

Sistem ve Ağ İzleme, Test Etme Araçları

Erkan Esmer

Nisan, 2016

İçindekiler

1	Giriş	2
2	Nessus	3
3	Nmap-Zenmap	6
4	Wireshark	9

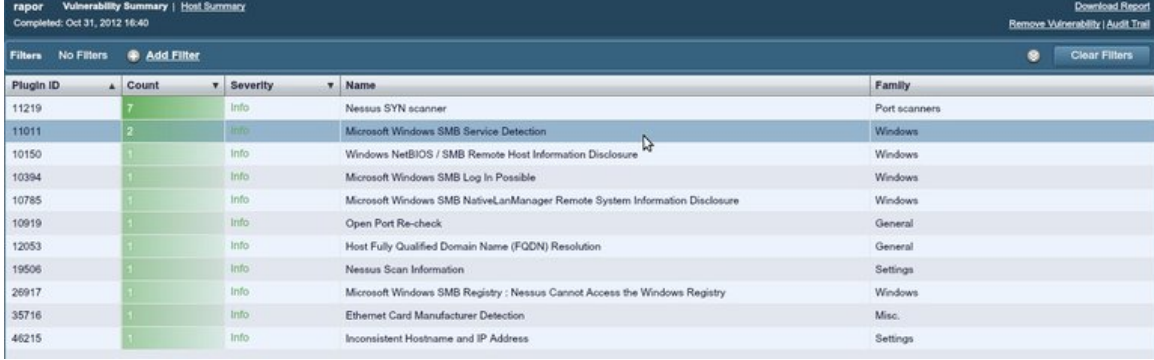
1 Giriş

Yazımızda, başlangıç ve tanıtma amacıyla gerek kendi sistemimizi gerekse uzaktaki sistemleri test etmeye yarayan, sistemlerimizi kontrol etmeye ve devam eden süreçleri ve sonuçlarını izlemeye yardımcı olan birkaç araca değineceğiz.

2 Nessus

Nessus, sistemimiz veya herhangi bir alan adımız için birtakım sorgulamalar yapan, testler uygulayan ve rapor ile sonuç bildiren bir nevi sağlamlık, uygunluk test aracıdır.

Nessus ile sistemimiz veya ağıımızdaki bir bilgisayar üzerinde kontroller yapabiliriz. Bu kontrol sonucu alacağımız rapor ile çalışan servisleri ve kullanılan portları görebilir, risk içeren durumlar için de çözüm önerisi ile birlikte yapmamız gereken müdahaleyi belirleyebiliriz.



Plugin ID	Count	Severity	Name	Family
11219	7	Info	Nessus SYN scanner	Port scanners
11011	2	Info	Microsoft Windows SMB Service Detection	Windows
10150	1	Info	Windows NetBIOS / SMB Remote Host Information Disclosure	Windows
10394	1	Info	Microsoft Windows SMB Log In Possible	Windows
10785	1	Info	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows
10919	1	Info	Open Port Re-check	General
12053	1	Info	Host Fully Qualified Domain Name (FQDN) Resolution	General
19506	1	Info	Nessus Scan Information	Settings
26917	1	Info	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Windows
35716	1	Info	Ethernet Card Manufacturer Detection	Misc.
46215	1	Info	Inconsistent Hostname and IP Address	Settings

Şekil 1:

Aynı zamanda Nessus ile uzaktaki bir sisteme de test uygulayabiliriz. Örneğin bir IP adresi arkasındaki makineye test uygulayıp gereklilikler üzerine kontrol yapabiliriz. Bu kontrol sonucu alacağımız rapor ile, örneğin bu bir web sayfasını barındıran bir sistem olsun, “SSL ile ilgili bir problem var mı?”, “Imap, Pop ve diğer protokoller ile ilgili bilgi veya alarm niteliğinde bir sonuç var mı?” gibi sorulara cevap alabiliriz.

