CTF: Capture The Flag

no Ensino de Segurança em Ambiente Controlado

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

Salvador/BA – 03 de Outubro de 2018

Ethical Hacker Academy

Histórico do Projeto

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!

Ethical Hacker Academy

Apresentação da Academia

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.**

Ethical Hacker Academy

Apresentação da Academia

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)

Ethical Hacker Academy

Atividades da Academia

O que já foi realizado?

- Cursos (Presenciais) para alunos e servidores do IFRN;
- Cursos (Presencias) 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).

Ethical Hacker Academy

Atividades da Academia

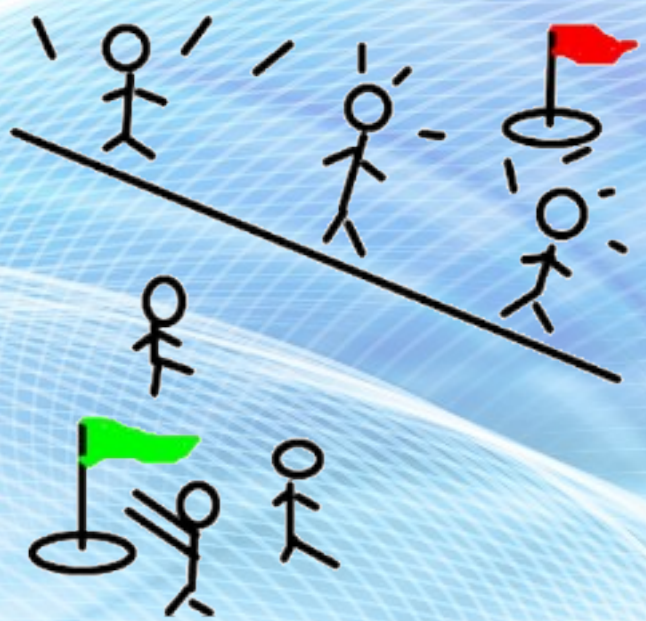
O que há de novo (2ª Fase)

- Exercitando segurança, na prática, em ambiente controlado

Ethical Hacker Academy

CTF: Ensino de Segurança em Ambiente Controlado

O que é?



CTF: Capture The Flag

Ensino de Segurança em Ambiente Controlado

O que é?

https://ctf-br.org/sobre

- No âmbito da informática, são competições que envolvem diversas competências dos profissionais/estudantes/entusiastas para a resolução de desafios relacionados à infosec (segurança da informação), com o objetivo de capturar a bandeira (normalmente um código) e pontuar.

Tipos:

- Attack/Defense: de forma genérica, as equipes recebem uma VM com diversos serviços (alguns vulneráveis), e o objetivo é capturar as bandeiras alheias e proteger as do seu time com patchs.
- Jeopardy-style: são apresentadas questões de diversas categorias, níveis de dificuldade e pontuações. As categorias variam de competição pra competição.

CTF: Capture The Flag

Ensino de Segurança em Ambiente Controlado

Jeopardy-Style : Principais Categorias

- Crypto (Criptografia)
- Forensics (Computação Forense)
- Networking (Redes)
- Miscellaneous (Diversos)
- Trivias (Triviais)
- Reversing (Eng. Reversa)
- Web Hacking
- Pwnables/Exploitation (Exploração de binários)
- PPC (Professional Programming and Coding)

https://ctftime.org/ctf-wtf

Ethical Hacker Academy

Atividades da Academia :: 2ª Fase

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 ≥ 7,0 → Cadastramento na “Plataforma CTF”

Ethical Hacker Academy

Atividades da Academia :: 2ª Fase

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

Painel

Seguro | https://acesso.eha.net.br/my/

Adriano

EHA/IFRN Módulo de Acesso

Página inicial

Personalizar esta página

AVISOS undefined

Navegação

Painel

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

Usuário autenticado

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

Ethical Hacker Academy

Módulo de Acesso

Curso: Módulo de A

Seguro | https://acesso.eha.net.br/course/view.php?id=2

Adriano

Página inicial | Este curso

> Meus cursos > Módulo de Acesso EHA/IFRN

Navegação

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

Avaliação do Módulo de Acesso

Clique para iniciar a avaliação (60 minutos)

