Facens

Pós-Graduação
Segurança Cibernética

Lenovo™

Facens

Desafio Lenovo


Proposta

Proposta

Construir um ambiente virtualizado para simulação de testes de invasão e monitoramento de ataques. O ambiente será composto por máquinas virtuais e sistemas embarcados onde dever ser possível o estudo cenários de ataques, ferramentas e monitoria de eventos.


Imersão

Imersão

- A área de Segurança Cibernética é multidisciplinar e envolve o conhecimentos diversos como sistemas operacionais, ferramentas, desenvolvimento de softwares, dentre outros
- Assim a proposta do **Desafio Lenovo** é introduzir os alunos do programa **Connors-Facens** em um ambiente onde eles terão contato com cenários simplificados, mas coerentes, com o desafios e tecnologias utilizadas no dia a dia das empresas

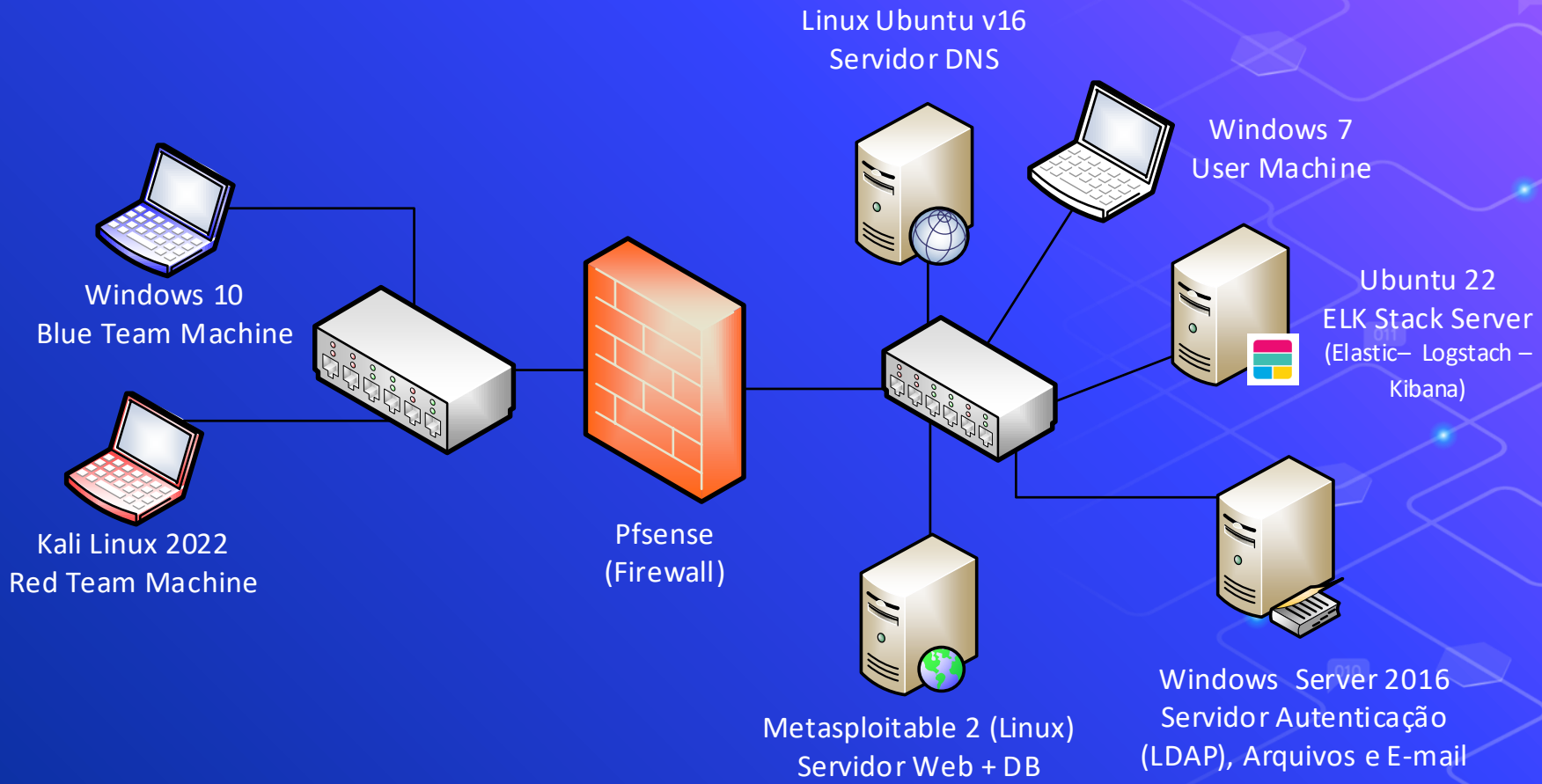

Fase 01
Desafio
Lenovo

Desafio Lenovo – Fase 01

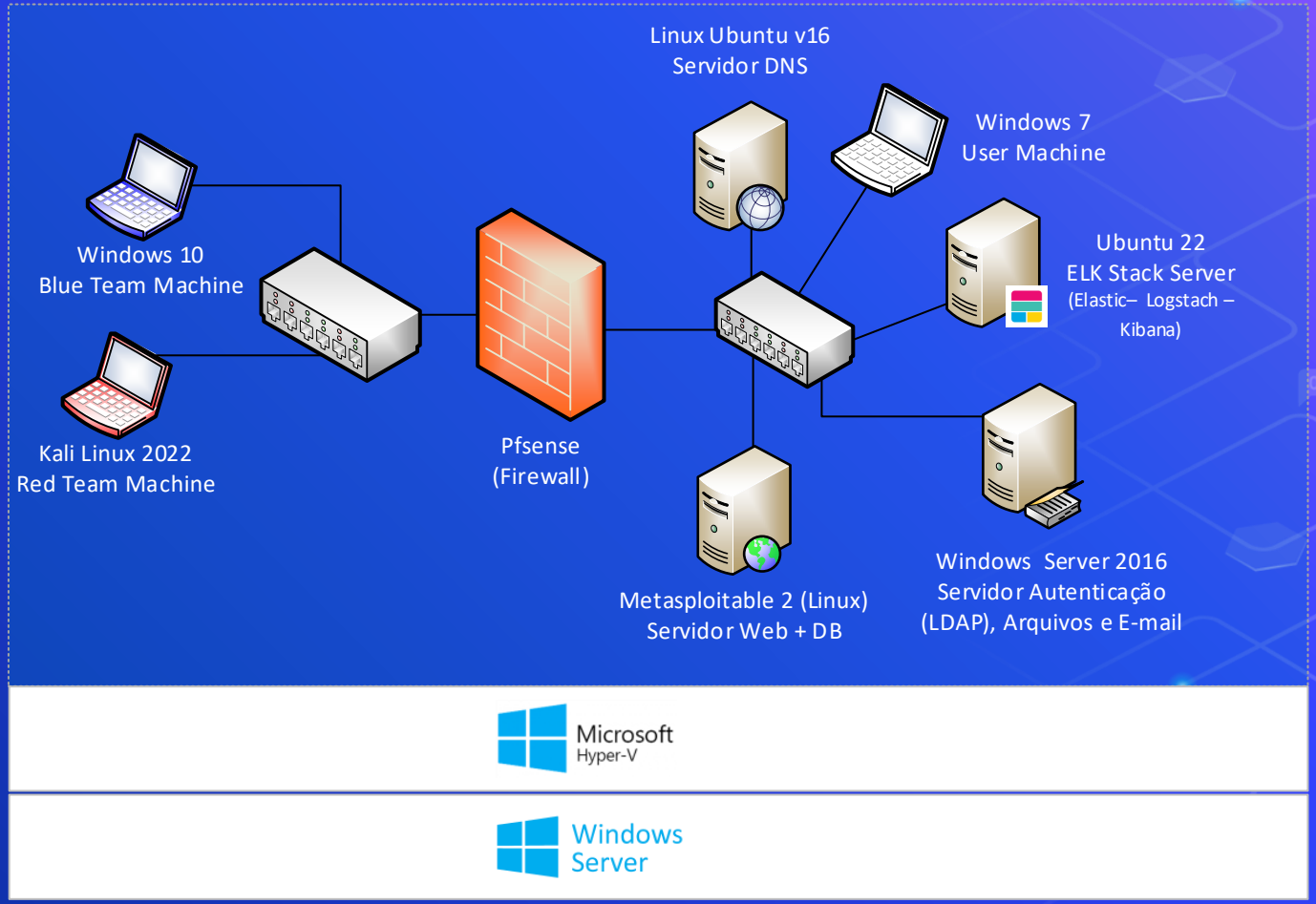
Facens

- As equipes deverão construir um ambiente virtualizado e um sistema de monitoramento de incidentes para este ambiente, que possibilite a criação de cenários de simulação e a detecção de incidentes nestes cenários
- Após a criação do ambiente serão propostos desafios de levantamento de vulnerabilidades, teste de invasão, exploração de vulnerabilidades, ataques de vírus que deverão ser detectados pelos sistemas de monitoramento

