**Ders Planı**

Ders 1.1.4 İnternette Şüphelilerin Tespiti

|  |  |  |
| --- | --- | --- |
| Ders 1.1.4 İnternette Şüphelilerin Tespiti | | Süre: 1 saat |
| **Gerekli Kaynaklar:**   * Windows 7, 8 veya 10 ve Office 2010 ve üstü kurulu olan bir dizüstü bilgisayar ya da PC * Projektör ve perde * Beyaz tahta, kağıt pano veya katılımcıların söyleyeceklerinin kaydedileceği başka olanak * Bu kaynaklar sadece eğitimcinin PowerPoint sunumu kullandığı durumda gereklidir | | |
| **Oturumun Amacı:**  Katılımcılara, kişinin çevrimiçi faaliyetleri ile gerçek kimliği arasındaki ilişki hakkında bilgi vermek ve bu bağlantıyı kurmanın önündeki güçlüklere değinmektir. | | |
| **Hedefler:**  Dersin sonunda katılımcılar:   * Önemli internet terimlerini açıklayabilecek, * IP adresinin ne olduğunu anlatabilecek, * Şüpheli IP adresinin nasıl bulunacağını tarif edebilecek, * Şüpheli IP adresi ile bir gerçek kişinin nasıl ilişkilendirileceğini anlatabilecek, * İnternette şüphelilerin tespitinin önündeki üç teknik engeli açıklayabilecektir. | | |
| **Eğitmen Rehberi**  Bu oturumda katılımcılara, internetteki şüphelilerin kimliklerinin tespiti ve kişinin çevrimiçi faaliyetleri ile gerçek kimliği arasındaki bağlantının kurulması hakkında bilgiler ve bu bağlantıyı kurmanın önündeki güçlükler aktarılacaktır.  Bu oturuma ilişkin tüm bilgiler, kaynak paketindeki “Oturum 1.1.4 – İnternette Şüphelilerin Tespiti” adlı Powerpoint sunumunda yer almaktadır. Materyallerin güncel olmasından eğitmen sorumludur. Değişiklikler yapılabilir ancak genel hedefe ulaşılması gerekmektedir. | | |
| **Ders İçeriği** | | |
| **Slayt Numaraları** | **İçerik** | |
| Slayt 2 - 4 | Eğitimci, IP adresi kavramını katılımcılara hatırlatmalıdır. Bu ders için önemli olan konular slaytlarda özetlenmiştir. | |
| Slayt 6 | Dersin bu bölümünde, çevrimiçi gerçekleşen şüpheli faaliyetlerle IP adreslerinin eşleştirilmesinin nasıl mümkün olabileceği işlenmektedir. Bu, internet soruşturmalarının gerekli bir unsurudur. | |
| Slayt 7 | Eğitimci, web sunucularının genellikle gelen tüm taleplerin kaydını tuttuğunu açıklamalıdır.  Ancak bunun sunucu üzerinde bir ayara bağlı olduğu ve sunucuyu kullanan kişileri gizlemek isteyen kişilerin bu kayıt sistemini kapatabilecekleri de anlatılmalıdır. Bu durumda web'de gezinme hareketlerinin kaydı tutulmayacaktır. | |
| Slayt 8 | Eğitmen bunun bir web sunucu kaydına örnek olduğunu açıklamalıdır. Slaytta ilgili yerleri göstererek aşağıdakileri vurgulamalıdır:   1. Kaynak IP adresi – 216.128.130.126 2. HTTP talebinin saat ve tarihi – 23/Eylül/2006:21:30:02 -0400 – Eğitimci saat dilimini de vurgulamalıdır, bu örnekte GMT-4'tür. 3. Talep edilen şey olan “/pgp/” kaynak olarak adlandırılır ve talebi alan sunucu üzerinde bir anlam ifade eder. Bu sunucu üzerindeki bir belge, klasör ya da disk görüntüsü olabilir. 4. Bu talebi gerçekleştiren bağlantıya tıkladığı sırada kullanıcının bulunduğu sayfadır. Buna gönderen denir. Bu örnekte, dir.yahoo.com ile başlayan uzun dizidir. Bu kayda bakarak, kullanıcının bu sayfayı incelemekte iken bir bağlantıya tıkladığını, bunun da sunucuya “/pgp/” kaynağı için bir talep gönderdiğini anlayabiliriz.   Tarayıcıyı gösteren dizi (Mozilla/4.0 ile başlar), istemci bilgisayarın kullanmakta olduğu web tarayıcısını gösterir fakat bu bilginin sahtesiyle değiştirilmesi mümkündür. | |
| Slayt 9 | Eğitimci, web'de gezinmeden farklı olarak epostanın alıcısı ve göndereninin doğrudan iletişim içinde olmadığını açıklamalıdır. | |
