Vlastimil Vagner
vagnev1@fel.cvut.cz

Semestrální práce Y36SPS Linux firewall

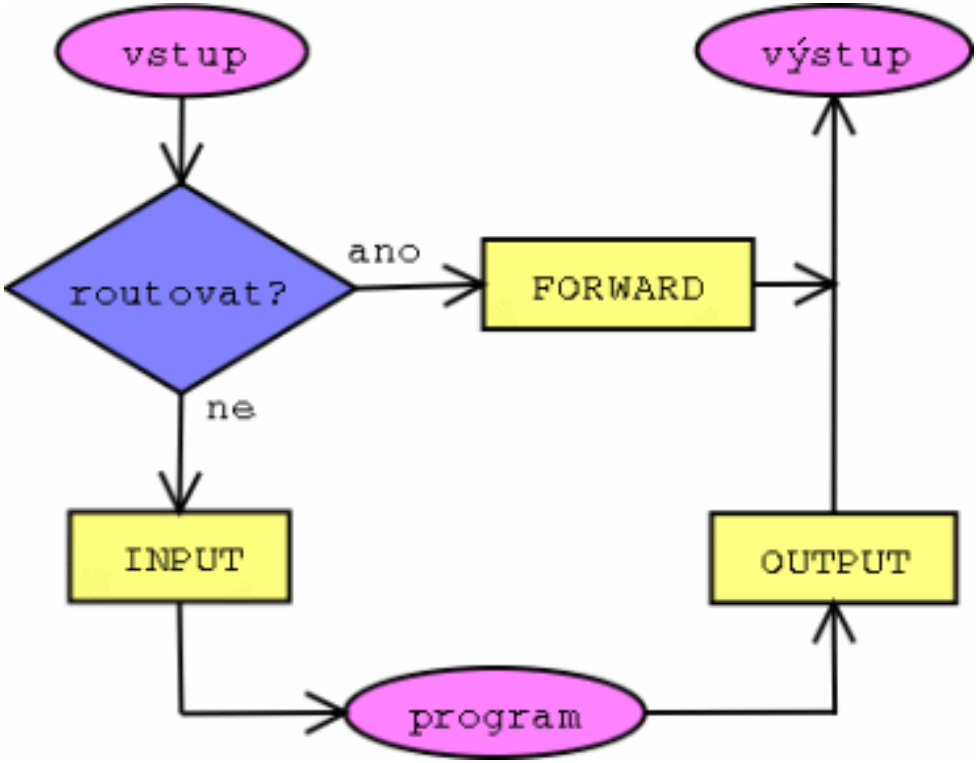
Zadání

- Vytvořit funkční univerzální skript pro automatické zabezpečení linuxu
- Skript prohledá OS, a podle zvoleného typu systému (server, router, pracovní stanice) doporučí postup pro zabezpečení stroje proti síťovým útokům
- Použití nástroje IPTABLES

Předpoklady

- Router s 2 síťovými kartami etho a eth1.
- Běh služeb ftp, http(s), smtp, ssh, pop3, imap, rsync a dns
- Uvnitř sítě je počítač (ssh server, port 2222)
- Požadavky na HTTP jsou transparentně směrovány na proxy-cache
- Musíme nastavit IP addr pro vnější a vnitřní rozhraní
- Nastavení cest k modulům

Princip



Stavový firewall

- Stavový firewall si na rozdíl od paketového filtru navíc udržuje tabulku všech navázaných spojení, která mu slouží pro zjištění, zda pakety náleží do některého otevřeného spojení nebo nikoli. Kvůli paketovému filtru ani stavovému firewallu není nutné měnit stávající aplikace.

IPTABLES

- Konfigurace se provádí pomocí pravidel, podle kterých se Netfilter rozhoduje, co se kterým paketem dělat. Každé pravidlo patří do jedné z tabulek a vztahuje se na jeden řetězec.
- Pokud není nalezeno vyhovující pravidlo, použije se výchozí akce pro řetězec.
- Iptables pracuje se třemi základnimi tabulkami

Splněné požadavky

- zamezení IP spoofování
- routing dovnitř pro navázaná spojení
- zahazování nepovolených paketů
- kontrola nesmyslné IP adresy paketů
- optimalizaci datovych cest (TOS flag)
- nastavení pravidel pro povolené služby
- uvolnění loopback a lokálních paketů
- portscan
- skript pro obnovení původního nastavení

Co je třeba dodělat

- Důkladněji otestovat skript
- Rozšířit jeho použití pro server

Ukázka

```
150 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 80 -j ACCEPT  #WWW server
151 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 110 -j ACCEPT #POP3 server
152 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 143 -j ACCEPT #IMAP server
153 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 443 -j ACCEPT #HTTPS server
154 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 873 -j ACCEPT #rsync server
155
156 # Sluzbu AUTH nefiltrovat pomoci DROP, protoze to muze vest k prodlevam pri navazovani nekterych spojeni. Proto jej
157 # sice zamitneme, ale tak, aby nedoslo k nezadoucim prodlevam.
158 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 113 -m limit --limit 12/h -j LOG
159 $IPTABLES -A INPUT -i $INET_IFACE -p TCP --dport 113 -j REJECT --reject-with tcp-reset #AUTH server
160
161 # Propoustime pouze ICMP ping
162 $IPTABLES -A INPUT -i $INET_IFACE -p ICMP --icmp-type echo-request -j ACCEPT
163
164 # Loopback neomezovat
165 $IPTABLES -A INPUT -i $LO_IFACE -j ACCEPT
166
167 # Stejne jako pakety z lokalni site, jsou-li urceny pro nas
168 $IPTABLES -A INPUT -i $LAN1_IFACE -d $LAN1_IP -j ACCEPT
169 $IPTABLES -A INPUT -i $LAN1_IFACE -d $INET_IP -j ACCEPT
170
171 # Broadcasty na lokalnim rozhrani jsou take nase
172 $IPTABLES -A INPUT -i $LAN1_IFACE -d $LAN1_BCAST -j ACCEPT
173
174 # MS klienti maji chybu v implementaci DHCP
175 $IPTABLES -A INPUT -i $LAN1_IFACE -p udp --dport 67 -j ACCEPT
176
177 # Pakety od navazanych spojeni jsou v poradku
178 $IPTABLES -A INPUT -d $INET_IP -m state --state ESTABLISHED,RELATED -j ACCEPT
179
180 # Vsechno ostatni je zakazano - tedy logujeme, maxim. 12x5 pkt/hod
181 $IPTABLES -A INPUT -m limit --limit 12/h -j LOG --log-prefix "INPUT drop: "
182
183 #
184 # Retezec OUTPUT
```

Děkuji za pozornost