



SEGURANÇA CIBERNÉTICA

APRESENTAÇÃO E CONCEITOS DE SEGURANÇA CIBERNÉTICA

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

- **Situação:** Parques tecnológicos são construídos para manter e processar todas as informações úteis às empresas.



**Essas informações
existiam antes?**

Compreendendo o problema

- Vamos conhecer o Mentimeter!



<https://www.menti.com/>

Compreendendo o problema

- **Situação:** Essas informações são mais facilmente comprometidas hoje, pois estão mais acessíveis...



Qual é o impacto desse comprometimento?

Objetivos

- Conhecer o professor
- Conhecer a disciplina
- Compreender o sistema d
- Conhecer a história e evolução da segurança cibernética
- Compreender o valor da informação para os negócios e as pessoas



Apresentação

Quem é o
professor?

Chamada, Presença e Contato

- Será controlada a presença
 - Chamada ocorrerá sempre nos 15 minutos finais
 - Em tempo real, na aula – Lista do Teams
 - “Estou frequentando mas a matrícula...”
- Contato

Professor

Informações de Contato

Daniel Caetano

prof@caetano.eng.br



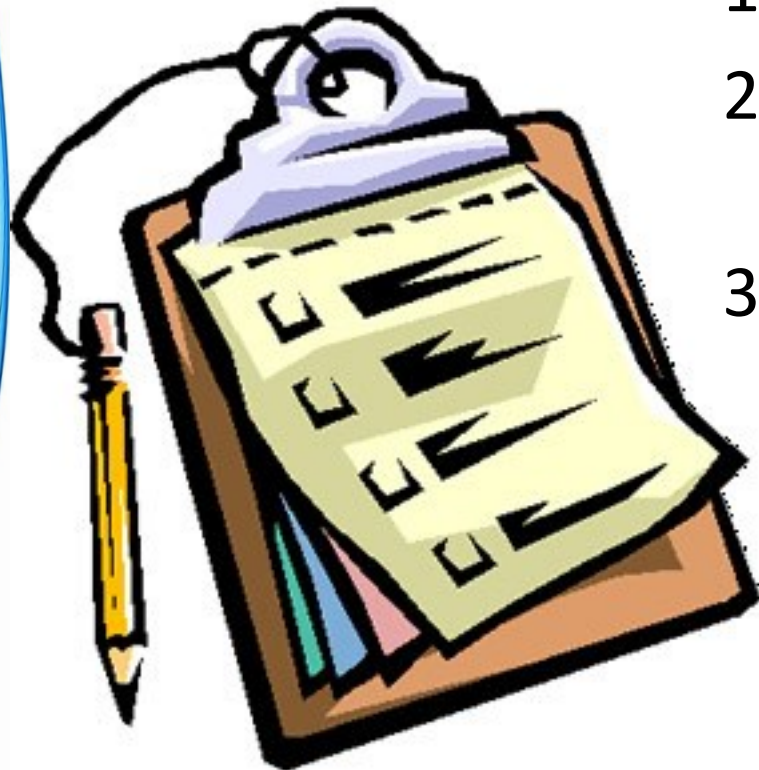
PLANO DE ENSINO E PLANO DE AULA

Plano de Ensino

Disponível no SIA/YUDQS/AURA

<https://estudante.estacio.br/>

1. Entre no **Ambiente Virtual**
2. Clique no
NOME DA DISCIPLINA
3. Clique em
PLANO DE ENSINO



Plano de Aula – Turma de 2ª

- 21/02 – 1. Apresentação
- 28/02 – [Carnaval]
- 07/03 – 2. Princípios I
- 14/03 – 3. Princípios II
- 21/03 – Packet Tracer Cisco
- 28/03 – 4. Ataques I
- 04/04 – 5. Ataques II
- 11/04 – 6. Ataques III
- 18/04 – Revisão
- **25/04 – P1 (AV1)**
- **02/05 – 7. Vulnerabilidades I**
- **09/05 – 8. Vulnerabilidades II**
- 16/05 – 9. Contramedidas I
- 23/05 – 10. Contramedidas II
- 30/05 – Revisão
- **06/06 – P2 (AV2)**
- 13/06 – Vista
- **20/06 – P3 (AV3)**
- 27/06 – Encerramento
- **Aulas que possuem conteúdo digital no ambiente AURA**
Esse conteúdo extra é considerado CRÉDITO DIGITAL e as horas e notas dos mesmos são computadas em separado!

