SEGURANÇA

Trabalho Prático 2 | Configuração avançada de um equipmento

Introdução

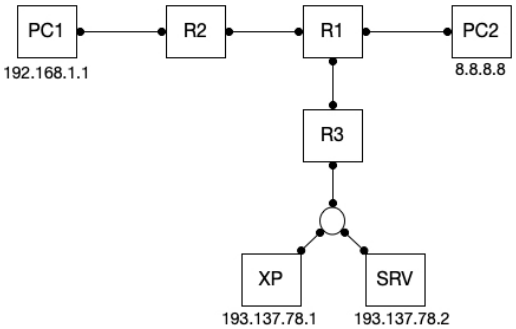
Neste trabalho prático, o objetivo principal é conseguir estimular a aplicação prática dos conhecimentos adquiridos no âmbito das aulas de segurança, assim como promover a pesquisa de soluções técnicas que promovam as melhores práticas de segurança em redes.
A implementação do cenário, análise dos componentes que o compõem e a avaliação das questões de segurança que possam estar envolvidas na implementação das melhores regras e soluções serão tidas em consideração para a nota final.

Equipas

Os grupos que foram criados para o primeiro trabalho prático são válidos neste segundo trabalho. No caso de ocorrerem alterações aos elementos de cada grupo, deverão comunicar de imediato ao docente via email (vapi@isec.pt). Os elementos que não tenham grupo definido ou que não constem na lista de grupos disponível no moodle não serão objeto de avaliação, não tendo classificação no trabalho prático.
Assim, reforça-se que é imperativo que todos os elementos que pretendam ser alvo de avaliação neste trabalho devem pertencer a um grupo, validar se o seu nome consta na lista de grupos criado no moodle.
O momento de avaliação de cada grupo vai ser definido pelo docente, sendo a lista publicada em endereço a ser disponibilizado posteriormente.

Cenário do trabalho prático

O cenário de trabalho é o que se apresenta a seguir.



Podemos verificar que, neste diagrama, apenas dispomos de 3 routers (R1, R2 e R3) e 4 equipamentos.
O PC1 possui endereço privado (RFC 1918), enquanto que os XP, SRV e PC2 possuem endereços públicos.
As redes estão a simular os seguintes cenários:

- PC1: rede de utilizadores finais (estudantes, por exemplo)
- XP e SRV: rede de servidores
- PC2: rede externa (WAN, Google.com, hacker, ...)

Em termos de configuração, os equipamentos deverão ser:

- PC1, SRV e PC2: vpcs 1, 2 e 3, respetivamente
- XP: soft loopback
- R1, R2 e R3: Cisco 7200

É objetivo, neste trabalho, que se consigam efetuar as seguintes configurações nos 3 routers R1, R2 e R3:

- Proteções gerais
  - Não permitir spoofing a partir da rede externa (PC2)
  - Não permitir saída de RFC 1918 para a rede exterior
  - Pode-se fazer telnet ou ssh para os routers a partir de qualquer rede
    - Implementar medidas de proteção de ataques de força bruta
    - Deve existir logging de tentativas de acesso com sucesso e sem sucesso para o servidor de logging central, localizado em 193.137.78.1
- NAT PC1:
  - Deve sair para a rede externa com o endereçamento 193.137.79.1

- Logging
  - Deverão realizar operações de logging das atividades relevantes do R1 para o servidor de logging 193.137.78.1 (para além das tentativas de acesso por telnet ou ssh)
- Autenticação
  - O acesso ao router deve ser possível por autenticação local e *RADIUS*
  - Deve ser criado um utilizador local "noc" com password "nocpwd"
  - Deve ser criado um utilizador RADIUS "remote" com password "remotepwd"
- Firewall
  - PC1:
    - Deve conseguir realizar ligações tcp, udp e icmp para o exterior
    - Não deve ser possível realizar qualquer acesso a esta rede (não existem servidores internos, por isso, não faz sentido abrir portos)
  - XP
    - Não deve ter nenhum porto aberto para o exterior ou para o PC1
    - Deve conseguir realizar todas as operações tcp, udp e icmp para o exterior sem qualquer restrição
    - Se realizar acesso telnet ao R1 com o username "myaccess" e password "mypwd", deve ser aberta uma firewall que permite que seja possível pingar do PC2 para o XP
  - SRV:
    - Deve permitir acesso aos serviços de FTP a partir da rede PC1
    - Deve permitir acesso HTTP, SMTP, POP/IMAP a todo o mundo
    - Deve permitir queries DNS apenas a partir do PC1, devendo este serviço ter os portos abertos para funcionar corretamente
  - O acesso à Internet a partir do PC1 deve estar vedado todos os fim-de-semana (não deve ser possível realizar qualquer comunicação de dentro para fora ou de fora para dentro)

Prazos e Entregáveis

O prazo de entrega encontra-se definido na página do moodle.
Os entregáveis do trabalho são:

- Um relatório onde seja explicado de forma sucinta, mas completa, os seguintes pontos
  - Configuração das firewalls
  - Configuração de logging
  - Configuração da autenticação
  - Configuração do NAT
- Todos os ficheiros do ambiente GNS3 e VPCS

Os ficheiros devem ser entregues num ficheiro comprimido (.zip, .rar, ...).
O relatório produzido deve permitir que uma pessoa externa à cadeira, com conhecimentos básicos de GNS3 e CISCO; assim como sendo possuidor da imagem de WindowsXP disponibilizada aos alunos, possa executar todo o trabalho apresentado.

Esclarecimentos

Esclareceimentos relativos ao trabalho prático podem ser discutidos durante as aulas destinadas para o efeito, via email para o docente (vapi@isec.pt) ou via moodle.