Ethical Hacker Academy

Módulo de Acesso

Módulo de Acesso E

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

Adriano

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

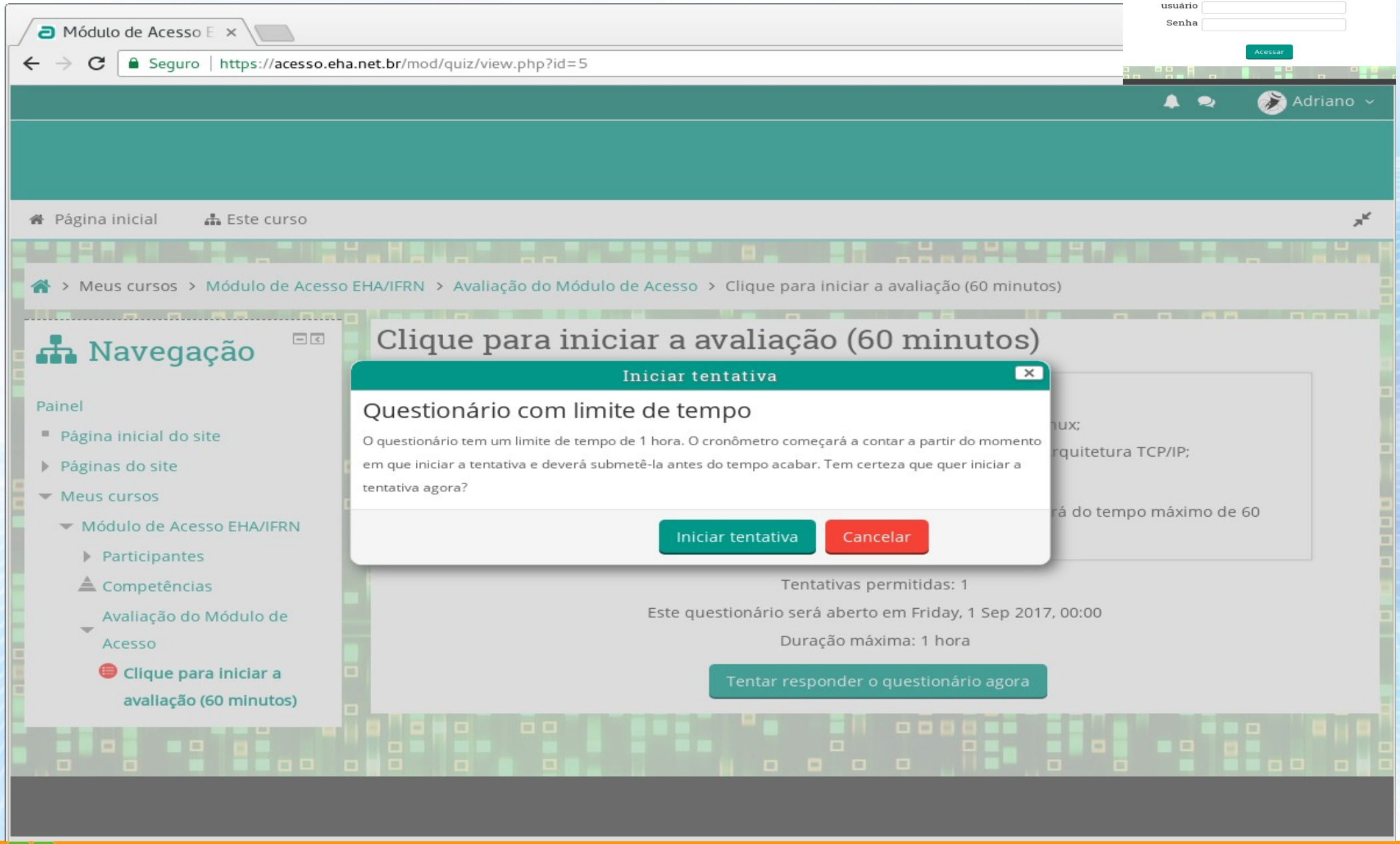
Este questionário será aberto em Friday, 1 Sep 2017, 00:00

