Guia do Usuário Nessus 4.4

14 de junho de 2011

(Revisão 10)

Índice

INTRODUÇÃO

Este documento descreve como usar a **interface do usuário Nessus (UI)** da Tenable Security Network. Envie-nos seus comentários e sugestões pelo e-mail support@tenable.com.

A interface de usuário Nessus é uma interface da Web que complementa o scanner de vulnerabilidades Nessus. Para usar o cliente, é preciso um scanner Nessus em operação instalado e estar familiarizado com o seu uso.

PADRÕES E CONVENÇÕES

Este documento é a tradução de uma versão original em inglês. Algumas partes do texto permanecem em inglês para indicar a representação do próprio produto.

Em toda a documentação, os nomes de arquivos, daemons e executáveis são indicados com a fonte **`courier bold`**, por exemplo, **`gunzip`**, **`httpd`** e **`/etc/passwd`**.

As opções de linha de comando e palavras-chaves também são impressas indicadas com a fonte **`courier bold`**. As opções de linha de comando podem ou não conter o prompt da linha de comando e o texto gerado pelos resultados do comando. Normalmente, o comando executado será apresentado em **negrito** para indicar o que o usuário digitou. Um exemplo da execução do comando **`pwd`** do Unix é apresentado a seguir:

```
# pwd
/opt/nessus/
#
```

As observações e considerações importantes são destacadas com este símbolo nas caixas de texto escurecidas.

As dicas, exemplos e práticas recomendadas são destacados com este símbolo em branco sobre fundo azul.

DESCRIÇÃO DA INTERFACE DO USUÁRIO NESSUS

DESCRIÇÃO

A interface do usuário (IU) Nessus é uma interface da Web desenvolvida para o scanner Nessus, que consiste em um servidor HTTP simples e um cliente da Web, dispensando a instalação de qualquer software além do servidor Nessus. A partir do Nessus 4, todas as plataformas aproveitam o mesmo código básico, eliminando a maioria dos erros específicos de plataforma e acelerando a implementação de novos recursos. As características principais são:

- Gera arquivos **`.nessus`** usados pelos produtos da Tenable como padrão de dados de vulnerabilidades e políticas de varredura.
- Uma sessão de política, lista de alvos e os resultados de várias varreduras podem ser armazenados em um único arquivo **`.nessus`**. Consulte o guia de formatos de arquivos do Nessus para obter mais detalhes.

- A interface do usuário exibe, em tempo real, os resultados das varreduras, de modo que não seja preciso esperar a conclusão de uma varredura para ver os resultados.
- Unifica a interface do scanner Nessus, independentemente da plataforma de base. As mesmas funções existem no Mac OS X, Windows e Linux.
- As varreduras continuarão sendo executadas no servidor, mesmo se o usuário for desconectado por qualquer motivo.
- Os relatórios de varredura do Nessus podem ser carregados por meio da interface do usuário Nessus e comparados a outros relatórios.

PLATAFORMAS COMPATÍVEIS

Uma vez que a interface do usuário Nessus é um cliente da Web, funciona em qualquer plataforma com um navegador.

Para melhor desempenho, a interface do usuário on-line do Nessus deve ser visualizada com o Microsoft Internet Explorer 7 e 8, Mozilla Firefox 3.5.x e 3.6.x ou Apple Safari.

INSTALAÇÃO

A partir do Nessus 4.2, o gerenciamento do servidor Nessus pelo usuário é realizado por uma interface da Web ou SecurityCenter e dispensa o uso de um NessusClient autônomo. O NessusClient autônomo continua a conectar e operar o scanner, mas deixará de ser atualizado.

Consulte o Guia de Instalação do Nessus 4.4 para obter instruções sobre como instalar o Nessus. Não é necessário instalar nenhum outro software.

OPERAÇÃO

VISÃO GERAL

O Nessus oferece uma interface simples, mas poderosa, para gerenciar as atividades de varredura de vulnerabilidades.

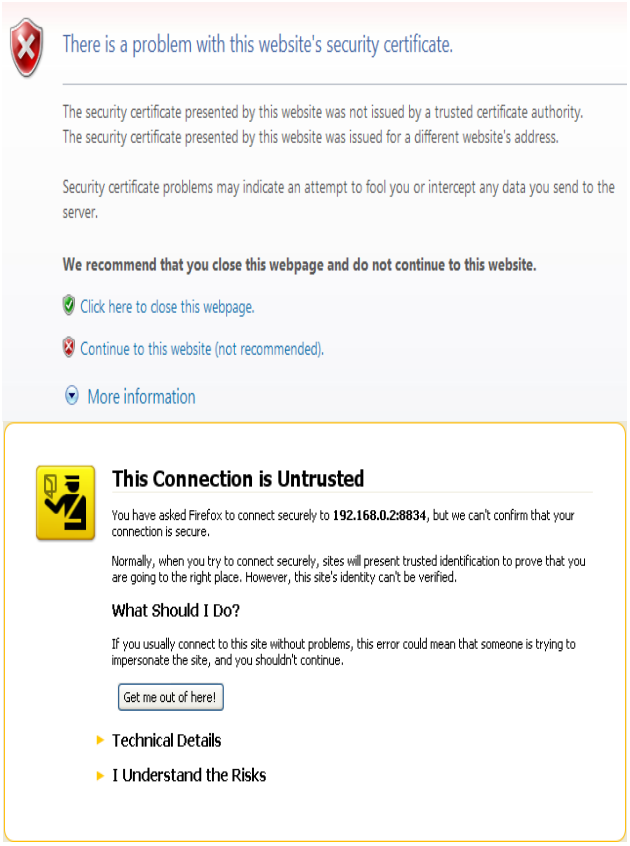
Conexão com a interface de usuário do Nessus

Para iniciar a interface de usuário do Nessus, proceda da seguinte maneira:

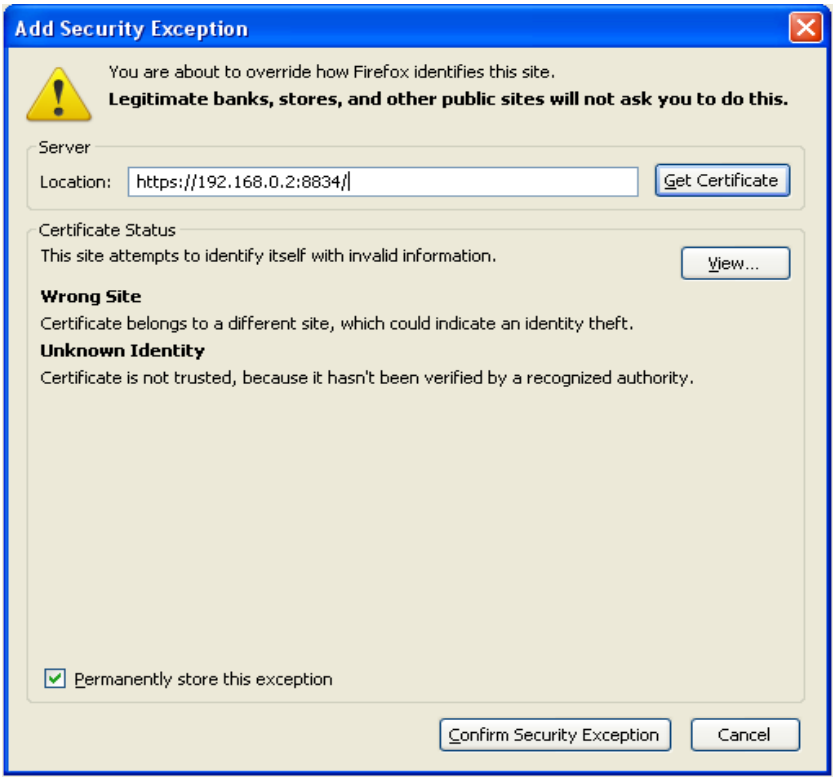
- Abra o navegador de sua preferência.
- Digite https://[IP do servidor]:8834/ na barra de navegação.

Certifique-se de se conectar à interface de usuário por meio de HTTPS, pois não são permitidas conexões HTTP sem criptografia.

Ao tentar se conectar à interface de usuário do Nessus pela primeira vez, a maioria dos navegadores exibirá um erro indicando que o site não é confiável, devido ao certificado SSL autoassinado:

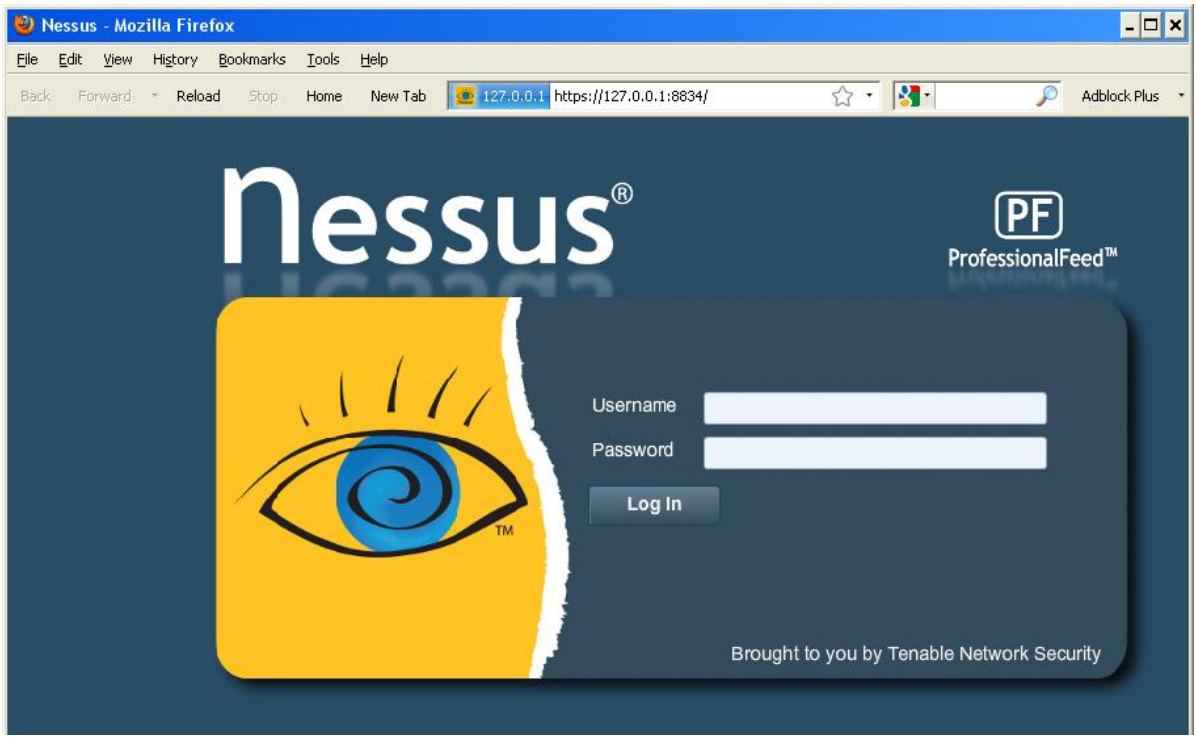


Os usuários do Microsoft Internet Explorer podem clicar em "Prosseguir para o Web site (não recomendado)" para carregar a interface de usuário do Nessus. Os usuários do Firefox 3.x podem clicar em "Eu compreendo os Riscos" e, depois, em "Adicionar exceção..." para abrir a caixa de diálogo de exceções de sites:

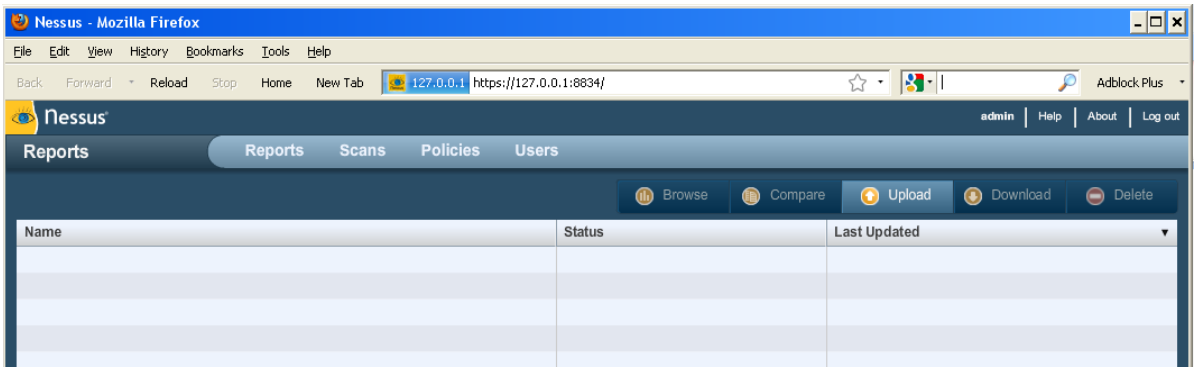


Verifique se a barra "Local:" indica a URL do servidor Nessus e clique em "**Confirm Security Exception**" (Confirmar exceção de segurança). Para obter mais informações sobre como instalar um certificado SSL personalizado, consulte o Guia de Instalação do Nessus.

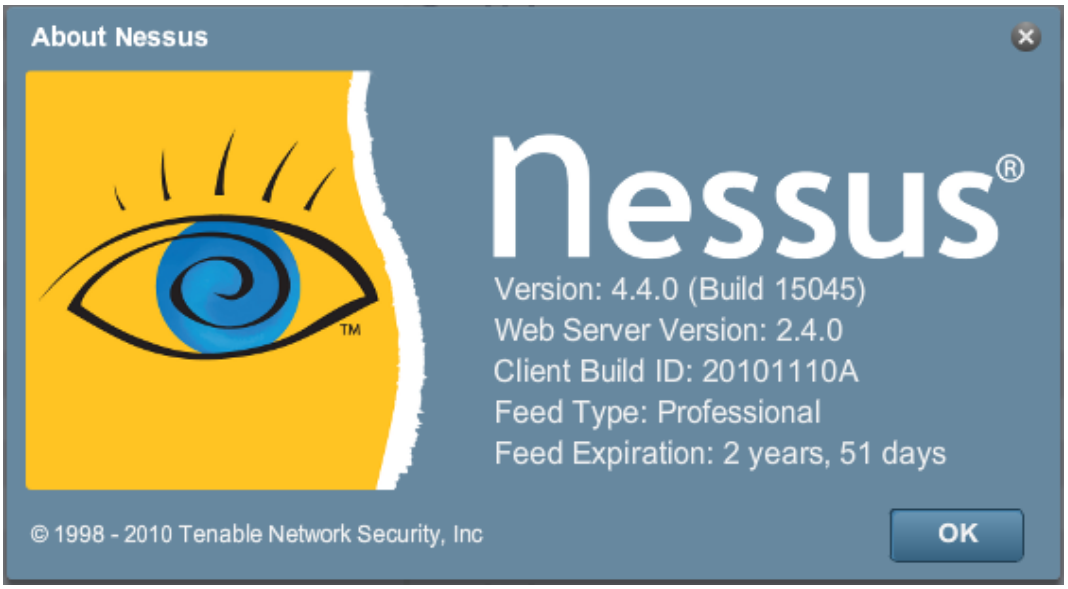
Depois que o navegador confirmar a exceção, a seguinte tela de abertura será exibida:



Autentique-se usando uma conta e senha criadas anteriormente com o gerenciador do servidor. Após a autenticação bem-sucedida, a interface do usuário exibirá os menus para a realização de varreduras:



Em qualquer ponto durante o uso do Nessus, as opções no canto superior direito estarão presentes. A notação "admin" localizada no canto superior direito da tela acima corresponde à conta conectada no momento. Clique nesta conta para alterar a senha atual. O link "Help" (Ajuda) permite acessar a documentação do Nessus, com instruções detalhadas sobre o uso do software. A opção "About" (Sobre) exibe informações sobre a instalação do Nessus, incluindo versão, tipo de feed, vencimento do feed, versão do cliente e versão do servidor Web. "Log out" (Sair) encerrará a sessão atual.



Visão geral das Políticas

Uma "política" do Nessus consiste em opções de configuração relacionadas à realização de uma varredura de vulnerabilidade. Algumas das opções são, entre outras, as seguintes:

- Parâmetros que controlam aspectos técnicos da varredura, como intervalos de tempo, número de hosts, tipo de scanner de porta etc.
- Credenciais para varreduras locais (por exemplo: Windows, SSH), varreduras autenticadas de bancos de dados Oracle, HTTP, FTP, POP, IMAP ou autenticação pelo Kerberos.
- Especificações individualizadas de varreduras por família ou plugin.
- Verificações de políticas de conformidade de bancos de dados, detalhamento do relatório, definições varredura de detecção de serviços, verificações de conformidade de Unix, entre outras opções.

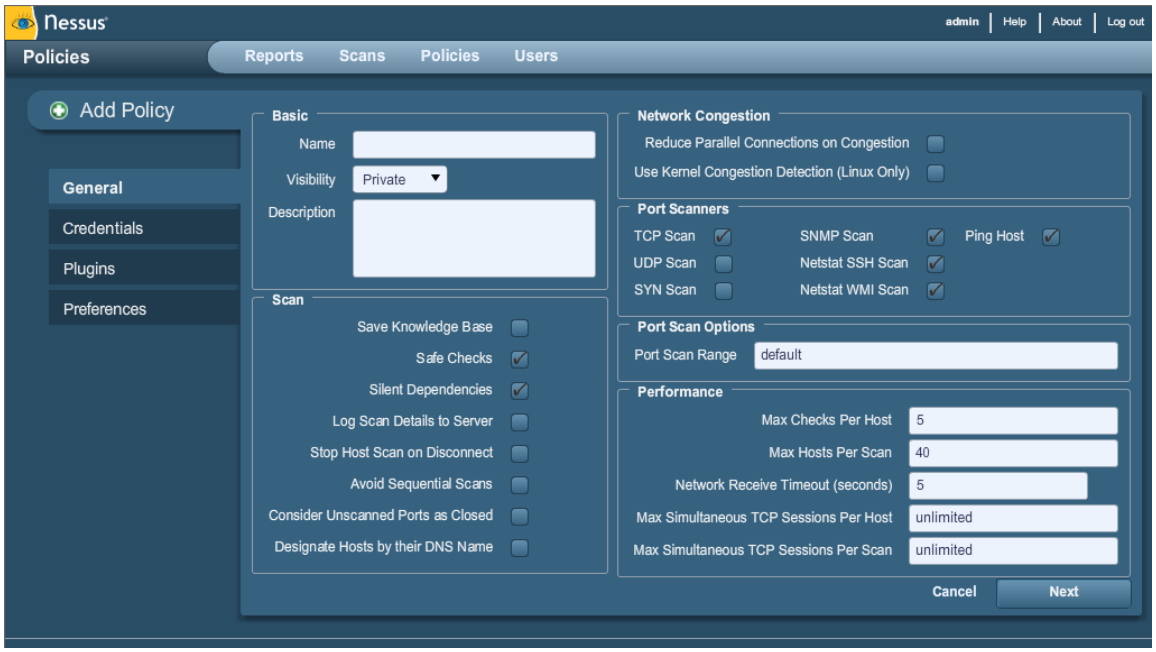
POLÍTICAS PREDEFINIDAS

O Nessus é distribuído com várias políticas predefinidas criadas pela Tenable Network Security, Inc. As políticas são fornecidas como modelos para ajudá-lo a criar políticas adequadas à sua organização ou para serem usadas sem modificações para varreduras básicas dos seus recursos.

Nome da política	Descrição
Varredura de rede externa	Esta política foi projetada para a verificação de hosts externos e que normalmente apresentam menos serviços à rede. Os plugins relacionados a vulnerabilidades conhecidas de aplicativos da Web (as famílias de plugins CGI Abuses e CGI Abuses: XSS) são ativados com a aplicação desta política. Além disso, todas as 65.535 portas são verificadas em cada alvo.
Varredura de rede interna	Esta política foi projetada levando-se em conta a melhoraria do desempenho, pois pode ser usada para verificar redes internas de grande porte com muitos hosts, vários serviços expostos e sistemas incorporados, como impressoras. Os plugins "CGI Abuse" não estão ativados e um conjunto de portas padrão é examinado, mas não todas as 65.535.
Testes de aplicativos da Web	Esta política de varredura é usada para verificar os sistemas e fazer com que o Nessus detecte vulnerabilidades conhecidas e desconhecidas nos aplicativos da Web. Os recursos de "difusão" do Nessus são ativados com esta política, o que fará com que o Nessus detecte todos os sites descobertos e verifique as vulnerabilidades presentes em cada um dos parâmetros, incluindo XSS, SQL, injeção de comandos e vários outros.
Preparar para auditorias de PCI DSS	Esta política ativa as verificações de conformidade com a norma PCI DSS integradas, compara os resultados das varreduras aos padrões PCI e gera um relatório sobre o comportamento da conformidade. É importante observar que uma varredura de compatibilidade bem-sucedida não garante a conformidade nem uma infraestrutura segura. As organizações que estejam se preparando para uma avaliação da PCI DSS podem usar essa política para preparar suas redes e seus sistemas para a conformidade com a PCI DSS.

