
# GRIS

## Grupo de Resposta a Incidentes de Segurança


# OLÁ,

## Eu sou Sidney

Diretor do GRIS

Aluno de Ciência da Computação na UFRJ

Membro do Laboratório de Redes e Multimídia(Labnet)

Desenvolvedor do Núcleo de Inovação do CSS (Inova-CCS)

E,

# Eu sou Breno

Diretor do GRIS e graduando em Engenharia da Computação & Informação

Membro da Epic Leet Team

Membro da Equipe Siga

*[...] Oferecer orientação e suporte acadêmico aos alunos da UFRJ, sem fins lucrativos, no que tange a temática da Segurança da Informação em todas as suas vertentes, nos âmbitos de Ensino, Pesquisa e Extensão [...] ”*

RIA

(Resposta a Incidentes e Acidentes)

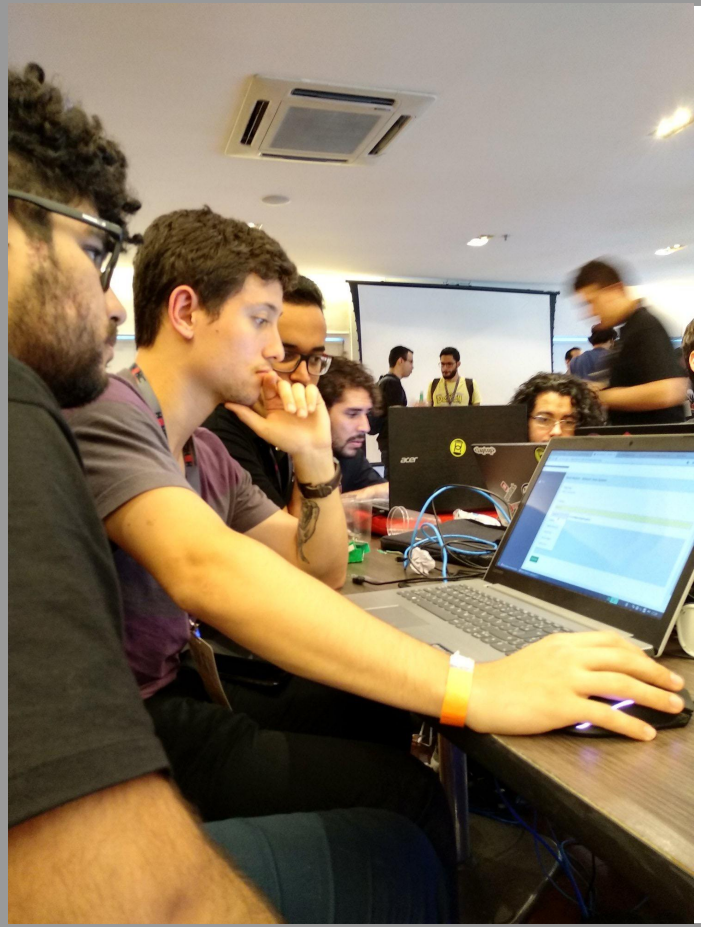
RSS

(Redes, Sites e Sistemas)

EDP

(Ensino, Desenvolvimento e Pesquisa)

**Competições**



# Capture the Flag (CTF)

- Competição que testa conhecimentos técnicos e raciocínio lógico dos hackers.
- Existem dois tipos mais comuns:
  - Tipo "*Jeopardy*": uma lista de desafios que são resolvidos em qualquer ordem. Cada desafio possui uma bandeira com pontuações diferentes de acordo com o nível do desafio.
  - Tipo "*Attack/Defense*": Cada time recebe uma *Virtual Machine* e deve proteger com *patchs* se proteger enquanto ataca seus oponentes para capturar a bandeira.


04/10/2019


26-27/10/2019


UFRJ
H2HC
ENTEST

# Disclaimer e Recomendações

- O conteúdo dessa palestra causa vício
- Use o bom senso SEMPRE
- Utilize SEMPRE ambientes controlados
- Transparência e ética SEMPRE
- Tente sempre entender
  Como? Onde? Quando? Porque? O que?
- Atualize e atualize-se
- Políticas de senha, Privacidade... WPS DESLIGADO
- SOFTWARE LIVRE

# Pentest

- Teste de Penetração, em tradução literal
- WhiteBox:

  **Possui conhecimento total da aplicação**

- GrayBox:

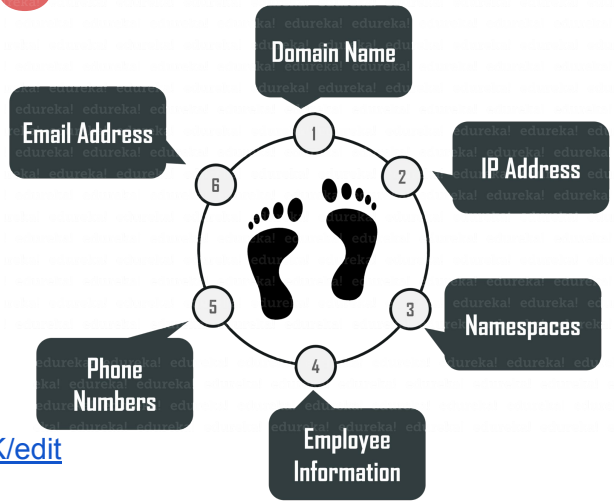
  **Possui parcial conhecimento da aplicação**

