Workbook: LAB_Autenticazione_802.1X_con_Windows_NPS

1. Obiettivo del Laboratorio

Questo laboratorio ha lo scopo di implementare e testare un'architettura di sicurezza per il controllo degli accessi alla rete cablata (NAC) utilizzando lo standard **IEEE 802.1X**.

L'obiettivo è configurare uno switch Cisco affinché agisca come "Authenticator", bloccando l'accesso fisico alla porta di rete fino a quando il dispositivo collegato ("Supplicant") non fornisce credenziali valide, verificate da un server centrale ("Authentication Server") tramite protocollo RADIUS.

Alla fine del laboratorio sarai in grado di:

- Installare e configurare il ruolo NPS (Network Policy Server) su Windows Server.
- Configurare AAA (Authentication, Authorization, Accounting) e 802.1X su switch Cisco.
- Configurare un client Windows per l'autenticazione LAN.
- Verificare il processo di autenticazione e lo sblocco della porta.

2. Prerequisiti

- **Piattaforma:** PNetLab.
- **Switch:** 1x Cisco IOL L2 (es. i86bi_linux-l2-adventerprisek9).
- **Server:** 1x Windows Server 2012 R2 (con ruolo NPS installato).
- **Client:** 1x Windows 10 Tiny o Windows XP.

3. Piano di Indirizzamento IP

Useremo la subnet **192.168.1.0/24** come VLAN di gestione e servizio.

Dispositivo	Ruolo	Interfaccia	Indirizzo IP	Subnet Mask	Gateway
SRV-RADIUS	Auth Server	Ethernet0	192.168.1.10	255.255.255.0	-
SW-AUTH	Authenticator	VLAN 1	192.168.1.254	255.255.255.0	-
PC-CLIENT	Supplicant	Ethernet0	192.168.1.20	255.255.255.0	192.168.1.254

4. Piano di Cablaggio

Dispositivo A	Interfaccia A	Dispositivo B	Interfaccia B	Descrizione
SW-AUTH	Ethernet0/0	**PC-CLIENT**	Ethernet0	Porta controllata (802.1X)
SW-AUTH	Ethernet0/1	**SRV-RADIUS**	Ethernet0	Link al server RADIUS

5. Fasi di Configurazione

Fase 1: Preparazione del Server (Windows Server)

Obiettivo: Preparare il server con indirizzo statico e installare il servizio NPS.

1. **Configurazione IP:**
   - Accedi alla console di Windows Server.
   - Assegna l'IP statico 192.168.1.10 alla scheda di rete.
   - Disabilita il Firewall di Windows (per semplificare il lab) o crea una regola per permettere il traffico UDP porte 1812 e 1813.
2. **Installazione Ruolo NPS:**
   - Apri "Server Manager".
   - Clicca su "Add roles and features".
   - Seleziona il ruolo **"Network Policy and Access Services"**.
   - Completa l'installazione.
3. **Configurazione NPS (RADIUS):**
   - Apri la console "Network Policy Server" (da Tools).
   - **Aggiungi Client RADIUS:**
     - Vai su *RADIUS Clients and Servers* -> *RADIUS Clients*.
     - Nuovo Client:
       - **Friendly Name:** SW-AUTH
       - **Address (IP):** 192.168.1.254 (L'IP dello switch)
       - **Shared Secret:** Cisco123 (Ricorda questa password!)
   - **Crea Policy di Connessione:**
     - Crea una nuova "Network Policy".
     - **Condition:** User Groups (aggiungi "Domain Users" o crea un utente locale se non sei in dominio).
     - **Permission:** Access granted.
     - **Authentication Method:** EAP-MSCHAP v2 (o PEAP).

Fase 2: Configurazione dello Switch (Cisco IOL)

Obiettivo: Configurare la connettività di base e attivare 802.1X.

1. **Configurazione Base e IP:**
```
Cisco CLI
hostname SW-AUTH
!
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
 no shutdown
!
! Verifica ping verso il server
do ping 192.168.1.10
```

2. **Configurazione AAA e RADIUS:**
```
Cisco CLI
! Attiva il modello AAA
aaa new-model
!
! Definisce il server RADIUS (l'IP del server Windows)
radius server NPS
 address ipv4 192.168.1.10 auth-port 1812 acct-port 1813
 key Cisco123
!
! Crea il gruppo AAA che punta al server
aaa group server radius RADIUS-GROUP
 server name NPS
!
! Definisce la lista di autenticazione 'dot1x' usando il gruppo
RADIUS
aaa authentication dot1x default group RADIUS-GROUP
```

3. **Attivazione 802.1X:**
```
Cisco CLI
! Attiva 802.1X globalmente
dot1x system-auth-control
!
! Configura la porta verso il Client (e0/0)
interface Ethernet0/0
 description Link-to-PC-Client
 switchport mode access
```

```
 !
 ! Attiva l'autenticazione sulla porta
 authentication port-control auto
 dot1x pae authenticator
!
! (Opzionale) Configura la porta verso il Server (e0/1) come
normale access
interface Ethernet0/1
 description Link-to-Radius-Server
 switchport mode access
```

Fase 3: Configurazione del Client (Windows PC)

Obiettivo: Abilitare il servizio "Wired AutoConfig" e configurare le credenziali.

1. **Attiva Servizio 802.1X:**
   - Apri services.msc (Servizi).
   - Trova il servizio **"Wired AutoConfig"** (Configurazione automatica reti cablate).
   - Impostalo su "Automatico" e avvialo.

2. **Configura Scheda di Rete:**
   - Vai su "Connessioni di Rete" -> Tasto destro sulla scheda Ethernet -> Proprietà.
   - Ora dovresti vedere una tab chiamata **"Authentication"** (Autenticazione).
   - Abilita "Enable IEEE 802.1X authentication".
   - Scegli il metodo di rete (es. Microsoft: Protected EAP o PEAP).
   - Nelle impostazioni aggiuntive, disabilita la verifica del certificato server (per semplicità di lab).
   - Clicca su "Additional Settings" -> "Replace credentials" e inserisci Username e Password dell'utente creato sul Server (es. Administrator).

Fase 4: Verifica Finale

1. **Collega il cavo (o riavvia l'interfaccia):**
   - Su Switch: `interface e0/0 -> shutdown -> no shutdown`
2. **Controlla lo Switch:**
   - `show dot1x interface Ethernet0/0 details`
   - Dovresti vedere Status: AUTHORIZED e l'username del client.
3. **Test Ping:**
   - Dal PC Client, prova a pingare il server (192.168.1.10). Se risponde, la porta è sbloccata.

6. Diagramma di Rete