



GTER 45 | GTS 31

22 A 24 DE MAIO DE 2018, FLORIANÓPOLIS - SC
SENAI (CTAI)



EHA/IFRN: Ethical Hacker Academy

Treinando Segurança em Ambiente Controlado



Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos

Florianópolis/SC – 24 de Maio de 2018

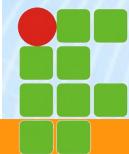


O que é (ou pretende ser) a EHA/IFRN

- **Programa ≠ Projeto**
- **Ensino, Pesquisa e Extensão**
- **Início: 2013**
 - IFRN Câmpus Natal Central
 - IFRN Câmpus Currais Novos
- **Slogan “Hacking com Responsabilidade”**



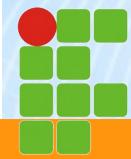
***Não é um projeto de curta duração...
...pretende ser um programa contínuo de educação!***





Objetivos

- **Promover a cultura da Segurança da Informação e Hacking Ético;**
- **Incentivar a pesquisa aplicada em Segurança da Informação, Software Livre e Computação;**
- **Capacitar e certificar os alunos para o mercado de Segurança da Informação.**



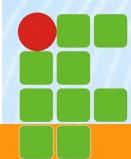


Público-Alvo

- **Interno: Alunos e servidores do IFRN**
- **Externo:**
 - **Estudantes e profissionais da área de Informática;**
 - **Poetas, carecas, bruxas e lobisomens...**



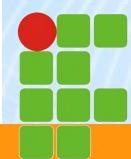
***Para implantar uma “cultura de Hacking Ético”
é necessário atingir a todos (sem restrições)***





O que já foi realizado?

- Cursos (Presenciais) para alunos e servidores do IFRN;
- Cursos (Presenciais) aberto à comunidade externa;
- Participação em eventos (palestras e minicursos);
- Consultorias e perícias esporádicas (cooperação técnica);
- Website/Blog: “www.segurancaderedes.com.br”;
- Canal Youtube: “youtube.com/segurancaderedes”
- Adequação de ementas (cursos técnicos e de tecnologia).





O que há de novo (2ª Fase)

- Exercitando segurança, na prática, em ambiente controlado

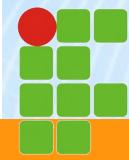


Two side-by-side screenshots of web interfaces. Both feature the Ethical Hacker Academy logo at the top. The left screenshot is titled 'EHA/IFRN Módulo de Acesso' and shows input fields for 'usuário' and 'Senha' with a 'Acessar' button below. The right screenshot is titled 'EHA/IFRN Ambiente CTF' and also shows input fields for 'usuário' and 'Senha' with a 'Acessar' button below. Both interfaces have a green header bar and a decorative footer bar at the bottom.



Módulo de Acesso

- Formalizando o Interesse: E-Mail para contato@eha.net.br
 - Público Interno (IFRN): Número de Matrícula
 - Público Externo: Dados pessoais pra cadastro
- Cadastramento no Módulo de Acesso
- Agendamento pra “Avaliação do Módulo de Acesso”
 - Fundamentos de Sistema Operacional Linux
 - Fundamentos de Redes de Computadores
 - Fundamentos de Segurança da Informação
- Nota $\geq 7,0 \rightarrow$ Cadastramento na “Plataforma CTF”



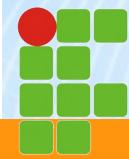
Módulo de Acesso: Como Funciona?

- Ambiente Moodle (personalizado);
- Perguntas Objetivas compreendendo o conteúdo informado;
- 60 minutos para realização da avaliação;
- Resultado informado ao final da tentativa;
- Caso nota < 7,0 nova tentativa somente após 15 (quinze) dias.



Importante!!!

- **O Cadastramento em ambas as plataformas é MANUAL;**
- **A “Equipe” operacional é pequena;**
- **A paciência é uma virtude...**



Ethical Hacker Academy

Módulo de Acesso



EHA/IFRN
Módulo de Acesso

usuário

Senha

Acessar

Screenshot of the EHA/IFRN Módulo de Acesso web application interface.

The browser title bar shows "Painel" and the URL "Seguro | https://acesso.eha.net.br/my/".

The main header features the "ETHICAL HACKER ACADEMY" logo and the text "EHA/IFRN Módulo de Acesso".

The top navigation bar includes icons for notifications, messages, and user profile (Adriano), along with links for "Personalizar esta página" and "Logout".