COMO CRIAR UMA NOVA POLÍTICA

Depois de se conectar à interface de usuário do servidor Nessus, é possível criar uma política personalizada ao clicar na opção "**Policies**" (Políticas) na barra superior e no botão "**+ Add**" (Adicionar) à direita. A tela "**Add Policy**" (Adicionar Política) é exibida como no exemplo a seguir:



Observe que existem quatro guias de configuração: **General** (Geral), **Credentials** (Credenciais), **Plugins** e **Preferences** (Preferências). Na maioria dos ambientes, não é necessário modificar as configurações padrão, mas permitem um controle mais individualizado sobre o funcionamento do scanner Nessus. Essas guias são descritas a seguir.

General (Geral)

A guia General permite nomear a política e configurar as operações de varredura. Há seis caixas de opções agrupadas que controlam o comportamento do scanner:

O painel "**Basic**" (Básico) é usado para definir os aspectos da política em si:

Opção	Descrição
Name	Define o nome a ser exibido na interface de usuário do Nessus para identificar a política.
Visibility	Controla se a política é compartilhada com outros usuários ("Shared") ou mantida somente para uso privado ("Private"). Somente usuários administrativos podem compartilhar políticas.
Description	Oferece uma breve descrição da política de varredura para resumir a finalidade geral (por exemplo: "varreduras em servidores de Web sem verificações locais ou serviços não HTTP").

O quadro "**Scan**" (Varredura) define as opções sobre como a varredura deve se comportar:

Opção	Descrição
Save Knowledge Base	O scanner Nessus salva as informações de varredura no banco de dados de conhecimento do servidor Nessus para uso posterior. Isto inclui portas abertas, plugins utilizados, serviços descobertos etc.
Safe Checks	A opção Safe Checks (Verificações Seguras) desativa todos os plugins que podem afetar negativamente o host remoto.
Silent Dependencies	Se esta opção for selecionada, a lista de dependências não será incluída no relatório. Se desejar incluir a lista de dependências no relatório, desmarque a caixa de seleção.
Log Scan Details to Server	Salva detalhes adicionais da varredura no log do servidor Nessus (`nessusd.messages`), incluindo a ativação ou encerramento do plugin ou se um plugin foi interrompido. O log resultante pode ser usado para confirmar se determinados plugins foram usados e se os hosts foram examinados.
Stop Host Scan on Disconnect	Se estiver selecionado, o Nessus cessará a varredura se detectar que o host parou de responder. Isto pode ocorrer se os usuários desligarem seus PCs durante uma varredura, se um host parar de responder depois de um plugin de negação de serviço ou se o mecanismo de segurança (por exemplo: IDS) bloqueou o tráfego para um servidor. Se as varreduras continuarem nesses computadores, o tráfego desnecessário será enviado e atrasará a verificação.
Avoid Sequential Scans	Normalmente, o Nessus verifica uma lista de endereços IP em sequência. Se a opção estiver marcada, o Nessus verificará a lista de hosts em ordem aleatória. Isto pode ser útil para ajudar a distribuir o tráfego de rede direcionado a uma sub-rede específica durante varreduras extensas.
Consider Unscanned Ports as Closed	Se uma porta não for examinada com um scanner de porta selecionado (por exemplo: fora do intervalo especificado), será considerada fechada pelo Nessus.
Designate Hosts by their DNS Name	Deve-se usar o nome do host em vez do endereço IP na impressão do relatório.

O painel "**Network**" (Rede) apresenta opções que controlam melhor a varredura de acordo com a rede de destino a ser verificada:

Opção	Descrição
Reduce Parallel Connections on Congestion	Permite que o Nessus detecte o envio de um grande número de pacotes e quando o pipe da rede atingir a capacidade máxima. Se forem detectados, o Nessus reduzirá a

	velocidade da varredura ao nível adequado para diminuir o congestionamento. Ao diminuir o congestionamento, o Nessus tentará reutilizar o espaço disponível no pipe da rede automaticamente.
Use Kernel Congestion Detection (Linux Only)	Permite que o Nessus monitore a CPU e outros mecanismos internos em caso de congestionamento e diminua o ritmo de maneira proporcional. O Nessus tentará usar sempre o máximo de recursos disponível. Este recurso está disponível apenas para os scanners Nessus instalados em Linux.

O painel "**Port Scanners**" (Scanners de Portas) controla os métodos de varredura de portas que devem ser ativados para a varredura:

Opção	Descrição
TCP Scan	Usa o scanner de TCP integrado do Nessus para identificar portas TCP abertas nos alvos. Este scanner é otimizado e possui algumas funções de ajuste automático.  Em algumas plataformas (por exemplo: Windows e Mac OS X), se o sistema operacional estiver causando problemas graves de desempenho com o uso do scanner TCP, o Nessus iniciará o scanner SYN.
UDP Scan	Esta opção usa o scanner de UDP integrado do Nessus para identificar as portas UDP abertas nos alvos.  O UDP é um protocolo "sem estado", ou seja, a comunicação não é feita com diálogos de reconhecimento. A comunicação por UDP nem sempre é confiável e, devido à natureza dos serviços UDP e dos dispositivos de rastreamento, nem sempre são detectáveis de maneira remota.
SYN Scan	Usa o scanner de SYN integrado do Nessus para identificar portas TCP abertas nos alvos. As varreduras SYN são um método popular para realizar varreduras de portas e, geralmente, são consideradas um pouco menos invasivas do que as varreduras TCP. O scanner envia um pacote SYN à porta, aguarda a resposta SYN-ACK e determina o estado da porta de acordo com uma resposta ou a falta de resposta.
SNMP Scan	Instrui o Nessus a examinar alvos para um serviço de SNMP. O Nessus detectará as configurações de SNMP correspondentes durante a varredura. Se as configurações forem feitas pelo usuário em "Preferences" (Preferências), o Nessus examinará totalmente o host remoto e produzirá resultados de auditoria mais detalhados. Por exemplo:

	muitas verificações do roteador Cisco determinam as vulnerabilidades presentes ao examinar a versão do string SNMP devolvido. Estas informações são necessárias para as auditorias.
Netstat SSH Scan	Esta opção usa o **`netstat`** para verificar se há portas abertas no computador local. Depende da disponibilidade do comando **`netstat`** por meio de uma conexão SSH com o alvo. Esta varredura se destina a sistemas do tipo Unix e requer credenciais de autenticação.
Netstat WMI Scan	Esta opção usa o **`netstat`** para verificar se há portas abertas no computador local. Depende da disponibilidade do comando **`netstat`** por meio de uma conexão WMI com o alvo. Esta varredura se destina a sistemas do tipo Windows e requer credenciais de autenticação.  A varredura por WMI usa o **`netstat`** para determinar portas abertas, portanto, ignora todos os intervalos de portas especificados. Se um enumerador de portas (Netstat ou SNMP) for executado, o intervalo de portas torna-se "all" (todas).
Ping Host	Esta opção permite enviar um teste de "ping" aos hosts remotos em várias portas para determinar se estão "ativos".

O painel "**Port Scan Options**" (Opções de Varredura de Portas) instrui o scanner a localizar um intervalo de portas específico. Os valores a seguir são permitidos para a opção "Port Scan Range" (Intervalo de Varredura de Portas):

Valor	Descrição
"default"	Se a palavra-chave "default" for usada, o Nessus examinará cerca de 4.790 portas comuns. A lista de portas pode ser encontrada no arquivo **`nessus-services`**.
"all"	Se a palavra-chave "all" for usada, o Nessus examinará todas as 65.535 portas.
Custom List	Um intervalo personalizado de portas pode ser selecionado com o uso de uma lista delimitada por vírgulas de portas ou intervalos de portas. Por exemplo: é possível usar "21,23,25,80,110" ou "1-1024,8080,9000-9200". A opção "1-65535" verificará todas as portas.

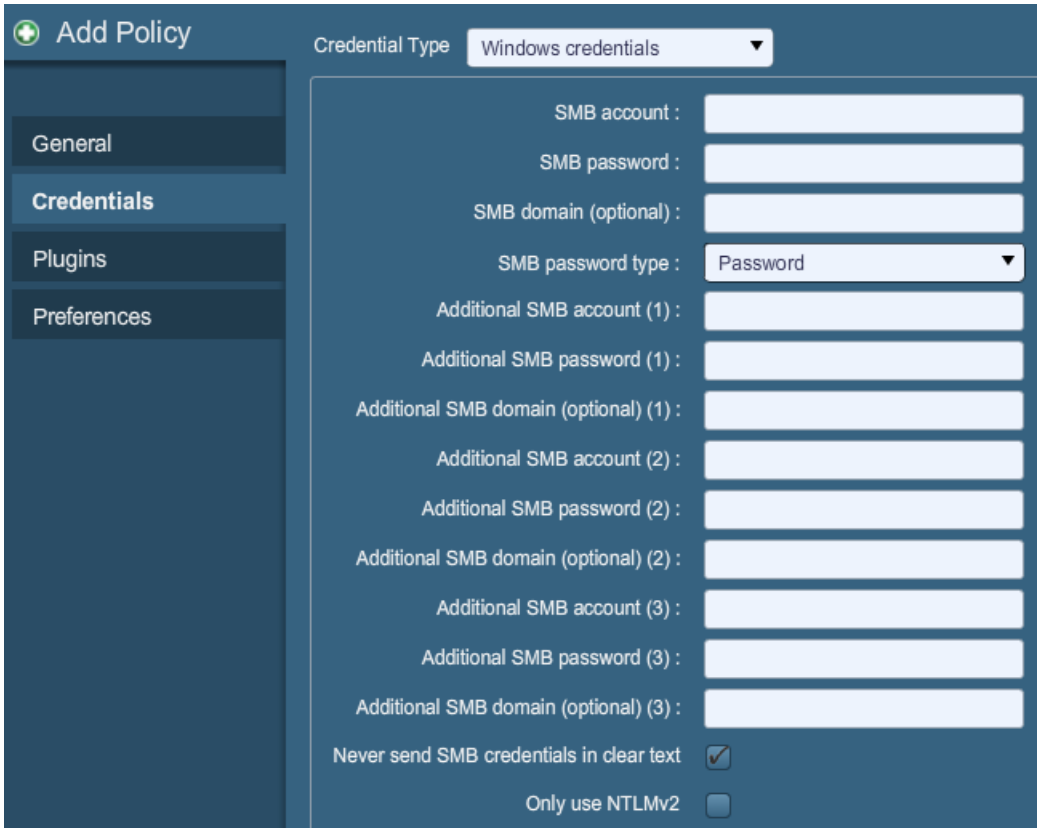
 O intervalo especificado para uma varredura de portas será aplicado às varreduras TCP e UDP.

O painel "**Performance**" (Desempenho) possui duas opções que controlam o número de varreduras a ser iniciado. Essas opções podem ser mais as importantes ao configurar uma varredura, pois têm maior impacto sobre o tempo de varredura e a atividade da rede.

Opção	Descrição
Max Checks Per Host	Esta configuração limita o número máximo de verificações que um scanner Nessus realiza em um único host ao mesmo tempo.
Max Hosts Per Scan	Esta configuração limita o número máximo de hosts que um scanner Nessus pode verificar ao mesmo tempo.
Network Receive Timeout (seconds)	O valor padrão é cinco segundos. Este é o tempo que o Nessus deve esperar por uma resposta do host, exceto se definido com outro valor por um plugin. Se a varredura for feita em uma conexão lenta, será preciso definir este valor com um número maior de segundos.
Max Simultaneous TCP Sessions Per Host	Esta configuração limita o número máximo de sessões TCP estabelecidas para um único host.
Max Simultaneous TCP Sessions Per Scan	Esta configuração limita o número máximo de sessões TCP estabelecidas para toda a varredura, independentemente do número de hosts verificados.  Para os scanners Nessus instalados em computadores com Windows XP, Vista e 7, este valor deve ser no máximo 19 para se obter resultados precisos.

Credentials (Credenciais)

A guia Credentials (Credenciais) na imagem abaixo permite configurar o scanner Nessus para o uso de credenciais de autenticação durante a varredura. A definição de credenciais permite que o Nessus realize um número maior de verificações e gere resultados de varredura mais precisos.



O item de menu suspenso "**Windows credentials**" (Credenciais do Windows) possui configurações para fornecer ao Nessus informações, como o nome da conta SMB, senha e nome do domínio. O protocolo SMB (bloqueio de mensagens do servidor) é um protocolo de compartilhamento de arquivos que permite aos computadores compartilhar informações de forma transparente através da rede. Se as informações forem fornecidas, o Nessus poderá encontrar informações locais de um host Windows remoto. Por exemplo: o uso de credenciais permite que o Nessus determine se foram aplicados patches de segurança importantes. Não é necessário modificar outros parâmetros de SMB em relação às configurações predefinidas.

Se uma conta SMB de manutenção for criada com privilégios limitados de administrador, o Nessus pode realizar varreduras em diversos domínios de maneira fácil e segura.

A Tenable recomenda que os administradores de rede criem contas específicas de domínio para facilitar os testes. O Nessus conta com diversas verificações de segurança para Windows NT, 2000, Server 2003, XP, Vista, Windows 7 e Windows 2008, que serão mais precisas se uma conta de domínio for fornecida. Na maioria dos casos, o Nessus tentará aplicar diversas verificações caso uma conta não seja fornecida.

O serviço de registro remoto do Windows permite que computadores remotos com credenciais acessem o registro do computador a ser auditado. Se o serviço não estiver em execução, não será possível ler chaves e valores do registro, mesmo com credenciais completas. Para obter mais informações, consulte o artigo "Dynamic Remote Registry Auditing - Now you see it, now you don't!" no blog da Tenable.

Os usuários podem selecionar "**SSH settings**" (Configurações SSH) no menu suspenso e inserir credenciais para a varredura de sistemas Unix. As credenciais são usadas para obter informações locais de sistemas Unix remotos para auditoria de patches ou verificações de conformidade. Existe um campo para a inserção do nome de usuário do SSH da conta que realizará as verificações no sistema Unix de destino, juntamente com a senha ou chave pública do SSH e um par de chaves privadas. Existe também um campo para a inserção da frase-senha da chave SSH, se necessário.

O Nessus 4 permite o uso dos algoritmos criptográficos **`blowfish-cbc`**, **`aes-cbc`** e **`aes-ctr`**

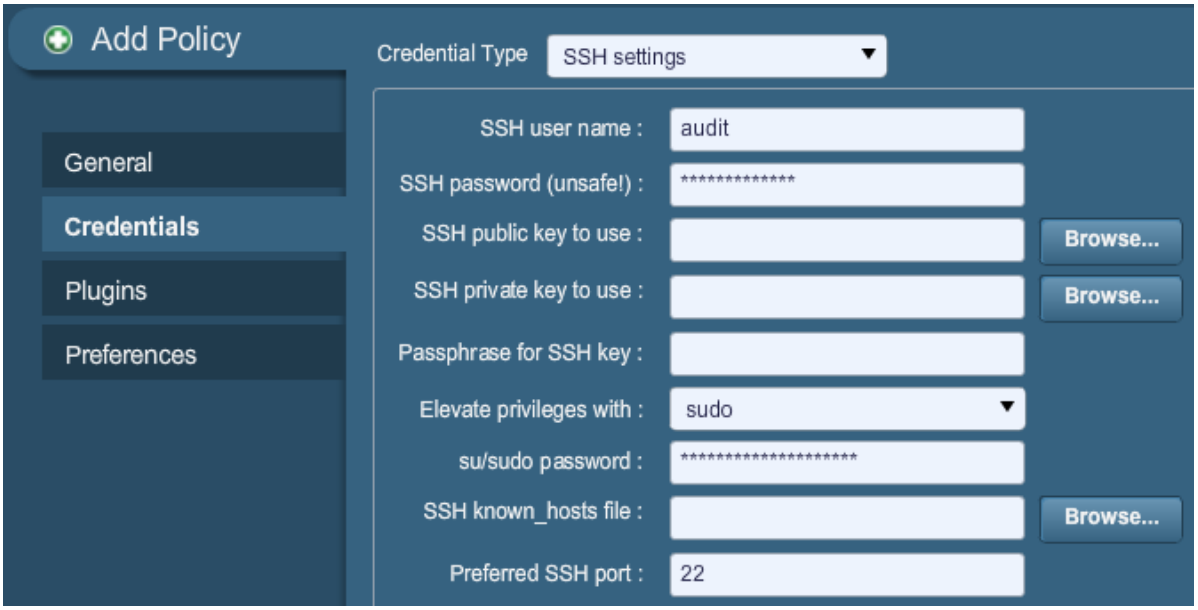
As varreduras credenciadas mais eficazes são aquelas em que as credenciais fornecidas têm privilégios "root". Uma vez que muitos locais não permitem o login remoto como root, os usuários do Nessus podem acessar "**`su`**" ou "**`sudo`**" com uma senha distinta em uma conta criada para ter os privilégios "**`su`**" ou "**`sudo`**".

O Nessus pode usar o acesso por chaves SSH para se autenticar em um servidor remoto. Se um arquivo SSH known_hosts estiver disponível e fornecido com base na política de varredura, o Nessus tentará fazer o login apenas nos hosts deste arquivo. Além disso, a opção "Preferred SSH port" (Porta SSH preferencial) pode ser configurada para indicar ao Nessus que se conecte com o SSH se estiver funcionando em uma porta que não seja a porta 22.

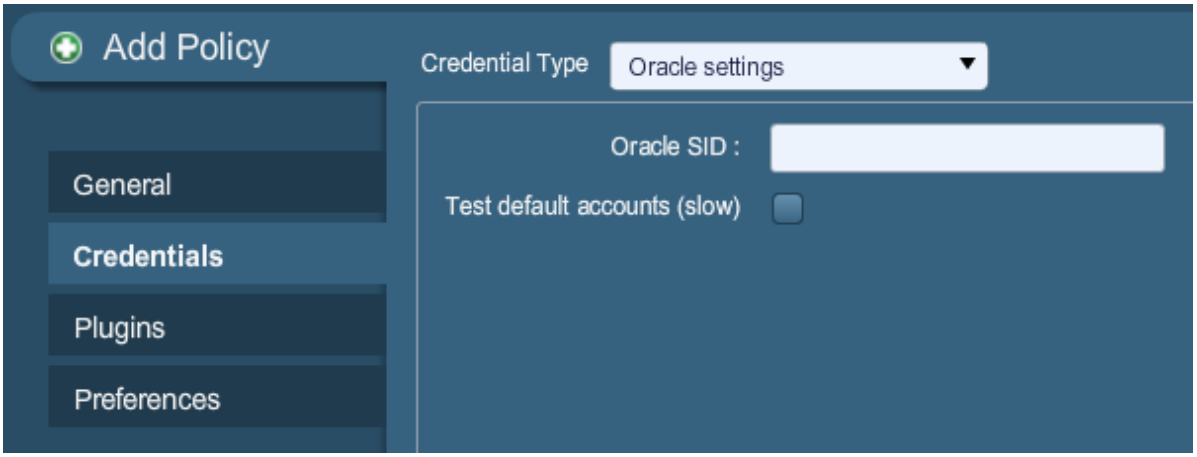
O Nessus criptografa todas as senhas armazenadas nas políticas. No entanto, as boas práticas recomendam o uso de chaves SSH, e não senhas SSH, para autenticação. Isto assegura que o mesmo nome de usuário e senha usados para auditar os servidores SSH conhecidos não sejam usados para efetuar o login em um sistema que não esteja sob seu controle. Dessa forma, não é recomendável usar senhas SSH, a menos que seja necessário.

O Nessus também oferece uma opção "su+sudo", que pode ser usada caso um sistema não conceda privilégios de login remotos a contas privilegiadas.