Ambiente de Simulação



Estrutura para suporte ao Ambiente



Conectividade do Ambiente

- O Servidor Web e de DNS são acessíveis tanto na rede interna quanto externa. As demais máquinas não.
- O computador de usuário (User Machine) pode acessar computadores fora da rede, mas não pode ser acessado remotamente
- O computador Blue Team pode acessar qualquer computador da rede interna
- O computador Red Team pode acessar apenas o Servidor Web e Servidor de DNS
- Todas as máquinas devem ter um endereço de IP Fixo
- As máquinas devem estar em uma rede sem acesso a internet e isolada das demais redes da Facens

Serviços do Ambiente

Facens

- O firewall pfsense deve implementar as regras de conectividade
- Toda a autenticação de usuários deve ser feita pelo Servidor de LDAP (incluindo as máquinas Linux)
  - Os arquivos dos usuários devem ser armazenados neste servidor e compartilhados com as demais máquinas
- O servidor de DNS deve prover a tradução de nome de domínios para as máquinas da rede interna
- Ao menos, o servidor Web e o servidor de E-mails devem ter um domínio (url) mapeado pelo servidor de DNS
- O ELK Stack Server deve fazer o registro de Logs de todas as máquinas da rede interna conforme a estratégia de monitoria definida

Regras da Simulação

- Red Team é responsável por implementar teste de invasão (coleta de dados, exploração de vulnerabilidades, roubo de dados, acesso não autorizados etc.)
