Segurança
Experimento N°02
Ataques (Básicos) á uma Rede Local

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

1. Introdução:

No suporte de uma rede privada ou especializada local, pode ocorrer a observação de diversos ataques - que necessitam ser identificados por Engenheiros de Rede - de forma a preparar contramedidas de segurança para impedir as consequências desse ataque.

Entende-se que o (re)conhecimento básico dos modelos de ataques em rede (Gathering, DDoS, Flood, entre outras) é necessário para que esses profissionais adaptem suas redes no que se refere a conexões e acesso de usuários, para tratar ataques maliciosos e indevidos (tal como implementar um IDS).

O objetivo deste experimento é gerar situações básicas de ataques em redes de computadores – similares ao que pode acontecer em ambientes acadêmico, de seu emprego ou em ambiente pessoais – e dar suporte a capacidade dos alunos em analisar e identificar tais situações.

Será então "provocados" - EM UM AMBIENTE CONTROLADO – diversos fatos de ataque cibernético básicos para estudo e avaliação dos alunos.

Lembramos que para estudo de tal atividade, não serão aceitas realizações pelos alunos que envolvam sites de terceiros e/ou externos ao ambiente controlado do laboratório, pois, como já exposto em diversas aulas, essas atividades são passíveis do entendimento da realização de um crime cibernético, passível de punição judicial.

2. Ambiente e Necessidades Preliminares

- Durante a execução do laboratório nos dias 18/09/2018 (apoio em 20/09/2018) serão realizadas diversas situações de ataques a rede do laboratório da sala de aula, provocadas pelo instrutor. Ao final, serão disponibilizados arquivos de tráfego da rede ("sniffer" ou ".pcap" de tráfego dessa rede.
- Ao início da atividade, cada aluno deverá informar seu IP e deverá colocar à disposição um servidor HTTP (htttp.server na porta 8000) em seus ambientes locais. Seus IP´s e seus serviços HTTP disponibilizados podem se tornar indisponíveis em algum momento, o que deve ser relatado ao instrutor.
- No ambiente do Campus Virtual serão disponibilizados diversos arquivos de tráfego de rede (em "modo promíscuo"), que devem der utilizados pelos alunos de forma a formar o conhecimento necessário para explicitação do Experimento 3. Se os alunos entenderem que apenas um dos arquivos (tal como um log de operação das redes ao qual são "guardiões") é suficiente para realização da tarefa, isso não é considerado impeditivo para exposição do experimento.

3. Semana Universitária

Para o cumprimento excepcional de um laboratório da disciplina - durante a semana universitária - propomos a realização de um estudo teórico escrito – A SER ANEXADO COMO UM TÓPICO DESTE EXPERIMENTO 02 - sobre o ambiente Linux Kali, no que se refere à determinados elementos disponibilizados no mesmo, a saber:

- cisco-torch
- dnsenum
- dnstracer

Neste sentido, escreva e discuta sobre esses elementos, seus parâmetros e resultados – bem como podemos analisar seus resultados. Esse estudo teórico será os primeiros objetos do Linx Kali que serão usados no Experimento 3 (após a Semana Universitária). Pedimos a atenção excepcional para não ocorrer cópias de trabalhos.

Cabe lembrar que o trabalho sobre o Linux Kali deve ser realizado no sentido de formar uma bagagem teórica já conhecida pelo aluno mas só podem ser utilizados no laboratório de redes.

Adicionalmente apresente também seu conhecimento dos aplicativos IPTABLES <https://e-tinet.com/linux/tabelas-do-iptables-firewall-linux/> e do IDS SNORT. <https://www.snort.org>.

4. Experimento

O objetivo deste experimento é analisar ataques segundo padrões observáveis em registros de acesso a rede (os arquivos disponibilizados). Neste sentido, esses arquivos serão disponibilizados na pasta "Experimento 2 – Arquivos de Dados" dentro do Campus Virtual.

O uso de comandos de "socket" do Python em laços permite que diversas situações possam, ser "provocadas". Outros comandos de sistema operacional (chamados de forma nativa ou com o python" podem ser utilizados.

É importante que, de tempos em tempos, se avalie a situação das portas (sus ou de "atacados") via NMAP (conhecimento já aprendido). Esse resultado é "PESSOAL" dos ambientes "atacados". Logo, encaminhe esse resultado para seu email ou repositório de arquivos. Ainda, para todos os alunos, se qualquer IP realiza um "PortScan", todos os alunos "deverão" ser capazes de observá-los e aponta-los no Experimento.

No contexto do trabalho, sugerimos adicionar explanações sobre algumas técnicas matemáticas que podem ser utilizadas na detecção dessas "situações de rede ocorridas".

Para execução do experimento dois alunos serão convidados a ativar o wireshark "em modo promíscuo" em momento combinado com o instrutor:

a) Inicie o experimento o comando **ifconfig** para verificar seu IP e anuncie ao professor.
b) Para criação de um HTTP na sua máquina você pode se utilizar da chamada: **python3 -m http.server –bind <seu_ip> 8000**
c) Para testar use o comando **telnet <seu_ip> 8000<ENTER> GET / HTTP/1.1<ENTER><ENTER>**. Vai retornar o conteúdo do diretório aonde o python3 foi executado.

d) Escolha o IP do servidor da sala de aula e realize o aplicativo **nmap** (a qualquer momento do experimento), devendo colocar o nmap para atuar **da porta 21 a 443 e, adicionalmente a porta 8000.**

e) Escolha 1 IP de um colega ao lado e realize o código **python3 ddos.py <ip_destino> 8000.** Peça para ele observar o que acontece no servidor HTTP.

f) Atenção: alguns fatos de ataque a rede estão sendo realizados por deliberação com o instrutor. Esses serão objetos do experimento e devem ser avaliados junto ao arquivo pcap que será disponibilizado.

5. Orientações Adicionais

- O arquivo .pcap será disponibilizado na **pasta "PCAPS"** com o nome **Experimento02Dia01**. Outros arquivos serão nomeados como **Experimento02Dia02** e serão gerados na aula na quinta feira.
- Código do **ddos.py** se encontra na pasta "CODIGOS".
- Existe um código disponibilizado chamado **arp.py** MAS ELE NÃO É PARA SER UTILIZADO.
- O **nmap** já é de conhecimento dos alunos.