Veja o exemplo a seguir de como usar o "**`sudo`**" +para elevar os privilégios de uma varredura. Neste exemplo, a conta de usuário é "audit", que foi adicionada ao arquivo **`/etc/sudoers`** no sistema a ser verificado. A senha fornecida é a senha para a conta "audit" e não a senha raiz:

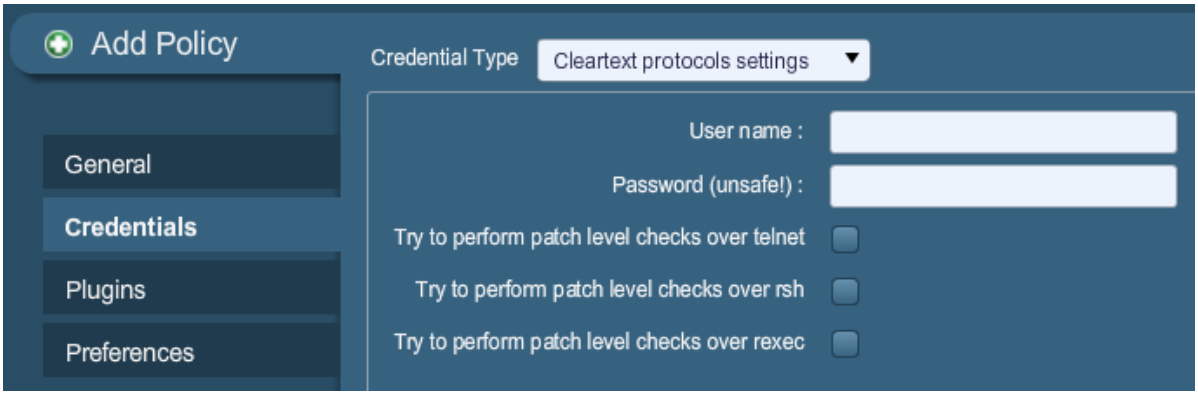


A guia Credentials também possui uma opção no menu para configuração do Oracle ("**Oracle settings**"), principalmente o Oracle SID, e uma opção para teste de contas padrão conhecidas no software Oracle:



"**Kerberos configuration**" (Configuração do Kerberos) permite especificar credenciais com o uso de chaves do Kerberos a partir de um sistema remoto:

Além disso, se um método seguro de varreduras credenciadas não estiver disponível, os usuários podem forçar o Nessus a executar varreduras por meio de protocolos sem segurança ao selecionar o item "**Cleartext protocol settings**" (Configurações de protocolo de texto simples) no menu suspenso. Os protocolos de texto simples disponíveis para esta opção são **telnet**, **rsh** e **rexec**.

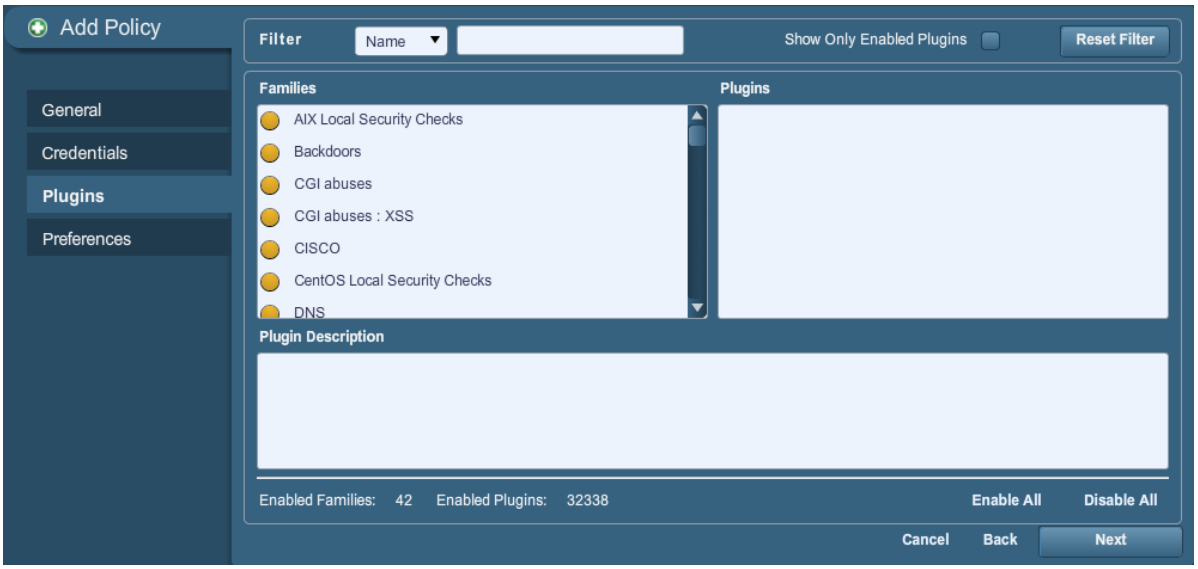


Normalmente, todas as senhas (e a própria política) são criptografadas. Se a política for salva em um arquivo `.nessus` e o arquivo `.nessus` for posteriormente copiado em uma instalação do Nessus distinta, nenhuma senha da política poderá ser usada pelo segundo scanner Nessus, pois não será capaz de decodificá-las.

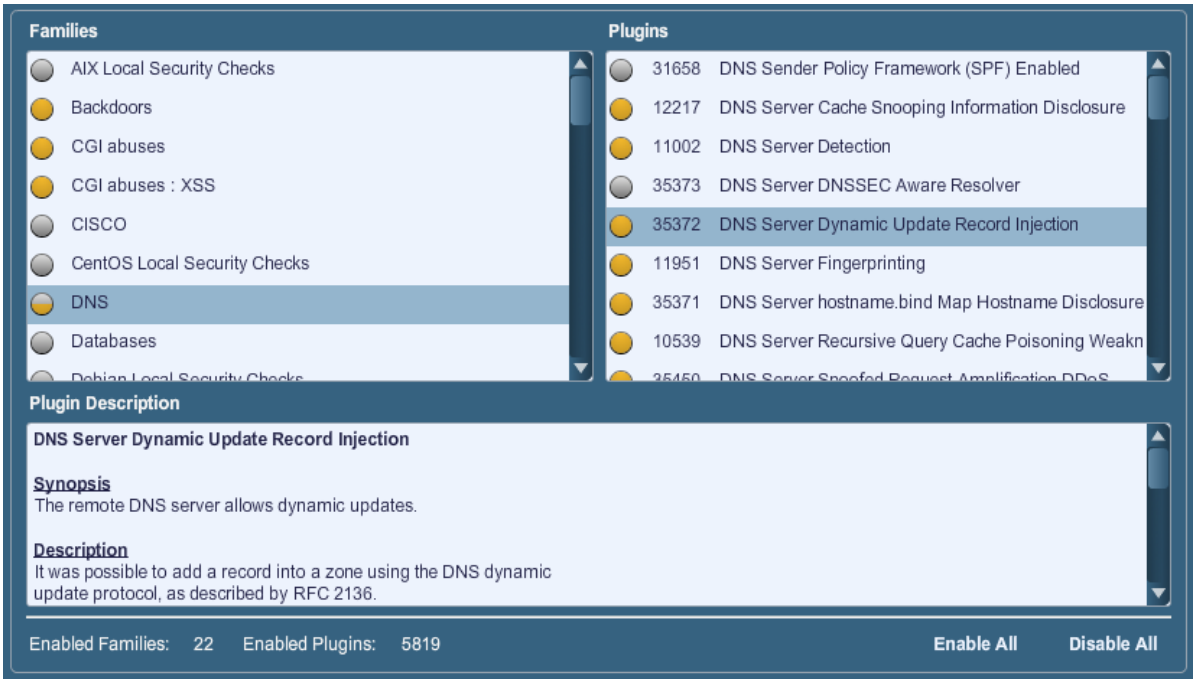
Não é recomendável usar credenciais em texto simples de qualquer tipo. Se as credenciais forem enviadas de maneira remota (por meio de uma varredura do Nessus, por exemplo), poderão ser interceptadas por qualquer pessoa com acesso à rede. Use mecanismos de autenticação criptografada sempre que possível.

Plugins

A guia Plugin Selection (Seleção de Plugins) permite que o usuário escolha verificações de segurança específicas por família de plugin ou verificações individuais.

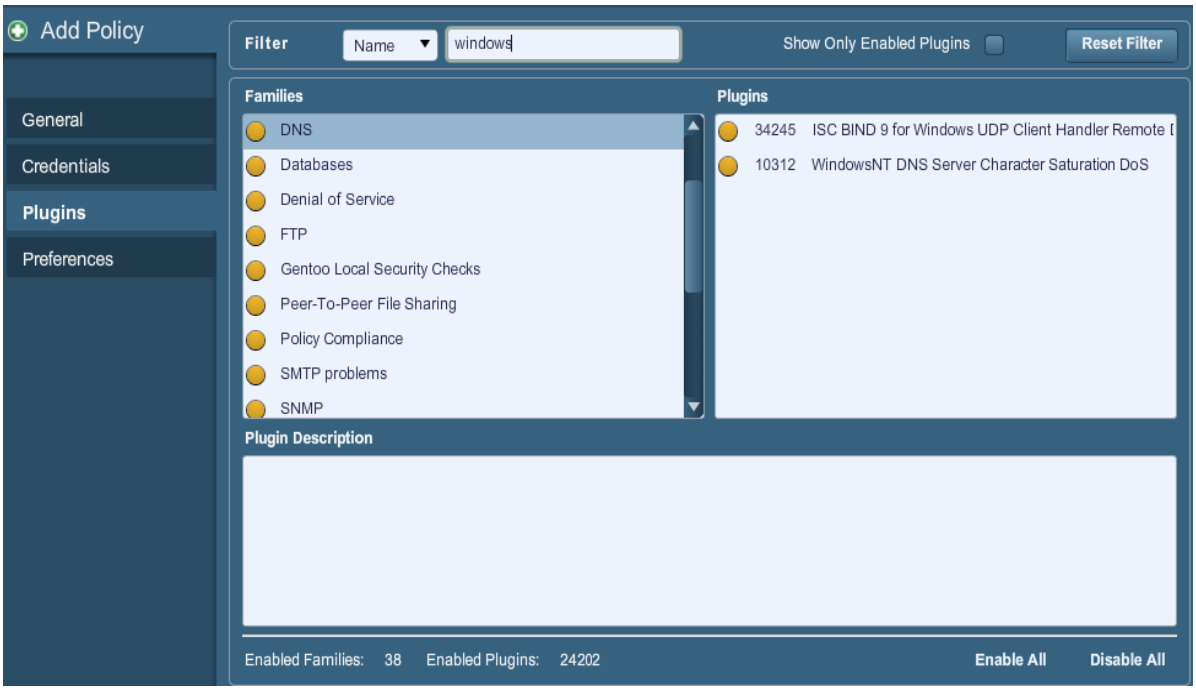


É possível clicar no círculo amarelo ao lado de uma família de plugins para ativar ou desativar a família inteira. A seleção da família exibirá a lista dos plugins no painel superior direito. Plugins individuais podem ser ativados ou desativado para criar políticas de varredura específicas. Depois que os ajustes forem feitos, o número total de famílias e plugins selecionados será exibido na parte inferior. Um círculo metade cinza e metade amarelo ao lado de uma família de plugins indica que alguns plugins estão ativados, mas não todos eles.



A seleção de um plugin específico mostrará o resultado do plugin a ser exibido como em um relatório. O resumo e a descrição fornecerão mais detalhes sobre a vulnerabilidade a ser examinada. Ao rolar o painel "Plugin Description" (Descrição dos Plugins) para baixo, é possível ver mais referências, se estiverem disponíveis, e a pontuação CVSSv2, que apresenta uma classificação básica de risco.

Na parte superior da guia de famílias de plugins, pode-se pesquisar um plugin específico por nome ou ID. Na caixa ao lado de "**Filter**" (Filtro), digite o texto para busca e tecle Enter:



Ao criar e salvar uma política, todos os plugins selecionados inicialmente são armazenados. Quando novos plugins forem recebidos com a atualização de feeds de plugins, serão ativados automaticamente se a família à qual estiverem associados for ativada. Se a família estiver desativada ou parcialmente ativada, os novos plugins da família também serão desativados automaticamente.

A família "Denial of Service" contém alguns plugins que podem causar falhas em uma rede corporativa caso a opção "Safe Checks" (Verificações Seguras) não estiver ativa, mas contém algumas verificações úteis que não causam danos. A família "Denial of Service" pode ser usada junto com "Safe Checks" para garantir que nenhum plugin potencialmente nocivo seja executado. No entanto, recomenda-se que a família "Denial of Service" não seja usada em uma rede de produção.

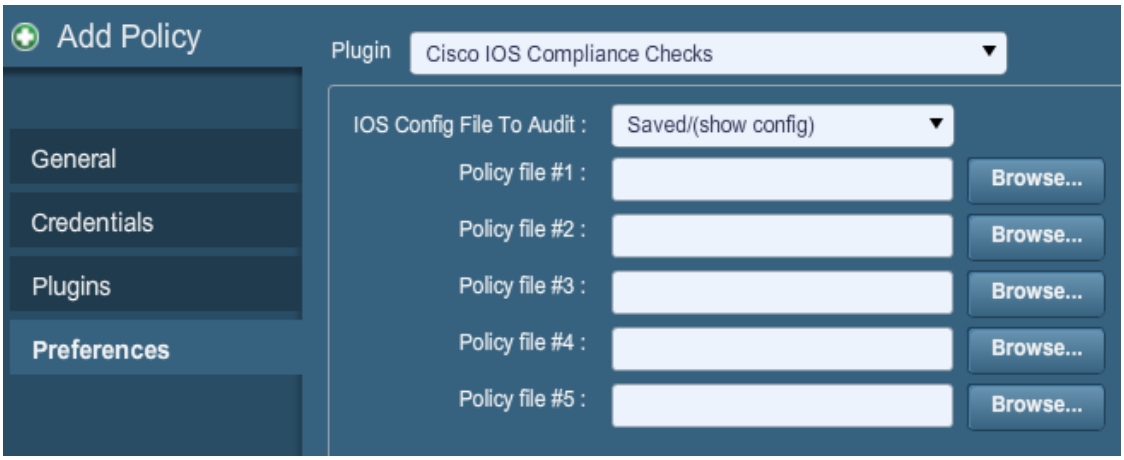
Abaixo da janela que mostra os plugins, o usuário encontrará duas opções que o ajudarão a selecionar os plugins.

Opção	Descrição
Enable all	Verifica e ativa todos os plugins e suas famílias. É a maneira conveniente de reativar todos os plugins depois de criar uma política com algumas famílias ou plugins desativados. Observe que alguns plugins podem exigir opções de configuração adicionais.

Disable all	Desmarca e desativa todos os plugins e suas famílias. A execução de uma varredura com todos os plugins desativados não irá gerar nenhum resultado.

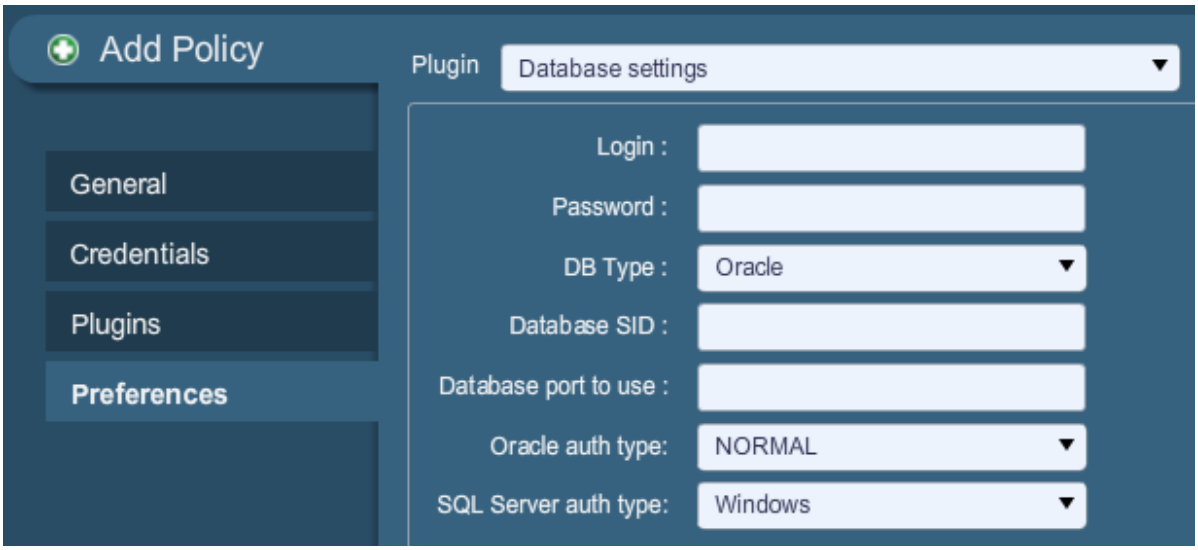
Preferences (Preferências)

A guia "**Preferences**" (Preferências) contém meios de controle individualizados para configuração de varreduras. Selecione um item no menu suspenso para exibir itens de configuração adicionais para a categoria selecionada. Observe que esta é uma lista dinâmica de opções de configuração e depende do feed de plugins, das políticas de auditoria e de outras funções às quais o scanner Nessus conectado tem acesso. Um scanner com ProfessionalFeed pode ter opções de configuração mais avançadas do que um scanner configurado com o HomeFeed. Esta lista também pode mudar à medida que os plugins são adicionados ou modificados.



"**Cisco IOS Compliance Checks**" permite que os clientes do ProfessionalFeed enviem arquivos de políticas que serão usados para determinar se um dispositivo Cisco IOS verificado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo. As políticas podem aplicadas com base nas configurações Salvo (`show config`), Em Execução (`show running`) ou Inicialização (`show startup`).

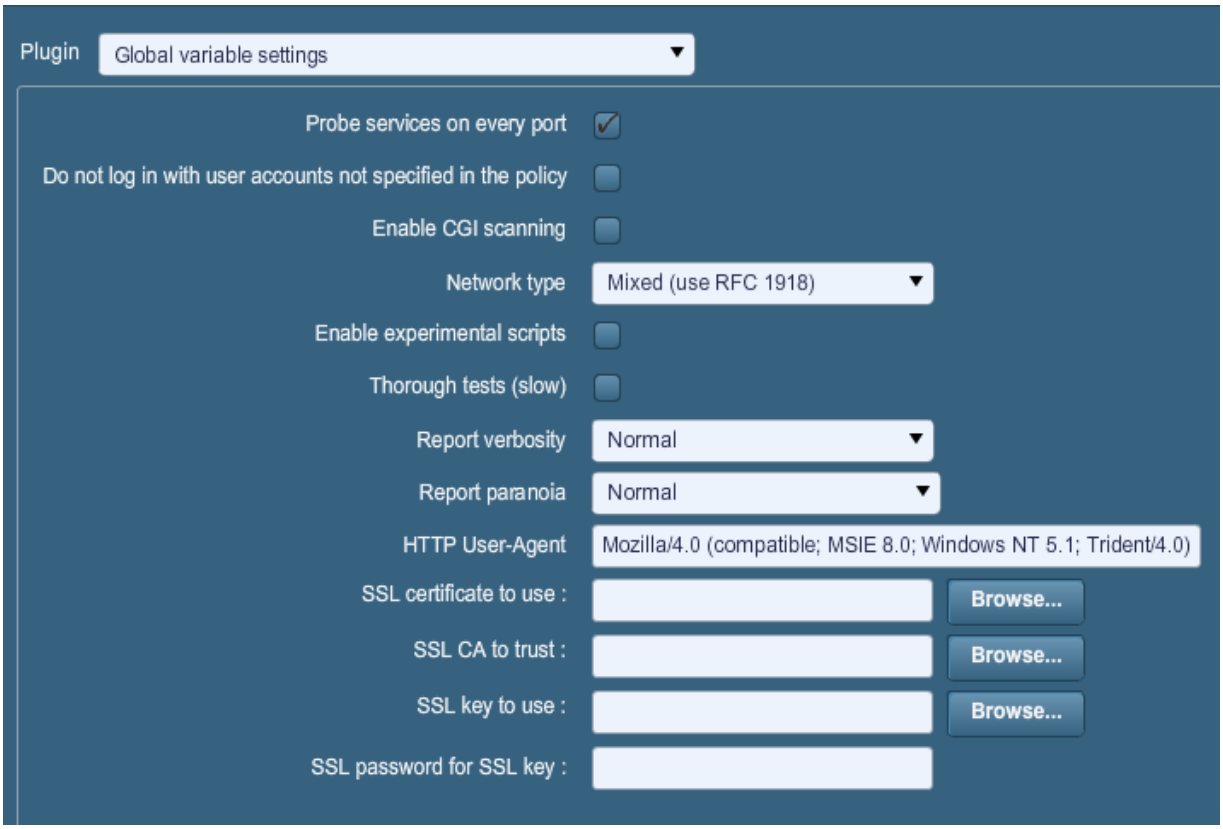
"**Database Compliance Checks**" permite que os clientes do ProfessionalFeed enviem arquivos de políticas que serão usados para determinar se um banco de dados testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.



