
# Engenharia Social Técnica em Testes de Invasão com o SET

**Rafael Soares Ferreira**
**Sócio Diretor Técnico**
**rafael@clavis.com.br**

# Apresentação


- Grupo Clavis
- Sócio Diretor Técnico
- Detecção e resposta a incidentes de segurança
- Testes de invasão em redes, sistemas e aplicações

# Contatos


rafaelsoaresferreira@gmail.com

rafaelsoaresferreira

@rafaelsferreira

www.facebook.com/rafaelsoaresferreira

# Agenda

- Engenharia Social em Testes de Invasão
- SET – Social Engineering Toolkit
- Exemplos
- Conclusões

# Engenharia Social em Testes de Invasão

CLAVIS segurança da informação

- Quando dentro do escopo, avalia a cultura de segurança dos usuários da infraestrutura;

- Os colaboradores devem ser continuamente treinados para lidar com ataques deste tipo;

# SET – Social Engineering Toolkit

CLAVIS segurança da informação

- Auxílio para ataques de Engenharia Social
- Open-Source
- Desenvolvido em Python
- Integrado com o Metasploit Framework

# Spear-Phishing Attacks

CLAVIS segurança da informação

- Ou “Pesca de Arpão”, consiste no envio de emails maliciosos modelados para alvos específicos
- Geralmente, integrado com *payloads* do Metasploit Framework

# Spear-Phishing Attacks

CLAVIS segurança da informação

```
set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OF
F
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

# Website Attacks

Possui diversas modalidades de ataques que utilizam página web

- **Java Applet** – cria de applets java maliciosos;
- **Metasploit Browser** – utiliza exploits client-sides do Metasploit para navegadores;

# Website Attacks

CLAVIS
segurança da informação

- **Credential Harvester** – clona uma página com campos de usuário e senha para coletar credenciais;
- **TabNabbing** – espera o usuário mudar de aba e carrega outro site na aba anterior;
- **Man Left in the Middle** – utiliza HTTP Referer para interceptar campos e coletar dados dele;

# Website Attacks

- **Web-Jacking** – faz um link parecer legítimo, mas, quando clicado, abre uma janela com o link malicioso;

- **Multi-Attack** – combina alguns ataques citados anteriormente, lançando-os simultaneamente;

# Website Attacks

CLAVIS segurança da informação

```
 and the Back|Track team. This method utilizes iframe replacements to
 make the highlighted URL link to appear legitimate however when clicked
 a window pops up then is replaced with the malicious link. You can edit
 the link replacement settings in the set_config if its too slow/fast.

 The Multi-Attack method will add a combination of attacks through the web attac
k
 menu. For example you can utilize the Java Applet, Metasploit Browser,
 Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
 all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>
```

KALI LINUX

# Infectious Media Generator

- Cria um arquivo de *autorun* para USB/CD/DVD;
- Quando o dispositivo é detectado no sistema da vítima, o arquivo malicioso é executado;

# Infectious Media Generator

CLAVIS segurança da informação

```
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 3

 The Infectious USB/CD/DVD module will create an autorun.inf file and a
 Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
 run if autorun is enabled.

 Pick the attack vector you wish to use: fileformat bugs or a straight executabl
e.

   1) File-Format Exploits
   2) Standard Metasploit Executable

  99) Return to Main Menu

set:infectious>
```

KALI LINUX

# Arduino-Based Attack

CLAVIS segurança da informação

- Utiliza um sistema baseado em Arduino para exploração;
- Por ser reconhecido como Teclado USB, eles dispositivos conseguem ultrapassar proteções de auto-execução;

# Arduino-Based Attack

CLAVIS segurança da informação

```
X10 based communication devices in order for this to work.

Select a payload to create the pde file to import into Arduino:

  1) Powershell HTTP GET MSF Payload
  2) WSCRIPT HTTP GET MSF Payload
  3) Powershell based Reverse Shell Payload
  4) Internet Explorer/FireFox Beef Jack Payload
  5) Go to malicious java site and accept applet Payload
  6) Gnome wget Download Payload
  7) Binary 2 Teensy Attack (Deploy MSF payloads)
  8) SDCard 2 Teensy Attack (Deploy Any EXE)
  9) SDCard 2 Teensy Attack (Deploy on OSX)
 10) X10 Arduino Sniffer PDE and Libraries
 11) X10 Arduino Jammer PDE and Libraries
 12) Powershell Direct ShellCode Teensy Attack
 13) Peensy Multi Attack Dip Switch + SDCard Attack

 99) Return to Main Menu

set:arduino>
```

KALI LINUX

# SMS Spoofing Attack

- Permite a criação de mensagens SMS com origem falsa;
- Utilizado para disseminar links maliciosos;

# SMS Spoofing Attack

CLAVIS segurança da informação

```
 99) Return back to the main menu.

set> 7

The SMS module allows you to specially craft SMS messages and send them
to a person. You can spoof the SMS source.

This module was created by the team at TB-Security.com.

You can use a predefined template, create your own template or specify
an arbitrary message. The main method for this would be to get a user to
click or coax them on a link in their browser and steal credentials or
perform other attack vectors.

  1) Perform a SMS Spoofing Attack
  2) Create a Social-Engineering Template

 99) Return to Main Menu

set:sms>
```

KALI LINUX

# Wireless Access Point Attack

CLAVIS segurança da informação

- Cria pontos de acesso utilizando uma interface de rede sem fio e redireciona todas as requisições DNS para o atacante;
- O ataque serve de ponte para possibilitar o lançamento de outros ataques;

# Wireless Access Point Attack

CLAVIS segurança da informação

```
set> 8

 The Wireless Attack module will create an access point leveraging your
 wireless card and redirect all DNS queries to you. The concept is fairly
 simple, SET will create a wireless access point, dhcp server, and spoof
 DNS to redirect traffic to the attacker machine. It will then exit out
 of that menu with everything running as a child process.

