

Stredná odborná škola technická
Kukučínova 483/12, 058 01 Poprad

STREDOŠKOLSKÁ ODBORNÁ ČINNOSŤ

č. odboru: 12- Elektronika a hardvér

Radius server na Linuxe Zeroshell

2016
Poprad

riešiteľ
Martin Chlebovec
ročník štúdia: **štvrtý**

Stredná odborná škola technická
Kukučínova 483/12, 058 01 Poprad

STREDOŠKOLSKÁ ODBORNÁ ČINNOSŤ

č. odboru: 12 – Elektrotechnika a hardvér

Radius server na Linuxe Zeroshell

2016

Poprad

riešiteľ

Martin Chlebovec

ročník štúdia: **štvrtý**

konzultanti:

Mgr. Jozef Dolinský

Bc. Matúš Kruppa

ČESTNÉ VYHLÁSENIE

Vyhlasujem, že som prácu spracoval sám a uviedol som všetky použité pramene a literatúru, z ktorých som čerpal informácie.

V Poprade 7.2.2016

Podpis:.....

POĎAKOVANIE

Osobitné poďakovanie patrí pánovi majstrovi Bc. Matúšovi Kruppovi a pánovi Mgr. Jozefovi Dolinskému, ktorí mi umožnili pracovať na tomto projekte a aj vďaka ich odborným radám a skúsenostiam som prácu úspešne dokončil. Konzultácie prebiehali osobne, alebo externou mailovou formou.

OBSAH

| | |
|---|----|
| <u>Čestné vyhlásenie</u> | |
| <u>Poďakovanie</u> | |
| <u>Obsah</u> | |
| <u>Úvod</u> | 6 |
| <u>Zoznam skratiek</u> | 7 |
| <u>1 Radius server - AAA</u> | 8 |
| <u>1. 1 Využitie Radius servera v praxi</u> | 8 |
| <u>1. 2 Hardvér použitý pre prácu</u> | 9 |
| <u>1. 3 Hierarchické zapojenie v sieti</u> | 9 |
| <u>2 802.1X</u> | 10 |
| <u>2. 1 EAP.</u> | 10 |
| <u>2. 2 PEAP s TLS tunelom</u> | 11 |
| 2. 3 CHAP | 11 |
| <u>3 Linux Zeroshell</u> | 13 |
| <u>3. 1 Webové prostredie Zeroshell-u.</u> | 13 |
| <u>3. 2 Používatelia a certifikáty.</u> | 14 |
| <u>3. 3 Používatelia a skupiny</u> | 14 |
| <u>4 Priebeh overenia</u> | 15 |
| <u>5 Výhody a nevýhody</u> | 16 |
| <u>5. 1 Rozdiely oproti WPA2-PSK.</u> | 16 |
| <u>Ciele práce</u> | 17 |
| <u>Záver</u> | 18 |
| <u>Zhrnutie</u> | 19 |
| <u>Zoznam použitej literatúry</u> | 20 |
| <u>Prílohy</u> | 21 |

ÚVOD

Moja práca bola vytvorená na hodinách odborného výcviku a aj prácou doma vo voľnom čase. Problematiku v mojej práci tvorí zabezpečenie wi-fi sietí v domáciach, ale najmä podnikových sieťach. Snažím sa poukázať nato, ako mnoho používateľov zabúda na dostatočné zabezpečenie wi-fi sietí a neuvedomujú si riziko odcudzenia dát. Poukazujem na zabezpečovanie priority a oboznamujem o zabezpečení siete s Radius serverom. Pre prácu som sa rozhodol aj preto, lebo ma fascinuje široká škála využití Linuxu najrôznejších distribúcií. Pre moju prácu som využil Radius server a hybridný WAN router. Pre tvorbu siete s dodatočným zabezpečením Radius serverom bolo nutné využiť typ zabezpečenia WPA2 Enterprise. Tento typ umožňuje od klientov pokúšajúcich sa pripojiť do siete vyžadovať prihlasovacie informácie ako meno a heslo s dodatkom vyžiadania certifikátu.