The left sidebar contains a "Navegação" section with a tree menu:

- Painel
 - Página inicial do site
 - Páginas do site
 - Meus cursos
 - Módulo de Acesso EHA/IFRN

The main content area displays the authenticated user information:

Usuário autenticado



Adriano Cansian
País: Brasil
Cidade/Município: GTS31/CGI.BR
cansian@meuamigo.com.br

Ethical Hacker Academy

Módulo de Acesso



EHA/IFRN
Módulo de Acesso

usuário

Senha

Acessar

The screenshot shows a web browser window for the 'Módulo de Acesso' course on the EHA/IFRN platform. The top bar includes a back button, forward button, refresh button, a lock icon indicating 'Seguro', and the URL 'https://acesso.eha.net.br/course/view.php?id=2'. On the right side of the top bar are icons for notifications, messages, and user profile (Adriano). Below the top bar, there's a green header bar with a decorative pattern. The main content area has a green header 'Avaliação do Módulo de Acesso'. To the left is a sidebar titled 'Navegação' (Navigation) with a tree icon. Under 'Painel', it lists 'Página inicial do site' and 'Páginas do site'. Under 'Meus cursos', it lists 'Módulo de Acesso EHA/IFRN' which is expanded to show 'Participantes', 'Competências', 'Avaliação do Módulo de Acesso', and 'Avaliação de competências'. A central call-to-action button says 'Clique para iniciar a avaliação (60 minutos)' with a play icon.

Ethical Hacker Academy

Módulo de Acesso



EHA/IFRN
Módulo de Acesso

usuário
Senha

Acessar

Adriano

Módulo de Acesso Seguro | https://acesso.eha.net.br/mod/quiz/view.php?id=5

Página inicial Este curso

Meus cursos > Módulo de Acesso EHA/IFRN > Avaliação do Módulo de Acesso > Clique para iniciar a avaliação (60 minutos)

Navegação

- Painel
 - Página inicial do site
 - Páginas do site
 - Meus cursos
 - Módulo de Acesso EHA/IFRN
 - Participantes
 - Competências
 - Avaliação do Módulo de Acesso
 - Clique para iniciar a avaliação (60 minutos)

Clique para iniciar a avaliação (60 minutos)

A avaliação é composta de 40 (quarenta) questões, sendo:

- 15 (quinze) questões sobre Fundamentos do sistema operacional GNU/Linux;
- 15 (quinze) questões sobre Fundamentos de Redes de Computadores e Arquitetura TCP/IP;
- 10 (dez) questões sobre Fundamentos de Segurança da Informação.

Cada aluno/participante terá direito a uma única tentativa e, para isso, disporá do tempo máximo de 60 (sessenta) minutos.

Tentativas permitidas: 1

Este questionário será aberto em Friday, 1 Sep 2017, 00:00

Duração máxima: 1 hora

Tentar responder o questionário agora

Ethical Hacker Academy

Módulo de Acesso



EHA/IFRN
Módulo de Acesso

usuário
Senha

Acessar

Adriano

Módulo de Acesso E x Seguro | https://acesso.eha.net.br/mod/quiz/view.php?id=5

Página inicial Este curso

Meus cursos > Módulo de Acesso EHA/IFRN > Avaliação do Módulo de Acesso > Clique para iniciar a avaliação (60 minutos)

Navegação

- Painel
 - Página inicial do site
 - Páginas do site
- Meus cursos
 - Módulo de Acesso EHA/IFRN
 - Participantes
 - Competências
 - Avaliação do Módulo de Acesso
 - Clique para iniciar a avaliação (60 minutos)

Clique para iniciar a avaliação (60 minutos)

Iniciar tentativa

Questionário com limite de tempo

O questionário tem um limite de tempo de 1 hora. O cronômetro começará a contar a partir do momento em que iniciar a tentativa e deverá submetê-la antes do tempo acabar. Tem certeza que quer iniciar a tentativa agora?

Iniciar tentativa Cancelar

Tentativas permitidas: 1

Este questionário será aberto em Friday, 1 Sep 2017, 00:00

Duração máxima: 1 hora

Tentar responder o questionário agora

Ethical Hacker Academy

Módulo de Acesso



EHA/IFRN
Módulo de Acesso

usuário

Senha

Acessar

Adriano

Clique para iniciar a avaliação

Seguro | https://acesso.eha.net.br/mod/quiz/attempt.php?attempt=53

Página inicial Este curso

Meus cursos > Módulo de Acesso EHA/IFRN > Avaliação do Módulo de Acesso > Clique para iniciar a avaliação (60 minutos)

Navegação do questionário

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40		

Questão 1
Ainda não respondida
Vale 1 ponto(s).
▼ Marcar questão

Parte mais importante da configuração é de acordo com o que possam ser configurados no computador e o que é necessário que

Escolha uma:

- a.
- b.
- c.
- d.

Próxima página

Finalizar tentativa ...