 You can then launch any SET attack vector you want, for example the Java
 Applet attack and when a victim joins your access point and tries going to
 a website, will be redirected to your attacker machine.

 This attack vector requires AirBase-NG, AirMon-NG, DNSSpoof, and dhcpd3.


   1) Start the SET Wireless Attack Vector Access Point
   2) Stop the SET Wireless Attack Vector Access Point

  99) Return to Main Menu

set:wireless>
```

KALI LINUX

# QR Code Generator Attack

- Cria um QR Code que aponta para um site malicioso;
- É possível enviar por email, bluetooth e etc.

# QR Code Generator attack

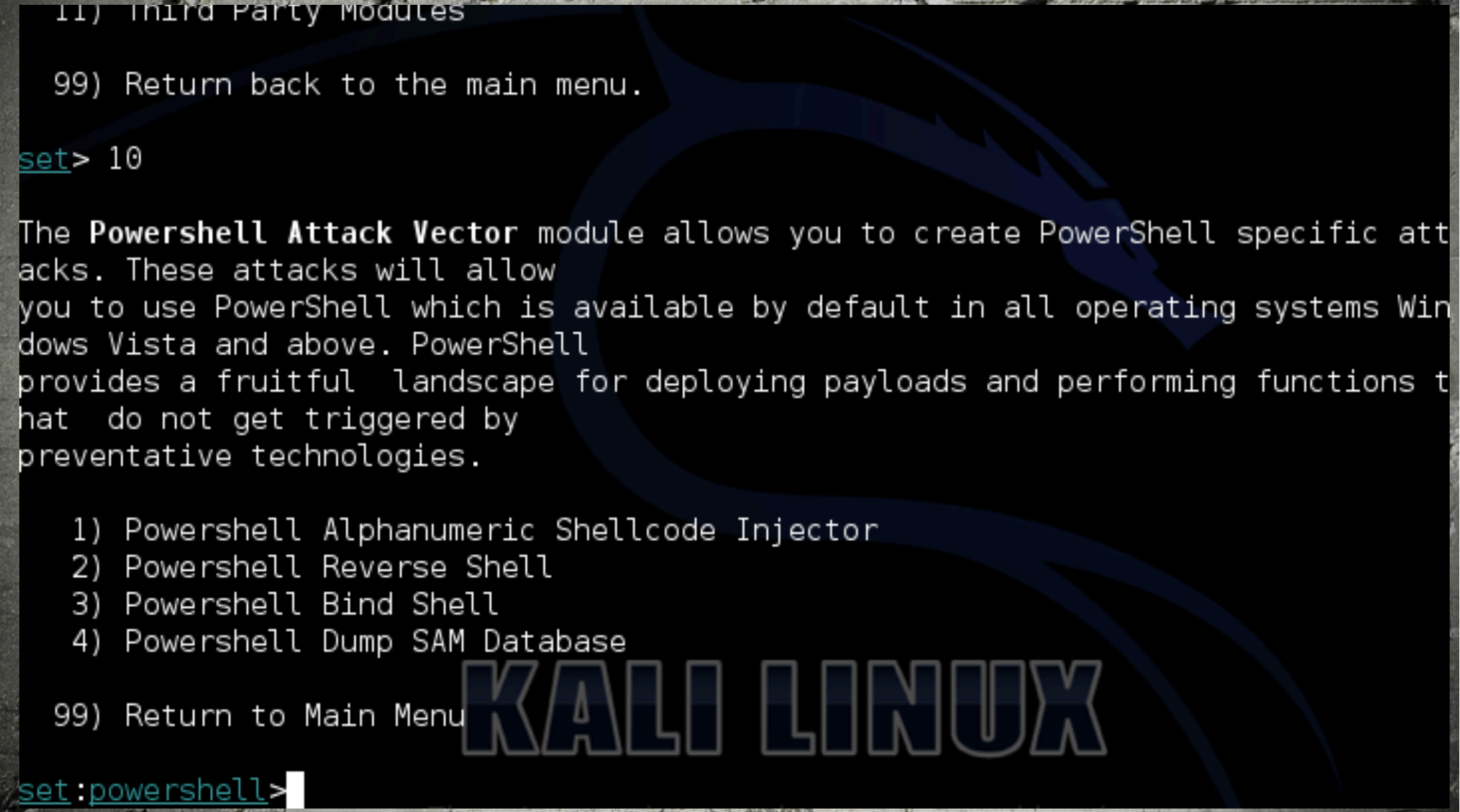
CLAVIS segurança da informação

```
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 9

The QRCode Attack Vector will create a QRCode for you with whatever URL you want.

When you have the QRCode Generated, select an additional attack vector within SET
 and
deploy the QRCode to your victim. For example, generate a QRCode of the SET Java
Applet
and send the QRCode via a mailer.

Enter the URL you want the QRCode to go to:
```

# PowerShell Attack

- Permite a criação de ataques específicos a PowerShell;
- PowerShell está disponível a partir do Windows Vista;
- Powershell permite acesso administrativo ao sistema'

# PowerShell Attack



# Conclusão

CLAVIS segurança da informação

- É preciso implementar controles contra tais técnicas;

- Tais controles são complementados com treinamento e conscientização de segurança;

- Cultura de Segurança é importante!

# Dúvidas?

Perguntas?

Críticas?

Sugestões?

CLAVIS
segurança da informação

# Muito Obrigado!

rafael@clavis.com.br

@rafaelsferreira


**Rafael Soares Ferreira**
**Sócio Diretor Técnico**