TÉCNICO LISBOA

SIRS-LETI-24-25-Project

Instituto Superior Técnico, Universidade de Lisboa

Segurança Informática em Redes e Sistemas

Licenciatura em Engenharia Informática e de Telecomunicações 2024-25

Objetivos

Nas aulas teóricas da disciplina de SIRS, exploramos diversos mecanismos de segurança. O objetivo deste projeto é aplicar esses conhecimentos na prática, configurando esses tipos de mecanismos numa rede composta por múltiplos computadores, routers e outros equipamentos. Idealmente, esta experiência seria realizada numa rede física real. No entanto, devido ao elevado número de grupos de trabalho e dispositivos necessários, essa abordagem não é viável. Por essa razão, o projeto será desenvolvido numa rede virtual, onde a configuração e utilização dos mecanismos de segurança são muito semelhantes aos de uma rede real. Desta forma, o projeto permite consolidar e aprofundar os conhecimentos adquiridos nas aulas teóricas e no estudo autónomo da disciplina de SIRS, proporcionando uma experiência prática essencial para a compreensão dos conceitos de segurança em redes.

No projeto serão usados mecanismos de segurança para proteger a rede da LETISEC, uma start-up tecnológica da área da cibersegurança. A empresa tem a sede num escritório em Oeiras e um segundo escritório em New York, EUA. A comunicação entre os dois escritórios é feita através da Internet e portanto exposta a um risco elevado. A empresa está preocupada com a possibilidade de potenciais adversários terem acesso à sua propriedade intelectual e dados de negócio, bem como outras ameaças que possam comprometer a sua operação. A rede da LETISEC será emulada usando o software Kathará.

Enunciado e Entrega

Além deste texto, o *enunciado do projeto* inclui:

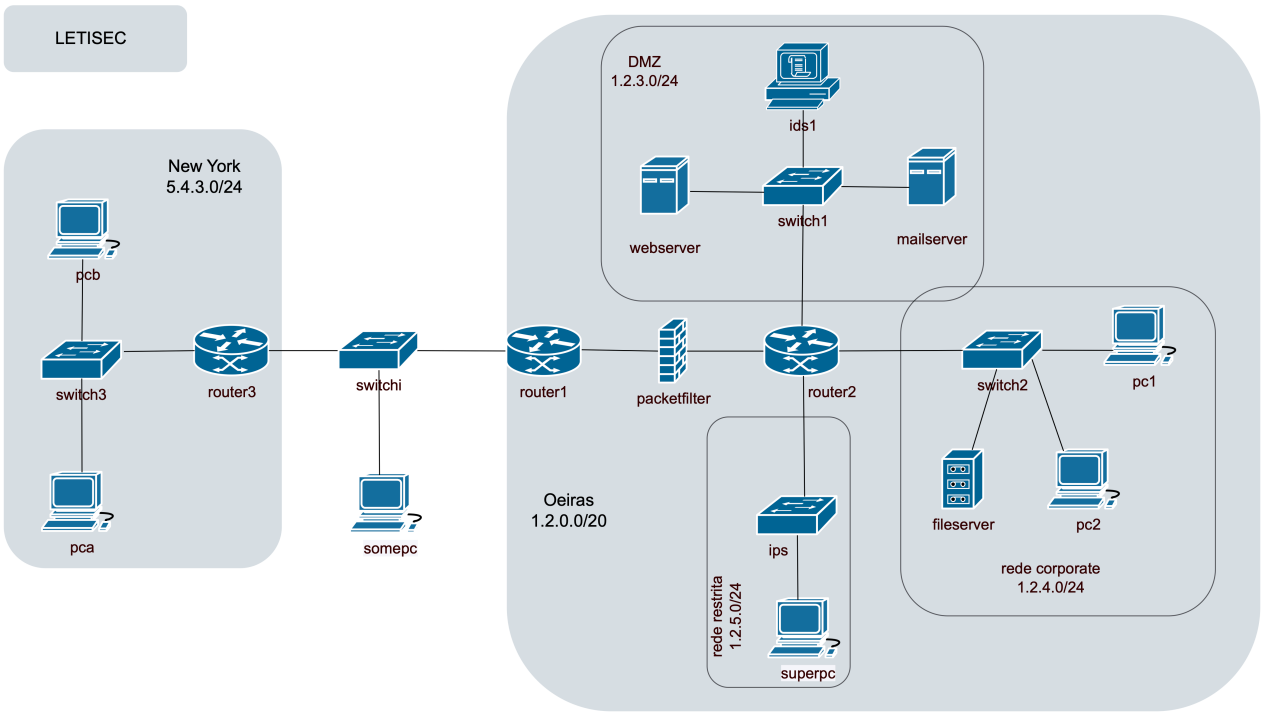
- um ficheiro zip com a emulação da rede (um laboratório Kathará), incluindo todas as VM e os encaminhamentos das camadas 2 e 3 configurados (switchs e routers);
- o ficheiro relatorio-questionario.docx contendo o questionário que servirá de base à elaboração do relatório do projeto.

