

# Crimes Virtuais: A Visão do Hacker

Gilles Velleneuve Trindade Silvano  
gillesvtsilvano@gmail.com

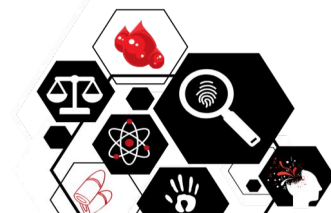
# Agenda



- Breve introdução
  - Lei dos Crimes Cibernéticos (Lei 12.737/2012)
  - Segurança da Informação
  - Ataques e Malwares
- Visão do Hacker
  - Crimes “normais” x Crimes Cibernético
  - Phishing
  - Força Bruta
  - Exploit
- Mecanismos de Defesa
- A perícia em Sistemas de Informação



# Introdução



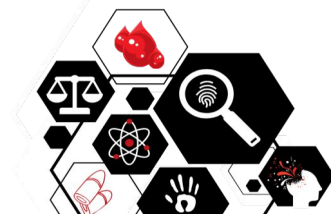
# Introdução

- Lei 12.737/2012 (Lei Carolina Dieckmann)
  - 36 imagens da atriz foram publicadas na web
  - Ameaças de extorsão R\$ 10.000,00
- Hipótese das fotos terem sido copiadas/recuperadas de uma máquina fotográfica que havia sido enviado para conserto
- Constatou-se que a caixa de e-mail da atriz havia sido violada

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante **violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou **instalar vulnerabilidades** para obter vantagem ilícita:

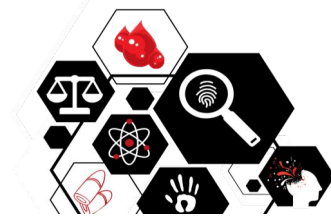
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

# Introdução - Mecanismos de Segurança



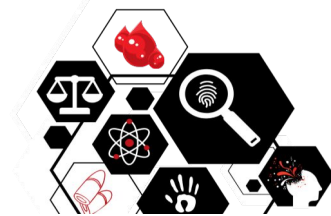
- ABNT NBR ISO/IEC 27002:2013
  - Controles Físicos
  - **Controles Lógicos**
    - Criptografia
    - Assinatura digital
    - **Controle de acesso (formulários de login)**
    - Protocolos seguros (Windows)
  - **Ameaças**
    - **Confidencialidade**
    - **Integridade**
    - Disponibilidade





# Introdução

SEGURANÇA DA INFORMAÇÃO



# Introdução - Segurança da Informação

## CONFIDENCIALIDADE

- Informação inacessível  
sem Autorização

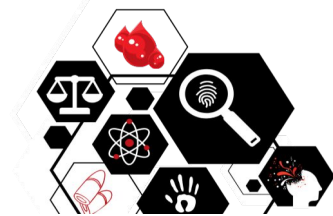
## INTEGRIDADE

- Informação mantida em  
seu estado correto

## DISPONIBILIDADE

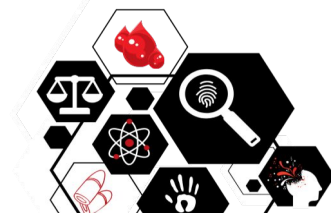
- Informação disponível  
somente após  
autorização

**SEGURANÇA DA INFORMAÇÃO**



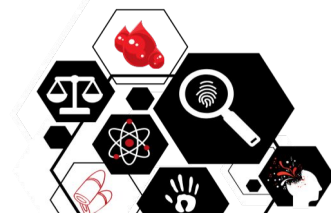
# A Visão do Hacker





# Crimes Cibernéticos “Comuns”

- **Estelionato e furtos eletrônicos (fraudes bancárias)** - Arts. 115 §3º e §4º, II e 171 do CP
- **Falsificação e supressão de dados** - Arts. 297, 298, 299, 313-A, 313-B do CP
- **Invasão de dispositivo Informático e furto de dados** - Art. 154-A do CP
- **Armazenamento; posse; produção; troca; publicação de vídeos e imagens contendo pornografia infantil juvenil** - Arts. 241, 241-A, 241-B do ECA
- **Assédio e aliciamento de crianças** - Art. 241-D do ECA
- **Ciberterrorismo** - Art. 2º, §1º, inc. IV da Lei 13260/2016



# Crimes Cibernéticos “Comuns”

- **Ameaça** - Art. 147 do CP
- **Divulgação de estupro/pornografia adulta** - Art. 218-C do CP
- **Interrupção de serviço** - Art. 266, §1º do CP
- **Cyberbullying (criação e publicação de perfis falsos, veiculação de ofensas em blogs e comunidades virtuais)** - Arts. 138, 139 e 140 do CP
- **Incitação e apologia ao crime** - Arts. 286 e 287 do CP
- **Crimes de ódio** - Art. 20 da Lei 7.716/89
- **Crimes contra a propriedade intelectual e artística** - Art. 184 do CP e Lei 9.609/98
- **Venda ilegal de medicamentos** - Art. 237 do CP

# Crimes “Normais” x Crimes Cibernético



X





Novos usuários de Internet  
este ano



157 804 425



Celulares vendidos hoje



3 079 946 652

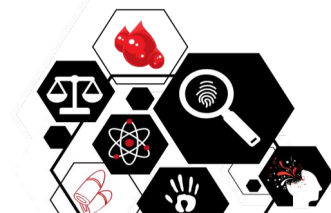


Total de cibertiques no  
mundo hoje



19 387 867 277

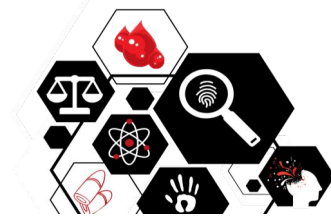




# Crimes Cibernéticos

- **65%** dos adultos já foram vítimas de algum crime virtual
- Cada crime resolvido custa ao estado **28 dias e custa U\$ 334,00**

