TIEA222 Tietoturva, laboratoriotyö 2
IEEE 802.1X/RADIUS + Captive Portal

Joel Lehtonen et al.

15.9.2010, v1.2

1 Johdanto

Tietoturvavaatimusten kasvu ja 802.11-verkkojen yleistyminen sekä heikko tietoturva ovat luoneet todellisen tarpeen 802.1X:n kehittämiselle. Lähiverkkojen datasiirto on siirtynyt fyysisestä siirtotiestä käyttämään radiotaajuuksia, jolloin verkkoon pääsyä ei voida rajata tiettyyn fyysiseen pisteeseen. Tästä syystä verkkojen omistajatahoilla on syntynyt selkeä tarve kontrolloida verkkoon pääsyä, koska kuka tahansa pystyy hyödyntämään langattoman verkon resursseja kytkemällä WLAN-verkkokortin tietokoneeseen ja kytkeytymään verkkoon ollessaan tukiaseman kantomatkan sisäpuolella. Sama ongelma on myös langallisen IEEE 802 -verkon liityntäpisteissä, jotka sijaitsevat julkisissa tiloissa.

Koska kytkimen portti tai langattoman verkon liityntäpiste (AP) toimii käyttäjälle lähiverkon pääsykohtana, on se luonnollinen paikka kontrolloida verkkoon pääsyä sekä suodattaa datavirrasta protokollia ja paketteja.

Monet organisaatiot ovat kyllästyneet hajautettuihin käyttäjätietokantoihin. Internet-palveluiden lisääntyessä operaattorit ovat joutuneet kasvattamaan soittosarjojen ja palveluiden lukumäärää, jonka seurauksena käyttäjätunnus- ja salasanatietokantoja on jouduttu monistamaan ja niitä on useita. Käyttäjätunnusten ja salasanatietokantojen hallinnointi on paisunut mahdottomaksi, jonka takia organisaatiot ovat tarvinneet keskitetyn käyttäjätunnusten hallinnoinnin. Tämä on tarkoittanut investointeja Authentication, Authorization ja Accounting (AAA-protokolla) -palvelun toteuttaviin protokolliin. Eräs tunnetuimmista protokollista on Remote Authentication Dial-In User Service (RADIUS). Avainidea on tuottaa yksi keskitetty tietokanta, jonka avulla käyttäjät voidaan tunnistaa turvallisesti kaikissa olosuhteissa, jossa AAA-protokollat kuljettavat verkon reunalta autentikointiliikenteen turvallisesti verkon autentikointipalvelimelle.

Pian langattomien verkkojen julkaisun jälkeen, niiden ensimetreillä, todettiin langattoman verkon Wireless Encryption Protocol (WEP) -protokollan suojauksen purun olevan helppoa. WEP:n tarkoitus oli turvata päätelaitteen ja liityntäpisteen välinen dataliikenne. Protokollan toteutus oli heikko ja siinä ei ollut ominaisuuksia, jolla salausavaimien jakelu ja hallinnointi olisi voitu toteuttaa helposti. Monet tahot ovat esittäneet 802.1X:n tavaksi jolla avainten jakelu voidaan toteuttaa turvallisesti liityntäpisteelle ja päätelaitteille. [1]

2 Esitehtävät

Vastaa näihin kysymyksiin ennen laboratorioon tuloasi. Näytä vastaukset assistentille ennen työn aloittamista. Lähetä näidenkin kysymysten vastaukset muiden kysymysten vastausten kanssa ohjeen lopussa olevien ohjeiden mukaisesti.

Q1: Tutustu IEEE 802.1X -standardiin ja kerro lyhyesti sen tarkoituksesta.

Q2: Tutustu RADIUS-protokollaan ja kerro lyhyesti sen tarkoituksesta.

Q3: Mikä on Captive Portal ja miten se toimii?

Q4: Miten toteuttaisit mahdollisimman käyttäjäystävällisen ja mielellään mahdollisimman automaattisen verkon käyttäjien tunnistamisen, joka mahdollistaisi erilaisten päätelaitteiden, kuten tietokoneen, matkapuhelimen ja PDA:n verkkoon kirjautumisen?

