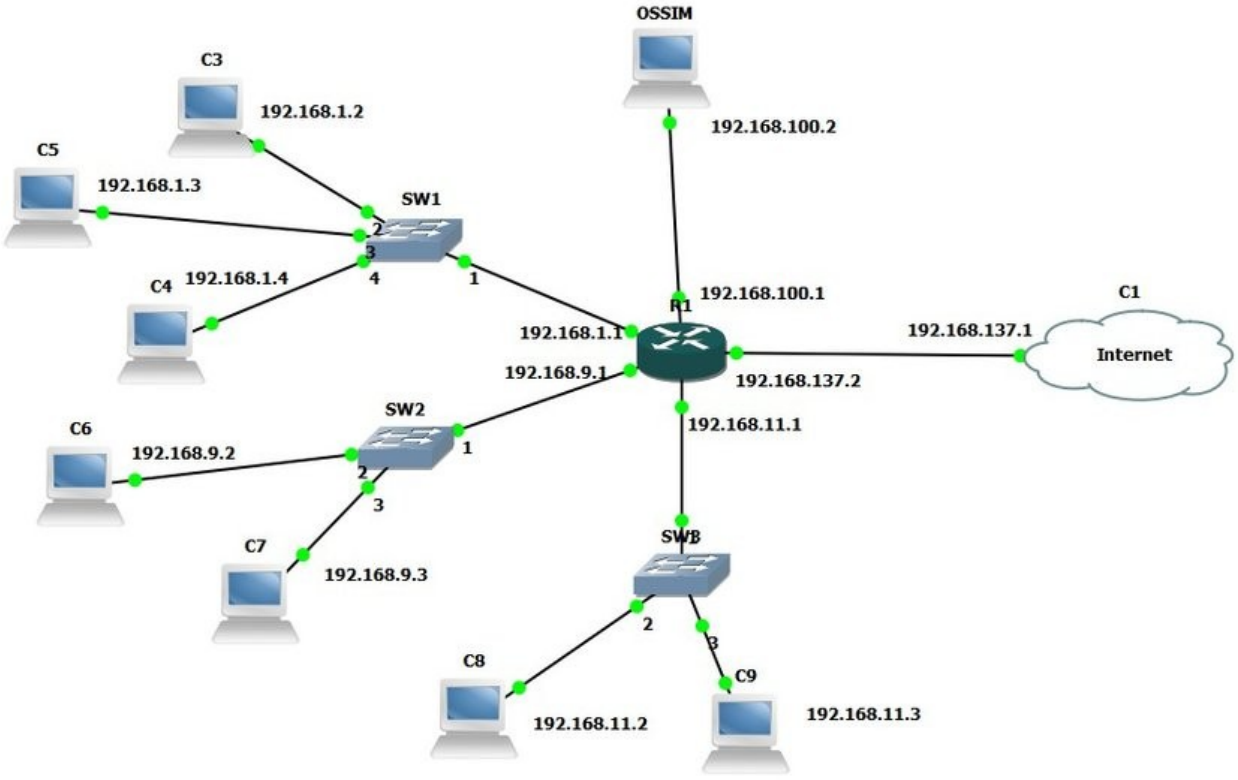
CdLM Ingegneria Informatica
Indirizzo cyber security

NETWORK SECURITY



AAA - RADIUS SERVER

Radius (*Remote Authentication Dial-In User Service*):

- un servizio dedicato ai meccanismi di autenticazione, autorizzazione ed accounting.
- implementa un protocollo standard
- permette l'autenticazione di numerose applicazioni e dispositivi di rete:
  - modems, DSL, access points, VPNs, network ports, web servers.

CISCO

Microsoft
Network Policy Server

AAA - RADIUS SERVER

Radius si occupa solo dei meccanismi AAA, non dispone di un proprio database.

- può appoggiarsi a servizi esterni:
- LDAP, SQL, Active Directory, eDirectory o file di testo.

- Negli ISP (Internet Service Provider) si usa RADIUS per:
  - autenticare gli accessi alla propria rete
  - definirne i parametri di funzionamento come il limite di banda grazie al sistema di autorizzazione del protocollo AAA.

