Journal of Computer Science
https://dergipark.org.tr/en/pub/bbd
https://doi.org/10.53070/bbd.990930

Journal of Computer Science
ISSN: 2548-1304
Volume: IDAP-2021, Issue: Special, pp: 82-92
@Anatolian Science

Kampüs Ağlarında İnternet Erişimi İçin Bağlantı Katmanı Kimlik Doğrulama Uygulaması

A Link-Layer Authentication Application for Internet Access in Campus Networks

Semra YILDIRIM*[1], Kenan İNCE[2]

[1] Bilgisayar Mühendisliği Bölümü, İnönü Üniversitesi, Malatya, Türkiye
[2] Bilgisayar Mühendisliği Bölümü, İnönü Üniversitesi, Malatya, Türkiye
(semrayldrm44@gmail.com, kenanince@gmail.com)

Received: Sep.3, 2021 Accepted: Sep.16, 2021 Published: Oct.20, 2021

Özetçe— Günümüzde internetin kullanılmadığı bir sektör kalmamış durumdadır. Bunun sonucu olarak hayatımızın her alanında güvenli ve sürdürülebilir internet bağlantısı zaruret haline gelmiştir. Bu denli yaygınlaşan çevrimiçi cihazların yönetimi beraberinde güvenlik sorununu da ortaya çıkarmaktadır. Özellikle internet sağlayıcısı durumunda bulunan kurum ve kuruluşlar için ağa bağlı cihazların tanımlanması, kütük dosyalarının işlenmesi ve herhangi bir hukuki durumda iz sürülebilir olması büyük önem arz etmektedir. Bunu sağlayabilmek adına kurumlar internet hizmeti sunduğu personelini tanımlayabilmeli, yetkisiz girişleri engelleyebilmeli ve çalışma alanı dışındaki web hizmetlerine erişimi kısıtlayabilmelidir. Günümüzde bunu gerçekleştirmek amacıyla belirli bir ölçekten büyük olan kurumlarda güvenlik duvarları hizmet vermektedir. Ayrıca kullanıcı tanımlama konusunda kısıtlayıcı portallar (Captive Portal) kullanılmaktadır.

Bu çalışmada İnönü Üniversitesi örnek alınarak, üniversite kampüs alanları için bir kısıtlayıcı portal uygulaması geliştirilmiştir. Geliştirilen uygulama Eve-Ng ortamında farklı senaryolar üretilerek test edilmiş ve kullanıcı kayıtlanması, yetkilendirilmesi ve internet erişimi başarılı bir şekilde simüle edilmiştir.

Anahtar Kelimeler : *Captive portal, eve-ng, yerel alan ağı, kimlik doğrulama, internet erişimi, ldap.*

Abstract— Today, there is no sector where the internet is not used. As a result, a secure and sustainable internet connection has become a necessity in all areas of our lives. The management of online devices, which have become so widespread, also raises the security problem. Especially for institutions and organizations that are internet providers, it is of great importance to identify devices connected to the network, to process log files and to be traceable in any legal situation. In order to achieve this, institutions should be able to identify the personnel to whom they provide internet services, prevent unauthorized access and restrict access to web services outside the working area. Today, in order to achieve this, firewalls serve in institutions larger than a certain scale. In addition, Captive Portals are used for user identification.

In this study, a Captive Portal application has been developed for university campus areas, taking İnönü University as an example. The developed application has been tested by producing different scenarios in Eve-Ng environment and user registration, authorization and internet access have been successfully simulated.

Keywords : *Captive portal, eve-ng, local area network, authentication, internet access, ldap.*

1.Giriş

Birden fazla makinenin, ihtiyaca göre farklılık gösteren, farklı veri iletim hız ve kapasitesine sahip kablolar kullanılarak birbirlerine bağlanması ile oluşturulan yapılara ağ denmektedir. Ağlar aracılığı ile makineler arasında yazılım, donanım, dosya alışverişi gibi kaynak paylaşımları yapılabilmektedir.

Bilişim sektöründeki gelişmeler gün geçtikçe katlanan bir hız ile artmaktadır. Bunun bir sonucu olarak internet kullanımı da iş, sağlık, eğitim gibi alanlardan sosyal hayatımıza, hatta günlük rutin aktivitelerimize kadar ulaşmış, hayatımızın merkezine yerleşmiştir. İnternet kullanımının etki alanının genişlemesi ve kullanıcı sayısının artması ile ağ yapıları devasa boyutlara ve karmaşıklığa ulaşmıştır. İnternet kullanımı, her yaştan, her sektörden geniş bir kullanıcı kitlesine ulaşmış ve modern hayatın temel bir gereksinimi haline gelmiştir. İnternete kablo kullanılarak ya da kablosuz biçimde iki farklı metotla bağlanılabilir. Günümüzde çoğu kurum ve kuruluş kablosuz yerel alan ağları (WLAN) ile internete kablosuz erişim sağlamaktadır. Kablosuz ağlar, son kullanıcılar ve erişim noktası arasında veri taşımak için radyo iletimlerini kullanır (Soewito, 2014). Buna ek olarak internet kullanıcı sayısının milyarlar seviyesine gelmiş olması ve internetin hayatın her alanında bu denli etkili olması birtakım riskleri de beraberinde getirmektedir. İnternet erişimi ile gerçekleştirilen işlemler güvenlik tehditleriyle karşı karşıya kalabilmektedir. Kötü amaçlı kullanıcılar ağdan ücretsiz yararlanmak, izinsiz veri ve kaynak erişimi sağlamak ve ağı kullanılamaz hale getirmek gibi birçok sebeple internet ağlarına sızmaya çalışabilmektedir. Bu noktada ağdaki kullanıcıların birtakım kısıtlamalar ile denetim altına alınması, kullanıcı erişimlerinin yetkilendirmeler ile sınırlandırılması ve ağ üzerindeki kullanıcı aktivitelerinin izlenmesi ve kaydedilmesi gerekmektedir. 5651 sayılı kanun ile birlikte istemcilerin ağ üzerindeki ziyaret bilgilerinin loglanması kanuni bir zorunluluk haline gelmiştir. Bu alanda yapılan çalışmalar ile ağ güvenliğini sağlamak adına birçok farklı yöntem denenmiştir.