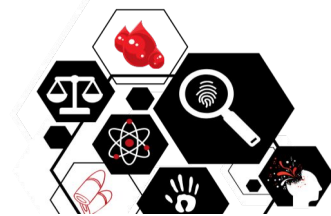




# A Visão do Hacker

MALWARES

# Introdução - Malwares (**Malicious Software**)

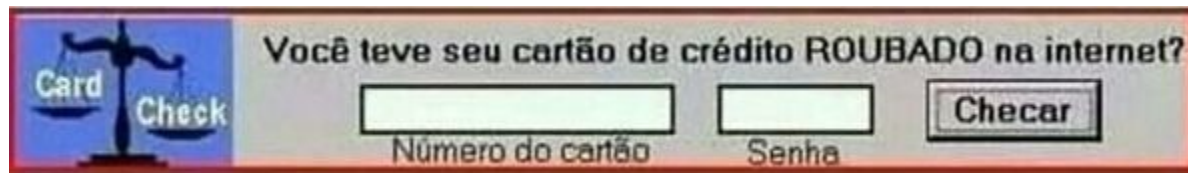


trojan virus  
screenlogger backdoor  
ransomware  
adware rootkit exploit  
keylogger sniffer worm  
spyware



# Introdução - Ataques: Phishing

- Termo vem de Fishing (pescaria)
- Utiliza uma “isca” (ex.: uma propaganda) para obter dados do usuário
- Comumente utilizado em conjunto com alguma técnica de engenharia social

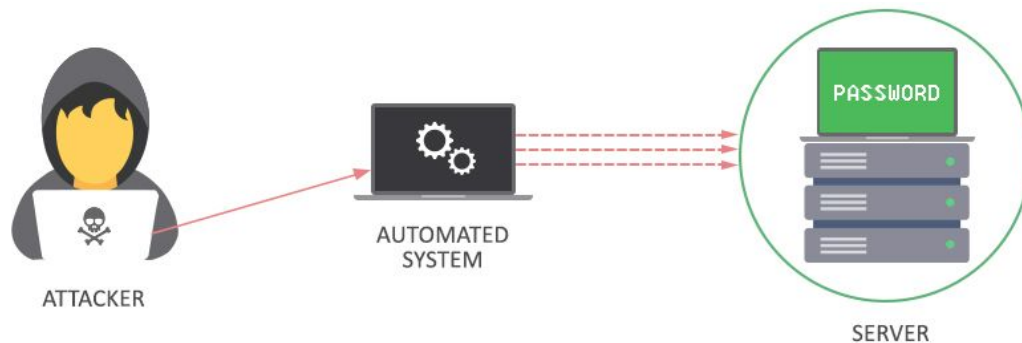


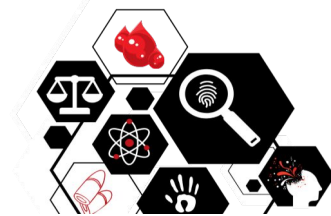




# Introdução - Ataques: Força Bruta

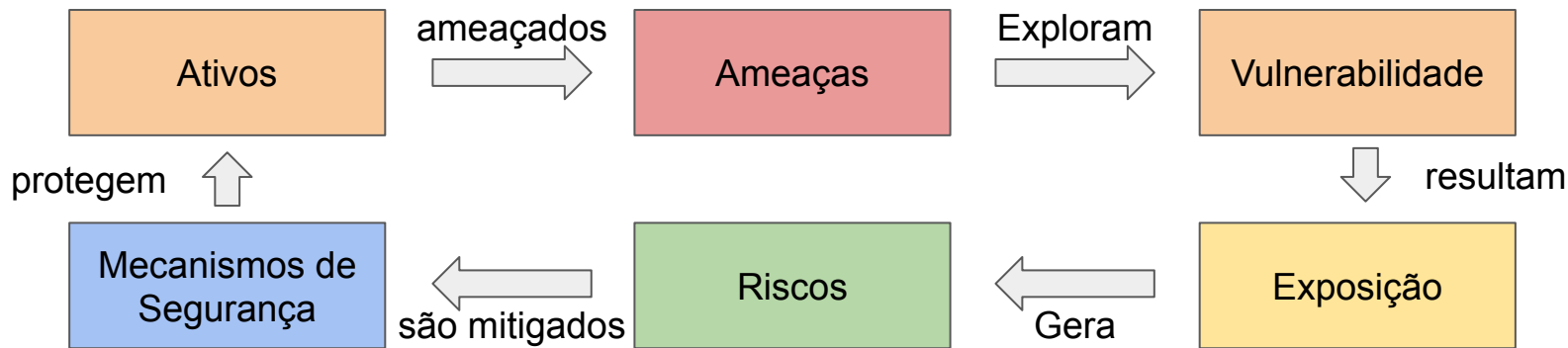
- Tentativa e erro em mecanismos de segurança (ex. formulários de login)
- Sistema automático faz a tentativa e verifica se ela foi bem sucedida
- Termo se dá pela busca “às cegas” por uma credencial válida
  - Alguns métodos derivados são mais inteligentes (ex. Rainbow tables)

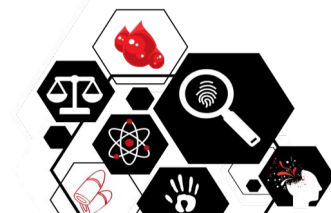




# Introdução - Ataques: Exploit

- Código que explora uma **vulnerabilidade** específica conhecida
- Vulnerabilidade é condição do software que, quando explorada (**exploit**), pode resultar em uma **ameaça**
- Ameaça é a hipotética violação à segurança da informação causada por um **exploit**



