Gestão e Segurança de Redes

LETI 2017/18

Projeto 2

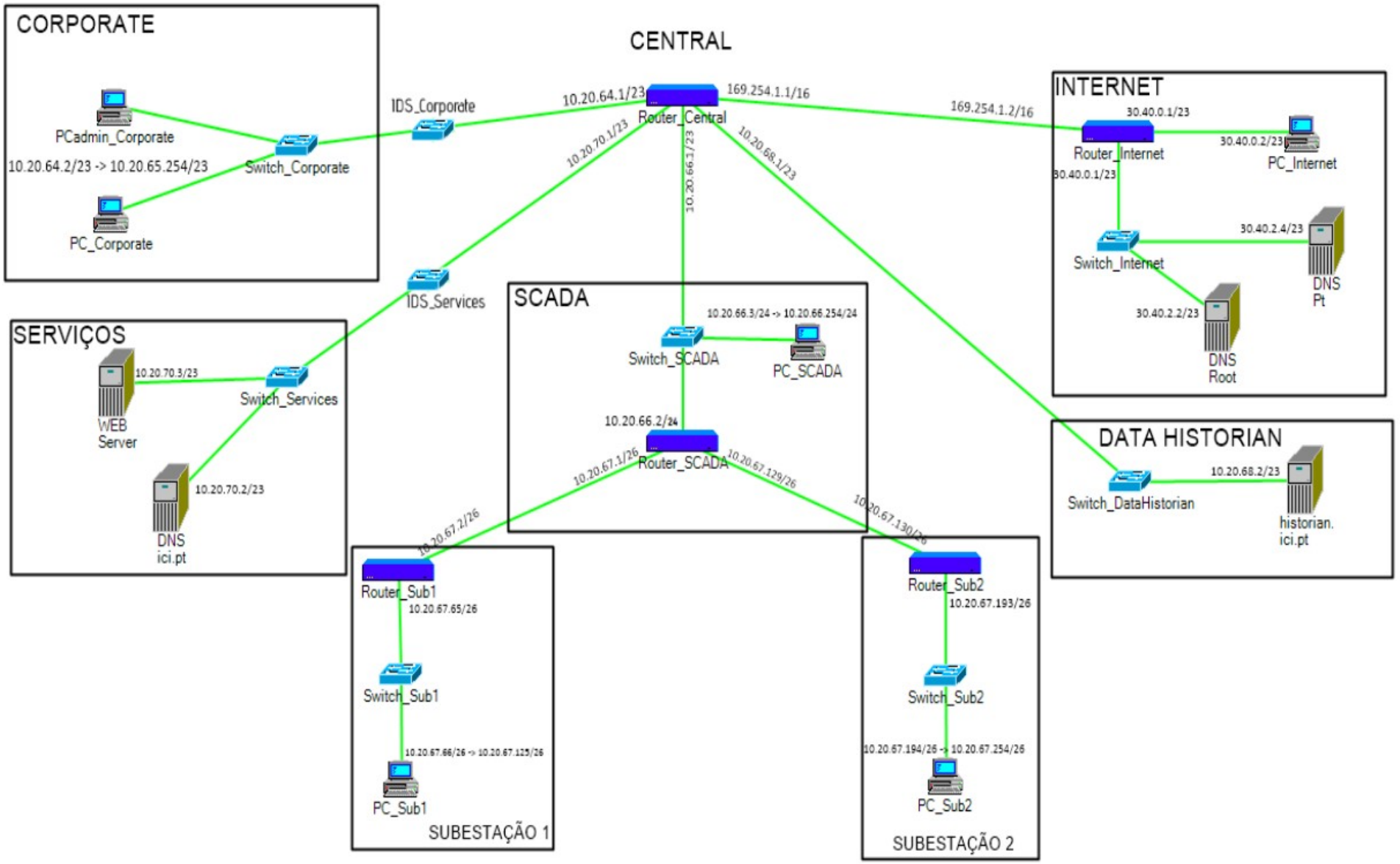
Grupo: 15

Membros do grupo:

Nº: 79779 Nome: Ana Rita Rocha
Nº: 82527 Nome: Carolina Neves
Nº: 82547 Nome: João Bernardo Alves