Ağ güvenliğinin sağlanması noktasında ilk olarak 1999 yılında **"**Wired Equivalent Privacy" ifadesinin kısaltması olan WEP (Kabloluya Eşdeğer Gizlilik) protokolü geliştirilmiştir. WEP, ortaya çıkışından itibaren güçsüz bir algoritmaya, güvenlik zaafiyetleri bulunan ve basit yöntemlerle kırılabilecek bir şifreleme mekanizmasına (RC4) sahiptir. Ayrıca WEP ile kimlik denetimi de yapılamamaktadır. Birçok teknoloji şirketinin önderliğinde genel Wi-Fi standartları geliştirmek ve farklı cihazların uyumlu şekilde çalışmasını sağlamak için kurulmuş bir organizasyon olan Wi-Fi Alliance tarafından 2003 yılında WPA geliştirilmiştir. "Wi-Fi Protected Access" ifadesinin kısaltması olan WPA (Wi-Fi Korumalı Erişim), WEP'teki zayıflıkların tümünü ortadan kaldıran WEP tabanlı bir protokoldür fakat kendisinden önceki cihazların sistemlerini destekleyememiştir. WPA saldırılara karşı daha uzun vadede bir direnç göstermiş fakat kullanılan TKIP şifreleme yöntemi de bir süre sonra kırılabilir hale gelmiş ve saldırılar karşısında yeterince güvenli olmadığı kanıtlanmıştır. Bu güvenlik açıkları, TKIP'nin benzer saldırılara izin veren WEP ile aynı mekanizmalardan bazılarını kullanmasından kaynaklanmaktadır (Aryeh, Asante ve Danso, 2016). **"**Wi-Fi Protected Access II" ifadesinin kısaltması olan WPA2 (Wi-Fi Korumalı Erişim II), Wi-Fi Alliance tarafından 2004 yılında WPA'daki eksiklikleri gidermek adına, tamamen yeni bir şifreleme mekanizması kullanılarak geliştirilmiştir. WPA2 şifreleme yöntemi için güvenlik protokolü olarak CCMP-AES'i kullanır ve WPA, veri bütünlüğü için Michael algoritmasını kullanırken, WPA2 daha sağlam, verimli ve daha güçlü bir algoritma olan CBC-MAC'yi kullanır (Adnan ve ark., 2015). WPA2'de client odaklı saldırıların gerçekleştirilebildiği güvenlik zafiyetleri bulunmaktadır.

İnternet kullanıcı sayısının artması ile birlikte geliştirilen yöntemler yetersiz kalmaya başlamıştır. Birçok insanın internet erişimi sağladığı, ev, kütüphane, kampüs gibi hayatımızın hemen her alanında kullanılan yerel alan ağlarında IP dağıtımı, erişim ve yetki denetleme, güvenliği sağlama gibi konular ağ yapısı için zorunlu ve zorlu görevler haline gelmiştir. Az sayıda kullanıcının bulunduğu ağ yapılarında kullanıcı kayıtlarını ve IP dağıtımını manuel olarak yapmak, güvenliği ağı izleyerek kontrol altında tutabilmek, yetkilendirmeyi sağlamak ve gerekirse değiştirebilmek mümkün olabilmektedir fakat kullanıcı sayısı arttıkça bu işlemlerin dinamik olarak gerçekleştirilmesine duyulan ihtiyaç artmakta hatta zorunluluk haline gelmektedir. Bu sorunu çözmek için birçok farklı sistem geliştirilmiştir. IEEE 802.1x protokolü kablolu ve kablosuz ağlarda port tabanlı kimlik denetimi sağlayan bir yöntemdir. Kullanıcılar ağa dahil edilmeden önce kimlik kontrölünden geçirilir. Başarılı kimlik denetimi

sağlanamadığı takdirde port kullanıma kapatılarak ağ altyapısı izinsiz erişimlerden korunur. 802.1x protokolü OSI (Open Systems Interconnection)'ye göre ikinci katman protokolüdür. Kullanıcı kimlik denetiminden geçtikten sonra ip aldığından dolayı ağ erişim kayıtlanması sırasında sadece MAC adresi bilgisi bulunur ve başka bir ağa erişim durumunda MAC adresi taşınmaz (Akın ve Sezer, 2009). Bu durum da 802.1x protokolünün tek başına yeterli olmadığını göstermektedir. Ağ güvenliğini sağlamak amacıyla geliştirilen bir diğer yöntem de kısıtlayıcı portaldır. Tarayıcı üzerinden istemcinin kimliğinin onaylanabileceği bir sistem olan kısıtlayıcı portal, bu alanda en çok kullanılan kimlik doğrulama yöntemlerinden biri olarak karşımıza çıkmaktadır. Kısıtlayıcı portal tekniği ile LAN (Local Area Network)'ı kullanmak isteyen herhangi bir kullanıcıyı oturum açmak için yeniden yönlendiren, RADIUS (Remote Authentication Dial-In User Service) ile kullanıcının kimlik bilgilerinin geçerliliğinin kontrol edildiği ve ağın Unifi cihazı ile yönetildiği bir sistem (Diyah, 2019) geliştirilmiştir. Ayrıca istemci tarafında dijital sertifika zorunluluğu getiren (Glazer, Hussey ve Shea, 2003) veya istemci tarafında aktif bir uygulama çalıştırılmasını gerektiren (Doğan ve Türe, 2013) sistemler de geliştirilmiştir. Bir başka çalışmada ise istemci ile sunucu arasında anahtar kod yöntemi kullanan bir sistem (Ju ve Han, 2005) geliştirilmiştir. Bu çalışmalarda, kısıtlayıcı portal yönlendirme sınırı olması, kampüs, şirket gibi çok sayıda kullanıcıdan oluşan yerel alan ağlarında eş zamanlı erişimin tam verim ile gerçekleştirilememesi ve kullanıcı tarafında uygulama yükleme veya sertifika zorunluluğu gibi ek yükler getirilmesinden ötürü sorunlara tam anlamı ile bir çözüm sağlanamadığı görülmektedir.

Biz bu çalışmada istemci makineye herhangi bir uygulama yükleme zorunluluğu getirmeyen ve istemciye, ağa ilk bağlandığı durum için tek seferlik denetim sağlayan bir sistem geliştirdik. İstemci ağa bağlanmak istediğinde kullanılan ağ anahtarı ile sunucu cihaza yönlendirilir. Daha önce ağ üzerinde kimlik kaydı yapılmayan bir kullanıcı (ağda ilk kez internet erişimi sağlamaya çalışan kullanıcı) ise kayıt işlemlerinin yapılmasını sağlayan uygulamamıza yönlendirilir. Kullanıcının uygulama ekranındaki kimlik kontrolünden geçmesi durumunda ağa kaydı sağlanır ve internete erişir. Kimlik kontrolü sağlanana kadar kullanıcılar her internet erişim isteğinde uygulamaya yönlendirilir. Sistemde kaydı var olan, geçerli bir kullanıcının ise direkt olarak internete çıkışı sağlanır. Böylece kullanıcılar her oturumda kimlik denetimine tabi tutulmaz, sadece ilk oturumda kimlik denetiminden geçirilir. Geliştirilen sistemde ağ üzerinden internet erişimi sağlaması istenmeyen kullanıcılar ve erişilmesi istenmeyen adresler de engellenebilmektedir. Aynı zamanda ağdaki kullanıcıların hangi adresler ile ağa bağlandığı da kayıt altında tutulmaktadır. Böylece herhangi bir sorgulama durumunda ağ kaynaklarına erişim sağlayan kullanıcılar da tespit edilebilecektir.

