GOHACKING SECURITY ESSENTIALS

(GHSE)

GoHacking

CYBER SECURITY TRAININGS

NÍVEL INICIANTE

Carga Horária: 40hs

GoHacking

(GHSE)

Laios Barbosa

Cyber Security Specialist

Engenheiro de Computação pelo Instituto Militar de Engenharia (IME), Pós-graduado em Segurança da Informação e Instrutor de Defesa Cibernética e Pentesting nas Forças Armadas (desde 2011). Foi instrutor do SANS Institute, um dos mais renomados centros de treinamento de cybersecurity do mundo.

Detentor de uma das Certificações Internacionais em Segurança Cibernéticas mais desejadas e reconhecidas no cenário mundial, a SANS GIAC Security Expert (GSE), Analista Nr 291.

Atualmente, trabalhando como Incident Handler e Gestor de Segurança da Informação, possui mais de 15 anos de experiência em administração de redes e sistemas, tratamento de incidentes e segurança ofensiva.

Participou ativamente nos Grandes Eventos (Copa do Mundo 2014, Jogos Olímpicos 2016) na Gerência e Proteção dos Sistemas de Comando e Controle do Ministério da Defesa e na integração e segurança de sistemas das Forças Armadas.

Grande fã de CTF, costuma competir em eventos internacionais como o SANS NetWars, onde se sagrou campeão das categorias Core (principal), DFIR (forense) e Defense, além de ser Campeão do Torneio dos Campeões do NetWars, como jogador individual e em time.

FORMAÇÃO:

Engenheiro de Computação
INSTITUTO MILITAR DE ENGENHARIA (IME)

Pós-Graduação em Segurança da Informação
UNIBRATEC

CERTIFICAÇÕES:

- Certified Information System Security Professional (ISC2) — *CISSP*
- SANS GIAC Experienced Incident Handler — *GX-IH*
- SANS GIAC Reverse Engineering Malware — *GREM*
- SANS GIAC Response and Industrial Defense — *GRID*
- SANS GIAC Security Expert — *GSE (291)*
- SANS GIAC Experienced Intrusion Analyst — *GX-IA*
- SANS GIAC Defending Advanced Threats — *GDAT*
- SANS GIAC Certified Forensic Analyst — *GCFA*
- SANS GIAC Security Professional — *GSP (257)*
- SANS GIAC Experienced Cybersecurity Specialist — *GX-CS*
- SANS GIAC Mobile Device Security Analyst — *GMOB*
- SANS GIAC Certified Windows Security Administrator — *GCWN*
- Offensive Security Certified Expert — *OSCE*
- SANS GIAC Advisory Board — *GIAC*
- SANS GIAC Python Coder — *GPYC*
- SANS GIAC Certified Incident Handler — *GCIH*
- Offensive Security Certified Professional — *OSCP*
- CERT Incident Response Process Professional — *CERT.BR*
- SANS GIAC Network Forensic Analyst — *GNFA*
- SANS GIAC Certified Intrusion Analyst — *GCIA*
- Offensive Security Wireless Professional — *OSWP*
- SANS GIAC Exploit Researcher and Advanced Penetration Tester — *GXPN*
- SANS GIAC Penetration Tester — *GPEN*
- SANS GIAC Certified Enterprise Defender — *GCED*
- SANS GIAC Experienced Penetration Tester — *GX-PT*
- SANS GIAC Assessing and Auditing Wireless Networks — *GAWN*
- SANS GIAC Web Application Penetration Tester — *GWAPT*
- SANS GIAC Security Essentials — *GSEC*

GoHacking

(GHSE)

O curso GoHacking Security Essentials (GHSE) é a porta de entrada para quem deseja iniciar sua jornada no fascinante universo da Segurança Cibernética. Voltado para iniciantes, ele apresenta os conceitos fundamentais necessários para compreender e atuar de forma segura e eficaz no ambiente digital. Com uma abordagem clara e didática, o curso fornece o conhecimento básico indispensável para construir uma carreira sólida nessa área em constante crescimento.

Ao longo do curso, você será introduzido aos princípios essenciais de redes de computadores, explorando como os dados trafegam na Internet e como proteger informações sensíveis. Além disso, serão abordados os fundamentos de sistemas operacionais, destacando o funcionamento interno de computadores e servidores, com ênfase na identificação de vulnerabilidades e implementação de boas práticas de segurança.

Outro pilar do curso é a introdução à programação, oferecendo as bases necessárias para criar scripts e ferramentas que auxiliem na análise e mitigação de ameaças cibernéticas. Combinando teoria e prática, o Security Essentials prepara os alunos para compreender as ameaças cibernéticas e como combatê-las, dando os primeiros passos rumo a uma carreira promissora em Segurança da Informação. Se você está começando agora e busca entender como proteger sistemas, dados e redes de forma eficiente, o GHSE é o curso ideal. Venha aprender com os melhores especialistas do mercado brasileiro e construir o conhecimento necessário para se destacar no mundo da cibersegurança!