Tutustu myös työssä käytettyyn pfSense [2] -palomuuriohjelmistoon ja HP ProCurve -kytkimen ohjekirjaan [3], jos ne eivät ole ennestään tuttuja. HP ProCurve -kytkimen ohjekirjasta kannattaa tutustua erityisesti Command Line Interfacen käyttöön.

3 Laboratoriotyön kuvaus

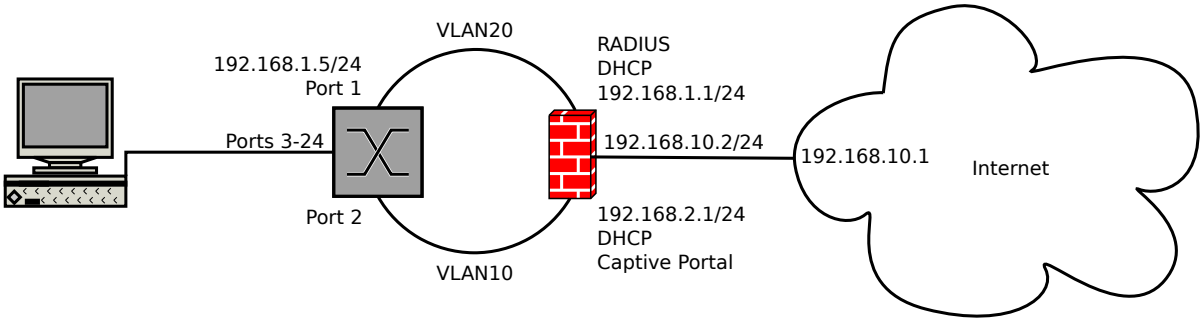
Laboratoriotyössä tutustutaan RADIUS-palvelimeen, IEEE 802.1X porttikohtaiseen ja Captive Portal WWW-pohjaiseen tunnistautumiseen sekä näiden toteuttamiseen laboratorioympäristössä.

Laboratoriossa on valmiina verkkoympäristö, jonka kautta kuka tahansa käyttäjä pääsee verkkoon. Riittää, että pääsee kiinni verkkolaitteeseen, joka tässä työssä on tavallinen Ethernet-kytkin. Kytkimen tilalla voit ajatella käytettävän myös WLAN-tukiasemaa, jolloin verkkoon liittyminen on vielä helpompaa. Tällaisessa avoimessa verkossa käyttäjien hallinnointi on hyvin hankalaa, ja siksi halutaan ottaa käyttöön järjestelmä, joka pystyy tunnistamaan verkkoa käyttävän käyttäjän.

Tässä työssä keskitytään vain käyttäjän tunnistamiseen keskitetysti ja jätetään huomioimatta käyttäjän muu seuranta.

3.1 Konfiguroi pfSense-palomuuriohjelma

Käytä kuvaa 1 apunasi ja konfiguroi pfSense-palomuuriohjelmaan palomuurin verkkoliitännät, DHCP-palvelut sisäverkon verkkoliitännöille sekä Radius-palvelin. Palomuuriin on valmiiksi jo osa asetuksista määritelty, joten sinun ei välttämättä tarvitse kaikkia asetuksia erikseen määritellä.



Kuva 1: Laboratorioverkon topologia.

Palomuuria pääset konfiguroimaan menemällä osoitteeseen http://192.168.1.1 . Tunnus on admin ja salasana on pfsense. Kun konfiguroit asetuksia palomuuriin, muista aina tallentaa tekemäsi asetukset! Jossain tapauksissa sinun pitää vielä erikseen painaa Apply Changes -nappia. PfSense ilmoittaa tästä aina tarvittaessa.