Como Estudar?



- Até o fim do ensino médio...
 - Professor: apresenta os conteúdos completos
 - Teoria-prática: são exercitadas todas as situações em sala
 - Alunos: estudam após a aula, repetindo exercícios.
- E na faculdade...?
 - O procedimento do ensino médio... não é eficiente.
 - Alunos: estudam antes da aula os conteúdos
 - Conjunto: na aula, discutem o conteúdo diante de uma situação-problema
 - Professor: organiza os conceitos principais do conteúdo
 - Teoria-prática: exercitadas situações relevantes em sala.

Disciplina Presencial + Digital

- Como funciona?
 - Aluno se prepara entre as aulas, conhece a teoria
 - Vídeos, textos, desafios...
 - Na aula: discussão e complemento do conteúdo
 - Na aula: teoria-prática com atividades participativas
- Como é a preparação semanal?
 - Varia muito de acordo com o conteúdo... Mas...
 - Toda semana serão passadas atividades
 - **Conteúdo** para absorver e analisar...
 - Complementado por um **desafio**: Atividade Autônoma Aura
 - Algumas aulas têm bastante conteúdo digital
 - Esse conteúdo será **discutido** em sala e cai em prova!

Ambiente Aura

- Você acompanha seus conteúdos...

<https://estudante.estacio.br/login>



Home



Turmas



Biblioteca e Periódicos



Sistema de Avaliações

Ambiente Aura - Turma

Turma

Segurança Cibernética



Início

Cont. complementar

Trabalhos



Plano de Ensino



Baixar



Plano de Aula



Baixar



Tema 1

Princípios e Conceitos de
Segurança Cibernética



Tema 2

Ameaças, Vulnerabilidades
e Tipos de Ataques



Tema 3

Crédito Digital

As Principais
Vulnerabilidades Comuns
da Open Web Application
Security Project (owasp)

Tema 1

Princípios e Conceitos de Segurança Cibernética

De acordo com o Plano de Ensino da disciplina, não há conteúdos digitais para esse tema.

Conteúdos Complementares (0)

Ainda não há conteúdo complementar anexado a este tema.



Adicionar Conteúdo Complementar

Ambiente Aura - Turma

Turma

Segurança Cibernética



Início

Cont. complementar

Trabalhos



Plano de Ensino



Baixar



Plano de Aula



Baixar



Tema 1

Princípios e Conceitos de Segurança Cibernética



Tema 2

Ameaças, Vulnerabilidades e Tipos de Ataques



Tema 3 Crédito Digital

As Principais Vulnerabilidades Comuns da Open Web Application Security Project (owasp)

Tema 3

As Principais Vulnerabilidades Comuns da Open Web Application Security Project (owasp)



As Principais Vulnerabilidades Comuns da Open Web Application Security Project (owasp): Injeção, Quebra de Autenticação e Exposição de Dados Sensíveis e Entidades Externas de Xml, Quebra de Controle de Acessos e Configurações de Segurança Incorretase Software Cliente e Gerenciamento de Correção de Bugs e Documentação do Software e da Arquitetura



Nenhuma visualização



As Principais Vulnerabilidades Comuns da Open Web Application Security Project (owasp): Cross-site Scripting e Desserialização Insegura e Registro e Monitorização Insuficiente



TRABALHOS, DATAS E CRITÉRIO DE APROVAÇÃO

Trabalhos, Datas e Aprovação (2ª)

