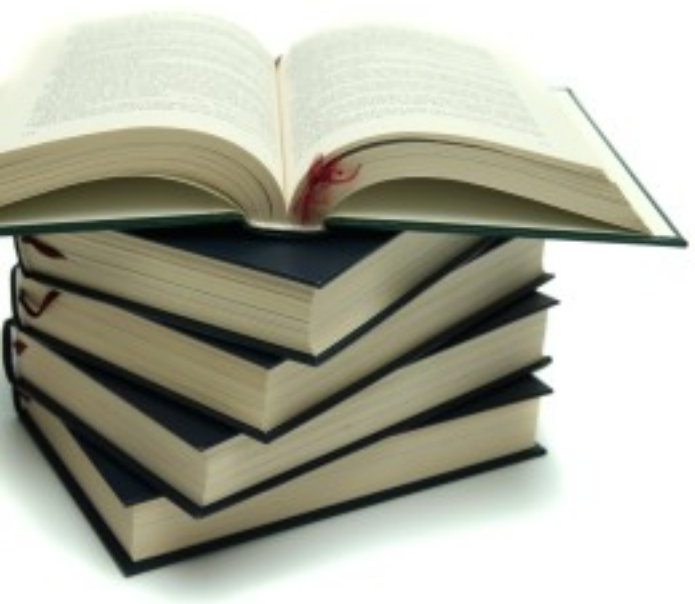
Cursul 6



6

Servicii de securitate

12 noiembrie 2009

There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government.

Bruce Schneier

Bruce Schneier's secure handshake is so strong, you won't be able to exchange keys with anyone else for days. (Bruce Schneier Facts)

Cuprins

- Serviciul SSH
- Facilități SSH; forme de autentificare
- Firewall-uri în Linux: iptables
- GPG
- openssl

Remote connection

- telnet
- rsh, rlogin
- SSH
- VNC
- FreeNX
- RDP

SSH

- Ce este SSH?
  - protocol de comunicare între două dispozitive de rețea printr-un canal securizat
- SSH-2, standard din 2006 (RFC 425x), implementat din 2000
  - SSH-1, „inherent design flaws” (MitM attacks)
- Client-server
  - TCP, portul 22
- OpenSSH
  - „sigle most popular implementation of SSH-2”
  - „This is a software monopoly but at least it was written by people who care about security, so it's not like Microsoft's monopoly.” (Theo de Raadt)
  - echipa OpenBSD
  - 5.3 (1 octombrie 2009)
- Pe sisteme Debian-based, pachetele openssh-client, openssh-server

Comenzi/componente OpenSSH

- ssh
  - clientul SSH
- scp, sftp
  - copierea de fișiere
- sshd
  - serverul SSH
- ssh-keygen
  - generarea de perechi chei publice/private pentru autentificare
- ssh-agent, ssh-add
  - stocarea cheilor și a passphrase-urilor

Facilități oferite de SSH/OpenSSH

- Conectare la distanță pe canal sigur
- Copiere de fișiere la distanță
- Autentificare pe bază de chei publice
- X Forwarding
- Tunelare, reverse tunneling
- SOCKS proxy

Conectare la distanță

- ssh anaconda.cs.pub.ro
  - se folosește ca login numele utilizatorului curent
- ssh razvan@anaconda.cs.pub.ro
- ssh -l razvan anaconda.cs.pub.ro
- ssh -l razvan anaconda.cs.pub.ro -p 2222
- ssh -l razvan anaconda.cs.pub.ro -p 2222 „/sbin/ifconfig eth0”

Copiere la/de la distanță

- scp my_file.txt razvan@anaconda.cs.pub.ro:
  - upload
  - nu mai merge -l :-(
  - nu uitați simbolul două puncte (:) (de la sfârșit)
- scp my_file.txt razvan@anaconda.cs.pub.ro:/tmp/rd/
- scp my_file.txt razvan@anaconda.cs.pub.ro:code/channel/
- scp razvan@anaconda.cs.pub.ro:code/test.c .
  - download
  - destinația este directorul curent (punct - .) (la sfârșit)
- scp -r razvan@anaconda.cs.pub.ro:code/ local-copy
- scp -P 2222 -r razvan@anaconda.cs.pub.ro:code/ /tmp/rd/
  - portul trebuie pus înainte de sursă
- scp -r razvan@swarm.cs.pub.ro:local-swarm/ razvan@anaconda.cs.pub.ro:local-anaconda
  - Merge?
    - depinde :-)