MÓDULO 1 - A importância da Segurança da Informação

1. Visão geral sobre o cenário atual de ameaças cibernéticas
2. Principais ameaças e tendências
3. Segurança da Informação e Segurança Cibernética
4. Incidentes de segurança
5. Impactos de incidentes de segurança em organizações e indivíduos
6. Nomenclatura, terminologias e conceitos básicos iniciais
7. Leis, regulamentações e normas relacionadas à Segurança da Informação
8. Boas práticas de Segurança da Informação
9. Carreiras e oportunidades em Segurança da Informação
10. Certificações e mercado de trabalho

GoHacking

(GHSE)

MÓDULO 2 – Os Pilares da Segurança da Informação

1. Ciclo de vida dos dados
2. Principais conceitos de Segurança da Informação
3. Pessoas, Processos e Tecnologias
4. Confidencialidade, Integridade e Disponibilidade
5. Códigos maliciosos (malwares)
6. Gerenciamento de Risco
7. Modelos e Frameworks de Segurança da Informação
8. Cyber Kill Chain
9. MITRE ATT&CK
10. Controles Críticos de Segurança (CIS Controls)
11. NIST Cybersecurity Framework (CSF)
12. Higiene Cibernética (conscientização)
13. Privacidade: principais normas e conceitos
14. Fundamentos de Criptografia
15. Autenticação e Autorização

MÓDULO 3 – Conceitos Fundamentais de Redes de Computadores

1. Estrutura e funcionamento das redes de computadores
2. Modelos de referência: OSI e TCP/IP
3. Principais protocolos de rede
4. Camada física
5. Internet Protocol (IP)
6. Protocolos TCP e UDP
7. ICMP, DNS, HTTP, HTTPS, SSH, SMB, outros
8. Aspectos de segurança nos protocolos de rede

GoHacking

(GHSE)

MÓDULO 4 – Conceitos Fundamentais de Sistemas Operacionais

1. Introdução a Sistemas Operacionais
2. Virtualização
3. Fundamentos de Linux
4. Fundamentos de Windows
5. Estrutura de arquivos e diretórios
6. Utilização de linha de comando “tela preta”
7. Gerenciamento de processos e serviços
8. Gerenciamentos de usuários e privilégios
9. Aspectos de segurança nos sistemas operacionais

MÓDULO 5 – Conceitos Fundamentais de Programacão

1. Lógica de programação
2. Principais linguagens de programação e suas características
3. Introdução a linguagens de programação aplicadas à segurança (Python, Bash)
4. Criação de scripts básicos para automação de tarefas de segurança
5. Boas práticas de codificação
6. Desenvolvimento Seguro

MÓDULO 6 – Princípios de Segurança Ofensiva (Red Team)

1. Operações Cibernética Ofensivas
2. Metodologias dos ataques cibernéticos
3. Fundamentos de Open Source Intelligence (OSINT)
4. Introdução a Testes de Invasão (Pentesting)
5. Principais modelos e referências de pentesting
6. Ética e responsabilidade na realização de testes de invasão

GoHacking

(GHSE)

7. Análise de Vulnerabilidades
8. Operações de Red Team
9. Ferramentas básicas de segurança ofensiva
10. Relatório de Teste de Invasão

MÓDULO 7 – Princípios de Segurança Defensiva (Blue Team)

1. Operações Cibernéticas Defensivas
2. Defesa em Profundidade
3. Planejamento e implementação de políticas e controles de segurança
4. Hardening de servidores/serviços
5. Prevenção, Monitoramento e Detecção de eventos de segurança
6. Principais ferramentas de segurança para proteção e monitoramento
7. Fundamentos de Centro de Operações de Segurança (SOC)
8. Incidentes Cibernéticos
9. Tratamento e Resposta a Incidentes Cibernéticos
10. Fundamentos de Forense Computacional
11. Proteção de Ambiente Corporativos
12. Infraestrutura de Microsoft Active Directory (AD)
13. Fundamentos de segurança em AD

MÓDULO 8 – Desafios em Segurança da Informação

1. Internet das Coisas (IoT) e as novas fronteiras de segurança cibernética
2. Princípios de ambiente de Nuvem/Cloud
3. Fundamentos de Segurança em ambiente de Nuvem/Cloud
4. Princípios de Inteligência Artificial (IA)
5. Fundamentos de IA aplicada em Segurança Cibernética

GoHacking

(GHSE)

PRÉ-REQUISITOS

- Familiaridade com utilização de computadores
- Familiaridade na utilização da Internet
- Familiaridade com Tecnologia da Informação (TI)

PÚBLICO-ALVO

- Estudantes de TI
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação
- Profissionais de outras áreas com interesse em aprender Segurança da Informação
- Qualquer pessoa com afinidade e interesse em aprender Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS)
- Acesso à Internet
- Leitor de PDF
- Software de virtualização (Virtual Box ou VMware)

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso
- Apostila do Curso no formato PDF
- Gravações das sessões ao vivo
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

GoHacking

(GHSE)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Compreender a relevância da segurança da informação no mundo atual
- Identificar os principais tipos de ameaças cibernéticas
- Reconhecer o impacto de incidentes de segurança em indivíduos e organizações
- Entender a legislação e normas aplicáveis à segurança da informação
- Compreender os pilares da segurança da informação
- Desenvolver estratégias para proteger os pilares de segurança em cenários reais
- Compreender a estrutura básica das redes de computadores
- Reconhecer os modelos OSI e TCP/IP e sua aplicação prática
- Explicar o funcionamento dos principais protocolos de rede
- Identificar vulnerabilidades comuns em redes de computadores
- Descrever o papel dos sistemas operacionais na segurança cibernética
- Explorar recursos de segurança em sistemas operacionais como Windows e Linux
- Entender os fundamentos de lógica de programação
- Criar scripts básicos em linguagens como Python e Bash
- Automatizar tarefas básicas relacionadas à segurança cibernética
- Identificar vulnerabilidades em sistemas e redes
- Entender a execução de um Teste de Invasão
- Utilizar ferramentas básicas de segurança ofensiva
- Detectar e responder a incidentes de segurança
- Colaborar na construção de uma postura defensiva robusta contra ataques cibernéticos
- Entender os principais desafios em novos cenários para segurança da informação

GoHacking

CYBER SECURITY TRAININGS