Lab Documentation: Firewall Authentication (Lab 4)

Objective of the Lab

The goal of this lab is to configure FortiGate to communicate with a remote LDAP server for server-based password authentication. Additionally, you will set up a captive portal to prompt network users for their login credentials, enabling active authentication.

Topology

The lab involves the following network components:

- FortiGate Firewall (Local-FortiGate)
- FortiAuthenticator configured as an LDAP server
- Client machine for accessing the network and testing authentication

Network Topology:

- LDAP Server IP Address: 10.0.1.150
- Local-FortiGate IP Address: 10.0.1.254

Components Used

1. Local-FortiGate GUI: Used for configuration and management.
2. LDAP Server: Acts as the remote authentication source.
3. Remote Users: Preconfigured Active Directory (AD) user group 'AD_users', including two users: 'aduser1' and 'aduser2'.
4. Web Filter: Preconfigured to block specific categories, such as Potentially Liable, Adult/Mature Content, and Security Risk.
5. Firewall Policies: Used to control network access and enforce authentication.

Steps of the Lab

1. Prerequisites:

- Restore the Local-FortiGate configuration file.

  1. Log in to the Local-FortiGate GUI (admin/password).
  2. Navigate to Configuration > Revisions.
  3. Revert to the configuration labeled 'local-firewall-authentication'.
  4. Reboot the device.

2. Configure the LDAP Server:

- Log in to the Local-FortiGate GUI.
- Go to User & Authentication > LDAP Servers and click Create New.
- Configure the server with the provided parameters.

3. Assign LDAP User Group to a Firewall Group:

- Navigate to User & Authentication > User Groups.
- Edit the 'Remote-users' firewall group.
- Add 'AD_users' from the LDAP server to the group.

4. Add Remote User Group to Firewall Policy:

- Navigate to Policy & Objects > Firewall Policy.
- Edit the existing port3 to port1 firewall policy.
- Set the source to 'Remote-users', enable Web Filter, and configure logging options.

5. Authentication Configuration:

- Enable captive portal functionality for active authentication.

Testing the Lab

1. LDAP Authentication:

- Use the CLI to test authentication:

diagnose test authserver ldap External_Server aduser1 Training!

- Verify a successful authentication message.

2. User Login via Captive Portal:

- Open a browser on the Local-Client VM and visit elite-hackers.com.
- Enter credentials (aduser1/Training!) when prompted.
- Verify access is denied due to the web filter policy.

3. Monitoring Active Authentications:

- Go to Dashboard > Users & Devices > Firewall Users in the Local-FortiGate GUI.
- Confirm aduser1 appears as an authenticated user.
- Deauthenticate the user if necessary.

Results

1. Successfully configured FortiGate to use a remote LDAP server for authentication.

2. Verified that users in the 'AD_users' group are prompted for login credentials via the captive portal.

3. Confirmed network access restrictions are enforced based on firewall policies and web filters.

4. Monitored and managed user authentication sessions effectively.