2. Kullanılan Sistemler

Geliştirilen sistemde kullanıcı kayıtlarının tutulması, kayıtlı bilgilere göre yetkilendirme ve denetimin sağlanması, kullanıcıların ağda izleyecekleri yolun belirlenmesi ve tüm bunların test edileceği bir ortam sağlanması gibi işlemler için farklı yöntem ve teknolojilerden yararlanılmıştır.

2.1. DHCP (Dynamic Host Configuration Protocol – Dinamik Host Yapılandırma Protokolü):

Bilgisayarlar, akıllı telefonlar, IOT cihazlar vb. internet ile işlem yapmak isteyen her türlü makinenin IP adresi, ağ geçidi, alt ağ maskesi, DNS sunucu adresi gibi bilgilere sahip olması gerekmektedir. Bir ağda kullanılan her IP adresinin tek bir cihaza atanmış olması şarttır. DHCP sunucularından önce bu konfigürasyon işlemleri manuel olarak gerçekleştirilmekteydi. Ağdaki cihaz sayısının artması ile birlikte her cihaza ayrı ayrı konfigürasyon işlemlerinin yapılması zorlaşmakta, aynı zamanda bir hata durumunda IP çakışması da yaşanabilmektedir. DHCP sunucuları ağdaki cihazların birbirleriyle iletişim halinde bulunabilmesi ve dış ağlara ulaşabilmesi için gerekli olan tüm konfigürasyonları otomatik olarak gerçekleştiren, her cihazın eşsiz birer IP adresine sahip olmasını sağlayan cihazlardır. Küçük ölçekli ağ yapılarında routerlar, daha geniş kapsamlı ağlarda ise DHCP sunucusu olarak kullanılan bilgisayarlar bu görevi üstlenmektedir.

İstemci cihaz, ağa ilk erişiminde bir IP adresi olmadığından dolayı DHCP sunuyu bulmak amacıyla ağa bir DHCP Discover mesajı gönderir. Mesaj DHCP sunucusuna ulaşınca sunucu istemciye, içerisinde istemciye atamayı düşündüğü IP adresi ve bu adresi kullanacağı süreyi (lease time) barındıran bir DHCP Offer mesajı gönderir. İstemci DHCP Offer mesajını alınca sunucuya, atanması düşünülen IP adresini

ve belirlenen süreyi onayladığını ve istediğini belirten bir DHCP Request mesajı iletir. DHCP sunucusu konfigürasyon bilgilerinin atanmasını onaylıyor ise sonuç olarak bir DHCPACK paketi göndererek işlemin başarılı bir şekilde tamamlandığını, onaylamıyor ise (belirtilen IP adresi süreç içerisinde başka bir cihaza atanmış olabilir) DHCPNACK paketi göndererek konfigürasyonun yapılamadığını belirtir. IP ataması yapıldıktan sonra kullanım süresi (lease time) dolmadan evvel istemci IP adresini kullanımının yenilenmesini ister. Aksi halde IP adresi süre sonunda başka bir cihaza atanabilmektedir. İstemcinin ağdan ayrılması durumunda kullandığı IP adresi başka cihazlara atanabilmek için DHCP'nin kullanılabilir IP adreslerinin arasına yeniden katılır. Sunucu tarafından DHCPNACK mesajı ile konfigürasyon ayarları reddedilmiş ise istemci, içerisinde "DHCP: Requested Address" alanının bulunduğu, bir önceki DHCP Discover mesajından farklı yeni bir DHCP Discover mesajı yayınlar ve yeni bir IP adresinin atanmasını ister fakat bu isteğinin de reddedilmesi durumunda TCP/IP kapatılmakta ve cihaz artık ağ etkinliğine katılamamaktadır (D. Shinder, T. Shinder ve Hinkle, 2000).

2.2. Kimlik Denetimi:

Authentication (doğrulama), istemcilerin ağ ile bağlantı kurmadan önce denetimden geçerek kimlik doğruluğunu kanıtlamasıdır. Bu işlem için genellikle kullanıcılara ait veriler ve şifre alınarak veritabanı kaydı yapılır. Kullanıcı ağa erişmek için veritabanındaki veriler ile uyumlu olacak kullanıcı adı ve şifre bilgisini sağlamalıdır. Güvenliğin artırılması amacı ile şifrelerin belirli kurallara bağlı kalınarak oluşturulması sağlanmalıdır. Ayrıca kullanıcı ve sunucu arasındaki bilgi alışverişinin şifrelenerek üçüncü bir kişinin erişimine kapatılması gerekmektedir.

Authorization (yetkilendirme), kimlik denetiminden başarılı bir şekilde geçen cihazların ağ üzerinde hangi işlemleri yapma yetkisinin olup olmadığının belirlenmesidir. Kullanıcılar ait oldukları grupların erişim haklarına göre yetkilendirilir. Şayet bir kullanıcı iki farklı gruba tanımlı ise tanımlı olduğu her iki grubun da erişim yetkilerinin tümüne sahip olmalıdır.

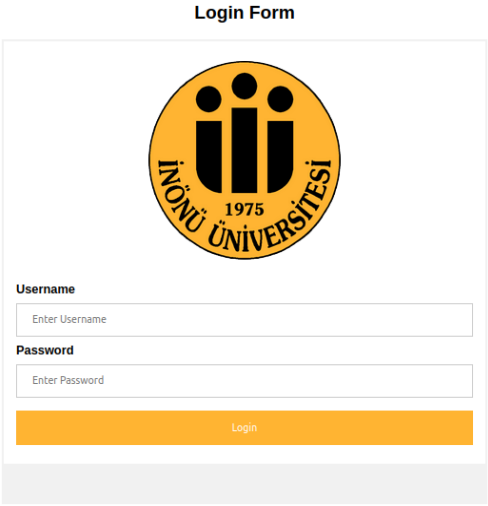
Bilişim sistemlerinde hatalı çalışma, isteklere cevap verememe ve çökme gibi problemler oluşabilmektedir. Bu problemlerin, problemin türüne ve kapsamına göre belirli sürelerde giderilmesi gerekir. Accounting (aktivite izlemesi), yaşanabilecek herhangi bir sorun durumunda, probleme daha kısa sürede çözüm üretilebilmesi adına sistemdeki kullanıcıların aktivitelerinin kayıt altına alınması işlemidir. Kullanıcıların ağ üzerindeki erişimlerinin türü, saati, veri bağlantıları gibi bilgiler oluşacak sorunların nasıl bir süreçte ortaya çıktığı hakkında bilgi vermektedir. Authentication, authorization ve accounting birbirlerini takip eden işlemler olup kısaca "AAA" olarak kullanılabilmektedir.