Autentificare folosind chei publice

- De ce?
  - mai sigură – nu trebuie să reții parole
    - poate fi protejată prin passphrase
  - one key to rule them all (acces la toate conturile)
  - automatizare
    - merge și la autentificare fără chei, folosind expect (da' mai greu :-) și ne e lene)
- Cine se autentifică la cine?
  - serverul la client (tot timpul)
    - ~/.ssh/known_hosts
    - /etc/sshd/ssh_host_*_key{,.pub}
  - clientul la server
    - situația obișnuită în care se discută despre autentificare folosind chei publice
- RSA, DSA
- Comunicarea efectivă este criptată folosind cheie simetrică
  - mai rapidă

Generarea unei perechi de chei

- ssh-keygen
  - utilitar implicit interactiv
- ssh-keygen -t rsa
  - solicită nume fișier cheie privată (implicit ~/.ssh/id_rsa)
    - cheia publică primește extensia .pub
  - solicită introducerea passphrase-ului
- ssh-keygen -t rsa -f /tmp/my_key
  - solicită introducere passphrase-ului
- ssh-keygen -t rsa -f /tmp/my_key -N „”
  - fără passphrase
- ssh-keygen -t rsa -f /tmp/my_key -N „s@|dh43)k2D-#A”

Copierea unei chei pe server

- Cheia publică trebuie să fie adăugată în fișierul ~/.ssh/authorized_keys al utilizatorului de la distanță
- First choice: manually
  - scp /tmp/my_key.pub razvan@anaconda.cs.pub.ro:
  - ssh razvan@anaconda.cs.pub.ro „cat /tmp/my_key.pub >> ~/.ssh/authorized_keys”
    - se presupune directorul ~/.ssh/ creat
- Second choice: automatically
  - ssh-copy-id -i /tmp/my_key razvan@anaconda.cs.pub.ro
    - creează directoare etc.
    - are nevoie de acces la cheia privată
- Third choice: my way
  - cat id_rsa.pub | ssh -l root koala.cs.pub.ro „cat - >> ~user/.ssh/authorized_keys”
    - trebuie creat directorul ~/.ssh/
    - util pentru administratori – vrei să adaugi cheia publică a cuiva la un cont

Conectarea/copierea folosind chei publice

- La fel ca până acum
- Trebuie să ai acces la cheia privată
- Dacă folosești mai multe chei private?
  - cheia privată se mai cheamă **identity file**
  - ssh -i /tmp/my_key -l razvan anaconda.cs.pub.ro
  - scp -i /tmp/my_key ....

ssh-agent

- Agent de autentificare
- Reține chei private (identități)
  - permite introducerea o singură dată a passphrase-ului
- Rulează ca un daemon
- Interacțiune folosind comanda ssh-add
- Pornit cu interfața grafică
- Pentru linia de comandă
  - ssh-agent bash ; un nou shell
  - eval $(ssh-agent) ; în shell-ul curent

ssh-agent (2)

- ssh-add
  - adaugă cheile private implicite (~/.ssh/id_rsa, ~/.ssh/id_dsa)
  - solicită passphrase-ul dacă este cazul
- ssh-add /tmp/my_key
- ssh-add -l, ssh-add -L
- ssh-add -d /tmp/my_key
- ssh-add -D
- Avantaje
  - nu se mai solicită passphrase
  - nu trebuie menționată cheia privată în cazul în care sunt mai multe
  - agent-forwarding pentru scp user1@a.com: user2@b.com:

Tunelare și reverse tunneling

- ssh -L 8080:anaconda.cs.pub.ro:80 -l razvan anaconda.cs.pub.ro
  - conexiunile pe portul local 8080 sunt transmise securizat către portul 80 al anaconda.cs.pub.ro
- ssh -N -L 8080:swarm.cs.pub.ro:80 -l razvan anaconda.cs.pub.ro
  - -N - nu se execută comandă (forwarding only)
  - conexiune securizată până la anaconda.cs.pub.ro
  - nesecurizată între anaconda.cs.pub.ro și swarm.cs.pub.ro
- ssh -N -R 2222:localhost:22 -l razvan anaconda.cs.pub.ro
  - conexiunile pe portul 2222 de pe anaconda.cs.pub.ro ajung pe portul 22 al sistemului local
  - dacă nu avem adresă IP publică (suntem în spatele lui NAT)
- ssh -N -R 8080:localhost:80 -l razvan anaconda.cs.pub.ro
  - acces securizat la serverul web între anaconda.cs.pub.ro și stația locală

SOCKS proxy

- ssh -D 8080 -l razvan anaconda.cs.pub.ro
- totul este proxy-at prin anaconda.cs.pub.ro (no more limitations :-P)

