

Ali
Gholami

Koroush
Rajab Zadeh

Metasploit

Soc. Eng.



Reverse Eng.

Security

Mohamad
Khajavi

The background features a dark, textured surface resembling a film strip, with a vertical line down the center. Overlaid on this are three concentric circles: a small solid black circle in the center, a medium gray circle, and a large dark gray circle.

[Introduction]



1. DEVELOPED BY HD MOORE

2. OPEN SOURCE

3. WRITTEN IN PERL IN 2003

4. REWRITTEN IN RUBY IN 2007

5. PURCHASED BY RAPID7 IN 2009

اسلايد ٢

Development

Resources

1. EXPLOIT CODES

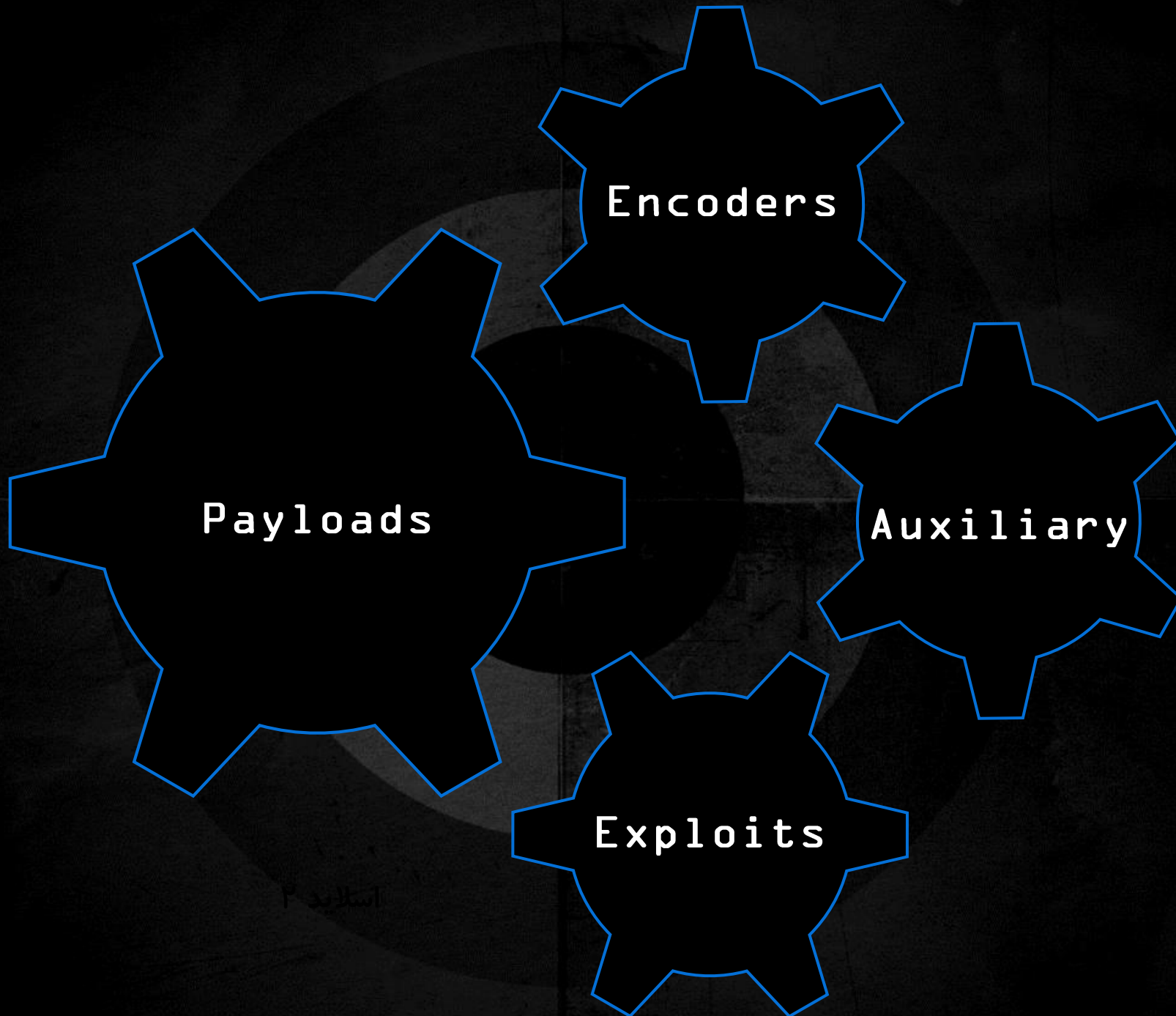
2. OPCODE DATABASES

3. SHELL-CODE DATABASES

Development

Resources

Modules



Development

Resources

Modules

Usage

1. PENETRATION TESTING

2. IDS SIGNATURE DEVELOPMENT

3. EXPLOIT RESEARCH

اسلايد ۲

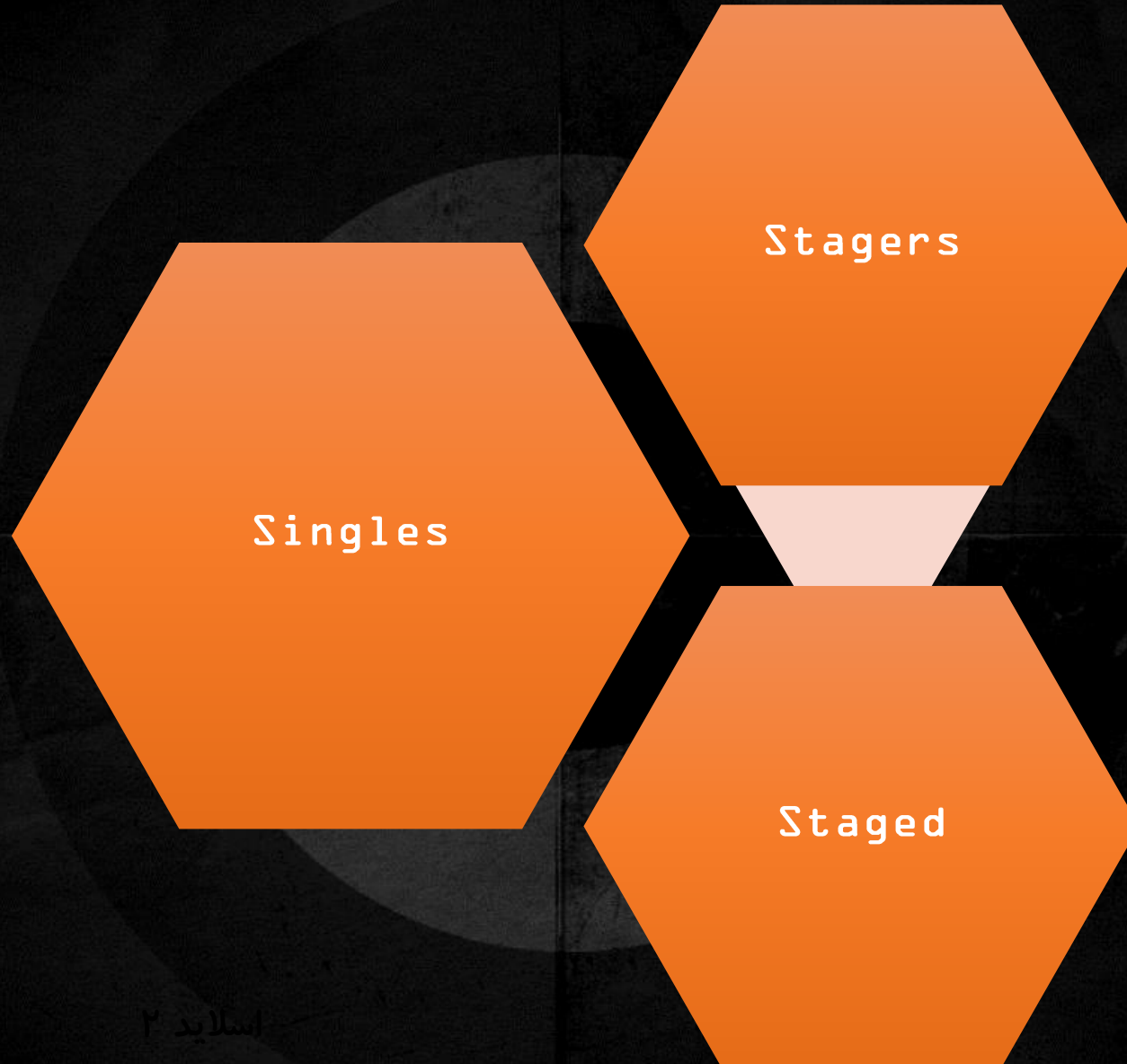
Development

Resources

Modules

Usage

Payloads



335 PAYLOADS

اسلايد ۲

Development

Resources

Modules

Usage

Payloads



MISSILE(EXPLOIT)

