Defesa Cibernética – 360h

O curso irá capacitar o indivíduo para analisar, desenvolver e colocar em prática processos para a defesa de máquinas e afins. Desta forma o tornando um especialista capaz de atuar como consultor e assessor em várias frente que demandam em ter um sistema a prova de invasões.

Disciplinas:

- Segurança Defensiva e Resposta a Incidentes
    - Introdução a segurança defensiva
    - Quem é o inimigo e Como hackers atuam
    - Mitre & Attack
    - Exploit Database
    - APTs
    - Malwares
    - Processo de Contratação de ferramentas
    - Gestão de ferramentas de segurança
    - Conhecendo uma rede corporativa de grande porte
    - Proteção contra malwares
    - Windows Internals
    - AMSI bypass
    - UAC Bypass
    - Sysmon Bypass
    - ETW bypass
    - Análise Heurística de ameaças
    - EDR x AV convencional
    - MSS
    - Firewall Next Generation x Firewalls convencionais
    - Ferramentas de detecção de Ameaças
    - Machine Learn em defesa cibernética
    - Micro Segmentação
    - Nano Segmentação
    - Publicação segura de serviços e recursos
    - WAF - Web Application Firewall
    - Vazamento de dados
    - DLP e CASB
    - Proteção de Domínio
    - Phishing e Spear Phishing
    - Security Awareness
    - DevSecOps e APP sec
    - Correlação de eventos
    - SIEM
    - SOAR
    - IDS/IPS
    - IOCs
    - Threat Intelligence
    - Análise de Malware

        - Maldoc
        - Introdução a engenharia reversa
        - Resposta a Incidentes
        - Cadeia de Custódia
        - First responder
        - Como a memória ram funciona
        - Dump de Memória
        - FTK-Imager
        - Análise de Memória
        - IPED - Polícia Federal

- Detecção de Intrusão, Configuração de Perímetro e Análise de Logs
    - Segurança da Informação
    - Pilares da Segurança da Informação
    - Governança de Tecnologia em Segurança da Informação
    - Incidente de Segurança da Informação
    - Sistemas de Detecção de Intrusão
    - Pós-detecção
    - Exemplos e sistemas de detecção de intrusão

- Criptografia e Criptoanálise, Privacidade e Comunicações Digitais
    - Esteganografia
    - Técnicas de esteganografia clássica
    - Esteganografia moderna
    - Bit Menos Significativo
    - Criptografia Clássica
    - Métodos da Transposição e Substituição
    - Criptografia Moderna Simétrica
    - Codificação de caracteres
    - Criptografia XOR e com DES
    - Algoritmos de criptografía Simétrica
    - Criptografia Assimétrica com PGP
    - Hash
    - Principais algoritmos de hash
    - Colisão
    - Criptografia Quântica
- Gestão da Segurança da Informação
    - Normas e Padrões em Segurança da Informação (ISSO/ NIST /PCI)
    - ISSO 27001
    - A estruturação de Seções
    - NIST 800-53
    - Ameaças, Vulnerabilidades, Riscos e Tipos de Ataques em Segurança
    - Segurança em Internet das Coisas, Ciberataques e Ransomware
    - Segurança em Cloud Computing
    - Segurança em dispositivos móveis e pessoais

- Gerenciamento de Projeto de Redes de Computadores
    - Arquitetura de Camadas
    - Ciclo de Vida de Uma Rede
    - Planejamento de uma Rede
    - Disponibilidade de rede
    - Projetar uma Rede de Computadores
    - Tipos de Redes
    - Topologias de Redes
    - Segurança de rede
    - Dimensionamento de links
    - Implantação de Redes
    - Operar e Otimizar Redes
    - Conectores de Cabos e Guias de identificação de Ferramentas

- Análise Forense Aplicada a Sistemas Linux
    - Introdução à Forense
    - Fases de Investigação
    - Análise de um incidente
    - Documentação
    - Análise Forense
    - Análise de arquivos de log
    - Coletando hashes
    - Dump de memória RAM
    - Criando e montando imagens
    - Sistema de Arquivos, Análise de Memória e Volatility
    - Criando um perfil no Volatility
    - Malware e Além
    - Comandos úteis

- Introdução à Segurança da Informação
    - Como me proteger?
    - Entendendo Ataques
    - Incidentes de Segurança
    - Monitoramento de Segurança de Camadas
    - Ameaças Mobile
    - Ameaças Avançadas (APTs)
    - Segurança em Dispositivos Móveis
    - Telefonia Móvel

- Teste de Invasão em Redes e Sistemas
    - Introdução ao Teste de Invasão
    - Metodologias (PCI-DSS, PTES, OWASP Testing Guide v4)
    - Identificando hosts
    - Nessus
    - Sub-grupo de métricas: Impact
    - Métricas Base Modificadas

- Introdução à Engenharia Reversa
    - Estrutura de Software
    - Arquitetura de Computadores
    - Opcodes
    - Registradores
    - Implementação de Pilha
    - Seções
    - Execução de Aplicativos
    - Ferramentas para análise
    - Tipos de Malware
    - TCP View
    - Métodos de Ofuscação
    - Introdução a Ransomware
    - Sistemas Apple / Android
    - Lista de Programas Linux / Windows
    - Implementação da Backdoor

- Análise Forense Aplicada a sistemas Windows
    - Histórico do Sistema Windows
    - Processo de Boot
    - Dado x Metadado
    - Caso Concreto
    - Comandos Básicos do CMD
    - Coleta e Análise FTK Imager
    - Registry – Forense Windows
    - Quesitação do Requerente
    - Princípio da localidade de Referência
    - Windows Shell Bags
    - Windows Indexing Service
    - Tudo sobre a Lixeira do Windows
    - Evento dos Logs
    - Prática Forense HD Criptografado