UnB | Mestrado Profissional em Engenharia Elétrica - PPEE

RC – Redes de Comunicações

DEPARTAMENTO:	Engenharia Elétrica-EnE/FT	
DISCIPLINA:	Redes de Comunicações	**CÓDIGO:** 366226
DATA ENTREGA:	**Segundo Cronograma Disciplina**	**TURMA:** A
PROFESSOR:	Georges Daniel Amvame-Nze, Dr.	

Projeto Final

Grupos & Avaliação

Para realização deste Projeto Final, da disciplina de Redes de Comunicação, os alunos deverão manter os Grupos conforme pré-estabelecido em sala de aula e apresentado no *CampusVirtual*. Cada Grupo deverá desenvolver um NSOC – *Network Security Operation Center*, de pequeno porte. A **Nota Máxima do Projeto será de 10,0 pontos**. Todos os passos e metodologia deverão ser criteriosamente apresentados e discutidos, com embasamento técnico-acadêmico. Recomenda-se zelar pela entrega de um trabalho altamente legível e sem Plágio. Tais medidas visam garantir o trabalho individual de cada Grupo.

Introdução

Um centro de operações de segurança de rede (NSOC) é uma instalação que abriga uma equipe de segurança da informação responsável por monitorar e analisar a postura de segurança de uma organização continuamente, e neste trabalho vocês irão representar esta equipe. O objetivo da equipe do NSOC é detectar, analisar e responder a incidentes de segurança cibernética usando uma combinação de soluções de tecnologia e um forte conjunto de processos. Os centros de operações de segurança geralmente contam com analistas e engenheiros de segurança, além de gerentes que supervisionam as operações de segurança. A equipe do NSOC trabalha em estreita colaboração com equipes de resposta a incidentes organizacionais para garantir que os problemas de segurança sejam resolvidos rapidamente durante e/ou após a descoberta. Os centros de operações de segurança monitoram e analisam as atividades dos ativos de suas redes tais como servidores, terminais de usuários, bancos de dados, aplicativos, sites e outros sistemas, a procura por atividades anômalas que possam indicar um incidente ou comprometimento de segurança da rede corporativa.

Então, como visto acima, o vosso grupo será responsável por garantir que possíveis incidentes de segurança sejam corretamente identificados, analisados, investigados e relatados graça ao seu centro NSOC.

Enunciado do Projeto *(Todos as atividades deverão ser devidamente comentadas e justificadas)*

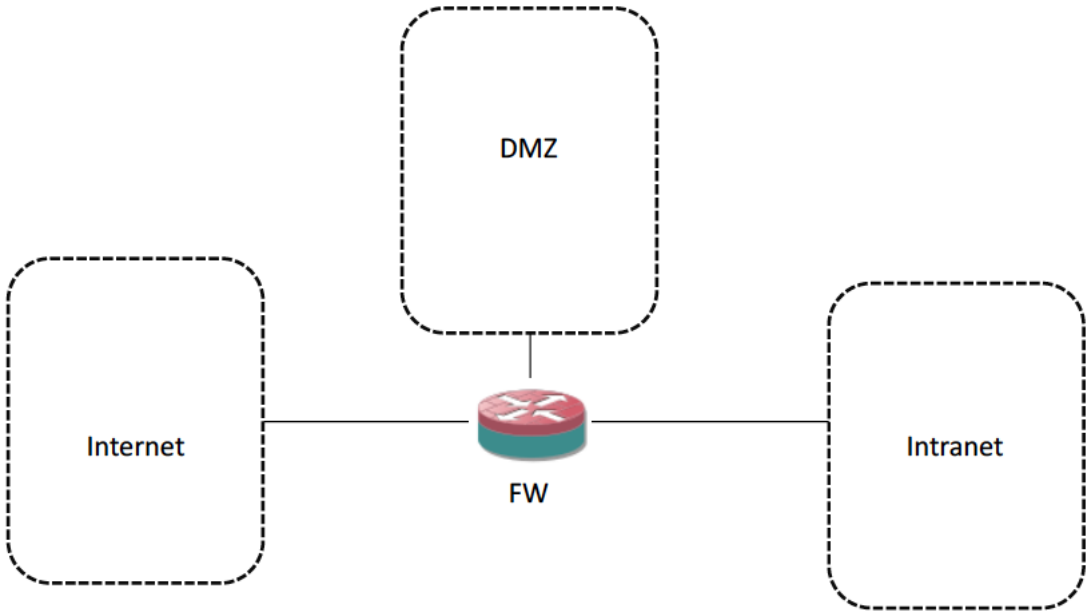

Figura 1 – Topologia a ser configurada e monitorada por cada grupo no GNS3.

Atividade nº1:

Configurar uma Topologia de Rede de acordo com o cenário da Figura 1, a partir de duas redes Básicas, distribuídas aleatoriamente nessa Intranet e/ou de acordo com o entendimento do Grupo. Justificar a escolha dos dispositivos de redes que irão compor a Infraestrutura de simulação (a mesma deverá ser totalmente operacional), e mostrar que essa Infraestrutura tem ampla conectividade com a Intranet e Internet. **(2,5 pontos)**

192.168.**Gr**.0/24 e 172.24.**Gr**.0/24, onde Gr = ID do seu Grupo no CampusVirtual.
Ex: Caso o ID do Grupo = 1 → 192.168.**1**.0/24 e 172.24.**1**.0/24

Atividade nº2:

A. Instalar e configurar um servidor ZABBIX para que o NSOC tenha um gerenciamento dos seus ativos de rede, via protocolo SNMP. A plataforma ZABBIX terá de possibilitar: **(2,5 pontos)**
   i. a descoberta dinâmica dos ativos da rede;
   ii. a visualização dos principais gráficos de desempenho dos ativos (*Igual ao do servidor ZABBIX*)
   iii. a visualização do MAPA da topologia.

iv. de mostar que quando um dos ativos ou link de comunicação da DMZ estiver desligado, o MAPA da topologia irá acusar o não funcionamento do mesmo.

Atividade nº3:

A. Com o auxílio do aplicativo *IPerf*: **(2,5 pontos)**
   i. Propor e gerar Tráfegos que simulam aplicações que fazem uso dos protocolos FTP, TCP e UDP de/para DMZ;
   ii. Analisar criteriosamente os tráfegos gerados via *Wireshark*;
   iii. Instalar e configurar o KIBANA (na porta 443) para que se possa visualizar e classificar esses tráfegos de acordo com a sua porta, protocolo, origem e destino (dentre outros parâmetros que possam, porventura, serem julgados necessários pelo entendimento de cada Grupo);

Atividade nº4:

A. Com o intuito de implementar medidas para permitir/bloquear/rastrear o acesso aos serviços da DMZ e aos dispositivos da Intranet: **(2,5 pontos)**
   i. Instalar e configurar um Firewall e Sensor IDS/IPS para gerenciar a segurança do NSOC;
   ii. Iniciar a geração de tráfego para Internet, de/para DMZ e de/para Intranet. Avalie junto aos demais integrantes do seu grupo quais medidas devem ser aplicadas para permitir ou não os tráfegos gerados. Configurar o Firewall e Sensor IDS/IPS para que as medidas de segurança se adequam a vossa regra de negócio;
   iii. Comente os resultados apresentados no iten ii, no aspecto da Segurança Cibernética e Inspeção Profunda de Pacotes oriundos da Internet, DMZ e Intranet.