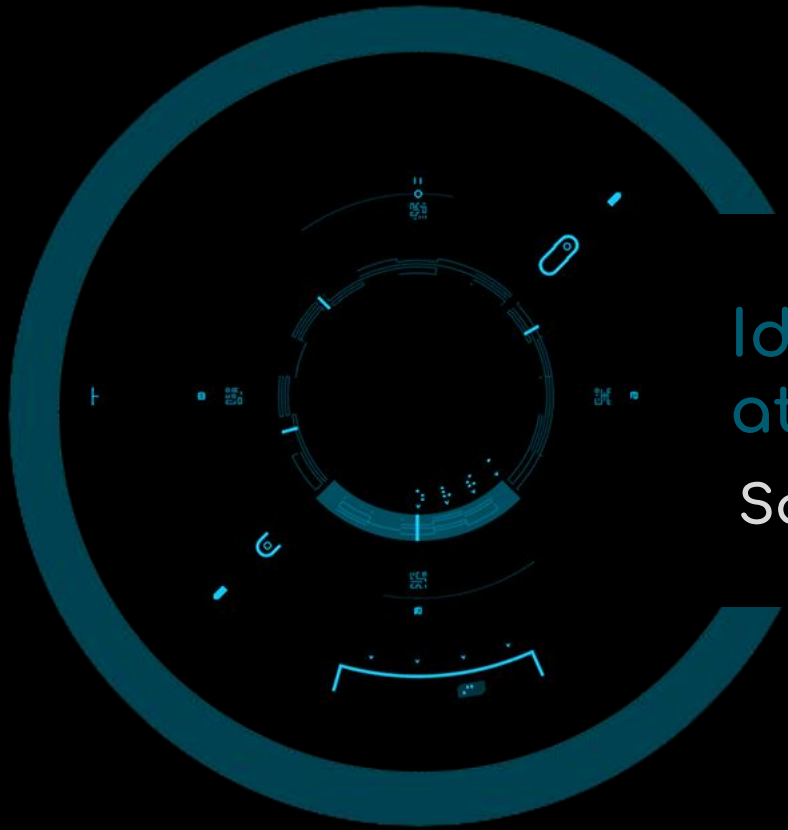


Identificando vulnerabilidades através do Teste de Invasão

Samantha Nunes

Sobre o que vamos falar?

- Segurança da Informação
- Teste de Invasão
- Ferramentas que podem ser utilizadas
- Próximos passos com base nos resultados do teste

O que é segurança da informação?

Visa preservar a integridade, confidencialidade e a disponibilidade da informação

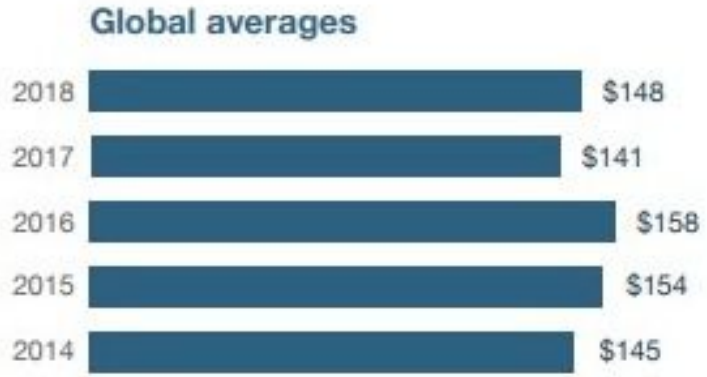
Por que Segurança da Informação é importante?

Quanto tempo em média sua empresa leva para identificar uma violação?

