Universidade de Aveiro

Extra Theoretical Exam – Security in Communication Networks
June 13th, 2022

Duration: 2h00m. Carefully justify all your answers.

Considering the corporate network depicted in annex:

1. Propose a set of architectural changes to the corporate network in order to protect the network from DDoS attacks and allow the implementation of multiple traffic flow control within the network. (5.0 points)

2. Assuming that the corporation desires to deploy a cluster of servers to provide services to the public (Internet). The services include (i) an HTTPS Web Server with multiple sites/domains (TCP port 443), (ii) an email server (TCP port 465 for Secure SMTP communication between servers and TCP port 993 for client access via IMAPS), and an user VPN server (UDP port 1194). Propose the required network architectural changes and present a list of the (high level) traffic flow control/firewall rules at the multiple locations. (5.0 points)

3. Propose an interconnection solution, between a cluster of database servers on this corporation internal data center and another corporation datacenter servers, able to provide confidentiality at the network level for database synchronization traffic (and only that traffic). Present also the required changes for the traffic flow policies at the firewalls to allow the establishment of the connection and data transmission. (3.0 values)

4. Assuming that in this corporate network are multiple Ethernet sockets in public or semi-public spaces, propose a solution for controlling the access of machines to the network. (3.0 values)

5. Propose a solution, that includes the data gathering process and the definition of alert rules, for an intrusion detection system able to detect:
   a) Login failures to the internal database service from internal authenticated machines (note that machine credentials are not the same as the service credentials). (2.0 points)
   b) Internal communication between BotNet agents in multiple compromised machines within the network. (2.0 points)

- On Layer 2 switches in buildings 1 and 2, access ports are configured for VLANs 1,2,3,4,5,6;
- The links between Layer2 switches and Layer3 are made using trunk/inter-switch links with transport permission for all VLAN;
- Interfaces between Layer 3 switches are Layer 3 ports;
- Interfaces between Layer 3 switches and routers are Layer 3 ports;
- Layer3 switches and routers have OSPFv2 and OSPFv3 protocols active on all IP networks;
- Internet access routers (Routers 1 and 2) are both advertising (by OSPF) default routes;
- All interfaces have an OSPF cost of 1;
- Routers A and B support intrusion detection/ prevention and firewall basic services.
- The company has an internal Datacenter for internal services.