A *entrega do projeto* tem obrigatoriamente de incluir 3 componentes:

- um diagrama da rede;
- a configuração da rede;
- a resposta ao questionário a reportar o trabalho realizado.

A rede do projeto

Uma representação simplificada da rede encontra-se abaixo. Como se pode ver, a rede da LETISEC contém os dispositivos habituais neste tipo de redes: servidores, estações de trabalho (PCs), routers, switches (também designados bridges), dispositivos de segurança e servidores com serviços específicos. A configuração básica da rede já está feita e é fornecida sob a forma de um laboratório Kathará, mas ainda não inclui mecanismos de segurança.



A rede tem três partes:

1. Escritório de Oeiras (Oeiras): contém vários dispositivos e usa *inicialmente* endereços da gama 1.2.0.0/20;
2. Escritório de New York (NY): contém menos dispositivos e usa *inicialmente* endereços da gama 5.4.3.0/24;
3. Internet: representada de forma extremamente simplificada por um único switch e um PC para efeito de testes. Todos os endereços de fora das gamas dos dois escritórios são parte da Internet.

O escritório de Oeiras tem 4 subredes, interligadas por dois routers:

- uma subrede que contém apenas uma firewall, em concreto, um packet filter;
- a DMZ, onde se encontra:
  - um switch,
  - um servidor web,
  - um servidor de correio eletrónico e
  - um detetor de intrusões;
- a subrede corporate, onde se encontra:
  - um switch,
  - um servidor de ficheiros e

    - as estações de trabalho dos colaboradores da empresa.
- a subrede restrita onde encontra apenas um PC.

O escritório de New York contém apenas um router, um switch e duas estações de trabalho.

Por simplicidade não existe DNS, logo toda a comunicação tem de ser feita usando endereços IPv4.

Personalização

Tarefa 1: Acima está dito que os dispositivos têm *inicialmente* determinados endereços IP. A razão do uso do termo *inicialmente* é a de que *os endereços IP têm de ser obrigatoriamente todos alterados pelo grupo de trabalho. É obrigatório somar ao primeiro número de cada endereços IP o número do grupo.* Por exemplo, para o grupo número 77, a rede de Oeiras vai ter endereços da gama 78.2.0.0/20. A primeira tarefa de cada grupo é fazer essa substituição.

Tarefa 2: Fazer um diagrama da rede detalhado, usando qualquer software adequado para esse efeito (à escolha do grupo). Nesse diagrama têm de ser representados todos os dispositivos, indicados o seu nome e os endereços IP de todas as interfaces de rede que tenham esse tipo de endereços. Pode ser usado como ponto de partida o diagrama fornecido acima. Este diagrama serve para o grupo usar como referência enquanto desenvolve o projeto, mas tem também de ser entregue dentro de um prazo específico e será avaliado (ver prazo abaixo).

