Short brief of SSH

Vložil/a il_man [1], 6 Listopad, 2005 - 15:25

- Encryption [2]
- Security [3]

K cemu SSH je? Mno pouziva se na pripojeni ke vzdalenemu serveru... kde nam povoli spoustet prikazy (vzdaleny terminal), popripade kopirovat ruzne soubory, vlastne jako by jsme byli u daneho pocitace. Kdykoliv se ssh z nejaky masiny pripoji na jinou tak vytvori sifrovany kanal tim se stava mnohem vyhodnejsi oproti napr. telnetu, rsh apod.

Problem s temito "starsimi" protokoly (telnet atd..) je hlavne ten, ze posilaji naprosto vsechno nezasifrovane cili vcetne vasich prihlasovacich udaju potazmo prikazu... pro cloveka ktery si odchytava vami poslane pakety neni problem je cist ci hur je menit, pak misto treba ls / muze poslat rm -r / atd. Diky tomu, ze tyto protokoly nemaji "poneti" s kym to hovori tak je utoku cela rada.
Pri pripojeni na neznamy stroj se nam zobrazi neco jako:

```
$ ssh ssh-server.cz
The authenticity of host 'ssh-server.cz' (xxx.xxx.xxx.xxx) can't beestablished.
RSA key fingerprint is 98:e4:54:d8:f7:c2: ......
Are u sure u want to continue connecting (yes/no) ?
```

mno a ted pokud budeme souhlasit tak se nam klic toho pocitace prida permanentne k nasim znamym klicum (/etc/ssh/ssh_known_hosts) pote pokazde, kdyz se budeme chtit prihlasit znova k tehle masine tak, uz se nas to nebude ptat, jestli chceme verit-ulozit klic, ale rovnou nas pozada o zadani jmena... pokud jsme paranoidni tak se da nastavit aby nas klient pokazde kontoloval fingerprinty...

Pokud se na stroj takto prihlasime, nebo i predtim poprve, tak je dobre ocheckovat jestli klic-fingerprint, ktery jsme prijmuly do znamych souhlasi s klicem stroje kam se chceme prihlasit, protoze se nam mohlo stat, ze nam nekdo tento klic podvrhnul ...

Overeni muzeme provest nekolika zpusoby, jeden trosku krkolomny, proste zavolat adminovi, aby nam ho rekl, nebo vhodnejsi zpusob pokud je klic zverejnen nekde na strankach, tak prez ssl nebo jinou zabezpecenou cestu ho zkontrolovat ... pokud neni nejaka jina cesta "venkem" muzeme udelat jinou vec a to podivat se primo na stroji kam jsme se prihlasili ten se da zkontrolovat ve slozce /etc/ssh/ prikazem:

```
ls *.pub | xargs -nl  ssh-keygen -lf
```

ten vam vypise vsechny figerprinty jak rsa tak dsa pro vsechny verejne klice...
pokud chcete vypsat jen jeden klic:

```
ssh-keygen -lf /etc/ssh/ssh_host_typklice_key.pub
```

Timto jsme odbyli prihlaseni k masine, ale co kdyz nas nebavi neustale zadavat prihlasovaci udaje nebo nam tato metoda pripada malo bezpecna? Co pak? Tady na scenu prichazi metoda zvana Identity/Pubkey, zadavani jmena a hesla je sice zasifrovano ale existuji i ruzne jine metody jak tyto udaje zjisti treba keylogger atd.

Co my vlastne muzeme udelat je ze, pocitaci ke kteremu se chceme pripojit, poskytneme nas verejny klic a tim mu vlastne dame pro pristi prihlaseni vedet, ze jsme to my.

Mno a jak to vlastne probiha ? Pocitaci poskytneme nas public (verejny) klic on vezme nejaky data a podle tohoto klice je zasifruje a posle nam je (rika se tomu challenge) nas pocitac je rozsifruje a posle mu je zpatky... zde je jasne, ze jediny kdo to muze rozsifrovat jsme my, protoze jsme jedini kdo ma privatni-soukromy klic... pokud se tento zpusob vlastne nepovede tak se nas pocitac klasicky zepta na jmeno a heslo...

Tak ted z praxe nejdriv jak na to ve widlich :) budete potrebovat prog. jmenem puttygen nebo neco podobneho... mno ten pustite vyberete jaky z klicu chcete generovat a kliknete generate :) je to u nej myslim spojeny s pohybem mysi po obrazovce takze s ni budete muset parkrat pohnout, aby byl ten klic opravdu nahodny ... po vygenerovani se nam vlastne cely ukaze i s fingerprintem... zde si pote muzete urcit jakesi heslo (key passphrase), kterym se to jeste jednou zasifruje .. duvod? kdyby se nekdo dostal na vase konto a chtel by se pak prihlasit pomoci vaseho klice na jiny pocitac, tak by mu nekladl zadny odpor, kdezto ted bude muset vedet i toto "heslo", kterym se pri generovani klicu sifruje tajny klic ... mno a ted kdyz jste ho zadali, uz si staci jen ulozit jak privatni tak verejny klic.