AAA - RADIUS SERVER

Tra i meccanismi di autorizzazione usati da RADIUS il più frequente è la gestione del protocollo 802.1x per l'accesso fisico alle porte rete IEEE 802 cioè cablate o wireless.

- Per una rete cablata può essere sufficiente il controllo dell'accesso ai locali dove sono presenti le prese di rete
- nel caso wireless la rete si estende un modo difficilmente controllabile anche all'esterno dell'area di pertinenza.
- meccanismi di accesso:
  - l'uso di una password condivisa e conosciuta (pre shared Key)
  - attraverso servizi di autenticazione come RADIUS.

AAA - RADIUS SERVER

- Lo standard 802.1x:
- propone una struttura di supporto architetturale di autenticazione versatile attraverso l'utilizzo di protocolli esistenti
- EAP (Extensible Authentication Protocol).
- 802.1x, EAP ed altri protocolli definiscono nei dettagli il meccanismo di autenticazione
- La soluzione 802.1x, con l'uso di RADIUS, si presta bene ad applicazioni di mobilità e l'autenticazione su vari access point.

AAA - RADIUS SERVER

Processo di autenticazione:

- un nodo si connette ad una rete protetta ma non è in grado di fare alcuna operazione, nemmeno fare richieste DHCP.

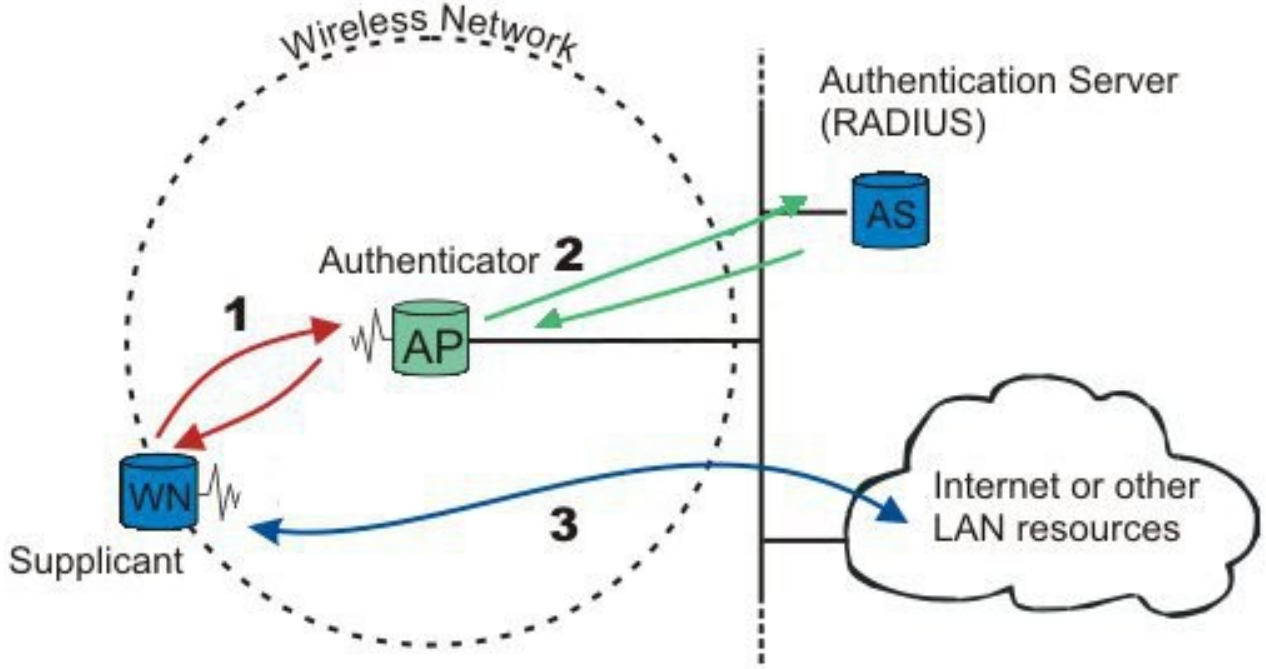
- Per perfezionare la connessione:
  - il nodo invia una richiesta di autenticazione
  - la richiesta è intercettata dallo switch o dall'access point, al quale il nodo è connesso.
  - la richiesta non può essere inoltrata direttamente al server di autenticazione (il RADIUS).
  - Fa da tramite l'autenticatore, cioè ancora lo switch o l'access point.
  - Se l'autenticazione va a buon fine la porta alla quale il dispositivo è collegato, viene abilitata al traffico di rete.