Trabalho	Valor	Data
Desafios até Aula 05	0,5 em Prova	Domingo (Web)
Desafios após Aula 05	0,5 em Prova	Domingo (Web)
Atividade Avaliativa A – Aula 06	3,0 na AV1	11/04
Avaliação P1	7,0 na AV1	25/04 (Aula)
Atividade Avaliativa B – Aula 09	2,5 na AV2	16/05
Atividade Avaliativa C – Aula 10	2,5 na AV2	23/05
Avaliação P2	5,0 na AV2	06/06 (Aula)
Avaliação P3	10,0 na AV3	20/06 (Aula)
Avaliação Digital (AVD)	10,0 na AVD	26/05~11/06
Avaliação Digital Substitutiva (AVDS)	10,0 na AVDS	16/06~24/06

Os desafios serão sempre postados no mural:

<https://padlet.com/djcaetano/segciber>

Composição da Nota AV1

- T1: nota que varia de 0,0 a 3,0
- P1: nota obtida na avaliação P1

$$\underbrace{AV1}_{0,0 \text{ a } 10,0} = \underbrace{T1}_{0,0 \text{ a } 3,0} + \underbrace{P1}_{0,0 \text{ a } 7,0}$$

Composição da Nota A''''

- Fiquei com AV1 < 4,0!

Calma!



- **Pode ser que tenha Nova Chance** (NOTA AV1)
 - Agendar/Executar: 02/05 a 13/05

$$\underbrace{AV1}_{0,0 \text{ a } 10,0} = \text{máx}(\underbrace{AV1}_{0,0 \text{ a } 10,0}, \underbrace{AVR1}_{0,0 \text{ a } 10,0})$$

Informações: <https://portal.estacio.br/novachance/>

Composição da Nota AV2

- T2: nota que varia de 0,0 a 5,0
- P2: nota obtida na avaliação P2

$$\underbrace{AV2}_{0,0 \text{ a } 10,0} = \underbrace{T2}_{0,0 \text{ a } 5,0} + \underbrace{P2}_{0,0 \text{ a } 5,0}$$

Composição da Nota AV2

- Fiquei com AV2 < 4,0!

Calma!



- **Pode ser que tenha Nova Chance** (NOTA AV1)
- Agendar/Executar: 12/06 a 17/06

$$\underbrace{AV2}_{0,0 \text{ a } 10,0} = \text{máx}(\underbrace{AV2}_{0,0 \text{ a } 10,0}, \underbrace{AVR2}_{0,0 \text{ a } 10,0})$$

Informações: <https://portal.estacio.br/novachance/>

Composição da Nota AV3

- P3 é a nota obtida na avaliação P3 (PNI).

$$\underbrace{AV3}_{0,0 \text{ a } 10,0} = \underbrace{P3}_{0,0 \text{ a } 10,0}$$

Composição da Nota AVD

- A AVD é composta simplesmente da nota obtida na avaliação AVD, que é uma Prova que Digital sobre o Conteúdo Digital da Disciplina:
 - AVD: 26/05 a 11/06
 - AVDS: 16/06 a 24/06

$$\underbrace{AVD}_{0,0 \text{ a } 10,0} = \text{máx}(\overbrace{AVD}^{0,0 \text{ a } 10,0}, \overbrace{AVDS}^{0,0 \text{ a } 10,0})$$

Critério de Aprovação

A = Maior nota entre { **AV1** , **AV2** , **AV3** }

B = Segunda maior nota entre { **AV1** , **AV2** , **AV3** }

C = Maior nota entre as **AVDs**

Critérios de Aprovação (TODOS precisam ser atendidos)

1) **A** \geq 4,0; **B** \geq 4,0; **C** \geq 4,0

2) **A** + **B** + **C** \geq 18,0

3) Frequência \geq 75%

(Média 6,0!)

(Cuidado!)

de prova!

e férias mais cedo!

ATENÇÃO: Se você tiver mais que uma nota AVx ou AVD abaixo de 4,0, ainda que o SIA aponte uma média maior que 6,0, você estará **REPROVADO!**

Reforço de Estudo

- Aulas complementares de apoio
 - Prepara AV1: 09/04 – Aula ONLINE com hora predefinida!
 - Prepara AVD: 21/05 – Aula ONLINE com hora predefinida!
 - Prepara AV2: 28/05 – Aula ONLINE com hora predefinida!