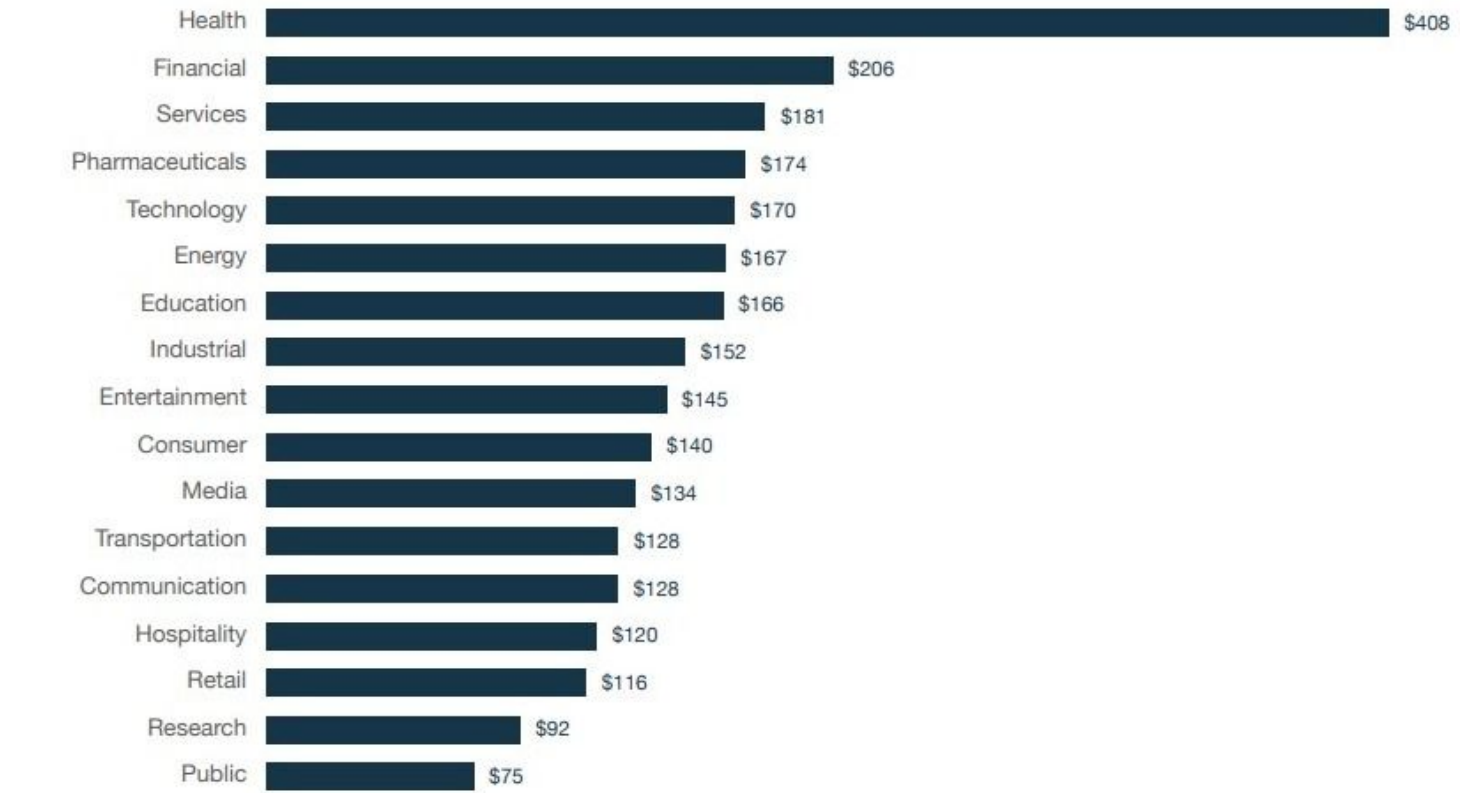
196 dias

Fonte: 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview

Custo por registro perdido ou roubado



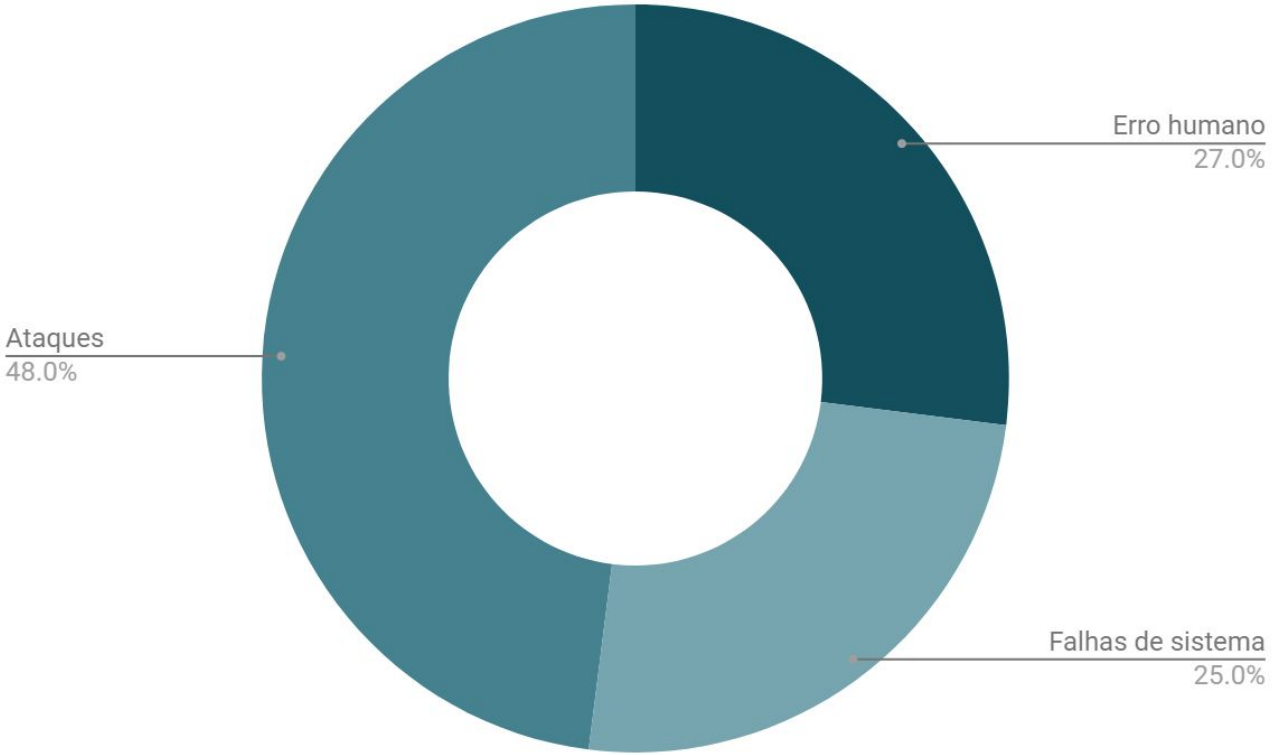
Fonte: 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview



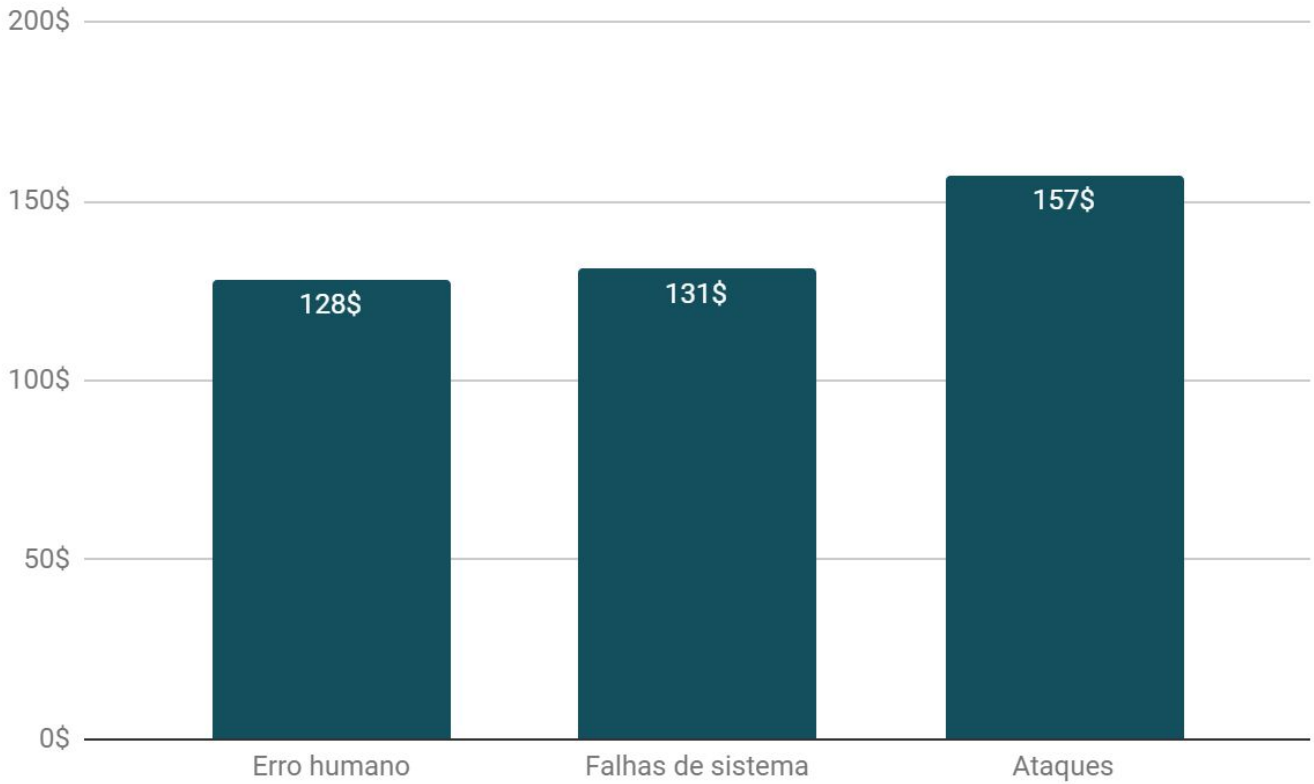
Custo por registro perdido ou roubado por setor

Reputação da organização

E qual a raíz dos problemas?