Reflective
DLL
Injection

STAGE

STAGER

iveX

WARHEAD(PAYLOAD)

NoNX

0rd

Development

Resources

Modules

Usage

Payloads

Procedure

1. CHOOSE AND CONFIGURE AN
EXPLOIT(OS ORIENTED)
2. EXPLOIT RESEARCH
3. CHOOSE AND CONFIGURE A PAYLOAD
(EXPLOIT ORIENTED)
4. CHOOSE THE ENCODING TECHNIQUE
5. DEPLOY...



Application

1. LET'S CHECK THIS DIRECTORY OUT

- `usr/share/metasploit-framework`

2. EXPLORE THE MODULES

- `cd modules`

3. FIND ALL MODULES RELATED TO ANDROID

- `FIND -l | grep android`

4. EXPLORE THE PAYLOADS

- `cd modules/payloads`

- AN INSTANCE OF THE METASPLOIT
- LIST THE PAYLOADS
- SET COMMAND FRAMEWORK
 - `msfvenom -l payloads`
 - `set payload windows/x64/shell/reverse_tcp_uuid`
- COMBINE THE ENCODERS AND PAYLOAD AND
- USE COMMAND
 - `msfvenom -l encoders`
 - `use exploit/multi/handler`
- TERMINAL COMMAND:
 - `cd modules/payloads`

What's
Inside

MSFVENOM

MSFCONSOLE

```
root@packetresearch:/opt/metasploit# msfconsole  
[*] Starting the Metasploit Framework console.../
```