Certifikát v sebe kopíruje dôležité informácie, napríklad kopíruje v sebe identitu servera v rámci lokálnej siete, následne trasu k nemu a mnoho iných informácií. Celý proces prihlasovania i komunikácie v sieti je šifrované za pomoci TLS tunela so silnou 256-bitovou symetrickou šifrou. Prácu sa mi podarilo sprevádzkovať v čase kratšom ako 3 dni a dnes sa plnohodnotne využíva v budove praxe. Počas študovania týchto technológií som sa mnohému priučil a verím, že to využijem aj pri plánovaní a stavaní sietí po škole.

ZOZNAM SKRATIEK

Live CD – spúšťacie CD – obraz príkazového riadku pre vykonávanie jednoduchých operácií

LAN – označenie pre lokálnu sieť, ktorá najčastejšie pokrýva jednu budovu

WPA/WPA2 – typ šifrovaného zabezpečenia špecifikovaný štandardom 802.11i

Radius server – server využívajúci službu Radius pre overovanie klientov

TLS – protokol slúžiaci na šifrovanie dát – AES, symetrické šifrovanie

GNU GPL – licencia šírenia voľného softvéru

DHCP – protokol, ktorý prideluje IP adresy v sieti

AAA – autentizácia, autorizácia, akontácia

Provider – poskytovateľ internetového pripojenia

EAP – rozširujúci autentizačný protokol

PEAP – protected EAP – šifrované EAP s opravou nedostatkov

EAPoL – EAP rámce zasielané skrz lokálnu sieť s ethernet hlavičkou

1 RADIUS SERVER - AAA

Skratka pre Remote Authentication Dial-In User Service – systém používaný pre autentizáciu a autorizáciu klientov v sieti, najčastejšie pripájajúcich sa skrz bezdrôtové pripojenie. Toto riešenie poskytuje Radius server formou prihlasovania do siete menom a heslom a v poslednom rade aj overením certifikátu. Ak sú údaje pri autentizácii zadane, prechádzka krok k autorizácii, kedy Radius server na základe prihlasovacích údajov prístup do siete povolí – Access Allowed, alebo zamietne – Access Denied.

Trojité označenie AAA označuje 3 hlavné podslužby, s ktorými služba Radius pracuje:

- 1.) Autentizácia – prihlásenie meno, heslo
- 2.) Autorizácia – povolenie/zamietnutie prístupu po výsledku autentizácie
- 3.) Akontácia – využívanie siete, monitorovanie používateľov, obmedzenia, platby

Radius server počúva na porte UDP 1812 protokolu TCP/IP. Prístupový bod kontaktuje Radius server s tým, že zariadenie žiada o autentizáciu a odošle mu prihlasovacie informácie od klienta taktiež skrz šifrovaný tunel. Radius server následne porovná údaje s databázou a v prípade správnej kombinácie sa klient autorizuje a je mu pridelená IP adresa po povolení prístupu – Access Allowed.

1.1 VYUŽITIE RADIUS SERVERA V PRAXI

Radius server sa využíva v niekoľkých smeroch, no je používaný v súčasnosti najmä u regionálnych internetových providerov, ktorý túto službu prevádzkujú na overovanie klientov pre ich prístup do providerovej siete overením. Toto overenie sa realizuje z routra klienta/zákazníka, ktorý pri prvom spustení siete vyplní v routri prihlasovacie informácie a aj protokol, ktorým sa toto overenie prevádzkuje. Medzi najčastejšie patrí PPTP na vytáčané pripojenie, taktiež pri WAN internete skrz anténu, či PPPoE pre xDSL linky. Všetky tieto tunelovacie protokoly poskytujú šifrované spojenie s ochranou pred odcudzením dát. V prípade, že má klient tieto informácie vyplnené vo formulári svojho routra správne, je overený a môže ísť na web skrz providerovu sieť. V našom prípade ho využívame na ochranu

siete pred nedovoleným prístupom cudzích osôb. Radius server umožňuje kombinovať metódy prístupu. Môžeme medzi seba zamiešať overenie mena a hesla, certifikátov, čipových kariet, filtrovanie MAC adries.

1.2 HADRVER POUŽITÝ PRE PRÁCU

Na prácu bol využitý starý nevyužívaný počítač.

Parametre počítača:

- CPU: Intel Celeron Dual-Core 3Ghz
- GPU: VGA
- RAM: 512MB
- HDD: 2,5GB

Celá zostava beží na operačnom systéme Linux Zeroshell vo verzii 1.0_16. Inštalácia bola jednoduchá, no pomerne zaujímavá, nakoľko sme na inštaláciu potrebovali 2 súbory. Jedným bol takzvaný Live CD, ktorý spustil iba základný príkazový riadok a prostredníctvom neho bolo možné rozbaľiť obsah druhého súboru na HDD počítača. Po nakopírovaní a reštartovaní počítača bolo možné nastaviť hlavnú bootovateľnú partíciu.