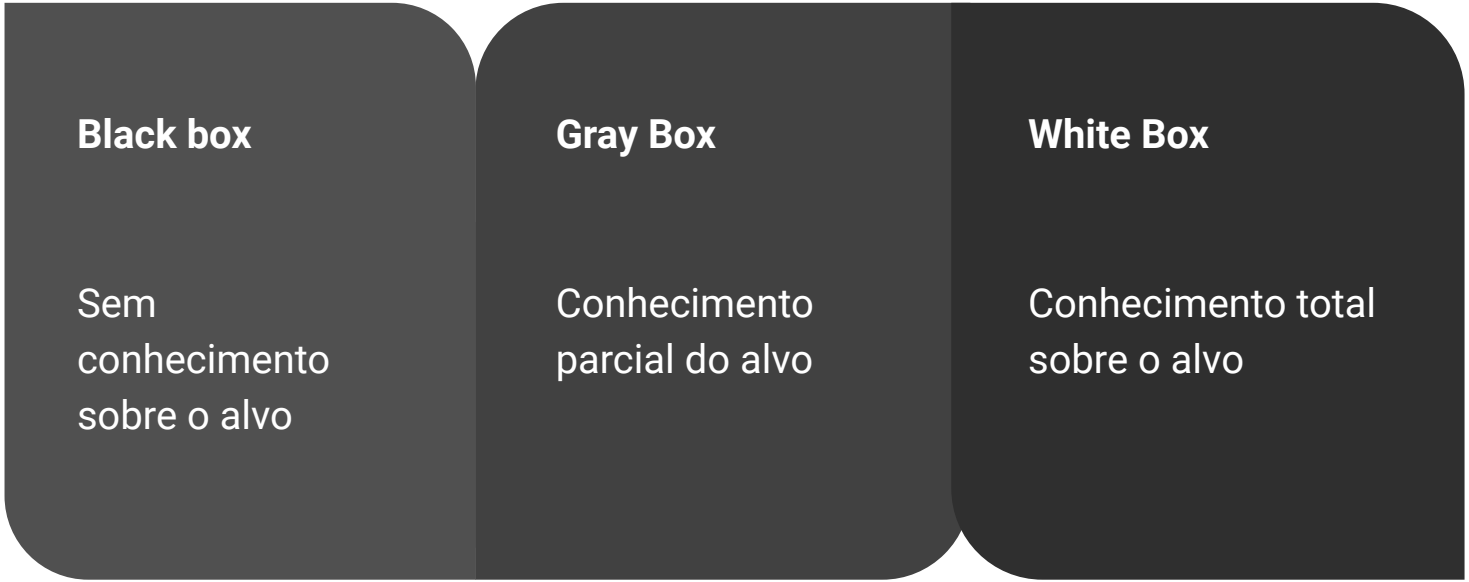
Distribuição por tipo de causa raíz



Custo por tipo de causa raíz

Teste de invasão

O primeiro passo para identificar as vulnerabilidades



Tipos de Teste de Invasão

Fases do teste de invasão

Preparação

Coleta de dados

Modelagem de ameaças

Análise de Vulnerabilidades

Exploração de falhas

Pós exploração de falhas

Geração de Relatório

Preparação

Compreender sobre a área de atuação da empresa e sobre o **objetivo** do testes de invasão

Alinhamento para evitar falhas de comunicação

Preparação

Compreender sobre a área de atuação da empresa e sobre o **objetivo** do testes de invasão

O que pode ser testado?

Preparação

Compreender sobre a área de atuação da empresa e sobre o **objetivo** do testes de invasão

Ao encontrar vulnerabilidade o teste deve continuar?

Dependendo das vulnerabilidades exploradas, podem ser expostas **informações estratégicas**

Preparação

Compreender sobre a área de atuação da empresa e sobre o **objetivo** do testes de invasão

- Quem está autorizado a realizar os testes?
- Caso algo inesperado ocorra, quem deve ser acionado?
- Pode utilizar engenharia social?

Elo fraco da segurança da informação

Engenharia social

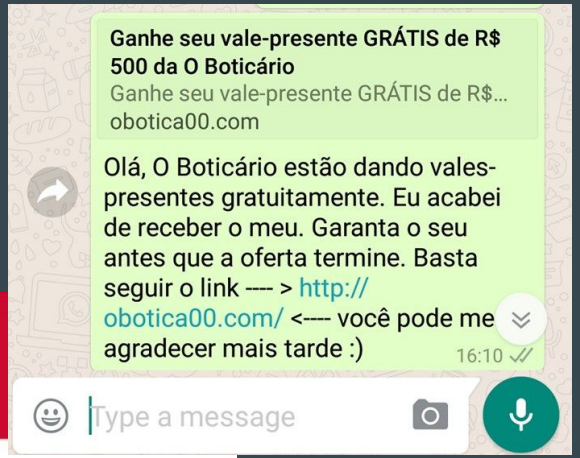
a arte de enganar

Ação de tentar obter informações ou influenciar alguém a realizar alguma ação apoiando-se na confiança de outras pessoas

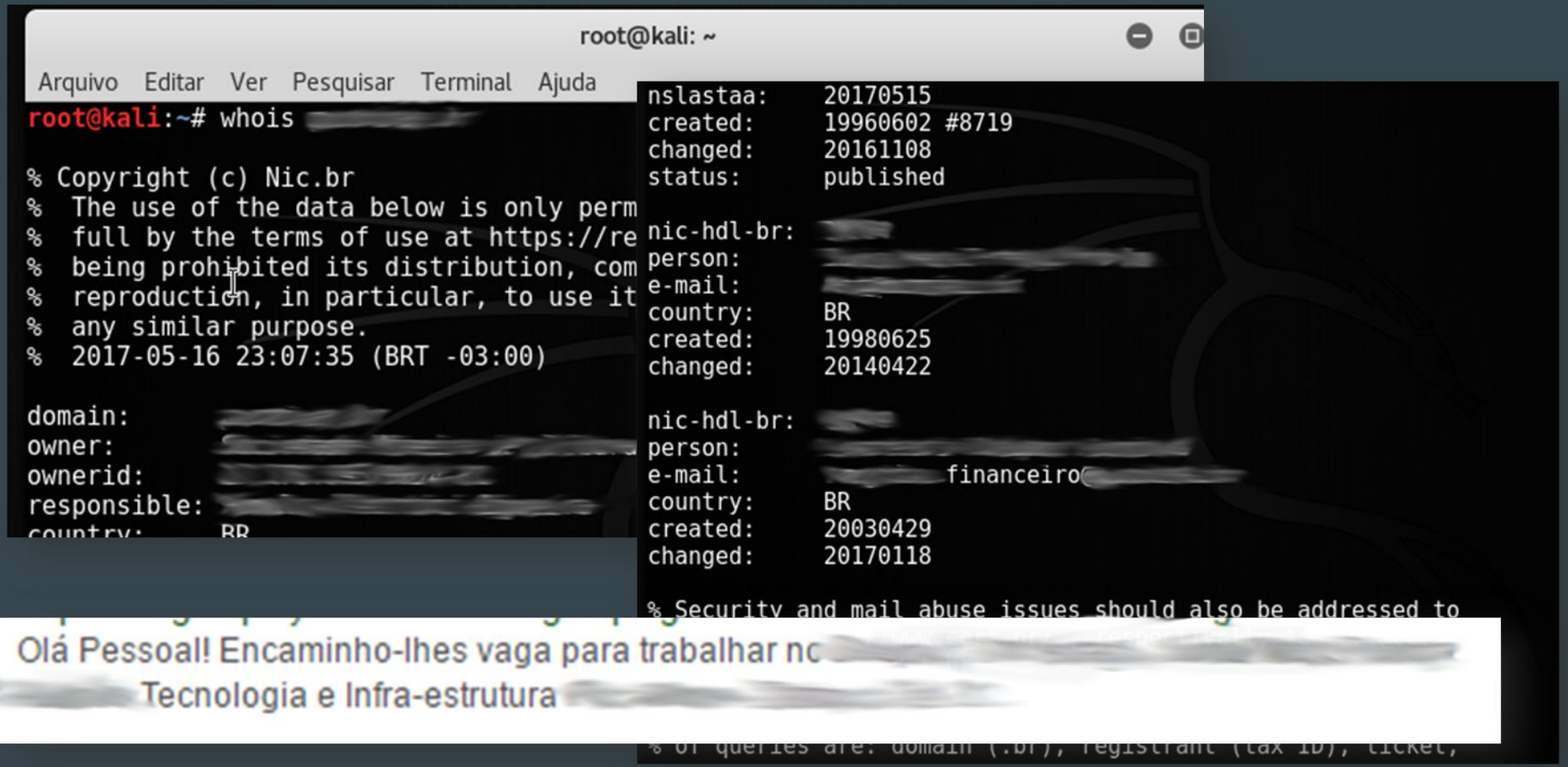
...


