|  |  |
| --- | --- |
| **ŽILINSKÁ UNIVERZITA V ŽILINE**  **FAKULTA RIADENIA A INFORMATIKYNázov fakultyNázov vysokej školy** | |
| **Android aplikácia na sledovanie polohy mobilného zariadeniaIMPLEMENTÁCIA FIREMNEJ SIETE** | |
|  | |
|  | |
| **2016** | **Andrej Hucík**  **Miroslav Kozák**  **Andrej Šišila** |

|  |  |
| --- | --- |
| Žilinská univerzita v ŽilineŽILINSKÁ UNIVERZITA V ŽILINE  Fakulta riadenia a informatikyFAKULTA RIADENIA A INFORMATIKY | |
| **Android aplikácia na sledovanie polohy mobilného zariadeniaIMPLEMENTÁCIA FIREMNEJ SIETE**  SERVEROVÉ OPERAČNÉ SYSTÉMY | |
| Bakalárska prácaSEMESTRÁLNA PRÁCA | |
| Študijný program: | Informatika - stará akreditáciaAplikované sieťové inžinierstvo |
| Katedra: | Katedra informatikyKatedra informačných sietí |
| Vedúci bakalárskej práce: | doc. Ing. Michal Varga PhD.Ing. Pavel Segeč, PhD. |
| Skupina: | SOS3 (Utorok) |
| ŽilinaŽilina 20162016 | **Andrej Hucík**  **Miroslav Kozák**  **Andrej Šišila** |

**ABSTRAKT**

**ABSTRACT**

Obsah

Zoznam ilustrácií

Zoznam tabuliek

Zoznam ukážok zdrojových kódov

Úvod

Základom každej firmy, či už malej, strednej alebo veľkej, je stabilná a bezpečná sieťová infraštruktúra.

V našej práci sa budeme zaoberať implementáciou a konfiguráciou menšej firemnej siete, ktorá bude pozostávať z jedného smerovača, jedného prepínača, dvoch serverov ých systémov a dvoch pracovných staníc. Potom na potrebných uzloch nastavíme potrebné služby, ktoré umožnia firme fungovať jednoduchšie a efektívnejšie.

1. Ciele práce

Hlavným cieľom našej práce je vytvorenie jednoduchej sieťovej infraštruktúry, ktorú bude možné nasadiť do podnikového prostredia. Vytvorenie a konfigurácia takejto siete si vyžadovalo splnenie nasledovných čiastkových cieľov:

* Inštalácia operačného systému na serverové systémy, pracovné stanice a smerovač, a ich následná základná konfigurácia
* DNS: Master/Slave riešenie s replikáciou a overením
* Podpora viacerých virtuálnych web serverov a s inštaláciou niektorej z web aplikácii typu CMS or Wiki
* Firewall na smerovači cez netfilter s NAT
* Firewall na server systémoch
* NTP čas pre firmu
* SSH prístup
* DHCP s prideľovaním IP adries
* Email
* VoIP

1. Inštalácia a konfigurácia zariadení

Vytvorenie virtuálnych strojov, inštalácia Debianu 8, konfigurácia firewallu, konfigurácia prepínača, konfigurácia serverov, konfigurácia desktopov

Nainštalovali sme funkčný Linux OS - Debian 8 stable, vykonali sme základnádnú konfigurácia nainštalovaného OS a nakonfigurovali sme funkčný firewall, ktorý spĺňa požiadavky zadania.

* 1. Vytvorenie novej VM a jeho nastavenie.

a. VM sme nazvali podľa zadania.

b. Študent prejde postupne jednotlivými nastaveniami, ktoré ponúka nástroj VB.

c. Pre jednotlivé VM sme správne nastavili sieťové adaptéry a virtualizačné parametre, napríklad PAE/NX a paravirtualizačné rozhranie v SYSTEM ACCELERATION.

d. Každej VM sme nastavili správny počet a funkčnosť sieťových adaptérov: 2 pre firewall, 1 pre servery a desktopy

e. Zdieľaný adresár sme na VM nepridávali.

* 1. Inštalácia Linux OS - Debian.

a. Stiahli sme si obraz disku Debian 8 stable 64 bitovú verziu.

b. Obraz disku (iso súbor) sme pripojili k diskovej mechanike VM a spustili sme inštaláciu OS.

i. Hostname – každá VM má svoje meno odvodené od jej funkcie napr. všetky servery majú označenie „SX“ a desktopy „DX“, kde X je poradové číslo servera/desktopu.

ii. Domain – nastavili sme pridelenú doménu: sos3.local.

iii. Servery nemajú grafické rozhranie, iba textové. Desktopy majú nainštalované grafické rozhranie XFCE.