2.3. Captive Portal (Kısıtlayıcı Portal):

Kısıtlayıcı portal kullanıcılar sisteme kayıt oluncaya kadar ağ trafiğini korumak amacıyla denetim cihazı olarak kullanılan bir router (yönlendirici) ya da gatewaydir (ağ geçidi) (Diyah, 2019). Ağa bağlanmak isteyen kullanıcıların, erişim gerçekleştirmeden önce bir giriş ekranına yönlendirilmesini sağlamaktadır. Yapılan yönlendirme işlemi kullanıcının tarayıcıda herhangi bir web hizmetine erişmek istemesi ile başlamaktadır. Tarayıcının çalıştırılmasının ardından HTTP (The Hypertext Transfer Protocol – Hiper Metin Aktarma İletişim Kuralı) istemcisi ağa erişmeyi bekleyen kullanıcıyı kullanıcı adı ve şifre gibi bilgiler istenen form ya da kullanıcı ve internet sağlayıcısı arasındaki bazı şartları barındıran bir sözleşmeye yönlendirmektedir. Kullanıcı, sözleşmeyi imzalarsa ya da ilettiği kullanıcı adı ve şifre ikilisi veritabanındaki kayıtlar ile uyum sağlarsa authentication adımını başarılı bir şekilde tamamlamış sayılmaktadır. Başarısız bir onaylama işlemi durumunda ise ağa erişimi engellenmektedir. Böylece internet tarayıcımız kullanıcıların denetimden geçmeden ağa erişmesine izin vermeyen bir kimlik kontrol noktası haline gelmektedir. Kısıtlayıcı portalın çalışma aşamaları şu şekildedir (Goeritno, Afrianto, Basri ve Ritzkal, 2017):

- Kablosuz istemcilerin DHCP'den IP adresi alması için kablosuz bağlantı yapmasına izin verilmektedir.
- Kimlik doğrulamadan önce, önceki sunucu tarafından yayılan tüm DHCP IP'leri kısıtlayıcı portala yönlendirilmektedir.
- Sadece kendini ağa başarılı bir şekilde tanıtan istemciler bir sonraki adıma geçebilmektedir.
- Kullanıcı giriş bilgileri loglanmakta ve en nihayetinde artık internet ağı kullanılabilmektedir.

Günümüzdeki mevcut sistemlerde de oldukça sık kullanılan bir yöntem olan kısıtlayıcı portal, hem kablolu hem de kablosuz her türlü sisteme uyarlanarak, ağ yapısı oluşturulabilecek her ortamda kullanılabilmektedir. Ancak kısıtlayıcı portalın kullanıcılara her oturumda kimlik denetimi zorunluluğu getirdiğinin de bilinmesi gerekmektedir. Şekil 1'de geliştirilen sistemdeki kısıtlayıcı portal ekranı görülmektedir.



Şekil 1. Geliştirilen sistemin kısıtlayıcı portal ekranı

2.4. Eve-Ng (Emulated Virtual Environment Next Generation):

Eve-Ng, sanal makinelerde çalıştırılan, sistemimiz üzerinden farklı işletim sistemleri ile çalışmamıza olanak sağlayan bir emülatör ortamıdır. Sanal ortamda, Cisco, Jupiter, Fortinet, Huawei, Alcatel, Aruba, Arista, CheckPoint, Extreme, F5, VMWare, Windows 7-8-10, Windows server 2003-2008-2012-2016, Linux gibi birçok farklı üreticinin ürünlerinin kullanılmasına ve bu ürünlerle karışık network laboratuvarları oluşturulmasına olanak tanımaktadır. Öğrenmek istenen sistemleri, test etmek istenen yazılımları ve ağ topolojilerini fiziksel ekipmana ücret ödemeden deneyimleme imkanı sunar. Korkmadan hata yapma imkanı tanıyan güvenli bir ortam sağlamaktadır. Windows, Mac OS veya Linux bilgisayarlarına kurulabilmesi için sanal bir makinede çalıştırılmakta ve grafiksel kullanıcı arayüzüne bir web tarayıcısı ile erişilmektedir (Brian Linkletter, 2017). Desteklenen sanallaştırma platformları ve yazılımlar VMware Workstation 14.0 ile sonraki sürümleri, VMware Player 14.0 ile sonraki sürümleri, VMware ESXi 6.0 ile sonraki sürümleri, Ubuntu Server 18.04 LTS as platform for bare metal, Google Cloud Platform ve AMD CPU based PC or Server olarak karşımıza çıkarken, desteklenmeyen donanım ve sistemler VirtualBox virtualization, Citrix XenServer, Microsoft HyperV, Ubuntu 20.x ve Proxmox olarak listelenmektedir (Dzerkals, t.y.). Eve-Ng, cisco packet tracer uygulaması ve GNS3 ile aynıdır ancak Eve-Ng daha fazla özelliğe sahiptir (Hawari ve Sumbawati, 2019). Eve-Ng ve GNS3 bazı özellikleri bakımından karşılaştırılacak olursa: erişim Eve-Ng'de web arayüzünden, GNS3'de ise yüklü client üzerinden sağlanır, Eve-Ng GNS3'ye kıyasla daha fazla cihazı destekler, Eve-Ng'de soft bir limit bulunmazken GNS3 QEMU'daki cihaz başına maksimum 2 GB'lık bir RAM desteği sağlar, Eve-Ng'de bir limit bulunmazken GNS3'de 16 adet sanal network desteği vardır ve Eve-Ng çoklu kullanıcı desteği sunarken GNS3 bunu sağlayamaz (Eroğlu, 2016).

