SN: 1306-3111/1308-7231 Status : Review
NWSA-Engineering Sciences Received: January 2013
NWSA ID: 2013.8.3.1A0349 Accepted: July 2013
E-Journal of New World Sciences Academy

Fatih Ertam, Türker Tuncer ve Engin Avcı
Firat University, Elazig-Turkey
fatih.ertam@firat.edu.tr
turkertuncer@firat.edu.tr; enginavci@firat.edu.tr

http://dx.doi.org/10.12739/NWSA.2013.8.3.1A0349

ADLİ BİLİŞİMDE AĞ CİHAZLARININ ÖNEMİ VE GÜVENİLİR YAPILANDIRMALARI

ÖZET

Ağ adli bilişimi, adli bilişimin alt dallarından birisi olarak kabul edilir. Ağ cihazları adli bilişimini ise Ağ adli bilişiminin bir alt dalı olarak görmek mümkündür. Adli bilişim uygulamalarında şüpheli kullanıcıların kişisel bilgisayarlarındaki verilerin tümünün kopyalanarak alınması ve incelenmesi suçun ya da suçsuzluğun tespiti için tek başına yeterli değildir. Kullanıcıların ağ üzerinde gerçekleştirdiği trafiğinde olaydan öncesi ve olay sırasında kaydediliyor olması önemlidir. Bu kayıtların bozulmaması için ağ cihazları üzerinde gerekli güvenlik önlemlerinin alınması, kullanıcının ağ üzerinde istediği cihazları takamaması, ağ sistemi içerisinde internete çıktığı IP adresinin ve MAC adresinin belirgin olması, kullanıcının ağın işleyişini bozma girişimlerinin en aza indirilmesi de oldukça önemlidir. Kullanıcılar, ağ cihazlarındaki kayıtlara müdahale etmemelidirler. Bu çalışmada, hem ağ adli bilişimi incelemelerini kolaylaştırmak hem de ağ güvenliğini artırabilmek için ağ cihazları üzerinde yapılması gereken yapılandırma ayarlarından bahsedilecektir.

Anahtar Kelimeler: Adli Bilişim, Ağ Adli Bilişimi, Ağ Güvenliği Ağ Cihazları Adli Bilişimi, Bilgi Güvenliği

IMPORTANCE OF NETWORK DEVICES AND THEIR SECURE CONFIGURATIONS AT DIGITAL FORENSICS

ABSTRACT

Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. Network forensics is a sub-branch of digital forensics. Network device forensics is also a sub-branch of network digital forensics. Forensic IT applications and examination of suspicious users' personal computers to be copied to all of the data alone is not sufficient for the determination of guilt or innocence. Users before the event and during the event is logged on the network traffic to be carried out is important. These records are necessary to preserve the security measures on the network devices, the devices required by the user on the network can not use, the internet user's IP address and MAC address of the output to be significant, the user attempts to disrupt the functioning of the network is very important in minimizing. Users, network devices must not interfere with the records. In this study, as well as to facilitate network forensics investigations on network devices to improve network security configuration settings to be discussed.

Keywords: Digital Forensics, Network Forensics, Network Security, Network Device Forensics, Information Security

1. GİRİŞ (INTRODUCTION)

Adli bilişim, bilişim sistemleri üzerinden genellikle veri olarak elde edilen delillerin toplanması, kaydedilmesi, sınıflandırılması ve analizi konusunda çeşitli standartlar oluşturmaya çalışan bir bilim dalı olarak kabul edilebilir. Başka bir ifade ile yasal konularda elektronik delillere uygulanan bilişim uygulamasıdır [1]. Adli bilişimin alt dalları olarak şunlardan bahsedebiliriz [1 ve 4]:

- Bilgisayar adli bilişimi,
- Ağ adli bilişimi,
- Ağ cihazları adli bilişimi,
- GSM (Global System for Mobile Communications, Küresel Mobil İletişim Sistemi) adli bilişimi,
- Sosyal medya adli bilişimi,
- GPS (Global Positioning System, Küresel Konumlandırma Sistemi) adli bilişimi,
- Olay müdahale adli bilişimi

Ağ adli bilişimi (Network Forensics), belirli bir sistem içerisinde kurulu olan yerel ağlar, geniş alan ağlar ya da internet ağ trafiklerinin izlenmesi, kayıt altına alınması analiz edilmesi ve analiz neticeleri doğrultusunda adli makamlara gerekli bilgilerin verilmesi olarak düşünülebilir. Ağ cihazları adli bilişimi (Network Device Forensics) ise adli bilişim altında ayrı bir disiplin olarak görülmekten çok ağ adli bilişiminin bir alt dalı olarak düşünülebilir. Mevcut ağ sistemi içerisinde bulunan Switch (anahtarlama cihazı), Hub (çoklayıcı), Router (Yönlendirici), Repeater (Tekralayıcı), Bridge (Köprü), Firewall (Güvenlik Duvarı), hatta kullanıcı bilgisayarı ağ kartı gibi cihazlar ağ cihazları olarak düşünüle bilinir. Bu cihazlar üzerinde tutulan bilginin değiştirilmeden alınması için bu cihazların doğru yapılandırılmaları gerekmektedir. Doğru yapılandırma aynı zamanda bu cihazların güvenliği için önemlidir. İzni olmayan kişilerin ağ cihazlarına erişimlerinin engellenmesi zorunluluktur. Ağ sistem yöneticisinin bilgisi olmadan ağa farklı cihazlar takarak ağa dâhil olmaya çalışması engellenmelidir.