3.1.1 Konfiguroi verkkoliitännät

PfSensen WWW-käyttöliittymästä verkkoliitännät konfiguroidaan Interfaces-valikon kautta. Sinulle on valmiiksi jo luotu olemassa olevat verkkoliitännät (WAN, LAN, OPT1). Lisäksi WAN (192.168.10.2) ja LAN (192.168.1.1) -verkkoliitännät on myös jo valmiiksi myös konfiguroitu. Sinun tehtävänä on konfiguroida OPT1-verkkoliitäntä.

Ota OPT1-verkkoliitäntä käyttöön ja määrittele sille staattinen IP-osoite 192.168.2.1/255.255.255.0. Asetussivulla "Bridge with" jätetään arvoon "none".

3.1.2 Konfiguroi DHCP-palvelut

DHCP-palvelut konfiguroidaan Services → DHCP server -kohdan kautta.

LAN-verkkoliitännälle DHCP-palvelu on jo konfiguroitu. Käytä sitä hyväksesi ja konfiguroi OPT1-verkkoliitännälle DHCP-palvelu. Aseta IP-osoitealueeksi 192.168.2.100-192.168.2.199.

3.1.3 Konfiguroi palomuurisääntöjä

Nyt sinulla pitäisi olla toimiva OPT1-verkkoliitäntä, josta saa DHCP:llä haettua automaattisesti IP-osoitteen. Palomuurissa ei ole kuitenkaan olemassa sääntöjä OPT1-verkkoliitännälle, joten oletuksena kaikki sen liikenne estetään.

Palomuurisääntöjä konfiguroidaan Firewall → Rules -kohdan kautta. Ota mallia LAN-verkkoliitännälle luodusta, kaiken sallivasta palomuurisäännöstä ja luo vastaava OPT1-verkkoliitännälle.

Kun olet tallentanut asetukset, muista painaa Apply Changes -nappia, että asetukset otetaan käyttöön.

3.1.4 Konfiguroi RADIUS-palvelu

PfSense käyttää RADIUS-palvelimena FreeRADIUS [4] -nimistä vapaan lähdekoodin (GPLv2) ohjelmistoa, jota kuvataan sen omilla projektisivuillaan maailman suosituimmaksi RADIUS-palvelimeksi. Se on saatavilla lähdekoodeineen tai kolmansien osapuolten kautta myös valmiiksi paketoituna useille käyttöjärjestelmille (Linux, BSD, Mac OSX, Windows).

RADIUS-palvelua pääsee konfiguroimaan Services → FreeRADIUS -kohdan kautta. RADIUS-palveluun sinun tulee konfiguroida uusi käyttäjä, uusi RADIUS-asiakas sekä palvelimen yleisiä asetuksia.

Luo uusi käyttäjä (Users-välilehti), ja määrittele käyttäjälle haluamasi käyttäjänimi ja salasana. PfSense vaatii lisäksi täyttämään kentän "Number of Multiple connections", laita siihen joku järkevä arvo. Katso muut kohdat läpi ja tallenna käyttäjäsi.

Luo seuraavaksi uusi RADIUS-asiakas (Clients-välilehti). RADIUS-asiakas on verkkolaite, joka haluaa todentaa käyttäjän RADIUS-palvelinta vasten. Tässä laboratoriotyössä RADIUS-asiakkaana toimii käyttämäsi kytkin. Vaikka kytkintä ei ole vielä konfiguroitu, voit silti jo luoda sitä varten RADIUS-asiakkaan palvelimelle. Anna RADIUS-asiakkaan IP-osoitteeksi kytkimelle tuleva IP-osoite (192.168.1.5), vapaavalintainen, verkkolaitetta kuvaava lyhytnimi sekä salasana, jolla RADIUS-asiakas tunnistautuu RADIUS-palvelimelle.

Yleisiin RADIUS-palvelimen asetuksiin (Settings-välilehti) määrittele, että RADIUS-palvelu toimii LAN-verkkoliitännässä ja kuuntelee porttia 1812.

