UNIVERSIDADE PRESBITERIANA MACKENZIE

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

Coordenadoria de Educação Continuada

MBA em *Cybersecurity Professional*

Estrutura Curricular – componente curricular/carga horária.

MÓDULO 1	
Nivelamento de Comandos de Terminal Linux e Windows	24
Ética Legislação e Direito Digital	32
Introdução à Segurança da Informação e Normativas	32
Open-Source Intelligence (OSINT) e Engenharia Social	32
Pentest em Sistema Operacional Windows	32
Pentest em Sistema Operacional Linux/MacOS	32
Pentest em Redes Corporativas Cabeadas	32
Carga horária total do módulo	**216 horas-aula**
MÓDULO 2	
Pentest em Redes Corporativas em Wireless	32
Pentest em Plataformas Web	40
Pentest em Dispositivos Móveis	32
Metodologias para Respostas a Incidentes	32
Cyber Practices	64
Gestão de Carreiras	16
Carga horária total do módulo	**216 horas-aula**
Total da carga horária do curso	**432 horas-aula**

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 1

1. Nome do Componente Curricular: **Nivelamento de comandos de Terminal Linux e Windows** (optativa)
2. Carga Horária: 24 horas
3. Ementa:

Neste componente curricular haverá o nivelamento de conhecimento para alunos que não conhecem o sistema operacional Linux e Windows no que se refere a comandos do terminal dos respectivos sistemas operacionais.

4. Objetivo:

Conhecer e compreender os principais comandos do terminal do Windows e Linux, com o propósito de facilitar o entendimento das aulas desta pós-graduação. Treinar a capacidade do aluno em conhecer e executar os principais comandos de Linux e Windows (prompt de comando) de modo a desenvolver pró atividade, foco no resultado, disciplina e compromisso com segurança. Através de exercícios interativos, discussões e exercícios em grupo os professores auxiliam os participantes a identificar e analisar.

5. Conteúdo Programático:
    - Comandos Terminal Windows
    - Comandos Terminal Linux
    - Fundamentos de rede (comandos básicos)
    - Protocolo TCP
    - Comandos Windows: Ping, ipconfig, ifconfig, etc;
    - Virtualização;
    - Como instalar um Linux/Windows com Máquina Virtual
    - Firewall e antivírus

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 2

1. Nome do Componente Curricular: **Ética, Legislação e Direito Digital**

2. Carga Horária: 32 horas

3. Ementa:

No componente curricular Ética, Legislação e Direito Digital serão trabalhados os conceitos de Ethical Hacking, Legislação Brasileira e Direito eletrônico.

4. Objetivo:

Compreensão das leis e suas consequências para o uso indevido de dispositivo informático; Habilidade de debater sobre a importância do Direito Digital nas estratégias jurídicas das empresas; Analisar os crimes eletrônicos e a importância da perícia e preservação de evidências; Analisar os principais aspectos do Marco Civil da Internet; Aprender como formalizar testes de invasões autorizados, de modo a desenvolver a Criatividade, Inovação, Disciplina e a Pró atividade através de aulas em laboratório, simulando situações cotidianas de explorações de ambiente e ataques, conscientizando o aluno sobre as diferenças entre o criminoso e o hacker ético e Problem Based Learning (PBL) discutindo um problema de segurança ocorrido em alguma empresa via invasão de rede crítica e discussão sobre sua possível solução e prevenção.

5. Conteúdo Programático:

- Ethical hacking Foudation,
- Marco Civil da internet,
- Código Penal,
- Código Civil,
- Licitude de contra-ataque na visão jurídica, Criminologia,
- Perícia Judicial
- Crimes cibernéticos

- Guerra Cibernética

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 3

1. Nome do Componente Curricular: **Introdução à Segurança da Informação e Normativas**
2. Carga Horária: 32 horas
3. Ementa

O componente curricular considerará os conceitos de Segurança da Informação.

4. Objetivo:

Compreensão de normas técnicas na área de segurança da Informação; Identificar e realizar assessment em organizações para entendimento da maturidade em relação a normas técnicas de Segurança da Informação de modo a desenvolver Criatividade, Inovação, Disciplina e Pró atividade através da apresentação das normas e simulação de empresas com processos para que o aluno consiga identificar se a organização está em compliance com a norma ou não.