Zostava v prílohe obr. č. 1

1.3 HIERARCHICKÉ ZAPOJENIE V SIETI

Najvyšším prvkom v sieti pri hviezdicovej topológii je router, respektíve najbližšie rozhranie, ku ktorému sa pripájajú všetky prvky v sieti, teda ním môže byť aj server. V našom prípade využívame router. Do WAN portu routera pripájame internet a do LAN portov pripájame klientov, avšak klienti pripojení pomocou kábla nebudú autentizovaní, nakoľko ich berieme ako dôveryhodných. Ako prepojenie routera s Radius serverom využívame LAN port, štandardnú kabeláž CAT 5e s konektormi RJ 45. Server je tak zapojený totožne, ako bežné klientské počítače v sieti.

2 802.1X

Štandard 802.1x definovaný organizáciou IEEE je protokol slúžiaci na zabezpečenie prístupu do siete na základe vyžadovania autentizácie, teda mena a hesla. Pokým nie je používateľ úspešne autentizovaný, celý jeho dátový prenos je blokovaný. “Uplatní sa i v bezdrátových sítich, kde je fyzické zabezpečenie v podstate nemožné a voľné pripojenie by mohlo byť snadno zneužitá k odcudzeniu cenných informácií.” (prevzaté z internetovej stránky Wikipédie: https://cs.wikipedia.org/wiki/IEEE_802.1X, sekcia využitia 802.1X).

Po pripojení k AP/Routru funguje Router ako overovací server, je pripojený LAN portu a klient komunikuje v prvej fáze overenia s Radius serverom skrz router. Radius server akceptuje iba EAP rámce počas autentizácie, prostredníctvom EAP protokolu sa Radiusu dostavia aj odpovede, v prípade, že je autentizácia úspešná, o výsledku je informovaný iba AP/Router, ktorý následne umožní dátovú prevádzku na svojich portoch. V routeroch/AP môžeme najčastejšie 802.1X zabezpečenie nájsť ako WPA, WPA2 s doložkou Enterprise. Každý router/AP musí byť s Radius serverom spárovaný. Tento krok sa vykonáva takzvaným zdieľaným tajomstvom, keď ľubovoľný textový reťazec zdieľajú oba zariadenia, Radius server tieto znaky zdieľa s konkrétnou IP adresou routera/AP.

2.1 EAP

Skratka pre Extensible Authentication Protocol - protokol slúžiaci ako autentizačný rámec najčastejšie používaný v bezdrôtových sieťach a PPP spojeniach. EAP rámec sprostredkúva prenos a používanie kľúčov generovaných podľa metód rozširujúcich EAP protokol, teda

nehovoríme o sieťovom protokole, ale o formáte sprav, využitie v sieťach so zabezpečením WPA/WPA2 Enterprise - 802.1x.

“EAP je autentizační rámec, nikoliv samotný autentizační mechanismus. Zajišťuje některé obecné funkce a sjednání autentizačních metod, které se nazývají metody EAP. Je definováno okolo 40 metod.” (prevzaté z: cs.wikipedia.org/wiki/Extensible_Authentication_Protocol)

2.2 PEAP S TLS TUNELOM

PEAP je obdoba EAP rámca so šifrovaním autentizácie prostredníctvom TLS tunela. Hlavnou ideou v PEAP je opraviť nedostatky v EAP a zvýšiť bezpečnosť. Vyvinutý spoločnosťami Cisco, Microsoft a RSA Security. V rámci používania TLS tunelu môžeme povedať, že je sieť veľmi dobre zabezpečená, nakoľko sa musí klient autentizovať aj certifikátom, taktiež meno a heslom, aj preto je nasadzovaný málo, ale má to aj výhodu v podobe duálneho overenia. Prostredníctvom tohto protokolu spolu komunikuje počítač žiadajúci o autentizáciu a server. Každý OS má v sebe tzv. prosebník. Prosebník môže byť nazývaný aj ako daemon, takýto softvér riadi prihlásenie k sieti akéhokoľvek typu, napríklad WEP, WPA, WPA2, či už PSK, alebo Enterprise. Pokým nie je zariadenie autentizované, akákoľvek dátová premávka je u neho blokována, teda je mu otvorený iba jeden port - k serveru, skrz router v prvom kroku. Celý proces riadi prosebník, ktorý klienta vyzve k zadaniu autentizačných informácií. Prosebník komunikuje s routrom a zašle mu údaje od klienta. O výsledku autentizácie je informovaný AP/router, ktorý na základe správneho overenia pridelí DHCP adresu a klientovi otvorí všetky porty pre komunikáciu v sieti.