<http://prepara.estacio.br/presencial>

- Resumo dos programas de reforço:

<https://portal.estacio.br/reforcoacademico/>



BIBLIOGRAFIA E FONTES DE INFORMAÇÃO

Bibliografia Básica



- **Segurança de Computadores – Princípios e Práticas**
 - Stallings (Minha Biblioteca - 978-85-352-6449-4)
- **Hackers Expostos: Segredos e Soluções para a Segurança de Redes**
 - Dscambray; McClure; Kurtz (Minha Biblioteca - 978-0-07-178028-5)
- **Segurança de Computadores e Teste de Invasão**
 - Basta; Basta; Brown (Minha Biblioteca - 978-0-8400-2093-2)

Bibliografia Complementar



- **Redes de computadores: uma abordagem top-down**
 - Froputan; Mosharraf (Minha Biblioteca - 978-85-8055-169-3)
- **Segurança de Redes sem Fio: Guia do Iniciante**
 - Wrightson (Minha Biblioteca - 978-0-07-178028-5)
- **Redes de Computadores e Internet**
 - Comer (Minha Biblioteca - 978-0-13-358793-7)

Material de Aula



- **Apresentações e outros itens de estudo**

<https://www.caetano.eng.br/>

11/02/2022, 10:15
00158955

Prof. Caetano

Home **Ensino** Publicações Pessoal

Nesta seção você encontra acesso ao material didático desenvolvido pelo Prof. Caetano para os cursos já ministrados. O material está dividido por períodos, visto que o material dos outros semestres provavelmente não está atualizado.

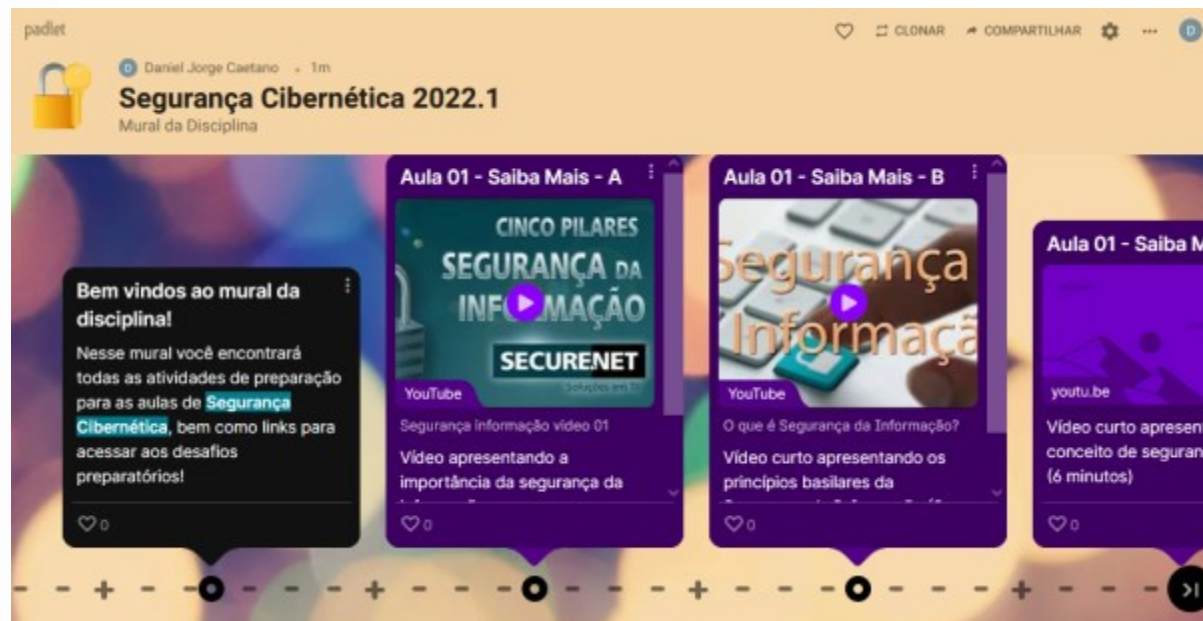
- **Selecione o ano/semestre atual**
- **Clique no nome da disciplina**

