Ficha Técnica do Trabalho Prático de Segurança

Realizado por:
Alexandre Baptista 2017012006
Abílio Costa 2017018177
Rui Mota 2017012857

Proteções gerais

- Não é permitido realizar spoofing a partir da rede externa esta funcionalidade foi completamente implementada;
- Não permite saída de RFC 1918 para a rede exterior;
- Possibilidade de fazer telnet e ssh a partir de qualquer rede:
    - Contém proteção de ataques de força bruta;
    - O servidor de logging central (syslog) está localizado no endereço 193.137.78.1, onde é registado o logging das tentativas de acesso com sucesso e sem sucesso a qualquer router.

NAT PC1

- Funcionalidade implementada na sua totalidade, o PC1 sai para a rede externa com ip 193.137.79.1.

Logging

- As atividades relevantes do R1, para além do registo das tentativas de telnet e ssh, estão a ser registadas no servidor de logging 193.137.78.1.

Autenticação

- Em todos os routers é permitida a autenticação local ou por RADIUS;
- O user “noc” está bem configurado em todos os routers.
- A autenticação por RADIUS do user RADIUS “remote” está implementada, mas a autorização por RADIUS não funciona.

Firewall

- PC1:
  - Consegue realizar ligações tcp, udp e icmp para o exterior (R2 f0/0_out).
  - A rede não pode ser acedida por fora a não ser que seja o retorno das ligações efetuadas pelas acls reflexivas (R2 f0/0_in).
- XP:
  - Tem os portos fechados para o exterior e o PC1 (R3 f0/0_in deny ip any any).
  - Consegue realizar todas as operações tcp, udp e icmp para todo o mundo (R3 f0/0_out).
  - A partir de uma lista dinâmica, com a autenticação do user “myaccess” no router R1 permite o PC2 pingar o XP. Para tal permitimos o echo request para o XP (R3 f0/0_in) e bloqueamos o echo-reply (R1 f0/1_in) e apenas desbloqueamos este último após a autenticação do user (R1 f0/1_in).
  - Nota: Várias vezes quando reiniciamos a topologia do projeto, tínhamos de criar sempre o username de novo para funcionar.
- SRV
  - Permite acesso aos serviços FTP a partir da rede PC1 (R3 f0/0_in).
  - Permite acesso HTTP, SMTP, POP/IMAP a todo o mundo (R3 f0/0_in).
  - Permite queries DNS apenas a partir do PC1 (embora só funcione com o protocolo TCP). (R3 f0/0_in).
- O acesso à Internet do PC1 está vedado todos os fins-de-semana (R2 f0/0_out e R2 f0/0_in).