Okno prosebníka v prílohe obr. č. 3

2.3 CHAP

Protokol slúžiaci na preukázanie totožnosti pri PPP spojeniach. Radius server ho využíva v druhej fáze preukázania totožnosti certifikátom.

Klient aj autentizačný server zdieľajú rovnaký šifrovací kľúč symetrickej šifry. Autentizácia v protokole CHAP prebieha v troch krokoch.

Najprv je ustanovené spojenie medzi klientom a autentizačným serverom. Následne autentizačný server odošle klientovi príkazom Challenge výzvu, obsahujúcu náhodný reťazec. Klient vhodne spojí prijatý náhodný reťazec so zdieľaným tajomstvom (šifrovacím kľúčom) a výsledok zašifruje pomocou algoritmu. Výsledok vloží do odpovede a odošle autentizačnému serveru, ako EAPoL.

Autentizačný server dostane zašifrovanú správu od klienta a následne zašifruje pôvodnú správu, ktorú odoslal klientovi rovnakým spôsobom, ako to urobil klient, teda rovnakým algoritmom a porovná svoju a správu klienta, či sú zhodné. Ak je výsledok zhodný, tak dôjde k potvrdeniu autentizácie, pri nezhode k zamietnutiu autentizácie. Pakety Challenge môžu byť v priebehu komunikácie odosielané kedykoľvek v náhodných opakujúcich intervaloch z dôvodu overenia klienta, teda proces prihlasovania sa opakuje – na pozadí. Výhoda protokolu CHAP je obojstranná autentizácia, teda autentizácia klienta proti serveru a autentizácia servera proti klientovi.

Nastavenie sieťového profilu v prílohe - obr. č. 4

3 Linux Zeroshell

Zeroshell je distribúcia Linuxu, ktorá umožňuje beh Radius servera a iných služieb. Vyniká vysokým výkonom aj na slabších počítačových zostavách.

Minimálne požiadavky pre plynulý beh služieb:

CPU: 233Mhz

RAM: 96MB

HDD: 1,5GB

Tieto nízke požiadavky dokonale umožňujú chod servera aj na minulo-generačných počítačoch, pre ktoré už dnes nenájdeme iné využitie. Inštalácia tejto distribúcie bola pomerne zaujímavá, na CD bolo nutne napáliť Live CD, ktorý simuloval Terminál operačného systému. Okrem toho bolo nutne stiahnuť na USB kľúč aj obraz Zeroshell-u. Pri Live CD v príkazovom riadku bolo nutne obsah USB kľúča rozbaľiť na HDD počítača niekoľkými príkazmi, tým prekopíroval súbory na HDD spoločne s bootovateľnými súbormi. Linux Zeroshell je distribuovaný pod licenciou GNU GPL2 a je teda šírený voľne bez obmedzení. Zeroshell je navrhnutý pre poskytovanie aj iných služieb, ako VPN, DHCP a menej známych.

3.1 WEBOVÉ ROZHRANIE ZEROSHELL-U

Služby Radius servera je možné spravovať prostredníctvom webového rozhrania Zeroshellu, adresa Radius servera je adresou sieťovej karty servera. Administrátor siete sa prostredníctvom administrátorského mena a hesla prihlási do servera, kde môže vykonávať potrebné opatrenia, či editovať účty. V prehliadači z klientského počítača je možné spustiť toto

rozhranie a vhodne nakonfigurovať službu Radius. Okrem toho webové prostredie ponúka aj niekoľko služieb, ktoré môžu na servery bežať, napríklad DNS, Net Balancer, Kerberos, iné. Webové rozhranie je taktiež šifrované, konkrétne HTTPS protokolom.