O software necessário para fornecer o serviço da LETISEC não está instalado, mas também não se pretende que fique operacional, já que o projeto é sobre segurança de redes. No entanto, pretende-se configurar algum software que forneça uma emulação básica desse serviço e que permita fazer alguns testes:

- estações de trabalho: não contêm software específico, só o que já vem na imagem;
- servidor web: executar o Apache2, contendo uma página simples de apresentação da empresa;
- servidor de correio eletrónico: a configuração de um servidor deste tipo é complexa e está fora do âmbito da cadeira, de modo que vamos emulá-lo executando o comando nc (netcat) em modo servidor e à escuta nos portos TCP/465 (SMTPS) e TCP/993 (IMAPS).
- servidor de ficheiros: também não vamos usar nenhum software específico, mas emulá-lo usando o comando nc em modo servidor à escuta no porto TCP/X em cada servidor, sendo *X = 25000 + número do grupo*.

Testes

Para testar o funcionamento da rede e dos serviços que serão concretizados é fundamental usar ferramentas adequadas. Além de comandos bem conhecidos como o *ping*, *tcpdump*, *traceroute*, *nmap* e *curl*, recomenda-se o uso do *netcat (nc)* que permite estabelecer conexões TCP e enviar texto sobre essa conexão:

- Para ficar à escuta numa porta na máquina de destino (servidor): `nc -l -p <porta>`
- Para enviar pacote TCP executar no client: `echo <string_a_enviar> | nc <ip_destino> <porta_destino>`
- A string deve aparecer no terminal do servidor.

Configuração

A rede base está configurada, mas não existem mecanismos de segurança. O projeto consiste em implementar 4 tipos de mecanismos de segurança: VPN, SSH, firewall (packet filter) e detetor de intrusões.

Recomendações importantes:

- A ordem da configuração dos mecanismos de segurança não é arbitrária. Em concreto, as firewalls podem interferir com o funcionamento da VPN e do SSH, logo é conveniente configurar as firewalls depois de

configurar a VPN e o SSH.
- O grupo deve ir tomando notas e preenchendo o questionário à medida que vai resolvendo o projeto. O questionário documenta o trabalho feito, logo é essencial não o deixar para o fim.

VPN - OpenVPN

Para proteger as comunicações entre os dois escritórios, NY tem de ser ligado a Oeiras através de uma VPN. Configure essa VPN usando o software OpenVPN [2][14]. O router de acesso à Internet de NY será um cliente OpenVPN e o router de acesso de Oeiras será um servidor OpenVPN. Todo o tráfego de NY para Oeiras e vice-versa tem de ser encaminhado através de um túnel entre esses dois routers. Portanto, se alguém na Internet tentar escutar essa comunicação:

- observará tráfego cifrado, logo incompreensível;
- observará como endereços IP de origem e destino os do cliente OpenVPN e do servidor OpenVPN, portanto *não* observará endereços IP internos da rede da LETISEC.

A comunicação tem de ser protegida usando o algoritmo AES-128-GCM. As chaves do cliente OpenVPN devem ser geradas no cliente, não no servidor OpenVPN.

Observe que a comunicação está a ser efetivamente cifrada, escutando a comunicação na Internet.

SSH - OpenSSH

A empresa tem um administrador de rede que tem de trabalhar remotamente no servidor web. O administrador tem uma conta nesse servidor que usa para fazer o acesso usando o protocolo SSH. O administrador viaja muito e por isso, apesar de sob o ponto de vista de segurança não ser muito boa ideia, abriu o acesso por SSH a esse servidor a partir de qualquer ponto do mundo. Por exemplo, pode fazer esse acesso a partir de um PC ligado à Internet, como o *somepc* no caso da nossa rede emulada.

Configure o protocolo SSH fornecido pelo pacote OpenSSH [4][13] de modo a permitir esse acesso. A autenticação tem de ser baseada em criptografia de chave pública, *não* em password.

Teste o funcionamento desses protocolos usando os comandos:

- *ssh* para fazer login remoto e
- *scp* para copiar ficheiros entre dois computadores.

Observe que a comunicação está a ser efetivamente cifrada, escutando a comunicação na Internet.

Firewall - iptables

A rede da LETISEC tem duas firewalls (packet filters):

- *packetfilter* que filtra pacotes entre a Internet e Oeiras;
- *router3* que filtra pacotes entre a Internet e NY.