As opções "**Database settings**" (Configurações de banco de dados) são usadas para especificar o tipo de banco de dados a ser verificado e as configurações e credenciais correspondentes:

Opção	Descrição
Login	O nome de usuário do banco de dados.
Password	A senha para o nome de usuário fornecido.
DB Type	Oracle, SQL Server, MySQL, DB2, Informix/DRDA e PostgreSQL são permitidos.
Database SID	ID do sistema de banco de dados para auditar.
Database port to use	Porta de escuta do banco de dados.
Oracle auth type	Normal, Sysoper e Sysdba são permitidos.
SQL Server auth type	Windows ou SQL são permitidos.

"**Do not scan fragile devices**" (Não verificar dispositivos frágeis) instrui o scanner Nessus a não fazer a varredura em impressoras nem hosts Novell Netware, se for selecionado. Uma vez que ambas as tecnologias são mais propensas a condições de negação de serviço, o Nessus pode omitir sua varredura. Isto é recomendável se a varredura for realizada durante o horário comercial.

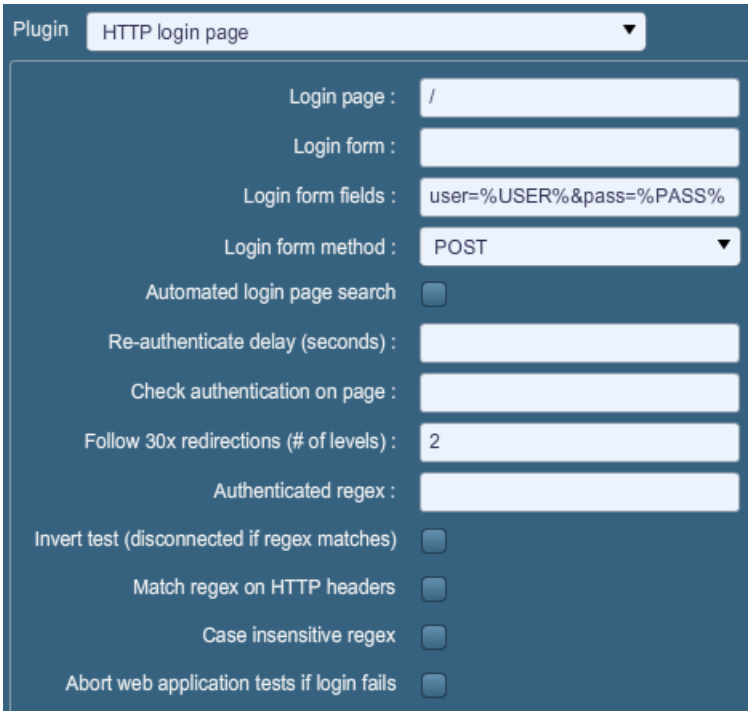


"**Global variable settings**" (Configurações de variáveis globais) contém uma grande variedade de opções de configuração para o servidor Nessus.

Opção	Descrição
Probe services on every port	Relaciona cada porta aberta ao serviço que está sendo executado na porta. Observe que, em alguns casos raros, isto pode prejudicar alguns serviços e causar efeitos colaterais inesperados.
Do not log in with user accounts not specified in the policy	Usado para evitar o bloqueio de contas se a política de senhas estiver definida para bloquear as contas depois de algumas tentativas inválidas.
Enable CGI scanning	Ativa a varredura de CGI. Desative esta opção para acelerar a auditoria de uma rede local.
Network type	Permite especificar se os IPs públicos roteáveis, IPs roteáveis privados não pertencentes à Internet ou uma combinação de ambos estão em uso. Selecione "Mixed" (Combinado) se os endereços RFC 1918 forem usados com diversos roteadores de rede.
Enable experimental scripts	Faz com que os plugins "em teste" sejam usados na varredura. Não ative esta opção durante a varredura de uma rede de produção.

Thorough tests (slow)	Permite que os plugins realizem testes "completos". Por exemplo: ao examinar compartilhamentos de arquivos SMB, um plugin pode analisar com três níveis de profundidade em vez de 1. Isto pode aumentar o tráfego da rede e as análises, em alguns casos. Observe que, por ser mais completa, a varredura deve ser mais invasiva e é mais provável que afete a rede, mas os resultados de auditoria podem ser melhores.
Report verbosity	Um valor mais alto irá gerar mais ou menos informações sobre a atividade do plugin no relatório.
Report paranoia	Em alguns casos, o Nessus não pode determinar remotamente se uma falha está presente ou não. Se Report paranoia (Sensibilidade do relatório) for definido como "**Paranoid**" (Sensível), uma falha sempre será relatada, mesmo se houver dúvidas sobre o host remoto afetado. Por outro lado, a configuração de sensibilidade "**Avoid false alarm**" (Evitar alarmes falsos) fará com que o Nessus não comunique nenhuma falha sempre que houver uma sombra de incerteza sobre o host remoto. A opção ("**Normal**") é a configuração padrão entre as configurações acima.
HTTP User-Agent	Especifica o tipo de navegador que o Nessus representará durante a varredura.
SSL certificate to use	Permite que o Nessus use certificado SSL no lado cliente para se comunicar com um host remoto.
SSL CA to trust	Especifica a Autoridade Certificadora (CA) para confiabilidade do Nessus.
SSL key to use	Especifica uma chave SSL local que será usada para se comunicar com o host remoto.
SSL password for SSL key	A senha usada para gerenciar a chave SSL especificada.

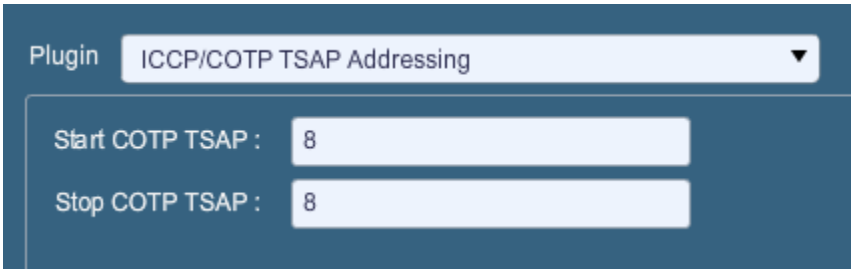
Para facilitar os testes de aplicativos da Web, o Nessus pode importar cookies HTTP de um outro software (por exemplo: navegador, proxy de Web etc.) com as configurações "**HTTP cookies import**" (Importação de cookies HTTP). Um arquivo de cookie pode ser enviado para que o Nessus utilize cookies para acessar um aplicativo da Web. O arquivo do cookie deve estar no formato Netscape.



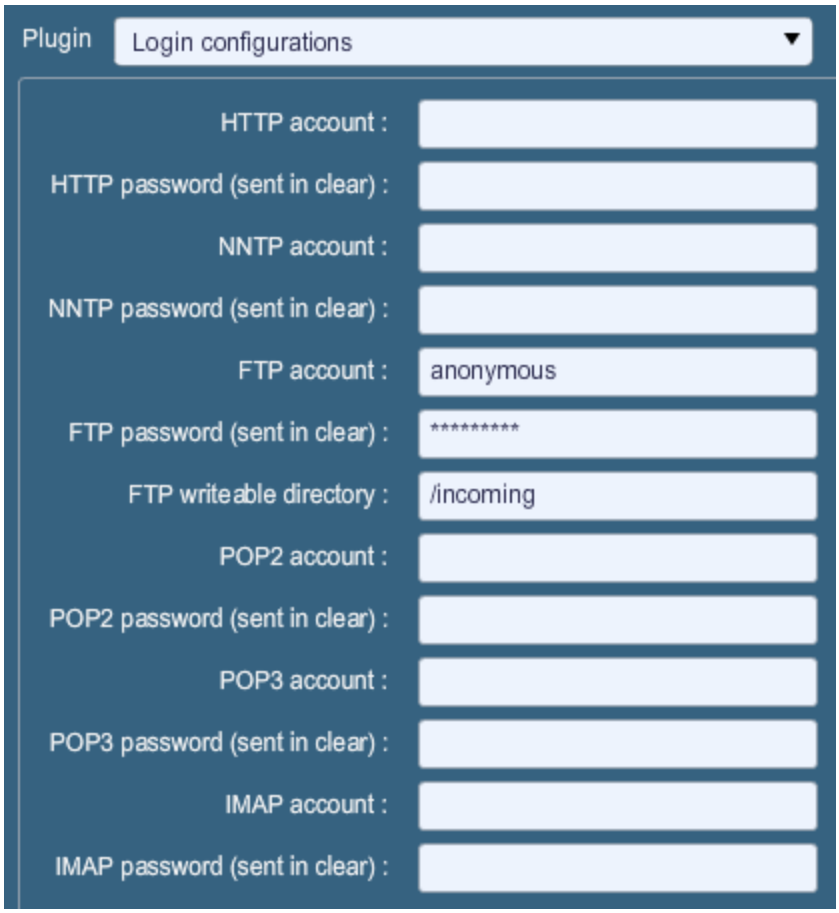
As configurações "**HTTP login page**" (Página de login de HTTP) permitem controlar o local em que os testes autenticados de um aplicativo de Web personalizado têm início.

Opção	Descrição
Login page	O URL básico para a página de login do aplicativo.
Login form	O parâmetro "action" do método do formulário. Por exemplo: o formulário de login de **`<form method="POST" name="auth_form" action="/login.php">`** deve ser "**`/login.php`**".
Login form fields	Especifica os parâmetros de autenticação (por exemplo: **`login=%USER%&password=%PASS%)`**. Se as palavras-chaves %USER% e %PASS% forem usadas, serão substituídas por valores fornecidos no menu suspenso "Login configurations" (Configurações de login). Este campo pode ser usado para fornecer mais de dois parâmetros, se necessário (por exemplo: um nome de "grupo" ou alguma outra informação é necessária para o processo de autenticação).
Login form method	Especifica se a ação de login é realizada por meio de uma solicitação GET ou POST.
Automated login page search	Instrui o Nessus a pesquisar uma página de login.
Re-authenticate delay (seconds)	O intervalo entre as tentativas de autenticação. Previne o acionamento de mecanismos de bloqueio por força bruta.

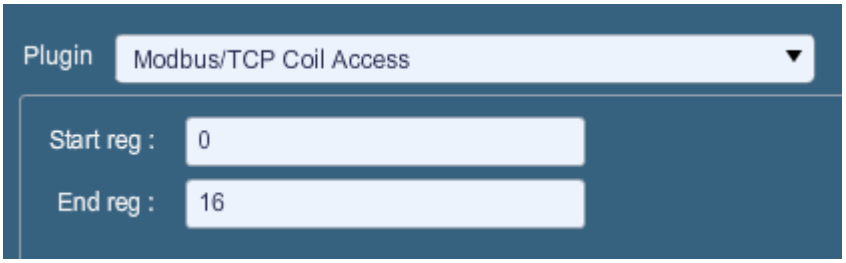
Check authentication on page	O URL de uma página da Web protegida que requer autenticação para ajudar o Nessus a definir o status de autenticação.
Follow 30x redirections (# of levels)	Se um código de redirecionamento 30x for recebido de um servidor Web, instruirá o Nessus a seguir o link fornecido ou não.
Authenticated regex	Um padrão regex para pesquisa na página de login. O recebimento de um código de resposta 200 nem sempre é suficiente para determinar o estado da sessão. O Nessus pode tentar localizar um determinado string, como "Authentication successful!" (Autenticação concluída).
Invert test (disconnected if regex matches)	Um padrão regex para pesquisa na página de login. Se for encontrado, indica ao Nessus que a autenticação não foi concluída (por exemplo: "Authentication failed!").
Match regex on HTTP headers	O Nessus pode pesquisar um determinado padrão regex nos cabeçalhos de resposta HTTP para definir melhor o estado de autenticação, ao invés de pesquisar no corpo de uma resposta.
Case insensitive regex	Normalmente, as pesquisas por regex diferenciam maiúsculas de minúsculas. O comando instrui o Nessus a ignorar a caixa.
Abort web application tests if login fails	Se as credenciais fornecidas não funcionarem, o Nessus interromperá os testes personalizados de aplicativos da Web, mas não as famílias de plugins de CGI.



O menu "**ICCP/COTP TSAP Addressing"** (Endereçamento ICCP/COTP TSAP) está relacionado especificamente às verificações Scada. O menu determina um valor de Pontos de Acesso de Serviço de Transporte (TSAP) do protocolo de Transporte Orientado a Conexões (COTP) em um servidor ICCP. Os valores de início e parada são definidos inicialmente como "8".



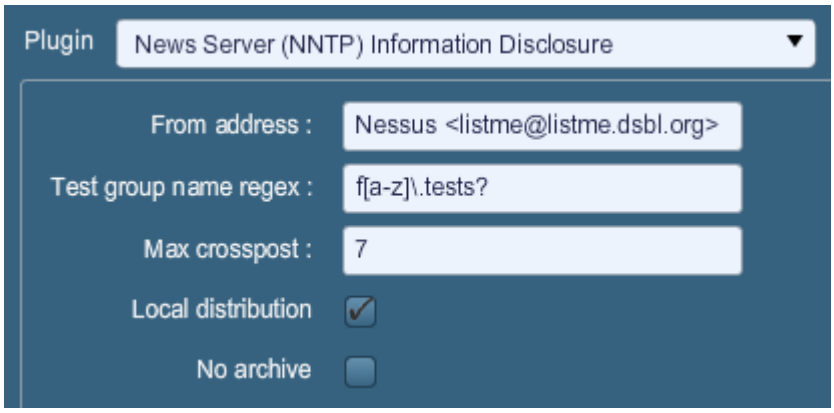
"**Login configurations**" (Configurações de Login) permite que o scanner Nessus use credenciais ao verificar HTTP, NNTP, FTP, POP2, POP3 ou IMAP. Ao fornecer credenciais, o Nessus pode realizar verificações mais abrangentes para determinar as vulnerabilidades. As credenciais de HTTP fornecidas aqui serão usadas apenas para autenticação básica e resumida. Para configurar as credenciais de um aplicativo da Web personalizado, use o menu suspenso "HTTP login page" (Página de login HTTP).



As opções "**Modbus/TCP Coil Access**" estão disponíveis para os usuários do ProfessionalFeed. Este item de menu é gerado dinamicamente pelos plugins SCADA disponíveis com o ProfessionalFeed. O Modbus usa o código de função 1 para ler "bobinas" em um escravo Modbus. As bobinas representam configurações de saída binárias e normalmente são correlacionadas com atuadores. A capacidade de ler bobinas pode permite a um atacante criar um perfil do sistema, identificar intervalos de registros e alterá-los por meio de uma mensagem "write coil" (gravar bobina). Os valores padrão são "0" para o reg Start e "16" para o reg End.

"As opções "**Nessus SYN scanner**" e "**Nessus TCP scanner**" permitem configurar os scanners SYN e TCP originais para detectar a presença de um firewall.

Valor	Descrição
Automatic (normal)	Esta opção pode ajudar a identificar se um firewall está localizado entre o scanner e o destino (**padrão**).
Disabled (softer)	Desativa o recurso **Firewall detection** (Detecção de firewall).
Do not detect RST rate limitation (soft)	Desativa a funcionalidade de monitoramento do número de reinícios definidos e determina se há uma limitação configurada por um dispositivo de rede local.
Ignore closed ports (aggressive)	Tenta executar os plugins mesmo que a porta estiver fechada. Recomenda-se que esta opção não seja usada em uma rede de produção.



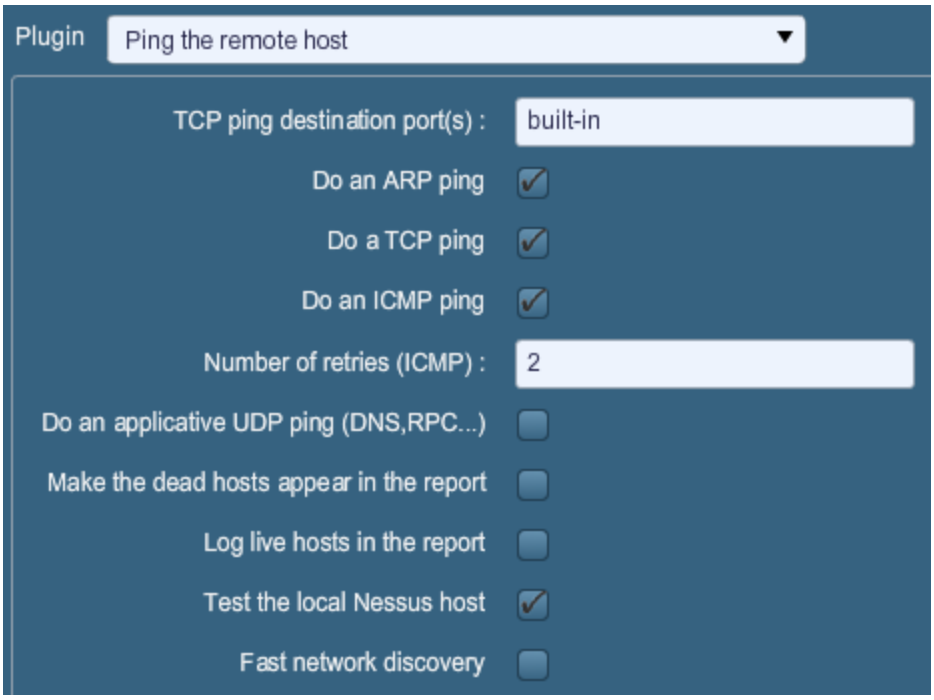
"A opção "**News Server (NNTP) Information Disclosure**" (Divulgação de Informações do Servidor de Notícias (NNTP)) pode ser usada para determinar a existência de servidores de notícias capazes de distribuir spam. O Nessus tentará publicar uma mensagem ao(s) servidor(es) de notícias NNTP (Protocolo de Transporte de Notícias em Rede) para verificar se é possível enviar uma mensagem a servidores de notícias em um ponto da rede remota.

Opção	Descrição
From address	O endereço que o Nessus usará ao tentar enviar uma mensagem ao(s) servidor(es) de notícias. Essa mensagem será excluída automaticamente após um breve intervalo de tempo.
Test group name regex	Nome do grupo de notícias que receberá uma mensagem de teste do endereço especificado. O nome pode ser especificado como uma expressão regular (regex) para que a mensagem possa ser enviada simultaneamente a vários grupos de notícias. Por exemplo: o valor padrão "**f[a-z]\.tests?**" transmitirá uma

	mensagem de e-mail a todos os grupos de notícias com nomes que começam com qualquer letra (de "a" a "z") e terminam com ".tests" (ou alguma variação que corresponda ao string). O ponto de interrogação age como um caractere curinga opcional.
Max crosspost	O número máximo de servidores de notícias que receberão a publicação de teste, independentemente do número de correspondências de nomes. Por exemplo: se o crosspost Max for "**7**", a mensagem de teste será enviada apenas a sete servidores de notícias, mesmo que haja 2.000 servidores de notícias correspondentes ao regex neste campo.
Local distribution	Se esta opção for selecionada, o Nessus tentará enviar apenas uma mensagem ao(s) servidor(es) de notícias local(is). Caso contrário, tentará encaminhar a mensagem a um ponto remoto.
No archive	Se esta opção for selecionada, o Nessus solicitará para não arquivar a mensagem de teste enviada ao(s) servidor(es) de notícias. Caso contrário, a mensagem será arquivada como qualquer outra publicação.

"**Oracle Settings**" (Configurações do Oracle) configura o Nessus com o Oracle Database SID e inclui uma opção para testar contas padrão conhecidas no software da Oracle.

"**PCI DSS Compliance**" fará com que o Nessus compare os resultados das varreduras com as normas de conformidade PCI DSS vigentes. Este recurso está disponível apenas para os clientes do ProfessionalFeed.

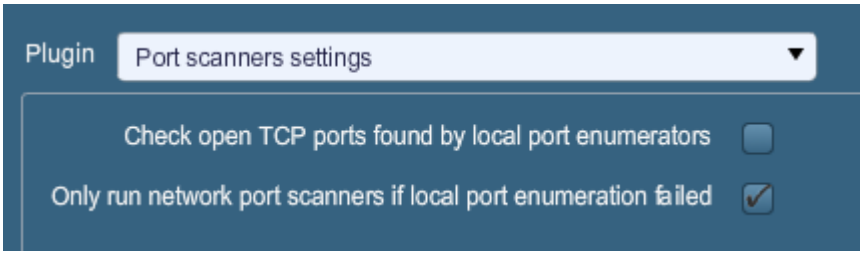


"As opções "**Ping the remote host**" (Teste de ping para o host remoto) permitem um controle individualizado sobre a capacidade do Nessus de enviar testes de conexão a hosts durante a varredura de descoberta. Isto pode ser feito com ping ARP, ping TCP, ping ICMP ou ping UDP de aplicativo.

