

DESEC

INFORMATION SECURITY



MANUAL DO ALUNO



MANUAL DO ALUNO

Este manual vai te guiar por todas plataformas que fornecemos aos alunos, explicando o que é cada plataforma, como usar e como concluir o treinamento.

DESEC ACADEMY é nossa plataforma de aulas, onde o aluno consome conteúdo das aulas, tem fórum para dúvidas, baixa modelos de documentos, realiza atividades e envia tarefas para avaliação.

The screenshot shows the DESEC Academy homepage with a chalkboard background. At the top, it says "DESEC ACADEMY" and "Dsec Academy - Information Security". It also says "You are not logged in. (Log in)". Below the header, there's a quote: "Nós não vendemos produtos, nós vendemos experiência" - Ricardo Longatto. The page is divided into four main sections:

- 01 EXPERTISE**: Descrição: "DESEC revolucionou o mercado de treinamentos no Brasil. Somos diferentes e estamos sempre inovando, o que nos torna líder no mercado. A DESEC não vende produtos, nós vendemos experiência." Botões: "read more"
- 02 VLAB**: Descrição: "Virtual Lab é nossa nova plataforma de complemento de estudo, onde o aluno através de uma série de tarefas práticas deve comprovar seu conhecimento técnico aprendido em nossos treinamentos." Botões: "read more"
- 03 Dsec Hacker Challenge**: Descrição: "DHC é nossa plataforma de competição onde os competidores são submetidos a vários desafios técnicos e quem resolve primeiro vence. A DESEC é organizadora oficial do Hack4k4." Botões: "read more"
- 04 Ambientes Realísticos**: Descrição: "Com nosso ambiente realístico você consegue comprometer um sistema externo, fazer pivoting para outro host, até comprometer a rede interna que não estava exposta diretamente à internet." Botões: "read more"

Ao ser aceito no curso você recebe os dados de acesso, use o seguinte link para acessar o ambiente.

<http://www.desec.com.br/academy/login/index.php>

The screenshot shows the "Log in" page of the DESEC Academy. It has a "Username" field containing "ricardolongatto" and a "Password" field with masked input. There are checkboxes for "Remember username" and "Forgotten your username or password?". A "Log in" button is at the bottom. The background features a chalkboard with various diagrams and text.

Após efetuar o login você deve escolher Treinamento Pentest Profissional.

TREINAMENTO PENTEST PROFISSIONAL

Professor: Ricardo Longatto

TREINAMENTO PENTEST PROFISSIONAL

Deseec Academy - Information Security

Página principal / Treinamento Pentest Profissional

Ranking Academy

O seu progresso

Ranking dos melhores alunos.

Information - View the ladder

Progress Bar

Progress: 9%

Mouse over or touch bar for info.

Navegação

- Página principal
- Painel do utilizador
- Páginas do site
- Disciplina atual
- Treinamento Pentest Profissional**
 - Participantes
 - Medalhas
 - Geral

Fórum Notícias

Fórum - Informe sobre problemas técnicos

Este fórum serve para reportar possíveis erros encontrados ao submeter exercícios, realizar quizzes, resolver desafios no vlab etc.

SEJA BEM VINDO

Bem Vindo - Treinamento Pentest Profissional

Módulo 01 - Introdução

Fórum Módulo 01 - Introdução

Aula 01 - Introdução à Segurança da Informação

Aula 02 - Introdução ao Pentest

Aula 03 - Carreira em Pentest

Aula 04 - Preparação - Conduzindo um pentest

Modelos de Propostas e Contratos

Modelo de contrato

No canto esquerdo nós temos o Ranking que conforme você avança na plataforma vai ganhando mais pontos e medalhas e logo abaixo temos uma barra de progresso.

Ranking Academy

Ranking dos melhores alunos.

Information - View the ladder

Progress Bar

Progress: 8%

Mouse over or touch bar for info.

No corpo do Academy temos o curso completo com todos os módulos, fórum, modelos de documentos, exercícios e tarefas.