Material de Estudo



- Conteúdo e atividades de preparação

<https://padlet.com/djcaetano/segciber>



Aula NN
Saiba Mais

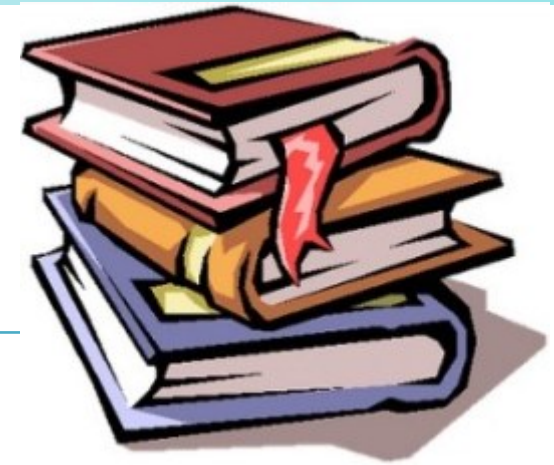
Aula NN
A Seguir...

Aula NN
Desafio

Atividade Autônoma Aura

ATENÇÃO: As postagens mais novas estarão à direita!

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2022a/ara0076.php (Segurança Cibernética – Aula 01)
Minha Biblioteca	<ul style="list-style-type: none">• Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 7 a 9;• Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2), págs 1 a 11.
Material Adicional	<ol style="list-style-type: none">1) O que é Segurança da Informação? https://youtu.be/OrtRqR_mw2) Segurança informação video 01 https://youtu.be/ZD66EMgB1FA3) Segurança Cibernética: Funcionamento e Exemplos https://youtu.be/mLWd6kO2Udk4) Você sabe o que é CIBERSEGURANÇA? https://youtu.be/CU2yQxzkvFg



IMPORTÂNCIA DAS INFORMAÇÕES

Importância da Informação

- Necessidades das empresas
 - Saber fazer
 - Aprimorar o que faz
 - Conhecer a quem vender
 - Satisfazer aos clientes.
- Tudo isso exige informações
 - São essenciais para os negócios!
 - Informações são ativos!



Importância da Informação

- Informações de pessoas físicas
 - Dados pessoais
 - Informações bancárias
 - Informações operacionais
 - Internet das Coisas (IoT)
 - Automação residencial
 - Sistemas de vigilância
 - ...



Importância da Informação

- O mundo mudou muito nas últimas décadas
 - Documentos e processos são digitais: nuvem
 - Todos os dispositivos “sempre online”!



Importância da Informação

- Informação em constante risco
 - É preciso proteger os negócios!
 - Marco Civil da Internet
 - Lei Geral de Proteção de Da
- Isso é suficiente?
 - O que fazer?





RECORDANDO:

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Princípios Fundamentais

- Equação fundamental da segurança

$$\textit{Praticidade} = \frac{1}{\textit{Segurança}}$$

- Objetivo: garantir
 - **Confidencialidade**
 - **Integridade**
 - **Disponibilidade.**

Princípios Fundamentais

- Qual a preocupação em cada caso?
 - Confidencialidade
 - Informação protegida da visualização não autorizada
 - Controle da coleta e compartilhamento de informações
 - Integridade
 - Informação protegida do manuseio não autorizado
 - Sistemas protegidos de adulteração de suas funções
 - Disponibilidade
 - Informação deixa de estar acessível no momento necessário



Princípios Fundamentais

- O que configura a quebra em cada caso?
 - Confidencialidade
 - Exposição de informações a pessoas não autorizadas
 - Integridade
 - Sistema ou informação manipulada/destruída sem autorização
 - Disponibilidade
 - Indisponibilidade do sistema ou informação no momento de uso



Preocupações Adicionais

- Preocupações decorrentes:
 - Autenticidade
 - Confiabilidade do conteúdo e autoria
 - Os autores são quem dizem ser
 - Os dados transmitidos são genuínos
 - Determinação de responsabilidade
 - Irretratabilidade / Não-repúdio
 - Registros para apuração de responsabilidades



