PROJETO PEDAGÓGICO

INSTITUIÇÃO DE ENSINO	
RAZÃO SOCIAL:	CURSOS VIRTUAIS LTDA
NOME FANTASIA:	CURSOSVIRTUAIS.NET
CNPJ:	08.179.401/0001-62
REGISTRO ABED:	7734 - CATEGORIA INSTITUCIONAL

CURSO	
NOME:	CIBERSEGURANÇA
MODALIDADE:	CAPACITAÇÃO LIVRE OFERTA - EAD

Metodologia: O conteúdo do curso é disponibilizado ao aluno para estudo online em uma interface diagramada de fácil navegação AVA (Ambiente Virtual de Estudos). O acesso ao material é bastante intuitivo e proporciona uma experiência de interatividade no processo de aprendizagem a distância. O curso conta com a realização de atividade avaliativa ao término de cada aula/módulo e também realização da prova final.

Formato: O curso é ofertado de forma assíncrona e conta com atividades complementares síncronas, permitindo que o aluno organize seus estudos conforme sua disponibilidade. Os módulos de aprendizado são liberados de maneira assíncrona e progressiva, sendo necessário concluir cada etapa para avançar à seguinte. Complementarmente, o curso conta com atividade síncrona por meio do suporte em tempo real com o professor, disponível às terças e quintas-feiras, das 15h às 16h, na ferramenta de tira-dúvidas.

Tutoria e Formas de Interação: Os alunos recebem suporte de uma tutoria especificamente designada. A interação é realizada por meio do da Área do Aluno, no Ambiente Virtual de Estudos (AVA). A tutoria consiste na assistência didática, compartilhamento de informações, troca de experiências visando o melhor aproveitamento dos conteúdos estudados.

Prova final/Certificação: A prova final é quantitativa. A geração do certificado é condicionada à verificação de aproveitamento mínimo de 70% (setenta por cento) na prova 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 o ambiente de estudos na área do aluno, que é um AVA otimizado para nossa plataforma de ensino.

Materiais Didáticos: O conteúdo programático é lastreado em materiais didáticos atualizados. Dentre as ferramentas de aprendizagem além do material de estudo estão a prova final, grupo de estudos com o tutor/professor, e atividades atividade avaliativas sobre cada aula do 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. O Ambiente Virtual de Estudos (AVA) utilizado 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: Cibersegurança

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.

ATIVIDADES/AULAS:
1) Cibersegurança
2) Segurança em Redes de Computadores
3) Segurança de Dados
4) Testes de Invasão
5) Levantamento de Informações
6) Varreduras e Testes
7) Vírus, Trojans, Rootkits e Afins
8) Técnicas de Força Bruta
9) Ataques a Servidores Web
10) Ataques a Redes
11) Exploits

CONTEÚDO PROGRAMÁTICO DETALHADO:
A importância da segurança da informação
As ameaças cibernéticas
Engenharia social
Malwares
Tipos de ataque
Roubo de credenciais
Phishing e spear phishing
Segurança digital
Práticas recomendadas de segurança
Autenticação de dois fatores
Senhas seguras
Dispositivos e redes seguras
Atualizações e patches de segurança
Redes públicas e privadas
Criptografia
Firewall e antivírus
Identificação e resposta a incidentes
Proteção de dados e LGPD
Boas práticas no ambiente de trabalho
Uso seguro de dispositivos pessoais e corporativos
Educação e conscientização
Classificação da informação
Princípios da segurança da informação
Sistema seguro
Técnica e gestão
Principais ameaças
Sala cofre
Monitoramento online
Mecanismos de autenticação
Biometria
Tipos de hacker
Principais tipos de ataques
Firewall
Firewall - função
Firewall - políticas
Firewall - mecanismos de filtragem
Firewall - stateful

UTM - unified threat management
Firewall - limitações
Netfilter/iptables
Tabela filter
Prerouting e postrouting
Comandos iptables
Listando as regras
Manipulando tabelas
Gravação em log
Exemplo de script iptables
Liberando forward
Incrementando o firewall
Mostrar e apagar regras
Firewall stateful
Política padrão do firewall
Bloquear e liberar portas
Bloqueios e permissões via multiport
Bloquear host por protocolo
Fazer mascaramento da rede
NAT e redirecionamento
Proxy transparente
Logs
O que é segurança da informação
Conceito de segurança da informação
Dados sensíveis
Tipos de dados
Processamento de dados
Finalidade do uso de dados
Anonimização
Medidas de segurança
Proteção de dados pessoais
Incidentes de segurança
Responsabilidades e boas práticas
Sanções administrativas
Compartilhamento de dados
Segurança em dispositivos móveis
Senhas e autenticação
Política de segurança
Conscientização e treinamento
A importância da governança de dados
Tipos de pentest
Blind
Double blind
Gray box
Double gray box
Tandem
Reversal
As fases de um ataque
Levantamento de informações
Varredura
Ganhando acesso
Mantendo acesso
Limpando rastros
Categorias de ataques
Server side attacks
Client side attacks
Metodologias existentes
Como conduzir um teste de invasão
Aspectos legais
O que deve conter no relatório
Google hacking

