INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

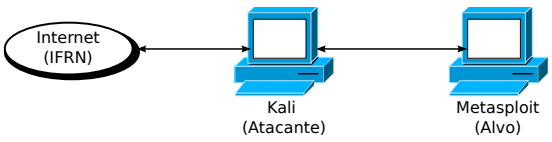
Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 06: Análise de Vulnerabilidades do MetasploitTable com o Nessus

Olá turma, hoje iremos começar a fase de análise de vulnerabilidades no teste de penetração. Para isso, iremos demonstrar como realizar uma análise de vulnerabilidades de uma máquina alvo utilizando o Nessus. Vamos lá?

Configurando o Ambiente

Para estudarmos estes conceitos e ferramentas, e para as aulas posteriores, iremos utilizar duas máquinas virtuais (Kali Linux e MetasploitTable2). A MetasploitTable2 será a máquina que iremos utilizar como alvo e o Kali Linux será utilizado para análise de segurança e realização de ataques.

Coloque ambas máquinas com interface em Rede Nat, para que elas possam acessar a internet e se comunicarem entre si.



Metasploitable

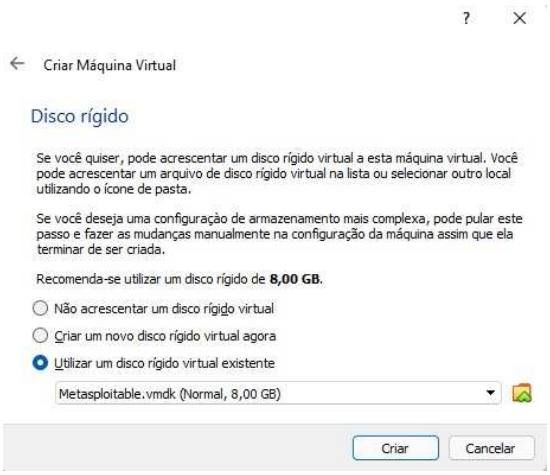
O Metasploitable é um sistema operacional, baseado em Linux, vulnerável intencionalmente criado para fins educacionais e de teste de segurança. Ele é projetado para ser usado em conjunto com ferramentas como o Metasploit, permitindo que os profissionais de segurança e os estudantes pratiquem a identificação e exploração de vulnerabilidades de forma ética e legal.

Para deixar ele rodando em uma máquina virtual, siga os seguintes passos:

1. Faça o download da imagem no site da Rapid 7 ou no Sourceforge (`http://sourceforge.net/projects/metasploitable/files/Metasploitable2/`)

2. Extraia os arquivos para uma pasta. Terá um arquivo chamado Metasploittable.vmdk que trata de um disco virtual com o sistema.

3. Crie uma máquina virtual Linux 64 bits, com memória RAM de 2048 MB. Informe que será utilizado um disco rígido existente ("Metasploittable.vmdk").



Uma vez criada a máquina com o disco do metasploitable, você poderá inicia-la normalmente. Na tela de logins utilize o nome de usuário e a senha padrão que são:

```
Usuário: msfadmin
Senha:   msfadmin
```

Análise de Vulnerabilidades

A análise de vulnerabilidades é o processo de identificação, avaliação e classificação das vulnerabilidades em sistemas, redes ou aplicações de software. Essas vulnerabilidades são potenciais falhas de segurança que podem ser exploradas por invasores para comprometer a integridade, disponibilidade ou confidencialidade dos sistemas.

Durante um teste de penetração, os analistas de segurança procuram ativamente por vulnerabilidades, usando uma variedade de técnicas e ferramentas. São exemplos de ferramentas: Nessus, OpenVAS, Nexpose e Nikto .

No teste de penetração, está fase é realizada depois da fase de enumeração (varredura) onde já sabemos quais são as máquinas e as principais informações. O objetivo final da análise de vulnerabilidade em um teste de penetração é identficar as vulnerabilidades para depois explora-las em um ambiente controlado.

Após identificadar todas as vulnerabilidades de sua infraestrutura, o analista de segurança deverá listá-las por ordem de importância, ou seja, em primeiro lugar as falhas capazes de causar maior prejuízo a empresa.