Nessus’u kurup çalıştırmak için neler yapmamız gerekiyor bir bakalım. Önce

<http://www.tenable.com/products/nessus/nessus-download-agreement>

adresinden Nessus uygulamasını indirmemiz gerekiyor. Yükleme sayfasını açtığımızda önce ‘Yükleme Sözleşmesi’ çıkar ve indirmemiz için kabul etmemiz gerekir. Yine bu sayfada “To use Nessus, you need an activation code. Obtain one here.” bağlantısını kullanarak aktivasyon kodu da almamız gerekmektedir. Zira çalıştırmamız için aktivasyon kodunu girerek Nessus’u kayıt ettirmemiz şart. Sonrasında gelen sayfada ilgili .deb paketini indirip

```
dpkg -i Nessus-5.0.1 .... deb
```

komutu ile .deb paketimizi sistemimize kurmalıyız.

Kurulumu yapıp aktivasyon kodumuzu da aldıktan sonra tarayıcımızdan

<https://localhost:8834/register/>

adresini açarak Nessus’u aktive ediyoruz. Ardından yine tarayıcımızdan

<https://localhost:8834>

adresini çağırdığımızda Nessus açılacak ve bizden giriş yapmamızı bekleyecek. Root kullanıcı adını kullanarak giriş yapıyoruz. Gelen ekranda menüyü görmekteyiz. Buradan Scans düğmesini kullanarak tarama yapabilir, kayıt edip Reports düğmesi altında saklayabiliriz.

Şimdi örnek olarak alınmış iki raporu temel anlamda inceleyelim.

İlk örneğimizde smb isimli servis için yapılan kontrolde 139 ve 445 numaralı portlar kullanılmaktaymış. Bu portların kullanılması, dolayısıyla açık olması ile ilgili açıklamayı “Description” alanında görmekteyiz. Severity alanı

rapor Vulnerability Summary Host Summary				Download Report	
Completed: Oct 31, 2012 16:40				Remove Vulnerability / Audit Trail	
Filters No Filters Add Filter				Clear Filters	
Plugin ID	Count	Host	Port	Plugin ID: 11011 Port / Service: smb (139/tcp) Severity: Info	
11219	7	192.168.0.70	139 / tcp	Plugin Name: Microsoft Windows SMB Service Detection Synopsis: A file / print sharing service is listening on the remote host. Description: The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network. Solution: n/a Risk Factor: None Plugin Output: An SMB server is running on this port. Plugin Publication Date: 2002/06/05 Plugin Last Modification Date: 2012/01/31	
11011	2	192.168.0.70	445 / tcp		
10150	1				
10394	1				
10785	1				
10919	1				
12053	1				
19506	1				
26917	1				
35716	1				
46215	1				

Şekil 2:

yanında Info-Bilgi mesajı olduğunu, herhangi bir risk taşımadığını ve çözüme gerek olmadığını görüyoruz. İncelediğimiz bu sonuca göre bilgi bazında bir dönüş aldık ve riskli bir durumla karşılaşmadık.

İkinci örneğimize bakalım. Aşağıda bir alan adının taraması sonucu oluşan raporu görmekteyiz.

rapor2 Vulnerability Summary Host Summary					Re
Completed: Oct 31, 2012 18:17					
Filters No Filters Add Filter					
Plugin ID	Count	Severity	Name	Family	
42873	4	Medium	SSL Medium Strength Cipher Suites Supported	General	
45411	4	Medium	SSL Certificate with Wrong Hostname	General	
15901	3	Medium	SSL Certificate Expiry	General	
51192	3	Medium	SSL Certificate Cannot Be Trusted	General	
53491	3	Medium	SSL / TLS Renegotiation DoS	General	
57582	3	Medium	SSL Self-Signed Certificate	General	
57792	3	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	
20007	2	Medium	SSL Version 2 (v2) Protocol Detection	Service detection	
46803	2	Medium	PHP expose_php Information Disclosure	Web Servers	
62565	2	Medium	TLS CRIME Vulnerability	General	
22254	1	Medium	Web Server Expect Header XSS	CGI abuses : XSS	
34324	1	Low	FTP Supports Clear Text Authentication	FTP	
42880	1	Low	SSL / TLS Renegotiation Handshakes MITM Plaintext Data Injection	General	
22964	8	Info	Service Detection	Service detection	

Şekil 3:

İncelemek istediğimiz satırı seçtiğimizde detayları ve çözüm önerisini görebiliyoruz.