2.5. LDAP (Lightweight Directory Access Protocol – Basit Dizin Erişim Protokolü):

LDAP, TCP/IP ağlarında çalışan dizin hizmetlerini sorgulamak ve değiştirmek için kullanılan bir uygulama protokolüdür ve ağ kimlik doğrulama ve yetkilendirme işlemlerinin yönetimini merkezileştirmeye yardımcı olmaktadır (Dell Technologies, t.y.). LDAP, veritabanından farklı olarak verileri tablolarda değil belirli kurallar dahilinde hiyerarşik bir dizin yapısında depolamaktadır. Data Information Tree (DIT) olarak isimlendirilen bu yapıda her bir nesne bir düğüm olarak tutulmaktadır. Düğümlerin atası olan bir adet düğüm mutlaka bulunmakta ve bir nesnenin birçok çocuk düğümü bulunabilmektedir. Nesneler LDAP dizinine LDIF (LDAP Data Interchange Format) adı verilen dosyalar ile eklenmektedir. İşlemleri gerçekleştirmek için gerekli olan LDAP oturumları, LDAP

sunucusuna bağlanan istemciler tarafından, varsayılan olarak 389 numaralı TCP bağlantı noktasında başlatılmaktadır (Amitash, 2018). LDAP istemcisi aradığı bilginin formatını, LDAP için yazılmış ve LDAP istemcisinin içine gömülmüş API (Application Programming Interface) vasıtasıyla oluşturmakta ve TCP/IP aracılığıyla da "Dizin Sistemi Aracı (DSA)" olarak bilinen sunucuya göndermektedir (Akın, Yüce ve Demir, 2008). Sunucu ise gerekli bilgiyi aynı yöntemi kullanarak istemciye iletmektedir. LDAP verilere erişim için, DC (Domain Compponent), OU (Organizational Unit), CN (Common Name) gibi kısaltmalar ile isimlendirilmelerin yapıldığı standart bir hiyerarşik dizilim kullanmaktadır. OU, CN ve DC'lerin biraraya gelerek oluşturdukları DN (Distinguished Name) ise her nesne için özgün olan ayırt edici isimlendirmedir. Örneğin; "inonu.com" domainindeki "student" klasörüne "semra" nesnesini eklemek için oluşturulması gereken LDIF dosyası ve bu veri için DN kısmı Tablo 1'deki gibi olmalıdır.

Tablo 1. Örnek LDIF dosyası

addStudent.ldif	
Kod Satırı	**Açıklama**
dn: cn=semra, ou=student, dc=inonu, dc=com	Bir nesneyi diğerlerinden ayıran ağaç bilgisinin (dn) belirlendiği satırdır. Ağaç bilgisi, kullanıcı adı (cn), organizasyon birimi (ou), domain adı ve domain uzantısı (dc) gibi özelliklerin birleşiminden oluşur.
objectClass: posixAccount	ObjectClass girdinin tipi hakkında bilgi verir. PosixAccount ise *POSIX* (Taşınabilir İşletim Sistemi Arayüzü) sistemler için kullanılan objectClass türüdür.
objectClass: shadowAccount	Kullanıcı parolası için bilgi hizmeti sağlayan yardımcı nesne sınıfıdır. Parolanın geçerlilik süresi, parola değişiklikleri arasında geçen gün sayısı, kullanıcı girişinin devre dışı bırakılacağı tarih gibi bilgileri barındıran öznitelikler içerir.
objectClass: inetOrgPerson	Kuruluşlara ait kişi girdileri oluşturulması için tavsiye edilen ve çok sayıda nitelik barındıran nesne sınıfıdır. Girişler uid niteliğinin değerine göre adlandırıldığından uid niteliği bu nesne sınıfı için gereklidir.
cn: semra	Kullanıcının adını içeren özniteliktir.
sn: yildirim	Kullanıcının soyadını içeren özniteliktir.
uid: semra	Kullanıcının oturum açma kimliğini tanımlayan özniteliktir.
uidNumber: 10000	Kullanıcıyı sisteme tanıtan ve kullanıcının erişebileceği sistem kaynaklarını belirleyen özniteliktir.

gidNumber: 5000	Kullanıcı grubunu belirlemek için kullanılır. Oluşturulan kullanıcı, üyesi olduğu kullanıcı grubunun tüm erişim haklarına sahiptir.
givenName: semra	Kullanıcının adını içeren özniteliktir. Genellikle "cn" ile aynı değer kullanılır.
displayName: Semra Yildirim	Girişleri görüntülerken kullanılması tercih edilen ismi belirlemek için kullanılır.
userPassword: smr	Kullanıcının adını içeren özniteliktir.
loginShell: /bin/bash	Bir kural dahilinde oturum açılması gerektiğini belirten özniteliktir. Genellikle ortam değişkenlerini ayarlama gibi işleri yürüten bir dosyayı okur.
homeDirectory: /home/semra	Kullanıcı kimliği tanımlandığında kullanıcı için oluşturulacak dizini belirtir.

Bu veriyi eklemek için Linux terminalinde şu komut çalıştırılmalıdır:

```
ldapadd -x -H ldap://localhost/ -D cn=admin, dc=inonu, dc=com -W -f addStudent.ldif
```

Eklenen veriyi bulmak için ise Linux terminalinde şu komut çalıştırılmalıdır:

```
ldapsearch -x -H ldap://localhost/ -b dc=inonu, dc=com -W
```

LDAP, veritabanları ile karşılaştırıldığında, veritabanlarında yazma ve okuma işlemlerinin her ikisinin de olabildiğince hızlı bir biçimde gerçekleştirilmesi hedeflenirken, LDAP'ta ise temel hedef aranan veriye en hızlı şekilde ulaşabilmektir. NOSQL bir veritabanı ile çalışırken sunucuyu değiştirmeniz durumunda tüm istemcileri aynı anda değiştirmeniz gerekir (Ldap.com, t.y.). İlişkisel bir veritabanı ile çalışırken ise, gerekli olması halinde sadece yeni bir veritabanı sürücüsü kurma şansınız olmakta ve bunun için de tüm istemcilerinizi yeni veritabanıyla konuşabilmeleri için güncellemeniz gerekmektedir (Ldap.com, t.y.). Ancak LDAP'ın birçok farklı dizin sunucusu ve istemci API'leri bulunduğundan süreç içerisinde seçiminizi kolaylıkla değiştirebilirsiniz (Ldap.com, t.y.).

2.6. IPTables:

Linux kerneline sisteme erişmesi istenmeyen ve sistem üzerinden geçerken yapısında değişiklik yapılması gereken paketleri, sistemden erişilmesi istenmeyen sunucuları vb. belirtmek ve gerekli kontrolleri sağlamak amacıyla bir filtre dahil edilmiştir. Linux çekirdeğinde bulunan ve "Netfilter" olarak isimlendirilen bu araçta filter, nat, mangle, raw ve security olmak üzere beş adet tablo bulunmaktadır. Filter, sisteme ulaşacak ve sistemden çıkış yapacak paketlerin bu işlemlere yetkilerinin bulunup bulunmadığının belirlendiği tablodur ve INPUT, OUTPUT ve FORWARD zincirleri bulunmaktadır. Nat, Network Address Translation kurallarını düzenler. IP paketi üzerindeki hedef ve kaynak adreslerin değiştirilmesi, IP adresi dönüştürme ve gizleme gibi işlemlerin karar mekanizmasını oluşturmak için gerekmektedir. INPUT, OUTPUT, PREROUTING ve POSTROUTING zincirleri bulunmaktadır. Mangle tablosu özel paket değişiklikleri yapmakta, TCP başlığındaki QOS bitlerini değiştirmektedir (Natarajan, 2011). INPUT, OUTPUT, FORWARD, PREROUTING ve POSTROUTING zincirleri bulunmaktadır. Raw tablosu bağlantılardaki olağan dışı durumlar için kurallar yapılandırmak amacıyla kullanılmaktadır. PREROUTING ve OUTPUT zincirleri bulunmaktadır. Security tablosu, filter tablosundan sonra makinenin güvenliğinden sorumludur ve başarılı bir güvenlik aracı olan SELinux'tan oluşmaktadır. INPUT, OUTPUT ve FORWARD zincirleri bulunmaktadır.