Para assistir as aulas basta clicar na aula que deseja assistir

Aula 01 - Introdução a Segurança da Informação

Aula 02 - Introdução ao Pentest

Aula 03 - Carreira em Pentest

Aula 04 - Preparação - Conduzindo um pentest

Aula 01 - Introdução a Segurança da Informação

The screenshot shows a video player interface. At the top, it displays 'mod1' and 'from Ricardo Longatto'. Below that, the word 'Exemplo' is overlaid. The main content area shows a computer screen with the 'Event Viewer' application open. The logs show multiple 'Information' events related to logon attempts, with one specific event highlighted where the 'Account Name' is 'petter'. A red bracket groups several log entries. To the right of the Event Viewer, there is a video frame of a man with glasses and a dark shirt, identified as Ricardo Longatto. A blue rectangular box with white text overlays the video frame, stating 'Servidor TS sofrendo ataque de força bruta 40 minutos após conectar na internet.' (Server TS suffering a brute force attack 40 minutes after connecting to the internet). The video player has a play button, a timestamp of '13:00', and an 'HD' indicator.

Cada módulo conta com um fórum específico para aquele módulo.

Fórum Modulo 01 - Introdução

Basta clicar em ***criar um novo tópico*** para postar uma dúvida ou clicar em um tópico existente para responder a uma postagem.

Tópico	Iniciado por	Respostas	Última mensagem
PCI-DSS no PenTest.	Ricardo Leopoldo	2	Eduardo Barros · Sex, 24 Jun 2016, 03:35
Certificação	Augusto Gusmão	4	Eduardo Barros · Sex, 24 Jun 2016, 03:07
Certificação, validade e quando realizar.	Ricardo Leopoldo	7	Eduardo Barros · Qui, 23 Jun 2016, 00:34
Relatório de Entrega	Eduardo Berto	5	Jeyson · Seg, 16 Mai 2016, 19:40
Certificações iniciais em Pentest	Alexandre Topeca	4	Jeyson · Seg, 16 Mai 2016, 17:57

Alguns módulos possuem arquivos e modelos de documentos e para baixar basta clicar no documento/arquivo.

 Modelo de contrato

 Modelo de Proposta comercial

 Modelo de NDA

 Modelo de NDA2

Alguns módulos possuem **quizzes** onde você deve responder algumas questões relacionadas ao que foi ensinado em aula.

 Quiz - Módulo 02

Basta selecionar a resposta que considera correta e clicar em **SUBMETER** logo em seguida clique em **SEGUINTE**

Pergunta 1

Por responder

Nota de 3,00

 Marcar
pergunta

 Editar
pergunta

Qual o comando é utilizado no Kali Linux, para iniciar um serviço apache?

Selecione uma opção de resposta:

- a. service apache stop
- b. apache + start
- c. cat apache start
- d. service apache2 start

Submeter

Seguinte

Preste atenção que os **quizzes** possuem um limite de tempo, então só clique em iniciar se estiver preparado.

1 **2** **3**

Terminar tentativa

Tempo restante **0:03:42**

Após terminar de responder clique em **SUBMETER TUDO E TERMINAR**

Submeter tudo e terminar

Logo em seguida você tem o feedback e o resultado.

Pré-visualizar	Terminada	10,00	Parabéns isso mostra que você está progredindo bem em nosso curso.
	Submetido Quarta, 13 Julho 2016, 11:29		

OBS: Preste atenção pois você tem apenas 2 tentativas, limite de tempo e a nota válida é a da última tentativa.

Quiz - Módulo 02

Tentativas permitidas: 2

Tempo limite: 5 minutos

Método de avaliação: Última tentativa

Síntese das tentativas anteriores

Tentativa	Estado	Nota / 10,00	Rever	Feedback
1	Terminada Submetido Sábado, 18 Junho 2016, 14:16	5,00	Não é permitido	
2	Terminada Submetido Sábado, 18 Junho 2016, 14:17	8,67	Não é permitido	Parabéns isso mostra que você está progredindo bem em nosso curso.

A sua nota final do teste é 8,67/10,00.

Feedback global

Parabéns isso mostra que você está progredindo bem em nosso curso.

Não são permitidas mais tentativas

Alguns módulos possuem tarefas obrigatórias que devem ser entregues, estas tarefas são avaliadas e interferem na nota final.

Tarefa - Módulo 03

Tarefa - Módulo 03

Objetivo desse exercício, é criar um script em bash que automatize o parsing em sites, e que funcione várias vezes seguidas com sites diferentes.