Webové rozhranie v prílohe - obr. č. 5

3.2 POUŽÍVATELIA A CERTIFIKÁTY

Každý používateľ musí mať vo svojom počítači nainštalovaný certifikát. Certifikát, ktorý overí server v lokálnej sieti ako dôveryhodný. Každé zariadenie, ktoré sa snaží autentizovať tento certifikát predkladá v druhom autentizačnom kroku s protokolom CHAP. Administrátor siete, ktorý ju zabezpečuje, musí do každého klientského wi-fi zariadenie nainštalovať takýto certifikát a vhodne upraviť nastavenia overenia tak, aby proces prebehol bez overenia. Výhodu majú najmä Android a Unix zariadenie všeobecne, nakoľko si tento certifikát dokážu vyžiadať zo servera pri každej autentizácii. Takouto možnosťou disponuje aj Windows 8, 10. Používateľ, ktorý daným certifikátom nedisponuje - nechcený používateľ je serverom odmietnutý, lebo sa nepreukázal žiadaným certifikátom s cestou k overovaciemu serveru. V prípade prvej úspešne autentizovanej a autorizovanej fáze sa dostávame k druhej - CHAP overeniu. Momentálne využívame certifikát predinštalovaný iba pri operačných systémoch Windows 7 a Windows XP, prípadne Vista.

Rozhranie admina v sekcii kônt v prílohe - obr. č. 6

3.3 POUŽÍVATELIA A SKUPINY

Vytvorení používatelia sú po vytvorení radení do skupín, ktoré môžeme ľubovoľne vytvárať, upravovať ich. K dispozícii je mnoho funkcií na limitovanie takýchto používateľov. Tieto funkcie sa využívajú pri firemných sieťach či dovolenkových hotspotoch. Klient po autentizácii a autorizácii prejde do akontačného režimu vrámci jeho skupiny. Skupina môže mať vplyv na rýchlosť sťahovania/odosielania, objem prenesených dát, či dokonca aj

účtovanie za využívanie služieb. Preto sú takýto používatelia vrámci skupín radení do tzv. virtuálnych LAN sietí. Hovoríme teda skratkou o VLAN sieťach. Používateľ nemá možnosť prepínať medzi sieťami. V prípade, že sa chce presunúť do inej, musí sa autentizovať iným účtom.

Rozhranie admina v skupinovej sekcii v prílohe - obr. č. 7

4 PRIEBEH OVERENIA

Radius server počúva na UDP porte 1812. Klient po kliknutí na meno siete, respektíve vyžiadaní pripojenia k sieti je vyzvaný prosebníkom na zadanie mena a hesla. (Klient musí mať vopred nainštalovaný certifikát a nastavenú cestu k nemu v sieťovom profile) Správa sa zapuzdří ako EAPoL, je odoslaná prostredníctvom TLS tunela na AP, ten správu rozbalí a odstráni z nej oL, teda Ethernet hlavičku a výsledkom je EAP hlavička, v skutočnosti ale ide len o minimálnu zmenu rámca. Následne sa správa odosiela na Radius prostredníctvom portu 1812. Tu je ale TLS tunel konštruovaný medzi IP adresami, zatiaľ čo medzi AP a klientom na základe MAC adries, nakoľko klient nemá pridelenú IP adresu, tu sa končí metóda PEAP. Po autentizácii sa prechádza k druhému kroku, kedy cez CHAP, kde svoj certifikát predloží certifikát a porovnáva sa s certifikátom klienta, následne Radius odošle na klienta challenge výzvu so správou, ktorá obsahuje náhodný reťazec, klient správu šifruje verejným kľúčom, hashovacou funkciou MD5 a odošle na Radius. Radius zašifruje taktiež verejným kľúčom pôvodnú správu a skúma, či sú zhodné. Tu skúma, či bola správa zmenená, v prípade, že nie, klient je autentizovaný aj v tomto kroku. Na AP prichádza Access v podobe Allowed, prístup

povolený, alebo Access Reject, teda zakázaný. Access odpoveď prichádza na AP po porte 1813. V prípade Allowed je pridelená IP adresa klientovi. Samotný klient však o výsledkoch autentizácie nie je informovaný. Následne je na základe svojho mena a hesla umiestnený do danej skupiny, respektíve VLAN siete.