X Forwarding

- Serverul trebuie să permită X Forwarding
- ssh -X -l razvan anaconda.cs.pub.ro
  - comenzile rulate prin SSH sunt redate pe sistemul local

Configurare server SSH

- /etc/ssh/sshd_config
- /etc/init.d/ssh start|stop|restart|reload
- Port 22
- HostKey /etc/ssh/ssh_host_rsa_key
- SyslogFacility AUTH
- LogLevel INFO
  - logging în /var/log/auth.log
- PubkeyAuthentication yes
- PasswordAuthentication no
  - autentificare dezactivată fără parole (doar folosind chei publice)
- AllowUsers / DenyUsers
- PermitRootLogin
- man sshd_config

Useful tools

- corkscrew
  - tunelare trafic SSH prin proxy-uri HTTP
- dropbear
  - implementare SSH pentru sisteme embedded
  - fără SSH-1, fără scp
- SSHFS
  - SSH filesystem, folosește FUSE
- Putty, WinSCP
  - Clienți de SSH/SCP pe Windows
- WebShell
  - sesiune shell pe o conexiune HTTP (interfață în browser)

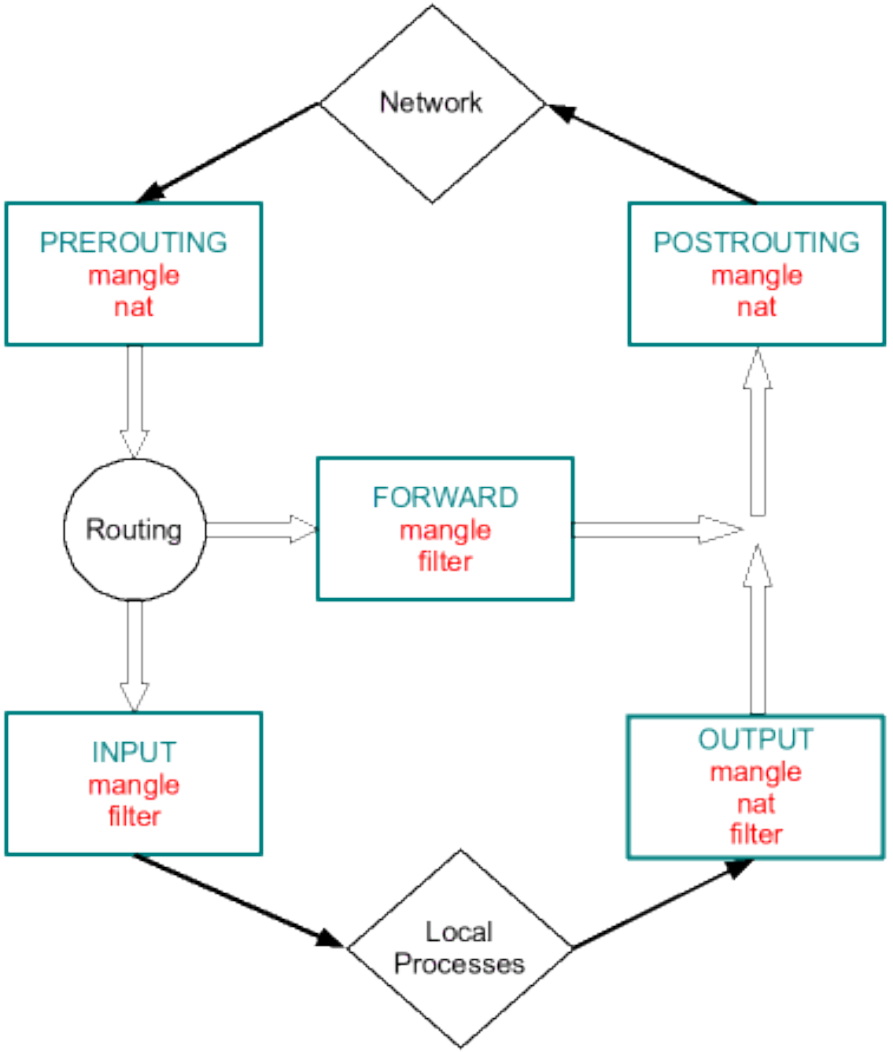
Firewall-uri

- Hardware
  - viteză mare
  - oferă și criptare
- Software
  - viteză mai mică
  - flexibile
  - personale și la nivelul sistemelor de operare

iptables

- Interfață în userspace pentru controlul tabelelor furnizate de modulul netfilter
  - filter
  - nat
  - mangle
- ip6tables pentru ipv6
- Folosește tabele
- Fiecare tabelă folosește lanțuri
  - lanțuri predefinite (INPUT, OUTPUT, FORWARD)
  - lanțuri definite de utilizator
  - versiunea anterioară se numea ipchains
- Lanțurile conțin reguli (de filtrare, translatare de adrese, mangling)

iptables (2)