Estado do trabalho

Número da tentativa	Esta é a tentativa 1.
Estado da submissão	Nenhuma tentativa
Estado da avaliação	Sem avaliação
Última alteração	Segunda, 11 Julho 2016, 14:49
Comentários à submissão	» Comentários (0)

Enviar trabalho

Para enviar uma tarefa clique em **ENVIAR TRABALHO**

Tarefa - Módulo 03

Objetivo desse exercício, é criar um script em bash que automatize o parsing em sites, e que funcione várias vezes seguidas com sites diferentes.



Nesta tela clique em e em seguida em Enviar Ficheiro

Na próxima tela clique em **Choose File** e selecione o seu arquivo em seguida clique em **Enviar este ficheiro**.

This screenshot shows a file upload form. It includes fields for 'Anexo' (Attachment) with a 'Choose File' button (which has 'No file chosen' displayed), 'Gravar como' (Save as) with an empty input field, 'Autor' (Author) with the value 'Joao da silva sauro', and 'Escolher licença' (Select license) with a dropdown menu showing 'Todos os direitos reservados.' (All rights reserved.). At the bottom is a large 'Enviar este ficheiro' (Send this file) button.

Selecione **GUARDAR ALTERAÇÕES**



Nesta tela você ainda pode alterar ou reenviar o trabalho feito, assim que tiver certeza que esta tudo certo clique em **SUBMETER O TRABALHO**

Estado do trabalho

Número da tentativa	Esta é a tentativa 1.
Estado da submissão	Trabalho em curso (não submetido)
Estado da avaliação	Sem avaliação
Última alteração	Quarta, 13 Julho 2016, 11:37
Submissão de Ficheiros	 scriptmod3.sh
Comentários à submissão	 Comentários (0)
	Editar submissão
	Fazer alterações à sua submissão
	Submeter o trabalho

Assim que este trabalho for submetido não poderá fazer mais alterações.

Submeter o trabalho

Uma tela de confirmação irá surgir e você deve marcar a opção e clicar em **CONTINUAR**.

* This assignment is my own work, except where I have acknowledged the use of the works of other people.

Tem a certeza de que pretende submeter o seu trabalho para avaliação? Não poderá realizar mais alterações.

[Continuar](#) [Cancelar](#)

Ao terminar você vai ver uma tela do estado do trabalho **SUBMETIDO PARA AVALIAÇÃO**.

Estado do trabalho

Número da tentativa	Esta é a tentativa 1.
Estado da submissão	Submetido para avaliação
Estado da avaliação	Sem avaliação
Última alteração	Quarta, 13 Julho 2016, 11:38
Submissão de Ficheiros	 scriptmod3.sh
Comentários à submissão	 Comentários (0)

Basta aguardar que conforme os trabalhos são corrigidos sua nota é gerada no VLAB. Você pode prosseguir com o curso tranquilamente.

Em alguns módulos você vai ver uma mensagem como esta:

Esse módulo possui laboratórios no VLAB.

Que indica que este módulo tem laboratórios no VLAB, você deve ir para o VLAB para finalizar estes laboratórios antes de prosseguir com o curso.

VLAB - VIRTUAL LAB é nossa plataforma de laboratórios onde o aluno coloca em prática tudo que aprende em aula, alguns módulos do curso vão ter laboratórios que devem ser realizados no VLAB.

Quando você é aceito no treinamento você recebe um link para gerar sua senha do VLAB, após gerar sua senha você pode logar na plataforma.

<http://www.desec.com.br/vlab/login.php>

CURSO DE PENTEST PROFISSIONAL**Bem vindo ao Virtual Lab**

Faça seu login

E-mail:

Senha:

Após se autenticar você tem acesso a plataforma do VLAB.

Logado como: Ricardo Longatto | [sair](#) Pontuação Geral: 650 pontos Ranking Geral: 1º [+ Download da VPN](#)

Módulos Disponíveis:

Módulo03	Módulo04	Módulo05	Módulo06	Módulo07	Módulo08	Módulo10	Módulo14	Módulo15
Módulo16	Módulo17	Módulo18	Módulo19	Tarefas do Academy				

LAB1 LAB2 LAB3 LAB4 LAB5 LAB6

(*) CONCLUIDO

10 10 10 10 10 10

100,0%

No topo você tem informações sobre sua **pontuação, posição no ranking geral** e botão para fazer **download da VPN**.