Duração máxima: 1 hora

Tentar responder o questionário agora

Ethical Hacker Academy

Módulo de Acesso



Ethical Hacker Academy

Módulo de Acesso

Clique para iniciar a

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

Adriano

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

Finalizar tentativa ...

Tempo restante 0:59:48

Questão 1

Ainda não respondida

Vale 1 ponto(s).

Marcar questão

Escolha uma:

a.

b.

c.

d.

Próxima página

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

Painel

Seguro | https://ctf.eha.net.br/my/

Rubens

EHA/IFRN :: Ambiente CTF

Página inicial | Painel | Eventos | Meus desafios | Personalizar esta página

AVISOS undefined

Ranking

Ranking EHA/IFRN (07/10/2017)

Navegação

Painel

- Página inicial do site
- Páginas do site
- Desafios

Usuário autenticado

Rubens Kurl
País: Brasil
Cidade/Município: GTERGTS/NIC.BR
rubens@amigodeadriano.com.br

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

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

Seu progresso

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/77f7fc620b1d9ddbcd140c60ded039571lcc188d123aa4a12fc48b645935b2b7URL`

- **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" Agosto/2017 → Setembro/2018**
  - **Categorias: Criptography, Networking, Forensics e Miscelaneous.**

WriteUps

- **Resolução detalhada de Desafios CTF**
  - **Apresentações 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)

WriteUp #EHA_Crypto_01

Pontos importantes do Desafio!!!

#EHA_Crypto_01

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Crypto_01

Keypad

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Crypto_01

7352 236 84636

Keypad

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-1hxsSosU

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

Puxa... Meu pendrive deu pau... Sumiu tudo...

Tudo o que tenho está nesse arquivo:

```
https://www.eha.net.br/desafios/44298e64779fa6b973063418d05ec0432a7ee9e07d644fb7b20c0bccb9963967
```

Será que você encontra a FLAG assim mesmo?

Nível: Básico

Pontuação: 100 pontos (primeiro a acertar) || 10 pontos (participantes que acertarem posteriormente)

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

```
# file 44298e64779fa6b973063418d05ec0432a7ee9e07d644fb7b20c0bccb9963967
44298e64779fa6b973063418d05ec0432a7ee9e07d644fb7b20c0bccb9963967: Zip archive data,
at least v2.0 to extract
```

Um Zip (Compactado)

Vamos renomear para facilitar e, em seguida, tentar descompactar

```
# mv 44298e64779fa6b973063418d05ec0432a7ee9e07d644fb7b20c0bccb9963967 forensics_01.zip
# unzip forensics_01.zip
Archive:  forensics_01.zip
  inflating: c6ddd86ce44d6ecfda60da0749693c4f3eb408a550b65d673a0c95e7f00b5891
```

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

```
# file c6ddd86ce44d6ecfda60da0749693c4f3eb408a550b65d673a0c95e7f00b5891
c6ddd86ce44d6ecfda60da0749693c4f3eb408a550b65d673a0c95e7f00b5891: DOS/MBR boot
sector, code offset 0x3c+2, OEM-ID "mkfs.fat", sectors/cluster 4, root entries 512,
sectors 40960 (volumes <=32 MB) , Media descriptor 0xf8, sectors/FAT 40,
sectors/track 62, heads 62, hidden sectors 2048, serial number 0x2e9c4fbf, label:
"EHA_IFRN   ", FAT (16 bit)
```

