T.C.

KARADENİZ TEKNİK ÜNİVERSİTESİ

OF TEKNOLOJİ FAKÜLTESİ

YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

SİBER GÜVENLİK UYGULAMALARI DERSİ PROJESİ

352580

Tuğba CAN

IP Nedir ?

TCP/IP protokolü ile haberleşen makinelerin birbirlerini tanımaları için verilmiş numaralardır. Örneğin: 192.168.10.54 gibi bir IP adresi olabilir. Bu karşıdaki bilgisayarla ilteişim kurabilmemiz için yeterlidir.

Port Nedir ?

Bilgisayarlardaki giriş çıkış noktaları port olarak adlandırılmaktadır. Programların haberleşmesini yaptığı birbirleriyle köprü kurdukları portlardan bahsedilecektir.

Soket Nedir ?

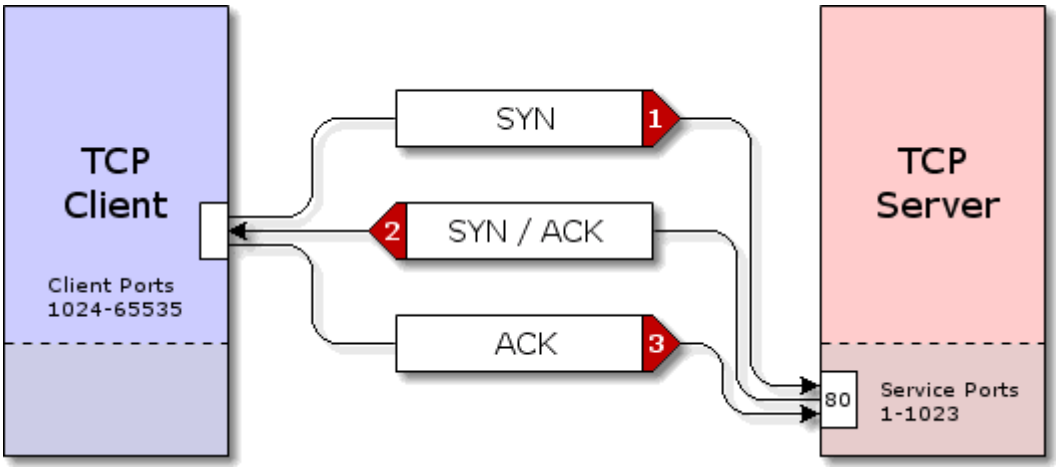
Türkçesi soket olan bu kelimenin anlamı işe IP + PORT = socket olarak tanımlanabilir. Socketler sayesinde bir makineden diğerine iletişim kurulup veri transferi sağlanabilir.

TCP Nedir ?

TCP, veri güvenliğinin garanti altına alındığı, bağlantı temelli (connection-oriented) bir iletişim protokülüdür. TCP protokolü stream soketleri üzerinden sağlanmaktadır.

TCP Üçlü El Sıkışma – TCP 3 Way Handshake

İstemci-sunucu arasında bir veri akışının sağlanması için Üçlü El Sıkışma(3 Way Handshake) denilen olayın gerçekleşmesi gerekir. TCP/IP protokolünü yani paketlerin doğru sırayla istenilen hedefe götüren bir ve ilk bağlantıyı sağlayan protokolü kullanır.



Şekil 1

Üçlü El Sıkışma(3 Way Handshake) Nedir ?

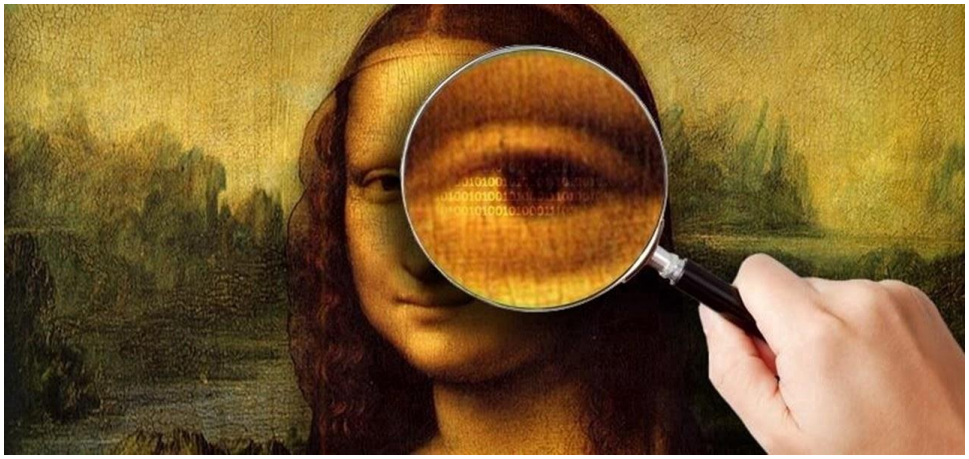
Örneğin bir A bilgisayarı B bilgisayarına bir veri aktarmak istesin.A bilgisayarı istemci(client),B bilgisayarı sunucu(server) olsun.A bilgisayarından B bilgisayarına bir bağlantı kurmak için işletim sisteminin oluşturduğu rastgele bir sequence numarası ile SYNchronize mesajı yollanır.Bu yollanan bit "1" olarak ayarlanmıştır.

