INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA PERNAMBUCO Campus Igarassu	Curso Técnico em Informática para Internet	
	Segurança de Sistemas para Internet	2° período / 2018.1
	Prof. Ramon Mota	**Prática 01**

Título: Trabalhando conceitos básicos de segurança: Exemplificando o conceito de disponibilidade através de ataque de SYN flood.

Objetivo:

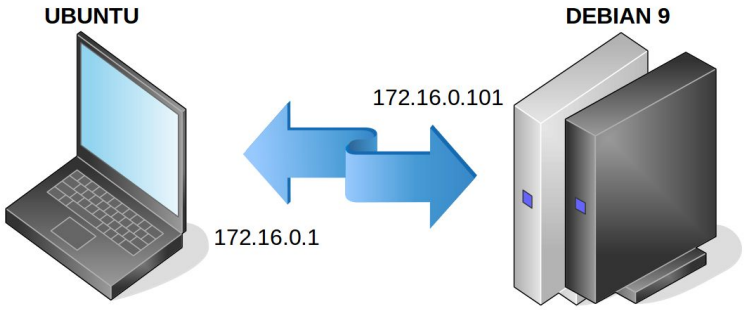
I. Exemplificar conceito básico de segurança - Disponibilidade;
II. Conhecer e praticar com ferramentas de segurança;
III. Compreender o ataque de Negação de Serviço através da técnica SYN flood.

1. Introdução

Esta prática tem como objetivo a realização de um ataque do tipo Syn Flood contra um servidor WEB (Apache). Através da prática queremos trabalhar o conceito básico de segurança da informação DISPONIBILIDADE, que neste caso é quebrado através de um pseudo ataque de negação de serviço distribuído (conhecido como Distributed Denial of Service - DDoS).

2. Cenário

Serão utilizados o sistema Ubuntu instalado no desktop do laboratório e a máquina virtual “Debian 9” disponibilizada através do Virtualbox, segundo imagem a seguir.



3. Prática

Para esta prática, a máquina “Debian 9” será o alvo e o “Ubuntu” será o atacante.

3.1 Preparação do alvo

Para realizar o pseudo ataque com sucesso teremos que desabilitar a proteção padrão do S.O. usando o comando a seguir.

```
#sysctl -w net.ipv4.tcp_syncookie=0
```

Teste se o Servidor Apache na máquina alvo está rodando. Faça o teste usando um navegador para acessar o endereço da máquina “Debian 9” - 172.16.0.101.

3.2 Executar ataque contra alvo

Verificar se a ferramenta hping3 está instalada no “Ubuntu”. Caso não esteja, instale com o comando a seguir. Lembre-se de executar os comando como usuário root.

```
#apt-get install hping3
```

Após instalação da ferramenta hping3, execute o comando abaixo para realizar o ataque.

```
#hping3 IP_ALVO -p 80 -S --faster --rand-source
```

Algumas detalhes do comando:

`-p 80`	Define a porta alvo do ataque (o serviço WEB).
`-S`	Cria pacotes TCP com a *flag* SYN ativa.
`--faster`	Envia os pacotes gerados a cada microsegundos.
`--rand-source`	Define de forma randômica e aleatória os endereços IPs de origem dos pacotes.

Após poucos segundos, e se tudo foi executado corretamente, o servidor apache na máquina alvo deve estar inacessível. **Teste, tentando acessar novamente a página WEB do alvo**.

4. Resultados

Como resultado do ataque, o servidor WEB apache não consegue responder as requisições legítimas, configurando assim o ataque de Negação de Serviço. Desta forma, o conceito de segurança da informação DISPONIBILIDADE foi quebrado.

4.1 Identificação do SYN flood

É possível identificar as requisições de conexão TCP usadas para realização do ataque de negação de serviço. Para isso, na máquina alvo “Debian 9”, execute o comando a seguir.

```
#netstat -taupn
```