Opção	Descrição
TCP ping destination port(s)	Especifica a lista de portas a serem verificadas por meio do teste de ping TCP. Se tiver dúvidas com relação às portas, deixe esta configuração com o valor padrão "interno".
Number of Retries (ICMP)"	Permite especificar o número de tentativas de ping ao host remoto. O valor padrão é 6.
Do an applicative UDP ping (DNS, RPC...)	Executa um teste de ping UDP em aplicativos específicos que usam UDP, incluindo DNS (porta 53), RPC (porta 111), NTP (porta 123) e RIP (porta 520).
Make the dead hosts appear in the report	Se esta opção for selecionada, os hosts que não responderam à solicitação de ping serão incluídos no relatório de segurança como hosts "inativos".
Log live hosts in the report	Selecione esta opção para comunicar especificamente a capacidade de enviar um ping a um host remoto.
Test the local Nessus host	Esta opção permite que o usuário inclua ou exclua o host do Nessus local da varredura. Esta opção é usada quando o host Nessus estiver dentro do intervalo de rede de destino da varredura.

Fast network discovery	Normalmente, ao enviar um "ping" a um IP remoto com uma resposta, o Nessus realiza varreduras adicionais para verificar se não se trata de um proxy transparente ou um balanceador de carga gerando ruído, mas sem resultado (alguns dispositivos respondem a todas as portas de 1 a 65.535, mas não há nenhum serviço em segundo plano). As verificações podem demorar um pouco, especialmente se o host remoto estiver protegido por um firewall. Se a "descoberta rápida de rede" estiver ativada, o Nessus não realizará as varreduras.

Para examinar os sistemas VMware convidados, o "ping" deve ser desativado. Na política de varredura em "Advanced" (Avançado) -> "Ping the remote host" (Ping para o host remoto), desmarque o ping de TCP, ICMP e ARP.



"**Port scanner settings**" (Configurações do scanner de portas) oferece duas opções adicionais para controlar a atividade de varredura de portas:

Opção	Descrição
Check open TCP ports found by local port enumerators	Se um enumerador de portas locais (por exemplo: WMI ou netstat) encontrar uma porta, o Nessus também verificará se está aberta remotamente. Isto ajuda a determinar se alguma forma de controle de acesso está em uso (por exemplo: TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed	Nesse caso, use primeiro a enumeração de portas locais.

"**SMB Registry: Start the Registry Service during the scan**" (Registro de SMB: Iniciar o Serviço de Registro durante a varredura) permite que o serviço intermedeie algumas das exigências de varredura para computadores em que o registro SMB não funcione todo o tempo.

No menu "**SMB Scope**" (Escopo de SMB), se a opção "**Request information about the domain**" (Solicitar informações sobre o domínio) estiver selecionada, os usuários do domínio, e não os usuários locais, serão consultados.

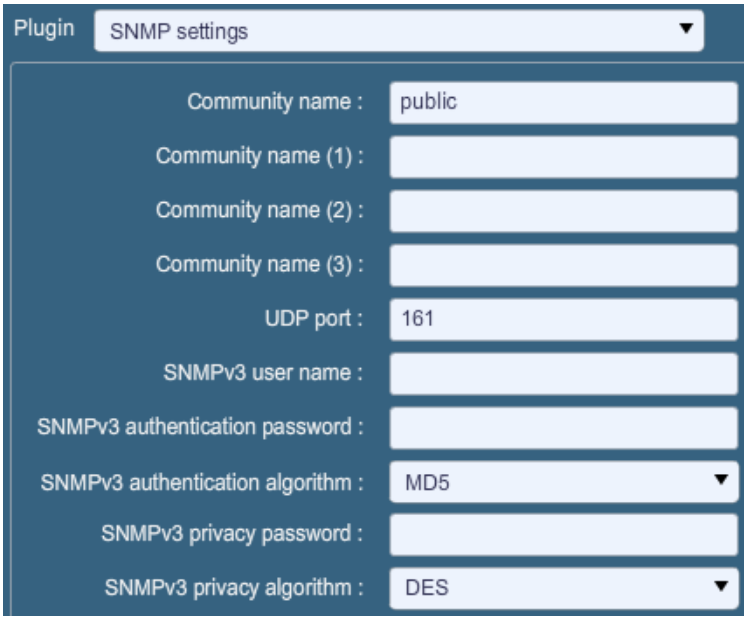
"**SMB Use Domain SID to Enumerate Users**" (SMB usa o SID de Domínio para Enumerar Usuários) especifica o intervalo de SID a ser usado para realizar uma consulta inversa de

nomes de usuários no domínio. A configuração padrão é recomendada para a maioria das varreduras.

"**SMB Use Host SID to Enumerate Local Users**" (SMB usa o SID de Host para Enumerar Usuários) especifica o intervalo de SID a ser usado para executar uma consulta inversa de nomes de usuários locais. A configuração padrão é recomendada.

"**SMTP settings**" (Configurações de SMTP) especifica as opções para os testes de SMTP (Protocolo Simples de Transporte de Correio) executados em todos os dispositivos dentro do domínio verificado que estão executando serviços SMTP. O Nessus tentará retransmitir mensagens por meio do dispositivo ao domínio de terceiros especificado ("**Third party domain**"). Se a mensagem enviada a "**Third party domain**" for recusada pelo endereço especificado no campo "**To address**" (Endereço de destino), ocorrerá falha na tentativa de spam. Se a mensagem for aceita, o servidor de SMTP foi usado com sucesso para retransmitir o spam.

Opção	Descrição
Third party domain	O Nessus tentará enviar spam por meio de cada dispositivo de SMTP para o endereço listado neste campo. O endereço de domínio de terceiros deve estar fora do intervalo do site que está sendo examinado ou do site que está realizando a varredura. Caso contrário, o teste pode ser interrompido pelo servidor SMTP.
From address	As mensagens de teste enviadas ao(s) servidor(es) SMTP aparecerão como se fosse originadas do endereço especificado neste campo.
To address	O Nessus tentará enviar mensagens endereçadas ao destinatário da mensagem indicado neste campo. O endereço **postmaster** é o valor padrão, pois é um endereço válido na maioria dos servidores de correio.



"**SNMP settings**" (Configurações de SNMP) permite configurar o Nessus para se conectar e autenticar no serviço SNMP do destino. Durante a varredura, o Nessus fará algumas tentativas de descobrir o string da comunidade e usá-la em testes subsequentes. Até quatro strings de nomes de comunidades separadas podem ser usados por política de varredura. Se o Nessus não localizar o string e/ou a senha da comunidade, não poderá realizar uma auditoria completa do serviço.

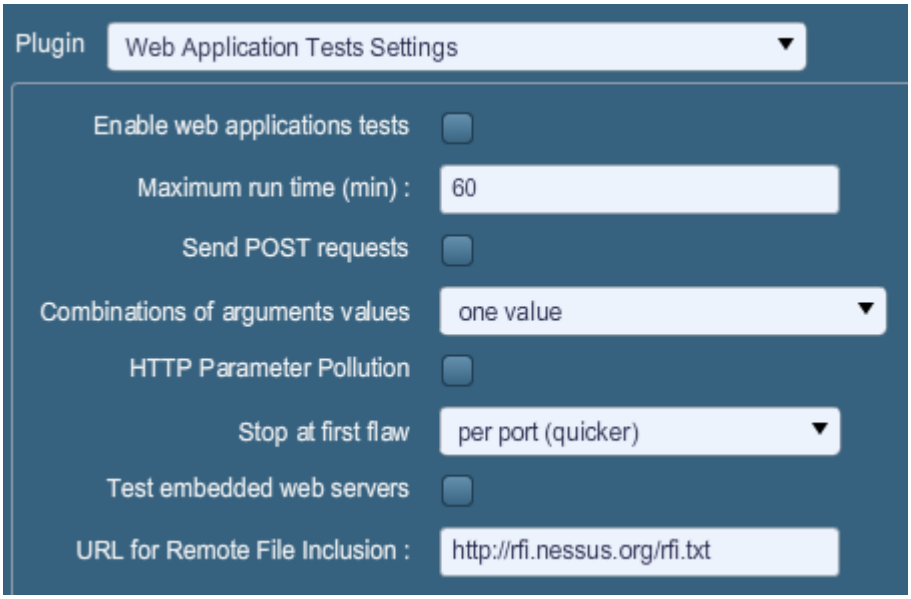
Opção	Descrição
Community name (0-3)	O nome da comunidade SNMP.
UDP port	Instrui o Nessus a verificar uma porta diferente caso o SNMP esteja sendo executado em uma porta que não seja a porta 161.
SNMPv3 user name	O nome de usuário de uma conta que usa SNMPv3.
SNMPv3 authentication password	A senha do nome de usuário especificado.
SNMPv3 authentication algorithm	Selecione MD5 ou SHA1, dependendo do algoritmo reconhecido pelo serviço remoto.
SNMPv3 privacy password	A senha usada para proteger a comunicação SNMP criptografada.
SNMPv3 privacy algorithm	O algoritmo de criptografia a ser usado para o tráfego SNMP.

"**Service Detection**" (Detecção de Serviços) controla o modo como o Nessus testará serviços SSL: portas SSL conhecidas (por exemplo: 443), todas as portas ou nenhuma. O teste de funcionalidade SSL em todas as portas pode afetar o host verificado.