Entre as várias ferramentas de análise de vulnerabilidade se destaca o Nessus. Será com ela que iremos trabalhar na aula de hoje.

Nessus

O Nessus é uma das ferramentas de análise de vulnerabilidades mais populares e amplamente utilizadas em segurança da informação. Desenvolvido pela Tenable, o Nessus é conhecido por sua capacidade de identificar uma ampla variedade de vulnerabilidades em sistemas, redes e aplicativos.

O Nessus possui uma extensa base de dados de vulnerabilidades, que é constantemente atualizada com informações sobre novas vulnerabilidades e ameaças.

O Nessus possui duas versões do programa: Essential e a Professional. No Kali Linux precisaremos instalar o scanner de vulnerabilidades Nessus Home versão Essential. Esse scanner é gratuito somente para usos domésticos limitado a efetuar o scanning de 16 endereços IP. Para isso, devemos nos registrar no programa Tenable para Educação.

Instalação

Para instalar o nessus siga os seguintes passos:

1. Acesse o site `https://pt-br.tenable.com/products/nessus` e faço o download da versão Essential. Faça um cadastro como estudante, informando o seu nome, sobrenome e e-mail. Você receberá um código de ativação por e-mail e um link para a página de download.

2. Na página de download baixe a versão mais recente de acordo com o seu sistema operacional. Na sequência irei mostrar a instalação no Kali Linux.

3. Abra o terminal do Linux. Vá até a pasta de "Downloads" e localize o arquivo do Nessus_XXX.deb.

4. Digite:

```
sudo dpkg -i Nessus_XXX.deb
```

5. Habilitar e iniciar o Nessus através do comando

```
sudo systemctl enable nessusd
sudo systemctl start nessusd
```

6. Verifique se o serviço está rodando

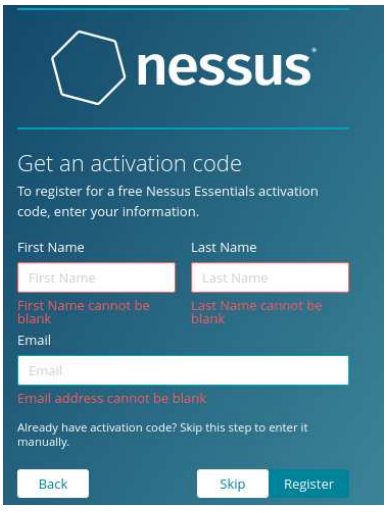
```
sudo systemctl status nessusd.service
```

7. Abra o endereço `https://localhost:8834/` no navegador. Irá surgir uma mensagem de erro de certificado, aceite o erro e continue na página. Com isto, você conseguirá acessar o Nessus.

8. Na sequência, você deverá visualizar a tela de boas vindas, clique em "Continue".

9. Na próxima tela, entre as opções possíveis selecione "Register for Nessus Essential", e clique em "Continue".

10. Na tela seguinte, será questionado se você deseja ativar o Nessus, inserindo seu nome e e-mail e clicando em "Register" ou clique em "Skip" se você já realizou o registro e se já recebeu o e-mail com o código de ativação.



11. Na sequência você deverá informar o "Activation Code" (código de ativação) que você recebeu por e-mail e clique em "Continue".

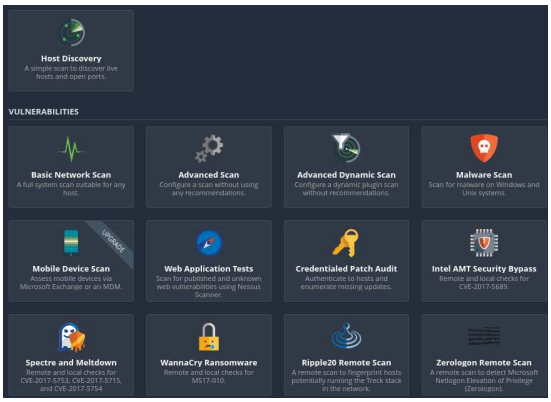
12. Posteriormente, você deverá criar um usuário e uma senha para administrar o Nessus. Ao final clique em "Submit". O Nessus vai começar a fazer o download dos plugins e isto poderá demorar um pouco.