Tempo restante 0:59:48

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



The screenshot shows the user interface of the EHA/IFRN Ambiente CTF platform. At the top, there's a navigation bar with links for "Página inicial", "Painel", "Eventos", "Meus desafios", and a "Personalizar esta página" button. On the left, a sidebar titled "Navegação" contains links for "Painel", "Página inicial do site", "Páginas do site", and "Desafios". The main content area features a large banner with the text "EHA/IFRN :: Ambiente CTF". Below the banner, it says "AVISOS undefined" and "Ranking Ranking EHA/IFRN (07/10/2017)". On the right, a "Usuário autenticado" section displays the user profile of "Rubens Kurl", showing "País: Brasil", "Cidade/Município: GTERGTS/NIC.BR", and the email "rubens@amigodeadriano.com.br".

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



EHA/IFRN
Ambiente CTF

usuário

Senha

Acessar

CTF EHA/IFRN: Cate x Seguro | https://ctf.eha.net.br/course/index.php

EHA/IFRN :: Ambiente CTF

Página inicial Painel Eventos Meus desafios Ocultar blocos Visualização padrão

Desafios

Navegação

Painel

- Página inicial do site
- Páginas do site
- Desafios
 - Para Esquentar...
 - Miscellaneous
 - Crypto
 - Forensics
 - Networking

Buscar cursos Vai Expandir tudo

Para Esquentar...

Miscellaneous

Crypto

Forensics

Networking

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



EHA/IFRN
Ambiente CTF

usuário
Senha

Acessar

Curso: #EHA_Desaf ... Seguro | https://ctf.eha.net.br/course/view.php?id=10

#EHA_Desafios_Resolv ...

Página inicial Painel Eventos Meus desafios Este curso Ocultar blocos Visualização padrão

Meus desafios > #EHA_Desafios_Resolvidos

Navegação

- Painel
 - Página inicial do site
 - Páginas do site
 - Meus desafios
 - #EHA_Desafios_Resolvidos
 - Participantes
 - Emblemas
 - Competências
 - Notas
 - Desafios Resolvidos #EHA_PraEsquentar
 - #EHA_Crypto_01
 - #EHA_Crypto_02
 - #EHA_Crypto_03
 - #EHA_Networking_01
 - #EHA_Forensics_01
 - #EHA_Misc_01
 - #EHA_Misc_08
 - #EHA_Misc_07
 - #EHA_Forensics_08
 - #EHA_Forensics_07
 - #EHA_Networking_07
 - #EHA_Misc_06
 - #EHA_Misc_05

Desafios Resolvidos #EHA_PraEsquentar

Esse espaço é destinado aos novos integrantes da EHA/IFRN. Você que chegou agora e não participou dos desafios anteriores à sua chegada encontrará aqui TODOS os desafios que já foram inseridos (e resolvidos) na plataforma. Sugerimos que NÃO veja os WriteUps (respostas aos desafios) antes de fazê-los, para treinar seus conhecimentos e intuição. Depois é só ir conferindo os WriteUps (links disponíveis no website do projeto = www.eha.net.br). Para não "começar zerado" nos novos desafios, cada desafio deste espaço que você resolver acumulará 01 (um) ponto no ranking geral da EHA/IFRN. Qualquer dúvida: contato@eha.net.br.

#EHA_Crypto_01

 - Baixe o arquivo (link abaixo) e boa sorte em seu primeiro desafio...

<http://www.eha.net.br/desafios/77f7fc620b1d9ddbcd140c60ded0395711cc188d123aa4a12fc48b645935b2b7URL>

 - Desafio resolvido (100 pontos) pela primeira vez por:
 - Eduardo Medeiros
 - 16/09/2017 10h28m

Se já descobriu a FLAG, clique e responda no formato eha{FLAG}

#EHA_Crypto_02

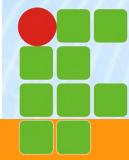
Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



Como anda?

- Primeira “Temporada” iniciada em Agosto/2017
 - **Categorias:** Criptografia, Networking, Forensics e Miscelaneous.
- Recesso (desde Dezembro/2017);
- Retorno (finalização da temporada) em Junho/2018;
- **Novidades para a “Segunda Temporada” (Julho/2018):**
 - Ranking por Categoria;
 - Novas Categorias.



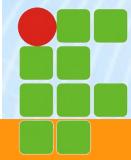
Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUps

- **Resolução detalhada de Desafios CTF**
- **Periodicidade Quinzenal (ou após resolução de desafios);**
- **Apresentação Ao Vivo (Youtube/Hangout);**
- **Disponibilização (Editada) de alguns WriteUps no Canal Youtube.**



Ethical Hacker Academy

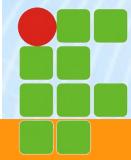
Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_01

Baixe o arquivo (link abaixo) e boa sorte em seu primeiro desafio...

<https://www.eha.net.br/desafios/77f7fc620b1d9ddbcd140c60ded0395711cc188d123aa4a12fc48b645935b2b7>



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



EHA/IFRN
Ambiente CTF

usuário
Senha

WriteUp #EHA_Crypto_01

Pontos importantes do Desafio!!!

