**ESQUEMA DE PLANO DE AULA PRÁTICA**

**Tarefa 3b** "Ferramentas de Aquisição de Informações"

Tópico no Moodle: Scanner de Vulnerabilidades OpenVAS

Data: 28-09-2012

Tempo de Aula: 1 hora-aula

Grupo: <Aluno\_1> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 <Aluno\_2> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ASSUNTO**

Utilização básica do Analisador de Vulnerabilidades OpenVAS (**Open Vulnerability Assessment System**). OpenVAS é um scanner de segurança de redes, que analisa vulnerabilidades em serviços associados à portas TCP, numa máquina em uma rede.

O tópico é estudado de forma mais simplificada, através do uso do OpenVAS, com uma interface gráfica OpenVAS-cliente e um servidor-OpenVAS situados numa máquina, para verificar vulnerabilidades em outra máquina em rede. Esta última, podendo ser o próprio “localhost”, uma máquina servidor ou um servidor Web que hospeda um *site*.

Numa forma mais profissional, o OpenVAS pode ser utilizado usando um cliente com interface gráfica na Web, o chamado **Greenbone Security Assistance**.

 **BIBLIOGRAFIA BÁSICA**Página OpenVAS:www.openvas.org

Links Importantes: http://www.youtube.com/watch?v=CTyvTqoQzzA

<http://www.slideshare.net/firebits/oficina-de-anlise-em-vulnerabilidades-openvas4-garoahc>

 **OBJETIVOS DA AULA**

Conhecer um analisador de vulnerabilidades, quanto a seus resultados básicos:

1. Definição de um projeto
2. Número de vulnerabilidades, níveis de severidade (Alto, Médio, Baixo)
3. Mostrando os resultados relativos à Host-Porta-Serviço-Severidade, quanto a indicação sobre um “Security Hole” (uma vulnerabilidade encontrada), uma “Security Warning” (advertência) ou uma “Security Note” (nota sobre segurança), impacto, software afetado, o que deve ser feito para consertar a vulnerabilidade, entre outras informações.

**INFRAESTRUTURA OpenVAS**



**SELEÇÃO DO CONTEÚDO – A PRÁTICA**

Um conteúdo mínimo, consistindo de um roteiro de aula, com o OpenVAS, visando o objetivo acima, pode ser colocada como:

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.***

Por simplicidade, use uma senha, que você deve criar. O certificado deve ser usado, caso o OpenVAS-Client e o OpenVAS-server estiverem em máquinas separadas na rede, e deve ser cirado no ato da instalação do OpenVAS.

 **EXECUTANDO O OpenVAS (Básico) –** Linux Ubuntu 11.10

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

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

**Para executar um scan:**

inicie o OpenVAS-server com o comando:

**#*sudo openvasd*** (usar senha de administrador = network)

Depois abra o OpenVAS client usando:

**#openvas-client** (abrirá uma interface do cliente)



Use o **Scan Assistent** para configurar um novo projeto de scan.

Crie um novo projeto usando o ícone azul com o símbolo “?”.

Ao abrir o assistente informe para as etapas (1) **nome da tarefa**, o (2) **escopo**, o (3) **alvo** e no final (4) execute.

Na tela de conexão do cliente com o servidor OpenVAS, informe o **endereço ip do servidor** **OpenVAS**, o **login** e a **senha** para utilizá-lo.

**Obs: Em caso de acesso remoto é altamente aconselhado o uso de um certificado para a comunicação em cliente e servidor.**

No passo seguinte, preencha o **nome do scan**.
 ( por exemplo: scan-bosco-inspired-1525 )

A seguir, preencha o **escopo do scan**. (por exemplo: user-host, internet server, ...)

Depois, você preenche o alvo a escanear, que pode ser **um endereço ip de um host remoto, uma URL de algum site,** ou mesmo uma **rede a ser escaneada**.

(por exemplo, um localhost, user: bosco, senha: 01031978 (que é uma senha criada para acessar o openvas-server), ou 150.162.60.159 ou um site web.

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, mostrando algo como:

1. Número de vulnerabilidades, níveis de severidade (Alto, Médio, Baixo)
2. Mostrando os resultados relativos à Host-Porta-Serviço-Severidade, quanto a indicação sobre um “Security Hole” (uma vulnerabilidade encontrada), uma “Security Warning” (advertência) ou uma “Security Note” (nota sobre segurança), impacto, software afetado, o que deve ser feito para consertar a vulnerabilidade, entre outras informações.

**MOSTRE SEU EXPERIMENTO (Deposite a tarefa no Moodle).**

Suas respostas, devem ser depositadas no prazo previsto pelo professor no sistema MOODLE, no link definido para tal, conforme os itens abaixo:

1. Informe o nome de sua tarefa.
2. O escopo de sua tarefa.
3. O seu alvo.
4. Quantas vulnerabilidades de nível ALTO.
5. Quantas vulnerabilidades de nível MÉDIO.
6. Quantas vulnerabilidades de nível BAIXO.
7. Exemplifique uma vulnerabilidade encontrada.
8. Indique o impacto.
9. Indique o software afetado.
10. Indique o que fazer para contornar a vulnerabilidade.