  - É permitido o comprometimento dos servidores, alteração e roubo de arquivos
- O Red Team possui apenas o endereço IP/url do servidor Web e Dns. Os demais IP´s não devem ser divulgados a eles pelo Blue Team
- Blue Team é responsável pela segurança do ambiente, especificamente pela análise dos eventos da rede por meio do ELK Server
  - O Blue Team deve identificar ataques por meio dos logs coletados pelo ELK Server.
  - A configuração dos Agentes e da coleta de eventos é de responsabilidade do Blue team

Regras da Simulação (cont.)

- O Blue Team tem acesso total as todas as máquinas exceto a Kali Linux (Red Team)
- As versões indicadas para sistemas operacionais devem ser assim como as distribuições. Na impossibilidade de instalar a versão indicada, deve-se instalar a penúltima versão lançada. Nunca a mais recente.
- Exceto pela máquina Kali Linux, todas as demais não devem instalar patchs de atualização e/ou ter este serviço habilitado por padrão
- Os alunos irão se alternar entre o Blue e Red Team entre as rodadas de simulação
- Após a configuração do Ambiente e antes do início da rodada de simulação, um snapshot, de cada máquina virtual deve ser salvo, para possibilitar a simulação em condições reais para o momento de troca dos times

Regras da Simulação (cont.)