5 VÝHODY A NEVÝHODY RADIUS SERVERA

Výhody:

- šifrovaná autentizácia 256-bitovým symetrickým kľúčom
- VLAN siete, skupiny používateľov
- vytváranie kônt
- obojstranné overenie
- možnosť postavenia na akomkoľvek počítači
- 2 metódy overenia
- Spol'ahlivosť

Nevýhody:

- možnosť využitia iba pre bezdrôtové siete
- nepotrebnosť inštalácie pre Unix zariadenia (ľahší prístup)
- nutnosť inštalácie certifikátov pre každý bezdrôtový počítač

- nutnosť správne nastaviť sieťový profil
- nemožnosť obmedziť jeden počítač na konto

5.1 ROZDIELY OPROTI WPA2-PSK

Pri WPA2 Personal (PSK) sa využíva takzvaný zdieľaný kľúč, heslo, ktoré používajú všetci klienti pri autentizácii. Pri WPA2 Enterprise sa využíva duálne overenie, teda autentizácia za pomoci Radius služieb, respektíve servera, na ktorom tieto služby bežia a taktiež využívame aj overenie certifikátom. Existuje ešte niekoľko metód, ktoré je možné využiť, ako napríklad overenie za pomoci čipovej karty. Pri WPA2 Enterprise by mal mať každý klient preukázať svoju identitu každý vlastnými prihlasovacími údajmi. Privátny kľúč má každý pripojený klient generovaný ako jedinečný. Po úspešnej autentizácii je klient umiestnený do svojej skupiny a následne do vlastnej VLAN siete. Najmä predchádza odpočúvaniu.

CIELE PRÁCE

Cieľom mojej práce bolo najmä oboznámiť so zabezpečovacími mechanizmami Radius servera so zabezpečením siete WPA2 Enterprise. V práci rozoberám implementáciu Radius zariadení v sieťach a taktiež ich postavenie v sieti voči ostatným prvkom siete. Vysvetľujem, na akom princípe práca funguje a taktiež rozoberám rozdiely voči totožnému zabezpečeniu s doložkou Personal a naším Enterprise.

ZÁVER

Práca je momentálne reálne nasadená na praxi v učebni PD 310. Bola testovaná pod rôznymi operačnými systémami, napríklad: Android, Windows, iOS, Linux, so všetkými Radius server dokáže pracovať. Radius server bežal nepretržite vyše 60 dní bez akýchkoľvek problémov. Linux Zeroshell disponuje aj inými službami, ako DNS, VPN, DHCP. Po prezentácii práce budú zakomponované aj tieto služby pre plnohodnotnú prevádzku servera.

ZHRNUTIE

Hlavnou myšlienkou bolo postaviť autentizačné zariadenie na starom - nevyužitom počítači a poukázať nato, že žiaden počítač nepatrí do starého železa a dá sa plnohodnotne využiť aj s minimálnym výkonom pre poskytovanie takýchto sieťových služieb. Cena celej práce bola 0 €, nakoľko sa na ňu využil nepoužívaný počítač a nepoužívaný router. Osvojil som si rôzne pojmy, typy serverov, akými sa dajú overovať používatelia pred nepovoleným prístupom do siete, na druhej strane som zistil, že slovenské zdroje ponúkajú o podobných

riešeníach veľmi málo informácii, či dokonca žiadne. V škole sme sa doposiaľ s niečím podobným nikdy nestretli, ani na teoretickom, ani na praktickom vyučovaní.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] Remote Authentication Dial In User Service (RADIUS)
RFC 2865 [<http://www.faqs.org/rfcs/rfc2865.html>]

- [2] Radius - Linux Zeroshell

[<http://gljs.sk/linux/Windows7-WPA-Enterprise.pdf>]

[3] Accounting - Účtovanie

[<http://www.zeroshell.org/radius-accounting/>]

[4] 802.1X, EAP

[https://cs.wikipedia.org/wiki/IEEE_802.1X]

[5] CCNA - (knižné vydanie - 2010, Vydavateľ: Computer Press - RADIUS, VLAN)

[6] Certifikačné authority, certifikáty X509 PEM, TLS

[<http://www.zeroshell.org/x509details>]

[7] TLS, šifrovanie

[https://sk.wikipedia.org/wiki/Transport_Layer_Security]

[8] Asymetrické šifrovanie

[<http://www.ktl.elf.stuba.sk/~orgon/lednický/?page=15>]

