F15 NET3900

Modules 8,9 Assignment

Instructions:

The grade for each question is shown next to the question number.

Note the provided document references.

Please submit this assignment via Bb, email or via paper to me at a lecture or lab.

The solutions will be posted to Bb following the due date.

This assignment is due by midnight Monday October 19.

1/8 User Roles are assigned to users based on Role Derivation Methods. What are the four methods and briefly explain them in your own words.

Ref1: ArubaOS User Guide page 351; "Assigning User Roles", Methods 1-4 only

The user guide can be found here.

https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=12930

Ref2: Module 9 slides 9-17

i) Initial User Role: This role is assigned to clients after they associate/connect but before they are authenticated.

ii) User Derived Role: This role is assigned to users whose clients match certain criteria such MAC address, DHCP Option Code, etc.

iii) Default Role (per Authentication Method): This is the post authentication role assigned to a user if no other method is configured. It is authentication method (i.e. 802.1X or MAC) specific.

iv) Server Derived Role: Roles are assigned to users based on server rules. Server rules derive the role from attributes returned from the authentication server during authentication (i.e. from Access-Accept reply). Server rules are applied to a server group.

2/3 User Roles are defined using Firewall Session Policies. Describe the three advantages of Firewall Session Policies over regular ACLs in your own words.

Ref 1: ArubaOS User Guide, page 342; "Configuring Firewall Policies"

Ref 2: Module 8, slide 3

i) Bi-directional: This means that policy can specify whether the connection is outbound or inbound. For example, I may permit a policy only if it is outbound from the user but not inbound to the user.
ii) Session-aware or Stateful: This means that the Firewall tracks the session state of network connections such as TCP.
iii) Dynamic: Policy address information can change based on context. For example the "user" alias means the IP address of the connected user which changes from user to user.

3/2 What is the difference in behaviour between the following two policies and why:

i)
```
ip access-list session pingTest1
 any any svc-icmp permit
```

ii)
```
ip access-list session pingTest2
  user any svc-icmp permit
```

Ref: Module 8, slide 14

i) The echo request can be initiated from the client going outbound or from the server going inbound. This is because the src/dst addresses use the "any" system alias.
ii) The echo request can only be initiated from the client going outbound but is blocked when initiated in the other direction. This is because the policy specifies a specific src address of "user".

4/3 Consider the following session policy:

```
1 netdestination dns-srv
2 host 10.252.1.20

3 ip access-list session NewPolicy
4    user network 10.254.0.0 255.255.0.0 any permit
5    user host 10.254.1.20 any deny
6    user alias dns-srv any permit
```

Will the policy permit or deny the following packets and which statement will perform the action?

a) Source IP = user; Dest IP = 10.254.1.20

b) Source IP = user; Dest IP = 10.253.1.20

c) Source IP = user; Dest IP = 10.252.1.20

Ref: Module 8 slide 8 for examples for Aliases

Packets follow first rule match.

a) Permit due to statement 4. The dst address is within the scope of the subnet.

b) Deny due to the implicit deny at the end of the policy. The packet does not match any other rules.

c) Permit due to statement 6. This frame is included in the alias dns-srv.

5/2. When are the key words "user" and "any" used?

Ref: Module 8 slide 11

user: Used in place of the IP address of the connected user. The user must have an IP address for this system-defined alias to work.

any: Means any device with or without an IP address

6/1 What does the blacklisting feature do?

Ref: Module 8 slide 33

i) De-authenticate client from the network

ii) Block user from further associations during the blacklisting period

iii) Block user from associating to other SSIDs on the wireless network.

7/1 What does the "Show References" button under the Roles tab do?

Ref: Module 9 slide 7

It shows where the Role is used in the configuration. (i.e. AAA Profile).