EMENTA DE TREINAMENTOS – FORMAÇÃO HACKERSEC

Treinamento: Fundamental Hacking

Resumo: Nesse treinamento você vai aprender a base para se tornar um hacker ético profissional e começar na área de cibersegurança. Essencial para quem está iniciando na área e não tem nenhum conhecimento.

Conteúdo:

1. Hacker e Segurança da Informação
2. Equipamentos
3. Segurança na Internet
4. Máquina Virtual
5. Windows
6. Linux
7. Redes e Internet
8. HTML5
9. JavaScript
10. Programação PHP 7
11. Banco de Dados SQL
12. Programação Python 3
13. Malwares e Sistemas de defesa
14. Sistemas Operacionais de Pentest
15. Deep Web

Treinamento: Pentest

Resumo: Nesse treinamento você vai aprender como realizar testes de invasão (pentest) de forma profissional para identificar vulnerabilidades em sistemas, servidores e aplicações reais.

Conteúdo:

1. Introdução a InfoSec e Pentest
2. Escrita de Proposta e Relatório
3. Laboratório de Pentest
4. Engenharia Social
5. Anonimização
6. OSINT – Coleta de Informações
7. Varreduras de Rede
8. Enumeração de Informações e Serviços
9. Análise de Vulnerabilidades
10. Web Hacking
11. Quebra de Senhas
12. Exploitation
13. Post Exploitation
14. Comando e Controle – C2
15. Buffer OverFlow
16. Man-in-the-Middle
17. Ataques em redes WiFi
18. Programação para Pentest
19. Desenvolvimento de relatórios de Pentest

Treinamento: Forense Computacional

Resumo: Capacitar o aluno a compreender as fases da perícia computacional, instruir na utilização de ferramentas voltadas à coleta e análise de dados digitais. Educar quanto aos aspectos legais da computação forense, apresentar as perícias (in live e post-mortem).

Conteúdo:

1. Introdução a Perícia Forense Computacional
2. Aspectos legais da Computação Forense
3. O Perito Digital
4. Etapas da perícia digital
5. Preparação de laboratório de perícia
6. Preparando uma estação forense
7. Possíveis cenários de perícia digital
8. Representação de dados
9. Hashes
10. Live Forensics (análise viva)
11. Post-Mortem Forensics (análise morta)
12. Recuperação Avançada de Dados

Treinamento: Detecção de Intrusão

Resumo: Você vai aprender a realizar Detecção de Intrusão com método de análise dados para trabalhar na área de cibersegurança defensiva.

Conteúdo:

1. Introdução a Detecção de Intrusão
2. Práticas com Linux (Bruteforce Prevention)
3. Introdução ao Machine Learning
4. Pré-processamento de Datasets
5. Avaliação de desempenho dos IDS
6. k-Nearest Neighbors (R ou Python)
7. S.M.O.T.E
8. Support-vector Machines
9. Neural Networks
10. Decision Trees
11. Ensemble Learning
12. Stacking Ensemble Learning
13. Estudo de Caso

Treinamento: Web Security

Resumo: Aprenda como proteger sua aplicação web de forma prática e objetiva com os melhores especialistas do mercado de cibersegurança.

Conteúdo:

1. Introdução a Web Security
2. Servidores Web
3. Vulnerabilidades em Aplicações Web
4. Instalando LAB Básico
5. Protegendo sua Aplicação Web
6. Instalando LAB Avançado
7. Protegendo seu Web Server
8. Desenvolvimento Seguro