Posudek bakalářské práce

předložené na Matematicko-fyzikální fakultě
Univerzity Karlovy v Praze

❑ ~~posudek vedoucího~~ ❑ posudek oponenta

- **Autor/ka: Andrej Kalický**

  Název práce: Firewall a internetová (síťová) bezpečnost

  Studijní program a obor: Informatika, obor Správa počítačových systémů

  Rok odevzdání: 2009

Jméno a tituly vedoucího/oponenta: RNDR. ing. Jiří Peterka

Pracoviště: KSI MFF UK

	excelentní	odpovídající	slabší	nevyhovující
Náročnost zadaného tématu				x
Míra splnění zadání				x
Struktura textové části práce				x
Jazyková a typografická úroveň		x		
Analýza				x
Vývojová dokumentace		N/A		
Uživatelská dokumentace		N/A		
Kvalita zpracování softwarové části		N/A		
Stabilita aplikace		N/A		

Nejvýznamnější klady:
žádné

Nejzávažnější nedostatky:
Hlavní část předkládané práce je pouze zkráceným slovenským překladem vybraných partií z několika titulů odborné literatury (byť uvedených v seznamu použité literatury).

Způsob, jakým je se zdrojovou literaturou pracováno – tedy doslovný překlad celých kapitol, byť místy krácený (mnohdy i na podstatných věcech) - je zcela neadekvátní práci s odbornou literaturou a vymyká se logice a účelu bakalářské práce. Mohl by být přijatelný u práce v oboru překladatelství (z angličtiny), ale u bakalářské práce na MFF UK je nutné hodnotit celou práci jako hrubý plagiát.

Konkrétní výčet toho, odkud byly hlavní části práce (kapitoly 2 a 3) opsány, je uveden v příloze tohoto posudku, stejně jako ukázka zdrojového a opsaného textu.

Předkládaná práce podle je mého názoru v zásadním rozporu s požadavky, kladenými na bakalářskou práci (zejména pokud jde o korektní práci s literaturou) a nemůže být připuštěna k obhajobě.

	výborně	velmi dobře	dobře	neprospěl/a
Návrh známky				x

Datum: v Praze. 15.6.2009

Podpis:

Příloha k posudku oponenta

(na bakalářskou práci Andreje Kalického: Firewall a internetová (síťová) bezpečnost

Str. 14 až 17:

Kapitola 2: Firewally: doslovný překlad části hesla „Firewall" na Wikipedii, počínaje částí „History", a konče částí „Subsequent developments". Pouze první a poslední dva odstavce na str. 16, v paragrafu „Následující vývoj", jsou opsány z dokumentu „Evolution of the firewall industry" ((2)).

Str. 18 až 27

Odstavec 2.2.1 až 2.3: opsáno z dokumentu "Evolution of the firewall industry" ((2)), počínaje heslem "How Packet Filters Work" (odstavec 2.2.1) až po heslo "Summary of Performance Vs. Security" (odstavec 2.3).

Str. 27 až 28

Odstavec 2.4: opsáno z knihy "Firewalls and Internet Security" (1), kapitola 9.6, strany 194 a 195

Str. 28 až 29

Odstavec 2.5.: opsáno z hesla „Personal Firewall" na Wikipedii (16)

Str. 29

Odstavec "Distributed Firewalls"" opsáno z knihy "Firewalls and Internet Security" (1), kapitola 9.5, strana 193

Str. 29 až 33

Odstavec 2.6 : opsáno z knihy „Building Internet Firewalls" (12), kapitola 6, strany 122 až 136, místy značně kráceno

Str. 34 až 43

Celá kapitola 3 (Filtrování služeb): opsáno z z knihy "Firewalls and Internet Security" (1), kapitola 10, strany 197 až 210, místy kráceno

Na následující stránce je ukázka původního textu a obsahu posuzované práce:

- Vlevo je ukázka z knihy "Firewalls and Internet Security", strany 197 a 198
- Vpravo je ukázka z práce, kapitoly 3, strany 34 a 35

10

Filtering Services

The decision about what services to filter is based on a desired policy. Nonetheless, some general rules are prudent for most policies. In this chapter, we present our philosophy about these. They are not to be viewed as hard-and-fast rules, but rather as suggestions, or perhaps as a template policy to be customized. This chapter discusses *what* to filter and *why*. The *how* is covered in Chapter 11. The astute reader will note that the services discussed here are a small subset of the ones from Chapter 2. Rather than discuss every possible service, we focus on the more interesting ones, with an eye toward pedagogy.