3.2 Konfiguroi HP ProCurve 2524 -kytkin

Käytössä on HP ProCurve 2524 -kytkin ja siihen sinun tulee konfiguroida VLAN:t ja IEEE 802.1X/Radius -tunnistautuminen. Tarkoituksena on, että kytkimen portti 1 on VLAN:ssa 20 ja palomuurin LAN-portissa, kytkimen portti 2 on VLAN:ssa 10 ja palomuurin OPT1-portissa, loput kytkimen portit 3-24 ovat portteja, joihin käyttäjät voivat tunnistautua omalla tietokoneellaan. Työn aikana sinulla ei pitäisi olla tarvetta koskea verkkojohtoihin, varsinkaan porteissa 1 ja 2 oleviin.

Kytkimen konfiguroiminen tapahtuu sarjaportin kautta. Tähän voit käyttää työpöydältä löytyvää Putty-ohjelmaa. Kun saat kytkimeen yhteyden, voi tarvita muutaman enterin painalluksen, siirry konfigurointitilaan komennolla configure. Komentokehotteen alusta näet, missä tilassa olet (config)#.

```
HP ProCurve Switch 2524# configure
HP ProCurve Switch 2524(config)#
```

Aina ajantasaisen kytkimen konfiguraation näet komennolla **show running-config**. Jos haluat poistaa jonkin määrittelyn, tapahtuu se kuten sen asettaminenkin, mutta komento aloitetaan **no** -sanalla. Lisätietoja käytettävissä olevista komennoista ja niiden parametreista saat painamalla ? (toimii myös komennon syöttämisen aikana). Nuolinäppäimillä (ylös ja alas) voit selata komentohistoriaasi ja näin mahdollisesti helpottaa komentojen antamista.

Huom! Vaikka tietäisit miten asetukset tallennetaan kytkimen muistiin, niin ÄLÄ TALLENNA tekemiäsi asetuksia!

Konfiguroi kytkimeen VLAN:t tunnistautuneille (VLAN 20) ja tunnistamattomille (VLAN 10) käyttäjille. Kytkimessä on jo valmiina oletus-VLAN, VLAN 1. Tätä ei tarvitse erikseen konfiguroida, muuten kuin poistaa siltä IP-osoite (oletus DHCP). Muista määritellä myös primary-vlan, jota kytkin käyttää omaan liikennöintiinsä esimerkiksi Radius-palvelimelle.

Osa asetuksista on oletuksena konfiguroituna, joten katso running-config ja tee vain tarpeelliset muutokset.

```
vlan 1
   name "DEFAULT_VLAN"
   untagged 3-26
   no ip address
   no untagged 1-2
   exit
vlan 20
   name "auth"
   untagged 1
   ip address 192.168.1.5 255.255.255.0
   exit
vlan 10
   name "unauth"
   untagged 2
   exit
primary-vlan 20
```

Konfiguroi Radius-palvelimen tiedot ja määritä IEEE 802.1X/Radius -pohjainen tunnistautuminen portteihin 3-24. Korvaa alla olevasta konfiguraatiosta <salasana>-kohta salasanalla, jonka määritit RADIUS-palvelimen RADIUS-asiakkaalle.

```
radius-server host 192.168.1.1 key <salasana>
aaa authentication port-access eap-radius
aaa port-access authenticator active
```

```
aaa port-access authenticator 3-24
aaa port-access authenticator 3-24 auth-vid 20
aaa port-access authenticator 3-24 unauth-vid 10
```

3.3 Konfiguroi XSupplicant

Käyttämääsi tietokoneeseen on asennettu XSupplicant-ohjelma [5], jonka avulla voi helposti kirjautua verkkolaitteelle, kun käytetään IEEE 802.1X -porttikohtaista tunnistautumista.

Ohjelma voi olla jo käynnissä, joten katso ensiksi tehtäväpalkin ilmoitusaluetta. Ilmoitusalueella pitäisi näkyä O-kirjain, jossa on aaltoja vasemmassa reunassa. Jos ohjelma ei ole käynnissä, käynnistä se Start → Programs → XSupplicant → XSupplicant Tray Application. Ohjelma aukeaa vain ilmoitusalueelle.

