik IP Verilmesinin Engellenmesi

Source Guard Özelliği

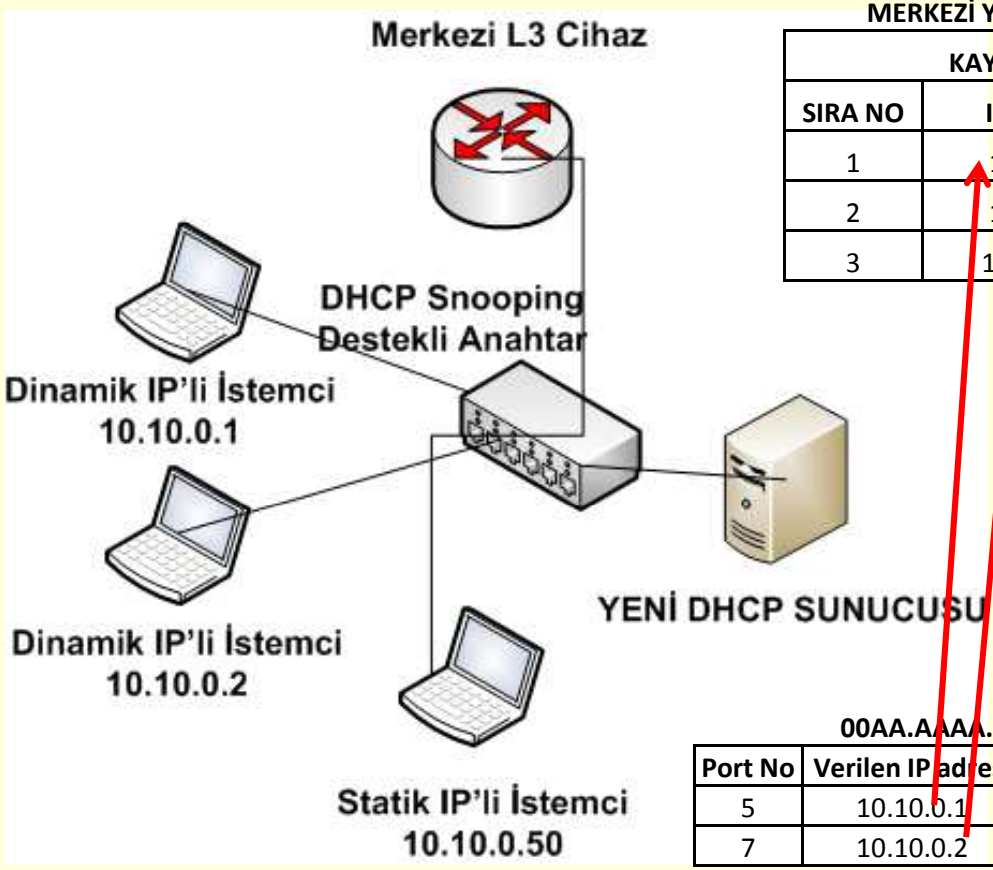
00AA.AAAA.AAAA MAC ADRESLİ ANAHTARIN DHCP BINDING TABLOSU

Port No	Verilen IP adresi	Istemcinin MAC Adresi	Verilme Tarihi	Verilme Saati
5	10.10.0.1	00BB.BBBB.BBBB	10.10.2008	10:21
7	10.10.0.2	00BB.BBBB.BBBC	10.10.2008	12:10

Anahtar cihazı "Source Guard" açıldığı zaman tuttuğu bu tablo dışındaki bir IP adresi dışında hiçbir istemcinin ağa erişmesine izin vermez.

Ancak bu özelliğe sahip anahtar cihazları biraz pahalı olduğundan bütün istemcileri böyle bir cihaza bağlamak pek mümkün olmuyor.

Başka Bir Çözüm



MERKEZİ YÖNLERDİRİCİ ARP TABLOSU

KAYIT OLAN İSTEMCİNİN		
SIRA NO	IP ADRESİ	MAC ADRESİ
1	10.10.0.1	00BB.BBBB.BBBB
2	10.10.0.2	00BB.BBBB.BBBC
3	10.10.0.50	00CC.CCCC.CCCC

← **FARK**

Yöneticiyi uyaran Log!

00AA.AAAA.AAAA MAC ADRESLİ ANAHTARIN DHCP BINDING TABLOSU

Port No	Verilen IP adresi	Istemcinin MAC Adresi	Verilme Tarihi	Verilme Saati
5	10.10.0.1	00BB.BBBB.BBBB	10.10.2008	10:21
7	10.10.0.2	00BB.BBBB.BBBC	10.10.2008	12:10

Belirli sıklıkta merkezi L3 cihazının ARP tablosu DHCP sunucusu tarafından alınıp ARP tablosundakİ IPler ile DHCP tablosu ile karşılaştırılır.

Sonuçlar

Giderek daha yaygın olarak kamuya açık yerlerde birbirlerini tanımayan istemciler aynı yerel alan ağlarına bağlanmaktadırlar.

- Buda DHCP atağı gibi bir çok atağın daha çok gündeme gelmesine sebep olmaktadır. Yeni kurulan alt yapılarda bu gibi tehditlerin de göz önünde bulundurulması önemlidir.

- DHCP logunun dikkatlice tutulmasının yanı sıra Option 82 desteğinin de bulunması durumunda kullanıcı takibinde bu veride mutlaka değerlendirilmelidir.

Teşekkürler

Gökhan AKIN

İTÜ/BİDB Ağ Grubu Başkanı
ULAK-CSIRT Güvenlik Grubu Üyesi

http://www2.itu.edu.tr/~akingok