| Slayt 11 | Eğitimci, epostaların gönderilme ve iletilme sürecinin SMTP (Basit Posta Transfer Protokolü), epostanın kontrol edilmesi ve alınmasını sağlayanın ise POP (Posta Kutusu Protokolü) ya da alternatifi IMAP olduğunu açıklamalıdır.  Eğitimci, eposta alıp verme sürecini giden posta sunucusu ve gelen posta sunucusu örnekleri üzerinden anlatmalıdır.  Eğitimci, web tabanlı eposta (örneğin Gmail) uygulamasında ise, kişinin gelen posta sunucusuyla iletişim için POP3 kullanmak yerine bir web sunucusuna giriş yaparak doğrudan sunucu üzerinde epostasını okuduğunu açıklamalıdır. | |
| Slayt 13 | Eğitimci, katılımcılara bu formatta gördüklerinde tanıdık gelmese bile, okudukları her epostanın buna benzer başlıkları olduğunu anlatmalıdır.  Eğitimcinin özellikle vurgulayacakları:   1. Received [Alınan] başlığı altında bu epostayı işleyen IP adresleri 2. Gönderen ve alan eposta adresleri 3. Konu 4. Tarih   Eğitimci, epostanın kaynağını saklamak isteyen birinin bu bilgileri değiştirebileceğini, bu nedenle eposta başlıklarını doğru analiz etmek için teknik bilgiye ihtiyaç olduğunu anlatmalıdır. | |
| Slayt 14 | Eğitimci, katılımcılara IP adresi olduğunu düşündükleri diğer hizmetleri sormalıdır.  Skype, Pokemon Go, DropBox, Facebook, Google, Microsoft gibi örnekler üzerinden tartışma yürütülmesini sağlamalıdır. | |
| Slayt 15 | Dersin bu bölümünde, çevrimiçi gerçekleşen şüpheli faaliyetlerle IP adreslerinin eşleştirilmesinin nasıl mümkün olabileceği işlenmektedir. Bu, internet soruşturmalarının gerekli bir unsurudur. | |
| Slayt 16 | Eğitimci, internetin kısa bir giriş dersinde işlenebileceğinden çok daha karmaşık olduğunu belirtmelidir. Katılımcıları, dünyadaki her kişi ile internetteki her IP adresi arasında bire bir eşleştirme yapılamayacağına dair uyarmalıdır. IP adresinin bir kişiyi teşhis etmemesinin çeşitli sebepleri vardır (IP adresi gerekli fakat tek başına yeterli olmayan bir bilgidir).  İki somut örnek ele alınmalıdır:   1. Statik ve dinamik IP adresleri: Eğitimci, katılımcılara evlerinde ne tür bir internet bağlantısı kullandıklarını düşünmelerini söylemelidir. Büyük olasılıkla kablo veya DSL hizmetleri kullanıyorlardır. Her iki durumda da İnternet Servis Sağlayıcısının IP adreslerini periyodik olarak değiştirmesinin neredeyse kesin olduğunu belirtmelidir. Dolayısıyla bir abonenin teşhis ve tespit edilebilmesi için hangi IP adresinin kullanıldığı kadar bu IP adresinin ne zaman kullanıldığı da bilinmelidir. Kurumlar içinde de benzeri bir durum meydana gelebilir ve bir bilgisayar her kapatılıp açıldığında yeni bir IP adresi alabilir. 2. Ağ adresi çevirme - Eğitimci, 4 milyar IP adresi bulunmasına rağmen bunların teker teker değil, gruplar halinde tahsis edildiğini açıklamalıdır. Bir grup bir kuruma tahsis edildikten sonra, o gruptaki IP adreslerini başka hiçbir kurum kullanamaz. Eğitimci, bunun IP adresi tahsisi için çok verimsiz bir yöntem olduğunu, bu nedenle IP adreslerinin tükenmeyle karşı karşıya kaldığını açıklamalıdır. Bu ve başka nedenlerle, IP adreslerinin daha uzun olabilen yeni bir sürümü çıktığını (IP sürüm 6) anlatmalıdır. İnternette kullanılmasına izin verilmeyen bazı IP adres grupları olduğunu belirtmelidir. Bu adresler ortak ağ yapısı üzerinde iletilmeyecektir. 10 ile başlayan IP adreslerini ya da “192.168” ile başlayan IP adreslerini örnek verebilir. Bu IP adreslerinin yerel ağlarda kullanılabilse de internette kullanılamayacağını açıklamalıdır. Eğitimci, bu tür IP adreslerinin verimliliği nasıl arttırdığını aşağıdaki biçimde anlatabilir:    1. Bir kurum içindeki her bir bilgisayara, internette kullanılamayan bir IP adresi tahsis edilir.    2. Kuruma tahsis edilen gerçek internet IP adresi sayısı çok azdır, belki sadece bir adettir.    3. Kurum bilgisayarlarından biri internetteki başka bir bilgisayarla iletişim kurmak istediği zaman, kurumun altyapısı (özellikle internet ağ geçidi) kurumun dahili IP adresi yerine gerçek internet IP adresini koyduktan sonra trafiği internete gönderir.    4. Bu şekilde çok sayıda bilgisayar tek bir IP adresi üzerinden internette iletişim kurabilir, bunun adı da Ağ Adresi Çevirmedir (NAT).   Bu yöntemin bir özelliği de, kurumun içindeki tüm bilgisayarların internette tek bir IP adresi olan tek bir bilgisayar gibi görünmeleridir. Bir soruşturmada bu IP adresi ortaya çıkabilirse, gerçekte trafiği hangi bilgisayarın çıkardığını sağlamak sadece kurumun yapabileceği bir şeydir. | |
