O que pretendo discutir com os nossos colegas é quais são as ferramentas e métodos que utilizam para enumeração ,scanning e testes de vulnerabilidades em redes, sejam essas ferramentas para uso online ou em nossa maquina.

1. Penetration testing

Penetration-test é o método usado para testar e descobrir vulnerabilidades numa rede e a possibilidade de ver como estas podem ser exploradas ou corrigidas.

Para ser feito um teste de penetração são contratados profissionais (ou pessoas internas à rede) para explorar a rede, da mesma forma que um cracker faria e em seguida são entregues os resultados indicando todas as falhas encontradas e como corrigi-las.

Para se fazer um teste de penetração é necessário passar diversas fases, para as quais são utilizadas diversas ferramentas. As fases serão indicadas nos pontos seguintes.

1.1- Reconhecimento da rede

A enumeração consiste no reconhecimento da rede e dos sistemas atingíveis. Os resultados esperados são: nomes de domínios, nomes de servidores, informação do ISP, endereços IP envolvidos e também um mapa da rede. Inclui ainda informação de registros de domínios para os servidores.

Para fazer o reconhecimento da rede, podem ser utilizadas diversas ferramentas e técnicas, conforme o objectivo do ataque. Indico abaixo algumas ferramentas, que poderão ser usadas no reconhecimento.

• Nslookup – funciona em Windows e Linux. Serve para mapear endereços IP para um determinado domínio.

• Whois –Nos dá toda a informação sobre um domínio registado (entidade que registou, endereço físico, contactos, domain servers, etc)

• ARIN

• Dig – serve para perguntar a um servidor DNS informação acerca de outras coisas, por exemplo, a versão do name server que a empresa está a utilizar…

• Engenharia social

• Web site alvo

1.2-Scanning

Nesta fase de um teste de penetração é a identificação de portas abertas e serviços a correr, na máquina(s) ou rede alvo, chegando assim a enumeração de vulnerabilidades no alvo.

Também nesta fase do teste podemos incluir diversas ferramentas e tecnicas, conforme o objectivo do teste e a configuração da máquina/rede alvo. Ferramentas deste tipo foram analisadas no ponto 3 deste mesmo relatório.

As ferramentas mais utilizadas para fazer scanning, são:

• telnet –Serve para mostrar informação sobre uma aplicação ou serviço (versão, plataforma.

• nmap – port scanner

• hping2 – port scanner

• netcat – port scanner

• ping – testa conectividade IP

• traceroute – Ele conta os “hops” da rede, desde a máquina em que é executado até à máquina/sistema alvo.

• queso – OS fingerprinting.

1.3- Teste de vulnerabilidade

Os testes de vulnerabilidades consistem na determinação de que buracos de segurança e vulnerabilidades podem ser aplicadas à rede/máquina alvo. Quem efectuar o teste vai tentar identificar nas máquinas na rede alvo todas as portas abertas, sistemas operativos e aplicações a serem executadas; incluindo o sistema operativo, patches aplicados e service packs aplicados.

Nas etapas anteriores, são identificadas as máquinas que estão ligadas e que portas e serviços têm disponíveis.

Existe, na geral quatro categorias de vulnerabilidades que podem ser encontradas:

• Os bugs específicos do sistema operativo, exploits, vulnerabilidades e buracos de segurança

• As fraquezas no firewall e routers, entre diversas marcas

• A exploração de scripts de web server

• As partilhas e confianças exploráveis entre sistemas e pastas.

O scan de vulnerabilidades pode ser feito de várias formas, que indicarei nos pontos seguintes.

1.3.1- Ferramentas e Manuais

As análises das vulnerabilidades de um computador pode ser feita manualmente, com base na informação recolhida nos pontos anteriores. Ou seja, são percorridas as listas de vulnerabilidades existentes, em busca de alguma que possa existir para cada uma das aplicações instaladas na máquina.

1.3.2- Nessus

O Nessus é a melhor ferramenta para inventariar vulnerabilidades com código fonte disponível.

Instalação

Esta ferramenta é constituida por duas partes: o cliente e o servidor, que podem ou não, ser instaladas em máquinas diferentes.
A instalação é bastante simples:

• executa-se a script de instalação
• adiciona-se um utilizador

Utilização

O Nessus tem de ter o servidor instalado numa máquina *IX, mas o cliente pode ser executado em Windows ou em *IX.

O cliente desta ferramenta, pode correr em modo gráfico ou em modo de comando. O modo de comando tem a vantagem de poder ser incluído em scripts, o modo gráfico tem a vantagem de ser facilmente seleccionável quais os testes de vulnerabilidade que são executados.

1.3.3- SARA-Security Auditor's research assistant

O SARA é um scanner de rede, que procura serviços e os analisa.
Esta ferramenta produz relatórios em diversos formatos: html, XML, interactivos e CSV, importável para folhas de cálculo.

Instalação

A instalação do SARA é muito simples: basta descomprimir o tgz, e executar ./configure, make, make install.

Relativamente à configuração, podem fazer-se algumas configurações específicas, mas deixando tudo o que vem por default, obtêm-se resultados interessantes.

Utilização

O SARA pode ser executado em três modos: interactivo (interface web), linha de comando, ou modo remoto.. No caso presente, optei pelo modo interactivo.

O modo remoto pode ser útil, no caso de se desejar ter o servidor de SARA numa determinada máquina e um cliente gráfico, na própria máquina.

Este modo tem algumas limitações: só é permitido um utilizador de cada vez, um teste não pode ser interrompido, o servidor não foi feito para ficar permanentemente à espera de pedidos, é preciso ter preocupações com a segurança.

Pode ser definido o tipo de "ataque" que é feito à máquina/rede em causa. Pode variar entre cinco níveis de severidade.

1.3.4- Comparação entre detectores de vulnerabilidades

A detecção manual de vulnerabilidades é, com certeza a que permite mais pormenor, mas é muito difícil de ser implementada com perfeição.

Relativamente às duas ferramentas utilizadas, o SARA é, sem dúvida, mais rápida, mas é também a menos eficiente. Além de apresentar resultados muito menos detalhados e não apresentar formas de resolução das vulnerabilidades (como o Nessus), apresenta falsos positivos.

Relativamente à forma de apresentação de resultados, o SARA é muito inferior. O servidor tem ainda problemas de funcionamento, no sentido que entre dois testes, se

não for removido, não funciona corretamente.

Tem no entanto, uma funcionalidade interessante, que é ir guardando e apresentando em paralelo os resultados de testes anteriores.

Esta característica pode ser interessante, do ponto de vista de armazenamento de informação sobre todo o parque de servidores de uma empresa, por exemplo.