AAA - RADIUS SERVER

- L'identità del nodo e del server di autenticazione è importante per la sicurezza, fra i diversi metodi implementati da EAP:
  - EAP-MD5
  - Lightweight EAP
  - EAP-TLS
  - EAP-TTLS
  - Protected EAP -PEAP
  - EAP-MSCHAPv2
- diversi metodi fanno uso di certificati X.509 per garantire l'identità del server e del nodo che accede alla rete
- Si evitano attacchi del tipo man in middle (dispositivo estraneo alla rete che viene interposto ed usato per intercettare dati)

AAA - RADIUS SERVER

- Il meccanismo di connessione tramite server Radius



AAA - Autenticazione, Autorizzazione e Accounting

- I processi di Autenticazione, Autorizzazione e Accounting
- fondamentali per la sicurezza aziendale e non

- attività AAA tutelano
  - l'accesso ai dati
  - l'accesso fisico ai locali
  - l'uso di risorse in genere

AAA - Autenticazione, Autorizzazione e Accounting

IT manager

- (troppo spesso) unico responsabile della sicurezza di accesso alle risorse
- gestore delle risorse utilizzate nelle attività aziendale

- login di un utente
  - piccola parte di un processo ampio e complesso

- username e password utente:
  - accesso a file system condivisi
  - al sistema ERP,
  - posta elettronica portale web aziendale

AAA - Autenticazione, Autorizzazione e Accounting

Integrazione di reti pubbliche e private

- globalizzazione informatica facilitazione del lavoro e dello scambio di informazioni
- aggravio il problema della sicurezza.
- autenticazione forte o a più fattori
- password complesse con cambi periodici
- token
- smartcard
- cellulare
- caratteristiche biometriche

I tre fattori sono noti come il segreto, il possesso e l'essere: quello che so, quello che possiedo e quello che sono).

AAA - Autenticazione, Autorizzazione e Accounting

aaA -Accounting

- consente di tracciare l'utilizzo delle risorse
- chi ha fatto cosa.
- Importante a livello legale (L. 133/200 del 27 Novembre 2008)
- requisiti di legge minimi richiesti
- correlare dati per scoprire se un account ha fatto accessi in orari o da luoghi non attesi
- verifica di azioni sospette (accesso da una rete pubblica di un utente che risulta, dalla timbratura cartellini, presente in azienda.
- La complessità da superare data dalla disomogeneità dei dati raccolti
- log in formato testo con tracciati record proprietari, difficilmente leggibili e voluminosi.
- procedure in grado di armonizzare i dati in formati univoci e in grado di correlare fonti differenti
- "non ripudiabilità dei dati", azione richiesta per legge
- forma di memorizzazione, in genere attraverso una firma lettronica, per garantire la veridicità dei dati ovvero che i dati non sono stati manomessi.

AAA - Autenticazione, Autorizzazione e Accounting

aAa .Autorizzazione

- integrata con l'autenticazione
- riconosciuto l'utente accerta che possa accedere alle sole risorse di competenza.
  - Le informazioni necessarie per questo processo sono strettamente legate all'applicativo e alle prestazioni dello stesso
  - Un file system
    - NTFS
    - EXT4
  - posta elettronica
  - portale web

- Ridurre la complessità della definizione dei permessi
  - non dare permessi all'utente
  - consentire l'eredità in base all'appartenenza a gruppi definiti con criteri funzionali.
  - Il gruppo avrà i permessi per accedere alla risorsa.
  - numero di gruppi sia inferiore al numero di utenti
  - abbinare il permesso ad una funzione e non ad un utente.
  - profili e di appartenenza ad un profilo
  - gruppi integrati e gestiti attraverso directory, meccanismi descritti nella autenticazione