Özellikle üniversiteler gibi büyük ağlarda 23 Mayıs 2007 Tarihli ve 26530 sayılı resmi gazete gazetede ayrıntıları verilen 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"[2] da belirtilen kayıtların alınması yasal bir zorunluluktur.

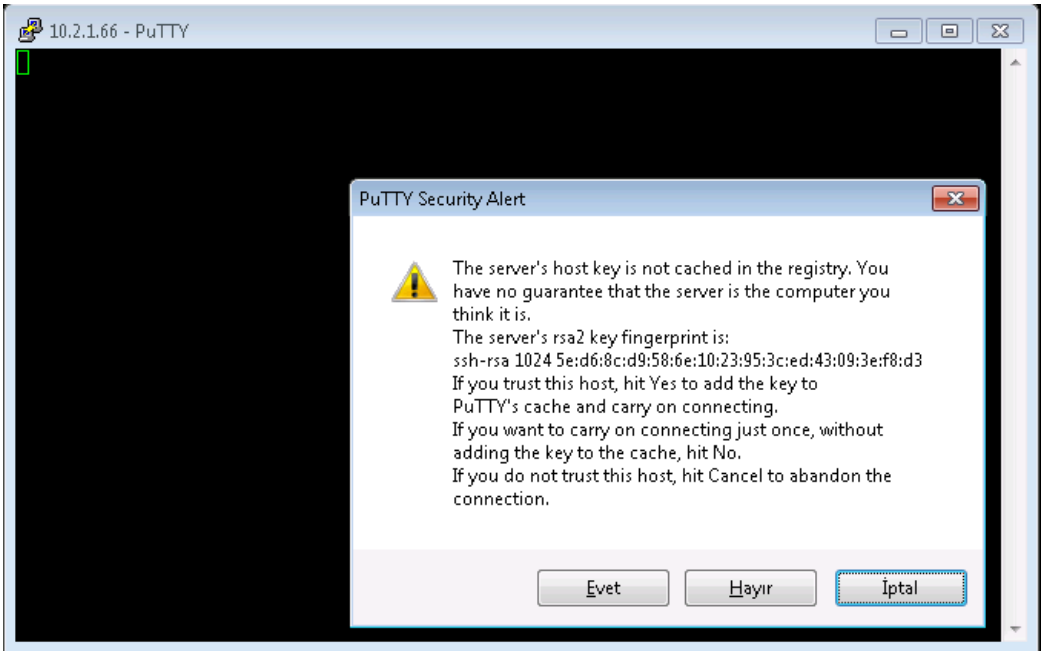
Akıllı anahtarlama cihazları üzerinde yapılandırma dosyası çalıştırılabilen, yönetilebilen cihazlardır[8]. Bu çalışmada daha çok yönetilebilir/akıllı anahtarlama cihazları üzerinde yapılması gereken yapılandırma ayarlarından bahsedilecektir. Bu yapılandırma ayarlarını MAC (Media Access Control) adresi kilitleme, DHCP (Dynamic Host Configuration Protocol) sunucu kontrolü, SPANNINGTREE aktif edilmesi, ARP (Address Resolution Protocol, Adres Çözümleme Protokolü) zehirlenmesinin engellenmesi, güvenli SSH (Secure Shell, Güvenli Kabuk) bağlantısı, VLAN (virtual Local Area Network, Sanal Yerel Alan Ağı) tanımlanması, yapılandırma dosyalarının alınması olarak düşünebiliriz. Bu yapılandırma ayarlarının yapılmaması durumunda ise oluşabilecek problemler tartışma ve sonuç bölümünde irdelenecektir.

2. ÇALIŞMANIN ÖNEMİ (RESEARCH SIGNIFICANCE)

Son yıllarda sık sık ağ güvenlik problemlerinin meydana gelmesinde, internet dolandırıcılığında, veri hırsızlığında kötücül yazılımlar anahtar suçlu olmuştur [3]. Yönetilebilir anahtarlama cihazlarına uzaktan erişebilmek için açık kaynak kodlu PuTTy yazılımı kullanılmıştır[3]. Yapılandırma dosyalarının denenebilmesi için