13. Ao final coloque o seu usuário e senha.

14. Quando logar, você será questionado se desejará utilizar a versão paga Expert. Não precisa, pois iremos utilizar a versão gratuita Essential.

Descoberta de Hosts

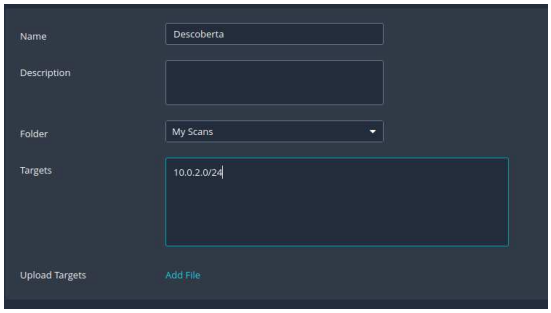
A interface web do Nessus contém diversas abas na parte superior da tela. Vamos começar pela aba "Scans" e executar o Nessus em nossa rede-alvo. Saber quais hosts estão em sua rede é o primeiro passo para qualquer avaliação de vulnerabilidade. O Nessus vem com alguns scans pré-definido que abrange desde descoberta de equipamentos a descoberta de vulnerabilidades. Alguns destes scans estão mostrados na figura abaixo.



Para realizar o scan de descoberta:

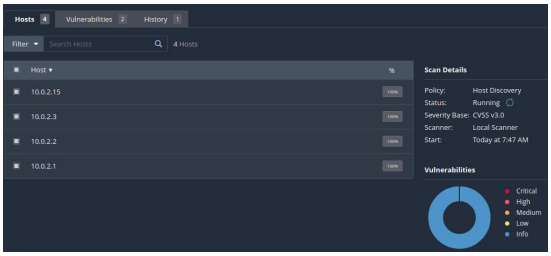
1. Clique em "New Scan". Selecione o tipo de "Host Discovery".

2. Irá surgir uma tela, preencha as informações do scan, que são basicamente: o nome de nosso scan ("Name") e em quais redes/máquinas deverá ser executado o scan ("Targets"). Coloque como alvo o endereço da sua rede Nat.



3. Para iniciar o scan imediatamente, clique no botão Lançar ( ).

O Nessus executará a varredura de descoberta de host. Depois que o scan for concluído, clique nele para visualizar os resultados. Será apresentado os hosts que o Nessus descobriu , e qualquer informação associada disponível, como endereço IP, FQDN, sistema operacional e portas abertas.

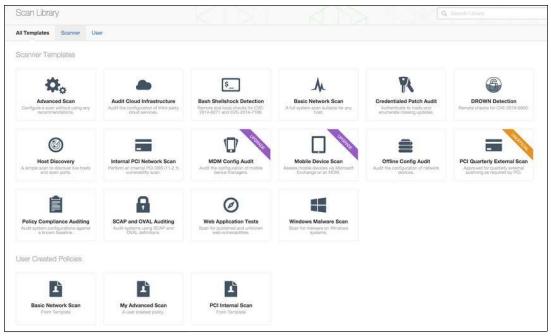


Escaneando Vulnerabilidades

A principal funcionalidade do Nessus é o escaneamento de vulnerabilidades. Para realizar um escaneamento, siga os passos:

1. Na barra de navegação superior, clique em "Scans". irá surgir a página "My Scans".

2. No canto superior direito, clique no "New Scan". Irá surgir uma tela com Templates de Scans.



Existem vários templates de scans pré-definido, dentre eles temos:

- Varredura de rede básica: executa uma verificação completa do sistema que é adequada para qualquer host. Use este modelo para verificar um ativo ou ativos com todos os plug-ins do Nessus ativados. Por exemplo, você pode executar uma varredura de vulnerabilidade interna nos sistemas de sua organização.