AAA - Autenticazione, Autorizzazione e Accounting

Aaa - Autenticazione

- Ha lo scopo di riconoscere l'utente., uso di una username, in genere pubblica, e di una password, il segreto
- Garantire la sicurezza la password
  - politiche di complessità
  - di cambio periodico
  - di segretezza.
- sensibilizzare l'utente all'importanza della procedura di autenticazione.
- risorse di autenticazione come le directory facilmente riutilizzabili e integrabili con processi aziendali, riduzione di fonti di autenticazione
- uso di procedure di Single Sign-On o gestione identità, favoriscono i processi di gestione delle utenze.
- Active Directory eDirectory o database relazionali come SQL Server mySQL OpenLDAP
- Meccanismo di autenticazione fa ricorso ad un directory per memorizzare i dati dell'utente
- directory è un database a struttura gerarchica, non relazionale, normalmente ottimizzato per essere letto
- Un DB è formato da tabelle a campi fissi ed è ottimizzato per operazioni di lettura e scrittura in ugual misura
- Un'unica fonte di autenticazione non riduce il numero di autenticazioni, legato al numero di applicazioni a
- cui si deve accedere, consente di avere una unica identità, quindi una sola username ed una sola password.

AAA – Server RADIUS

- Server Radius

- Esistono diverse implementazioni per un server RADIUS, fra le più usate il
  - RADIUS Cisco
  - Microsoft NPS (Network Policy Server)
  - FreeRADIUS, una applicazione open source.

- FreeRADIUS è quindi
  - liberamente scaricabile dal sito http://freeradius.org/
  - pacchettizzato e disponibile nelle varie distribuzioni.
  - In rete si trovano anche la descrizione delle più comuni configurazioni.

AAA - Server RADIUS

Installare FreeRADIUS ed il web frontend Daloradius su Ubuntu / Debian

```
sudo apt update
sudo apt -y upgrade
sudo reboot
```

- Step 1: Apache

```
sudo apt -y install apache2
sudo apt -y install php libapache2-mod-php php-{gd,common,mail,mail-mime,mysql,pear,db,mbstring,xml,curl}
```

```
$ php -v
PHP 7.2.19-0ubuntu0.18.04.2 (cli) (built: Aug 12 2019 19:34:28) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologieswith Zend OPcache v7.2.19-0ubuntu0.18.04.2, Copyright (c) 1999-2018, by Zend Technologies
```

AAA - Server RADIUS

Step 2: MariaDB

```
sudo apt -y install mariadb-server
mysql_secure_installation
```

database name: radius

database user: radius

database user password: radiuspassword

```
$ mysql -u root -pCREATE DATABASE radius;GRANT ALL ON radius.*
TO radius@localhost IDENTIFIED BY "radiuspassword";FLUSH
PRIVILEGES;quit
```

Step 3: FreeRADIUS

```
sudo apt -y install freeradius freeradius-mysql freeradius-utils
```

AAA - Server RADIUS

- Step 4: Configurazione Freeradius

```
sudo su
mysql -u root -p radius < /etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
mysql -u root -p -e "use radius;show tables;"

sudo ln -s /etc/freeradius/3.0/mods-available/sql /etc/freeradius/3.0/mods-enabled/

sudo nano /etc/freeradius/3.0/mods-enabled/sql
```

AAA – Server RADIUS

```
sql {
driver = "rlm_sql_mysql"
dialect = "mysql"

# Connection info:
server = "localhost"
port = 3306
login = "radius"
password = "radiuspassword"

# Database table configuration for everything except Oracle
radius_db = "radius"
}

# Set to 'yes' to read radius clients from the database ('nas' table)
# Clients will ONLY be read on server startup.
read_clients = yes

# Table to keep radius client info
client_table = "nas"
```

AAA - Server RADIUS

```
sudo chgrp -h freerad /etc/freeradius/3.0/
mods-available/sql

sudo chown -R freerad:freerad
/etc/freeradius/3.0/mods-enabled/sql

sudo systemctl restart freeradius.service
```