"Wake-on-LAN" controla os hosts que receberão pacotes "mágicos" WOL antes de realizar uma varredura, além do tempo de espera (em minutos) para a inicialização dos sistemas. A lista de endereços MAC do WOL é inserida por meio de um arquivo de texto enviado com um endereço MAC de host por linha. Por exemplo:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
[…]
```

"**Unix Compliance Checks**" permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Unix que serão usado para determinar se um sistema testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.



"**Web Application Tests Settings**" (Configurações dos Testes de Aplicativos de Web) verifica os argumentos das CGIs (Common Gateway Interfaces) remotas descobertas no processo de espelhamento de Web ao tentar enviar erros comuns de programação de CGI, como cross-site scripting, inclusão remota de arquivos, execução de comandos, ataques transversais ou injeção de SQL. Ative esta opção marcando a caixa de seleção "Enable web applications tests" (Ativar testes de aplicativos de Web). Os testes dependem dos seguintes plugins NASL:

- 11139, 42424, 42479, 42426, 42427, 43160 – Injeção de SQL (abuso de CGI)
- 39465, 44967 – Execução de comandos (abuso de CGI)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (abuso de CGI: XSS)
- 39467, 46195, 46194 – Directory Traversal (abuso de CGI)
- 39468 – HTTP Header Injection (abuso de CGI: XSS)
- 39469, 42056, 42872 – Inclusão de arquivo (abuso de CGI)
- 42055 - String de formato (abuso de CGI)
- 42423, 42054 - Server Side Includes (abuso de CGI)

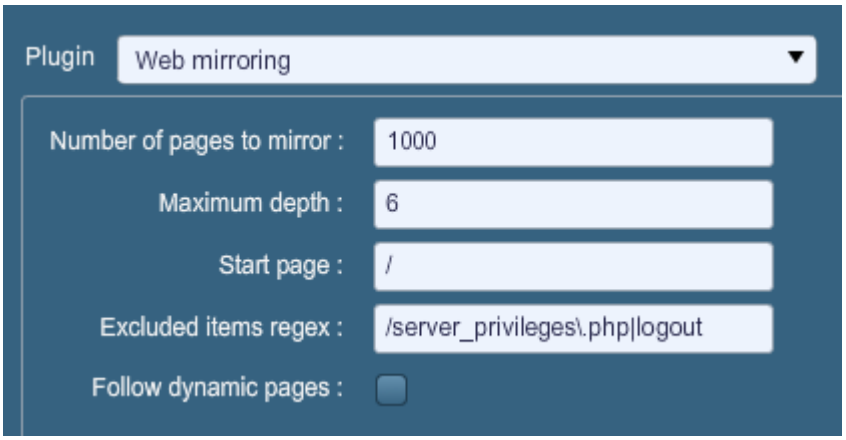
- 44136 - Cookie Manipulation (abuso de CGI)
- 46196 - XML Injection (abuso de CGI)
- 40406, 48926, 48927 - Mensagens de erro
- 47830, 47832, 47834, 44134 - Ataques adicionais (abuso de CGI)

Nota: Esta lista de plugins relacionados a aplicativos de Web é atualizada com frequência. Os plugins adicionais podem depender das configurações desta opção de preferência.

Opção	Descrição
Maximum run time (min)	Esta opção gerencia o tempo (em minutos) usado na execução de testes de aplicativos de Web. O valor inicial desta opção é 60 minutos e se aplica a todas as portas e CGIs de um determinado site. A varredura de sites da rede local com aplicativos pequenos normalmente é realizada em menos de uma hora. No entanto, sites com aplicativos maiores podem exigir um valor maior.
Send POST requests	Os testes de "solicitação de POST" são usados para testes avançados de formulários da Web. Normalmente, os testes de aplicativos de Web usarão apenas solicitações GET, a menos que esta opção esteja ativada. Em geral, aplicativos mais complexos usam o método POST quando um usuário envia dados ao aplicativo. Esta configuração permite um teste mais completo, mas pode aumentar consideravelmente o tempo exigido. Se esta opção for selecionada, o Nessus testará cada script/variável com as solicitações GET e POST.
Combinations of arguments values	Esta opção gerencia a combinação de valores dos argumentos usados nas solicitações de HTTP. Este menu suspenso possui três opções: **one value** – Testa um parâmetro por vez com um string de ataque sem tentar variações de parâmetros adicionais "sem ataque". Por exemplo: o Nessus tentaria aplicar "`/test.php?arg1=XSS&b=1&c=1`" onde "b" e "c" permitem outros valores, sem testar cada combinação. Este é o método mais rápido de teste com o menor conjunto de resultados gerados. **All pairs (slower but efficient)** – Esta forma de teste é um pouco mais lenta, mas é mais eficaz que o teste "one value". Ao verificar diversos parâmetros, verifica também o string de ataque, as variações de uma única variável e usa o primeiro valor com todas as outras variáveis. Por exemplo: o Nessus tenta aplicar "`/test.php?a=XSS&b=1&c=1&d=1`" e percorre as variáveis , de modo que uma receba o string de ataque e a outra redefine todos os valores possíveis (conforme descoberto durante o processo de espelhamento) e qualquer outra variável recebe o primeiro valor. Neste caso, o Nessus nunca testará "`/test.php?a=XSS&b=3&c=3&d=3`" quando o primeiro valor de cada variável for "1".

	All combinations (extremely slow) – Este método de teste realiza um teste completo de todas as combinações possíveis de sequências de ataque com entrada válida nas variáveis. Enquanto o teste "All-pairs" (Todos os pares) cria um conjunto menor de dados para maior desempenho, esta opção é bastante lenta, pois usa um conjunto completo de dados de testes. Esse método de teste **pode levar muito tempo** para ser concluído.
HTTP Parameter Pollution	Ao realizar testes de aplicativos da Web, esta opção tenta contornar qualquer mecanismo de filtragem por meio da injeção de conteúdo em uma variável enquanto fornece a mesma variável com conteúdo válido. Por exemplo: um teste de injeção SQL normal pode ter o seguinte aspecto: "`/target.cgi?a='&b=2`". Com a opção HTTP Parameter Pollution (HPP) ativada, a solicitação pode parecer a seguinte: "`/target.cgi?a='&a=1&b=2`".
Stop at first flaw	Esta opção determina um ataque em uma nova falha. Isto é feito ao nível do script. A detecção de uma falha de XSS não desativará as pesquisas de injeção de SQL ou injeção de cabeçalho, mas haverá, no máximo, um relatório para cada tipo em uma determinada porta, a menos que "thorough tests" (testes completos) esteja definido. Observe que várias falhas do mesmo tipo (por exemplo: XSS, SQLI etc.) podem ser relatadas às vezes, se forem detectadas pelo mesmo ataque. O menu suspenso possui quatro opções: **per CGI** – Assim que uma falha é encontrada em uma CGI por um script, o Nessus passa à CGI conhecida seguinte no mesmo servidor ou, se não houver outras CGIs, à porta/servidor seguinte. Esta é a opção padrão. **per port (quicker)** – Assim que uma falha é encontrada em um servidor Web por um script, o Nessus pára e alterna para o outro servidor Web em uma porta diferente. **per parameter (slow)** – Quando um tipo de falha é encontrado em um parâmetro de uma CGI (por exemplo: XSS), o Nessus alterna para o parâmetro seguinte da mesma CGI ou da CGI conhecida ou para a porta/servidor seguinte. **look for all flaws (slower)** – Execute testes completos, independentemente das falhas encontradas. Esta opção pode gerar um relatório muito detalhado e, na maioria dos casos, não é recomendável.
Test Embedded web servers	Os servidores Web incorporados são, muitas vezes, estáticos e não contêm scripts de CGI personalizáveis. Além disso, os servidores Web incorporados podem travar ou deixar de responder quando passam por uma varredura. A Tenable recomenda que os servidores Web incorporados sejam

	examinados separadamente de outros servidores Web com esta opção.
URL for Remote File Inclusion	Durante testes de inclusão remota de arquivos (RFI), esta opção especifica um arquivo em um host remoto para ser usado nos testes. Por padrão, o Nessus usará um arquivo seguro hospedado no servidor Web da Tenable para os testes de RFI. Se o scanner não tiver acesso à Internet, recomenda-se usar um arquivo hospedado internamente para realizar testes mais precisos de RFI.



"**Web Mirroring**" (Espelhamento de Web) define os parâmetros de configuração para o utilitário original de espelhamento de conteúdo do servidor Web do Nessus. O Nessus realiza o espelhamento do conteúdo da Web para aprimorar a análise de vulnerabilidades e ajudar a reduzir o impacto sobre o servidor.

Se os parâmetros de espelhamento da Web forem definidos de maneira a espelhar um site inteiro, o aumento significativo do tráfego poderá ocorrer durante a varredura. Por exemplo: se houver 1 gigabyte de material em um servidor Web e o Nessus estiver configurado para espelhar todo o conteúdo, a varredura irá gerar pelo menos 1 gigabyte de tráfego do servidor para o scanner Nessus.

Opção	Descrição
Number of pages to mirror	Número máximo de páginas a espelhar.
Maximum depth	Limita o número de links que o Nessus seguirá em cada página inicial.
Start page	O URL da primeira página a ser verificada. Se forem necessárias várias páginas, use dois pontos para separá-las (por exemplo: "/:/php4:/base").
Excluded items regex	Permite que partes do site não estejam sujeitas ao rastreamento. Por exemplo: para excluir o diretório

	"/manual" e todas as CGIs Perl, defina esse campo como: **(^/ manual)	(\ . pl (\ ?. *) ?$) .**
Follow dynamic pages	Se esta opção for selecionada, o Nessus seguirá os links dinâmicos e pode exceder os parâmetros definidos acima.

"**Windows Compliance Checks**" permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Microsoft Windows, que serão usados para determinar se um sistema testado cumpre as normas de conformidade especificadas. Até cinco políticas podem ser selecionadas ao mesmo tempo.

"**Windows File Contents Compliance Checks**" (Verificações de Conformidade do Conteúdo de Arquivos do Windows) permite que os clientes do ProfessionalFeed enviem arquivos de auditoria do Windows que pesquisam tipos específicos de conteúdos no sistema (por exemplo: cartões de crédito, números de documentos de identidade) para ajudar a determinar o cumprimento de normas internas da empresa ou normas externas.

Quando todas as opções forem configuradas da maneira desejada, clique em "**Submit**" (Enviar) para salvar a política e voltar à guia Políticas (Políticas). A qualquer momento, clique em "**Edit**" (Editar) para fazer alterações em uma política criada ou clique em "**Delete**" (Excluir) para excluir completamente uma política.

IMPORTAR, EXPORTAR E COPIAR POLÍTICAS

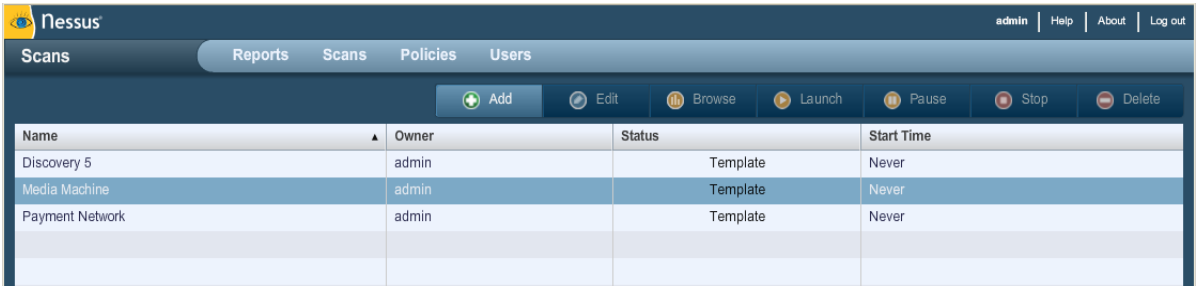
O botão "**Import**" (Importar) na barra de menus superior direita permite enviar políticas criadas ao scanner. Na caixa de diálogo "**Browse**" (Procurar...), selecione a política no sistema local e clique em "**Submit**" (Enviar).

O botão "**Export**" (Exportar) na barra de menus permite baixar uma política existente do scanner para o sistema de arquivos local. A caixa de diálogo de download do navegador permite abrir a política em um programa externo (por exemplo: editor de texto) ou salvá-la em um diretório de sua preferência.

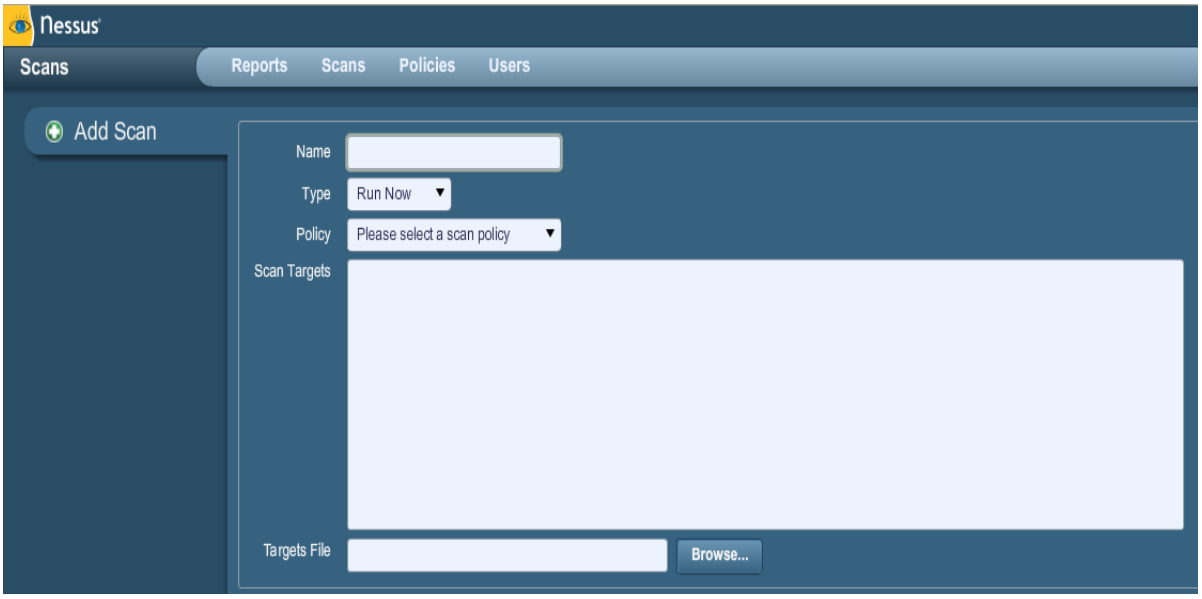
As senhas e os arquivos `.audit` presentes em uma política **não** serão exportados.

Para criar uma política semelhante à uma política existente, mas com algumas modificações, selecione a política básica na lista e clique em "**Copy**" (Copiar) na barra de menus superior direita. Isto criará uma cópia da política original, que pode ser editada com as modificações necessárias. Isto permite criar políticas padrão com algumas alterações necessárias para um determinado ambiente.

CRIAR, INICIAR E PROGRAMAR UMA VARREDURA



Depois de criar uma política, é possível criar uma nova varredura ao clicar na opção "**Scans**" (Varreduras) na barra de menus superior e no botão "**+ Add**" (Adicionar) à direita. A tela "**Add Scan**" (Adicionar Varredura) será exibida da seguinte maneira:



Existem cinco campos para informar o alvo da varredura:

- **Name** – Define o nome que será exibido na interface do usuário do Nessus para identificar a política.
- **Type** – Selecione "Run Now" (executar imediatamente a varredura após o envio), "Scheduled" (horário em que a varredura deve começar) ou "Template" (salvar como modelo para varreduras recorrentes).
- **Policy** – Selecione uma política já criada a ser usada pela varredura para definir os parâmetros que controlam o comportamento de varredura do servidor Nessus.
- **Scan Targets** – Os alvos podem ser inseridos com um endereço IP simples (por exemplo: 192.168.0.1), um intervalo de IPs (por exemplo: 192.168.0.1-192.168.0.255), uma sub-rede com a notação CIDR (por exemplo: 192.168.0.0/24) ou um host conversível (por exemplo: www.nessus.org).
- **Targets File** – É possível importar um arquivo de texto com uma lista de hosts ao clicar em "**Browse...**" (Procurar) e selecionar um arquivo no computador local.

O arquivo de host deve ser formatado como texto ASCII, com um host por linha e sem espaços ou linhas extras. A codificação Unicode/UTF-8 não é reconhecida.

Exemplo de formatos de arquivos de host:

Hosts individuais:

192.168.0.100
192.168.0.101
192.168.0.102

Intervalo de hosts:

192.168.0.100-192.168.0.102

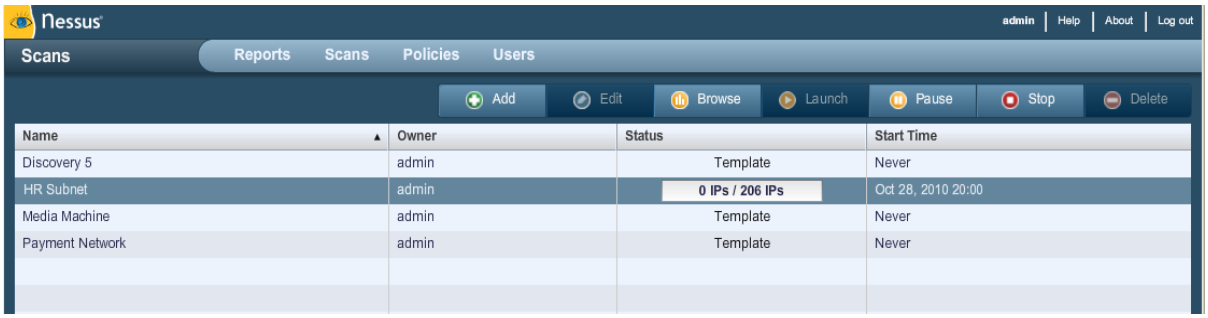
Bloco CIDR de hosts:

192.168.0.1/24

Servidores virtuais:

www.tenable.com[192.168.1.1]
www.nessus.org[192.168.1.1]
www.tenablesecurity.com[192.168.1.1]

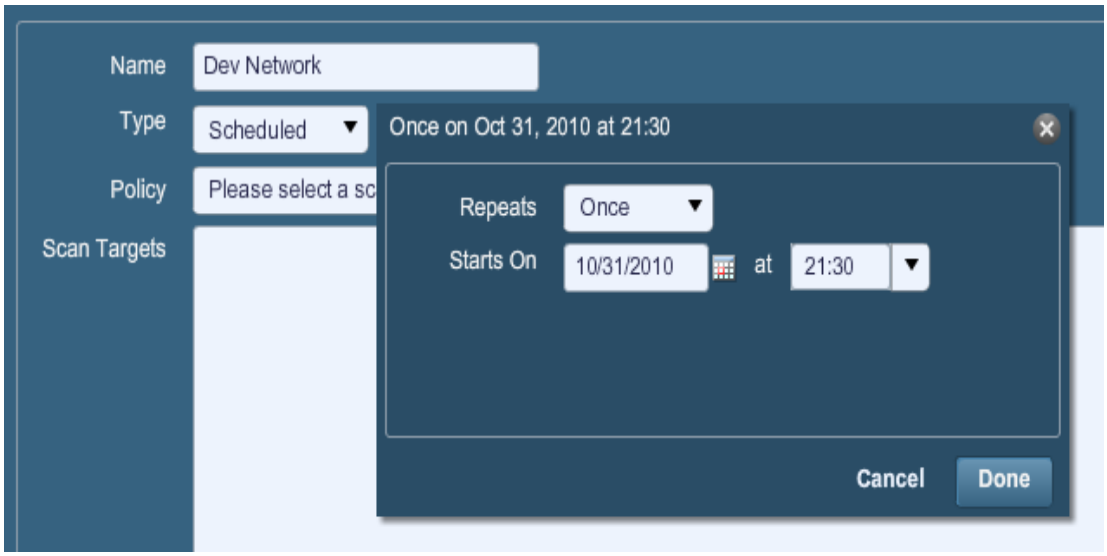
Depois de inserir as informações de varredura, clique em "**Submit**" (Enviar). Depois do envio, a varredura iniciará imediatamente (se "Run Now" for selecionado) antes que a tela retorne à página geral de "**Scans**" (Varreduras).



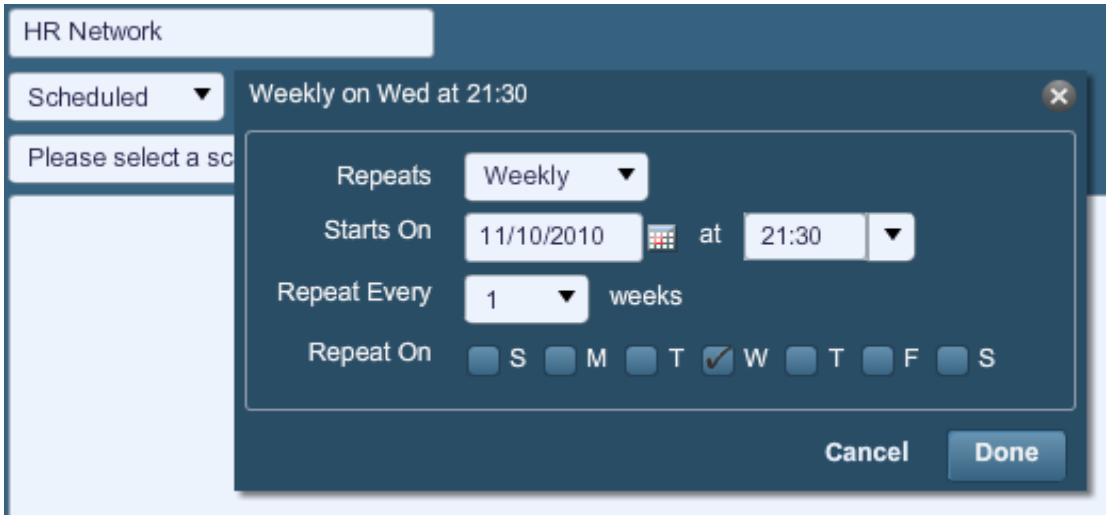
Depois que a varredura for iniciada, a lista Scans exibirá todas as varreduras em execução, em pausa ou em forma de modelo, além de informações básicas sobre cada varredura. Depois de selecionar uma varredura específica na lista, os botões de ação no canto superior direito permitem pesquisar os resultados da varredura em progresso, pausar e reiniciar a varredura ou parar e excluir totalmente a varredura. Os usuários podem também editar os modelos de varreduras.

Quando for concluída por qualquer motivo, a varredura será retirada da lista "**Scans**" e estará disponível para revisão na guia "**Reports**" (Relatórios).

Se uma varredura estiver designada como "Scheduled" (Programada), uma opção será exibida para definir o horário de início desejado e a frequência:

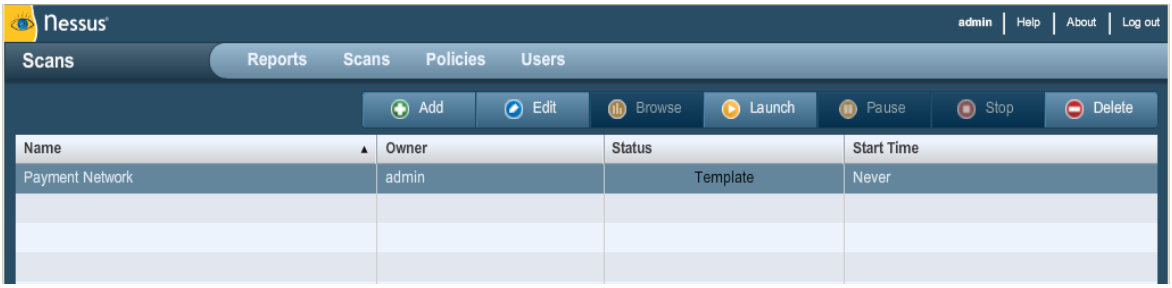


No menu suspenso "Repeats" (Repetições), a varredura pode ser programada para ser executada uma única vez, diariamente, semanalmente, mensalmente ou anualmente. Essa opção também pode ser especificada para iniciar em uma data e horário específicos. Ao salvar a varredura, o Nessus iniciará a varredura no horário especificado.



As varreduras são iniciadas com base no horário definido no servidor do scanner Nessus.

Se uma varredura for salva como um modelo, aparecerá na lista de varreduras dessa maneira e aguardará para ser iniciada.



As varreduras programadas estão disponíveis apenas para os clientes do ProfessionalFeed.

RELATÓRIOS

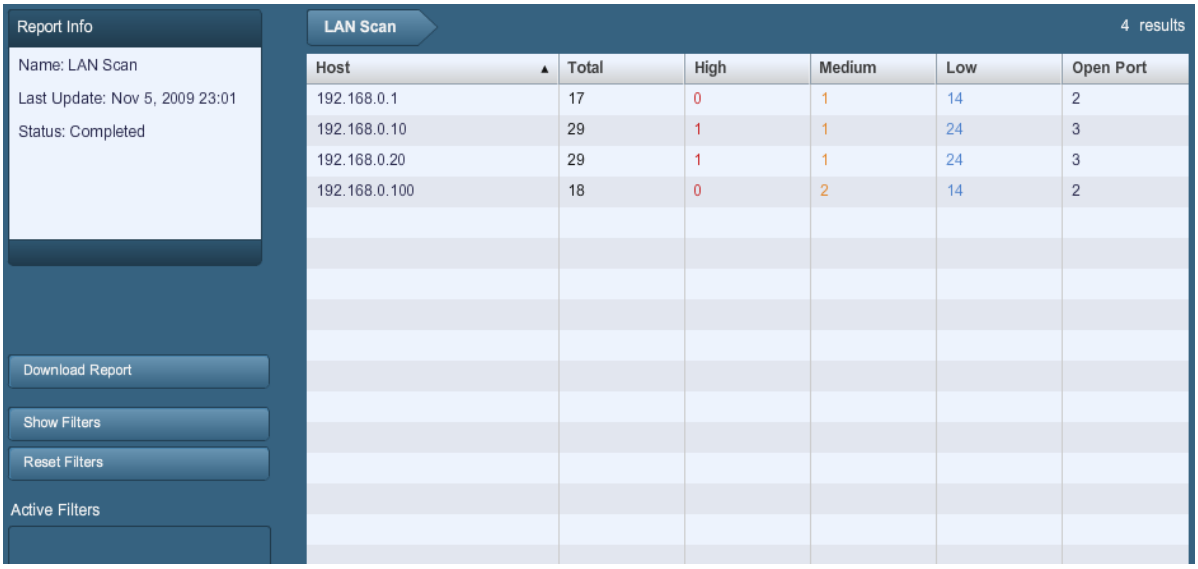
Com o lançamento do Nessus 4.2, as folhas de estilo de relatórios estão integradas ao sistema de emissão de relatórios. Com o uso de filtros de relatório e os recursos de exportação, os usuários podem criar relatórios dinâmicos à sua própria escolha em vez de selecioná-los em uma lista específica. Além disso, o suporte para folhas de estilo foi aprimorado para que as atualizações ou a inclusão de uma folha de estilo sejam realizadas por meio de feeds de plugins. Isto permitirá que Tenable distribua mais folhas de estilo sem a necessidade de uma atualização ou nova versão principal.

Ao clicar no guia "**Reports**" (Relatórios) na barra de menus superior da interface, a lista de varreduras em execução e concluídas será exibida:

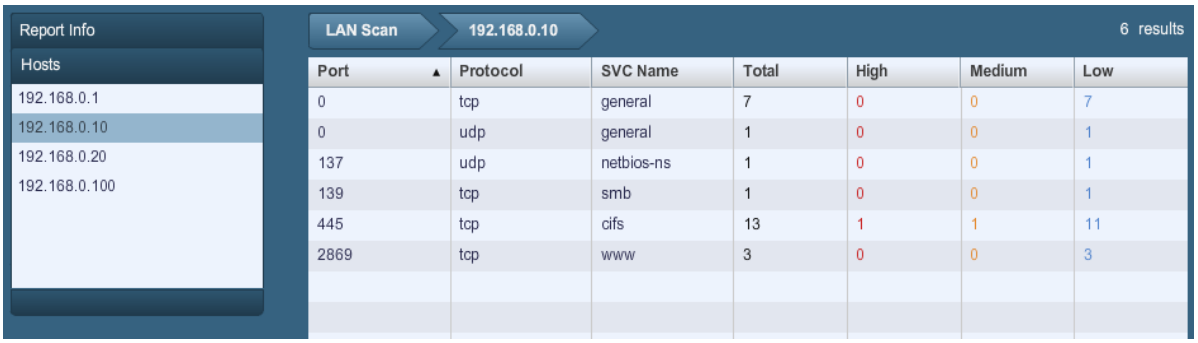
A tela "Reports" (Relatórios) funciona como um ponto central para exibir, comparar, enviar e baixar resultados de varreduras. Use a tecla "Shift" ou "Ctrl" para selecionar vários relatórios de uma só vez.

Browse (Procurar)

Para pesquisar os resultados de uma varredura, selecione um nome na lista "Reports" e clique em "**Browse**". Isto permite exibir os resultados ao navegar pelos hosts, portas e vulnerabilidades específicas. A primeira tela de resumo mostra cada host examinado, junto com uma análise de vulnerabilidades e portas abertas:



Ao selecionar um host, o relatório será subdividido por número de porta e exibirá informações associadas, como o protocolo e o nome do serviço, além de um resumo das vulnerabilidades categorizado pela gravidade do risco. Ao navegar pelos resultados da varredura, a interface de usuário manterá a lista de hosts e uma série de setas clicáveis para auxiliar na navegação rápida até um componente específico do relatório:



Selecione uma porta para exibir todos os resultados de vulnerabilidade associados à porta e ao serviço:

LAN Scan › 192.168.0.10 › 445 / tcp — List | Detail — 13 results

Plugin ID	Name	Port	Severity
11011	SMB Detection	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

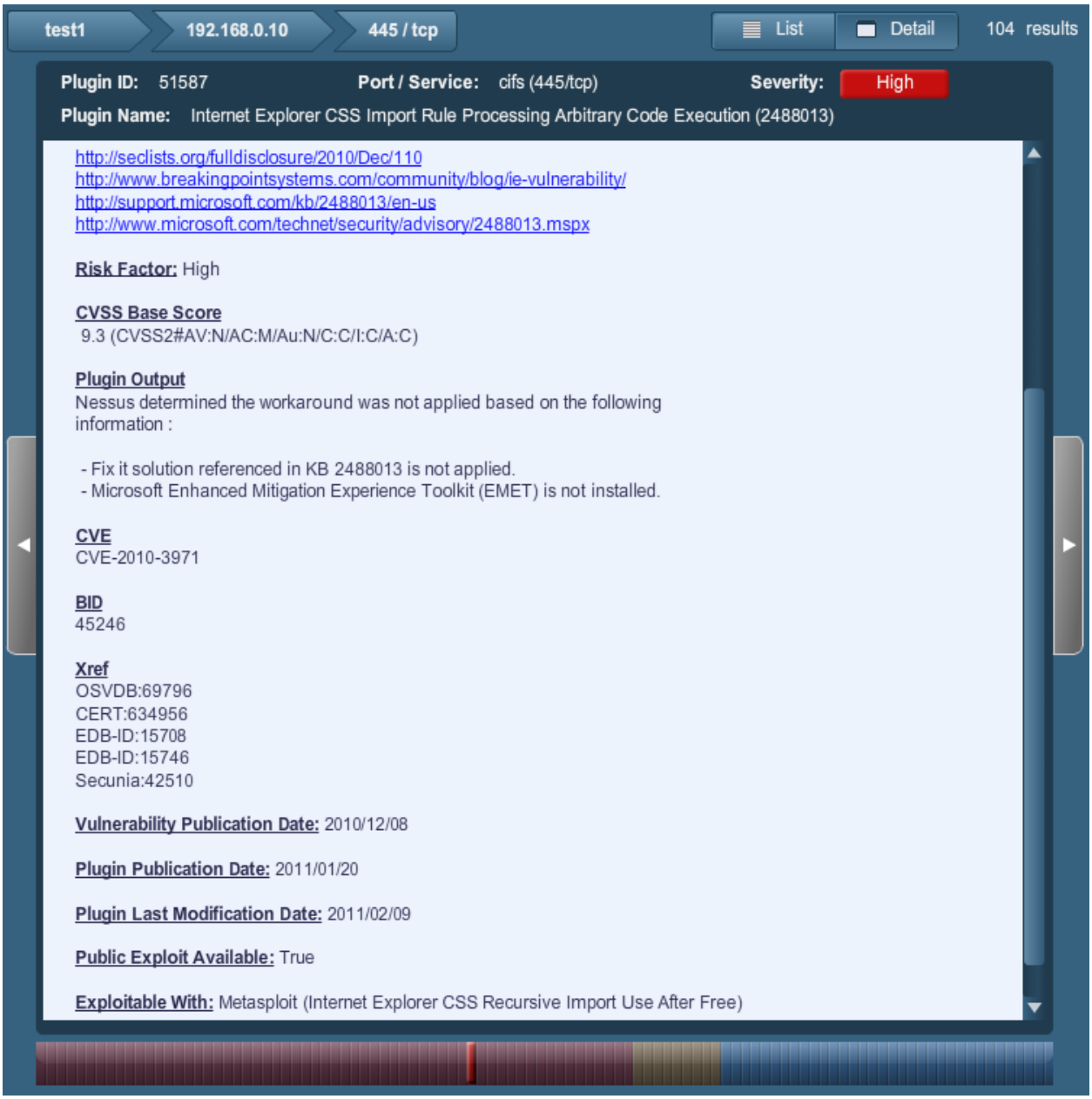
No exemplo acima, vemos que o host 192.168.0.10 tem 13 vulnerabilidades associadas à porta TCP 445 (CIFS ou Sistema Comum de Arquivos da Internet). O resumo das conclusões exibe o ID do plugin Nessus, o nome da vulnerabilidade, a porta, o protocolo e a gravidade. Ao clicar uma vez em qualquer título de coluna, os resultados podem ser classificados pelo conteúdo da coluna. Um segundo clique inverte a classificação dos resultados:

LAN Scan › 192.168.0.10 › 445 / tcp — List | Detail — 13 results