A Imagem de uma Partição FAT

Vamos renomear para facilitar...

```
# mv c6ddd86ce44d6ecfda60da0749693c4f3eb408a550b65d673a0c95e7f00b5891 imagem.raw
```

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

Vamos utilizar uma ferramenta de forense para tentar ver o conteúdo:

```
# fls imagem.raw
r/r 3:    EHA_IFRN     (Volume Label Entry)
r/r * 9:  0b60cfc10f4f72f02caff8a1d6fa264c21349fb19c1f2d2eb13ce49fd1e7525e
r/r * 15:2fbf650fccabec995b53b6090185dd4d75475dcd724593bc268a77353fcdee40
r/r * 21:652dfa6b8e8aa5bb3344b4788304de762a64111f2023b964f60f5569c297563b
r/r * 27:6a333b30d8204a026c832a4b281efd12f0e3a20d06da779dfc06961243a1e637
r/r * 33:bfda50f578acbc5cbaf3a084e8e72921ae111414d20b55d122e75b14fce6499c
r/r * 39:c3f608066dd51693dcef6c424d85a13f8cf1639880bfc6ee9ab22fa180e136b9
r/r * 45:e61aca44e6cba84a35ac26966400538b5a091a1ff9a5c2bee8ac8820f116f9b9
r/r * 51:f45a285f0fc6d20e40c633d53e79234c2e9668730ffec8b329a046c2221f4113
v/v 654067:   $MBR
v/v 654068:   $FAT1
v/v 654069:   $FAT2
d/d 654070:   $OrphanFiles
```

Arquivos Apagados

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

Compreendendo a saída do comando fls (SleuthKit)

```
# fls imagem.raw
(...)

r/r * 9:    0b60cfc10f4f72f02caff8a1d6fa264c21349fb19c1f2d2eb13ce49fd1e7525e

(...)
```

Número do I-Node

Nome (original)
do arquivo apagado

"Asterisco"
Indica que é um arquivo
que foi apagado

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

Utilizando o icat (também do Sleuthkit) para recuperar arquivos

```
icat [arquivo_imagem] [número_do_inode] > arq_saída
```

```
# icat imagem.raw 9  > 0b60cfc10f4f72f02caff8a1d6fa264c21349fb19c1f2d2eb13ce49fd1e7525e
# icat imagem.raw 15 > 2fbf650fccabec995b53b6090185dd4d75475dcd724593bc268a77353fcdee40
# icat imagem.raw 21 > 652dfa6b8e8aa5bb3344b4788304de762a64111f2023b964f60f5569c297563b
# icat imagem.raw 27 > 6a333b30d8204a026c832a4b281efd12f0e3a20d06da779dfc06961243a1e637
# icat imagem.raw 33 > bfda50f578acbc5cbaf3a084e8e72921ae111414d20b55d122e75b14fce6499c
# icat imagem.raw 39 > c3f608066dd51693dcef6c424d85a13f8cf1639880bfc6ee9ab22fa180e136b9
# icat imagem.raw 45 > e61aca44e6cba84a35ac26966400538b5a091a1ff9a5c2bee8ac8820f116f9b9
# icat imagem.raw 51 > f45a285f0fc6d20e40c633d53e79234c2e9668730ffec8b329a046c2221f4113
```

Para muitos arquivos a ferramenta "Testdisk" é mais rápida

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

Verificando os tipos de arquivos recuperados:

```
# file *
0b60cfc10f4f72f02caff8a1d6fa264c21349fb19c1f2d2eb13ce49fd1e7525e: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
2fbf650fccabec995b53b6090185dd4d75475dcd724593bc268a77353fcdee40: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
652dfa6b8e8aa5bb3344b4788304de762a64111f2023b964f60f5569c297563b: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
6a333b30d8204a026c832a4b281efd12f0e3a20d06da779dfc06961243a1e637: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
bfda50f578acbc5cbaf3a084e8e72921ae111414d20b55d122e75b14fce6499c: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
c3f608066dd51693dcef6c424d85a13f8cf1639880bfc6ee9ab22fa180e136b9: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
e61aca44e6cba84a35ac26966400538b5a091a1ff9a5c2bee8ac8820f116f9b9: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
f45a285f0fc6d20e40c633d53e79234c2e9668730ffec8b329a046c2221f4113: PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
```