Logado como: Ricardo Longatto | [sair](#) Pontuação Geral: 650 pontos Ranking Geral: 1º [+ Download da VPN](#)

Logo em seguida temos os módulos disponíveis no qual contém os laboratórios práticos do treinamento.

Módulos Disponíveis:

Módulo03	Módulo04	Módulo05	Módulo06	Módulo07	Módulo08	Módulo10	Módulo14	Módulo15
Módulo16	Módulo17	Módulo18	Módulo19	Tarefas do Academy				

Ao clicar no módulo podemos ver os laboratórios disponíveis para aquele módulo, o quadradinho na cor branca indica os laboratórios não realizados, os coloridos significam que já foi realizado, e no canto direito temos o progresso do modulo.



Ao clicar no quadradinho temos a descrição do desafio, como mostrado abaixo.

Virtual Lab

LAB2

Enumere o SMB e consiga a chave que esta dentro de key.txt

Servidor: 172.16.1.4

9+

OK

Neste caso o desafio pede para realizar a enumeração do SMB do host com IP 172.16.1.4, então você deve usar a VPN para acessar a rede e realizar o desafio.

Exemplo: Resolvendo o desafio e encontrando a key.txt

```
smb: \> ls
.
..
key.txt.txt

        40931 blocks of size 524288. 3
smb: \> get key.txt.txt
getting file \key.txt.txt of size 78 as key.txt
tes/sec)
smb: \> exit
root@kalicurso:~# cat key.txt.txt
MUITO BEM

PARA CONCLUIR USE A KEY PARA PONTUAR NO VLAB

KEY: 101001001010
```

Ao encontrar o código basta colocar o código encontrado e clicar em **OK**, se o código estiver incorreto você vai receber a seguinte mensagem

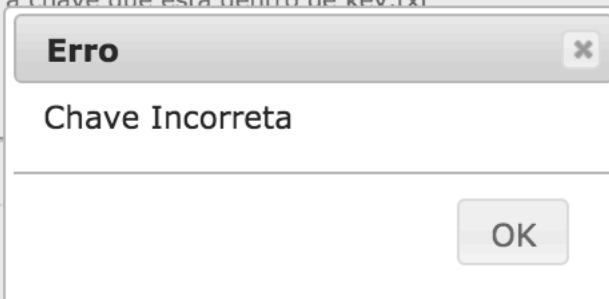
LAB2

Enumere o SMB e consiga a chave que esta dentro de key.txt

Servidor: 172.16.1.4

Entre com a chave

OK



Caso a resposta esteja correta o quadradinho fica colorido e a pontuação é atribuída

LAB1 LAB2 LAB3 LAB4 LAB5

10 10 10 10 10

(%) CONCLUÍDO

80,0%

Virtual Lab

LAB2

Enumere o SMB e consiga a chave que esta dentro de key.txt

Servidor: 172.16.1.4

 
OK

Como podemos ver abaixo, o desafio foi concluído

LAB1 LAB2 LAB3 LAB4 LAB5

10 10 10 10 10

(%) CONCLUÍDO

100,0%

RANKING GERAL

O ranking geral mostra sua posição perante aos outros alunos, conforme você avança no VLAB vai pontuando e conquistando posições no RANKING.

Você pode verificar o ranking geral sempre que quiser no seguinte link

<http://www.desec.com.br/vlab/ranking-geral.php>

ALUNOS	PONTUAÇÃO
1º Ricardo Longatto [Teste]	650
2º raphael nascimento freitas	560
3º Felipe Oliveira Francisco	560
4º Juliano Ventola	560
5º Jeyson Donizete Basso	560
6º Vitor Bernades Aguiar	560
7º Kaique Redivo Bonato	530
8º João Paulo Ferreira	490
9º Romário Xavier Da Silva	490
10º Augusto Gusmão de Castro Toledo	480
11º Mario Marcio Soares Patriota	430
12º Pedro Henrique	402
13º Daniel da Silva Saibt	370
14º Anderson de Godoy	340
15º Jose Rogelio Gomes Junior	340
16º Leandro Inácio Santos de Carvalho	331
17º Rodrigo Ferreira de Melo	322
18º Daniel Nasciutti Abdala	320

Ao concluir todo o VLAB você terá uma **pontuação máxima de 560 pontos**, porém temos um Módulo chamado **TAREFAS DO ACADEMY**.