Magnitude dos Impactos

- **Baixa**: Efeito adverso limitado nas operações, ativos ou indivíduos
 - Não inviabiliza a execução das tarefas, mas afeta a efetividade das ações
 - Dano desprezível aos ativos organizacionais
 - Perdas financeiras insignificantes
 - Dano reduzido a indivíduos
- **Moderada**: Efeito adverso sério nas operações , ativos ou indivíduos
 - Não inviabiliza a execução das tarefas, mas afeta muito sua efetividade
 - Dano significativo aos ativos organizacionais
 - Perdas financeiras significativa
 - Dano significativo a indivíduos, sem ferimentos sérios ou ameaças à vida
- **Alta**: Efeito adverso catastrófico nas operações, ativos ou indivíduos
 - Praticamente inviabiliza a execução das tarefas
 - Grande dano aos ativos organizacionais
 - Grandes perdas financeiras
 - Dano grave a indivíduos, envolvendo ferimentos sérios ou ameaças à vida



Exemplos de Magnitudes

- Confidencialidade
 - Alta: informações salariais e familiares
 - Média: projetos em que um funcionário trabalhou
 - Baixa: curriculum vitae de um funcionário
- Integridade
 - Alta: informações hospitalares sobre alergias
 - Média: desfiguração de um fórum de *hobbistas*
 - Baixa: informações de votações anônimas online
- Disponibilidade
 - Alta: sistema de refrigeração de reatores nucleares
 - Média: site informativo de uma universidade fora do ar
 - Baixa: site para consulta a lista telefônica online fora do ar



CONHECENDO OS ADVERSÁRIOS

Conhecendo o Adversário

- Crackers
 - Muito conhecimento em TIC
 - Redes com fio
 - Redes sem fio
 - Telefonia
 - Conhecimento avançado de programação
 - Conhecimentos de eletrônica, psicologia etc...
 - Ação: **quebra da legalidade**



Hackers x Crackers

- Público: Hackers = Crackers
 - Mas a comunidade não entende *assim*
- Hackers
 - Muito conhecimento em TIC
 - Redes com fio
 - Redes sem fio
 - Telefonia
 - Conhecimento avançado de programação
 - Conhecimentos de eletrônica, psicologia etc...
 - Ação: **SEM quebra da legalidade**



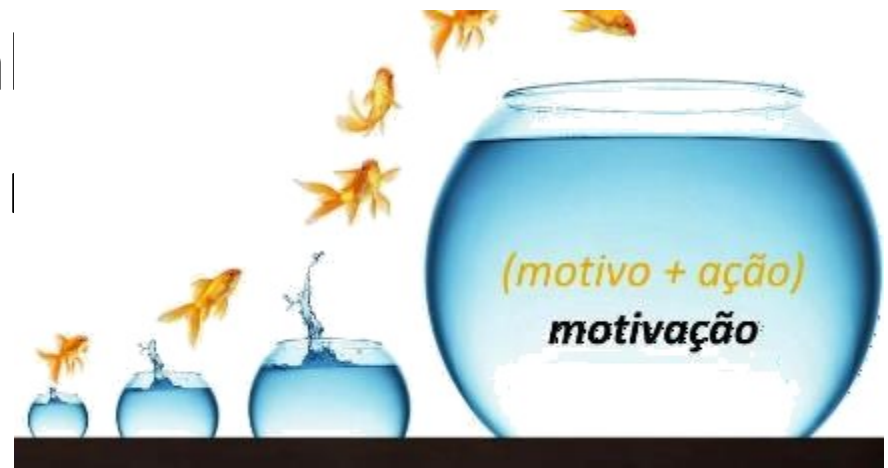
Atuação Legal: Hackers

- Identificação e correção de falhas
 - Contratados para isso
- Exemplos de tarefas
 - Análise de código
 - Teste de Invasão (*pentesting*)
 - Exploits
 - Metaexploits



Motivações dos Hackers e Crackers

- Curiosidade
- Paixão por quebra-cabeças
- Reconhecimento e fama
- Vingança
- Ganho financeiro
 - É sempre uma motivação ruim?
- Razões ideológicas (patriotismo etc.)
 - É sempre uma motivação ruim?
- ...



