Mestrado em Engenharia Informática
Gestão de Sistemas e Redes
Ano Letivo 2016/2017
1º Ano-1º Semestre
Docente: Lina Brito

2º Trabalho Prático – Nessus

Trabalho Elaborado por:
Duarte Costa nº.2084813
José Gouveia nº.2044912
Pedro Mendonça nº.2071213

Sumário

Introdução

No âmbito da disciplina de Gestão de Sistemas de redes foi nos proposto um trabalho de pesquisa, acerca de uma ferramenta de gestão de redes. Tendo em conta as ferramentas distribuídas pela professora, nós decidimos escolher a ferramenta de gestão Nessus por ser uma das mais utilizadas no mercado.

O que é uma rede?

Uma rede é formada por um conjunto de máquinas eletrónicas, capazes de trocar informação, recursos de *hardware* e de *software*, que estão interligados por um sistema de comunicação. A eficácia dos serviços prestados está associada com um bom desempenho da rede.[1]

Em que consiste gerir uma rede?

Gerir uma rede consiste na coordenação (monitorização e controle de atividades) de recursos físicos (modems, routers, etc) e lógicos (protocolos), dispersos na rede, assegurando confiabilidade, segurança e tempos de resposta aceites.

O modelo clássico de gestão de rede pode ser reduzido em três passos. Recolher dados, um processo geralmente automático na monitorização dos recursos geridos. Diagnostico, análise dos dados. Controle, depois de detetado o problema, cabe atuar sobre o recurso em falha.[2]

Em que consiste um sistema de gestão?

Um sistema de gestão consiste num conjunto de ferramentas integradas para o controle e monitorização de uma rede. Oferece uma interface podendo ser, ou não, gráfica que traduz a informação sobre o estado da rede. Pode ainda conter um conjunto de determinados comandos que permitem executar todas as atividades de gestão.

Dispositivos geridos de certa forma contêm objetos geridos, nesses objetos a informação é recolhida "Management Information Base (MIB)".

Gestor e agentes comunicam um com o outro usando um protocolo de gestão SNMP.[2][3]

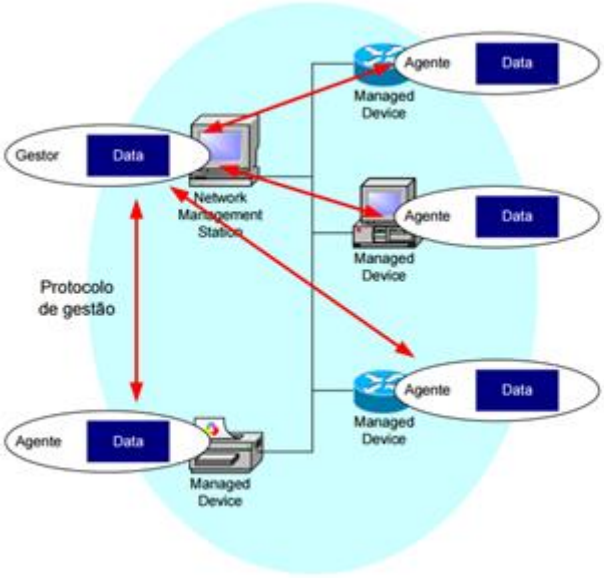

Figura 1 Modelo Gestor-Agente

Objetivos

- Escolher uma ferramenta apropriada, que poderá ser de uma das seguintes categorias:
  - Ferramenta de monitorização e medição automatizadas;
  - Ferramentas de inventário (autodiscovery), de construção de topologia de redes, etc.;
  - Ferramentas para simulação redes, de QoS, etc.;
  - Ferramentas de interação com utilizadores e de suporte a utilizadores.
  - Outro tipo de ferramentas/plataformas de gestão de redes;
- Instalar a ferramenta de gestão de redes.
- Desenvolvimento de um trabalho de pesquisa acerca da ferramenta e executar um cenário de utilização da ferramenta.
- Adquirir um bom conhecimento sobre a ferramenta para depois partilhar com a turma.

Fundamentação teórica

O Nessus é uma ferramenta de gestão de redes que foi desenvolvida pela Tenable Network Security®. É uma ferramenta ligada as vulnerabilidades e monitorização de toda a rede, muito utilizada. Tem como foco principal a segurança da rede, sendo possível identificar as vulnerabilidades em tempo real. Uma dos pontos fortes do Nessus é a tecnologia cliente-servidor, nesta tecnologia os servidores podem ser colocados em pontos estratégicos, podendo a rede ser testada em pontos diferentes. Suporta a tecnologia multiagente.[4]

Existe uma versão do Nessus para uso pessoal, esta versão não tem qualquer tipo de custos para o utilizador, apenas utiliza no máximo de 16 ip's por *Scanner* e as funcionalidades são bastante reduzidas em relação a versão paga.

No caso de ser necessária uma versão mais sofisticada, existe uma versão paga. Esta versão é muito boa, pois, permite o uso de ferramentas como, *Agent-based Scanning, Mobile Device Management Integration.*[5]

Abaixo iremos falar um pouco do Nessus Agent e no Nessus Maneger, contudo não iremos experimentar essas ferramentas, devido a estas representem custos, pois, não estão inseridas nas funcionalidades gratuitas do Nessus.

Nessus Agents

São ferramentas leves e autónomas de diagnóstico de vulnerabilidades. Estas ferramentas podem ser usadas remotamente em qualquer dispositivo mesmo em dispositivos móveis. O agente é capaz de realizar um diagnóstico a rede, estando ou não conectado. A diagnóstico com base em agentes Nessus estão disponíveis para plataformas Windows outras plataformas adjacentes.[6]

Nessus Manager

A mais recente linha de produtos Nessus inclui serviços como, total gestão de serviços e análises, administração centralizada e proporciona uma fácil programação de sondas múltiplas. Com o Nessus Manager é possível agendar análises as vulnerabilidades ao longo de vários dias, para que seja possível garantir que todos os dispositivos são descobertos. Isto permite-nos conseguir uma visão abrangente da rede.[6]

Tipo/Classificação da ferramenta escolhida/Implementação

Nessus é uma ferramenta de gestão que pode ser implementado de forma local ou de forma geograficamente distribuída (Nessus Cloud). Para este trabalho o Nessus será implementado localmente, em redes estipuladas pelo grupo

O Nessus funciona como uma se fosse uma ferramenta de integração, porque podemos realizar diferentes tipos de diagnósticos recorrendo a pequenas ferramentas que fazem parte desta plataforma usando a mesma interface para garantir ao utilizador o mesmo "*look and feel*". Isto releva uma caraterística importante neste tipo de *softwares* que não existir a integração de diferentes bases de dados.

A vantagem desta abordagem é de não gerar custos adicionais na integração das ferramentas, mas por outro lado existe a necessidade de um operador relacionar e interpretar os dados resultantes da utilização das diferentes ferramentas, o que se pode tornar impossível devido à grande quantidade de dados que possam ser gerados por estas ferramentas.

Enquadramento em relação à abordagem de desenvolvimento da ferramenta – isolada, coordenada ou integrada.

O *Nessus* está enquadrado no grupo de ferramentas que estão destinadas a detetar vulnerabilidades na rede. Permite uma abordagem integrada na deteção das vulnerabilidades existentes na rede, porque nós podemos efetuar vários tipos de testes à rede (Basic Network Scan, Malware Scan, Host Discovery, Badlock Detection, etc) usando sempre a mesma interface sem necessidade de usar outros programas.

Com base no modelo FCAPS (Faults, Configurations, Accounting, Performance, Security), esta ferramenta enquadra-se na componente de segurança. A gestão das vulnerabilidades é feita com base nos relatórios gerados pela aplicação, estes relatórios indicam as possíveis razões da ocorrência da falha e a sua solução.

Quanto as falhas o nessus faz um port scan ao computador alvo, depois disso um conjunto de scripts (escritos em NASL, Scripting Language, Nessus Attack) ligam-se a cada porta aberta para verificar problemas de segurança, caso ajam estes são informados ao gestor de rede.[7]

Modelos subjacentes

No que diz a modelo organizacional no Nessus existem duas formas de organização. A primeira consiste no scan de vulnerabilidades em redes locais, e a segunda no scan de vulnerabilidades em redes distribuídas. Na primeira forma, um Nessus Manager ordena o Nessus Scanner a realizar os scans, este realiza os scans a todos os *hosts* como podemos verificar na figura seguinte.