Iptables kurulumu için Linux terminalinde şu komut çalıştırılmalıdır:

```
sudo apt-get install iptables
```

Güvenlik duvarı için tanımlı mevcut kuralları görüntülemek için Linux terminalinde şu komut çalıştırılmalıdır:

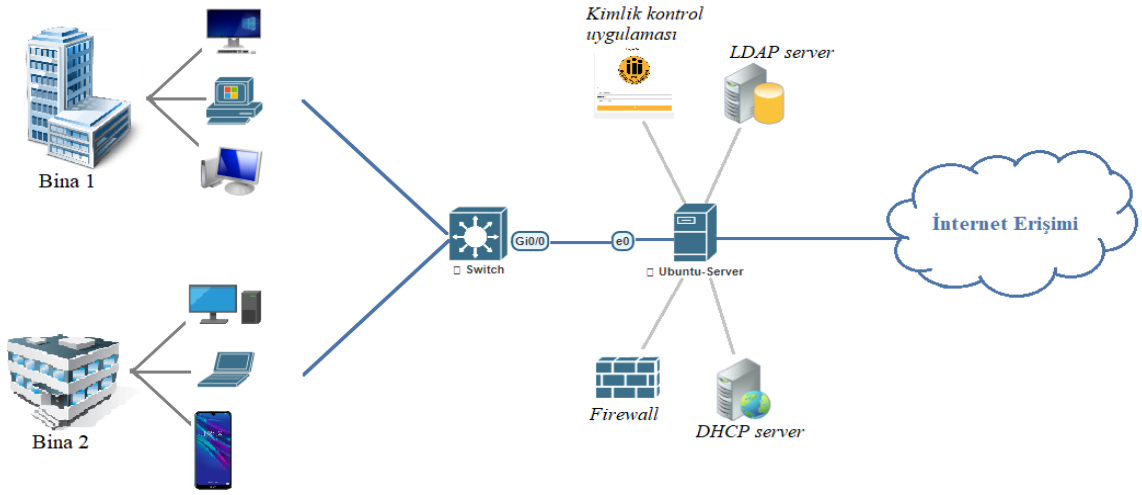
```
sudo iptables -L -n -v
```

Burada "-L" kuralları listelemek istediğimizi, "-n" IP adresi, port vb. bilgileri sayısal bir biçimde görmek istediğimizi, "-v" paket, byte vb. ayrıntılı bilgilere de ihtiyaç duyduğumuzu belirtmektedir. Paket giriş çıkışını engellemek, paket bilgilerini değiştirmek, paket yönlendirmeleri yapmak, ağ arayüzleri, portlar, MAC adresleri için ayrıcalıklı kurallar tanımlamak, tanımlanan kuralları silmek ya da değiştirmek için kullanılabilecek çok sayıda iptables komutu bulunmaktadır. Iptables kurulumdan sonra Linux terminalinde bu komutlar kullanılarak rahatlıkla bir güvenlik duvarı yapılandırması gerçekleştirilebilmektedir. Gerekli yapılandırma sağlandıktan sonra şu komut çalıştırılarak yapılan değişiklikler kalıcı hale getirilmelidir:

```
sudo iptables-save
```

3. Önerilen Sistem

VMware Workstation 16.0 Player üzerinden Eve-Ng kurulumu yapılarak proje süresince sistemin testleri Eve-Ng laboratuvarlarında gerçekleştirildi. Eve-Ng, donanım maliyetini en aza indirmesi, web tarayıcısı üzerinden erişim sağlandığından ötürü zamandan ve mekandan bağımsız, taşınabilir çalışma alanı sunması ve korkusuzca hata yapılabilecek bir emülatör ortamı olması sebebiyle tercih edilmiştir. Eve-Ng ortamında bir laboratuvar oluşturularak Şekil 2'de görüldüğü gibi bir sistem topolojisi kurulmuştur.