Todos (os 8 arquivos) eram arquivos de imagem (PNG)

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

0b60cfc10f4f72f02caff8a1d6fa264c21349fb19c1f2d2eb13ce49fd1e7525e

70,6 kB

2fbf650fccabec995b53b6090185dd4d75475dcd724593bc268a77353fcdee40

200,3 kB

6a333b30d8204a026c832a4b281efd12f0e3a20d06da779dfc06961243a1e637

71,8 kB

652dfa6b8e8aa5bb3344b4788304de762a64111f2023b964f60f5569c297563b

186,9 kB

bfda50f578acbc5cbaf3a084e8e72921ae111414d20b55d122e75b14fce6499c

79,0 kB

c3f608066dd51693dcef6c424d85a13f8cf1639880bfc6ee9ab22fa180e136b9

130,7 kB

e61aca44e6cba84a35ac26966400538b5a091a1ff9a5c2bee8ac8820f116f9b9

154,2 kB

f45a285f0fc6d20e40c633d53e79234c2e9668730ffec8b329a046c2221f4113

145,9 kB

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Forensics_01

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Networking_01

Ataque no dia da Independência?

Um Malware (conhecido) fez sondagens ao servidor da EHA/IFRN logo no dia da Independência do Brasil (07/09/2017)!!!

Vamos usar isso para aprender...

Baixe o arquivo (link abaixo) com os logs do servidor web e descubra/informe (na forma de flag, claro) qual O NOME desse Malware:

```
https://www.eha.net.br/desafios/26bb8f743f7b89153ce412e4212dc3a939b0e1a526f9cd0f2ea832103d018872
```

Nível: Básico

Pontuação: 50 pontos (primeiro a acertar) || 05 pontos (participantes que acertarem posteriormente)

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Networking_01

```
# file 26bb8f743f7b89153ce412e4212dc3a939b0e1a526f9cd0f2ea832103d018872
26bb8f743f7b89153ce412e4212dc3a939b0e1a526f9cd0f2ea832103d018872: ASCII text
```

Uma arquivo Texto (Deve ser, mesmo, um arquivo de LOG)

Vamos renomear para facilitar...

```
# mv 26bb8f743f7b89153ce412e4212dc3a939b0e1a526f9cd0f2ea832103d018872 access.log
```

Quantas Linhas?

```
#  wc -l access.log
231 access.log
```

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Networking_01

Vamos ver as primeiras linhas para identificar o formato dos LOGS:

```
# head -10 access.log
66.249.66.25 - - [07/Sep/2017:07:07:13 -0300] "GET / HTTP/1.1" 200 8279 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X
Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)"
46.17.46.8 - - [07/Sep/2017:07:13:17 -0300] "\x16\x03\x01" 400 0 "-" "-"
46.17.46.8 - - [07/Sep/2017:07:13:18 -0300] "GET /vtigercrm/vtigerservice.php HTTP/1.1" 404 485 "-" "libwww-perl/6.26"
66.249.66.25 - - [07/Sep/2017:08:27:58 -0300] "GET / HTTP/1.1" 200 8279 "-" "Mozilla/5.0 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)"
66.249.76.55 - - [07/Sep/2017:09:22:02 -0300] "GET / HTTP/1.1" 200 8279 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X
Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)"
38.142.119.130 - - [07/Sep/2017:09:22:09 -0300] "GET / HTTP/1.1" 400 2972 "-" "-"
86.105.212.20 - - [07/Sep/2017:09:26:14 -0300] "GET /xmlrpc.php HTTP/1.1" 405 219 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-
US; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6"
86.105.212.20 - - [07/Sep/2017:09:26:14 -0300] "GET /feed/ HTTP/1.0" 404 463 "-" "-"
66.249.76.56 - - [07/Sep/2017:09:27:03 -0300] "GET / HTTP/1.1" 200 8279 "-" "Mozilla/5.0 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)"
180.76.15.18 - - [07/Sep/2017:09:55:01 -0300] "GET /robots.txt HTTP/1.1" 404 464 "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2)
Gecko/20100101 Firefox/6.0.2"
```

