Segurança - Trabalhos Finais e Alunos

Disciplina	**Segurança em Redes de Computadores**
Professor:	**Rafael Timóteo de Sousa Júnior**
Monitor:	**Valério Martins (valerioaymoremartins@gmail.com)**

Obs: Os trabalhos de número 01) até 05) serão apresentados em 06/12/2018
e os trabalhos de número 06) até 09) serão apresentados em 08/12/2018
(a última semana é para exposição final do Professor Titular)

01) AES (algoritmo de encriptação por bloco de chave simétrica)

- **JOÃO PAULO FERNANDES**
- **GUSTAVO MADRUGA**

- O que é e origem
- algoritmo / modelo tridimensional
- transformação (SubBytes, ShiftRows, MixColumns, AddRoundKey)
- derivação de chaves
- decriptação
- vulnerabilidades
- aplicações

02) APT (Advanced Persistent Threats)

- **CAIO VITOR**
- **JOÃO FIUZA**
- **RODRIGO ANDRADE**

- Detalhamento A...P...T...
- Características
- Modelo (Reconhecimento (Footprint), Escaneamento (Scanning), Exploração (Exploiting). Limpar traços / evidências)
- Defesas contra APT
- Exemplos (Stuxnet, Duqu, Flame, etc.)

03) Firewall Bridge

- **ALINE ALVES**
- **GUSTAVO VIANA**
- **JOÃO PAULO BOTELHO**

- O que é
- Detalhamento (Filtro de Pacotes, Firewall de Estado de Sessão, Proxy Firewall, Firewall de Aplicação)
- Cenários e pacotes

04) SSL/TLS

- **FELIPE ALONSO**
- **ADRIANO BRANDÃO**
- **THAIS CARVALHO**

- No protocolo TCP/IP
- Arquitetura (Handshake, Record, Alert, Change Chypher Spec, Troca de Mensagens,
- SSL e TLS: Diferenças entre si / SSL: Versões e diferenças / TLS: Versões e diferenças
- Estudo de Caso: (Interceptação da chave simétrica, Falsificação de chave pública, Ataque de reprodução, Handshaking/Man-in-the-middle)

05) Certificação Digital:

- **GABRIELA SARPI**
- **KADICHARI FARIAS**
- **WELLINGTON CAVEDO**

- Detalhamento
- Assinados e Auto-assinados
- ICP/PKI
- X.509
- Tipos (A1/S1, etc) + Vulnerabilidades
- Confiabulidade

06) One Time Pad (técnica de encriptação – cifra de uso único):

- **FELIPE PEREIRA**
- **CAIO RONDON**
- **MIRELLA SALES**
- **RAFAEL ZERBINI**

- Detalhamento
- Cifras de Bloco e de Fluxo e One Time Pad
- Exemplos e Uso (algorítmo)
- Vulnerabilidades / Problemas

07) IPSec (IP Security)

- **RÔMULO MAGALHÃES**
- **PEDRO GABRIEL**
- **JUNIA PEREIRA**
- **LUCAS COELHO**

- Detalhamento
- Gerenciamento de Chaves
- Composição do IPSec (Cabeçalho, payload)
- Funcionamento (autenticação, operação (transporte. tunel, etc), etc)
- Exemplos e Uso (algorítmo)
- Vulnerabilidades / Problemas

08) Redes I2P (Invisible Internet Project)

- **ARTHUR CARDOSO**
- **ARTHUR COSTA**
- **RAYSSA**

- O que é e origem
- Detalhamento (Tuneis, BD de redes, Criptografia, Pilha de protocolo)
- Acesso e funcionamento / - Exemplos e Uso
- Vulnerabilidades / Problemas

09) VPN (rede de acesso restrito que utiliza um meio de comunicação público)

- **FELIPE BARRETO**
- **JOÃO VITOR MENDES**
- **LUCAS GARCIA**

- Detalhamento e tipos
- Funcionamento (acessos remotos e P2P, criptografia e tunelamento)
- Implementações no Mercado e Uso
- Vantagens e desvantagens