Ardından B bilgisayarından istemciye SYN(Synchronize) ve ACK(Acknowledgement)bayraklarını "1" olarak ayarlar ve A bilgisayarının gönderdiği SYN yani sıra numarasını bir artırıp ACK numarası(Acknowledgement Number) olarak ayarlayıp bu mesajı A bilgisayarına iletilir.Böylelikle A bilgisayarı sırayı doğru yapar hem de A bilgisayarının bir sonraki paket sıra numarası belirlenmiş olur. Ayrıca B bilgisayarı da kendi işletim sistemi tarafından rastgele bir ACK numarası belirtilmiş olur ACK ve SYN paketini yollar.

Son olarak A bilgisayarı B bilgisayarının gönderdiği paketi alır sonraki paketi hazırlar ve ACK bayrağını "1" olarak ayarlar.B bilgisayarının gönderdiği sıra numarasını 1 arttırarak B bilgisayarına göndereceği paketin ACK numarası(Acknowledgement Number) olarak ayarlar.Artık SYN bayrağını değiştirmeye gerek yoktur.Çünkü bağlantı sağlanmış oldu SYN ve ACK paketini yollar.Bu sisteme Üçlü El Sıkışma(TCP 3 Way Handshake) denir.

Steganografi Nedir?

Steganografi, eski Yunanca'da Gizlenmiş Yazı anlamına gelmektedir ve bilgiyi gizleme tekniğine verilen addır. Steganografi tekniğine tarihte gösterilebilecek örnekler arasında Sparta kralı Demaratus'un Yunanistan'a ikaz gönderirken mesajını gizlemek için ahşap tablet ve balmumu kullanması, Amerikan Devrim Savaşı sırasında casusların kullandığı görünmez mürekkep veya Leonardo Da Vinci'nin resmettiği tablosuna gizli mesajlar eklemesi örnek olarak gösterilebilir.



Steganografi tekniğinin günümüz dijital dünyasında edindiği yer ise, eski zamanlarda kullanılan yöntemlere benzerlik göstermektedir. Örneğin, hackerlar bir resmi veya fotoğrafı, onların görüntülerini değiştirmeden onların içerisine gizli bir kod yerleştirerek manipülasyon gerçekleştirebilir. Bu teknik genellikle sansürlenme durumundan kurtulmak gibi etik sebeplerden dolayı yapılsa da, her teknoloji veya teknikte olduğu gibi, bu teknik de kötü amaçlı kişiler tarafından CryptoMining (Bilgisayarınızın Kripto Para bulma işlemi için kullanılmasını sağlayan zararlı yazılım), Ransomware (Fidye) Zararlı Yazılımı veya karşı tarafa Zararlı JavaScript kodları iletmek amacıyla kötüye kullanılabilir. Bu zararlı yazılımlara örnek olarak:

AdGholas (Image, Text ve HTML dosyalarına zararlı JavaScript kodları enjekte eder.)

Cerber (Image dosyalarına zararlı kod enjekte eder.)

DNSChanger (PNG formatındaki dosyalarının Least Significant Bitlerini kullanarak zararlı AES şifreleme anahtarlarını enjekte eder.)

Stegano (PNG formatında bulunan zararlı kod içeren bir banner.)

Stegoloadr / Lurk (Bu zararlı yazılım Steganography ve Cryptography tekniklerini birlikte kullanarak şifrelenmiş bir URL'i zararlı yazılım hedefe bulaştıktan sonraki aşama payloadlarında iletmeyi amaçlar.)

Sundown (Kullanıcı bilgilerini çalmak veya exploitation aşamasındaki kodlarını gizlemek için kullanılan açıldığında beyaz görüntüye sahip PNG dosyalarıdır.)

SyncCrypt (Image dosyalarında bulunan bir Ransomware yazılımıdır.)

TeslaCrypt (HTTP 404 döndüren sayfalarda komuta kontrol sunucularına ait kodlar bulunduran HTML comment tag'leridir.)