- BlackBox:

  **Simula a realidade do “hacker”, pois não tem conhecimento sobre a aplicação**

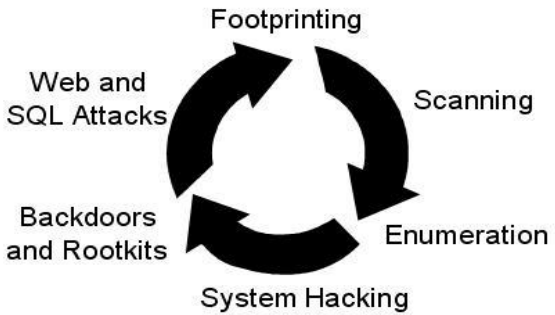
# Footprinting Passivo

- Google hacking ... Shodan
- Maltego...theharvester
- Whois
- Redes sociais
- OSINT
- https://drive.google.com/file/d/1JoBmQDAs9GlcIhd5Q0rOh8NZCyrIlonK/edit

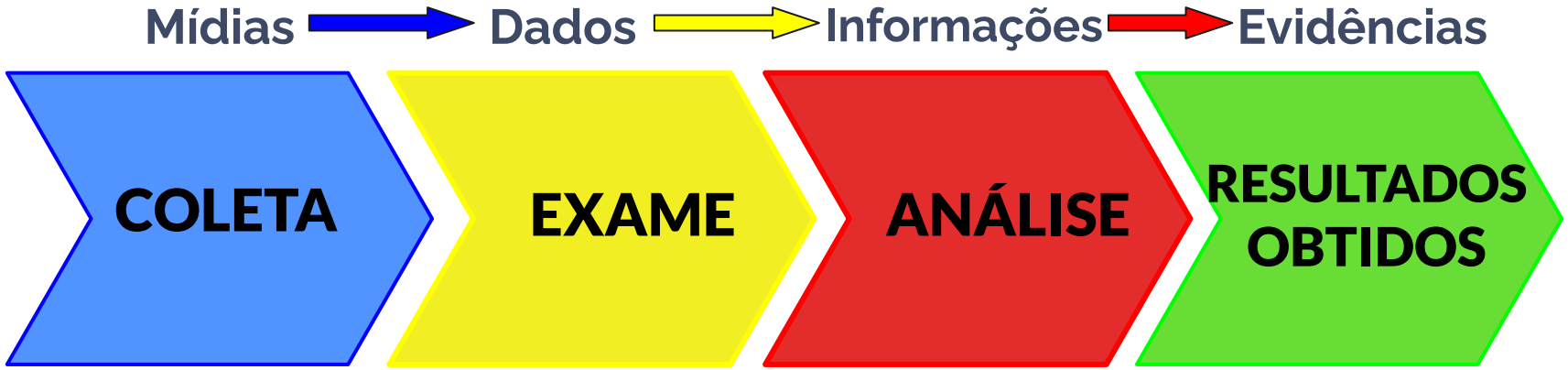


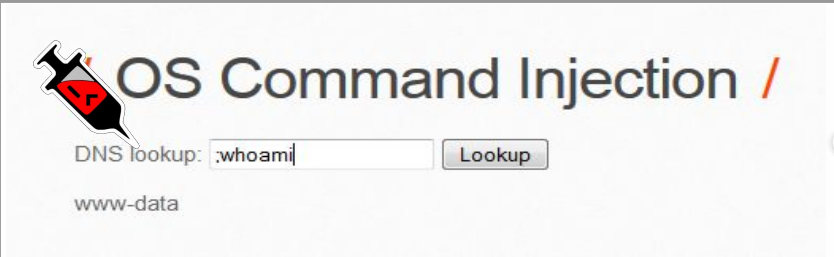
# Footprinting Ativo

- Scan de portas
- Coleta de lixo
- Engenharia Social
- TailGating



# Forense

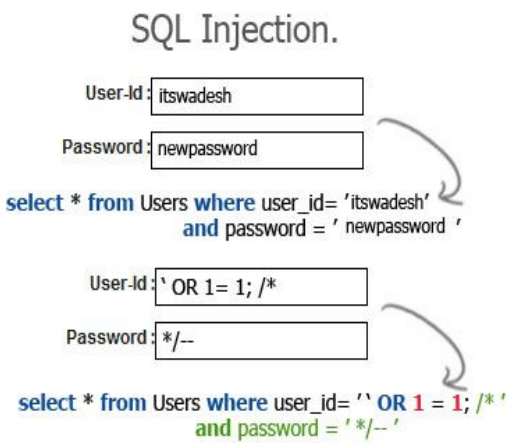

Mídias
Dados
Informações
Evidências
COLETA
EXAME
ANÁLISE
RESULTADOS OBTIDOS





# Hackearam meu site

- Sql-injection
- XSS
- Command injection
- LFI
- ...



# OBRIGADO



sid@dcc.ufrj.br


breno_css@poli.ufrj.br


@outeirosid