Tópicos Especiais em Segurança da Informação

TP5 - Varreduras múltiplas em portas específicas

Arthur do Prado Labaki

07-06, 2022

GBC 235

Informações adicionais

Nem todos os exercícios estão com imagem aqui no relatório, mas todas as imagens integradas nesse relatório, quanto códigos, planilhas ou gifs de demonstração estão em meu repositório no GitHub abaixo.
Link do meu GitHub

Resolução do item 1)

Foi escolhido a Universidade federal de São Carlos (AS52888).

Resolução do item 2)

Para melhor execução do exercício, foi escolhido 3 blocos de *IPs* da UFSCar, sendo:

- Bloco A: 200.136.248.0/22
- Bloco B: 186.219.80.0/20
- Bloco C: 200.133.224.0/20

Resolução do item 3)

Um endereço *IPv4* é um número de 32 bits, dividido em 8 bits. Ele identifica exclusivamente um *host* em uma rede *TCP/IP*. Já o bloco de IP pode ser entendido como um segmento contínuo de endereços IP que estão associados a uma organização ou país. O endereço IP pode ser dividido em x.y.z.w/k, em que x,y,z,w são bits, que variam em valor de 0 a 255, em que representam rede e *host* (dependendo da classe) e o k é o número de bits na parte de rede do endereço (máscara de rede ou sub-redes).
O bloco de endereços escolhidos da UFSCar foi 200.136.248.0/22 contendo 1,024 *hosts*, 186.219.80.0/20 e 200.133.224.0/20 contendo 4,098 *hosts* cada .

Resolução dos itens 4, 5 e 7)

Foi encontrado páginas de login, como PfSense, IP Phone, IntelBras, entre outros. Ainda foi encontrado paginas Index of/, Moodle, páginas de professores e outras mais. Também foi encontrado portas SSH e Telnet abertas, mas não foi possível obter conexão.
Todas as informações estão dispostas na planilha abaixo.
Link para a minha planilha

Resolução do item 6)

A função do protocolo SSH é garantir que haja uma conexão segura entre o computador e o servidor remoto, o que garante a transferência de dados sem nenhuma perda de informação. A principal vantagem do protocolo SSH é que ele permite a criptografia de dados mesmo em conexões não seguras. Telnet funciona como um SSH mais rudimentar. Portanto esses protocolos facilitam administração de diversos *hosts* por um único computador, pois garantem a segurança dos dados e ainda a rapidez da gerencia de servidores ou maquinas.

Resolução do item 8)

Serviços web e remotos facilitam muito o controle da empresa, porém ao expor essas portas, se não for tomado os devidos cuidados, eles podem se tornar pontos de acesso a pessoas mal intencionadas, por meio de vulnerabilidades. As formas de prevenir ou mitigar os riscos são, dentre eles, ofuscar essas portas para não serem encontradas facilmente por ferramentas de *port scanning*, remover serviços que não sejam essenciais das portas, e também estar sempre atualizados de vulnerabilidades que possam ocorres nos serviços abertos.