Segurança Informática em Redes e Sistemas  
LETI 2024/25

Relatório do Projeto

Nº do grupo: \_\_\_\_\_\_\_\_\_\_\_ Membros do grupo que realizaram o projeto:

Nº: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nº: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nº: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responda às questões abaixo.

# Personalização da rede

1. Em todos os endereços IP, somou ao primeiro número de cada endereços IP o número do grupo? [ ] Sim [ ] Não
2. O servidor web executa o Apache2 e contém uma página simples de apresentação da empresa? [ ] Sim [ ] Não
3. O servidor de correio eletrónico (mailserver) está a executar o comando netcat em modo servidor à escuta nos portos TCP/465 (SMTPS) e TCP/993 (IMAPS)? [ ] Sim [ ] Não
4. O servidor de ficheiros (fileserver) está a executar o *netcat* em modo servidor à escuta no porto TCP/X, onde *X = 25000 + número do grupo?* [ ] Sim [ ] Não

# VPN – OpenVPN

1. A VPN funciona da forma indicada no enunciado? [ ] Sim completamente [ ] Mais ou menos [ ] Não
2. Configurou a proteção das comunicações com o algoritmo AES-128-GCM? [ ] Sim [ ] Não
3. Configuração da VPN: servidor
   1. Indique todos os ficheiros[[1]](#footnote-1) que criou/alterou dentro da VM para configurar o OpenVPN.
   2. Transcreva para aqui as linhas que alterou/colocou nesses ficheiros.
4. Configuração da VPN: cliente
   1. Indique todos os ficheiros que criou/alterou dentro da VM para configurar o OpenVPN.
   2. Transcreva para aqui as linhas que alterou/colocou nesses ficheiros.
5. Teste do funcionamento da VPN:
   1. Indique o(s) comando(s) completos[[2]](#footnote-2) que usou para gerar tráfego que permita verificar se o tráfego é enviado através da VPN.
   2. Indique em que VM(s) esse(s) comando(s) pode(m) ser executados de modo a fazer essa verificação. Indique só uma possibilidade (podem existir mais).
   3. Indique o(s) comando(s) completos que usou no *switchi* para verificar se o tráfego é de facto enviado através da VPN, portanto, 1) cifrado e 2) com endereços IP de origem do cliente e do servidor OpenVPN.
   4. Transcreva para aqui um excerto de tráfego capturado que sugira que o tráfego 1) está cifrado e 2) com endereços IP de origem do cliente e do servidor OpenVPN.

# SSH – OpenSSH

1. O SSH funciona da forma indicada no enunciado, com autenticação baseada em criptografia de chave pública, não em password? [ ] Sim completamente [ ] Mais ou menos [ ] Não
2. Configuração do servidor OpenSSH:
   1. Indique todos os ficheiros que criou/alterou dentro da VM para configurar o servidor OpenSSH.
   2. Transcreva para aqui as linhas que alterou/colocou nesses ficheiros.
3. Configuração do cliente OpenSSH:
   1. Indique todos os ficheiros que criou/alterou dentro da VM para configurar o cliente OpenSSH.
   2. Transcreva para aqui as linhas que alterou/colocou nesses ficheiros.
4. Teste do funcionamento do SSH:
   1. Indique o(s) comando(s) *ssh* e *scp* completos que usou para testar a configuração do OpenSSH (um exemplo de cada um desses dois comandos)
   2. Indique em que VM(s) esse(s) comando(s) pode(m) ser executados de modo a fazer essa verificação. Indique só uma possibilidade (podem existir mais).