Satırın detayında gördüğümüz gibi Severity =Medium olan, yani orta seviye bir güvenlik açığı bulunmakta. Bununla ilgili açıklamayı Description kısmında görüyoruz. Çözüm önerisi olarak da Apache servisini 2.2 veya daha yukarisına güncellememiz gerektiği yazmakta.

İşte temel bir bakışla Nessus, kontrol ettiğimiz sistemimizle ilgili güvenlik testleri uygulamamızı ve bilgiler edinmemizi sağlayan başarılı bir araçtır. Kullanıcılar için vazgeçilmezdir.

rapo2 Vulnerability Summary | Host Summary

Completed: Oct 31, 2012 18:17

Download Report
Remove Vulnerability / Audit Trail

Filters No Filters Add Filter Clear Filters

Plugin ID	Count	Host	Port
42873	4	www. [REDACTED]	80 / tcp
45411	4	www. [REDACTED]	443 / tcp
15901	3	www. [REDACTED]	8443 / tcp
51192	3		
53491	3		
57582	3		
57792	3		
20007	2		
46803	2		
62565	2		
22254	1		
34324	1		
42880	1		
20064	0		

Plugin ID: 57792 **Port / Service:** www (80/tcp) **Severity:** Medium

Plugin Name: Apache HTTP Server httpOnly Cookie Information Disclosure

Synopsis: The web server running on the remote host has an information disclosure vulnerability.

Description:
The version of Apache HTTP Server running on the remote host has an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

Solution:
Upgrade to Apache version 2.2.22 or later.

See Also:
http://l4-the-wildcat.de/apache_a26sa%446c.php
http://mpd.apache.org/security/vulnerabilities_22.html
<http://svn.apache.org/viewvc?view=revision&revision=1235454>

Risk Factor: Medium

STIG Severity: i

3 Nmap-Zenmap

Nmap ile belirlediğiniz bir bilgisayarın işletim sistemini, açık portlarını ve portları kullanan servislerinin tespitini yapabilirsiniz.

```
1 Nmap -v -A www.google.com //komutuyla google.com adresindeki sistemi ,
2 nmap -v -sP 192.168.0.9/16 //komutuyla ağdaki bilgisayarı gözden geçirebilirsiniz .
```

Örneğin resimde gördüğünüz gibi yaptığımız tarama sonucunda

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
80/tcp    open  http         Apache httpd 2.2.3 ((CentOS))
|_html-title:
110/tcp   open  pop3         Courier pop3d
|_pop3-capabilities: USER IMPLEMENTATION(Courier Mail Server) UIDL APOP TOP OK(K
Here s what I can do) STLS PIPELINING LOGIN-DELAY(10)
113/tcp   closed auth
143/tcp   open  imap         Courier Imapd (released 2004)
|_imap-capabilities: THREAD=ORDEREDSUBJECT QUOTA STARTTLS THREAD=REFERENCES UIDP
LUS ACL2=UNION SORT ACL IMAP4rev1 IDLE NAMESPACE CHILDREN
443/tcp   open  ssl/http     Apache httpd 2.2.3 ((CentOS))
|_ssl2: server still supports SSLv2
|_html-title: Site doesn't have a title (text/html).
465/tcp   open  ssl/smtp     qmail smtpd
|_ssl2: server still supports SSLv2
|_smtp-commands: EHLO AUTH=LOGIN CRAM-MD5 PLAIN,
AUTH LOGIN CRAM-MD5 PLAIN, PIPELINING, 8BITMIME
|_HELP qmail home page: http://pobox.com/~djb/qmail.html
587/tcp   closed submission
```

Şekil 5:

21 portu ProFtpD servisi tarafından kullanılıyor ve açık.
80 portu açık ve Httpd servisi tarafından kullanılıyor.
110 portu açık ve pop3d servisi kullanıyor.
113 kapalı ve 143 açık Imapd kullanıyor.
465 portu açık smtpd kullanıyor.

Man nmap komutu ile nmap 'in yardım sayfasına ulaşabilir. Kullanımı ile ilgili örneklere ulaşabilirsiniz.

ZenMap ise nmap uygulamasının grafik arayüzlü hâlidir. ZenMap uygulamasını