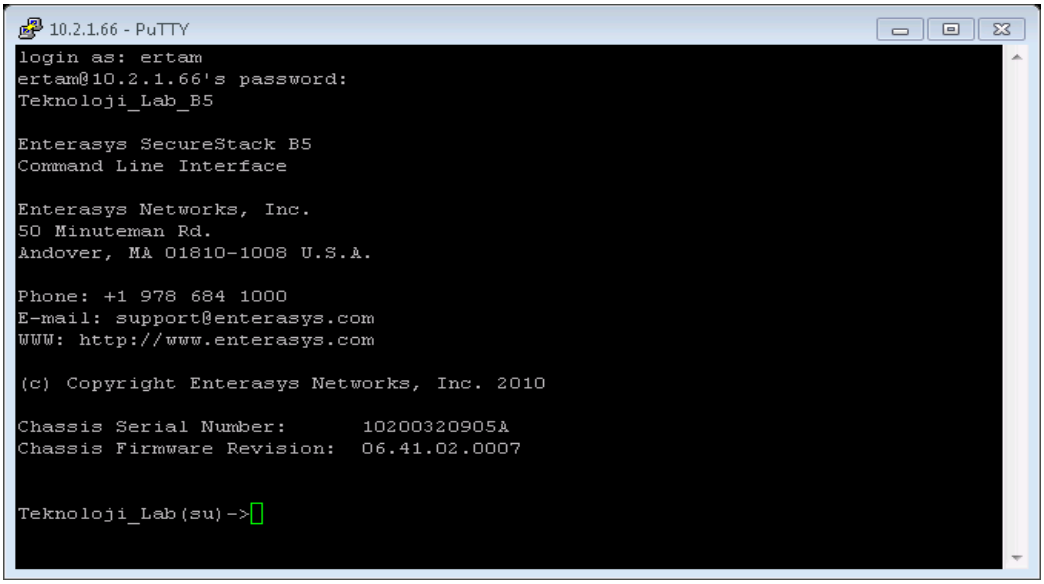
yönetilebilir anahtarlama cihazı olarak Enterasys firmasına ait B5G124-48 anahtarlama cihazı kullanılmıştır. Özellikle aktif olarak çalışan bir ağ yapısı içerisinde hazırlanan yapılandırmalar çalıştırılarak gözlemlenmiştir.

Anahtarlama cihazına öncellikle yönetim portundan RS-232 seri kablo bağlantısı ile erişilerek IP (Internet Protocol) adresi ataması yapılmıştır. Ağ cihazlarına IP adresi verilmesi yönetilebilirliği kolaylaştırmasına rağmen güvenliği azaltmaktadır. Çok fazla sayıda anahtarlama cihazının bulunduğu ağlarda problem oluşması durumunda anahtarlama cihazının bulunduğu fiziksel alana gidilerek problemin giderilmeye çalışılması işlerin oldukça yavaş ilerlemesine sebep olacaktır. Bu güvenlik zafiyetinin önlenebilmesi için anahtarlama cihazlarına telnet bağlantısı yerine daha güvenli olan SSH bağlantısı ile bağlanılması uygun bir yapılandırma yöntemi olacaktır. Telnet ile yapılan bağlantılarda ağ trafiğini bilginiz dışında dinleyen birisinin kullanıcı adı ve şifrenizi öğrenebilmesi olası iken, SSH ile yapılan bağlantılarda Şekil 1'de görüldüğü gibi iletişim güçlü bir şifreleme yöntemi ile gerçekleşir.



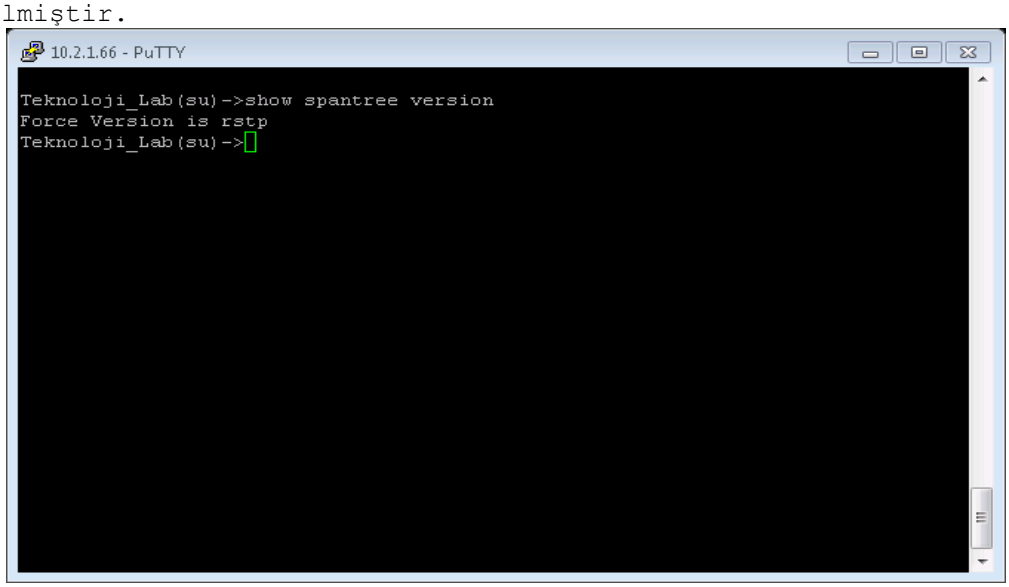
Şekil 1. SSH ile anahtarlama cihazı bağlantısı
(Figure 1. SSH connection with the switching device)

Bu karşılıklı şifreleme yöntemi ile ağ yöneticisi kullanıcı adı ve şifresini yazdıktan sonra Şekil 2'de gösterildiği gibi anahtarlama cihazı arabirimine girmiş olur. Artı bir güvenlik önlemi olarak telnet ile yapılacak bağlantıların reddedilmesi için anahtarlama cihazı üzerinde telnet bağlantısının pasif edilmesi gereklidir. Böylece sadece SSH ile bağlantı sağlanacak ve sizin trafiğiniz dinlense bile kullanıcı adı ve şifrenizin ele geçirilme olasılığı oldukça azalacaktır. SSH bağlantısının dinlenip şifre ele geçirilmesi oldukça düşük bir olasılık olmasına rağmen yüzde yüz güvenlik diye bir kavramdan bahsedemeyeceğimiz de aşikârdır.