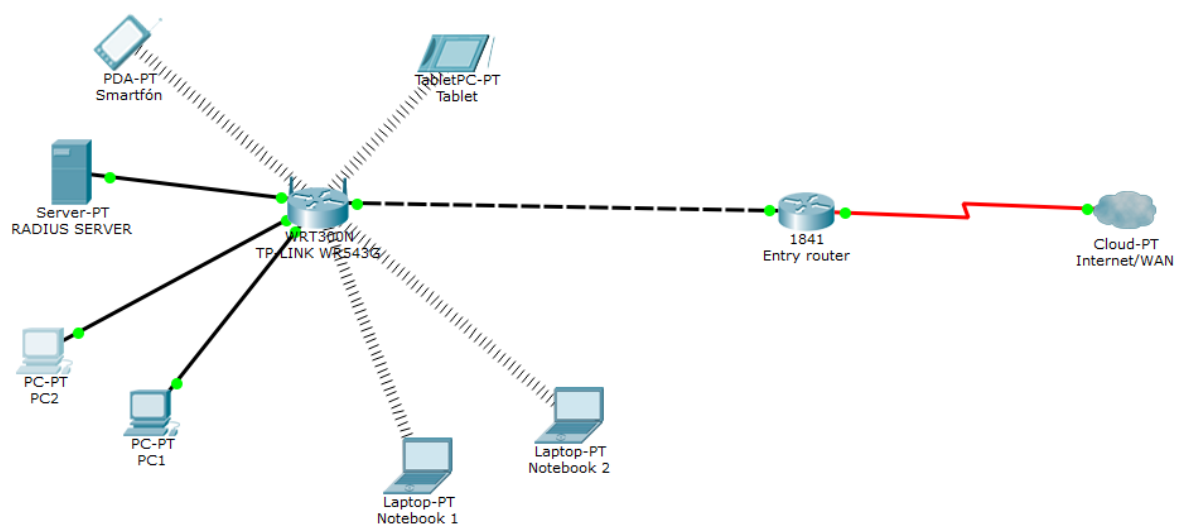
[9] Inštalácia servera

[<http://gljs.sk/linux/radius.html>]