```
1 sudo apt-get install zenmap
```

komutu ile kurar, uçbirime “zenmap” yazarak çalıştırırız. Zenmap uygulamasında da nmap gibi sonuçlar alırız. Zenmap ekranına bakacak olursak

Nmap Output sekmesinde yaptığımız taramanın sonuçlarını görürüz.

Ports/Hosts sekmesi, tarama yaptığımız sistemde aktif olarak kullanılan portları ve kullandığı servisleri versiyonları ile birlikte listeler.

Topology sekmesinde, yaptığımız taramalar sonucu oluşan tarama haritamızı görüntüleyebiliriz. Bu ayrıca sistemimizden yapılan çıkış noktalarını da göstereceği için aydınlatıcı bir ağ haritamız olarak da nitelendirilebilir. Aynı zamanda bu çıkışı resim olarak da kayıt edebiliriz.

Host Details sekmesinde ise tarama yaptığımız makinenin açık port sayısı, kapalı port sayısı, işletim sistemi gibi bilgilerini görüntüleriz.

	Hostname	Port	Protocol	State	Version
✓	[REDACTED] (192.168.0.70)	902	tcp	open	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
✓	[REDACTED] (192.168.0.70)	912	tcp	open	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)



Şekil 6:

Nmap Output Ports / Hosts Topology Host Details Scans

▼ [REDACTED] (192.168.0.70)

► **Comments**

▼ **Host Status**

State:	up	
Open ports:	7	
Filtered ports:	0	
Closed ports:	993	
Scanned ports:	1000	
Up time:	Not available	
Last boot:	Not available	

▼ **Addresses**

IPv4: 192.168.0.70

IPv6: Not available

MAC: 90:E6:BA:D9:91:E0

▼ **Hostnames**

Name - Type: [REDACTED] PTR

▼ **Operating System**

Name: Microsoft Windows XP SP2 or SP3, or Windows Server 2003

Accuracy:

100%

► **Ports used**

► **OS Class**

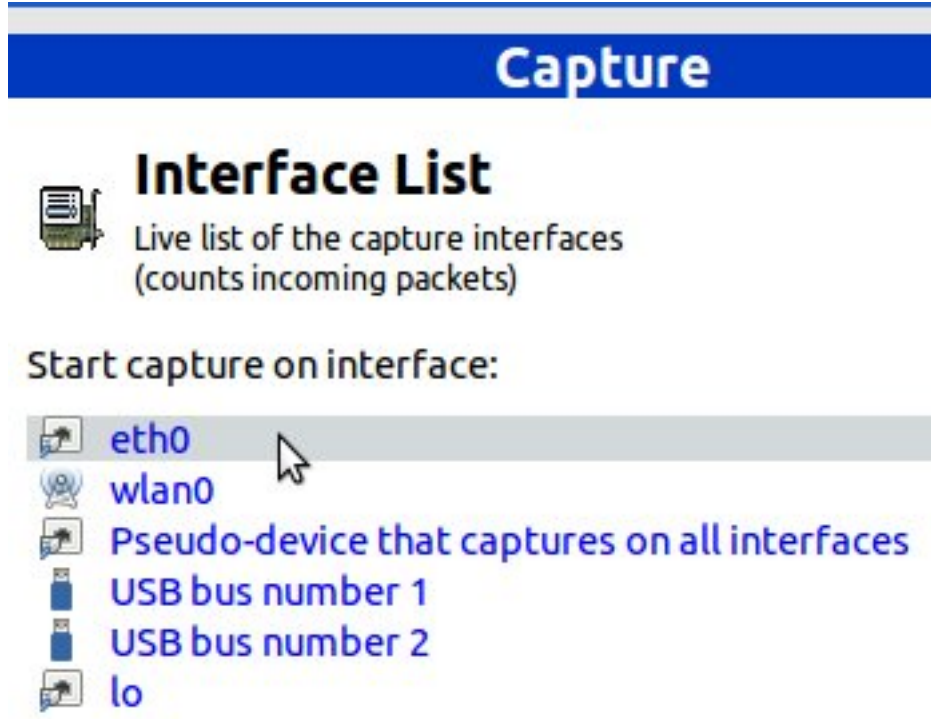
Şekil 7:

Scans sekmesinde ise yaptığımız taramaları liste hâlinde ve komutu ile birlikte görürüz. Tekrar belirtmeye gerek var mı bilemiyorum ama nmap’da olduğu gibi Zenmap’te de ağ dışı sistemleri tarayabiliriz. Mesela bu bir alanadı olabilir.

4 Wireshark

Wireshark, bir ağ protokol analiz aracıdır. Wireshark, yakaladığı paketleri protokol bilgileriyle birlikte görüntüler. Wireshark ile ağındaki veya kendi sisteminizdeki trafiği inceleyebilir, analizler yapabilirsiniz. Örneğin kendi sisteminizden yaptığınız bir işlem sonucu (bir web sayfası açma gibi) nasıl bir trafik doğduğunu veya bir ağ içerisinde makinelerin işlemleri sonucu doğan trafiği izleyebilirsiniz.

Wireshark, açılınca bizden izleyeceği arabirimi seçmemizi ister. “Interface List” başlığı altından izleyeceğimiz arabirimi seçeriz. Genelde 1 veya 2 adet ethernet kartı olduğunu varsayarsak eth0 seçimini yaparız.



Şekil 8:

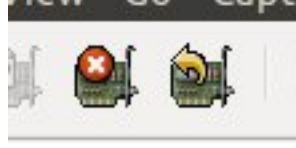