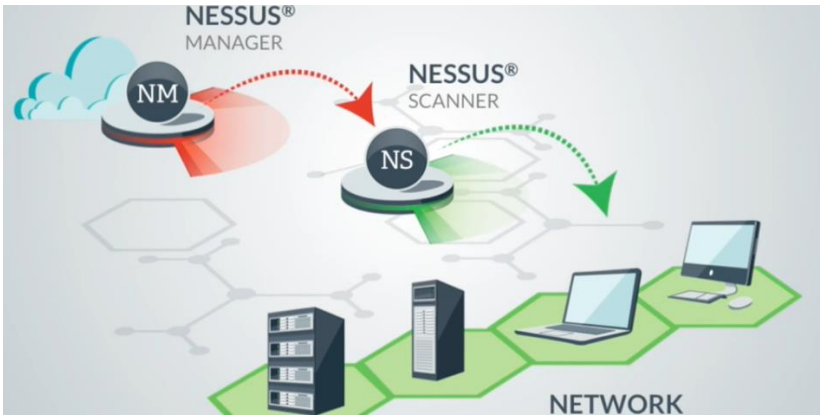

Figura 2 Arquitectura do Nessus para redes locais [8]

Na segunda forma, cada dispositivo tem um Nessus Agent que faz os *scans* e depois envia os resultados para o Nessus Scanner, que reencaminha esses resultados para o Nessus Manager.

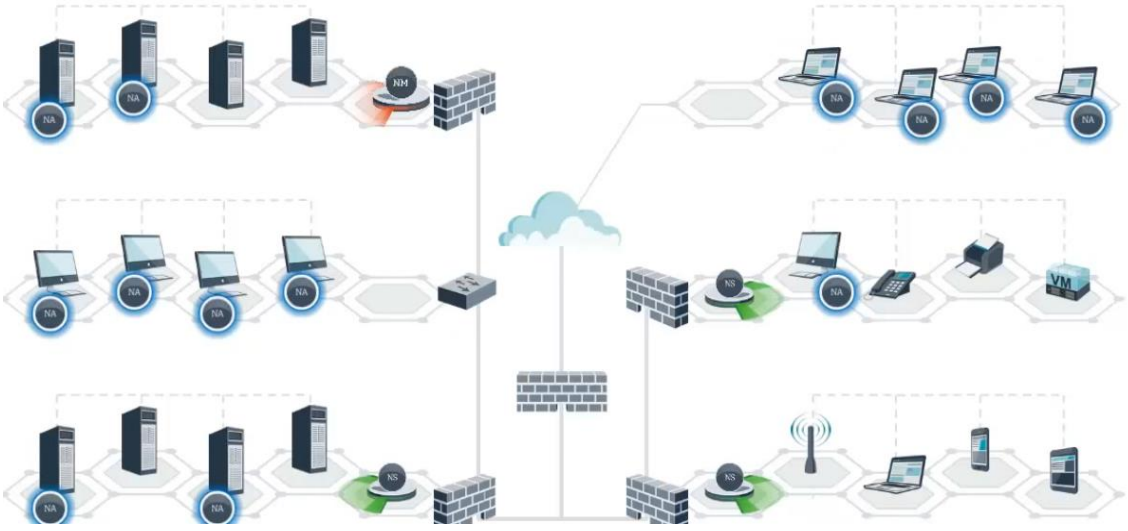

Figura 3 Arquitectura do Nessus para redes distribuídas [9]

No modelo comunicacional a comunicação é estabelecida através uma conexão TCP entre o *Manager* e os *hosts*, em que o *Manager* manda pacotes UDP para os *hosts* e estes respondem através de mensagens ICMP. O grande problema é que não há nenhuma maneira confiável de saber se uma porta está aberta, porque um serviço de escuta baseado em UDP normalmente não responderá a uma sonda e também não responderá se a porta estiver fechada.[8]

Quanto ao modelo funcional já foi abordado no tópico acima.

No que diz respeito ao modelo informacional, não se consegue concluir nada acerca desta ferramenta.

Classificação da ferramenta em termos de estrutura e componentes

O Nessus é uma ferramenta de deteção de vulnerabilidades, tal como já foi referido anteriormente, partilhando algumas caraterísticas com outros sistemas de deteção de vulnerabilidades. Um detetor de vulnerabilidades é constituído por 4 unidades principais, sendo estas: o *Scan Engine,* a *Scan Database* e a interface com o utilizador.

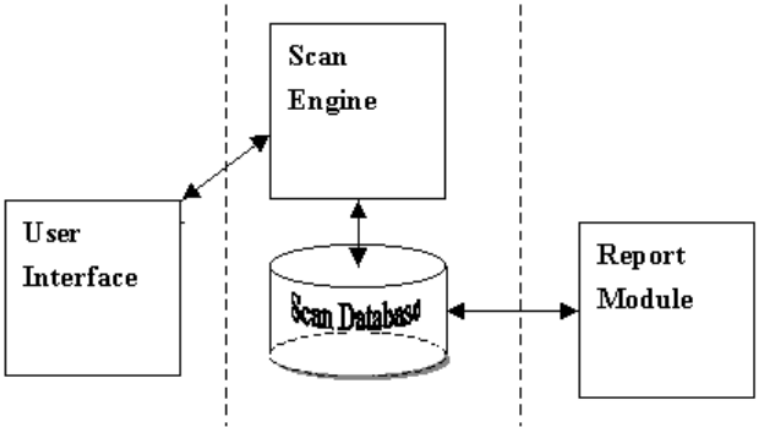

Figura 4 Arquitetura de um detetor de vulnerabilidades

O *Scan Engine*, executa verificações de segurança de acordo com os *plug-ins* (fazem parte da base de dados de conhecimento, *Scan Database,* de vulnerabilidades que o *Scanner* é capaz de detetar) instalados, identificando assim o sistema de informação e as suas vulnerabilidades. Este pode fazer mais do que um *scan* ao mesmo tempo e compara os resultados com resultados de vulnerabilidades já conhecidas pelo sistema.

A *Scan DataBase* guarda toda a informação sobre as vulnerabilidades, os resultados dos *Scans* e outros dados utilizados pelo *Scanner*. A quantidade de *Plug-ins* e a frequência que estes sofrem *updates* varia dependendo de fornecedor para fornecedor. Cada *Plug-in* pode conter não só o caso de teste mas também a descrição das próprias vulnerabilidades. Os *Plug-ins* usam um género de dicionário de nomes comuns, para saber publicamente as vulnerabilidades de segurança, chamado de *Common Vulnerabilities and Exposures (CVE).* Este dicionário permite que possa ser trocada informação entre bases de dados e ferramentas de segurança, isto serve de base para que possamos avaliar a cobertura das ferramentas que são utilizadas. Com um relatório que use identificadores *CVE,* podemos saber rapidamente e de forma precisa a informação necessária para corrigir os possíveis erros que possam surgir.[9]

O *Report Module* fornece vários tipos diferentes de relatórios que possam ser gerados nos resultados dos *scans* realizados pelo detetor de vulnerabilidades tais como relatórios tecnicamente detalhados com as sugestões para corrigir as vulnerabilidades para os administradores de sistema, relatórios de resumo para os gestores de segurança e ainda relatórios de nível mais gráfico para os executivos da instituição.

Por último a Interface com utilizador permite ao administrador operar com o *scanner*, esta interface pode ser gráfica (GUI) ou através de uma linha de comandos.[10]

Cenário de rede utilizado

Cenário 1

Neste cenário decidiu-se criar uma rede local através de um dispositivo móvel, nesta rede foram adicionados 3 computadores e 1 telemóvel.

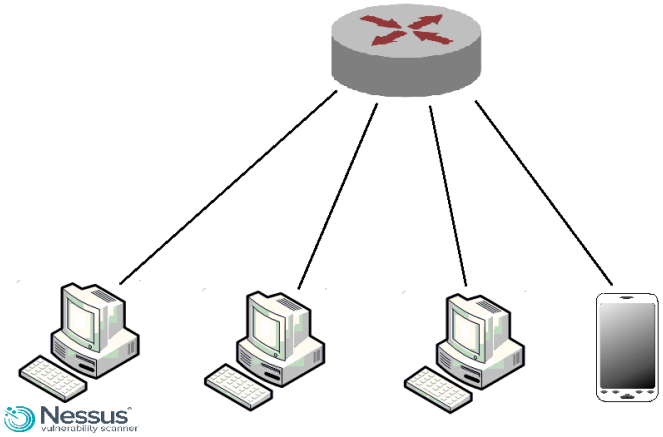

Figura 5 Cenário 1

Cenário 2

Para este cenário decidiu-se criar uma rede local através de um dispositivo móvel e foram adicionados 2 computadores e 2 telemóveis.