Comandos avançados do Google
Operadores básicos de sintaxe
Filtrar por local do termo
Restringir por domínio, tipo de arquivo ou imagem
Informações sobre a página ou domínio
Filtrar por data ou fonte
Atalhos temáticos e respostas instantâneas
Boas práticas rápidas
Google hacking database
Footprint
Consulta a informações de domínio
Consultando servidores DNS
Consultando websites antigos
Webspiders
SSL Labs
Buscando relacionamentos
Prática dirigida
Rastreamento de e-mails
Campos de rastreamento
Fingerprint
Fingerprint passivo
Fingerprint ativo
Descobrindo um sistema operacional usando ICMP
Calculando HOP
Fingerprint através do xprobe2
O que é engenharia social?
Tipos de engenharia social
Baseada em pessoas
Baseada em computadores
Formas de ataque
Insider attacks
Roubo de identidade
Phishing scam
URL obfuscation
Dumpster diving
Persuasão
Engenharia social reversa
No tech hacking
Varreduras ICMP
Varreduras TCP
Nmap
Métodos de varredura
Tunelamento
Anonymizer
Enumeração e informação de serviços
Aquisição de banners
Técnicas clássicas
Ferramentas
Dicas para uso efetivo
Mapeando graficamente a rede
Lanmap e Cheops
AutoScan
Descobrindo vulnerabilidades
Instalando o nessus (ubuntu/debian)
Registrando e iniciando
Definindo vetores de ataque
Negação de serviço (dos e ddos)
DDoS
Ferramentas de DDoS
Considerações éticas e legais
Boas práticas

Principais tipos de ataques de negação de serviço
Ping flood
SYN flood
Smurf attack
Recomendações
Sequestro de sessão (session hijacking)
Ferramentas recomendadas
Prática com ferramentas de hijacking
Contramedidas gerais contra DoS e hijacking
Backdoor
Cavalo de tróia ou trojan horse
Rootkits
User-land
Kernel-land
Vírus e worms
Netcat
Opções do netcat
Netcat – utilização
Encadeando netcats
Keylogger
Brute force
Wordlist
Download de wordlist
Geração de wordlist
John the Ripper
Arquivo de configuração
Seções comuns do john.conf
Modos de operação do JtR
Modo wordlist
Modo single crack
Modo incremental
Modo external
Comandos de uso na linha de comando
Exemplo prático
Módulos adicionais
Interface gráfica (GUI)
THC-Hydra
Protocolos suportados
Hydra com interface gráfica (xHydra)
Hydra via terminal
Ataque a formulários web com Hydra
Considerações finais
BruteSSH2
Rainbow Crack
Ferramentas relacionadas
Rainbow tables
Utilizando o RainbowCrack
Passo 1 - Gerando rainbow tables com rtgen
Passo 2 - Organizando as rainbow tables com rtsort
Passo 3 - Quebrando hashes com rcrack
Recomendações
Entendendo a aplicação web
Principais classes de vulnerabilidades
Command injection
SQL injection
Cross-site scripting (XSS)
CSRF
Insecure direct object reference
Falha de autenticação e gerenciamento de sessão
Insecure cryptographic storage
Failure to restrict URL access

Ferramentas para exploração
OWASP ZAP (Zed Attack Proxy)
Ataques a servidores web - DoS e DDoS
Fingerprint em web server
WhatWeb
httprecon
Nmap com NSE (Nmap Scripting Engine)
Wappalyzer
Online scanner
Security Headers
SSL Labs - SSL Test
Shodan
O que é um sniffer?
Como surgiu o sniffer?
CAM flooding com macof
ARP poisoning (ARP spoofing)
Principais protocolos vulneráveis a sniffers
Principais ferramentas
Dsniff
Ettercap
TCPDump
Wireshark
DNS pharming
Ataque DNS (DNS spoofing)
Contramedidas contra sniffers
Evasão de firewall/IDS com Nmap
Firewall tester (FTester)
Detectando honeypots
Contramedidas contra honeypots
Apagando rastros
Ferramentas úteis para apagar rastros
Contramedidas de proteção de logs
Ataques a redes sem fio
Wardriving
Ataques ao protocolo WEP
Passo a passo com Aircrack-ng (WEP)
SSID oculto
MAC spoofing
Ataque de força bruta em WPA
Tabelas rainbow para WPA
Rogue access point
Wi-Fi phishing
Contramedidas contra ataques wireless
O que é um exploit?
Fontes para estudo de exploits
Organização dos processos na memória
Estrutura da pilha (stack) na arquitetura Intel x86
Prólogo e epílogo de função
Shellcode
Exemplo de shellcode
Buffer overflow
Stack smashing e heap smashing
Exploração prática com código C vulnerável
Compilando e executando um exploit
Consequências de falhas de programação
Execução remota e controle do programa