Politiche di filtraggio e di nat

La rete da proteggere appartiene all'azienda FAKE. Tale azienda ha due server pubblicamente accessibili: un server web (che dovrà essere raggiungibile tramite il nome www.fake.com) e un server ftp (che dovrà essere raggiungibile tramite il nome ftp.fake.com). Entrambi i server sono dotati di indirizzi IP privati e sono connessi alla DMZ. Il server web dispone anche di un web proxy, in ascolto sulla porta 8080. Fake ha inoltre una rete locale (LAN) con una macchina (local1) dotata di indirizzo IP privato. Due firewall (int-firewall e ext-firewall) separano la LAN dalla DMZ e la DMZ da Internet. A causa della crisi economica, FAKE ha deciso che un solo indirizzo IP pubblico è più che sufficiente. Tale indirizzo è assegnato all'interfaccia di rete di ext-firewall direttamente connessa ad Internet.

Int-firewall e ext-firewall applicano le regole di filtraggio per limitare il traffico di rete tra LAN e DMZ e tra DMZ e Internet. Entrambi i firewall applicano anche regole di nat. Ext-firewall deve consentire agli host in internet di accedere al server web e al server ftp utilizzando gli indirizzi www.fake.com e ftp.fake.com, che si risolvono entrambi nell'unico indirizzo IP pubblico disponibile.

La macchina local1 è usata dall'amministratore di rete, ed è l'unica macchina che deve essere in grado di accedere da remoto (tramite ssh) a int-firewall e a ext-firewall.

Politiche di filtraggio dei pacchetti

- Utilizzare una policy di negazione implicita per tutti i pacchetti in transito su entrambi i firewall
- Utilizzare una policy di negazione implicita per tutti i pacchetti in ingresso in entrambi i firewall
- Utilizzare una policy di negazione implicita per tutti i pacchetti in uscita da entrambi i firewall
- Consentire a local1 di aprire connessioni ssh verso int-firewall ed ext-firewall
- Consentire connessioni TCP sulla porta 80 dalla LAN verso il server web
- Consentire le risposte del server web a connessioni originate dalla LAN
- Consentire connessioni TCP sulla porta 21 dalla LAN verso il server FTP ftp.fake.com
- Consentire le risposte di ftp.fake.com a connessioni originate dalla LAN
- Consentire connessioni TCP sulla porta 80 da Internet verso il server web
- Consentire le risposte del server web a connessioni originate da Internet
- Consentire connessioni TCP sulla porta 21 da Internet verso il server FTP ftp.fake.com

- Consentire le risposte di ftp.fake.com a connessioni originate da Internet

Politiche di Network Address Translation

- Consentire agli host in Internet di accedere al sito web installato nella DMZ utilizzando l'indirizzo www.fake.com
- Consentire agli host in Internet di accedere al server FTP installato nella DMZ utilizzando l'indirizzo ftp.fake.com

Politiche di filtraggio dei protocolli

- Consentire agli host della LAN di accedere a server web in Internet solo utilizzando il server web installato nella DMZ di FAKE come proxy (non trasparente)

Implementazione delle politiche di filtraggio e di nat

Prima di iniziare

Segue un piccolo elenco di comandi fondamentali. Questi comandi NON fanno parte della soluzione dell'esercitazione, servono solo per ricordare alcuni comandi utili e la loro sintassi.

- *firewall:~# man iptables*

  l'unico comando di cui avete veramente bisogno. Visualizza la pagina di manuale del comando iptables. Per uscire dalla pagina di manuale, premere *q*

- *firewall:~# iptables -t filter -L -v -n*

  visualizza le regole attualmente incluse nelle catene appartenenti alla tabella filter e le loro policy di default. L'opzione *-n* evita che iptables provi ad eseguire il reverse lookup degli indirizzi IP

- *firewall:~# iptables -t filter -P FORWARD DROP*

  imposta la policy di negazione implicita (*DROP*) sulla catena *FORWARD* della tabella *filter*

- *firewall:~# iptables -t filter -A FORWARD -p tcp --dport 22 -i eth0 -j DROP*

  esempio di comando utilizzato per aggiungere una regola di packet filtering statico. Questo comando aggiunge una regola alla catena *FORWARD* della tabella filter. La regola inserita blocca (*-j DROP*) tutti i pacchetti *TCP* aventi *22* come numero di porta di destinazione e che hanno eth0 come interfaccia di ingresso

- *firewall:~# iptables -t filter -D FORWARD 2*

  esempio di eliminazione selettiva di una singola regola. Questo comando elimina la seconda regola della catena *FORWARD* nella tabella filter

- *firewall:~# iptables -t filter -F FORWARD*

  eliminazione di tutte le regole appartenenti alla catena *FORWARD*. Questo comando non modifica la policy di default della catena.