#EHA_Crypto_01

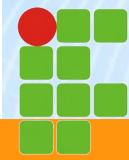


Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_01



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



EHA/IFRN
Ambiente CTF

usuário

Senha

Acessar

WriteUp #EHA_Crypto_01

Keypad



7352 236 84636

7 (4 vezes) = "S"

3 (2 vezes) = "E"

5 (1 vez) = "J"

2 (1 vez) = "A"

2 (2 vezes) = "B"

3 (2 vezes) = "E"

6 (1 vez) = "M"

8 (3 vezes) = "V"

4 (3 vezes) = "I"

6 (2 vezes) = "N"

3 (1 vez) = "D"

6 (3 vezes) = "O"

FLAG:

eha{SEJA BEM VINDO }



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



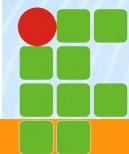
WriteUp #EHA_Crypto_01

Baixe o arquivo (link abaixo) e boa sorte em seu primeiro desafio...

<https://www.eha.net.br/desafios/77f7fc620b1d9ddbcd140c60ded0395711cc188d123aa4a12fc48b645935b2b7>



<https://www.youtube.com/watch?v=5e-1hxssSosU>



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_05

Puxa... Não pare na primeira... siga adiante até a FLAG ;)

Baixe o arquivo e mãos à obra...

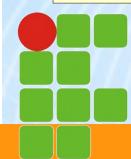
<http://www.eha.net.br/desafios/2f964946c2c3498ac74b9910f03cc31cbbab9fa03c73707425f1f048a12ae9cc>

```
# file 2f964946c2c3498ac74b9910f03cc31cbbab9fa03c73707425f1f048a12ae9cc
2f964946c2c3498ac74b9910f03cc31cbbab9fa03c73707425f1f048a12ae9cc: JPEG image data,
JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline,
precision 8, 626x577, frames 3
```

Um arquivo de imagem JPG!!!

Vamos renomear para facilitar...

```
# mv 2f964946c2c3498ac74b9910f03cc31cbbab9fa03c73707425f1f048a12ae9cc 05.jpg
```



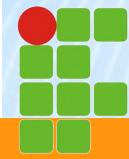
WriteUp #EHA_Crypto_05

Conteúdo do Arquivo:

Sabe a capital do país que tem esta bandeira?



Pergunte ao Google, ué?



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_05

Pesquisa Google Seguro | https://www.google.com/search?tbs=sbi:AMhZZit_1zzaDiXLg2ZFjj9c_1IMPPd4ZNBlnPfY2Npjvi9m74xYVcTtUwY41TWnc7N_1ElawaEwwcpI4C

Google 05.jpg zambia flag

Todas **Imagens** Maps Shopping Mais Configurações Ferramentas Fazer login

Aproximadamente 2 resultados (1,29 segundos)

Tamanho da imagem: 626 × 577
Não foram encontrados outros tamanhos desta imagem.

Melhor sugestão para esta imagem: [zambia flag](#)

Flag of Zambia - Wikipedia
https://en.wikipedia.org/wiki/Flag_of_Zambia Traduzir esta página
The flag of Zambia is the national flag of Zambia. It was adopted upon independence on October 24, 1964. Before that, Zambia was the British protectorate of ...

The Flag of Zambia
www.africa.upenn.edu/Country_Specific/Zamflag.html Traduzir esta página
THE FLAG OF ZAMBIA, hoisted for the first time at midnight, 23rd October, 1964, symbolizes patriotism and the nation's wealth. Its basic color is green with an ...

Imagens visualmente semelhantes

ZÂMBIA!!!

Qual a Capital???
Pergunte de novo!!!



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_05

Pesquisa por Capital da Zâmbia Google:

capital da zâmbia - F X Seguro | https://www.google.com.br/search?dcr=0&source=hp&q=capital+da+zâmbia&oq=capital+da+zâmbia

Google capital da zâmbia

Todas Maps Imagens Notícias Shopping Mais Configurações Ferramentas

Aproximadamente 61.700.000 resultados (0,59 segundos)

Zâmbia / Capital

Lusaka

Mwembeshi Barlaston Park Lusaka Silver Rest Chongwe

Nampundwe Chilanga Map data ©2017 Google

Mais sobre Lusaka

Zâmbia – Wikipédia, a encyclopédia livre
https://pt.wikipedia.org/wiki/Zâmbia

A Zâmbia (em inglês: Zambia [IPA: /'zæmbɪə/]), oficialmente conhecida como República da Zâmbia, é um país localizado no sudeste da África. Sua capital é Lusaka, localizada no sudeste do país. Em 24 de ...

Capital: Lusaka Independência: do Reino Unido
Cidade mais populosa: Lusaka Língua oficial: Inglês

Lusaka - Wikipedia
https://pt.wikipedia.org/wiki/Lusaka

Lusaka ou Lusaca é a capital e maior cidade da Zâmbia. É também a sede da província de Lusaka e do distrito de Lusaka. Lusaka está situada ao sul do país e ...