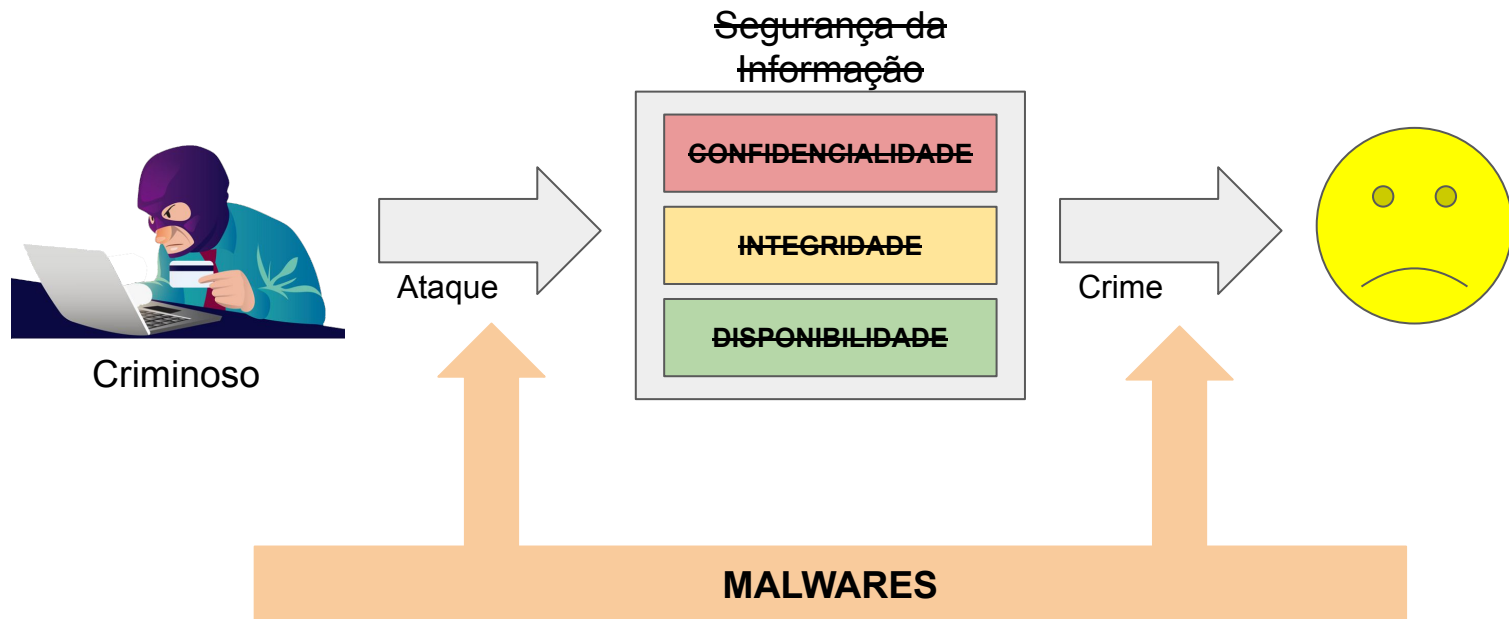


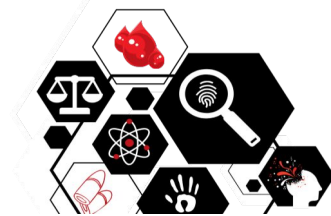
# Introdução - Ataques: Exploit

- Top Produtos com vulnerabilidades em 2019
- Aplicações
  - Acrobat Reader DC, Acrobat DC e Cpanel
- Microsoft é a empresa com mais produtos
  - Desktop e Servidor
- Android domina mercado de dispositivos móveis

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	<a href="#">Android</a>	<a href="#">Google</a>	OS	<a href="#">414</a>
2	<a href="#">Debian Linux</a>	<a href="#">Debian</a>	OS	<a href="#">360</a>
3	<a href="#">Windows 10</a>	<a href="#">Microsoft</a>	OS	<a href="#">357</a>
4	<a href="#">Windows Server 2016</a>	<a href="#">Microsoft</a>	OS	<a href="#">357</a>
5	<a href="#">Windows Server 2019</a>	<a href="#">Microsoft</a>	OS	<a href="#">351</a>
6	<a href="#">Acrobat Reader Dc</a>	<a href="#">Adobe</a>	Application	<a href="#">342</a>
7	<a href="#">Acrobat Dc</a>	<a href="#">Adobe</a>	Application	<a href="#">342</a>
8	<a href="#">Cpanel</a>	<a href="#">Cpanel</a>	Application	<a href="#">321</a>
9	<a href="#">Windows 7</a>	<a href="#">Microsoft</a>	OS	<a href="#">250</a>
10	<a href="#">Windows Server 2008</a>	<a href="#">Microsoft</a>	OS	<a href="#">248</a>
11	<a href="#">Windows Server 2012</a>	<a href="#">Microsoft</a>	OS	<a href="#">246</a>
12	<a href="#">Windows 8.1</a>	<a href="#">Microsoft</a>	OS	<a href="#">242</a>
13	<a href="#">Windows Rt 8.1</a>	<a href="#">Microsoft</a>	OS	<a href="#">235</a>
14	<a href="#">Ubuntu Linux</a>	<a href="#">Canonical</a>	OS	<a href="#">190</a>

