VPN Spoofing Attack Tree

Designed by Abdelaziz El-Sheikh

Attack Tree 01 - Higher Level View

Grant Access to the Staff Web Portal through a VPN

Gain Authorized Access

- Obtain valid User Credentials (AT-01-1)
- Bypass Multi-Factor Authentication (AT-01-2)
- Access the Web Portal through the VPN (AT-01-3)

Spoof VPN Client

- Create a malicious VPN Client Application (AT-01-4)
- Obtain valid VPN client Credentials (AT-01-5)
- Compromise a legitimate VPN client device (AT-01-6)

Manipulate VPN Server

- Exploit Vulnerabilities in the VPN Server Software (AT-01-7)
- Gain unauthorized access to the VPN server Configuration (AT-01-8)
- Compromise the VPN Server Operating System (AT-01-9)

Malware

- Credential Stealers (AT-02-1)
- Spyware (AT-02-2)
- Key Logging (AT-02-3)

Brute-Force Attack

- Dictionary Attack (AT-02-4)
- Credential Stuffing (AT-02-5)

Social Engineering

- Baiting (AT-02-6)
- Shoulder Surfing (AT-02-7)
- Phishing (AT-02-8)

Legend

Shape	Description
▭	Scenario
⌓	AND
⌃	OR
—	Connector