Network
PREROUTING
mangle
nat
POSTROUTING
mangle
nat
Routing
FORWARD
mangle
filter
INPUT
mangle
filter
OUTPUT
mangle
nat
filter
Local
Processes

Sintaxa iptables

- iptables <tabelă> <comandă> <lanț> <opțiuni comandă>
- Tabela implicită este filter (filtrare, firewall)
- iptables -t filter -L
- iptables -t filter -L -n
- iptables -t nat -L OUTPUT -v
- iptables -t mangle -L OUTPUT -v -n --line-number

Comenzi iptables

- flush reguli
  - iptables -t filter -F
  - iptables -t nat -F PREROUTING
- politica implicită
  - poate fi configurată explicit
  - iptables -t filter -P INPUT DROP
- lanț nou (creare, ștergere, redenumire)
  - iptables -N mychain
  - iptables -X
  - iptables -X mychain
  - iptables -E mychain mynewchain

Comenzi iptables (2)

- Lucrul cu reguli
- <opțiuni comandă> = <specificare de reguli>
  - parte de match + parte de acțiune (-j action)
- Adăugare regulă (append)
  - iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
- Inserare regulă
  - iptables -t filter -I INPUT 2 -s 10.38.1.2 -d 141.85.37.25 -p tcp - -dport 80 ! --syn -j ACCEPT
- Ștergere regulă
  - iptables -t nat -D 1
  - iptables -t mangle -D OUTPUT -d 141.85.37.25 -p icmp -j TTL --ttl-set 8
- Înlocuire regulă
  - iptables -t nat -R PREROUTING 1 -i eth1 -p tcp - -dport 8080 -j DNAT --to-destination 10.38.5.6:80

Persistența regulilor

- Regulile sunt introduse în linia de comandă
- Nu s-a impus un utilitar care să permită automatizare generării regulilor
- Cum se păstrează regulile?

```
# iptables-save > /etc/network/iptables.rules


# cat /etc/network/if-up.d/iptables
#!/bin/bash
iptables-restore < /etc/network/iptables.rules
exit 0
```

Interfețe peste iptables

- Firewall Builder (http://www.fwbuilder.org/)
- Firestarter (http://www.fs-security.com/)
- IPTables Firewall (RedHat only) (http://www.iptablesfirewall.com/)
- Webmin module (http://www.webmin.com/)

GPG

- GNU Privacy Guard
- Suite of cryptographic software
- Alternativă free la PGP (Pretty Good Privacy)
- Semnarea mesajelor
- Criptarea informației

Operații GPG

- Generarea perechii de chei
  - gpg –gen-key
- Listare chei
  - gpg --list-keys
- Export cheie publică
  - gpg --armor --export AEA0A627 >> rd_gpg.pub
- Import cheie publică (pe alt sistem)
  - gpg --import rd_gpg.pub
- Verificare fingerprint
  - gpg --fingerprint

Operații GPG

- Semnarea unei chei
  - gpg --sign-key AEA0A627
- Criptarea unui mesaj
  - gpg -r AEA0A627 --armor --output todo.enc --encrypt todo-2009-11-08.txt
- Decriptarea unui mesaj
  - gpg --decrypt todo.enc > out.txt
- Semnarea unui fișier
  - gpg --default-key 449BE5C2 --armor --sign todo-2009-11-08.txt
  - gpg --default-key 449BE5C2 --armor --detach-sig todo-2009-11-08.txt
- Verificarea unui fișier (semnătura este validă)
  - gpg --default-key 449BE5C2 --verify todo-2009-11-08.txt.asc

GPG frontends

- Seahorse (GNOME)
- Kgpg
- Front-end-uri pentru clienți de e-mail
- Mac GPG

openssl

- Cryptographic toolkit
- SSL/TLS
- OpenSSL crypto library
- openssl – utilitar în linia de comandă
  - generare de chei publice/private
  - operații cu chei publice
  - **lucru cu certificate X.509**

openssl – lucrul cu certificate

- Crearea unei chei private
  - openssl genrsa -out www.gogu.com.key 1024
- Crearea unui CSR (Certificate Signing Request)
  - openssl req -new -key www.gogu.com.key -out www.gogu.com.csr
- Obținerea unui certificat self-signed
  - openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
- Semnarea unui CSR (de un CA – Certification Authority)
  - openssl x509 -req -days 365 -in www.gogu.com.csr -CA server.crt -CAkey server.key -set_serial 01 -out www.gogu.com.crt

openssl – inspecție certificate

- openssl rsa -noout -text -in server.key
- openssl x509 -noout -text -in server.crt
- openssl rsa -noout -text -in www.gogu.com.key
- openssl req -noout -text -in www.gogu.com.csr
- openssl x509 -noout -text -in www.gogu.com.crt