Step 5: Daloradius

```
wget https://github.com/lirantal/daloradius/archive/master.zip

unzip master.zip

mv daloradius-master daloradius

cd daloradius

mysql -u root -p radius < contrib/db/fr2-mysql-daloradius-and-freeradius.sql

mysql -u root -p radius < contrib/db/mysql-daloradius.sql

cd ..
```

AAA - Server RADIUS

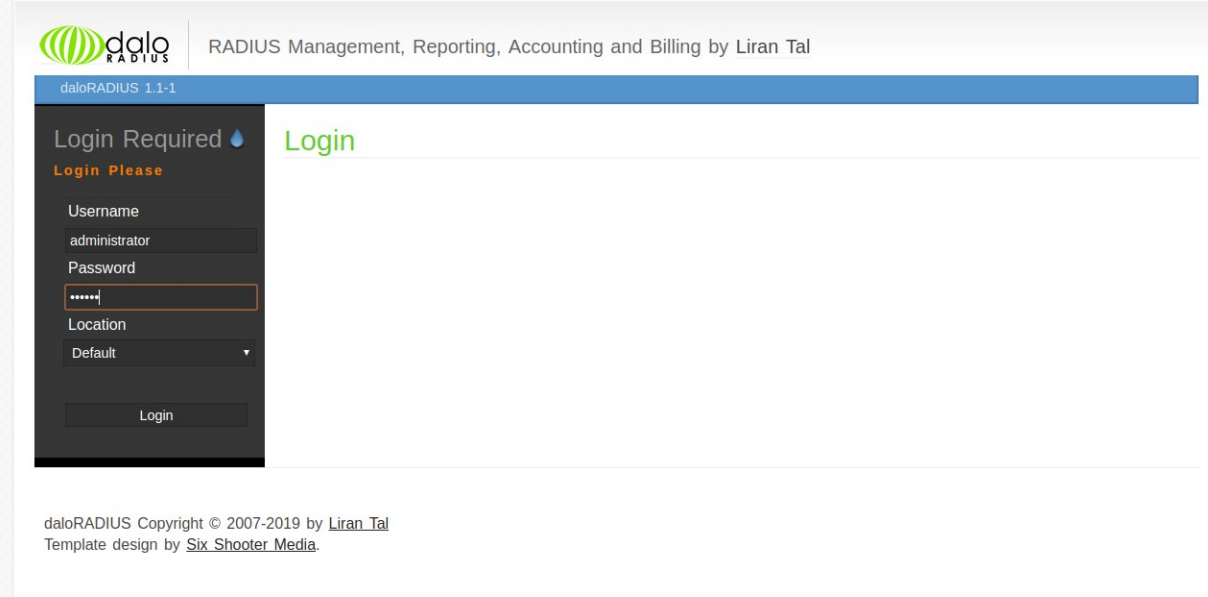
```
sudo mv daloradius /var/www/html/
sudo chown -R www-data:www-data /var/www/html/daloradius/
sudo chmod 664
/var/www/html/daloradius/library/daloradius.conf.php

sudo nano /var/www/html/daloradius/library/daloradius.conf.php

$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = 'radiuspassword';
$configValues['CONFIG_DB_NAME'] = 'radius';

sudo systemctl restart freeradius.service apache2
```