# Introdução - A Visão do Hacker

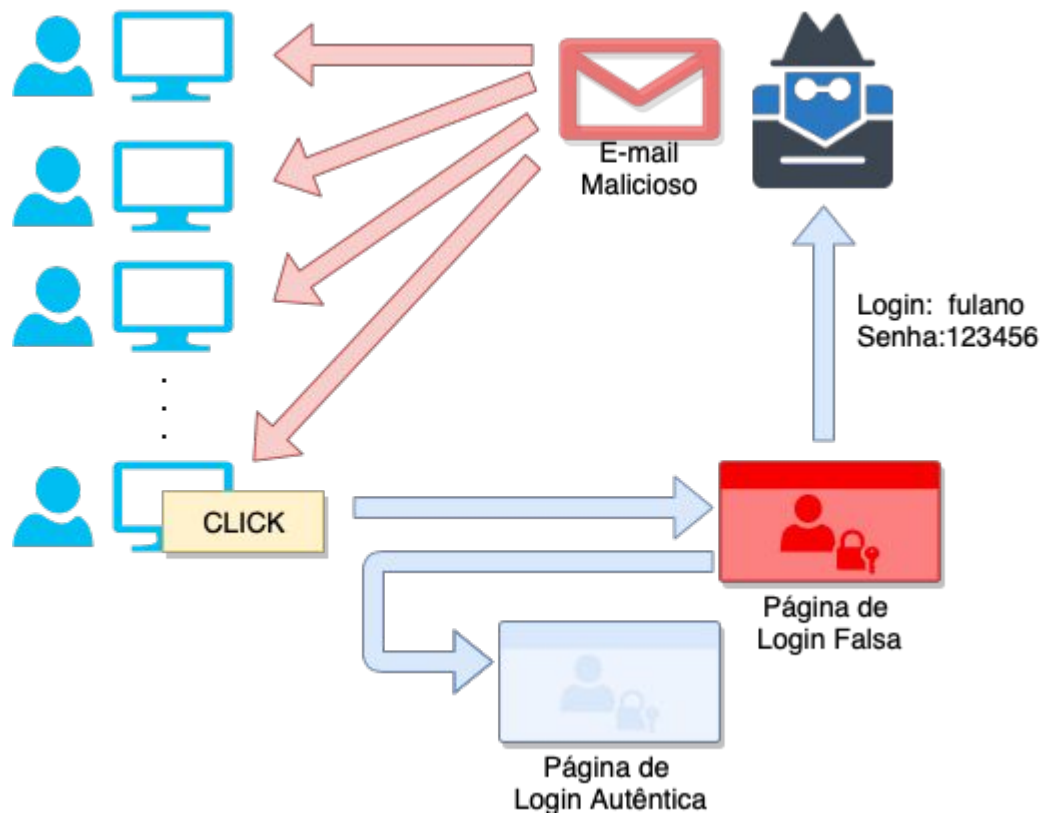




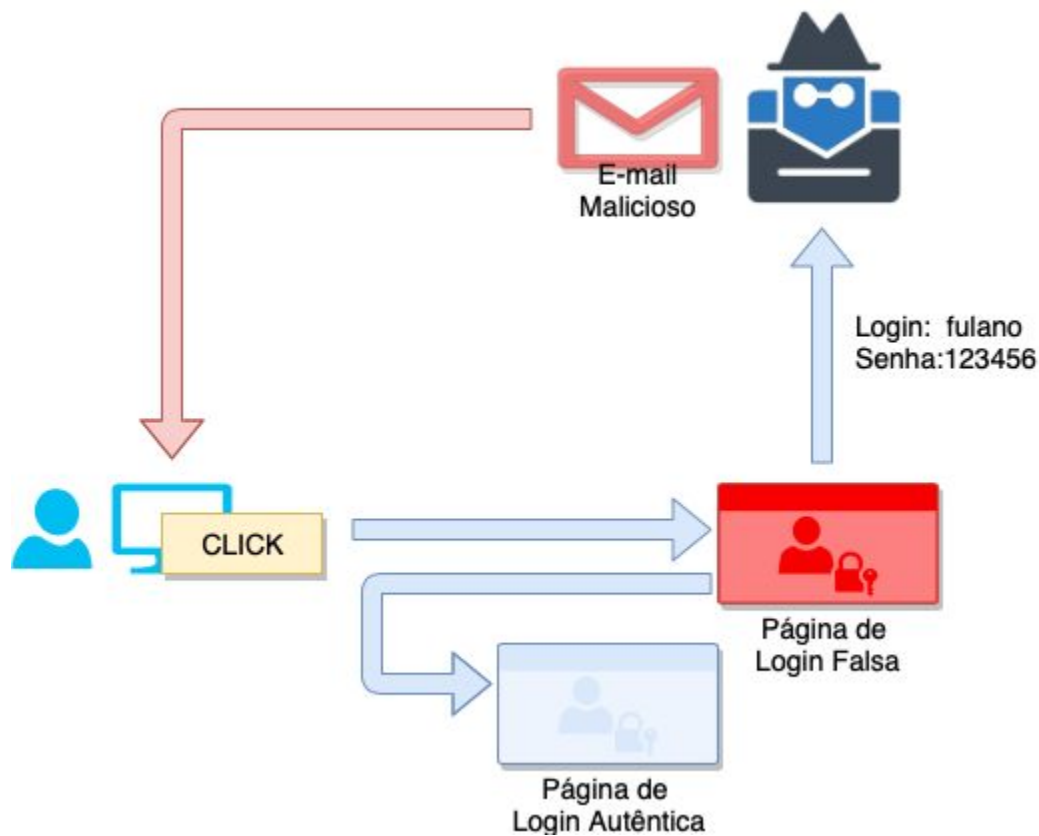
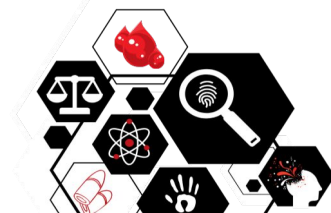
# A Visão do Hacker

PHISHING

# Blind Phishing



# Spear Phishing



Top 10 nomes usados por  
sites de phishing ▼

Empty target	599 129
Caixa	72 640
HM Revenue & Customs	28 379
Microsoft Corporation	25 859
Apple	17 228
Yahoo!	12 339
Banco Santander group	10 315
PayPal	7 965
Банк "СЕВЕРНАЯ КАЗНА" ОАО	6 257
Facebook	5 730



## Emails enviados hoje ▼

120 008 870 399 222






localhost:8000

Promoção BB - gillesperito@gmail.com - Gmail

Autoatendimento Pessoa Física - Banco do Brasil



[Atendimento / SAC / Ouvidoria](#)

A

A

+

-

Acessível para deficientes visuais

## Autoatendimento Pessoa Física

Titular

✓ 1º Titular

2º Titular

3º Titular

4º Titular

Senha de autoatendimento (8 dígitos)

ENTRAR

LIMPAR

Selecione o titular da conta.

**Como acessar?**

[Requisitos mínimos](#)

[Termo de uso do autoatendimento](#)


**Outros acessos**

[Produtor Rural](#)

[Não correntista](#)


[Utilizando certificado digital A3](#)

[Precisa de ajuda?](#)

**Gerenciador Financeiro**

Acesse a conta da sua empresa.

[Saiba mais](#)

**Gerenciador Financeiro Produtor Rural / Private**

Faça a gestão de seus negócios

[Saiba mais](#)