Classificação da Comunidade

- Na terminologia da comunidade
 - Chapéu Branco (White Hat) - Hacker
 - Chapéu Preto (Black Hat) - Cracker
 - Chapéu Cinza (Gray Hat)

black

dos, sen

s “no

resa con



Classificação “Formal”



- Novatos (n00b)
 - Habilidades muito limitadas em conhecimento e capacidade de programação
 - Dependem e confiam em “kits” para os ataques
 - Podem causar mais danos do que imaginam, por ignorância sobre os ataques que praticam
 - Motivação principal é a notoriedade e a fama

Classificação “Formal”

- Cyberpunks (Punks Cibernéticos)
 - Desenvolvem seus próprios softwares
 - Compreendem os sistemas que atacam
 - Envolvem-se em roubos de senha, cartão e fraudes em telecomunicações
 - Motivação principal é a notoriedade, mas em geral possuem também motivação ideológica



Classificação “Formal”



- Internos
 - (Ex-)Funcionários Descontentes
 - Usam seu conhecimento e permissões nos sistemas
 - **Maior fonte de ameaças à segurança**
 - Ladrões menores (funcionários, consultores...)
 - Conhecem computação e falhas do sistema da empresa
 - Motivados por ganância ou necessidade

Classificação “Formal”

- Coders (Codificadores)
 - Mentores dos novatos
 - Escrevem scripts e ferramentas para outros
 - Motivados pelo senso de poder e prestígio
 - Perigosos por suas motivações ocultas
 - Ferramentas que desenvolvem costumam serem *trojans*



Classificação “Formal”

- Criminosos Profissionais
 - Especializados em espionagem corporativa
 - Costumam atuar por contrato (aluguel)
 - Altamente motivados e treinados
 - Não poupam investimentos leitura e equipamentos
 - Atuam com tecnologia de ponta



Classificação “Formal”

- Terroristas Cibernéticos
 - Atuam em todos os tipos de ataques destrutivos
 - Motivações normalmente político-ideológicas
 - Possuem muitos recursos e conhecimento
 - Crescimento grande desde o fim da guerra-fria



Classificação “Formal”

- Hacktivistas
 - Querem erradicar entidades ou causas “do mal”
 - Por definição, agem por ideologia
 - Tentam interferir em questões políticas



Classificação “Formal”

- Hackers da Velha Guarda
 - Normalmente agem pelo desafio intelectual
 - Possuem um desrespeito enorme pela propriedade
 - Muitas vezes parecem não ter intenção criminosa



Histórico da Atuação Hacker/Cracker

- **1940** – Surgem com os computadores
- **1950** – Conceito moderno: uso diferenciado da tecnologia para resolver problemas
- **1960** – Sistemas multiusuário: contornar controle de acesso
- **1970** – Telecomunicação: telefonar de graça
- **1980** – Modems e o *hacking* de comunicações
 - Virus, vermes, trojans... Uso de BBSs e Internet
- **1990** – Internet: difusão maior de vírus
- **2000** – eCommerce: fraudes, scams...

Entidades Certificadoras

- Associação de Controle e Auditoria de Sistemas da Informação (ISACA): www.isaca.org
- EC-Council: www.eccouncil.org/
- ISC2: www.isc2.org
- CompTIA: www.comptia.org/certifications/security
- Certificação de Garantia da Informação Global (GIAC): www.giac.org/certifications/cyber-defense



ATIVIDADE

Atividade

- Discussão
- Alguém tem conhecimento de algum tipo de ataque que tenha impactado a segurança da informação em alguma empresa?
- Quais princípios de segurança da informação foram afetados nesse ataque?
- Qual o impacto que isso teve nos negócios da empresa?



ENCERRAMENTO

Resumo e Próximos Passos

- Planos de Ensino e Aula, datas e critérios
 - Principais fontes de informação
 - Princípios da Segurança da Informação
 - Hackers x Crackers – Questão Ética
 - **Pós Aula:** Saiba Mais, A Seguir e Desafio!
 - No mural: <https://padlet.com/djcaetano/segciber>
-
- Principais mecanismos de proteção
 - O que é melhor em cada caso?



PERGUNTAS?