In this chapter, when we describe a service, we include a summary about how to handle it from a security point of view. It looks something like the following:

protocol	out	in	comment
PROT	x	y	*optional comment*

In this table, legal values for *x* and *y* are as follows:

- **allow** let it through
- **block** don't let it through
- **filter** an application-level proxy should make the decision
- **tunnel** block the port for PROT, but allow users to tunnel it with a more secure protocol

The *out* column refers to the decision about outbound traffic for port PROT. For TCP packets, "outbound" is straightforward; it refers to connections initiated from the inside. "Inbound" refers to connections initiated from the outside.

The meaning is less clear for UDP, because the protocol itself is connectionless. Furthermore, some of the protocols of interest are *not* simple query/response services. For query/response services, we thus speak of an "inbound query," which elicits an "outbound response"; similarly, "outbound queries" elicit "inbound responses." For protocols that do not fit this model, we can speak only of inbound and outbound packets.

10.1 Reasonable Services to Filter

10.1.1 DNS

DNS represents a dilemma for the network administrator. We need information from the outside, but we don't trust the outside. Thus, when we get host name-to-IP address mappings from the outside, it is best not to base any security-related decisions on them. To be more precise, we absolutely must not trust such information for internal purposes, though we may have to rely on it for something like sending sensitive e-mail to external partners.

This has some consequences. Although under some circumstances it might be okay to do name-based authentication for internal machines, it is never acceptable for external machines. We must also ensure that no other internal-to-internal trust relationship depends on any information learned from the outside.

The basic threat is simple: Outsiders can contaminate the DNS cache, notably by including extraneous information in their responses. The details are explained in [Bellovin, 1995]. The rules for outbound DNS queries can be summarized as follows:

protocol	outbound query	inbound response	comment
DNS	allow	filter	*block internal info*

The best way to filter DNS is to use a DNS proxy that does two things [Cheswick and Bellovin, 1996]. First, it redirects queries for internal information to internal DNS servers. Second, it censors inbound responses to ensure that no putatively internal information is returned. This is most likely to occur in the Additional Information or Authoritative Server sections of the response, but could occur anywhere. Nevertheless, one simple rule covers all cases: If it was not in the request, we do not want to know it. (Note that a query for internal information will never be sent to external servers, and hence should never be returned in response to our query.)

Inbound queries are simpler. Put your DNS server in the DMZ. For that matter, you can (and often should) out-source it;[3] as a matter of operational correctness, you should have at least two DNS servers for each zone, and they should be as far apart as possible [Elz *et al.*, 1997]. Do you operate your own machines in widely separated parts of the Internet?

You should be especially certain that you don't have them all on the same LAN. (There are security reasons, too—what if someone DDoS's your link? Make them work harder!) The rules are thus quite simple:

protocol	outbound response	inbound query	comment
DNS	allow	DMZ	

Dealing with the DNS is one of the more difficult problems in setting up a firewall, especially if you use a simple packet filter. It is utterly vital that the gateway machine use it, but it poses many risks.

3. Some people don't believe in out-sourcing such things. We're tempted to ask if they run their own fiber, too. Your ISP—with whom you have a business and contractual relationship—can do far worse things by playing with your traffic than by playing with your DNS. To be sure, you may want to run the primary server yourself, if only for ease of updates, and the advent of DNSsec will make that more necessary.

3 Filtrovanie služieb

Rozhodnutie, aké služby filtrovať paketovým filtrom a firewallom, závisí od požadovanej bezpečnostnej politiky. Napriek tomu niektoré všeobecné filtrujúce pravidlá je rozumné aplikovať pre väčšinu politík. Táto kapitola rozoberá čo filtrovať a prečo. Je zameraná na najzaujímavejšie služby.