3. DENEYSEL YÖNTEM (EXPERIMENTAL METHOD)

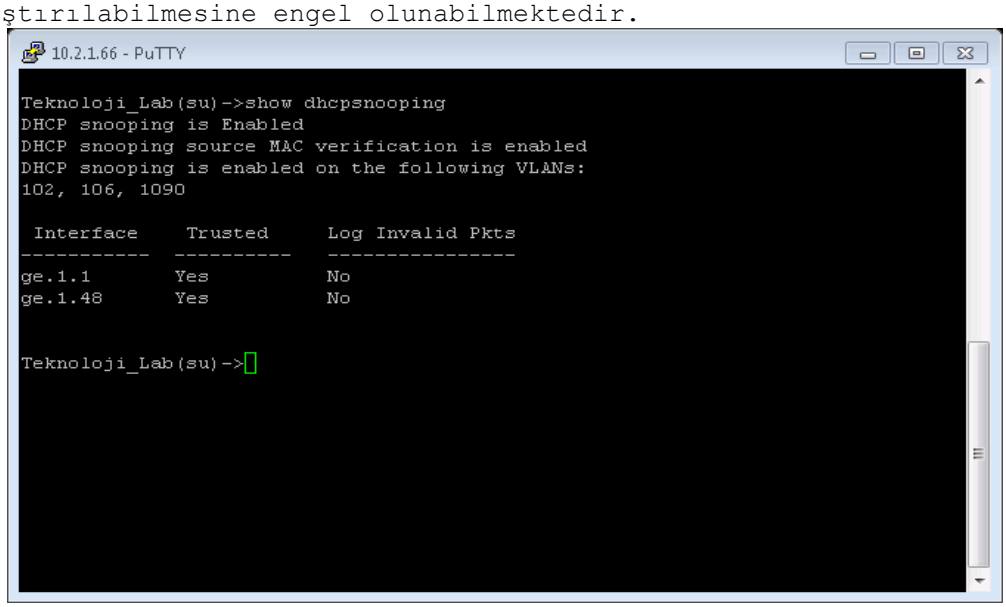
Anahtarlama cihazında oluşabilecek döngülerin engellenebilmesi için cihazda SPANNINGTREE aktif hale getirilmiştir. Böylece anahtarlama cihazında kullanıcılara ayrılan portlara giriş yapılırken anahtarlama cihazından çıkan bir kablonun tekrar anahtarlama cihazına takılması gibi bir durum olsa bile bu anahtarlama cihazındaki çalışmayı engellemeyecektir. Aksi takdirde anahtarlama cihazı kendi içerisinde bir döngüye girecek ve gereksiz bir ağ trafiği oluşturarak ağın sağlıklı bir şekilde çalışmasına engel olacaktır. Şekil 3'de anahtarlama cihazı için ayarlanan SPANTREE sürümü gösterilmiştir SPANNINGTREE için RSTP (Rapid Spanning Tree Protocol) sürümü seçilmiştir.



DHCP, istemci cihazların; IP adresi, alt ağ maskesi, varsayılan ağ geçidi ve DNS adresi gibi bilgileri otomatik olarak edinmesini sağlayan bir protokoldür [5]. Getirdiği bu faydanın yanında, birtakım

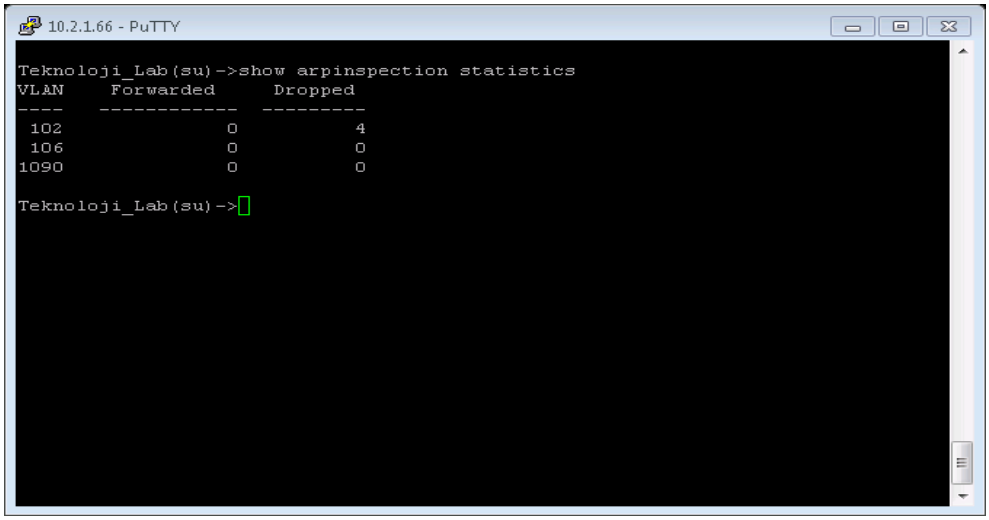
güvenlik tehditlerine açık kapı bırakması ağlarda DHCP ile ilgili gerekli önlemlerin alınmasını zorunlu kılmaktadır.

