**Aula prática de OpenVAS**

O OpenVAS (**Open Vulnerability Assessment System**) é um scanner de segurança de redes com um cliente em interface gráfica.

O núcleo é composto por um servidor que realiza testes de vulnerabilidades na rede (NVTs) para detecção de problema de segurança em aplicações e sistemas remotos (para alguém que está de fora).

OpenVAS é um software livre derivado do Nessus (um primeiro scanner de vulnerabilidades). Logo é uma excelente opção de ferramenta para uso em auditorias de segurança.



Estrutura do OpenVAS

Instalação

O OpenVAS-Server só esta disponível para línux ou Freebsd, o cliente esta disponivel para Línux, Freebsd e Windows.

Nesse postei irei demonstrar a instalação no Debian e no Fedora.

Instalação no Debian:

***# apt-get install libopenvas2
# apt-get install libopenvas2-dev
# apt-get install libopenvasnasl2
# apt-get install libopenvasnasl2-dev
# apt-get install openvas-server
# apt-get install openvas-server-dev***

Instalação no Fedora:

Para instalação no Fedora é necessário adicionar o repositório atomicorp.

**Usando o Lynx (yum -y install lynx):**
***lynx -source http://www.atomicorp.com/installers/atomic.sh | sh***

**Usando o Wget:**
***wget -q -O – http://www.atomicorp.com/installers/atomic.sh | sh***

Após isso execute:

***#yum install  openvas-client.x86\_64***

***#yum install  openvas-server.x86\_64***

Lembrando que estou usando um sistema operacional compativel com a arquitetura x86\_64.

No decorrer do processo de instalação o yum irá encontrar as dependências necessárias para a instalação correta dos pacote.

Por se tratar de um software com arquitetura cliente – servidor, o server pode ser instalado em uma máquina da rede e ser acessado pelo cliente que roda em outra máquina. É claro que isso é arriscado, pois alguém estiver monitorando as informações da rede, vai ter acesso as informações trocadas entre o cliente e o servidor OpenVAS.

Para manter a segurança durante o uso do OpenVAS é recomendada **a criação de um certificado, para cliente e servidor trocarem informações por SSL**. Para gerar um **certificado de segurança** use:

***#openvas-mkcert***

Ao executar esse script, você terá que responder uma serie de perguntas relativas a duração do certificado e localização geográfica.

Criando novo usuário.

Para criar um novo usuário, execute:

***#openvas-adduser***

Você terá que escolher o tipo de autenticação do usuário, se será por senha (pass) ou cerificado (cert), essa opção faz a mesma coisa que ***openvas-mkcert-client.***

***Executando o OpenVAS (Básico)***

Para executar o OpenVAS, primeiro deve se iniciar o servidor:

***#/etc/init.d/openvasd start***

Após a inicialização do servidor OpenVAS,  execute o OpenVAS-client.

#**openvas-client**



 OpenVAS Client

Para executar um scan:

1-click em New.

2- Use o **scan assistent** para configurar o scan (ícone azul com o símbolo ?).

3- Ao abrir o assistente informe o **nome do projeto**, o **escopo**, o **alvo** e no final execute.

4- Na tela de conexão informe o **endereço ip do servidor** **OpenVAS**, o **login** e **senha** para utilizar.

**Em caso de acesso remoto é altamente aconselhado o uso de certificados para a comunicação em cliente e servidor.**

5-Após preencher os campos, click em ok para começar o scan.

Ao término do scan é gerado um relatório sobre as principais vulnerabilidades encontradas num host ou na rede.

**Exercícios:**

inicie o OpenVAS-server com o comando:

**#/etc/init.d/openvasd start**

Depois abra o OpenVAS cliente.

Crie um novo projeto. File->New.

Use o **scan assistent** para configurar o novo scan. File->Scan Assistent.

No passo 1, preencha o **nome do scan**. scan-bosco-inspired-1525

No passo 2, preencha o **escopo do scan**. user-host

No passo 3, você preenche o alvo, que pode ser **um endereço ip de um host remoto** ou uma **rede**. localhost bosco 01031978 senha do openvas-server (openvasd)

**Após seguir os passos, execute o scan.**

**Outros resultados precisa-se trabalhar com os clientes GSD e o GSA do OpenVAS.**

**---------------------------------------------------------------------------------------------------------**

Interessante:

Rode a ferramenta **Wireshark** na máquina alvo e visualize os pacotes enviado pelo OpenVAS.

2- Configure o **iptables** **(o firewall do Linux, que roda junto ao kernel)** na máquina alvo, para o **iptables** não aceitar a passagem de pacotes placa de rede descartando-o. Não permite a passagem do pacote,. que passem para

**#iptables -p INPUT DROP**

**#iptables -p OUTPUT DROP**

Execute o OpenVAS novamente contra a máquina alvo. Verifique o resultado.

3- Execute o OpenVAS contra a máquina alvo. E insira as regras acima no **iptables** da máquina alvo.

Verifique o resultado.