Cuvinte cheie

- SSH
- OpenSSH
- ssh, scp
- chei publice/private
- ssh-keygen
- ssh-agent, ssh-add
- ~/.ssh/known_hosts
- ~/.ssh/authorized_keys
- tunelare, reverse tunneling
- SOCKS proxy
- X Forwarding
- sshd
- /etc/ssh/sshd_confing
- firewall
- iptables, netfilter
- tabelă, lanț, regulă
- iptables-save, iptables-restore
- GPG, PGP
- gpg
- semnare, criptare
- openssl
- CSR, certificat
- CA

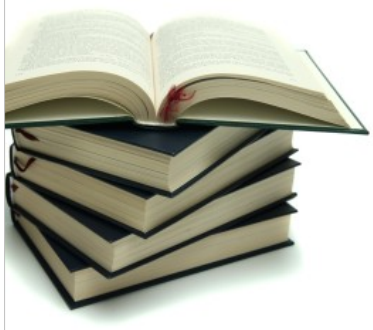
Bibliografie

- SSH, The Secure Shell: The Definitive Guide
- http://www.linuxjournal.com/article/4412 (101 Uses of OpenSSH)
- http://talks.rosedu.org/prezentari (SSH)
- http://www.netfilter.org/
- http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables
- http://www.shell-tips.com/sheets/linux_quickref.pdf
- http://www.tc.umn.edu/~brams006/selfsign.html

Întrebări

?

Cursul 6



6

Servicii de securitate

12 noiembrie 2009

Moto

There are two types of encryption: one that will prevent your sister from reading your diary and one that will prevent your government.

Bruce Schneier

Bruce Schneier's secure handshake is so strong, you won't be able to exchange keys with anyone else for days. (Bruce Schneier Facts)

Cuprins

- Serviciul SSH
- Facilități SSH; forme de autentificare
- Firewall-uri în Linux: iptables
- GPG
- openssl

Remote connection

- telnet
- rsh, rlogin
- SSH
- VNC
- FreeNX
- RDP

SSH

- Ce este SSH?
  - protocol de comunicare între două dispozitive de rețea printr-un canal securizat
- SSH-2, standard din 2006 (RFC 425x), implementat din 2000
  - SSH-1, „inherent design flaws” (MitM attacks)
- Client-server
  - TCP, portul 22
- OpenSSH
  - „sigle most popular implementation of SSH-2”
  - „This is a software monopoly but at least it was written by people who care about security, so it's not like Microsoft's monopoly.” (Theo de Raadt)
  - echipa OpenBSD
  - 5.3 (1 octombrie 2009)
- Pe sisteme Debian-based, pachetele openssh-client, openssh-server

Comenzi/componente OpenSSH

- ssh
  - clientul SSH
- scp, sftp
  - copierea de fișiere
- sshd
  - serverul SSH
- ssh-keygen
  - generarea de perechi chei publice/private pentru autentificare
- ssh-agent, ssh-add
  - stocarea cheilor și a passphrase-urilor

Facilități oferite de SSH/OpenSSH

- Conectare la distanță pe canal sigur
- Copiere de fișiere la distanță
- Autentificare pe bază de chei publice
- X Forwarding
- Tunelare, reverse tunneling
- SOCKS proxy

Conectare la distanță

- ssh anaconda.cs.pub.ro
  - se folosește ca login numele utilizatorului curent
- ssh razvan@anaconda.cs.pub.ro
- ssh -l razvan anaconda.cs.pub.ro
- ssh -l razvan anaconda.cs.pub.ro -p 2222
- ssh -l razvan anaconda.cs.pub.ro -p 2222 „/sbin/ifconfig eth0”