Ağda sahte DHCP sunucusu kuran ve çalıştıran bir kişi, aynı ağda DHCP isteğinde bulunan istemci cihazlara varsayılan ağ geçidi adresi kendisine ait olan bir DHCP cevabı dönebilir. İstemci bu cevabı aldığı andan itibaren ağ geçidi adresi olarak bu sahte adresi kullanmaya başlar ve yerel ağın dışında bir adresi hedefleyen paketleri ilk olarak sahte DHCP kurulumu yapan kişinin makinesine yönlenir. Bu durum ağ yöneticisinin bilgisi dışında paketleri gitmeleri gereken doğru adreslere kendi üzerinden gönderirken tüm paketleri izleme olanağına sahip olur. Böyle bir duruma engel olunabilmesi için Şekil 4'de gösterildiği gibi DHCPSNOOPING aktif hale getirilmiştir. Anahtarlama cihazındaki UPLINK portlarından, üzerinde VLAN tanımlı olanlar için DHCPSNOOPING güvenilir halde çalıştırılmakta diğer tüm portlarda ise porta takılı bir makinede sahte DHCP sunucusu kurulsa bile çalıştırılabilmesine engel olunabilmektedir.



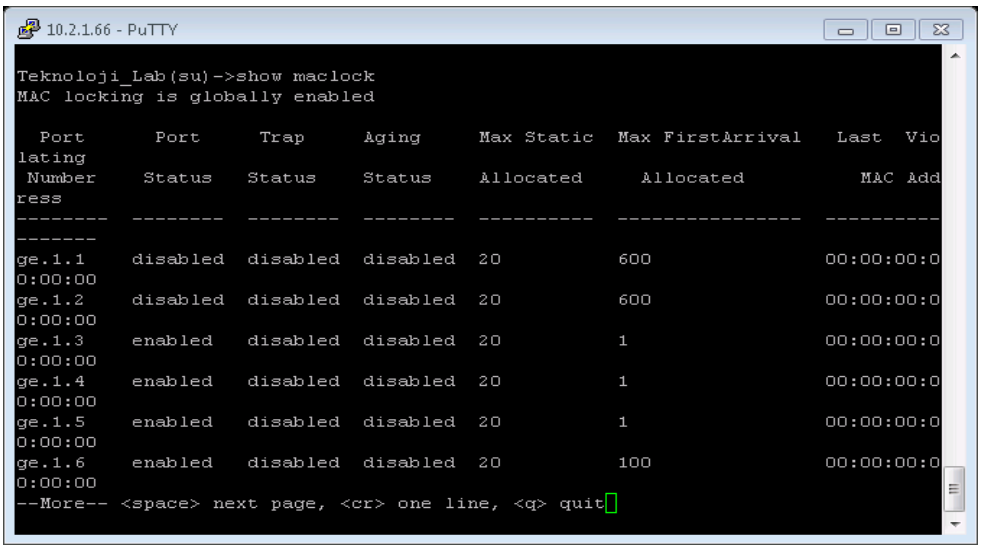
Şekil 4. DHCPSNOOPING durumu
(Figure 4. DHCPSNOOPING status)

ARP, OSI (Open System Interconnection) katman modeline göre ağ katmanında yer alır [6]. Bu katmanda yer alan ARP, IP adreslerini MAC adreslerini çevirir. Bu IP adreslerine karşılık gelen MAC adreslerini ARP tablolarında tutar ve ARP tabloları da belirli aralıklarla güncellenir. Bir IP adresine karşılık, sahte bir MAC adresi oluşturulmasına ARP zehirlenmesi denilir. ARP tablolarında tutulan IP ve MAC adresi eşleştirmelerine müdahale etmek mümkündür. Bu tablolara yapılacak müdahale ile ağ trafiği artırılarak, ağ isteklere cevap veremez hale getirilebilir. ARP zehirlenmelerinde, saldırgan ağ trafiğini değiştirebilir ya da ağ trafiğini tamamen durdurabilir. Bu problemin giderilebilmesi için Şekil 5'de gösterildiği gibi anahtarlama cihazı üzerinde ARPINSPECTION aktif hale getirilmiştir.



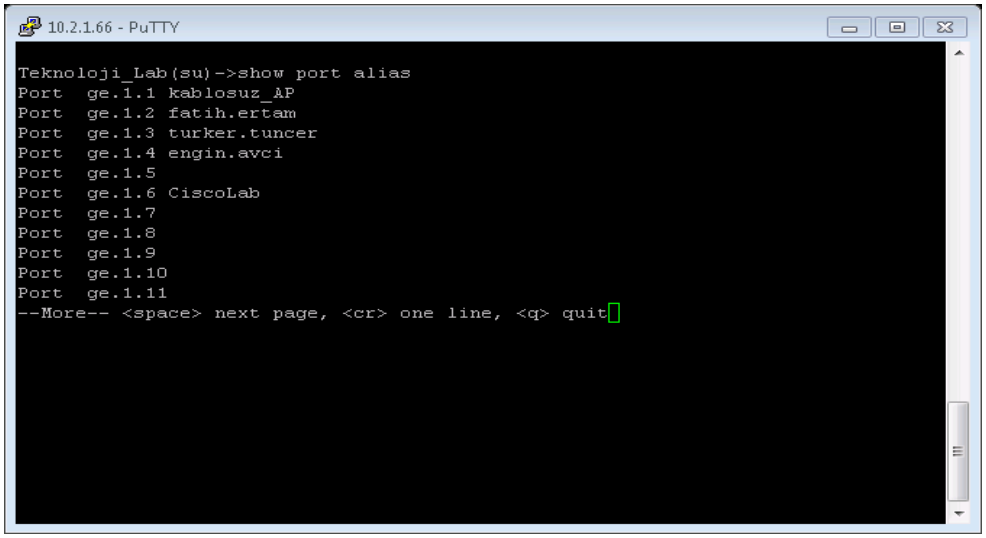
Şekil 5. ARPINSPECTION istatistiği
(Figure 5. ARPINSPECTION statistics)