Tarefas do Academy

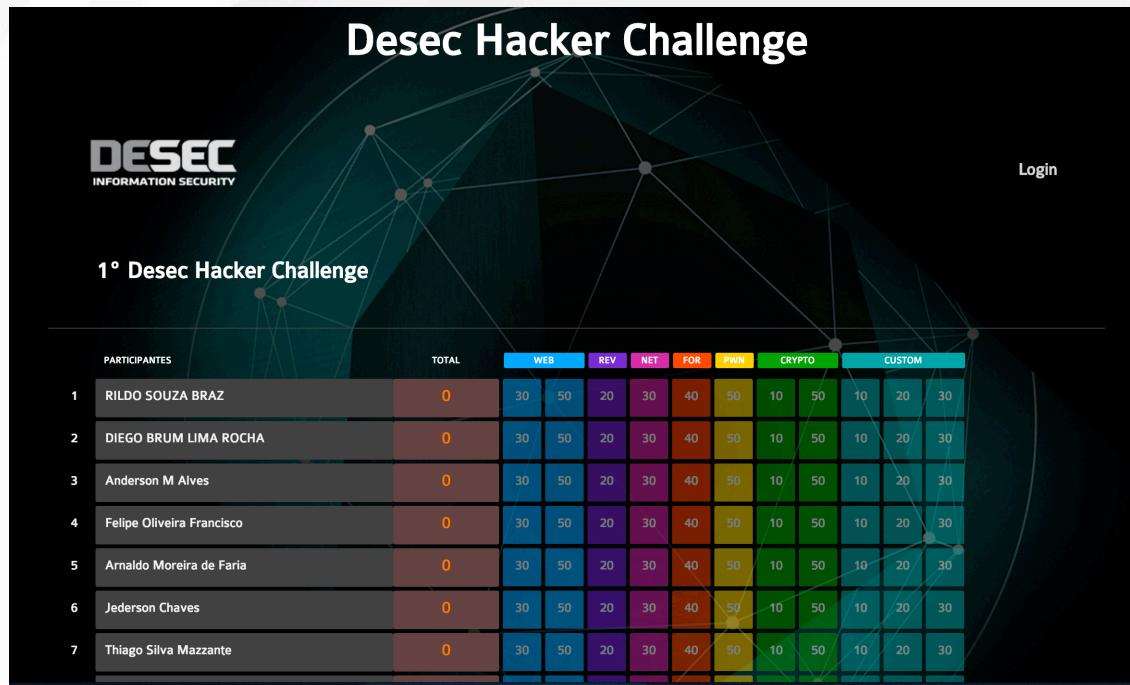
Este módulo refere-se as tarefas exigidas no Academy (Plataforma de aulas), então todas tarefas submetidas no Academy para avaliação são avaliadas com notas de 10 a 100 e essas notas que vão diferenciar o ranking final.

No exemplo abaixo a tarefa submetida no Academy no módulo 3 (MOD3) passou por avaliação e teve nota máxima de 100, já as outras atividades ainda não foram corrigidas.



Com isso você consegue saber quando suas tarefas do Academy foram corrigidas e qual foi sua nota.

DHC – DESEC HACKER CHALLENGE é nossa plataforma de *Capture The Flag*, basicamente um campeonato hacking de invasão de sistemas criado apenas para os alunos do curso de Pentest.



O usuário e senha para se autenticar são os mesmos do VLAB.



O DHC ocorre de tempos em tempos e todos são avisados por mensagem no Academy/E-mail e grupo no face.

O vencedor geralmente ganha prêmios, tais como, livros, mais tempo de acesso a VPN etc. Além de receber um certificado que venceu o campeonato para exibir no currículo.

VPN

A VPN fornece acesso a uma rede de estudo no qual conta com diversos hosts, servidores Windows e Linux, aplicações web etc.