İzleme başladığında resimde gördüğümüz gibi trafikteki paketin kaynağını, hedefini, kullandığı protokolü ve bilgisini görebiliriz.

33	0.532842	192.168.0.166	192.168.0.255	NBNS	92 Name query NB SENGINE-4573551<20>
34	0.534304	192.168.0.166	192.168.0.255	NBNS	92 Name query NB HW23761-58<20>
35	0.578178	192.168.0.139	255.255.255.255	UDP	170 Source port: 50139 Destination port: mvs-capacity
36	0.604510	91.240.109.41	192.168.0.20	TCP	435 [TCP segment of a reassembled PDU]
37	0.604527	192.168.0.20	91.240.109.41	TCP	66 56902 > http [ACK] Seq=1 Ack=370 Win=123 Len=0 TSval=3652713 TSecr=204827774
38	0.605313	91.240.109.41	192.168.0.20	HTTP	66 HTTP/1.0 200 OK (text/html)
39	0.605546	192.168.0.20	91.240.109.41	TCP	66 56902 > http [ACK] Seq=1 Ack=371 Win=123 Len=0 TSval=3652714 TSecr=204827774
40	0.605835	91.240.109.41	192.168.0.20	TCP	66 http > 56902 [ACK] Seq=371 Ack=2 Win=136 Len=0 TSval=204827774 TSecr=3652714
41	0.607115	192.168.0.20	91.240.109.41	TCP	74 56903 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=3652714 TSecr=
42	0.607394	91.240.109.41	192.168.0.20	TCP	74 http > 56903 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=2048
43	0.607412	192.168.0.20	91.240.109.41	TCP	66 56903 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3652714 TSecr=204827775

Frame 1: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)
Ethernet II, Src: Dell_42:ac:2c (24:b6:fd:42:ac:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.76 (192.168.0.76), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 56029 (56029), Dst Port: mvs-capacity (10007)
Data (128 bytes)

Şekil 9:

Buradaki düğmeleri kullanarak izlemeyi durdurabilir tekrar başlatabiliriz.



Şekil 10:

Wireshark ekranında yakalanan paketleri gördüğümüz bölümün altındaki bölümde, seçtiğimiz satırın teknik detaylarını görebiliriz. Şimdi satırla beraber detayının da sonuçlarına bakalım. Örneğin seçtiğimiz satırda 0.64 IP numaralı makinenin tüm ağa yayın yaparak bir isim sorgulaması yaptığını görüyoruz. Bu satırın detayına, satırı seçerek alttaki bölümden ulaşabiliriz. Ya da satıra çift tıkladığımızda detay ekranı açılır. Buradan kaynak ve hedef portu, datanın uzunluğu, kullanılan protokolün versiyonu gibi bilgilere ulaşabiliriz.

68	2.553500	192.168.0.64	192.168.0.255	NBNS	92 Name query NB BASKI6<00>
----	----------	--------------	---------------	------	-----------------------------

Şekil 11:

Bu kayıt, ağ ortamında sıradan bir aksiyon olarak nitelendirilebilir.

Bir de aşağıdaki çıktımıza bakacak olursak; hedef port 10019 olan, kaynağı ise her seferinde farklı olan ve farklı IP no'lu bilgisayarlardan gelen aksiyonlar var. Adet olarak da dikkat çekici diyebiliriz.

