Siber Güvenlik Sorun Raporu Örneği

Bu raporum bir şirketin çalışanlarının yaşamış olduğu problemi ve benim de içerisinde olduğum (Burak Kılıç) siber güvenlik takımı çalışanlarının attığı adımları detaylarıyla anlatan örnek bir senaryoyu kapsamaktadır. Aşağıda yaşanan sorun ve sonrasında duruma dair raporlar iki bölüme ayrılmış bir şekilde yer almaktadır.

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

Bölüm 1: DNS ve ICMP Trafiğinde yaşanan soruna bir özet hazırlanması
Problem ilk olarak şirket çalışanlarının şirketin websitesi olan www.example.com adresine bağlanmaya çalıştıklarında aldıkları “UDP port 53 unreachable” hatasını almalarıyla başladı. Sorun ilk olarak bugün 10:54’de rapor edildi. Port 53 normalde UDP protokolü kullanılarak DNS sunucusuna bağlanmak için kullanılmaktadır. Yukarıdaki komut dizisinden alınan kayıtta internet tarayacısından DNS sunucusuna giden UDP mesajı ilk iki satırda gözükmektedir. Onun hemen altında ise üçüncü ve dördüncü satırlarda DNS sunucusundan internet tarayacısına gönderilen ICMP hata cevabıdır. Port 53 DNS sunucusu ile alakalı olduğu için buradan sorunun DNS sunucusu ile alakalı olduğunu bilebiliriz. Komut dizininde ayrıca hata kodlarını tanımlamak için kullanılan numarada 35084 yazmakta ve bu numara “A?” komutuyla işaretlenmiş durumdadır. Bunların her ikisi DNS protokolü ile alakalı olduğunu kanıtlamaktadır.

Bölüm 2: Verilerin analizini açıklamak ve yaşanan sorunun neyden kaynaklanabileceğini tahmin ederek en az bir sebep ortaya koymak
Komut dizininde, ilk satırda tarih ve saat bilgisi görülmektedir. 13:24:32.192571 şeklinde gözüken numaralarda 13:24 saati, 32.192571 ise saniyeyi gösterir. Bazı çalışanların www.example.com websitesine girmeye çalışırken "Destination host unreachable" yazılı hatayı farketmesi üzerine sorun raporlanmıştır. Biz güvenlik analizcileri ise halihazırda sorunu raporlayıp yöneticilerimize bildirdik, bunun üzerine de güvenlik mühendisleri sorunla ilgilenmeye başladılar. Sorunu araştırırken "tcpdump" kullanarak paketlerin neden ulaşmadığı konusunda komut dizininde DNS portu 53'ün ulaşılamaz olduğuna denk gelindi. Bu durumda DNS sunucusunun mu çalışmıyor olduğunu, yoksa güvenlik duvarının mı trafiği engellediğini bulmak için kolları sıvadık. Güvenlik duvarında bir port'u engellemenin, o port'dan gelecek saldırıyı engellemek için kullanıldığı durumlar olmaktadır. Böyle bir engelleme de söz konusu olabilir. Aynı zamanda DNS sunucusu bir DOS (Denial of Service) saldırısı sebebiyle de çökmüş olabilir.

Hazırlayan: Burak KILIÇ