A VPN fica disponível para download no VLAB

Para instalar a VPN você pode seguir a **aula 12 do módulo 02**

Resumo:

No seu Linux certifique-se que tenha o **OPENVPN** instalado e descompacte o arquivo dentro de **/etc/openvpn/**

```
tar xvf seuarquivovpn.tar -C /etc/openvpn/
```

Em seguida inicie o serviço do OPENVPN

```
service openvpn start
```

Após uns 5 segundos execute um ifconfig para ver se a interface tap subiu e pegou um IP no range 172.20.0.X que tem rota para 172.16.1.0/24

```
tap0      Link encap:Ethernet  HWaddr 72:0b:1d:04:8b:83
          inet addr:172.20.0.2  Bcast:172.20.255.255  Mask:255.255.0.0
          inet6 addr: fe80::700b:1dff:fe04:8b83/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:25 errors:0 dropped:0 overruns:0 frame:0
             TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:100
             RX bytes:3845 (3.7 KiB)  TX bytes:12390 (12.0 KiB)

root@kalicurso:/tmp# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
default         192.168.16.2   0.0.0.0       UG    0      0      0 eth0
172.16.1.0     172.20.0.1    255.255.255.0  UG    0      0      0 tap0
```

REDE VPN DE ESTUDO

172.16.1.0/24

Tempo de acesso: O tempo de acesso da VPN é de 3 meses contado a partir da data da compra do curso. Após isso você pode comprar um tempo adicional.

**Ao terminar o acesso à VPN,
você pode contratar períodos adicionais.**

Planos para VPN Adicional

- 30 dias - R\$ 150
- 60 dias - R\$ 280
- 90 dias - R\$ 390

Contratar VPN Adicional

Ambiente Realístico Online é uma infra online para ataques reais, ou seja, você consegue fazer um ataque completo através da internet.

Tudo que fornecemos de informação é o domínio de teste

www.grandbusiness.com.br

VM OFFLINE – Maquinas Virtuais OFFLINE

Fornecemos algumas maquinas virtuais que são essências para o estudo durante o treinamento, se você tem a VPN não irá precisar das VM OFFLINE, mas caso sua VPN tenha expirado e você não quiser comprar um plano adicional, pode baixar as VM OFFLINE e instalar usando VMWare ou Virtual Box.

As VM ficam disponíveis para download no Academy.

 VM utilizada no módulo 10

 VM metasploitable2 com firewall

 VM Web SQLI

 VM WEB LFI

 VM WEB postgree

Suporte e Grupo

Caso necessite de suporte você pode usar o suporte via Fórum ou através de E-mail.

Via Fórum:

No ACADEMY existe um fórum para cada módulo, basta escolher o módulo no qual tem dúvida e criar um novo tópico. Nossa equipe ou os próprios colegas do curso vão ajudar com as dúvidas.

Através de E-mail:

Basta enviar um e-mail para suporte@pentestprofissional.com.br com a dúvida, sempre que puder envie um printscreen e detalhes sobre o problema, isso agiliza na hora de responder.

Grupo no Facebook

Entre para o grupo exclusivo do curso no facebook, teremos um chat com todos os alunos cadastrados.

<https://www.facebook.com/groups/703721316436551/>

CERTIFICADO

A DESEC entrou no mercado com a proposta de revolucionar o mercado de treinamento especializado, com base nisso a DESEC não dá certificado para ninguém. Você precisa **CONQUISTAR** seu certificado.

Para obter nosso certificado com validação on site você precisa:

- Assistir todas as aulas do Academy
- Realizar todos os laboratórios do VLAB
- Passar em todos os QUIZZES do Academy
- Entregar todas as tarefas do Academy com nota superior a 70%

Para validar seu certificado online acesse

<http://www.desec.com.br/certificate-authentication/>

DESEC
INFORMATION SECURITY

Expertise em Segurança da Informação

CURSO DE PENTEST PROFISSIONAL

Validação de Certificado

Informe a chave de segurança

DIGITE A CHAVE DE SEGURANÇA

6ct5ky

DIGITE O CÓDIGO ACIMA

VALIDAR CERTIFICADO

* A chave de segurança é impressa no Certificado de Conclusão de Curso

Digite a chave de validação e o captcha, caso o certificado seja valido você vai ver o certificado.