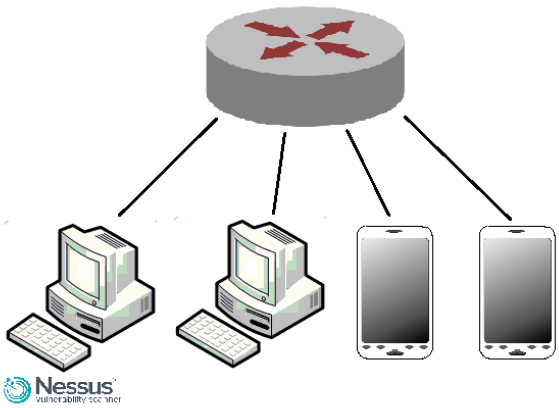

Figura 6 Cenário 2

Cenário 3

Neste cenário foram utilizados todos os *host's* da rede da Universidade da Madeira com o *ip* 10.2.0.0/16.

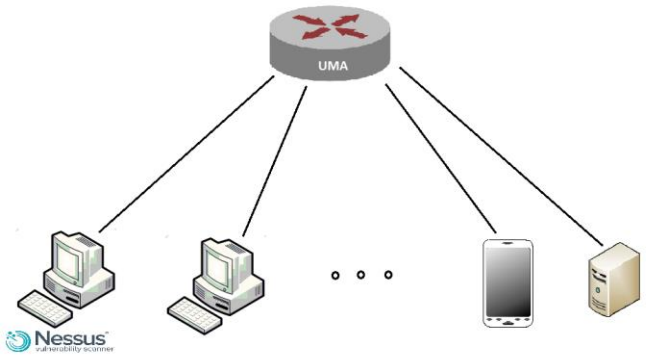

Figura 7 Cenário 3

Descrição da Ferramenta

Requisitos

Para que o Nessus possa ser instalado é necessário que as máquinas tenham de respeitar alguns requisitos mínimos de *hardware*, *software* e de licenciamento, para que este sistema possa correr sem problemas. Em primeiro lugar é recomendado que a máquina onde estamos a correr o sistema tenha as seguintes caraterísticas a nível de hardware.[11]

Cenário	**Mínimo de Hardware recomendado**
Para 50,000 hosts	**CPU:** 1 *dual-core* 2GHz CPU **Memória:** 2GB RAM (4 GB recomendados) **Espaço em disco:** 30 Gb
Para mais de 50,000 hosts	**CPU:** 1 dual-core 2 GHz CPU (2 dual-core recomendado) **Memória:** 2GB RAM(8GB RAM recomendado) **Espaço em Disco:** 30GB (Espaço adicional deve ser acrescentado)

O Nessus também pode ser instalado recorrendo às máquinas virtuais, que devem de seguir os mesmos requisitos do que as máquinas ditas convencionais. Se estivermos a usar uma ligação NAT (*Network Address Translation*) para aceder à rede, muitas dos *Vulnerability checks*, *host enumeration* e o *operating system identification* são negativamente afetados.

O Nessus é suportado por várias distribuições de Linux, Windows e MAC OS X, isto aplica-se ao *Manager* e aos *Agents*. O Nessus pode ser utilizado usando a linha de comandos ou uma interface gráfica recorrendo aos *Browsers* para correr as ferramentas de deteção de falhas, também é necessário instalar o J*ava* antes de o Nessus ser instalado para que possamos obter os relatórios das vulnerabilidades detetadas.[12]

Para podermos algumas funcionalidades deste *software* de deteção de falhas temos de obter uma licença para que o programa saiba que tipo de funcionalidades o utilizador desta plataforma possa aceder. O Nessus faculta-nos dois tipos de licenças, um deles é por subscrição e a outra por *Managed SecurityCenter*, a chave que é atribuída a um utilizador irá identificar qual a versão do Nessus, quantos endereços *ip* podemos identificar, quantos *scanners* remotos e agentes podem ser vinculados ao Nessus Manager[13].

Instalação

Para instalar o Nessus devemos de ir ao *site* oficial e escolher uma versão que se adeque ao sistema operativo onde este irá correr e fazer o *download* da instalação (Ver Ilustração 1)[14].

Figura 8 Download do instalador

O segundo passo é registarmo-nos para obter uma conta para que possamos pedir uma chave de ativação para podermos utilizar o programa em questão. Dá para pedir uma chave para a versão *Home* sem custos para o utilizador mas em contra partida não podemos aceder a todas as funcionalidades e temos também um número máximo de *ip´s* a que podemos fazer *scan*.

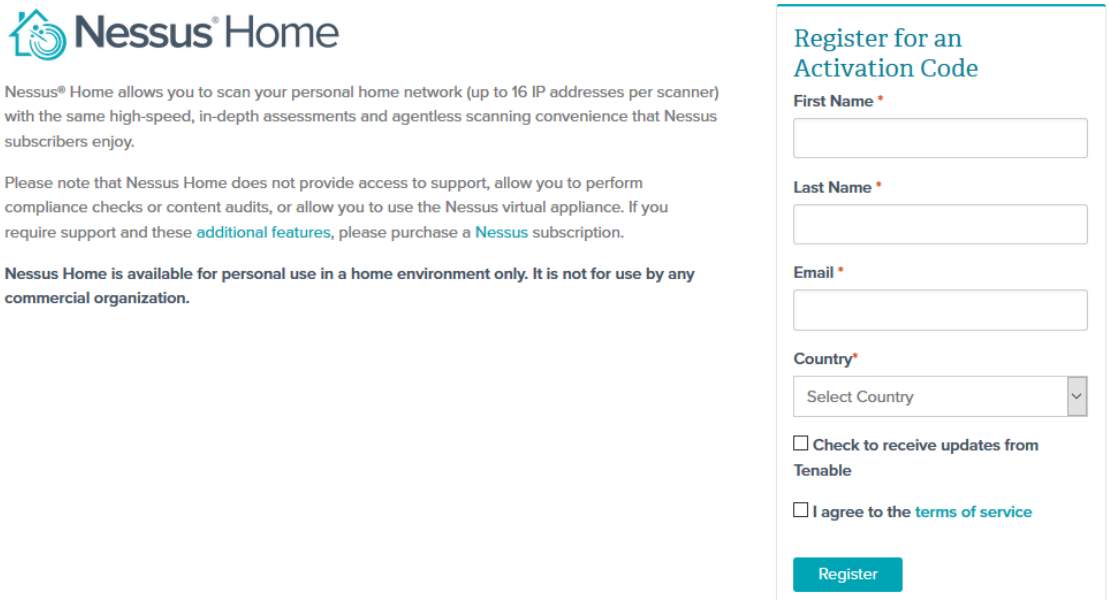

Figura 9 Registo no site

Depois do registo ser efetuado é enviado para o *email* associado a chave referente à versão do Nessus que foi pedida pelo o utilizador. A instalação é relativamente simples e é feita através de um *Wizard* comum.

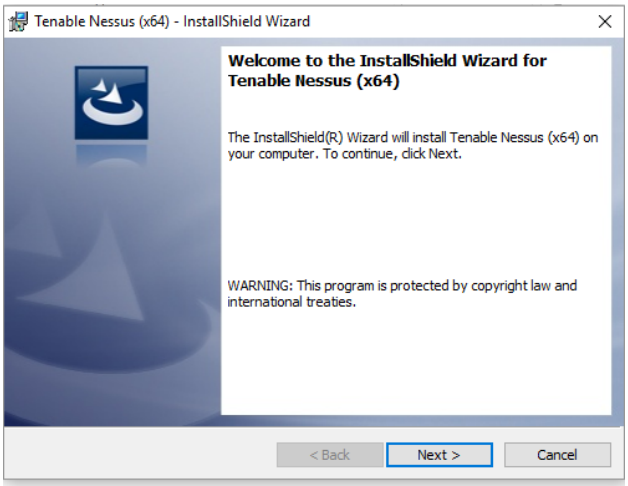

Figura 10 Instalação

Após o registo e a instalação do Nessus estar completo só basta criar um utilizador (como esta demonstrado na figura abaixo) e de seguida associar uma chave, que foi enviada para o *email*, para associar qual é a versão do Nessus que o utilizador está autorizado a usar.