Copiere la/de la distanță

- scp my_file.txt razvan@anaconda.cs.pub.ro:
  - upload
  - nu mai merge -l :-(
  - nu uitați simbolul două puncte (:) (de la sfârșit)
- scp my_file.txt razvan@anaconda.cs.pub.ro:/tmp/rd/
- scp my_file.txt razvan@anaconda.cs.pub.ro:code/channel/
- scp razvan@anaconda.cs.pub.ro:code/test.c .
  - download
  - destinația este directorul curent (punct - .) (la sfârșit)
- scp -r razvan@anaconda.cs.pub.ro:code/ local-copy
- scp -P 2222 -r razvan@anaconda.cs.pub.ro:code/ /tmp/rd/
  - portul trebuie pus înainte de sursă
- scp -r razvan@swarm.cs.pub.ro:local-swarm/ razvan@anaconda.cs.pub.ro:local-anaconda
  - Merge?
    - depinde :-)

Autentificare folosind chei publice

- De ce?
  - mai sigură – nu trebuie să reții parole
    - poate fi protejată prin passphrase
  - one key to rule them all (acces la toate conturile)
  - automatizare
    - merge și la autentificare fără chei, folosind expect (da' mai greu :-) și ne e lene)
- Cine se autentifică la cine?
  - serverul la client (tot timpul)
    - ~/.ssh/known_hosts
    - /etc/sshd/ssh_host_*_key{,.pub}
  - clientul la server
    - situația obișnuită în care se discută despre autentificare folosind chei publice
- RSA, DSA
- Comunicarea efectivă este criptată folosind cheie simetrică
  - mai rapidă

Generarea unei perechi de chei

- ssh-keygen
  - utilitar implicit interactiv
- ssh-keygen -t rsa
  - solicită nume fișier cheie privată (implicit ~/.ssh/id_rsa)
    - cheia publică primește extensia .pub
  - solicită introducerea passphrase-ului
- ssh-keygen -t rsa -f /tmp/my_key
  - solicită introducere passphrase-ului
- ssh-keygen -t rsa -f /tmp/my_key -N „”
  - fără passphrase
- ssh-keygen -t rsa -f /tmp/my_key -N „s@|dh43)k2D-#A”

Copierea unei chei pe server

- Cheia publică trebuie să fie adăugată în fișierul ~/.ssh/authorized_keys al utilizatorului de la distanță
- First choice: manually
  - scp /tmp/my_key.pub razvan@anaconda.cs.pub.ro:
  - ssh razvan@anaconda.cs.pub.ro „cat /tmp/my_key.pub >> ~/.ssh/authorized_keys”
    - se presupune directorul ~/.ssh/ creat
- Second choice: automatically
  - ssh-copy-id -i /tmp/my_key razvan@anaconda.cs.pub.ro
    - creează directoare etc.
    - are nevoie de acces la cheia privată
- Third choice: my way
  - cat id_rsa.pub | ssh -l root koala.cs.pub.ro „cat - >> ~user/.ssh/authorized_keys”
    - trebuie creat directorul ~/.ssh/
    - util pentru administratori – vrei să adaugi cheia publică a cuiva la un cont

Conectarea/copierea folosind chei publice

- La fel ca până acum
- Trebuie să ai acces la cheia privată
- Dacă folosești mai multe chei private?
  - cheia privată se mai cheamă **identity file**
  - ssh -i /tmp/my_key -l razvan anaconda.cs.pub.ro
  - scp -i /tmp/my_key ....

ssh-agent

- Agent de autentificare
- Reține chei private (identități)
  - permite introducerea o singură dată a passphrase-ului
- Rulează ca un daemon
- Interacțiune folosind comanda ssh-add
- Pornit cu interfața grafică
- Pentru linia de comandă
  - ssh-agent bash ; un nou shell
  - eval $(ssh-agent) ; în shell-ul curent

ssh-agent (2)

- ssh-add
  - adaugă cheile private implicite (~/.ssh/id_rsa, ~/.ssh/id_dsa)
  - solicită passphrase-ul dacă este cazul
- ssh-add /tmp/my_key
- ssh-add -l, ssh-add -L
- ssh-add -d /tmp/my_key
- ssh-add -D
- Avantaje
  - nu se mai solicită passphrase
  - nu trebuie menționată cheia privată în cazul în care sunt mai multe
  - agent-forwarding pentru scp user1@a.com: user2@b.com:

Tunelare și reverse tunneling

- ssh -L 8080:anaconda.cs.pub.ro:80 -l razvan anaconda.cs.pub.ro
  - conexiunile pe portul local 8080 sunt transmise securizat către portul 80 al anaconda.cs.pub.ro
- ssh -N -L 8080:swarm.cs.pub.ro:80 -l razvan anaconda.cs.pub.ro
  - -N - nu se execută comandă (forwarding only)
  - conexiune securizată până la anaconda.cs.pub.ro
  - nesecurizată între anaconda.cs.pub.ro și swarm.cs.pub.ro
- ssh -N -R 2222:localhost:22 -l razvan anaconda.cs.pub.ro
  - conexiunile pe portul 2222 de pe anaconda.cs.pub.ro ajung pe portul 22 al sistemului local
  - dacă nu avem adresă IP publică (suntem în spatele lui NAT)
- ssh -N -R 8080:localhost:80 -l razvan anaconda.cs.pub.ro
  - acces securizat la serverul web între anaconda.cs.pub.ro și stația locală