131	5.431887	192.168.0.107	255.255.255.255	UDP	170 Source port: 58254 Destination port: 10019
132	5.439610	192.168.0.37	255.255.255.255	UDP	170 Source port: 57105 Destination port: mvs-capacity
133	5.453701	192.168.0.87	255.255.255.255	UDP	170 Source port: 53129 Destination port: 10019
134	5.456364	192.168.0.37	255.255.255.255	UDP	170 Source port: 57106 Destination port: 10019
135	5.627779	192.168.0.18	255.255.255.255	UDP	170 Source port: 59952 Destination port: mvs-capacity
136	5.643260	192.168.0.18	255.255.255.255	UDP	170 Source port: 59953 Destination port: 10019
137	5.672097	192.168.0.76	255.255.255.255	UDP	170 Source port: 61728 Destination port: mvs-capacity
138	5.734542	192.168.0.76	255.255.255.255	UDP	170 Source port: 61729 Destination port: 10019
139	5.812834	192.168.0.107	255.255.255.255	UDP	170 Source port: 58255 Destination port: mvs-capacity
140	5.872717	192.168.0.39	255.255.255.255	UDP	170 Source port: 51397 Destination port: mvs-capacity
141	5.883144	192.168.0.139	255.255.255.255	UDP	170 Source port: 62550 Destination port: mvs-capacity
142	5.912734	192.168.0.39	255.255.255.255	UDP	170 Source port: 51398 Destination port: 10019

Şekil 12:

Bu aldığımız çıktı, çalışma esnasında gerçek ortamdan alınmıştır. Yazımızın konusu detaylı bir analizi içermediği için satırlarla ilgili yorumlardan ziyade işlevselliği üzerine dikkat çekmeyi şimdilik yeterli görüyoruz. Yakaladığımız satırlarda 10019 portuyla ilgili çok kayıt var ve her satırda kaynak portlarının farklı olması kesin doğru olmamakla birlikte şüphe uyandırıcı ve ilgilenilmesi gereken bir durumu işaret ediyor olabilir.

İşte Wireshark, bu tespiti yapmamızı sağlamakta ve bize yardımcı olmaktadır. Bu veya buna benzer durumlarda gerekli araştırmayı yaparak önlem almamız, hem daha kararlı bir sistem üzerinde çalışmamızı sağlayacak hem de kontrolümüzü artıracak ve daha bilinçli bir vaziyet alacağız diye acizane düşünmekteyiz.

Wireshark için şimdilik bu kadar. Umarız analiz boyutunda daha derin çalışmalarımız ve paylaşımlarımız olur. Ayrıca <http://ask.wireshark.org> adresinden de soru ve cevapları takip edebilirsiniz.

Yukarıda değindiğimiz iki uygulama dışında tabii ki bu işler için daha çok uygulama ve araç bulunmakta. Bizler bu yazıyla aslında bir başlangıç yapmak istedik. Bu tür ihtiyaçlara yönelik araçlar, suistimal edilme ihtimalini de yüksek seviyede barındırdığından sorumluluk bilinciyle hareket etmeye çalıştık ve bu araçları barındıran bu yazı ortaya çıktı. Daha derinlemesine incelemeleri paylaşabilme ve hepimiz adına yararlı olması umuduyla...