Pentesting

Material sobre pentesting

- Introdução

Introdução

O que é Pentesting

Penetration test é uma área de consultoria de segurança digital, qual tem como finalidade testar a segurança de um determinado sistema para achar possiveis brechas e propor soluções mas não implementa-lás.

O Pentest pode ser dividido em fases, cada qual com suas proprias peculiaridades.

Fases do Pentesting

Reconhecimento Inicial

Essa primeira fase se baseia em conseguir as informações básicas sobre a empresa ou sistema. Entre elas estão:

- possíveis usuários
- domínios da rede
- e-mails
- formas de contato com os usuarios
- etc.

Varredura de Dados

Nessa fase o principal é conseguir mais informações tendo como base as informações conseguidas incialmente. Agora tendo foco em conseguir informações

- faixa de ips que o sitema usa
- fazer varredura nos endereços e portas
- descobrir serviços utilizados
- estimar quantas máquinas possui
- conseguir o nome das máquinas
- SO utilizado
- etc.

Ganho de acesso

Agora que já tem todas as informações que pode precisar, deve coloca-lás uso e começar a atacar o sistema

- parte importante

Manter acesso

Depois de ter conseguido acesso e escalonado para root voce deve conseguir manter o acesso, colocando um backdoor, por exemplo:

- instalar um root kit
- colocar serviço
- programar um cron
- definir uma exceção
- etc

Apagar rastros

No final de tudo, deve-se tentar apagar as evidências de que houve uma invasão, pois ser capaz de fazer isso só evidência mais falhas na segurança do sistema, por causa disso deve:

- esconder a origem da invasão
- apagar os logs que gerou
- esconder os arquivos e programas inseridos no sistema