- Devem ser criados, além do administrador, um usuário comum e um usuário com privilégios de administrador para cada servidor e máquina do ambiente (exceto para o Kali Linux)
- O sistema de envio e recebimento de e-mails deve estar operante. Cada vez que um usuário receber um e-mail, este deve ser lido, o conteúdo aberto e/ou baixado para a máquina


E agora ????

Fases do Desafio

Simulação

3

Alunos serão divididos em dois times (Red e Blue) que executarão respectivamente ataques e detecção de ataques

Construção do Ambiente

2

A partir dos conhecimentos adquiridos nos Workshops os alunos, divididos em grupos, irão criar o ambiente para a simulação

Workshops Temáticos

1

Aquisição de Conhecimentos que preparam para a construção do ambiente e para o desafio

Fases do Desafio

- Temas:
  - Hyper V
  - Windows server
  - Linux
  - Pfsense
  - ELK Stack
  - Kali Linux

Formato do Workshop

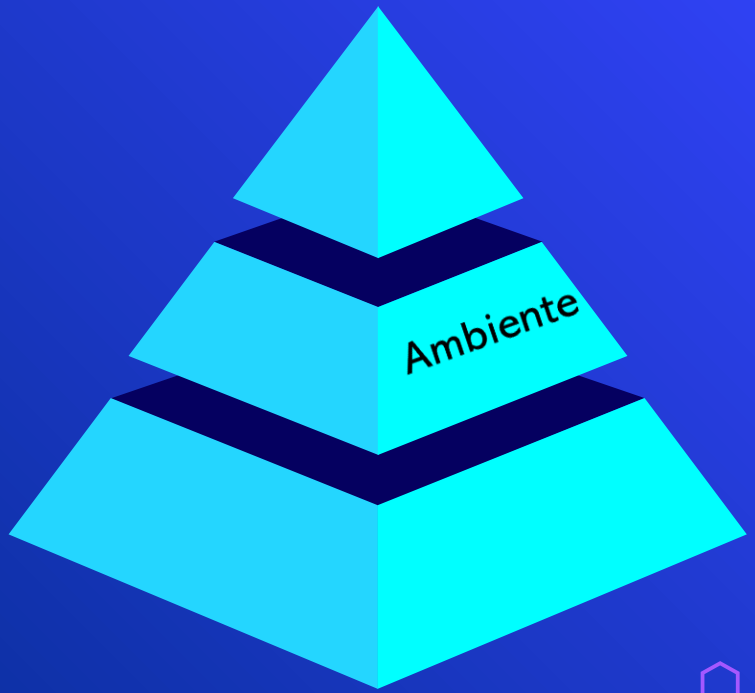
- Duração: 4h horas
- Alunos serão divididos em 5 duplas
- No workshop deve contemplar
  - Aula expositiva sobre o tema
  - Demonstração prática dos pontos abordados
  - Material previamente disponibilizado (slides, textos, etc.)
  - Uma ou mais dinâmicas no decorrer do Workshop visando demonstrar práticas sobre a ferramenta ou tecnologia a apresentada
- Tempo de aprendizado e elaboração do workshop : **2 semanas + 1 para realização dos Workshops**

Conteúdo mínimo do Workshop

Facens

	Tema	Conteúdo Mínimo
1	Hyper V	Definição. Instalação e Configuração. Criação de Máquinas Virtuais. Gestão de máquinas virtuais.
2	Windows Server	Instalação e Configuração. Criação de usuários e permissões. Exemplo de Instalação de serviços. Tarefas de configuração gerais do servidor
3	Linux	Instalação e Configuração. Criação de usuários e permissões. Exemplo de Instalação de serviços. Comandos do Linux. Arquivos de configuração.
4	pfsense	Definição e Utilização. Instalação e configuração. Criação de regras de filtragem de pacotes.
5	ELK Stack	Definição e Utilização. Instalação e configuração do Ambiente de monitoramento. Interface de análise dos logs e eventos.
6	Kali Linux	O que é a Distribuição. Funcionalidades. Etapas de um Pentest. Documentação.

