Segurança da Informação – GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Apresentação e Plano de Curso

Auditoria e Segurança da Informação (GBC083)

Informações básicas

- Email: miani@ufu.br
- Página do curso:
  - Teams – procurar por "GBC083 - 2024/02" (chave de acesso: tnm327g)
- Horário de atendimento – sala 1B-148:
  - Terça-feira – 15:00 – 16:30 ou Quarta-feira – 14:00 – 14:50;
  - Outros horários são possíveis! Basta enviar um email para marcar atendimento fora do horário acima.

Apresentação

- Prof. Dr. Rodrigo Sanches Miani
  - Professor Adjunto da Faculdade de Computação (FACOM) da Universidade Federal de Uberlândia (UFU) desde 2013;
  - Membro permanente do Programa de Pós-graduação em Ciência da Computação da FACOM
- Mestrado e Doutorado pela FEEC/Unicamp
- Trabalho na área de segurança desde 2006 (início do mestrado);
- Projetos/parcerias/publicações nacionais/internacionais;
- Atualmente trabalho com sistemas de detecção de intrusão e análise de malware e outros problemas na intersecção – cybersecurity x ciência de dados.

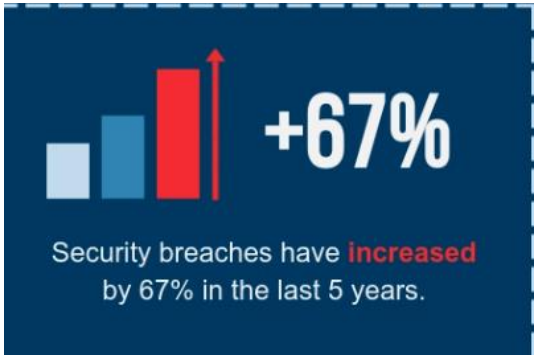
Gostaria de conhecer vocês!

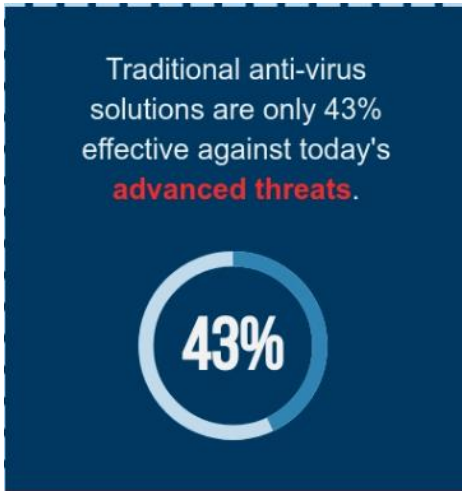
1. Nome
2. Terminando o curso?
3. Trabalha? Se sim, onde e qual área?
4. Teve algum contato com a área de segurança (acadêmico ou profissional)?

Motivação

https://www.techtarget.com/searchsecurity/infographic/7-security-awareness-statistics-to-keep-you-up-at-night

Motivação





https://www.techtarget.com/searchsecurity/infographic/7-security-awareness-statistics-to-keep-you-up-at-night
https://blog.teamascend.com/5-need-to-know-cybersecurity-statistics-for-2019

Motivação

Ou seja, precisamos entender os principais **conceitos de segurança**.

O foco do curso está na compreensão de **mecanismos de segurança criptográficos**. Contudo, a área é ampla e possui diversas ramificações: segurança de redes, segurança de aplicações, políticas de segurança entre outros.

Oportunidades!

- https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html

- Em linhas gerais, existe um grande "gap" de profissionais na área de segurança;

- Esse "gap" gira em torno de 4 milhões de empregos!

Oportunidades!

- Chief Information Security Officer (CISO)
- Analista de Segurança
- Analista de Riscos em Segurança de Informação
- Especialista de Segurança
- Especialista em Vendas de Soluções de Segurança
- Especialista Forense de Segurança em TI
- Pesquisador em Segurança
- Técnico de Respostas a Incidentes em Ciber-segurança
- E por aí vai...

Objetivos

- Conhecer os principais serviços relacionados com a segurança da informação e sua implementação através de técnicas de **criptografia**;
- Conhecer e entender fundamentos de **criptografia**. Conhecer funcionamento de algoritmos simétricos e assimétricos;
- Adquirir capacidade de escolher técnicas de **criptografia** conforme a necessidade.