Lusaka

**Mas essa AINDA não
é a flag!!!**

Puxa... Não pare na primeira...
siga adiante até a FLAG ;)





usuário

Senha

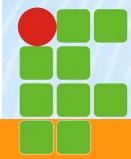
WriteUp #EHA_Crypto_05

Nós já usamos estenografia antes, não foi?

```
# steghide extract -sf 05.jpg
Enter passphrase: ←
wrote extracted data to
"0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557e1f".
```

Lusaka

*Novo arquivo que estava escondido na imagem...
Segue o Desafio!!!*



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_05

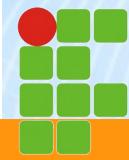
Qual o tipo do novo arquivo?

```
# file 0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557e1f  
0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557e1f: ASCII text
```

Um arquivo Texto!!!

```
# more 0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557e1f  
Q1poOTFBWSZTWeWsbCIAAZ7fgAAQAAj/4j///A///wYAb7fx1975e99vXz31b7jrvbevb31t5e  
+3m8Oniaan5GpiY0p6ZMIY0U9BiabCmFB1PyZMAU8ptPUMAExHhA0AJqRCfk2SU8mzU1MwjaGhia  
TTT0mp+pmpppPJBLTfqemkMJtE2hpiKbEGmKb1MmjaEmpjKemjAMFHqYQaajZHpqYA1Mk8FBVU/NM  
mhqY1PaaYJ6CGaQ00jGJmmio52+fdMcGEoAi4CYfIyUuek0mzaaUSU6INVxWKeiRDEymdWW1037  
(...)  
CwNF5zPBPytlamTPgBXqL01+fHM24v6K6RRQaGIgXb08pqyXmz8mad0xH1E7EMJ8XfdNiw0cvL3v  
f+TaZBok7PvP71O/ZWsaqAe0Gdjs0AKsJSDx3Egwze9fHJ4ntJSaeotbreRfvR6W0t0ZaSWxngnk  
x0bN8BBLh31H9Ai084ogTcfGMWYIQwTq4cD2a7VeLqkYME/hdyRThQkOWsbCIA==
```

**Codificado
(BASE64)?**



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



EHA/IFRN
Ambiente CTF

usuário
Senha

Acessar

WriteUp #EHA_Crypto_05

Decodificando usando BASE64:

```
# base64 -d 0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557elf > temp
# file temp
temp: bzip2 compressed data, block size = 900k
```

Descompactando com BZIP2:

```
# mv temp arquivo.bz2
# bunzip2 arquivo.bz2
# ls
05.jpg 0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557elf arquivo
```

Qual o tipo do novo arquivo?

```
# file arquivo
arquivo: ASCII text
```





usuário
Senha

Acessar

WriteUp #EHA_Crypto_05

Vamos olhar o conteúdo do novo arquivo:

```
# more arquivo
H4sICP6HyVkJAAz11Y2M1Y2ZhODBiN2VmZDE4YzkxODM4Y2FjZmRiNjdiZDg5Njc5ODMzOGVhM2U4
ZDUzYmY1MWY4ZTMwMzU0N2UApZV7PBOMHsaXud/q5H7fMpNqoTXbXDYq171ZuSRkrnNbyS20qJhy
1xK5L8okt8MWw8itMLSRCi+K0CvOOF6JJvbWOZ/zz/18z1/neT7P8/z3+/35PYcDioCAABJwPds
NC7htSyGLg4AgGUBAEuAJgBN9PdH+Af6ooz8kMTAAGOU9oYBUF5+/oHBviZIP0CUGgTJBOfh67
(...)
oN1Q3e97I8bx8zkhVeZzw/GzCTUh/OJrvTCmkQzXJUSE/kMWNnJLs+P1TfhkvypOa9dXXoA9tXXs
fCkyLXeuudKUegUbC5JNs3p7h2YuxJ/D7RPRBv4vQKoC/qOKxF/9/+NS7N+4/C9UnsOJif+6v+-n
7/5cHY1fj/8CPA/yG7sHAAA=
```

Codificado
(BASE64)?
De Novo?

Um arquivo compactado
com GZIP!!!

```
# base64 -d arquivo > arquivo2
# file arquivo2
arquivo2: gzip compressed data, was
"9ecc5cfa80b7efd18c91838cacfdb67bd896798338ea3e8d53bf51f8e303547", last modified:
Mon Sep 25 19:49:34 2017, from Unix
```

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

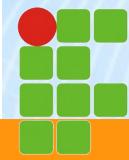


WriteUp #EHA_Crypto_05

Vamos descompactar então com GZIP:

```
# mv arquivo2 arquivo2.gz
# gunzip arquivo2.gz
# ls
05.jpg  0d895ea3296638b84a1b3e63a8106a3051f2e5ef1448abf129501d048a557elf  arquivo
arquivo2
# file arquivo2
arquivo2: Zip archive data, at least v2.0 to extract
```

Não pare... Agora temos um arquivo ZIP!!!