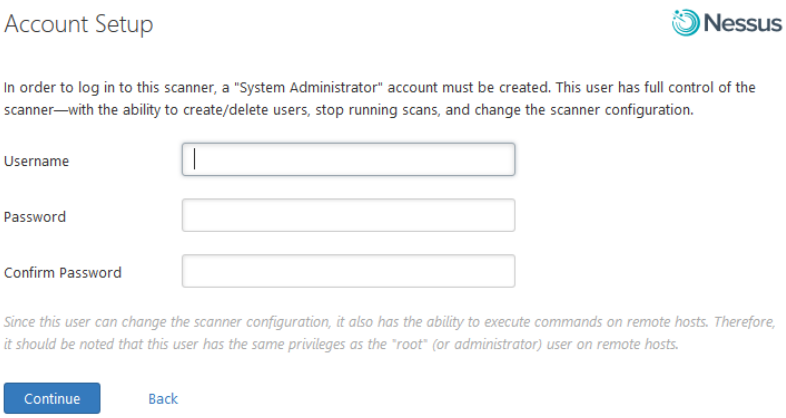

Figura 11 Criação de um utilizador

Funcionalidades

Para podermos aceder às funcionalidades devemos abrir o *Browser* e colocar o link "https://localhost:8834/#/" e fazer o login com um utilizador antes criado.

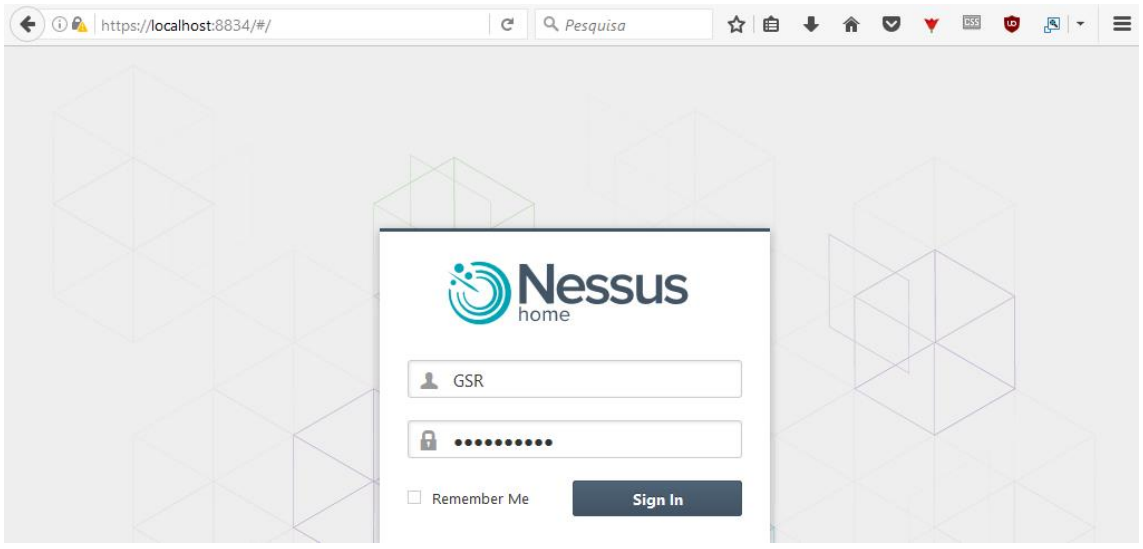

Figura 12 Login

Após o login somos redirecionados para uma página inicial da aplicação, se quisermos aceder às funcionalidades, basta clicar no botão "*New Scan*".

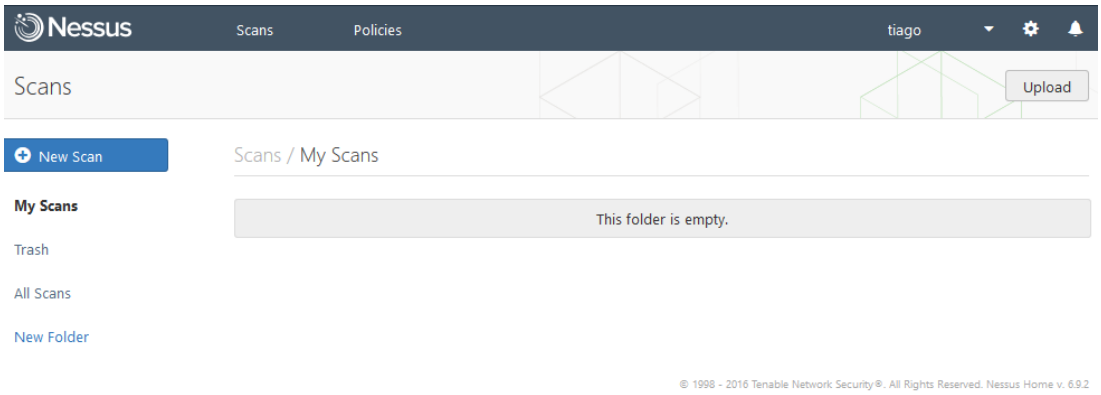

Figura 13 Criação de um novo Scan

Após o passo anterior ter sido executado o gestor é encaminhado para outra página com as funcionalidades suportadas pela versão do Nessus que o utilizador pode ter acesso.

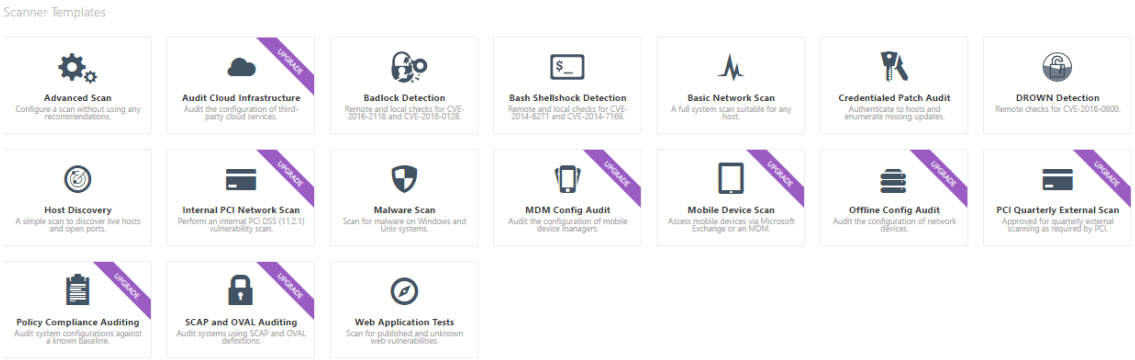

Figura 14 Funcionalidades da ferramenta

Como nós podemos ver na figura acima existe algumas funcionalidades etiquetadas com um "*Upgrade*", essas funcionalidades só podem ser utilizadas se utilizarmos uma versão paga, as quais não iremos abordar, só abordando as gratuitas: [15]

- ***Advance Scan*** →É um *template* para os utilizadores que possam ter o total controlo do seu *scan* ou da política de configuração;
- ***Badlock Detection*** →Esta política é utilizada para fazer verificações remotas ou locais das vulnerabilidades de *Badlock*;
- ***Bash Shellshock Detection*** → verificações remotas e credenciadas para *Bash Shellshock;*
- ***Basic network scan*** → para fazer *scan* a *hosts* internos e externos;
- ***Credentialed Patch Audit*** → faz o *login* nos sistemas e enumera que *software updades* estão em falta;

- ***Drown Detection*** → verificações remotas para CVE-2016-0800;
- ***Host discovery*** → identifica todos os *hosts* que estão numa determinada rede e as suas portas que estão abertas;
- ***Malware Scan*** → para procurar *malware* instalado nas máquinas;
- ***Web Application Tests*** → para possibilitar que os utilizadores possam fazer *scans* genérico para as aplicações *web*;

Utilização das funcionalidades

Uma vez que existem muitas funcionalidades iremos explorar apenas as mais importantes ao nosso ver, nomeadamente: "Host discovery", "Badlock Detection"," Basic Network Scan". Para a exploração das ferramentas vamos utilizar os cenários criados anteriormente.