Configure essas duas firewalls usando o netfilter / iptables [1][12][15] de modo a concretizar a seguinte política de segurança:

1. Todos os pacotes não explicitamente permitidos pelo resto da política são proibidos.
2. É permitido fazer ping e traceroute entre todas as máquinas (só para efeitos de depuração de erros, pois em termos de segurança não é boa ideia permitir da Internet executar esses comandos para dentro da rede da empresa).
3. Qualquer máquina da Internet e da rede da LETISEC pode:
    - aceder ao servidor web da empresa usando o protocolo HTTP (TCP/80) e SSH;
    - entregar correio ao servidor de correio eletrónico da empresa (TCP/465, SMTPS);

4. As máquinas da DMZ da LETISEC:
    - podem responder aos pedidos que recebem (web e correio eletrónico);
    - o servidor de correio eletrónico pode entregar mensagens a outros servidores de correio eletrónico da Internet (porto TCP/465).
5. As máquinas da rede da LETISEC (i.e., da subrede corporate de Oeiras e da subrede de NY):
    - podem aceder aos servidores web (via SSH e HTTP)
        - da Internet (i.e. externos à empresa) e
        - da própria empresa;
    - podem aceder ao servidor de ficheiros;
    - podem aceder ao servidor de correio eletrónico da empresa (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 (ou seja, é preciso bloquear IP Spoofing [11]).

Teste se cada firewall está a bloquear todo o tráfego que deve bloquear. Para testar se uma firewall está a negar o acesso a uma porta podem testar essa porta usando o netcat.

Será avaliada não apenas a corretude, mas também a simplicidade das regras, que revela que as regras foram escritas manualmente pelo grupo e não usando ferramentas automáticas.

Detecção e Prevenção de Intrusões - snort

O detetor de intrusões *snort* [3][17] deve ser configurado de modo a detetar e a bloquear ("prevenção") ataques e intrusões na rede. O sistema de deteção de intrusões (IDS) deve ser colocado na máquina designada *ids1* e o sistema de prevenção de intrusões (IPS) na máquina *ips*. O switch ao qual o computador do ids1 está ligado está configurado para funcionar como *hub*, logo o IDS recebe todo o tráfego que passa por esse *switch* (compare o ficheiro switchoff.startup com o ficheiro switchc1.startup para perceber a diferença). Esta parte tem 3 passos:

Primeiro passo: a instalação do software snort em si, pois este não está disponível na imagem *quagga* usada em todas as imagens do ficheiro lab.conf. Para o efeito é preciso criar duas novas imagens com o snort seguindo as instruções fornecidas no slide “Installing software inside a VM” [15]. Depois substitua as imagens *quagga* das VMs *ids1* e *ips* pelas novas imagens.

Segundo passo: o snort da máquina *ids1* tem de ser configurado para alertar para um conjunto de ataques. O snort contém um conjunto enorme de regras que é atualizado periodicamente. Estas regras e a configuração do snort estão geralmente disponíveis na pasta /etc/snort. No nosso caso interessam apenas dois ficheiros: o /etc/snort/snort.conf (onde está a configuração do snort) e o /etc/snort/rules/local.rules (onde devem ser colocadas as novas regras). Nota: no ficheiro /etc/snort/snort.conf é preciso dar à opção *config checksum_mode* o valor *none*.

Considere os seguintes alarmes:

1. Tentativa de acesso ao porto TCP/20 (FTP) da máquina webserver, pois pode ser uma tentativa de carregar ficheiros inválidos. *Esta regra é implementada apenas pelos grupos com número ímpar*;
2. Tentativa de acesso ao porto TCP/23 (telnet) de qualquer máquina da subrede LAN, pois o telnet não protege as comunicações. *Esta regra é implementada apenas pelos grupos com número par*.