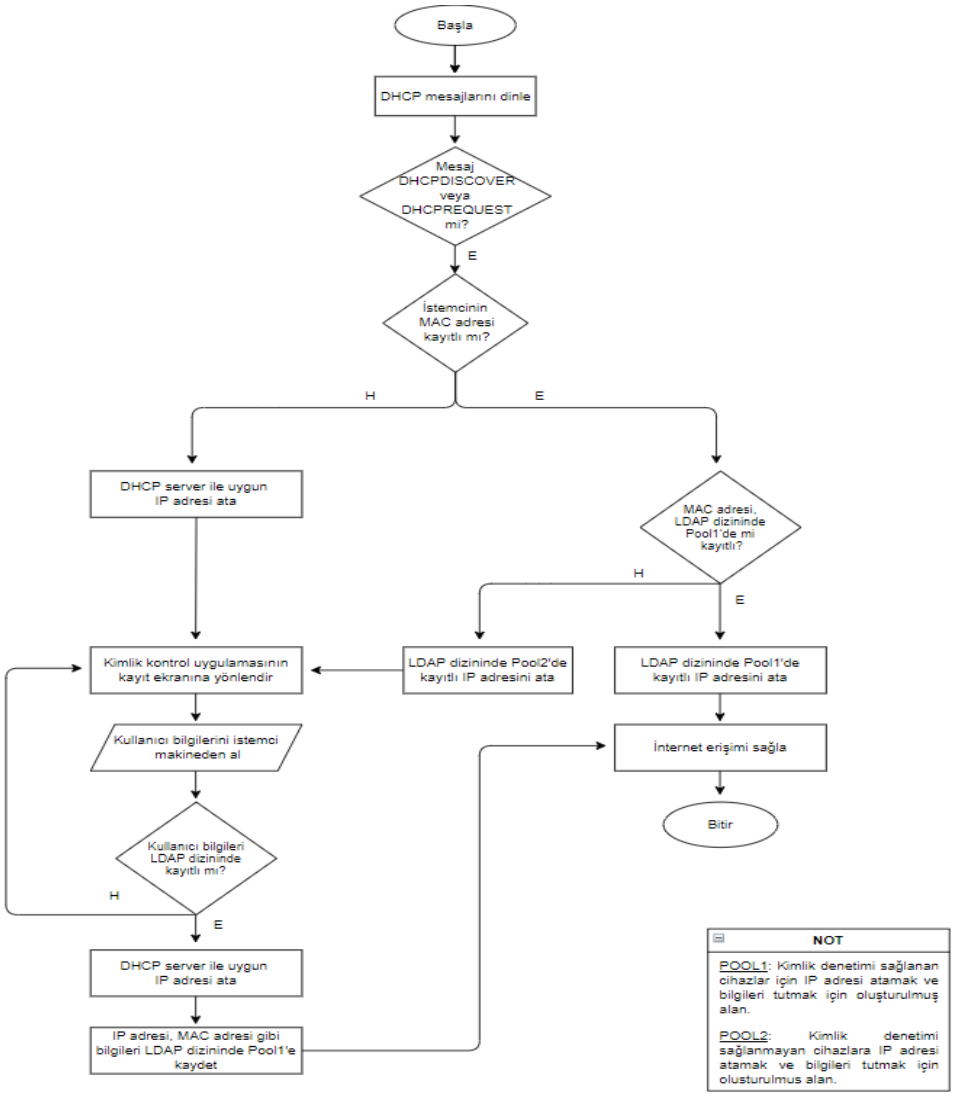
Şekil 2. Kullanılan ağ topolojisi

Topolojideki switch cihazı ağdaki tüm trafiği yakalayacak ve Ubuntu servera yönlendirecektir. İstemciler ağa ilk bağlantı kurduklarında internet erişimi sağlayabilmek için IP adresi, alt ağ maskesi, DNS sunucu adresi gibi bilgilere ihtiyaç duymaktadır. Bunun için ise en yakın DHCP sunucunu ararlar. Saldırganlar ağdan ücretsiz yararlanmak, ağa zarar vermek, bilgi çalmak, şantaj gibi sebeplerle ağa sızmak isteyebilir ve ağa ikinci bir DHCP kurabilirler. İstemci en yakındaki DHCP sunucusuna erişim sağladığından ötürü sahte DHCP'den IP alarak tüm paketlerini bu yol üzerinden göndermeye başlar. Böylece ağın tüm trafiği sahte DHCP üzerinden geçer ve saldırgan tüm paketleri ve veri alışverişlerini izleyebilir. Büyük ölçüde bir güvenlik zafiyetine sebep olan bu durumu engellemek için Cisco cihazlarda DHCP araya girme (DHCP snooping) özelliği bulunmaktadır. Bu çalışmada Cisco switch cihazı üzerinde bu özellik aktif hale getirilmiştir. DHCP araya girme özelliği ile ağdaki portlar güvenli ve güvenli değil şeklinde ayrıştırılmaktadır. Güvenli olarak belirtilen portlar üzerinden DHCP yayını yapılabilirken güvenli olmadığı belirtilen portlardan gönderilen DHCP paketleri bloke edilir. Topolojideki switch cihazına Ubuntu serverın bulunduğu portun güvenli olduğu bilgisi verilmiş ve diğer

tüm portlardan DHCP yayını yapılmasının önüne geçilmiştir. Anahtarlar üzerinde DHCP araya girme özelliğini aktif hale getirmek için switch üzerinden komutlar ile konfigürasyonlar yapılır. Bu komutlardan biri şu şekildedir:

```
#ip dhcp snooping information option.
```

Bu komut option 82 olarak bilinen parametrenin kullanımını etkinleştirmek için kullanılır. Bu parametre DHCP paketinde bulunan "Options" kısmının 82 indisli veri alanıdır (Korkmaz ve Köse, 2017). Switch cihaz, Ubuntu makineye yönlendirdiği her pakete kendi MAC adresini ve port bilgisini yazdığı option 82 parametresini eklemekte ve Ubuntu cihazdan gelen paketler de dahil olmak üzere gelen her pakette bu parametrenin bilgileriyle kendi bilgilerini karşılaştırarak güvenli cihaza karar vermektedir. Ağa bağlanmak isteyen kulanıcılar switch üzerinden bu denetimler ile Linux sunucusuna yönlendirilir. Bu çalışmada Linux cihazda, yapılandırılan DHCP konfigürasyonları ile iki adet pool oluşturulmuştur. Ağa daha önce hiç bağlanmamış kullanıcı MAC adresi bilinmeyen, yabancı bir kullanıcı olduğundan dolayı ilk pooldan IP alır ve bu haliyle internet erişimi sağlayamaz. MAC adresi bilinmediği için güvenlik duvarında yapılandırılan iptables kuralları gereği doğrulama işleminin gerçekleştirilmesi için yazdığımız uygulamaya yönlendirilir. Bu uygulama ve iptables kuralları yardımı ile kullanıcı hangi web sitesine erişim sağlamak isterse istesin kısıtlayıcı portal giriş formu ile karşılaşır. Kullanıcının internet erişim isteği ile başlayan bu süreç Şekil 3'teki akış diyagramında gösterilmiştir.



Şekil 3. Geliştirilen sistemin akış diyagramı

Kullanıcı kayıtları Ubuntu serverdaki LDAP dizininde tutulmakta, dolayısıyla AAA işlemleri de burada gerçekleştirilmektedir. Uygulamanın kayıt ekranındaki form alanlarını doldurup onaylayan kullanıcının bilgileri LDAP dizinine kayıtlı veriler ile karşılaştırılır. Kullanıcı bilgileri LDAP dizinindeki bilgiler ile eşleşmez ise her internet erişim isteğinde aynı prosedür tekrar tekrar uygulanır. Iptables kurallarıyla ve DHCP ayarlamaları ile IP adresi bloklanabilir. Kullanıcı bilgileri ile LDAP dizinindeki verilerin eşleşmesi durumunda ise öncelikle kullanıcının yetkisine karar verilir. Admin ise kullanıcı ekleme ve silme gibi işlemlerin yapılabildiği admin işlemleri ekranını görüntüleyebilmektedir. Fakat kullanıcı olarak tanımlı ise MAC adresi kayıt altına alınarak DHCP sunucusundaki ikinci pooldan IP adresi alması sağlanır ve bu durumda artık internet erişimi sağlayabilir. Bundan sonraki her oturumda MAC adresi bilindiğinden ötürü sistemden kaydı silinene kadar kısıtlayıcı portal ekranı ile karşılaşmadan internet erişimi sağlayabilecektir.