| Slayt 17 | Eğitimci, IP adresi üzerinden abone kimlik bilgisi talep edilebileceğini açıklamalıdır. Bu bilgiyi İnternet Servis Sağlayıcısından istemek için gereken prosedür ülkeden ülkeye değişmekteyse de, genellikle savcılık veya mahkeme emri gerekmektedir. İSS'lerin kayıtları ne süreyle saklayacağı da ülkeden ülkeye değişir. Eğitim hazırlandığı sırada 2 yıl olağan bir süredir.  Elde edilen IP adresinin hangi İSS'ye ait olduğunu bulmak için https://www.whoismyisp.org/ yararlı bir kaynaktır.  Eğitimci, İSS'nin ülke sınırları içinde bulunmaması durumunda, bilginin elde edilmesi için karşılıklı adli yardımdan yararlanılması gerekebileceğini açıklamalıdır. | |
| Slayt 18 | Eğitimci, çokuluslu hizmet sağlayıcıların, bir abonenin giriş yaptığı IP adresi gibi kayıtları sakladığını açıklamalıdır. Örneğin bir Facebook hesabının şüpheli bulunması durumunda, bu hesabın hareketleriyle ilişkilendirilebilecek bir IP adresi elde etmek mümkündür.  Çokuluslu İSS'lerle işbirliğini de kapsayan uluslararası işbirlikleri bu eğitimin başka bir dersinde ayrıntılı olarak anlatılmıştır. | |
| Slayt 19 | Eğitimci, soruşturma sonucunda IP adresinin bir şirkete ait olduğunun öğrenildiği senaryoyu anlatacaktır. Şirketlerin tüm bilgisayarlarda tek bir IP adresi kullanmak için NAT'den yararlandığı açıklanmalıdır. Bu durumda hangi bilgisayarın IP adresini ne zaman kullandığını ancak o şirketin bulabilmesi mümkündür. Dolayısıyla soruşturma için şirketle bağlantı kurulması gerekecektir.  Bu bağlantının nasıl kurulacağı ülke yasalarına göre değişir.  Eğitimci, kayıtların yurtdışında bulunmasının da durumu zorlaştırabileceğini anlatmalıdır. Örneğin şirket bir çokuluslu holdingin bünyesinde ise, kullandığı altyapıyı kendisi yönetmiyor ve işletmiyor olabilir. Bu durumda kayıtlar varsa da başka bir yargı alanında yer almaktadır. Ülkenizdeki şirketin kayıtları verip veremeyeceği, kuruma ve teknik altyapısına bağlıdır. | |
| Slayt 21 | Eğitimci, suçluların IP adreslerini kasten karıştırıp kimlik tespitini imkansız hale getirebileceğini belirtmelidir.  Bazı teknolojilerin ise normal kullanımları sırasında şüpheli IP adreslerini tanınamaz hale getirdiğine değinmelidir. | |
| Slayt 22 | Eğitimci, internette bazı hizmetlerin sadece internet hareketlerinin kaynağını gizleme işlevi gördüğünü anlatmalıdır. Ardından, bir sonraki slaytta yer alan örnek web sayfası gösterilir.  Eğitimci, benzer hizmetlerin eposta kaynağını gizlemek için de kullanıldığını belirtmelidir.  TOR gibi diğer hizmetlerin ise kaynak IP verisini gizlediğini anlatmalıdır. | |
| Slayt 24 | Eğitimci, Taşıyıcı sınıfı NAT'nin IP adresi üzerinden şüphelinin kimlik tespiti bakımından ciddi bir sorun olduğunu belirtmelidir. Bir kullanıcı ile IP adresini şüpheye yer bırakmayacak şekilde eşleştirmek için, port numarası denen bir bilginin de gerekli olması bu soruna yol açmaktadır. Port numaraları genellikle hizmet kayıtlarında saklanmaz. Eğitimci, web sunucu günlükleri ve eposta başlıklarına dönerek, iki kaynakta da port numarası bilgisi yer almadığını belirtmelidir.  Eğitimciye not: Konu hakkında ayrıntılı bilgi için https://en.wikipedia.org/wiki/Carrier-grade\_NAT adresi incelenebilir. | |
| **Pratik Çalışmalar**  Bu derste öngörülen bir pratik çalışma bulunmamaktadır. | | |
| **Değerlendirme /Bilgi Testi**  Bu oturum için bilgi sınavı ve değerlendirme hazırlanmamıştır. | | |