Kullanıcıların ağ sistem sorumlusunun bilgisi dışında anahtarlama cihazından gelen kabloya ayrı bir anahtarlama cihazı ya da ağ cihazı takarak birden fazla cihazı kullanabilmelerine engel olabilmek için anahtarlama cihazı üzerinde MAC adresi kilitlemesi yapılmıştır. Böylece anahtarlama cihazının her bir portuna bağlı tek bir aktif cihazın takılabilmesi sağlanmıştır. Şekil 6'da bu durum gösterilmektedir.



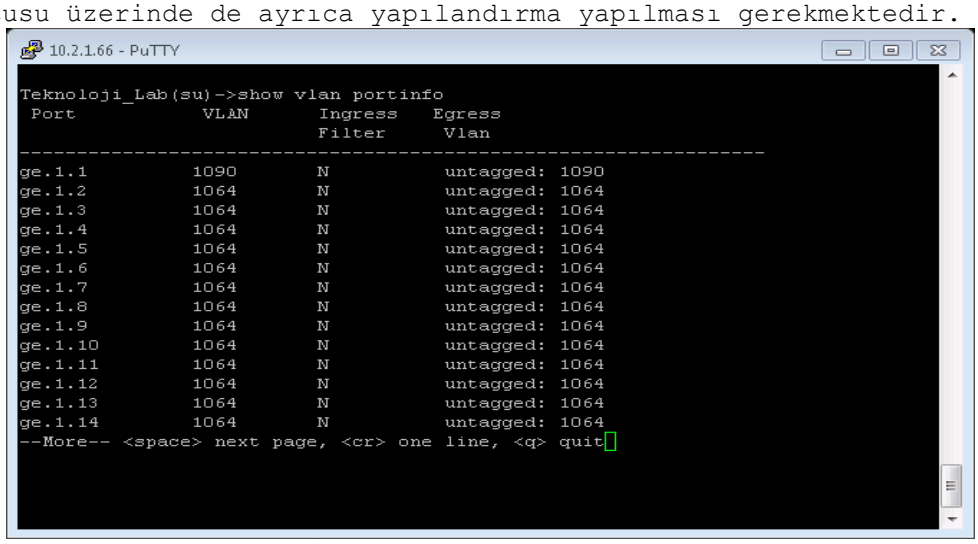
Şekil 6. Mac Kilitlemesi
(Figure 6. Mac locking)

Anahtarlama cihazında bulunan portların işaretlenmesi ve isimlendirilmesi, porta takılı olan ucun tespit edilebilmesini hızlandıracaktır. Bu yüzden mümkün olduğunca port üzerinde Şekil-7 de görüldüğü gibi isimlendirmeler yapılmalıdır. Ayrıca anahtarlama cihazı üzerinde fiziksel olarak da etiketlendirme yapılması adli bilişim incelemelerini hızlandıracaktır.



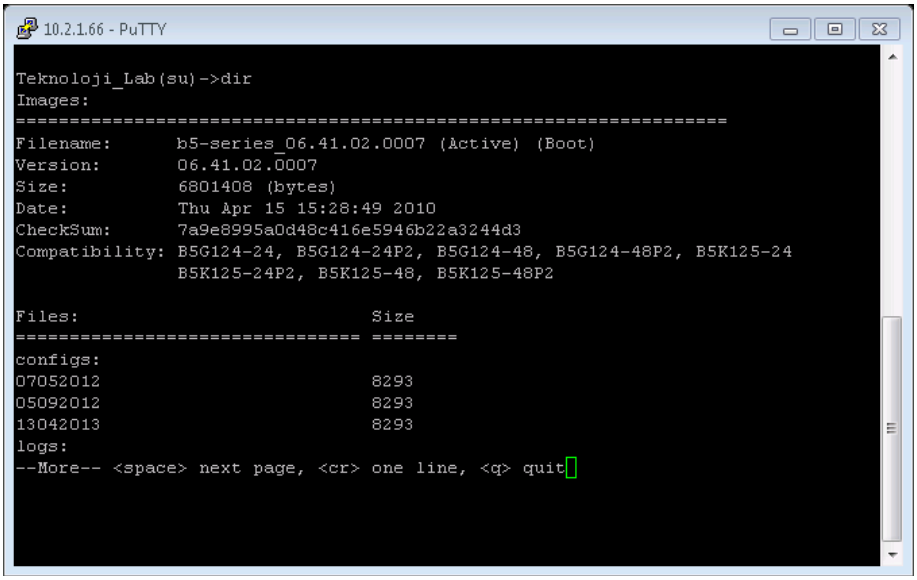
Şekil 7. Port etiketleri
(Figure 7. Port tags)

VLAN sanal yerel ağ olarak kabul edilir [7]. Ağ üzerinde ayrı VLAN'lar oluşturulması ve belli anahtarlama cihazlarına takılı portların belli VLAN lar üzerinden IP adresi alarak ağa dâhil olması hem ağ trafiğini rahatlatacak hem de olası bir şüpheli tespitini kolaylaştıracaktır. VLAN için yönlendirici, güvenlik duvarı ve DHCP sunucusu üzerinde de ayrıca yapılandırma yapılması gerekmektedir.