4. Sonuç

Bu çalışmadaki ana hedef kullanıcıların tek sefere mahsus bir kimlik denetimi işlemi ile kendilerini sisteme tanıtması ve sonraki her oturumda sistem tarafından otomatik olarak tanınarak internet erişimi izninin sağlanmasıdır. İstemcinin ağa ilk bağlantı kurduğu senaryoda, kullanıcı erişmek istediği internet sitesi için web tarayıcısından erişim isteğinde bulunacaktır. Kullanıcının bu isteğini yakalayan switch cihazı kullanıcıyı kimlik denetiminin sağlandığı kısıtlayıcı portal ekranına yönlendirir. Kullanıcı bu ekranda yer alan formu doldurarak onaylar. Kullanıcının girdiği kimlik bilgileri kayıtlı veriler ile eşleşmezse kullanıcının her internet erişim isteğinde tekrar tekrar aynı prosedürler uygulanır. Kimlik bilgilerinin eşleştiği durumda ise kullanıcının MAC adresi Linux cihazda kayıt altına alınarak, kullanıcının ağ yapısında tanınan bir istemci olması sağlanır. Kullanıcının kendini ağa daha önce tanıtmış olduğu senaryoda ise, istemci MAC adresi Linux cihazda kayıt altında tutulduğundan dolayı istemci cihaz hiçbir işlem yapmaya gerek duymadan direkt olarak internet erişimi sağlayabilmektedir. Bu sistem ile kullanıcı tarafına hiçbir uygulama yükleme ya da sertifika zorunluluğu gibi ek yükler getirilmeden kullanıcının hızlı ve güvenli bir şekilde internet erişimi gerçekleştirmesi sağlanmıştır. Geliştirilen sistemin avantaj ve dezavantajları Tablo 2'de verilmiştir.

Tablo 2. Geliştirilen sistemin avantaj ve dezavantajları

Avantajları	Dezavantajları
• İstemci makineler her oturumda kimlik denetimine tabi tutulmaz. Kimlik denetimi tek sefere mahsustur. • Kablolu/kablosuz bağlantı farketmeksizin bilgisayar, cep telefonu gibi her türlü cihaz için tek bir uygulama kullanılır. • Kampüs alan ağında kayıtlı kullanıcıların internete çıkış izni olan ve olmayan tüm cihaz bilgileri kayıt altında tutulur. • Admin paneli üzerinden cihazların internet erişim izinleri değiştirilebilir. Bu sayede gerek görüldüğü takdirde kullanıcıya verilen internet hizmeti kolayca kesilebilir.	• Misafir kullanıcılar için internet erişim izninin manuel olarak sağlanması gerekmektedir.

Teşekkür

Bu çalışma İnönü Üniversitesi Bilimsel Araştırma Projeleri Daire Başkanlığı'nın (SRPD) FBG-2020-2143 numaralı projesi ile desteklenmiştir. Değerli geri bildirimleri için İnönü Üniversitesi SRPD'ye teşekkürlerimi sunarım.

Kaynaklar

Adnan A. H. ve ark. (2015) A comparative study of WLAN security protocols: WPA, WPA2. International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, pp. 165-169.

Akın G., Sezer U. (2009) Güvenlik amaçlı SNMP Walk ile merkezi loglama yazılımı. INET-TR 2009, İstanbul.

Akın G., Yüce H., Demir H. (2008, May) FreeRADIUS - LDAP ile kimlik denetimi klavuzu. Ulaknet Çalıştayı.

Amitash (2018) LDAP ve veritabanı arasındaki fark. http://www.differencebetween.net/technology/difference-between-ldap-and-database/. Accessed 28 June 2021.

Aryeh F. L., Asante M., Danso A. E. Y. (2016) Securing wireless network using pfSense captive portal with RADIUS authentication. *Ghana Journal of Technology* 1(1): 40-45.

Dell Technologies web sitesi, LDAP yapılandırması. https://www.delltechnologies.com/tr-tr/documentation/unity-family/unity-p-security-config-guide/10-unity-c-security-config-guide-ldap-appendix.htm. Accessed 28 June 2021.

Diyah H. (2019, July 25) Access point implementation to Unifi device with RADIUS and captive portal authentication method in PT XYZ. https://doi.org/10.31227/osf.io/ve6db.

Doğan R. Ö., Türe H. (2013) Opengate captive portal için kullanıcı dostu bir uygulama yazılımı.

Dzerkals U., Eve-ng professional cookbook [Electronic version]. https://www.eve-ng.net/index.php/documentation/professional-cookbook/, pp. 13-14. Accessed 26 June 2021.

Eroğlu Y. (2016) Unetlab – GNS3'e dişli rakip!. https://blog.yavuzeroglu.com/unetlab/unetlab-gns3e-disli-rakip.html. Accessed 26 June 2021.

Glazer, G., Hussey, C & Shea, R. (2003, March 20). CertificateBased Authentication for DHCP [Electronic version]. http://www.thesnowpit.ca/research/other/cbda.pdf. Accessed 20 June 2021.

Goeritno A., Afrianto Y., Basri H., Ritzkal (2017, May 17-18) Penerapan integrasi captive portal dengan single sign on (sso) pada layanan hotspot dan sistem informasi akademik. Seminar Nasional ke-2: Sains, Rekayasa, & Teknologi UPH, Tangerang/Endonezya.

Hawari M. S., Sumbawati M. S. (2019) Pembelajaran kolaborasi dengan aplikasi Eve-ng pada pembelajaran jaringan komputer di Universitas Negeri Surabaya. *Journal of IT-Edu*, 04(01): 240-247.

Ju H., Han J. (2005) DHCP message authentication with an effective key management, World Academy of Science Engineering and Technology.

Korkmaz M. H., Köse C. (2017, May 15-18) Port-based DHCP server design with authentication. 25th Signal Processing and Communications Applications Conference (SIU), Antalya/Turkey.

Ldap.com, Why choose LDAP. https://ldap.com/why-choose-ldap/. Accessed 28 June 2021.

Linkletter B. (2017) How to set up the UNetLab or Eve-ng network emulator on a Linux system. https://www.brianlinkletter.com/2017/02/how-to-set-up-the-eve-ng-network-emulator-on-a-linux-system/. Accessed 26 June 2021.

Natarajan R. (2011) Linux firewall tutorial: IPTables tables, chains, rules Fundamentals. https://www.thegeekstuff.com/2011/01/iptables-fundamentals/. Accessed 12 June 2021.

Shinder D., Shinder T., Hinkle T. (2000, March 11) DHCP server management. Managing windows 2000 network services, ISBN:978-1-928994-06-0, Syngress, pp. 101-162.

Soewito B. (2014) Building secure wireless access point based on certificate authentication and firewall captive portal. EPJ Web of Conferences, Paris.