Payload caught by AV? Fly under the radar with Dynamic Payloads in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>

```
      =[ metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]  
+ -- --=[ 1398 exploits - 877 auxiliary - 237 post           ]  
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf >

What's
Inside

MSFVENOM

MSFCONSOLE

Meterpreter
shell

- METERPRETER IS AN ADVANCED, DYNAMICALLY *EXTENSIBLE PAYLOAD* THAT USES *IN-MEMORY DLL INJECTION* STAGERS AND IS *EXTENDED* OVER THE NETWORK AT RUNTIME.
- IT COMMUNICATES OVER THE STAGER SOCKET AND PROVIDES A *COMPREHENSIVE CLIENT-SIDE RUBY API*.
- IT FEATURES COMMAND HISTORY, TAB COMPLETION, CHANNELS, AND MORE.

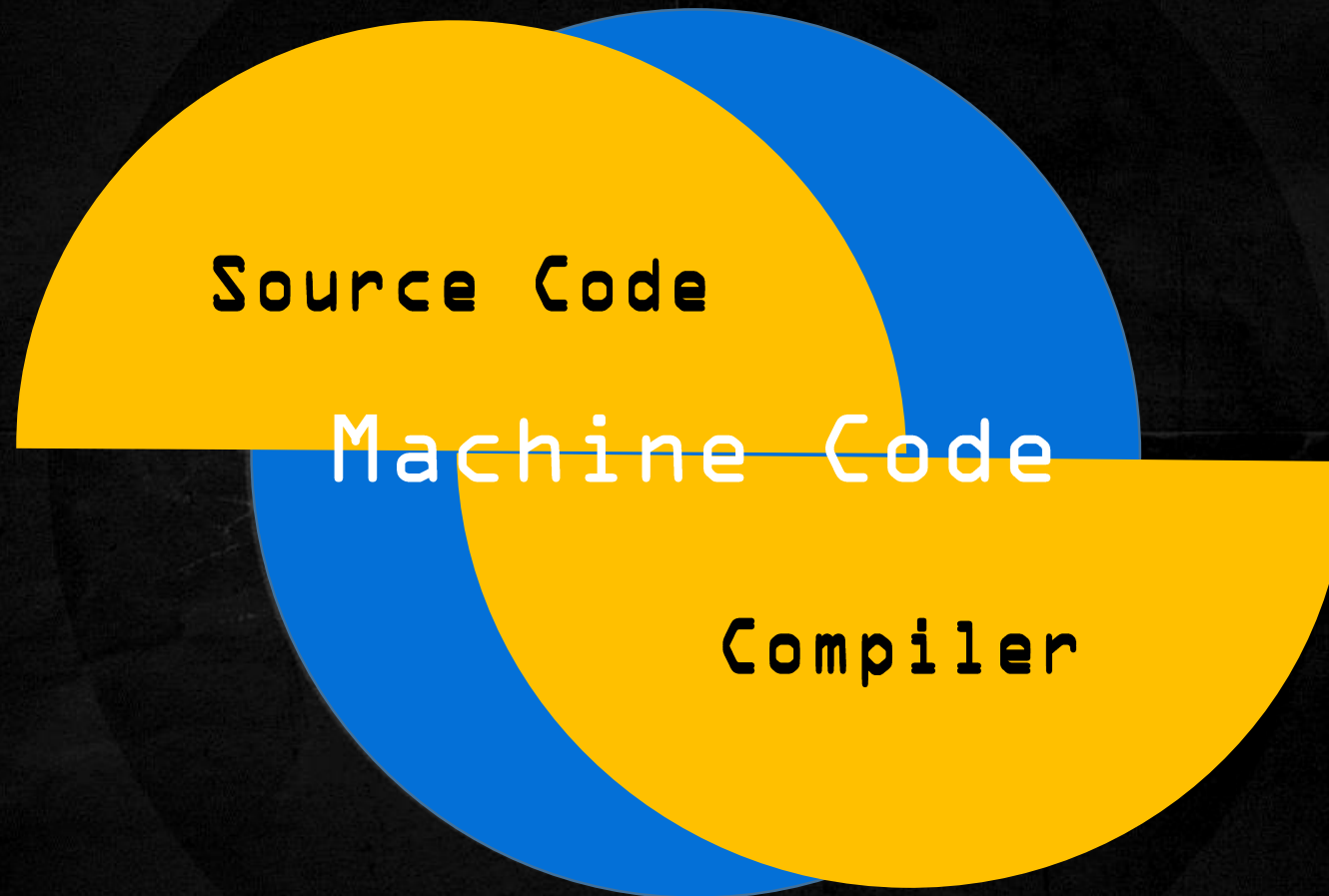
What's
Inside

MSFVENOM

MSFCONSOLE

Meterpreter
shell

Apktool



What's
Inside

MSFVENOM

MSFCONSOLE

Meterpreter
shell

Apktool

- DISASSEMBLING RESOURCES TO NEARLY ORIGINAL FORM (including `resources.arsc`, `classes.dex`, `.png` and XMLs)
- REBUILDING DECODED RESOURCES BACK TO BINARY APK/JAR
- ORGANIZING AND HANDLING APKs THAT DEPEND ON FRAMEWORK RESOURCES

What's
Inside

MSFVENOM


MSFCONSOLE

Meterpreter
shell

Apktool

Smali
Injection

- DECOMPILING APK FILES
 - `Apktool d file_name.apk`
- COMPILING SMALI DIRECTORY
 - `Apktool b directory_name`



Shell-Code

SHELL-CODE LITERALLY REFERS TO
WRITTEN CODE THAT STARTS A
COMMAND SHELL

What's
Shell-code?

Types

Local

Remote

Download &
Execute

Staged

What's
Shell-code?

Types

Shell-code
Encodings

- MOST PROCESSES FILTER OR RESTRICT THE DATA THAT CAN BE INJECTED.
- SHELL-CODE MUST BE SMALL, NULL-FREE AND ALPHANUMERIC.
- TO AVOID THE INTRUSION DETECTION OF THE SHELL-CODE WHICH IS BEING SENT OVER THE NETWORK, ENCRYPTION AND SELF-DECRYPTION OR POLYMORPHISM IS USED.

What's
Shell-code?

Types

Shell-code
Encodings

Buffer
Overflow

WHERE A PROGRAM, WHILE WRITING DATA
TO A BUFFER, **OVERRUNS** THE BUFFER'S
BOUNDARY AND OVERWRITES ADJACENT
MEMORY LOCATIONS.

اسلايد ۲

What's
Shell-code?

Types

Shell-code
Encodings

Buffer
Overflow

Android-
Attack
Scenario

#22



Target: Android