Teste do cenário 1(Host Discovery)

Para este teste utilizou-se a funcionalidade **Host Discovery,** esta funcionalidade consiste no envio de vários tipo de *ping's* para todos os hosts da rede. Estes *ping's* podem ser do tipo, ARP, ICMP, TCP, UDP (DNS, RPC, NTP, etc.).

Iniciou-se o teste para verificar todos os dispositivos ligados à rede obtivemos o seguinte resultado.

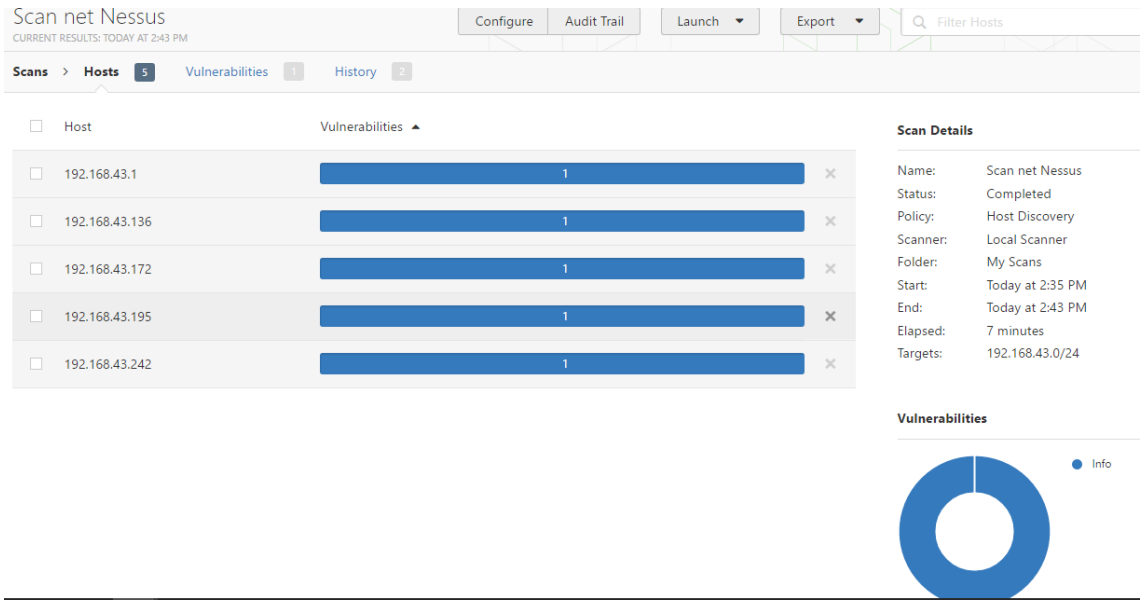

Figura 15 Hosts descobertos no Scan

Após concluído o teste verificamos que o *software* conseguiu identificar todos os dispositivos presentes na rede. Para cada dispositivo é apresentado o *ip*, o tipo de dispositivo (se for um portátil ira ser mostrado "*DESKTOP-1U5SBR3*") e o *MAC Adress*.

Teste Cenário 2(Basic Network Scan)

Utilizando a funcionalidade **Basic Network Scan**, que consiste em verificar se existem vulnerabilidades, na ligação à internet, nos dispositivos ligados à rede. Obtivemos o seguinte resultado.

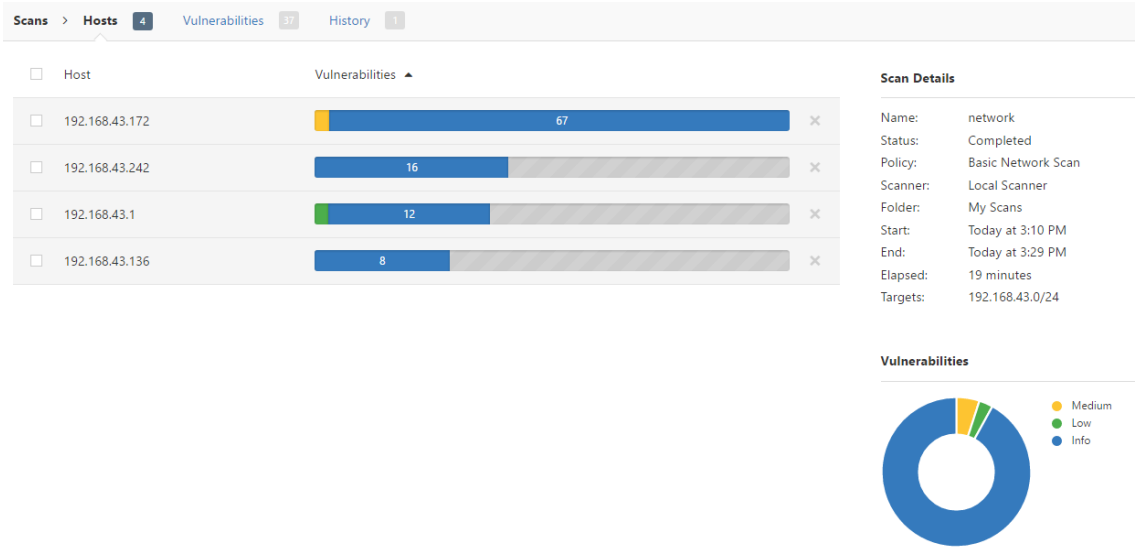

Figura 16 Vulnerabilidades encontradas nos hosts

Neste teste verificamos a existência de duas vulnerabilidade de médio grau, num dos portáteis ligado a rede, *SMB Signing Disable e SSL Certificate Cannot Be Trusted*. Passemos a explicar abaixo cada uma das vulnerabilidades detalhadamente.

- SSL Certificate Cannot Be Trusted

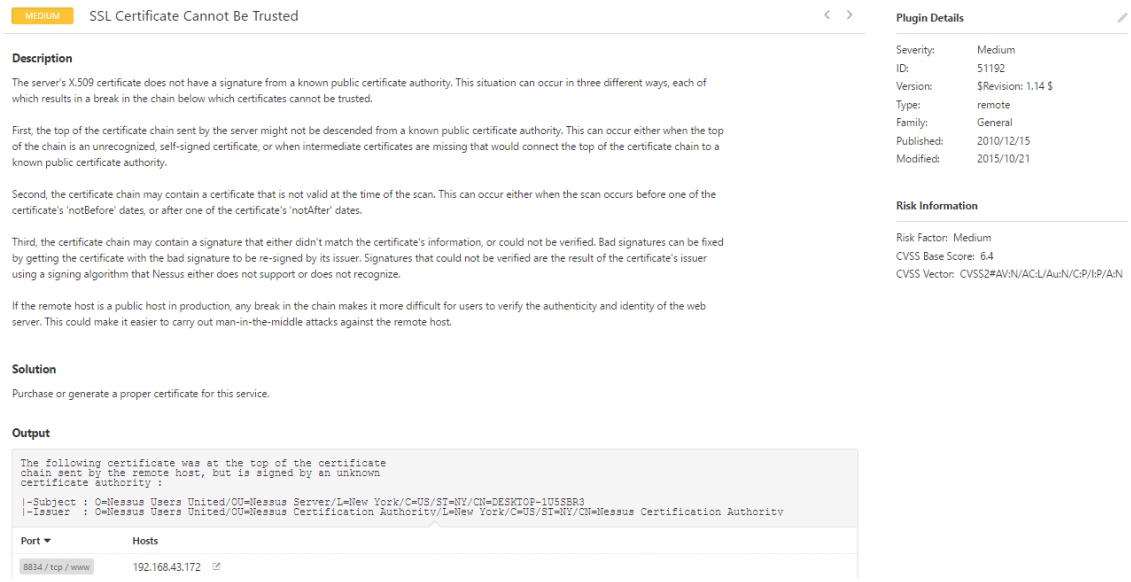

Figura 17 Apresentação da vulnerabilidade e da sua resolução

Na descrição é apresentado que o certificado X.509 não tem a assinatura de uma autoridade de certificação pública conhecida. E retrata as diversas situações e que esta situação pode acontecer.