SOCKS proxy

- ssh -D 8080 -l razvan anaconda.cs.pub.ro
- totul este proxy-at prin anaconda.cs.pub.ro (no more limitations :-P)

X Forwarding

- Serverul trebuie să permită X Forwarding
- ssh -X -l razvan anaconda.cs.pub.ro
  - comenzile rulate prin SSH sunt redate pe sistemul local

Configurare server SSH

- /etc/ssh/sshd_config
- /etc/init.d/ssh start|stop|restart|reload
- Port 22
- HostKey /etc/ssh/ssh_host_rsa_key
- SyslogFacility AUTH
- LogLevel INFO
  - logging în /var/log/auth.log
- PubkeyAuthentication yes
- PasswordAuthentication no
  - autentificare dezactivată fără parole (doar folosind chei publice)
- AllowUsers / DenyUsers
- PermitRootLogin
- man sshd_config

Useful tools

- corkscrew
  - tunelare trafic SSH prin proxy-uri HTTP
- dropbear
  - implementare SSH pentru sisteme embedded
  - fără SSH-1, fără scp
- SSHFS
  - SSH filesystem, folosește FUSE
- Putty, WinSCP
  - Clienți de SSH/SCP pe Windows
- WebShell
  - sesiune shell pe o conexiune HTTP (interfață în browser)

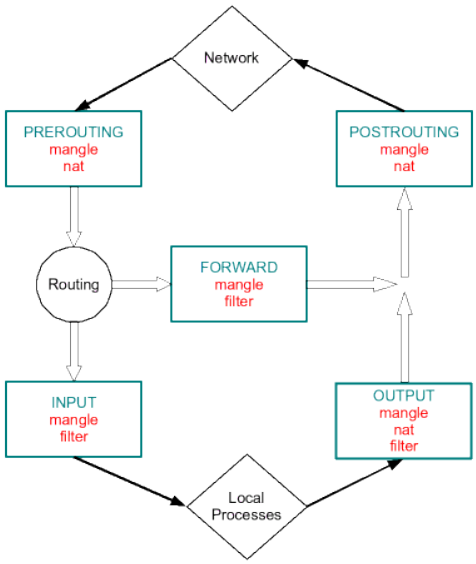
Firewall-uri

- Hardware
  - viteză mare
  - oferă și criptare
- Software
  - viteză mai mică
  - flexibile
  - personale și la nivelul sistemelor de operare

iptables

- Interfață în userspace pentru controlul tabelelor furnizate de modulul netfilter
  - filter
  - nat
  - mangle
- ip6tables pentru ipv6
- Folosește tabele
- Fiecare tabelă folosește lanțuri
  - lanțuri predefinite (INPUT, OUTPUT, FORWARD)
  - lanțuri definite de utilizator
  - versiunea anterioară se numea ipchains
- Lanțurile conțin reguli (de filtrare, translatare de adrese, mangling)

iptables (2)


Network
PREROUTING
mangle
nat
POSTROUTING
mangle
nat
Routing
FORWARD
mangle
filter
INPUT
mangle
filter
OUTPUT
mangle
nat
filter
Local
Processes

Sintaxa iptables

- iptables <tabelă> <comandă> <lanț> <opțiuni comandă>
- Tabela implicită este filter (filtrare, firewall)
- iptables -t filter -L
- iptables -t filter -L -n
- iptables -t nat -L OUTPUT -v
- iptables -t mangle -L OUTPUT -v -n --line-number

Comenzi iptables

- flush reguli
  - iptables -t filter -F
  - iptables -t nat -F PREROUTING
- politica implicită
  - poate fi configurată explicit
  - iptables -t filter -P INPUT DROP
- lanț nou (creare, ștergere, redenumire)
  - iptables -N mychain
  - iptables -X
  - iptables -X mychain
  - iptables -E mychain mynewchain

Comenzi iptables (2)