- *firewall:~# iptables -t filter -F*

  eliminazione di tutte le regole appartenenti a tutte le catene della tabella filter. Le policy di default delle catene non vengono modificate

Implementazione delle politiche di NAT

Policy:

Consentire agli host in Internet di accedere al sito web installato nella DMZ utilizzando l'indirizzo www.fake.com

Prima di implementare la policy, verificare che è impossibile per remote1 accedere al server web nella DMZ di fake

remote1:~# w3m www.fake.com

Implementazione:

ext-firewall:~# iptables -t nat -A PREROUTING -p tcp -i eth1 --dport 80 -j DNAT --to-destination 192.168.1.1

Verificare che www.fake.com è diventato accessibile da remote1

Policy:

Consentire agli host in Internet di accedere al server FTP installato nella DMZ utilizzando l'indirizzo ftp.fake.com

Prima di implementare la policy, verificare che è impossibile per remote1 accedere al server FTP nella DMZ di fake

remote1:~# ftp ftp.fake.com

Implementazione:
ext-firewall:~# iptables -t nat -A PREROUTING -p tcp -i eth1 --dport ftp -j DNAT --to-destination 192.168.1.2

Verificare che ftp.fake.com è diventato accessibile da remote1, e che è possibile scaricare file

Implementazione delle politiche di filtraggio

Policy:

Utilizzare una policy di negazione implicita per tutti i pacchetti in transito su entrambi i firewall

Prima di implementare la policy, verificare che è possibile per local1 accedere al server web e al server FTP nella DMZ di FAKE

local1:~# w3m www

local1:~# ftp ftp

Implementazione:

int-firewall:~# iptables -t filter -P FORWARD DROP

ext-firewall:~# iptables -t filter -P FORWARD DROP

Verificare l'impossibilità di comunicare tra le macchine nella DMZ e local1

Verificare l'impossibilità di comunicare tra le macchine nella DMZ e Internet

Verificare che è ancora possibile aprire connessioni ssh verso i firewall

Policy:

Utilizzare una policy di negazione implicita per tutti i pacchetti in ingresso su entrambi i firewall

Utilizzare una policy di negazione implicita per tutti i pacchetti in uscita su entrambi i firewall

Implementazione:

int-firewall:~# iptables -t filter -P INPUT DROP

int-firewall:~# iptables -t filter -P OUTPUT DROP

ext-firewall:~# iptables -t filter -P INPUT DROP

ext-firewall:~# iptables -t filter -P OUTPUT DROP

Verificare che non è più possibile aprire connessioni ssh verso i firewall

Policy:

Consentire a local1 di aprire connessioni ssh verso int-firewall ed ext-firewall

Implementazione:

Iniziamo con il consentire le connessioni ssh da local1 a int-firewall

int-firewall:~# iptables -t filter -A INPUT -p tcp --dport ssh -s 192.168.2.1 -m state --state NEW,ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A OUTPUT -p tcp --sport ssh -d 192.168.2.1 -m state --state ESTABLISHED -j ACCEPT

Verificare che è ora possibile aprire una connessione ssh da local1 a 192.168.2.254 (**N.B.** L'apertura della connessione può richiedere qualche tempo, poiché local1 prova ad effettuare un DNS reverse lookup sull'indirizzo IP al fine di determinare il relativo hostname. Per evitare questo inconveniente, aggiungete la riga “192.168.2.254 int-firewall” al file di configurazione /etc/hosts di local1)

Ora introduciamo le regole necessarie per consentire connessioni ssh da local1 a ext-firewall

int-firewall:~# iptables -t filter -A FORWARD -p tcp --dport ssh -s 192.168.2.1 -d 192.168.1.254 -m state --state NEW,ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A FORWARD -p tcp --sport ssh -d 192.168.2.1 -s 192.168.1.254 -m state --state ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -t filter -A OUTPUT -p tcp --sport ssh -d 192.168.2.1 -m state --state ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -t filter -A INPUT -p tcp --dport ssh -s 192.168.2.1 -m state --state

NEW,ESTABLISHED -j ACCEPT

Verificare che è ora possibile aprire una connessione ssh da local1 a 192.168.1.254 (**N.B.** L'apertura della connessione può richiedere qualche tempo, poiché local1 prova ad effettuare un DNS reverse lookup sull'indirizzo IP al fine di determinare il relativo hostname. Per evitare questo inconveniente, aggiungete la riga "192.168.1.254 ext-firewall" al file di configurazione /etc/hosts di local1)

Policy:

Consentire connessioni TCP sulla porta 80 dalla LAN verso il server web

Consentire le risposte del server web a connessioni originate dalla LAN

Implementazione:

int-firewall:~# iptables -t filter -A FORWARD -s 192.168.2.0/24 -d 192.168.1.1 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A FORWARD -d 192.168.2.0/24 -s 192.168.1.1 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT

Verificare che è ora possibile per local1 accedere al server web nella DMZ di FAKE

Policy:

Consentire connessioni TCP sulla porta 21 dalla LAN verso il server FTP ftp

Consentire le risposte di ftp a connessioni originate dalla LAN

Implementazione:

int-firewall:~# iptables -t filter -A FORWARD -s 192.168.2.0/24 -d 192.168.1.2 -p tcp --dport ftp -m state --state NEW,ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A FORWARD -d 192.168.2.0/24 -s 192.168.1.2 -p tcp --sport ftp -m state --state ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A FORWARD -d 192.168.2.0/24 -s 192.168.1.2 -p tcp --sport ftp-data -m state --state RELATED,ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A FORWARD -s 192.168.2.0/24 -d 192.168.1.2 -p tcp --dport ftp-data -m state --state ESTABLISHED -j ACCEPT

