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 interacção 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.

Discussão

Vantagens:

* *Software* de alta qualidade;
* Fácil instalação;
* Custo mínimo;
* Funciona em diversos SO’s;
* Possui vasta documentação na internet;
* Trabalha em paralelo com o Nmap;
* Pode processar vários arquivos ao mesmo tempo;
* Pode processar vários tipos de arquivos com formatos diferentes;
* Possibilidades de agendar scaners;
* Permite interromper scans;
* Tem sugestões de resolução de problema;
* Possui uma versão *home* para o uso doméstico;
* Possui atualizações de *plugins* automáticas;
* Possui uma GUI muito intuitiva;

<http://slideplayer.com.br/slide/325729/>

<http://www.ataliba.eti.br/content/instalando-e-configurando-o-nessus>

Desvantagens:

* Alguns ataques podem não ser detetados porcausa que 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 alarmes falsos, 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.

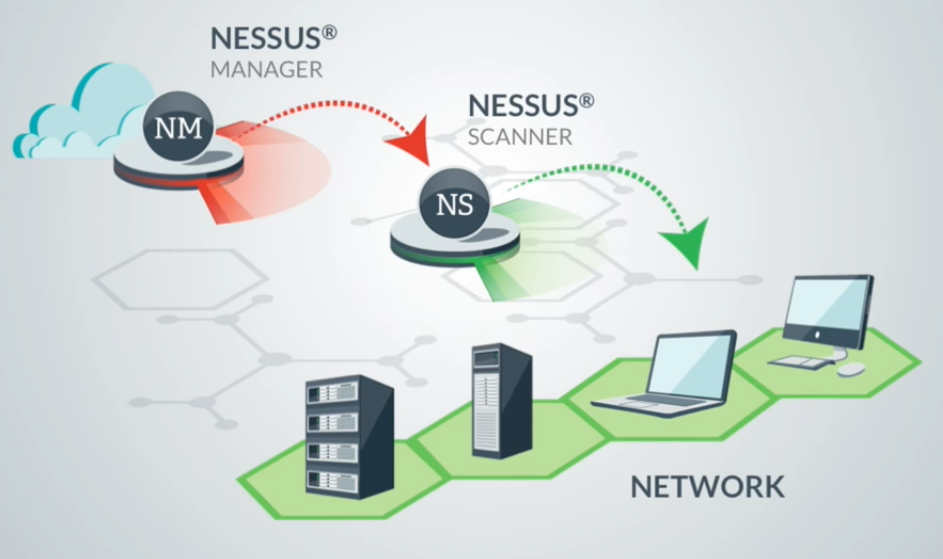
Limitações

1. Os scans precisam de ser executados regularmente, pois novas vulnerabilidades podem surgir.
2. É sempre necessário a presença de alguém para a análise dos dados após o scan.
3. Um scanner de vulnerabilidades apenas consegue descobrir vulnerabilidades já conhecidas.
4. Não resolve

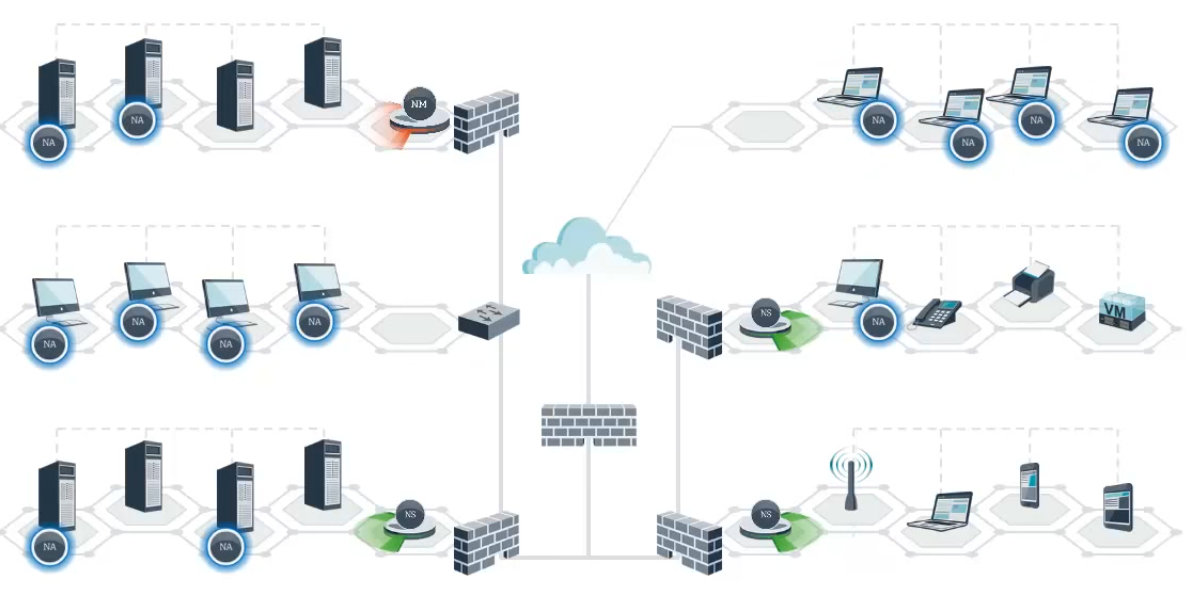
Nmap (Network Mapper): é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. Determina quais hosts estão disponíveis na rede, quais serviços os hosts oferecem, quais sistemas operacionais eles estão executando e que tipos de filtro de pacotes/firewalls estão em uso. Normalmente utilizado para auditorias de segurança, mas muitos administradores de sistemas e rede consideram-no útil para tarefas rotineiras como: inventário de rede; gerenciamento de serviços de atualização agendados; monitoramento de host ou disponibilidade de serviço.

Modelo Organizacional

O Nessus funciona de duas formas, a primeira, o scan de vulnerabilidades em redes locais e a segunda, o scan de vulnerabilidades em redes distribuídas. Na primeira forma, um Nessus Manager ordena o Nessus Scanner a realizar os scans e este realiza os scans a todos os hosts como podemos verificar na figura seguinte.



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.



<http://www.hardware.com.br/guias/seguranca-linux-windows/usando-nessus.html>

O teste Nessus é feito em duas partes. A primeira é o portscan, onde ele utiliza o Nmap,combinado com alguns testes adicionais para descobrir quais estão abertas em cada host. A partir daí, entram em ação os plugins, que testem cada porta em busca de vulnerabilidades conhecidas.

<https://elearning.ipca.pt/1213/pluginfile.php/93387/mod_label/intro/CD_LESIPL_TP2-a7532_a7814.pdf>

IV. CONCLUSÃO

Este trabalho que teve como objectivo testar o sistema Nessus e a maioria de seus recursos de verificação de falhas e vulnerabilidades de segurança e funcionalidades em um ambiente prático onde foram testados hosts que realmente continham vulnerabilidades. Concluiu-se que a ferramenta é de grande ajuda ao administrador de redes/sistemas encontrando facilmente falhas em hosts e ainda indicando a possível solução do problema o que facilita bastante o seu trabalho. Estes relatórios gerados pelo Nessus podem ser guardados em diversos formatos, incluindo HTML, latex e PDF, um recurso extremamente interessante na hora de apresentar os resultados e explicar os problemas para outras pessoas 6 .

<https://www.tenable.com/blog/the-nessus-port-scanning-engine-an-inside-look>

É feita 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.