- Lucrul cu reguli
- <opțiuni comandă> = <specificare de reguli>
  - parte de match + parte de acțiune (-j action)
- Adăugare regulă (append)
  - iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
- Inserare regulă
  - iptables -t filter -I INPUT 2 -s 10.38.1.2 -d 141.85.37.25 -p tcp - -dport 80 ! --syn -j ACCEPT
- Ștergere regulă
  - iptables -t nat -D 1
  - iptables -t mangle -D OUTPUT -d 141.85.37.25 -p icmp -j TTL --ttl-set 8
- Înlocuire regulă
  - iptables -t nat -R PREROUTING 1 -i eth1 -p tcp - -dport 8080 -j DNAT --to-destination 10.38.5.6:80

Persistența regulilor

- Regulile sunt introduse în linia de comandă
- Nu s-a impus un utilitar care să permită automatizare generării regulilor
- Cum se păstrează regulile?

```
# iptables-save > /etc/network/iptables.rules


# cat /etc/network/if-up.d/iptables
#!/bin/bash
iptables-restore < /etc/network/iptables.rules
exit 0
```

Interfețe peste iptables

- Firewall Builder (http://www.fwbuilder.org/)
- Firestarter (http://www.fs-security.com/)
- IPTables Firewall (RedHat only) (http://www.iptablesfirewall.com/)
- Webmin module (http://www.webmin.com/)

GPG

- GNU Privacy Guard
- Suite of cryptographic software
- Alternativă free la PGP (Pretty Good Privacy)
- Semnarea mesajelor
- Criptarea informației

Operații GPG

- Generarea perechii de chei
  - gpg –gen-key
- Listare chei
  - gpg --list-keys
- Export cheie publică
  - gpg --armor --export AEA0A627 >> rd_gpg.pub
- Import cheie publică (pe alt sistem)
  - gpg --import rd_gpg.pub
- Verificare fingerprint
  - gpg --fingerprint

Operații GPG

- Semnarea unei chei
  - gpg --sign-key AEA0A627
- Criptarea unui mesaj
  - gpg -r AEA0A627 --armor --output todo.enc --encrypt todo-2009-11-08.txt
- Decriptarea unui mesaj
  - gpg --decrypt todo.enc > out.txt
- Semnarea unui fișier
  - gpg --default-key 449BE5C2 --armor --sign todo-2009-11-08.txt
  - gpg --default-key 449BE5C2 --armor --detach-sig todo-2009-11-08.txt
- Verificarea unui fișier (semnătura este validă)
  - gpg --default-key 449BE5C2 --verify todo-2009-11-08.txt.asc

GPG frontends

- Seahorse (GNOME)
- Kgpg
- Front-end-uri pentru clienți de e-mail
- Mac GPG

openssl

- Cryptographic toolkit
- SSL/TLS
- OpenSSL crypto library
- openssl – utilitar în linia de comandă
  - generare de chei publice/private
  - operații cu chei publice
  - **lucru cu certificate X.509**

openssl – lucrul cu certificate

- Crearea unei chei private
  - openssl genrsa -out www.gogu.com.key 1024
- Crearea unui CSR (Certificate Signing Request)
  - openssl req -new -key www.gogu.com.key -out www.gogu.com.csr
- Obținerea unui certificat self-signed
  - openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
- Semnarea unui CSR (de un CA – Certification Authority)
  - openssl x509 -req -days 365 -in www.gogu.com.csr -CA server.crt -CAkey server.key -set_serial 01 -out www.gogu.com.crt

openssl – inspecție certificate

- openssl rsa -noout -text -in server.key
- openssl x509 -noout -text -in server.crt
- openssl rsa -noout -text -in www.gogu.com.key
- openssl req -noout -text -in www.gogu.com.csr
- openssl x509 -noout -text -in www.gogu.com.crt

Cuvinte cheie

- SSH
- OpenSSH
- ssh, scp
- chei publice/private
- ssh-keygen
- ssh-agent, ssh-add
- ~/.ssh/known_hosts
- ~/.ssh/authorized_keys
- tunelare, reverse tunneling
- SOCKS proxy
- X Forwarding
- sshd
- /etc/ssh/sshd_confing
- firewall
- iptables, netfilter
- tabelă, lanț, regulă
- iptables-save, iptables-restore
- GPG, PGP
- gpg
- semnare, criptare
- openssl
- CSR, certificat
- CA

Bibliografie

- SSH, The Secure Shell: The Definitive Guide
- http://www.linuxjournal.com/article/4412 (101 Uses of OpenSSH)
- http://talks.rosedu.org/prezentari (SSH)
- http://www.netfilter.org/
- http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables
- http://www.shell-tips.com/sheets/linux_quickref.pdf
- http://www.tc.umn.edu/~brams006/selfsign.html

Întrebări