5. Conteúdo Programático:
   - Introdução à segurança da informação: conceitos e definições básicas;
   - Tipos de ameaças e vulnerabilidades que podem afetar a segurança da informação;
   - Norma técnica ISO ABNT 27.001 e ISO ABNT 27.002;
   - Os 3 pilares da segurança da informação;
   - Noções de criptografia, certificados digitais e chaves;
   - Conscientização sobre segurança da informação;
   - Lei Geral de Proteção de Dados;
   - Lei Carolina Dieckmann (14.155)
   - Convenção de Budapeste.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 4

1. Nome do Componente Curricular: **Open Source Intelligence (OSINT) e engenharia Social**
2. Carga Horária: 32 horas
3. Ementa

Técnicas de engenharia social como vetor de ataque. O módulo contempla o uso de ferramentas livres para a elaboração de ataques dessa natureza e a utilização de técnicas rebuscadas de exploração psicológica de colaboradores e de terceiros a fim de conseguir dados valiosos sobre o ativo.

4. Objetivos

Compreender o uso dos vetores de ataques de engenharia social, especialmente os de tipo phishing; Identificar as técnicas utilizadas na Engenharia Social; Identificar riscos de segurança e vetores de ataque aos SO de modo a desenvolver Criatividade, Inovação, Disciplina e Pró atividade através de aulas em laboratório simulando situações em que são empregadas técnicas de Engenharia Social, Com problematização e discussão sobre um problema de segurança que tenha ocorrido via invasão por meio de alguma técnica de Engenharia Social, análise do impacto sofrido e análise da metodologia aplicada na resposta ao incidente. Problem Based Learning (PBL) discutindo um problema de segurança ocorrido em alguma empresa via invasão por meio de alguma técnica de Engenharia Social.

5. Conteúdo Programático:
   - Introdução à Open Source Intelligence (OSINT) e engenharia social: conceitos e definições básicas;
   - Fontes de informação abertas e públicas utilizadas na OSINT (Google Hacking);
   - Técnicas de coleta e análise de informações na OSINT, como web scraping e busca avançada em motores de busca;
   - Ferramentas de OSINT para investigação digital, como o Maltego e o recon-ng;
   - Conceitos básicos de engenharia social, incluindo pretexting, phishing e tailgating;

- Técnicas de engenharia social para obtenção de informações confidenciais, como o uso de pretextos e manipulação psicológica;
- Tipos de ataques de engenharia social, incluindo engenharia social em redes sociais e engenharia social em engenharia reversa;
- Medidas de proteção e prevenção contra-ataques de engenharia social, incluindo treinamento de conscientização e políticas de segurança.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 5

1. Nome do Componente Curricular: **Pentest em Sistema Operacional Windows**

2. Carga Horária: 32 horas

3. Ementa

Neste componente curricular serão considerados os ataques a sistemas operacionais, focando especialmente no sistema Windows. É avaliada a evolução na segurança do sistema, a larga produção de exploits contra o sistema, a análise de eventos (logs) e a execução remota.

4. Objetivo:

Entender as vulnerabilidades da execução remota no Windows através de aula simulando invasões de Sistemas Operacionais (SO) e testando a eficiência da aplicação de estratégias de defesa e reação em resposta a esses incidentes; Identificar o padrão de gerenciamento que um SO faz no computador; identificar riscos de segurança e vetores de ataque aos SO de modo a desenvolver Criatividade, Inovação, Disciplina e Pró atividade, através de aulas simulando invasões de Sistemas Operacionais (SO) e testando a eficiência da aplicação de estratégias de defesa e reação em resposta a esses incidentes. Problematização: discussão sobre algum problema de segurança que tenha ocorrido recentemente em SO.

5. Conteúdo Programático:

- Sistema Operacional (SO) Windows: uma rápida visão da arquitetura;

- Riscos à segurança das informações no SO;
- Identificação de vulnerabilidades;
- Exploits e Payloads
- Exploração de ambiente;
- Movimentação lateral;
- Persistência;
- Escalação de Privilégios

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 6

1. Nome do Componente Curricular: **Pentest em Sistema Operacional Linux/MacOS**
2. Carga Horária: 32h
3. Ementa:

Componente curricular considerará os ataques a sistemas operacionais, focando especialmente no sistema Linux e MacOS. É avaliada a evolução na segurança do sistema, a larga produção de exploits contra o sistema, a análise de eventos (logs) e a execução remota.