Verificare che è ora possibile per local1 accedere al server ftp nella DMZ di FAKE

Policy:

Consentire connessioni TCP sulla porta 80 da Internet verso il server web

Consentire le risposte del server web a connessioni originate da Internet

Implementazione:

ext-firewall:~# iptables -t filter -A FORWARD -i eth1 -p tcp --dport www -d 192.168.1.1 -m state --state NEW,ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -t filter -A FORWARD -o eth1 -p tcp --sport www -s 192.168.1.1 -m state --state ESTABLISHED -j ACCEPT

Verificare che è possibile per remote1 accedere a www.fake.com

Policy:

Consentire connessioni TCP sulla porta 21 da Internet verso il server FTP ftp.fake.com

Consentire le risposte di ftp.fake.com a connessioni originate da Internet

Implementazione:

ext-firewall:~# iptables -t filter -A FORWARD -i eth1 -p tcp --dport ftp -d 192.168.1.2 -m state --state NEW,ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -t filter -A FORWARD -o eth1 -p tcp --sport ftp -s 192.168.1.2 -m state --state ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -t filter -A FORWARD -o eth1 -p tcp --sport ftp-data -s 192.168.1.2 -m state --state RELATED,ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -t filter -A FORWARD -i eth1 -p tcp --dport ftp-data -d 192.168.1.2 -m state --state ESTABLISHED -j ACCEPT

Verificare che è ora possibile per remote1 accedere al server ftp.fake.com

Implementazione delle politiche di filtraggio dei protocolli

Policy:

Consentire agli host della LAN di accedere a server web in Internet solo utilizzando il server web installato nella DMZ di FAKE come proxy (non trasparente).

Allo stato attuale, la rete LAN è completamente isolata da Internet. Questo garantisce ottimi livelli di sicurezza, a scapito di una scarsa usabilità (per local1 è possibile accedere solo ai servizi erogati dalle macchine nella DMZ). Per consentire alle macchine della LAN di accedere a siti web in Internet senza rendere necessario un contatto diretto tra macchine della LAN e Internet è possibile configurare i client in modo da usare il server www installato nella DMZ di FAKE come proxy. Questo significa che tutte le connessioni verso un server web aperte da un client nella LAN verranno inoltrate verso la porta 8080 di www (dove è in ascolto il software *tinyproxy*). Tinyproxy aprirà le connessioni HTTP a server web in Internet per conto dei client nella LAN, mediando (e loggando, ed eventualmente filtrando) tutte le comunicazioni. Come conseguenza, è inoltre necessario:

- configurare ext-firewall in modo da consentire a www di aprire connessioni verso server web in Internet, e di ricevere le relative risposte
- configurare ext-firewall in modo da effettuare SNAT (.in quanto www ha un indirizzo IP privato)
- configurare int-firewall in modo da consentire le connessioni da host nella LAN alla porta 8080 di www, e le relative risposte
- configurare local1 in modo da usare www come proxy
- configurare tinyproxy in modo da accettare le connessioni provenienti dalle macchine della LAN

Implementazione:

ext-firewall:~# iptables -t nat -A POSTROUTING -p tcp --dport 80 -s 192.168.1.1 -o eth1 -j MASQUERADE

ext-firewall:~# iptables -A FORWARD -p tcp -i eth0 -s 192.168.1.1 --dport 80 -o eth1 -m state --state NEW,ESTABLISHED -j ACCEPT

ext-firewall:~# iptables -A FORWARD -p tcp -o eth0 -d 192.168.1.1 --sport 80 -i eth1 -m state --

state ESTABLISHED -j ACCEPT

A questo punto www.fake.com deve essere in grado di raggiungere www.google.com

int-firewall:~# iptables -t filter -A FORWARD -i eth0 -o eth1 -s 192.168.2.0/24 -d 192.168.1.1 -p tcp --dport 8080 -m state --state NEW,ESTABLISHED -j ACCEPT

int-firewall:~# iptables -t filter -A FORWARD -o eth0 -i eth1 -d 192.168.2.0/24 -s 192.168.1.1 -p tcp --sport 8080 -m state --state ESTABLISHED -j ACCEPT

local1:~# export HTTP_PROXY=http://192.168.1.1:8080/

A questo punto, le richieste di local1 vengono dirottate verso il transparent proxy. Provate ad eseguire il comando

local1:~# w3m www.google.com

Occorre configurare tinyproxy per servire le richieste provenienti da local1. Sulla macchina www.fake.com, modificate il file di configurazione /etc/tinyproxy/tinyproxy.conf aggiungendo la riga “Allow 192.168.2.0/24 ”

www:~# vim /etc/tinyproxy/tinyproxy.conf

e riavviate il proxy per rendere attive le modifiche

www:~# /etc/init.d/tinyproxy restart

Riprovate ad eseguire il comando

local1:~# w3m www.google.com

Diagramma di rete