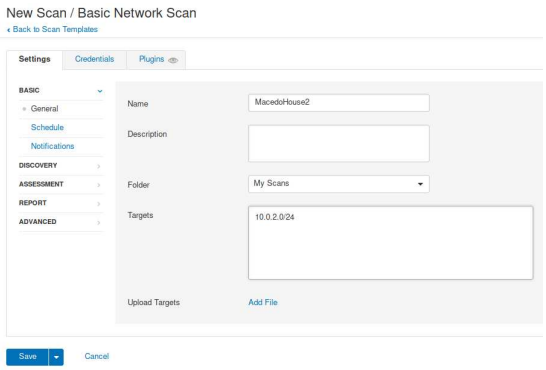
- Varredura de rede avançada: este modelo tem as mesmas configurações padrão do modelo de varredura básico, mas permite opções de configuração adicionais, ou seja, permitem que você verifique mais profundamente usando configuração personalizada, como verificações mais rápidas ou mais lentas. Use os modelos avançados com cuidado.

- Varredura dinâmica avançada: você pode configurar filtros dinâmicos de plug-in. Isso permite que você adapte suas verificações para vulnerabilidades específicas.

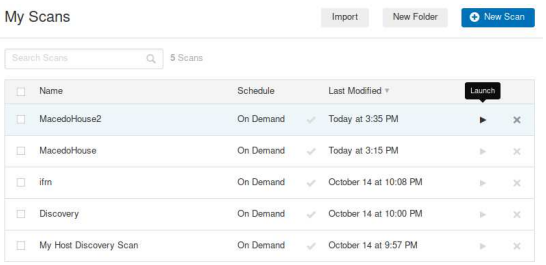
- Verificação de malware: verifica malware em sistemas Windows e Unix.

3. Em Discovery, selecione o modelo "Basic Network Scan";

4. Na tela de configurações, digite um nome para a varredura e as informações do alvo (que poderá ser ser o domínio, endereços IPv4 ou endereços IPv6 de uma rede ou de um endereço específico). No nosso caso coloque o endereço IP do Metasploit e clique em "Save".



5. Para iniciar a verificação imediatamente, clique no botão clique no botão Lançar ().



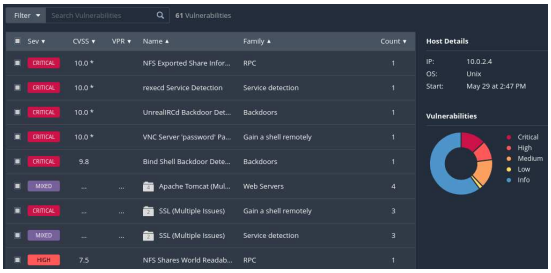
6. Ao final do processo, clique no Scan para abrir a tela dos resultados, o Nessus agrupa em três abas: Hosts descobertos, vulnerabilidades e Histórico.

As vulnerabilidades são divididas em baixa, média, alta e crítica. O Nessus ainda mostra informações sobre o ativo de rede, tais como, serviços, endereços, sistema operacional e portas. Clicando em cada host é possível obtermos suas informações e suas vulnerabilidades.

A classificação das vulnerabilidades utiliza o padrão CVSS (*Common Vulnerability Scoring System*), do NIST (*National Institute of Standards and Technology*). A classificação é calculada de acordo com o impacto causado no sistema caso o problema seja explorado.

7. Para visualizar s vulnerabilidades, utilize a aba Vulnerabilities. É possível ver as informações de um equipamento específico, para isso, clique no mesmo.

8. Para ver os detalhes da vulnerabilidade, clique na linha da vulnerabilidade. A página de detalhes da vulnerabilidade mostrará as informações do plug-in e a saída para cada instância em um host.



Se a página de resumo do Nessus não fornecer informações suficientes sobre uma vulnerabilidade, tente uma boa e velha pesquisa no Google. Além disso, procure fazer pesquisas em http://www.securityfocus.com/, http://www.packetstormsecurity.org/, http://www.exploit-db.org/ e http://www.cve.mitre.org/. Por exemplo, você pode procurar vulnerabilidades usando o sistema CVE.

Atividade

1. Faça o download e instalação do Nessus no Kali Linux;

2. Faça um scans de vulnerabilidade do seu Kali e do Metasploitable.

3. Com o tcpdump observe as mensagens trocadas entre o Nessus e as máquinas alvo.

4. Em grupos analise os resultados do Nessus e discuta as vulnerabilidades identificadas, destacando as mais críticas.