Şekil 8. VLAN atanmış portlar
(Figure 8. Ports are assigned to VLAN)

Anahtarlama cihazı üzerindeki mevcut yapılandırmanın hem anahtarlama cihazı üzerine hem de ayrı bir sunucu üzerine kaydedilerek zaman zaman karşılaştırılması, olası bir yapılandırma değişikliğinin fark edilebilmesini sağlayacaktır. Şekil-9 da yapılandırma dosyalarının belirli zaman aralıklarında kaydedilmiş dosyalar görülmektedir.



Şekil 9. Anahtarlama cihazındaki yedeklenmiş yapılandırma dosyaları (Figure 9. Switching device configuration files are backup)

4. BULGULAR VE TARTIŞMALAR (FINDINGS AND DISCUSSIONS)

Mevcut incelemelerden anlaşılacağı sunucu üzerinde ağ trafiği oluşturan bir problem görülmektedir. Anahtarlama cihazı üzerinde yapılan ayarlar ile anahtarlama cihazının güvenliği sağlanmış ve ağ adli bilişimi vakalarında gerekli verinin bozulmadan alınabilmesine imkân tanınmıştır.

Anahtarlama cihazına IP adresi verilerek uzaktan bağlantı yapılabilmesi sağlanmıştır. Uzaktan bağlanabilmenin yönetim kolaylığı açısından avantajı olmakla birlikte, kötü niyetli kişilerinde ağ trafiğini dinleyerek kullanıcı adı ve şifrelerini ele geçirebilmesi ve anahtarlama cihazı arabirimine bağlanabilmeleri de olasıdır. Bu olasılığı en aza indirebilmek için anahtarlama cihazına telnet bağlantısı yapılabilmesi engellenmiştir, bunun yerine SSH adı verilen güvenli bağlantı aktif edilmiştir.

Anahtarlama cihazına fiziksel olarak ulaşabilen ya da bilinçsiz ağ teknisyenleri tarafından yapılabilecek hatalardan olan anahtarlama cihazı üzerindeki bir porttan çıkan kablonun tekrar anahtarlama cihazı üzerindeki bir porta takılarak anahtarlama cihazının döngüye girerek hizmet veremez duruma gelmesini engellemek için "SPANNINGTREE" aktif edilmiştir. "SPANNINGTREE" nin aktif edilmesi ile aynı anahtarlama cihazına bağlı kullanıcıların iletişim sürelerinin artacak olmasına rağmen, güvenlik ve verimli çalışma üst seviyeye çıkacağı için tercih edilmiştir.

Kötü niyetli bir kullanıcının sahte DHCP sunucusu kurarak ağ üzerindeki diğer bilgisayarların trafiğini dinleyebilmesini engelleyebilmek için DHCPSNOOPING aktif edilmiştir.

Arp zehirlenmesi verilen atakların engellenebilmesi için anahtarlama cihazı üzerinde ARPINSPECTION ile ilgili yapılandırma yapılmıştır.

Anahtarlama cihazından gelen UTP (Unshielded Twisted Pair, Korumasız Bükümlü Kablo) kablonun kullanılarak anahtarlama cihazı gibi aktif cihazların takılmasının önüne MACLOCKING aktif edilerek geçilmiştir. Böylece kullanıcılar ağ yöneticisinin bilgisi olmadan sisteme MAC adresine sahip yeni aktif cihazlar takamayacaklardır. Böylece adli bilişim incelemesinde gereksiz trafik oluşturarak delillerin ele geçirilmesinin zorlaştırılmasına imkân verilmemiş olunacaktır.

Portlara etiketler verilerek anahtarlama cihazı arabirimine girildiğinde kullanıcıların kolay tespit edilebilmesi sağlanacaktır. Bu işlem güvenlik açısından bir kolaylık getirmemesine rağmen kullanıcı tespiti açısından hız kazandırmaktadır.

Yeni VLAN oluşturularak olası bir adli bilişim incelemesinde şüpheliye ait IP adresi bilgisinden bulunduğu fiziksel alanın tespitinin daha kolay yapılabilmesi sağlanmıştır. Aynı zamanda yeni VLAN'ların oluşturulması problem yaşanan bir VLAN içerisindeki ağ probleminin başka VLAN'ları etkilemesi sağlanarak ağın daha sağlıklı çalışabilmesine imkân tanınmıştır.

Yapılandırma dosyaları hem anahtarlama cihazı üzerinde yedeklenmiş hem de başka bir sunucu üzerinde yedeklenmiştir. Böylece bir problem olması durumunda yedek yapılandırmanın yüklenebilmesine imkân tanınmıştır. Yedek yapılandırmanın aynı zamanda fiziksel sunucuda olması anahtarlama cihazı üzerinde olası bir donanım arızasından kaynaklanabilecek bir hatada yedek bir anahtarlama cihazının kurularak hızlı bir şekilde yapılandırmasının yapılabilmesini sağlayacaktır.

