Ethical Hacking e CyberSecurity – 360 h

Neste curso será abordado a importância do profissional Hacker ético no mercado, os Tipos de Segurança da Informação, Infraestrutura, Princípio de administração de redes seguras, Introdução a conceitos básicos, Segurança de dados, Conhecimento de Leis que guardam o usuário, Ataques Web, Metodologia de respostas a incidentes e Análise forense.

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

- Ethical Hacking - Técnicas e Ferramentas
    - Ethical Hacking – Fundamentos
    - Preparando seu ambiente de testes
    - Técnicas de Ethical Hacking
    - Ferramentas na prática
    - Segurança em ambiente Web

- Analista de SOC (Security Operation Center)
    - Introdução ao SOC
    - SIEM
    - Criando um SOC
    - Frameworks e Acesso Físico
    - Plano de comunicação e Threat Intelligence
    -
- Estratégias de Segurança Cibernéticas
    - Introdução à Segurança Computacional
    - Introdução à Privacidade e Proteção dos Dados
    - Governança
    - Ataques e suas características
    - Ferramentas e Processos

- Protocolo de Redes de Computadores
    - Modelos de Referência, TCP/IP
    - Portas de Comunicação
    - Processo de Transição do IPv4 para IPv6
    - Protocolo IMAP, SMTP, SSH , Telnet, DNS, HTTP E FTP
    - Função do Gateway
    - DROP e REJECT
    - Servidor FTP em Python
    - Tecnologia ATM, VPN e ADSI
    - Sistemas Autônomos
    - Sistemas de Detecção de Intrusão
    - Desafios no uso IDS
    - Vantagens no uso do IDS Suricata

- Gestão de Segurança da Informação
    - Pilares da Segurança da Informação
    - Nomes e Padrões em Segurança da Informação (ISO / NIST / PCI)
    - Ameaças, vulnerabilidades, Riscos e tipos de ataques em segurança
    - Política e Conscientização em Segurança da Informação
    - Segurança em Internet das Coisas, Ciberataques e Ransomware
    - Segurança em Cloud Computing e segurança em dispositivos móveis

- 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

- Administração de Sistema Operacional Linux
    - Virtualização
    - Virtual Box
    - Diretórios
    - Manipulação de Arquivos
    - Rede
    - Configurando a Rede
    - Contas e Permissões
    - Execução de Programas
    - Monitoramento de Execução

- 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

- Análise Forense Computacional
    - O Perito Forense
    - Análise
    - Coleta
    - Análise Forense em Windows