Respondam às seguintes questões sobre o projeto implementado pelo grupo:

O projeto é baseado no projeto 1 do grupo ou na resolução de referência fornecida pelos docentes da cadeira?	É baseado no projeto 1 do grupo.
Criou uma conta *admin* nos dois servidores da LAN de serviços?	Não, só no servidor web, como indicado no enunciado.
Configurou o OpenSSH?	Sim.
É possível fazer *ssh* e *scp* do PC da Internet para os servidores da LAN de serviços?	Não, só é possível fazer ssh e scp nos PC's dos engenheiros para o servidor web, como indicado no enunciado.
É possível fazer *ssh* e *scp* dos PCs dos engenheiros para os dois servidores da LAN de serviços?	Não, só é possível fazer ssh e scp dos PC's dos engenheiros para o servidor web, como indicado no enunciado.
Ao fazer *ssh* e *scp,* a autenticação é baseada em criptografia de chave pública?	Sim.
Configurou as VPNs usando o pacote OpenVPN? Funcionam?	Sim.
Configurou o *netfilter / iptables* no *router* do edifício central?	Sim.
Esse *router* bloqueia a maior parte dos acessos da Internet à ICI?	Sim.
Esse *router* bloqueia a maior parte dos acessos da DMZ às outras subredes da ICI?	Sim.
Criou um novo nó para instalar o *snort* na rede da DMZ?	Sim.
Instalou o *snort* na rede DMZ?	Sim.
Instalou o *snort* na subrede *corporate?*	Sim.
Indique o conteúdo do 1º pedido HTTP usado para testar o *snort.*	nmap <ip no Corporate ou DMZ>
Qual das regras do ficheiro *web-attacks.rules* é activada por esse pedido?	alert tcp any any -> any 80 (msg:"tcp traffic on port 80"; sid:1, rev:1;)
Indique o conteúdo do 2º pedido HTTP usado para testar o *snort.*	ping <ip no Corporate ou DMZ>
Qual das regras do ficheiro *web-attacks.rules* é activada por esse pedido?	alert icmp any any -> any any (msg:"ICMP packet"; sid:447; rev:3;)


CORPORATE
PCadmin_Corporate
10.20.64.2/23 -> 10.20.65.254/23
Switch_Corporate
PC_Corporate
IDS_Corporate
CENTRAL
10.20.64.1/23
Router_Central
169.254.1.1/16
169.254.1.2/16
INTERNET
30.40.0.1/23
Router_Internet
30.40.0.2/23
PC_Internet
30.40.0.1/23
30.40.2.4/23
Switch_Internet
DNS
Pt
30.40.2.2/23
DNS
Root
10.20.70.1/23
10.20.66.1/23
10.20.68.1/23
IDS_Services
SERVIÇOS
10.20.70.3/23
Switch_Services
WEB
Server
10.20.70.2/23
DNS
ici.pt
SCADA
10.20.66.3/24 -> 10.20.66.254/24
Switch_SCADA
PC_SCADA
10.20.66.2/24
Router_SCADA
10.20.67.1/26
10.20.67.129/26
10.20.67.130/26
10.20.67.2/26
DATA HISTORIAN
10.20.68.2/23
Switch_DataHistorian
historian.
ici.pt
Router_Sub1
10.20.67.65/26
Switch_Sub1
10.20.67.66/26 -> 10.20.67.125/26
PC_Sub1
SUBESTAÇÃO 1
Router_Sub2
10.20.67.193/26
Switch_Sub2
10.20.67.194/26 -> 10.20.67.254/26
PC_Sub2
SUBESTAÇÃO 2

Decisões

Na tomada de decisões em relação à configuração das **Firewalls**, foram feitas as seguintes alterações no Router do Edifício Central:

Tabelas de acesso do serviço WWW para a Internet:
iptables -A FORWARD -s 30.40.0.0/22 -d 10.20.70.3 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -d 30.40.0.0/22 -s 10.20.70.3 -p tcp --sport 80 -j ACCEPT