Como solução o software recomenda comprar ou gerar um próprio certificado para este serviço.

- SMB Signing Disable

Na descrição, o *software* diz-nos que não foi pedida uma assinatura no servidor SMB remoto. Desta forma um invasor remoto pode explorar a situação e realizar ataques contra o serviço SMB.

Quanto a solução, consiste em encontrar e assinalar “sempre” a configuração da “política Servidor de rede Microsoft” e assinar digitalmente comunicações.

Teste cenário 3(Badlock Detection)

Utilizando a funcionalidade **Badlock Detection** isto consiste em verificar se existem vulnerabilidades do tipo *badlock* (analisar as vulnerabilidades relacionadas com ataques as bases de dados com intuito de modificar dados) nos dispositivos ligados à rede. Fizemos o teste utilizando o cenário 3 e obtivemos o seguinte resultado.

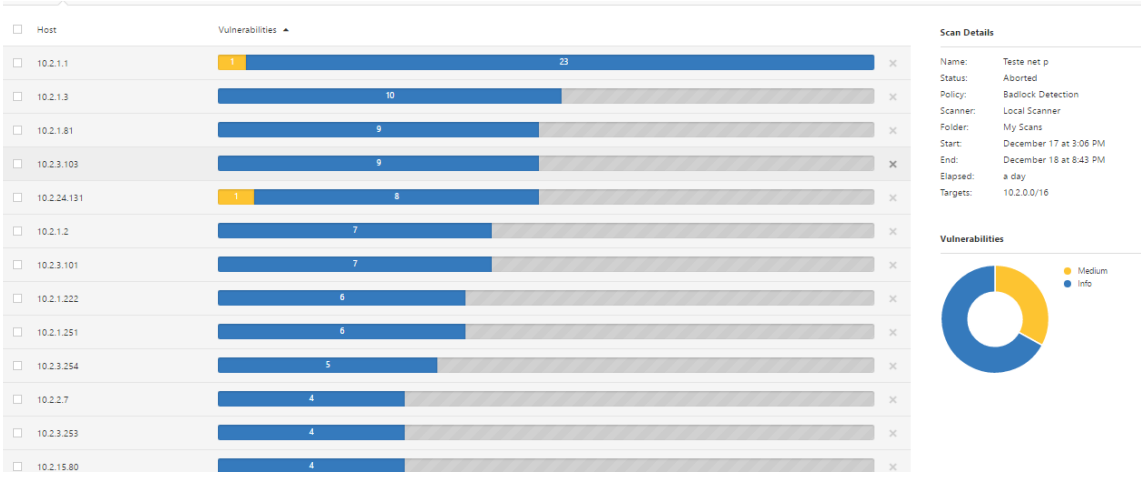

Figura 18 Resultado do teste de Badlock

Verificamos que o *scan* aos *badlocks* identificou vários *ip's* de *hosts* e servidores da universidade que estão ligados a internet, e fornecem algum serviço. Um deles é um servidor muito conhecido, vinhático.uma.pt. Neste servidor foi detetada uma vulnerabilidade de médio grau.

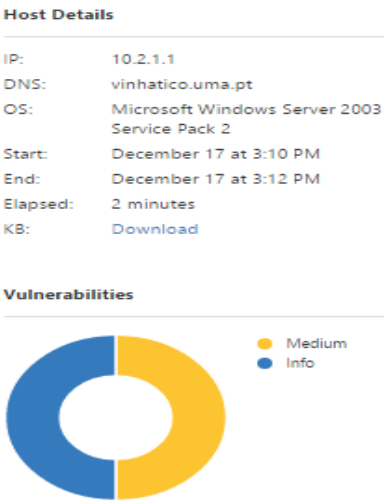

Figura 19 Identificação do host

Esta vulnerabilidade de médio grau é descrita como, o anfitrião remoto do Windows é afetado por uma vulnerabilidade de elevação de privilégios nos protocolos SAM (*Security Account Manager*). Deste modo invasor intermediário capaz de intercetar comunicações entre um cliente e um servidor pode alterar os dados da Base de Dados.

A solução consiste em atualizar o sistema operativo atual, Microsoft Windows Server 2003 Service Pack 2, para um *patch* lançado pela Miscrosoft posteriormente como, Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, e 10.

Ainda para o cenário de utilização número 3 utilizou-se novamente a ferramenta utilizada no segundo teste **Basic Network Scan** mas agora para de maior dimensão, para descobrir mais a cerca desta ferramenta que é uma das mais importantes do Nessus. Neste teste obteve-se uma gama de resultados muito significante, como podemos verificar na imagem que se segue.

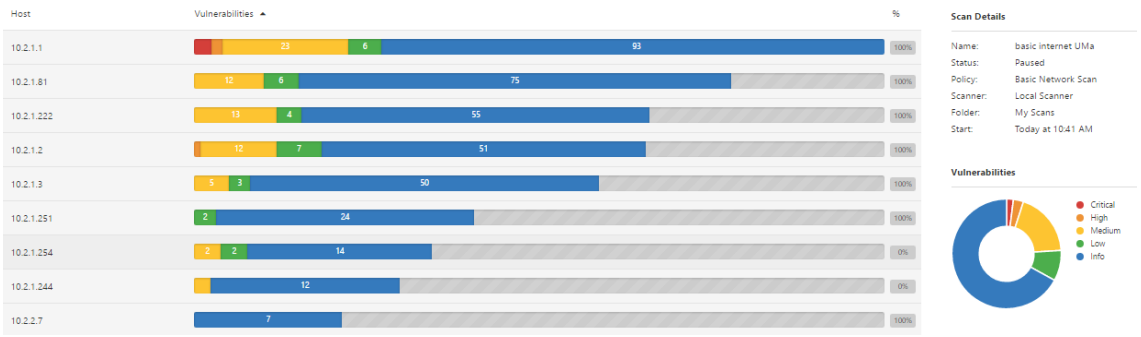

Figura 20 Resultado do teste Basic Network Scan

Por uma questão de simplificação vamos analisar apenas as vulnerabilidades *critical* e as *high* do servidor vinhatico.uma.pt, que foi uma vez mais o ponto mais crítico do teste. Segue-se abaixo a figura que mostra as vulnerabilidades encontradas, e exploração de cada uma das vulnerabilidades detalhadamente.

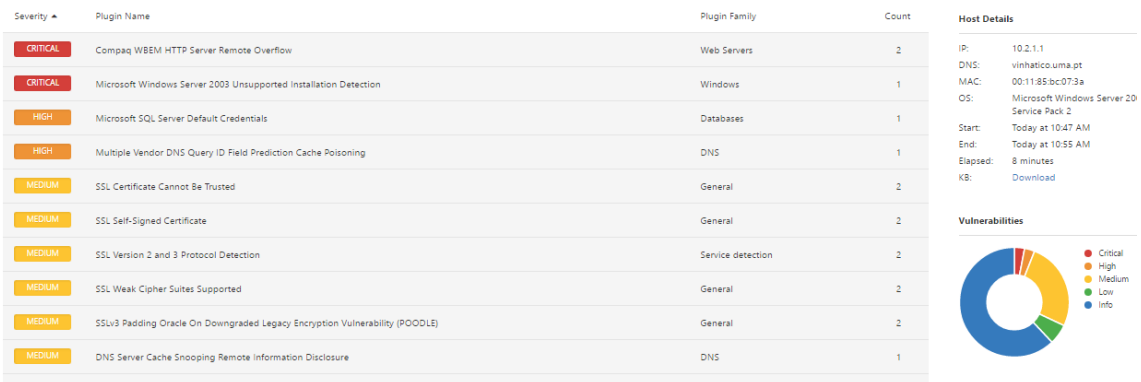

Figura 21 Vulnerabilidades encontradas no servidor vinhatico.uma.pt

- Compaq WBEM HTTP Server Remote Overflow

A primeira vulnerabilidade diz que o *host* remoto está executando um servidor Compaq Web Management e que esta versão deste *software* é vulnerável a um *overflow* do *buffer*, o que pode permitir que um invasor execute código arbitrário no *host* remoto.

A solução é a atualização para o *HP HTTP Server* versão 5.96 ou posterior ou para o *System Management Homepage* versão 2.0 ou posterior. Para saber mais a cerca da vulnerabilidade o utilizador pode clicar no local identificado na imagem abaixo.