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



WriteUp #EHA_Crypto_05

Descompactando o arquivo ZIP:

```
# mv arquivo2 arquivo3.zip
# unzip arquivo3.zip
Archive: arquivo3.zip
inflating: 9ecc5cfa80b7efd18c91838cacfdb67bd896798338ea3e8d53bf51f8e303547e
# file 9ecc5cfa80b7efd18c91838cacfdb67bd896798338ea3e8d53bf51f8e303547e
9ecc5cfa80b7efd18c91838cacfdb67bd896798338ea3e8d53bf51f8e303547e: PNG image data, 500
x 500, 8-bit/color RGBA, non-interlaced
```

Ufa!!! Uma Imagem PNG!!!

```
# mv 9ecc5cfa80b7efd18c91838cacfdb67bd896798338ea3e8d53bf51f8e303547e imagem.png
```

Qual o conteúdo dessa imagem???



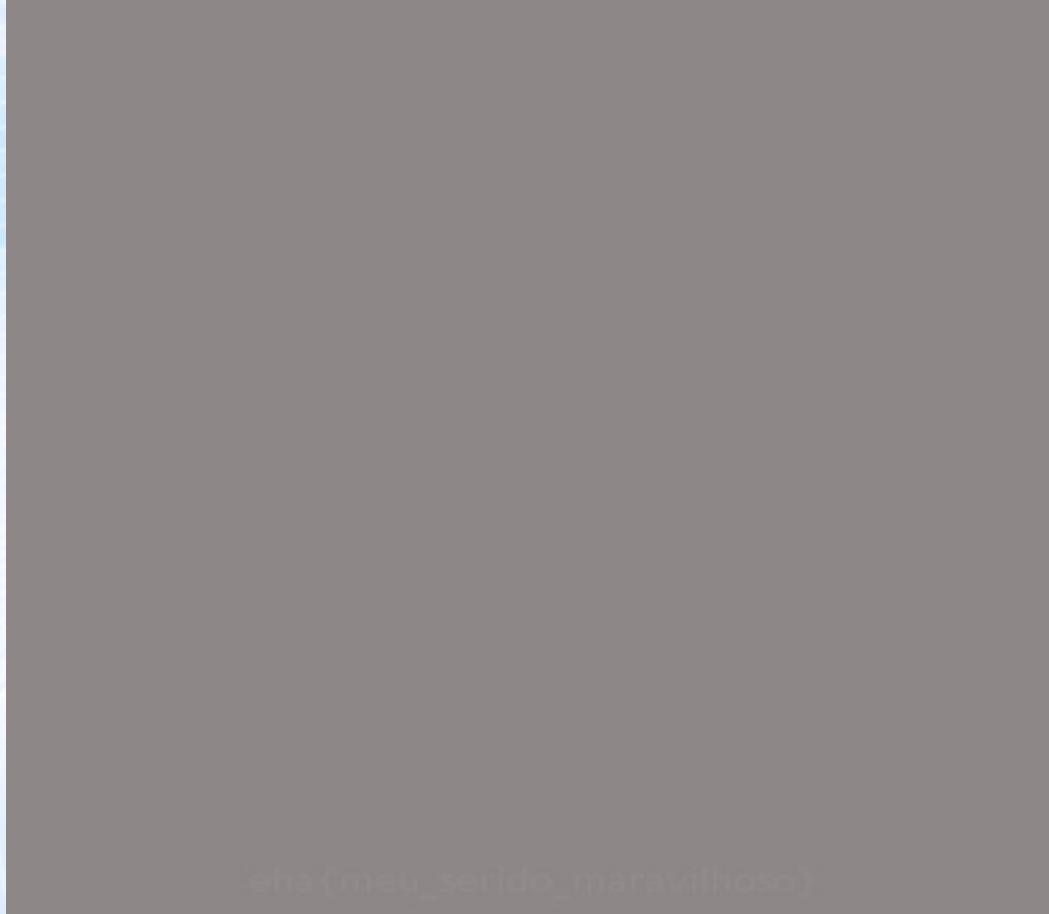
Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

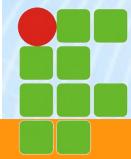


WriteUp #EHA_Crypto_05

Conteúdo da Imagem PNG:



?????