Itaú
Itaú Bankline
Procedimento de Segurança do Itaú Bankline.
Cartão de Segurança
Itaú
3019 1213
0800 121314
XXX XXX XXX
Referência do seu Cartão de Segurança:
111 111 111
Para confirmar a sua titularidade confirme os dados abaixo.
Atenção: Digite aqui a senha do seu Cartão Eletrônico de 6 dígitos: ••••••
Preencha atentamente as informações acima, é prudente confe
reforça a sua segurança e permite o acesso ao Internet
Em caso de dúvida, ligue para o SOS Bankline:
Grande São Paulo e localidades com DDD 11: 3019 1213 | Demais


Bradesco
Prezado(a) Cliente
Lembramos você que em nosso sistema ainda não consta a Sincronização de seu Token/ Tabela de segurança.
O seu prazo para sincronização foi prorrogado e deverá ser efetuado até o dia 02/01/2015
Evite o bloqueio do acesso ONLINE da sua conta na Internet e também do acesso nos Caixas eletrônicos Bradesco fazendo agora mesmo a Sincronia Semestral.
Clique no link abaixo para iniciar:
Iniciar já o Sincronismo
Atenciosamente,
Banco Bradesco


Ganhe seu vale-presente GRÁTIS de R$ 500 da O Boticário
Ganhe seu vale-presente GRÁTIS de R$...
obotica00.com
Olá, O Boticário estão dando vales-presentes gratuitamente. Eu acabei de receber o meu. Garanta o seu antes que a oferta termine. Basta seguir o link ---- > http://obotica00.com/ <---- você pode me agradecer mais tarde :)
16:10
Type a message

Phishing


root@kali: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@kali:~# whois
% Copyright (c) Nic.br
% The use of the data below is only perm
% full by the terms of use at https://re
% being prohibited its distribution, com
% reproduction, in particular, to use it
% any similar purpose.
% 2017-05-16 23:07:35 (BRT -03:00)
domain:
owner:
ownerid:
responsible:
country: BR
nslastaa: 20170515
created: 19960602 #8719
changed: 20161108
status: published
nic-hdl-br:
person:
e-mail:
country: BR
created: 19980625
changed: 20140422
nic-hdl-br:
person:
e-mail: financeiro
country: BR
created: 20030429
changed: 20170118
% Security and mail abuse issues should also be addressed to
Olá Pessoal! Encaminho-lhes vaga para trabalhar nc
Tecnologia e Infra-estrutura

Coleta de informação

O objetivo dessa fase é **conhecer o alvo**

Vagas de emprego

Através de vagas de emprego, dependendo do detalhamento, é possível compreender toda a infraestrutura e sistemas utilizados

Analista de Suporte TI

Prestar atendimento e suporte de 1º nível. Dar auxílio no diagnóstico e interação com as demais áreas relacionadas. Realizar manutenção de rotina e demais atividades pertinentes ao cargo. Realizar documentação de procedimentos referente a solução de problemas. Atuar na configurações de e-mail e demais atividades inerentes a função de analista. Ensino superior completo em Tecnologia da Informação. Conhecimentos em sistema operacional, Windows Vista 7, 8, 10, efetuando configurações em instalações de sistema, manutenção em Hardware e Software. Habilidades com rotinas de b
comunicação e escrita verbal. Bons co
Outlook, Windows Server 2008 supe
roteadores. Práticas em DNS, AD, DH
Wireless. Ser comprometido.

BENEFÍCIOS

Celular fornecido pela empresa, Tíquet

HORÁRIO

De segunda a sexta, das 8h às 18h.

REGIME DE CONTRATAÇÃO

CLT (Efetivo)

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

Windows Server 2008

Não sou um robô reCAPTCHA Privacidade - Termos

Search More Options

4 total entries

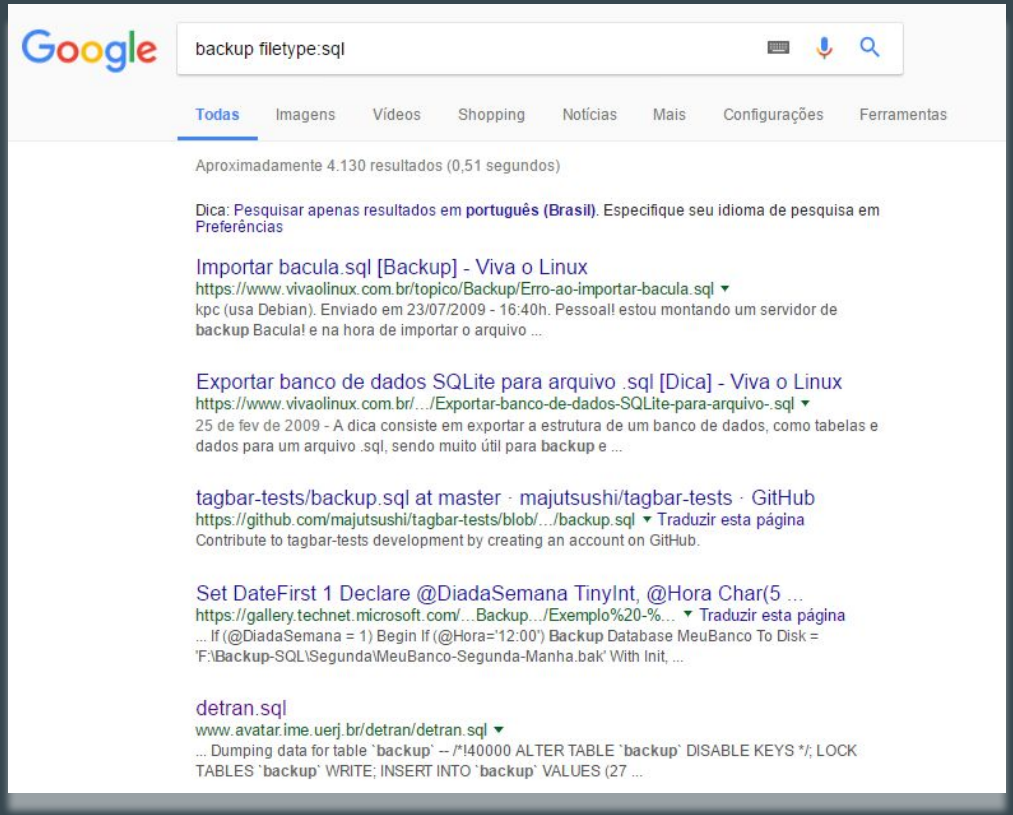
Date	D	A	V	Title	Platform	Author
2016-11-08	⬇	-	◷	Microsoft Windows Server 2008/2012 - LDAP RootDSE Netlogon Denial of Service	Windows	Todor Donev
2011-09-07	⬇	-	✔	Microsoft Windows Server 2008 R1 - Local Denial of Service	Windows	Randomdude
2009-11-12	⬇	-	✔	Microsoft Windows Server 2000 < 2008 - Embedded OpenType Font Engine Remote Code...	Windows	H D Moore
2009-02-10	⬇	-	-	Bypassing Windows Server 2008 Password Protection	Papers	Glafkos Cha...