Na opísanie a zhrnutie, ako zaobchádzať so službami z bezpečnostného hľadiska, si pomôžeme nasledujúcou tabuľkou:

protocol	out	in	comment
PROTOKOL	x	y	*komentár*

V tabuľke môžu *x* a *y* nadobúdať hodnoty:

- **allow** nechať prejsť (prepustiť)
- **block** nenechať prejsť (neprepustiť)
- **filter** proxy na aplikačnej úrovni rozhodne
- **tunnel** blokovať port PROTOKOLu, ale povoliť užívateľom vytvoriť tunel pomocou bezpečnejšieho protokolu

Stĺpec *out* odkazuje na rozhodnutie o odchádzajúcom (outbound) spojení pre port PROTOKOLu. Pre TCP pakety je odchádzajúce spojenie priamo iniciované z vnútra. Prichádzajúce (inbound) je naopak iniciované z vonku.

Odlišný význam je pre protokol UDP, pretože je bezspojový. Okrem toho, nie všetky protokoly sú jednoduchého query/response službami. Pre query/response služby môžeme hovoriť o "inbound query" (prichádzajúcej požiadavke), ktorá vyvolá "outbound response" (odchádzajúcu odpoveď). Podobne "outbound query" vyvolá "inbound response". Pre protokoly nezapadajúce do tohto modelu môžeme hovoriť iba o prichádzajúcich a odchádzajúcich paketoch (napr. TCP).

3.1 Služby rozumné filtrovať [1]

DNS

DNS predstavuje dilemu pre sieťových administrátorov. Potrebujeme informácie z vonku a pritom nedôverujeme name-to-IP mapovaniu z vonku. Presnejšie, absolútne nemôžeme dôverovať takýmto informáciám pre vnútorné účely. Hoci môžeme byť od nich závislí, napríklad v prípade posielania e-mailu vonkajším spolupracovníkom.

Toto má aj dôsledky. Hoci za určitých okolností môže byť v poriadku name-based autentifikácia pre interné počítače, ale nikdy nie je akceptovateľná pre externé. Musíme zaistiť, aby žiadny dôveryhodný vzťah internal-to-internal (vzťah vnútornej komunikácie) nezávisel od informácie poskytnutej z vonku.

Hrozba je jednoduchá: útočník môže kontaminovať DNS cache do značnej miery priložením cudzej informácie k vyžiadanej odpovedi (response). Pravidlá pre odchádzajúce DNS požiadavky môžeme sumarizovať ako:

protocol	outbound query	inbound response	comment
DNS	allow	filter	*Blokovať interné informácie*

Najlepším spôsobom ako filtrovať DNS je použitie DNS proxy, ktoré prináša dve výhody:

- Presmerovanie požiadaviek o interných informáciách na vnútorný DNS server. Požiadavka tak nebude nikdy priamo odoslaná na vonkajšie servery.
- Cenzurovanie prichádzajúcich odpovedí na zaistenie, aby neviedli zdanlivo interné informácie. To sa môže objaviť v odpovedi zvlášť v sekcii *Additional Information* alebo *Authoritative Server*.

Prichádzajúce požiadavky (queries) sa dajú riešiť jednoduchšie: a to umiestnením DNS servera do DMZ. Záležitosťou operatívnej správnosti je mať aspoň dva DNS servery pre každú zónu. A zaistiť, aby boli od seba v separovaných častiach Internetu a nie všetky v tej istej LAN. Z bezpečnostného hľadiska tak sťažiť útoky typu DDoS (Distributed denial of service – zahltenie servera požiadavkami).

protocol	outbound response	inbound query	comment
DNS	allow	DMZ	

Pohrávanie s DNS je jedným z najzložitejších problémov nastavenia firewallu, obzvlášť pri použití jednoduchého paketového filtra. Ak [illegible] alebo application gateways treba povoliť vonkajší DNS vnútorne, informácie poskytované vonkajšiemu svetu môžu byť minimálne. Dynamické paketové filtre dokážu zaobchádzať rovnako s DNS tak dokonale ako s každým iným UDP založeným protokolom.

Vnútorné počítače potrebujú použiť DNS na dosiahnutie vonkajších sietí. [illegible] spolu s spustení name servera pre doménu na gateway počítači a nejakom vnútornom. NS na vnútornom počítači má skutočné informácie, pokiaľ gateway name server má slabší [illegible] popis zóny.

Problémové miesta sú:

- Povoliť pre Gateway príklad interných adries mien (napríklad pre doménu mailu).
- Povoliť pre vnútorné počítače príklad externých názvov [illegible].
- Poskytnúť spôsob pre prechádzajúce UDP pakety ako prekročiť firewall.