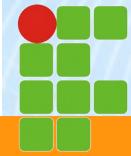
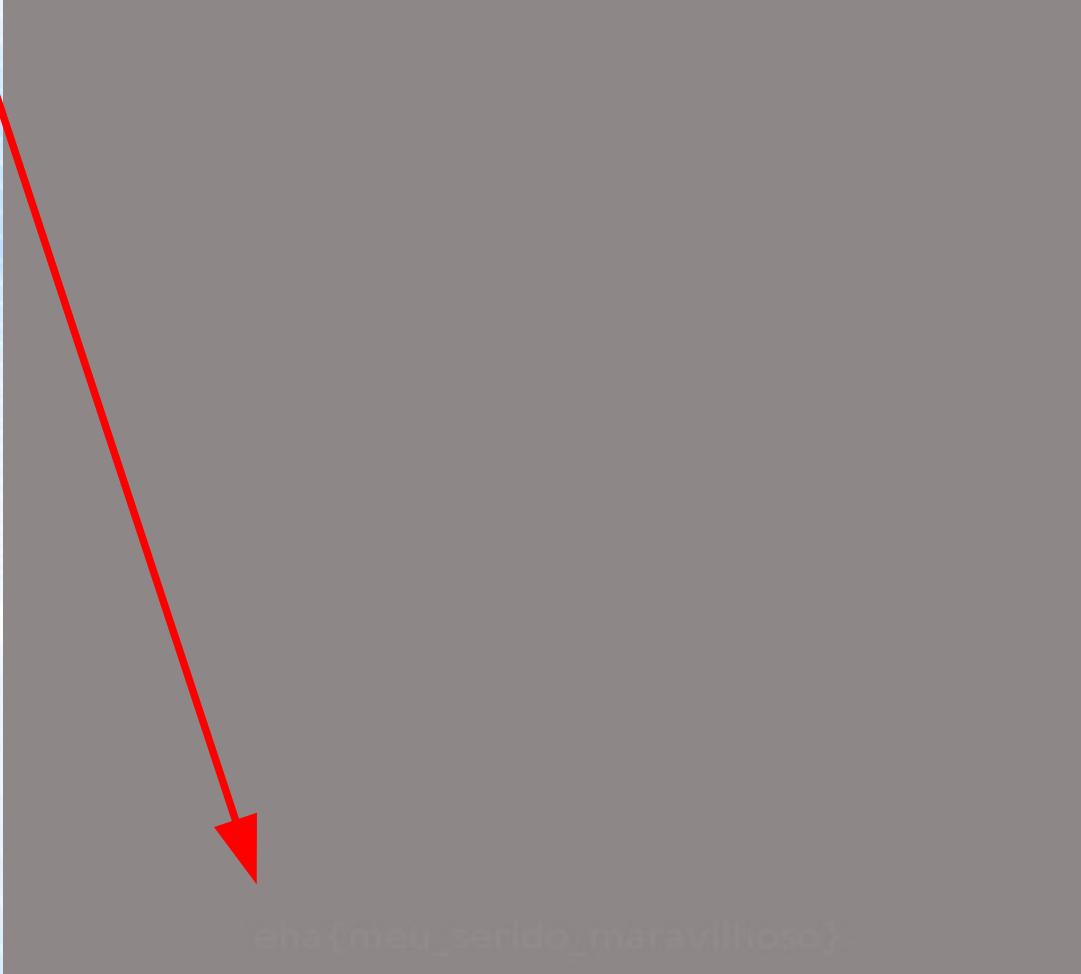


Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Crypto_05

Olhem ATENTAMENTE:



Ethical Hacker Academy

Ambiente CTF (Capture The Flag)



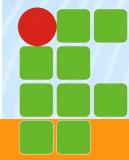
WriteUp #EHA_Crypto_05

Ampliando...



A **FLAG!!!**

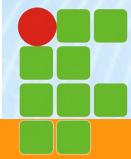
eha{meu_serido_maravilhoso}





Links de Referência

- **CTF-BR.ORG**
 - <https://ctf-br.org>
- **ShellterLabs**
 - <https://shellterlabs.com>
- **CTFTIME.ORG**
 - <https://ctftime.org>





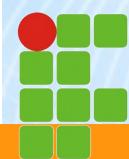
O que vem por aí (2018.2)

- Cursos Presenciais e EaD (gratuitos) para iniciantes:
 - Área: Sistemas Operacionais e Redes de Computadores
 - Introdução ao Sistema Operacional Linux (60h : 80h/a)
 - Área: Segurança da Informação
 - Introdução ao Ethical Hacking (60h : 80h/a)
 - Introdução a Computação Forense (60h : 80h/a)



PPCs aprovados e oferta autorizada IFRN/CN

<https://diaccn.ifrn.edu.br/fic>





O que (ainda) vem por aí (Planejamento)