© Banco do Brasil

Central de Atendimento BB - 4004 0001 / 0800 729 0001

SAC BB - 0800 729 0722

Ouvidoria - 0800 729 5678

Deficientes auditivos/fala - 0800 729 0088

Segurança



# A Visão do Hacker

FORÇA BRUTA

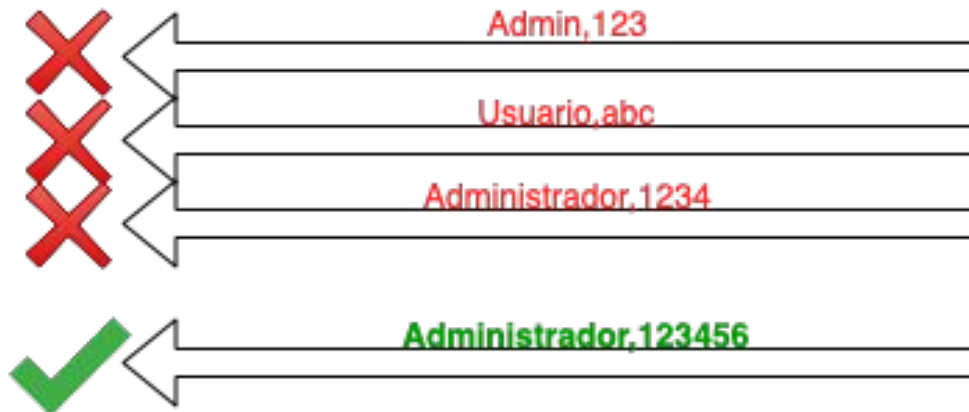
# Força Bruta



Usuários



Senhas





# Força Bruta - Ataque de Dicionário

## Dicionário de Usuários.txt

user  
adm  
admin  
Administrator  
Admin  
root

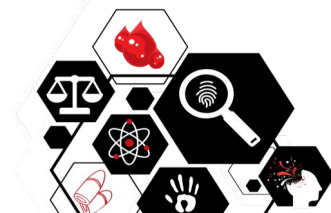
X

## Dicionário de Senhas.txt

ccbcfb  
ddcfef  
fbaede  
bddadc  
afeaba  
fefaae  
ffbcba  
...

$\{\text{user, adm, admin, ... root}\} \times \{\text{ccbcfb, fbaede, ... ffbcba}\} = \{(\text{user, cbcfb}), (\text{user, ddcfef}) \dots (\text{root, ffbcba})\}$

Quão segura é a sua senha?



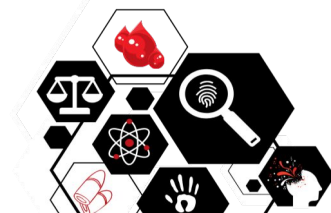
# HOW SECURE IS MY PASSWORD?

**123456**

Your password would be cracked

**INSTANTLY**

Quão segura é a sua senha?



# HOW SECURE IS MY PASSWORD?

**1a2b3c4**

It would take a computer about

**2 SECONDS**

to crack your password

Quão segura é a sua senha?



# HOW SECURE IS MY PASSWORD?

@1a2b3c4

It would take a computer about

**19 MINUTES**

to crack your password

Quão segura é a sua senha?



# HOW SECURE IS MY PASSWORD?

**@1A2b3c4#**

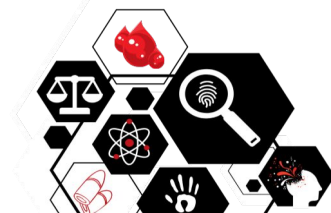
It would take a computer about

**4 WEEKS**

to crack your password



Quão segura é a sua senha?



# HOW SECURE IS MY PASSWORD?

**@1A2b3c42###9**

It would take a computer about

**34 THOUSAND YEARS**

to crack your password

Quão segura é a sua senha?



# HOW SECURE IS MY PASSWORD?

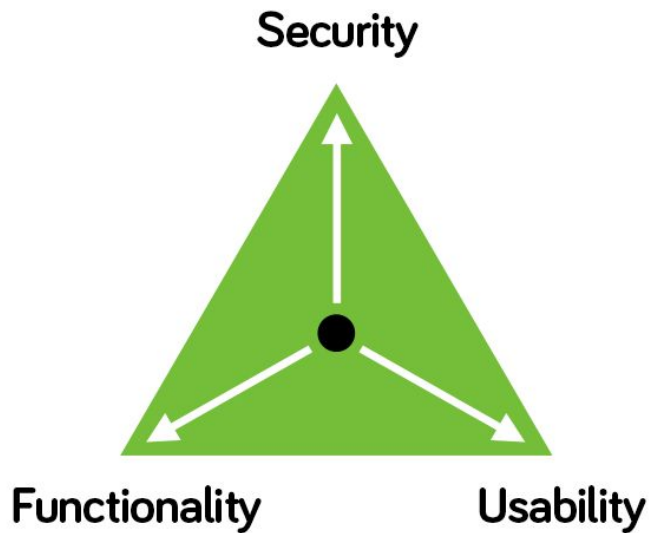
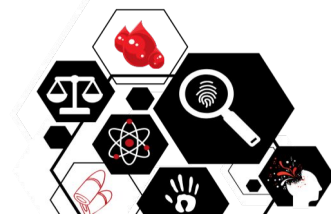
@1A2b3c42##9\*