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Networking_01

Observando os logs é fácil perceber o IP que mais se repete...

```
# cat access.log | sort | more
120.25.199.116 - - [08/Sep/2017:02:17:32 -0300] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 404 467 "-" "-"
120.25.199.116 - - [08/Sep/2017:02:17:42 -0300] "GET /pma/scripts/setup.php HTTP/1.1" 404 460 "-" "-"
120.25.199.116 - - [08/Sep/2017:02:17:52 -0300] "GET /myadmin/scripts/setup.php HTTP/1.1" 404 464 "-" "-"
120.75.22.175 - - [07/Sep/2017:17:26:15 -0300] "HEAD http://178.79.189.235:80/mysql/admin/ HTTP/1.1" 404 196 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:15 -0300] "HEAD http://178.79.189.235:80/mysql/dbadmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:15 -0300] "HEAD http://178.79.189.235:80/mysql/sqlmanager/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:16 -0300] "HEAD http://178.79.189.235:80/mysql/mysqlmanager/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:16 -0300] "HEAD http://178.79.189.235:80/phpmyadmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:16 -0300] "HEAD http://178.79.189.235:80/phpMyadmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:16 -0300] "HEAD http://178.79.189.235:80/phpMyAdmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:17 -0300] "HEAD http://178.79.189.235:80/phpmyadmin2/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:17 -0300] "HEAD http://178.79.189.235:80/phpmyadmin3/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:17 -0300] "HEAD http://178.79.189.235:80/phpmyadmin4/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:17 -0300] "HEAD http://178.79.189.235:80/phpmyAdmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:18 -0300] "HEAD http://178.79.189.235:80/2phpmyadmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:18 -0300] "HEAD http://178.79.189.235:80/myadmin/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:18 -0300] "HEAD http://178.79.189.235:80/phpmy/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
120.75.22.175 - - [07/Sep/2017:17:26:18 -0300] "HEAD http://178.79.189.235:80/phppma/ HTTP/1.1" 404 195 "-" "Mozilla/5.0 Jorgee"
(...)
```

... e o "agente" utilizado para as sondagens!!!

Ethical Hacker Academy

Ambiente CTF (Capture The Flag)

WriteUp #EHA_Networking_01

```
120.75.22.175 - - [07/Sep/2017:17:26:15 -0300] "HEAD http://178.79.189.235:80/mysql/admin/ HTTP/1.1" 404 196 "-" "Mozilla/5.0 Jorgee"
(...)
```

Um Malware (conhecido) fez sondagens ao servidor da EHA/IFRN logo no dia da Independência do Brasil (07/09/2017)!!!

Vamos usar isso para aprender...

Baixe o arquivo (link abaixo) com os logs do servidor web e descubra/informe (na forma de flag, claro) qual O NOME desse Malware:

eha{Jorgee}

http://sipadcg.org/jorgee
https://fortiguard.com/encyclopedia/ips/44308
https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=30164

Links de Referência

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

Ethical Hacker Academy

Atividades da Academia

O que vem por aí

- 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

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 do RN
Câmpus Currais Novos

Ricardo Kléber

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

CTF: Capture The Flag

no Ensino de Segurança em Ambiente Controlado

ricardokleber@ricardokleber.com.br

www.segurancaderedes.com.br

www.youtube.com/segurancaderedes

ETHICAL HACKER ACADEMY

Salvador/BA – 03 de Outubro de 2018