Avaa XSupplicant-ohjelma kaksoisklikkaamalla ilmoitusalueen kuvaketta. Aloita konfigurointi luomalla uusi profiili (Profiles). Anna profiilille haluamasi nimi, protokollaksi EAP-MD5 ja määrittele, että käyttäjätunnus ja salasana kysytään joka kerta erikseen.

Luo uusi yhteys (Connections) ja anna sille haluamasi nimi. Katso, että verkkoadapteriksi on määritelty Ethernet-kortti (esim. Intel PRO 10/100) eikä siis WLAN-kortti tms ja liitä edellä luomasi profiili tähän yhteyteen. Network ja DNS -välilehdiltä määrittele, että dynaamiset IP ja DNS -tiedot haetaan automaattisesti. Network-välilehdeltä varmista, että kohta "Renew IP information after each login" on rastitettuna. Kun olet tallentanut asetuksesi, sulje asetusikkuna.

3.4 Testaa IEEE 802.1X/RADIUS -tunnistautuminen

Käytä XSupplicant-ohjelmaa tunnistautuaksesi kytkimelle. Katso kirjautumisikkunasta, että yhteydeksi on valittu edellä luomasi yhteys ja anna tunnus ja salasana (käyttäjä, jonka teit RADIUS-palvelimelle).

Kun olet painanut Connect-nappia, eteesi tulee tilaikkuna, josta näet onnistuiko tunnistautuminen vai ei ja saamasi IP-osoite, jonka pitäisi olla muotoa 192.168.1.xxx. Jos tunnistautuminen onnistui ja pääset Internetiin, olet konfiguroinut onnistuneesti RADIUS-tunnistautumisen kytkimeen ja palomuuriin.

Voit vielä kokeilla, että olet konfiguroinut onnistuneesti palomuurin OPT1-verkkoliitännän. Pura yhteys painamalla Disconnect-nappia. Avaa komentokehote (Start → Run → cmd [enter]) ja anna seuraavat komennot.

```
C:\> ipconfig /release
C:\> ipconfig /renew
```

Sinun pitäisi saada IP-osoite, joka on muotoa 192.168.2.xxx. Jos saat oikeanlaisen IP-osoitteen ja Internet toimii, on OPT1-verkkoliitäntä konfiguroitu oikein.

3.5 Konfiguroi Captive Portal

Captive Portal on WWW-sivujen kautta toimiva tunnistautumistapa, joka ei vaadi käyttäjän laitteelta muuta tukea kuin WWW-selaimen. Tässä laboratoriotyössä on tarkoituksena, että WWW-sivulla tehty tunnistautuminen tapahtuu edelleen RADIUS-palvelinta vasten, jolloin on myös automaattisesti käytössä RADIUS-palvelimelle konfiguroidut käyttäjät.

Luo uusi RADIUS-asiakas Captive Portal -palvelua varten. Määrittele RADIUS-asiakkaan IP-osoitteeksi 192.168.1.1. Määrittele myös lyhytnimi ja salasana.

Konfiguroi pfSensestä Captive Portal -palvelu Services → Captive Portal -kohdan kautta. Määrittele, että Captive Portal toimii OPT1-verkkoliitännässä, ja varmista, että "Enable logout popup window" on rastitettu. Määrittele, että käytetään RADIUS-tunnistautumista ja konfiguroi ensisijaiseksi RADIUS-palvelimeksi konfiguroimasi RADIUS-palvelin. Katso muut kohdat läpi ja tallenna tekemäsi asetukset.

Jos Captive Portal ei tunnu toimivan, kokeile käynnistää Captive Portal -palvelu uudelleen Status → Services -kohdasta.

3.6 Testaa Captive Portal -tunnistautuminen

Jos olet konfiguroinut kaiken oikein, nyt sinun pitäisi päästä Internetiin vain joko tunnistautumalla kytkimen kautta (XSupplicant) tai tunnistautumalla WWW-sivun kautta (Captive Portal).