Google Hacking

Encontrar arquivos dentro de sites, páginas que **deveriam ser secretas**

backup filetype:sql

Usando Filetype é possível encontrar arquivos com extensões específicas

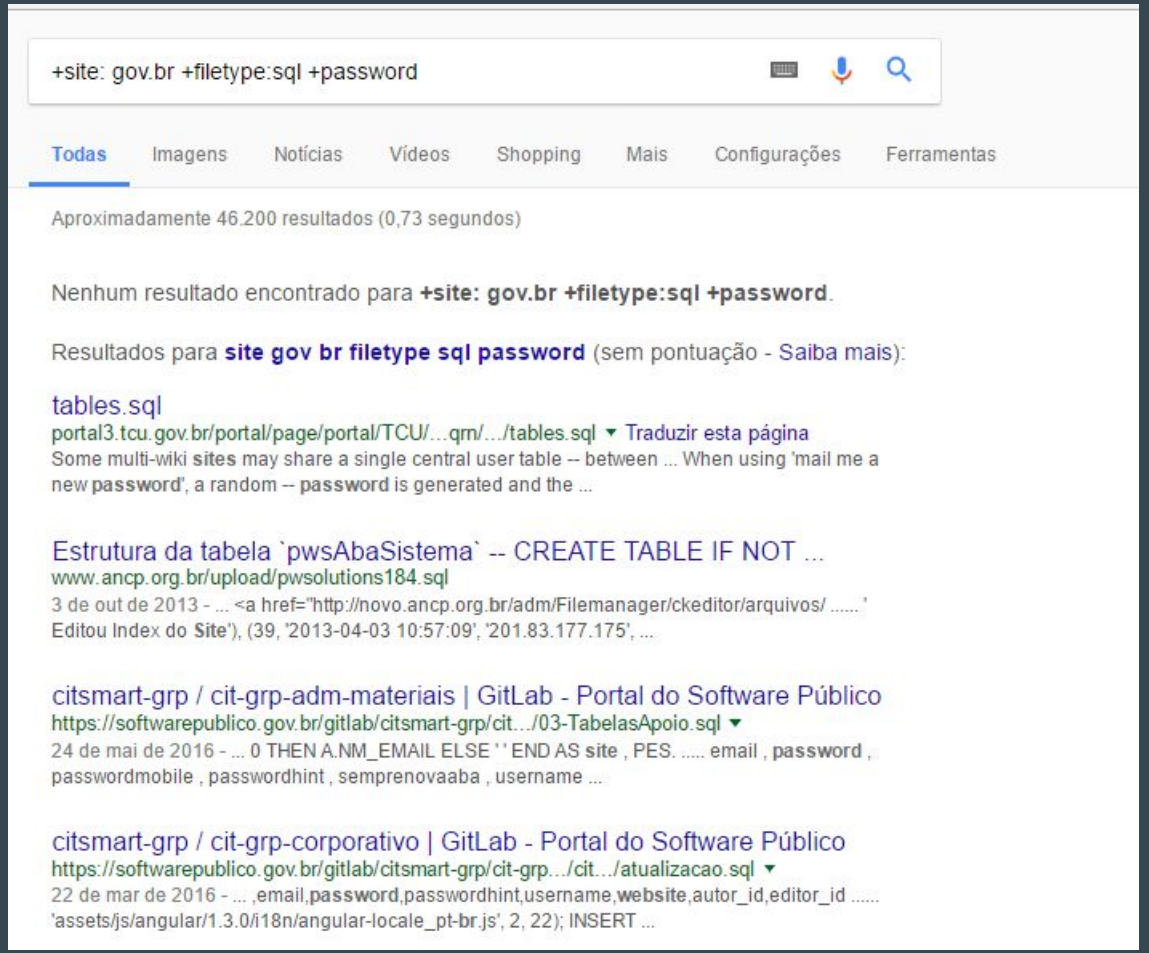


```
/*!40000 ALTER TABLE `backup` DISABLE KEYS */;
LOCK TABLES `backup` WRITE;
INSERT INTO `backup` VALUES (27,'c89c43df4b1a370dea4b6a5402afbfec','b','MARCOS PEREIRA DA SILVA','11771928883','marcos.3101@gmail.com','21-8578-1055','00283372601','Rua SÃ£o Gabriel, 501 ap 101 - Cachambi -
Rio de Janeiro - RJ - CEP 2078-292','110108034'),(28,'d59470f3b67327fb5b3ba25fa864c57b','a','Mauro Roberto P. Duarte','62642537749','mauro.pavao@gmail.com','95051984','01133174590','Estrada Henrique de Melo
711 casa 02','11423275165'),(29,'e657244973308f97132951743286ea04','c','Luis Roberto Cunha Barreiro','84692278749','luisbarreiro2001@yahoo.com.br','7896-6122  /  2576-9313','03352208876','Rua AraxÃ¡ 99 -
GrajaÃº - cep-20561-110','11.008610-7'),(30,'ecfb10fae0a9a306cef925a6772e2c38','a','MARCOS ANDRE MURTA','4280869774','jack.tatu@ig.com.br','021-2261-7234','00180846566','Rua pelotas n 189 \nEngenho
Novo','11.903858-1'),(31,'951e0de54f8b025499deefff0a8b3950','c','Adilson do Carmo','32931000744','jdarc2706@yahoo.com.br','(21) 9379-3649','01040405694','Rua ItuÃ¡, nÂº 1642, aptÂº 205, Jardim Guanabara,
Ilha do Governador, Cep. 21.940-180, Rio de Janeiro, RJ','110072061'),(32,'9ce7a5c2544323be8c1c59dd6ad20832','a','alex lopes lyrio','3745091744','alexlyrio@oi.com.br','78309755','00258006209','RUA TIAIA N17
```