It would take a computer about

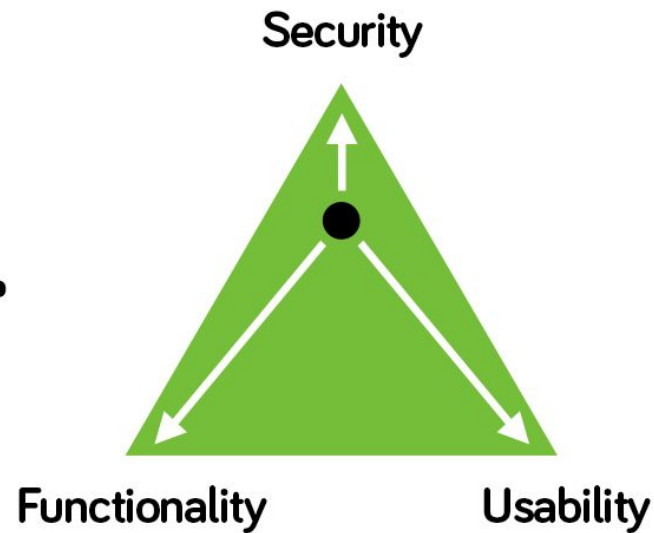
**3 MILLION YEARS**

to crack your password

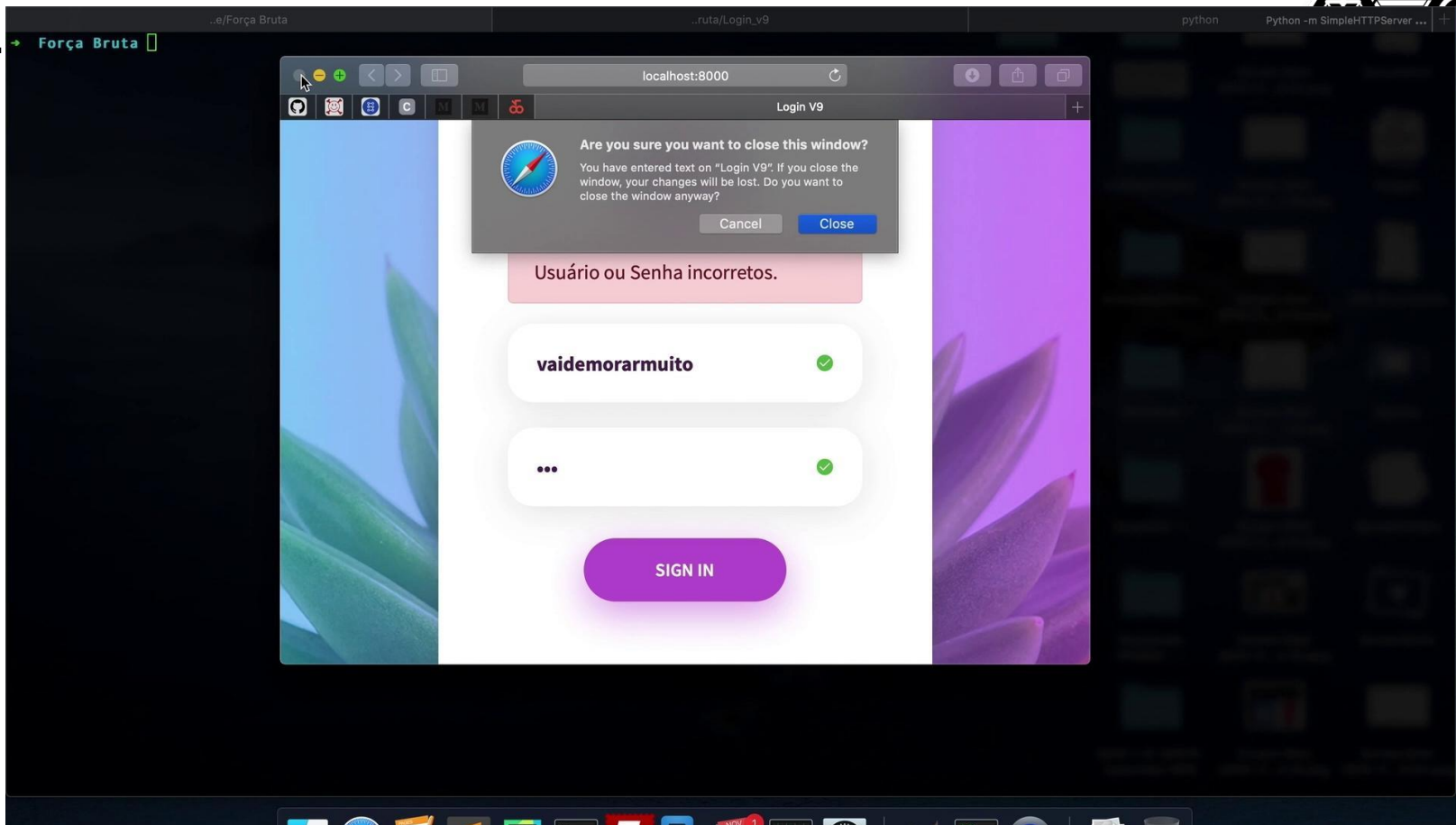
# Força Bruta - Opostos

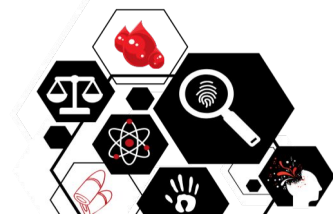


**VS.**



F





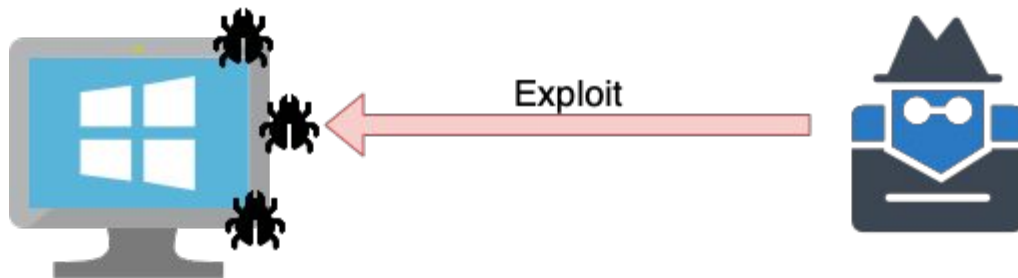
# A Visão do Hacker

EXPLOIT



# Exploit

- Zero-day exploits
- The Shadow Brokers (TSB) publicaram vários exploits da NSA (2016)
- Eternalblue + Doublepulsar



