# PROJETO PEDAGÓGICO

| INSTITUIÇÃO DE ENSINO | |
|---|---|
| NOME: | CURSOS VIRTUAIS LTDA |
| CNPJ: | 08.179.401/0001-62 |
| REGISTRO ABED: | 7734 - CATEGORIA INSTITUCIONAL |

| CURSO | |
|---|---|
| NOME: | HACKER E SEGURANÇA |
| MODALIDADE: | EAD - APERFEIÇOAMENTO / LIVRE OFERTA |

**Metodologia:** O conteúdo do curso é disponibilizado ao aluno para estudo online em uma interface diagramada de fácil navegação chamada de Sala de Aula Virtual. O acesso ao material é bastante intuitivo e proporciona uma experiência de interatividade no processo de aprendizagem a distância.

**Sincronicidade:** O curso é caracterizado como síncrono, a partir do momento da matrícula, com a indicação por parte do aluno, da data que iniciará, tendo em vista que passa a ter data de início e término definidas. As aulas/módulos de estudo são disponibilizados de forma gradual, sendo necessário que o aluno complete os estudos de um módulo para prosseguir para o módulo seguinte no período de estudos programado.

**Tutoria e Formas de Interação:** Os alunos recebem suporte de uma tutoria especificamente designada. A interação é realizada por meio do sistema de Sala de Aula Virtual. A tutoria consiste na assistência didática, compartilhamento de informações, troca de experiências visando o melhor aproveitamento dos conteúdos estudados.

**Avaliação final/Certificação:** A avaliação final é quantitativa. A geração do certificado é condicionada à verificação de aproveitamento mínimo de 70% (setenta por cento) nas atividades da avaliação final. O curso conta com ferramenta de avaliação de conteúdo (aprendizagem) correspondente à carga horária certificada.

**Organização curricular:** O curso apresenta organização curricular elaborada a partir de projetos pedagógicos específicos por uma equipe pedagógica multidisciplinar, que acompanha toda a concepção dos conteúdos.

**Tecnologia de EAD/e-learning:** Após a elaboração dos conteúdos é realizada a migração para a Sala de Aula Virtual, que é um ambiente de aprendizagem online otimizado para EAD.

**Materiais Didáticos:** O conteúdo programático é lastreado em materiais didáticos atualizados. Dentre as ferramentas de aprendizagem além do material de estudo estão a avaliação final, grupo de estudos com o tutor/professor e sistema de anotações sobre o curso.

**Interação e Suporte Administrativo:** O curso conta – além do suporte de tutoria - com uma infraestrutura de apoio que prevê a interação entre alunos e professores/tutores; e alunos e equipe de apoio administrativo. Essa interação é garantida por meios eletrônicos e/ou por meio telefônico, conforme o caso. A Sala de Aula Virtual utilizada pela CURSOS VIRTUAIS LTDA é uma plataforma proprietária, desenvolvida e atualizada permanentemente.

**Sobre a Instituição de Ensino:** A CURSOS VIRTUAIS LTDA é uma escola de educação à distância. Iniciamos nossas atividades em 2006 e contamos com mais de 500 mil alunos matriculados em diversos cursos. Além disso, somos associados da ABED - Associação Brasileira de Educação a Distância. Legalmente constituída inscrita no CNPJ 08.179.401/0001-62, atua com a idoneidade e credibilidade auxiliando diversos órgãos públicos e empresas privadas, além de milhares de profissionais, servidores públicos, estudantes e professores de todo o país.

**ESTRUTURA DO CURSO - COMPONENTES CURRICULARES**

**NOME DA CAPACITAÇÃO:** Hacker e Segurança

**OBJETIVO DE APRENDIZAGEM:** Proporcionar ao aluno uma visão abrangente sobre os temas do conteúdo programático. Melhorar as competências específicas do curso e desenvolver habilidades de pensamento crítico e analítico acerca do tema estudado.