Jakmile jsme tyto dva klice vygenerovali, tak nas verejny musime prenest na pocitac kam se bude chtit prihlasovat ... preneseme ho do ~/.ssh nebo neco podneho ... mno a ted ho pridame do souboru authorized_keys, pokud jsme ho pojmenovali treba "key" tak ho tam prekopcime jednoduchym prikazem cat key > ~/.ssh/autorized_keys ...

Takze ted kdyz se budeme chtit pripojit, tak nejdriv budeme muset nasemu klientovi rict, aby pouzival nas vygenerovany privatni klic, v pripade "meho" putty kliknete na auth/browse a najdete vas privat. klic date ok:) kdyz se budeme nyni pripojovat tak se siti preda akorat informace o tom jaky klic se ma pouzit, na odsifrovani kontrolnich dat a putty se nas zeptat na keyphrase pokud jsme tedy nejakou zvolili, aby se nas privat klic mohl pouzit ... cili siti se neprenesly zadne citlive udaje jako heslo a jmeno...

Kdyz budeme tyto klice generovat pod nejakym linuxem tak vam pomuze snad tahle mala tabulka:

SSH protokol	generovani	jmena
1	ssh-keygen -t rsa1	identity,identity.pub
2	ssh-keygen -t rsa	id_rsa,id_rsa.pub
2	ssh-keygen -t dsa	id_dsa,id_dsa.pub

jinak v nastaveni serveru ssh v configu pak mate radky HostKey cesta/ke/klici, pokud se rozhodnete ty klice menit nebo budete pridavat tak je samo musite zmenit/pridat i v tomto configuracnim souboru.

Sifra RSA a DSA se pouziva jen pri autentizaci a ne pri samotne praci, protoze je asymetricka (pouziva sifrovaci klice) = pomalejsi. Na prenos dat se pouzivaji jine napr Blowfish, Cast128 atd.. ktere sou symetricke. Muzete si vybrat da se to nastavit ve vesem klientovi teda aspon vetsinou.

SSH tunneling

O co jde? Asi hodne z vas uz tohle sluvko nekde zaslechlo... mno jde o vytvoreni kanalu/spojeni s nejakym jinym pocitacem, ktere bude sifrovano a muze byt pripojeno na jakykoliv jeho port a vas port... prakticke vyuziti je napr. kdyz mam poskytovatele pripojeni, ktery nedovoluje odesilat postu, cili 25 port je blokovan a co mi tedy muzeme udelat? vytvorit si prave tunel z mail.nekde.cz primo k nam na masinu treba na port 666 :) co se ted vlastne deje? na firewallu u meho poskytovatele to vypada jako bych mel pusteny ssh ale ja si spokojene posilam postu jedine co ted staci udelat je posilat postu na localhost (na 127.0.0.1) na port 666 a muzu posilat posty kolik je mi libo.

Jak na to? jednoduse v linu staci napsat:

```
ssh -L 666:mail.nekde.cz:25 mail.nekde.cz
```

ted sem prave vytvoril tunel ze stroje mail.nekde.cz z 25 portu na muj port 666. Lze se pak jednoduse overit jestli to funguje. Staci napsat napr. nestat -ln --tcp a vypiseme si vsechny otevrene porty na localu ... a jeste overit funkcnost staci telnet 127.0.0.1 666 a objevi se na nem uvodni obrazovka na stroji mail.nekde.cz :) Jinak pro windows existuje prog. zvany stun(n)el a ten vlastne tyto uplne nejjednodussi tunely vytvari, ale moc sem s nim nedelal... jen pro pripojeni na jisty irc server pac muj klient nepodporoval kryptovani...

Dalsi moznosti vyuziti kterou uvitaji hlavne lidi jako ja, kteri jsou za pocitacem s NATem a potebuji aby se nekdo z venci mohl pripojit na jejich komp. Jak to vlastne vypada? no prikaz vypada asi nejak takhle

```
ssh -R 5555:localhost:80 firewall.nekde.cz
```

5555 - na ktery port...
localhost:80 - co a kam budeme tunelovat...
firewall.nekde.cz - kam se budeme hlasit = pocitac s natem...

Ted uz je to mozna trosku jasnejsi prepinac R, znamena remote (vzdaleny) L je local (mistni). Vlastne staci nejakemu cloveku zvenci se pripojit na firewall.nekde.cz na port 5555 a uvidi nase stranky :) takhle se daji mimochodem i spoustet ftpka a hrat hry... vyuziti je urcite hodne... pozor ale u ftp musite nastavit pasiv jinak vam to nepujde, protoze pocitace by komunikovali na dvou portech na jednom by si vymenovali ridici data a na druhem normalni data nebo proste to co chcete prenaset ...

Vyhody SSH

- Zbezpecena komunikace (end to end)
- Hesla neputuji siti - pri pouziti te pokrocilejsi metody pouziti klicu
- Umi prenaset soubory scp, sftp atd...

Nevyhody

mno asi oproti nekryptovanym je jasne ze je trosku pomalejsi.. nejde udp cili vsechno spojeni musi byt pres tcp... a to bude asi vse :)

URL článku: https://security-portal.cz/clanky/short-brief-ssh

Odkazy:
[1] https://security-portal.cz/users/ilman
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/security