4. Objetivo:

Entender as vulnerabilidades da execução remota no Linux e no MacOS através de aula simulando invasões de Sistemas Operacionais (SO) e testando a eficiência da aplicação de estratégias de defesa e reação em resposta a esses incidentes; Identificar o padrão de gerenciamento que um SO faz no computador; identificar riscos de segurança e vetores de ataque aos SO de modo a desenvolver nos estudantes Criatividade, Inovação, Disciplina e Pró atividade, através de aulas simulando invasões de Sistemas Operacionais (SO) e testando a eficiência da aplicação de estratégias de defesa e reação em resposta a esses incidentes. Problematização: discussão sobre algum problema de segurança que tenha ocorrido recentemente em SO.

5. Conteúdo Programático:

- Sistemas Operacionais (SO) Linux e MacOS.
- Riscos à segurança das informações nos SOs compreendendo as temáticas:
- Identificação de vulnerabilidades;
- Exploits e Payloads
- Exploração de ambiente;
- Movimentação lateral;
- Persistência;
- Escalação de Privilégios

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 7

1. Nome do Componente Curricular: **Pentest em redes corporativas cabeadas**

2. Carga Horária: 32 horas

3. Ementa:

Técnicas de pentest em redes corporativas cabeadas com a identificação do ambiente corporativo fundamentadas no ciclo de pentest. O módulo prevê o uso da ferramenta livres para exploração utilizando essas técnicas.

4. Objetivo

Identificar e compreender as vulnerabilidades da rede corporativa das empresas através de aula em laboratório simulando invasões em redes cabeadas; Identificar ataques às redes cabeadas corporativas; executar ataques às redes cabeadas corporativas de modo a desenvolver nos alunos Criatividade, Inovação, Disciplina e Pró atividade, através de aulas em laboratório simulando invasões em redes cabeadas. Problematização e discussão sobre um problema de segurança que tenha ocorrido recentemente, análise do impacto para a empresa e da metodologia aplicada na resposta ao incidente. Team Based Learning (TBL) discutindo um caso de falha de segurança numa rede cabeada e desenvolvimento de sua possível solução.

5. Conteúdo Programático:

- Redes corporativas cabeadas. Topologia de uma rede corporativa. Identificação de ameaças;
- Planejamento e reconhecimento;
- Introdução a ferramentas de Pentest, como o Nmap, o Metasploit e o Wireshark;
- Escaneamento de vulnerabilidades;
- Identificação de vulnerabilidades comuns em redes cabeadas, como falhas de autenticação, vulnerabilidades de protocolos de rede e configurações de segurança inadequadas;
- Exploração das vulnerabilidades;
- Pivoteamento;
- Golden Ticket AD;

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 8

1. Nome do Componente Curricular: **Pentest em redes corporativas wireless**

2. Carga Horária: 32 horas

3. Ementa

Neste componente curricular serão estudados pentests em redes corporativas wireless, considerando possibilidades de brechas em pontos de acesso (APs), repetidores e roteadores inseridos em um cenário com ataques de ARPspoofing, ARPoisoning, Man-In-The-Middle (MITM), SSl stripping. São abordados, ainda, ataques às chaves WEP e WPA-PSK. Utilização de Hardware Wireless (Antena USB).

4. Objetivo

Compreender os cenários em que ocorrem vulnerabilidades segurança na estrutura da rede WI-FI (Wireless: sem fio). Manipular a infraestrutura de redes wireless corporativas; identificar ataques às redes wireless corporativas de modo a propiciar o desenvolvimento de Criatividade, Inovação, Disciplina e Pró atividade, através de aulas em laboratório

simulando invasões em redes wireless. Problematização e discussão sobre algum problema de segurança que tenha ocorrido recentemente, análise do impacto para a empresa e da metodologia aplicada na resposta ao incidente. Simulação de invasão a uma rede wireless (ambiente de teste e seguro).

5. Conteúdo Programático:

- Redes corporativas wireless;
- Topologia de uma rede wireless;
- Identificação de ameaças;
- Identificação em rede WEP, WPA, WPA2;
- Tentativa de obtenção de credenciais de Wifi em rede WEP;
- Tentativa de obtenção de credenciais de Wifi em rede WPA e WPA2;
- Usando a placa de vídeo para performance de brute force;
- Tentativa de obtenção de credenciais administrativas do Equipamento de Wifi.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 9

1. Nome do Componente Curricular: **Pentest em plataformas Web**
2. Carga Horária: 40 horas
3. Ementa

Neste componente curricular serão considerados os pentests em plataformas Web, abordando ataques de injeção de SQL, ataques de escalonamento de privilégios, ataques a banco de dados, ataques de XSS e Cross-site Request Forgery. Baseado no OWASP top 10.