**CONTEÚDO PROGRAMÁTICO:**
Introdução à segurança da informação
O que é segurança?
Padrões/Normas
Por que precisamos de segurança?
Princípios básicos da segurança da informação
Ameaças e ataques
Mecanismos de segurança
Serviços de segurança
Certificações
War Games
Introdução ao Teste de Invasão
Visão geral sobre o Pentest
Tipos de Pentest
As fases de um ataque
Categorias de ataques
Metodologias existentes
Como conduzir um teste de invasão
Aspectos Legais
Google Hacking
Comandos Avançados do Google
Google Hacking Database
Levantamento de informações
Contramedidas
Footprint
Consulta a informações de domínio
Consultando servidores DNS
Consultando websites antigos
Webspiders
Netcraft
Buscando relacionamentos
Rastreamento de E-mails
Fingerprint
O que é Engenharia Social?
Tipos de Engenharia Social
Engenharia Social Reversa
No Tech Hacking
Varreduras Internet Control Messages Protocol (ICMP)
Varreduras TCP
Nmap
Métodos de Varredura
Tunelamento
Anonymizer
Enumeração de informações
Aquisição de banners
Mapeando graficamente a rede
Descobrindo Vulnerabilidades
Definindo vetores de ataque
Testando o sistema
O que é negação de serviço?
DDoS

DoS
Principais tipos de ataques
Sequestro de Sessão
Backdoor
Cavalo de Tróia ou Trojan Horse
Rootkits
Vírus e worms
Netcat
Keylogger
Ignorando Proteções
Evasão de Firewall/IDS com Nmap
Firewall Tester
Detectando Honeypots
Técnicas de Força Bruta
Wordlist
John The Ripper
THC-Hydra
BruteSSH2
Rainbow Crack
Utilizando o Rainbow Crack para criação de Rainbow Tables
Vulnerabilidades em aplicações web
Entendendo a aplicação web
Principais Classes de Vulnerabilidades
Apagando Rastros
Por que encobrir rastros?
Técnicas de Sniffing
O que é um sniffer?
Arp Spoof
Principais protocolos vulneráveis a sniffer
DNS Pharming
Ataques a Servidores WEB
Descobrindo Vulnerabilidades com Nikto
Ataques a Redes Sem Fio
Wardriving
Ataques ao protocolo WEP
SSID Oculto
MAC Spoofing
WPA Brute Force
WPA Rainbow Tables
Rougue Access Point
Wifi Phishing
Exploits
Mas afinal, o que é um exploit?
Organização dos Processos na Memória
Shellcode
Buffer Overflow
Segurança na Internet
Senhas
O que não se deve usar numa elaboração de senha
Com que frequência devo mudar minhas senhas
Certificado digital
O que é autoridade certificadora?
Vulnerabilidades
Como um vírus pode afetar um computador
Vírus propagado por e-mail
Vírus de macro
WORM
Backdoors
Como é feita a inclusão de um backdoor em um computador
Como um cavalo de tróia pode ser diferenciado de um vírus
Negação de serviço (Denial of service)

Segurança:Banda larga e redes sem fio
Quais são os riscos de uso de banda larga
O que fazer para proteger uma rede conectada
Quais são os riscos do uso de redes wireless
Como funcionam os exploits
Exemplo de exploit baseado no buffer overflow
Descrição do programa vulnerável
Técnicas para evitar vulnerabilidades
Tomando Controle de Programas Vulneráveis
Organização dos processos em memória
Buffer overflow e ataques envolvidos
Código arbitrário
Vírus Uma Ameaça Global
Principais tipos de vírus
Aprenda Mais Sobre DdoS
Desmistificando o ataque
Ferramentas Ddos
Como se prevenir
Definições de segurança
Analisando o nível de perigo
Protocolos
Ferramentas TCP/IP
Footprinting
Trojans
Denial of Service
Sniffers
Scanners
Criptografia
Crackeando
Anonimidade
Firewall
Códigos-fonte
Técnicas avançadas