5. SONUÇLAR (CONCLUSIONS)

Ağ adli bilişimi, adli bilişim için çok önemlidir [9-10]. Bu çalışmada adli bilişimin bir alt dalı olan ağ adli bilişimi ve ağ cihazları adli bilişimi inceleme alanı içerisinde bulunan anahtarlama cihazlarının güvenli yapılandırmalarından bahsedilmiştir. Bahsedilen çalışmalar tamamen yeterli olmamakla birlikte ağ adli bilişimi incelemelerine yardımcı olabilecek şekilde anahtarlama cihazlarının yapılandırmalarını kapsamaktadır. Ağ anahtarlama cihazları genel ağ yapılandırması içerisinde önemli bir yere sahiptir ve hemen hemen tüm büyük ağlarda kenar anahtarlama cihazı ya da daha büyük işlem hızına sahip omurga anahtarlama cihazları olarak yer almaktadırlar. Tablo 1. de ağ adli bilişimi açısından anahtarlama cihazı üzerinde yapılan işlemlerin karşılaştırılması verilmiştir. Tablodan da anlaşılacağı üzere yapılması beklenen işlemlerin yapılmaması durumunda genel olarak ağın yönetilmesinde ve güvenliğinin sağlanmasında ciddi problemler ortaya çıkabilecektir.

Tablo 1. Ağ adli bilişimi açısından anahtarlama cihazı üzerinde yapılan işlemlerin karşılaştırılması
(Table 1. Comparison of the processing switching device for network forensic computing)

Anahtarlama Cihazında Yapılan İşlem	**Yapılması Durumunda Gerçekleşenler**	**Yapılmaması Durumunda Gerçekleşenler**
Anahtarlama cihazına yönetim IP adresi verilmesi	Yönetim Kolaylığı	Güvenlik seviyesinin artırılması
Telnet Bağlantısının pasif edilmesi	İstemciler üzerinden kolay bağlantı sağlanamaması	Trafiğin dinlenilerek kullanıcı adı ve şifrenin ele geçirilebilmesi
SSH bağlantısının aktif edilmesi	Daha güvenli bağlantı sağlanması	Güvenli bağlantı sağlanamaması
Spanning Tree aktif edilmesi	Döngülerin engellenmesi	Döngülerin oluşarak anahtarlama cihazının çalışamaz hale gelebilmesi
Dhcp snooping aktif edilmesi	Sahte DHCP sunucuların engellenmesi	Sahte DHCP sunucuların engellenememesi
Arp inspection aktif edilmesi	Arp zehirlenmesi atağının önüne geçilmesi	Arp zehirlenmesi atağının önüne geçilememesi
Mac locking aktif edilmesi	Kullanıcıların anahtarlama cihazından gelen uca tek bir cihaz bağlayabilmesi	Kullanıcı gelen hatta anahtarlama cihazı takarak istediği kadar aktif cihazı kullanabilmesi
Port alias kullanılması	Porttan çıkan hattın nereye gittiğinin kolay tespiti	Anahtarlama cihazı arabiriminin kolay kullanılamaması
VLAN oluşturulması	Olası problemlerde sadece o VLAN üzerindeki kullanıcıların etkilenmesi	Yapılandırma ayarlarının zorlaşması
Yapılandırma dosyasının yedeklenmesi	İstenilen yapılandırma zamanına geri dönülebilmesi	Olası problemlerde yapılandırmanın tekrardan oluşturulması

NOT (NOTICE)

Bu çalışma, 20-21 Mayıs 2013 tarihleri arasında Elazığ Fırat Üniversitesinde yapılan 1.Uluslararası Adli Bilişim ve Güvenlik Sempozyumunda sözlü sunum olarak sunulan çalışmanın hakemlik sürecinden geçirilmiş ve yeniden yapılandırılmış halidir.

KAYNAKLAR (REFERENCES)

1. Daniel, L. and Daniel, L., (2011). "Digital Forensic: The Subdisciplines", Digital Forensic for Legal Professions, S17-23
2. http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (15.04.2013 tarihinde girildi)
3. http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html (15.04.2013 tarihinde girildi)

4. Jeon, S.D., (2006). Digital forensic technology tendency and expectation, information policy 13/4.
5. Wang, J-H. and Lee, T.L., (2002). Enhanced intranet management in a DHCP-enabled environment, Computer Software and Applications Conference, 2002. COMPSAC 2002. Proceedings. 26th Annual International.
DOI: 10.1109/CMPSAC.2002.1045119, S:893-898.
6. Kumar, S. and Tapaswi, S., (2012). A centralized detection and prevention technique against ARP poisoning, Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference
DOI: 10.1109/CyberSec.2012.6246087, S:259-264.
7. Kok, C.W.I., Beg, M.S., and Gehlot, N., (2000). Inter bridge VLAN registration protocol for IP subnet VLAN, Local Computer Networks, 2000. 25th Annual IEEE Conference
DOI: 10.1109/LCN.2000.891093, S:520-521.
8. Ertam, F. ve Dilmen, H., (2013). Yönetilebilir Anahtarlama Cihazları Kullanılarak Öğrenci Laboratuvarlarının Internet Bağlantısının Etkin Kullanımı, 2013 Akademik Bilişim Konferansı, Antalya.
9. Jiang, D. and Shuai, G., (2011). Research on the clients of network forensics, Computer Research and Development (ICCRD), 3rd International Conference on Volume:1
DOI: 10.1109/ICCRD.2011.5764059, S:466-468.
10. Wagener, G., Dulaunoy, A., and Engel, T., (2008). Towards an Estimation of the Accuracy of TCP Reassembly in Network Forensics, Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on Volume:2,
DOI: 10.1109/FGCN.2008.118, S: 273-278.