4. Objetivo

Compreender o contexto em que ocorrem as vulnerabilidades em plataforma web. Manipular a infraestrutura da plataforma web; identificar e explorar ataques à plataforma web; a fim de desenvolver Criatividade, Inovação, Disciplina e Pró atividade, através de

aulas em laboratório simulando invasões de plataforma web. Problematização, discussão sobre um problema de segurança (falha) que permitiu a invasão a uma plataforma web e exercícios práticos.

5. Conteúdo Programático:

- Introdução ao Pentest em plataformas Web: conceitos e definições básicas;
- Fases de um Pentest em plataformas Web, incluindo a fase de planejamento, a fase de teste e a fase de relatório;
- Identificação de vulnerabilidades comuns em plataformas Web, como falhas de autenticação, vulnerabilidades de SQL injection, Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF);
- Uso de ferramentas de Pentest em plataformas Web, como o OWASP ZAP, o Burp Suite e o Nikto;
- Técnicas de exploração de vulnerabilidades em plataformas Web, incluindo a exploração de falhas de injeção SQL e a exploração de vulnerabilidades de XSS;
- Análise de riscos e impactos associados a vulnerabilidades identificadas;
- Testes de segurança de APIs (Application Programming Interfaces) que fornecem dados e serviços para a plataforma Web;
- Elaboração de relatórios de Pentest em plataformas Web, incluindo recomendações para a correção de vulnerabilidades e medidas de segurança adicionais.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 10

1. Nome do Componente Curricular: **Pentest em dispositivos móveis**
2. Carga Horária: 32 horas
3. Ementa

Serão considerados os ataques a dispositivos móveis (smartphones e tablets), focando no sistema operacional Android.

4. Objetivo

Compreender os riscos existentes no uso de dispositivos móveis; Manipular a infraestrutura de segurança dos dispositivos móveis; identificar e explorar padrões de ataques aos dispositivos móveis a fim de propiciar aos estudantes Criatividade, Inovação, Disciplina e Pró atividade, através de aulas em laboratório simulando invasões de dispositivos móveis: celulares e tablets. Problematização, discussão sobre um problema de segurança (falha) que permitiu a invasão a um dispositivo móvel. Problem Based Learning (PBL) discutindo a invasão a um dispositivo móvel e buscar sua possível solução de segurança.

5. Conteúdo Programático:

- Introdução ao Pentest em dispositivos móveis: conceitos e definições básicas;
- Introdução ao Android;
- Pentests aos dispositivos móveis;
- Uso de ferramentas de Pentest em dispositivos móveis, como o OWASP Mobile Security Testing Guide (MSTG) e o Burp Suite Mobile Assistant;
- AndroBugs - uma ferramenta de análise estática de segurança para aplicativos Android, que permite detectar vulnerabilidades de segurança em código-fonte e binário.
- Drozer - uma ferramenta de teste de penetração para dispositivos Android, que permite verificar vulnerabilidades de segurança em aplicativos e dispositivos Android.
- Needle - uma estrutura de teste de segurança para aplicativos móveis, que permite realizar testes de penetração em aplicativos iOS e Android.
- Appie - uma ferramenta de teste de penetração para dispositivos móveis que permite verificar vulnerabilidades em aplicativos Android e iOS.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR -11

1. Nome do Componente Curricular: **Metodologias para Respostas a Incidentes**
2. Carga Horária: 32 horas
3. Ementa

Metodologias existentes para o aprimoramento e treinamento de alunos nas respostas a incidentes, bem como no reconhecimento e na identificação de ataques cibernéticos.

4. Objetivo

Conhecer e entender os tipos de incidentes com respeito às invasões que burlam a Segurança das Informações e seus efeitos no contexto da organização; conhecer as estratégias de defesa contra esses incidentes; revisar sobre informações críticas e probes e scans típicos; como gerir o tratamento de major events; descobrir causas fundamentais das vulnerabilidades; ter uma visão geral de ferramentas típicas dos invasores de forma a desenvolver nos alunos Pró atividade, Foco no resultado, Disciplina e Compromisso com segurança, através de exercícios interativos, discussões e exercícios em grupo os professores auxiliam os participantes a identificar e analisar um conjunto de incidentes e vulnerabilidades e, então, propor estratégias de resposta apropriadas. Os alunos também irão explorar outros aspectos do trabalho de um CSIRT, incluindo análise de artefatos, desenvolvimento de advisories, alertas e interação com administração superior.