* 1. Základná konfiguráciu systému.

a. Študent si zopakuje použitie príkazov pre vykonanie základných operácii v linuxovom prostredí - práca so súbormi (prezeranie, editovanie, kopírovanie a presúvanie, tvorba odkazov a pod.).

b. Študent doinštaluje ďalšie balíky: pre študenta vhodný textový editor (odporúčame zvoliť jeden a ten následne používať), mc, ssh klienta aj ssh server, telnet, tcpdump (ak poznáte a ovládate iný nástroj na odchytávanie sieťovej prevádzky, môžete zvoliť ten, ale nezabúdajte na absenciu grafického prostredia), bind9-host, dkms (z vlastných skúseností odporúčam stručne pozrieť význam balíka), arping a dsniff. Študent následne „uprace“ (vyčistí) po balíkoch s použitím nástroja apt-cache.

c. Študent doinštaluje tzv. Guest Additions do systému.

d. Študent stručne preskúma využitie konfiguračných adresárov a súborov: /etc/profile.d/, /etc/skel/, ~/.profile, ~/.bashrc a porozmýšľa nad ich možným využitím (súvislosť s rôznymi systémovými premennými prostredia - PATH, EDITOR, PAGER, VISUAL a pod.)

e. Študent si zopakuje príkazy pre zobrazenie rôznych sieťových nastavení systému a jeho sieťovú konfiguráciu.

f. Študent vykoná zapojenie siete s danými servermi a klientmi cez fyzický prepínač v stojane labu B301. Prepínač musí byť prázdny so zapnutým Rapid STP.

g. Študent vykoná základnú sieťovú konfiguráciu. Tá zahŕňa nastavenie statických IP adries na rozhraniach a povolenie prepínania (IP\_FORWARD).

h. Študent vytvorí SNAPSHOT nastaveného systému, aby tak mal uchovaný stav čistého systému so základnou konfiguráciou.

* 1. Skript pre automatické pridanie záznamov do iptables.

Náš firewall ktorý je pomenovaný ako fw je založený na kernelovom module netfilter.

Netfilter je framework obsiahnutý v jadre Linuxu od verzie 2.4.x, ktorý ponúka veľa možností pre filtrovanie paketov, preklad sieťových adries (NAT) alebo preklada sieťových portov (PAT). Netfilter nahrádza zastaraný modul ipchains v linuxovom jadre verzie 2.2.Iptables je user-space nástroj v Linuxe, ktory slúži na profesionálne nastavovanie pravidiel firewallov v jadre. Pravidlá firewallov ovplyvňovať prichádzajúce, odchádzajúce aj prechádzajúce pakety. Pravidlá sú v jadre spracovávaná niekoľkých netfilter modulmi.

Vytvorili sme skript s názvom firewall.sh ktorý slúži na automatické pridávanie záznamov do iptables. Nastavili sme premennú: **I=/sbin/iptables** . Nastavili sme práva tak ,aby sme mohli daný skript spúšťať , prikazom **chmod 744 firewall.sh .** Následne sme mohli spúšťať skript manuálne a to : **./firewall.sh .**Vložené pravidlá cez iptables sa po reštarte systému stratia.Chceli sme, aby sa skript s pravidlami pre firewall spúšťal pri štarte operačného systému automaticky.Preto sme dopísali v **/etv/network/interfaces**pre daný interface riadok : **up /usr/sbin/firewall.sh.**

Hneď na začiatku skriptu sme vyčistili aktuálne tabuľky v iptables : **$I -F -t filter**a  
**$I -F -t nat**.

Pokračovali sme nastavením predvolenej politiky pre INPUT ,FORWARD A OUTPUT .

**$I -P INPUT DROP -** input všetko zahadzuje **$I -P FORWARD DROP -** forward všetko zahadzuje

Pre output sme politiku nemenili , teda ostala defaultne accept (všetko povoľ). Ďalej sme povolili všetku prevádzku, ktorá prichádza na lo (loopback) rozhranie.

**$I -A INPUT -i lo -j ACCEPT**

Povolili sme všetky prichádzajúce ICMP správy a všetky prichádzajúce správy, ktoré sú súčasťou už existujúceho spojenia :

**$I -A INPUT -p icmp -j ACCEPT**🡪 povoli pingy na FW

**$I -A FORWARD -i eth1 -o eth0 -p icmp -j ACCEPT🡪**povoli pingy z vnútra siete von

**$I -A INPUT -i eth0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT🡪**povolí pakety ktoré patria už existujúcemu spojeniu.

Nastavili sme SSH prístup.

**$I -A INPUT -i eth1 -p tcp --sport 22 -j ACCEPT**

Doteraz sme využívali NAT maškarádu. Avšak je lepšie použiť SNAT/DNAT

SNAT je nastavenie NAT prekladu z privátnej siete do vonkajšej/verejnej.

**$I -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 158.193.139.74**

Nakoniec sme vytvorili snapshot nášho plne funkčného firewallu.

* 1. Automatické spúšťanie vlastných skriptov pri štarte systému.

Chceme, aby sa skript s pravidlami pre firewall spúšťal pri štarte operačného systému s „root“ oprávneniami. Docielili sme to tým, že sme do súboru „/etc/rc.local“ pridali absolútnu cestu bash skriptu. Skripty sa nachádzajú v adresári „/etc/skripty“.