# Firewall – iptables

1. As duas firewalls funcionam da forma indicada no enunciado? [ ] Sim completamente [ ] Mais ou menos [ ] Não
2. As regras foram criadas manualmente e são tão simples quanto o possível? [ ] Sim [ ] Mais ou menos [ ] Não
3. Configuração da firewall *packetfilter*. Indique os comandos iptables completos executados para implementar cada um dos 8 pontos da política (se em algum ponto não for preciso fazer nada, diga isso mesmo):
   1. Todos os pacotes não explicitamente permitidos pelo resto da política são proibidos.
   2. É permitido fazer ping e traceroute entre todas as máquinas (para efeitos de depuração de erros).
   3. Qualquer máquina da Internet e da rede da LETISEC pode:
      1. aceder ao servidor web da empresa usando o protocolo HTTP (TCP/80) e SSH;
      2. entregar correio ao servidor de correio eletrónico da empresa (TCP/465, SMTPS);
   4. As máquinas da DMZ da LETISEC:
      1. podem responder aos pedidos que recebem (web e correio eletrónico);
      2. o servidor de correio eletrónico pode entregar mensagens a outros servidores de correio eletrónico da Internet (TCP/465, SMTPS).
   5. As máquinas da rede da LETISEC (i.e., da subrede corporate de Oeiras e da subrede de NY):
      1. podem aceder aos servidores web (via SSH e HTTP)
         1. da Internet (i.e. externos à empresa) e
         2. da própria empresa;
      2. podem aceder ao servidor de ficheiros;
      3. podem aceder ao servidor de correio eletrónico da empresa nos portos TCP/465 e TCP/993.
   6. Os computadores de cada LAN podem comunicar livremente entre si.
   7. Nenhum pacote pode sair de Oeiras ou NY com um endereço IP de origem fora da gama de endereços dessas subredes.
   8. Nenhum pacote pode entrar em Oeiras ou NY com um endereço IP de origem da gama de endereços dessas subredes (bloquear IP Spoofing).
4. Configuração da firewall no router *router3*. Indique os comandos iptables completos executados para implementar cada um dos 8 pontos da política (se em algum ponto não for preciso fazer nada, diga isso mesmo):
   1. Todos os pacotes não explicitamente permitidos pelo resto da política são proibidos.
   2. É permitido fazer ping e traceroute entre todas as máquinas (para efeitos de depuração de erros).
   3. Qualquer máquina da Internet e da rede da LETISEC pode:
      1. aceder ao servidor web da empresa usando o protocolo HTTP (TCP/80) e SSH;
      2. entregar correio ao servidor de correio eletrónico da empresa (TCP/465, SMTPS);
   4. As máquinas da DMZ da LETISEC:
      1. podem responder aos pedidos que recebem (web e correio eletrónico);
      2. o servidor de correio eletrónico pode entregar mensagens a outros servidores de correio eletrónico da Internet (TCP/465, SMTPS).
   5. As máquinas da rede da LETISEC (i.e., da subrede corporate de Oeiras e da subrede de NY):
      1. podem aceder aos servidores web (via SSH e HTTP) e correio eletrónico
         1. da Internet (i.e. externos à empresa) e
         2. da própria empresa;
      2. podem aceder ao servidor de ficheiros.
   6. Os computadores de cada LAN podem comunicar livremente entre si.
   7. Nenhum pacote pode sair de Oeiras ou NY com um endereço IP de origem fora da gama de endereços dessas subredes.
   8. Nenhum pacote pode entrar em Oeiras ou NY com um endereço IP de origem da gama de endereços dessas subredes (bloquear IP Spoofing).
5. Teste do funcionamento. Dê um exemplo (pois testar todos os casos é impossível) de comando completo que usou para testar cada um dos seguintes casos:
   1. Todos os pacotes não explicitamente permitidos pelo resto da política são proibidos.
   2. É permitido fazer ping e traceroute entre todas as máquinas (para efeitos de depuração de erros).
   3. Qualquer máquina da Internet e da rede da LETISEC pode:
      1. aceder ao servidor web da empresa usando o protocolo HTTP (TCP/80) e SSH;
      2. entregar correio ao servidor de correio eletrónico da empresa (TCP/465, SMTPS);
   4. As máquinas da DMZ da LETISEC:
      1. podem responder aos pedidos que recebem (web e correio eletrónico);
      2. o servidor de correio eletrónico pode entregar mensagens a outros servidores de correio eletrónico da Internet (TCP/465, SMTPS).
   5. As máquinas da rede da LETISEC (i.e., da subrede corporate de Oeiras e da subrede de NY):
      1. podem aceder aos servidores web (via SSH e HTTP) e correio eletrónico
         1. da Internet (i.e. externos à empresa) e
         2. da própria empresa;
      2. podem aceder ao servidor de ficheiros.
   6. Os computadores de cada LAN podem comunicar livremente entre si.
   7. Nenhum pacote pode sair de Oeiras ou NY com um endereço IP de origem fora da gama de endereços dessas subredes.
   8. Nenhum pacote pode entrar em Oeiras ou NY com um endereço IP de origem da gama de endereços dessas subredes (bloquear IP Spoofing).

# 5. Detecção e prevenção de intrusões – snort

1. Primeiro passo: criou as novas imagem contendo o *snort?* [ ] Sim completamente [ ] Mais ou menos [ ] Não
2. Segundo passo: o *snort* da máquina *ids1* faz deteção de intrusões da forma indicada no enunciado? [ ] Sim completamente [ ] Mais ou menos [ ] Não
3. Segundo passo: Configurou apenas a regra/alarme do *snort* que diz respeito ao seu grupo (1 ou 2)? [ ] Sim [ ] Não
4. Terceiro passo: o *snort* da máquina *ips* faz prevenção (bloqueio) de intrusões da forma indicada no enunciado? [ ] Sim completamente [ ] Mais ou menos [ ] Não
5. Indique a sequência de comandos e operações que usou para criar uma das duas imagens Kathará contendo o software *snort*.
6. Indique a sequência de comandos que usa para executar o *snort* na máquina *snort.*
7. Segundo passo: Configuração da *snort* como detetor de intrusões: alarme 1 ou 2
   1. Indique todos os ficheiros que criou/alterou dentro da VM para configurar o *snort* de modo a gerar o alarme 1 ou 2.
   2. Transcreva para aqui as linhas que alterou/colocou nesses ficheiros.
8. Terceiro passo: Configuração da *snort* para detecção e prevenção de intrusões:
   1. Indique todos os ficheiros que criou/alterou dentro da VM para configurar o *snort*.
   2. Transcreva para aqui as linhas que alterou/colocou nesses ficheiros.
9. Teste do funcionamento do *snort*:
   1. Indique o(s) comando(s) completos que usou para testar o segundo passo.
   2. Indique o(s) comando(s) completos que usou para testar o terceiro passo.

1. Repare que estamos a falar de ficheiros que existem no sistema emulado, não aos ficheiros \*.startup que fazem parte do Kathará, não da rede que estamos a emular. [↑](#footnote-ref-1)
2. Ou seja, não basta indicar apenas “ping” ou “nc”, mas a linha que contém o comando e que foi executada no terminal. [↑](#footnote-ref-2)