5. Conteúdo Programático:
   - Introdução às metodologias para resposta a incidentes: conceitos e definições básicas;
   - Fases da resposta a incidentes: preparação, identificação, contenção, análise, erradicação, recuperação e lições aprendidas;
   - Estabelecimento de políticas e procedimentos de resposta a incidentes;
   - Criação de uma equipe de resposta a incidentes e definição de papéis e responsabilidades;

- Identificação de incidentes de segurança, incluindo o monitoramento de eventos e o uso de ferramentas de detecção de intrusão;
- Contenção de incidentes, incluindo a desativação de serviços comprometidos e a isolamento de sistemas afetados;
- Análise de incidentes, incluindo a coleta de evidências e a identificação de vetores de ataque;
- Recuperação de incidentes, incluindo a restauração de serviços afetados e a implementação de medidas de segurança adicionais para evitar futuros incidentes.

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR - 12

1. Nome do Componente Curricular: **Cyber Practices**

2. Carga Horária: 64 horas

3. Ementa

Desenvolvimento de um Projeto Prático de uma simulação de rede corporativa onde o aluno enfrentará desafios a serem resolvidos com base no aprendizado obtidos nos componentes curriculares anteriores.

4. Objetivo:

Desenvolver um Projeto que será utilizado para composição do TCC do aluno utilizando conhecimentos de Pentest de redes, sistemas operacionais, sistemas Web, movimentação lateral, pivoteamento, exploração de vulnerabilidades em computadores e elaboração de relatório técnico de forma a estimular nos estudantes Pontualidade, Criatividade, Inovação e Pró atividade, através da apresentação de projeto de Teste de Penetração, simulando uma corporação, com a composição de relatórios práticos desenvolvidos com base no mercado atual de segurança. O Projeto contará com o apoio docente para a construção do plano de desenvolvimento da pesquisa e orientação pedagógica para o desenvolvimento da pesquisa pela realização de encontros presenciais. Ao final, o componente curricular prevê a apresentação do relatório de pentest como conclusão de curso.

5. Conteúdo Programático:

Desenvolver um relatório de Pentest que aborde aspectos teóricos e práticos relevantes para realização de pentest (hacker ético) em ambiente controlado, simulando um ambiente corporativo, com servidores e estações de trabalho, identificando e explorando possíveis vulnerabilidades. A dinâmica dessas aulas será em realizar uma mentoria para que o aluno consiga explorar o ambiente controlado. Plano de aulas:

- Introdução ao ambiente controlado
- Mentoria 1
- Mentoria 2
- Mentoria 3
- Mentoria 4
- Mentoria 5
- Mentoria 6
- Resolução do exercício

IDENTIFICAÇÃO DO COMPONENTE CURRICULAR – 13

1. Nome do Componente Curricular: **Gestão de Carreiras**
2. Carga Horária: 16 horas
3. Ementa

Capacitar os alunos a gerenciarem suas carreiras em cibersegurança, desenvolvendo habilidades técnicas, de liderança e de comunicação, identificando oportunidades de crescimento profissional e implementando estratégias eficazes de gestão de carreira.

4. Objetivo

Capacitar os alunos a aplicar estratégias de gestão de carreira em cibersegurança, identificando oportunidades de crescimento profissional, desenvolvendo habilidades

técnicas e comportamentais, negociando salários e benefícios, e adaptando-se às mudanças e desafios do mercado de trabalho em cibersegurança; Aprofundar os conhecimentos técnicos em cibersegurança; Comunicação e colaboração; Gerenciamento de projetos; Habilidades de liderança; Resolução de problemas estimulando a Inovação, Disciplina e Foco no Resultado, através de aulas expositivas em que o professor apresentará os conceitos e informações relevantes para a gestão de carreiras em cibersegurança por meio de aulas expositivas. Essa metodologia pode ser combinada com atividades práticas, como estudos de caso e exercícios.

5. Conteúdo Programático:

- Definição de carreira em cibersegurança;
- Tendências e desafios da carreira em cibersegurança;
- O papel da gestão de carreira no sucesso profissional em cibersegurança;
- Certificação na área de Cibersegurança e sua importância no mercado de trabalho.