## Top exploits no mundo ▼

Exploit.Win32.CVE-2017-11882.gen 28.62%

Exploit.Win32.ShadowBrokers.ae 10.19%

Exploit.Script.Blocker 5.13%

Exploit.MSOffice.CVE-2018-0802.gen 4.35%

Exploit.MSOffice.Pederr.gen 3.38%

Exploit.AndroidOS.Lotus 2.00%



## Top exploits no Brasil ▼

Exploit.Win32.CVE-2017-11882.gen 58.36%

Exploit.MSOffice.CVE-2017-11882.a 19.17%

Exploit.Script.Generic 7.25%

Exploit.Script.Blocker.u 4.52%

Exploit.Script.Blocker 1.94%

Exploit.MSOffice.CVE-2018-0802.gen 1.65%

Exploit.MSOffice.CVE-2018-0802.a 1.15%

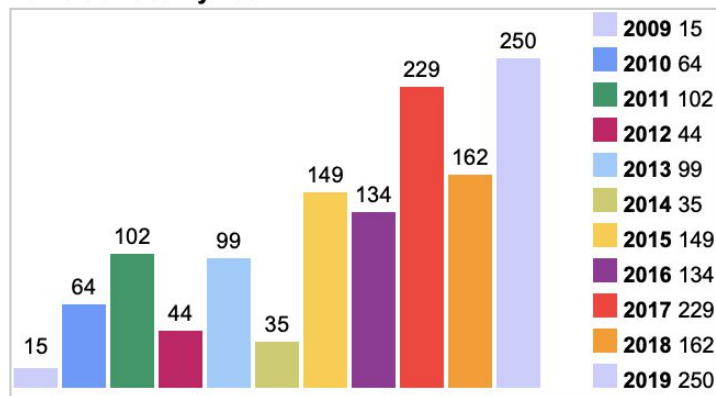




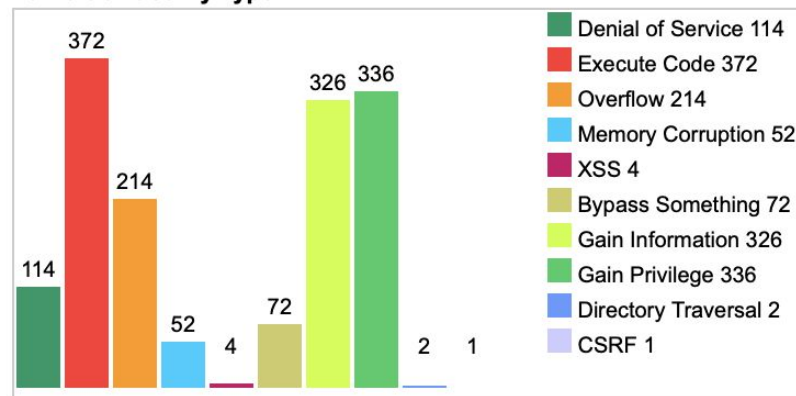
# Exploit - CVE-2017-11882

- Microsoft Office
- Problema em como o software gerencia memória
- Executa código com o usuário local
  - Caso o usuário tenha acesso de Administrador, total controle do sistema
- Requer que o usuário abra o arquivo malicioso no MS Office

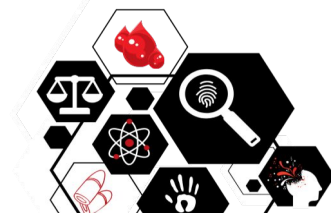
Vulnerabilities By Year



Vulnerabilities By Type



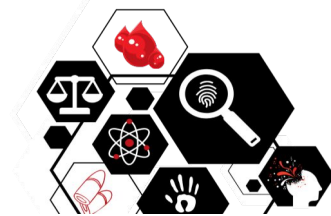




# Windows Timeline



# Exploit



```
gillesilvano — root@kali: ~ — ssh root@172.16.215.140 — 90x26
set PAYLOAD windows/x64/meterpreter_reverse_https
set PAYLOAD windows/x64/meterpreter_reverse_ipv6_tcp
set PAYLOAD windows/x64/meterpreter_reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PAYLOAD windows/x64/me
set PAYLOAD windows/x64/messagebox
set PAYLOAD windows/x64/meterpreter/bind_ipv6_tcp
set PAYLOAD windows/x64/meterpreter/bind_ipv6_tcp_uuid
set PAYLOAD windows/x64/meterpreter/bind_named_pipe
set PAYLOAD windows/x64/meterpreter/bind_tcp
set PAYLOAD windows/x64/meterpreter/bind_tcp_rc4
set PAYLOAD windows/x64/meterpreter/bind_tcp_uuid
set PAYLOAD windows/x64/meterpreter/reverse_http
set PAYLOAD windows/x64/meterpreter/reverse_https
set PAYLOAD windows/x64/meterpreter/reverse_named_pipe
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set PAYLOAD windows/x64/meterpreter/reverse_tcp_rc4
set PAYLOAD windows/x64/meterpreter/reverse_tcp_uuid
set PAYLOAD windows/x64/meterpreter/reverse_winhttp
set PAYLOAD windows/x64/meterpreter/reverse_winhttps
set PAYLOAD windows/x64/meterpreter_bind_named_pipe
set PAYLOAD windows/x64/meterpreter_bind_tcp
set PAYLOAD windows/x64/meterpreter_reverse_http
set PAYLOAD windows/x64/meterpreter_reverse_https
set PAYLOAD windows/x64/meterpreter_reverse_ipv6_tcp
set PAYLOAD windows/x64/meterpreter_reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PAYLOAD windows/x64/meterpreter/
```



# Mecanismos de Defesa

# Phishing




# Força Bruta



☐

I'm not a robot

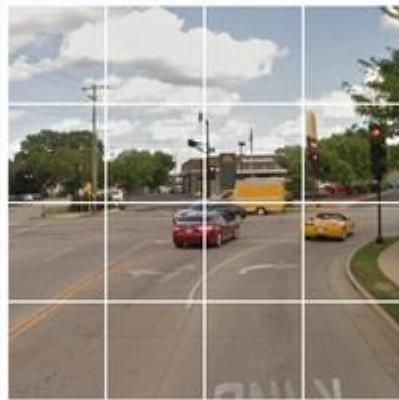
  
ReCAPTCHA




arch nemsib

[Privacy & Terms](#)



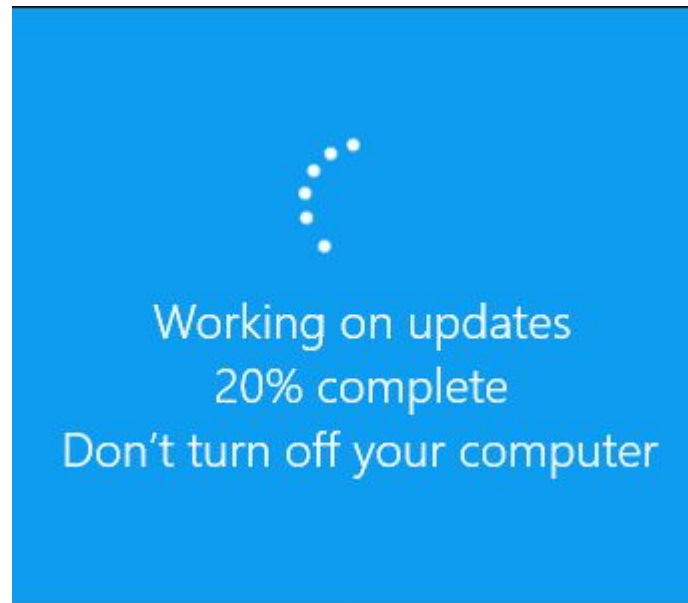
Select all squares with  
**traffic lights**  
If there are none, click skip