Po otestovaní funkčnosti firewallu sme urobili snapshoty všetkých VM.

1. DHCP a VLAN

Servery sú vo VLAN 10, desktopy vo VLAN 20. Smerovanie medzi VLANami je vykonávané na FW. Preto sme na FW museli nainštalovať balíčky „isc-dhcp-server“ a „vlan“ t.j. „apt-get install isc-dhcp-server vlan“. Potom sme editovali súbor „/etc/network/interfaces“ tak, že sme odstránili adresné informácie z vnútorného interfacu eth1, ale nechali sme „auto eth1“, aby sa port zapol (UP). Následne sme pridali subinterface eth1.10 pre VLAN 10 (servery) a eth1.20 pre VLAN 20 (desktopy). Adresný rozsah pre jednotlivé VLAN bola sieť 192.168.0.0/24 rozdelená na dve /25 siete: 192.168.0.0 - 192.168.0.127 pre VLAN 10 a 192.168.0.128 - 192.168.0.255 pre VLAN 20.

FW je DHCP relay server. Všetky DHCP požiadavky prepošle FW DHCP serveru, ktorý pridelí klientovi IP adresu a ďalšie nakonfigurované informácie. Týmto spôsobom je FW zodpovedný iba za filtrovanie premávky a server za služby poskytované na sieti.

IP adresa DHCP servera sa do konfiguračného súboru „/etc/default/isc-dhcp-relay“ DHCP relay agenta musí zadať BEZ úvodzoviek a musíme počúvať na obidvoch subinterfacoch t.j. eth1.10 aj eth1.20.

1. DNS a DHCP (dokončenie)

V rámci našej doménovej zóny „sos3.local“ sme si museli nastaviť dva DNS servery: Master (S1) a Slave (S2). Slave zrkadlí hlavný DNS server a v prípade poruchy ho zastúpi. Keďže si Slave DNS server všetko stiahne z Master DNS servera, netreba ho primárne konfigurovať, ale stačí mu nastaviť „allow-transfer“ na privátnu IP Master DNS.

Na obidva servery sme nainštalovali DNS server a nástroje na overenie jeho funkčnosti príkazom „apt-get install bind9 bind9utils dnsutils“.

Master DNS serveru sme upravovali súbory „/etc/resolv.conf“ (konfigurácia adries DNS serverov), „/etc/bind/master/db.sos3.local“ (view-lokálny), „/etc/bind/master/db.sos3.external“ (view-verejný), „/etc/bind/named.conf.local“ (definovanie lokálnych a verejných DNS View).

V adresári „/etc/bind“ na S1 sme vytvorili adresár „master“, do ktorého sme ukladali zónové súbory pre DNS.

Viewy sme nastavovali na Master DNS serveri súbormi „/etc/bind/named.conf.local“, „/etc/bind/master/db.sos3.local“, „/etc/bind/master/db.sos3.external“. Pri dotazovaní na doménové meno nášho DNS zvnútra sa použijú privátne adersy DNS serverov zo súboru „/etc/bind/master/db.sos3.local“. Pri dotazovaní na doménové meno nášho DNS zvonku sa použijú verejné adersy DNS serverov zo súboru „/etc/bind/master/db.sos3.external“. O tom, aký súbor sa použije, rozhoduje súbor „/etc/bind/named.conf.local“

Počítače v lokálnej sieti sa dokážu navzájom pingať pomocou svojich hostname. Preklad hostname názvov na IP adresy je definovaný v súbore „/etc/bind/master/db.sos3.local“

DHCP server (S2) sme museli upraviť tak, aby prideľoval aj DNS adresy serverov. Súbor „/etc/dhcp/dhcpd.conf“ na S1 sme upravili tak, že sme doň pridali privátne IP adresy DNS serverov (option domain-name-servers). Do časti pre podsieť sme definovali názvy týchto serverov. Voľbu „option host-name“ sme zmenili z pôvodného „example.org“ na „sos3.local“. Tým, že sme nastavili DNS server, nemusíme meniť na jednotlivých hostoch súbor „/etc/resolv.conf“

Firewall bol nakonfigurovaný tak, aby prepúšťal DNS požiadavky na lokálnej sieti, a tiež aby prepúšťal požiadavky z internetu na obidva DNS servery t.j. aby boli obidva DNS servery viditeľné zvonku (PREROUTING). Záznamy pre DNS sú pre obidve verejné IP adresy pre udp aj tcp port 53 (zdrojový aj cieľový)

V prípade, že sa vyskytli problémy, skúšali sme vypnúť firewall, kontrolovali sme konfiguračné súbory Master DNS servera príkazmi „named-checkconf“ a „named-checkzone“ a príkazom „tcpdump“ sme monitorovali prenášané správy. Pri každej zmene konfiguračných súborov bolo treba reštartovať bind9 / isc-dhcp-server / interface.

Zdroje

<https://www.howtoforge.com/two_in_one_dns_bind9_views>

1. Záver