Plugin ID	Name	Port	Severity ▾
10396	Microsoft Windows SMB Shares Access	cifs (445/tcp)	High
26919	SMB guest account for all users	cifs (445/tcp)	Medium
10397	SMB LanMan Pipe Server browse listing	cifs (445/tcp)	Low
10859	SMB get host SID	cifs (445/tcp)	Low
10860	SMB use host SID to enumerate local users	cifs (445/tcp)	Low
10395	SMB shares enumeration	cifs (445/tcp)	Low
11011	SMB Detection	cifs (445/tcp)	Low
10394	SMB log in	cifs (445/tcp)	Low
10785	SMB NativeLanMan	cifs (445/tcp)	Low
23974	SMB Share Hosting Office Files	cifs (445/tcp)	Low
10400	SMB accessible registry	cifs (445/tcp)	Low
10428	SMB fully accessible registry	cifs (445/tcp)	Low
26920	SMB NULL session	cifs (445/tcp)	Low

Selecione uma vulnerabilidade na lista para exibir todos os detalhes da conclusão, incluindo uma sinopse, uma descrição técnica, a solução, o fator de risco, a pontuação CVSS,

resultados relevantes que demonstram a conclusão, referências externas, data de publicação da vulnerabilidade, data de publicação/modificação do plugin e disponibilidade da exploração:



A disponibilidade da exploração exibirá todas as explorações publicamente conhecidas da vulnerabilidade, incluindo as encontradas em estruturas de vulnerabilidade (públicas ou comerciais), como Canvas, Core ou Metasploit.

A tela de detalhes da vulnerabilidade exibe vários métodos para navegar pelo relatório:

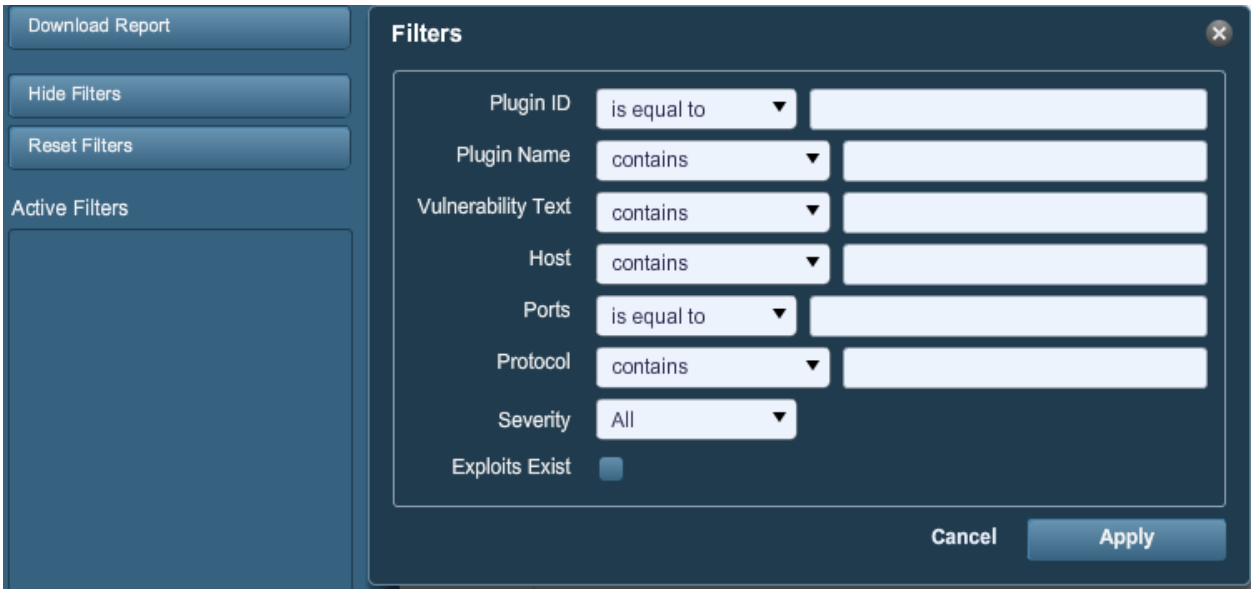
- As teclas de seta superiores podem ser selecionadas para tornar a uma porta, host ou descrição da varredura.

- Os botões "**List**" e "**Detail**" alternam entre os detalhes da vulnerabilidade e a última exibição da lista (no exemplo acima, as vulnerabilidades associadas à porta 445).
- As setas de cor cinza à esquerda ou à direita percorrem as outras vulnerabilidades associadas à porta selecionada.
- A barra de botões na parte inferior permite saltar até uma vulnerabilidade específica na lista de acordo com a gravidade do risco. No exemplo acima, as vulnerabilidades de médio e alto risco se destacam.

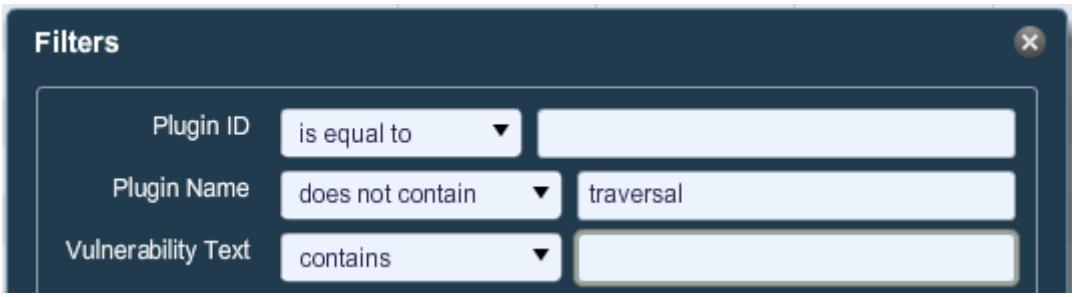
Filtros de relatórios

A Nessus oferece um sistema de filtros flexível para auxiliar na exibição de resultados específicos do relatório. Os filtros podem ser usados para exibir os resultados de acordo com qualquer aspecto dos resultados de vulnerabilidades. Quando vários filtros forem usados, é possível criar exibições mais detalhadas e personalizadas dos relatórios.

Para criar um filtro, clique primeiro em "**Show Filters**" (Exibir filtros) no lado esquerdo da tela. Os filtros podem ser criados pelas telas de resumo de relatório, host ou subdivisão em nível de porta.



Um filtro é criado ao selecionar o campo, argumento de filtro e um valor de filtragem:



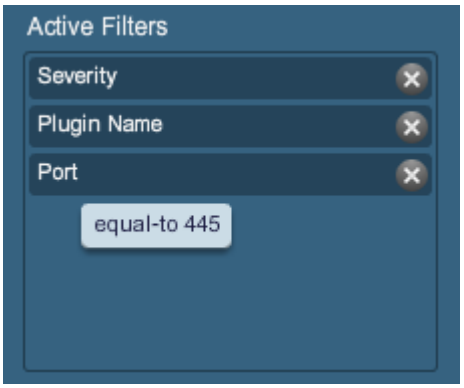
Os filtros de relatório aceitam uma grande variedade de critérios:

Opção	Descrição
ID do plugin	Filtra os resultados se o ID do plugin for igual a ("*is equal to*") ou diferente de ("*is not equal to*") um determinado número (por exemplo: 42111).
Nome do plugin	Filtra os resultados se o nome do plugin contiver ("*contains*"), não contiver ("*does not contain*"), começar com ("*starts with*") ou não começar com ("*does not start with*") uma determinada sequência (por exemplo: "Microsoft Windows").
Vulnerability Text	Filtra os resultados se a saída do plugin contiver ("*contains*"), não contiver ("*does not contain*"), começar com ("*starts with*") ou não começar com ("*does not start with*") uma determinada sequência (por exemplo: "denial of service").
Host	Filtra os resultados se o host do plugin contiver ("*contains*"), não contiver ("*does not contain*"), começar com ("*starts with*") ou não começar com ("*does not start with*"), for igual a ("*is equal to*") ou for diferente de ("*is not equal to*") um determinado string (por exemplo: 192.168).
Ports	Filtra os resultados se a porta for igual a ("*is equal to*") ou diferente de ("*is not equal to*") um determinado número (por exemplo: 443).
Protocol	Filtra os resultados se o protocolo contiver ("*contains*"), não contiver ("*does not contain*"), começar com ("*starts with*") ou não começar com ("*does not start with*") um determinado string (por exemplo: "http").
Severity	Filtra os resultados com base na gravidade de risco: Baixa ("*Low*"), Média ("*Medium*"), Alta ("*High*") ou Grave ("*Critical*").  As classificações de gravidade são derivadas da respectiva pontuação CVSS, em que o valor inferior a 5 é "baixo", inferior a 7 é "médio", inferior a 10 é "alto" e uma pontuação CVSS de 10 será indicada como "Grave".
Exploits Exist	Filtro que detecta se a vulnerabilidade tem uma exploração pública conhecida.

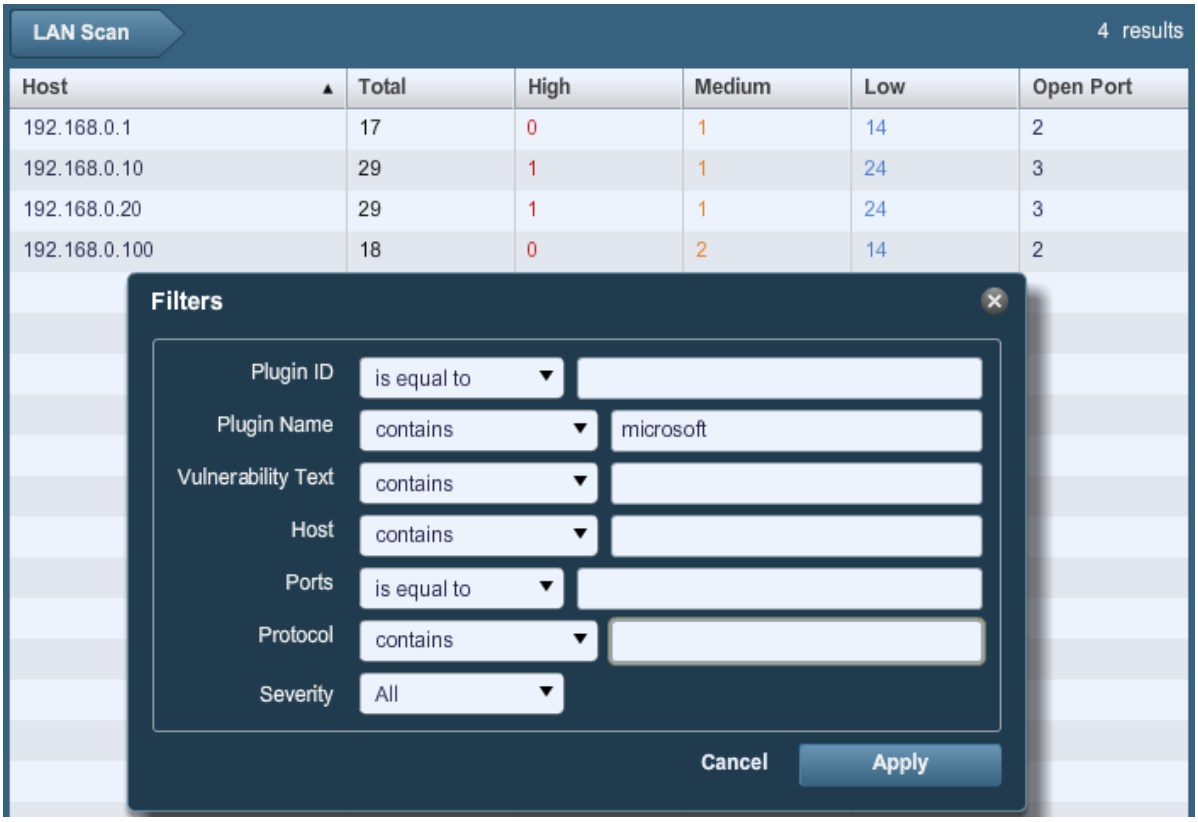
Quando um filtro é usado, é possível delimitar o string ou o valor numérico por vírgulas para filtrar com base em vários strings. Por exemplo: para filtrar os resultados de maneira a exibir apenas os servidores Web, é preciso criar um filtro "Ports", selecionar "is equal to" e inserir "80,443,8000,8080". Isto exibirá os resultados associados a essas quatro portas.

 Os critérios de filtragem **não** distinguem maiúsculas e minúsculas.

À medida que os filtros são criados, são listados no lado esquerdo. Para visualizar os detalhes dos filtros ativos, passe o mouse sobre o nome de cada filtro:



Quando um filtro é criado, os resultados da varredura são atualizados para refletir os novos critérios de filtragem. No exemplo abaixo, a criação de um filtro para exibir apenas os resultados com "Microsoft" no nome do plugin excluirá a maioria dos resultados:



Depois da aplicação do filtro:

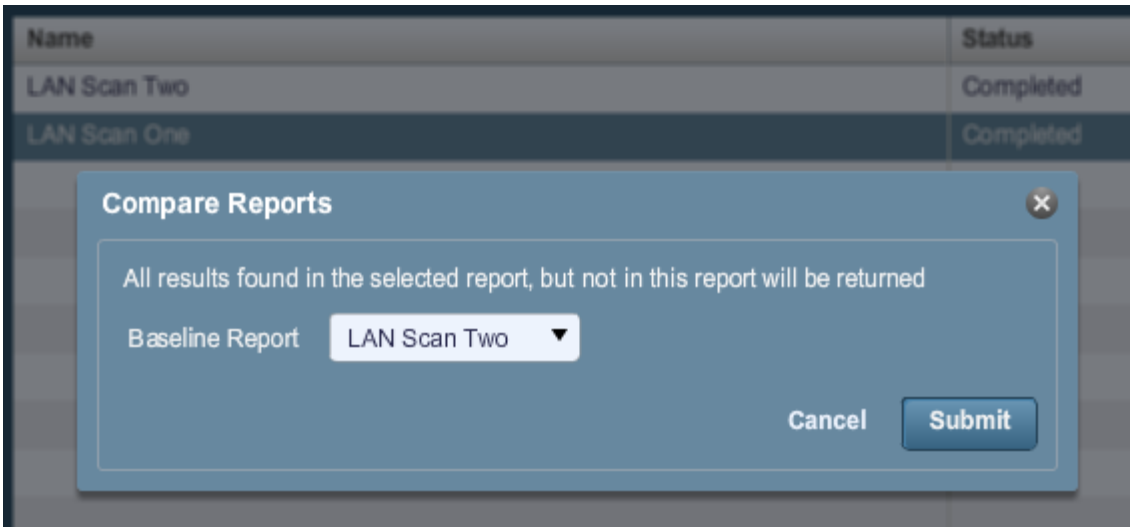
Depois que os resultados forem filtrados para gerar o conjunto de dados desejado, clique em "**Download Report**" para exportar apenas os resultados filtrados.

Compare (Comparar)

A função "Compare" está disponível apenas para os usuários do ProfessionalFeed.

Com o Nessus 4.4, é possível comparar dois relatórios de varredura para exibir as diferenças. A capacidade de exibir as diferenças de varredura ajuda a indicar as mudanças de um determinado sistema ou rede ao longo do tempo. Isto permite analisar a conformidade ao mostrar como as vulnerabilidades são corrigidas, se os sistemas recebem correções à medida que novas vulnerabilidades são encontradas ou se duas varreduras estão direcionadas aos mesmos hosts.

Para comparar relatórios, selecione um varredura na lista "**Reports**" e clique em "**Compare**" na barra de menus à direita. O menu de diálogo resultante exibirá uma lista suspensa de outros relatórios para comparar. Selecione um e clique em "**Submit**" (Enviar):

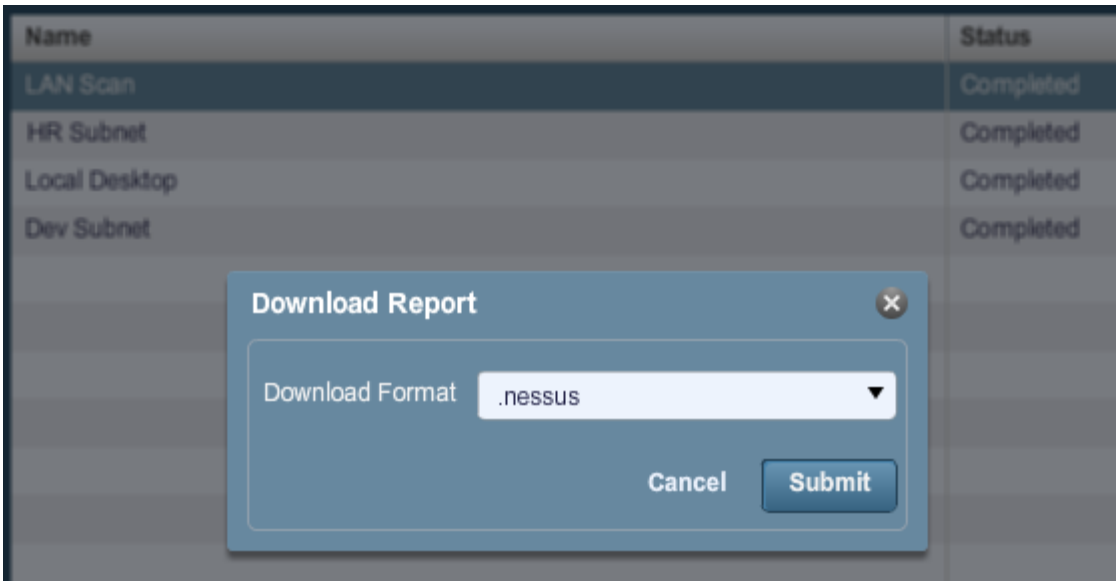


O Nessus irá comparar os dois relatórios e produzir uma lista dos resultados não encontrados em ambos os relatórios. Esses resultados são o diferencial da varredura e destacam as vulnerabilidades descobertas ou corrigidas entre as duas varreduras. No exemplo acima, "LAN Scan One" é um varredura de toda a sub-rede 192.168.0.0/24 e "LAN Scan Two" é uma varredura de três hosts selecionados na sub-rede 192.168.0.0/24. O recurso "Compare" exibe as diferenças e realça os hosts que não foram verificados na "LAN Scan Two":

Upload e download

Os resultados das varreduras podem ser exportados de scanner e importados para um scanner diferente. Os recursos "**Upload**" e "**Download**" facilitam o gerenciamento das varreduras, comparação de relatórios, backup de relatórios e a comunicação entre grupos ou organizações em uma empresa.

Para exportar uma varredura, selecione-a na tela "**Reports**" e clique em "**Download**". Isto exibirá a caixa de diálogo de download de relatórios:

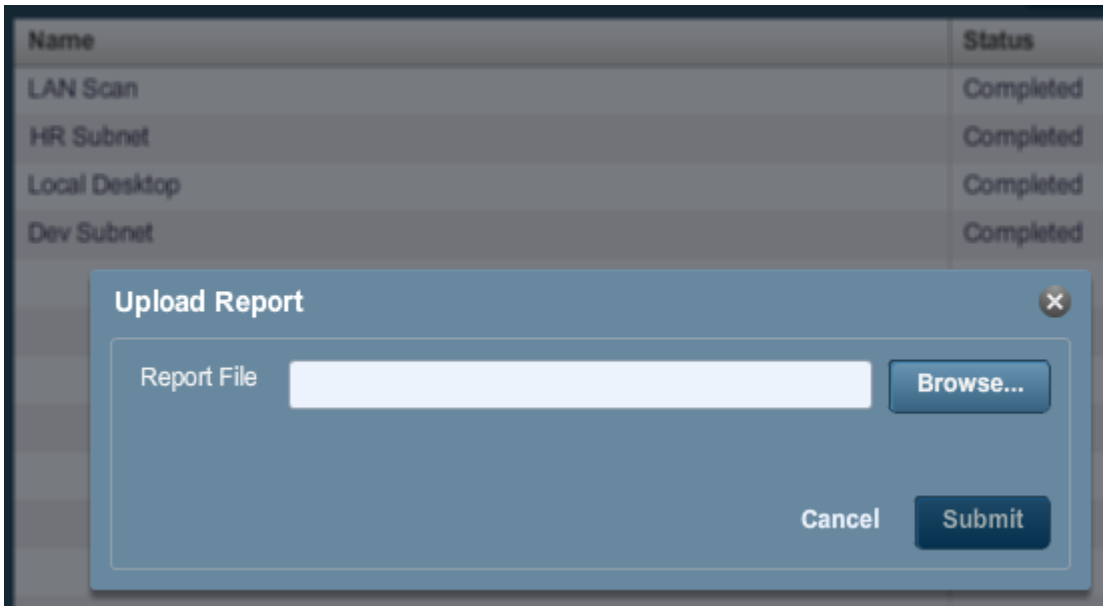


Os relatórios podem ser baixados em qualquer um dos quatro formatos a seguir:

Opção	Descrição
`.nessus`	Um formato do tipo XML, padrão do Nessus 4.2 e versões posteriores. Este formato usa um conjunto extenso de tags XML, que tornam a extração e a análise de informações mais granular.
`.nessus` **(v1)**	Um formato do tipo XML usado do Nessus 3.2 ao 4.0.2, compatível com o Nessus 4.x e Security Center 3.
Detailed HTML Report (by finding)	Um relatório comum gerado em HTML, que pode ser visualizado em qualquer navegador discriminado por vulnerabilidade (Nessus Plugin ID).
Detailed RTF Report (by finding)	Um relatório gerado no formato Rich Text (RTF).
Executive HTML export (top 10 most vulnerable hosts)	Um relatório com gerado em HTML, que contém apenas os 10 hosts com mais vulnerabilidades.
HTML export	Um relatório com gerado em HTML discriminado por host.
NBE export	Exportação delimitada por barras verticais, que pode ser usada para importação em muitos programas externos.

Depois de selecionar o formato `.nessus` ou NBE, a caixa de diálogo "Save File" (Salvar Arquivo) do navegador será exibida, permitindo que o usuário salve os resultados da varredura no local de sua escolha. Os relatórios em HTML são exibidos no navegador e podem ser salvos com a função "File -> Save" ("Arquivo > Salvar").

Para importar uma varredura, clique no botão "**Upload**" na tela "**Reports**":



Com o botão "**Browse...**" (Procurar), selecione o arquivo de varredura `.nessus` que deseja importar e clique em "**Submit**" (Enviar). O Nessus analisará as informações e as disponibilizará na interface "**Reports**".

Formato de arquivo .nessus

O Nessus usa um formato de arquivo específico (`.nessus`) para importar e exportar varreduras. Este formato tem as seguintes vantagens:

- É um arquivo do tipo XML compatível com versões anteriores e futuras e facilita a implementação.
- Autossuficiente: um único arquivo `.nessus` contém a lista de alvos e as políticas definidas pelo usuário, além dos próprios resultados da varredura.
- Seguro: as senhas não são salvas no arquivo. Em vez disso, usa-se uma referência a uma senha armazenada em um local seguro no host local.

O processo de criação de um arquivo `.nessus` que contém os alvos, as políticas e os resultados das varreduras é, primeiramente, gerar a política e salvá-la. Em seguida, gerar a lista de endereços de destino e, por último, executar uma varredura. Quando a varredura for concluída, todas as informações podem ser salvas em um arquivo `.nessus` com a opção "**Download**" da guia "**Reports**". Consulte o documento "Formato de Arquivo Nessus" para obter mais detalhes sobre os arquivos `.nessus`.

Delete (Excluir)

Quando os resultados da varredura forem concluídos, selecione um varredura na lista "Reports" e clique no botão "**Delete**" (Excluir). Isto excluirá a varredura da interface de usuário. **Essa ação não pode ser desfeita**. Use o recurso "**Download**" para exportar os resultados de varredura antes da exclusão.

USERS (USUÁRIOS)

A guia "**Users**" (Usuários) oferece uma interface para gerenciar os usuários do scanner Nessus. Os novos usuários podem ser incluídos por meio do Nessus Server Manager (Mac OS X/Windows), comando **`nessus-adduser`** (*nix) ou interface de usuário (todas as plataformas). Para criar um novo usuário por meio da interface de usuário do Nessus, clique em "**Add**" no menu superior direito. Serão solicitados o nome de usuário, a senha e a opção de tornar o usuário um administrador do scanner Nessus:

Para editar ou excluir um usuário, selecione o nome de usuário na lista "**Users**" e clique em "**Edit**" ou "**Delete**" no menu superior direito, conforme o necessário.

OUTROS CLIENTES NESSUS

Além da interface de usuário do Nessus, a Tenable oferece suporte para dois métodos adicionais de comunicação com o servidor Nessus: a interface de linha de comando e o SecurityCenter.

INTERFACE DE LINHA DE COMANDO

A interface de linha de comando (CLI) está disponível no servidor Nessus. Para executar uma varredura com a operação de linha de comando, execute a varredura no modo de lote com a seguinte sintaxe:

Sistema operacional	Comando
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`
FreeBSD	`# /usr/local/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>`

Max OS X	**# /Library/Nessus/run/bin/nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>**
Windows	**%programfiles%\Tenable\Nessus\nessus -q [-pPS] <host> <port> <user> <password> <targets-file> <result-file>**

A tabela a seguir descreve os vários argumentos usados para executar uma varredura no modo de lote.

Argumento	Descrição
-q	Modo de lote. Executa a varredura do Nessus de maneira não interativa.
-p	Obtém uma lista dos plugins instalados no servidor.
-p	Obtém uma lista das preferências do servidor e do plugin.
-s	Gera a saída SQL para **-p** e **-P**.
<host>	O host **nessusd** ao qual se conecta.
<port>	A porta à qual o usuário se conectará no host **nessusd** remoto.
<user>	O nome de usuário ao qual o **nessusd** se conecta.
<password>	A senha associada ao nome do usuário.
<targets-file>	O nome do arquivo que contém os computadores submetidas à varredura.
<results-file>	O nome do arquivo no qual os resultados serão armazenados ao término da varredura.

Outras opções também estão disponíveis para executar uma varredura no modo de lote. As opções são descritas na tabela a seguir.

Opção	Descrição
-V	Faz com que o modo de lote exiba mensagens de estado na tela.
-x	Não verifica os certificados SSL.
-v	Versão. Exibe o número da versão e desconecta.

`-h`	Ajuda. Mostra o resumo dos comandos e desconecta.
`-T <type>`	Salva os dados como <tipo>, onde <tipo> pode ser "nbe", "html", "nessus" ou "text".

Como converter um relatório

É possível usar se o Nessus para realizar uma conversão entre formatos de relatórios. O Nessus pode usar qualquer relatório NBE e transformá-lo no formato HTML, texto ou `.nessus`.

Use os comandos a seguir para converter um relatório:

Sistema operacional	Comando
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
FreeBSD	`# /usr/local/nessus/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
Max OS X	`# /Library/Nessus/run/bin/nessus -i in.nbe -o out.[html|txt|nessus]`
Windows	`%programfiles%\Tenable\Nessus\nessus -i in.nbe -o out.[html|txt|nessus]`

A opção `-i` especifica o arquivo NBE que está sendo convertido. A opção `-o` especifica o nome do arquivo e tipo no qual o relatório será convertido, que pode ser texto, HTML ou o formato `.nessus`.

Os relatórios contidos nos arquivos `.nessus` também podem ser convertidos em HTML pela linha de comando. A sintaxe é a seguinte:

O arquivo `.nessus` deve ser salvo no formato de download "nessus (v1)" para que a conversão em HTML funcione.

Sistema operacional	Comando
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
FreeBSD	`# /usr/local/nessus/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
Max OS X	`# /Library/Nessus/run/bin/nessus --dot-nessus in.nessus -i <ReportName> -o out.html`
Windows	`%programfiles%\Tenable\Nessus\nessus --dot-nessus in.nessus -i <ReportName> -o out.html`

O parâmetro **--dot-nessus** indica que o arquivo de entrada **.nessus** deve ser usado. <ReportName> é o nome do relatório da maneira como aparece no arquivo de entrada **.nessus**.

Linha de comando com arquivos .nessus

Vários argumentos podem ser transmitidos para permitir o trabalho com os arquivos **.nessus**, seja como entrada ou saída, pela linha de comando. Os argumentos são descritos na tabela a seguir.

Argumento	Descrição
--dot-nessus <file>	Quando usado, é sempre fornecido como o primeiro parâmetro transmitido ao binário do **nessus** para indicar que um arquivo **.nessus** será usado. <arquivo> é o local e o nome do arquivo **.nessus** que será usado.
--policy-name <policy>	Nome da política contida no arquivo **.nessus** designado. O parâmetro de política é fornecido no início de uma varredura pela linha de comando. Observe que o nome da política indicado deve ser exatamente o nome da política, incluindo as aspas simples, exibido quando o parâmetro "**--list-policies**" for usado (veja exemplo a seguir).
--list-policies	Fornece os nomes de todas as políticas de varredura contidas no arquivo **.nessus** designado.
--list-reports	Fornece os nomes de todos os relatórios contidos no arquivo **.nessus** designado.
--target-file <file>	Substitui os alvos indicados no arquivo **.nessus** designado e usa os alvos contidos no arquivo especificado.

O comando a seguir exibirá uma lista de todos os relatórios contidos no arquivo "**scan.nessus**":

O arquivo **.nessus** deve ser salvo no formato de download "nessus (v1)" para que o parâmetro **--list-reports** se alterne para o modo ativo.

Sistema operacional	Comando
Linux, Solaris, Enterasys	**# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-reports**
FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-reports**
Max OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-reports**
Windows	**%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-reports**

Veja a seguir um exemplo de resultado:

```
List of reports contained in scan.nessus:
- '08/03/10 11:19:55 AM - Full Safe w/ Compliance'
- '08/03/10 01:01:01 PM - Full Safe w/ Compliance'
- '08/03/10 01:32:10 PM - Full Safe w/ Compliance'
- '08/03/10 02:13:01 PM - Full Safe w/ Compliance'
- '08/03/10 02:45:00 PM - Full Safe w/ Compliance'
```

O comando a seguir exibirá uma lista de todas as políticas contidas no arquivo "**scan.nessus**":

O arquivo **.nessus** deve ser salvo no formato de download "nessus (v1)" para que o parâmetro **--list-policies** se alterne para o modo ativo.

Sistema operacional	Comando
Linux, Solaris, Enterasys	**# /opt/nessus/bin/nessus --dot-nessus scan.nessus --list-policies**
FreeBSD	**# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --list-policies**
Max OS X	**# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --list-policies**
Windows	**%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --list-policies**

Um exemplo do resultado deste comando é apresentado a seguir:

```
List of policies contained in scan.nessus:
- 'Full Safe w/ Compliance'
```

Observe que, quando os nomes de relatórios ou políticas forem transmitidos como parâmetros ao Nessus pela linha de comando, o nome deve ser transmitido exatamente como exibido nos comandos acima, incluindo as aspas simples (`'Safe w/ Compliance'`).

Comando Scan

Considerando a existência de uma política com a indicada no exemplo acima, uma varredura pode ser iniciada com as seguintes configurações:

O arquivo **.nessus** especificado na varredura deve estar no formato "nessus (v1)" para que a varredura seja processada.

Sistema operacional	Comando
Linux, Solaris, Enterasys	`# /opt/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>`
FreeBSD	`# /usr/local/nessus/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>`
Max OS X	`# /Library/Nessus/run/bin/nessus --dot-nessus scan.nessus --policy-name 'Full Safe w/ Compliance' <host> <port> <user> <password> <results-file>`
Windows	`%programfiles%\Tenable\Nessus\nessus --dot-nessus scan.nessus --policy-name "Full Safe w/Compliance" <host> <port> <user> <password> <results-file>`

No exemplo acima, os parâmetros **<host>**, **<port>**, **<user>**, **<password>** e **<results-file>**são indicados da maneira documentada acima. Não é necessário um arquivo <targets-file>, pois os alvos contidos no arquivo **.nessus** são usados na varredura.

O formato do relatório gerado será decidido com base na extensão do arquivo fornecida no comando **nessus** . No comando acima, se o nome indicado para o parâmetro <results-file> for "**report.nbe**", o relatório será gerado no formato **.nbe**. Se o nome for "**report.nessus**", o relatório será gerado no formato **.nessus**.

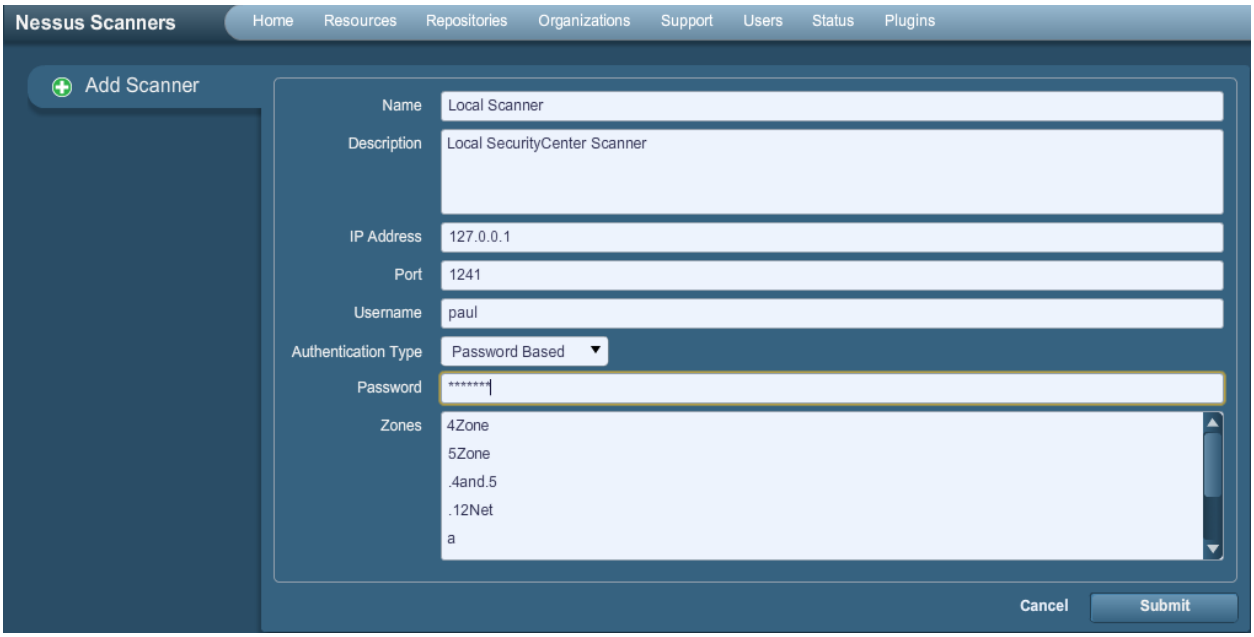
Se nada foi indicado no parâmetro <results-file>, o relatório será incluído no arquivo **scan.nessus**.

SECURITYCENTER

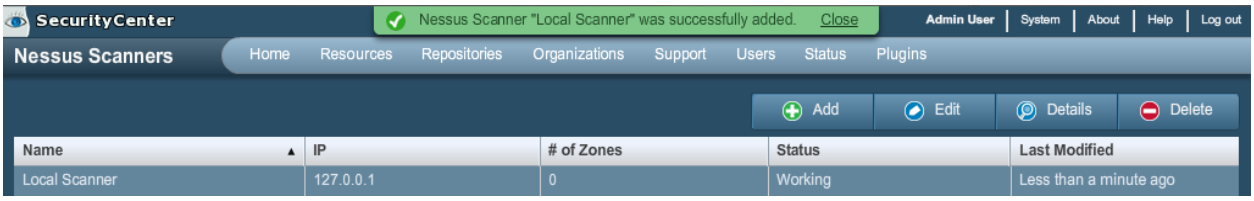
Configuração do SecurityCenter

O "Nessus Server" pode ser adicionado por meio da interface de administração do SecurityCenter. A interface o SecurityCenter pode ser configurada para acessar e controlar praticamente qualquer scanner Nessus. Clique na guia "Resources" (Recursos) e, em seguida, clique em "**Nessus Scanners**". Clique em "**Add**" (Adicionar) para abrir o diálogo "Add Scanner" (Adicionar Scanner). O endereço IP do scanner Nessus, a porta do Nessus (padrão: 1241), o ID de login administrativo, o tipo de autenticação e a senha (criada durante a configuração do Nessus) são obrigatórios. Os campos de senha não estarão disponíveis se a autenticação "SSL Certificate" (Certificado SSL) for selecionada. Além disso, as zonas às quais o scanner Nessus será atribuído podem ser selecionadas.

Um exemplo de imagem da página "Add Scanner" do SecurityCenter é mostrado abaixo:



Depois de adicionar com êxito o scanner, a seguinte página é exibida após a seleção do scanner:



Consulte mais informações no "Guia de Administração do SecurityCenter".

PARA OBTER MAIS INFORMAÇÕES

A Tenable possui vários documentos que descrevem a instalação, implementação, configuração, operação do usuário e testes gerais do Nessus. O documentos estão listados a seguir:

- **Guia de Instalação do Nessus** – instruções passo a passo da instalação.
- **Verificações de Credenciais do Nessus para Unix e Windows** – informações sobre como realizar varreduras autenticadas de rede com o scanner de vulnerabilidades Nessus,
- **Verificações de Conformidade do Nessus** – guia geral para compreender e executar verificações de conformidade com o Nessus e o SecurityCenter.
- **Referência de Verificações de Conformidade do Nessus** – guia completo da sintaxe das verificações de conformidade do Nessus.
- **Formato de arquivo Nessus v2** – descreve a estrutura do formato de arquivo `.nessus`, que foi introduzido com o Nessus 3.2 e NessusClient 3.2.
- **Especificação do protocolo Nessus XML-RPC** – descreve o protocolo e a interface XML-RPC do Nessus.

- **Monitoramento de Conformidade em Tempo Real** – descreve como as soluções da Tenable podem ser usadas para ajuda a cumprir muitos tipos diferentes de normas do governo e do setor financeiro.

Entre em contato conosco pelo e-mail support@tenable.com, sales@tenable.com ou visite nosso site no endereço http://www.tenable.com/.

SOBRE A TENABLE NETWORK SECURITY

Tenable Network Security, líder em monitoramento unificado de segurança, é a criadora do scanner de vulnerabilidades Nessus e de soluções de primeira classe sem agente para o monitoramento contínuo de vulnerabilidades, pontos fracos de configuração, vazamento de dados, gerenciamento de logs e detecção de comprometimentos para ajudar a garantir a segurança da rede e o cumprimento das leis e normas FDCC, FISMA, SANS, CAG e PCI. Os produtos premiados da Tenable são utilizados por muitas organizações da Global 2000 e por órgãos públicos para tomar a iniciativa de reduzir os riscos nas redes. Para mais informações, visite http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com