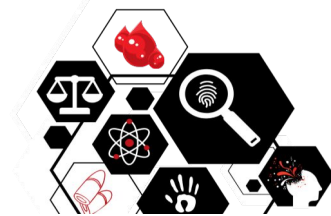


[SKIP](#)

# Exploit





# Perícia em Sistemas de Informação



# Phishing

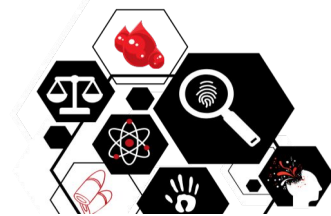
- Os Servidores das páginas falsas possuem um registro de **Nome de Domínio (DNS)**
  - [www.meusite.com.br](http://www.meusite.com.br)
- Esse registro é cadastrado no nome de uma pessoa física

## Domínio **ufrn.br**

TITULAR	UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
DOCUMENTO	24.365.710/0001-83
RESPONSÁVEL	MARCOS CESAR MADRUGA ALVES PINHEIRO



The screenshot displays a web-based geolocation tool. On the left, a sidebar contains a search bar with 'Host/IP' and '186.236.200.174'. Below the search bar, a list of details is shown: Hostname: 186.236.200.174, IP Address: 186.236.200.174, Country: Brazil, Country Code: BR, Region: Rio Grande do Norte, City: Natal, Postal Code: 59000-000, Latitude: -5.795000, and Longitude: -35.209440. On the right, a map of Brazil shows a red pin indicating the location. A tooltip over the pin displays: Country: Brazil, City: Natal, IP Address: 186.236.200.174. The map includes state names and a scale bar.



- Os Servidores enviam as credenciais para um outro computador ou salvam na própria memória
- Em algum momento o Hacker irá acessar esses dados e irá registrar seu acesso
  - Perícia irá revelar de qual computador o Hacker acessou <https://www.geodatatool.com/en/?ip=186.236.200.174>

A diagram showing a flow from a top box to a bottom box labeled 'User'. The top box contains a blue arrow pointing right, which then turns down and right into the 'User' box.



E-mail  
Malicioso

IP

Login: fulano  
Senha:123456

Para onde essa  
informação foi enviada?

Página de Login Falsa



# Força Bruta

- Os registros dos Servidores que hospedam as páginas de Login mantêm registro das tentativas
  - Auxilia os Peritos a encontrarem a fonte das tentativas

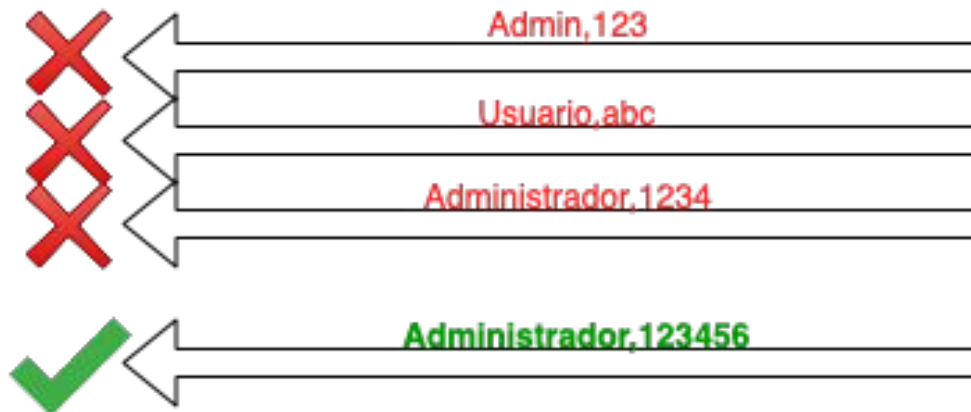
De onde estão vindo essas tentativas?



Usuários



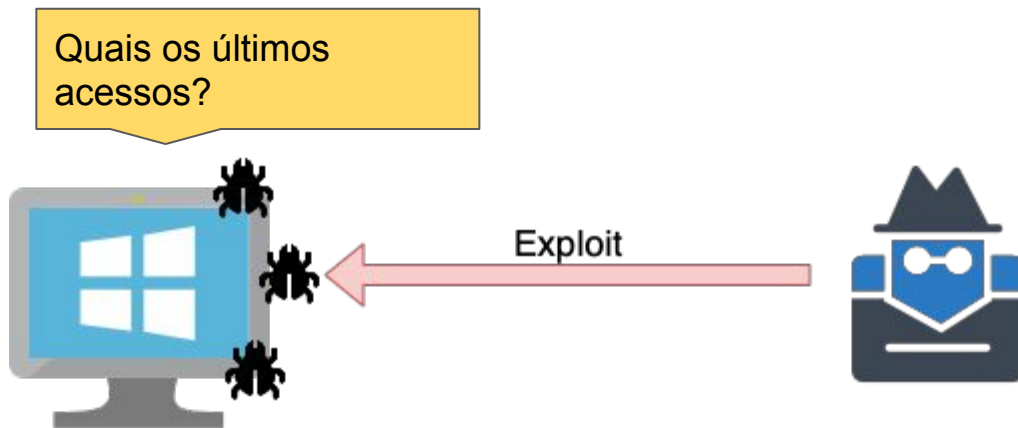
Senhas



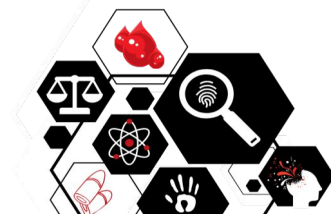


# Exploit

- Os Sistemas Operacionais mais comuns guardam registros de acesso



# Revisando

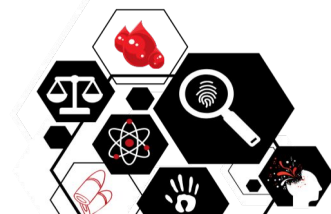


- Segurança da Informação
  - Confidencialidade, Integridade e Disponibilidade (CID)
- Crimes “Normais” x Crimes Cibernéticos
- Malwares
- Ataques
  - Phishing
  - Força Bruta
  - Exploit
- Mecanismos de Defesa
- Perícia em S.I.



# Crimes Virtuais: A Visão do Hacker

Gilles Velleneuve Trindade Silvano  
gillesvtsilvano@gmail.com



# Crimes Virtuais: A Visão do Hacker

Gilles Velleneuve Trindade Silvano  
gillesvtsilvano@gmail.com

Perguntas?