Sibergüvenlik Olay Raporu

1	No.	Time	Source	Destination	Protocol	Info
74	119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
76	121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
77	122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
78	123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
80	125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
81	126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
83	128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
84	129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

Bölüm 1: Bu ağ kesintisine sebep olmuş olabilecek sebeplerin belirleyin

Web sitenin zaman aşımı hata mesajını vermesinin olası bir açıklaması şu olabilir:

Komut satırı şunları gösteriyor:

Olayın arka planı şu olabilir: “DoS SYN Flood” Saldırısı

Bölüm 2: Saldırının websitenin arızalanmasına nasıl sebep olduğunu açıklayın

Web sitesi ziyaretçileri web sunucusuyla bağlantı kurmaya çalıştığında, TCP protokolü kullanılarak “Three Way Handshake” meydana gelir. “TCP Handshake”in üç adımını açıklayın:
1. SYN (Bağlanma isteği)
2. SYN-ACK (Bağlantı isteğini alınca sunucudan gelen yanıt)
3. ACK (Hedef sunucudan gelen yanıtın onaylanması)

Kötü niyetli bir kişi aynı anda çok sayıda SYN paketi gönderdiğinde neler olduğunu açıklayınız: Sunucuya çok sayıda SYN paketi gönderildiğinde sunucu aşırı yük altına girer, her pakete yanıt veremez hale ve düzgün çalışamaz hale gelir.

Komut satırının neyi gösterdiğini ve bunların sunucuyu nasıl etkilediğini anlatın: Sunucu çok fazla gelen SYN paketleri yüzünden aşırı yük altına girdiği için website’ye gelen yeni ziyaretçilere “connection timed out” hatası veriyor. Sunucu yeni bağlantılar kuramıyor.