INSERT INTO `backup` VALUES (27,'c89c43df4b1a370dea4b6a5402afbfec','b','MARCOS PEREIRA DA SILVA','11771928883','marcos.3101@gmail.com','21-8578-1055','00283372601','Rua SÃ£o Gabriel, 501 ap 101 - Cachambi -Rio de Janeiro - RJ - CEP 2078-292','110108034'),(28,'d59470f3b67327fb5b3ba25fa864c57b','a','Mauro Roberto P. Duarte','62642537749','mauro.pavao@gmail.com','95051984','01133174590','Estrada Henrique de Melo 711 casa 02','11423275165'),(29,'e657244973308f97132951743286ea04','c','Luis Roberto Cunha Barreiro','84692278749','luisbarreiro2001@yahoo.com.br','7896-6122 / 2576-9313','03352208876','Rua AraxÃ¡ 99 - GrajaÃº - cep-20561-110','11.008610-7'),(30,'ecfb10fae0a9a306cef925a6772e2c38','a','MARCOS ANDRE MURTA','4280869774','jack.tatu@ig.com.br','021-2261-7234','00180846566','Rua pelotas n 189 \nEngenho Novo','11.903858-1'),(31,'951e0de54f8b025499deefff0a8b3950','c','Adilson do


```
GAMA','60147563704','gabriel_gama_33@hotmail.com','39795725 - 83192218','00565265663','RUA JOAO PINHEIRO, 426 - CASA 17 - PIEDADE - RJ','810756'),(56,'39cccde380fd4922b4fd1abf5a6ced1e','a','paulo roberto de
souza','34109862787','robertosouzalo@hotmail.com','32792825','00330283554','R condessa belmont n73 casa4','11.011101-6'),(57,'7012c5f80b49117becb45cb3f06afcc6','a','DOMINGOS MENDES VIEIRA DE
CARVALHO','35967480706','talitanun@gmail.com','(21) 88642016','01139235398','RUA PROFESSORA ESTER DE MELO, 147/201 BENFICA','11017120-7'),(58,'748b5d2889806663dd9778003945bbae','b','Antonio JosÃ©
Machado','35173599715','gabriellamaria@globo.com','(21) 38223184','00081268071','Rua: Catulo Cearense \nNÂº: 91 fundos \nComplemento: Casa 6 \nBairro: Engenho de Dentro\nEstado: RJ \nCidade: RJ
\n','161182531'),(59,'28916f64bdd7a5d2c9dfec517bc74697','a','JORGE VIEIRA','38822105753','jana.vieira@globo.com','38724330','00071538153','Rua Padre Champagnat,21 ap.803','161048192'),
(60,'dad27322bac4186029d598af274e83f8','a','RICARDO JOSE BRAGA DE OLIVEIRA','86501607787','txmetro@ig.com.br','21 7827 7973','306971119','RUA GAL OTAVIO POVOA, 348 VILA DA PENHA','161099543'),
(61,'3a1e8566658edc81129fce535efb215d','c','Cilas Franco Fernandes Junior','5192189730','cilas_fernandes@hotmail.com','37693726','00259888735','Rua PaquetÃ¡ ,50 ,Austin, Nova IguaÃ§u ','11943515543'),
(62,'a00694b26bd82a8afd24cf55b21e2905','c','Manoel Antonio GonÃ§alves','22386408787','fabi.caramuru@gmail.com','(21)3011-9928','00134648205','Travessa Carlos Xavier, nÂº 126, apt. 102, Madureira, Rio de
Janeiro-RJ. ','110125550'),(63,'ec893dbb4d6d0db797b432d7e440d760','a','Luiz Saluti Nunes','79127320715','luizsalucci@ig.com.br','(021) 2281-2853','03461153966','Rua BarÃ£o do Bom Retiro,1243/402 Engenho
```

+site: gov.br
+filetype:sql
+password



Robots.txt

Controlam permissões de acesso a determinadas páginas ou pastas dos sites.

O robots.txt controla qual informação de um site deve ou não deve ser indexada pelos sites de busca.

```
# If the Joomla site is installed within a folder such as at
# e.g. www.example.com/joomla/ the robots.txt file MUST be
# moved to the site root at e.g. www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to the disallowed
# path, e.g. the Disallow rule for the /administrator/ folder
# MUST be changed to read Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/orig.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Disallow: /administrator/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /images/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /libraries/
Disallow: /logs/
Disallow: /media/
Disallow: /modules/
Disallow: /plugins/
Disallow: /templates/
Disallow: /tmp/

Allow: /
```

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Vulnerable Files ▾ Search Search

« prev 1 2 » next

Date	Title	Summary
2016-05-12	inurl:demo.browse.php intitle:getid3	Vulnerable Files The getID3 demo can allow directory traversal, deleting files, etc. https://github.com/JamesHeinrich/getID3/blob/master/demos/demo.browse.php Se...
2013-	-site:simplemachines.org "These are the paths and URLs to	Vulnerable Files Dork: -site:simplemachines.org "These are the paths and URLs to your SMF installation" Details:

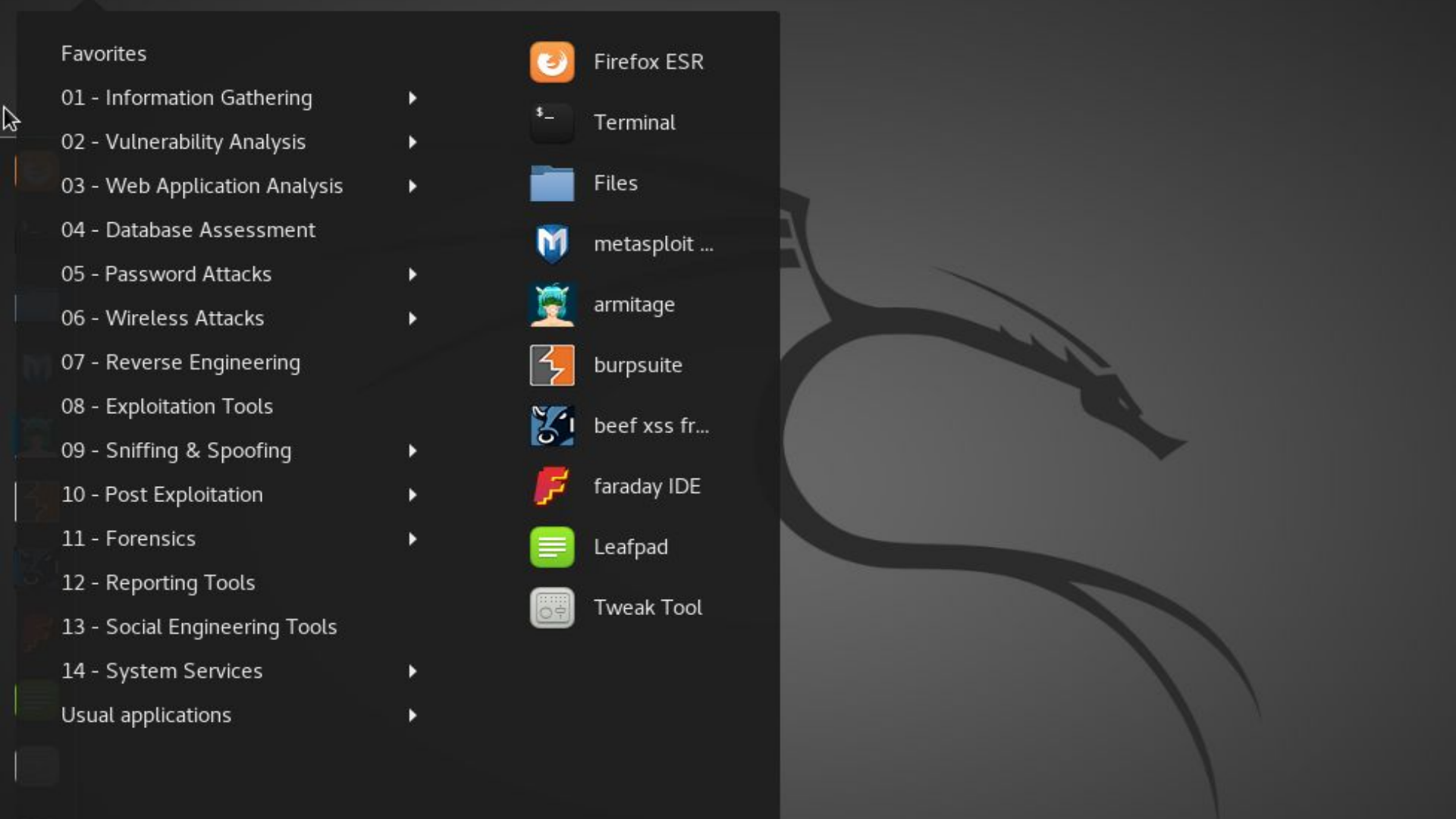
Modelagem de ameaças

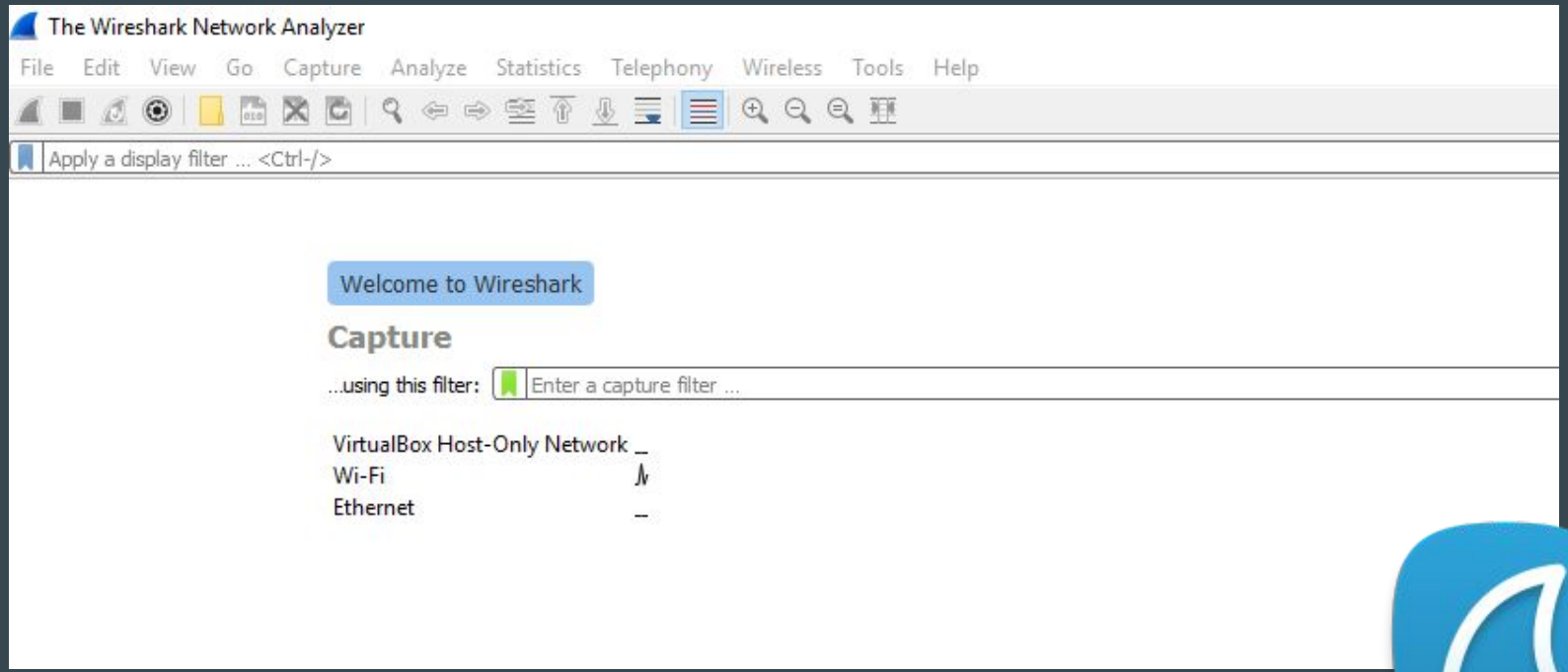
As informações encontradas na fase de coleta de informações serão utilizadas como base para **analisar** como poderia ocorrer um ataque

Análise de Vulnerabilidades

Analisar e **identificar** as vulnerabilidades


KALI LINUX™
“the quieter you become, the more you are able to hear”


Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
Firefox ESR
Terminal
Files
metasploit ...
armitage
burpsuite
beef xss fr...
faraday IDE
Leafpad
Tweak Tool



Análise manual

Exploração de falhas

As informações encontradas na fase de coleta de informações serão utilizadas como base para **analisar** como poderia ocorrer um ataque

Nessa fase são executados exploits

Dados, comandos ou códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas

Browse Exploit Database

Every Exploit, Shellcode and Paper. All in one place.

39,124 total entries

<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	A	V	Title	Platform	Author
2017-05-26	⬇	-	◷	QWR-1104 Wireless-N Router - Cross-Site Scripting	Hardware	Touhid M.Sh...
2017-05-26	⬇	-	◷	JAD java Decompiler 1.5.8e - Local Buffer Overflow	Linux	Juan Sacco
2017-05-26	⬇	-	✔	Microsoft MsMpEng - Multiple Problems Handling ntdll!NtControlChannel Commands	Windows	Google Secu...
2017-05-26	⬇	-	✔	Google Chrome 60.0.3080.5 V8 JavaScript Engine - Out-of-Bounds Write	Linux	halbecaf
2017-05-25	⬇	-	-	Introduction to Manual Backdooring	Papers	abatchy17
2017-05-25	⬇	-	✔	Apple WebKit / Safari 10.0.3(12602.4.8) - 'WebCore::FrameView::scheduleRelayout'...	Multiple	Google Secu...
2017-05-25	⬇	-	✔	Apple WebKit / Safari 10.0.3(12602.4.8) - 'Editor::Command::execute' Universal Cross-Site...	Multiple	Google Secu...

AndroBugs Framework

Android vulnerability analysis system

OWASP

The Open Web Application Security Project

OWASP Top 10 – 2017 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities
A10 – Underprotected APIs (NEW)

Demonstração

SQL Injection


Applications
Places
Firefox ESR
Thu 21:28
Kali Linux, an Offensive Security Project - Mozilla Firefox
Would you like to improve your search experience with suggestions? Learn more...
No
Yes
192.168.15.98/dvwa/vulnerabilities/sqli/?id=' union select user, password from users -- &Submit=Submit#
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection


Applications
Places
burp-StartBurp
Thu 22:03
Intruder attack 10
DVWA
Vulnerability: Brute

Pós exploração de falhas

Analisar as informações sobre o sistema invadido e são verificadas o que é possível realizar com o acesso adquirido

Avaliar quais dessas vulnerabilidades são relevantes para a organização

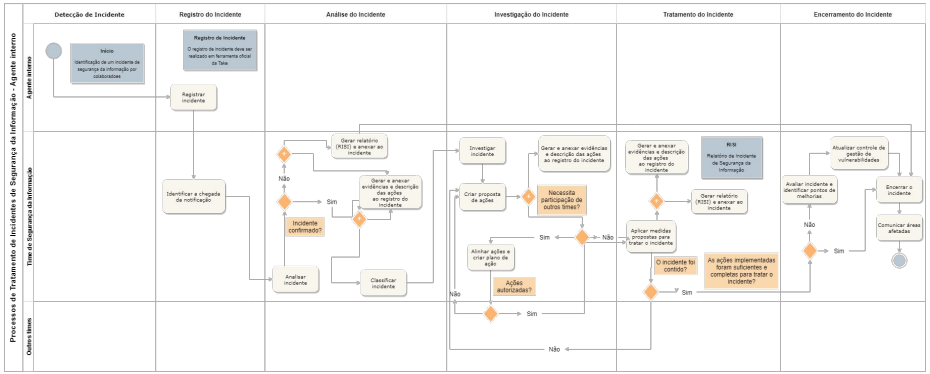
Geração de relatórios

Incluir todos os dados sobre as vulnerabilidades e avaliar quanto a criticidade

Recebi o relatório e agora?