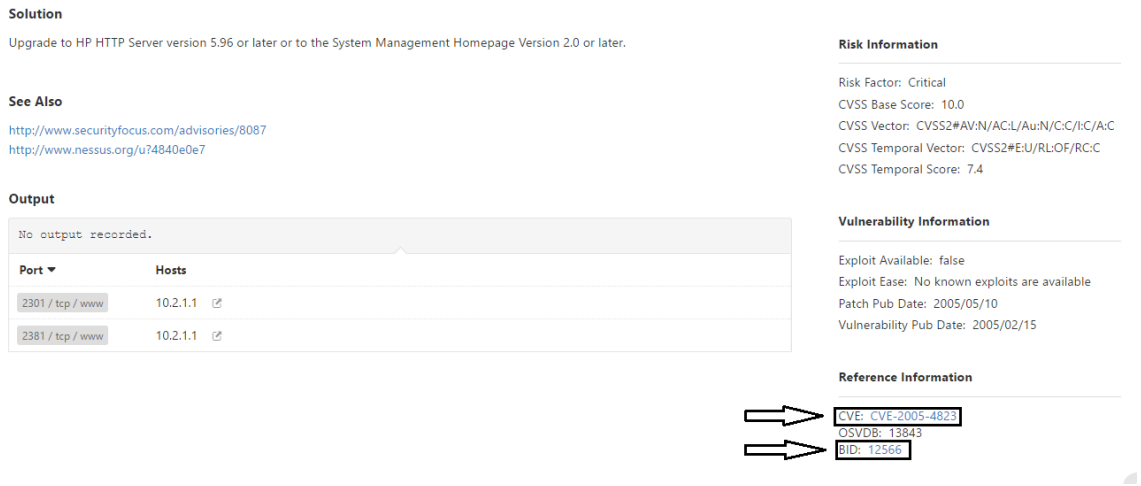

Figura 22 Demonstração de onde saber mais sobre uma vulnerabilidade

Após clicar no *link* o utilizador é reencaminhado para a seguinte página.

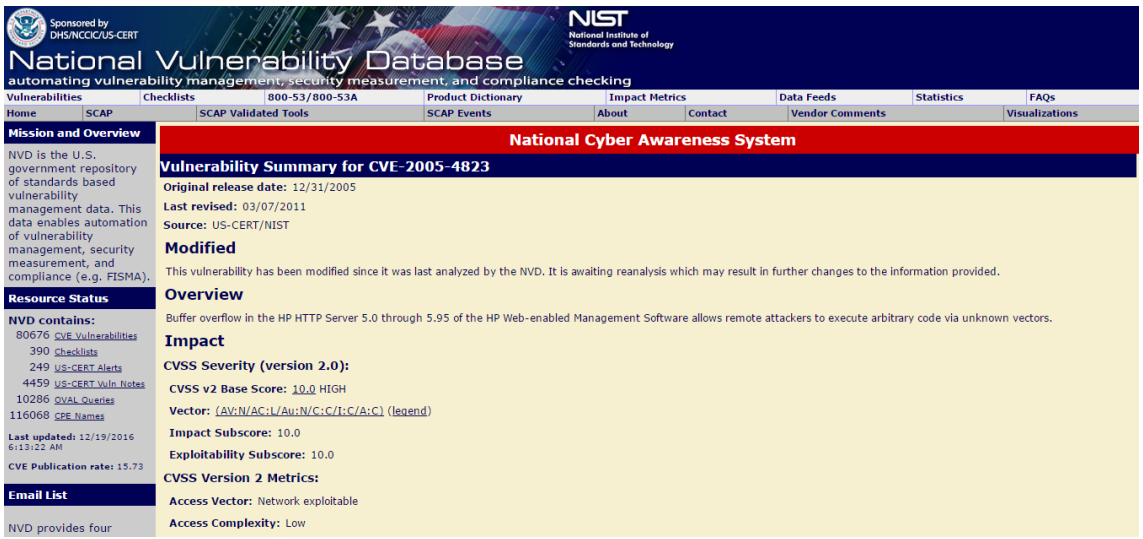

Figura 23 Site oficial da base de dados de vulnerabilidades

- Microsoft Windows Server 2003 Unsupported Installation Detection

A segunda vulnerabilidade diz que o *host* remoto está executando o Microsoft Windows Server 2003. Suporte para este sistema operacional pela Microsoft terminou 14 de julho de 2015.

Uma proposta de solução dada pelo *software* consiste em atualizar o sistema para uma versão do Windows que é atualmente suportada.

- Microsoft SQL Server Default Credentials

Na terceira vulnerabilidade temos que o SQL Server tem uma senha comum para uma ou mais contas.

A resolução desse problema é simples, apenas tem de ser escolhida uma senha segura para as contas afetadas.

- Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Na quarta vulnerabilidade temos que o resolvedor de DNS remoto não usa portas aleatórias ao fazer consultas a servidores DNS de terceiros. O que permite a um invasor remoto, não autenticado explorar isso para corromper o servidor DNS remoto, permitindo que um invasor desvie o tráfego legítimo para *sites* arbitrários.

A solução proposta pelo programa foi a de entrar em contacto com o fornecedor do servidor DNS para obter um novo *patch*.

Teste cenário 3(Host Discovery)

Foi feito um teste à funcionalidade **Host Discovery,** mas o intuito foi apenas explorar a funcionalidade de agendamento de *scans*. Como podemos verificar na figura seguinte. Esta ferramenta oferece alguma autonomia, na medida que é possível agendar *scans* à rede para a deteção de vulnerabilidades.

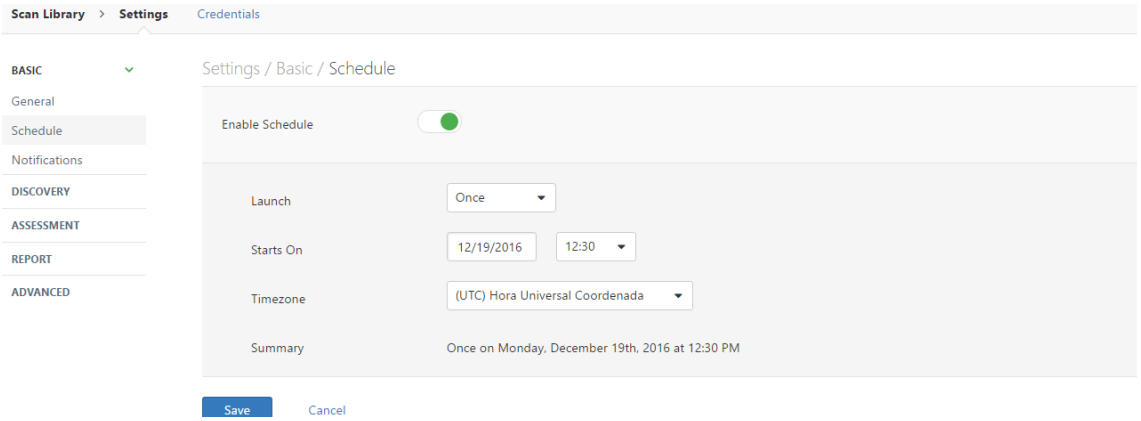

Figura 24 Agendamento do scan

Agendou-se um *scan* e verificou-se que na lista de *scans* o *scan* estava agendado, como podemos verificar na seguinte figura.

Figura 25 Scan agendado

Após a hora agenda o *scan* já se encontava a correr como podemos vericar na figura seguinte.

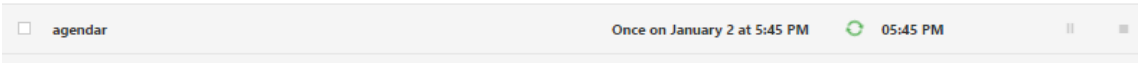

Figura 26 Scan iniciado após a data prevista

Caso o gestor queira guardar os resultados dos *scans* para consultar depois, estes podem ser exportados para formatos de documentos tais como html, pdf, csv, Nessus e Nessus D8, como podemos ver na seguinte imagem[16].

Figura 27 Exportação dos resultados

Discussão

Devido ao exorbitante preço na ordem 640€ anuais [17], para a versão privada que suporta menos hosts. A exploração da nossa ferramenta recaiu apenas na parte gratuita, o que limita um pouco o que esta ferramenta é capaz de fazer. Foi feito um esforço por parte de grupo, enviando um *email* para a Nessus, para que o fabricante fornece-se um licença para a exploração.

