Certificado

nº 5413284167542020608

Certificamos que **Thiago Miranda de Souza**, RG **441088**, matrícula nº **416754/541328**, concluiu o curso com carga horária de **440 horas**:

Cibersegurança

O curso foi concluído em **09/05/2020** com base legal na Constituição/88 Artigo 206º II, Artigo 209º, Lei nº 9.394/96, Decreto nº 5.154/2004 e Resolução CNE - MEC nº 04/99 Artigo 7º § 3º. O aluno obteve **aproveitamento de 66%** na prova aplicada ao final do curso.

Ibiúna/SP, 09 de maio de 2020

SOMOS ASSOCIADOS
ABED
ASSOCIAÇÃO BRASILEIRA DE EDUCAÇÃO A DISTÂNCIA

Thiago Miranda de Souza
Aluno(a)

Otávio Medeiros Dias
Professor Geral

Grade curricular:

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.

08.179.401/0001-62

CURSOS VIRTUAIS LTDA

Rua dos Caiçaras, S/N - QD 6 LT 10
Vale das Araucárias - CEP 18150-000
IBIUNA - SP

Registro nº 5413284167542020608 Livro 9-E Folha 54

Curso (modalidade EAD) com fundamento legal na Constituição Federal/88 Artigo 206º Inciso II e Artigo 209º, Lei nº 9.394/96, Decreto nº 5.154/2004 e Resolução CNE - MEC nº 04/99 Artigo 7º § 3º.