## **Öğreneceğimiz başlıca terimler şunlardır :**

* Siber güvenlik nedir ?
* Hacker nedir?
* Beyaz şapkalı hacker nedir ?
* Gri şapkalı hacker nedir ?
* Siyah şapkalı hacker nedir ?
* Cracker nedir ?
* Penetrasyon testi nedir?
* Exploit nedir?
* Phishing nedir ?
* Sniffing nedir ve Çeşitleri ?
* Spoffing nedir?

# **SIK KULLANILAN TERİMLER**

**Siber güvenlik nedir ?**

Siber güvenlik, sistemleri, ağları ve programları dijital saldırılara karşı

koruma uygulamasıdır. Bu siber saldırılar genellikle hassas bilgilere

erişmeyi, değiştirmeyi veya imha etmeyi amaçlar; kullanıcılardan para

çekmek ,veya normal iş süreçlerini kesintiye uğratmak.siber güvenlik

ise yapılan bu illegal saldırıları önlemek için oluşturulmuş bir alandır.

**Hacker nedir?**

Diğer adıyla bilgisayar korsanı dediğimiz bireyler, bir sorunun üstesinden gelmek için bilgisayar, ağ veya diğer becerileri kullanan bir bireydir. Hacker terimi, teknik becerileri olan herkese hitapta bulunabilir,

ancak genellikle suç işlemek için sistemlerine veya ağlarına yetkisiz

erişim sağlamak için yeteneklerini kullanan bir kişi anlamına gelir. Örneğin bir bilgisayar korsanı, insanlara kimlik hırsızlığı, zarar veya

sistem çökertme yoluyla zarar vermek için bilgi çalabilir ve genellikle

fidye toplamak için bu sistemleri rehin tutabilir.

Hacker terimi, tarihsel olarak bölücü bir terimdir, bazen teknik sorunlara yaklaşımında yaratıcılığın yanı sıra, yüksek derecede beceri sergileyen bir kişiye hayranlık terimi olarak da kullanılır.Bu terim daha çok

beceriyi yasa dışı veya etik olmayan amaçlar için kullanan bir kişiye

uygulanmaktadır.

**Beyaz şapkalı hacker nedir ?**

****

Beyaz şapkalı hacker dediğim bireyler ise ;Bir sisteme

izinli bir şekilde girerek bulduğu herhangi bir açığı,

sistem sahibine bildirerek açığın kapanmasını sağlayan kişilere denir. Bu karşılık sistem sahibi teşekkür

niyetine ödüller de verebilir. Yani kısacası iyi niyetli

bilgisayar uzmanları veya korsanları. Bu kişilere etik hacker de denilebilir

**Gri şapkalı hacker nedir ?**

****

Gri şapkalı hacker’lar dediğim bireyler ise beyaz

şapkalı hackerlar gibi sistem açığını sahiplerine

bildirip rapor etmesi ve açığın kapanmasına yardımcı olur. Beyaz şapkalı hackerlar dan en büyük

fark ise açığı bulduğu sisteme izin girmesdiri. Beyaz şapkalı hackerlar ise izinli bir şekilde sistem üzerinde taramaya

gerçekleştirerek açıkları bulurlar.

**Siyah şapkalı hacker nedir ?**

****

Bu tür hacker grupları ise kötü niyetli hackerlar olup bulduğu bir açığı

kötüye kulananlardır. Örneğin bankaların sistem açığını bularak tüm

bireylerin kredi kartı bilgilerine erişerek tüm verileri

ele geçirmesi. Yada Bir web sitesinin açığını bularak

siteyi erişime kapatması. En kötüsü Herhangi bir

bireyin bilgisayarına sızarak bulduğu açıktan faydalanıp bilgisayar üzerindeki tüm bilgilerini şifreleyerek hepsini devre

dışı bırakması sonucu kullanıcın bu bilgilerine erişme için fidye istemesidir.

**Cracker nedir ?**

Bu tür hackerlar kısacası ücretli olarak yapılmış bir program için

“key”(crack) ler oluşturarak programı ücretsiz bir şekilde kullanmasını

sağlayan bireylerdir.

**Penetrasyon testi nedir?**

Penetrasyon testi , bir sistem üzerinde tarama, analiz, bilgi toplama,

sızma, zafiyet ama vb. attacklarda bulunarak kötü niyetli hackerlardan önce açıkları bulup kapatarak sistemi koruma altına alma işlemidir.

**Exploit nedir?**

Exploit , herhangi bir sistem üzerinde(bilgisayar ,sunucular, vb diğer

sistemler) sızma, sömürme gibi işlemleri gerçekleştirerek var olan

açıklardan faydalanıp sisteme sızma işlemidir.Exploitler günümüzde

sistemlere sısmak için kullanılan en sık yöntemlerdir.

**Phishing nedir ?**

Phishing , Türkçe karşılığı kimlik avı, oltama gibi anlamlarına gelip

kullanıcıları bir takım linkler,e-postalar veya sahte scriptlerle kandırıp

bilgilerini ele geçirme amacı güder.

**Sniffing nedir ?**

Türkçe karşılığı koklama olarak adlandırılan bu teknik terim , herhangi

bir sistemde ortadaki adam saldırısını kullanarak bilgileri ele geçirme

işlemidir. Ortadaki adam saldırısını kısaca anlatmak gerekirse bir sistemde kullanıcı ve modem arasına girerek kullanıcının internet üzerinde girdiği birtakım bilgilerini modeme gönderilmeden önce araya

girip bilgileri alma işlemidir.

Birkaç sniffing çeşitlerinden bahsetmek gerekirse;

Çeşitleri ;

* -IP Sniffing
* -MAC Sniffing
* -MSN Sniffing
* -Network Sniffing

vb. çeşitlerdeki sniffing saldırıları günümüzde çok kullanılan ve tehlikeli bir saldırı çeşididir. Bu saldırı çeşitlerini kali Linux araçları bölümünde uygulamalı olarak kullanacağız.

**Spoffing nedir?**

Spoffing Türkçe karşılığı sızma olup sistemler üzerinde sık kullanılan

yöntemdir.

Örnek vermek gerekirse herhangi bir sistemde bulunan açıktan faydalanarak bu sisteme sızıp bilgileri ele geçirebiliriz.Sızma İşlemlerinde

ise genellikle **exploitler** yardımıyla olur.Örnek olarak sızma işleminde

kullanılan popüler araçlarından biri **Metasploittir**