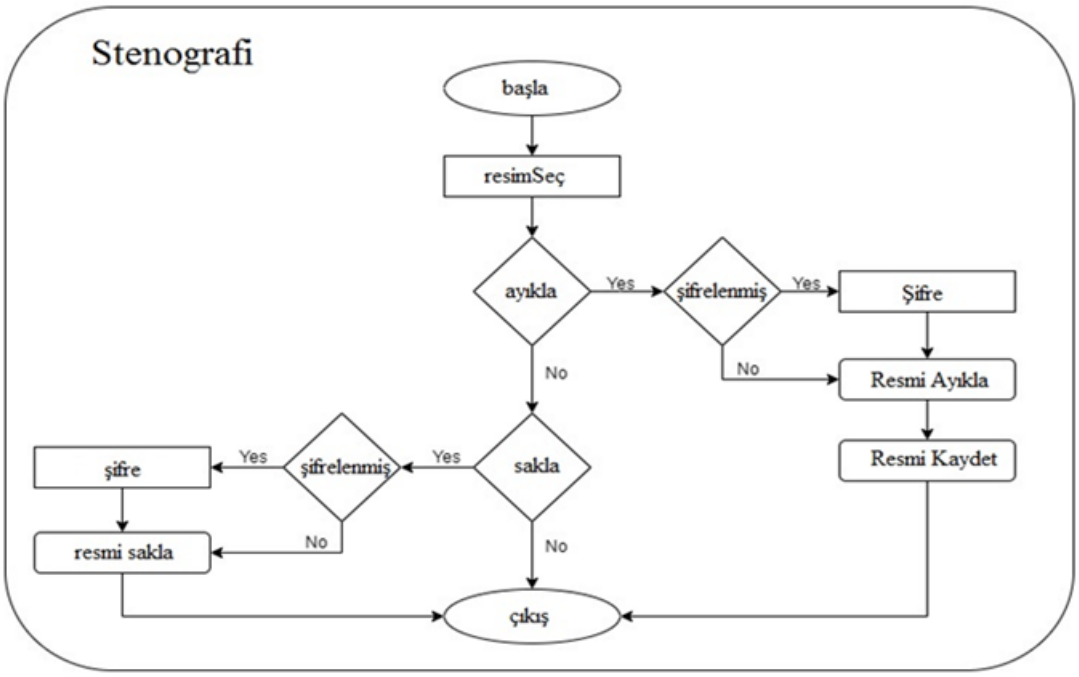
Vawtrak / Neverquest (Favicon dosyalarının Least Significant Bitlerini kullanarak sakladığı URL sayesinde zararlı payloadlar indirmeyi amaçlar.)

VeryMal (macOS kullanıcılarını hedef alan, white bar içerisine gömülmüş zararlı JavaScript zararlı kodlarıdır.)

Zbot (JPEG dosyalarının sonuna gizli veriler ekler.)

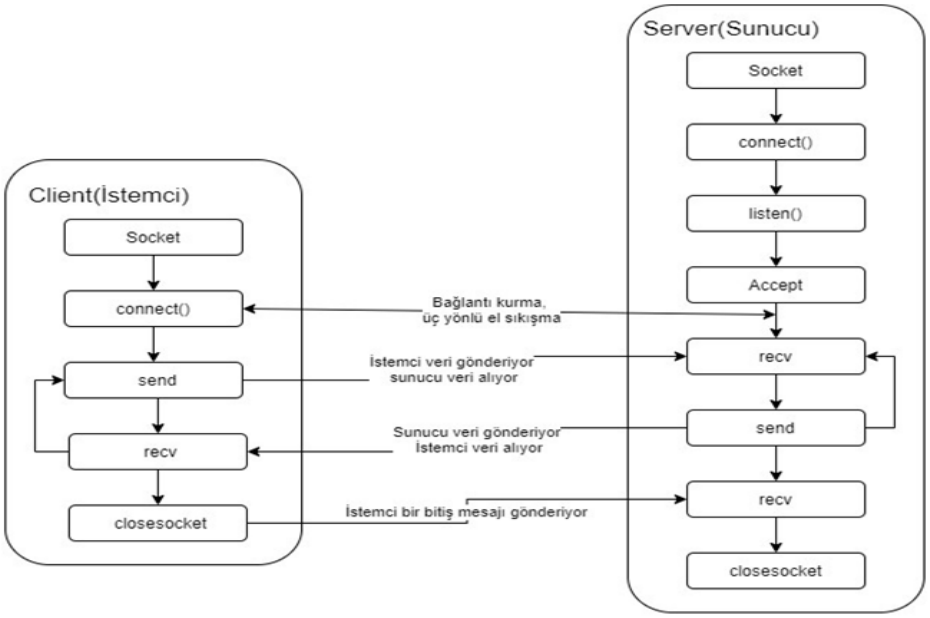
ZeroT (Ünlü şarkıcı Britney Spears'ın fotoğrafını kullanarak zararlı yazılımlar enjekte eden Çin asıllı zararlı yazılımdır.)

Steganografi Akış Şeması



Şekil 2

Soket Programlama Akış Diyagramı



Şekil 3

Kaynakça

https://medium.com/@anilcelik/tr-steganography-nedir-45f9cc4f550a

https://ensarkarabudak.com/tcp-uclu-el-sikisma-tcp-3-way-handshake/

https://demirten.gitbooks.io/linux-sistem-programlama/content/sockets/tcp.html

https://berkarat.com/c-socket-programlama/

https://osmanmarangoz.wordpress.com/2009/06/14/soket-programlamasocket-programming/