Terceiro passo: configurar o snort do *ips* de modo a *detetar e bloquear* a seguinte situação quando ocorrer: mais de 20 pacotes ICMP Echo Request por minuto com o mesmo IP de origem e dirigidos a qualquer porto do *superpc* pois pode ser uma tentativa de ICMP flood attack. Caso essa situação ocorra, deve ser também gerado um alarme. Na pasta root do *ips* está um script denominado *snort.sh* que deve ser usado para correrem o snort nessa máquina.

Teste a deteção dos ataques acima começando por definir comandos ou scripts que os executem.

Avaliação

Entrega

O projeto é entregue no Fénix. Prazos e forma de entrega (sendo XXX o nº do grupo):

- Até dia 9 de Maio às 17 horas: entregar um diagrama da rede sob a forma de um ficheiro chamado diagramaXXX.pdf ou diagramaXXX.png no Fénix;
- Até dia 27 de Maio às 17 horas: entregar todos os ficheiros do laboratório sob a forma de um ficheiro katharaXXX.tgz no Fénix. Incluir o laboratório Kathará com todos os ficheiros .startup e as subpastas. Se alguns comandos não puderem ser automatizados dessa forma, explicar e indicá-los no relatório. Não é preciso entregar as imagens com o snort. Recomenda-se o uso do comanto *tar -Sczvf proj.tgz pasta_proj/* para comprimir eficazmente os ficheiros (*tar -xvf proj.tgz* para descomprimir);
- Até dia 27 de Maio às 17 horas: entregar o relatório/questionário preenchido sob a forma de um ficheiro chamado relatorioXXX.pdf no Fénix. Esse relatório tem de ser obrigatoriamente criado com base no ficheiro *relatorio-questionario.docx* fornecido.

Discussão

- As discussões são no dia 3 e 4 de Junho;
- As discussões são em grupo, logo todos os elementos do grupo que pretendem ter aprovação ao projeto têm de estar presentes. As classificações no projeto são individuais, ou seja, podem diferir entre os elementos do grupo;
- O projeto é realizado em grupo, logo todos os elementos do grupo têm de fazer o projeto e mostrar conhecimento de *todas* as suas componentes;
- O objetivo do projeto é configurar *uma rede única*, logo é preciso entregar uma rede única configurada e funcional, não duas ou mais configurações parciais.

Bibliografia

- [1] iptables Tutorial 1.2.2 https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
- [2] OpenVPN Howto, https://openvpn.net/index.php/open-source/documentation/howto.html
- [3] Snort Users Manual 2.9.12 – The Snort Project, 2018
- [4] OpenSSH, http://www.openssh.org/
- [5] Kathará web page: https://www.kathara.org/
- [6] Kathará Wiki: https://github.com/KatharaFramework/Kathara/wiki
- [7] Kathará Labs: https://github.com/KatharaFramework/Kathara-Labs/wiki
- [8] Kathará man pages: https://www.kathara.org/man-pages/kathara.1.html
- [9] Guia de Configuração do Kathará: https://github.com/tecnico-sec/Kathara-Setup
- [10] Guia de Laboratório - Network Routing: https://github.com/tecnico-sec/Kathara-Route
- [11] Guia de Laboratório - Network Vulnerabilities: https://github.com/tecnico-sec/Kathara-NetVulns
- [12] Guia de Laboratório - Web Server and Firewall: https://github.com/tecnico-sec/Kathara-WebServer-Firewall
- [13] Guia de Laboratório - Secure Shell: https://github.com/tecnico-sec/Kathara-SSH
- [14] Guia de Laboratório - Virtual Private Network: https://github.com/tecnico-sec/Kathara-VPN
- [15] Miguel Correia. "Kathará". Slides de Segurança Informática em Redes e Sistemas, LETI, Instituto Superior Técnico, 2024

- [16] Miguel Correia. "iptables: a brief introduction". Slides de Segurança Informática em Redes e Sistemas, LETI, Instituto Superior Técnico, Maio de 2022
- [17] Miguel Correia. "snort: a brief introduction". Slides de Segurança Informática em Redes e Sistemas, LETI, Instituto Superior Técnico, Maio de 2022

Caso venham a surgir correções ou clarificações neste documento, podem ser consultadas no histórico (*History*).

Bom trabalho!

Os docentes de SIRS