- Cursos Presenciais e EaD (gratuitos) intermediários/avançados:
 - Área: Sistemas Operacionais e Redes de Computadores
 - Introdução à Programação com Shell Script (60h : 80h/a)
 - Administração de Redes com Linux (60h : 80h/a)
 - Gerência de Redes com Linux (60h : 80h/a)
 - Programação para Web com Linux (60h : 80h/a)
 - VPNs com Linux (60h : 80h/a)
 - Proxies com Linux (60h : 80h/a)
 - Área: Segurança da Informação
 - Firewalls com Linux (60h : 80h/a)
 - Sistemas de Detecção de Intrusões com Linux (60h : 80h/a)
 - Análise Forense em Redes de Computadores (60h : 80h/a)
 - Análise Forense em Memória (60h : 80h/a)



<https://diaccn.ifrn.edu.br/fic>



Ethical Hacker Academy

Atividades da Academia



<https://diaccn.ifrn.edu.br/fic>



INSTITUTO FEDERAL
Rio Grande do Norte
Campus Currais Novos

Catálogo de Cursos Disponíveis para Oferta na Modalidade
Formação Inicial e Continuada
<https://diaccn.ifrn.edu.br/fic>

Início

Cursos FIC Disponíveis para Oferta na Modalidade EaD (Ensino à Distância)

- Área: Sistemas Operacionais e Redes de Computadores
 - [Introdução ao Sistema Operacional Linux \(60h : 80h/a\)](#)
- Área: Segurança da Informação
 - [Introdução ao Ethical Hacking \(60h : 80h/a\)](#)
 - [Introdução a Computação Forense \(60h : 80h/a\)](#)

Cursos FIC Disponíveis para Oferta na Modalidade Presencial

- Área: Sistemas Operacionais e Redes de Computadores
 - [Introdução ao Sistema Operacional Linux \(60h : 80h/a\)](#)
 - [Introdução à Programação com Shell Script \(60h : 80h/a\)](#)
 - [Administração de Redes com Linux \(60h : 80h/a\)](#)
 - [Gerência de Redes com Linux \(60h : 80h/a\)](#)
 - [Programação para Web com Linux \(60h : 80h/a\)](#)
 - [VPNs com Linux \(60h : 80h/a\)](#)
 - [Proxies com Linux \(60h : 80h/a\)](#)
- Área: Segurança da Informação
 - [Introdução ao Ethical Hacking \(60h : 80h/a\)](#)
 - [Introdução à Computação Forense \(60h : 80h/a\)](#)
 - [Firewalls com Linux \(60h : 80h/a\)](#)
 - [Sistemas de Detecção de Intrusões com Linux \(60h : 80h/a\)](#)
 - [Análise Forense em Redes de Computadores \(60h : 80h/a\)](#)
 - [Análise Forense em Memória \(60h : 80h/a\)](#)

Pesquisar ...

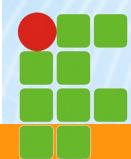
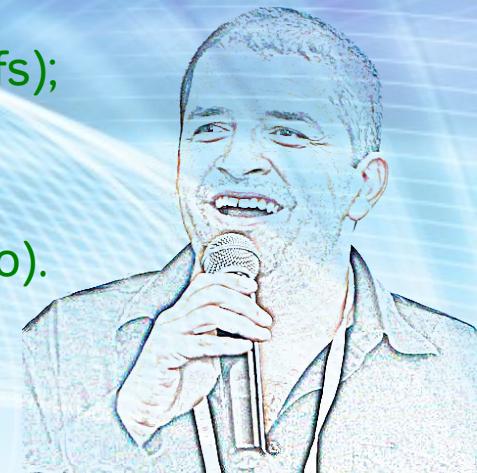
LINKS ÚTEIS

- [Portal IFRN](#)
- [Website Câmpus CN](#)
- [SUAP \(Sist.Acadêmico\)](#)
- [Biblioteca \(SIABI\)](#)
- [Docentes IFRN](#)
- [Calendário Acadêmico](#)



O que (ainda) vem por aí (Planejamento)

- Pós-Graduação Lato Sensu (SemiPresencial)
 - Área: Segurança da Informação
- Situação (atual):
 - Demais eixos do câmpus já iniciaram ofertas de pós-graduação;
 - Modelo semipresencial autorizado para pós-graduação em alimentos;
 - Corpo docente multicampi (novo conceito);
 - Estabilização de docentes (diminuição de ritmo da expansão dos Ifs);
 - Curso de Graduação (TSI) do câmpus com Conceito 5;
 - Maioria do corpo docente com mestrado (concluindo doutoramento).

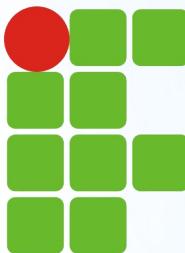




Perguntas !?

Informações Complementares !?





INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE



EHA/IFRN: Ethical Hacker Academy

Hacking com Responsabilidade



ricardokleber@ricardokleber.com



www.segurancaderedes.com.br



www.youtube.com/segurancaderedes



Florianópolis/SC – 24 de Maio de 2018