Testaa, että Captive Portal -tunnistautuminen toimii. Käytä XSupplicant-ohjelmaa ja anna sille väärät tunnukset ja salasanat (jos olet vielä tunnistautuneena paina disconnect-nappia), jotta tunnistautuminen kytkimen kanssa epäonnistuu. Avaa verkkoselain ja yritä mennä jollekin WWW-sivulle. Jos Captive Portal on oikein konfiguroitu, sinulle pitäisi tulla eteen kirjautumislomake. Anna kirjautumislomakkeelle käyttäjäsi tunnus ja salasana. Nyt pyytämäsi sivun pitäisi aueta.

Periaatteessa tässä ei tarvitsisi edes antaa vääriä tunnuksia XSupplicant-ohjelman kautta, mutta kyseisessä ohjelmassa on sellainen ominaisuus, että käytettäessä DHCP-palvelimia ja ohjelman disconnect-toiminallisuutta, ei uusia IP-tietoja haeta DHCP-palvelimelta disconnectin jälkeen. Tässä tapauksessa se on tarpeen, koska Captive Portal toimii eri VLAN:ssa ja eri IP-verkossa kuin IEEE 802.1X/RADIUS -tunnistautuneet käyttäjät.

3.7 Siivoa jälkesi

Ennen kuin lähdet työpisteeltäsi, poista tekemäsi asetukset palomuurista, kytkimestä ja tietokoneeltasi.

Lataa oletusasetukset pfSense-palomuuriin menemällä Diagnostics → Backup/Restore. Restore configuration -kohdasta katso, että Restore area on ALL ja hae asetustiedosto painamalla Browse... -nappia. Asetustiedosto on käyttämäsi tietokoneen työpöydällä oleva **pfsense-default.xml** -tiedosto. Lopuksi paina Restore configuration -nappia. Palomuuri lataa asetukset ja käynnistää itsensä uudelleen.

Kytkimestä saat asetuksesi poistettua antamalla uudelleenkäynnistymiskomennon **boot**. Vastaa myöntävästi uudelleenkäynnistyksen varmistuskysymykseen ja kieltävästi (no) olemassa olevien asetusten tallentamista koskevaan kysymykseen.

Lopuksi poista vielä XSupplicant-ohjelmasta tekemäsi profiili ja yhteys.

4 Kysymyksiä

Vastaa työssä esitettyjen kysymysten lisäksi alla oleviin kysymyksiin ja palauta vastauksesi viikon kuluessa sähköpostitse osoitteeseen tietoturva@zouppen.iki.fi .

Q5: Mikä oli käyttämäsi työohjeen versionumero?

Q6: Työssä käytettiin tunnistautumisprotokollana EAP-MD5. Miten se toimii ja mitä muita vaihtoehtoja tälle on? Ovatko muut vaihtoehdot tietoturvaltaan parempia ja millälailla? Tutustu ainakin EAP-TTLS ja PEAP/EAP-MSCHAPv2.

Q7: Missä tilanteissa tai paikoissa IEEE 802.1X/RADIUS -tunnistautuminen olisi käyttökelpoisin tapa tunnistaa käyttäjät?

Q8: Missä tilanteissa tai paikoissa Captive Portal -tunnistautuminen olisi käyttökelpoisin tapa tunnistaa käyttäjät?

Q9: Mitä opit tästä laboratoriotyöstä? Oliko työstä muuta hyötyä kuin kurssimerkintä?

Q10: Mitä ongelmia sinulla oli tämän laboratoriotyön tekemisessä?

Viitteet

[1] Wikipedia: IEEE 802.1X
http://fi.wikipedia.org/wiki/IEEE_802.1X (16.9.2009)

[2] pfSense
http://www.pfsense.com (16.9.2009)

[3] ProCurve Series 2500 Switches Management and Configuration Guide
http://ftp.hp.com/pub/networking/software/2500-MgmtConfig-Oct2005-59692354.pdf
(16.9.2009)

[4] The FreeRADIUS Project
http://freeradius.org/ (16.9.2009)

[5] The Open1X Project
http://open1x.sourceforge.net/ (16.9.2009)