Tabelas de acesso do serviço DNS para a Internet:
iptables -A FORWARD -s 30.40.0.0/22 -d 10.20.70.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -d 30.40.0.0/22 -s 10.20.70.2 -p tcp --sport 53 -j ACCEPT
iptables -A FORWARD -s 30.40.0.0/22 -d 10.20.70.2 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -d 30.40.0.0/22 -s 10.20.70.2 -p udp --sport 53 -j ACCEPT
E tabelas do ping para testar:
iptables -A FORWARD -s 30.40.0.0/22 -d 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 30.40.0.0/22 -s 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 30.40.0.0/22 -s 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 30.40.0.0/22 -d 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de acesso do serviço DNS para a LAN Corporate:
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.70.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.70.2 -p tcp --sport 53 -j ACCEPT
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.70.2 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.70.2 -p udp --sport 53 -j ACCEPT
E tabelas do ping para testar:
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de acesso do serviço DNS para a LAN SCADA:
iptables -A FORWARD -s 10.20.66.0/24 -d 10.20.70.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -d 10.20.66.0/24 -s 10.20.70.2 -p tcp --sport 53 -j ACCEPT
iptables -A FORWARD -s 10.20.66.0/24 -d 10.20.70.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -d 10.20.66.0/24 -s 10.20.70.2 -p tcp --sport 53 -j ACCEPT
E tabelas do ping para testar:
iptables -A FORWARD -s 10.20.66.0/24 -d 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.66.0/24 -s 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 10.20.66.0/24 -s 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.66.0/24 -d 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de acesso do serviço DNS para a LAN Data Historian:
iptables -A FORWARD -s 10.20.68.0/23 -d 10.20.70.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -d 10.20.68.0/23 -s 10.20.70.2 -p tcp --sport 53 -j ACCEPT
iptables -A FORWARD -s 10.20.68.0/23 -d 10.20.70.2 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -d 10.20.68.0/23 -s 10.20.70.2 -p tcp --sport 53 -j ACCEPT
E tabelas do ping para testar:
iptables -A FORWARD -s 10.20.68.0/23 -d 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.68.0/23 -s 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 10.20.68.0/23 -s 10.20.70.2 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.68.0/23 -d 10.20.70.2 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de ping entre a LAN Corporate e a LAN SCADA:
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.66.0/24 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.66.0/24 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.66.0/24 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.66.0/24 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de ping entre a LAN Corporate e a LAN Data Historian:
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.68.0/23 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.68.0/23 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.68.0/23 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.68.0/23 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de ping entre a LAN Data Historian e a LAN SCADA:
iptables -A FORWARD -s 10.20.68.0/23 -d 10.20.66.0/24 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.68.0/23 -s 10.20.66.0/24 -p icmp --icmp-type 0 -j ACCEPT
iptables -A FORWARD -d 10.20.68.0/23 -s 10.20.66.0/24 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -s 10.20.68.0/23 -d 10.20.66.0/24 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de ping entre a LAN Corporate e para a Internet:
iptables -A FORWARD -s 10.20.64.0/23 -d 30.40.0.0/22 -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 30.40.0.0/22 -p icmp --icmp-type 0 -j ACCEPT

Tabelas de SSH entre a LAN Corporate e o Web Server:
iptables -A FORWARD -s 10.20.64.0/23 -d 10.20.70.3 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -d 10.20.64.0/23 -s 10.20.70.3 -p tcp --sport 22 -j ACCEPT

No Router da LAN SCADA foram feitas as seguintes alterações:

Bloqueio de acesso entre as duas subestações:
iptables -A FORWARD -s 10.20.67.0/25 -d 10.20.67.128/25 -j DROP
iptables -A FORWARD -d 10.20.67.0/25 -s 10.20.67.128/25 -j DROP

Por não termos conseguido ativar os alert do web-attack.rules, decidimos criar duas regras, no ficheiro myAttacks.rules com as regras indicadas na capa. Os pedidos que ativam essas regras são os seguintes:

nmap:
- nmap 10,20,64,2 (PCadmin_Corporate)
- nmap 10,20,64,3 (PC_Corporate)
- nmap 10,20,70,2 (DNS_ici_Services)
- nmap 10,20,70,3 (WebServer_Services)

ping:
- ping 10,20,64,2 (PCadmin_Corporate)
- ping 10,20,64,3 (PC_Corporate)
- ping 10,20,70,2 (DNS_ici_Services)
- ping 10,20,70,3 (WebServer_Services)