Plano de ação

Ter uma gestão de incidentes e vulnerabilidades definida



Text

Time de Segurança da Informação

Comitê de segurança da informação

Ter um membro de cada time da organização

Tem um plano de resposta a incidentes

Com o plano é possível economizar mais de US $340.000 por violação em média

Fonte: 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview

Resposta a Incidentes

O ataque tem fases e é um momento de pânico, por isso é importante ter os procedimentos prontos necessários para agir e minimizar impactos

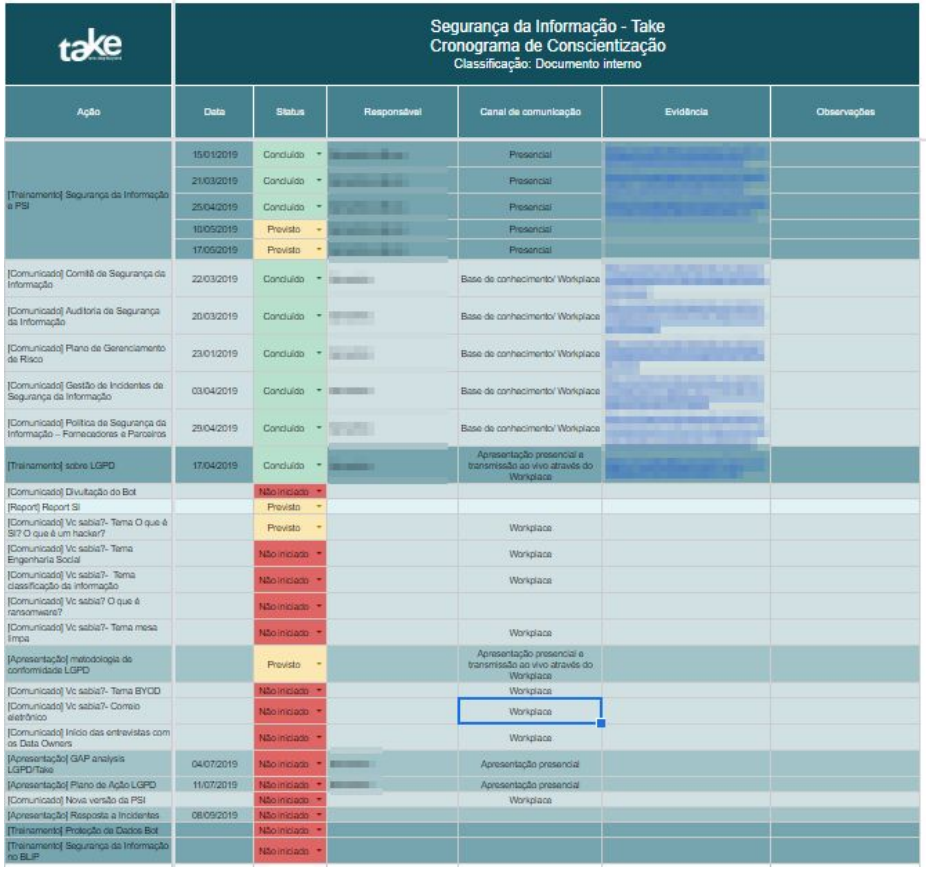
Gerenciamento de continuidade do negócio

É possível economizar mais de US $13 por violação em média

Fonte: 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview

Política de segurança da Informação

Conscientização



take

Segurança da Informação - Take
Cronograma de Conscientização
Classificação: Documento interno

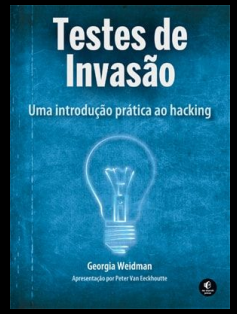
Ação	Data	Status	Responsável	Canal de comunicação	Evidência	Observações
[Treinamento] Segurança da Informação e PSI	15/01/2019	Concluído		Presencial		
	21/03/2019	Concluído		Presencial		
	25/04/2019	Concluído		Presencial		
	16/05/2019	Previsto		Presencial		
	17/05/2019	Previsto		Presencial		
[Comunicado] Comitê de Segurança da Informação	22/03/2019	Concluído		Base de conhecimento/ Workplace		
[Comunicado] Auditoria de Segurança da Informação	20/03/2019	Concluído		Base de conhecimento/ Workplace		
[Comunicado] Plano de Gerenciamento de Risco	23/01/2019	Concluído		Base de conhecimento/ Workplace		
[Comunicado] Gestão de Incidentes de Segurança da Informação	03/04/2019	Concluído		Base de conhecimento/ Workplace		
[Comunicado] Política de Segurança da Informação – Fornecedores e Parceiros	29/04/2019	Concluído		Base de conhecimento/ Workplace		
[Treinamento] sobre LGPD	17/04/2019	Concluído		Apresentação presencial e transmissão ao vivo através do Workplace		
[Comunicado] Divulgação do Bot		Não iniciado				
[Report] Report SI		Previsto				
[Comunicado] Vc sabia?- Tema O que é SI? O que é um hacker?		Previsto		Workplace		
[Comunicado] Vc sabia?- Tema Engenharia Social		Não iniciado		Workplace		
[Comunicado] Vc sabia?- Tema classificação da informação		Não iniciado		Workplace		
[Comunicado] Vc sabia? O que é ransomware?		Não iniciado				
[Comunicado] Vc sabia?- Tema mesa limpa		Não iniciado		Workplace		
[Apresentação] metodologia de conformidade LGPD		Previsto		Apresentação presencial e transmissão ao vivo através do Workplace		
[Comunicado] Vc sabia?- Tema BYOD		Não iniciado		Workplace		
[Comunicado] Vc sabia?- Correio eletrônico		Não iniciado		Workplace		
[Comunicado] Início das entrevistas com os Data Owners		Não iniciado		Workplace		
[Apresentação] GAP analysis LGPD/Take	04/07/2019	Não iniciado		Apresentação presencial		
[Apresentação] Plano de Ação LGPD	11/07/2019	Não iniciado		Apresentação presencial		
[Comunicado] Nova versão da PSI		Não iniciado		Workplace		
[Apresentação] Resposta a Incidentes	08/09/2019	Não iniciado				
[Treinamento] Proteção de Dados Bot		Não iniciado				
[Treinamento] Segurança da Informação no BUP		Não iniciado				

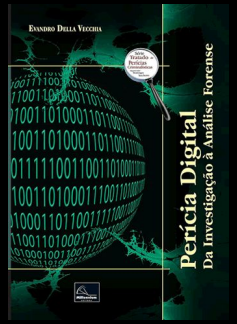
Proteção de dados

Lei geral de proteção de dados (LGPD)

Referências e atribuições

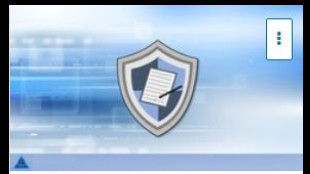
Livros





Build Security Incident Response for GDPR data...
Roland Costea, Cybersecurity & Privacy Leader

Fundamentos de Ethical Hacking: curso prático
Marcos Flávio Araújo Assunção, Professor, consultor e autor na...



Construindo uma Política de Segurança da Informação (PSI)
Cláudio Dodt, InfoSec Evangelist, CISSP, CISM, ISO 27K LA , ITIL...

The Complete Cyber Security Course : Network Security!
Nathan House, Leading Cyber Security Expert

Fundamentos de Riscos, Governança de TI e COBIT5
Felipe Antonio, Profissional de Tecnologia, Riscos e Auditoria

Security Management: Excellence in Private...
Alex Goldstein, CPP, Security Consultant and Educator

Cursos Udemy

Referências e atribuições

freepik.com pixabay

Imagens

Artigos

2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview

http://bit.ly/2IghzZX

Obrigada!

Samantha Nunes
@samanthamoraisn