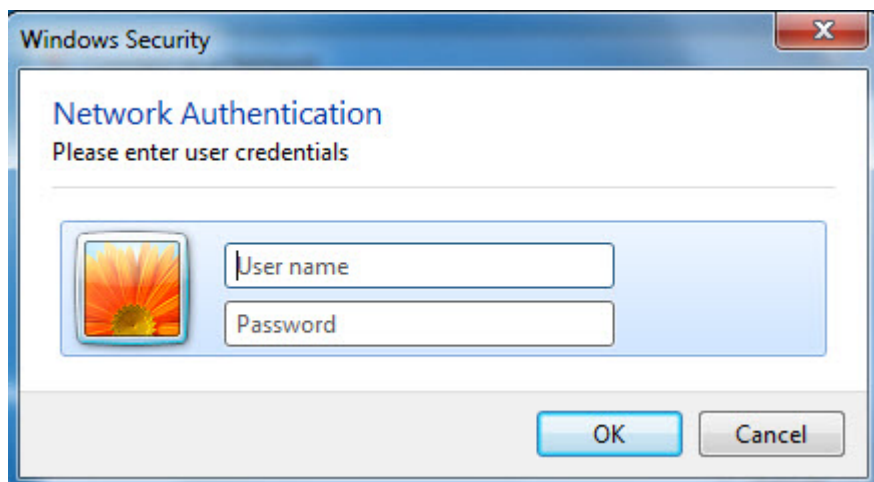
PRÍLOHY



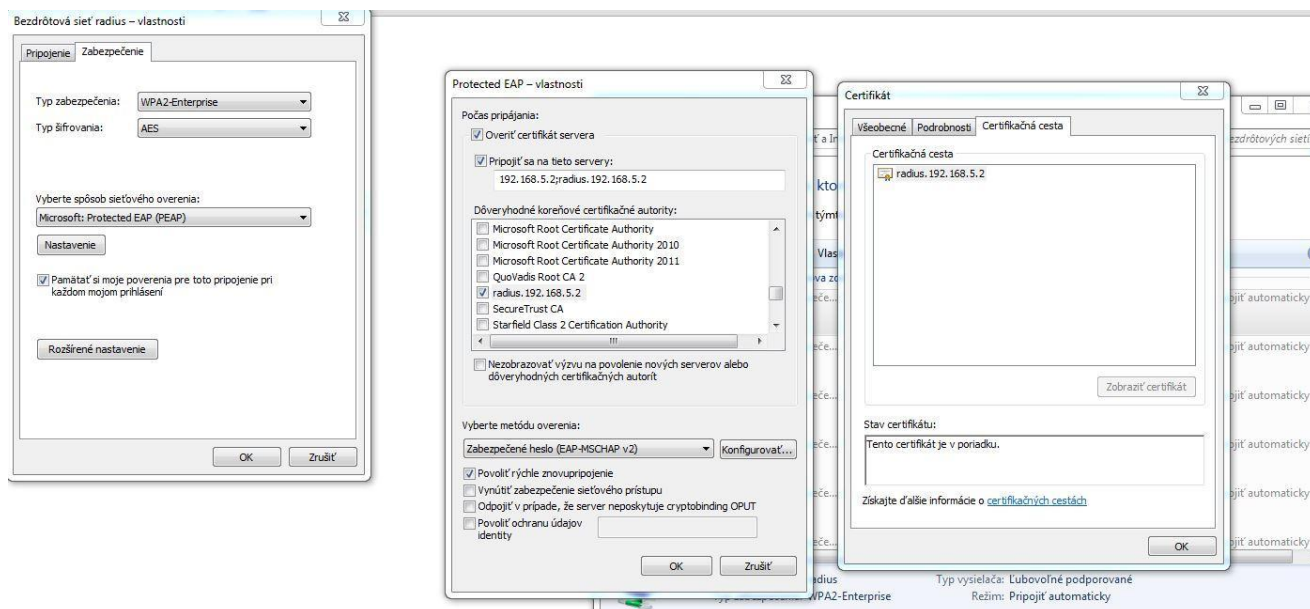
Obr. č. 1 - Server pri zapojení do siete s routrom



Obr. č. 2 - Hierarchické zapojenie v sieti



Obr. č. 3 - Okno prosebníka vo Windowse 7



Obr. č.4 - Sieťový profil radius WPA2 siete

ZEROSHELL Net Services Release 1.0.beta14 [About](#)

SYSTEM

- Setup
- Logs
- Utilities

USERS

- Users
- Groups
- LDAP / NIS
- RADIUS
- Captive Portal

NETWORK

- Hosts
- Router
- DNS
- DHCP
- VPN
- QoS
- Wireless
- Net Balancer

SECURITY

- Kerberos 5
- Firewall
- X.509 CA
- HTTP Proxy

AutoUpdate Settings ✓ Status: **Active**

Show Last connection: December 06, 2015 13:26

Available Updates ✓ Auto Install

| Fix ID | Description | Date | Require |
|---|-------------|------|---------|
| No updates available for release 1.0.beta14 | | | |

Installed Updates

| Fix ID | Description | Date | Required by |
|----------------------|-------------|------|-------------|
| No updates installed | | | |

Obr. č. 5 - Webové rozhranie Zeroshellu

Windows Access (windowsaccess)

Account Information

Username uid Primary Group gid

Home Directory Default Shell ☐ bash ☐ sh ☐ tcsh ☒ other

User Information

Firstname Lastname Organization

Description E-Mail Phone

RADIUS Accounting

Expiration (mm/dd/yyyy) / / Accounting Class

Credit: 0.00 €

Limits - - Costs (postpaid)






User Password

Password Confirm

Authentication Protocol

Kerberos 5 ☒ RADIUS (VLAN) ☒

Obr. č. 6 - Rozhranie administrátora pri vytváraní sieťového účtu

| USERS | | List | View | Add | Edit | Delete | X509 | Kerberos 5 | | |
|---|--------------|----------------------|------|-----|------|--------|-------------------|-----------------------------|--|------------------------------------|
| Entries found: 4 | | | | | | | | Search <input type="text"/> | | Primary Group <input type="text"/> |
|  Username | Group | Description | | | | | E-mail | | | |
|  admin | 0 | System Administrator | | | | | | | | |
|  androidaccess | test1 | Android AP | | | | | sdf | | | |
|  MartinChlebovec | test1 | Martin Chlebovec | | | | | chlebovec.martin@ | | | |
|  windowsaccess | test1 | Windows Access | | | | | sdfsdf | | | |

Obr. č. 7 - Rozhranie administrátora v zozname dostupných skupín používateľov