AAA – Server RADIUS

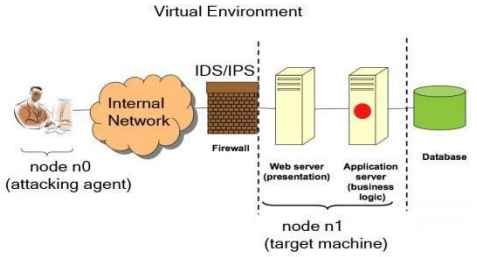
http://ip-address/daloradius/login.php

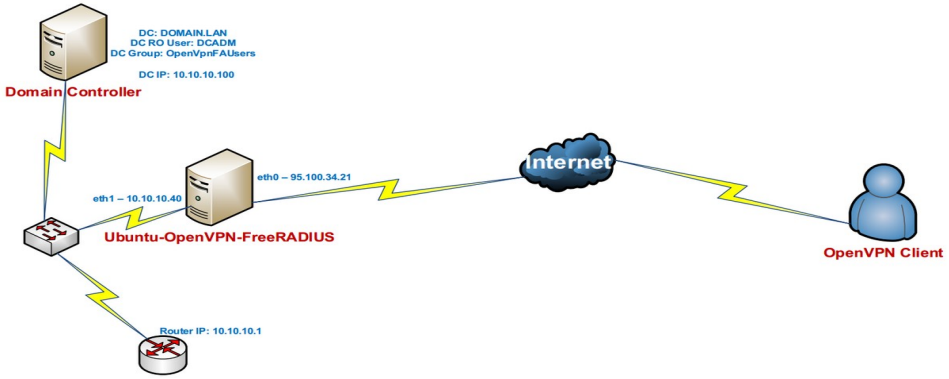
- Default login details:
  Username: administrator
  Password: radius

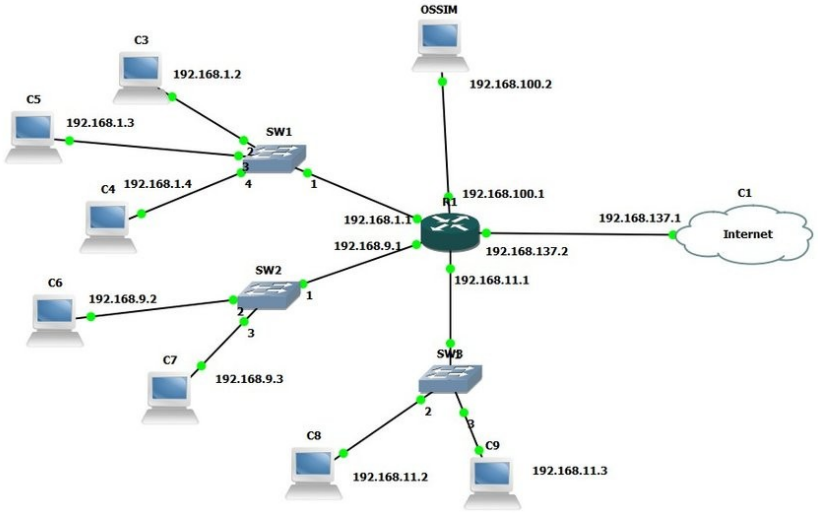
- Cambiare la password
- dopo il primo login.

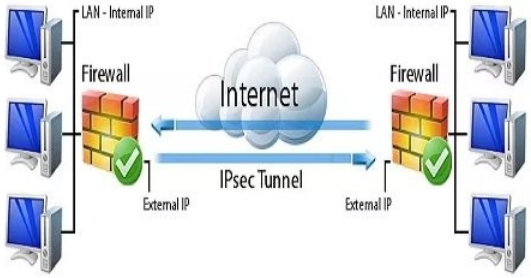



DATA PROTECTION
COMPUTER
CYBER SECURITY
NETWORK SECURITY
DEVICES


Virtual Environment
IDS/IPS
Internal Network
Firewall
Database
Web server (presentation)
Application server (business logic)
node n0
(attacking agent)
node n1
(target machine)


DC: DOMAIN.LAN
DC RO User: DCADM
DC Group: OpenVpnFAUsers
DC IP: 10.10.10.100
Domain Controller
eth1 – 10.10.10.40
eth0 – 95.100.34.21
Ubuntu-OpenVPN-FreeRADIUS
Internet
OpenVPN Client
Router IP: 10.10.10.1


OSSIM
192.168.100.2
C3
192.168.1.2
C5
192.168.1.3
SW1
C4
192.168.1.4
R1
192.168.100.1
192.168.1.1
192.168.137.1
C1
Internet
192.168.9.1
192.168.137.2
SW2
C6
192.168.9.2
192.168.11.1
C7
192.168.9.3
SW3
C8
192.168.11.2
C9
192.168.11.3


LAN - Internal IP
LAN - Internal IP
Firewall
Internet
Firewall
IPsec Tunnel
External IP
External IP


NETWORK SECURITY

La saggezza vi darà la morale,
La conoscenza vi darà la verità,
La verità vi darà libertà,
La conoscenza libera vi darà la saggezza ….

GRAZIE PER L'ATTENZIONE