Fases do Desafio



- Criação das máquinas Virtuais
  - DNS e pfsense (dupla)
  - Máquinas de usuário, Red/Blue Team e Servidor Web (dupla)
  - Servidor ELK (dupla)
  - Servidor Autenticação (LDAP) (trio)
- Prazo : 2 semanas

Fases do Desafio

- Divisão dos alunos em dois times
  - Red Team (Ataque)
    - Identificar e executar ações para coleta de informações e acessos não autorizados
    - Registra por meio de um relatório todos os dados coletados e invasões bem sucedidas
  - Blue Team (Defesa)
    - Monitorar e identificar ataques
    - Elaborar um relatório contendo todo os eventos de ataques detectados e possíveis medidas para bloquear e prevenir o ataque no futuro

Fases do Desafio (cont.)

- Prazos
  - 1 semana para preparação da estratégia de ataque (RT) e familiarização com o ELF (BT) e verificação do funcionamento das máquinas
  - 1 semana para o desenvolvimento da simulação
  - Após a 1ª rodada de uma semana inverte-se os componentes dos times e a simulação roda por mais 2 semanas

Equipe vencedora – Fase 01

- Pontos serão atribuídos para cada ataque/coleta de dados realizada com sucesso sem que esta tenha sido detectada no monitoramento ou pela o Blue Team
- Ao final a equipe com maior pontuação vence o desafio

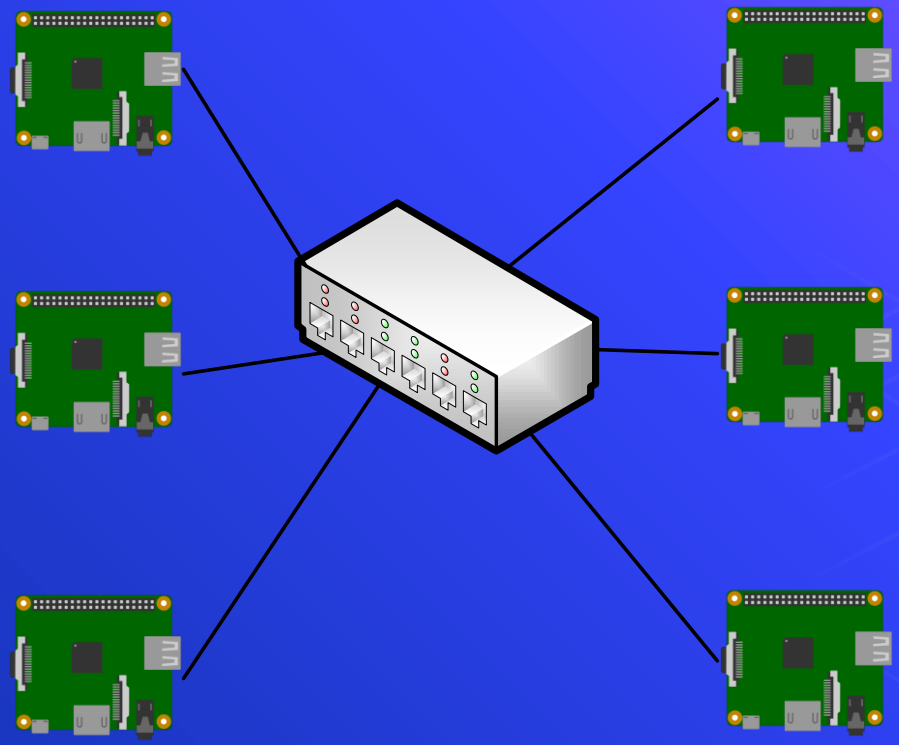

Fase 02
Desafio
Lenovo

Desafio Lenovo – Fase 02

Facens

- **Vamos complicar só um pouquinho o desafio, ok?**
- No ambiente de simulação iremos trabalhar com dispositivos com softwares embarcados
- Os dispositivos tem como objetivo atacar outros dispositivos executando ações danosas
- O cenário será configurado da seguinte forma:

Ambiente de Simulação



Galileo Trojan Bots

Galileo Defense Bots

Galileo Trojan Bot

Facens

- Galileo é uma placa da Intel que suportam a execução de sistemas operacionais e softwares
- O objetivo é configurar três placas com um sistema operacional para implementar uma ação visando infectar ou travar um bot defensivo (Galileo Defense Bot)
- Para isso, o Trojan Bot poderá:
  - Executar ataques para explorar vulnerabilidades
  - Usar vírus para infectar o sistema alvo
  - Criptografar o sistema do alvo
  - Dentre outras ações danosas

Galileo Defense Bot

Facens

- O objetivo é configurar três placas com um sistema operacional e um software para monitoramento de ataques
- Estas máquinas devem executar rotinas para alertar os administradores no caso de um ataque do Trojan Bot
- Não há a necessidade de impedir o ataque, mas sim de alertar a ocorrência deste
  - Se o ataque comprometer o dispositivo, antes de um aviso ser enviado, o ataque será considerado bem sucedido
- Deve-se utilizar o ELK como mecanismo de detecção de eventos para as placas criadas – salvo alguma limitação técnica
- No mínimo o Defense Bot deve identificar o ataque antes que seja comprometido
  - Se conseguir impedir o ataque isso será considerado um diferencial implementado pelo time

Conectividade do Ambiente

- As placas serão consideradas dispositivos confiáveis, ou seja, não há restrição de comunicação entre elas
- Todas estarão no mesmo ambiente de rede
- Todas possuem um IP fixo
- Os endereços IP são compartilhados entre as equipes

Regras da Simulação

Facens

- A única limitação de atividades está relacionada a limitação de recursos da placa
- Cada time pode escolher o melhor sistema operacional para atender a necessidade do ataque a ser implementado ou estratégia defensiva
- O Red Team ficará responsável pela criação dos Trojan Bots
- O Blue Team ficará responsável por criar os Defensive Bots
- No máximo cada time atacante pode implementar três placas para a simulação
- O ataque pode ser executado/programado para ocorrer a qualquer momento e deve ser o mais discreto possível


E agora ????

Fases do Desafio

Construção da Placa

Definição da ação a ser desenvolvida, programação da placa , configuração do SO e documentação do processo

Simulação

Implementação do ataque por um dos times e verificação do resultado

Estudo da placa Galileo

Estou sobre o funcionamento da placa, documentação programação, instalação

Fases do Desafio

- Nesta etapa não temos um Workshop, mas os alunos podem compartilhar informações
- Devem pesquisar a documentação da placa, configuração desta, gravação de dados e funcionamento do SO
- Prazo: 2 semanas

Fases do Desafio

- Nesta etapa cada grupo constrói sua placa
  - Gravação desta
  - Carregamento do SO
  - Configuração da ação de ataque
  - Documentação o bot criado
- Prazo : 2 semanas

Fases do Desafio

- Cada time irá disponibilizar as respectivas placas no ambiente que ficarão ativas durante toda a simulação
- O RT deve programar para executar as tentativas de ataque de tempos em tempos
- O BT pode criar outros agentes de análise de logs (diferentes da simulação fase 1) que julgarem pertinente
- Prazo para execução do ataque : 1 semana
- Após 1 semana é feito o levantamento das evidência do ataque e detecção e após isso os times trocam de papel (mais uma semana)

Equipe vencedora – Fase 01

- Pontos serão atribuídos para cada ataque/coleta que conseguir infectar e/ou comprometer o dispositivo adversário sem que este seja detectado pelo time adversário
- Cada equipe deve gerar evidências que comprovem o sucesso no ataque
- O Vencedor será aquele que conseguir mais pontos


Gestão do
Projeto

Gestão do Projeto

Facens

- Seguiremos o mesmo modelo utilizado nas outras atividades
- Daily, Review, Retro atividade no Jira, etc.
- O cronograma das atividades será elaborado no decorrer da semana
- Formatos e horários serão combinados com a Profa. Andreia

Obrigado!

Questões?

Luciano Freire

luciano.freire@facens.br

Andreia Leles

andreia.leles@facens.br