Vantagens

Após a utilização da ferramenta conseguimos identificar diversos pontos fortes desta ferramenta. A possibilidade de agendar uma verificação para uma determinada data a qualquer uma das funcionalidades da ferramenta. A sugestão de resolução das vulnerabilidades é sempre apresentada ao gestor de forma sucinta, e se o gestor quiser saber mais acerca da vulnerabilidade pode consultar a base de dados de vulnerabilidades disponibilizado pelo Nessus. É possível fazer o *download* dos resultados das análises caso o gestor necessite de consultar mais tarde. Ainda encontramos mais algumas vantagens como por exemplo a interface gráfica muito intuitiva e um vasto suporte *online*, fica abaixo uma lista das vantagens encontradas por nós e as encontradas na net.

- Possibilidades de agendar *scanners*;
- Permite interromper *scans*;
- Permite pausar *scans*;
- Tem sugestões de resolução de problema;
- Possui uma versão *home* para o uso doméstico;
- Possui uma GUI muito intuitiva;
- Possui vasta documentação na internet;

Outras vantagens encontradas na Internet, nomeadamente:

- *Software* de alta qualidade;
- Fácil instalação;
- Custo mínimo;
- Funciona em diversos SO's;
- Possui atualizações de *plugins* automáticas;
- Trabalha em paralelo com o Nmap;
- Pode processar vários arquivos ao mesmo tempo;
- Pode processar vários tipos de arquivos com formatos diferentes;

[18] [19]

Desvantagens

Na área das vulnerabilidades esta ferramenta dispõe de poucas desvantagens, contudo existem. Aquando encontrada uma vulnerabilidade não existe qualquer tipo de alarme, pelo menos na versão gratuita. As vulnerabilidades são encontradas, contudo a resolução mesmo das mais básicas, tem de ser feitas pelo gestor. Cada análise tem de ser analisada exaustivamente pelo gestor. Caso o gestor queira explorar outras áreas da gestão, que não a deteção de vulnerabilidades, tem de instalar um *software* de um novo fabricantes.

Com uma pesquisa na Internet encontramos outras desvantagens que são apresentadas abaixo.

- Alguns ataques podem não ser detetados porque grandes partes das assinaturas são muito específicas;
- Pode ser "enganado" por meio de técnicas como a inserção de espaços em branco no *stream* de dados do ataque;
- É comum produzir grande número de vulnerabilidades falsas, tanto positivos como negativos. Isso se deve a comportamentos imprevisíveis dos usuários e de sistemas;
- Devem ser realizadas muitas sessões para coletar dados para o sistema, com o intuito de caracterizar os padrões normais de comportamento.
- Os scans precisam de ser executados regularmente, pois novas vulnerabilidades podem surgir.
- Um scanner de vulnerabilidades apenas consegue descobrir vulnerabilidades já conhecidas.
- Para utilizar a ferramenta como Gesto-Agente é preciso pagar.

[18]

Conclusão

Este trabalho teve como objetivo testar a plataforma de gestão Nessus e a algumas das suas funcionalidades para a verificação de falhas e vulnerabilidades de segurança. Num ambiente prático feito por nós, foram testados alguns *hosts* e em alguns deles foram encontradas vulnerabilidades.

Concluiu-se que a ferramenta poderá ser uma grande ajuda para o administrador de redes/sistemas, porque tem uma interface gráfica muito intuitiva, é uma das ferramentas mais populares que se pode encontrar no mercado relacionadas com as vulnerabilidades, encontra facilmente falhas em *hosts* e ainda indica a possível solução do problema, permite agendar *scans*, permite ter *plugins* para deteção de novas vulnerabilidades que estão diretamente ligados a *Scan Database* onde vão buscar os dados os dados de vulnerabilidades conhecidas, o que pode ser uma limitação caso existam novas vulnerabilidades, permite a fácil exportação dos relatórios gerados pelo Nessus, entre outros. Contudo contem limitações, uma vez que existem meios de contornar os *scans* do Nessus, e algumas das vulnerabilidades produzidas são falsas.

Após a utilização desta ferramenta de deteção de vulnerabilidades concluiu-se que esta ferramenta pode ser útil e vantajosa para o caso de ser necessária um ferramenta de deteção de vulnerabilidades, contudo se o âmbito de gestão for além das vulnerabilidades poderá não ser a ferramenta mais adequada. Nós após este trabalho utilizaríamos esta ferramenta, mas só se necessitássemos de uma ferramenta exclusivamente para as vulnerabilidades, se fosse necessária uma ferramenta num âmbito mais geral iriamos ver outras ferramentas, mesmo que não fossem tão fortes na parte das vulnerabilidades.

Bibliografia

[1] «Rede de computadores», *Wikipédia, a enciclopédia livre*. 12-Out-2016.

[2] «Artigo - Gerenciamento de Redes de Computadores: Uma Breve Introdução». [Em linha]. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php. [Acedido: 02-Jan-2017].

[3] «rp10-az-snmp - SNMP.pdf». .

[4] «Nessus», *Wikipédia, a enciclopédia livre*. 25-Ago-2015.

[5] «Nessus Vulnerability Scanner», *Nessus Vulnerability Scanner*. [Em linha]. Disponível em: https://nessusfmrl.wordpress.com/. [Acedido: 02-Jan-2017].

[6] «Tenable Network Security lança Nessus Manager». [Em linha]. Disponível em: http://www.gti.es/pt-pt/ConoceGTI/NotasPrensa/Paginas/NotasPrensa/Tenable-Network-Security-lan%C3%A7a-Nessus-Manager.aspx. [Acedido: 02-Jan-2017].

[7] «Nessus como ferramenta para verificação de vulnerabilidades (Debian) [Dica]». [Em linha]. Disponível em: https://www.vivaolinux.com.br/dica/Nessus-como-ferramenta-para-verificacao-de-vulnerabilidades-(Debian). [Acedido: 02-Jan-2017].

[8] «The Nessus Port Scanning Engine: An Inside Look - Blog | Tenable Network Security». [Em linha]. Disponível em: https://www.tenable.com/blog/the-nessus-port-scanning-engine-an-inside-look. [Acedido: 03-Jan-2017].

[9] «CVE - About CVE». [Em linha]. Disponível em: http://cve.mitre.org/about/. [Acedido: 03-Jan-2017].

[10] «- vulnerability.pdf». .

[11] «Hardware Requirements». [Em linha]. Disponível em: https://docs.tenable.com/nessus/6_9/Content/HardwareRequirements.htm. [Acedido: 03-Jan-2017].

[12] «Software Requirements». [Em linha]. Disponível em: https://docs.tenable.com/nessus/6_9/Content/SoftwareRequirements.htm. [Acedido: 03-Jan-2017].

[13] «Licensing Requirements». [Em linha]. Disponível em: https://docs.tenable.com/nessus/6_9/Content/LicensingRequirements.htm. [Acedido: 03-Jan-2017].

[14] «Install Nessus on Windows». [Em linha]. Disponível em: https://docs.tenable.com/nessus/6_9/Content/WindowsInstall.htm. [Acedido: 03-Jan-2017].

[15] «Template Library». [Em linha]. Disponível em: https://docs.tenable.com/nessus/6_6/Content/6_Features/Template_Library.htm. [Acedido: 03-Jan-2017].

[16] «Nessus V2 File Format - nessus_v2_file_format.pdf». .

[17] «Tenable Network Security, Inc. Nessus Professional - Annual Subscription (New) [SERV-NES] - $2,190.00». [Em linha]. Disponível em: https://store.tenable.com/index.php?main_page=product_info&cPath=1&products_id=94. [Acedido: 03-Jan-2017].

[18] «Ferramentas de Auditoria Prof.: Cheila Bombana Ferramentas de Auditoria Instrumentos informatizados utilizados para realizar uma atividade de auditoria. - ppt carregar». [Em linha]. Disponível em: http://slideplayer.com.br/slide/325729/. [Acedido: 03-Jan-2017].

[19] ataliba, «Instalando e Configurando o Nessus», *(Des)Informação*, 22-Jul-2003. [Em linha]. Disponível em: http://www.ataliba.eti.br/content/instalando-e-configurando-o-nessus. [Acedido: 03-Jan-2017].