Ementa

- Conceitos de Segurança
- Tipos de Ataques
- Serviços e Mecanismos de Segurança
- Criptografia e Criptoanálise
- Algoritmos simétricos
  - Técnicas clássicas
  - Cifras de bloco
  - Advanced Encryption Standard (AES)
  - Modos de Operação

Ementa

- Cifradores Assimétricos
  - Conceitos e aplicações
  - RSA
- Message Authentication Codes (MAC)
  - Algoritmos Hash
  - Assinaturas digitais
- Infraestrutura de Chave Pública
- Segurança Camada de Aplicação da Arquitetura TCP/IP
- Implementação de Serviços de Segurança

Metodologia

- Aulas expositivas;
- Resolução de exercícios/laboratórios solicitados pelo professor;
- Prova.

Avaliação

- A nota final será composta pelas seguintes avaliações:
  - NF = média(P)*55% + média(TP)*45%
  - Provas (P) – 2 provas distribuídas ao longo do semestre;
  - Trabalhos Práticos (TP) – entre seis trabalhos práticos distribuídos ao longo do semestre. Os trabalhos permitirão que os alunos pratiquem o conteúdo teórico da disciplina;
    - Alguns trabalhos terão pesos diferentes!
  - Importante: o plano da disciplina contempla uma prova de recuperação sobre todo o conteúdo visto durante o semestre. A nota final do aluno após a recuperação será NF = (NR+ NA)/2, onde NA representa a nota do aluno antes da recuperação.

Avaliação – Trabalhos práticos

- Entrega eletrônica usando o Microsoft Teams;
- Tarefas atrasadas serão penalizadas:
  - 1 dia – 10% da nota;
  - 2 a 3 dias – 20% da nota;
  - Entre 4 a 21 dias – 50% da nota;
  - Mais de 21 dias – o TP não será pontuado.

Datas importantes

Semana	Data	Conteúdo
1	10/dez	Apresentação da disciplina
1	11/dez	Tópico 1 - Conceitos de Segurança - Parte 1
2	17/dez	Tópico 1 - Conceitos de Segurança - Parte 2
2	18/dez	Tópico 2 - Princípios de Criptografia
3	04/fev	Revisão - Tópicos 1 e 2
3	05/fev	Tópico 3 - Criptoanálise e ataques
4	11/fev	Tópico 4 - Criptografia simétrica - Técnicas clássicas
4	12/fev	Tópico 5 - Criptografia simétrica - Cifra de bloco - Parte 1
5	18/fev	Tópico 5 - Criptografia simétrica - Cifra de bloco - Parte 2
5	19/fev	Tópico 6 - Criptotrafia simétrica - DES - Parte 1
6	25/fev	Tópico 6 - Criptotrafia simétrica - DES - Parte 2
6	26/fev	Tópico 7 - AES - Parte 1
7	04/mar	Recesso - Carnaval
7	05/mar	Recesso - Carnaval
8	11/mar	Tópico 7 - AES - Parte 2
8	12/mar	Tópico 8 - Modos de cifra de bloco
9	18/mar	Discussão da primeira parte da disciplina - Dúvidas
9	19/mar	P1
10	25/mar	Tópico 9 - Criptografia de chave pública
10	26/mar	Tópico 10 - RSA - Parte 1
11	01/abr	Tópico 10 - RSA - Parte 2
11	02/abr	Tópico 11 - Funções de Hash
12	08/abr	Tópico 12 - Integridade, autenticação e não repúdio
12	09/abr	Tópico 13 - Infraestrutura de chaves públicas - Parte 1
13	15/abr	Tópico 13 - Infraestrutura de chaves públicas - Parte 2
13	16/abr	Tópico 14 - Segurança na camada de transporte - Parte 1
14	22/abr	Tópico 14 - Segurança na camada de transporte - Parte 2
14	23/abr	Aula extra - Tópico a decidir
15	29/abr	Discussão da segunda parte da disciplina - Dúvidas
15	30/abr	P2
16	06/mai	Recuperação
6	07/mai	Encerramento da disciplina

Referências – Bibliografia básica

- Criptografia e segurança de redes. William Stallings – 6 ed;
- Modern Cryptography: Theory and Practice – Wembo Mao;
- A Graduate Course in Applied Cryptography - Dan Boneh e Victor Shoup.
- https://www.youtube.com/@criptografia
  - Canal com todas as aulas do curso!
  - Gravadas durante a pandemia, portanto, não julguem os "parcos" recursos utilizados… ☺